



Manuale dell'amministratore della piattaforma Business Intelligence

- SAP BusinessObjects Business Intelligence platform 4.1 Support Package 1

2013-09-19

Copyright

© 2013 SAP AG o una sua affiliata. Tutti i diritti riservati. Non è ammessa la riproduzione o la trasmissione del presente documento, né di alcuna delle sue parti, in qualsiasi formato o per qualsiasi fine senza l'esplicita autorizzazione di SAP AG. Le informazioni qui contenute sono soggette a modifica senza preavviso. Alcuni prodotti software commercializzati da SAP AG e dai suoi distributori contengono componenti software di proprietà di altri produttori di software. Le specifiche nazionali dei prodotti possono variare. Tali informazioni sono fornite da SAP AG e dalle sue affiliate ("Gruppo SAP") solo a scopo informativo, senza alcun fine illustrativo o di garanzia di qualsiasi natura; il Gruppo SAP non si assume alcuna responsabilità per eventuali errori od omissioni presenti nelle informazioni. Le uniche garanzie applicabili ai prodotti e ai servizi del Gruppo SAP sono quelle espressamente menzionate nelle apposite clausole contrattuali eventualmente previste per i singoli prodotti o servizi. Nessuna parte del presente documento è da interpretarsi come garanzia aggiuntiva. SAP e gli altri prodotti e servizi SAP qui menzionati, nonché i relativi loghi, sono marchi o marchi registrati di SAP AG in Germania e in altri Paesi. Per ulteriori informazioni e comunicazioni sui marchi consultare <http://www.sap.com/italy/about/company/legal/copyright/index.epx>.

2013-09-19

Sommario

Capitolo 1	Cronologia del documento.....	21
Capitolo 2	Introduzione.....	23
2.1	Informazioni sul manuale.....	23
2.1.1	Destinatari del manuale.....	23
2.1.2	Informazioni sulla piattaforma Business Intelligence	23
2.1.3	Variabili.....	24
2.1.4	Terminologia.....	24
2.2	Prima di iniziare.....	26
2.2.1	Concetti fondamentali.....	26
2.2.2	Strumenti di amministrazione principali.....	29
2.2.3	Attività principali.....	31
Capitolo 3	Architettura.....	35
3.1	Presentazione dell'architettura.....	35
3.1.1	Diagramma componenti.....	36
3.1.2	Livelli architettura.....	37
3.1.3	Database.....	38
3.1.4	Server, host e cluster.....	39
3.1.5	Server di applicazioni Web.....	39
3.1.6	Software Development Kit.....	41
3.1.7	Origini dati.....	43
3.1.8	Autenticazione e Single Sign On.....	44
3.1.9	Integrazione SAP.....	46
3.1.10	Controllo integrato delle versioni.....	47
3.1.11	Percorso di aggiornamento.....	47
3.2	Server, servizi, nodi e host.....	47
3.2.1	Modifiche al server dalla versione XI 3.1.....	49
3.2.2	Servizi.....	51
3.2.3	Categorie di servizio.....	59
3.2.4	Tipi di server.....	63
3.2.5	Server.....	69

3.3	Applicazioni client.....	71
3.3.1	Installato con gli Strumenti client della piattaforma SAP BusinessObjects Business Intelligence.....	72
3.3.2	Installato con la piattaforma SAP BusinessObjects Business Intelligence.....	76
3.3.3	Disponibile separatamente.....	77
3.3.4	Client di applicazioni Web.....	79
3.4	Workflow del processo.....	83
3.4.1	Avvio e autenticazione.....	83
3.4.2	Oggetti programma.....	85
3.4.3	Crystal Reports.....	86
3.4.4	Web Intelligence.....	91
3.4.5	Analisi.....	93
Capitolo 4	Configurazione guidata del sistema.....	95
4.1	Introduzione alla Configurazione guidata del sistema.....	95
4.2	Specifica dei prodotti utilizzati.....	95
4.3	Scelta di un modello di distribuzione.....	97
4.4	Specifica dei percorsi delle cartelle di dati.....	98
4.5	Verifica delle modifiche.....	100
4.6	File di registro e file di risposta.....	100
4.6.1	Utilizzo di un file di risposta.....	101
Capitolo 5	Gestione delle licenze.....	105
5.1	Gestione dei codici di licenza.....	105
5.1.1	Visualizzazione delle informazioni sulle licenze.....	105
5.1.2	Per aggiungere un codice di licenza.....	105
5.1.3	Visualizzazione dell'attività dell'account corrente.....	106
Capitolo 6	Gestione di utenti e gruppi.....	107
6.1	Panoramica della gestione dei server.....	107
6.1.1	Gestione utenti.....	107
6.1.2	Gestione gruppi.....	108
6.1.3	Tipi di autenticazione disponibili	109
6.2	Gestione di account Enterprise e generali.....	111
6.2.1	Per creare un account utente.....	111
6.2.2	Per modificare un account utente.....	112
6.2.3	Per eliminare un account utente.....	113
6.2.4	Per creare un nuovo gruppo.....	114
6.2.5	Per modificare le proprietà di un gruppo.....	114
6.2.6	Per visualizzare i membri del gruppo.....	114

6.2.7	Per aggiungere i sottogruppi.....	115
6.2.8	Per specificare l'appartenenza al gruppo.....	115
6.2.9	Per eliminare un gruppo.....	116
6.2.10	Aggiunta in blocco di utenti o gruppi di utenti.....	116
6.2.11	Per abilitare l'account Guest.....	117
6.2.12	Aggiunta di utenti ai gruppi.....	117
6.2.13	Modifica delle impostazioni password.....	119
6.2.14	Concessione del diritto di accesso a utenti e gruppi.....	121
6.2.15	Controllo dell'accesso alle caselle di posta in entrata dell'utente.....	121
6.2.16	Configurazione delle opzioni di BI Launch Pad.....	121
6.3	Gestione degli alias.....	125
6.3.1	Per creare un utente e aggiungere un alias di terze parti.....	125
6.3.2	Per creare un nuovo alias per un utente esistente.....	126
6.3.3	Per assegnare un alias da un altro utente.....	127
6.3.4	Eliminazione di un alias.....	127
6.3.5	Per disattivare un alias.....	128
Capitolo 7	Impostazione dei diritti.....	129
7.1	Funzionamento dei diritti nella piattaforma BI.....	129
7.1.1	Livelli di accesso.....	129
7.1.2	Impostazioni dei diritti avanzati.....	130
7.1.3	Ereditarietà.....	131
7.1.4	Diritti specifici del tipo.....	136
7.1.5	Determinazione dei diritti effettivi.....	137
7.2	Gestione delle impostazioni di protezione per gli oggetti nella CMC.....	138
7.2.1	Per visualizzare i diritti per un principale su un oggetto.....	139
7.2.2	Per assegnare principali a un elenco di controllo di accesso per un oggetto.....	140
7.2.3	Per modificare la protezione per un principale su un oggetto.....	140
7.2.4	Impostazione dei diritti su una cartella di livello superiore nella piattaforma BI.....	141
7.2.5	Controllo impostazioni di protezione per un principale.....	141
7.3	Utilizzo di livelli di accesso.....	144
7.3.1	Scelta tra i livelli di accesso Visualizza e Visualizza su richiesta.....	146
7.3.2	Per copiare un livello di accesso esistente.....	147
7.3.3	Per creare un nuovo livello di accesso.....	148
7.3.4	Per rinominare un livello di accesso.....	148
7.3.5	Per eliminare un livello di accesso.....	148
7.3.6	Per modificare i diritti in un livello di accesso.....	149
7.3.7	Analisi e relazione tra livelli di accesso e oggetti.....	150
7.3.8	Gestione dei livelli di accesso tra i siti.....	150
7.4	Interruzione dell'ereditarietà.....	151
7.4.1	Per disabilitare l'eredità.....	152

7.5	Utilizzo dei diritti per delegare l'amministrazione.....	153
7.5.1	Scelta tra le opzioni Modificare i diritti che gli utenti hanno sugli oggetti.....	155
7.5.2	Diritti del proprietario.....	156
7.6	Riepilogo delle indicazioni per l'amministrazione dei diritti.....	156

Capitolo 8

	Protezione della piattaforma BI.....	159
8.1	Panoramica della protezione	159
8.2	Pianificazione del ripristino d'emergenza.....	159
8.3	Raccomandazioni generali per la protezione della distribuzione.....	160
8.4	Configurazione della protezione per server di terze parti in bundle.....	161
8.5	Relazione di trust attiva.....	161
8.5.1	Token di accesso.....	161
8.5.2	Meccanismo dei ticket per la distribuzione della protezione.....	162
8.6	Sessioni e registrazione delle sessioni.....	163
8.6.1	Registrazione delle sessioni CMS.....	163
8.7	Protezione dell'ambiente.....	164
8.7.1	Da browser a server Web.....	164
8.7.2	Comunicazione tra il server Web e la piattaforma BI.....	164
8.8	Controllo delle modifiche alla configurazione della protezione	165
8.9	Controllo dell'attività sul Web.....	165
8.9.1	Protezione contro tentativi di accesso non autorizzati.....	165
8.9.2	Limitazioni relative alle password.....	166
8.9.3	Limitazioni relative all'accesso.....	166
8.9.4	Limitazioni per l'utente.....	166
8.9.5	Limitazioni all'account Guest.....	167
8.10	Estensioni di elaborazione.....	167
8.11	Panoramica della protezione dei dati della piattaforma BI.....	168
8.11.1	Modalità di protezione dell'elaborazione dei dati.....	168
8.12	Crittografia nella piattaforma BI.....	170
8.12.1	Utilizzo delle chiavi cluster.....	171
8.12.2	Responsabili crittografia.....	174
8.12.3	Gestione delle chiavi di crittografia in CMC.....	175
8.13	Configurazione dei server per SSL.....	180
8.13.1	Creazione di file di chiavi e certificati.....	180
8.13.2	Impostazione di SSL quando il certificato viene gestito da un'autorità di certificazione.....	182
8.13.3	Configurazione del protocollo SSL.....	184
8.14	Informazioni sulla comunicazione tra componenti della piattaforma BI	189
8.14.1	Panoramica dei server della piattaforma BI e delle porte di comunicazione.....	189
8.14.2	Comunicazione tra componenti della piattaforma BI	191
8.15	Configurazione della piattaforma BI per i firewall.....	199
8.15.1	Per configurare il sistema per i firewall.....	200

8.15.2	Debug di una distribuzione con firewall.....	203
8.16	Esempi di scenari di firewall tipici.....	204
8.16.1	Esempio: livello applicazione distribuito su una rete separata.....	204
8.16.2	Esempio: livello thick client e database separato dai server della piattaforma BI mediante un firewall.....	207
8.17	Impostazioni firewall per gli ambienti integrati.....	209
8.17.1	Linee guida specifiche del firewall per Oracle EBS.....	210
8.17.2	Configurazione del firewall per l'integrazione con JD Edwards EnterpriseOne.....	212
8.17.3	Linee guida specifiche del firewall per Oracle EBS.....	213
8.17.4	Configurazione del firewall per l'integrazione con PeopleSoft Enterprise	214
8.17.5	Configurazione del firewall per l'integrazione con Siebel.....	216
8.18	Piattaforma BI e server proxy inverso	218
8.18.1	Server reverse proxy supportati	218
8.18.2	Distribuzione delle applicazioni Web	218
8.19	Configurazione di server proxy inverso per applicazioni Web della piattaforma BI.....	219
8.19.1	Istruzioni dettagliate per la configurazione di server reverse proxy.....	219
8.19.2	Per configurare il server reverse proxy.....	220
8.19.3	Per configurare il server proxy inverso Apache 2.2 per la piattaforma BI	220
8.19.4	Per configurare il server proxy inverso WebSEAL 6.0 per la piattaforma BI	220
8.19.5	Per configurare Microsoft ISA 2006 per la piattaforma BI	221
8.20	Configurazione speciale per la piattaforma BI in distribuzioni di proxy inversi.....	223
8.20.1	Abilitazione del proxy inverso per Servizi Web.....	223
8.20.2	Abilitazione del percorso principale per i cookie di sessione per ISA 2006.....	226
8.20.3	Abilitazione di reverse proxy per SAP BusinessObjects Live Office.....	228
Capitolo 9	Autenticazione.....	231
9.1	Opzioni di autenticazione nella piattaforma BI.....	231
9.1.1	Autenticazione principale.....	232
9.1.2	Plug-in di protezione.....	233
9.1.3	Single Sign On alla piattaforma BI.....	234
9.2	autenticazione Enterprise.....	236
9.2.1	Presentazione dell'autenticazione Enterprise.....	236
9.2.2	Impostazioni di autenticazione Enterprise.....	236
9.2.3	Modifica delle impostazioni del database.....	237
9.2.4	Abilitazione dell'Autenticazione affidabile.....	239
9.2.5	Configurazione dell'Autenticazione affidabile per l'applicazione Web.....	241
9.3	Autenticazione LDAP.....	250
9.3.1	Utilizzo dell'autenticazione LDAP.....	251
9.3.2	Configurazione dell'autenticazione LDAP.....	253
9.3.3	Mappatura di gruppi LDAP.....	263
9.4	Autenticazione Windows AD.....	273

9.4.1	Utilizzo dell'autenticazione Windows AD.....	273
9.4.2	Preparazione del controller di dominio.....	274
9.4.3	Configurazione dell'autenticazione AD nella CMC.....	275
9.4.4	Configurazione del servizio della piattaforma BI per l'esecuzione del SIA.....	282
9.4.5	Configurazione del server di applicazioni Web per l'autenticazione AD.....	284
9.4.6	Impostazione del Single Sign On	292
9.4.7	Risoluzione dei problemi relativi all'autenticazione Windows AD.....	306
9.5	Autenticazione SAP.....	308
9.5.1	Configurazione dell'autenticazione SAP	308
9.5.2	Creazione di un account utente per la piattaforma BI.....	309
9.5.3	Connessione ai sistemi di autorizzazione SAP.....	310
9.5.4	Impostazione delle opzioni di autenticazione SAP.....	312
9.5.5	Importazione dei ruoli SAP	317
9.5.6	Configurazione di Secure Network Communication (SNC).....	321
9.5.7	Impostazione del Single Sign On nel sistema SAP.....	334
9.5.8	Configurazione di SSO per SAP Crystal Reports e SAP NetWeaver.....	338
9.6	Autenticazione PeopleSoft.....	339
9.6.1	Panoramica.....	339
9.6.2	Abilitazione dell'autenticazione PeopleSoft Enterprise.....	339
9.6.3	Mappatura di ruoli PeopleSoft alla piattaforma BI.....	340
9.6.4	Pianificazione degli aggiornamenti utente.....	344
9.6.5	Utilizzo del Ponte di protezione PeopleSoft.....	345
9.7	Autenticazione JD Edwards.....	356
9.7.1	Panoramica.....	356
9.7.2	Abilitazione dell'autenticazione JD Edwards EnterpriseOne.....	356
9.7.3	Mappatura dei ruoli JD Edwards EnterpriseOne alla piattaforma BI.....	357
9.7.4	Pianificazione degli aggiornamenti utente.....	360
9.8	Autenticazione Siebel.....	362
9.8.1	Abilitazione dell'autenticazione Siebel.....	362
9.8.2	Mappatura di ruoli alla piattaforma BI.....	363
9.8.3	Pianificazione degli aggiornamenti utente.....	366
9.9	Autenticazione Oracle EBS.....	368
9.9.1	Abilitazione dell'autenticazione Oracle EBS.....	368
9.9.2	Mappatura dei ruoli Oracle E-Business Suite alla piattaforma BI.....	369
9.9.3	Eliminazione mappatura ruoli	373
9.9.4	Personalizzazione dei diritti per gruppi e utenti Oracle EBS mappati	373
9.9.5	Configurazione del Single Sign On (SSO) per SAP Crystal Reports e Oracle EBS.....	375
Capitolo 10	Amministrazione del server.....	377
10.1	Utilizzo dell'area di gestione Server della console CMC.....	377
10.2	Gestione dei server mediante gli script in Windows	380

10.3	Gestione dei server in Unix	381
10.4	Visualizzazione e modifica dello stato del server.....	381
10.4.1	Visualizzazione dello stato dei server.....	381
10.4.2	Avvio, arresto e riavvio dei server.....	383
10.4.3	Arresto di Central Management Server.....	385
10.4.4	Abilitazione e disabilitazione dei server.....	386
10.5	Aggiunta, duplicazione o eliminazione di server.....	387
10.5.1	Aggiunta, duplicazione ed eliminazione di server.....	387
10.6	Cluster di Central Management Server.....	391
10.6.1	Cluster di Central Management Server.....	391
10.7	Gestione di gruppi di server.....	395
10.7.1	Creazione di un gruppo di server.....	396
10.7.2	Utilizzo di sottogruppi di server.....	397
10.7.3	Modifica dell'appartenenza di gruppo di un server.....	398
10.7.4	Accesso degli utenti a server e gruppi di server.....	399
10.8	Configurazione degli Adaptive Processing Server per i sistemi di produzione.....	400
10.9	Valutazione delle prestazioni del sistema.....	401
10.9.1	Monitoraggio dei server della piattaforma BI.....	401
10.9.2	Analisi delle specifiche dei server.....	401
10.9.3	Visualizzazione delle specifiche del sistema.....	402
10.9.4	Registrazione dell'attività dei server.....	402
10.10	Configurazione delle impostazioni server.....	403
10.10.1	Per modificare le proprietà di un server.....	404
10.10.2	Applicazione delle impostazioni dei servizi a più server.....	404
10.10.3	Utilizzo di modelli di configurazione.....	405
10.11	Configurazione delle impostazioni di rete del server.....	407
10.11.1	Opzioni dell'ambiente di rete.....	408
10.11.2	Opzioni di identificazione host del server.....	408
10.11.3	Configurazione di un computer multi-home.....	410
10.11.4	Configurazione dei numeri di porta.....	413
10.12	Gestione dei nodi.....	416
10.12.1	Utilizzo dei nodi.....	416
10.12.2	Aggiunta di un nuovo nodo.....	419
10.12.3	Ricreazione di un nodo.....	423
10.12.4	Eliminazione di un nodo.....	427
10.12.5	Ridenominazione di un nodo.....	429
10.12.6	Spostamento di un nodo.....	430
10.12.7	Parametri script.....	434
10.12.8	Aggiunta di dipendenze dei server Windows.....	439
10.12.9	Modifica delle credenziali utente per un nodo.....	440
10.13	Assegnazione di un nuovo nome a un computer in una distribuzione della piattaforma BI.....	441

10.13.1	Modifica dei nomi dei cluster.....	441
10.13.2	Modifica di indirizzi IP.....	441
10.13.3	Assegnazione di nuovi nomi ai computer.....	443
10.14	Utilizzo di librerie a 32 e a 64 bit con la piattaforma BI.....	447
10.15	Gestione dei segnaposto per server e nodi.....	448
10.15.1	Visualizzazione dei segnaposto server.....	448
10.15.2	Visualizzazione e modifica dei segnaposto per un nodo.....	448
Capitolo 11	Gestione dei database CMS (Central Management Server).....	451
11.1	Gestione delle connessioni di database di sistema CMS.....	451
11.1.1	Selezione di SQL Anywhere come database CMS.....	451
11.1.2	Selezione di SAP HANA come database CMS.....	452
11.2	Selezione di un database CMS nuovo o esistente.....	453
11.2.1	Selezione di un database CMS nuovo o esistente in Windows.....	454
11.2.2	Per selezionare un database CMS nuovo o esistente in UNIX.....	455
11.3	Ricreazione del database di sistema CMS.....	455
11.3.1	Nuova creazione del database di sistema CMS in Windows.....	456
11.3.2	Per creare nuovamente il database di sistema CMS in UNIX.....	457
11.4	Copia dei dati da un database di sistema CMS a un altro.....	457
11.4.1	Preparazione per la copia di un database di sistema CMS.....	458
11.4.2	Copia di un database di sistema CMS in Windows.....	458
11.4.3	Copia di dati da un database di sistema CMS in Unix.....	459
Capitolo 12	Gestione dei server del contenitore di applicazioni Web (WACS).....	461
12.1	WACS.....	461
12.1.1	Server contenitore applicazioni Web (WACS).....	461
12.1.2	Aggiunta o rimozione di WACS aggiuntivi alla distribuzione.....	464
12.1.3	Aggiunta o rimozione di servizi dal server WACS.....	468
12.1.4	Configurazione di HTTPS/SSL.....	469
12.1.5	Metodi di autenticazione supportati.....	473
12.1.6	Configurazione di AD Kerberos per server WACS	473
12.1.7	Configurazione del Single Sign On AD Kerberos	480
12.1.8	Configurazione di servizi Web RESTful.....	482
12.1.9	WACS e ambiente IT.....	491
12.1.10	Configurazione delle proprietà delle applicazioni Web.....	494
12.1.11	Risoluzione dei problemi.....	495
12.1.12	Proprietà del server WACS.....	499
Capitolo 13	Backup e ripristino del sistema.....	501
13.1	Panoramica di backup e ripristino.....	501

13.2	Terminologia.....	501
13.3	Casi d'uso per il backup e il ripristino.....	503
13.4	Backup.....	505
13.4.1	Backup dell'intero sistema.....	506
13.4.2	Backup delle impostazioni server.....	509
13.4.3	Backup del contenuto BI.....	512
13.5	Ripristino del sistema.....	512
13.5.1	Ripristino dell'intero sistema.....	513
13.5.2	Ripristino delle impostazioni server.....	518
13.5.3	Ripristino del contenuto BI.....	521
13.6	Script BackupCluster e RestoreCluster.....	521
Capitolo 14	Copia della distribuzione della piattaforma BI.....	525
14.1	Panoramica della copia del sistema.....	525
14.2	Terminologia.....	525
14.3	Casi di utilizzo per la copia del sistema.....	526
14.4	Pianificazione della copia del sistema.....	527
14.5	Considerazioni e limitazioni.....	528
14.6	Procedura di copia del sistema.....	530
14.6.1	Per eseguire l'esportazione da un sistema di origine.....	530
14.6.2	Per eseguire l'importazione in un sistema di destinazione.....	535
Capitolo 15	Gestione delle versioni.....	539
15.1	Gestione di diverse versioni delle risorse BI	539
15.2	Utilizzo dell'opzione Impostazioni sistema gestione versioni.....	540
15.2.1	Impostazione del sistema di gestione delle versioni ClearCase in Windows.....	541
15.2.2	Impostazione del sistema di gestione delle versioni ClearCase in Unix.....	541
15.3	Confronto tra versioni diverse dello stesso processo.....	542
15.4	Aggiornamento del contenuto di Subversion.....	542
Capitolo 16	Promotion Management.....	545
16.1	Promotion Management.....	545
16.1.1	Panoramica.....	545
16.1.2	Funzionalità.....	545
16.1.3	Diritti di accesso per l'applicazione.....	546
16.1.4	Supporto di WinAD in Promotion Management.....	547
16.2	Introduzione allo strumento Promotion Management.....	547
16.2.1	Accesso all'applicazione Promotion Management.....	547
16.2.2	Componenti dell'interfaccia utente.....	548
16.2.3	Utilizzo delle opzioni di impostazione.....	550

16.3	Utilizzo dello strumento Promotion Management.....	556
16.3.1	Creazione ed eliminazione di cartelle.....	557
16.3.2	Per creare un processo.....	558
16.3.3	Per creare un nuovo processo copiando un processo esistente	560
16.3.4	Per eseguire la ricerca di un processo.....	561
16.3.5	Per modificare un processo.....	562
16.3.6	Per aggiungere un infoobject a un processo.....	562
16.3.7	Per gestire le dipendenze di un processo.....	563
16.3.8	Per eseguire la ricerca di oggetti dipendenti	564
16.3.9	Per promuovere un processo quando i repository sono connessi.....	565
16.3.10	Promozione di un processo mediante un file BIAR.....	567
16.3.11	Per pianificare la promozione di un processo.....	570
16.3.12	Per visualizzare la cronologia di un processo.....	571
16.3.13	Per eseguire il rollback di un processo.....	572
16.4	Per gestire versioni diverse di un infoobject.....	575
16.4.1	Diritti di accesso dell'applicazione Gestione delle versioni	576
16.4.2	Backup e ripristino di file Subversion.....	577
16.5	Utilizzo dell'opzione della riga di comando.....	578
16.5.1	Per eseguire lo strumento da riga di comando in Windows.....	578
16.5.2	Per eseguire lo strumento da riga di comando in UNIX.....	579
16.5.3	Parametri degli strumenti della riga di comando.....	580
16.5.4	File delle proprietà di esempio.....	587
16.6	Utilizzo di Enhanced Change and Transport System.....	588
16.6.1	Prerequisiti.....	589
16.6.2	Per configurare la piattaforma BI e l'integrazione con CTS+.....	589
16.6.3	Per promuovere un processo utilizzando CTS.....	597
Capitolo 17	Differenza visiva.....	601
17.1	Differenza visiva nello strumento Promotion Management.....	601
17.1.1	Confronto di oggetti o file mediante la differenza visiva.....	602
17.1.2	Confronto di oggetti o file nel sistema di gestione delle versioni.....	603
17.1.3	Pianificazione del confronto.....	604
Capitolo 18	Gestione delle applicazioni.....	607
18.1	Gestione delle applicazioni mediante CMC.....	607
18.1.1	Panoramica.....	607
18.1.2	Impostazioni comuni per le applicazioni.....	608
18.1.3	Impostazioni specifiche dell'applicazione.....	609
18.2	Gestione delle applicazioni mediante le proprietà BOE.war	652
18.2.1	File WAR BOE.....	652

18.3	Personalizzazione dei punti di ingresso per l'accesso a BI Launch Pad e OpenDocument.....	663
18.3.1	Percorsi dei file BI Launch Pad e OpenDocument.....	663
18.3.2	Per definire una pagina di accesso personalizzata.....	665
18.3.3	Aggiunta di un'autenticazione affidabile all'accesso.....	665
18.4	Personalizzazione dell'interfaccia Web Intelligence.....	666
18.4.1	Scheda Funzionalità.....	667
18.4.2	Scheda Elementi dell'interfaccia utente.....	667
18.4.3	Per personalizzare l'aspetto dell'interfaccia Web Intelligence.....	678
Capitolo 19	Gestione di connessioni e universi.....	681
19.1	Gestione delle connessioni.....	681
19.1.1	Eliminazione di una connessione universo.....	681
19.2	Gestione degli universi.....	682
19.2.1	Eliminazione di universi.....	682
Capitolo 20	Monitoraggio.....	685
20.1	Informazioni sul monitoraggio.....	685
20.2	Termini relativi al monitoraggio.....	685
20.2.1	Architettura.....	687
20.3	Configurazione del supporto di database per il monitoraggio	688
20.3.1	Configurazione per l'utilizzo del database Derby.....	689
20.3.2	Configurazione per l'utilizzo del database di controllo.....	689
20.4	Proprietà di configurazione.....	696
20.4.1	URL dell'endpoint JMX.....	701
20.4.2	Autenticazione HTTPS per le probe di monitoraggio.....	702
20.4.3	Crittografia delle password per le probe.....	702
20.5	Integrazione con altre applicazioni.....	703
20.5.1	Integrazione dell'applicazione di monitoraggio con IBM Tivoli.....	703
20.5.2	Integrazione dell'applicazione di monitoraggio con SAP Solution Manager	706
20.6	Supporto cluster per il server di monitoraggio.....	706
20.7	Risoluzione dei problemi.....	707
20.7.1	Cruscotto.....	707
20.7.2	Avvisi.....	707
20.7.3	Elenco di controlli.....	708
20.7.4	Probe.....	708
20.7.5	Metriche.....	709
20.7.6	Grafico.....	709
Capitolo 21	Controllo.....	711
21.1	Panoramica.....	711

21.2	Pagina di controllo CMC.....	717
21.2.1	Stato del controllo.....	717
21.2.2	Configurazione del controllo eventi.....	719
21.2.3	Impostazioni di configurazione dell'archivio dati di controllo (ADS).....	721
21.3	Eventi di controllo.....	723
21.3.1	Eventi di controllo e dettagli.....	734

Capitolo 22

Ricerca piattaforma.....753

22.1	Informazioni sul servizio di ricerca piattaforma.....	753
22.1.1	SDK applicazione di ricerca piattaforma.....	753
22.1.2	Ambiente cluster.....	754
22.2	Impostazione della ricerca piattaforma.....	754
22.2.1	Distribuzione di OpenSearch.....	754
22.2.2	Configurazione del proxy inverso.....	756
22.2.3	Configurazione delle proprietà dell'applicazione nella CMC.....	757
22.3	Utilizzo della ricerca piattaforma.....	763
22.3.1	Indicizzazione del contenuto nel repository CMS.....	763
22.3.2	Elenco errori di indicizzazione	764
22.3.3	Risultati della ricerca.....	764
22.4	Integrazione del servizio di ricerca piattaforma con la funzionalità di ricerca di SAP NetWeaver Enterprise.....	771
22.4.1	Creazione di un connettore nella funzionalità di ricerca di SAP NetWeaver Enterprise	772
22.4.2	Importazione del ruolo di un utente nella piattaforma BI.....	773
22.5	Ricerca dalla funzionalità di ricerca di NetWeaver Enterprise.....	773
22.6	Controllo.....	774
22.7	Risoluzione dei problemi.....	775
22.7.1	Riparazione automatica.....	775
22.7.2	Scenari di problemi.....	775

Capitolo 23

Federazione.....779

23.1	Federation.....	779
23.2	Termini correlati a Federation.....	780
23.3	Gestione dei diritti di protezione.....	782
23.3.1	Diritti richiesti sul sito di origine.....	782
23.3.2	Diritti richiesti nel sito di destinazione.....	783
23.3.3	Diritti specifici di Federation.....	784
23.3.4	Replica della protezione per un oggetto.....	786
23.3.5	Replica della protezione mediante i livelli di accesso.....	787
23.4	Opzioni di tipi e modalità di replica.....	787
23.4.1	Replica unilaterale	788

23.4.2	Replica bilaterale	788
23.4.3	Aggiornamento da origine o da destinazione.....	789
23.5	Replica di utenti e gruppi di terze parti.....	790
23.6	Replica di universi e connessioni agli universi.....	791
23.7	Gestione degli elenchi di replica.....	792
23.7.1	Creazione di elenchi di replica.....	793
23.7.2	Modifica degli elenchi di replica.....	795
23.8	Gestione delle connessioni remote.....	796
23.8.1	Creazione di connessioni remote.....	797
23.8.2	Modifica delle connessioni remote.....	799
23.9	Gestione dei processi di replica.....	799
23.9.1	Creazione di processi di replica.....	800
23.9.2	Pianificazione dei processi di replica.....	802
23.9.3	Modifica dei processi di replica.....	803
23.9.4	Visualizzazione di un registro dopo un processo di replica.....	803
23.10	Gestione dell'eliminazione di oggetti.....	804
23.10.1	Modalità di utilizzo dell'eliminazione di oggetti.....	804
23.10.2	Limiti dell'eliminazione di oggetti.....	805
23.10.3	Frequenza di eliminazione degli oggetti.....	806
23.11	Gestione del rilevamento e della risoluzione dei conflitti.....	807
23.11.1	Risoluzione di conflitti di replica unilaterale.....	807
23.11.2	Risoluzione conflitti di replica bilaterale.....	809
23.12	Utilizzo dei Servizi Web in Federation.....	812
23.12.1	Variabili di sessione	812
23.12.2	Memorizzazione di file nella cache	812
23.12.3	Distribuzione personalizzata	813
23.13	Pianificazione remota e istanze eseguite localmente.....	814
23.13.1	Pianificazione remota.....	814
23.13.2	Istanze eseguite localmente.....	816
23.13.3	Condivisione di istanze.....	816
23.14	Importazione e promozione di contenuto replicato.....	817
23.14.1	Importazione di contenuto replicato.....	817
23.14.2	Importazione del contenuto replicato e continuazione della replica	818
23.14.3	Promozione del contenuto da un ambiente di test.....	819
23.14.4	Puntamento a un sito di destinazione.....	819
23.15	Procedure consigliate.....	820
23.15.1	Limitazioni della release corrente.....	823
23.15.2	Risoluzione dei messaggi di errore.....	824
Capitolo 24	Configurazioni supplementari per gli ambienti ERP.....	827
24.1	Configurazioni per l'integrazione di SAP NetWeaver.....	827

24.1.1	Integrazione con SAP Netweaver Business Warehouse (BW).....	827
24.2	Configurazione per l'integrazione JD Edwards.....	879
24.2.1	Configurazione del Single Sign On (SSO) per SAP Crystal Reports.....	879
24.2.2	Configurazione delle integrazioni di Secure Socket Layer per JD Edwards	880
24.3	Configurazione per l'integrazione PeopleSoft Enterprise.....	881
24.3.1	Configurazione di Single Sign-On (SSO) per SAP Crystal Reports e PeopleSoft Enterprise..	882
24.3.2	Configurazione per le comunicazioni Secure Sockets Layer.....	883
24.3.3	Regolazione delle prestazioni per i sistemi PeopleSoft.....	885
24.4	Configurazione per l'integrazione Siebel.....	886
24.4.1	Configurazione di Siebel per l'integrazione con la piattaforma SAP BusinessObjects Business Intelligence.....	886
24.4.2	Creazione della voce di menu Crystal Reports.....	887
24.4.3	Contextual Awareness.....	889
24.4.4	Configurazione di Single Sign-On (SSO) per SAP Crystal Reports e Siebel.....	891
24.4.5	Configurazione per le comunicazioni Secure Sockets Layer.....	892
Capitolo 25	Gestione e configurazione dei registri.....	895
25.1	Registrazione delle analisi dei componenti	895
25.2	Livelli del registro di analisi.....	895
25.3	Configurazione dell'analisi per i server.....	896
25.3.1	Per impostare il livello del registro nella console CMC.....	897
25.3.2	Per impostare il livello del registro per più server nella console CMC.....	897
25.3.3	Per configurare l'analisi del server tramite il file BO_trace.ini.....	898
25.4	Configurazione dell'analisi per le applicazioni Web.....	900
25.4.1	Impostazione del livello del registro di analisi delle applicazioni Web nella CMC.....	901
25.4.2	Per configurare le impostazioni di analisi utilizzando il file BO_trace.ini.....	901
25.5	Configurazione dell'analisi per Upgrade Management Tool.....	906
25.5.1	Configurazione dell'analisi per Upgrade Management Tool.....	906
25.6	Configurazione dell'analisi per le applicazioni client della piattaforma BI.....	906
Capitolo 26	Integrazione con SAP Solution Manager.....	909
26.1	Panoramica sull'integrazione.....	909
26.2	Elenco di controllo dell'integrazione di SAP Solution Manager.....	909
26.3	Gestione della registrazione di System Landscape Directory.....	910
26.3.1	Registrazione della piattaforma BI in System Landscape.....	911
26.3.2	Quando viene attivata la registrazione SLD?.....	912
26.3.3	Registrazione della connettività SLD	912
26.4	Gestione degli agenti di Solution Manager Diagnostics.....	913
26.4.1	Panoramica di Solution Manager Diagnostics (SMD).....	913
26.4.2	Utilizzo degli agenti SMD.....	913

26.4.3	Account utente SMAAdmin.....	914
26.5	Gestione della strumentazione delle prestazioni.....	915
26.5.1	Strumentazione delle prestazioni per la piattaforma BI.....	915
26.5.2	Impostazione della strumentazione delle prestazioni per la piattaforma BI.....	915
26.5.3	Strumentazione delle prestazioni per il livello Web.....	917
26.5.4	File di registro di strumentazione	917
26.6	Analisi con SAP Passport.....	917
Capitolo 27	Amministrazione della riga di comando.....	919
27.1	Script UNIX.....	919
27.1.1	Utilità per gli script.....	919
27.1.2	Modelli di script.....	924
27.1.3	Script utilizzati nella piattaforma BI.....	925
27.2	Script Windows.....	926
27.2.1	ccm.exe.....	926
27.3	Righe di comando server.....	930
27.3.1	Panoramica sulle righe di comando.....	930
27.3.2	Opzioni standard per tutti i server.....	931
27.3.3	Central Management Server.....	932
27.3.4	Server di elaborazione Crystal Reports e Crystal Reports Cache Server.....	933
27.3.5	Server di elaborazione di Dashboards e Server cache di Dashboards.....	934
27.3.6	Job Server.....	936
27.3.7	Adaptive Processing Server.....	937
27.3.8	Report Application Server.....	937
27.3.9	Server di elaborazione Web Intelligence.....	940
27.3.10	Input e Output File Repository Server.....	941
27.3.11	Event Server.....	943
Capitolo 28	Repository diagnostic tool	945
28.1	Panoramica dello Strumento di diagnostica del repository.....	945
28.2	Utilizzo dello strumento di diagnostica del repository.....	946
28.2.1	Per utilizzare lo strumento Repository Diagnostic Tool.....	946
28.2.2	Parametri di Repository Diagnostic Tool.....	947
28.3	Incoerenze tra CMS e FRS.....	954
28.4	Incoerenze nei metadati CMS.....	955
Capitolo 29	Appendice sui diritti.....	959
29.1	Appendice sui diritti.....	959
29.2	Diritti generali.....	959
29.3	Diritti per tipi di oggetti specifici.....	962

29.3.1	Diritti sulla cartella.....	962
29.3.2	Categorie.....	962
29.3.3	Documenti Desktop Intelligence.....	963
29.3.4	Note.....	965
29.3.5	Report Crystal.....	966
29.3.6	Documenti Web Intelligence.....	966
29.3.7	Utenti e gruppi.....	967
29.3.8	Livelli di accesso.....	970
29.3.9	Diritti sugli universi (.unv)	970
29.3.10	Diritti sugli universi (.unx)	972
29.3.11	Livelli di accesso agli oggetti universo.....	973
29.3.12	Diritti di connessione.....	974
29.3.13	Applicazioni.....	976

Capitolo 30 **Appendice sulle proprietà dei server.....993**

30.1	Informazioni sull'appendice sulle proprietà dei server.....	993
30.1.1	Proprietà comuni dei server.....	993
30.1.2	Proprietà dei servizi principali.....	996
30.1.3	Proprietà dei servizi di connettività.....	1011
30.1.4	Proprietà dei servizi Crystal Reports.....	1016
30.1.5	Proprietà dei servizi Analysis.....	1026
30.1.6	Proprietà dei servizi Data Federation.....	1028
30.1.7	Proprietà dei servizi di Web Intelligence.....	1028
30.1.8	Proprietà dei servizi di Dashboards.....	1037

Capitolo 31 **Appendice sulle metriche server.....1041**

31.1	Informazioni sull'appendice sulle metriche server.....	1041
31.1.1	Metriche server comuni	1042
31.1.2	Metriche del Central Management Server.....	1044
31.1.3	Metriche di Connection Server.....	1048
31.1.4	Metriche di Event Server.....	1049
31.1.5	Metriche del File Repository Server.....	1050
31.1.6	Metriche di Adaptive Processing Server.....	1050
31.1.7	Metriche del server del contenitore di applicazioni Web.....	1056
31.1.8	Metriche di Adaptive Job Server.....	1057
31.1.9	Metriche di Crystal Reports Server.....	1059
31.1.10	Metriche del server Web Intelligence.....	1062
31.1.11	Metriche server di Dashboards.....	1064

Capitolo 32	Appendice: segnaposto per server e nodi.....	1067
32.1	Segnaposto server e nodo.....	1067
Capitolo 33	Appendice: schema archivio dati di controllo.....	1079
33.1	Panoramica.....	1079
33.2	Diagramma schema.....	1079
33.3	Tabelle dell'archivio dati di controllo.....	1079
Capitolo 34	Appendice sullo schema dei database di monitoraggio.....	1091
34.1	Schema del database di tendenza.....	1091
Capitolo 35	Appendice sul foglio di lavoro della copia di sistema.....	1095
35.1	Foglio di lavoro della copia del sistema.....	1095
Appendice A	Ulteriori informazioni.....	1097
Indice		1099

Cronologia del documento

La seguente tabella contiene una panoramica delle modifiche principali apportate al documento.

Versione	Data	Descrizione
Piattaforma SAP BusinessObjects Business Intelligence 4.1	Maggio 2013	Prima versione di questo documento.
Piattaforma SAP BusinessObjects Business Intelligence 4.1 pacchetto di supporto 1	Agosto 2013	<ul style="list-style-type: none">• Il capitolo “Promotion Management” è stato aggiornato.• Il capitolo “Gestione delle licenze” è stato aggiornato.• Altre correzioni e aggiornamenti minori.

Introduzione

2.1 Informazioni sul manuale

In questo manuale vengono fornite informazioni e procedure per la distribuzione e la configurazione della piattaforma SAP BusinessObjects Business Intelligence (la "piattaforma BI"). Le procedure sono fornite per le attività comuni. Le informazioni concettuali e i dettagli tecnici sono forniti per tutti gli argomenti avanzati.

Per informazioni sull'installazione di questo prodotto, consultare il *Manuale d'installazione della piattaforma SAP BusinessObjects Business Intelligence*.

2.1.1 Destinatari del manuale

Il manuale illustra le procedure di distribuzione e configurazione della piattaforma BI. È consigliabile consultarlo se si intende eseguire una qualsiasi delle attività seguenti:

- pianificare la prima distribuzione
- configurare la prima distribuzione
- apportare modifiche significative all'architettura di una distribuzione esistente
- migliorare le prestazioni del sistema.

Questo manuale è destinato agli amministratori di sistema responsabili della configurazione, della gestione e della manutenzione di un'installazione della piattaforma BI. La dimestichezza con il sistema operativo e l'ambiente di rete è utile, così come una generale comprensione della gestione dei server delle applicazioni Web e delle tecnologie relative agli script. Tuttavia, per fornire assistenza a tutti i livelli di esperienza amministrativa, questo manuale mira a offrire informazioni complementari e concettuali sufficienti a chiarire tutte le funzionalità e attività amministrative.

2.1.2 Informazioni sulla piattaforma Business Intelligence

La piattaforma BI è una soluzione flessibile e scalabile per la distribuzione di informazioni agli utenti finali in più formati, inclusi cruscotti e report interattivi, mediante un'applicazione Web: intranet, extranet, Internet o portale aziendale. La piattaforma BI è una suite integrata per la creazione di report, l'analisi e la distribuzione di informazioni, che offre una soluzione ideale per aumentare la produttività degli utenti finali e ridurre l'onere delle attività amministrative. Sia che venga utilizzata per la distribuzione di report settimanali sulle vendite, per la fornitura ai clienti di offerte di servizi personalizzati o per l'integrazione di informazioni cruciali nei portali aziendali, la piattaforma BI garantisce sempre vantaggi tangibili che riguardano l'intera azienda e non solo.

2.1.3 Variabili

In questo manuale vengono utilizzate le seguenti variabili.

Variabile	Descrizione
<i>INSTALLDIR</i>	La directory in cui viene installata la piattaforma BI. Su un computer Windows, la directory predefinita è <code>C:\Programmi (x86)\SAP BusinessObjects\</code> .
<i>DIRPLATFORM64</i>	Nome del sistema operativo Unix. I valori accettabili sono: <ul style="list-style-type: none"> • <code>aix_rs6000_64</code> • <code>linux_x64</code> • <code>solaris_sparcv9</code> • <code>hpux_ia64</code>
<i>DIRSCRIPT</i>	La directory in cui si trovano gli script di amministrazione della piattaforma BI. In Windows la directory è <code>DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts</code> . In Unix la directory è <code>DIRINSTALL/sap_bobj/enterprise_xi40/DIRPLATFORM64/scripts</code> .

2.1.4 Terminologia

In questa documentazione relativa alla piattaforma BI vengono utilizzati i termini seguenti:

aggiornamento

Tutte le attività di pianificazione, preparazione, migrazione e post-elaborazione necessarie per completare un processo di migrazione.

Archivio dati di controllo (ADS)

Il database utilizzato per la memorizzazione dei dati di controllo.

chiave cluster

Utilizzata per decrittografare le chiavi nel database CMS. È possibile modificare la chiave cluster utilizzando CCM, ma non è possibile reimpostarla analogamente a una password. Si tratta di una chiave di crittografia con la quale viene crittografato il contenuto e pertanto è estremamente importante non perderla.

cluster

Un cluster è costituito da due o più server CMS (Central Management Server) che operano insieme e utilizzano un singolo database CMS.

clustering

Indica la creazione di un cluster. Ad esempio, per creare un cluster:

1. Installare un CMS e un database CMS nel computer.
2. Installare un CMS nel computer B.
3. Fare in modo che il CMS sul computer B punti al database CMS sul computer A.

CMS

Central Management Server.

componenti aggiuntivi

Prodotti che interagiscono con la piattaforma BI ma dispongono del proprio programma di installazione, ad esempio SAP BusinessObjects Explorer.

computer

Il software della piattaforma BI viene installato in un computer.

database CMS

Il database utilizzato dal CMS per memorizzare informazioni sulla piattaforma BI.

database in bundle; server di applicazioni Web in bundle

Il database o il server di applicazioni Web fornito con la piattaforma BI.

distribuzione

Il software della piattaforma BI installato, configurato e in esecuzione su uno o più computer.

installazione

Un'istanza dei file della piattaforma BI creati dal programma di installazione su un computer.

migrazione

Il processo di trasferimento del contenuto di Business Intelligence da una versione principale precedente, ad esempio la versione XI 3.1, tramite Upgrade Management Tool. Non è possibile eseguirlo per le distribuzioni con la stessa versione principale, vedere "promozione".

nodo

Un gruppo di server della piattaforma BI eseguiti sullo stesso computer e gestiti dallo stesso agente SIA (Server Intelligence Agent).

Pacchetto di supporto

Aggiornamenti per una versione principale o secondaria.

Patch

Aggiornamenti minimi per una specifica versione del pacchetto di supporto.

Piattaforma BI

Abbreviazione per piattaforma SAP BusinessObjects Business Intelligence.

promozione

Il processo di trasferimento del contenuto di Business Intelligence tra distribuzioni con la stessa versione principale, ad esempio 4.0, tramite l'applicazione Promotion Management.

server

Un processo della piattaforma BI. Un server ospita uno o più servizi.

Server di applicazioni Web

Un server di applicazioni Web elabora contenuto dinamico, ad esempio il server di applicazioni Web in bundle per 4.1 è Tomcat 7.

Server Intelligence Agent (SIA)

Un SIA è un processo che gestisce un gruppo di server. Le attività di gestione includono l'arresto, l'avvio e il riavvio dei server.

versione principale

Versionsi software, ad esempio 4.0.

versione secondaria

Versionsi software, ad esempio 4.1.

2.2 Prima di iniziare

2.2.1 Concetti fondamentali

2.2.1.1 Server Intelligence

Server Intelligence è un componente fondamentale della piattaforma BI. Le modifiche applicate ai processi del server nella Central Management Console (CMC) vengono estese agli oggetti server corrispondenti dal Central Management Server (CMS). Server Intelligence Agent (SIA) viene utilizzato per riavviare o chiudere automaticamente un server quando riscontra una condizione insolita e viene utilizzato da un amministratore per gestire un nodo.

CMS archivia le informazioni sui server nel database del sistema CMS per poter ripristinare in modo semplice le impostazioni predefinite del server. Dal momento che SIA interroga periodicamente il CMS affinché richieda informazioni sui server gestiti, SIA conosce lo stato in cui i server dovrebbero trovarsi e quando agire.

Nota:

Un'installazione della piattaforma BI rappresenta un'istanza univoca dei file della piattaforma BI creati dal programma di installazione su un computer. È possibile utilizzare un'istanza di un'installazione della piattaforma BI solo all'interno di un singolo cluster. I nodi appartenenti a cluster differenti che condividono la stessa installazione della piattaforma BI non sono supportati perché questo tipo di distribuzione non può essere corretto né aggiornato. Solo le piattaforme Unix supportano più installazioni del software sullo stesso computer, a condizione che ogni installazione venga eseguita con un account utente univoco e venga installata in una cartella separata in modo da non condividere file con le altre installazioni. Tenere presente che tutti i computer nel cluster devono presentare versione e livello patch identici.

Argomenti correlati

- [Server, host e cluster](#)

2.2.1.2 Server, servizi, nodi e host

Nella piattaforma BI i termini server e servizio vengono utilizzati per fare riferimento ai due tipi di software eseguiti su una piattaforma BI.

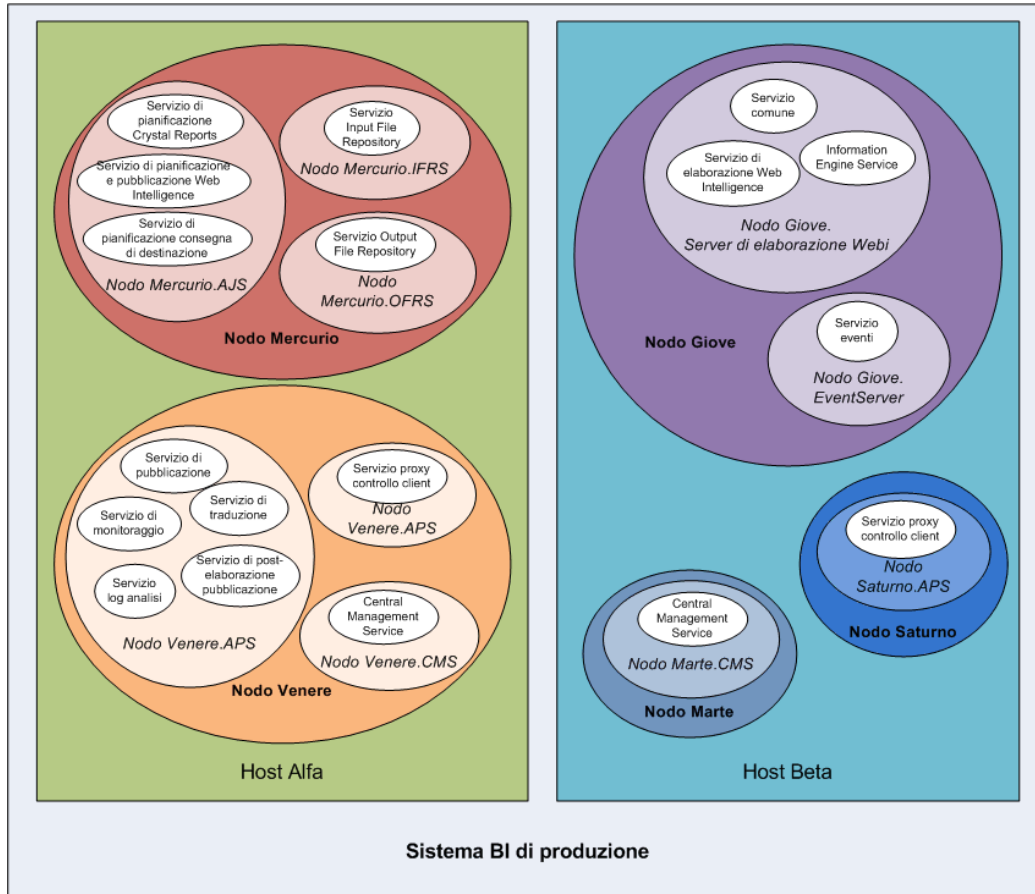
Il termine “server” viene utilizzato per descrivere un processo a livello di sistema operativo (in alcuni sistemi viene definito daemon) che ospita uno o più servizi. Ad esempio, CMS e Adaptive Processing Server sono server. Un server viene eseguito con un account di sistema operativo specifico e dispone di un proprio PID.

Un servizio è un sottosistema del server che esegue una funzione specifica. Il servizio viene eseguito nello spazio di memoria del relativo server con l'ID processo del contenitore principale (server). Ad esempio, il servizio di pianificazione di Web Intelligence è un sottosistema eseguito in Adaptive Job Server.

Un nodo è un insieme di server della piattaforma BI eseguiti nello stesso host e gestiti dallo stesso Server Intelligence Agent (SIA). In un solo host possono trovarsi uno o più nodi.

La piattaforma BI può essere installata in un solo computer, suddivisa tra più computer connessi tra loro in una Intranet o in una rete WAN.

Il diagramma che segue mostra un'installazione ipotetica della piattaforma BI. Nelle installazioni reali il numero di host, nodi, server e servizi, nonché il tipo di server e di servizi è variabile.



Due host formano il cluster denominato ProductionBISystem:

- Nell'host denominato HostAlpha è installata la piattaforma BI. L'host è configurato per contenere due nodi:
 - NodeMercury include un Adaptive Job Server (NodeMercury.AJS) con servizi per la pianificazione e la pubblicazione di report, un Input File Repository Server (NodeMercury.IFRS) con un servizio che consente di memorizzare i report di input e un Output File Repository Server (NodeMercury.OFRS) con un servizio che consente di memorizzare l'output dei report.
 - NodeVenus include un Adaptive Processing Server (NodeVenus.APS) con servizi che forniscono funzionalità per la pubblicazione, il monitoraggio e la traduzione, un Adaptive Processing Server (NodeVenus.APS2) dotato di un servizio che fornisce il controllo dei client, e un Central Management Server (NodeVenus.CMS) con un servizio che fornisce i servizi CMS.
- Nell'host denominato HostBeta è installata la piattaforma BI. L'host è configurato per contenere tre nodi:
 - NodeMars contiene un Central Management Server (NodeMars.CMS) con un servizio che fornisce i servizi CMS. La presenza di CMS su due computer consente il bilanciamento del carico e funzionalità di prevenzione e failover.
 - NodeJupiter contiene un server di elaborazione di Web Intelligence (NodeJupiter.Web Intelligence) dotato di un servizio che fornisce la funzionalità di creazione di report Web

Intelligence e un Event Server (`NodeJupiter.EventServer`) per consentire il monitoraggio di report dei file.

- NodeSaturn contiene un Adaptive Processing Server (`NodeSaturn.APS`) dotato di un servizio che fornisce il controllo dei client.

2.2.2 Strumenti di amministrazione principali

2.2.2.1 Configurazione guidata del sistema

La Configurazione guidata del sistema è uno strumento che consente di configurare in modo semplice e veloce la distribuzione della piattaforma BI. La procedura guida l'utente nella scelta delle opzioni di configurazione di base fino a ottenere una distribuzione di lavoro che utilizza impostazioni comuni come le seguenti:

- i server dei prodotti che si desidera avviare automaticamente con la piattaforma BI
- se si desidera ottimizzare la distribuzione per ottenere il massimo livello di prestazioni oppure risorse hardware limitate
- la posizione delle cartelle di sistema

Per impostazione predefinita, la procedura guidata è impostata per essere eseguita automaticamente quando si accede alla Central Management Console (CMC), tuttavia questa impostazione può essere modificata nella procedura guidata. È anche possibile avviare la procedura guidata in qualsiasi momento dall'area di "gestione" della CMC.

2.2.2.2 Central Management Console (CMC)

La Central Management Console (CMC) è uno strumento basato su Web che si utilizza per eseguire attività amministrative (quali la gestione di server, contenuti e utenti) e per configurare le impostazioni di protezione. Poiché la console CMC è un'applicazione basata su Web, è possibile eseguire tutti i task amministrativi mediante un browser Web in qualsiasi computer in grado di connettersi al server di applicazioni Web.

Tutti gli utenti possono accedere a CMC per modificare le impostazioni delle preferenze. Solo i membri del gruppo Amministratori possono modificare le impostazioni di gestione, a meno che tale diritto non venga esplicitamente concesso ad altri utenti. I ruoli possono essere assegnati in CMC per garantire

privilegi utente per portare a termine attività amministrative minori, quali la gestione di utenti nel gruppo e di report nelle cartelle appartenenti al proprio team.

2.2.2.3 Central Configuration Manager (CCM)

CCM (Central Configuration Manager) è uno strumento di configurazione per la gestione dei nodi e la risoluzione dei problemi del server fornito in due modalità. In un ambiente Microsoft Windows, CCM consente di gestire server locali e remoti tramite l'interfaccia utente grafica o la riga di comando. In ambiente Unix lo script di shell di CCM (`ccm.sh`) consente di gestire i server da una riga di comando.

CCM viene utilizzato per creare e configurare nodi e per avviare o interrompere il server di applicazioni Web, se questo è il server di applicazioni Web Tomcat in bundle predefinito. In Windows è anche possibile configurare parametri di rete, ad esempio la crittografia SSL (Secure Sockets Layer). Questi parametri si applicano a tutti i server in un nodo.

Nota:

La maggior parte dei task di gestione server viene ora gestita tramite la console CMC, non CCM. CCM è ora utilizzato per la risoluzione dei problemi e per la configurazione dei nodi.

2.2.2.4 Strumento Repository Diagnostic Tool

Lo strumento Repository Diagnostic Tool (RDT) consente di esaminare, diagnosticare e risolvere i conflitti che possono verificarsi tra il database di sistema CMS (Central Management Server) e l'archivio di file FRS (File Repository Server). È possibile impostare un limite per il numero di errori che lo strumento RDT può trovare e ripristinare prima di interrompersi.

Utilizzare lo strumento RDT dopo aver ripristinato il sistema della piattaforma BI.

2.2.2.5 Upgrade Management Tool

Upgrade Management Tool (in precedenza Importazione guidata) viene installato come parte della piattaforma BI e guida gli amministratori attraverso il processo di importazione di utenti, gruppi e cartelle di versioni precedenti della piattaforma BI. Consente inoltre di importare e aggiornare eventi, gruppi di server, oggetti repository e calendari.

Per informazioni sull'esecuzione dell'aggiornamento da una versione precedente della piattaforma BI, consultare il *Manuale di aggiornamento della piattaforma SAP BusinessObjects Business Intelligence*.

2.2.3 Attività principali

In base alla situazione, può essere opportuno concentrarsi su sezioni specifiche di questa guida; inoltre, altre risorse possono essere disponibili per situazioni specifiche. Per ciascuna delle situazioni seguenti, è presente un elenco di attività proposte e di argomenti di lettura.

Argomenti correlati

- [Pianificazione o esecuzione della prima distribuzione](#)
- [Configurazione della distribuzione](#)
- [Miglioramento delle prestazioni del sistema](#)
- [Central Management Console \(CMC\)](#)

2.2.3.1 Pianificazione o esecuzione della prima distribuzione

Se si sta pianificando di distribuire o si distribuisce per la prima volta la piattaforma BI, è consigliabile leggere le sezioni seguenti di questo manuale:

- Per acquisire familiarità con i componenti della piattaforma BI, leggere la sezione “Panoramica dell'architettura”.
- “Informazioni sulla comunicazione tra componenti della piattaforma BI”
- “Panoramica della protezione”
- Se si intende utilizzare l'autenticazione di terze parti, leggere “Opzioni di autenticazione disponibili nella piattaforma BI”.
- Dopo l'installazione, leggere “Utilizzo dell'area di gestione Server della console CMC”

Per ulteriori informazioni sull'installazione della piattaforma BI, consultare il *Manuale di installazione della piattaforma SAP BusinessObjects Business Intelligence*. Per valutare le esigenze specifiche e progettare l'architettura di distribuzione più appropriata, consultare il *Guida alla pianificazione della piattaforma SAP BusinessObjects Business Intelligence*.

Argomenti correlati

- [Presentazione dell'architettura](#)
- [Comunicazione tra componenti della piattaforma BI](#)
- [Panoramica della protezione](#)
- [Opzioni di autenticazione nella piattaforma BI](#)
- [Utilizzo dell'area di gestione Server della console CMC](#)

2.2.3.2 Configurazione della distribuzione

Se è stata appena completata l'installazione della piattaforma BI ed è necessario eseguire le attività di configurazione iniziali, ad esempio la configurazione di firewall e la gestione utenti, si consiglia di consultare le seguenti sezioni:

Argomenti correlati

- [Introduzione alla Configurazione guidata del sistema](#)
- [Comunicazione tra componenti della piattaforma BI](#)
- [Panoramica della protezione](#)
- [Informazioni sul monitoraggio](#)

2.2.3.3 Miglioramento delle prestazioni del sistema

Se si desidera valutare l'efficacia della propria distribuzione e modificarla per ottimizzare le risorse, leggere le sezioni seguenti:

- Se si desidera utilizzare un modello di distribuzione per configurare il sistema, leggere “Introduzione alla Configurazione guidata del sistema”.
- Se si desidera monitorare il sistema esistente, leggere “Informazioni sul monitoraggio”.
- Per attività e procedure di manutenzione quotidiane che riguardano i server della CMC, leggere “Utilizzo dell'area di gestione Server della console CMC”.

Argomenti correlati

- [Introduzione alla Configurazione guidata del sistema](#)
- [Informazioni sul monitoraggio](#)
- [Utilizzo dell'area di gestione Server della console CMC](#)

2.2.3.4 Utilizzo di oggetti in CMC

Un oggetto è un documento o un file creato nella piattaforma BI o in altro software, che viene memorizzato e gestito nel repository della piattaforma BI. Se si utilizzano oggetti in CMC, consultare le seguenti sezioni:

- Per informazioni sull'impostazione di utenti e gruppi in CMC, consultare “Panoramica della gestione degli account”.
- Per impostare la protezione per gli oggetti, consultare “Funzionamento dei diritti nella piattaforma BI”.
- Per informazioni generali sull'utilizzo degli oggetti, consultare il *Manuale dell'utente della piattaforma SAP BusinessObjects Business Intelligence*.

Argomenti correlati

- [Panoramica della gestione dei server](#)
- [Funzionamento dei diritti nella piattaforma BI](#)

Architettura

3.1 Presentazione dell'architettura

In questa sezione vengono presentati i componenti generali dell'architettura della piattaforma, del sistema e dei componenti di servizio che costituiscono la piattaforma SAP BusinessObjects Business Intelligence. Le informazioni consentono agli amministratori di comprendere gli elementi base del sistema e di creare un piano per lo sviluppo, la gestione e la manutenzione del sistema.

Nota:

per un elenco di piattaforme supportate, lingue, database, server di applicazioni Web, server Web e di altri sistemi supportati da questa versione, consultare il documento *Product Availability Matrix* (Supported Platforms/PAR), disponibile nella sezione SAP BusinessObjects di SAP Support Portal all'indirizzo: <https://service.sap.com/bosap-support>.

La Business Intelligence (BI) è stata progettata per garantire elevate prestazioni in svariati scenari utente e di distribuzione. Ad esempio, tramite servizi di piattaforma specializzati è possibile gestire l'accesso ai dati e la generazione di report su richiesta oppure la pianificazione dei report basata su tempi ed eventi. È possibile ridurre il carico di lavoro del processore dovuto alle operazioni di pianificazione ed elaborazione creando server dedicati per la gestione di servizi specifici. L'architettura è progettata per soddisfare le esigenze di quasi tutti i tipi di distribuzione BI ed è sufficientemente flessibile per passare da alcuni utenti con un singolo strumento a decine di migliaia con più strumenti e interfacce.

È possibile integrare la piattaforma BI negli altri sistemi tecnologici dell'organizzazione utilizzando API di servizi Web, Java o .NET.

Gli utenti finali possono accedere ai report, crearli, modificarli e interagire con essi tramite strumenti e applicazioni speciali tra cui:

- Client installati dal programma di installazione di Strumenti client della piattaforma BI:
 - Web Intelligence Rich Client
 - Business View Manager
 - Strumento di conversione dei report
 - Universe Design Tool
 - Query come servizio Web
 - Information Design Tool (in precedenza Information Designer)
 - Translation Management Tool (in precedenza Translation Manager)
 - Widget (in precedenza Widget BI)
- Client disponibili separatamente:

- SAP Crystal Reports
- SAP BusinessObjects Dashboards (in precedenza Xcelsius)
- SAP BusinessObjects Analysis (in precedenza Voyager)
- BI Workspaces (in precedenza Dashboard Builder)

I reparti IT possono utilizzare strumenti di gestione di dati e sistema tra cui:

- Visualizzatori di report
- Central Management Console (CMC)
- Central Configuration Manager (CCM)
- Repository Diagnostic Tool (RDT)
- Strumento di amministrazione di Data Federation
- Upgrade Management Tool (in precedenza Importazione guidata)
- Universe Design Tool (in precedenza Universe Designer)
- SAP BusinessObjects Mobile

Per fornire flessibilità, affidabilità e scalabilità, è possibile installare i componenti della piattaforma BI in uno o più computer. È anche possibile installare contemporaneamente due versioni diverse della piattaforma BI nello stesso computer, benché questa configurazione sia consigliata solo come parte del processo di aggiornamento o di test.

I processi server possono essere scalati in verticale (un computer esegue più processi server, o tutti) per ridurre i costi oppure in orizzontale (i processi server sono distribuiti tra due o più computer connessi in rete) per migliorare le prestazioni. Inoltre, è possibile eseguire più versioni ridondanti dello stesso processo server su più di un computer, in modo tale che l'elaborazione possa continuare se si verifica un problema nel processo principale.

Nota:

Benché sia possibile utilizzare una combinazione di piattaforme Windows e Unix o Linux, è consigliabile non mescolare i sistemi operativi per i processi CMS (Central Management Server).

3.1.1 Diagramma componenti

La piattaforma SAP BusinessObjects Business Intelligence è una piattaforma BI (Business Intelligence) che fornisce gli strumenti di analisi e creazione dei report a livello aziendale. I dati possono essere analizzati da una grande varietà di sistemi di database supportati, inclusi i sistemi OLAP multidimensionali o di testo, e i report BI possono essere pubblicati in diversi formati su più sistemi di pubblicazione.

Il diagramma dell'architettura disponibile nella SAP Community Network illustra i componenti della piattaforma BI, inclusi server e strumenti client, nonché altri prodotti analitici, componenti di applicazioni Web e database che possono fare parte di un ambiente di piattaforma BI: <http://scn.sap.com/docs/DOC-43663>

La piattaforma BI crea report da una connessione di sola lettura ai database dell'organizzazione e utilizza i database in esso inclusi per la memorizzazione delle relative informazioni sulla configurazione, sul controllo e su altre funzioni. I report BI creati dal sistema possono essere inviati a una varietà di

destinazioni, inclusi file system e posta elettronica. In alternativa, è possibile accedervi attraverso siti Web o portali.

La piattaforma BI è un sistema indipendente che può esistere su un solo computer (ad esempio un piccolo ambiente di sviluppo o di test pre-produzione) o essere scalato in un cluster con molti computer che eseguono componenti diversi (ad esempio, un ambiente di produzione su larga scala).

3.1.2 Livelli architettura

La piattaforma SAP BusinessObjects Business Intelligence può essere vista come una serie di livelli concettuali.

Livello client

Il livello client contiene tutte le applicazioni client desktop che interagiscono con la piattaforma BI al fine di fornire una varietà di funzionalità di creazione report, analisi e amministrazione. Fra gli esempi si ricordino il Central Configuration Manager (programma di installazione della piattaforma BI), Information Design Tool (programma di installazione degli strumenti client della piattaforma BI) e SAP Crystal Reports 2011 (disponibile e installato separatamente).

Livello Web

Il livello Web contiene le applicazioni Web distribuite in un server di applicazioni Web Java. Le applicazioni Web forniscono tramite un browser Web le funzionalità della piattaforma BI agli utenti finali. Tra gli esempi di applicazioni Web figurano l'interfaccia Web amministrativa della Central Management Console (CMC) e BI Launch Pad.

Il livello Web contiene anche i Servizi Web. Attraverso il server di applicazioni Web, i Servizi Web forniscono agli strumenti software le funzionalità della piattaforma BI, come l'autenticazione delle sessioni, la gestione dei privilegi utente, la pianificazione, la ricerca, l'amministrazione, la creazione di report e la gestione di query. Ad esempio, Live Office è un prodotto che utilizza i Servizi Web per integrare la creazione di report della piattaforma BI con i prodotti Microsoft Office.

Livello gestione

Il livello di gestione (anche noto come intelligence tier) coordina e controlla tutti i componenti della piattaforma BI. Comprende CMS (Central Management Server), Event Server e i servizi correlati. Il server CMS gestisce le informazioni relative alla configurazione e alla protezione, invia richieste di servizio ai server, gestisce il controllo e mantiene il database di sistema CMS. Event Server gestisce gli eventi basati su file che si verificano nel livello di archiviazione.

Livello archiviazione

Il livello di archiviazione è responsabile della gestione di file, quali documenti e report.

Input File Repository Server gestisce i file che contengono le informazioni da utilizzare nei report, come i seguenti tipi di file: .rpt, .car, .exe, .bat, .js, .xls, .doc, .ppt, .rtf, .txt, .pdf, .wid, .rep, .unv.

Output File Repository Server gestisce i report creati dal sistema, come i seguenti tipi di file: .rpt, .csv, .xls, .doc, .rtf, .txt, .pdf, .wid, .rep.

Il livello di archiviazione gestisce inoltre la funzione di cache dei report per il salvataggio delle risorse di sistema quando gli utenti accedono ai report.

Livello di elaborazione

Il livello di elaborazione analizza i dati e produce i report. Si tratta dell'unico livello che accede ai database contenenti i dati dei report. Questo livello è costituito da Adaptive Job Server, Connection Server (a 32 e 64 bit) e dai server di elaborazione quali Adaptive Processing Server o il server di elaborazione Crystal Reports.

Livello dati

È costituito dai server di database che ospitano il database di sistema CMS e l'archivio dati di controllo. È costituito anche da qualsiasi server di database contenente dati relazionali, OLAP o altri tipi di dati per la creazione di report e applicazioni analitiche.

3.1.3 Database

La piattaforma BI utilizza più database differenti.

- Database di reporting

Questo termine fa riferimento alle informazioni sull'organizzazione. Sono le informazioni di origine analizzate e restituite dai prodotti della SAP BusinessObjects Business Intelligence Suite. In genere le informazioni vengono archiviate in un database relazionale, ma possono essere contenute anche in file di testo, documenti di Microsoft Office o sistemi OLAP.

- Database di sistema CMS

Il database di sistema CMS viene utilizzato per archiviare le informazioni della piattaforma BI, ad esempio i dettagli relativi a utenti, server, cartelle, documenti, configurazione e autenticazione. Viene gestito mediante il server CMS e talvolta definito come *repository di sistema*.

- Archivio dati di controllo

L'Archivio dati di controllo (ADS, Auditing Data Store) viene utilizzato per archiviare le informazioni relative a eventi registrabili che si verificano nella piattaforma BI. Tali informazioni possono essere utilizzate per il monitoraggio dell'uso dei componenti di sistema, dell'attività dell'utente o di altri aspetti del funzionamento quotidiano.

- Database Lifecycle Management

Nel database Lifecycle Management vengono registrate le informazioni relative alla configurazione e alla versione di un'installazione della piattaforma BI, nonché gli aggiornamenti.

- Database Monitoraggio

Monitoraggio utilizza il database Java Derby per memorizzare informazioni sui componenti e sulla configurazione del sistema per il supporto SAP.

Se non è disponibile un server di database da utilizzare con il sistema CMS e i database dell'archivio dati di controllo, il programma di installazione della piattaforma BI può installarlo e configurarlo automaticamente. Per stabilire quale database supportato è più adatto ai requisiti della propria organizzazione, è consigliabile valutare i requisiti rispetto alle indicazioni del fornitore di server di database.

3.1.4 Server, host e cluster

La piattaforma BI è costituita da raccolte di server eseguiti su uno o più host. Per le piccole installazioni, ad esempio sistemi di test o di sviluppo, è possibile utilizzare un solo host per un server di applicazioni Web, un server di database e tutti i server della piattaforma BI.

Per le installazioni di medie e grandi dimensioni è possibile utilizzare server in esecuzione su più host. È possibile, ad esempio, utilizzare un host server di applicazioni Web insieme a un host server della piattaforma BI. In questo modo vengono liberate risorse sull'host server della piattaforma BI per consentire l'elaborazione di un numero maggiore di informazioni rispetto al caso in cui viene ospitato anche un server di applicazioni Web.

Per le installazioni di grandi dimensioni è possibile utilizzare diversi host server della piattaforma BI raggruppati in un cluster. Se, ad esempio, un'organizzazione include un gran numero di utenti SAP Crystal Reports, è possibile creare server di elaborazione Crystal Reports su più host server della piattaforma BI per garantire la disponibilità di una notevole quantità di risorse per elaborare le richieste dei client.

I principali vantaggi derivanti dalla presenza di più server sono i seguenti:

- Miglioramento delle prestazioni

Diversi host server della piattaforma BI sono in grado di elaborare una coda di informazioni di report in modo più rapido rispetto a un solo host server della piattaforma BI.

- Bilanciamento del carico

Se un server registra un carico più elevato rispetto agli altri server presenti in un cluster, il CMS invia automaticamente nuovo lavoro a un server che include risorse migliori.

- Maggiore disponibilità

Se un server rileva una condizione imprevista, il CMS reindirizza automaticamente il lavoro verso server diversi fino a quando la condizione non viene corretta.

3.1.5 Server di applicazioni Web

Un server di applicazioni Web funge da livello di traduzione tra un'applicazione browser Web o rich e la piattaforma BI. Sono supportati i server di applicazioni Web in esecuzione in Windows, Unix e Linux.

Per un elenco dettagliato dei server di applicazioni Web supportati, consultare il documento *Supported Platforms/PARs*, disponibile all'indirizzo <https://service.sap.com/bosap-support>.

Se non è disponibile un server di applicazioni Web da utilizzare con la piattaforma BI, il programma di installazione può installare e configurare automaticamente un server di applicazioni Web Tomcat. Per identificare il server di applicazioni Web supportato più adatto ai requisiti di un'organizzazione è consigliabile valutare i requisiti rispetto alle informazioni indicate dal fornitore di server di applicazioni Web.

Nota:

quando si configura un ambiente di produzione, è consigliabile che il server di applicazioni Web sia ospitato in un sistema separato. L'esecuzione della piattaforma BI e di un server di applicazioni Web nello stesso host in un ambiente di produzione può determinare una riduzione delle prestazioni.

3.1.5.1 Server del contenitore applicazioni Web (WACS)

Per ospitare le applicazioni Web della piattaforma BI è necessario un server di applicazioni Web.

Se si ricopre il ruolo di amministratore di server di applicazioni Web Java avanzato con esigenze amministrative avanzate, utilizzare un server di applicazioni Web Java supportato per l'hosting delle applicazioni Web della piattaforma BI. Se si utilizza un sistema operativo Windows supportato per ospitare la piattaforma BI e si preferisce un processo di installazione del server di applicazioni Web semplice o non si dispone delle risorse necessarie per amministrare un server di applicazioni Web Java, è possibile installare il server del contenitore applicazioni Web (WACS) durante l'installazione della piattaforma BI.

WACS è un server della piattaforma BI che consente l'esecuzione di applicazioni Web della piattaforma BI, quali la CMC (Central Management Console), BI Launch Pad e Servizi Web, anche senza una precedente installazione di un server di applicazioni Web Java.

L'utilizzo di WACS offre numerosi vantaggi:

- Il server WACS richiede interventi minimi per l'installazione, la manutenzione e la configurazione. Viene installato e configurato dal programma di installazione della piattaforma BI e non sono richieste ulteriori operazioni per iniziare a utilizzarlo.
- Con il server WACS non occorre avere competenze di amministrazione e manutenzione di server di applicazioni Java.
- Il server WACS offre un'interfaccia amministrativa coerente con quella di altri server della piattaforma BI.
- Analogamente ad altri server della piattaforma BI, WACS può essere installato in un host dedicato.

Nota:

Esistono alcune limitazioni all'uso di un server WACS anziché un server di applicazioni Web Java dedicato:

- Il server WACS è disponibile solo nei sistemi operativi Windows supportati.
- Le applicazioni Web personalizzate non possono essere distribuite nel WACS, in quanto questo server supporta solo le applicazioni Web installate con la piattaforma BI.

- Il server WACS non può essere utilizzato con un bilanciatore di carico Apache.

Oltre al WACS, è possibile utilizzare un server di applicazioni Web dedicato. Questo consente al server di applicazioni Web dedicato di ospitare applicazioni Web personalizzate, mentre la CMC e altre applicazioni Web della piattaforma BI sono ospitate dal WACS.

3.1.6 Software Development Kit

Il Software Development Kit (SDK) consente agli sviluppatori di incorporare aspetti della piattaforma SAP BusinessObjects Business Intelligence nelle applicazioni e nei sistemi utilizzati da un'organizzazione.

La piattaforma BI include SDK per lo sviluppo di software sulle piattaforme Java e .NET.

Nota:

I kit .NET SDK per la piattaforma BI non sono installati per impostazione predefinita e devono essere scaricati dal sito SAP Service Marketplace.

La piattaforma BI supporta i seguenti SDK:

- Java SDK e .NET SDK per la piattaforma Business Intelligence

Gli SDK per la piattaforma BI consentono alle applicazioni di eseguire attività come l'autenticazione, la gestione della sessione, l'utilizzo degli oggetti repository, la pianificazione e la pubblicazione di report nonché la gestione dei server.

Nota:

Per l'accesso completo alle funzioni di protezione, di gestione dei server e di controllo, utilizzare l'SDK Java.

- SDK dei servizi Web RESTful della piattaforma Business Intelligence

L'SDK dei servizi Web RESTful della piattaforma BI consente di accedere alla piattaforma BI mediante il protocollo HTTP. È possibile utilizzare questo SDK per accedere alla piattaforma BI, passare al repository della piattaforma BI, accedere alle risorse ed eseguire la pianificazione delle risorse di base. È possibile accedere a questo SDK scrivendo applicazioni che utilizzano qualsiasi linguaggio di programmazione che supporti il protocollo HTTP oppure utilizzando qualsiasi strumento che supporti l'esecuzione di richieste HTTP.

- Java Consumer SDK e .NET Consumer SDK per la piattaforma Business Intelligence

Implementazione dei servizi Web basati su SOAP che consente di impostare le opzioni di autenticazione e protezione utente, accesso a documenti e report, pianificazione, pubblicazioni e gestione del server.

I servizi Web della piattaforma BI utilizzano standard quali XML, SOAP, AXIS 2.0 e WSDL. La piattaforma segue la specifica dei servizi Web WS-Interoperability Basic Profile 1.0.

Nota:

Le applicazioni dei servizi Web sono al momento supportate unicamente con le seguenti configurazioni della funzione di bilanciamento del carico:

1. Persistenza dell'indirizzo IP di origine.
2. Persistenza della porta di destinazione e dell'indirizzo IP di origine (disponibile solo in un Content Services Switch Cisco).
3. Persistenza SSL.
4. Persistenza di sessione basata su cookie.

Nota:

La persistenza SSL può causare problemi di affidabilità e protezione in alcuni browser Web. Chiedere all'amministratore della rete di determinare se la persistenza SSL è appropriata per l'organizzazione.

- SDK Java di connessione e del driver di accesso ai dati

Questi SDK consentono di creare driver di database per il server di connessione e di gestire le connessioni di database.

- SDK Java del livello semantico

L'SDK Java del livello semantico consente di sviluppare un'applicazione Java che esegue attività di amministrazione e protezione su universi e connessioni. È ad esempio possibile implementare i servizi per la pubblicazione di un universo in un repository oppure recuperare una connessione protetta dal repository nell'area di lavoro. Questa applicazione può essere incorporata nelle soluzioni Business Intelligence che integrano la piattaforma BI come OEM.

- Report Application Server Java SDK e .NET SDK

Gli SDK di Report Application Server consentono alle applicazioni di aprire, creare e modificare i report Crystal già esistenti, effettuando operazioni come l'impostazione dei valori dei parametri, la modifica delle origini dati e l'esportazione in altri formati, tra cui XML, PDF, Microsoft Word e Microsoft Excel.

- Visualizzatore Java e .NET Crystal Reports Viewer

I visualizzatori consentono alle applicazioni di visualizzare ed esportare report Crystal. Sono disponibili i seguenti visualizzatori:

- Visualizzatore di pagine di report DHTML: presenta i dati e consente di eseguire operazioni quali drill down, esplorazione delle pagine, zoom, visualizzazione di prompt, ricerca, evidenziazione, esportazione e stampa.
- Visualizzatore di parti di report: consente di visualizzare le singole parti di un report, tra cui grafici, testo e campi.

- Report Engine Java SDK e .NET SDK

Gli SDK di Report Engine consentono alle applicazioni di interagire con i report creati con SAP BusinessObjects Web Intelligence.

Gli SDK di Report Engine includono librerie che è possibile utilizzare per creare uno strumento di progettazione di report Web. Le applicazioni create con questi SDK sono in grado di visualizzare, creare o modificare svariati tipi di documenti Web Intelligence. Gli utenti possono modificare documenti aggiungendo, rimuovendo e modificando oggetti quali tabelle, grafici, condizioni e filtri.

- SDK dell'applicazione di ricerca piattaforma: è l'interfaccia tra l'applicazione client e il servizio di ricerca piattaforma. Ricerca piattaforma supporta l'SDK pubblico fornito come parte dell'SDK di Ricerca piattaforma.

Quando un parametro di richiesta ricerca viene inviato tramite l'applicazione client al livello SDK, il livello SDK converte il parametro di richiesta in un formato codificato XML e lo passa al servizio Ricerca piattaforma.

Gli SDK possono essere utilizzati in combinazione per fornire un'ampia gamma di funzionalità BI alle applicazioni in uso. Per ulteriori informazioni su questi SDK, inclusi i manuali per lo sviluppatore e i riferimenti alle API, visitare il sito Web <http://help.sap.com>.

3.1.7 Origini dati

3.1.7.1 Universi

L'universo astrae la complessità dei dati utilizzando un linguaggio aziendale anziché un linguaggio dati per accedere, modificare e organizzare i dati. Il linguaggio aziendale viene memorizzato sotto forma di oggetti in un file di universo. Web Intelligence e Crystal Reports utilizzano gli universi per semplificare il processo di creazione degli utenti necessario per l'esecuzione di query e analisi semplici e complesse da parte dell'utente finale.

Gli universi sono un componente fondamentale della piattaforma BI. Tutti gli oggetti universo e le relative connessioni vengono memorizzati e protetti nel repository centrale da Connection Server. Per accedere al sistema e creare gli universi, gli strumenti di progettazione degli universi devono accedere alla piattaforma BI. L'accesso agli universi e la protezione a livello di riga possono anche essere gestiti al livello del gruppo o del singolo utente dall'ambiente di progettazione.

Il livello semantico consente a Web Intelligence di recapitare i documenti, utilizzando più provider di dati sincronizzati, incluse le origini dati OLAP (online analytical processing) e CWM (common warehousing metamodel).

3.1.7.2 Business Views

Le viste aziendali semplificano la creazione e l'interazione di report limitando la complessità dei dati per gli sviluppatori di report. Le viste aziendali consentono di separare le connessioni dati, l'accesso ai dati, gli elementi aziendali e il controllo dell'accesso.

Le viste aziendali possono essere utilizzate solo da Crystal Reports e hanno lo scopo di semplificare la protezione dell'accesso ai dati e della visualizzazione per la creazione di report Crystal. Le viste aziendali supportano la combinazione di più origini dati in una sola visualizzazione. Business Views è completamente supportato nella piattaforma BI.

La piattaforma Business Intelligence include una serie di servizi di gestione delle piattaforme preconfigurati e dedicati per attività quali la gestione delle password, le metriche dei server e il controllo dell'accesso degli utenti, per supportare le funzioni di gestione decentralizzate.

3.1.8 Autenticazione e Single Sign On

La protezione del sistema viene gestita attraverso il Central Management Server (CMS), plug-in di protezione e strumenti di autenticazione di terze parti, ad esempio SiteMinder o Kerberos. Questi componenti autenticano gli utenti e autorizzano l'accesso utente per la piattaforma BI, le relative cartelle e altri oggetti.

Sono disponibili i plug-in di protezione Single Sign On dell'autenticazione utente seguenti:

- Enterprise (predefinito), incluso il supporto per Autenticazione affidabile da utilizzare con metodi di autenticazione come SAML, X.509, SAP NW SSO e altri metodi supportati dal server di applicazioni.
- LDAP
- Windows Active Directory (AD)

Quando si utilizza un sistema ERP (Enterprise Resource Planning), il Single Sign On viene utilizzato per autenticare l'accesso dell'utente al sistema ERP in modo che i report possano essere verificati nei dati ERP. Sono supportati i Single Sign On di autenticazione utente seguenti per i sistemi ERP:

- SAP ERP e Business Warehouse (BW)
- Oracle E-Business Suite (EBS)
- Siebel Enterprise
- JD Edwards Enterprise One
- PeopleSoft Enterprise

3.1.8.1 Plug-in di protezione

I plug-in di protezione automatizzano la creazione e la gestione di account consentendo la mappatura di account utente e gruppi da sistemi di terze parti nella piattaforma BI. È possibile mappare account utente di terze parti ad account utente Enterprise esistenti o creare nuovi account utente Enterprise che corrispondano a ogni voce mappata nel sistema esterno.

I plug-in di protezione gestiscono dinamicamente elenchi di utenti e gruppi di terze parti. Dopo aver mappato un gruppo LDAP (Lightweight Directory Access Protocol) o Windows Active Directory (AD)

alla piattaforma BI, tutti gli utenti che appartengono a quel gruppo possono accedere alla piattaforma BI. Le modifiche successive alle appartenenze a gruppi di terzi vengono propagate automaticamente.

La piattaforma BI supporta i seguenti plug-in di protezione:

- Plug-in di protezione Enterprise

Il server Central Management Server (CMS) gestisce informazioni di protezione quali account utente, appartenenza a gruppi e diritti oggetti per la definizione di privilegi di utenti e gruppi. Questa operazione prende il nome di autenticazione Enterprise.

L'autenticazione Enterprise è sempre abilitata e non può essere disabilitata. Utilizzare l'autenticazione Enterprise predefinita del sistema se si preferisce creare account e gruppi distinti da utilizzare con la piattaforma BI oppure se non è stata ancora impostata una gerarchia di utenti e gruppi in un server LDAP o Windows AD.

Autenticazione affidabile è un componente dell'autenticazione Enterprise che si integra con soluzioni Single Sign On di terze parti, tra cui Java Authentication and Authorization Service (JAAS). Le applicazioni che stabiliscono una connessione fidata con il Central Management Server possono usare l'Autenticazione affidabile per accedere al sistema senza password.

- Plug-in di protezione di LDAP
- Windows AD

Nota:

Sebbene un utente possa configurare l'autenticazione Windows AD per la piattaforma BI e le applicazioni personalizzate tramite la console CMC, quest'ultima e BI Launch Pad non supportano l'autenticazione Windows AD con NTLM. Gli unici metodi di autenticazione supportati da CMC e BI Launch Pad sono Windows AD con Kerberos, LDAP, Enterprise e Autenticazione affidabile.

3.1.8.2 Integrazione ERP (Enterprise Resource Planning)

Un'applicazione ERP (Enterprise Resource Planning) supporta le funzioni essenziali dei processi aziendali mediante la raccolta di informazioni in tempo reale relative alle operazioni quotidiane. La piattaforma BI supporta Single Sign-On e la creazione di report dai sistemi ERP seguenti:

- SAP ERP e Business Warehouse (BW)
- Siebel Enterprise
- Oracle E-Business Suite
- JD Edwards EnterpriseOne
- PeopleSoft Enterprise

Nota:

- Il supporto di SAP ERP e BW viene installato per impostazione predefinita. Utilizzare l'opzione di installazione Personalizza / Espandi per deselezionare il supporto dell'integrazione SAP se non è richiesto il supporto di SAP ERP o BW.

- Il supporto di Siebel Enterprise, Oracle E-Business Suite, JD Edwards EnterpriseOne o PeopleSoft non viene installato per impostazione predefinita. Utilizzare l'opzione di installazione "Personalizza / Espandi" per selezionare e installare l'integrazione dei sistemi ERP non SAP.

Per informazioni dettagliate sulle specifiche versioni supportate dalla piattaforma BI, consultare il documento *Supported Platforms/PARs* disponibile all'indirizzo <https://service.sap.com/bosap-support>.

Per configurare l'integrazione ERP, consultare il capitolo *Configurazioni supplementari per gli ambienti ERP* di questo manuale.

3.1.9 Integrazione SAP

La piattaforma BI si integra con l'infrastruttura SAP esistente grazie agli strumenti SAP seguenti:

- SAP System Landscape Directory (SLD)

Lo strumento System Landscape Directory di SAP NetWeaver è l'origine centrale dei dati System Landscape più importanti per la gestione del ciclo di vita del software. Fornendo una directory contenente le informazioni relative a tutto il software installabile disponibile da SAP e i dati aggiornati automaticamente sui sistemi già installati in un landscape, si ottiene la base per il supporto dello strumento nella pianificazione delle attività del ciclo di vita del software nel System Landscape.

Il programma di installazione della piattaforma BI registra il fornitore, il nome e la versione dei prodotti con SLD, nonché nomi, versioni e percorso di componenti front-end e server.

- SAP Solution Manager

SAP Solution Manager è una piattaforma che consente di integrare contenuto, strumenti e metodologie per implementare, supportare, realizzare e monitorare le soluzioni SAP e non SAP di un'organizzazione.

Il software non SAP con integrazione certificata da SAP viene inserito in un repository centrale e trasferito automaticamente al server SLD (System Landscape Directories) di SAP. I clienti SAP possono quindi identificare facilmente quale versione di integrazione di prodotti di terze parti è stata certificata da SAP nel proprio ambiente del sistema SAP. Questo servizio offre pertanto informazioni relative ai prodotti di terze parti aggiuntive rispetto ai cataloghi in linea.

SAP Solution Manager è disponibile per i clienti SAP senza costi aggiuntivi e include l'accesso diretto al supporto SAP, nonché informazioni sul percorso di aggiornamento SAP. Per ulteriori informazioni su SLD, consultare la sezione "Registrazione della piattaforma BI in System Landscape".

- CTS Transport (CTS+)

Change and Transport System (CTS) consente di organizzare i progetti di sviluppo in ABAP Workbench e nella personalizzazione, quindi di trasportare le modifiche tra i sistemi SAP presenti nel System Landscape. Come per gli oggetti ABAP, è inoltre possibile trasportare gli oggetti Java (J2EE, JEE) e le tecnologie non ABAP specifiche di SAP (quali Web Dynpro Java e SAP NetWeaver Portal) nel landscape.

- Monitoraggio con CA Wily Introscope

CA Wily Introscope è un prodotto per la gestione delle applicazioni Web che consente di monitorare e diagnosticare i problemi di prestazioni che si possono verificare all'interno dei moduli SAP basati su Java in fase di produzione, comprese la visibilità nelle applicazioni Java personalizzate e le connessioni ai sistemi back-end. Consente di isolare i colli di bottiglia delle prestazioni nei moduli NetWeaver, compresi i singoli servlet, JSP, EJB, JCO, classi, metodi e altro. Fornisce inoltre il monitoraggio in tempo reale con overhead limitato, la visibilità delle transazioni end-to-end, i dati cronologici per la pianificazione dell'analisi o della capacità, cruscotti personalizzati, allarmi di soglia automatici e un'architettura aperta per estendere il monitoraggio oltre gli ambienti NetWeaver.

3.1.10 Controllo integrato delle versioni

I file che costituiscono la piattaforma BI in un sistema server sono ora sottoposti al controllo delle versioni. Il programma di installazione installerà e configurerà il sistema di controllo delle versioni Subversion. In alternativa, è possibile immettere dettagli per l'utilizzo di un sistema di controllo delle versioni Subversion o ClearCase esistente.

Un sistema di controllo delle versioni consente di mantenere e ripristinare revisioni diverse di file di configurazione e altri file. Ciò significa che è sempre possibile ripristinare un determinato stato di un qualsiasi momento del passato.

3.1.11 Percorso di aggiornamento

È possibile eseguire l'aggiornamento da una versione precedente di SAP BusinessObjects Enterprise (ad esempio XI 3.x), tuttavia è necessario innanzitutto installare la piattaforma SAP BusinessObjects Business Intelligence 4.x, quindi effettuare la migrazione di impostazioni e dati dal sistema esistente utilizzando Upgrade Management Tool.

Per informazioni sulle modalità di aggiornamento da una versione precedente, consultare il *Manuale per l'aggiornamento della piattaforma SAP BusinessObjects Business Intelligence*.

3.2 Server, servizi, nodi e host

Nella piattaforma BI i termini server e servizio vengono utilizzati per fare riferimento ai due tipi di software eseguiti su una piattaforma BI.

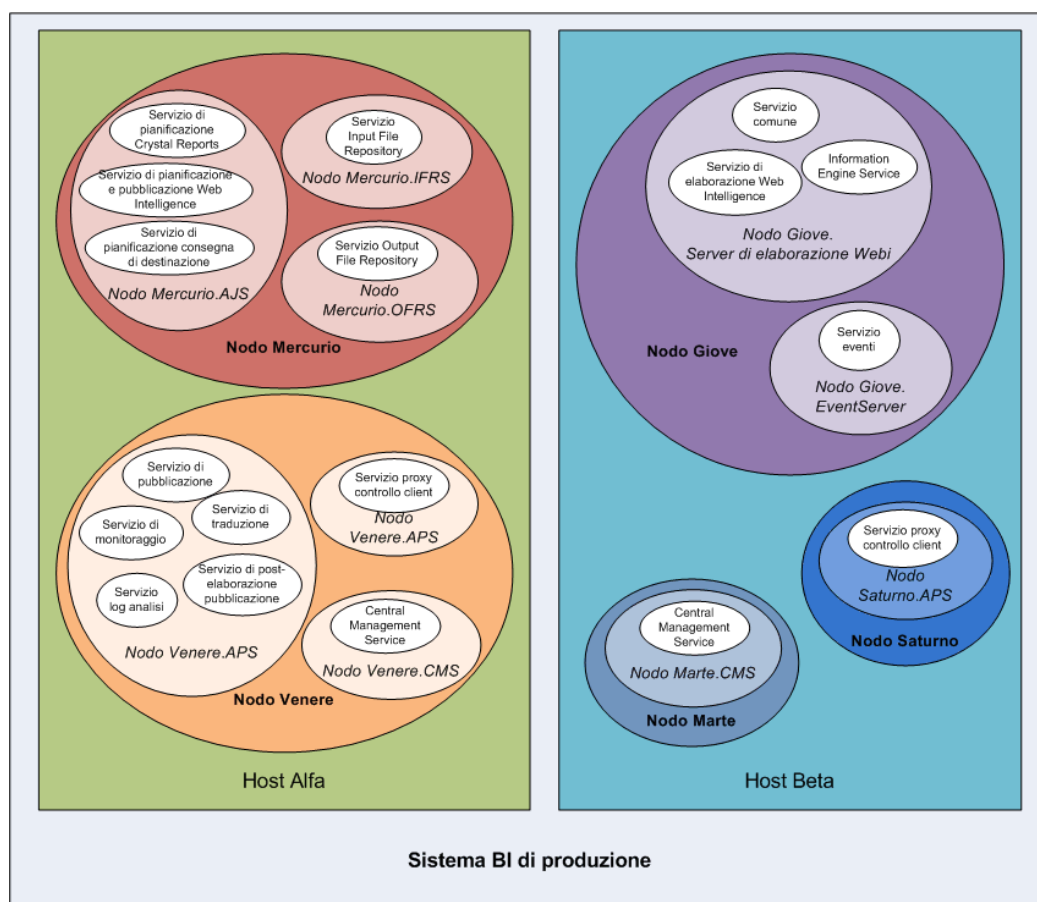
Il termine “server” viene utilizzato per descrivere un processo a livello di sistema operativo (in alcuni sistemi viene definito daemon) che ospita uno o più servizi. Ad esempio, CMS e Adaptive Processing Server sono server. Un server viene eseguito con un account di sistema operativo specifico e dispone di un proprio PID.

Un servizio è un sottosistema del server che esegue una funzione specifica. Il servizio viene eseguito nello spazio di memoria del relativo server con l'ID processo del contenitore principale (server). Ad esempio, il servizio di pianificazione di Web Intelligence è un sottosistema eseguito in Adaptive Job Server.

Un nodo è un insieme di server della piattaforma BI eseguiti nello stesso host e gestiti dallo stesso Server Intelligence Agent (SIA). In un solo host possono trovarsi uno o più nodi.

La piattaforma BI può essere installata in un solo computer, suddivisa tra più computer connessi tra loro in una Intranet o in una rete WAN.

Il diagramma che segue mostra un'installazione ipotetica della piattaforma BI. Nelle installazioni reali il numero di host, nodi, server e servizi, nonché il tipo di server e di servizi è variabile.



Due host formano il cluster denominato ProductionBISystem:

- Nell'host denominato HostAlpha è installata la piattaforma BI. L'host è configurato per contenere due nodi:

- NodeMercury include un Adaptive Job Server (`NodeMercury.AJS`) con servizi per la pianificazione e la pubblicazione di report, un Input File Repository Server (`NodeMercury.IFRS`) con un servizio che consente di memorizzare i report di input e un Output File Repository Server (`NodeMercury.OFRS`) con un servizio che consente di memorizzare l'output dei report.
- NodeVenus include un Adaptive Processing Server (`NodeVenus.APS`) con servizi che forniscono funzionalità per la pubblicazione, il monitoraggio e la traduzione, un Adaptive Processing Server (`NodeVenus.APS2`) dotato di un servizio che fornisce il controllo dei client, e un Central Management Server (`NodeVenus.CMS`) con un servizio che fornisce i servizi CMS.
- Nell'host denominato HostBeta è installata la piattaforma BI. L'host è configurato per contenere tre nodi:
 - NodeMars contiene un Central Management Server (`NodeMars.CMS`) con un servizio che fornisce i servizi CMS. La presenza di CMS su due computer consente il bilanciamento del carico e funzionalità di prevenzione e failover.
 - NodeJupiter contiene un server di elaborazione di Web Intelligence (`NodeJupiter.WebIntelligence`) dotato di un servizio che fornisce la funzionalità di creazione di report Web Intelligence e un Event Server (`NodeJupiter.EventServer`) per consentire il monitoraggio di report dei file.
 - NodeSaturn contiene un Adaptive Processing Server (`NodeSaturn.APS`) dotato di un servizio che fornisce il controllo dei client.

3.2.1 Modifiche al server dalla versione XI 3.1

La seguente tabella illustra le maggiori modifiche apportate ai server della piattaforma BI dalla versione XI 3.1. I tipi di modifiche includono:

- Server il cui nome è stato modificato fra una versione e l'altra, pur fornendo funzionalità identiche o simili.
- Server che non vengono più offerti nelle versioni più recenti.
- Servizi comuni o correlati che sono stati consolidati nei server Adaptive.

Ad esempio, i servizi di pianificazione offerti dai singoli server Job in XI 3.1 sono stati spostati in Adaptive Job Server in 4.0.

- Nuovi server introdotti.

Tabella 3 - 1: Modifiche ai server

XI 3.1	4.0	4.0 Feature Pack 3	4.1
Connection Server [1]	Connection Server Connection Server 32	Connection Server Connection Server 32	Connection Server Connection Server 32

XI 3.1	4.0	4.0 Feature Pack 3	4.1
Crystal Reports Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Crystal Reports Processing Server	Servizio di elaborazione di Crystal Reports 2011 Server di elaborazione Crystal Reports (per i report di SAP Crystal Reports for Enterprise)	Servizio di elaborazione di Crystal Reports 2011 Server di elaborazione Crystal Reports (per i report di SAP Crystal Reports for Enterprise)	Servizio di elaborazione di Crystal Reports 2011 Server di elaborazione Crystal Reports (per i report di SAP Crystal Reports for Enterprise)
Dashboard Server (Dashboard Builder) [2]	Dashboard Server (Spazi di lavoro BI)	Non disponibile a partire da 4.0 Feature Pack 3	Non disponibile in 4.1
Dashboard Analytics Server (Dashboard Builder) [2]	Dashboard Analytics Server (Spazi di lavoro BI)	Non disponibile a partire da 4.0 Feature Pack 3	Non disponibile in 4.1
Desktop Intelligence Cache Server [3]	Non disponibile a partire da 4.0	Non disponibile a partire da 4.0	Non disponibile in 4.1 [3]
Desktop Intelligence Job Server [3]	Non disponibile a partire da 4.0	Non disponibile a partire da 4.0	Non disponibile in 4.1 [3]
Server di elaborazione Desktop Intelligence [3]	Non disponibile a partire da 4.0	Non disponibile a partire da 4.0	Non disponibile in 4.1 [3]
Destination Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Server elenco dei valori	Server di elaborazione Web Intelligence	Server di elaborazione Web Intelligence	Server di elaborazione Web Intelligence
Multi-Dimensional Analysis Server	Adaptive Processing Server	Adaptive Processing Server	Adaptive Processing Server
Program Job Server	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)	Crystal Reports 2011 Report Application Server (RAS)
Job Server Web Intelligence	Adaptive Job Server	Adaptive Job Server	Adaptive Job Server
Server cache Xcelsius [4]	Server cache Dashboard Design (Xcelsius) [5]	Server cache Dashboards (Xcelsius)	Server cache Dashboards (Xcelsius)

XI 3.1	4.0	4.0 Feature Pack 3	4.1
Server di elaborazione Xcelsius [4]	Server di elaborazione Dashboard Design (Xcelsius) [5]	Server di elaborazione Dashboards (Xcelsius)	Server di elaborazione Dashboards (Xcelsius)

- [1] In 4.0, il Connection Server 32 è a 32 bit ed esegue connessioni in modo specifico a origini dati che non sono in grado di gestire il middleware a 64 bit. Il Connection Server è a 64 bit ed esegue connessioni a tutte le altre origini dati. Per ulteriori informazioni, consultare il *Manuale dell'Accesso ai dati*.
- [2] Il server Dashboard e Dashboard Analytics sono stati rimossi dalla versione 4.0 Feature Pack 3. La configurazione del server non è più richiesta per la funzionalità relativa agli spazi di lavoro BI (in precedenza Dashboard Builder in XI 3.1).
- [3] Desktop Intelligence non era disponibile nella versione 4.0 e nei relativi pacchetti di manutenzione. L'applicazione client Desktop Intelligence è disponibile nella versione 4.1, tuttavia in tale versione non sono disponibili i server Desktop Intelligence. I report Desktop Intelligence possono essere convertiti in documenti Web Intelligence utilizzando lo Strumento di conversione dei report.
- [4] La cache Xcelsius e i servizi di elaborazione sono stati introdotti a partire dalla versione XI 3.1 Service Pack 3 per ottimizzare le richieste Query come servizio Web sulle origini di dati relazionali da Xcelsius. Servizi di elaborazione e cache equivalenti sono disponibili sul server di elaborazione Dashboards e il server cache di Dashboards 4.0 Feature Pack 3.
- [5] I server Dashboard Design in 4.0 sono stati rinominati in Dashboards in 4.0 Feature Pack 3 per rispecchiare le modifiche di denominazione del prodotto apportate a SAP BusinessObjects Dashboards.

3.2.2 Servizi

Quando si aggiungono server, è necessario includere alcuni servizi sull'Adaptive Job Server, ad esempio, il Servizio di pianificazione consegna di destinazione.

Nota:

nelle prossime versioni di manutenzione potrebbero essere aggiunti nuovi servizi o tipi di server.

Servizio	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio di connessione adattivo	Servizi di connessione	Adaptive Processing Server	Offre servizi di connettività per i driver basati su Java

Servizio	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio di pianificazione aggiornamento autenticazione	Servizi principali	Adaptive Job Server	Fornisce la sincronizzazione degli aggiornamenti per i plug-in di protezione di terze parti
Servizio applicazione Web BEx	Analysis Services	Adaptive Processing Server	Fornisce l'integrazione delle applicazioni Web SAP Business Warehouse (BW) Business Explorer (BEx) con BI Launch Pad
Servizio applicazione Web BOE	Servizi principali	Server del contenitore di applicazioni Web	Fornisce applicazioni Web per WACS, inclusi CMC (Central Management Console), BI Launch Pad e OpenDocument
Servizio Business Process BI	Servizi principali	Server del contenitore di applicazioni Web	Fornisce i servizi Web BI Business Process per WACS, consentendo l'incorporazione della tecnologia BI nelle applicazioni Web. Il servizio BI Business Process è obsoleto.
Servizio Central Management	Servizi principali	Central Management Server	Fornisce funzionalità di gestione di server, utenti, gestione delle sessioni e protezione (diritti di accesso e autenticazione). Affinché il cluster possa funzionare, è necessario che sia disponibile almeno un servizio Central Management nel cluster.
Servizio proxy controllo client	Servizi principali	Adaptive Processing Server	Raccoglie gli eventi di controllo inviati dai client e li inoltra al server CMS

Servizio	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio di elaborazione Crystal Reports 2011	Servizi Crystal Reports	Crystal Reports Processing Server	Accetta ed elabora i report Crystal Reports 2011; è in grado di condividere i dati contenuti in più report per ridurre il numero di accessi al database
Servizio di pianificazione Crystal Reports 2011	Servizi Crystal Reports	Adaptive Job Server	Esegue i processi pianificati di una versione precedente di Crystal Reports e pubblica i risultati in una determinata posizione di output
Servizio di modifica e visualizzazione Crystal Reports 2011	Servizi Crystal Reports	Report Application Server (RAS)	Elabora le richieste di visualizzazione e modifica per i report Crystal Reports 2011.
Servizio cache Crystal Reports	Servizi Crystal Reports	Crystal Reports Cache Server	Limita il numero di accessi al database generati dai report Crystal e velocizza la generazione di report mediante la gestione di una cache di report
Servizio di elaborazione Crystal Reports	Servizi Crystal Reports	Crystal Reports Processing Server	Accetta ed elabora i report Crystal; è in grado di condividere i dati contenuti in più report per ridurre il numero di accessi al database
Servizio di pianificazione Crystal Reports	Servizi Crystal Reports	Adaptive Job Server	Esegue i processi pianificati di una versione nuova di Crystal Reports e pubblica i risultati in una determinata posizione di output

Servizio	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio di accesso ai dati personalizzato	Servizi Web Intelligence	Adaptive Processing Server	Fornisce connessioni dinamiche a origini dati che non richiedono un Connection Server. Questo servizio consente di accedere e aggiornare i report creati utilizzando alcuni fornitori di dati personali quali file CSV. Consultare <i>Manuale dell'utente di SAP BusinessObjects Web Intelligence Rich Client</i> per ulteriori informazioni sulla creazione di una query o l'aggiornamento di un documento basato su un file di testo.
Servizio cache Dashboards	Servizi Dashboards	Server cache di Dashboards	Limita il numero di accessi al database generati dai report Dashboards e velocizza la generazione di report mediante la gestione di una cache di report
Servizio elaborazione di Dashboards	Servizi Dashboards	Server di elaborazione di Dashboards	Accetta ed elabora i report Dashboards; è in grado di condividere i dati contenuti in più report per ridurre il numero di accessi al database
Servizio Data Federation	Servizi Data Federation	Adaptive Processing Server	Esegue query sulle origini dati sottostanti ed elabora queste ultime per un universo con più origini

Servizio	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio di pianificazione consegna di destinazione	Servizi principali	Adaptive Job Server	Esegue i processi pianificati e pubblica i risultati in una posizione di output, ad esempio file system, server FTP, posta elettronica o la posta in arrivo di un utente Nota: Quando si aggiungono server, è necessario includere alcuni servizi di Adaptive Job Server, fra cui questo servizio.
Servizio di recupero documenti	Servizi Web Intelligence	Adaptive Processing Server	Salvataggio automatico e ripristino di documenti Web Intelligence
Servizio DSL Bridge	Servizi Web Intelligence	Adaptive Processing Server	Supporto per la sessione DSL (Dimensional Semantic Layer)
Servizio eventi	Servizi principali	Event Server	Controlla la presenza di eventi di file in un File Repository Server (FRS) e attiva i report da eseguire quando richiesto
Servizio di accesso ai dati di Excel	Servizi Web Intelligence	Adaptive Processing Server	Supporta i file Excel caricati nella piattaforma BI come origini dati. Consultare <i>Manuale dell'utente di SAP BusinessObjects Web Intelligence Rich Client</i> per ulteriori informazioni sulla creazione di una query o l'aggiornamento di un documento basato su un file Excel.

Servizio	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio Information Engine	Servizi Web Intelligence	Server di elaborazione Web Intelligence	Servizio richiesto per l'elaborazione di documenti Web Intelligence
Servizio archivio file di input	Servizi principali	Input File Repository Server	Gestisce i report pubblicati e gli oggetti programma che possono essere utilizzati per la generazione di nuovi report quando si riceve un file di input
Servizio Insight to Action	Servizi principali	Adaptive Processing Server	Consente di richiamare le azioni e offre supporto per RRI
Servizio ClearCase di Lifecycle Management	Servizi Lifecycle Management	Adaptive Processing Server	Fornisce il supporto ClearCase per LCM
Servizio di pianificazione di Lifecycle Management	Servizi Lifecycle Management	Adaptive Job Server	Esegue processi pianificati Lifecycle Management
Servizio Lifecycle Management	Servizi Lifecycle Management	Adaptive Processing Server	Servizio Lifecycle Management principale
Servizio di monitoraggio	Servizi principali	Adaptive Processing Server	Fornisce funzioni di monitoraggio
Servizio di analisi multidimensionali	Analysis Services	Adaptive Processing Server	Assicura l'accesso ai dati OLAP (Online Analytical Processing) multidimensionali; converte i dati non elaborati in formato XML, che può essere visualizzato in Excel, PDF o nelle tabelle a campi incrociati e nei grafici di Analysis (in precedenza Voyager)

Servizio	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio di connessione nativo	Servizi di connessione	Connection Server	Fornisce servizi di connettività nativi per l'architettura a 64 bit
Servizio di connettività nativo (32 bit)	Servizi di connessione	Connection Server	Fornisce servizi di connettività nativi per l'architettura a 32 bit
Servizio archivio file di output	Servizi principali	Output File Repository Server	Gestisce una raccolta di documenti completati
Servizio di pianificazione ricerca piattaforma	Servizi principali	Adaptive Job Server	Esegue una ricerca pianificata per indicizzare tutto il contenuto del repository CMS (Central Management Server)
Servizio di ricerca piattaforma	Servizi principali	Adaptive Processing Server	Fornisce la funzionalità di ricerca per la piattaforma BI
Servizio di pianificazione metriche	Servizi principali	Adaptive Job Server	Fornisce i processi pianificati dei probe e pubblica i risultati in una posizione di output
Servizio di pianificazione programma	Servizi principali	Adaptive Job Server	Esegue i programmi la cui esecuzione è stata pianificata in un determinato orario
Servizio di pianificazione pubblicazione	Servizi principali	Adaptive Job Server	Esegue i processi di pubblicazione pianificati e pubblica i risultati in una posizione di output
Servizio di post-elaborazione pubblicazione	Servizi principali	Adaptive Processing Server	Esegue operazioni sui report dopo il completamento, ad esempio l'invio di report a una posizione di output

Servizio	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio di pubblicazione	Servizi principali	Adaptive Processing Server	Si coordina con il servizio di post-elaborazione pubblicazione e il servizio di destinazione per la pubblicazione dei report in una posizione di output, ad esempio file system, server FTP, posta elettronica o la casella posta in arrivo di un utente
Servizio Rebean	Servizi Web Intelligence	Adaptive Processing Server	SDK utilizzato da Web Intelligence ed Explorer
Servizio di replica	Servizi principali	Adaptive Job Server	Esegue processi di federazione pianificati per replicare i contenuti tra i siti federati
Servizio Web RESTful	Servizi principali	Server contenitore applicazioni Web (WACS)	Fornisce la gestione di sessione delle richieste Servizio Web RESTful.
Servizio di pianificazione query di protezione	Servizi principali	Adaptive Job Server	Esegue i processi di Query protezione pianificati
Servizio token di protezione	Servizi principali	Adaptive Processing Server	Supporto Single Sign On SAP
Servizio di traduzione	Servizi principali	Adaptive Processing Server	Traduce elementi InfoObject con l'input proveniente dal client di Translation Manager
Servizio di pianificazione differenza visiva	Servizi Lifecycle Management	Adaptive Job Server	Esegue processi pianificati di Differenza visiva (Lifecycle Management) e pubblica i risultati in una posizione di output

Servizio	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio Differenza visiva	Servizi Lifecycle Management	Adaptive Processing Server	Determina se i documenti sono visivamente identici per la promozione di documenti e Lifecycle Management
Servizio di visualizzazione	Servizi Web Intelligence	Adaptive Processing Server	Un servizio modello di oggetto visualizzazione comune utilizzato da Web Intelligence
Servizio comune di Web Intelligence	Servizi Web Intelligence	Server di elaborazione Web Intelligence	Supporta l'elaborazione di documenti Web Intelligence
Servizio principale di Web Intelligence	Servizi Web Intelligence	Server di elaborazione Web Intelligence	Supporta l'elaborazione di documenti Web Intelligence
Servizio di elaborazione di Web Intelligence	Servizi Web Intelligence	Server di elaborazione Web Intelligence	Accetta ed elabora i documenti Web Intelligence
Servizio di pianificazione di Web Intelligence	Servizi Web Intelligence	Adaptive Job Server	Consente il supporto di processi Web Intelligence pianificati
SDK di servizi Web e servizio QaaWS	Servizi principali	Server del contenitore di applicazioni Web	Servizi Web su WACS

3.2.3 Categorie di servizio

Nota:

nelle prossime versioni di manutenzione potrebbero essere aggiunti nuovi servizi o tipi di server.

Categoria del servizio	Servizio	Tipo server
Analysis Services	Servizio applicazione Web BEx	Adaptive Processing Server

Categoria del servizio	Servizio	Tipo server
Analysis Services	Servizio di analisi multidimensionali	Adaptive Processing Server
Servizi di connessione	Servizio di connessione adattivo	Adaptive Processing Server
Servizi di connessione	Servizio di connessione nativo	Connection Server
Servizi di connessione	Servizio di connettività nativo (32 bit)	Connection Server
Servizi principali	Servizio di pianificazione aggiornamento autenticazione	Adaptive Job Server
Servizi principali	Servizio Central Management	Central Management Server
Servizi principali	Servizio proxy controllo client	Adaptive Processing Server
Servizi principali	Servizio cruscotto	Dashboard Server
Servizi principali	Servizio di configurazione destinazione	Adaptive Job Server
Servizi principali	Servizio di pianificazione consegna di destinazione	Adaptive Job Server
Servizi principali	Servizio eventi	Event Server
Servizi principali	Servizio Insight to Action	Adaptive Processing Server
Servizi principali	Servizio archivio file di input	Input File Repository Server
Servizi principali	Servizio di monitoraggio	Adaptive Processing Server
Servizi principali	Servizio archivio file di output	Output File Repository Server
Servizi principali	Servizio di pianificazione ricerca piattaforma	Adaptive Job Server
Servizi principali	Servizio di ricerca piattaforma	Adaptive Processing Server
Servizi principali	Servizio di pianificazione metriche	Adaptive Job Server
Servizi principali	Servizio di pianificazione programma	Adaptive Job Server
Servizi principali	Servizio di pianificazione pubblicazione	Adaptive Job Server
Servizi principali	Servizio di post-elaborazione pubblicazione	Adaptive Processing Server

Categoria del servizio	Servizio	Tipo server
Servizi principali	Servizio di pubblicazione	Adaptive Processing Server
Servizi principali	Servizio di replica	Adaptive Job Server
Servizi principali	Servizio Web RESTful	Server del contenitore di applicazioni Web
Servizi principali	Servizio di pianificazione query di protezione	Adaptive Job Server
Servizi principali	Servizio token di protezione	Adaptive Processing Server
Servizi principali	Servizio Single Sign-On	Central Management Server, Connection Server, server di elaborazione Crystal Reports, RAS, server di elaborazione di Dashboards e server di elaborazione di Web Intelligence
Servizi principali	Servizio log analisi	Qualsiasi server
Servizi principali	Servizio di traduzione	Adaptive Processing Server
Servizi principali	Servizio di pianificazione importazione gruppi e utenti	Adaptive Job Server
Servizi principali	Servizio contenitore applicazioni Web	Server del contenitore di applicazioni Web
Servizi Crystal Reports	Servizio di elaborazione Crystal Reports 2011	Crystal Reports Processing Server
Servizi Crystal Reports	Servizio di pianificazione Crystal Reports 2011	Adaptive Job Server
Servizi Crystal Reports	Servizio di modifica e visualizzazione Crystal Reports 2011	Report Application Server (RAS)
Servizi Crystal Reports	Servizio cache Crystal Reports	Crystal Reports Cache Server
Servizi Crystal Reports	Servizio di elaborazione Crystal Reports	Crystal Reports Processing Server
Servizi Crystal Reports	Servizio di pianificazione Crystal Reports	Adaptive Job Server
Servizi Dashboards	Servizio cache Dashboards	Server cache di Dashboards
Servizi Dashboards	Servizio elaborazione di Dashboards	Server di elaborazione di Dashboards

Categoria del servizio	Servizio	Tipo server
Servizi Data Federation	Servizio Data Federation	Adaptive Processing Server
Servizi Lifecycle Management	Servizio ClearCase di Lifecycle Management	Adaptive Processing Server
Servizi Lifecycle Management	Servizio di pianificazione di Lifecycle Management	Adaptive Job Server
Servizi Lifecycle Management	Servizio Lifecycle Management	Adaptive Processing Server
Servizi Lifecycle Management	Servizio di pianificazione differenza visiva	Adaptive Job Server
Servizi Lifecycle Management	Servizio Differenza visiva	Adaptive Processing Server
Servizi Web Intelligence	Servizio di accesso ai dati personalizzato	Adaptive Processing Server
Servizi Web Intelligence	Servizio di recupero documenti	Adaptive Processing Server
Servizi Web Intelligence	Servizio DSL Bridge	Adaptive Processing Server
Servizi Web Intelligence	Servizio di accesso ai dati di Excel	Adaptive Processing Server
Servizi Web Intelligence	Servizio Information Engine	Server di elaborazione Web Intelligence
Servizi Web Intelligence	Servizio Rebean	Adaptive Processing Server
Servizi Web Intelligence	Servizio di visualizzazione	Adaptive Processing Server
Servizi Web Intelligence	Servizio comune di Web Intelligence	Server di elaborazione Web Intelligence
Servizi Web Intelligence	Servizio principale di Web Intelligence	Server di elaborazione Web Intelligence
Servizi Web Intelligence	Servizio di monitoraggio Web Intelligence	Adaptive Processing Server
Servizi Web Intelligence	Servizio di elaborazione di Web Intelligence	Server di elaborazione Web Intelligence
Servizi Web Intelligence	Servizio di pianificazione di Web Intelligence	Adaptive Job Server

3.2.4 Tipi di server

Un asterisco accanto al nome di un servizio indica che si tratta di un servizio secondario. Alcuni servizi secondari vengono creati automaticamente, tuttavia è necessario scegliere di includere altri servizi secondari dopo aver selezionato il servizio principale dal quale dipende un servizio secondario.

Nota:

nelle prossime versioni di manutenzione potrebbero essere aggiunti nuovi servizi o tipi di server.

Tipo server	Servizio	Categoria del servizio
Qualsiasi server	Servizio log analisi	Servizi principali
Adaptive Job Server	Servizio di pianificazione aggiornamento autenticazione	Servizi principali
Adaptive Job Server	Servizio di pianificazione Crystal Reports 2011	Servizi Crystal Reports
Adaptive Job Server	Servizio di pianificazione Crystal Reports	Servizi Crystal Reports
Adaptive Job Server	Servizio di configurazione destinazione	Servizi principali
Adaptive Job Server	Servizio di pianificazione consegna di destinazione	Servizi principali
Adaptive Job Server	Servizio di pianificazione di Lifecycle Management	Servizi Lifecycle Management
Adaptive Job Server	Servizio di pianificazione ricerca piattaforma	Servizi principali
Adaptive Job Server	Servizio di pianificazione metriche	Servizi principali
Adaptive Job Server	Servizio di pianificazione programma	Servizi principali
Adaptive Job Server	Servizio di pianificazione pubblicazione	Servizi principali
Adaptive Job Server	Servizio di replica	Servizi principali
Adaptive Job Server	Servizio di pianificazione query di protezione	Servizi principali

Tipo server	Servizio	Categoria del servizio
Adaptive Job Server	Servizio di pianificazione importazione gruppi e utenti	Servizi principali
Adaptive Job Server	Servizio di pianificazione differenza visiva	Servizi Lifecycle Management
Adaptive Job Server	Servizio di pianificazione di Web Intelligence	Servizi Web Intelligence
Adaptive Processing Server	Servizio di connessione adattivo	Servizi di connessione
Adaptive Processing Server	Servizio applicazione Web BEx	Analysis Services
Adaptive Processing Server	Servizio proxy controllo client	Servizi principali
Adaptive Processing Server	Servizio di accesso ai dati personalizzato	Servizi Web Intelligence
Adaptive Processing Server	Servizio Data Federation	Servizi Data Federation
Adaptive Processing Server	Servizio di recupero documenti	Servizi Web Intelligence
Adaptive Processing Server	Servizio DSL Bridge	Servizi Web Intelligence
Adaptive Processing Server	Servizio di accesso ai dati di Excel	Servizi Web Intelligence
Adaptive Processing Server	Servizio Insight to Action	Servizi principali
Adaptive Processing Server	Servizio ClearCase di Lifecycle Management	Servizi Lifecycle Management
Adaptive Processing Server	Servizio Lifecycle Management	Servizi Lifecycle Management
Adaptive Processing Server	Servizio di monitoraggio	Servizi principali
Adaptive Processing Server	Servizio di analisi multidimensionali	Analysis Services
Adaptive Processing Server	Servizio di ricerca piattaforma	Servizi principali
Adaptive Processing Server	Servizio di post-elaborazione pubblicazione	Servizi principali
Adaptive Processing Server	Servizio di pubblicazione	Servizi principali
Adaptive Processing Server	Servizio Rebean	Servizi Web Intelligence
Adaptive Processing Server	Servizio token di protezione	Servizi principali
Adaptive Processing Server	Servizio di traduzione	Servizi principali

Tipo server	Servizio	Categoria del servizio
Adaptive Processing Server	Servizio Differenza visiva	Servizi Lifecycle Management
Adaptive Processing Server	Servizio di visualizzazione	Servizi Web Intelligence
Adaptive Processing Server	Servizio di monitoraggio Web Intelligence	Servizi Web Intelligence
Central Management Server	Servizio Central Management	Servizi principali
Central Management Server	Servizio Single Sign-On	Servizi principali
Connection Server	Servizio di connessione nativo	Servizi di connessione
Connection Server	Servizio di connettività nativo (32 bit)	Servizi di connessione
Connection Server	Servizio Single Sign-On	Servizi principali
Crystal Reports Cache Server	Servizio cache Crystal Reports	Servizi Crystal Reports
Crystal Reports Processing Server	Servizio di elaborazione Crystal Reports 2011	Servizi Crystal Reports
Crystal Reports Processing Server	Servizio di elaborazione Crystal Reports	Servizi Crystal Reports
Crystal Reports Processing Server	Servizio Single Sign-On	Servizi principali
Server cache di Dashboards	Servizio cache Dashboards	Servizi Dashboards
Server di elaborazione di Dashboards	Servizio elaborazione di Dashboards	Servizi Dashboards
Server di elaborazione di Dashboards	Servizio Single Sign-On	Servizi principali
Dashboard Server	Servizio cruscotto	Servizi principali
Event Server	Servizio eventi	Servizi principali
Input File Repository Server	Servizio archivio file di input	Servizi principali
Output File Repository Server	Servizio archivio file di output	Servizi principali
Report Application Server (RAS)	Servizio di modifica e visualizzazione Crystal Reports 2011	Servizi Crystal Reports
RAS	Servizio Single Sign-On	Servizi principali
Server del contenitore di applicazioni Web	Servizio Web RESTful	Servizi principali

Tipo server	Servizio	Categoria del servizio
Server del contenitore di applicazioni Web	Servizio contenitore applicazioni Web	Servizi principali
Server di elaborazione Web Intelligence	Servizio Information Engine	Servizi Web Intelligence
Server di elaborazione Web Intelligence	Servizio Single Sign-On	Servizi principali
Server di elaborazione Web Intelligence	Servizio comune di Web Intelligence	Servizi Web Intelligence
Server di elaborazione Web Intelligence	Servizio principale di Web Intelligence	Servizi Web Intelligence
Server di elaborazione Web Intelligence	Servizio di elaborazione di Web Intelligence	Servizi Web Intelligence

Tipo server	Servizio	Categoria del servizio
Adaptive Job Server	Servizio di pianificazione aggiornamento autenticazione	Servizi principali
Adaptive Job Server	Servizio di pianificazione Crystal Reports 2011	Servizi Crystal Reports
Adaptive Job Server	Servizio di pianificazione Crystal Reports	Servizi Crystal Reports
Adaptive Job Server	Servizio di pianificazione consegna di destinazione	Servizi principali
Adaptive Job Server	Servizio di pianificazione di Lifecycle Management	Servizi Lifecycle Management
Adaptive Job Server	Servizio di pianificazione ricerca piattaforma	Servizi principali
Adaptive Job Server	Servizio di pianificazione metriche	Servizi principali
Adaptive Job Server	Servizio di pianificazione programma	Servizi principali
Adaptive Job Server	Servizio di pianificazione pubblicazione	Servizi principali
Adaptive Job Server	Servizio di replica	Servizi principali

Tipo server	Servizio	Categoria del servizio
Adaptive Job Server	Servizio di pianificazione query di protezione	Servizi principali
Adaptive Job Server	Servizio di pianificazione differenza visiva	Servizi Lifecycle Management
Adaptive Job Server	Servizio di pianificazione di Web Intelligence	Servizi Web Intelligence
Adaptive Processing Server	Servizio di connessione adattivo	Servizi di connessione
Adaptive Processing Server	Servizio applicazione Web BEx	Analysis Services
Adaptive Processing Server	Servizio proxy controllo client	Servizi principali
Adaptive Processing Server	Servizio di accesso ai dati personalizzato	Servizi Web Intelligence
Adaptive Processing Server	Servizio Data Federation	Servizi Data Federation
Adaptive Processing Server	Servizio di recupero documenti	Servizi Web Intelligence
Adaptive Processing Server	Servizio DSL Bridge	Servizi Web Intelligence
Adaptive Processing Server	Servizio di accesso ai dati di Excel	Servizi Web Intelligence
Adaptive Processing Server	Servizio Insight to Action	Servizi principali
Adaptive Processing Server	Servizio ClearCase di Lifecycle Management	Servizi Lifecycle Management
Adaptive Processing Server	Servizio Lifecycle Management	Servizi Lifecycle Management
Adaptive Processing Server	Servizio di monitoraggio	Servizi principali
Adaptive Processing Server	Servizio di analisi multidimensionali	Analysis Services
Adaptive Processing Server	Servizio di ricerca piattaforma	Servizi principali
Adaptive Processing Server	Servizio di post-elaborazione pubblicazione	Servizi principali
Adaptive Processing Server	Servizio di pubblicazione	Servizi principali
Adaptive Processing Server	Servizio Rebean	Servizi Web Intelligence
Adaptive Processing Server	Servizio token di protezione	Servizi principali
Adaptive Processing Server	Servizio di traduzione	Servizi principali

Tipo server	Servizio	Categoria del servizio
Adaptive Processing Server	Servizio Differenza visiva	Servizi Lifecycle Management
Adaptive Processing Server	Servizio di visualizzazione	Servizi Web Intelligence
Central Management Server	Servizio Central Management	Servizi principali
Connection Server	Servizio di connessione nativo	Servizi di connessione
Connection Server	Servizio di connettività nativo (32 bit)	Servizi di connessione
Crystal Reports Cache Server	Servizio cache Crystal Reports	Servizi Crystal Reports
Crystal Reports Processing Server	Servizio di elaborazione Crystal Reports 2011	Servizi Crystal Reports
Crystal Reports Processing Server	Servizio di elaborazione Crystal Reports	Servizi Crystal Reports
Server cache di Dashboards	Servizio cache Dashboards	Servizi Dashboards
Server di elaborazione di Dashboards	Servizio elaborazione di Dashboards	Servizi Dashboards
Dashboard Server	Servizio cruscotto	Servizi principali
Event Server	Servizio eventi	Servizi principali
Input File Repository Server	Servizio archivio file di input	Servizi principali
Output File Repository Server	Servizio archivio file di output	Servizi principali
Report Application Server (RAS)	Servizio di modifica e visualizzazione Crystal Reports 2011	Servizi Crystal Reports
Server del contenitore di applicazioni Web	Servizio Web RESTful	Servizi principali
Server di elaborazione Web Intelligence	Servizio Information Engine	Servizi Web Intelligence
Server di elaborazione Web Intelligence	Servizio comune di Web Intelligence	Servizi Web Intelligence
Server di elaborazione Web Intelligence	Servizio principale di Web Intelligence	Servizi Web Intelligence
Server di elaborazione Web Intelligence	Servizio di elaborazione di Web Intelligence	Servizi Web Intelligence

3.2.5 Server

I server sono raccolte di servizi eseguiti su un host mediante Server Intelligence Agent (SIA). Il tipo di server viene definito in base ai servizi eseguiti al suo interno. I server possono essere creati in Central Management Console (CMC). Nella tabella che segue sono riportati i diversi tipi di server che possono essere creati nella console CMC.

Server	Descrizione
Adaptive Job Server	Server generico che elabora processi pianificati. Quando si aggiunge un Job Server al sistema della piattaforma BI, è possibile configurarlo in modo da elaborare report, documenti, programmi o pubblicazioni e inviare i risultati a destinazioni differenti.
Adaptive Processing Server	<p>Server generico che ospita i servizi responsabili dell'elaborazione di richieste provenienti da diverse origini.</p> <p>Il programma di installazione installa un Adaptive Processing Server (APS) per sistema host. In base alle funzionalità installate, il server APS può ospitare un numero elevato di servizi, tra cui il servizio di monitoraggio, il servizio Lifecycle Management, il servizio di analisi multidimensionale (MDAS), quello di pubblicazione e altri ancora.</p> <p>Per i sistemi di produzione o di test, la procedura consigliata consiste nel creare ulteriori APS e nel configurarli in base alle specifiche esigenze aziendali. Per ulteriori informazioni, consultare Introduzione alla Configurazione guidata del sistema e Configurazione degli Adaptive Processing Server per i sistemi di produzione.</p>
Central Management Server (CMS)	Gestisce un database di informazioni sul sistema della piattaforma BI (nel database di sistema CMS) e le azioni utente sottoposte a controllo (nell'archivio dati di controllo). Tutti i servizi della piattaforma sono gestiti dal server CMS. Il CMS controlla anche l'accesso ai file di sistema in cui sono memorizzati i documenti e le informazioni su utenti, gruppi di utenti, livelli di protezione (inclusa l'autenticazione e l'autorizzazione) e il contenuto.
Connection Server	Fornisce l'accesso al database dei dati di origine. Supporta i database relazionali, nonché OLAP e altri formati. Il Connection Server è responsabile della gestione della connessione e dell'interazione con le varie origini dati e della fornitura di un insieme di funzionalità comuni ai client.

Server	Descrizione
Crystal Reports Cache Server	Intercetta le richieste di report inviate dai client al Page Server. Se il Cache Server non è in grado di soddisfare la richiesta con una pagina di report memorizzata, passa la richiesta al server di elaborazione Crystal Reports, il quale esegue il report e restituisce i risultati. Il Cache Server memorizza quindi la pagina del report per consentirne l'eventuale utilizzo in futuro.
Crystal Reports Processing Server	Risponde alle richieste di pagina elaborando report e generando pagine EPF (Encapsulated Page Format). Il vantaggio principale del formato EPF è che supporta l'accesso alla pagina su richiesta in modo che venga restituita solo la pagina richiesta, non l'intero report. Le prestazioni del sistema risultano migliorate e il traffico di rete viene ridotto sensibilmente per i report di grandi dimensioni.
Server cache di Dashboards	Intercetta le richieste di report inviate dai client a Dashboard Server. Se il Cache Server non è in grado di soddisfare la richiesta con una pagina di report memorizzata, passa la richiesta a Dashboard Server, il quale esegue il report e restituisce i risultati. Il Cache Server memorizza quindi la pagina del report per consentirne l'eventuale utilizzo in futuro.
Server di elaborazione di Dashboards	Risponde alle richieste di Dashboards elaborando report e generando pagine EPF (Encapsulated Page Format). Il vantaggio principale del formato EPF è che supporta l'accesso alla pagina su richiesta in modo che venga restituita solo la pagina richiesta, non l'intero report. Le prestazioni del sistema risultano migliorate e il traffico di rete viene ridotto sensibilmente per i report di grandi dimensioni.
Event Server	Monitora gli eventi del sistema, che possono avere la funzione di trigger per l'esecuzione di un report. Quando si imposta l'attivazione di un evento, Event Server monitora la condizione e invia una notifica al server CMS per segnalare che si è verificato un evento. Il server CMS avvia quindi qualsiasi processo dipendente dall'evento. Event Server gestisce gli eventi basati su file che si verificano nel livello di archiviazione.

Server	Descrizione
File Repository Server	Responsabile della creazione di oggetti del file system, quali report esportati e file importati in formati non nativi. Un FRS di input memorizza gli oggetti report e programma che sono stati pubblicati nel sistema dagli amministratori o dagli utenti finali. Un FRS di output memorizza tutte le istanze di report generate dal Job Server.
Server di elaborazione Web Intelligence	Elabora documenti SAP BusinessObjects Web Intelligence.
Report Application Server	Offre funzionalità per la creazione di report ad-hoc che consentono agli utenti di creare e modificare report Crystal utilizzando l'SDK (Software Development Kit) di SAP Crystal Reports Server Embedded.

3.3 Applicazioni client

È possibile interagire con la piattaforma BI mediante due tipi principali di applicazioni client:

- Applicazioni desktop

Tali applicazioni devono essere installate in un sistema operativo Microsoft Windows supportato e sono in grado di elaborare dati e creare report a livello locale.

Nota:

Il programma di installazione della piattaforma BI non installa più le applicazioni desktop. Per installare le applicazioni desktop in un server, utilizzare il programma di installazione autonomo Strumenti client della piattaforma SAP BusinessObjects Business Intelligence.

I client desktop consentono di ridurre il carico di lavoro dovuto all'elaborazione di report BI su alcuni computer. La maggior parte delle applicazioni desktop accede direttamente ai dati di un'organizzazione tramite driver installati sul desktop e comunica con la distribuzione della piattaforma BI tramite CORBA o SSL CORBA crittografato.

Tali applicazioni includono Crystal Reports e Live Office.

Nota:

Benché Live Office sia un'applicazione ricca di funzionalità, si interfaccia con i servizi Web della piattaforma BI via HTTP.

- Applicazioni Web

Queste applicazioni risiedono su un server di applicazioni Web ed è possibile accedervi tramite un browser Web supportato sui sistemi operativi Windows, Macintosh, Unix e Linux.

Ciò consente di fornire accesso BI (business intelligence) a grandi gruppi di utenti, senza la necessità di dover distribuire prodotti software desktop. La comunicazione viene gestita via HTTP, con o senza crittografia SSL (HTTPS).

Alcuni esempi di questo tipo di applicazione sono BI Launch Pad, SAP BusinessObjects Web Intelligence, la Central Management Console (CMC) e i visualizzatori di report.

3.3.1 Installato con gli Strumenti client della piattaforma SAP BusinessObjects Business Intelligence

3.3.1.1 Web Intelligence Rich Client

Web Intelligence Rich Client è uno strumento di analisi e creazione report ad-hoc disponibile per gli utenti aziendali con o senza accesso alla piattaforma BI.

Consente agli utenti business di accedere ai dati mediante universi (.unv e .unx), query BEx o altre origini utilizzando termini aziendali familiari in un'interfaccia di trascinamento e rilascio. I workflow consentono di analizzare le domande molto ampie o molto circoscritte e di porre ulteriori domande in qualsiasi fase del workflow di analisi.

Gli utenti di Web Intelligence Rich Client possono continuare a utilizzare i file dei documenti Web Intelligence (.wid) anche quando non sono in grado di connettersi a un CMS (Central Management Server).

3.3.1.2 Business View Manager

Business View Manager consente agli utenti di creare oggetti di livello semantico che semplificano la complessità del database sottostante.

Business View Manager consente di creare connessioni dati, connessioni dati dinamiche, basi dati, elementi aziendali, viste aziendali e viste relazionali. Consente inoltre di impostare la protezione dettagliata a livello di colonna e di riga per gli oggetti contenuti in un report.

I progettisti possono creare connessioni a più origini dati, unire le tabelle, creare alias dei nomi di campi, creare campi calcolati, quindi utilizzare la struttura semplificata come vista aziendale. Progettisti e utenti di report possono quindi utilizzare la vista aziendale come base per i propri report anziché creare le proprie query direttamente dai dati.

3.3.1.3 Strumento di conversione dei report

Lo Strumento di conversione dei report converte i report in formato Web Intelligence e li pubblica su un server CMS (Central Management Server).

I report possono essere recuperati dalle cartelle `Pubblica`, `Preferiti` o `Posta in arrivo` del CMS. Terminata la conversione, è possibile pubblicare i report nella stessa cartella del report Web Intelligence originale o in una cartella differente. Lo strumento non converte tutte le funzionalità e i report Web Intelligence. Il livello di conversione dipende dalle funzioni del report originale. Alcune funzioni impediscono la conversione del report, mentre altre vengono modificate, reimplementate o rimosse dallo strumento durante la conversione.

Lo Strumento di conversione dei report consente anche di controllare i report convertiti. Questa operazione agevola l'identificazione dei report che non sono stati convertiti totalmente dallo Strumento di conversione dei report e l'individuazione del motivo.

3.3.1.4 Universe Design Tool

Universe Designer Tool (in precedenza Universe Designer) consente ai progettisti di dati di combinare i dati provenienti da più origini in un livello semantico che nasconde la complessità del database agli utenti finali. Limita la complessità dei dati utilizzando un linguaggio aziendale anziché tecnico per accedere, modificare e organizzare i dati.

Universe Designer Tool offre un'interfaccia grafica per la selezione e la visualizzazione delle tabelle in un database. Le tabelle del database sono rappresentate come simboli di tabella nel diagramma di uno schema. I progettisti possono utilizzare questa interfaccia per manipolare tabelle, creare join tra tabelle, tabelle alias, contesti e risolvere loop negli schemi.

È anche possibile creare universi da origini metadati. Universe Designer Tool viene utilizzato per la generazione degli universi al termine del processo di creazione.

3.3.1.5 Query come servizio Web

Query come servizio Web è un'applicazione basata su procedure guidate che consente di creare query in un servizio Web e di integrarle in applicazioni predisposte per il Web. È possibile salvare le query per creare un catalogo di query standard selezionabili secondo le necessità.

Il contenuto di Business Intelligence (BI) è normalmente legato a una particolare interfaccia utente di strumenti BI. Nel caso di Query come servizio Web non è così, in quanto il contenuto BI può essere consegnato a qualsiasi interfaccia utente in grado di elaborare i servizi Web.

L'applicazione Query come servizio Web è progettata per essere utilizzata, come altri servizi Web, su qualsiasi applicazione Microsoft Windows. Query come servizio Web è basato sulle specifiche di servizio Web W3C SOAP, SDL e XML. È composto da due componenti principali:

- Componente server

Il componente server, incluso nella piattaforma BI, archivia il catalogo Query come servizio Web e ospita i servizi Web pubblicati.

- Strumento client

È questo il modo in cui gli utenti aziendali creano e pubblicano le query come servizio Web nel server. È possibile installare lo strumento client in diversi computer che possono accedere e condividere lo stesso catalogo memorizzato nel server. Lo strumento client comunica con i componenti server tramite servizi Web.

Query come servizio Web consente di utilizzare le query Web come parte di una gamma di soluzioni lato client, tra cui:

- Microsoft Office, Excel e InfoPath
- SAP NetWeaver
- OpenOffice
- Regole di business e applicazioni per la gestione dei processi
- Piattaforme Enterprise Service Bus

3.3.1.6 Information Design Tool

Information Design Tool (in precedenza Information Designer) è un ambiente di progettazione di metadati che consente di estrarre, definire e manipolare i metadati dalle origini relazionali e OLAP per creare e distribuire universi SAP BusinessObjects.

3.3.1.7 Translation Management Tool

La piattaforma BI fornisce il supporto per documenti e universi multilingue. Un documento multilingue contiene versioni localizzate dei metadati degli universi e i prompt del documento. Un utente può creare report, ad esempio, dallo stesso universo nelle lingue scelte.

Translation Management Tool (in precedenza Translation Manager) è lo strumento che definisce gli universi multilingue e gestisce la traduzione degli universi e di altre risorse analitiche nel repository CMS.

Translation Management Tool:

- Traduce l'universo o documenti per destinatari che utilizzano lingue diverse.
- Definisce le parti della lingua dei metadati di un documento e la traduzione appropriata. Genera un formato XLIFF esterno e importa i file XLIFF per ottenere informazioni tradotte.
- Elenca l'universo o la struttura del documento da tradurre.
- Consente di tradurre i metadati mediante l'interfaccia utente o uno strumento di traduzione esterno, importando ed esportando i file XLIFF.
- Crea documenti multilingue.

3.3.1.8 Strumento di amministrazione di Data Federation

Lo strumento di amministrazione di Data Federation (in precedenza Data Federator) è un'applicazione rich client che offre funzionalità facili da usare per la gestione del servizio Data Federation.

Completamente integrato nella piattaforma BI, il servizio Data Federation consente universi con più origini grazie alla distribuzione di query in più origini dati nonché la federazione dei dati tramite una sola base dati.

Lo strumento di amministrazione di Data Federation consente di ottimizzare le query Data Federation e ottimizzare il motore delle query Data Federation per ottenere le migliori prestazioni possibili.

Lo strumento di amministrazione Data Federation può essere utilizzato per effettuare le seguenti operazioni.

- Verificare le query SQL.
- Visualizzare i piani di ottimizzazione che descrivono in dettaglio la distribuzione delle query federate in ciascuna origine.
- Calcolare le “statistiche” e impostare i parametri di sistema per ottimizzare i servizi Data Federation e ottenere le migliori prestazioni possibili.
- Gestire le proprietà per controllare in che modo le query vengono eseguite in ciascuna origine dati al livello del connettore.
- Monitorare le query SQL in esecuzione.
- Sfogliare la cronologia delle query eseguite.

3.3.1.9 Widget per la piattaforma BI

I widget sono piccole applicazioni che consentono l'accesso agevole e rapido alle funzioni utilizzate con maggiore frequenza e forniscono informazioni visive dal desktop. I widget per la piattaforma BI (in

precedenza BI Widgets) consentono all'organizzazione di fornire l'accesso ai contenuti di Business Intelligence (BI) esistenti nella piattaforma BI. In alternativa, è possibile aggiungere applicazioni Web Dynpro registrate come widget XBCML (Extensible Business Client Markup Language) sui server SAP NetWeaver Application Server come widget del desktop.

Per eseguire il rendering di widget XBCML sul desktop dell'utente, si utilizza SAP Web Dynpro Flex Client. SAP Web Dynpro Flex Client è un motore di rendering basato su Adobe Flex utilizzato per il rendering di widget. Per informazioni dettagliate su come configurare le applicazioni Web Dynpro, vedere l'argomento *Abilitazione dei widget sul server SAP NetWeaver Application Server* nel manuale *Manuale dell'utente dei widget per SAP BusinessObjects*.

Nota:

Il supporto di SAP Web Dynpro Flex Client per XBCML Widgets inizia nella versione 7.0 EhP2 SP3. Il supporto della coda di Flex Client è limitato solo ai problemi di Flex Client trovati solo nei widget XBCML nelle versioni specificate.

Grazie ai widget, è possibile eseguire ricerche nel contenuto esistente, ad esempio in documenti Web Intelligence, modelli Dashboards e applicazioni Web Dynpro, quindi incollare le informazioni chiave sul desktop in modo da renderle disponibili quando necessario.

La natura dei widget consente di utilizzare per il contenuto le seguenti funzionalità dell'ambiente dei widget:

- Dimensione e posizionamento controllati dall'utente
- Aggiornamento automatico
- Impostazione facoltativa come finestra dell'applicazione principale
- Protezione completa della piattaforma BI (solo per le parti di report Web Intelligence e i modelli Dashboards)
- Visualizzazione salvata
- Stato del contesto dati salvato (solo per le parti di report Web Intelligence)
- Collegamenti OpenDocument Web Intelligence a report dettagliati (solo per i documenti Web Intelligence)
- Visualizzazioni a schede (solo per i modelli Dashboards)

3.3.2 Installato con la piattaforma SAP BusinessObjects Business Intelligence

3.3.2.1 Central Configuration Manager (CCM)

CCM (Central Configuration Manager) è uno strumento di configurazione per la gestione dei nodi e la risoluzione dei problemi del server fornito in due modalità. In un ambiente Microsoft Windows, CCM

consente di gestire server locali e remoti tramite l'interfaccia utente grafica o la riga di comando. In ambiente Unix lo script di shell di CCM (`ccm.sh`) consente di gestire i server da una riga di comando.

CCM viene utilizzato per creare e configurare nodi e per avviare o interrompere il server di applicazioni Web, se questo è il server di applicazioni Web Tomcat in bundle predefinito. In Windows è anche possibile configurare parametri di rete, ad esempio la crittografia SSL (Secure Sockets Layer). Questi parametri si applicano a tutti i server in un nodo.

Nota:

La maggior parte dei task di gestione server viene ora gestita tramite la console CMC, non CCM. CCM è ora utilizzato per la risoluzione dei problemi e per la configurazione dei nodi.

3.3.2.2 Upgrade Management Tool

Upgrade Management Tool (in precedenza Importazione guidata) viene installato come parte della piattaforma BI e guida gli amministratori attraverso il processo di importazione di utenti, gruppi e cartelle di versioni precedenti della piattaforma BI. Consente inoltre di importare e aggiornare eventi, gruppi di server, oggetti repository e calendari.

Per informazioni sull'esecuzione dell'aggiornamento da una versione precedente della piattaforma BI, consultare il *Manuale di aggiornamento della piattaforma SAP BusinessObjects Business Intelligence*.

3.3.2.3 Strumento Repository Diagnostic Tool

Lo strumento Repository Diagnostic Tool (RDT) consente di esaminare, diagnosticare e risolvere i conflitti che possono verificarsi tra il database di sistema CMS (Central Management Server) e l'archivio di file FRS (File Repository Server).

Segnala inoltre lo stato del ripristino e le azioni completate. Per determinare la sincronizzazione tra il file system e il database, è necessario che lo strumento RDT venga utilizzato al termine di un backup a caldo da parte dell'utente. Può essere utilizzato anche dopo un ripristino e prima di avviare i servizi della piattaforma BI. L'utente può impostare un limite per il numero di errori che lo strumento RDT può trovare e ripristinare prima di interrompersi.

3.3.3 Disponibile separatamente

3.3.3.1 SAP BusinessObjects Analysis, versione per Microsoft Office

SAP BusinessObjects Analysis, versione per Microsoft Office, è un'eccellente alternativa a Business Explorer (BEx) e consente agli analisti aziendali di esplorare dati OLAP (Online Analytical Processing) multidimensionali.

Gli analisti possono rispondere rapidamente a domande concernenti l'azienda e condividere quindi la propria analisi e lo spazio di lavoro con altri in forma di *analisi*.

SAP BusinessObjects Analysis, versione per Microsoft Office, consente agli analisti di:

- Rilevare tendenze, valori fuori norma e dettagli memorizzati nei sistemi finanziari senza l'assistenza di un amministratore di database;
- Ottenere risposte a domande aziendali visualizzando al contempo con efficienza insiemi di dati multidimensionali piccoli o grandi;
- Accedere all'intera gamma di origini dati OLAP disponibili nell'azienda e condividere risultati con un'interfaccia semplice e intuitiva;
- Accedere a più origini OLAP diverse nella stessa analisi per ottenere una visione complessiva dell'azienda e dell'impatto incrociato che una tendenza potrebbe avere su un'altra;
- Interrogare, analizzare, confrontare e prevedere fattori di sviluppo aziendali;
- Utilizzare una gamma completa di calcoli aziendali e temporali.

3.3.3.2 SAP Crystal Reports

Il software SAP Crystal Reports consente agli utenti di progettare report interattivi da un'origine dati.

3.3.3.3 SAP BusinessObjects Dashboards

SAP BusinessObjectsDashboards (in precedenza Xcelsius) è uno strumento per la visualizzazione dei dati e la creazione di cruscotti dinamici e interattivi. I dati e le formule vengono importati o immessi direttamente in un foglio di lavoro di Excel incorporato. Un'interfaccia Flash fornisce un'area di disegno in cui è possibile visualizzare una varietà di analitiche e cruscotti.

I dati possono essere aggiornati dinamicamente dalla piattaforma BI ed esportati in svariati formati che gli utenti dei dati possono visualizzare nei formati standard, ad esempio PowerPoint, PDF o Flash.

3.3.3.4 SAP BusinessObjects Explorer

SAP BusinessObjects Explorer è un'applicazione per l'individuazione dei dati che, grazie a funzionalità di ricerca avanzate, consente di recuperare direttamente e rapidamente le risposte a domande aziendali dai dati aziendali.

Quando si installa SAP BusinessObjects Explorer, al CCM (Central Configuration Manager) e alla CMC (Central Management Console) della piattaforma BI vengono aggiunti i server seguenti:

- Server master Explorer: gestisce tutti i server Explorer.
- Server di indicizzazione Explorer: fornisce e gestisce l'indicizzazione dei dati e dei metadati dello spazio informazioni.
- Server di ricerca Explorer: elabora le query di ricerca e restituisce i risultati.
- Server di esplorazione Explorer: fornisce e gestisce l'esplorazione dello spazio informazioni e le funzioni di analisi, incluse le funzioni di ricerca nei dati, filtro e aggregazione.

3.3.4 Client di applicazioni Web

I client di applicazioni Web risiedono su un server di applicazioni Web ed è possibile accedervi da un computer client con un browser Web. Le applicazioni Web vengono distribuite automaticamente durante l'installazione della piattaforma BI.

Per gli utenti è facile accedere alle applicazioni Web da un browser Web ed è possibile proteggere le comunicazioni con la crittografia SSL se si prevede di consentire agli utenti di accedere dall'esterno della rete dell'organizzazione.

Le applicazioni Web Java possono inoltre essere riconfigurate o distribuite dopo l'installazione iniziale utilizzando lo strumento WDeploy della riga di comando, che consente di distribuire le applicazioni Web a un server di applicazioni Web in due modi:

1. Modalità autonoma

Tutte le risorse di applicazioni Web vengono distribuite a un server di applicazioni Web che gestisce contenuto sia statico che dinamico. Questa opzione è adatta alle installazioni di piccole dimensioni.

2. Modalità divisa

Il contenuto statico delle applicazioni Web (HTML, immagini, CSS) viene distribuito a un server Web dedicato, mentre il contenuto dinamico (JSP) viene distribuito a un server di applicazioni Web. Questa opzione è adatta alle installazioni di dimensioni maggiori, in cui sarà possibile evitare che il server di applicazioni Web gestisca il contenuto Web statico.

Per ulteriori informazioni su WDeploy, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

3.3.4.1 Central Management Console (CMC)

La Central Management Console (CMC) è uno strumento basato su Web che si utilizza per eseguire attività amministrative (quali la gestione di server, contenuti e utenti) e per configurare le impostazioni di protezione. Poiché la console CMC è un'applicazione basata su Web, è possibile eseguire tutti i task amministrativi mediante un browser Web in qualsiasi computer in grado di connettersi al server di applicazioni Web.

Tutti gli utenti possono accedere a CMC per modificare le impostazioni delle preferenze. Solo i membri del gruppo Amministratori possono modificare le impostazioni di gestione, a meno che tale diritto non venga esplicitamente concesso ad altri utenti. I ruoli possono essere assegnati in CMC per garantire privilegi utente per portare a termine attività amministrative minori, quali la gestione di utenti nel gruppo e di report nelle cartelle appartenenti al proprio team.

3.3.4.2 BI Launch Pad

BI Launch Pad (in precedenza InfoView) è un'interfaccia basata sul Web a cui gli utenti finali accedono per visualizzare, pianificare e tenere traccia dei report BI pubblicati. BI Launch Pad può accedere, esportare e interagire con qualsiasi tipo di elemento Business Intelligence, tra cui report, analitiche e cruscotti.

BI Launch Pad consente agli utenti di gestire:

- Esplorazione e ricerca nei contenuti BI
- Accesso al contenuto BI (creazione, modifica e visualizzazione).
- Pianificazione e pubblicazione di contenuto BI.

3.3.4.3 Spazi di lavoro BI

BI Workspaces (in precedenza Dashboard Builder) consente di tenere traccia delle attività e delle prestazioni aziendali utilizzando moduli (modelli per i dati) e workspace Business Intelligence (BI) (visualizzazione dei dati in uno o più moduli). I moduli e gli spazi di lavoro BI forniscono le informazioni necessarie per modificare le regole di business al variare delle condizioni. Consente di tenere traccia e di analizzare i dati aziendali principali attraverso i moduli e gli spazi di lavoro BI. Supporta inoltre analisi e decisioni di gruppo tramite funzioni integrate di collaborazione e flusso di lavoro. BI Workspaces presenta le funzionalità seguenti:

- Esplorazione basata su schede

- Creazione di pagine: gestione di moduli e spazi di lavoro BI
- Uno strumento intuitivo di creazione delle applicazioni
- Collegamento del contenuto tra i moduli per analisi approfondite dei dati

Nota:

gli spazi di lavoro BI sono parte integrante dell'applicazione BI Launch Pad. Pertanto, per utilizzare le funzionalità degli spazi di lavoro BI, è necessario acquistare una licenza della piattaforma SAP BusinessObjects Business Intelligence che includa nell'accordo l'utilizzo di BI Launch Pad.

3.3.4.4 Visualizzatori di report

Ogni visualizzatore di report supporta una diversa piattaforma e un browser differente. È possibile impostare le preferenze in BI Launch Pad e nella Central Management Console (CMC). Esistono due categorie di visualizzatori:

- Visualizzatori di report lato client (visualizzatore Active X o Java)

I visualizzatori di report lato client vengono scaricati e installati nel browser dell'utente. Quando un utente richiede un report, il server delle applicazioni elabora la richiesta e recupera le pagine del report dalla piattaforma BI. Il server di applicazioni Web trasferisce quindi le pagine del report al visualizzatore lato client, che le elabora e le visualizza nel browser Web. Per scegliere un visualizzatore di report lato client, selezionare **Preferenze > Crystal Reports > Web ActiveX (ActiveX richiesto) o Web Java (Java richiesto)**.

- Visualizzatori di report client zero (visualizzatore DHTML)

I visualizzatori di report client zero risiedono nel server di applicazioni Web. Quando un utente richiede un report, il server di applicazioni Web recupera le pagine del report dalla piattaforma BI e crea pagine DHTML che vengono visualizzate nel browser Web. Per scegliere il visualizzatore di report client zero (DHTML), selezionare **Preferenze > Crystal Reports > Web (download non richiesto)**

Tutti i visualizzatori di report elaborano le richieste di report e presentano le pagine di report che appaiono nel browser Web.

Per ulteriori informazioni su una funzionalità specifica o sul supporto per la piattaforma fornito da ogni visualizzatore di report, consultare il *Manuale dell'utente di BI Launch Pad*, il manuale *Report Application Server .NET SDK Developer Guide* o il *Manuale per gli sviluppatori dell'SDK Java dei visualizzatori*.

3.3.4.5 SAP BusinessObjects Web Intelligence

SAP BusinessObjects Web Intelligence è uno strumento Web che offre funzionalità di query, creazione di report e analisi per le origini dati relazionali in un unico prodotto basato sul Web.

Consente agli utenti di creare report, eseguire query ad-hoc, analizzare i dati e formattare i report in un'interfaccia con trascinamento della selezione. Web Intelligence nasconde la complessità delle origini dati sottostanti.

I report possono essere pubblicati su un portale Web supportato o in applicazioni Microsoft Office che utilizzano SAP BusinessObjects Live Office.

3.3.4.6 SAP BusinessObjects Analysis, versione per OLAP

SAP BusinessObjects Analysis, versione per OLAP (in precedenza Voyager), è uno strumento OLAP (Online Analytical Processing) disponibile nel portale di BI Launch Pad per l'utilizzo dei dati multidimensionali. Consente inoltre di combinare le informazioni provenienti da diverse origini dati OLAP all'interno di un unico spazio di lavoro. I provider OLAP supportati includono SAP BW e Microsoft Analysis Services.

L'insieme di funzionalità OLAP di Analysis combina elementi di SAP Crystal Reports (accesso diretto dei dati ai cubi OLAP per la creazione di report di produzione) e SAP BusinessObjects Interactive Analysis (creazione di report analitici ad-hoc con universi da origini dati OLAP). Offre una gamma di calcoli aziendali e temporali, nonché funzionalità quali dispositivi di scorrimento tempo che semplificano l'analisi dei dati OLAP.

Nota:

l'applicazione Web Analysis, versione per OLAP, è disponibile solo come applicazione Web Java. Non esiste un'applicazione corrispondente per .NET.

3.3.4.7 SAP BusinessObjects Mobile

SAP BusinessObjects Mobile consente agli utenti di accedere in modalità remota agli stessi report BI (Business Intelligence), metriche e dati in tempo reale disponibili sui client desktop da un dispositivo wireless. Il contenuto viene ottimizzato per i dispositivi mobili in modo tale che gli utenti possano accedere, navigare e analizzare con facilità i dati dei report familiari senza ulteriore formazione.

Grazie a SAP BusinessObjects Mobile, il personale del settore amministrativo e di gestione delle informazioni può mantenersi sempre aggiornato e prendere decisioni utilizzando le informazioni più recenti. Il personale addetto alle vendite e all'assistenza sul campo è in grado di fornire informazioni corrette su clienti, prodotti e ordini di lavoro, dove e quando si rende necessario.

SAP BusinessObjects Mobile supporta una vasta gamma di dispositivi mobili, tra cui BlackBerry, Windows Mobile e Symbian.

Per ulteriori informazioni sull'installazione, sulla configurazione e sulla distribuzione di prodotti Mobile, consultare il *Manuale d'installazione e distribuzione di SAP BusinessObjects Mobile*. Per informazioni

sull'utilizzo di SAP BusinessObjects Mobile, consultare il manuale *Utilizzo di SAP BusinessObjects Mobile*.

3.4 Workflow del processo

Quando vengono eseguiti task, quali la registrazione, la pianificazione o la visualizzazione di un report, le informazioni fluiscono nel sistema e i server comunicano tra loro. Nella sezione seguente vengono descritti alcuni flussi di processo della piattaforma BI.

Per visualizzare ulteriori workflow del processo con aiuti visivi, consultare i tutorial ufficiali relativi ai prodotti della piattaforma SAP BusinessObjects Business Intelligence 4.x presso:
<http://scn.sap.com/docs/DOC-8292>

3.4.1 Avvio e autenticazione

3.4.1.1 Accesso alla piattaforma BI

Questo workflow descrive l'accesso di un utente all'applicazione Web della piattaforma BI da un browser Web. Questo workflow si applica alle applicazioni Web quali BI Launch Pad e la Central Management Console (CMC).

1. Il browser (client Web) invia la richiesta di registrazione tramite il server Web al server di applicazioni Web, dove è in esecuzione l'applicazione Web.
2. Il server di applicazioni Web stabilisce che si tratta di una richiesta di accesso. Il server di applicazioni Web invia nome utente, password e tipo di autenticazione al server CMS per l'autenticazione.
3. Il server CMS convalida il nome utente e password sul database appropriato (in questo caso viene utilizzata l'autenticazione Enterprise e le credenziali utente vengono autenticate nel database di sistema CMS).
4. Una volta ottenuta la convalida, il server CMS crea una sessione per l'utente nella memoria.
5. Il server CMS invia una risposta al server di applicazioni Web per segnalare l'avvenuta convalida.
6. Il server di applicazioni Web genera un token di accesso per la sessione utente nella memoria. Per il resto della sessione, il server di applicazioni Web utilizza il token di accesso per convalidare l'utente rispetto al server CMS. Il server di applicazioni Web genera la pagina Web successiva da inviare al client Web.
7. Il server di applicazioni Web invia la pagina Web successiva al server Web.

8. Il server di applicazioni Web invia la pagina Web al client Web dove viene visualizzata mediante il browser dell'utente.

3.4.1.2 Avvio di SIA

È possibile configurare un SIA (Server Intelligence Agent) in modo tale che venga avviato automaticamente con il sistema operativo host oppure manualmente mediante Central Configuration Manager (CCM).

Un SIA recupera le informazioni sui server che gestisce da un server CMS (Central Management Server). Se il SIA utilizza un server CMS locale e il server CMS non è in esecuzione, il SIA avvia il server CMS. Se un SIA utilizza un server CMS remoto, tenterà di connettersi al server CMS.

Una volta avviato il SIA, si verificano gli eventi descritti di seguito.

1. Il SIA cerca un server CMS nella propria cache.
 - a. Se il SIA è configurato per l'avvio di un server CMS locale e il server CMS non è in esecuzione, il SIA avvia il server CMS e si connette.
 - b. Se il SIA è configurato per l'utilizzo di un server CMS (locale o remoto) in esecuzione, tenterà di connettersi al primo server CMS che trova nella cache. Se il server CMS al momento non è disponibile, tenterà di connettersi al server CMS successivo nella cache. Se nessuno dei server CMS di cache è disponibile, il SIA attende che uno di essi diventi disponibile.
2. Il server CMS verifica l'identità del SIA per assicurare che sia valido.
3. Una volta effettuata correttamente la connessione del SIA a un server CMS, viene richiesto l'elenco dei server da gestire.

Nota:

Un SIA non archivia le informazioni sui server che gestisce. Le informazioni di configurazione che indicano quale server è gestito da un SIA sono memorizzate nel database di sistema CMS e il SIA le recupera dal server CMS all'avvio.

4. Il server CMS esegue una query sul database di sistema CMS per ottenere l'elenco dei server gestiti dal SIA. Viene anche recuperata la configurazione di ogni server.
5. Il server CMS restituisce l'elenco di server e le informazioni sulla configurazione al SIA.
6. Per ogni server configurato per l'avvio automatico, il SIA esegue l'avvio con la configurazione appropriata e ne monitora lo stato. Ciascun server avviato dal SIA è configurato per l'utilizzo dello stesso CMS utilizzato dal SIA.

Eventuali server non configurati per l'avvio automatico insieme al SIA non verranno avviati.

3.4.1.3 Arresto di SIA

Server Intelligence Agent (SIA) viene interrotto automaticamente quando si arresta il sistema operativo host. In alternativa è possibile interrompere manualmente il SIA in Central Configuration Manager (CCM).

Quando si arresta il SIA vengono effettuate le seguenti operazioni:

- Il SIA indica al server CMS si sta spegnendo.
 - a. Se il SIA si arresta perché si sta arrestando il sistema operativo host, il SIA richiede l'arresto dei relativi server. Se i server non si arrestano entro 25 secondi, verrà forzato lo spegnimento.
 - b. Se il SIA viene arrestato manualmente, attenderà che il server gestito termini l'elaborazione dei processi in corso. I server gestiti non accetteranno nuovi processi. Una volta completati tutti i processi, i server si arrestano. Una volta arrestati tutti i server, si arresta anche il SIA.

Nota:

durante un arresto forzato, il SIA indica a tutti i server gestiti di arrestarsi immediatamente.

3.4.2 Oggetti programma

3.4.2.1 Impostazione di una pianificazione per un oggetto programma

Questo workflow descrive il modo in cui un utente pianifica l'esecuzione di un oggetto programma che dovrà verificarsi in un secondo momento da un'applicazione Web quale Central Management Console (CMC) o BI Launch Pad.

1. L'utente invia la richiesta di pianificazione dal client Web attraverso il server Web al server di applicazioni Web.
2. Il server di applicazioni Web interpreta la richiesta e stabilisce che si tratta di una richiesta di pianificazione. Il server di applicazioni Web invia l'ora pianificata, i valori di accesso al database, i valori dei parametri, la destinazione e il formato al Central Management Server (CMS) specificato.
3. Il server CMS garantisce che l'utente disponga dei diritti per pianificare l'oggetto. Se l'utente dispone di diritti sufficienti, il CMS aggiunge un nuovo record al database di sistema CMS e aggiunge la rispettiva istanza all'elenco di pianificazioni in sospeso.
4. Il CMS invia al server di applicazioni Web una risposta relativa al completamento dell'operazione di pianificazione.
5. Il server di applicazione Web genera la pagina HTML successiva e la invia attraverso il server Web al client Web.

3.4.2.2 Esecuzione di un oggetto programma pianificato

Questo workflow descrive il processo di un oggetto programma pianificato in esecuzione a un'ora specifica. Devono essere in esecuzione anche Adaptive Job Server e Input File Repository Server.

Nota:

Questo workflow richiede che siano in esecuzione il CMS, Adaptive Job Server e Input File Repository Server.

1. Il server CMS controlla il database di sistema CMS per determinare se sono presenti eventuali report SAP Crystal da pianificare all'ora prestabilita.
2. Quando giunge l'ora pianificata del processo, CMS localizza un Servizio di pianificazione programma disponibile in esecuzione su un Adaptive Job Server. Il server CMS invia le informazioni sul processo al Servizio di pianificazione programma.
3. Il Servizio di pianificazione programma comunica con l'Input File Repository Server (FRS) per conseguire un oggetto programma.

Nota:

questa fase richiede inoltre la comunicazione con il CMS per localizzare gli oggetti e il server necessario.

4. Il Servizio di pianificazione programma lancia il programma.
5. Il Servizio di pianificazione programma aggiorna periodicamente il CMS con lo stato del processo. Lo stato attuale è Elaborazione in corso.
6. Il Servizio di pianificazione programma invia un file di registro a Output FRS. Output FRS segnala a Servizio di pianificazione programma che l'oggetto è stato pianificato correttamente mediante l'invio di un file di registro dell'oggetto.

Nota:

questa fase richiede inoltre la comunicazione con il CMS per localizzare gli oggetti e il server necessario.

7. Il Servizio di pianificazione programma aggiorna il CMS con lo stato del processo. Lo stato attuale è Operazione riuscita.
8. Il server CMS aggiorna lo stato del processo in memoria, quindi scrive le informazioni relative all'istanza nel database di sistema CMS.

3.4.3 Crystal Reports

3.4.3.1 Visualizzazione di una pagina del report SAP Crystal di cache

Questo workflow è relativo alla richiesta da parte dell'utente di una pagina in un report SAP Crystal (ad esempio dal visualizzatore di report in BI Launch Pad) quando la pagina del report risulta già esistere su un server cache. Tale workflow si applica sia a SAP Crystal Reports 2011 che a SAP Crystal Reports for Enterprise.

Nota:

Questo workflow richiede che siano in esecuzione il CMS e Crystal Reports Cache Server.

1. Il client Web invia una richiesta di visualizzazione in un URL tramite il server Web al server di applicazioni Web.
2. Il server di applicazioni Web interpreta la richiesta e stabilisce che si tratta di una richiesta di visualizzare la pagina di report selezionata. Il server di applicazioni Web invia una richiesta a CMS per verificare che l'utente disponga dei diritti di visualizzazione necessari per il report.
3. CMS controlla il database del sistema CMS per verificare che l'utente disponga dei diritti necessari a visualizzare il report.
4. Il server CMS invia una risposta al server di applicazioni Web per verificare che l'utente disponga dei diritti sufficienti per visualizzare il report.
5. Il server di applicazioni Web invia una richiesta a Crystal Reports Cache Server per la pagina del report (file .epf).
6. Crystal Reports Cache Server verifica se il file richiesto .epf esiste nella directory cache. In questo esempio, viene trovato il file .epf.
7. Crystal Reports Cache Server restituisce la pagina richiesta al server di applicazioni Web.
8. Il server di applicazioni Web invia attraverso il server Web la pagina al client Web in cui viene eseguito il rendering e la visualizzazione della pagina.

3.4.3.2 Visualizzazione di una pagina SAP Crystal Reports 2011 non memorizzata nella cache

Questo workflow descrive la richiesta da parte dell'utente di una pagina di un report SAP Crystal Reports 2011 (ad esempio dal visualizzatore di report in BI Launch Pad) quando la pagina non è già esistente in un server cache.

Nota:

Questo workflow richiede che siano in esecuzione il CMS, Crystal Reports Cache Server, il servizio di elaborazione di Crystal Reports 2011 e Output File Repository Server.

1. L'utente invia la richiesta di visualizzazione attraverso il server Web al server di applicazioni Web.

2. Il server di applicazioni Web interpreta la richiesta, stabilisce che si tratta della richiesta di visualizzare una pagina di report selezionata e invia una richiesta al Central Management Server (CMS) per verificare che l'utente disponga di diritti sufficienti per visualizzare il report.
3. CMS controlla il database del sistema CMS per verificare che l'utente disponga dei diritti necessari a visualizzare il report.
4. Il server CMS invia una risposta al server di applicazioni Web per verificare che l'utente disponga dei diritti sufficienti per visualizzare il report.
5. Il server di applicazioni Web invia una richiesta a Crystal Reports Cache Server per la pagina del report (file `.epf`).
6. Crystal Reports Cache Server determina se il file richiesto esiste nella directory cache.
In questo esempio, il file richiesto `.epf` non viene rilevato nella directory cache.
7. Crystal Reports Cache Server invia la richiesta al server di elaborazione Crystal Reports 2011.
8. Il servizio di elaborazione di Crystal Reports 2011 esegue una query su Output File Repository Server (FRS) per l'istanza di report richiesta e Output FRS invia l'istanza di report richiesta al servizio di elaborazione di Crystal Reports 2011.

Nota:

questa fase richiede inoltre la comunicazione con il CMS per localizzare gli oggetti e il server necessario.

9. Il server di elaborazione Crystal Reports 2011 apre l'istanza di report e controlla se nel report sono presenti dati.
Il servizio di elaborazione di Crystal Reports 2011 determina che il report contiene dati e crea il file `.epf` per la pagina di report richiesta senza doversi connettere al database di produzione.
10. Il server di elaborazione Crystal Reports 2011 invia il file `.epf` a Crystal Reports Cache Server.
11. Crystal Reports Cache Server scrive il file `.epf` nella directory cache.
12. Crystal Reports Cache Server invia la pagina richiesta al server di applicazioni Web.
13. Il server di applicazioni Web invia attraverso il server Web la pagina al client Web in cui viene eseguito il rendering e la visualizzazione della pagina.

3.4.3.3 Visualizzazione di un report SAP Crystal Reports 2011 su richiesta

Questo workflow descrive il processo di richiesta da parte di un utente di visualizzare una pagina di report SAP Crystal Reports 2011 su richiesta per visualizzare i dati più recenti, ad esempio dal visualizzatore di report in BI Launch Pad.

Nota:

Questo workflow richiede che siano in esecuzione il CMS, Crystal Reports Cache Server, il servizio di elaborazione di Crystal Reports 2011 e Input File Repository Server.

1. L'utente invia la richiesta di visualizzazione attraverso il server Web al server di applicazioni Web.

2. Il server di applicazioni Web interpreta la richiesta e stabilisce che si tratta di una richiesta di visualizzare la pagina di report selezionata. Il server di applicazioni Web invia una richiesta a CMS per verificare che l'utente disponga dei diritti di visualizzazione necessari per il report.
3. CMS controlla il database del sistema CMS per verificare che l'utente disponga dei diritti necessari a visualizzare il report.
4. Il server CMS invia una risposta al server di applicazioni Web per verificare che l'utente disponga dei diritti sufficienti per visualizzare il report.
5. Il server di applicazioni Web invia una richiesta a Crystal Reports Cache Server per la pagina del report (file .epf).
6. Crystal Reports Cache Server verifica che la pagina esista già. A meno che il report non soddisfi i requisiti per la condivisione di report su richiesta (entro un'ora impostata per un'altra richiesta, accesso al database, parametri), Crystal Reports Cache Server invia una richiesta al server di elaborazione di Crystal Reports 2011 affinché generi la pagina.
7. Il server di elaborazione di Crystal Reports 2011 richiede l'oggetto report da Input File Repository Server (FRS). Input FRS invia una copia dell'oggetto al server di elaborazione Crystal Reports 2011.

Nota:

questa fase richiede inoltre la comunicazione con il CMS per localizzare gli oggetti e il server necessario.

8. Il server di elaborazione Crystal Reports 2011 apre il report in memoria e verifica se il report contiene dati. In questo esempio non sono presenti dati nell'oggetto report, pertanto il server di elaborazione Crystal Reports 2011 si collega all'origine dati per recuperare i dati e generare il report.
9. Il server di elaborazione di Crystal Reports 2011 invia la pagina (file .epf) a Crystal Reports Cache Server. Crystal Reports Cache Server archivia una copia del file .epf nella directory cache in previsione di nuove richieste di visualizzazione.
10. Crystal Reports Cache Server invia la pagina al server di applicazioni Web.
11. Il server di applicazioni Web invia attraverso il server Web la pagina al client Web in cui viene eseguito il rendering e la visualizzazione della pagina.

3.4.3.4 Impostazione di una pianificazione per un report SAP Crystal

Questo workflow è relativo alla pianificazione da parte di un utente di un report SAP Crystal da eseguire in un secondo momento da un'applicazione Web quale Central Management Console (CMC) o BI Launch Pad. Il workflow si applica sia a SAP Crystal Reports 2011 che a SAP Crystal Reports for Enterprise.

1. Il client Web invia una richiesta di pianificazione in un URL tramite il server Web al server di applicazioni Web.
2. Il server di applicazioni Web interpreta la richiesta di URL e stabilisce che si tratta di una richiesta di pianificazione. Il server di applicazioni Web invia l'ora pianificata, i valori di accesso al database, i valori dei parametri, la destinazione e il formato al Central Management Server (CMS) specificato.

3. Il server CMS garantisce che l'utente disponga dei diritti per pianificare l'oggetto. Se l'utente dispone dei diritti necessari, il server CMS aggiunge un nuovo record al database di sistema CMS. Il server CMS aggiunge inoltre l'istanza all'elenco di pianificazioni in attesa.
4. CMS invia una risposta al server di applicazioni Web per segnalare l'avvenuta operazione di pianificazione.
5. Il server di applicazione Web genera la pagina HTML successiva e la invia attraverso il server Web al client Web.

3.4.3.5 Esecuzione di un report SAP Crystal Reports 2011 pianificato

Questo workflow descrive il processo di un report SAP Crystal Reports 2011 pianificato in esecuzione a un'ora specifica.

1. Il server CMS controlla il database di sistema CMS per determinare se sono presenti eventuali report SAP Crystal da pianificare all'ora prestabilita.
2. Quando giunge l'ora del processo pianificato, CMS individua un servizio di pianificazione Crystal Reports 2011 disponibile in esecuzione su un Adaptive Job Server (in base al valore **Numero max. processi consentiti** configurato su ogni Adaptive Job Server). CMS invia le informazioni del processo (ID report, formato, destinazione, informazioni di accesso, parametri e formule di selezione) al servizio di pianificazione Crystal Reports 2011.
3. Il servizio di pianificazione Crystal Reports 2011 comunica con Input File Repository Server (FRS) per ottenere un modello di report in base all'ID report richiesto.

Nota:

questa fase richiede inoltre la comunicazione con il CMS per localizzare gli oggetti e il server necessario.

4. Il servizio di pianificazione Crystal Reports 2011 avvia il processo JobChildserver.
5. Il processo secondario (JobChildserver) avvia `ProcReport.dll` alla ricezione del modello da parte di Input File Repository Server. `ProcReport.dll` contiene tutti i parametri passati da CMS al servizio di pianificazione Crystal Reports 2011.
6. `ProcReport.dll` avvia `crpe32.dll`, che elabora il report in base ai parametri passati.
7. Mentre `crpe32.dll` sta ancora elaborando il report, i record vengono recuperati dall'origine dati come indicato nel report.
8. Il Servizio di pianificazione Crystal Reports 2011 aggiorna periodicamente il CMS con lo stato del processo. Lo stato attuale è Elaborazione in corso.
9. Terminata la compilazione del report nella memoria del servizio di pianificazione di Crystal Reports 2011, è possibile esportarlo in un altro formato, ad esempio PDF (Portable Document Format). Quando si esporta in PDF, viene utilizzato `crxfpdf.dll`.
10. Il report con i dati salvati viene inviato alla posizione pianificata (come un'e-mail) e quindi ad Output FRS.

Nota:

questa fase richiede inoltre la comunicazione con il CMS per localizzare gli oggetti e il server necessario.

11. Il Servizio di pianificazione Crystal Reports 2011 aggiorna il CMS con lo stato del processo. Lo stato attuale è Operazione riuscita.
12. Il server CMS aggiorna lo stato del processo in memoria, quindi scrive le informazioni relative all'istanza nel database di sistema CMS.

3.4.4 Web Intelligence

3.4.4.1 Visualizzazione su richiesta di una pianificazione per un documento SAP BusinessObjects Web Solution

Questo workflow descrive il processo di visualizzazione da parte di un utente di un documento SAP BusinessObjects Web Intelligence su richiesta per visualizzare i dati più recenti, ad esempio dal visualizzatore Web Intelligence in BI Launch Pad.

1. Un browser invia la richiesta di visualizzazione al server di applicazioni Web tramite il server Web.
2. Il server di applicazioni Web interpreta la richiesta e stabilisce che si tratta di una richiesta di visualizzare un documento Web Intelligence. Il server di applicazioni Web invia una richiesta a CMS per verificare che l'utente disponga dei diritti di visualizzazione necessari per il documento.
3. CMS controlla il database del sistema CMS per verificare che l'utente disponga dei diritti necessari a visualizzare il documento.
4. Il server CMS invia una risposta al server di applicazioni Web per verificare che l'utente disponga dei diritti sufficienti per visualizzare il documento.
5. Il server di applicazioni Web invia una richiesta a Server di elaborazione Web Intelligence che richiedere il documento.
6. Server di elaborazione Web Intelligence richiede il documento da Input File Repository Server (FRS) e il file dell'universo su cui è stato generato il documento richiesto. Il file dell'universo contiene informazioni di metalevello, inclusa la protezione a livello di riga e di colonna.
7. L'Input FRS invia una copia del documento a Server di elaborazione Web Intelligence, nonché il file dell'universo su cui è stato generato il documento richiesto.

Nota:

questa fase richiede inoltre la comunicazione con il CMS per localizzare gli oggetti e il server necessario.

8. Web Intelligence Report Engine (sul server di elaborazione Web Intelligence) apre il documento in memoria e lancia `QT.dll` e un Connection Server in elaborazione.
9. `QT.dll` genera, convalida e rigenera SQL e si collega al database per eseguire la query. Connection Server utilizza SQL per trasferire i dati dal database al modulo di report in cui viene elaborato il documento.

10. Server di elaborazione Web Intelligence invia al server di applicazioni Web la pagina del documento visualizzabile richiesta.
11. Il server di applicazioni Web invia attraverso il server Web la pagina del documento al client Web in cui viene eseguito il rendering e la visualizzazione della pagina.

3.4.4.2 Impostazione di una pianificazione per un documento SAP BusinessObjects Web Intelligence

Questo workflow è relativo alla pianificazione da parte dell'utente di un documento SAP BusinessObjects Web Intelligence da eseguire in un secondo momento da un'applicazione Web quale Central Management Console (CMC) o BI Launch Pad.

1. Il client Web invia una richiesta di pianificazione in un URL tramite il server Web al server di applicazioni Web.
2. Il server di applicazioni Web interpreta la richiesta di URL e stabilisce che si tratta di una richiesta di pianificazione. Il server di applicazioni Web invia l'ora pianificata, i valori di accesso al database, i valori dei parametri, la destinazione e il formato al Central Management Server (CMS) specificato.
3. Il server CMS garantisce che l'utente disponga dei diritti per pianificare l'oggetto. Se l'utente dispone dei diritti necessari, il server CMS aggiunge un nuovo record al database di sistema CMS. Il server CMS aggiunge inoltre l'istanza all'elenco di pianificazioni in attesa.
4. CMS invia una risposta al server di applicazioni Web per segnalare l'avvenuta operazione di pianificazione.
5. Il server di applicazione Web genera la pagina HTML successiva e la invia attraverso il server Web al client Web.

3.4.4.3 Esecuzione di un documento SAP BusinessObjects Web Intelligence pianificato

Questo workflow è relativo all'esecuzione di un documento pianificato SAP BusinessObjects Web Intelligence a un'ora specifica.

1. Central Management Server (CMS) verifica il database del sistema CMS per determinare se l'esecuzione di un documento Web Intelligence sia in pianificazione.
2. Quando giunge l'ora pianificata, CMS localizza un Servizio di pianificazione Web Intelligence disponibile in esecuzione su un Adaptive Job Server. CMS invia la richiesta di pianificazione e tutte le informazioni relative ad essa al servizio di pianificazione Web Intelligence.
3. Il servizio di pianificazione Web Intelligence individua un server di elaborazione Web Intelligence disponibile basato sul valore **Numero max. connessioni** configurato in ogni server di elaborazione Web Intelligence.
4. Il server di elaborazione Web Intelligence determina la posizione dell'Input File Repository Server (FRS) che ospita il documento e il file di metalinguaggio dell'universo su cui si basa il documento. Il

server di elaborazione Web Intelligence richiede quindi il documento al server Input FRS. Il server Input FRS individua il documento Web Intelligence e il file dell'universo su cui si basa il documento, quindi li invia al server di elaborazione Web Intelligence.

Nota:

questa fase richiede inoltre la comunicazione con il CMS per localizzare gli oggetti e il server necessario.

5. Il documento Web Intelligence viene posizionato in una directory temporanea nel server di elaborazione Web Intelligence. Nel server di elaborazione di Web Intelligence viene aperto il documento in memoria e `QT.dll` genera l'SQL dall'universo su cui si basa il documento. Le librerie di Connection Server incluse nel server di elaborazione Web Intelligence si collegano all'origine dati. I dati query passano attraverso `QT.dll` per tornare al modulo di report nel server di elaborazione Web Intelligence in cui il documento viene elaborato. Viene creata una nuova istanza funzionante.
6. Il server di elaborazione Web Intelligence carica l'istanza del documento nel server Output FRS.

Nota:

questa fase richiede inoltre la comunicazione con il CMS per localizzare gli oggetti e il server necessario.

7. Il server di elaborazione Web Intelligence notifica al servizio di pianificazione Web Intelligence (su Adaptive Job Server) il completamento della creazione del documento. Se è pianificato l'invio di un documento a una destinazione (file system, FTP, SMTP o Posta in arrivo), Adaptive Job Server recupera il documento elaborato dal server Output FRS e lo invia alle destinazioni specificate. Si supponga che ciò non accada in questo esempio.
8. Il servizio di pianificazione Web Intelligence aggiorna il CMS con lo stato del processo.
9. Il server CMS aggiorna lo stato del processo in memoria, quindi scrive le informazioni relative all'istanza nel database di sistema CMS.

3.4.5 Analisi

3.4.5.1 Visualizzazione di uno spazio di lavoro SAP BusinessObjects Analysis, versione per OLAP

Questo workflow descrive la richiesta da parte di un utente di visualizzare uno spazio di lavoro SAP BusinessObjects Analysis, versione per OLAP da BI Launch Pad.

Nota:

Questo workflow richiede che siano in esecuzione il CMS, Adaptive Processing Server (contenente il servizio di analisi multidimensionale (MDAS)) e Input File Repository Server.

1. Il client Web invia una richiesta tramite il server Web al server di applicazioni Web per visualizzare un nuovo spazio di lavoro. Il client Web comunica con il server di applicazioni Web utilizzando la tecnologia DHTML AJAX (Asynchronous JavaScript and XML). La tecnologia AJAX consente di eseguire aggiornamenti parziali della pagina, per evitare di eseguire il rendering di una nuova pagina a ogni nuova richiesta.
2. Il server di applicazioni Web traduce la richiesta e la invia al server CMS per determinare se un utente ha diritto a visualizzare o creare un nuovo workspace.
3. Il server CMS recupera le credenziali dell'utente dal database di sistema CMS.
4. Se l'utente è autorizzato a visualizzare o creare uno spazio di lavoro, il server CMS invia un segnale di conferma al server di applicazioni Web. Allo stesso tempo, invia anche un elenco di uno o più servizi di analisi multidimensionale (MDAS) disponibili.
5. Il server di applicazioni Web seleziona un servizio MDAS dall'elenco di scelte disponibili e gli invia una richiesta CORBA per trovare il/i server OLAP appropriato/i per creare un nuovo spazio di lavoro o aggiornarne uno esistente.
6. È necessario che il servizio MDAS comunichi con l'Input File Repository Server (FRS) per recuperare il documento dello spazio di lavoro appropriato contenente informazioni sul database OLAP sottostante e una query OLAP iniziale salvata con esso. Il server Input FRS recupera lo spazio di lavoro Analysis appropriato dalla directory sottostante, quindi invia nuovamente tale spazio di lavoro al servizio MDAS.
7. Il servizio MDAS apre lo spazio di lavoro, formula una query e la invia al server di database OLAP. È necessario che il servizio MDAS disponga di un client di database OLAP appropriato configurato per l'origine dati OLAP. La query del client Web deve essere convertita nella query OLAP appropriata. Il server di database OLAP restituisce il risultato della query al servizio MDAS.
8. Il servizio MDAS, in base alla richiesta di creazione, visualizzazione, stampa o esportazione, esegue l'anteprima del rendering del risultato per consentire al server WAS Java di completare più rapidamente il rendering. Il servizio MDAS invia i pacchetti XML del risultato sottoposto a rendering al server di applicazioni Web.
9. Il server di applicazioni Web esegue il rendering dello spazio di lavoro e invia la pagina o la porzione di pagina formattata al client Web tramite il server Web. Il client Web visualizza la pagina aggiornata o la nuova pagina richiesta. Si tratta di una soluzione client zero che non richiede il download di componenti Java o ActiveX.

Configurazione guidata del sistema

4.1 Introduzione alla Configurazione guidata del sistema

Dopo aver installato la piattaforma SAP BusinessObjects Business Intelligence, generalmente si eseguono le attività di configurazione essenziali post-installazione, come la scelta di un modello di distribuzione e la selezione dei prodotti SAP BusinessObjects che verranno utilizzati dall'organizzazione. Per eseguire questa configurazione e rendere la piattaforma BI attiva nel più breve tempo possibile, eseguire la "Configurazione guidata del sistema".

Vantaggi importanti derivanti dall'uso della procedura guidata:

- La procedura guidata spiega e illustra i passaggi di configurazione da eseguire.
- Consente di ridurre le probabilità di errata configurazione del sistema.
- Le impostazioni vengono configurate automaticamente e in questo modo la configurazione del sistema risulta più veloce.

Per impostazione predefinita, la procedura guidata è impostata per essere eseguita automaticamente quando si accede alla Central Management Console (CMC), ma può anche essere avviata dall'area "Gestisci" della CMC. È possibile rieseguire la procedura guidata quando desiderato per modificare la configurazione e utilizzare sempre la pagina di gestione "Server" della CMC per ottimizzare le impostazioni, incluse quelle definite utilizzando la configurazione guidata.

Nota:

- Per una maggiore protezione, solo ai membri del gruppo Amministratori è consentito l'accesso alla procedura guidata.
- Per impedire l'esecuzione automatica della procedura guidata, l'utente con ruolo di "Amministratore" può selezionare la casella di controllo **Non visualizzare questa procedura guidata all'avvio della CMC** nella prima pagina della procedura guidata.
- Se si prevede di installare componenti aggiuntivi o di aggiungere nodi alla distribuzione della piattaforma BI, è consigliabile effettuare queste operazioni prima di eseguire la Configurazione guidata del sistema.

4.2 Specifica dei prodotti utilizzati

È possibile semplificare la configurazione dei server della piattaforma BI specificando i prodotti utilizzati dall'organizzazione e ottimizzare l'allocazione delle risorse arrestando i server per i prodotti non utilizzati

dall'organizzazione. A tale scopo, selezionare i prodotti nella pagina "Prodotti". Quando si specificano i prodotti utilizzati dall'organizzazione, la procedura guidata avvia tutti i server e le dipendenze necessarie per l'esecuzione di tali prodotti, e configura i server e le dipendenze in questione per essere avviati automaticamente a ogni avvio della piattaforma BI. È inoltre possibile migliorare il tempo di avvio e l'utilizzo delle risorse della piattaforma BI deselectando i prodotti non utilizzati.

Se ad esempio si seleziona il prodotto Crystal Reports, la piattaforma BI avvia automaticamente tutti i server Crystal Reports e le dipendenze corrispondenti.

Per visualizzare un elenco dei server avviati automaticamente per un prodotto, fare clic sull'icona ? accanto al nome del prodotto.

La procedura guidata configura i server dei prodotti come segue:

- La selezione di un prodotto determina l'avvio di tutti i server appartenenti a quel prodotto, nonché di altri server necessari per il relativo funzionamento (dipendenze), al termine della procedura guidata. La selezione di un prodotto imposta inoltre l'avvio automatico dei server del prodotto con la piattaforma BI. Se un server ospita i servizi di più prodotti e uno dei prodotti viene selezionato, il server viene avviato. Si noti che alcuni servizi di prodotti non selezionati potrebbero essere eseguiti se ospitati da un server che ospita anche i servizi di prodotti selezionati.
- La deselectazione di un prodotto determina l'arresto dei server utilizzati da quel prodotto, purché non ospitino anche i servizi di un prodotto ancora selezionato o appartenenti alla categoria Servizi principali. I server del prodotto arrestati sono impostati per non essere avviati automaticamente con la piattaforma BI. Se un server ospita servizi sia di prodotti selezionati che deselectati, rimane in esecuzione.
- La deselectazione di un prodotto potrebbe inoltre causare l'arresto di server che non appartengono al prodotto deselectato, se vi sono servizi dipendenti utilizzati solo dal prodotto deselectato in questione. Ciò determina la liberazione di risorse dal momento che i server dipendenti non sono più necessari.
- Ogni volta che un prodotto viene selezionato o deselectato, vengono avviati automaticamente tutti i server che ospitano i servizi appartenenti alla categoria Servizi principali della piattaforma BI, ad eccezione dei servizi ospitati dal WACS. Il WACS rimane nello stato corrente.
- La deselectazione dei prodotti non implica la disinstallazione o la rimozione dei file di tali prodotti.

Ogni volta che si apre la pagina "Prodotti", gli stati dei prodotti rappresentano lo stato corrente del sistema.

Se tutti i server di un prodotto sono in esecuzione, la casella di controllo di tale prodotto è selezionata. Se tutti i server di un prodotto sono arrestati, la casella di controllo è deselectata. Se sono in esecuzione solo alcuni server di un prodotto, mentre altri presentano un altro stato, ad esempio di arresto, nella pagina "Prodotti" viene visualizzata la casella di controllo **Mantieni configurazione esistente** a indicare che il sistema è stato configurato all'esterno della procedura guidata. Per utilizzare la procedura guidata per modificare la configurazione è possibile deselectare la casella di controllo.

Nota:

- Nella pagina "Prodotti" vengono visualizzati tutti i prodotti installati nel cluster. Se ad esempio nel computer A sono installati i prodotti P1 e P2, mentre nel computer B sono installati i prodotti P2 e P3, nella pagina "Prodotti" saranno visualizzati P1, P2 e P3. I prodotti non installati non vengono visualizzati nella pagina "Prodotti".
- Per semplificare la distribuzione, non è necessario ripetere la configurazione di questa pagina per ogni nodo: viene infatti applicata all'intero cluster.

- Se in precedenza sono state modificate impostazioni nella CMC, viene visualizzato un messaggio che informa che le modifiche sono state apportate all'esterno della procedura guidata. È possibile scegliere di mantenere la configurazione esistente o di sostituire le impostazioni correnti.
- Le modifiche apportate nella procedura guidata non vengono applicate fino a quando non si fa clic su **Applica** nella pagina "Rivedi".

Dopo aver apportato tutte le modifiche desiderate, fare clic su **Avanti** per accedere alla pagina successiva della procedura guidata. È possibile anche utilizzare il pannello di spostamento a sinistra per passare direttamente a una pagina già visitata.

4.3 Scelta di un modello di distribuzione

L'installazione predefinita della piattaforma BI prevede la configurazione di una distribuzione di piccole dimensioni adatta a un ambiente demo su hardware del sistema limitato. Per adattarsi all'hardware e al caso di utilizzo previsto, ad esempio la preparazione di un sistema di test o di produzione, scegliere uno dei modelli predefiniti dalla pagina "Capacità". Questi modelli hanno lo scopo di consentire la rapida attivazione del sistema della piattaforma BI e di ridurre il tempo di distribuzione iniziale.

Sebbene la scelta di un modello di distribuzione appropriato possa essere utile per la configurazione iniziale e costituisca un punto di partenza, non sostituisce il ridimensionamento e l'ottimizzazione del sistema, che devono essere eseguite comunque. Per ottimizzare le prestazioni, è necessario ridimensionare il sistema facendo riferimento all'apposita guida: <http://www.sap.com/bisizing>.

La scelta di un modello di distribuzione appropriato è importante per diversi motivi:

- Influisce sulla capacità di gestione delle richieste del sistema. Una distribuzione di dimensioni maggiori offre una capacità superiore per la gestione di più richieste o di richieste più complesse. Questo tipo di distribuzione richiede tuttavia più risorse di sistema.
- La scelta di una distribuzione di dimensioni maggiori non garantisce prestazioni migliori, in particolare se non si dispone di sufficienti risorse hardware disponibili.
- Il modello di distribuzione scelto deve essere adeguato alle esigenze aziendali e alle risorse hardware disponibili. La scelta di un modello di distribuzione troppo piccolo per le esigenze aziendali o troppo grande per le risorse hardware disponibili potrebbe ridurre la capacità e le prestazioni del sistema.
- Modelli di distribuzione di dimensioni maggiori forniscono una migliore compartimentazione: si riduce la probabilità che gli errori di un prodotto influenzino altri prodotti. Scegliere un modello che bilanci le prestazioni e l'utilizzo delle risorse (RAM). Se ad esempio è disponibile una grande quantità di RAM, è necessario selezionare il modello di distribuzione più grande consentito dalla RAM in modo da ottenere una migliore compartimentazione del sistema.

Per selezionare un modello di distribuzione è possibile utilizzare il dispositivo di scorrimento o scegliere una quantità di RAM nell'elenco a discesa. Quando si modifica l'impostazione, osservare che l'indicatore "Numero di Adaptive Processing Server:" cambia per mostrare come verrà configurato il sistema scegliendo quella impostazione.

Nota:

- Il modello di distribuzione scelto influenza solo gli Adaptive Processing Server (APS). Non vengono invece influenzati gli altri server, ad esempio il CMS o gli Adaptive Job Server.

- RAM richiesta è la quantità minima di RAM richiesta per i server della piattaforma BI. Ad esempio, un computer con 16 GB di RAM, in cui il sistema operativo utilizza 1 GB di RAM, il server di database un altro GB e i server della piattaforma BI 10 GB, l'opzione RAM richiesta è uguale a 10 GB, non a 12 GB o 16 GB. Il numero indicato in RAM richiesta è solo un valore rappresentativo. Il sistema potrebbe richiedere una quantità maggiore di RAM nel caso di carichi pesanti. Per ottenere prestazioni ottimali del sistema, è necessario eseguirne sempre il ridimensionamento.
- Ogni volta che si apre la pagina "Capacità", il modello di distribuzione visualizzato rappresenta lo stato corrente del sistema, se corrisponde a uno dei modelli di distribuzione predefiniti. Se ad esempio è stato creato manualmente un Adaptive Processing Server supplementare utilizzando la CMC, lo stato corrente del sistema non corrisponde ad alcuno dei modelli di distribuzione. Nella pagina "Capacità" viene pertanto visualizzata la casella di controllo **Mantieni configurazione esistente** a indicare che il sistema è stato configurato al di fuori della procedura guidata. In una distribuzione a più nodi, la casella di controllo **Mantieni configurazione esistente** viene visualizzata anche se uno dei nodi contiene un numero di APS non corrispondente a un modello di distribuzione o se il numero di APS nei vari nodi è diverso. Per utilizzare la procedura guidata per modificare la configurazione è possibile deselectare la casella di controllo.
- Per semplificare la distribuzione, la configurazione APS selezionata viene applicata a ogni nodo (purché in tali nodi sia installato un APS). In questo modo, a un numero maggiore di nodi corrisponde un aumento della capacità del cluster.
- I componenti aggiuntivi, ad esempio Data Services o Analysis Application Design Service (AADS), non sono gestiti dalla procedura guidata. I servizi creati dai componenti aggiuntivi non vengono spostati in altri APS dalla procedura guidata.

Esempi:

- Se il servizio AADS è ospitato da un APS che ospita altri servizi dell'installazione principale della piattaforma BI, se si esegue la procedura guidata e si modificano le dimensioni del modello di distribuzione da piccole a medie, la procedura guidata crea sette nuovi APS in cui sposta tutti i servizi, ad eccezione di AADS, che rimane nell'APS iniziale.
- Il componente aggiuntivo Data Services crea un APS dedicato. La procedura guidata non modifica questo APS dedicato e non lo include nel conteggio del numero di APS del sistema.

File DeploymentTemplates.pdf

Per una descrizione dettagliata delle impostazioni configurate dalla procedura guidata per ogni modello di distribuzione disponibile, fare clic sul collegamento **modello di distribuzione** nella pagina "Capacità" per aprire il file `DeploymentTemplates.pdf`.

Il file `DeploymentTemplates.pdf` descrive i modelli di distribuzione in dettaglio. Si noti che i modelli non specificano il numero di utenti consentiti, in quanto tale numero dipende dal carico. È necessario eseguire il ridimensionamento del sistema per determinare il numero di utenti da supportare e, di conseguenza, la quantità di RAM necessaria, i requisiti della CPU e così via.

4.4 Specifica dei percorsi delle cartelle di dati

Utilizzare la pagina "Cartelle" per specificare il percorso in cui salvare i file di registro e di dati della piattaforma BI. È possibile specificare i percorsi delle cartelle o accettare quelli correnti.

Se la distribuzione della piattaforma BI contiene più nodi, è possibile definire i percorsi delle cartelle con due opzioni:

- Se si desidera configurare gli stessi percorsi di cartella per tutti i nodi, selezionare l'opzione **Tutti i nodi hanno gli stessi percorsi di cartella**.
- Se i server del cluster non sono configurati allo stesso modo, è possibile che i percorsi di installazione o le strutture di directory dei file siano diverse. È possibile selezionare l'opzione **I nodi hanno percorsi di cartella diversi** per configurare percorsi di cartella specifici per ogni nodo.

Ogni volta che viene aperta la pagina "Cartelle" della procedura guidata, i nomi delle cartelle vengono visualizzati come segue:

- Se tutti i nodi presentano cartelle con gli stessi valori, ovvero se le cartelle dei file di registro, quelle dei file di dati e le altre cartelle di tutti i server del cluster sono identiche, è selezionata l'opzione **Tutti i nodi hanno gli stessi percorsi** e vengono visualizzati i nomi delle cartelle correnti.
- Se tutte le cartelle di un determinato tipo (dei file di registro, dei file di dati, di controllo, dell'archivio file di input o dell'archivio file di output) sono identiche all'interno di ogni nodo, ma sono diverse tra i nodi, è selezionata l'opzione **I nodi hanno percorsi di cartella diversi** e vengono visualizzati i nomi delle cartelle correnti.
- Se tutte le cartelle di un determinato tipo sono identiche all'interno di ogni nodo e diverse tra i nodi, è selezionata l'opzione **I nodi hanno percorsi di cartella diversi** ma i nomi delle cartelle sono vuoti.

Se si modificano i percorsi delle cartelle, la procedura guidata configura il sistema per l'utilizzo delle nuove cartelle. Ad eccezione della cartelle dei dati di controllo, la procedura guidata non copia o sposta i contenuti delle cartelle originali nelle nuove cartelle. Se le nuove cartelle non presentano già il contenuto corretto o si desidera migrare dati presenti nelle cartelle originali, può essere necessario spostare o copiare tali dati nelle nuove cartelle.

Per le cartelle degli archivi dei file di input e output e le cartelle di dati, se il nuovo percorso di cartella è vuoto, è necessario copiare manualmente i file dal percorso di cartella precedente o ripristinare i file da un backup. Per la cartella dei file di registro, copiare i file dalla cartella precedente solo se si desidera che la nuova cartella contenga i file di registro presenti nel percorso di cartella precedente.

Suggerimento:

Se si intende copiare o ripristinare i file nelle nuove cartelle, eseguire l'operazione prima riavviare i nodi.

Scenari di esempio

- Se si modifica un percorso di cartella, e la cartella originale contiene report, tali report non saranno disponibili nella piattaforma BI fino a quando non verranno copiati nella nuova cartella e non verranno riavviati i nodi.
- Se la cartella originale contiene report danneggiati o modificati, e si desidera ripristinare un backup valido, recuperare i report dal backup e inserirli nella nuova cartella anziché copiare il contenuto dalla cartella originale.
- Se i file di dati sono stati originariamente collocati in un disco con lettera di unità X, e quest'ultima viene cambiata in Y nel sistema operativo, non è necessario copiare o spostare i file di dati: è sufficiente modificare il percorso di cartella nella piattaforma BI.

Se sono stati modificati manualmente alcuni percorsi di cartella, in modo che alcuni server di un nodo utilizzassero un gruppo di cartelle, mentre altri server dello stesso nodo ne utilizzassero di diverse, nella pagina "Cartelle" viene visualizzata la casella di controllo **Mantieni configurazione esistente a**

indicare che il sistema è stato configurato al di fuori della procedura guidata. È ad esempio possibile che due server File Repository Server dello stesso nodo siano configurati per utilizzare percorsi di cartelle dei file di registro diversi. Per utilizzare la procedura guidata per modificare la configurazione è possibile deselezionare la casella di controllo.

Per ulteriori informazioni sui tipi di file memorizzati in ogni cartella, fare clic sulle icone ?.

Nota:

Se si modifica uno dei percorsi di cartella seguenti, per fare in modo che le modifiche diventino effettive è necessario riavviare manualmente tutti i nodi al termine della procedura guidata:

- Archivio file di input
- Archivio file di output
- Cartella di registro
- Cartella dati

4.5 Verifica delle modifiche

Dopo aver completato la scelta delle impostazioni di configurazione, queste vengono visualizzate nella pagina "Rivedi" in modo che sia possibile verificarle, prima che le modifiche vengano applicate al sistema della piattaforma BI. Per ogni categoria di impostazioni è possibile fare clic su **Dettagli** per visualizzare una descrizione o un elenco dettagliato delle impostazioni e delle modifiche che verranno applicate.

Se si desidera modificare le impostazioni, è possibile accedere alle singole pagine direttamente dal menu di spostamento a sinistra della procedura guidata.

Le selezioni effettuate vengono salvate in un file di registro, che può essere scaricato dalla pagina Completato.

Viene anche generato e salvato un file di risposta. Il file di risposta consente di automatizzare la configurazione del sistema. È possibile fare clic sul pulsante **Scarica** per visualizzare il file di risposta o scaricarlo in un disco locale.

Quando si fa clic su **Applica**, le impostazioni di configurazione vengono applicate alla distribuzione della piattaforma BI. Al termine della procedura guidata, viene visualizzata la pagina "Completato", in cui sono mostrati i passaggi successivi da eseguire manualmente.

Argomenti correlati

- [File di registro e file di risposta](#)

4.6 File di registro e file di risposta

La pagina "Completato" riporta lo stato delle modifiche e consente di scaricare e visualizzare i file di registro e di risposta di una sessione.

I file di registro e di risposta vengono salvati automaticamente nella cartella Configurazione guidata del sistema, cui è possibile accedere dalla CMC. Nei nomi dei file è presente l'indicazione data e ora. Il formato dei nomi è il seguente `anno_mese_giorno_ora_minuti_secondi`. Per i file di registro viene utilizzata l'estensione `.log`, mentre per i file di risposta l'estensione `.ini`.

È anche possibile fare clic sui pulsanti **Scarica** per visualizzare i file di registro e di risposta o scaricarli in un disco locale.

Il file di registro presenta il contenuto seguente:

- Un record di tutte le modifiche apportate nella sessione di configurazione corrente.
- Il percorso in cui viene salvato il file di risposta.
- Un elenco che descrive i passaggi da seguire.

Argomenti correlati

- [Utilizzo di un file di risposta](#)

4.6.1 Utilizzo di un file di risposta

Ogni volta che viene completata la procedura guidata, viene salvato un file di risposta che contiene le selezioni o le risposte a tutte le domande delle pagine della procedura stessa. Il file di risposta può essere utilizzato per configurare altri cluster presenti nella distribuzione della piattaforma BI senza dover eseguire la procedura guidata per ognuno e può essere utilizzato in una data successiva se si desidera impostare il sistema sullo stesso stato di configurazione. L'utilizzo di un file di risposta consente di automatizzare la distribuzione e di evitare errori dell'operatore.

Per utilizzare un file di risposta, è necessario eseguire uno script che lo impieghi come parametro. Individuare innanzitutto il file di risposta da utilizzare, quindi salvarlo sul disco. I file di risposta vengono salvati automaticamente nella cartella Configurazione guidata sistema, cui gli amministratori possono accedere dalla CMC. Nei nomi dei file è presente l'indicazione data e ora. Il formato del nome è `anno_mese_giorno_ora_minuti_secondi` ed è seguito dall'estensione `.ini`. Dalla CMC è possibile visualizzare il file di risposta e salvarlo sul disco o utilizzare i comandi di menu **Organizza > Invia > Posizione file**.

È anche possibile scaricare il file di risposta per la sessione corrente della procedura guidata dalla pagina "Rivedi" o "Completato", quindi salvarlo sul disco.

Se si desidera modificare le impostazioni del file di risposta prima di utilizzarlo, è possibile modificarlo in un editor di testo. Per informazioni dettagliate, vedere il file di risposta di esempio riportato di seguito.

Esecuzione dello script

Una volta in possesso del file di risposta appropriato, utilizzarlo come parametro della riga di comando per gli script che eseguono la procedura guidata:

- In Windows, eseguire il file batch `SCW.bat`.
- In Unix, eseguire il file di script `scw.sh`.

I file batch e di script si trovano nella stessa cartella degli altri script di gestione dei server:

- In Windows: `<dirinstall>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.
- In Unix: `<dirinstall>/sap_bobj/enterprise_xi40/linux_x64/scripts`.

I file batch e di script utilizzano i parametri della riga di comando seguenti:

- `-help`: visualizza la Guida della riga di comando.
- `-r`: specifica il percorso e il nome del file di risposta.
- `-cms`: specifica il Central Management Server (CMS) cui si desidera accedere. Se questo parametro viene omesso, come impostazione predefinita del CMS vengono utilizzati il computer locale e la porta predefinita (6400). Esempio: `nome_computer:6500`
- `-username`: specifica un account che fornisce diritti amministrativi per la piattaforma BI. Se questo parametro viene omesso, viene utilizzato l'account Administrator predefinito.
- `-password`: specifica la password per l'account. Se non specificata, si tenta con una password vuota. Per utilizzare il parametro `-password`, è necessario utilizzare anche il parametro `-username`.

Esempi

In Windows: `SCW.bat -r c:\folder\filename.ini -cms cmsname:6400 -username "administrator" -password samplepassword`

In Unix: `./scw.sh -r /home/folder/filename.ini -cms cmsname:6400 -username "administrator" -password samplepassword`

File di risposta di esempio

```
# *****
# ***** Products *****
# *****

# Keep the existing configuration for products.
# Valid values = true or false.
# "true": the existing product configuration will be preserved.
# "false": the product configuration will be modified according to the "Products." settings below.

Products.KeepExistingConfiguration = true

# The "Products." settings below will be ignored if Products.KeepExistingConfiguration = true.

# Auto-start the servers for these products.
# Valid values = true or false.
# "true": the product's servers and their dependencies are auto-started with BI platform.
# "false": the product's servers are not auto-started with BI platform.

# Crystal Reports
Products.crystalreports = true

# Analysis edition for OLAP
Products.olap = true

# Web Intelligence
Products.webintelligence = false

# Dashboards (Xcelsius)
Products.dashboards = false

# Data Federator
Products.datafederator = true

# Lifecycle Manager
Products.LCM = true
```

```

# *****
# ***** Deployment Template *****
# *****

# Keep the existing configuration for the deployment template.
# Valid values = true or false.
# "true": the existing deployment template configuration will be preserved and the Capacity.DeploymentTemplate
# setting below will be ignored.
# "false": the deployment template configuration will be modified according to the Capacity.DeploymentTemplate
# setting below.

Capacity.KeepExistingConfiguration = true

# Specify the deployment template for all nodes.
# Valid values = xs, s, m, l, xl.

Capacity.DeploymentTemplate = xs

# *****
# ***** Folders *****
# *****

# Keep the existing configuration for folder locations.
# Valid values = true or false.
# "true": the existing folder configuration will be preserved.
# "false": the folder configuration will be modified according to the "Folders." settings below.

Folders.KeepExistingConfiguration = true

# The "Folders." settings below will be ignored if Folders.KeepExistingConfiguration = true.

# ----- All nodes use the same folders -----
# Use this section when you have one node, or when all nodes have the same folder locations. Otherwise, com
ment it out.

Folders.InputFileStore = <Path>
Folders.OutputFileStore = <Path>
Folders.Log = <Path>
Folders.Data = <Path>
Folders.Auditing = <Path>

# ----- Nodes use different folders -----
# Use this section when nodes have different folder locations. Otherwise, comment it out.

# ----- NodeOne -----
# Folders.NodeOne.InputFileStore = <Path>
# Folders.NodeOne.OutputFileStore = <Path>
# Folders.NodeOne.Log = <Path>
# Folders.NodeOne.Data = <Path>
# Folders.NodeOne.Auditing = <Path>

# ----- NodeTwo -----
# Folders.NodeTwo.InputFileStore = <Path>
# Folders.NodeTwo.OutputFileStore = <Path>
# Folders.NodeTwo.Log = <Path>
# Folders.NodeTwo.Data = <Path>
# Folders.NodeTwo.Auditing = <Path>

```

Tutte le impostazioni nel file di risposta devono essere specificate e non possono essere vuote, ad eccezione dei casi seguenti:

- Nel caso di una distribuzione a più nodi è possibile scegliere di omettere le impostazioni di cartella per uno o più nodi, in modo da lasciare inalterate le cartelle presenti in tali nodi. Per i nodi specificati nel file di risposta è invece necessario indicare tutti i percorsi di cartella.
- Se il parametro `KeepExistingConfiguration` è impostato su `true`, è possibile omettere le altre impostazioni di tale pagina. Se ad esempio `Products.KeepExistingConfiguration = true`, è possibile omettere le altre impostazioni della pagina "Prodotti" dal file di risposta

In alcuni casi, il file di risposta include prodotti diversi da quelli installati nel cluster di destinazione. In questi casi, si verificano i comportamenti seguenti:

- Se il file di risposta non contiene definizioni per i prodotti installati nel cluster di destinazione, l'operazione non riesce.
- Se il file di risposta contiene definizioni per prodotti non presenti nel cluster di destinazione, viene aggiunto un messaggio di avviso al file di registro e gli altri prodotti vengono configurati correttamente.

Nota:

- Dopo aver utilizzato un file di risposta per configurare un cluster, è necessario eseguire manualmente le altre operazioni descritte nella sezione "Next steps" del file di registro.
- Per una maggior protezione, è richiesto solo il supporto dell'autenticazione Enterprise (non Windows AD, LDAP o SAP).
- Se si preferisce rimandare il riavvio dei nodi al successivo riavvio pianificato, eseguire lo script subito prima di un periodo di inattività pianificato del sistema.

Gestione delle licenze

5.1 Gestione dei codici di licenza

In questa sezione viene descritto come gestire le chiavi di licenza per la distribuzione della piattaforma BI.

Argomenti correlati

- [Visualizzazione delle informazioni sulle licenze](#)
- [Per aggiungere un codice di licenza](#)
- [Visualizzazione dell'attività dell'account corrente](#)

5.1.1 Visualizzazione delle informazioni sulle licenze

L'area di gestione "Codici di licenza" della CMC identifica il numero di licenze titolari e per processore che sono associate a ogni codice.

1. Passare all'area di gestione "Codici di licenza" della CMC.
2. Selezionare un codice di licenza.

I dettagli associati al codice verranno visualizzati nell'area **Informazioni sul codice di licenza**. Per acquistare ulteriori codici di licenza, contattare il proprio rappresentante di vendita SAP.

Argomenti correlati

- [Per aggiungere un codice di licenza](#)
- [Visualizzazione dell'attività dell'account corrente](#)

5.1.2 Per aggiungere un codice di licenza

se si sta eseguendo l'aggiornamento da una versione di prova del prodotto, eliminare la chiave Valutazione prima di aggiungere nuovi codici di licenza o codici di attivazione dei prodotti. Dopo avere aggiunto i nuovi codici di licenza, sarà necessario abilitare nuovamente tutti i server.

Nota:

Se sono stati ricevuti nuovi codici di licenza in seguito a una modifica all'interno dell'organizzazione nella modalità con cui le licenze della piattaforma BI vengono implementate, è necessario eliminare i codici di licenza precedenti dal sistema al fine di mantenere la conformità.

1. Passare all'area di gestione **Codici di licenza** della CMC.
2. Digitare il codice nel campo **Aggiungi codice**.
3. Fare clic su **Aggiungi**.

Il codice verrà aggiunto all'elenco.

Argomenti correlati

- [Visualizzazione delle informazioni sulle licenze](#)
- [Visualizzazione dell'attività dell'account corrente](#)

5.1.3 Visualizzazione dell'attività dell'account corrente

1. Passare all'area di gestione **Impostazioni** della CMC.
2. Fare clic su **Visualizza le metriche di sistema globali**.

In questa sezione viene indicato l'utilizzo delle licenze correnti, insieme alle specifiche dei processi aggiuntivi.

Argomenti correlati

- [Per aggiungere un codice di licenza](#)
- [Visualizzazione delle informazioni sulle licenze](#)

Gestione di utenti e gruppi

6.1 Panoramica della gestione dei server

La gestione degli account include tutte le attività relative alla creazione, alla mappatura, alla modifica e all'organizzazione delle informazioni su utenti e gruppi. L'area di gestione "Utenti e gruppi" della Central Management Console (CMC) offre una posizione centrale per eseguire queste attività.

Dopo aver creato gli account utente e i gruppi, è possibile aggiungere oggetti e specificare i diritti di accesso. Quando accedono, gli utenti possono visualizzare gli oggetti utilizzando BI Launch Pad o un'applicazione Web personalizzata.

6.1.1 Gestione utenti

Nell'area di gestione "Utenti e gruppi" è possibile specificare tutte le informazioni necessarie affinché un utente possa accedere alla piattaforma BI. È anche possibile visualizzare i due account utente predefiniti riepilogati nella tabella "Account utente predefiniti".

Tabella 6 - 1: Account utente predefiniti

Nome account	Descrizione
Amministratore	L'utente appartiene ai gruppi Amministratori e Tutti . Un amministratore può eseguire tutte le attività in tutte le applicazioni della piattaforma BI (ad esempio CMC, CCM, Pubblicazione guidata e BI Launch Pad).
Guest	Questo utente appartiene al gruppo Tutti . L'account viene abilitato per impostazione predefinita e non viene assegnata una password dal sistema. Se si assegna una password, viene interrotto il Single Sign On a BI Launch Pad.

Nome account	Descrizione
SMAAdmin	Account di sola lettura utilizzato da SAP Solution Manager per accedere ai componenti della piattaforma BI.

Nota:

le migrazioni di oggetti vengono eseguite al meglio da membri del gruppo Amministratori, in particolare dall'account utente Administrator. La migrazione di un oggetto potrebbe implicare la migrazione anche di molti oggetti correlati. Un account amministratore delegato potrebbe non ottenere i diritti di protezione richiesti per tutti gli oggetti.

6.1.2 Gestione gruppi

I gruppi sono insiemi di utenti che condividono gli stessi privilegi di account, quindi è possibile creare gruppi basati su reparto, ruolo o posizione. I gruppi consentono di modificare i diritti degli utenti in una posizione specifica (un gruppo) anziché modificare i diritti per ciascun account utente singolarmente. È inoltre possibile assegnare i diritti dell'oggetto a un gruppo o a più gruppi.

Nell'area "Utenti e gruppi", è possibile creare gruppi che consentono a un certo numero di utenti di accedere a report o cartelle. Ciò consente di apportare delle modifiche in un punto preciso piuttosto che modificare individualmente ciascun account utente. È anche possibile visualizzare i diversi account di gruppo predefiniti riepilogati nella tabella "Account di gruppo predefiniti".

Per visualizzare i gruppi disponibili nella console CMC, fare clic su **Elenco gruppi** nel pannello Albero. In alternativa, è possibile fare clic su **Gerarchia gruppi** per visualizzare un elenco gerarchico di tutti i gruppi disponibili.

Tabella 6 - 2: Account di gruppo predefiniti

Nome account	Descrizione
Amministratori	I membri di questo gruppo possono eseguire tutte le attività in tutte le applicazioni della piattaforma BI (CMC, CCM, Pubblicazione guidata e BI Launch Pad). Per impostazione predefinita, il gruppo Amministratori contiene solo l'utente Administrator.
Tutti	Ogni utente è un membro del gruppo Tutti .
QaaWS Group Designer	I membri di questo gruppo hanno accesso a Query come Servizio Web.

Nome account	Descrizione
Utenti di Strumento di conversione dei report	I membri di questo gruppo hanno accesso all'applicazione Strumento di conversione dei report.
Traduttori	I membri di questo gruppo hanno accesso all'applicazione Translation Manager.
Utenti di Universe Designer	Il diritto di accedere alle cartelle Universe Designer e Connessioni viene concesso agli utenti che appartengono a questo gruppo. Essi possono verificare chi dispone dei diritti di accesso all'applicazione di progettazione. Aggiungere gli utenti a questo gruppo a seconda delle esigenze. Per impostazione predefinita questo gruppo non contiene utenti.

Argomenti correlati

- [Funzionamento dei diritti nella piattaforma BI](#)
- [Concessione del diritto di accesso a utenti e gruppi](#)

6.1.3 Tipi di autenticazione disponibili

Prima di impostare gli account utente e i gruppi all'interno della piattaforma BI, è opportuno decidere il tipo di autenticazione che si desidera utilizzare. Nella tabella "Tipi di autenticazione" sono riportate le opzioni di autenticazione che possono essere disponibili in base agli strumenti di protezione utilizzati dall'azienda.

Tabella 6 - 3: Tipi di autenticazione

Tipo di autenticazione	Descrizione
Enterprise	Utilizzare l'autenticazione Enterprise predefinita del sistema se si preferisce creare account e gruppi distinti da utilizzare con la piattaforma BI oppure se non è stata ancora impostata una gerarchia di utenti e gruppi in un server di directory LDAP o in un server Windows AD.

Tipo di autenticazione	Descrizione
LDAP	Se viene impostato un server di directory LDAP, è possibile utilizzare con la piattaforma BI gli account utente e i gruppi esistenti in LDAP. Quando gli account LDAP vengono mappati alla piattaforma BI, gli utenti possono accedere alle applicazioni della piattaforma BI con il nome utente e la password LDAP di cui dispongono. In questo modo si evita di creare nuovamente account utente e di gruppo individuali all'interno della piattaforma BI.
Windows AD	È possibile utilizzare gli account utente e i gruppi Windows AD già esistenti nella piattaforma BI. Quando gli account AD vengono mappati alla piattaforma BI, gli utenti possono accedere alle applicazioni della piattaforma BI con il nome utente e la password AD di cui dispongono. In questo modo si evita di creare nuovamente account utente e di gruppo individuali all'interno della piattaforma BI.
SAP	È possibile mappare i ruoli SAP esistenti negli account della piattaforma BI. Dopo avere mappato i ruoli SAP, gli utenti saranno in grado di accedere alle applicazioni della piattaforma BI utilizzando le proprie credenziali SAP. In questo modo si evita di creare nuovamente account utente e di gruppo individuali all'interno della piattaforma BI.
Oracle EBS	È possibile mappare i ruoli Oracle EBS esistenti negli account della piattaforma BI. Dopo avere mappato i ruoli Oracle EBS, gli utenti saranno in grado di accedere alle applicazioni della piattaforma BI utilizzando le proprie credenziali Oracle EBS. In questo modo si evita di creare nuovamente account utente e di gruppo individuali all'interno della piattaforma BI.
Siebel	È possibile mappare i ruoli Siebel esistenti negli account della piattaforma BI. Dopo avere mappato i ruoli Siebel, gli utenti saranno in grado di accedere alle applicazioni della piattaforma BI utilizzando le proprie credenziali Siebel. In questo modo si evita di creare nuovamente account utente e di gruppo individuali all'interno della piattaforma BI.

Tipo di autenticazione	Descrizione
PeopleSoft Enterprise	È possibile mappare i ruoli PeopleSoft esistenti negli account della piattaforma BI. Dopo avere mappato i ruoli PeopleSoft, gli utenti saranno in grado di accedere alle applicazioni SAP della piattaforma BI utilizzando le proprie credenziali PeopleSoft. In questo modo si evita di creare nuovamente account utente e di gruppo individuali all'interno della piattaforma BI.
JD Edwards EnterpriseOne	È possibile mappare i ruoli JD Edwards esistenti negli account della piattaforma BI. Dopo avere mappato i ruoli JD Edwards, gli utenti saranno in grado di accedere alle applicazioni della piattaforma BI utilizzando le proprie credenziali JD Edwards. In questo modo si evita di creare nuovamente account utente e di gruppo individuali all'interno della piattaforma BI.

6.2 Gestione di account Enterprise e generali

Poiché l'autenticazione Enterprise rappresenta il metodo di autenticazione predefinito della piattaforma BI, viene abilitata automaticamente alla prima installazione del sistema. Quando vengono aggiunti e gestiti utenti e gruppi, la piattaforma conserva all'interno del database le informazioni ad essi correlate.

Nota:

Quando un utente si disconnette dalla sessione Web nella piattaforma BI accedendo a una pagina non della piattaforma oppure chiudendo il browser, la sessione Enterprise non viene disconnessa e la licenza viene mantenuta. La sessione Enterprise verrà terminata dopo circa 24 ore. Per terminare la sessione Enterprise dell'utente e liberare la licenza per altri, l'utente deve disconnettersi dalla piattaforma.

6.2.1 Per creare un account utente

Quando si crea un nuovo utente vengono specificate le proprietà dell'utente e selezionato il gruppo o i gruppi di cui l'utente sarà membro.

1. Passare all'area di gestione "Utenti e gruppi" della CMC.
2. Scegliere **Gestisci > Nuovo > Nuovo utente**.

Viene visualizzata la finestra di dialogo "Nuovo utente".

3. Per creare un utente Enterprise:

- a. Nell'elenco **Tipo di autenticazione** selezionare **Aziendale**.
- b. Digitare il nome account, il nome completo, l'indirizzo di posta elettronica e le informazioni descrittive.

Suggerimento:

Utilizzare l'area riservata alle descrizioni per includere informazioni aggiuntive sull'utente o sull'account.

- c. Specificare le informazioni sulla password e le impostazioni.

4. Per creare un utente che eseguirà l'accesso utilizzando un tipo di autenticazione differente, selezionare l'opzione appropriata nell'elenco **Tipo di autenticazione** e digitare il nome dell'account.

5. Eseguire una delle azioni seguenti per designare l'account utente (in base al contratto di licenza della piattaforma BI):

- Selezionare **Utente simultaneo** se questo utente ha sottoscritto un contratto di licenza che definisce il numero di utenti a cui è consentito l'accesso simultaneo.
- Selezionare **Utente designato** se l'utente ha sottoscritto un contratto di licenza che associa uno specifico utente a una licenza. Le licenze degli utenti designati risultano utili per chi richiede l'accesso alla piattaforma BI indipendentemente dagli altri utenti al momento connessi.

6. Scegliere **Crea e chiudi**.

L'utente viene aggiunto al sistema e automaticamente al gruppo Tutti. Per l'utente vengono creati automaticamente una casella di posta in arrivo e un alias Enterprise.

Ora è possibile aggiungere l'utente a un gruppo o specificare i diritti di cui dispone.

Argomenti correlati

- [Funzionamento dei diritti nella piattaforma BI](#)

6.2.2 Per modificare un account utente

Utilizzare la seguente procedura per modificare le proprietà di un utente o la sua appartenenza a un gruppo.

Nota:

L'utente sarà coinvolto nella modifica se risulta collegato nel momento in cui questa viene effettuata.

1. Accedere all'area di gestione "Utenti e gruppi" della console CMC.
2. Selezionare l'utente di cui si desidera modificare le proprietà.
3. Fare clic su **Gestisci > Proprietà**.

Viene visualizzata la finestra di dialogo "Proprietà" dell'utente.

4. Modificare le proprietà dell'utente.

Oltre a tutte le opzioni disponibili quando l'account è stato creato per la prima volta, ora è possibile disattivare l'account selezionando la casella di controllo **Account disattivato**.

Nota:

Tutte le modifiche apportate all'account utente non verranno visualizzate fino al successivo accesso.

5. Fare clic su **Salva e chiudi**.

Argomenti correlati

- [Per creare un nuovo alias per un utente esistente](#)

6.2.3 Per eliminare un account utente

Utilizzare la seguente procedura per eliminare un account utente. L'utente potrebbe ricevere un messaggio di errore se risulta collegato nel momento in cui l'account viene eliminato. Eliminando un account utente vengono eliminati anche la cartella Preferiti, le categorie personali e la casella di posta dell'utente.

Se si ritiene che l'utente in futuro potrebbe nuovamente richiedere l'accesso all'account, anziché eliminarlo selezionare la casella di controllo **Account disattivato** nella finestra di dialogo "Proprietà" dell'utente selezionato.

Nota:

L'eliminazione di un account utente non impedisce necessariamente all'utente di accedere di nuovo alla piattaforma BI. Se l'account utente esiste anche in un sistema di terze parti e appartiene a un gruppo di terze parti mappato alla piattaforma BI, l'utente può comunque riuscire ad accedere.

1. Passare all'area di gestione "Utenti o Gruppi" della console CMC.
2. Selezionare l'utente da eliminare.
3. Scegliere **Gestisci > Elimina**.

Viene visualizzata la finestra di dialogo di conferma dell'eliminazione.

4. Fare clic su **OK**.

L'account utente viene eliminato.

Argomenti correlati

- [Per modificare un account utente](#)
- [Per eliminare un account utente](#)
- [Per disattivare un alias](#)

6.2.4 Per creare un nuovo gruppo

1. Accedere all'area di gestione "Utenti e gruppi" della console CMC.
2. Scegliere **Gestisci > Nuovo > Nuovo gruppo**.
Verrà visualizzata la finestra di dialogo "Crea nuovo gruppo utente".
3. Immettere il nome del gruppo e la descrizione.
4. Fare clic su **OK**.

Dopo aver creato un nuovo gruppo è possibile aggiungere utenti, aggiungere sottogruppi o specificare l'appartenenza al gruppo; in quest'ultimo caso il nuovo gruppo è in realtà un sottogruppo. Poiché i sottogruppi forniscono livelli aggiuntivi di organizzazione, si rivelano utili quando vengono impostati i diritti degli oggetti per il controllo dell'accesso utente al contenuto della piattaforma BI.

6.2.5 Per modificare le proprietà di un gruppo

È possibile modificare le proprietà di un gruppo apportando modifiche a una qualsiasi delle impostazioni.

Nota:

Gli utenti che appartengono al gruppo saranno interessati dalla modifica al successivo accesso.

1. Nell'area di gestione "Utenti e gruppi" della console CMC, selezionare il gruppo.
2. Fare clic su **Gestisci > Proprietà**.
Viene visualizzata la finestra di dialogo "Proprietà".
3. Modificare le proprietà per il gruppo.
Fare clic sui collegamenti dall'elenco di spostamento per accedere alle diverse finestre di dialogo e modificare le diverse proprietà.
 - Se si desidera modificare il titolo o la descrizione per il gruppo, fare clic su **Proprietà**.
 - Se si desidera modificare i diritti dei principali sul gruppo, fare clic su **Protezione utente**.
 - Se si desidera modificare i valori di profilo per i membri del gruppo, fare clic su **Valori di profilo**.
 - Se si desidera aggiungere il gruppo o un sottogruppo a un altro gruppo, fare clic su **Membro di**.
4. Fare clic su **Salva**.

6.2.6 Per visualizzare i membri del gruppo

È possibile utilizzare questa procedura per visualizzare gli utenti appartenenti a uno specifico gruppo.

1. Accedere all'area di gestione "Utenti e gruppi" della console CMC.
2. Espandere **Gerarchia gruppi** nel pannello **Albero**.
3. Selezionare il gruppo nel pannello **Albero**.

Nota:

se nel gruppo è presente un numero considerevole di utenti oppure se il gruppo è mappato a una directory di terze parti, l'aggiornamento dell'elenco potrebbe richiedere alcuni minuti.

Viene visualizzato l'elenco degli utenti appartenenti al gruppo.

6.2.7 Per aggiungere i sottogruppi

È possibile aggiungere un gruppo a un altro gruppo. In questo caso, il gruppo aggiunto diventa un sottogruppo.

Nota:

l'aggiunta di un sottogruppo è simile alla definizione dell'appartenenza al gruppo.

1. Nell'area di gestione "Utenti e gruppi" della console CMC, selezionare il gruppo che si desidera aggiungere come sottogruppo a un altro gruppo.
2. Scegliere **Azioni > Unisci gruppo**.
Verrà visualizzata la finestra di dialogo "Unisci gruppo".
3. Spostare il gruppo a cui si desidera aggiungere il primo gruppo dall'elenco **Gruppi disponibili** all'elenco **Gruppi di destinazione**.
4. Fare clic su **OK**.

Argomenti correlati

- [Per specificare l'appartenenza al gruppo](#)

6.2.8 Per specificare l'appartenenza al gruppo

È possibile trasformare un gruppo in un membro di un altro gruppo. Il gruppo che diviene membro viene chiamato sottogruppo. Il gruppo cui viene aggiunto il sottogruppo è il gruppo principale. Un sottogruppo eredita i diritti del gruppo principale.

1. Nell'area di gestione "Utenti e gruppi" della console CMC, fare clic sul gruppo da aggiungere a un altro gruppo.
2. Scegliere **Azioni > Membro di**.
Verrà visualizzata la finestra di dialogo "Membro di".
3. Fare clic su **Unisci gruppo**.

Verrà visualizzata la finestra di dialogo "Unisci gruppo".

4. Spostare il gruppo a cui si desidera aggiungere il primo gruppo dall'elenco **Gruppi disponibili** all'elenco **Gruppi di destinazione**.

Tutti i diritti associati al gruppo principale saranno ereditati dal nuovo gruppo appena creato.

5. Fare clic su **OK**.

Viene nuovamente visualizzata la finestra di dialogo "Membro di" e il gruppo principale viene visualizzato nell'elenco dei gruppi principali.

6.2.9 Per eliminare un gruppo

Quando un gruppo non risulta più necessario, è possibile eliminarlo. Non è possibile eliminare i gruppi predefiniti Amministratori e Tutti.

Nota:

- Gli utenti che appartengono al gruppo eliminato saranno interessati dalla modifica al successivo accesso.
- Gli utenti che appartengono al gruppo eliminato perderanno i diritti ereditati dal gruppo.

Per eliminare un gruppo di autenticazione di terze parti, ad esempio il gruppo utenti Windows AD, utilizzare l'area di gestione "Autenticazione " nella CMC.

1. Accedere all'area di gestione "Utenti e gruppi" della console CMC.
2. Selezionare il gruppo da eliminare.
3. Scegliere **Gestisci > Elimina**.

Viene visualizzata la finestra di dialogo di conferma dell'eliminazione.

4. Fare clic su **OK**.

Il gruppo viene eliminato.

6.2.10 Aggiunta in blocco di utenti o gruppi di utenti

Per aggiungere utenti o gruppi di utenti in massa alla CMC è possibile utilizzare un file CSV (comma-separated values). In un file CSV con formato corretto, le virgole separano i dati in una riga, come illustrato nell'esempio seguente:

```
Add,MyGroup,MyUser1,MyFullName,Password1,My1@example.com,ProfileName,ProfileValue
```

Al processo di aggiunta in blocco si applicano le condizioni seguenti:

- Tutte le righe del file CSV che contengono un errore vengono escluse dal processo di importazione.
- Gli account utente vengono inizialmente disabilitati dopo l'importazione.

- È possibile utilizzare password vuote quando si creano nuovi utenti. È invece necessario utilizzare una password valida per l'autenticazione di Enterprise per tutti i successivi aggiornamenti agli utenti esistenti.
 - Quando si aggiunge una credenzialeDB a un account, le credenziali del database vengono abilitate nel profilo dell'utente.
1. Nell'area di gestione **Utenti e gruppi** della CMC, selezionare **Gestisci > Importa > Utente/Gruppo/CredenzialeDB**.
Viene visualizzata la finestra di dialogo "Importa utente/gruppo/credenzialeDB".
 2. Fare clic su **Sfoglia**, selezionare un file CSV, quindi fare clic su **Verifica**.
Il file viene elaborato. Se i dati del file presentano un formato corretto, il pulsante **Importa** diventa attivo. Se il formato dei dati non è corretto, vengono visualizzate informazioni sull'errore, che deve essere risolto prima che la CMC possa verificare il file per l'importazione.
 3. Fare clic su **Importa**.
Gli utenti o i gruppi di utenti vengono importati nella CMC.
Per verificare gli utenti o i gruppi di utenti aggiunti, selezionare **Gestisci > Importa > Cronologia** nell'area di gestione **Utenti e gruppi**.

6.2.11 Per abilitare l'account Guest

Per impostazione predefinita, l'account Guest è disabilitato, per garantire che nessun utente possa utilizzarlo per accedere alla piattaforma BI. Questa impostazione predefinita disabilita anche la funzionalità Single Sign On anonimo della piattaforma BI e pertanto gli utenti non saranno in grado di accedere a BI Launch Pad senza aver prima fornito un nome utente e una password validi.

Eseguire l'attività seguente se si desidera abilitare l'account Guest in modo che gli utenti non richiedano ai propri account di accedere a BI Launch Pad.

1. Passare all'area di gestione **Utenti e gruppi** della CMC.
2. Fare clic su **Elenco utenti** nel pannello di spostamento.
3. Selezionare **Guest**.
4. Fare clic su **Gestisci > Proprietà**.
Viene visualizzata la finestra di dialogo "Proprietà".
5. Deselezionare la casella di controllo **Account disattivato**.
6. Fare clic su **Salva e chiudi**.

6.2.12 Aggiunta di utenti ai gruppi

È possibile aggiungere utenti ai gruppi nei seguenti modi:

- Selezionare il gruppo, quindi fare clic su **Azioni > Aggiungi membri al gruppo**.
- Selezionare l'utente, quindi fare clic su **Azioni > Membro di**.
- Selezionare l'utente, quindi fare clic su **Azioni > Unisci gruppo**.

Le procedure che seguono descrivono il modo in cui gli utenti vengono aggiunti ai gruppi adottando questi metodi.

Argomenti correlati

- [Per specificare l'appartenenza al gruppo](#)

6.2.12.1 Per aggiungere un utente a uno o più gruppi

1. Accedere all'area di gestione "Utenti e gruppi" della console CMC.
2. Selezionare l'utente che si desidera aggiungere a un gruppo.
3. Scegliere **Azioni > Unisci gruppo**.

Nota:

tutti gli utenti della piattaforma BI del sistema fanno parte del gruppo Tutti.

Verrà visualizzata la finestra di dialogo "Unisci gruppo".

4. Spostare il gruppo a cui si desidera aggiungere l'utente dall'elenco **Gruppi disponibili** all'elenco **Gruppi di destinazione**.

Suggerimento:

Utilizzare **MAIUSC + clic** o **CTRL + clic** per selezionare più gruppi.

5. Fare clic su **OK**.

6.2.12.2 Per aggiungere utenti a un gruppo

1. Nell'area di gestione "Utenti e gruppi" della console CMC, selezionare il gruppo.
 2. Scegliere **Azioni > Aggiungi membri al gruppo**.
- Viene visualizzata la finestra di dialogo "Aggiungi".

3. Fare clic su **Elenco utenti**.

L'elenco **Utenti/gruppi disponibili** viene aggiornato e vengono visualizzati tutti gli account utente del sistema.

4. Spostare l'utente che si desidera aggiungere al gruppo dall'elenco **Gruppi/utenti disponibili** all'elenco **Utenti/gruppi selezionati**.

Suggerimento:

- Per selezionare più utenti, utilizzare la combinazione **MAIUSC + clic** o **CTRL + clic**.
 - Per cercare un utente specifico, utilizzare il campo di ricerca.
 - Se sul sistema sono presenti molti utenti, fare clic sui pulsanti **Precedente** e **Successivo** per spostarsi all'interno dell'elenco di utenti.
5. Fare clic su **OK**.

6.2.13 Modifica delle impostazioni password

In CMC, è possibile modificare le impostazioni della password relative a un utente specifico o a tutti gli utenti del sistema. Le varie limitazioni elencate di seguito sono valide solo per gli account Enterprise; in altre parole, non si applicano ad account mappati a un database utente esterno (LDAP o Windows AD). In genere, tuttavia, il sistema esterno consente di inserire limitazioni simili per gli account esterni.

6.2.13.1 Per modificare le impostazioni della password utente

1. Passare all'area di gestione "Utenti e gruppi" della CMC.
2. Selezionare l'utente di cui si desidera modificare le impostazioni della password.
3. Fare clic su **Gestisci > Proprietà**.
Viene visualizzata la finestra di dialogo "Proprietà".
4. Selezionare o deselezionare la casella di controllo associata alle impostazioni password che si desidera modificare.
Le opzioni disponibili sono:
 - **Nessuna scadenza password**
 - **Modifica obbligatoria password all'accesso successivo**
 - **Modifica password non consentita**
5. Fare clic su **Salva e chiudi**.

6.2.13.2 Per modificare le impostazioni generali della password

1. Passare all'area di gestione "Autenticazione" della CMC.

2. Fare doppio clic su **Enterprise**.

Verrà visualizzata la finestra di dialogo "Enterprise".

3. Selezionare la casella di controllo per ciascuna impostazione della password da usare e specificare un valore se richiesto.

La seguente tabella identifica i valori minimo e massimo per ogni impostazione che è possibile configurare.

Tabella 6 - 4: Impostazioni password

Impostazione password	Minimo	Massimo consigliato
Attiva password con maiuscole e minuscole	N/D	N/D
Devono essere contenuti almeno N caratteri	0 caratteri	64 caratteri
È necessario modificare la password ogni N giorni	1 giorno	100 giorni
Impossibile riutilizzare le N password più recenti	1 password	100 password
È necessario attendere N minuti per modificare la password	0 minuti	100 minuti
Disattiva account dopo N tentativi di accesso non riusciti	1 non riuscito	100 non riusciti
Reimposta il conteggio degli accessi non riusciti dopo N minuti	1 minuto	100 minuti
Riattiva account dopo N minuti	0 minuti	100 minuti

4. Fare clic su **Aggiorna**.

Nota:

gli account utente inattivi non verranno disattivati automaticamente.

6.2.14 Concessione del diritto di accesso a utenti e gruppi

È possibile concedere a utenti e gruppi il diritto di accesso amministrativo ad altri utenti e gruppi. I diritti amministrativi includono: visualizzazione, modifica ed eliminazione di oggetti, nonché visualizzazione, eliminazione e sospensione di istanze di oggetti. Ad esempio, per la risoluzione dei problemi e la manutenzione del sistema, può essere opportuno concedere al reparto IT l'accesso per la modifica e l'eliminazione di oggetti.

Argomenti correlati

- [Per assegnare principali a un elenco di controllo di accesso per un oggetto](#)

6.2.15 Controllo dell'accesso alle caselle di posta in entrata dell'utente

Quando si aggiunge un utente, il sistema crea automaticamente una casella di posta in entrata per l'utente inserito. La casella di posta in entrata ha lo stesso nome dell'utente. Per impostazione predefinita, solo l'utente e l'amministratore dispongono dei diritti di accesso alla casella di posta dell'utente.

Argomenti correlati

- [Impostazione di una pianificazione per un oggetto programma](#)
- [Gestione delle impostazioni di protezione per gli oggetti nella CMC](#)

6.2.16 Configurazione delle opzioni di BI Launch Pad

Gli amministratori possono configurare il modo in cui gli utenti accedono alle applicazioni BI Launch Pad. Configurando le proprietà nel file BOE.war, è possibile specificare le informazioni disponibili nella schermata di accesso dell'utente. È inoltre possibile utilizzare la console CMC per impostare le preferenze di BI Launch Pad per gruppi specifici.

6.2.16.1 Configurazione della schermata di accesso di BI Launch Pad

Per impostazione predefinita, la schermata di accesso di BI Launch Pad richiede l'immissione del nome utente e della password. È possibile configurarla in modo che vengano richiesti anche il nome CMS e il tipo di autenticazione. Per modificare questa impostazione, è necessario modificare le proprietà di BI Launch Pad per il file BOE.war.

6.2.16.1.1 Configurazione della schermata di accesso di BI Lunch Pad

Per modificare le impostazioni predefinite di BI Launch Pad, è necessario impostare le proprietà personalizzate di BI Launch Pad per il file BOE.war. Questo file viene distribuito sul computer che ospita il server di applicazioni Web.

1. Accedere alla seguente directory nell'installazione della piattaforma BI:

```
<DIRINSTALL>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\
```

2. Creare un nuovo file utilizzando un editor di testo.
3. Salvare il file con questo nome:
Bllaunchpad.properties
4. Per includere le opzioni di autenticazione nella schermata di accesso di BI Launch Pad, aggiungere la riga seguente:

```
authentication.visible=true
```

5. Per modificare l'autenticazione predefinita, aggiungere la riga seguente:

```
authentication.default=<authentication>
```

Sostituire <authentication> con una delle opzioni seguenti:

Tipo di autenticazione	Valore <authentication>
Enterprise	SecEnterprise
LDAP	secLDAP
Windows AD	secWinAD
SAP	secSAPR3

6. Per richiedere agli utenti il nome del CMS nella schermata di accesso di BI Launch Pad, aggiungere la riga seguente:

```
cms.visible=true
```

7. Salvare e chiudere il file.
8. Riavviare il server di applicazioni Web.

Utilizzare WDeploy per ridistribuire il file `BOE.war` sul server di applicazioni Web. Per ulteriori informazioni sull'utilizzo di WDeploy, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*

6.2.16.2 Impostazione delle preferenze di BI Launch Pad per i gruppi di utenti

Gli amministratori possono specificare i valori predefiniti per le preferenze di BI Launch Pad, da applicare a tutti gli utenti di un gruppo di utenti.

Nota:

Quando gli utenti impostano le proprie preferenze, le impostazioni definite dall'amministratore non vengono applicate alla visualizzazione di un utente di BI Launch Pad. Gli utenti possono passare dalle proprie impostazioni delle preferenze a quelle definite dall'amministratore in qualsiasi momento.

Per impostazione predefinita, non vengono specificate preferenze di BI Launch Pad per i gruppi di utenti. Gli amministratori possono specificare i valori predefiniti per le preferenze seguenti:

- Scheda iniziale
- Posizione in cui vengono memorizzati i documenti
- Cartelle
- Categorie
- Numero di oggetti per pagina
- Colonne visualizzate nella scheda **Documento**
- Come visualizzare i documenti in BI Launch Pad, in una scheda o in una nuova finestra

6.2.16.2.1 Per impostare le preferenze di BI Launch Pad per un gruppo di utenti

1. Passare all'area di gestione "Utenti e gruppi" della CMC.
2. Selezionare il gruppo in Elenco gruppi.
3. Fare clic su **Azioni > Preferenze di BI Launch Pad**
Viene visualizzata la finestra di dialogo "Preferenze di BI Launch Pad".
4. Deselezionare **Nessuna preferenza definita**.
5. Per impostare la visualizzazione iniziale di un utente:
 - Per visualizzare la scheda iniziale al primo accesso dell'utente, fare clic su **Scheda iniziale** e scegliere una delle opzioni seguenti:

Opzione	Descrizione
Scheda iniziale predefinita	Visualizza la scheda iniziale predefinita della piattaforma BI.
Seleziona scheda iniziale	<p>Visualizza un sito Web specifico come scheda iniziale.</p> <p>Fare clic su Sfoglia scheda iniziale. Nella finestra "Selezionare una scheda iniziale personalizzata" selezionare un oggetto repository e fare clic su Apri.</p> <p>Nota: è possibile selezionare solo un oggetto già aggiunto al repository.</p>

- Per visualizzare la scheda Documenti al primo accesso dell'utente, fare clic su **Documenti**, quindi specificare il cassetto e il nodo che verranno aperti per impostazione predefinita. È possibile selezionare una delle opzioni seguenti:

Cassetto	Opzioni nodo
Documenti	<p>Scegliere una delle opzioni seguenti da visualizzare nella scheda Documenti:</p> <ul style="list-style-type: none"> • Preferiti • Categorie personali • Posta in arrivo
Cartelle	<p>Scegliere una delle opzioni seguenti:</p> <ul style="list-style-type: none"> • Cartelle pubbliche: visualizza le cartelle pubbliche nella scheda Documenti • Seleziona cartella pubblica <p>Fare clic su Sfoglia cartella per selezionare una cartella pubblica specifica da visualizzare nella scheda Documenti.</p>
Categorie	<p>Scegliere una delle opzioni seguenti:</p> <ul style="list-style-type: none"> • Categorie aziendali: visualizza le categorie aziendali nella scheda Documenti • Seleziona categoria aziendale <p>Fare clic su Sfoglia cartella per selezionare una categoria aziendale specifica da visualizzare nella scheda Documenti.</p>

Se, ad esempio, si desidera che il cassetto **Documenti** venga aperto nella Posta in arrivo BI dell'utente al suo primo accesso, fare clic su **Documenti** e quindi su **Posta in arrivo**.

6. In "Scegliere le colonne da visualizzare nella scheda Documenti" selezionare le informazioni riepilogative da visualizzare per ogni oggetto nel pannello Elenco dell'utente:

- **Tipo**

- **Ultima esecuzione**
- **Istanze**
- **Descrizione**
- **Creato da**
- **Creato il**
- **Posizione (categorie)**
- **Ricevuto il (Posta in arrivo)**
- **Da (Posta in arrivo)**

7. In "Imposta posizione di visualizzazione documento" scegliere la modalità di visualizzazione desiderata per i documenti.

Gli utenti possono aprire i documenti per la visualizzazione in nuove schede all'interno di BI Launch Pad o in nuove finestre del browser Web.

8. Immettere un numero nel campo **Impostare il numero massimo di elementi per pagina** per specificare il numero massimo di oggetti che si desidera mostrare in ogni pagina quando si visualizzano elenchi di oggetti.

9. Fare clic su **Salva e chiudi**.

Le preferenze specificate verranno utilizzate come preferenze predefinite per gli utenti del gruppo selezionato al passaggio 2. Gli utenti potranno tuttavia creare le proprie preferenze per BI Launch Pad, se dispongono del diritto per l'impostazione delle preferenze. Se non si desidera che gli utenti modifichino le preferenze, non concedere loro il diritto per la relativa impostazione.

6.3 Gestione degli alias

Se un utente dispone di più account nella piattaforma BI, è possibile collegarli utilizzando la funzione di assegnazione di alias. Questa opzione è utile quando un utente dispone di un account di terze parti mappato su Enterprise e di un account Enterprise.

Tramite l'assegnazione di un alias l'utente può connettersi utilizzando un nome utente e una password di terze parti, oppure un nome utente e una password Enterprise. In questo modo un alias consente a un utente di accedere tramite più di un tipo di autenticazione.

Nella console CMC le informazioni relative agli alias vengono visualizzate nella parte inferiore della finestra di dialogo "Proprietà" di un utente. Un utente può avere qualsiasi combinazione di alias Enterprise, LDAP o Windows AD.

6.3.1 Per creare un utente e aggiungere un alias di terze parti

Quando si crea un utente e si seleziona un tipo di autenticazione diverso da Enterprise, il sistema crea il nuovo utente nella piattaforma BI e genera un alias di terze parti per l'utente.

Nota:

affinché il sistema crei l'alias di terze parti è necessario che vengano soddisfatti i seguenti criteri:

- Lo strumento di autenticazione deve essere attivato nella CMC.
- Il formato del nome account deve corrispondere al formato richiesto per il tipo di autenticazione.
- L'account utente deve esistere nello strumento di autenticazione di terze parti e deve appartenere a un gruppo già mappato alla piattaforma BI.

1. Passare all'area di gestione "Utenti e gruppi" della CMC.
2. Scegliere **Gestisci > Nuovo > Nuovo utente**.
Viene visualizzata la finestra di dialogo "Nuovo utente".
3. Selezionare il tipo di autenticazione per l'utente, ad esempio Windows AD.
4. Digitare il nome account di terze parti per l'utente, ad esempio bsmith.
5. Selezionare il tipo di connessione per l'utente.
6. Scegliere **Crea e chiudi**.

L'utente viene aggiunto alla piattaforma BI e riceve un alias per il tipo di autenticazione selezionato, ad esempio secWindowsAD:ENTERPRISE:bsmith. Se necessario, è possibile assegnare e riassegnare gli alias agli utenti.

6.3.2 Per creare un nuovo alias per un utente esistente

È possibile creare alias per gli utenti della piattaforma BI esistenti. Questo può essere un alias Enterprise, oppure un alias per uno strumento di autenticazione di terze parti.

Nota:

affinché il sistema crei l'alias di terze parti è necessario che vengano soddisfatti i seguenti criteri:

- Lo strumento di autenticazione deve essere attivato nella CMC.
- Il formato del nome account deve corrispondere al formato richiesto per il tipo di autenticazione.
- L'account utente deve esistere nello strumento di autenticazione di terze parti e deve appartenere a un gruppo mappato alla piattaforma BI.

1. Passare all'area di gestione "Utenti o Gruppi" della console CMC.
2. Selezionare l'utente a cui si desidera aggiungere un alias.
3. Fare clic su **Gestisci > Proprietà**.
Viene visualizzata la finestra di dialogo "Proprietà".
4. Fare clic su **Nuovo alias**.
5. Selezionare il tipo di autenticazione.
6. Immettere il nome account per l'utente.
7. Fare clic su **Aggiorna**.

Viene creato un alias per l'utente. Quando si visualizza l'utente nella CMC, vengono mostrati almeno due alias: uno è quello assegnato all'utente in precedenza, l'altro è quello appena creato.

8. Fare clic su **Salva e chiudi** per uscire dalla finestra di dialogo "Proprietà".

6.3.3 Per assegnare un alias da un altro utente

L'assegnazione di un alias a un utente è il trasferimento di un alias di terze parti da un utente a quello correntemente visualizzato. Non è possibile assegnare o riassegnare gli alias Enterprise.

Nota:

se un utente dispone di un solo alias, ma questo viene assegnato a un altro utente, il sistema elimina l'account utente e la cartella Preferiti, le categorie personali e la casella di posta in arrivo associati a tale account.

1. Passare all'area di gestione "Utenti o Gruppi" della console CMC.
2. Selezionare l'utente a cui si desidera assegnare un alias.
3. Fare clic su **Gestisci > Proprietà**.
Viene visualizzata la finestra di dialogo "Proprietà".
4. Fare clic su **Assegna alias**.
5. Immettere l'account utente che presenta l'alias che si desidera assegnare e fare clic su **Trova**.
6. Spostare l'alias che si desidera assegnare dall'elenco **Alias disponibili** all'elenco **Alias da aggiungere a nomeutente**.

Dove *nomeutente* rappresenta il nome dell'utente a cui si assegna un alias.

Suggerimento:

Per selezionare più alias, utilizzare la combinazione **MAIUSC + clic** o **CTRL + clic**.

7. Scegliere **OK**.

6.3.4 Eliminazione di un alias

Quando si elimina un alias, esso viene rimosso dal sistema. Se un utente dispone di un solo alias, ma questo viene eliminato, il sistema elimina automaticamente l'account utente, la cartella Preferiti, le categorie personali e la casella di posta in arrivo associati a tale account.

Nota:

l'eliminazione di un alias dell'utente non impedisce necessariamente all'utente di accedere di nuovo alla piattaforma BI. Se l'account utente esiste ancora nel sistema di terze parti e appartiene a un gruppo mappato alla piattaforma BI, quest'ultima consente all'utente di effettuare la connessione. Il sistema crea un nuovo utente o assegna l'alias a un utente esistente a seconda dell'opzione di aggiornamento selezionata per lo strumento di autenticazione nell'area di gestione "Autenticazione" della console CMC.

1. Passare all'area di gestione "Utenti o Gruppi" della console CMC.
2. Selezionare l'utente di cui si desidera eliminare l'alias.
3. Fare clic su **Gestisci > Proprietà**.
Viene visualizzata la finestra di dialogo "Proprietà".
4. Fare clic sul pulsante **Elimina alias** accanto all'alias da eliminare.
5. Se viene richiesta una conferma, fare clic su **OK**.
L'alias viene eliminato.
6. Fare clic su **Salva e chiudi** per uscire dalla finestra di dialogo "Proprietà".

6.3.5 Per disattivare un alias

È possibile impedire a un utente di accedere alla piattaforma BI utilizzando un particolare metodo di autenticazione che prevede la disattivazione dell'alias utente ad esso associato. Per evitare che un utente possa accedere alla piattaforma BI, disattivare tutti gli alias corrispondenti.

Nota:

l'eliminazione di un utente dal sistema non impedisce necessariamente all'utente di accedere di nuovo alla piattaforma BI. Se l'account utente esiste ancora nel sistema di terze parti e se appartiene a un gruppo mappato alla piattaforma BI, il sistema consentirà comunque all'utente di effettuare l'accesso. Affinché un utente non possa più utilizzare uno degli alias che gli sono stati assegnati per accedere alla piattaforma BI, è opportuno disattivarlo.

1. Passare all'area di gestione "Utenti o Gruppi" della console CMC.
2. Selezionare l'utente di cui si desidera disattivare l'alias.
3. Fare clic su **Gestisci > Proprietà**.
Viene visualizzata la finestra di dialogo "Proprietà".
4. Deselezionare la casella di controllo **Attivato** per l'alias che si desidera disattivare.
Ripetere questo passaggio per tutti gli alias che si desidera disattivare.
5. Fare clic su **Salva e chiudi**.
L'utente non può più accedere utilizzando il tipo di autenticazione appena disattivato.

Argomenti correlati

- [Eliminazione di un alias](#)

Impostazione dei diritti

7.1 Funzionamento dei diritti nella piattaforma BI

I diritti costituiscono le unità di base per il controllo dell'accesso degli utenti a oggetti, utenti, applicazioni, server e altre funzionalità nella piattaforma BI. I diritti svolgono un ruolo importante nella protezione del sistema mediante la definizione delle singole azioni che gli utenti possono eseguire sugli oggetti. Oltre a consentire il controllo dell'accesso ai contenuti della piattaforma BI, i diritti consentono di delegare la gestione di utenti e gruppi a diversi reparti e di garantire al personale IT l'accesso amministrativo a server e gruppi di server.

È importante notare che i diritti vengono impostati su oggetti quali report e cartelle anziché sui "principali" (utenti e gruppi) che effettuano l'accesso. Ad esempio, per fornire a un gestore l'accesso a una particolare cartella, nell'area "Cartelle" aggiungere tale gestore all'"elenco di controllo degli accessi" (elenco dei principali che possono accedere a un oggetto) per la cartella. Non è possibile fornire al gestore l'accesso configurando le impostazioni dei diritti del gestore nell'area "Utenti e gruppi". Le impostazioni dei diritti per il gestore nell'area "Utenti e gruppi" vengono utilizzate per concedere ad altri principali (ad esempio amministratori delegati) l'accesso al gestore come a un oggetto nel sistema. In questo modo gli stessi principali sono oggetti per altri che dispongono di maggiori diritti di gestione.

Ciascun diritto su un oggetto può essere concesso, negato o non specificato. Il modello di protezione della piattaforma BI è progettato in modo tale che, se un diritto viene lasciato non specificato, viene negato. Inoltre, se le impostazioni hanno come risultato la concessione e la negazione di un diritto a un utente o un gruppo, il diritto viene negato. Questa progettazione "basata sul rifiuto" consente di garantire che gli utenti o i gruppi non acquisiscano automaticamente diritti non concessi in modo esplicito.

Esiste un'importante eccezione a questa regola. Se un diritto viene impostato esplicitamente su un oggetto secondario in contraddizione con i diritti ereditati dall'oggetto principale, il diritto impostato sull'oggetto secondario ha la priorità sui diritti ereditati. Questa eccezione si applica agli utenti che sono anche membri di gruppi. Se a un utente viene esplicitamente concesso un diritto negato al gruppo di tale utente, il diritto impostato sull'utente ha la priorità sui diritti ereditati.

Argomenti correlati

- [Priorità di diritti](#)

7.1.1 Livelli di accesso

I “livelli di accesso” sono gruppi di diritti che gli utenti utilizzano con frequenza. Consentono agli amministratori di impostare i livelli di protezione comuni in modo rapido e uniforme, evitando di impostare i singoli diritti uno ad uno.

La piattaforma BI prevede vari livelli di accesso predefiniti. Questi livelli di accesso predefiniti si basano su un modello di diritti crescenti, a partire da **Visualizza** fino a **Controllo completo**. Ogni livello di accesso accresce i diritti concessi nel livello precedente.

È tuttavia possibile creare livelli di accesso personalizzato e ciò consente di ridurre notevolmente i costi amministrativi e di manutenzione associati alla protezione. Considerare una situazione in cui un amministratore debba gestire due gruppi, responsabili vendite e dipendenti vendite. Entrambi i gruppi devono accedere a cinque report nel sistema della piattaforma BI, ma i responsabili vendite richiedono più diritti dei dipendenti vendite. I livelli di accesso predefiniti non soddisfano le esigenze dei due gruppi. Anziché aggiungere gruppi a ogni report come principali e modificarne i diritti in cinque posizioni diverse, l'amministratore può creare due nuovi livelli di accesso Responsabili vendite e Dipendenti vendite. L'amministratore, quindi, aggiunge entrambi i gruppi come principali ai report e assegna loro i rispettivi livelli di accesso. Quando è necessario modificare i diritti, l'amministratore può accedere e modificare i livelli di accesso. Poiché i livelli di accesso si applicano a entrambi i gruppi per tutti e cinque i report, i diritti di questi gruppi sui report vengono aggiornati rapidamente.

Argomenti correlati

- [Utilizzo di livelli di accesso](#)



7.1.2 Impostazioni dei diritti avanzati



Per fornire il controllo completo sulla protezione degli oggetti, la console CMC consente di impostare “diritti avanzati”. Questi diritti avanzati forniscono maggiore flessibilità poiché consentono di definire la protezione per gli oggetti a un livello granulare.

Utilizzare diritti avanzati, ad esempio, se è necessario personalizzare i diritti di un principale su un particolare oggetto o insieme di oggetti. Ancora più importante, i diritti avanzati possono essere utilizzati per negare in modo esplicito a utenti e gruppi eventuali diritti che non sarà possibile modificare quando, in futuro, si apporteranno modifiche all'appartenenza ai gruppi o ai livelli di protezione delle cartelle.

Nella tabella seguente vengono riepilogate le opzioni disponibili quando si impostano diritti avanzati.

Tabella 7 - 1: Opzioni diritti

Icona	Opzione diritti	Descrizione
	Concesso	Il diritto è concesso a un principale.
	Negato	Il diritto è negato a un principale.

Icona	Opzione diritti	Descrizione
	Non specificato	Il diritto non è specificato per un principale. Per impostazione predefinita, i diritti impostati su Non specificato sono negati.
	Applica a oggetto	Il diritto è applicato all'oggetto. Questa opzione diventa disponibile quando si fa clic su Concesso o Negato .
	Applica a oggetto secondario	Il diritto è applicato agli oggetti secondari. Questa opzione diventa disponibile quando si fa clic su Concesso o Negato .

Argomenti correlati

- [Diritti specifici del tipo](#)

7.1.3 Ereditarietà

I diritti su un oggetto vengono impostati per un principale in modo tale da controllare l'accesso all'oggetto. Tuttavia, è poco pratico impostare il valore esplicito di ogni diritto possibile su ogni oggetto per ogni principale. Si consideri un sistema con 100 diritti, 1.000 utenti e 10.000 oggetti: per impostare esplicitamente i diritti su ciascun oggetto il CMS deve archiviare miliardi di diritti in memoria e, più importante, è necessario che un amministratore imposti ciascun diritto manualmente.

I criteri di ereditarietà risolvono questi problemi. Grazie all'ereditarietà, i diritti di cui gli utenti dispongono per gli oggetti del sistema provengono da una combinazione delle singole appartenenze a gruppi e sottogruppi diversi e da oggetti che hanno ereditato diritti da cartelle principali e sottocartelle. Gli utenti possono ereditare diritti in quanto membri di un gruppo, i sottogruppi ereditano diritti dai gruppi principali, infine utenti e gruppi possono ereditare diritti dalle cartelle principali.

Per impostazione predefinita, gli utenti o i gruppi che dispongono dell'accesso a una cartella ereditano gli stessi diritti per tutti gli oggetti pubblicati successivamente nella cartella. Di conseguenza, la migliore strategia consiste prima di tutto nell'impostare i diritti appropriati per utenti e gruppi a livello di cartella, quindi pubblicare gli oggetti in quella cartella.

La piattaforma BI riconosce due tipi di ereditarietà: ereditarietà di gruppo ed ereditarietà di cartella.

7.1.3.1 Ereditarietà di gruppo

L'ereditarietà di gruppo consente ai principali di ereditare diritti in virtù dell'appartenenza a un gruppo. L'ereditarietà di gruppo si dimostra particolarmente utile quando si organizzano tutti gli utenti in gruppi che coincidono con le convenzioni di protezione correnti dell'organizzazione.

Nell'"esempio di ereditarietà di gruppo 1", è illustrato il funzionamento dell'ereditarietà di gruppo. Il Gruppo Rosso è un sottogruppo del Gruppo Blu, quindi eredita i diritti del Gruppo Blu. In questo caso, il diritto 1 viene ereditato come concesso e gli altri diritti come non specificati. Ogni membro del Gruppo Rosso eredita questi diritti. Inoltre, eventuali altri diritti impostati per il sottogruppo vengono ereditati dai membri. In questo esempio l'utente verde è un membro del gruppo rosso, quindi eredita il diritto 1 come concesso, i diritti 2, 3, 4 e 6 come non specificati e il diritto 5 come negato.



Figura 7 - 1: Ereditarietà di gruppo - Esempio 1

Se si abilita l'ereditarietà di gruppo per un utente che appartiene a più di un gruppo, quando il sistema verifica le credenziali prende in considerazione i diritti di tutti i gruppi principali. All'utente sono negati tutti i diritti negati in modo esplicito a un gruppo principale, oltre ai diritti definiti come non specificati; in questo modo, all'utente sono concessi solo i diritti concessi in uno o più gruppi (in modo esplicito o tramite i livelli di accesso) e mai negati in modo esplicito.

Nell'"esempio di ereditarietà di gruppo 2", l'utente verde è membro di due gruppi non correlati. Dal gruppo blu eredita i diritti 1 e 5 come concessi e il resto come non specificati, tuttavia, poiché l'utente verde appartiene anche al gruppo rosso e tale gruppo ha negato in modo esplicito il diritto 5, l'ereditarietà dal gruppo blu del diritto 5 per l'utente verde viene ignorata.

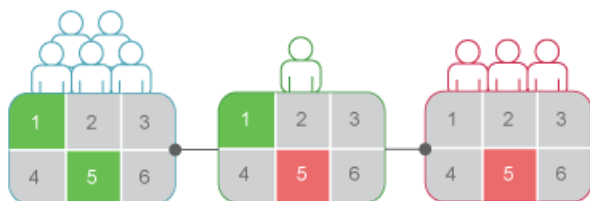


Figura 7 - 2: Ereditarietà di gruppo - Esempio 2

Argomenti correlati

- [Priorità di diritti](#)

7.1.3.2 Ereditarietà di cartella

L'ereditarietà di cartella consente ai principali di ereditare i diritti loro concessi su una cartella principale dell'oggetto. Tale schema di ereditarietà si rivela particolarmente efficace quando si organizza il contenuto della piattaforma BI in una gerarchia di cartelle che riflette le convenzioni di protezione correnti dell'organizzazione. Si supponga, ad esempio, di creare una cartella di nome Report vendite e di fornire al gruppo Vendite l'accesso **Visualizza su richiesta** per la cartella. Per impostazione predefinita, gli utenti che dispongono di diritti sulla cartella Report Vendite ereditano gli stessi diritti per i report pubblicati successivamente in questa cartella. Di conseguenza, il gruppo Vendite disporrà dell'accesso **Visualizza su richiesta** a tutti i report e sarà sufficiente impostare i diritti dell'oggetto una sola volta a livello di cartella.

In "Esempio di ereditarietà di cartella", sono stati impostati diritti su una cartella per il gruppo rosso. I diritti 1 e 5 sono stati concessi, mentre gli altri sono rimasti non specificati. Con l'ereditarietà di cartella abilitata, i membri del Gruppo Rosso dispongono a livello di oggetto di diritti identici a quelli disponibili a livello di cartella. I diritti 1 e 5 vengono ereditati come concessi e tutti gli altri rimangono non specificati.

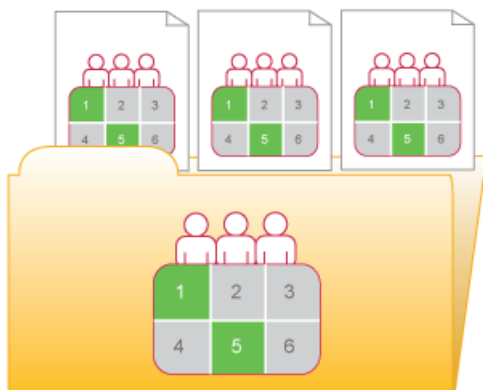


Figura 7 - 3: Esempio di ereditarietà di cartella

Argomenti correlati

- [Priorità di diritti](#)

7.1.3.3 Priorità di diritti

Secondo lo schema di “priorità dei diritti”, i diritti impostati sugli oggetti secondari hanno la priorità sui diritti impostati sugli oggetti principali. L'override dei diritti si applica nelle seguenti circostanze:

- In generale, i diritti impostati sugli oggetti secondari hanno la priorità sui diritti corrispondenti impostati sugli oggetti principali.
- In generale, i diritti impostati sui gruppi secondari o sui membri di gruppi hanno la priorità sui diritti corrispondenti impostati sui gruppi.

Non è necessario disabilitare l'eredità per impostare diritti personalizzati su un oggetto. L'oggetto secondario eredita le impostazioni dei diritti dell'oggetto principale ad eccezione dei diritti esplicitamente impostati sull'oggetto secondario. Inoltre, qualsiasi modifica apportata alle impostazioni dei diritti sull'oggetto principale viene applicata all'oggetto secondario

L'esempio relativo “allo schema di override dei diritti 1” illustra il meccanismo di override dei diritti per gli oggetti principali e secondari. All'utente blu viene negato il diritto di modifica del contenuto di una cartella; l'impostazione dei diritti è ereditata dalla sottocartella. Tuttavia, un amministratore concede all'utente blu i diritti di **modifica** di un documento nella sottocartella. Il diritto di **modifica** che l'utente blu riceve per il documento ha la priorità sui diritti ereditati derivanti dalla cartella e dalla sottocartella.

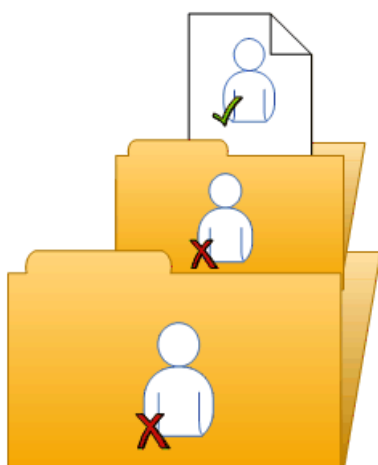


Figura 7 - 4: Esempio di override dei diritti 1

L'esempio relativo “allo schema di override dei diritti 2” illustra il meccanismo di override dei diritti per membri e gruppi. Al gruppo blu è negato il diritto di modifica di una cartella e il sottogruppo blu eredita questa impostazione dei diritti. Tuttavia, un amministratore concede all'utente blu, membro del gruppo blu e del sottogruppo blu, diritti di **modifica** sulla cartella. I diritti di **modifica** che l'utente blu riceve sulla cartella hanno la priorità sui diritti ereditati provenienti dal gruppo blu e dal sottogruppo blu.

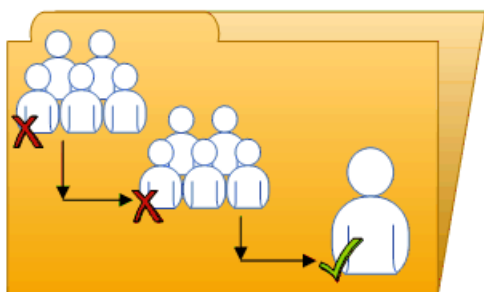


Figura 7 - 5: Esempio di override dei diritti 2

Lo “schema di priorità complessa dei diritti” illustra una situazione in cui gli effetti della priorità di diritti sono meno ovvii. L'utente viola è membro dei sottogruppi 1A e 2A, contenuti rispettivamente nei gruppi 1 e 2. I gruppi 1 e 2 hanno entrambi diritti di modifica sulla cartella. 1A eredita i diritti di **modifica** dal gruppo 1, ma un amministratore nega i diritti di **modifica** a 2A. Le impostazioni dei diritti su 2A sono prioritari rispetto alle impostazioni dei diritti del gruppo 2. L'utente viola, pertanto, eredita impostazioni di diritti contraddittori da 1A e 2A. 1A e 2A non hanno relazioni principale-secondario, pertanto l'override dei diritti non viene applicato; ciò significa che le impostazioni dei diritti di un sottogruppo non hanno la priorità su quelle di un altro poiché sono di pari stato. In conclusione, all'utente viola vengono negati i diritti di **modifica** a causa del modello di diritti “basati sul rifiuto” nella piattaforma BI.

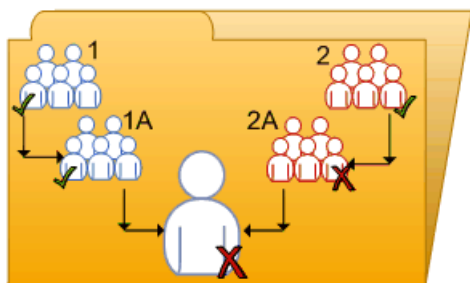


Figura 7 - 6: Priorità complessa dei diritti

L'override dei diritti consente di apportare variazioni minime alle impostazioni dei diritti di un oggetto secondario senza ignorare tutte le impostazioni dei diritti ereditate. Si consideri una situazione in cui un responsabile delle vendite deve visualizzare report riservati nella cartella Riservato. Il responsabile delle vendite fa parte del gruppo Vendite e come tale non ha accesso alla cartella e ai suoi contenuti. L'amministratore concede al responsabile i diritti di **visualizzazione** sulla cartella Riservato e continua a negare l'accesso al resto del gruppo Vendite. In questo caso, i diritti di **visualizzazione** concessi al responsabile delle vendite hanno la priorità sull'accesso negato che il responsabile eredita per il fatto di appartenere al gruppo Vendite.

7.1.3.4 Ambito dei diritti

Con “ambito dei diritti” si intende la possibilità di controllare l'estensione dell'eredità dei diritti. Per definire l'ambito di un diritto, decidere se il diritto si applica all'oggetto, all'oggetto secondario o a entrambi. Per impostazione predefinita, l'ambito di un diritto si estende sia agli oggetti sia agli oggetti secondari.

L'ambito dei diritti può essere utilizzato per proteggere il contenuto personale in percorsi condivisi. Considerare una situazione in cui il reparto finanziario ha condiviso la cartella Richieste di indennizzo che contiene sottocartelle Richieste di indennizzo personali per ogni dipendente. I dipendenti devono poter visualizzare la cartella Richieste di indennizzo e potervi aggiungere oggetti ma devono anche poter proteggere il contenuto delle loro sottocartelle Richieste di indennizzo personali. L'amministratore concede a tutti i dipendenti i diritti di **visualizzazione** e **aggiunta** sulla cartella Richieste di indennizzo e limita l'ambito di questi diritti alla sola cartella Richieste di indennizzo. In questo modo i diritti di **visualizzazione** e **aggiunta** non si applicano agli oggetti secondari nella cartella Richieste di indennizzo. L'amministratore concede quindi ai dipendenti i diritti di **visualizzazione** e **aggiunta** sulle rispettive sottocartelle Richieste di indennizzo personali.

L'ambito dei diritti può anche limitare i diritti effettivi di cui dispone un amministratore con delega. È possibile ad esempio che un amministratore con delega disponga dei **diritti di modifica in modo sicuro** e dei **diritti di modifica** per una cartella, ma l'ambito di questi diritti è limitato alla cartella e non è applicabile ai relativi oggetti secondari. L'amministratore con delega non può concedere questi diritti a un altro utente per uno degli oggetti secondari della cartella.

7.1.4 Diritti specifici del tipo

I “diritti specifici del tipo” riguardano unicamente tipi di oggetto specifici, ad esempio report Crystal, cartelle o livelli di accesso. I diritti specifici del tipo sono:

- Diritti generali per ogni tipo di oggetto

Questi diritti sono identici ai diritti globali generali (ad esempio diritto di aggiunta, eliminazione o modifica di un oggetto), ma è possibile impostarli su tipi di oggetto specifici in modo che abbiano la priorità sulle impostazioni dei diritti globali.

- Diritti specifici per il tipo di oggetto

Questi diritti sono disponibili solo per tipi di oggetto specifici. Ad esempio, il diritto di esportazione dei dati di un report è presente per i report Crystal, ma non per i documenti Word.

Il diagramma “Esempio di diritti specifici del tipo” illustra il funzionamento dei diritti specifici del tipo. Il diritto 3 rappresenta il diritto di modifica di un oggetto. Al gruppo blu vengono negati i diritti di **modifica** per la cartella di livello superiore, mentre vengono concessi i diritti di **modifica** per i report Crystal nella cartella e relativa sottocartella. Questi diritti di **modifica** sono specifici per i report Crystal e sostituiscono le impostazioni dei diritti a livello globale generale. Di conseguenza, i membri del gruppo blu dispongono dei diritti di **modifica** per i report Crystal ma non per il file XLF nella sottocartella.

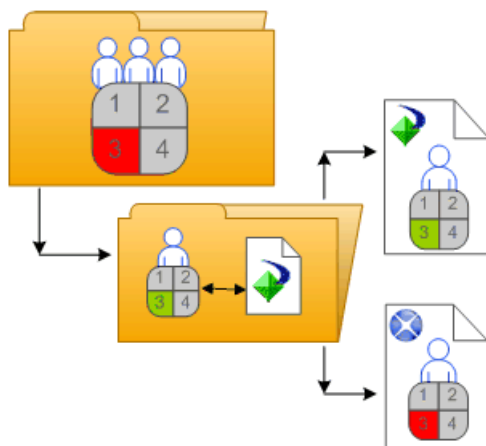


Figura 7 - 7: Esempio di diritti specifici del tipo

I diritti specifici del tipo sono utili poiché consentono di limitare i diritti dei principali in base al tipo di oggetto. Si consideri una situazione in cui un amministratore desidera che i dipendenti siano in grado di aggiungere oggetti a una cartella, ma non creare sottocartelle. L'amministratore concede i diritti di **aggiunta** al livello globale generale per la cartella, quindi nega i diritti di **aggiunta** per il tipo di oggetto cartella.

I diritti si suddividono nei seguenti insiemi in base ai tipi di oggetto a cui si applicano:

- **Generale**

Questi diritti riguardano tutti gli oggetti.

- **Contenuto**

Questi diritti sono suddivisi in base a determinati tipi di oggetto di contenuto. Esempi di tipi di oggetto contenuto sono i report Crystal e i file PDF di Adobe Acrobat.

- **Applicazione**

Questi diritti sono suddivisi in base all'applicazione della piattaforma BI interessata. Gli esempi di applicazione includono la console CMC e BI Launch Pad.

- **Sistema**

Questi diritti sono suddivisi in base al componente di sistema di base interessato. Tra gli esempi di componenti di sistema di base sono inclusi Calendari, Eventi e Utenti e Gruppi.

I diritti specifici del tipo si trovano negli insiemi **Contenuto**, **Applicazione** e **Sistema**. In ogni insieme, sono ulteriormente suddivisi in categorie basate sul tipo di oggetto.

7.1.5 Determinazione dei diritti effettivi

È opportuno considerare i seguenti aspetti quando si impostano diritti su un oggetto:

- Ciascun livello di accesso concede alcuni diritti, ne nega altri e non specifica gli altri diritti. Quando a un utente vengono concessi numerosi livelli di accesso, per impostazione predefinita il sistema aggrega i diritti effettivi e nega tutti i diritti non specificati.
- Quando vengono assegnati più livelli di accesso a un principale su un oggetto, il principale dispone della combinazione dei diritti di ciascun livello di accesso. All'utente in "Livelli di accesso multipli" vengono assegnati due livelli di accesso. Un livello di accesso concede all'utente i diritti 3 e 4, mentre l'altro livello di accesso concede solo il diritto 3. I diritti effettivi per l'utente sono 3 e 4.

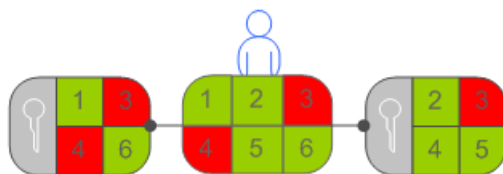


Figura 7 - 8: Livelli di accesso multipli

- I diritti avanzati possono essere combinati con livelli di accesso per personalizzare le impostazioni dei diritti per un principale su un oggetto. Ad esempio, se un diritto avanzato e un livello di accesso vengono entrambi assegnati in modo esplicito a un principale su un oggetto e il diritto avanzato è in contrasto con un diritto nel livello di accesso, il diritto avanzato eseguirà l'override del diritto nel livello di accesso.

I diritti avanzati possono avere la precedenza sulle relative controparti identiche nei livelli di accesso solo quando sono impostati per lo stesso oggetto e per lo stesso principale. Ad esempio, un diritto di aggiunta avanzato impostato al livello globale generale può avere la precedenza sul diritto di aggiunta generale in un livello di accesso; non può avere la precedenza su un diritto di aggiunta specifico di un tipo in un livello di accesso.

Tuttavia, i diritti avanzati non eseguono sempre l'override dei livelli di accesso. Ad esempio, a un principale viene negato un diritto **Modifica** su un oggetto principale. Sull'oggetto secondario, al principale viene assegnato un livello di accesso che concede il diritto **Modifica**. Per concludere, il principale dispone di diritti **Modifica** sull'oggetto secondario poiché i diritti impostati sull'oggetto secondario eseguono l'override dei diritti impostati sull'oggetto principale.

- L'override dei diritti rende possibile l'override dei diritti impostati su un oggetto secondario sui diritti ereditati dall'oggetto principale.

7.2 Gestione delle impostazioni di protezione per gli oggetti nella CMC

È possibile gestire le impostazioni di protezione per la maggior parte degli oggetti nella CMC con le opzioni di protezione del menu **Gestisci**. Queste opzioni consentono di assegnare principali all'elenco di controllo dell'accesso per un oggetto, visualizzare i diritti di un principale e modificare i diritti di un principale per un oggetto.

I dettagli specifici della gestione della protezione variano in base alle esigenze di protezione e al tipo di oggetto per cui si impostano i diritti. In generale, tuttavia, i workflow per i seguenti task sono molto simili:

- Visualizzazione dei diritti di un principale su un oggetto.
- Assegnazione dei principali all'elenco di controllo degli accessi per un oggetto e specifica dei diritti di tali principali.
- Impostazione dei diritti su una cartella di livello superiore nella piattaforma BI.

7.2.1 Per visualizzare i diritti per un principale su un oggetto

In generale, seguire questo workflow per visualizzare i diritti di un principale per un oggetto.

1. Selezionare l'oggetto per cui si desidera visualizzare le impostazioni di protezione.

2. Fare clic su **Gestisci > Protezione utente**.

Viene visualizzata la finestra di dialogo "Protezione utente" che riporta l'elenco di controllo degli accessi per l'oggetto.

3. Selezionare un principale dall'elenco di controllo degli accessi e fare clic su **Protezione vista**.

L'"Explorer autorizzazioni" avvia e visualizza un elenco dei diritti effettivi del principale sull'oggetto. Inoltre l'"Explorer autorizzazioni" consente di eseguire le seguenti operazioni.

- Spostarsi su un altro principale di cui si desidera visualizzare i diritti.
- Filtrare i diritti visualizzati in base ai seguenti criteri:
 - diritti assegnati
 - diritti concessi
 - diritti non assegnati
 - da livello di accesso
 - tipo di oggetto
 - nome del diritto
- Ordinare l'elenco dei diritti visualizzati in ordine crescente o decrescente in base ai seguenti criteri:
 - insieme
 - tipo
 - nome diritto
 - stato diritto (concesso, negato o non specificato)

È possibile fare clic su uno dei collegamenti nella colonna "Origine" per visualizzare l'origine dei diritti ereditati.

7.2.2 Per assegnare principali a un elenco di controllo di accesso per un oggetto

Un elenco di controllo degli accessi specifica gli utenti a cui sono concessi o negati diritti su un oggetto. In generale, si segue questo workflow per assegnare un principale a un elenco di controllo degli accessi e specificare i diritti di un principale su un oggetto.

1. Selezionare l'oggetto a cui aggiungere un principale.
2. Fare clic su **Gestisci > Protezione utente**.
Viene visualizzata la finestra di dialogo "Protezione utente" che riporta l'elenco di controllo degli accessi.
3. Fare clic su **Aggiungi principali**.
Viene visualizzata la finestra di dialogo "Aggiungi principali".
4. Spostare gli utenti e i gruppi da aggiungere come principali dall'elenco **Utenti/gruppi disponibili** all'elenco **Utenti/gruppi selezionati**.
5. Fare clic su **Aggiungi e assegna protezione**.
6. Selezionare i livelli di accesso che si desidera concedere al principale.
7. Scegliere se attivare o disattivare l'eredità di cartelle o gruppi.

Se necessario, è anche possibile modificare i diritti a livello granulare per ignorare alcuni diritti in un livello di accesso.

Argomenti correlati

- [Per modificare la protezione per un principale su un oggetto](#)

7.2.3 Per modificare la protezione per un principale su un oggetto

In generale, è consigliabile utilizzare i livelli di accesso per assegnare diritti a un principale. È tuttavia possibile ignorare alcuni diritti granulari in un livello di accesso. I diritti avanzati consentono di personalizzare i diritti per un principale in aggiunta ai livelli di accesso di cui il principale già dispone. In generale, seguire questo workflow per assegnare diritti avanzati a un principale su un oggetto.

1. Assegnare il principale all'elenco ACL per l'oggetto.
2. Dopo avere aggiunto il principale, accedere a **Gestisci > Protezione utente** per visualizzare l'elenco ACL per l'oggetto.
3. Selezionare il principale dall'elenco di controllo degli accessi e fare clic su **Assegna protezione**.
Viene visualizzata la finestra di dialogo "Assegna protezione".
4. Fare clic sulla scheda **Avanzate**.
5. Fare clic su **Aggiungi/Rimuovi diritti**.

6. Modificare i diritti per il principale.

Tutti i diritti disponibili vengono riepilogati nell'*appendice dei diritti*.

Argomenti correlati

- [Per assegnare principali a un elenco di controllo di accesso per un oggetto](#)

7.2.4 Impostazione dei diritti su una cartella di livello superiore nella piattaforma BI

In genere, per impostare i diritti su una cartella di livello superiore nella piattaforma BI, si segue la procedura descritta di seguito.

Nota:

Per questa versione, i principali richiedono diritti di **visualizzazione** in una cartella per spostarsi all'interno della cartella e visualizzarne gli oggetti secondari. Ciò significa che i principali richiedono diritti di **visualizzazione** per la cartella di livello superiore per visualizzare gli oggetti nelle cartelle. Per limitare i diritti di **visualizzazione** per un principale, è possibile concedere a un principale i diritti di **visualizzazione** in una cartella specifica e impostare l'ambito dei diritti da applicare unicamente a quella cartella.

1. Passare all'area CMC che contiene la cartella di livello superiore per cui si desidera impostare i diritti.
2. Fare clic su **Gestisci > Protezione di livello superiore > Tutti Oggetti**.
Oggetti rappresenta il contenuto della cartella di livello superiore. Se viene richiesta una conferma, fare clic su **OK**.
Viene visualizzata la finestra di dialogo "Protezione utente" contenente l'elenco di controllo degli accessi per la cartella di livello superiore.
3. Assegnare il principale all'elenco di controllo degli accessi per la cartella di livello superiore.
4. Se necessario, assegnare diritti avanzati al principale.

Argomenti correlati

- [Per assegnare principali a un elenco di controllo di accesso per un oggetto](#)
- [Per modificare la protezione per un principale su un oggetto](#)

7.2.5 Controllo impostazioni di protezione per un principale

In alcuni casi, può essere necessario sapere a quali oggetti un principale può accedere o meno. Per ottenere queste informazioni è possibile utilizzare una query protezione. Le query protezione consentono

di determinare gli oggetti sui quali un principale dispone di diritti e di gestire i diritti degli utenti. Per ogni query protezione, occorre fornire le seguenti informazioni:

- Principale query

Specificare l'utente o il gruppo per cui si desidera eseguire la query. È possibile specificare un principale per ogni gruppo di protezione.

- Autorizzazione query

Specificare i diritti per cui si desidera eseguire la query, lo stato di questi diritti e il tipo di oggetto su cui sono impostati. Ad esempio, è possibile eseguire una query protezione per tutti i report che un principale può aggiornare o per tutti i report che un principale non può esportare.

- Contesto della query

Specificare le aree CMC in cui si desidera effettuare la ricerca tramite la query protezione. Per ogni area, è possibile scegliere se includere oggetti secondari nella query protezione. Una query protezione può avere un massimo di quattro aree.

Quando si esegue una query protezione, i risultati vengono visualizzati nell'area "Risultati query" del riquadro Albero in **Query protezione**. Se si desidera ridefinire una query protezione, è possibile eseguire una seconda query all'interno dei risultati della prima query.

Le query protezione sono utili poiché consentono di visualizzare gli oggetti su cui un principale ha diritti e forniscono le posizioni di tali oggetti per consentire di modificare questi diritti. Si consideri una situazione in cui un dipendente del reparto vendite venga promosso a responsabile vendite. Il responsabile vendite necessita di diritti di **pianificazione** per i report Crystal per i quali in precedenza disponeva solo di diritti di **visualizzazione** e tali report si trovano in cartelle diverse. In questo caso, l'amministratore esegue una query protezione per il diritto del responsabile vendite di visualizzare report Crystal in tutte le cartelle e include oggetti secondari nella query. Dopo l'esecuzione della query protezione, l'amministratore può visualizzare tutti i report Crystal per i quali il responsabile vendite dispone di diritti di **visualizzazione** nell'area "Risultati query". Poiché nel riquadro Dettagli viene visualizzato il percorso di ogni report Crystal, l'amministratore può cercare ciascun report e modificare i diritti del responsabile vendite su di esso.

7.2.5.1 Per eseguire una query protezione

1. Nell'area "Utenti e gruppi", nel riquadro Dettagli, selezionare l'utente o il gruppo per il quale si desidera eseguire una query di protezione.
2. Scegliere **Gestisci > Strumenti > Crea query di protezione**.

Crea query di protezione: Nina

Principale query

Questa query consente di cercare oggetti per il seguente principale:

Nina

Autorizzazione query

Questa query cercherà oggetti in cui il principale dispone di tutte le seguenti autorizzazioni:

☐ Non eseguire la query in base alle autorizzazioni

Raccolta	Tipo	Nome diritto	
Generale	Generale	Aggiungere oggetti alla cartella	<input checked="" type="checkbox"/> <input type="button" value="X"/>
Generale	Generale	Aggiungi oggetti alle cartelle di proprietà dell'utente	<input checked="" type="checkbox"/> <input type="button" value="X"/>

Contesto della query

Questa query cercherà oggetti solo nelle seguenti sezioni della CMC:

☒ Cartelle
 (Tutto) ☒ Oggetto secondario query

☐ Cartelle
 (Tutto) ☐ Oggetto secondario query

Verrà visualizzata la finestra di dialogo "Crea query di protezione".

3. Accertarsi che il principale nell'area **Principale query** sia corretto.

Se si decide di eseguire una query protezione per un principale diverso, è possibile fare clic su **Sfoglia** per scegliere un altro principale. Nella finestra di dialogo "Cerca principale query", espandere **Elenco utenti** o **Elenco gruppi** per cercare il principale oppure per eseguire la ricerca del principale per nome. Al termine, fare clic su **OK** per tornare alla finestra di dialogo "Crea query di protezione".

4. Nell'area "Autorizzazione query" specificare i diritti e lo stato di ogni diritto per il quale si desidera eseguire la query.

- Se si desidera eseguire una query per diritti specifici di cui dispone il principale per gli oggetti, fare clic su **Sfoglia**, impostare lo stato di ogni diritto per cui si desidera eseguire la query di protezione, quindi scegliere **OK**.

Suggerimento:

È possibile eliminare diritti specifici dalla query facendo clic sul pulsante di eliminazione accanto al diritto oppure eliminare tutti i diritti dalla query facendo clic sul pulsante di eliminazione nella riga dell'installazione.

- Se si desidera eseguire una query di protezione generale, selezionare la casella di controllo **Non eseguire la query in base alle autorizzazioni**.

Quando si esegue questa operazione, la piattaforma BI esegue una query di protezione generale per tutti gli oggetti con il principale nei relativi elenchi ACL, indipendentemente dalle autorizzazioni di cui dispone il principale sugli oggetti.

5. Nell'area "Contesto della query", specificare le aree della CMC in cui si desidera eseguire la query.

- Selezionare una casella di controllo accanto a un elenco.
- Nell'elenco, selezionare un'area della CMC in cui si desidera eseguire la query.

Se si desidera eseguire una query in una posizione più specifica all'interno di un'area (ad esempio una cartella specifica in Cartelle), fare clic su **Sfoglia** per aprire la finestra di dialogo "Sfoglia per contesto della query". Nel riquadro dei dettagli selezionare la cartella in cui eseguire la query e fare clic su **OK**. Quando si torna alla finestra di dialogo **Query protezione**, la cartella specificata viene visualizzata nella casella sotto l'elenco.

- c. Selezionare **Oggetto secondario query**.
- d. Ripetere i passaggi precedenti per ciascuna area della CMC in cui si desidera eseguire una query.

Nota:

È possibile eseguire query in un massimo di quattro aree.

6. Fare clic su OK.

La query protezione viene eseguita e viene visualizzata l'area "Risultati query".

- 7. Per visualizzare i risultati della query, espandere Query protezione nel riquadro Albero e fare clic sul risultato di una query.**

Suggerimento:

I risultati della query vengono elencati in base ai nomi dei principali.

I risultati della query vengono visualizzati nel riquadro Dettagli.

L'area "Risultati query" conserva tutti i risultati delle query di protezione di una sessione utente fino alla disconnessione dell'utente. Per eseguire nuovamente la query ma con nuove specifiche, fare clic su **Azioni > Modifica query**. È anche possibile eseguire nuovamente esattamente la stessa query selezionandola e facendo clic su **Azioni > Riesegui query**. Per conservare i risultati delle query di protezione, fare clic su **Azioni > Esporta** per esplorare i risultati delle query di protezione come file CSV.

7.3 Utilizzo di livelli di accesso

I livelli di accesso consentono di eseguire le seguenti operazioni:

- Copiare un livello di accesso esistente, apportare modifiche alla copia, rinominarla e salvarla come un nuovo livello di accesso.
- Creare, rinominare ed eliminare i livelli di accesso.
- Modificare i diritti in un livello di accesso.
- Analizzare la relazione tra livelli di accesso e altri oggetti nel sistema.
- Replicare e gestire i livelli di accesso tra i siti.
- Utilizzare uno dei livelli di accesso predefiniti nella piattaforma BI per impostare in modo rapido e uniforme i diritti per molti principali.

La tabella seguente riassume i diritti contenuti in ogni livello di accesso.

Tabella 7 - 2: Livelli di accesso predefiniti

Livello di accesso	Descrizione	Diritti previsti
Visualizza	Se impostato a livello di cartella, un principale potrà visualizzare la cartella, gli oggetti all'interno della cartella e le istanze generate di ciascun oggetto. Se impostato a livello di oggetto, un principale potrà visualizzare l'oggetto, la relativa cronologia e le istanze generate.	<ul style="list-style-type: none"> • Visualizza oggetti • Visualizzare istanze documento
Pianificazione	Un principale può generare istanze pianificando l'esecuzione di un oggetto in base a un'origine dati specifica o con cadenza regolare. Il principale può visualizzare, eliminare e interrompere la pianificazione delle istanze di cui dispone. Può inoltre eseguire la pianificazione in diversi formati e destinazioni, impostare parametri e informazioni di accesso, selezionare i server per l'elaborazione di lavori, aggiungere contenuti alla cartella e copiare l'oggetto o la cartella.	Diritti del livello di accesso di visualizzazione , oltre a: <ul style="list-style-type: none"> • Pianifica il documento da eseguire • Definisci gruppi di server per elaborare i processi • Copia gli oggetti in un'altra cartella • Pianifica per destinazioni • Stampa i dati del report • Esporta i dati del report • Modifica oggetti posseduti dall'utente • Elimina istanze di proprietà dell'utente • Interrompere e riprendere istanze documento di proprietà dell'utente
Visualizza su richiesta	Un principale può aggiornare i dati su richiesta in base a un'origine dati.	Diritti del livello di accesso di pianificazione , oltre a: <ul style="list-style-type: none"> • Aggiorna i dati del report
Controllo completo	Un principale dispone del controllo amministrativo completo dell'oggetto.	Tutti i diritti disponibili, compresi: <ul style="list-style-type: none"> • Aggiungi oggetti alla cartella • Modifica oggetti • Modificare i diritti che gli utenti hanno sugli oggetti • Elimina oggetti • Elimina istanze

La tabella seguente riepiloga i diritti richiesti per eseguire determinati task sui livelli di accesso.

Task sul livello di accesso	Diritti richiesti
Creare un livello di accesso	<ul style="list-style-type: none"> • Diritto di aggiunta sulla cartella principale dei livelli di accesso
Diritti granulari di visualizzazione in un livello di accesso	<ul style="list-style-type: none"> • Diritto di visualizzazione sul livello di accesso
Assegnazione di un livello di accesso a un principale su un oggetto	<ul style="list-style-type: none"> • Diritto di visualizzazione sul livello di accesso • Il diritto Utilizza il livello di accesso per l'assegnazione della protezione sul livello di accesso • Il diritto Modifica dei diritti sull'oggetto o il diritto Modificare in modo sicuro i diritti degli utenti sugli oggetti sull'oggetto e sul principale <p>Nota: Gli utenti che dispongono del diritto Modificare in modo sicuro i diritti degli utenti sugli oggetti e desiderano assegnare un livello di accesso a un principale devono disporre dello stesso livello di accesso.</p>
Modificare un livello di accesso	<ul style="list-style-type: none"> • Diritti di visualizzazione e modifica sul livello di accesso
Eliminare un livello di accesso	<ul style="list-style-type: none"> • Diritti di visualizzazione ed eliminazione sul livello di accesso
Duplicare un livello di accesso	<ul style="list-style-type: none"> • Diritto di visualizzazione sul livello di accesso • Diritto di copia sul livello di accesso • Diritto di aggiunta sulla cartella principale dei livelli di accesso

7.3.1 Scelta tra i livelli di accesso **Visualizza** e **Visualizza su richiesta**

Quando si creano report sul Web, la decisione circa l'uso di dati dinamici o salvati è una delle più importanti da prendere. Qualsiasi sia la scelta, tuttavia, la piattaforma BI visualizzerà la prima pagina con estrema rapidità, in modo che sia possibile vedere il report mentre il resto dei dati è in fase di elaborazione. In questa sezione viene illustrata la differenza tra due livelli di accesso predefiniti che è possibile utilizzare per questa scelta.

Livello di accesso Visualizza su richiesta

La creazione di report su richiesta garantisce agli utenti accesso in tempo reale ai dati dinamici, direttamente dal server del database. Utilizzare dati dinamici per tenere gli utenti sempre aggiornati sui dati in costante modifica, in modo che possano accedere ad informazioni estremamente precise. Ad esempio, se i responsabili di un grande centro di distribuzione hanno l'esigenza di tenere costantemente

traccia delle merci in magazzino spedite, la creazione di report dinamica è la soluzione ideale per fornire loro le informazioni di cui hanno bisogno.

Prima di fornire dati dinamici per tutti i report, si deve comunque decidere se si desidera o meno che tutti gli utenti accedano al server del database in modo costante. Se i dati non sono in rapida e continua crescita, tutte le richieste al database concernenti i dati in questione non fanno altro che aumentare il traffico di rete e consumare risorse del server. In casi di questo genere, è preferibile pianificare i report su base periodica, in modo che gli utenti possano sempre visualizzare dati recenti (istanze dei report) senza dover accedere al server del database.

Gli utenti richiedono l'accesso **Visualizza su richiesta** per aggiornare i report rispetto al database.

Livello di accesso Visualizza

Per ridurre il traffico di rete e il numero di accessi al server del database è possibile pianificare l'esecuzione dei report a orari specificati. Dopo aver eseguito il report, gli utenti possono visualizzare l'istanza corrispondente in base alle esigenze specifiche, senza effettuare ulteriori accessi al database.

Le istanze dei report sono utili per gestire dati che non vengono continuamente aggiornati. Quando gli utenti passano da un'istanza di report all'altra ed eseguono un'analisi dettagliata per ottenere dettagli su colonne o grafici, non accedono direttamente al server del database, bensì ai dati salvati. Di conseguenza, i report con dati salvati non solo riducono al minimo il trasferimento di dati in rete, ma alleggeriscono anche il carico di lavoro del server del database.

Se il database delle vendite viene ad esempio aggiornato una volta al giorno, è possibile impostare la medesima pianificazione per l'esecuzione del report. I rappresentanti di vendita avranno quindi sempre a disposizione dati sulle vendite aggiornati, ma non dovranno accedere al database ogni volta che aprono un report.

Gli utenti richiedono solo l'accesso **Visualizza** per visualizzare le istanze di report.

7.3.2 Per copiare un livello di accesso esistente

Questa procedura è consigliata per creare un livello di accesso leggermente diverso da uno dei livelli di accesso esistenti.

1. Passare all'area "Livelli di accesso".
2. Nel pannello Dettagli, selezionare un livello di accesso.

Suggerimento:

Selezionare un livello di accesso che contenga diritti analoghi a quelli desiderati per il nuovo livello di accesso.

3. Scegliere **Organizza > Copia**.

Nel pannello Dettagli viene visualizzata una copia del livello di accesso selezionato.

7.3.3 Per creare un nuovo livello di accesso

Questa procedura è consigliata per creare un livello di accesso notevolmente diverso da uno dei livelli di accesso esistenti.

1. Passare all'area "Livelli di accesso".
2. Scegliere **Gestisci > Nuovo > Crea livello di accesso**.
Viene visualizzata la finestra di dialogo "Crea un nuovo livello di accesso".
3. Immettere un titolo e una descrizione per il nuovo livello di accesso, quindi fare clic su **OK**.
Si torna all'area "Livelli di accesso" e un nuovo livello di accesso viene visualizzato nel pannello **Dettagli**.

7.3.4 Per rinominare un livello di accesso

1. Nell'area "Livelli di accesso", nel pannello **Dettagli**, selezionare il livello di accesso che si desidera rinominare.
2. Fare clic su **Gestisci > Proprietà**.
Viene visualizzata la finestra di dialogo "Proprietà".
3. Nel campo **Titolo**, immettere un nuovo nome per il livello di accesso, quindi fare clic su **Salva e chiudi**.
Si torna all'area "Livelli di accesso".

7.3.5 Per eliminare un livello di accesso

1. Nell'area "Livelli di accesso", nel pannello **Dettagli**, selezionare il livello di accesso che si desidera eliminare.
2. Scegliere **Gestisci > Elimina livello di accesso**.

Nota:

Non è possibile eliminare i livelli di accesso predefiniti.

Viene visualizzata una finestra di dialogo con le informazioni sugli oggetti su cui questo livello di accesso ha effetto. Se non si desidera eliminare il livello di accesso, fare clic su **Annulla** per uscire dalla finestra di dialogo.

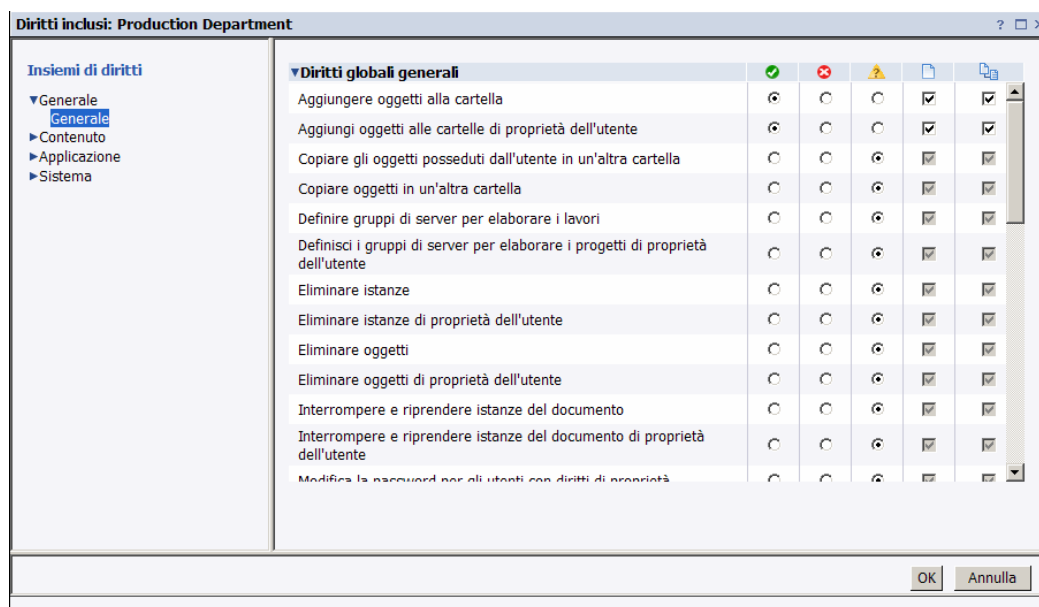
3. Fare clic su **Elimina**.

Il livello di accesso viene eliminato e si torna all'area "Livelli di accesso".

7.3.6 Per modificare i diritti in un livello di accesso

Per impostare diritti per un livello di accesso, è necessario innanzitutto impostare diritti globali generali che si applicano a tutti gli oggetti indipendentemente dal tipo, quindi specificare quando si desidera sovrascrivere le impostazioni generali in base al tipo di oggetto specifico.

1. Nell'area **Livelli di accesso**, nel pannello Dettagli, selezionare il livello di accesso per cui si desidera modificare i diritti.
2. Scegliere **Azioni > Diritti inclusi**.
Viene visualizzata la finestra di dialogo **Diritti inclusi** che visualizza un elenco dei diritti effettivi.
3. Fare clic su **Aggiungi/Rimuovi diritti**.



La finestra di dialogo **Diritti inclusi** visualizza gli insiemi di diritti per il livello di accesso nell'elenco di spostamento. La sezione **Diritti globali generali** è espansa per impostazione predefinita.

4. Impostare i diritti globali generali.
Ogni diritto può presentare lo stato **Concesso**, **Negato** o **Non specificato**. È possibile scegliere se applicare tale diritto solo all'oggetto, solo agli oggetti secondari o a entrambi.
5. Per impostare diritti di tipo specifico per il livello di accesso, nell'elenco di spostamento, fare clic sull'insieme dei diritti, quindi fare clic sul sottoinsieme relativo al tipo di oggetto per cui si desidera impostare i diritti.
6. Al termine, fare clic su **OK**.
Si torna all'elenco dei diritti effettivi.

Argomenti correlati

- [Gestione delle impostazioni di protezione per gli oggetti nella CMC](#)
- [Diritti specifici del tipo](#)

7.3.7 Analisi e relazione tra livelli di accesso e oggetti

Prima di modificare o eliminare un livello di accesso, è importante verificare che qualsiasi modifica apportata a tale livello non abbia un impatto negativo sugli oggetti in CMC. A tal fine è possibile eseguire una query di relazione sul livello di accesso.

Le query di relazione sono utili per la gestione dei diritti poiché consentono di visualizzare tutti gli oggetti interessati da un livello di accesso da un'unica posizione. Si consideri una situazione in cui una società ristrutturata la propria organizzazione e unisca due reparti, Reparto A e Reparto B, nel Reparto C. L'amministratore decide di eliminare i livelli di accesso per il Reparto A e per il Reparto B poiché tali reparti non esistono più. L'amministratore esegue query di relazione per entrambi i livelli di accesso prima di eliminarli. Nell'area "Risultati query", l'amministratore può visualizzare gli oggetti che saranno interessati dall'eliminazione dei livelli di accesso eseguita dall'amministratore. Nel pannello Dettagli, inoltre, l'amministratore può vedere la posizione degli oggetti in CMC in modo da poter modificare gli oggetti prima di eliminare i livelli di accesso.

Nota:

- Per visualizzare l'elenco di oggetti interessati, è necessario disporre di diritti di **visualizzazione** su tali oggetti.
- I risultati delle query di relazione per un livello di accesso restituiscono oggetti a cui il livello di accesso è stato assegnato in modo esplicito. Se un oggetto utilizza un livello di accesso in base alle impostazioni di eredità, quell'oggetto non compare nei risultati delle query.

7.3.8 Gestione dei livelli di accesso tra i siti

I livelli di accesso sono oggetti che è possibile replicare da un sito di origine a più siti di destinazione. È possibile scegliere di replicare i livelli di accesso se figurano nell'elenco di controllo degli accessi dell'oggetto di replica. Se ad esempio a un principale viene concesso il livello di accesso A per il report Crystal e quest'ultimo viene replicato tra più siti, viene anche replicato il livello di accesso A.

Nota:

Se nel sito di destinazione esiste un livello di accesso con lo stesso nome, la replica del livello di accesso non verrà eseguita. Prima della replica, l'amministratore del sito di destinazione, o l'utente stesso, dovrà rinominare uno dei livelli di accesso.

Dopo avere replicato un livello di accesso tra i siti, tenere presenti le considerazioni sull'amministrazione.

Modifica dei livelli di accesso replicati nel sito di origine

Se un livello di accesso replicato viene modificato nel sito di origine, il livello di accesso nel sito di destinazione verrà aggiornato all'esecuzione successiva pianificata della replica. Negli scenari di replica bilaterale, se si modifica un livello di accesso replicato nel sito di destinazione, verrà modificato anche quello del sito di origine.

Nota:

Assicurarsi che le modifiche a un livello di accesso in un sito non influiscano negativamente sugli oggetti di altri siti. Consultare gli amministratori del sito e consigliare loro di eseguire query di relazioni per il livello di accesso replicato prima di apportare modifiche.

Modifica dei livelli di accesso replicati nel sito di destinazione

Nota:

È applicabile unicamente alla replica unilaterale.

Qualsiasi modifica ai livelli di accesso replicati apportata in un sito di destinazione non viene riflessa nel sito di origine. Ad esempio, l'amministratore del sito di destinazione può concedere il diritto di pianificare report Crystal nel livello di accesso replicato, anche se questo diritto è stato negato nel sito di origine. Di conseguenza, anche se i nomi dei livelli di accesso e degli oggetti replicati rimangono invariati, i diritti effettivi dei principali sugli oggetti potrebbero variare da sito di destinazione a sito di destinazione.

Se il livello di accesso replicato varia tra sito di origine e sito di destinazione, la differenza nei diritti effettivi verrà rilevata alla successiva esecuzione del processo di replica. È possibile fare in modo che il livello di accesso del sito di origine abbia la precedenza sul livello di accesso del sito di destinazione o che il livello di accesso del sito di destinazione rimanga intatto. Tuttavia, se non si fa in modo che il livello di accesso del sito di origine abbia la precedenza sul livello di accesso del sito di destinazione, qualsiasi oggetto in attesa di replica che utilizza quel livello di accesso non verrà replicato.

Per impedire agli utenti di modificare i livelli di accesso replicati nel sito di destinazione, è possibile aggiungere utenti del sito di destinazione al livello di accesso come principali e concedere a tali utenti solo i diritti di **visualizzazione**. Ciò significa che gli utenti del sito di destinazione possono visualizzare il livello di accesso, ma non possono modificare i relativi diritti o assegnarlo ad altri utenti.

Argomenti correlati

- [Federation](#)
- [Analisi e relazione tra livelli di accesso e oggetti](#)

7.4 Interruzione dell'ereditarietà

L'ereditarietà consente di gestire le impostazioni di protezione senza impostare diritti per ogni singolo oggetto. Tuttavia, in alcuni casi, può non essere opportuno che i diritti vengano ereditati. Ad esempio, può essere necessario personalizzare i diritti per ogni oggetto. È possibile disabilitare l'ereditarietà per un principale in un elenco di controllo degli accessi di un oggetto. Quando si esegue questa operazione, è possibile scegliere se disabilitare l'ereditarietà del gruppo, della cartella o entrambe.

Nota:

Quando viene interrotta, l'ereditarietà è interrotta per tutti i diritti e non è possibile disattivarla per alcuni diritti e non per altri.

Nel diagramma "Interruzione dell'ereditarietà", l'ereditarietà di gruppi e cartelle è inizialmente attiva. L'Utente Rosso eredita i diritti 1 e 5 come concessi, i diritti 2, 3 e 4 come non specificati e il diritto 6 come esplicitamente negato. Tali diritti, impostati a livello di cartella per il gruppo, indicano che l'utente rosso e tutti gli altri membri del gruppo dispongono dei diritti per gli oggetti della cartella, A e B. Quando l'ereditarietà viene interrotta a livello di cartella, l'insieme dei diritti dell'utente rosso per gli oggetti presenti in quella cartella viene annullato finché un amministratore assegna all'utente nuovi diritti.

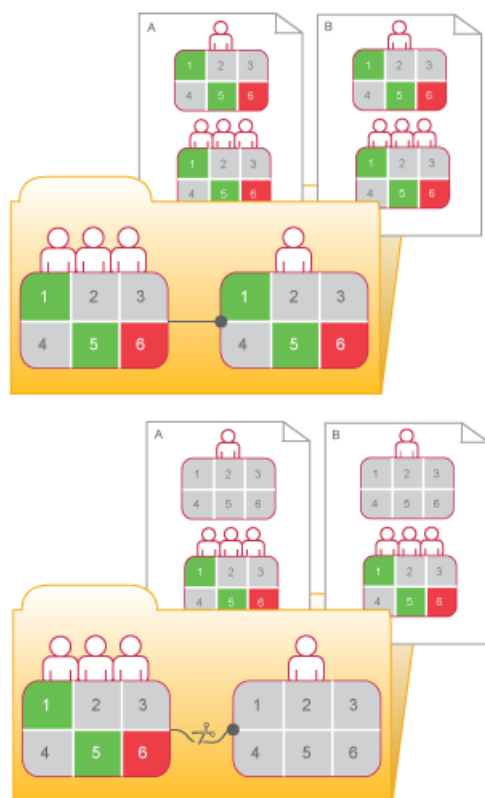


Figura 7 - 9: Interruzione dell'ereditarietà

7.4.1 Per disabilitare l'eredità

Questa procedura consente di disabilitare l'eredità di gruppo o cartella, o entrambi, per un principale nell'elenco di controllo degli accessi di un oggetto.

1. Selezionare l'oggetto per il quale si desidera disabilitare l'eredità.
2. Fare clic su **Gestisci > Protezione utente**.

Verrà visualizzata la finestra di dialogo "Protezione utente".

3. Selezionare il principale per il quale disabilitare l'eredità, quindi fare clic su **Assegna protezione**. Viene visualizzata la finestra di dialogo "Assegna protezione".
4. Configurare le impostazioni di eredità.
 - Per disabilitare l'eredità di gruppo (i diritti che il principale eredita dall'appartenenza al gruppo), deselezionare la casella di controllo **Eredita da gruppo principale**.
 - Per disabilitare l'eredità di cartella (i diritti che l'oggetto eredita dalla cartella), deselezionare la casella di controllo **Eredita da cartella principale**.
5. Fare clic su **OK**.

7.5 Utilizzo dei diritti per delegare l'amministrazione

Oltre a consentire il controllo dell'accesso a oggetti e impostazioni, i diritti consentono di suddividere le attività amministrative tra i gruppi funzionali dell'organizzazione. Ad esempio, può essere opportuno che persone di reparti diversi gestiscano i propri utenti e gruppi. In alternativa, è possibile che un amministratore si occupi della gestione di alto livello della piattaforma BI, ma che le attività di gestione dei server siano affidate al personale del reparto IT.

Presupponendo che la struttura del gruppo e quella della cartella siano allineate alla struttura di protezione dell'amministrazione delegata, è necessario concedere all'amministratore delegato diritti per tutti i gruppi di utenti ma non diritti completi sugli utenti controllati. Ad esempio, è possibile non ritenere opportuno che l'amministratore delegato modifichi gli attributi utente o li riassegna a gruppi diversi.

Nota:

le migrazioni di oggetti vengono eseguite al meglio da membri del gruppo Amministratori, in particolare dall'account utente Administrator. La migrazione di un oggetto potrebbe implicare la migrazione anche di molti oggetti correlati. Un account amministratore delegato potrebbe non ottenere i diritti di protezione richiesti per tutti gli oggetti.

La tabella contenente i "diritti per amministratori delegati" contiene un riepilogo dei diritti necessari agli amministratori delegati per eseguire azioni comuni.

Tabella 7 - 3: Diritti per amministratori delegati

Azione per amministratore autorizzato	Diritti richiesti dall'amministratore delegato
Creazione di nuovi utenti	Diritto di aggiunta nella cartella Utenti di livello superiore
Creazione di nuovi gruppi	Diritto di aggiunta nella cartella Gruppi utente di livello superiore

Azione per amministratore autorizzato	Diritti richiesti dall'amministratore delegato
Eliminazione di gruppi controllati nonché di singoli utenti di tali gruppi	Diritto di eliminazione sui relativi gruppi
Eliminazione solo degli utenti creati dall'amministratore delegato	Diritto di eliminazione proprietario nella cartella Utenti di livello superiore
Eliminazione solo degli utenti e dei gruppi creati dall'amministratore delegato	Diritto di eliminazione proprietario nella cartella Gruppi utente di livello superiore
Modifica solo degli utenti creati dall'amministratore delegato (compresa l'aggiunta di tali utenti ai gruppi)	Diritto di modifica proprietario e diritti di modifica proprietario in modo sicuro nella cartella Utenti di livello superiore
Modifica solo dei gruppi creati dall'amministratore delegato (compresa aggiunta di utenti a quei gruppi)	Diritto di modifica proprietario e diritti di modifica proprietario in modo sicuro nella cartella Gruppi utente di livello superiore
Modifica delle password per gli utenti nei relativi gruppi controllati	Diritto di modifica password sui relativi gruppi
Modifica password solo per i principali creati dall'amministratore delegato	Diritto Password di modifica proprietario nella cartella Utente di livello superiore o sui gruppi rilevanti Nota: L'impostazione del diritto Password di modifica proprietario su un gruppo ha effetto su un utente solo quando si aggiunge l'utente al gruppo rilevante.
Modifica nomi utenti, descrizione, altri attributi e riassegnazione utenti a gruppi diversi	Diritto di modifica sui gruppi rilevanti
Modifica di nomi utenti, descrizione, altri attributi e riassegnazione degli utenti ad altri gruppi, ma solo per gli utenti creati dall'amministratore delegato	Diritto di modifica proprietario nella cartella Utente di livello superiore o sui gruppi rilevanti Nota: L'impostazione del diritto di modifica proprietario sui gruppi rilevanti ha effetto su un utente solo quando si aggiunge l'utente al relativo gruppo.

7.5.1 Scelta tra le opzioni “Modificare i diritti che gli utenti hanno sugli oggetti”

Quando si imposta l'amministrazione delegata, fornire all'amministratore i diritti sui principali da controllare. È possibile fornire tutti i diritti (**Controllo completo**); è tuttavia buona norma utilizzare le impostazioni Diritti avanzati per conservare il diritto **Modifica dei diritti** e in alternativa fornire all'amministratore autorizzato il diritto **Modificare in modo sicuro i diritti degli utenti sugli oggetti**. È inoltre possibile fornire all'amministratore il diritto **Modificare in modo sicuro le impostazioni di eredità dei diritti** anziché il diritto **Modificare le impostazioni di eredità dei diritti**. Le differenze tra questi diritti sono descritte di seguito.

Modificare i diritti che gli utenti hanno sugli oggetti

Questo diritto consente a un utente di modificare qualsiasi diritto per qualsiasi utente su un oggetto. Ad esempio, se l'utente A dispone dei diritti **Visualizzare oggetti** e **Modificare i diritti che gli utenti hanno sugli oggetti**, potrà modificare i diritti per quell'oggetto in modo da fornire a se stesso o ad altri utenti il controllo completo dell'oggetto.

Modificare in modo sicuro i diritti degli utenti sugli oggetti

Questo diritto consente a un utente di concedere, negare o reimpostare su non specificato solo i diritti già concessi. Ad esempio, se l'utente A dispone dei diritti **Visualizzare oggetti** e **Modificare in modo sicuro i diritti degli utenti sugli oggetti**, non potrà assegnare a se stesso ulteriori diritti e potrà concedere o negare ad altri utenti solo i diritti (**Visualizzare oggetti** e **Modificare in modo sicuro i diritti**). Inoltre, l'utente A potrà modificare per gli utenti solo i diritti su oggetti per i quali dispone del diritto **Modificare in modo sicuro i diritti degli utenti sugli oggetti**.

Sono tutte le condizioni che devono esistere per l'utente A per la modifica dei diritti per l'utente B sull'oggetto O:

- L'utente A dispone del diritto **Modificare in modo sicuro i diritti degli utenti sugli oggetti** sull'oggetto O.
- Ogni diritto o livello di accesso che l'utente A modifica per l'utente B è concesso ad A.
- L'utente A dispone del diritto **Modificare in modo sicuro i diritti degli utenti sugli oggetti** sull'utente B.
- Se viene assegnato un livello di accesso, l'utente A dispone del diritto **Assegnare livello di accesso** sul livello di accesso che cambia per l'utente B.

L'ambito dei diritti può limitare ulteriormente i diritti effettivi che un amministratore autorizzato può assegnare. È possibile ad esempio che un amministratore con delega disponga dei **diritti di modifica in modo sicuro i diritti degli utenti sugli oggetti** e dei **diritti di modifica** per una cartella, ma l'ambito di questi diritti è limitato alla cartella e non è applicabile ai relativi oggetti secondari. L'amministratore autorizzato può concedere il diritto di **modifica** per la cartella (ma non per i relativi oggetti secondari) e solo con un ambito di “applicazione agli oggetti”. D'altro canto, se l'amministratore autorizzato dispone del diritto di **modifica** per una cartella con ambito di “applicazione agli oggetti secondari”, può concedere ad altri principali il diritto di **modifica** con entrambi gli ambiti per gli oggetti secondari della cartella, ma

per la cartella può concedere unicamente il diritto di **modifica** con ambito di “applicazione agli oggetti secondari”.

Inoltre, l'amministratore autorizzato non potrà modificare i diritti per quei gruppi per altri principali per cui non dispone del diritto Modificare in modo sicuro i diritti degli utenti sugli oggetti. È utile, ad esempio, se due sono gli amministratori autorizzati responsabili di concedere diritti a diversi gruppi di utenti per la stessa cartella, ma non si desidera che uno sia in grado di negare l'accesso ai gruppi controllati dall'altro amministratore. Il diritto Modificare in modo sicuro i diritti degli utenti sugli oggetti garantisce questa limitazione, poiché gli amministratori delegati in genere non dispongono del diritto Modificare in modo sicuro i diritti degli utenti sugli oggetti gli uni per gli altri.

Modificare in modo sicuro le impostazioni di eredità dei diritti

Questo diritto consente all'amministratore delegato di modificare le impostazioni di eredità per altri principali sugli oggetti a cui ha accesso. Per modificare in modo corretto le impostazioni di eredità di altri principali, un amministratore autorizzato deve disporre di questo diritto sull'oggetto e sugli account utente per i principali.

7.5.2 Diritti del proprietario

I diritti del proprietario sono validi solo per il proprietario dell'oggetto di cui vengono verificati i diritti. Nella piattaforma BI il proprietario di un oggetto è il principale che ha creato l'oggetto; se il principale viene eliminato dal sistema, la proprietà torna all'amministratore.

I diritti di proprietario sono utili per la gestione della protezione basata su proprietario. Ad esempio, è possibile creare una cartella o una gerarchia di cartelle in cui diversi utenti possono creare e visualizzare documenti, ma possono modificare o eliminare solo i propri documenti. Inoltre, i diritti del proprietario consentono agli utenti di modificare le proprie istanze di report ma non quelle create da altri. Nel caso del livello di accesso Pianificazione, gli utenti hanno la possibilità di modificare, eliminare, sospendere e ripianificare solo le proprie istanze.

I diritti del proprietario hanno funzioni analoghe ai corrispondenti diritti regolari. Tuttavia, i diritti proprietario sono efficaci solo se al principale sono stati concessi i diritti proprietario, ma quelli ordinari sono stati negati o non specificati.

7.6 Riepilogo delle indicazioni per l'amministrazione dei diritti

Per l'amministrazione dei diritti, tenere presenti le seguenti considerazioni:

- Utilizzare i livelli di accesso ove possibile. Gli insiemi predefiniti di diritti semplificano l'amministrazione raggruppando i diritti associati alle esigenze comuni degli utenti.

- Impostare i diritti e i livelli di accesso per le cartelle di livello superiore. L'abilitazione dell'ereditarietà consentirà di trasferire i diritti attraverso il sistema con un intervento minimo da parte dell'amministrazione.
- Se possibile, evitare di rompere l'eredità. Questo consente di ridurre la quantità di tempo necessaria per proteggere il contenuto aggiunto alla piattaforma BI.
- Impostare i diritti appropriati per utenti e gruppi a livello di cartella, quindi pubblicare gli oggetti in quella cartella. Per impostazione predefinita, gli utenti o i gruppi che dispongono dell'accesso a una cartella ereditano gli stessi diritti per tutti gli oggetti pubblicati successivamente nella cartella.
- Organizzare gli utenti in gruppi, assegnare livelli di accesso e diritti all'intero gruppo e assegnare livelli di accesso e diritti a membri specifici.
- Creare singoli account Administrator per ogni amministratore del sistema e aggiungerli al gruppo Administrators per definire meglio la responsabilità per le modifiche di sistema.
- Per impostazione predefinita, al gruppo Tutti vengono concessi diritti molto limitati alle cartelle di livello superiore nella piattaforma BI. Dopo l'installazione, è consigliabile rivedere i diritti dei membri del gruppo Tutti e assegnare la protezione di conseguenza.

Protezione della piattaforma BI

8.1 Panoramica della protezione

In questa sezione sono illustrati in modo dettagliato i metodi tramite cui la piattaforma BI affronta la protezione dei dati aziendali, fornendo allo stesso tempo ad amministratori e architetti di sistema risposte alle domande relative alla protezione.

L'architettura della piattaforma BI affronta i numerosi problemi di protezione delle aziende e delle organizzazioni moderne. La versione corrente supporta funzionalità come distribuzione della protezione, Single Sign On, protezione dell'accesso alle risorse, diritti granulari dell'oggetto e autenticazione di terze parti per la protezione contro gli accessi non autorizzati.

Poiché la piattaforma BI fornisce la struttura per un numero crescente di componenti della famiglia Enterprise di prodotti SAP BusinessObjects, in questa sezione vengono descritte in dettaglio le funzioni di protezione e le relative funzionalità per dimostrare come questa struttura rafforzi e gestisca la protezione. Per questo motivo, in questa sezione non sono riportati i dettagli veri e propri delle procedure ma le informazioni concettuali e i collegamenti alle procedure chiave.

Dopo una breve introduzione ai concetti relativi alla protezione per il sistema, verranno forniti alcuni dettagli per gli argomenti seguenti:

- Come utilizzare la crittografia e le modalità di protezione dell'elaborazione dei dati per proteggere i dati.
- Come impostare Secure Sockets Layer per le distribuzioni della piattaforma BI.
- Linee guida per impostare e gestire i firewall per la piattaforma BI.
- Configurazione dei server reverse proxy.

8.2 Pianificazione del ripristino d'emergenza

Occorre adottare alcune misure per proteggere l'investimento dell'azienda nella piattaforma BI, assicurando la massima continuità delle attività in caso di situazioni di emergenza. Questa sezione fornisce le indicazioni necessarie per elaborare un piano di ripristino di emergenza per la propria organizzazione.

Indicazioni generali

- Eseguire regolarmente un backup del sistema e inviare copie del backup ad altri uffici, se necessario.

- Archiviare in modo sicuro tutti i supporti del software.
- Archiviare in modo sicuro tutta la documentazione relativa alle licenze.

Indicazioni specifiche

Tre risorse del sistema richiedono un'attenzione particolare in termini di ripristino da situazioni di emergenza:

- Contenuto nei File Repository Server: è incluso il contenuto proprietario, ad esempio i report. Eseguire regolarmente un backup dei contenuti: in caso di problemi irreversibili, non esiste un modo per rigenerare i contenuti se non è stato eseguito un backup regolare.
- Il database di sistema utilizzato dal server CMS: questa risorsa contiene tutti i metadati essenziali per la distribuzione, ad esempio i dati degli utenti, i report e altre informazioni riservate importanti per l'organizzazione.
- File della chiave delle informazioni del database (.dbinfo): contiene la chiave principale per il database di sistema. Se per qualche motivo la chiave non è disponibile, non sarà possibile accedere al database di sistema. Dopo aver distribuito la piattaforma BI, si consiglia vivamente di memorizzare la password per questa risorsa in un luogo sicuro e noto. Senza la password non sarà possibile rigenerare il file e si perderà quindi l'accesso al database di sistema.

8.3 Raccomandazioni generali per la protezione della distribuzione

Di seguito sono riportate le linee guida per la protezione delle distribuzioni della piattaforma BI.

- Utilizzare i firewall per proteggere le comunicazioni tra il server CMS e altri componenti del sistema. Se possibile, nascondere sempre il CMS dietro al firewall. Come minimo, assicurarsi che il database di sistema sia protetto dietro il firewall.
- Aggiungere ulteriore crittografia ai File Repository Server. Una volta avviato il sistema, il contenuto proprietario verrà memorizzato in questi server. Aggiungere ulteriore crittografia attraverso il sistema operativo o uno strumento di terze parti.

Nota:

La piattaforma BI non supporta SFTP. Se è necessario utilizzare la funzionalità SFTP, fare riferimento alla nota SAP 1556571 o prendere in considerazione l'utilizzo della soluzione di un partner SAP.

- Distribuire un server reverse proxy davanti ai server di applicazioni Web per nasconderli dietro un singolo indirizzo IP. Questa configurazione instrada tutto il traffico Internet indirizzato a server di applicazioni Web privati attraverso il server reverse proxy, nascondendo quindi gli indirizzi IP privati.
- Applicare con rigore i criteri relativi alle password aziendali. Assicurarsi che le password utente vengano periodicamente modificate.
- Se si è deciso di installare il database di sistema e il server di applicazioni Web forniti con la piattaforma BI, è necessario consultare la relativa documentazione per verificare che i componenti vengano distribuiti con configurazioni di protezione adeguate.
- Utilizzare il protocollo Secure Sockets Layer (SSL) per tutte le comunicazioni di rete tra client e server nella distribuzione.
- Assicurarsi che la directory e le sottodirectory di installazione della piattaforma siano protette. In tali directory, infatti, durante il funzionamento del sistema potrebbero essere salvati dati temporanei sensibili.

- L'accesso alla console CMC (Central Management Console) dovrebbe essere limitato al solo accesso locale. Per informazioni sulle opzioni di distribuzione per la console CMC, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

Argomenti correlati

- [Configurazione del protocollo SSL](#)
- [Limitazioni relative alle password](#)
- [Configurazione della protezione per server di terze parti in bundle](#)

8.4 Configurazione della protezione per server di terze parti in bundle

Se si decide di installare componenti server di terze parti forniti in bundle con la piattaforma BI, è consigliabile accedere e consultare la documentazione relativa ai componenti in bundle riportati di seguito.

- Sybase SQL Anywhere: per informazioni dettagliate sulla protezione di questo database di sistema, consultare <http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.help.sqlanywhere.12.0.0/dbadmin/da-part-securing.html>.
- Apache Tomcat: per informazioni dettagliate sulla protezione di questo server di applicazioni Web, consultare <http://tomcat.apache.org/>.

8.5 Relazione di trust attiva

In un ambiente di rete, una relazione di trust tra due domini è in genere una connessione che consente a un dominio di riconoscere gli utenti che sono stati autenticati dall'altro dominio. Pur conservando la protezione, la relazione di trust consente agli utenti di accedere alle risorse in più domini senza dovere fornire ripetutamente le loro credenziali.

All'interno dell'ambiente della piattaforma BI, la relazione di trust attiva funziona in modo simile per fornire a ciascun utente l'accesso alle risorse in tutto il sistema. Un volta che l'utente è stato autenticato e gli è stata concessa una sessione attiva, tutti gli altri componenti della piattaforma BI possono elaborare le richieste e le operazioni dell'utente senza richiedere le credenziali. In questo modo, la relazione di trust attiva fornisce la base per la protezione distribuita della piattaforma BI.

8.5.1 Token di accesso

Un token di accesso è una stringa codificata che definisce i propri attributi di utilizzo e contiene informazioni sulla sessione dell'utente. Gli attributi di utilizzo di un token di accesso sono specificati quando viene generato il token di accesso. Questi attributi consentono di inserire limitazioni sul token di accesso per ridurre la possibilità di utilizzo del token da parte di utenti non autorizzati. Gli attributi correnti del token di accesso sono i seguenti:

- **Numero di minuti**

Questo attributo limita la durata del token di accesso.

- **Numero di accessi**

Questo attributo limita il numero di utilizzi del token di accesso per accedere alla piattaforma BI.

Entrambi gli attributi ostacolano l'accesso non autorizzato alla piattaforma BI con token di accesso recuperati da utenti autorizzati.

Nota:

la memorizzazione di un token di accesso in un cookie è un potenziale rischio per la protezione se la rete tra il browser e il server Web o delle applicazioni non è protetto, ad esempio se la connessione avviene su una rete pubblica senza utilizzare SSL o l'autenticazione affidabile. È buona norma utilizzare SSL (Secure Sockets Layer) per ridurre i rischi per la protezione tra il browser e il server Web o delle applicazioni.

Dopo avere disabilitato il cookie di accesso e il timeout del browser o del server Web, viene visualizzata la schermata di accesso. Quando il cookie viene abilitato e si verifica il timeout del server o del browser, l'utente viene riconnesso al sistema. Poiché le informazioni sullo stato sono legate alla sessione Web, tuttavia, lo stato dell'utente viene perso. Ad esempio, se l'utente aveva espanso l'albero di spostamento e selezionato un elemento, l'albero viene reimpostato.

Per la piattaforma BI, l'impostazione predefinita consiste nell'abilitazione dei token di accesso nel client Web. Tuttavia, è possibile disabilitare tali token per BI Launch Pad. Se i token di accesso vengono disabilitati nel client, la sessione utente sarà limitata dal timeout del server o browser Web. Allo scadere della sessione, all'utente verrà nuovamente richiesto l'accesso alla piattaforma BI.

8.5.2 Meccanismo dei ticket per la distribuzione della protezione

Per i sistemi Enterprise dedicati che servono un grande numero di utenti è necessaria in genere una forma di distribuzione della protezione. Un sistema Enterprise potrebbe richiedere una protezione distribuita per supportare funzionalità quali il trasferimento dell'attendibilità (la possibilità di consentire a un altro componente di agire per conto dell'utente).

La piattaforma BI affronta il problema della distribuzione della protezione implementando un meccanismo di ticket simile al meccanismo di ticket Kerberos. Il CMS concede ticket che autorizzano i componenti a eseguire azioni per un particolare utente. Nella piattaforma BI, per ticket si intende il token di accesso.

Questo token è il più utilizzato sul Web. Quando gli utenti vengono autenticati per la prima volta dalla piattaforma BI, ricevono i token di accesso dal server CMS. Il browser dell'utente memorizza tale token

nella cache. Quando l'utente esegue una nuova richiesta, altri componenti della piattaforma BI possono leggere il token di accesso dal browser dell'utente.

8.6 Sessioni e registrazione delle sessioni

In generale, una sessione è una connessione client-server che consente lo scambio di informazioni tra due computer. Lo stato di una sessione è rappresentato da una serie di dati che descrive gli attributi della sessione, la sua configurazione o il suo contenuto. Quando si stabilisce una connessione tra client e server sul Web, la natura del protocollo HTTP limita la durata di ciascuna sessione a una pagina singola di informazioni; in questo modo, il browser memorizza lo stato di ciascuna sessione solo per il periodo di visualizzazione di ogni singola pagina Web. Quando ci si sposta da una pagina Web a un'altra, lo stato della prima sessione viene annullato e sostituito con lo stato della sessione successiva. Di conseguenza, i siti Web e le applicazioni Web devono memorizzare lo stato di una sessione se si desidera riutilizzarne le informazioni in un'altra.

La piattaforma BI impiega due metodi comuni per memorizzare lo stato di una sessione:

- **Cookie:** un cookie è un piccolo file di testo in cui è archiviato lo stato della sessione sul lato client. Il browser Web dell'utente memorizza nella cache il cookie per un utilizzo successivo. Il token di accesso della piattaforma BI è un esempio di questo metodo.
- **Variabili di sessione:** una variabile di sessione è una parte di memoria in cui è archiviato lo stato della sessione sul lato server. Quando la piattaforma BI concede a un utente un'identità attiva sul sistema, informazioni come quelle relative al tipo di autenticazione dell'utente vengono memorizzate in una variabile di sessione. Per la durata della sessione, il sistema non dovrà richiedere all'utente le informazioni né dovrà ripetere eventuali operazioni necessarie per il completamento della richiesta successiva.

Per le distribuzioni Java, la sessione viene utilizzata per gestire le richieste .jsp, per le distribuzioni .NET, la sessione viene utilizzata per gestire le richieste .aspx.

Nota:

In teoria, il sistema conserva la variabile di sessione mentre l'utente esegue attività sul sistema; inoltre, per garantire la protezione e ridurre al minimo l'utilizzo delle risorse, il sistema dovrebbe distruggere la variabile di sessione appena l'utente ha terminato le proprie operazioni sul sistema. Tuttavia, poiché l'interazione tra un browser e un server Web può essere senza stato, individuare il momento dell'uscita dell'utente dal sistema può essere difficile se quest'ultimo non si disconnette in modo esplicito. Per risolvere questo problema, la piattaforma BI implementa la registrazione delle sessioni.

8.6.1 Registrazione delle sessioni CMS

Il CMS implementa un algoritmo di registrazione semplice. Quando un utente accede al sistema, gli viene concessa una sessione CMS, che il CMS conserva fino alla disconnessione o al rilascio della variabile di sessione del server di applicazioni Web.

La sessione del server di applicazioni Web è progettata per comunicare periodicamente al CMS di essere ancora attiva, in modo tale che la sessione CMS venga conservata fino alla chiusura della sessione del server. Se la sessione del server di applicazioni Web non riesce a comunicare con il CMS per un periodo di dieci minuti, il CMS chiude la sessione CMS. Questa condizione è utile negli scenari in cui i componenti lato client vengono chiusi in modo anomalo.

8.7 Protezione dell'ambiente

Per protezione dell'ambiente si intende la protezione dell'ambiente generale di comunicazione tra componenti client e server. Anche se Internet e i sistemi basati sul Web sono sempre più popolari, grazie alla loro flessibilità e alla gamma delle loro funzionalità, essi operano in un ambiente che può essere difficile proteggere. Durante la distribuzione della piattaforma BI, la protezione dell'ambiente viene suddivisa tra due aree di comunicazione: da browser a server Web e da server Web a piattaforma BI.

8.7.1 Da browser a server Web

Quando tra il browser e il server Web vengono trasmessi dati sensibili, è di solito necessario un certo grado di protezione. Le misure di protezione più importanti coinvolgono di solito due attività generali:

- Assicurare la protezione della comunicazione di dati.
- Assicurare che solo gli utenti autorizzati possano recuperare informazioni dal server Web.

Nota:

Queste attività sono in genere gestite dai server Web tramite vari meccanismi di protezione, come il protocollo SSL (Secure Sockets Layer) e altri meccanismi simili. È buona norma utilizzare SSL per ridurre i rischi per la protezione tra il browser e il server Web o delle applicazioni.

Le comunicazioni tra il browser e il server Web devono essere protette in modo indipendente dalla piattaforma BI. Per ulteriori dettagli sulla protezione delle connessioni client, consultare la documentazione del server Web.

8.7.2 Comunicazione tra il server Web e la piattaforma BI

Per proteggere l'area di comunicazione tra il server Web e il resto della rete Intranet aziendale, compresa la piattaforma BI, vengono di norma utilizzati i firewall. La piattaforma supporta firewall che utilizzano filtri IP o la tecnologia NAT (Network Address Translation) statica. Tra gli ambienti supportati possono essere inclusi più firewall, server Web o i server delle applicazioni.

8.8 Controllo delle modifiche alla configurazione della protezione

La piattaforma BI non controllerà le eventuali modifiche apportate alle configurazioni della protezione predefinite per gli elementi seguenti:

- File delle proprietà delle applicazioni Web (BOE, servizi Web)
- TrustedPrincipal.conf
- Personalizzazione eseguita su BI Launch Pad e OpenDocument

In generale, non verranno controllate tutte le modifiche alla configurazione della protezione apportate esternamente alla console CMC, incluse le eventuali modifiche eseguite tramite CCM (Central Configuration Manager). Le modifiche salvate tramite CMC possono essere controllate.

8.9 Controllo dell'attività sul Web

La piattaforma BI assicura la possibilità di registrare le attività sul Web all'interno del sistema e di controllarne i dettagli. Il server di applicazioni Web consente di selezionare gli attributi Web da registrare, ad esempio l'ora, la data, l'indirizzo IP, il numero di porta e così via. I dati di controllo vengono registrati su disco e archiviati in file csv, in modo da poter creare report dai dati o importarli in altre applicazioni.

8.9.1 Protezione contro tentativi di accesso non autorizzati

A prescindere dal livello di protezione di un sistema, è sempre presente almeno una posizione più vulnerabile agli attacchi: la posizione da cui gli utenti si connettono al sistema. È quasi impossibile proteggere completamente questo punto, in quanto indovinare un nome utente e una password rimane un sistema praticabile per penetrare nel sistema.

La piattaforma BI implementa diverse tecniche per ridurre la probabilità che un utente non autorizzato ottenga accesso al sistema. Le varie limitazioni elencate di seguito sono valide solo per gli account Enterprise; in altre parole, non si applicano ad account mappati a un database utente esterno (LDAP o Windows AD). In genere, tuttavia, il sistema esterno consente di inserire limitazioni simili per gli account esterni.

8.9.2 Limitazioni relative alle password

Le limitazioni relative alle password assicurano che gli utenti che eseguono l'autenticazione Enterprise predefinita creino password relativamente complesse. È possibile selezionare le seguenti opzioni:

- Attiva password con maiuscole e minuscole

Questa opzione garantisce che le password contengano almeno due delle seguenti classi di caratteri: lettere maiuscole, lettere minuscole, numeri o simboli di punteggiatura.

- La password deve contenere almeno N caratteri

Inserendo un minimo di complessità per le password è possibile ridurre le possibilità dell'utente di indovinare una password valida.

8.9.3 Limitazioni relative all'accesso

Le limitazioni relative all'accesso servono principalmente per evitare attacchi tramite dizionario (un metodo che consente a un utente non autorizzato di ottenere un nome utente valido e di tentare di scoprire la password corrispondente tramite le parole contenute in un dizionario). La velocità dell'hardware attuale consente a programmi dannosi di ottenere milioni di password al minuto. Per impedire attacchi tramite dizionario, la piattaforma BI dispone di un meccanismo interno che determina un ritardo (0,5 - 1 secondo) tra i tentativi di accesso. La piattaforma prevede inoltre diverse opzioni personalizzabili da utilizzare per ridurre il rischio di attacchi di questo tipo:

- Disattiva account dopo N tentativi di accesso
- Reimposta conteggio tentativi di accesso non riusciti dopo N minuti
- Riabilita account dopo N minuti

8.9.4 Limitazioni per l'utente

Le limitazioni per l'utente assicurano che gli utenti che eseguono l'autenticazione Enterprise predefinita creino le nuove password con una frequenza appropriata. È possibile selezionare le seguenti opzioni:

- La password deve essere modificata ogni N giorni
- Impossibile riutilizzare le N password più recenti
- Attendi N minuti per modificare la password

Queste opzioni possono essere utilizzate in molti modi. In primo luogo, eventuali utenti non autorizzati che tentassero un attacco tramite dizionario dovranno ricominciare ogni volta che le password sono modificate. Inoltre, poiché le modifiche delle password sono basate sul periodo del primo accesso di ciascun utente, l'utente non autorizzato non potrà determinare in modo agevole il momento in cui una password particolare verrà modificata. Inoltre, anche nel caso in cui un utente non autorizzato riuscisse a indovinare o ottenere in altro modo le credenziali di un altro utente, queste risulteranno valide solo per un tempo limitato.

8.9.5 Limitazioni all'account Guest

La piattaforma BI supporta il Single Sign On anonimo per l'account Guest. In questo modo, quando gli utenti si connettono alla piattaforma BI senza specificare un nome utente e una password, il sistema consente l'accesso automatico con l'account Guest. Se si assegna una password protetta all'account Guest o si disabilita completamente l'account Guest, si disabilita anche questo comportamento predefinito.

8.10 Estensioni di elaborazione

La piattaforma BI consente di proteggere ulteriormente l'ambiente di creazione dei report tramite l'utilizzo di estensioni di elaborazione personalizzate. Un'estensione di elaborazione è una libreria di dati collegata in modo dinamico che applica la logica aziendale a richieste particolari di visualizzazione o pianificazione nella piattaforma BI prima che queste siano elaborate dal sistema.

Tramite il supporto per le estensioni di elaborazione, l'SDK per l'amministrazione della piattaforma BI espone un "handle" che consente agli sviluppatori di intercettare la richiesta. Gli sviluppatori possono quindi aggiungere formule di selezione alla richiesta prima che il report sia elaborato.

Un esempio tipico è costituito da un'estensione di elaborazione di un report in cui sia rafforzata la protezione a livello di riga. Questo tipo di protezione consente di limitare l'accesso ai dati per le righe di una o più tabelle di database. Lo sviluppatore crea una libreria caricata dinamicamente che intercetta le richieste di visualizzazione o pianificazione relative a un report prima che tali richieste siano elaborate da Job Server, Processing Server o Report Application Server. Il codice inserito dallo sviluppatore individua per prima cosa l'utente proprietario del lavoro di elaborazione, quindi ricerca i privilegi di accesso ai dati dell'utente in un sistema di terze parti. Il codice genera quindi una formula di selezione record e la aggiunge al report per limitare i dati restituiti dal database. In questo caso, l'estensione di elaborazione funge da metodo per incorporare la protezione personalizzata a livello di riga nell'ambiente della piattaforma BI.

Abilitando le estensioni di elaborazione è possibile configurare i componenti server della piattaforma BI appropriati per caricare dinamicamente le estensioni di elaborazione in fase di esecuzione. All'interno dell'SDK è presente un'API documentata in modo completo che gli sviluppatori possono utilizzare per

creare estensioni di elaborazione. Per ulteriori informazioni, consultare la documentazione per gli sviluppatori disponibile nel supporto del prodotto.

8.11 Panoramica della protezione dei dati della piattaforma BI

Gli amministratori dei sistemi della piattaforma BI gestiscono il modo in cui i dati sensibili vengono protetti mediante:

- Un'impostazione di protezione a livello di cluster che determina quali applicazioni e quali client possono accedere al server CMS. Questa impostazione viene gestita attraverso Central Configuration Manager.
- Un sistema di crittografia a due chiavi che controlla sia l'accesso al repository CMS sia le chiavi utilizzate per crittografare/decrittare gli oggetti all'interno del repository. L'accesso al repository CMS viene impostato tramite Central Configuration Manager, mentre la console CMC utilizza un'area di gestione dedicata per le chiavi di crittografia.

Queste funzionalità consentono agli amministratori di impostare le distribuzioni della piattaforma BI su particolari livelli di conformità con la protezione dei dati e di gestire le chiavi di crittografia per crittografare i dati nel repository CMS.

8.11.1 Modalità di protezione dell'elaborazione dei dati

La piattaforma BI può operare in due modalità di protezione dell'elaborazione dei dati:

- La modalità di protezione dell'elaborazione dei dati predefinita. In alcune istanze, i sistemi eseguiti in questa modalità utilizzano chiavi di crittografia hardcoded e non seguono uno standard specifico. La modalità predefinita consente la compatibilità retroattiva con le versioni precedenti degli strumenti client e delle applicazioni della piattaforma BI.
- Una modalità di protezione dei dati il cui scopo è assicurare la conformità con le linee guida stabilite dallo standard FIPS (Federal Information Processing Standard), in particolare FIPS 140-2. In questa modalità, gli algoritmi e i moduli di crittografia conformi a FIPS vengono utilizzati per proteggere i dati sensibili. Quando la piattaforma viene eseguita in modalità conforme a FIPS, tutti gli strumenti client e le applicazioni non conformi alle linee guida FIPS vengono automaticamente disabilitati. Le applicazioni e gli strumenti client della piattaforma sono conformi allo standard FIPS 140-2. Le applicazioni e i client più datati non funzioneranno se la piattaforma BI viene eseguita in modalità conforme a FIPS.

La modalità di elaborazione dei dati è trasparente per gli utenti del sistema. In entrambe le modalità di protezione dell'elaborazione dei dati, i dati più importanti vengono crittografati e decrittati in background da un modulo di crittografia interno.

Si consiglia di utilizzare la modalità conforme a FIPS nelle seguenti circostanze:

- La distribuzione della piattaforma BI non deve necessariamente utilizzare o interagire con strumenti client o applicazioni precedenti della piattaforma BI.

- Gli standard dell'organizzazione relativi all'elaborazione dei dati vietano l'utilizzo delle chiavi di crittografia hardcoded.
- L'organizzazione deve proteggere i dati sensibili in base alle norme dello standard FIPS 140-2.

La modalità di protezione dell'elaborazione dei dati è impostata tramite Central Configuration Manager su entrambe le piattaforme Windows e UNIX. Ogni nodo di un ambiente in cluster deve essere impostato nello stesso modo.

8.11.1.1 Attivazione della modalità conforme a FIPS in Windows

Per impostazione predefinita, la modalità conforme a FIPS viene disattivata dopo l'installazione della piattaforma BI. È tuttavia possibile attivare la conformità FIPS per tutti i nodi della distribuzione.

1. Per avviare CCM, fare clic su **Programmi > SAP Business Intelligence > Piattaforma SAP BusinessObjects BI 4 > Central Configuration Manager**.
2. In CCM fare clic con il pulsante destro del mouse su Server Intelligence Agent (SIA) e scegliere **Arresta**.

Avvertenza:

Non procedere con il passaggio 3 fino a quando lo stato SIA non è contrassegnato come Interrotto.

3. Fare clic con il pulsante destro del mouse sul SIA e scegliere **Proprietà**.
La finestra di dialogo "Proprietà" viene visualizzata con la scheda **Proprietà**.
4. Aggiungere `-fips` al campo **Comando** e fare clic su **Applica**.
5. Fare clic su **OK** per chiudere la finestra di dialogo "Proprietà".
6. Riavviare il SIA.

L'agente SIA ora funziona in modalità conforme a FIPS.

L'impostazione conforme a FIPS deve essere attivata per tutti i SIA della distribuzione della piattaforma BI.

8.11.1.2 Attivazione della modalità conforme a FIPS in UNIX

È necessario arrestare tutti i nodi della distribuzione della piattaforma BI prima di tentare la procedura seguente.

Per impostazione predefinita, la modalità conforme a FIPS viene disattivata dopo l'installazione della piattaforma BI. Utilizzare le istruzioni riportate di seguito per attivare l'impostazione conforme a FIPS per tutti i nodi della distribuzione.

1. Dalla directory `DIRINSTALL/sap_bobj` aprire il file `ccm.config` per la modifica.
2. Aggiungere `-fips` al parametro del comando di avvio del nodo.

Il parametro del comando di avvio del nodo viene visualizzato nel formato: *NOMENODOLAUNCH*. Ad esempio per un nodo denominato "SAP", il parametro del comando di avvio è *SAPLAUNCH*.

3. Salvare le modifiche e **uscire**.
4. Riavviare il nodo.

Il nodo ora funziona in modalità conforme a FIPS.

L'impostazione conforme a FIPS deve essere attivata per tutti i nodi della distribuzione della piattaforma BI.

8.11.1.3 Disattivazione della modalità conforme a FIPS in Windows

Tutti i server della distribuzione della piattaforma BI devono essere interrotti prima di tentare la procedura seguente.

Se la distribuzione viene eseguita in modalità conforme a FIPS, utilizzare le istruzioni che seguono per disattivare l'impostazione.

1. In CCM, fare clic con il pulsante destro del mouse su Server Intelligence Agent (SIA) e scegliere **Arresta**.

Avvertenza:

non passare alla fase 2 prima che lo stato del nodo venga contrassegnato come "Interrotto".

2. Fare clic con il pulsante destro del mouse su SIA e scegliere **Proprietà**.
Viene visualizzata la finestra di dialogo "Proprietà", con la scheda **Proprietà** visualizzata.
3. Rimuovere `-fips` dal campo "Comando" e fare clic su **Applica**.
4. Fare clic su **OK** per chiudere la finestra di dialogo "Proprietà".
5. Riavviare il SIA.

8.12 Crittografia nella piattaforma BI

Dati sensibili

Lo scopo della crittografia della piattaforma BI è proteggere i dati più importanti archiviati nel repository CMS. Tali dati includono le credenziali utente, le informazioni relative alla connettività delle origini dati e qualsiasi altro tipo di oggetto in cui sono memorizzate delle password. I dati vengono crittografati per garantire la privacy e la protezione da eventuali danni, nonché per la gestione del controllo dell'accesso. Tutte le risorse di crittografia necessarie, compresi il modulo di crittografia e le librerie RSA, vengono installate per impostazione predefinita in ogni distribuzione della piattaforma BI.

La piattaforma BI utilizza un sistema di crittografia a due chiavi.

Chiavi di crittografia

La crittografia e la decrittazione dei dati sensibili vengono gestite in background tramite l'SDK, che interagisce con il modulo di crittografia interno. Gli amministratori del sistema gestiscono la protezione dei dati tramite chiavi di crittografia simmetriche senza crittografare o decrittare direttamente i blocchi di dati specifici.

Nella piattaforma BI, per crittografare/decrittare i dati sensibili vengono utilizzate chiavi di crittografia simmetriche. La console CMC dispone di un'area di gestione dedicata per le chiavi di crittografia. Utilizzare le "chiavi di crittografia" per visualizzare, generare, disattivare, revocare ed eliminare le chiavi. Il sistema assicura che qualsiasi chiave richiesta per decrittare i dati sensibili non possa essere eliminata.

Chiavi cluster

Le chiavi cluster sono chiavi di wrapping delle chiavi simmetriche che proteggono le chiavi di crittografia archiviate nel repository CMS. Utilizzando gli algoritmi delle chiavi simmetriche, le chiavi cluster mantengono un livello di controllo dell'accesso al repository CMS. A ogni nodo nella piattaforma BI viene assegnata una chiave cluster durante il processo di installazione. Gli amministratori del sistema possono utilizzare CCM per reimpostare la chiave cluster.

8.12.1 Utilizzo delle chiavi cluster

Durante la configurazione dell'installazione per la piattaforma BI, viene creata una chiave cluster di otto caratteri per l'agente SIA (Server Intelligence Agent). Tale chiave viene utilizzata per crittografare tutte le chiavi di crittografia nel repository CMS. Senza la chiave cluster corretta non è possibile accedere al server CMS.

La chiave cluster viene archiviata in formato crittografato in un file `dbinfo`. Per il nome del file `dbinfo` si segue questa convenzione: `_boe_<nome_sia>.dbinfo`, in cui `<nome_sia>` è il nome di Server Intelligence Agent per il cluster.

In Windows il file è archiviato nella directory seguente: `<DIRINSTALLAZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.

Nei sistemi Unix il file viene archiviato nella directory della piattaforma in `<DIRINSTAL LAZ>/sap_bobj/enterprise_xi40/`:

Piattaforma Unix	Directory della piattaforma
AIX	<DIRINSTALL>/sap_bobj/enterprise_xi40/aix_rs6000_64/ /
Solaris	<DIRINSTALL>/sap_bobj/enterprise_xi40/solaris_sparcv9/ cv9/
Linux	<DIRINSTALL>/sap_bobj/enterprise_xi40/linux_x64/

Nota:

La chiave cluster per un determinato nodo non può essere recuperata dal file `dbinfo`. Si consiglia agli amministratori del sistema di adottare con estrema precisione e attenzione le misure necessarie per proteggere le chiavi cluster.

Solo gli utenti con privilegi amministrativi possono reimpostare le chiavi cluster. Se richiesto, utilizzare CCM per reimpostare la chiave cluster per ogni nodo della distribuzione. Le nuove chiavi cluster vengono automaticamente utilizzate per il wrapping delle chiavi di crittografia presenti nel repository CMS.

8.12.1.1 Reimpostazione della chiave cluster in Windows

Prima di reimpostare la chiave cluster per il nodo, assicurarsi che tutti i server gestiti dall'agente SIA risultino interrotti.

1. Per avviare CCM, passare a **Programmi > SAP Business Intelligence > Piattaforma SAP BusinessObjects BI 4 > Central Configuration Manager**.
2. In CCM fare clic con il pulsante destro del mouse su Server Intelligence Agent (SIA) e scegliere **Arresta**.

Avvertenza:

Non procedere con il passaggio 3 fino a quando lo stato SIA non è contrassegnato come Interrotto.

3. Fare clic con il pulsante destro del mouse su Server Intelligence Agent (SIA) e scegliere **Proprietà**. Viene visualizzata la finestra di dialogo "Proprietà".
4. Fare clic sulla scheda **Configurazione**.
5. Fare clic su **Modifica** in "Configurazione chiave cluster CMS". Viene visualizzato un messaggio di avviso.
6. Fare clic su **Sì** per continuare. Viene visualizzata la finestra di dialogo "Modifica chiave cluster".
7. Immettere la stessa chiave di otto caratteri nei campi **Nuova chiave cluster** e **Conferma nuova chiave cluster**.

Nota:

in Windows, le chiavi cluster devono contenere una combinazione di caratteri maiuscoli e minuscoli. In alternativa, gli utenti possono anche generare una chiave casuale, che risulta necessaria per la conformità a FIPS.

8. Fare clic su **OK** per inviare la nuova chiave cluster al sistema.
Viene visualizzato un messaggio che conferma che la chiave cluster è stata reimpostata correttamente.
9. Riavviare il SIA.

In un cluster a più nodi, è necessario reimpostare le chiavi cluster per tutti gli agenti SIA della distribuzione della piattaforma BI sulla nuova chiave.

8.12.1.2 Reimpostazione della chiave cluster in UNIX

Prima di reimpostare la chiave cluster per un nodo, assicurarsi che tutti i server gestiti dal nodo siano stati interrotti.

1. Passare alla directory `<DIRINSTALLAZ>/sap_bobj`.
2. Digitare `./cmsdbsetup.sh` e premere **Invio**.
Verrà visualizzata la schermata "Informazioni sul database CMS".
3. Digitare il nome del nodo e premere **Invio**.
4. Digitare 2 per modificare la chiave cluster.
Viene visualizzato un messaggio di avviso.
5. Selezionare **Si** per continuare.
6. Digitare nel campo visualizzato una nuova chiave cluster di otto caratteri e premere **Invio**.

Nota:

Sulle piattaforme UNIX, una chiave cluster valida contiene qualsiasi combinazione di otto caratteri senza restrizioni.

7. Immettere nuovamente la nuova chiave cluster nel campo visualizzato e premere **Invio**.
Viene visualizzato un messaggio che indica che la chiave cluster è stata correttamente reimpostata.
8. Riavviare il nodo.

È necessario reimpostare tutti i nodi nella distribuzione della piattaforma BI per utilizzare la stessa chiave cluster.

8.12.2 Responsabili crittografia

Per gestire le chiavi di crittografia nella console CMC è necessario essere membri del gruppo Responsabili crittografia. L'account Administrator predefinito creato per la piattaforma BI è anche membro del gruppo Responsabili crittografia. Utilizzare questo account per aggiungere utenti al gruppo Responsabili crittografia secondo le esigenze. Si consiglia di limitare il numero di utenti a cui viene concessa l'appartenenza al gruppo.

Nota:

quando gli utenti vengono aggiunti al gruppo Amministratori, non ereditano i diritti richiesti per eseguire attività di gestione per le chiavi di crittografia.

8.12.2.1 Aggiunta di un utente al gruppo Responsabili crittografia

Per aggiungere un account utente al gruppo Responsabili crittografia, è necessario che l'account esista nella piattaforma BI.

Nota:

Per poter aggiungere un utente al gruppo Responsabili crittografia, è necessario essere membro sia del gruppo Amministratori sia del gruppo Responsabili crittografia.

1. Nell'area di gestione "Utenti e gruppi" della console CMC, selezionare il gruppo **Responsabili crittografia**.
2. Scegliere **Azioni > Aggiungi membri al gruppo**.
Viene visualizzata la finestra di dialogo "Aggiungi".
3. Fare clic su **Elenco utenti**.
L'elenco **Utenti o gruppi disponibili** viene aggiornato e vengono visualizzati tutti gli account utente del sistema.
4. Spostare l'account utente che si desidera aggiungere al gruppo Responsabili crittografia dall'elenco **Utenti o gruppi disponibili** all'elenco **Utenti o gruppi selezionati**.

Suggerimento:

per cercare un utente specifico, utilizzare il campo di ricerca.

5. Fare clic su **OK**.

Come membro del gruppo Responsabili crittografia, l'account appena aggiunto potrà accedere all'area di gestione "Chiavi di crittografia" della console CMC.

8.12.2 Visualizzazione delle chiavi di crittografia in CMC

L'applicazione CMC contiene un'area di gestione dedicata per le chiavi di crittografia utilizzate dal sistema della piattaforma BI. L'accesso a tale area è riservato ai membri del gruppo Responsabili crittografia.

1. Per avviare la CMC, fare clic su **Programmi > SAP Business Intelligence > Piattaforma SAP BusinessObjects BI 4 > Central Management Console della piattaforma SAP BusinessObjects BI**.

Viene visualizzata la home page della CMC.

2. Fare clic sulla scheda **Chiavi di crittografia**.

Viene visualizzata l'area di gestione "Chiavi di crittografia".

3. Fare doppio clic sulla chiave di crittografia per cui si richiedono ulteriori dettagli.

Argomenti correlati

- [Visualizzazione di oggetti associati a una chiave di crittografia](#)

8.12.3 Gestione delle chiavi di crittografia in CMC

I responsabili della crittografia utilizzano l'area di gestione "Chiavi di crittografia" per esaminare, generare, disattivare, revocare ed eliminare le chiavi utilizzate per proteggere i dati sensibili archiviati nel repository CMS.

Tutte le chiavi di crittografia attualmente definite nel sistema vengono elencate nell'area di gestione "Chiavi di crittografia". Le informazioni di base per ogni chiave vengono fornite sotto le intestazioni descritte nella tabella seguente:

Intestazione	Descrizione
Titolo	Nome che identifica la chiave di crittografia
Stato	Stato corrente della chiave
Ultima modifica stato	Indicatore di data e ora relativo all'ultima modifica associata alla chiave di crittografia
Oggetti	Numero di oggetti associati alla chiave

Argomenti correlati

- [Stato delle chiavi di crittografia](#)

- [Creazione di una nuova chiave di crittografia](#)
- [Eliminazione di una chiave di crittografia dal sistema](#)
- [Revoca di una chiave di crittografia](#)
- [Visualizzazione di oggetti associati a una chiave di crittografia](#)
- [Contrassegno delle chiavi di crittografia come compromesse](#)

8.12.3.1 Stato delle chiavi di crittografia

Nella tabella che segue vengono indicate tutte le opzioni possibili dello stato delle chiavi di crittografia nella piattaforma BI:

Stato	Descrizione
Active	È possibile designare come "Attiva" solo una chiave di crittografia del sistema. Tale chiave viene utilizzata per la crittografia dei dati sensibili che verranno archiviati nel database CMS. La chiave viene utilizzata anche per la decrittazione di tutti gli oggetti che appaiono nell'Elenco degli oggetti. Una volta creata una nuova chiave di crittografia, lo stato "Attiva" diventa "Disattivato". Una chiave attiva non può essere eliminata dal sistema.
Disattivata	Una chiave "disattivata" non può più essere utilizzata per la crittografia dei dati. Può comunque essere utilizzata per decrittare tutti gli oggetti che appaiono nell'elenco di oggetti. Non è possibile riattivare una chiave se è stata disattivata. Una chiave contrassegnata come "disattivata" non può essere eliminata dal sistema. Per eliminare una chiave, è necessario prima contrassegnarla come "revocata".
Compromesso	Una chiave di crittografia che si ritiene non protetta può essere contrassegnata come compromessa. Contrassegnando una chiave di questo tipo, in un secondo tempo sarà possibile crittografare di nuovo gli oggetti di dati ancora associati alla chiave. Una volta contrassegnata una chiave come compromessa, sarà necessario revocarla per poterla eliminare dal sistema..
Revocato	Quando una chiave di crittografia viene revocata, viene avviato un processo in cui tutti gli oggetti attualmente associati alla chiave vengono nuovamente crittografati con la chiave di crittografia "Attiva" corrente. Una volta revocata, una chiave può essere eliminata dal sistema senza problemi. Il meccanismo di revoca assicura che i dati presenti nel database CMS possano essere decrittati. Non è possibile riattivare in alcun modo una chiave revocata.

Stato	Descrizione
Disattivato: nuova crittografia in corso	Indica che la chiave di crittografia è in fase di revoca. Al termine del processo, la chiave verrà contrassegnata con "Revocato".
Disattivato: nuova crittografia sospesa	Indica che il processo di revoca di una chiave di crittografia è stato sospeso. Ciò normalmente accade se il processo viene esplicitamente sospeso o se un oggetto dati associato alla chiave non è disponibile.
Revocato-Compromesso	Si assegna a una chiave il flag Revocato-Compromesso se la chiave è stata contrassegnata come compromessa e tutti i dati in precedenza associati ad essa sono stati crittografati con un'altra chiave. Quando una chiave "disattivata" viene contrassegnata come compromessa, è possibile non intraprendere alcuna azione o revocare la chiave. Una volta revocata, la chiave compromessa può essere eliminata.

8.12.3.2 Visualizzazione di oggetti associati a una chiave di crittografia

1. Selezionare la chiave nell'area di gestione "Chiavi di crittografia" della console CMC.
2. Fare clic su **Gestisci > Proprietà**.
Viene visualizzata la finestra di dialogo "Proprietà" della chiave di crittografia.
3. Fare clic su "Elenco di oggetti" nel riquadro di spostamento a sinistra nella finestra di dialogo "Proprietà".
Tutti gli oggetti associati alla chiave di crittografia sono elencati a destra nel riquadro di spostamento.

Suggerimento:

utilizzare le funzioni di ricerca per cercare un oggetto specifico.

8.12.3.3 Creazione di una nuova chiave di crittografia

Avvertenza:

Quando si crea una nuova chiave di crittografia, il sistema disattiva automaticamente la chiave attualmente "attiva". Una volta disattivata, una chiave non può più essere ripristinata come chiave "attiva".

1. Nell'area di gestione "Chiavi di crittografia" della console CMC, fare clic su **Gestisci > Nuovo > Chiave di crittografia**.
Viene visualizzata la finestra di dialogo "Crea nuova chiave di crittografia".
2. Fare clic su **Continua** per creare la nuova chiave di crittografia.

3. Digitare il nome e una descrizione della nuova chiave di crittografia, quindi fare clic su **OK** per salvare le informazioni.

La nuova chiave viene indicata come unica chiave attiva nell'area di gestione "Chiavi di crittografia". La chiave "attiva" precedente è ora contrassegnata come "disattivata".

Tutti i nuovi dati sensibili generati e archiviati nel database CMS vengono crittografati con la nuova chiave di crittografia. È possibile revocare la chiave precedente e crittografare nuovamente gli oggetti dati utilizzando la nuova chiave attiva.

8.12.3.4 Contrassegno delle chiavi di crittografia come compromesse

È possibile contrassegnare una chiave di crittografia come compromessa se per qualche motivo la chiave non viene più considerata sicura. L'operazione è utile ai fini del rilevamento dei dati ed è possibile procedere all'identificazione degli oggetti dati associati alla chiave. Una chiave di crittografia deve essere disattivata per poter essere contrassegnata come compromessa.

Nota:

è inoltre possibile contrassegnare una chiave come compromessa dopo la revoca.

1. Passare all'area di gestione "Chiavi di crittografia" della CMC.
2. Selezionare la chiave di crittografia da contrassegnare come compromessa.
3. Fare clic su **Azioni > Contrassegna come compromessa**.
Viene visualizzata la finestra di dialogo "Contrassegna come compromessa".
4. Fare clic su **Continua**.
5. Selezionare una delle opzioni seguenti dalla finestra di dialogo "Contrassegna come compromessa":
 - **Si**: avvia il processo per crittografare nuovamente tutti gli oggetti dati associati alla chiave compromessa.
 - **No**: la finestra di dialogo "Contrassegna come compromessa" viene chiusa e la chiave di crittografia viene contrassegnata come "compromessa" nell'area di gestione "Chiavi di crittografia".

Nota:

se si seleziona **No**, i dati sensibili continueranno a essere associati alla chiave compromessa. La chiave compromessa verrà utilizzata dal sistema per decrittare gli oggetti associati.

Argomenti correlati

- [Revoca di una chiave di crittografia](#)
- [Stato delle chiavi di crittografia](#)
- [Visualizzazione di oggetti associati a una chiave di crittografia](#)

8.12.3.5 Revoca di una chiave di crittografia

Una chiave di crittografia disattivata può comunque essere utilizzata dagli oggetti dati associati alla stessa. Per interrompere l'associazione tra gli oggetti crittografati e la chiave disattivata, è necessario revocare la chiave.

1. Selezionare la chiave da revocare dall'elenco di chiavi dell'area di gestione "Chiavi di crittografia".
2. Fare clic su **Azioni > Revoca**.
Viene visualizzata la finestra di dialogo "Revoca".
3. Fare clic su **OK**.

Viene avviato un processo per crittografare tutti gli oggetti della chiave in base alla chiave attiva corrente. Se la chiave è associata a molti oggetti dati, verrà contrassegnata come "Disattivato: nuova crittografia in corso" finché il processo di crittografia non viene completato.

Una volta revocata, la chiave di crittografia può essere rimossa dal sistema senza alcun problema, poiché non vi sono oggetti dati sensibili che richiedono la chiave per la decrittazione.

8.12.3.6 Eliminazione di una chiave di crittografia dal sistema

Prima di eliminare una chiave di crittografia dalla piattaforma BI, è necessario verificare che nessun oggetto dati presente nel sistema la richieda. Tale restrizione assicura che tutti i dati sensibili archiviati nel repository CMS possano sempre essere decrittati.

Dopo avere revocato correttamente una chiave di crittografia, utilizzare le istruzioni seguenti per eliminare la chiave dal sistema.

1. Passare all'area di gestione "Chiavi di crittografia" della CMC.
2. Selezionare la chiave di crittografia da eliminare.
3. Scegliere **Gestisci > Elimina**.
Viene visualizzata la finestra di dialogo "Elimina".
4. Fare clic su **Elimina** per rimuovere la chiave di crittografia dal sistema.

La chiave eliminata non è più visualizzata nell'area di gestione "Chiavi di crittografia" della CMC.

Nota:

Una volta eliminata dal sistema, la chiave di crittografia non può più essere ripristinata.

Argomenti correlati

- [Revoca di una chiave di crittografia](#)
- [Stato delle chiavi di crittografia](#)

8.13 Configurazione dei server per SSL

È possibile utilizzare il protocollo Secure Sockets Layer (SSL) per tutte le comunicazioni di rete tra client e server presenti nella distribuzione della piattaforma BI.

Per impostare SSL per tutte le comunicazioni server è necessario procedere come segue:

- Distribuire la piattaforma BI con il protocollo SSL abilitato.
- Creare file di chiavi e certificati per ogni computer della distribuzione.
- Configurare la posizione di questi file nel Central Configuration Manager (CCM) e nel server delle applicazioni Web.
- In alternativa, configurare SSL per i certificati che vengono gestiti da un'autorità di certificazione.

Nota:

Se si utilizzano thick client, ad esempio Crystal Reports, e si prevede di utilizzarli per la connessione al CMS, sarà anche necessario configurare tali client per SSL. In caso contrario, si riceverà un messaggio di errore se si tenta di connettersi a un CMS configurato per SSL da un thick client con una configurazione diversa.

8.13.1 Creazione di file di chiavi e certificati

Per impostare il protocollo SSL per la comunicazione del server, utilizzare lo strumento da riga di comando SSLC per creare un file di chiavi e un file di certificato per ciascun computer della distribuzione.

Nota:

- è necessario creare certificati e chiavi per tutti i computer nella distribuzione in rete, inclusi quelli su cui sono installati componenti "thick client" come, ad esempio, Crystal Reports. Per i computer client utilizzare lo strumento da riga di comando `sslconfig` per eseguire la configurazione.
- per ottenere la massima protezione, tutte le chiavi private devono essere protette e non possono essere trasferite utilizzando canali di comunicazione non protetti.
- I certificati creati per le versioni precedenti della piattaforma BI non funzioneranno per la piattaforma SAP BusinessObjects Business Intelligence 4.0. Sarà necessario ricreare tali certificati.

8.13.1.1 Per creare file di chiavi e certificati per un computer

1. Eseguire lo strumento da riga di comando `sslc`.

Lo strumento SSLC viene installato con il software della piattaforma BI. Ad esempio, in Windows viene installato per impostazione predefinita in `<DIRINSTALLAZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64.`)

2. Immettere il comando seguente:

```
sslc req -config sslc.cnf -new -out cacert.req
```

Questo comando crea due file, una richiesta di certificazione di un'autorità di certificazione (`cacert.req`) e una chiave privata (`privkey.pem`).

3. Per decrittografare la chiave privata, immettere il seguente comando:

```
sslc rsa -in privkey.pem -out cakey.pem
```

Questo comando crea la chiave decrittografata `cakey.pem`.

4. Per firmare il certificato CA, immettere il seguente comando:

```
sslc x509 -in cacert.req -out cacert.pem -req -signkey cakey.pem -days 365
```

Questo comando crea un certificato a firma automatica, `cacert.pem`, che scade dopo 365 giorni. Scegliere il numero di giorni adatto alle esigenze di protezione specifiche.

5. Utilizzando un editor di testo, aprire il file `sslc.cnf`, disponibile nella stessa cartella dello strumento da riga di comando SSLC.

Nota:

È necessario utilizzare un editor di testo per Windows in quanto Windows Explorer potrebbe non riconoscere e visualizzare correttamente i file con estensione `.cnf`.

6. Eseguire le operazioni seguenti, in base alle impostazioni del file `sslc.cnf`:

- a. Posizionare i file `cakey.pem` e `cacert.pem` nelle directory specificate dalle opzioni `certificate` e `private_key` del file `sslc.cnf`. Per impostazione predefinita, le impostazioni nel file `sslc.cnf` sono:

```
certificate = $dir/cacert.pem
```

```
private_key = $dir/private/cakey.pem
```

- b. Creare il file con il nome specificato dall'impostazione `database` del file `sslc.cnf`.

Nota:

Per impostazione predefinita, il file si chiama `$dir/index.txt` e deve essere vuoto.

- c. Creare il file con il nome specificato dall'impostazione `seriale` del file `sslc.cnf`.

Tale file deve fornire un numero di serie con una stringa di ottetti (in formato esadecimale).

Nota:

per accertarsi di poter creare e firmare più certificati, scegliere un numero esadecimale alto con un numero pari di cifre, ad esempio `11111111111111111111111111111111`.

- d. Creare la directory specificata dall'impostazione `new_certs_dir` del file `sslc.cnf`.

7. Per creare una richiesta di certificato e una chiave privata, immettere il seguente comando:

```
sslc req -config sslc.cnf -new -out servercert.req
```

I file dei certificati e delle chiavi che sono stati generati si trovano nella cartella di lavoro corrente.

8. Per decrittografare la chiave nel file `privkey.pem`, immettere il seguente comando:

```
sslc rsa -in privkey.pem -out server.key
```

9. Per firmare il certificato con il certificato CA, immettere il seguente comando:

```
sslc ca -config sslc.cnf -days 365 -out servercert.pem -in servercert.req
```

Questo comando crea il file `servercert.pem`, che contiene il certificato firmato.

10. Utilizzare i comandi seguenti per convertire i certificati in certificati DER codificati:

```
sslc x509 -in cacert.pem -out cacert.der -outform DER
```

```
sslc x509 -in servercert.pem -out servercert.der -outform DER
```

Nota:

È necessario generare il certificato CA (`cacert.der`) e la relativa chiave privata (`cakey.pem`) una sola volta per ciascuna distribuzione. Tutti i computer nella stessa distribuzione condividono gli stessi certificati CA. Tutti gli altri certificati devono essere firmati tramite la chiave privata di un qualsiasi certificato CA.

11. Creare un file di testo (`passphrase.txt`) per memorizzare la `password` lunga di testo normale utilizzata per decrittare la chiave privata generata.

12. Archiviare i seguenti file di chiavi e certificati in un luogo sicuro (nella stessa directory) accessibile dai computer della distribuzione della piattaforma BI:

- Il file del certificato attendibile (`cacert.der`)
- Il file del certificato del server generato (`servercert.der`)
- Il file della chiave del server (`server.key`)
- Il file della passphrase (`passphrase.txt`)

Questa posizione sarà utilizzata per configurare il protocollo SSL per il CCM e il server delle applicazioni Web.

8.13.2 Impostazione di SSL quando il certificato viene gestito da un'autorità di certificazione

Quando si imposta SSL per le comunicazioni con i server, attenersi alla procedura che segue se il certificato è gestito da un'autorità di certificazione.

1. Esportare il certificato desiderato con la chiave privata nel formato PKCS #12 (.PFX).

Il file verrà utilizzato come certificato per l'autorità di certificazione.

2. Utilizzando OpenSSL, eseguire i comandi seguenti:

- a. Esportare il file della chiave privata dal file `.pfx`:

```
openssl pkcs12 -in filename.pfx -nocerts -out privkey.pem
```

b. Esportare il file di certificato dal file .pfx:

```
openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cacert.pem
```

c. Rimuovere la passphrase dalla chiave privata:

```
openssl rsa -in privkey.pem -out cakey.pem
```

3. Impostare alcuni file richiesti:

- Copiare il file `cakey.pem` in `C:\SSL\private\cakey.pem`.
- Copiare il file `cacert.pem` in `C:\SSL\cacert.pem`.
- Creare un file di testo vuoto (un file di indice di database) denominato `index.txt` nella cartella `C:\SSL`.
- Creare un altro file di testo: `C:\SSL\serial`.
- Aprire il file `C:\SSL\serial` in un editor di testo, digitare il valore seguente e salvare il file:
`11111111111111111111`

4. In un editor di testo aprire il file `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86\sslc.cnf`.

Scegliere una delle opzioni seguenti:

- Modificare il valore della variabile `policy` in `policy_anything`. Questa modifica consente di creare un certificato server che non presenta le stesse policy del certificato dell'autorità di certificazione.
- In alternativa, mantenere inalterato il valore della variabile `policy` come `policy_match`. Questo forzerà la presenza nel certificato server delle stesse policy del certificato dell'autorità di certificazione. In questo caso, potrebbe essere necessario modificare le proprietà `req_distinguished_name` nel modo appropriato.

5. Creare una richiesta di certificato e una chiave privata.

In un prompt dei comandi eseguire il comando seguente:

```
sslc req -config sslc.cnf -new -out servercert.req
```

Nota:

- Per `passphrase PEM`, digitare una password con almeno quattro caratteri.
- Per `Common Name`, digitare il nome di dominio completo del computer sul quale sono in esecuzione i server della piattaforma BI.
- Il file `servercert.req` viene creato in `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.
- I file `.rnd` e `privkey.pem` vengono modificati.

6. Decrittografare la chiave privata.

```
sslc rsa -in privkey.pem -out server.key
```

7. Firmare il certificato.

```
sslc ca -config sslc.cnf -days 365 -out servercert.pem -in servercert.req
```

Nota:

- Il file `servercert.pem` viene creato in `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.

- Il file `11111111111111111111.pem` viene creato in `C:\SSL\newcerts`.
- Viene creato un backup del file `serial`, denominato `serial.old`.
- Il valore di `serial` viene incrementato da `11111111111111111111` a `11111111111111111112`.

8. Convertire i certificati utilizzando la codifica DER.

Eeguire i comandi seguenti:

```
sslcert x509 -in cacert.pem -out cacert.der -outform DER
sslcert x509 -in servercert.pem -out servercert.der -outform DER
```

Nota:

- Il file `servercert.der` viene creato in `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.
- Il file `cacert.der` viene creato in `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.

9. Creare un file di testo denominato `passphrase.txt`.

Il contenuto del file deve essere la passphrase PEM utilizzata in precedenza.

10. Archiviare i seguenti file in una posizione sicura, ad esempio `C:\SSLCerts`.

- il file del certificato attendibile `cacert.der`
- il file del certificato del server generato `servercert.der`
- il file della chiave del server `server.key`
- il file della passphrase `passphrase.txt`

8.13.3 Configurazione del protocollo SSL

Dopo aver creato le chiavi e i certificati per ciascuna macchina nella distribuzione e averli memorizzati in una posizione sicura, è necessario indicare al Central Configuration Manager (CCM) e al server delle applicazioni Web tale posizione.

È inoltre necessario effettuare operazioni specifiche per configurare il protocollo SSL per il server di applicazioni Web e per qualsiasi computer che esegua un'applicazione thick client.

8.13.3.1 Per configurare il protocollo SSL nel CCM

1. In CCM, fare clic con il pulsante destro del mouse su Server Intelligence Agent e scegliere **Proprietà**.
2. Nella finestra di dialogo Proprietà, fare clic sulla scheda **Protocollo**.
3. Verificare che l'opzione **Abilita SSL** sia selezionata.
4. Fornire il percorso dei file per la directory in cui sono stati memorizzati i file delle chiavi e dei certificati.

Campo	Descrizione
Cartella certificati SSL	Cartella in cui sono archiviati tutti i file e i certificati SSL richiesti, Ad esempio: <code>d:\ssl</code>
File di certificato SSL server	Nome del file utilizzato per archiviare il certificato SSL server; Per impostazione predefinita, <code>servercert.der</code>
File dei certificati SSL attendibili	Nome del file con il certificato SSL attendibile; per impostazione predefinita <code>cacert.der</code> .
File chiave privata SSL	Nome del file della chiave privata SSL utilizzata per accedere al certificato. per impostazione predefinita <code>server.key</code> .
File della passphrase della chiave privata	Nome del file di testo contenente la passphrase utilizzata per accedere alla chiave privata; per impostazione predefinita <code>passphrase.txt</code> .

Nota:

Verificare di indicare la directory per il computer sul quale è in esecuzione il server.

8.13.3.2 Configurazione del protocollo SSL in Unix

Per configurare il protocollo SSL per un SIA è necessario utilizzare lo script `serverconfig.sh`. Questo script fornisce un programma basato su testo che consente di visualizzare informazioni sui server e di aggiungere ed eliminare server dall'installazione. Lo script `serverconfig.sh` viene installato nella directory `sap_bobj` dell'installazione.

1. Utilizzare lo script `ccm.sh` per interrompere il SIA e tutti i server SAP BusinessObjects.
2. Eseguire lo script `serverconfig.sh`.
3. Selezionare **3 - Modifica nodo** e premere **Invio**.
4. Specificare il SIA di destinazione e premere **Invio**.
5. Selezionare **1 - Modifica configurazione SSL di Server Intelligence Agent**.
6. Selezionare **ssl**.
Quando richiesto, specificare le posizioni dei certificati SSL.
7. Ripetere i passaggi da 1 a 6 per ogni SIA, se la distribuzione della piattaforma BI è un cluster SIA.
8. Avviare il SIA con lo script `ccm.sh` e attendere l'avvio dei server.

8.13.3.3 Per configurare il protocollo per il server delle applicazioni Web

1. Se si dispone di un server delle applicazioni Web J2EE, eseguire Java SDK con la seguente serie di proprietà di sistema. Ad esempio:

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=d:\ssl -DtrustedCert=cacert.der -DsslCert=clientcert.der
-DsslKey=client.key
-Dpassphrase=passphrase.txt
```

La tabella seguente mostra le descrizioni degli esempi riportati:

Esempio	Descrizione
<i>DcertDir=d:\ssl</i>	La directory in cui memorizzare tutti i certificati e le chiavi.
<i>DtrustedCert=cacert.der</i>	File del certificato sicuro. Se si specificano più file, utilizzare il punto e virgola come separatore.
<i>DsslCert=clientcert.der</i>	Certificato utilizzato dall'SDK.
<i>DsslKey=client.key</i>	Chiave privata del certificato SDK.
<i>Dpassphrase=passphrase.txt</i>	Il file che memorizza la passphrase per la chiave privata.

2. Se si dispone di un server delle applicazioni Web IIS, eseguire lo strumento `sslconfig` dalla riga di comando e seguire le fasi di configurazione.

8.13.3.4 Configurazione di thick client

Prima di eseguire la procedura descritta di seguito è necessario creare e salvare tutte le risorse SSL richieste, ad esempio certificati e chiavi private, in una directory nota.

Nella procedura che segue si suppone che l'utente si sia attenuto alle istruzioni per la creazione delle risorse SSL seguenti:

Risorsa SSL	
Cartella certificati SSL	d:\ssl
Nome file di certificato SSL server	servercert.der
Nome file con certificato SSL attendibile o certificato radice	cacert.der
Nome file chiave privata SSL	server.key
File contenente la password lunga per l'accesso al file della chiave privata SSL	passphrase.txt

Dopo aver creato le risorse elencate sopra, attenersi alle istruzioni riportate di seguito per configurare applicazioni thick client come CCM (Central Configuration Manager) o lo strumento Upgrade Management Tool.

1. Assicurarsi che l'applicazione thick client non sia in esecuzione.

Nota:

Verificare di indicare la directory per il computer sul quale è in esecuzione il server.

2. Eseguire lo strumento da riga di comando `sslconfig.exe`.

Lo strumento SSLC viene installato con il software della piattaforma BI. Ad esempio, in Windows viene installato per impostazione predefinita in <DIRINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64.

3. Eseguire il seguente comando:

```
sslconfig.exe -dir d:\SSL -mycert servercert.der -rootcert cacert.der -mykey server.key
-passphrase passphrase.txt -protocol ssl
```

4. Riavviare l'applicazione thick client.

Argomenti correlati

- [Per creare file di chiavi e certificati per un computer](#)

8.13.3.4.1 Per configurare l'accesso SSL per Translation Management Tool

Per consentire agli utenti l'utilizzo dell'accesso SSL con Translation Management Tool, è necessario aggiungere informazioni sulle risorse SSL al file di configurazione dello strumento (.ini).

1. Individuare il file `TransMgr.ini` nella directory seguente: `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\win32_x86`.
2. Utilizzando un editor di testo, aprire il file `TransMgr.ini`.
3. Aggiungere i parametri seguenti:

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=D:\SSLCert
-DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key
-Dpassphrase=passphrase.txt -jar program.jar
```

4. Salvare il file e chiudere l'editor di testo.

Gli utenti possono ora utilizzare SSL per accedere allo strumento Translation Management Tool.

8.13.3.4.2 Configurazione di SSL per lo Strumento di conversione dei report

Prima di eseguire la procedura descritta di seguito è necessario creare e salvare tutte le risorse SSL richieste, ad esempio certificati e chiavi private, in una directory nota. È inoltre necessario che lo Strumento di conversione dei report venga installato durante la distribuzione della piattaforma BI.

Nella procedura che segue si suppone che l'utente si sia attenuto alle istruzioni per la creazione delle risorse SSL seguenti:

Risorsa SSL	
Cartella certificati SSL	d:\ssl
Nome file di certificato SSL server	servercert.der
Nome file con certificato SSL attendibile o certificato radice	cacert.der
Nome file chiave privata SSL	server.key
File contenente la password lunga per l'accesso al file della chiave privata SSL	passphrase.txt

Dopo aver creato le risorse elencate sopra, attenersi alle istruzioni seguenti per configurare SSL per l'utilizzo dello Strumento di conversione dei report.

1. Creare una variabile di ambiente Windows `BOBJ_MIGRATION` sul computer che ospita lo Strumento di conversione dei report.

Suggerimento:

è possibile impostare tale variabile su qualsiasi valore.

2. Utilizzando un editor di testo, aprire il file `migration.bat` nella directory seguente:

```
<DIRINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\scripts\.
```

3. Individuare la riga seguente:

```
start "" "%JRE%\bin\javaw" -cp migration.jar;* -Xmx512m -Xss10m com.bo.migration.MigrationTool
```

4. Aggiungere la sintassi seguente al parametro `-Xss10m`:

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=d:\ssl
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
-Dbusinessobjects.migration
```

Nota:

Verificare che ci sia uno spazio tra ogni parametro e nessuno spazio alla fine delle righe.

5. Salvare il file e chiudere l'editor di testo.

Gli utenti possono ora utilizzare SSL per accedere allo Strumento di conversione dei report.

Argomenti correlati

- [Per creare file di chiavi e certificati per un computer](#)

8.14 Informazioni sulla comunicazione tra componenti della piattaforma BI

Se la piattaforma BI viene interamente distribuita sulla stessa subnet protetta, non è necessario eseguire configurazioni particolari dei firewall. È tuttavia possibile scegliere i distribuire alcuni componenti su subnet diverse separate da uno o più firewall.

È importante comprendere la comunicazione tra server della piattaforma BI, rich client e il server di applicazioni Web che ospita l'SDK di SAP BusinessObjects prima di configurare il sistema per l'utilizzo dei firewall.

Argomenti correlati

- [Configurazione della piattaforma BI per i firewall](#)
- [Esempi di scenari di firewall tipici](#)

8.14.1 Panoramica dei server della piattaforma BI e delle porte di comunicazione

È importante comprendere i server della piattaforma BI e le relative porte di comunicazione se il sistema viene distribuito con firewall.

8.14.1.1 Ogni server della piattaforma BI è associato a una porta di richiesta

Ogni server della piattaforma BI, ad esempio Input File Repository Server, è associato all'avvio a una porta di richiesta. Altri componenti della piattaforma BI, tra cui server, rich client e l'SDK ospitato nel server di applicazioni Web, possono utilizzare questa porta di richiesta per la comunicazione con il server.

Un server selezionerà il relativo numero della porta di richiesta in modo dinamico, a meno che non venga configurato per l'utilizzo di un numero di porta specifico. È necessario configurare manualmente un numero di porta specifico per i server che comunicano con altri componenti della piattaforma BI attraverso un firewall.

8.14.1.2 Ogni server della piattaforma BI viene registrato con il CMS

I server della piattaforma BI vengono registrati con il server CMS all'avvio. Quando un server viene registrato, il server CMS registra:

- Il nome host, o l'indirizzo IP, del computer host del server.
- Il numero della porta di richiesta specifico del server.

8.14.1.3 Porte utilizzate dal server CMS

Il server CMS utilizza due porte: la porta richiesta e la porta del server dei nomi. La porta di richiesta viene selezionata in modo dinamico per impostazione predefinita. La porta del server dei nomi è la 6400 per impostazione predefinita.

Tutti i server e le applicazioni client della piattaforma BI contatteranno inizialmente il server CMS sulla relativa porta del server dei nomi. Il server CMS risponderà a questo contatto iniziale restituendo il valore della relativa porta di richiesta. I server utilizzeranno questa porta richiesta per le comunicazioni successive con il server CMS.

8.14.1.4 Directory del Central Management Server (CMS) di servizi registrati

Il server CMS fornisce una directory dei servizi per i quali è registrato. Altri componenti della piattaforma BI, quali servizi Web, rich client e l'SDK ospitato nel server di applicazioni Web possono contattare il server CMS e richiedere un riferimento a un determinato servizio. Un riferimento a un servizio contiene il numero di porta richiesta del servizio, il nome host (o indirizzo IP) del computer host e l'ID del server.

I componenti della piattaforma BI potrebbero risiedere in una subnet diversa rispetto al server utilizzato. Il nome host (o indirizzo IP) contenuto nel riferimento al servizio deve essere instradabile dal computer del componente.

Nota:

il riferimento a un server della piattaforma BI contiene per impostazione predefinita il nome host del computer server. Se un computer presenta più nomi host, viene scelto quello principale. È possibile configurare un server affinché il relativo riferimento contenga l'indirizzo IP.

Argomenti correlati

- [Comunicazione tra componenti della piattaforma BI](#)

8.14.1.5 Gli agenti SIA comunicano con il server CMS

La distribuzione non funziona se l'agente SIA e il server CMS non possono comunicare tra loro. Verificare che le porte del firewall siano configurate in modo da consentire la comunicazione tra tutti i SIA e tutti i CMS nel cluster.

8.14.1.6 I processi secondari di Job Server comunicano con il livello dati e il server CMS

La maggior parte dei Job Server creano un processo secondario per gestire un task come la generazione di un report. Job Server crea uno o più processi secondari. Ogni processo secondario dispone di una propria porta di richiesta.

Per impostazione predefinita, Job Server seleziona in modo dinamico una porta di richiesta per ogni processo secondario. È possibile specificare un intervallo di numeri di porta selezionabili.

Tutti i processi secondari comunicano con il server CMS. Se la comunicazione attraverso un firewall, è necessario:

- Specificare l'intervallo di numeri di porta tra cui il Job Server può scegliere aggiungendo i parametri `-requestJSChildPortsporta più bassa-porta più alta` e `-requestPortporta` alla riga di comando del server. L'intervallo delle porte deve essere sufficientemente ampio per consentire il numero massimo di processi secondari come specificato da `-maxJobs`.
- Aprire l'intervallo di porte specificato sul firewall.

Molti processi secondari comunicano con il livello di dati. Ad esempio, un processo secondario potrebbe connettersi a un database di reporting, estrarre dati e calcolare valori per un report. Se il processo secondario di Job Server comunica con il livello di dati attraverso un firewall, è necessario:

- Aprire un percorso di comunicazione sul firewall da qualsiasi porta sul computer Job Server verso la porta di attesa del database sul computer server del database.

Argomenti correlati

- [Panoramica sulle righe di comando](#)

8.14.2 Comunicazione tra componenti della piattaforma BI

I componenti della piattaforma BI, ad esempio client browser, rich client, server e SDK ospitato nel server di applicazioni Web, comunicano tra loro nella rete durante i normali workflow. È necessario comprendere i workflow per distribuire i prodotti SAP Business Objects su subnet diverse separate da un firewall.

8.14.2.1 Requisiti per la comunicazione tra i componenti della piattaforma BI

Le distribuzioni della piattaforma BI devono rispettare questi requisiti generali.

1. Ogni server deve essere in grado di avviare la comunicazione con tutti gli altri server della piattaforma BI sulla relativa porta di richiesta.
2. Il Central Management Server utilizza due porte. Ogni server della piattaforma BI, rich client e il server di applicazioni Web che ospita l'SDK devono essere in grado di avviare la comunicazione con il CMS su entrambe le porte.
3. Ogni processo del Job Server secondario deve essere in grado di comunicare con il server CMS.
4. I thick client devono essere in grado di avviare la comunicazione con la porta richiesta dell'Input e dell'Output File Repository Server.
5. Se è abilitato il controllo per i thick client e le applicazioni Web, è necessario poter avviare la comunicazione con la porta richiesta dell'Adaptive Processing Server che ospita il servizio proxy controllo client.
6. In generale, il server di applicazioni Web che ospita l'SDK deve essere in grado di comunicare con la porta di richiesta di ogni server della piattaforma BI.

Nota:

il server di applicazioni Web deve unicamente poter comunicare con i server della piattaforma BI utilizzati nella distribuzione. Se ad esempio Crystal Reports non viene utilizzato, non è necessario che il server di applicazioni Web comunichi con i cache server Crystal Reports.

7. I Job Server utilizzano i numeri di porta specificati con il comando `-requestJSChildPorts porta più bassa-porta più alta`. Se non vengono specificati intervalli nella riga di comando, i server utilizzano numeri di porta casuali. Per consentire a un Job Server di comunicare con un server CMS, FTP o di posta su un altro computer, aprire tutte le porte dell'intervallo specificato da `-requestJSChildPorts` nel firewall.
8. Il server CMS deve essere in grado di comunicare con la porta di attesa del database CMS.
9. Il Connection Server, la maggior parte dei processi secondari dei Job Server e ogni server di elaborazione del database di sistema e di controllo devono essere in grado di avviare la comunicazione con la porta di attesa del database di creazione report.

Argomenti correlati

- [Requisiti di porta della piattaforma BI](#)

8.14.2.2 Requisiti di porta della piattaforma BI

In questa sezione sono elencate le porte di comunicazione utilizzate dai server della piattaforma BI, dai thick client, dal server di applicazioni Web che ospita l'SDK e dalle applicazioni software di terze parti. Se si distribuisce la piattaforma BI con i firewall, è possibile utilizzare queste informazioni per aprire il numero minimo di porte in tali firewall.

8.14.2.2.1 Requisiti di porta per le applicazioni della piattaforma BI

In questa tabella sono elencati i server e i numeri di porta utilizzati dalle applicazioni della piattaforma BI.

Prodotto	Applica- zione client	Server associati	Requisiti di porta del server
Crystal Re- ports	Designer di SAP Crystal Reports 2013	CMS Input FRS Output FRS Report Application Server (RAS) di Crystal Reports 2013 Server di elaborazione Crys- tal Reports 2013 Crystal Reports Cache Server	Porta server dei nomi CMS (6400 per impostazione predefinita) Porta richiesta CMS Porta richiesta Input FRS Porta richiesta Output FRS Porta richiesta del Report Application Server di Crystal Reports 2013 Porta richiesta del server di elabora- zione Crystal Reports Porta richiesta Crystal Reports Cache Server

Prodotto	Applica- zione client	Server associati	Requisiti di porta del server
Crystal Re- ports	Designer di SAP Crystal Reports for Enterprise	CMS Input FRS Output FRS Crystal Reports Processing Server Crystal Reports Cache Server	Porta server dei nomi CMS (6400 per impostazione predefinita) Porta richiesta CMS Porta richiesta Input FRS Porta richiesta Output FRS Porta richieste server di elaborazione Crystal Reports Porta richiesta Crystal Reports Cache Server
Dashboards	SAP Busine- ssObjects Dashboards	CMS Input FRS Output FRS Applicazione del provider di Servizi Web (dsws bobje.war) che ospita i ser- vizi Web Dashboards, Live Office e QaaWS richiesti per determinate connessioni all'origine dati	Porta server dei nomi CMS (6400 per impostazione predefinita) Porta richiesta CMS Porta richiesta Input FRS Porta richiesta Output FRS Porta HTTP (80 per impostazione pre- definita)
Live Office	Client Live Office	Applicazione del provider di Servizi Web (dsws bobje.war) che ospita il servizio Web Live Office	Porta HTTP (80 per impostazione pre- definita)
Piattaforma BI	SAP Busine- ssObjects Web Intelli- gence Rich Client	CMS Input FRS	Porta server dei nomi CMS (6400 per impostazione predefinita) Porta richiesta CMS Porta richiesta Input FRS

Prodotto	Applica- zione client	Server associati	Requisiti di porta del server
Piattaforma BI	Universe Design Tool	CMS Input FRS Connection Server	Porta server dei nomi CMS (6400 per impostazione predefinita) Porta richiesta CMS Porta richiesta Input FRS Porta Connection Server
Piattaforma BI	Business View Manager	CMS Input FRS	Porta server dei nomi CMS (6400 per impostazione predefinita) Porta richiesta CMS Porta richiesta Input FRS

Prodotto	Applica- zione client	Server associati	Requisiti di porta del server
Piattaforma BI	Central Co- nfiguration Manager (CCM)	CMS Server Intelligence Agent (SIA)	<p>È necessario che le seguenti porte siano aperte per consentire a CCM di gestire i server remoti della piattaforma BI:</p> <p>Porta server dei nomi CMS (6400 per impostazione predefinita)</p> <p>Porta richiesta CMS</p> <p>È necessario che le seguenti porte siano aperte per consentire a CCM di gestire i processi SIA remoti:</p> <p>Microsoft Directory Services (porta TCP 445)</p> <p>NetBIOS Session Service (porta TCP 139)</p> <p>NetBIOS Datagram Service (porta UDP 138)</p> <p>NetBIOS Name Service (porta UDP 137)</p> <p>DNS (porta TCP/UDP 53)</p> <p>(Si noti che alcune porte elencate in precedenza potrebbero non essere necessarie. Consultare l'amministratore di Windows).</p>
Piattaforma BI	Server Intelli- gence Agent (SIA)	Ogni server della piattaforma BI incluso il CMS	<p>Porta richiesta SIA (6410 per impostazione predefinita)</p> <p>Porta server dei nomi CMS (6400 per impostazione predefinita)</p> <p>Porta richiesta CMS</p>

Prodotto	Applica- zione client	Server associati	Requisiti di porta del server
Piattaforma BI	Strumento di conversione dei report	CMS Input FRS	Porta server dei nomi CMS (6400 per impostazione predefinita) Porta richiesta CMS Porta richiesta Input FRS
Piattaforma BI	Repository Diagnostic Tool	CMS Input FRS Output FRS	Porta server dei nomi CMS (6400 per impostazione predefinita) Porta richiesta CMS Porta richiesta Input FRS Porta richiesta Output FRS
Piattaforma BI	SDK della piattaforma BI ospitato nel server di applicazioni Web	Tutti i server della piattaforma BI richiesti dai prodotti distribuiti. Ad esempio, è necessaria la comunicazione con la Porta richiesta del server di elaborazione Crystal Reports 2013 se l'SDK sta recuperando i report Crystal dal CMS e sta interagendo con essi.	Porta server dei nomi CMS (6400 per impostazione predefinita) Porta richiesta CMS Porta richiesta per ogni server richiesto. Ad esempio la porta richiesta del server di elaborazione Crystal Reports 2013.
Piattaforma BI	Provider di Servizi Web (dswebsobje.war)	Tutti i server della piattaforma BI richiesti dai prodotti che accedono ai servizi Web. Ad esempio, la comunicazione con le porte di richiesta del server di elaborazione e la cache di Dashboards è necessaria se SAP BusinessObjects Dashboards accede alle connessioni dell'origine dati Enterprise attraverso il provider di Servizi Web.	Porta server dei nomi CMS (6400 per impostazione predefinita) Porta richiesta CMS Porta richiesta per ogni server richiesto. Ad esempio, Server cache Dashboards e Porte richiesta Server di elaborazione Dashboards.

Prodotto	Applica- zione client	Server associati	Requisiti di porta del server
Piattaforma BI	SAP BusinessObjects Analysis, versione per OLAP	CMS Adaptive Processing Server che ospita il servizio di analisi multidimensionale Input FRS Output FRS	Porta server dei nomi CMS (6400 per impostazione predefinita) Porta richiesta CMS Porta richiesta Adaptive Processing Server Porta richiesta Input FRS Porta richiesta Output FRS

8.14.2.2.2 Requisiti di porta per le applicazioni di terze parti

In questa tabella sono elencati i programmi software di terze parti utilizzati dai prodotti SAP BusinessObjects. Sono inclusi esempi specifici di alcuni fornitori di software, ma è possibile che per altri fornitori i requisiti di porta siano diversi.

Applicazione di terze parti	Componente SAP BusinessObjects che utilizza il prodotto di terze parti	Requisito di porta dell'applicazione di terze parti	Descrizione
Database di sistema CMS	Central Management Server (CMS)	Porta di attesa del server di database	Il server CMS è l'unico server che comunica con il database di sistema CMS.
Database di controllo CMS	Central Management Server (CMS)	Porta di attesa del server di database	Il server CMS è l'unico server che comunica con il database di controllo CMS.
Database di reporting	Connection Server Ogni processo secondario del Job Server Ogni server di elaborazione	Porta di attesa del server di database	Questi server recuperano informazioni dal database di reporting.

Applicazione di terze parti	Componente SAP BusinessObjects che utilizza il prodotto di terze parti	Requisito di porta dell'applicazione di terze parti	Descrizione
Server di applicazioni Web	Tutti i servizi Web e le applicazioni Web SAP BusinessObjects, inclusi BI Launch Pad e la console CMC	Porta HTTP e HTTPS Ad esempio, su Tomcat la porta HTTP predefinita è 8080 e la porta HTTPS predefinita è 443.	La porta HTTPS è richiesta solo se viene utilizzata la comunicazione HTTP.
Server FTP	Ogni Job Server	FTP in ingresso (porta 21) FTP in uscita (porta 22)	I Job Server utilizzano le porte FTP per consentire l' invio su FTP .
server e-mail	Ogni Job Server	SMTP (porta 25)	I Job Server utilizzano la porta SMTP per consentire l' invio tramite posta elettronica .
Server UNIX a cui i Job Server possono inviare contenuto	Ogni Job Server	rexec out (porta 512) (Solo UNIX) rsh out (porta 514)	(Solo UNIX) I Job Server utilizzano queste porte per consentire l' invio su disco .
Server di autenticazione	CMS Server di applicazioni Web che ospita l'SDK ogni thick client, ad esempio Live Office.	Porta di connessione per autenticazione di terze parti. Ad esempio, il server di connessione per il server LDAP Oracle è definito dall'utente nel file ldap.ora.	Le credenziali dell'utente sono archiviate nel server di autenticazione di terze parti. Il server CMS, l'SDK e i thick client elencati qui devono poter comunicare con il server di autenticazione di terze parti quando un utente effettua l'accesso.

8.15 Configurazione della piattaforma BI per i firewall

In questa sezione vengono fornite istruzioni dettagliate per la configurazione della piattaforma BI in un ambiente protetto da firewall.

8.15.1 Per configurare il sistema per i firewall

1. Determinare quali componenti della piattaforma BI devono comunicare attraverso un firewall.
2. Configurare manualmente la porta di richiesta per ogni server della piattaforma BI che deve comunicare attraverso un firewall.
3. Configurare un intervallo di numeri di porta per qualsiasi Job Server secondario che deve comunicare tramite un firewall aggiungendo i parametri `-requestJSChildPorts porta più bassa-porta più alta` e `-requestPort porta` alla riga di comando del server.
4. Configurare il firewall per consentire la comunicazione con le porte di richiesta e l'intervallo di porte del Job Server nei server della piattaforma BI configurati nel passaggio precedente.
5. (Facoltativo) Configurare il file hosts in ogni computer che ospita un server della piattaforma BI che deve comunicare attraverso un firewall.

Argomenti correlati

- [Comunicazione tra componenti della piattaforma BI](#)
- [Configurazione dei numeri di porta](#)
- [Panoramica sulle righe di comando](#)
- [Specifiche delle regole del firewall](#)
- [Configurazione del file HOSTS per i firewall che utilizzano NAT](#)

8.15.1.1 Specifica delle regole del firewall

È necessario configurare il firewall per consentire il traffico necessario tra i componenti della piattaforma BI. Per dettagli sulla specifica di queste regole, consultare la documentazione del firewall.

Specificare una regola di accesso in ingresso per ogni percorso di comunicazione che attraversa il firewall. Potrebbe non essere necessario specificare una regola di accesso per ogni server della piattaforma BI protetto dal firewall.

Utilizzare il numero di porta specificato nella casella **Porta richiesta** nella pagina Proprietà del server nella CMC. Tenere presente che ogni server su un computer deve utilizzare un numero di porta univoco. Alcuni server SAP Business Objects utilizzano più di una porta.

Nota:

Se la piattaforma BI viene distribuita tra firewall che utilizzano NAT, ogni server su tutti i computer richiede un numero di porta richiesta univoco. Ciò significa che due server nell'intera distribuzione non possono condividere la stessa Porta richiesta.

Nota:

non è necessario specificare regole di accesso in uscita. I server della piattaforma BI non avviano la comunicazione al server delle applicazioni Web o ad applicazioni client. I server della piattaforma BI possono avviare la comunicazione con altri server della piattaforma nello stesso cluster. Le distribuzioni con server in cluster in un ambiente con firewall in uscita non sono supportate.

Esempio:

In questo esempio vengono illustrate le regole di accesso in ingresso per un firewall tra il server di applicazioni Web e i server della piattaforma BI. In questo caso, vengono aperte due porte per il sistema CMS, una porta per l'Input File Repository Server (FRS) e una per l'Output FRS. I numeri di Porta richiesta sono i numeri di porta specificati nella casella **Porta richiesta** della pagina di configurazione della CMC per un server.

Computer di origine	Porta	Computer di destinazione	Porta	Azione
Server di applicazioni Web	Qualsiasi	CMS	6400	Consenti
Server di applicazioni Web	Qualsiasi	CMS	<numero Porta richiesta>	Consenti
Server di applicazioni Web	Qualsiasi	Input FRS	<numero Porta richiesta>	Consenti
Server di applicazioni Web	Qualsiasi	Output FRS	<numero Porta richiesta>	Consenti
Qualsiasi	Qualsiasi	CMS	Qualsiasi	Rifiuta
Qualsiasi	Qualsiasi	Altri server della piattaforma	Qualsiasi	Rifiuta

Argomenti correlati

- [Comunicazione tra componenti della piattaforma BI](#)

8.15.1.2 Configurazione del file HOSTS per i firewall che utilizzano NAT

Questa fase è necessaria solo se i server della piattaforma BI devono comunicare attraverso un firewall in cui è abilitato Network Address Translation (NAT). Questa operazione consente ai computer client di mappare il nome host di un server a un indirizzo IP instradabile.

Nota:

La piattaforma BI può essere distribuita in computer che utilizzano il sistema DNS (Domain Name System). In questo caso, i nomi host dei computer server possono essere mappati a indirizzi IP instradabili esternamente nel server DNS, invece del file `hosts` di ciascun computer.

Network Address Translation

Un firewall viene distribuito per proteggere una rete interno dall'accesso non autorizzato. I firewall che utilizzano "NAT" mapperanno gli indirizzi IP dalla rete interna a un indirizzo diverso utilizzato dalla rete esterna. La "conversione degli indirizzi" migliora la protezione nascondendo gli indirizzi IP interni alla rete esterna.

I componenti della piattaforma BI quali server, thick client e il server di applicazioni Web che ospita l'SDK utilizzeranno un riferimento per contattare un server. Il riferimento al servizio contiene il nome host del computer server. Tale nome host deve essere instradabile dal computer del componente della piattaforma BI. Ciò significa che il file `hosts` sul computer del componente deve essere mappato al nome host del computer server all'indirizzo IP esterno del computer server. L'indirizzo IP esterno del computer server è instradabile dal lato esterno del firewall, mentre l'indirizzo IP interno non lo è.

La procedura per configurare il file `hosts` è diversa per Windows e UNIX.

8.15.1.2.1 Configurazione del file hosts in Windows

1. Individuare tutti i computer che eseguono un componente della piattaforma BI che deve comunicare attraverso un firewall in cui è abilitato "Network Address Translation" ("NAT").
2. In ogni computer individuato nell'operazione precedente, aprire il file `hosts` utilizzando un editor di testi come Blocco note. Il file `hosts` si trova in `\Windows\System32\drivers\etc\hosts`.
3. Seguire le istruzioni del file `hosts` per aggiungere una voce per ogni computer dietro il firewall in cui sono in esecuzione uno o più server della piattaforma BI. Mappare il nome host del computer server o il nome di dominio completo al relativo indirizzo IP esterno.
4. Salvare il file `hosts`.

8.15.1.2.2 Configurazione del file hosts in UNIX

Nota:

il sistema operativo UNIX deve essere configurato in modo che consulti innanzitutto il file "hosts" per risolvere i nomi di dominio prima del DNS. Per ulteriori dettagli, consultare la documentazione dei sistemi Unix.

1. Individuare tutti i computer che eseguono un componente della piattaforma BI che deve comunicare attraverso un firewall in cui è abilitato "Network Address Translation" ("NAT").
2. Aprire il file "hosts" utilizzando un editor come `vi`. Il file `hosts` si trova nella directory `\etc`.
3. Seguire le istruzioni del file `hosts` per aggiungere una voce per ogni computer dietro il firewall in cui sono in esecuzione uno o più server della piattaforma BI. Mappare il nome host del computer server o il nome di dominio completo al relativo indirizzo IP esterno.
4. Salvare il file `hosts`.

8.15.2 Debug di una distribuzione con firewall

Se uno o più server della piattaforma BI non funziona quando il firewall è abilitato, anche se sono state aperte le porte corrette sul firewall, è possibile utilizzare i registri eventi per determinare qual è il server che tenta di ascoltare e quali sono le porte o gli indirizzi IP. È quindi possibile aprire tali porte sul firewall o utilizzare la console CMC (Central Management Console) per modificare i numeri di porta o gli indirizzi IP su cui i server tentano di mettersi in ascolto.

Ogni volta che un server della piattaforma BI viene avviato, il server scrive le seguenti informazioni nel registro eventi per ogni porta di richiesta a cui tenta di collegarsi.

- "Server": il nome del server e se è stato avviato correttamente.
- "Indirizzi pubblicati": elenco di combinazioni di indirizzi IP e porte inviate al servizio nomi che gli altri server utilizzeranno per comunicare con questo server.

Se il server si collega correttamente a una porta, il file di registro visualizza anche "In attesa sulla/e porta/e", l'indirizzo IP e la porta su cui il server è in ascolto. Se il server non riesce a collegarsi alla porta, il file di registro visualizza "Ascolto sulle porte non riuscito", l'indirizzo IP e la porta su cui il server tenta di mettersi in ascolto con esito negativo.

Quando viene avviato il server CMS scrive anche le informazioni relative a indirizzi pubblicati, porte in attesa e ascolto non riuscito per la porta servizio nomi del server.

Nota:

se il server è configurato per l'utilizzo di una porta con assegnazione automatica e di un nome host o indirizzo IP non valido, il registro eventi indica che il server non è riuscito a mettersi in ascolto sul nome host o indirizzo IP e porta "0". Se un nome host o indirizzo IP specificato non è valido, si verificherà un errore del server prima che il sistema operativo host sia in grado di assegnare una porta.

Esempio:

L'esempio seguente mostra una voce relativa a un server CMS che è correttamente in ascolto su due porte richiesta e una porta servizio nomi.

```
Server mynode.cms1 successfully started.
Request Port :
  Published Address(es): mymachine.corp.com:11032, mymachine.corp.com:8765
  Listening on port(s): [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:11032, 10.90.172.216:8765
Name Service Port :
```

```
Published Address(es): mymachine.corp.com:6400
Listening on port(s): [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:6400, 10.90.172.216:6400
```

8.15.2.1 Debug di una distribuzione con firewall

1. Leggere il registro eventi per determinare se il server è correttamente collegato alla porta specificata. Se il server non è stato in grado di collegarsi a una porta, è probabile che vi sia un conflitto di porta tra il server e un altro processo in esecuzione sullo stesso computer. La voce "Ascolto sulle porte non riuscito" indica la porta su cui il server sta tentando di mettersi in ascolto. Eseguire un'utilità come netstat per determinare quale processo ha occupato la porta, quindi configurare l'altro processo o il server per l'ascolto su un'altra porta.
2. Se il server è riuscito a collegarsi a una porta, "In attesa sulla/e porta/e" indica la porta su cui il server è in ascolto. Se un server è in ascolto su una porta e continua a non funzionare correttamente, assicurarsi che la porta sia aperta sul firewall o configurare il server in modo tale che ascolti su una porta aperta.

Nota:

Se tutti i server CMS della distribuzione stanno tentando di ascoltare su porte o indirizzi IP non disponibili, i CMS non verranno avviati e non sarà possibile accedere alla console CMC. Se si desidera modificare il numero di porta o indirizzo IP su cui il server CMS tenta di mettersi in ascolto, utilizzare Central Configuration Manager (CCM) per specificare un numero di porta o un indirizzo IP valido.

Argomenti correlati

- [Configurazione dei numeri di porta](#)

8.16 Esempi di scenari di firewall tipici

In questa sezione vengono forniti esempi di scenari di distribuzione di firewall tipici

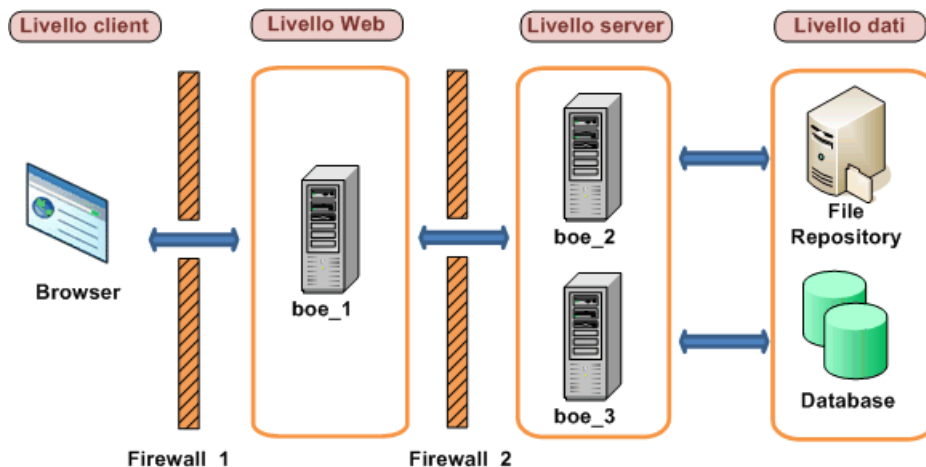
8.16.1 Esempio: livello applicazione distribuito su una rete separata

In questo esempio viene illustrato come configurare un firewall e la piattaforma BI in modo da utilizzarli insieme in una distribuzione in cui un firewall separa il server di applicazioni Web da altri server della piattaforma BI.

In questo esempio i componenti della piattaforma BI vengono distribuiti tra questi computer:

- Computer `boe_1`: ospita il server di applicazioni Web e l'SDK.
- Computer `boe_2`: ospita i server di livello Intelligence, inclusi Central Management Server, Input File Repository Server, Output File Repository Server ed Event Server.
- Computer `boe_3`: ospita i server del livello di elaborazione, inclusi Adaptive Job Server, Server di elaborazione Web Intelligence, Report Application Server, Crystal Reports Cache Server e Crystal Reports Processing Server.

Figura 8 - 1: Livello applicazione distribuito su una rete separata



8.16.1.1 Per configurare un livello applicazione distribuito su una rete separata

I passaggi seguenti illustrano come configurare questo esempio.

1. I seguenti requisiti di comunicazione si applicano a questo esempio:
 - Il server di applicazioni Web che ospita l'SDK deve essere in grado di comunicare con il sistema CMS su entrambe le porte.
 - Il server di applicazioni Web che ospita l'SDK di BusinessObjects Enterprise deve essere in grado di comunicare con qualsiasi server della piattaforma BI.
 - Il browser deve avere accesso alla Porta richiesta http o https sul server di applicazioni Web.
2. Il server di applicazioni Web deve comunicare con tutti i server della piattaforma BI sui computer `boe_2` e `boe_3`. Configurare i numeri di porta per ogni server su questi computer. Tenere presente che è possibile utilizzare qualsiasi porta libera compresa tra 1.025 e 65.535.

I numeri di porta scelti per questo esempio sono elencati nella tabella:

Server	Numero di porta
Central Management Server	6400
Central Management Server	6441

Server	Numero di porta
Input File Repository Server	6415
Output File Repository Server	6420
Event Server	6425
Adaptive Job Server	6435
Crystal Reports Cache Server	6440
Server di elaborazione Web Intelligence	6460
Report Application Server	6465
Crystal Reports Processing Server	6470

3. Configurare i firewall `Firewall_1` e `Firewall_2` per consentire la comunicazione sulle porte fisse sui server della piattaforma BI e il server di applicazioni Web configurati nel passaggio precedente. In questo esempio viene aperta la porta HTTP per il server di applicazioni Tomcat.

Tabella 8 - 6: Configurazione per Firewall_1

Porta	Computer di destinazione	Porta	Azione
Qualsiasi	boe_1	8080	Consenti

Tabella 8 - 7: Configurazione per Firewall_2

Computer di origine	Porta	Computer di destinazione	Porta	Azione
boe_1	Qualsiasi	boe_2	6400	Consenti
boe_1	Qualsiasi	boe_2	6441	Consenti
boe_1	Qualsiasi	boe_2	6415	Consenti
boe_1	Qualsiasi	boe_2	6420	Consenti
boe_1	Qualsiasi	boe_2	6425	Consenti
boe_1	Qualsiasi	boe_3	6435	Consenti
boe_1	Qualsiasi	boe_3	6440	Consenti
boe_1	Qualsiasi	boe_3	6460	Consenti

Computer di origine	Porta	Computer di destinazione	Porta	Azione
boe_1	Qualsiasi	boe_3	6465	Consenti
boe_1	Qualsiasi	boe_3	6470	Consenti

4. Questo firewall non è abilitato per NAT e non è pertanto necessario configurare il file `hosts`

Argomenti correlati

- [Configurazione dei numeri di porta](#)
- [Informazioni sulla comunicazione tra componenti della piattaforma BI](#)

8.16.2 Esempio: livello thick client e database separato dai server della piattaforma BI mediante un firewall

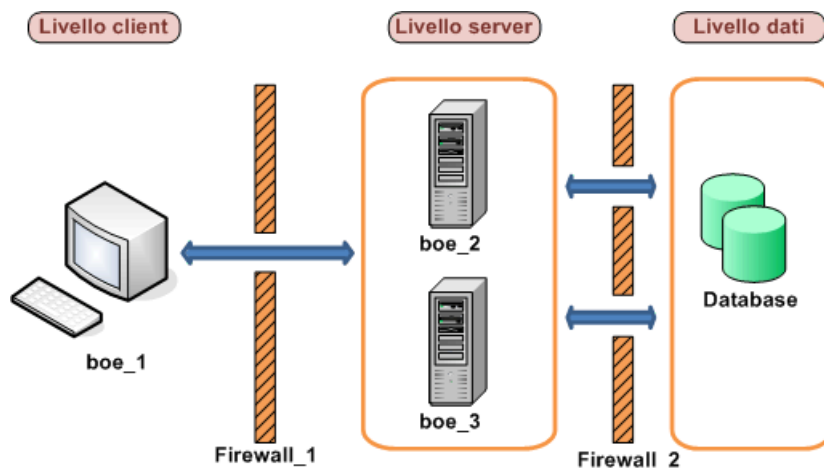
In questo esempio viene illustrato come configurare un firewall e la piattaforma BI in modo da utilizzarli insieme in uno scenario di distribuzione in cui:

- Un firewall separa un thick client dai server della piattaforma BI.
- Un firewall separa i server della piattaforma BI dal livello di database.

In questo esempio i componenti della piattaforma BI vengono distribuiti tra questi computer:

- Computer `boe_1`: ospita la Pubblicazione guidata. La Pubblicazione guidata è un thick client della piattaforma BI.
- Il computer `boe_2` ospita i server di livello Intelligence, inclusi Central Management Server (CMS), Input File Repository Server, Output File Repository Server ed Event Server.
- Il computer `boe_3` ospita i server del livello di elaborazione, inclusi Adaptive Job Server, Server di elaborazione Web Intelligence, Report Application Server, Crystal Reports Processing Server e Crystal Reports Cache Reports.
- Il computer `Database` ospita i database CMS di sistema e di controllo e il database di creazione report. Si noti che è possibile distribuire entrambi i database sullo stesso server di database oppure ciascun database su un server di database distinto. In questo esempio, tutti i database CMS e il database di creazione di report vengono distribuiti sullo stesso server di database.

Figura 8 - 2: Livello Rich Client e database distribuito su reti separate



8.16.2.1 Configurazione di livelli separati dai server della piattaforma BI da un firewall

I passaggi seguenti illustrano come configurare questo esempio.

1. Applicare i seguenti requisiti di comunicazione a questo esempio:

- La Pubblicazione guidata deve essere in grado di avviare la comunicazione con il sistema CMS su entrambe le porte.
- La Pubblicazione guidata deve essere in grado di avviare la comunicazione con l'Input e l'Output File Repository Server.
- Il Connection Server, ogni processo secondario di Job Server e ogni server di elaborazione devono avere accesso alla porta di attesa sul server del database di creazione di report.
- Il sistema CMS deve avere accesso alla porta di attesa del database sul server di database CMS.

2. Configurare una porta specifica per il sistema CMS, l'Input FRS e l'Output FRS. Tenere presente che è possibile utilizzare qualsiasi porta libera compresa tra 1.025 e 65.535.

I numeri di porta scelti per questo esempio sono elencati nella tabella:

Server	Numero di porta
Central Management Server	6441
Input File Repository Server	6415
Output File Repository Server	6416

3. Non è necessario configurare un intervallo di porte per i processi secondari di Job Server poiché il firewall tra i Job Server e i server di database vengono configurati in modo da consentire l'avvio della comunicazione da qualsiasi porta.

4. Configurare il firewall *Firewall_1* per consentire la comunicazione sulle porte fisse sui server della piattaforma configurati nel passaggio precedente. Si noti che la porta 6400 è il numero di porta predefinito per Porta server dei nomi di CMS e non occorre configurarla in modo esplicito nel passaggio precedente.

Porta	Computer di destinazione	Porta	Azione
Qualsiasi	boe_2	6400	Consenti
Qualsiasi	boe_2	6441	Consenti
Qualsiasi	boe_2	6415	Consenti
Qualsiasi	boe_2	6416	Consenti

Configurare *Firewall_2* per consentire la comunicazione sulla porta di attesa del server di database. Il server CMS (su **boe_2**) deve disporre dell'accesso al database di controllo e di sistema CMS e i Job Server (su **boe_3**) devono disporre dell'accesso ai database di sistema e di controllo. Si noti che non è stato configurato un intervallo di porte per i processi secondari dei Job Server poiché le comunicazioni con il server CMS non attraversano un firewall.

Computer di origine	Porta	Computer di destinazione	Porta	Azione
boe_2	Qualsiasi	Database	3306	Consenti
boe_3	Qualsiasi	Database	3306	Consenti

5. Questo firewall non è abilitato per NAT e non è pertanto necessario configurare il file `hosts`

Argomenti correlati

- [Informazioni sulla comunicazione tra componenti della piattaforma BI](#)
- [Configurazione della piattaforma BI per i firewall](#)

8.17 Impostazioni firewall per gli ambienti integrati

In questa sezione vengono illustrate in dettaglio considerazioni specifiche e impostazioni delle porte per le distribuzioni della piattaforma BI che si integrano con gli ambienti ERP indicati di seguito.

- SAP
- Oracle EBS
- Siebel
- JD Edwards

- PeopleSoft

I componenti della piattaforma BI includono client browser, rich client, server e l'SDK ospitato sul Web Application Server. I componenti del sistema possono essere installati su più computer. È utile conoscere i concetti base delle comunicazioni tra i componenti della piattaforma BI ed ERP prima di configurare il sistema per il funzionamento con i firewall.

Requisiti di porta per i server della piattaforma BI

Le porte indicate di seguito sono necessarie per i server corrispondenti nella piattaforma BI:

Requisiti di porta del server
<ul style="list-style-type: none"> • Porta server dei nomi Central Management Server • Porta Central Management Server • Porta richieste FRS di input • Porta richieste FRS di output • Porta richiesta Report Application Server • Porta richiesta Crystal Reports Cache Server • Porta richiesta Page Server Crystal Reports • Porta richiesta server di elaborazione Crystal Reports

8.17.1 Linee guida specifiche del firewall per Oracle EBS

La distribuzione della piattaforma BI deve essere conforme alle seguenti regole di comunicazione:

- Il CMS deve essere in grado di avviare le comunicazioni con il sistema SAP sulla porta gateway del sistema SAP.
- Adaptive Job Server e il server di elaborazione Crystal Reports (insieme ai componenti di Accesso dati) devono potere avviare le comunicazioni con il sistema SAP sulla porta gateway del sistema SAP.
- Il componente Publisher BW deve poter avviare le comunicazioni con il sistema SAP sulla porta gateway del sistema SAP.
- I componenti della piattaforma BI distribuiti sul lato SAP Enterprise Portal (ad esempio, iViews e KMC) devono essere in grado di avviare le comunicazioni con le applicazioni Web della piattaforma BI sulle porte HTTP/HTTPS.
- Il server di applicazioni Web deve poter avviare le comunicazioni sulla porta del servizio gateway del sistema SAP.
- Crystal Reports deve poter avviare le comunicazioni con l'host SAP sulla porta gateway del sistema SAP e sulla porta dispatcher del sistema SAP.

La porta su cui è in ascolto il servizio gateway SAP è la stessa specificata durante l'installazione.

Nota:

se un componente richiede un router SAP per la connessione a un sistema SAP, è possibile configurarlo mediante la stringa di tale router SAP. Ad esempio, durante la configurazione di un sistema di autorizzazione SAP per l'importazione di ruoli e utenti, la stringa del router SAP può essere utilizzata al posto del nome del server di applicazioni. In tal modo, la comunicazione tra il CMS e il sistema SAP viene effettuata mediante il router SAP.

Argomenti correlati

- [Installazione di un gateway SAP locale](#)

8.17.1.1 Requisiti delle porte in dettaglio

Requisiti delle porte per SAP

La piattaforma BI utilizza SAP JCO (SAP Java Connector) per comunicare con SAP NetWeaver (ABAP). È necessario configurare e garantire la disponibilità delle porte seguenti:

- Porta di ascolto servizio gateway SAP (ad esempio, 3300).
- Porta di ascolto servizio dispatcher SAP (ad esempio, 3200).

La tabella seguente riporta le configurazioni specifiche delle porte.

Computer di origine	Porta	Computer di destinazione	Porta	Azione
SAP	Qualsiasi	Server di applicazioni Web della piattaforma BI	Porta HTTP/HTTPS servizio Web	Consenti
SAP	Qualsiasi	CMS	Porta server dei nomi CMS	Consenti
SAP	Qualsiasi	CMS	Porta richiesta CMS	Consenti
Server di applicazioni Web	Qualsiasi	SAP	Porta servizio gateway sistema SAP	Consenti
Central Management Server (CMS)	Qualsiasi	SAP	Porta servizio gateway sistema SAP	Consenti
Crystal Reports	Qualsiasi	SAP	Porta servizio gateway sistema SAP e porta dispatcher sistema SAP	Consenti

8.17.2 Configurazione del firewall per l'integrazione con JD Edwards EnterpriseOne

Le distribuzioni della piattaforma BI che comunicheranno con il software JD Edwards devono essere conformi alle seguenti regole generali:

- Il server di applicazioni Web di CSM deve essere in grado di avviare le comunicazioni con JD Edwards EnterpriseOne tramite la porta JDENET e una porta selezionata in modo casuale.
- Crystal Reports con il componente Connettività dati del lato client deve essere in grado di avviare le comunicazioni con JD Edwards EnterpriseOne tramite la porta JDNET. Per il recupero dei dati, il lato JD Edwards EnterpriseOne deve essere in grado di comunicare con il driver tramite una porta casuale che non può essere controllata.
- Il server CMS deve essere in grado di avviare le comunicazioni con JD Edwards EnterpriseOne tramite la porta JDENET e una porta selezionata in modo casuale.
- Il numero di porta JDENET si trova nel file di configurazione di JD Edwards EnterpriseOne Application Server (JDE.INI), nella sezione JDENET.

Requisiti di porta per i server della piattaforma BI

Prodotto	Requisiti di porta del server
Piattaforma SAP BusinessObjects Business Intelligence	<ul style="list-style-type: none"> • Porta del server Sign On della piattaforma BI

Requisiti di porta per JD Edwards EnterpriseOne

Prodotto	Requisito porta	Descrizione
JD Edwards EnterpriseOne	Porta JDENET e porta selezionata in modo casuale	Utilizzata per la comunicazione tra la piattaforma BI e il server di applicazioni JD Edwards EnterpriseOne.

Configurazione del server di applicazioni Web per la comunicazione con JD Edwards

In questa sezione viene illustrato come configurare un firewall e la piattaforma BI in modo da utilizzarli insieme in uno scenario di distribuzione in cui un firewall separa il server di applicazioni Web da altri server della piattaforma.

Per la configurazione del firewall con i server e i client della piattaforma BI, vedere la sezione *Requisiti di porta della piattaforma BI* in questo manuale. Oltre alla configurazione standard del firewall, la comunicazione con i server JD Edwards richiede l'apertura di alcune porte supplementari.

Tabella 8 - 14: Per JD Edwards EnterpriseOne Enterprise

Computer di origine	Porta	Computer di destinazione	Porta	Azione
CMS con funzione Connettività protezione per JD Edwards EnterpriseOne	Qualsiasi	JD Edwards EnterpriseOne	Qualsiasi	Consenti
Server della piattaforma BI con funzione Connettività dati per JD Edwards EnterpriseOne	Qualsiasi	JD Edwards EnterpriseOne	Qualsiasi	Consenti
Crystal Reports con funzione Connettività dati lato client per JD Edwards EnterpriseOne	Qualsiasi	JD Edwards EnterpriseOne	Qualsiasi	Consenti
Server di applicazioni Web	Qualsiasi	JD Edwards EnterpriseOne	Qualsiasi	Consenti

8.17.3 Linee guida specifiche del firewall per Oracle EBS

La distribuzione della piattaforma BI deve consentire ai seguenti componenti di avviare le comunicazioni con la porta del listener del database Oracle:

- Componenti Web della piattaforma BI
- CMS (in particolare il plug-in di protezione Oracle EBS)

- Server di backend della piattaforma BI (in particolare il componente di accesso ai dati EBS)
- Crystal Reports (in particolare il componente di accesso ai dati EBS)

Nota:

il valore predefinito della porta del listener del database Oracle in tutti i casi sopracitati deve essere 1521.

8.17.3.1 Requisiti delle porte in dettaglio

Oltre alla configurazione del firewall standard per la piattaforma BI, è necessario aprire alcune porte supplementari per garantire il funzionamento in un ambiente Oracle EBS integrato:

Computer di origine	Porta	Computer di destinazione	Porta	Azione
Server di applicazioni Web	Qualsiasi	Oracle EBS	Porta del database Oracle	Consenti
Server CMS con connettività di protezione per Oracle EBS	Qualsiasi	Oracle EBS	Porta del database Oracle	Consenti
Server della piattaforma BI con connettività dati lato server per Oracle EBS	Qualsiasi	Oracle EBS	Porta del database Oracle	Consenti
Crystal Reports con connettività dati lato client per Oracle EBS	Qualsiasi	Oracle EBS	Porta del database Oracle	Consenti

8.17.4 Configurazione del firewall per l'integrazione con PeopleSoft Enterprise

Le distribuzioni della piattaforma BI che comunicano con PeopleSoft Enterprise devono essere conformi alle seguenti regole generali di comunicazione:

- Il CMS (Central Management Server) con il componente Connettività di protezione deve essere in grado di avviare le comunicazioni con il servizio Web PeopleSoft Query Access (QAS).
- I server della piattaforma BI con un componente Connettività dati devono essere in grado di avviare le comunicazioni con il servizio Web PeopleSoft QAS.
- Crystal Reports con il componente Connettività dati del lato client deve essere in grado di avviare le comunicazioni con il servizio Web PeopleSoft QAS.

- Enterprise Management (EPM) Bridge deve essere in grado di comunicare con il CMS e l'Input File Repository Server.
- EPM Bridge deve essere in grado di comunicare con il database PeopleSoft utilizzando una connessione ODBC.

Il numero di porta del servizio Web è lo stesso specificato nel nome del dominio PeopleSoft Enterprise.

Requisiti di porta per i server della piattaforma BI

Prodotto	Requisiti di porta del server
Piattaforma SAP BusinessObjects Business Intelligence	<ul style="list-style-type: none"> • Porta del server Sign On della piattaforma BI

Requisiti di porta per PeopleSoft

Prodotto	Requisito porta	Descrizione
PeopleSoft Enterprise: People Tools 8.46 o versione successiva	Porta HTTP/HTTPS servizio Web	Questa porta è richiesta quando si utilizza la connessione SOAP per PeopleSoft Enterprise per People Tools 8.46 e soluzioni successive

Configurazione della piattaforma BI e di PeopleSoft per i firewall

In questa sezione viene descritto come configurare la piattaforma BI e PeopleSoft Enterprise in modo da utilizzarli insieme in uno scenario di distribuzione in cui un firewall separa il server di applicazioni Web da altri server della piattaforma.

Per la configurazione firewall con i server e i client della piattaforma BI, fare riferimento al *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

Oltre alla configurazione firewall con la piattaforma BI, è necessario eseguire alcune operazioni di configurazione supplementari.

Tabella 8 - 18: Per PeopleSoft Enterprise: PeopleTools 8.46 o versione più recente

Computer di origine	Porta	Computer di destinazione	Porta	Azione
CMS con funzione Connettività protezione per PeopleSoft	Qualsiasi	PeopleSoft	Porta HTTP/HTTPS servizio Web PeopleSoft	Consenti

Computer di origine	Porta	Computer di destinazione	Porta	Azione
Server della piattaforma BI con funzione Connettività dati per PeopleSoft	Qualsiasi	PeopleSoft	Porta HTTP/HTTPS servizio Web PeopleSoft	Consenti
Crystal Reports con funzione Connettività dati lato client per PeopleSoft	Qualsiasi	PeopleSoft	Porta HTTP/HTTPS servizio Web PeopleSoft	Consenti
Ponte EPM	Qualsiasi	CMS	Porta server dei nomi CMS	Consenti
Ponte EPM	Qualsiasi	CMS	Porta richiesta CMS	Consenti
Ponte EPM	Qualsiasi	Input File Repository Server	Porta FRS di input	Consenti
Ponte EPM	Qualsiasi	PeopleSoft	Porta database PeopleSoft	Consenti

8.17.5 Configurazione del firewall per l'integrazione con Siebel

In questa sezione sono indicate le porte specifiche utilizzate per la comunicazione tra la piattaforma BI e le applicazioni eBusiness Siebel quando sono separate da firewall.

- L'applicazione Web deve essere in grado di avviare la comunicazione con il server Sign On della piattaforma BI per Siebel. Per il server Sign On di Enterprise per Siebel sono necessarie tre porte:
 1. La porta 7 Echo (TCP) per la verifica dell'accesso al server Sign On.
 2. La porta (8448 per impostazione predefinita) del server Sign On della piattaforma BI per Siebel per la porta di ascolto CORBA IOR.
 3. Una porta POA casuale per le comunicazioni CORBA che non possono essere controllate, di conseguenza tutte le porte devono essere aperte.
- Il server CMS deve essere in grado di avviare la comunicazione con il server Sign On della piattaforma BI per Siebel. Porta di attesa CORBA IOR configurata per ogni server Sign On (ad esempio 8448). È inoltre necessario aprire una porta POA casuale che resterà sconosciuta fino all'installazione della piattaforma BI.
- Il server Sign On della piattaforma BI per Siebel deve essere in grado di avviare la comunicazione con la porta SCBroker (broker di connessione Siebel), ad esempio 2321.

- I server back-end della piattaforma BI (componente Siebel Data Access) devono essere in grado di avviare la comunicazione con la porta SCBroker (broker di connessione Siebel), ad esempio 2321.
- Crystal Reports (il componente Siebel Data Access) deve essere in grado di avviare la comunicazione con la porta SCBroker (broker di connessione Siebel), ad esempio 2321.

Descrizione dettagliata delle porte

In questa sezione vengono indicate le porte utilizzate dalla piattaforma BI. Se si distribuisce la piattaforma BI in un ambiente con firewall, è possibile utilizzare queste informazioni per aprire in tali firewall il numero minimo di porte specifiche per l'integrazione con Siebel.

Tabella 8 - 19: Requisiti di porta per i server della piattaforma BI

Prodotto	Requisiti di porta del server
Piattaforma SAP BusinessObjects Business Intelligence	<ul style="list-style-type: none"> • Porta del server Sign On della piattaforma BI

Tabella 8 - 20: Requisito di porta per Siebel

Prodotto	Requisito porta	Descrizione
Applicazione eBusiness Siebel	2321	Porta SCBroker (broker di connessione Siebel) predefinita

Configurazione dei firewall della piattaforma BI per l'integrazione con Siebel

In questa sezione viene illustrato come configurare i firewall per Siebel e la piattaforma BI in modo da utilizzarli insieme in uno scenario di distribuzione in cui un firewall separa il server di applicazioni Web da altri server della piattaforma.

Computer di origine	Porta	Computer di destinazione	Porta	Azione
Server di applicazioni Web	Qualsiasi	Server Sign On della piattaforma BI per Siebel	Qualsiasi	Consentire
CMS	Qualsiasi	Server Sign On della piattaforma BI per Siebel	Qualsiasi	Consentire
Server Sign On della piattaforma BI per Siebel	Qualsiasi	Siebel	Porta SCBroker	Consentire
Server della piattaforma BI con funzione Connettività dati lato server per Siebel	Qualsiasi	Siebel	Porta SCBroker	Consentire
Crystal Reports con funzione Connettività dati lato client per Siebel	Qualsiasi	Siebel	Porta SCBroker	Consentire

8.18 Piattaforma BI e server proxy inverso

È possibile distribuire la piattaforma BI in un ambiente con uno o più server proxy inversi. Un server proxy inverso viene in genere distribuito davanti ai server di applicazioni Web per nasconderli dietro a un singolo indirizzo IP. Questa configurazione instrada tutto il traffico Internet indirizzato a server di applicazioni Web privati attraverso il server reverse proxy, nascondendo gli indirizzi IP privati.

Poiché il server proxy inverso converte gli URL pubblici in URL interni, deve essere configurato con gli URL delle applicazioni Web della piattaforma BI distribuite nella rete interna.

8.18.1 Server reverse proxy supportati

La piattaforma BI supporta i seguenti server proxy inversi:

- IBM Tivoli Access Manager WebSEAL 6
- Apache 2.2
- Microsoft ISA 2006

8.18.2 Distribuzione delle applicazioni Web

Le applicazioni Web della piattaforma BI vengono distribuite in un server di applicazioni Web. Le applicazioni vengono distribuite automaticamente durante l'installazione con lo strumento WDeploy. Lo strumento può inoltre essere utilizzato per distribuire manualmente le applicazioni dopo la distribuzione della piattaforma BI. In un'installazione predefinita di Windows le applicazioni Web vengono installate nella directory seguente:

```
C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps
```

WDeploy viene utilizzato per distribuire file WAR quali:

- **BOE:** include la console CMC, BI Launch Pad e Open Document
- **dswsbobje:** contiene l'applicazione Servizi Web

Se il server di applicazioni Web si trova dietro a un server reverse proxy, quest'ultimo deve essere configurato con i percorsi di contesto corretti dei file WAR. Per esporre tutte le funzionalità della piattaforma BI, configurare un percorso di contesto per ogni file WAR della piattaforma BI installato.

8.19 Configurazione di server proxy inverso per applicazioni Web della piattaforma BI

Il server proxy inverso deve essere configurato per la mappatura di richieste URL in arrivo all'applicazione Web corretta in distribuzioni in cui le applicazioni Web della piattaforma BI vengono distribuite dietro a un server proxy inverso.

In questa sezione sono contenuti esempi di configurazione specifici per alcuni dei server reverse proxy supportati. Fare riferimento alla documentazione del fornitore per il server reverse proxy per ottenere ulteriori informazioni.

8.19.1 Istruzioni dettagliate per la configurazione di server reverse proxy

Configurazione dei file WAR

Le applicazioni Web della piattaforma BI vengono distribuite come file WAR in un server di applicazioni Web. Assicurarsi di configurare una direttiva nel server reverse proxy per il file WAR richiesto per la distribuzione. È possibile utilizzare lo strumento WDeploy per distribuire i file WAR `BOE` o `dswsbobje`. Per ulteriori informazioni su WDeploy, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma BI*.

Specificare le proprietà BOE nella directory di configurazione personalizzata.

Il file `BOE.war` contiene proprietà globali e specifiche dell'applicazione. Se è necessario modificare le proprietà, utilizzare la directory di configurazione personalizzata. Per impostazione predefinita, la directory si trova in `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Avvertenza:

per evitare di sovrascrivere i file nella directory predefinita, non modificare le proprietà contenute nella directory `config\default`. Gli utenti devono utilizzare la directory `custom`.

Nota:

Su alcuni server di applicazioni Web, ad esempio la versione Tomcat in bundle con la piattaforma BI, è possibile accedere al file `BOE.war` direttamente. In scenari del genere è possibile configurare impostazioni personalizzate direttamente senza annullare la distribuzione del file WAR. Quando non è possibile accedere al file `BOE.war`, è necessario annullare la distribuzione, personalizzare e quindi distribuire nuovamente il file.

Uso coerente delle barre (/)

Definire i percorsi di contesto nel server proxy inverso così come vengono immessi in un URL del browser. Se, ad esempio, la direttiva contiene una barra (/) alla fine del percorso mirror nel server proxy inverso, immettere una barra alla fine dell'URL del browser.

Assicurarsi che il carattere '/' venga utilizzato in modo coerente nell'URL di origine e di destinazione nella direttiva del server proxy inverso. Se il carattere '/' viene aggiunto alla fine dell'URL di origine, deve anche essere aggiunta alla fine dell'URL di destinazione.

8.19.2 Per configurare il server reverse proxy

La procedura che segue è necessaria per il funzionamento delle applicazioni Web della piattaforma BI dietro a un server reverse proxy supportato.

1. Assicurarsi che il server reverse proxy sia configurato correttamente secondo le istruzioni del fornitore e la topologia della rete della distribuzione.
2. Determinare quale file WAR della piattaforma BI è richiesto.
3. Configurare il server reverse proxy per ogni applicazione file WAR della piattaforma BI. Si noti che le regole vengono specificate in modo diverso in ogni tipo di server reverse proxy.
4. Eseguire eventuali configurazioni speciali necessarie. Alcune applicazioni Web richiedono una configurazione speciale se distribuite in determinati server di applicazioni Web.

8.19.3 Per configurare il server proxy inverso Apache 2.2 per la piattaforma BI

In questa sezione viene fornito un workflow per la configurazione della piattaforma BI e di Apache 2.2 per l'utilizzo congiunto.

1. Assicurarsi che la piattaforma BI e Apache 2.2 siano installati in computer separati.
2. Assicurarsi che Apache 2.2 sia installato e configurato come server reverse proxy secondo quanto descritto nella documentazione del fornitore.
3. Configurare `ProxyPass` per ogni file WAR distribuito dietro il server reverse proxy.
4. Configurare `ProxyPassReverseCookiePath` per ogni applicazione Web distribuita dietro il server reverse proxy. Ad esempio:

```
ProxyPass /C1/BOE/ http://appservername:80/BOE/
ProxyPassReverseCookiePath / /C1/BOE
ProxyPassReverse /C1/BOE/ http://appservername:80/BOE/
ProxyPass /C1/explorer/ http://appservername:80/explorer/
ProxyPassReverseCookiePath / /C1/explorer
ProxyPassReverse /C1/explorer/ http://appservername:80/explorer/
```

8.19.4 Per configurare il server proxy inverso WebSEAL 6.0 per la piattaforma BI

In questa sezione viene spiegato come configurare la piattaforma BI e WebSEAL 6.0 per utilizzarli insieme.

Il metodo di configurazione consigliato consiste nella creazione di una sola giunzione che mappi tutte le applicazioni Web della piattaforma BI ospitati in un server di applicazioni Web interno o un server Web in un unico punto di montaggio.

1. Assicurarsi che la piattaforma BI e WebSEAL 6.0 siano installati in computer separati.
È possibile, ma non consigliabile, distribuire la piattaforma BI e WebSEAL 6.0 nello stesso computer. Per istruzioni sulla configurazione di questo scenario di distribuzione, consultare la documentazione del fornitore di WebSEAL 6.0.
2. Assicurarsi che WebSEAL 6.0 sia installato e configurato come descritto nella documentazione del fornitore.
3. Avviare l'utilità della riga di comando **pdadmin** di WebSEAL. Accedere a un dominio protetto come **sec_master** come un utente con diritti di amministratore.
4. Immettere il comando seguente al prompt **pdadmin sec_master**:

```
server task <instance_name-webseald-host_name> create -t  
<type> -h <host_name> -p <port> <junction_point>
```

Dove:

- **<nome_istanza-nome_host-webseald>** specifica il nome server completo dell'istanza di WebSEAL installata. Utilizzare il nome server completo nello stesso formato visualizzato nell'output del comando `server list`.
- **<tipo>** specifica il tipo di giunzione. Utilizzare `tcp` se la giunzione mappa a una porta HTTP interna. Utilizzare `ssl` se la giunzione mappa a una porta HTTPS interna.
- **<nome_host>** specifica il nome host DNS o l'indirizzo IP del server interno che riceverà le richieste.
- **<porta>** specifica la porta TCP del server interno che riceverà le richieste.
- **<punto_giunzione>** specifica la directory nello spazio oggetto protetto WebSEAL in cui viene montato lo spazio documento del server interno.

Esempio:

```
server task default-webseald-webseal.rp.sap.com  
create -t tcp -h 10.50.130.123 -p 8080/hr
```

8.19.5 Per configurare Microsoft ISA 2006 per la piattaforma BI

In questa sezione viene spiegato come configurare la piattaforma BI e ISA 2006 per utilizzarli insieme.

Il metodo di configurazione consigliato consiste nella creazione di una sola giunzione che mappi tutti i file WAR della piattaforma BI ospitati in un server di applicazioni Web interno o un server Web in un unico punto di montaggio. A seconda del server di applicazioni Web in uso, è necessario eseguire altre operazioni di configurazione nel server di applicazioni per consentirne l'utilizzo con ISA 2006.

1. Assicurarsi che la piattaforma BI e ISA 2006 siano installati in computer separati.
È possibile, ma non consigliabile, distribuire la piattaforma BI e ISA 2006 nello stesso computer. Per istruzioni sulla configurazione di questo scenario di distribuzione, consultare la documentazione di ISA 2006.
2. Assicurarsi che ISA 2006 sia installato e configurato come descritto nella documentazione del fornitore.
3. Avviare l'utilità Gestione di ISA Server.
4. Utilizzare il riquadro di spostamento per avviare un nuovo ruolo di pubblicazione.
 - a. Vai a
Matrici > NomeComputer > Criteri firewall > Nuovo > Regola di pubblicazione sul Web
Promemoria:
Sostituire `NomeComputer` con il nome del computer in cui è installato ISA 2006.
 - b. Digitare un nome di regola in **Nome regola di pubblicazione sul Web** e fare clic su **Avanti**.
 - c. Selezionare **Consenti** come azione regola e fare clic su **Avanti**.
 - d. Selezionare **Pubblica un singolo sito Web o un sistema di bilanciamento del carico** come tipo di pubblicazione e fare clic su **Avanti**.
 - e. Selezionare un tipo di connessione tra ISA Server e il sito Web pubblicato e fare clic su **Avanti**.
Ad esempio selezionare **Utilizzare connessioni non protette per connettersi al server Web pubblicato o alla server farm**.
 - f. Digitare il nome interno del sito Web da pubblicare (ad esempio il nome del computer che ospita la piattaforma BI) in **Nome sito interno** e fare clic su **Avanti**.
Nota:
Se il computer che ospita ISA 2006 non è in grado di connettersi al server di destinazione, selezionare **Utilizza nome computer o indirizzo IP per la connessione al server pubblicato** e digitare il nome o l'indirizzo IP nel campo fornito.
 - g. In "Dettagli nome pubblico" selezionare il nome di dominio (ad esempio **Qualsiasi nome di dominio**) e specificare i dettagli di pubblicazione interni (ad esempio /*). Fare clic su **Avanti**.
È ora necessario creare un nuovo listener Web per monitorare le richieste Web in arrivo.
5. Fare clic su **Nuovo** per avviare la Creazione guidata definizione listener Web.
 - a. Digitare un nome in **Nome listener Web** e fare clic su **Avanti**.
 - b. Selezionare un tipo di connessione tra ISA Server e il sito Web pubblicato e fare clic su **Avanti**.
Ad esempio selezionare **Non richiedere connessioni SSL protette con i client**.
 - c. Nella sezione "Indirizzi IP del listener Web" selezionare quanto segue e fare clic su **Avanti**.
 - Interno
 - Esterno
 - Host locale
 - Tutte le retiISA Server è ora configurato per la pubblicazione solo su HTTP.
 - d. Selezionare un'opzione "Impostazione di autenticazione", fare clic su **Avanti**, quindi su **Fine**.
Il nuovo listener è ora configurato per la regola di pubblicazione Web.

6. Fare clic su **Avanti** in "Gruppi di utenti", quindi su **Fine**.
7. Fare clic su **Applica** per salvare tutte le impostazioni per la regola di pubblicazione Web e aggiornare la configurazione di ISA 2006.
È ora necessario aggiornare le proprietà della regola di pubblicazione Web per mappare i percorsi delle applicazioni Web.
8. Nel riquadro di spostamento, fare clic con il pulsante destro del mouse sui Criteri firewall configurati e selezionare **Proprietà**.
9. Nella scheda "Percorsi" fare clic su **Aggiungi** per mappare i percorsi delle applicazioni Web SAP BusinessObjects.
10. Nella scheda "Nome pubblico" selezionare **Richiesta per i seguenti siti Web** e fare clic su **Aggiungi**.
11. Nella finestra di dialogo "Nome pubblico" digitare il nome del server ISA 2006 e fare clic su **OK**.
12. Fare clic su **Applica** per salvare tutte le impostazioni per la regola di pubblicazione Web e aggiornare la configurazione di ISA 2006.
13. Verificare le connessioni accedendo all'URL seguente:
`http://nome host server ISA:numero porta listener Web/percorso esterno applicazione`
Ad esempio: `http://myISAServer:80/Product/BOE/CMC`

Nota:

Può essere necessario aggiornare più volte il browser.

È necessario modificare i criteri HTTP per la regola appena configurata per assicurarsi di poter accedere alla console CMC. Fare clic con il pulsante destro del mouse sulla regola creata nell'utilità Gestione di ISA Server e selezionare **Configura HTTP**. È ora necessario deselezionare **Verifica normalizzazione** nell'area "Protezione URL".

Per accedere in remoto alla piattaforma BI è necessario creare una regola di accesso.

8.20 Configurazione speciale per la piattaforma BI in distribuzioni di proxy inversi

Alcuni prodotti della piattaforma BI richiedono configurazioni aggiuntive affinché possano funzionare correttamente nelle distribuzioni di proxy inverso. In questa sezione viene illustrato come eseguire configurazioni aggiuntive.

8.20.1 Abilitazione del proxy inverso per Servizi Web

In questa sezione vengono descritte le procedure richieste per abilitare i proxy inversi per i Servizi Web.

8.20.1.1 Per attivare il proxy inverso in Tomcat.

Per abilitare il proxy inverso nel server di applicazioni Web Tomcat, è necessario modificare il file `server.xml`. Tra le modifiche richieste sono incluse l'impostazione di `proxyPort` come porta di attesa del server proxy inverso e l'aggiunta di un nuovo `proxyName`. In questa sezione viene illustrata la procedura.

1. Arrestare Tomcat.
2. Aprire il file `server.xml` per Tomcat.

In Windows, il file `server.xml` si trova in `C:\Programmi (x86)\SAP BusinessObjects\Tomcat\conf`

In Unix `server.xml` si trova in `<CATALINA_HOME>/conf`. Il valore predefinito di `<CATALINA_HOME>` è `<DIRINSTALL>/sap_bobj/tomcat`.

3. Individuare questa sezione nel file `server.xml`:

```
<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!--See proxy documentation for more information about using
      this.-->
<!--
  <Connector port="8082"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
    enableLookups="false"
    acceptCount="100" debug="0" connectionTimeout="20000"
    proxyPort="80" disableUploadTimeout="true" />
-->
```

4. Rimuovere il commento all'elemento connettore eliminando `<!-- e -->`.
5. Modificare il valore di `proxyPort` in modo che rappresenti la porta di attesa del server proxy inverso.
6. Aggiungere un nuovo attributo `proxyName` all'elenco degli attributi del connettore. Il valore di `proxyName` deve rappresentare il nome del server proxy risolvibile sull'indirizzo IP corretto da parte di Tomcat.

Esempio:

```
<!--Define a Proxied HTTP/1.1 Connector on port 8082 -->
  <!--See proxy documentation for more information about using
        this.-->
  <Connector port="8082"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
    enableLookups="false"
    acceptCount="100" debug="0" connectionTimeout="20000"
    proxyName="my_reverse_proxy_server.domain.com"
    proxyPort="ReverseProxyServerPort"
    disableUploadTimeout="true" />
```

Dove `server_proxy_inverso.dominio.come` `PortaServerProxyInverso` devono essere sostituiti dal nome del server proxy inverso corretto e dalla relativa porta di attesa.

7. Salvare e chiudere il file `server.xml`.
8. Riavviare Tomcat.

9. Accertarsi che il percorso virtuale del server proxy inverso venga mappato alla porta del connettore Tomcat corretta. Nell'esempio precedente la porta è 8082.

Nell'esempio riportato di seguito viene illustrata una configurazione di esempio per Apache HTTP Server 2.2 per Servizi Web di SAP BusinessObjects con proxy inverso distribuiti in Tomcat:

```
ProxyPass /XI3.0/dswsbobje http://internalServer:8082/dswsbobje
ProxyPassReverseCookiePath /dswsbobje /XI3.0/dswsbobje
```

Per abilitare i servizi Web, è necessario identificare il nome del proxy e il numero di porta per il connettore.

8.20.1.2 Abilitazione del proxy inverso per Servizi Web su server di applicazioni Web diversi da Tomcat

Per la procedura seguente è necessario che le applicazioni Web della piattaforma BI siano configurate correttamente rispetto al server di applicazioni Web scelto. I nomi di `wsresources` fanno distinzione tra maiuscole e minuscole.

1. Arrestare il server di applicazioni Web.
2. Specificare l'URL esterno dei Servizi Web nel file `dsws.properties`.

Questo file si trova nell'applicazione Web `dswsbobje`. Se ad esempio l'URL esterno è `http://server_proxy_inverso.dominio.com/dswsbobje/`, aggiornare le seguenti proprietà nel file `dsws.properties`:

- `wsresource1=ReportEngine|reportengine web service alone|http://server_proxy_inverso.dominio.com/SAP/dswsbobje/services/ReportEngine`
- `wsresource2=BICatalog|bicatalog web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BICatalog`
- `wsresource3=Publish|publish web service alone|http://server_proxy_inverso.dominio.com/SAP/dswsbobje/services/Publish`
- `wsresource4=QueryService|query web service alone|http://server_proxy_inverso.dominio.com/SAP/dswsbobje/services/QueryService`
- `wsresource5=BIPlatform|BIPlatform web service|http://server_proxy_inverso.dominio.com/SAP/dswsbobje/services/BIPlatform`
- `wsresource6=LiveOffice|Live Office web service|http://server_proxy_inverso.dominio.com/SAP/dswsbobje/services/LiveOffice`

3. Salvare e chiudere il file `dsws.properties`.
4. Riavviare il server di applicazioni Web.
5. Accertarsi che il percorso virtuale del server proxy inverso venga mappato alla porta del connettore del server di applicazioni Web corretta. Di seguito viene illustrata una configurazione di esempio per Apache HTTP Server 2.2 su Servizi Web della piattaforma BI con proxy inverso distribuiti sul server di applicazioni Web scelto:

```
ProxyPass /SAPI/dswsbobje http://internalServer:<porta di attesa> /dsws
bobje
```

```
ProxyPassReverseCookiePath /dswsbobje /SAP/dswsbobje
```

dove <porta di attesa> è la porta di attesa del server di applicazioni Web.

8.20.2 Abilitazione del percorso principale per i cookie di sessione per ISA 2006

In questa sezione viene descritto come configurare server di applicazioni Web specifici per abilitare il percorso principale per l'utilizzo dei cookie di sessione con ISA 2006 come server proxy inverso.

8.20.2.1 Per configurare Apache Tomcat

Per configurare il percorso principale per il funzionamento dei cookie di sessione con ISA 2006 come server proxy inverso, aggiungere quanto segue all'elemento `<Connector>` in `server.xml`:

```
emptySessionPath="true"
```

1. Arrestare Tomcat.
2. Aprire il file `server.xml` che si trova nella directory:
`<CATALINA_HOME>\conf`
3. Individuare la seguente sezione nel file `server.xml`:

```
<!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
<!-- See proxy documentation for more information about using this -->
<!--
<Connector port="8082"
maxThreads="150" minSpareThreads="25" maxS
pareThreads="75" enableLookups="false"
acceptCount="100" debug="0" connectionTimeout="20000"
proxyPort="80" disableUploadTimeout="true" />
-->
```

4. Rimuovere il commento all'elemento connettore eliminando `<!-- e -->`.
5. Per configurare il percorso principale per il funzionamento dei cookie di sessione con ISA 2006 come server proxy inverso, aggiungere quanto segue all'elemento `<Connector>` in `server.xml`:

```
emptySessionPath="true"
```

6. Modificare il valore di `proxyPort` in modo che rappresenti la porta di attesa del server proxy inverso.
7. Aggiungere un nuovo attributo `proxyName` all'elenco degli attributi del connettore. Il valore deve rappresentare il nome del server proxy risolvibile sull'indirizzo IP corretto da parte di Tomcat.

Ad esempio:

```
<!--Define a Proxied HTTP/1.1 Connector on port 8082
-->
<!-- See proxy documentation for more information about using
this -->
<Connector port="8082"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" emptySessionPath="true"
acceptCount="100" debug="0" connectionTimeout="20000"
proxyName="my_reverse_proxy_server.domain.com"
proxyPort="ReverseProxyServerPort"
disableUploadTimeout="true" />
```

8. Salvare e chiudere il file `server.xml`.

9. Riavviare Tomcat.

Accertarsi che il percorso virtuale del server proxy inverso venga mappato alla porta del connettore Tomcat corretta. Nell'esempio precedente la porta è 8082.

8.20.2.2 Configurazione di Sun Java 8.2

È necessario modificare il file `sun-web.xml` per ogni applicazione Web della piattaforma BI.

1. Andare a `<SUN_WEBAPP_DOMAIN>\generated\xml\j2ee-modules\webapps\BOE\WEB-INF`
2. Aprire `sun-web.xml`.
3. Dopo il contenitore `<context-root>` aggiungere quanto segue:

```
<session-config>
  <cookie-properties>
    <property name="cookiePath" value="/" />
  </cookie-properties>
</session-config>
<property name="reuseSessionID" value="true"/>
```

4. Salvare e chiudere `sun-web.xml`.
5. Ripetere i passaggi 1-4 per ogni applicazione Web.

8.20.2.3 Configurazione di Oracle Application Server 10gR3

È necessario modificare il file `global-web-application.xml` o `orion-web.xml` per ogni directory di distribuzione delle applicazioni Web della piattaforma BI.

1. Andare a `<ORACLE_HOME>\j2ee\home\config\`
2. Aprire `global-web-application.xml` o `orion-web.xml`.
3. Aggiungere la riga seguente al contenitore `<orion-web-app>`:

```
<session-tracking cookie-path="/" />
```

4. Salvare e chiudere il file di configurazione.

5. Accedere alla console di amministrazione Oracle:

- a. Andare a **OC4J:home > Administration > Server Properties** (Amministrazione - Proprietà server).
- b. Selezionare **Options** (Opzioni) in "Command Line Options" (Opzioni della riga di comando).
- c. Fare clic su **Add another Row** (Aggiungi un'altra riga) e digitare quanto segue:

```
Doracle.useSessionIDFromCookie=true
```

6. Riavviare il server Oracle.

8.20.2.4 Per configurare WebSphere Community Edition 2.0

1. Aprire la console di amministrazione di WebSphere Community Edition 2.0.
2. Nel pannello di spostamento sinistro individuare "Server" e selezionare **Web Server**.
3. Selezionare i connettori e fare clic su **Modifica**.
4. Selezionare la casella di controllo **emptySessionPath** e fare clic su **Save**.
5. Digitare il nome del server ISA in **ProxyName**.
6. Digitare il numero della porta di attesa ISA in **ProxyPort**.
7. Arrestare e riavviare il connettore.

8.20.3 Abilitazione di reverse proxy per SAP BusinessObjects Live Office

Per abilitare la funzionalità Visualizza oggetto nel browser Web di SAP BusinessObjects Live Office per reverse proxy, modificare l'URL del visualizzatore predefinito. Questa operazione può essere eseguita in Central Management Console (CMC) o tramite le opzioni di Live Office.

Nota:

le operazioni descritte in questa sezione presuppongono che siano stati abilitati correttamente i proxy inversi per BI Launch Pad e per la piattaforma BI.

8.20.3.1 Regolazione dell'URL del visualizzatore predefinito nella CMC

1. Accedere alla CMC.
2. Nella pagina "Applicazioni", fare clic su **Central Management Console**.
3. Selezionare **Azioni > Impostazioni di elaborazione**.
4. Nel campo **URL** selezionare l'URL corretto del visualizzatore predefinito e fare clic su **Salva e chiudi**.

Ad esempio:

```
http://ReverseProxyServer:ReverseProxyServerPort/BOE/OpenDocument.jsp?sID  
Type=CUID&iDocID=%SI_CUID%
```

`ReverseProxyServer` e `ReverseProxyServerPort` sono il nome del server proxy inverso corretto e della relativa porta di attesa.

Autenticazione

9.1 Opzioni di autenticazione nella piattaforma BI

L'autenticazione è il processo con cui si verifica l'identità di un utente che tenta di accedere al sistema, mentre la gestione dei diritti è il processo che verifica se l'utente dispone dei diritti sufficienti per eseguire l'operazione richiesta sull'oggetto specificato.

I plug-in di protezione espandono e personalizzano le modalità di autenticazione degli utenti della piattaforma BI. I plug-in di protezione semplificano la creazione e la gestione di account consentendo la mappatura di account utente e gruppi da sistemi di terze parti nella piattaforma. È possibile mappare account utente o gruppi di terze parti ad account utente o gruppi della piattaforma BI esistenti o creare nuovi account utente o gruppi Enterprise che corrispondano a ciascuna voce mappata nel sistema esterno.

La versione attuale supporta i seguenti metodi di autenticazione:

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

Poiché la piattaforma BI è completamente personalizzabile, i processi di autenticazione possono variare da sistema a sistema.

Argomenti correlati

- [Presentazione dell'autenticazione Enterprise](#)
- [Configurazione dell'autenticazione SAP](#)
- [Utilizzo dell'autenticazione LDAP](#)
- [Requisiti di supporto e impostazione iniziale di Windows AD](#)
- [Abilitazione dell'autenticazione JD Edwards EnterpriseOne](#)
- [Abilitazione dell'autenticazione Oracle EBS](#)
- [Abilitazione dell'autenticazione PeopleSoft Enterprise](#)
- [Abilitazione dell'autenticazione Siebel](#)

9.1.1 Autenticazione principale

L'autenticazione principale si verifica al primo tentativo di collegamento al sistema da parte dell'utente. Durante l'autenticazione principale può verificarsi una delle due situazioni seguenti:

- Se non è configurata la funzione Single Sign-On, l'utente fornisce le proprie credenziali, ad esempio il nome utente, la password e il tipo di autenticazione.

Questi dettagli vengono immessi nella schermata di accesso.

- Se è configurato un metodo di Single Sign-On, le credenziali degli utenti vengono propagate in modo invisibile.

Tali dettagli vengono estratti utilizzando metodi come Kerberos o SiteMinder.

Il tipo di autenticazione può essere Enterprise, LDAP, Windows AD, SAP, Oracle EBS, Siebel, JD Edwards EnterpriseOne, PeopleSoft Enterprise in base ai tipi abilitati e configurati nell'area di gestione delle autenticazioni della console CMC (Central Management Console). Il browser Web dell'utente invia le informazioni tramite HTTP al server Web, che indirizza le informazioni al CMS o al server della piattaforma appropriato.

Il server di applicazioni Web passa le informazioni dell'utente a uno script lato server. Lo script comunica internamente con l'SDK e, alla fine, il plug-in di protezione appropriato autentica l'utente in base al database degli utenti.

Ad esempio, se l'utente accede a BI Launch Pad e specifica l'autenticazione Enterprise, l'SDK assicura che il plug-in di protezione della piattaforma BI esegua l'autenticazione. Il Central Management Server (CMS) utilizza il plug-in di protezione per verificare nome utente e password a fronte del database di sistema. Se invece l'utente specifica un metodo di autenticazione differente, l'SDK utilizza il plug-in di protezione corrispondente per autenticare l'utente.

Se il plug-in di protezione riscontra una combinazione corretta di credenziali, il server CMS concede all'utente un'identità di sistema attiva e vengono eseguite le azioni seguenti:

- Il CMS crea una sessione Enterprise per l'utente. Quando è attiva, questa sessione utilizza una licenza dell'utente sul sistema.
- Il CMS genera e codifica un token di accesso e lo invia al server di applicazioni Web.
- Il server di applicazioni Web memorizza le informazioni dell'utente in una variabile di sessione. Quando è attiva, questa sessione memorizza informazioni che consentono alla piattaforma BI di rispondere alla richiesta dell'utente.

Nota:

La variabile di sessione non contiene la password dell'utente.

- Il server di applicazioni Web mantiene il token di accesso in un cookie sul browser del client. Il token viene utilizzato solo a scopo di failover, ad esempio quando è presente un server CMS cluster o quando BI Launch Pad viene utilizzato in cluster per affinità di sessione.

Nota:

È possibile disabilitare il token di accesso, ma in tal caso viene disabilitato il failover.

9.1.2 Plug-in di protezione

I plug-in di protezione espandono e personalizzano le modalità di autenticazione degli utenti della piattaforma BI. La piattaforma BI viene attualmente fornita con i seguenti plug-in:

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

I plug-in di protezione semplificano la creazione e la gestione di account consentendo la mappatura di account utente e gruppi da sistemi di terze parti nella piattaforma BI. È possibile mappare account utente o gruppi di terze parti ad account utente o gruppi della piattaforma BI esistenti o creare nuovi account utente o gruppi Enterprise che corrispondano a ciascuna voce mappata nel sistema esterno.

I plug-in di protezione gestiscono dinamicamente elenchi di utenti e gruppi di terze parti. Una volta mappato un gruppo esterno nella piattaforma BI, tutti gli utenti che appartengono al gruppo in questione possono accedere correttamente alla piattaforma BI. Quando si apportano modifiche successive all'appartenenza al gruppo di terze parti, non è necessario aggiornare l'elenco nella piattaforma BI. Se ad esempio si esegue la mappatura di un gruppo LDAP alla piattaforma BI e successivamente si aggiunge un nuovo utente al gruppo, il plug-in di protezione crea dinamicamente un alias per il nuovo utente quando questo accede per la prima volta alla piattaforma BI con credenziali LDAP valide.

I plug-in di protezione consentono inoltre di assegnare diritti a utenti e gruppi in maniera coerente, in quanto gli utenti e i gruppi mappati sono considerati come gli account Enterprise. È possibile ad esempio mappare alcuni account utente o gruppi da Windows AD e alcuni da un server di elenchi in linea LDAP. In seguito, quando sarà necessario assegnare diritti o creare nuovi gruppi personalizzati nella piattaforma BI, sarà possibile impostare tutti i valori nella console CMC.

Ciascun plug-in di protezione funge da provider di autenticazione in quanto verifica le credenziali dell'utente corrente rispetto al database utente appropriato. Quando gli utenti accedono alla piattaforma BI, possono scegliere tra i diversi tipi di autenticazione abilitati e impostati nell'area di gestione Autenticazione della console CMC.

Nota:

Il plug-in di protezione di Windows AD non è in grado di autenticare gli utenti se i componenti server della piattaforma BI vengono eseguiti in UNIX.

9.1.3 Single Sign On alla piattaforma BI

Il Single Sign On alla piattaforma BI consente agli utenti che hanno già effettuato l'accesso al sistema operativo di accedere alle applicazioni che supportano SSO senza dover fornire nuovamente le credenziali. Quando un utente effettua l'accesso, viene creato un contesto di protezione per quell'utente. Questo contesto può essere propagato alla piattaforma BI per l'esecuzione del Single Sign On.

Anche il termine "Single Sign On anonimo" si riferisce al Single Sign On alla piattaforma BI e, in modo più specifico, alla funzionalità di Single Sign On dell'account utente Guest. Quando si abilita l'account utente Guest, vale a dire l'impostazione predefinita, qualsiasi account potrà accedere alla piattaforma BI come Guest e disporrà dell'accesso al sistema.

9.1.3.1 Supporto Single Sign-On

Il termine Single Sign On è utilizzato per descrivere scenari diversi. Al livello di base, si riferisce a una situazione in cui un utente è in grado di accedere a due o più applicazioni o sistemi fornendo le credenziali di accesso una sola volta, in modo da semplificare l'interazione degli utenti con il sistema.

Il Single Sign On a BI Launch Pad può essere fornito dalla piattaforma BI o da diversi strumenti di autenticazione, in base al tipo di server delle applicazioni e di sistema operativo.

Questi metodi di Single Sign On sono disponibili se si utilizza un server applicazioni Java in Windows:

- Windows AD con Kerberos
- Windows AD con SiteMinder

Questi metodi di Single Sign On sono disponibili se si utilizza IIS in Windows:

- Windows AD con Kerberos
- Windows AD con NTLM
- Windows AD con SiteMinder

I metodi seguenti di supporto Single Sign On sono disponibili in Windows o Unix, con qualsiasi server di applicazioni Web supportato per la piattaforma.

- LDAP con SiteMinder
- Autenticazione affidabile
- Windows AD con Kerberos
- LDAP tramite Kerberos su SUSE 11
- SAP NetWeaver SSO tramite autenticazione affidabile

Nota:

Windows AD con Kerberos è supportato se l'applicazione Java si trova in UNIX. Tuttavia, i servizi della piattaforma BI devono essere eseguiti in un server Windows.

Nella tabella di seguito vengono descritti i metodi del supporto di Single Sign-On per BI Launch Pad.

Modalità di autenticazione	Server CMS	Opzioni	Note
Windows AD	Solo Windows	Solo Windows AD con Kerberos	L'autenticazione Windows AD a BI Launch Pad e alla console CMC è disponibile direttamente.
LDAP	Qualsiasi piattaforma supportata	Solo server directory LDAP supportati con SiteMinder	L'autenticazione LDAP a BI Launch Pad e alla console CMC è disponibile direttamente. Per SSO a BI Launch Pad e alla console CMC è richiesto SiteMinder.
Enterprise	Qualsiasi piattaforma supportata	Autenticazione affidabile	L'autenticazione Enterprise a BI Launch Pad e alla console CMC è disponibile direttamente. Per il SSO con autenticazione Enterprise a BI Launch Pad e alla console CMC è richiesta l'autenticazione affidabile.

- [Single Sign On alla piattaforma BI](#)
- [Single Sign-On al database](#)
- [Single Sign-On end-to-end](#)

9.1.3.2 Single Sign-On al database

Dopo l'accesso alla piattaforma BI, il Single Sign On al database consente agli utenti di eseguire azioni che richiedono l'accesso al database, quali in particolare la visualizzazione e l'aggiornamento dei report, senza fornire nuovamente le credenziali di accesso. Il Single Sign On al database può essere combinato con il Single Sign On alla piattaforma BI, per consentire agli utenti un accesso ancora più semplice alle risorse necessarie.

9.1.3.3 Single Sign-On end-to-end

Il Single Sign On end-to-end si riferisce a una configurazione in cui gli utenti dispongono sia dell'accesso con Single Sign On alla piattaforma BI nel front-end, sia dell'accesso con Single Sign On ai database di back-end. Pertanto, per avere accesso alla piattaforma BI ed essere in grado di eseguire azioni che richiedono l'accesso al database, ad esempio la visualizzazione dei report, gli utenti dovranno fornire le proprie credenziali di accesso una sola volta, nel momento in cui accedono al sistema operativo.

Nella piattaforma BI, il Single Sign On end-to-end è supportato tramite Windows AD e Kerberos.

9.2 autenticazione Enterprise

9.2.1 Presentazione dell'autenticazione Enterprise

Poiché l'autenticazione Enterprise rappresenta il metodo di autenticazione predefinito della piattaforma BI, viene abilitata automaticamente alla prima installazione del sistema e non può essere disabilitata. Quando vengono aggiunti e gestiti utenti e gruppi, la piattaforma conserva all'interno del database le informazioni ad essi correlate.

Suggerimento:

Utilizzare l'autenticazione Enterprise predefinita del sistema se si preferisce creare account e gruppi distinti da utilizzare con la piattaforma BI oppure se non è stata ancora impostata una gerarchia di utenti e di gruppi in un server di directory di terze parti.

Non è necessario configurare o abilitare l'autenticazione Enterprise. È tuttavia possibile modificarne le impostazioni in base ai requisiti di protezione specifici dell'organizzazione. Le impostazioni dell'autenticazione Enterprise possono essere modificate solo mediante la console CMC (Central Management Console).

9.2.2 Impostazioni di autenticazione Enterprise

Impostazioni	Opzioni	Descrizione
Restrizioni password	Attiva password con maiuscole e minuscole	Questa opzione garantisce che le password contengano almeno due delle seguenti classi di caratteri: lettere maiuscole, lettere minuscole, numeri o simboli di punteggiatura.
	Devono essere contenuti almeno N caratteri	Inserendo un minimo di complessità per le password è possibile ridurre le possibilità dell'utente di indovinare una password valida.
Restrizioni utente	È necessario modificare la password ogni N giorni	Questa opzione garantisce che le password non diventino vulnerabili e vengano aggiornate regolarmente.
	Impossibile riutilizzare le N password più recenti	Questa opzione garantisce che le password non vengano ripetute con regolarità.

Impostazioni	Opzioni	Descrizione
	È necessario attendere N minuti per modificare la password	Questa opzione garantisce che, una volta immesse nel sistema, le nuove password non possano essere subito modificate.
Restrizioni accesso	Disattiva account dopo N tentativi di accesso non riusciti	Questa opzione di protezione specifica il numero di tentativi di accesso al sistema concessi all'utente prima che l'account venga disabilitato.
	Reimposta conteggio accessi non riusciti dopo N minuti	Questa opzione specifica un intervallo di tempo per la reimpostazione del contatore dei tentativi di accesso.
	Riattiva account dopo N minuti	Questa opzione specifica per quanto tempo viene sospeso un account dopo N tentativi di accesso non riusciti.
Sincronizza credenziali origine dati all'accesso	Abilita e aggiorna le credenziali dell'origine dati dell'utente all'accesso	Questa opzione abilita le credenziali dell'origine dati dopo l'accesso dell'utente.
Autenticazione affidabile	Autenticazione affidabile attiva	Specifica le impostazioni per la configurazione dell'Autenticazione affidabile.

Argomenti correlati

- [Abilitazione dell'Autenticazione affidabile](#)

9.2.3 Modifica delle impostazioni del database

1. Passare all'area di gestione "Autenticazione" della CMC.
2. Fare doppio clic su **Enterprise**.
Verrà visualizzata la finestra di dialogo "Enterprise".
3. Modificare le impostazioni.

Suggerimento:

per ripristinare il valore predefinito di tutte le impostazioni, fare clic su **Reimposta**.

4. Fare clic su **Aggiorna** per salvare le modifiche.

9.2.3.1 Per modificare le impostazioni generali della password

Nota:

gli account non utilizzati per un periodo di tempo esteso non vengono disattivati automaticamente. Gli amministratori devono eliminare manualmente gli account non attivi.

1. Passare all'area di gestione "Autenticazione" della CMC.
2. Fare doppio clic su **Enterprise**.
Verrà visualizzata la finestra di dialogo "Enterprise".
3. Selezionare la casella di controllo per ciascuna impostazione della password da usare e specificare un valore se richiesto.

La tabella seguente identifica i valori minimo e massimo per ogni impostazione correlata alla password che è possibile configurare.

Impostazione password	Minimo	Massimo consigliato
Attiva password con maiuscole e minuscole	N/D	N/D
Devono essere contenuti almeno N caratteri	0 caratteri	64 caratteri
È necessario modificare la password ogni N giorni	1 giorno	100 giorni
Impossibile riutilizzare le N password più recenti	1 password	100 password
È necessario attendere N minuti per modificare la password	0 minuti	100 minuti
Disattiva account dopo N tentativi di accesso non riusciti	1 non riuscito	100 non riusciti

Impostazione password	Minimo	Massimo consigliato
Reimposta il conteggio degli accessi non riusciti dopo N minuti	1 minuto	100 minuti
Riattiva account dopo N minuti	0 minuti	100 minuti

4. Fare clic su **Aggiorna**.

Nota:

gli account Enterprise inattivi non vengono disabilitati automaticamente. Devono essere eliminati manualmente dagli amministratori di sistema.

9.2.4 Abilitazione dell'Autenticazione affidabile

L'Autenticazione affidabile Enterprise viene utilizzata per eseguire il Single Sign On affidandosi al server di applicazioni Web per verificare l'identità di un utente. Questo metodo di autenticazione prevede la definizione dell'attendibilità tra il server CMS (Central Management Server) e il server di applicazioni Web che ospita l'applicazione Web della piattaforma BI. Una volta definita l'attendibilità, il sistema delega il compito di verificare l'identità di un utente al server di applicazioni Web. L'Autenticazione affidabile può essere utilizzata per supportare metodi di autenticazione quali SAML, x.509 e altri metodi che non dispongono di plug-in di autenticazione dedicati.

Gli utenti preferiscono accedere al sistema una sola volta, senza dovere immettere più volte la password durante le sessioni. L'Autenticazione affidabile fornisce una soluzione Single Sign On Java che consente di integrare l'autenticazione della piattaforma BI con soluzioni di autenticazione di terze parti. Le applicazioni che stabiliscono una connessione fidata con il Central Management Server (CMS) possono usare l'Autenticazione affidabile per accedere al sistema senza password.

Per abilitare l'Autenticazione affidabile, è necessario configurare un segreto condiviso nel server mediante le impostazioni di autenticazione Enterprise, mentre il client viene configurato mediante le proprietà specificate per il file `BOE.war`.

Nota:

- Per poter utilizzare l'autenticazione affidabile, è necessario avere creato utenti Enterprise o avere mappato utenti di terze parti che dovranno accedere alla piattaforma BI.
- L'URL di Single Sign On per BI Launch Pad è `http://server:porta/BOE/BI`.

Argomenti correlati

- [Per configurare il server per l'uso dell'Autenticazione affidabile:](#)
- [Configurazione di Autenticazione affidabile per l'applicazione Web](#)

9.2.4.1 Per configurare il server per l'uso dell'Autenticazione affidabile:

Per poter configurare Autenticazione affidabile, è necessario avere creato utenti Enterprise o avere mappato utenti di terze parti che dovranno accedere alla piattaforma BI.

1. Accedere alla CMC.
 2. Accedere all'area di gestione "Autenticazione".
 3. Fare clic sull'opzione **Enterprise**.
Viene visualizzata la finestra di dialogo "Enterprise".
 4. In "Autenticazione affidabile":
 - a. Fare clic su **Autenticazione affidabile attivata**.
 - b. Fare clic su **Nuova chiave privata condivisa**.
Viene visualizzato il messaggio Una chiave privata condivisa è stata generata ed è pronta per il download.
 - c. Fare clic su **Scarica chiave privata condivisa**.
Il segreto condiviso viene utilizzato dal client e dal server CMS per stabilire una connessione affidabile. È necessario configurare prima il server, quindi il computer client per Autenticazione affidabile.
Viene visualizzata la finestra di dialogo "Download di file".
 - d. Fare clic su **Salva**, quindi salvare il file `TrustedPrincipal.conf` in una delle directory seguenti:
 - `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\win64_x64\`
 - `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`
- Avvertenza:**
Non impostare il timeout su 0 (zero). Il valore 0 indica che il tempo di scarto consentito tra gli orari dei due orologi è illimitato e questa condizione può aumentare la vulnerabilità agli attacchi di tipo replay.
- e. Nel campo **Periodo validità segreto condiviso** immettere il numero di giorni di validità del segreto condiviso.
 - f. Specificare il tempo massimo, in millisecondi, di scarto possibile tra l'orologio del computer client e l'orologio nel CMS per le richieste di Autenticazione affidabile.
5. Fare clic su **Aggiorna** per salvare il segreto condiviso.

La piattaforma BI non controlla tutte le modifiche dei parametri di Autenticazione affidabile. È necessario eseguire manualmente il backup di tutte le informazioni di Autenticazione affidabile.

Il segreto condiviso viene utilizzato dal client e dal server CMS per stabilire una connessione affidabile. Il passaggio successivo consiste nella configurazione del client per Autenticazione affidabile.

9.2.5 Configurazione dell'Autenticazione affidabile per l'applicazione Web

Per configurare Autenticazione affidabile per il client, è necessario modificare le proprietà globali per il file `BOE.war` e le proprietà specifiche per le applicazioni BI Launch Pad e OpenDocument.

Utilizzare uno dei metodi seguenti per passare il segreto condiviso al client:

- Opzione `WEB_SESSION`
- File `TrustedPrincipal.conf`

Utilizzare uno dei metodi seguenti per passare il nome utente al client:

- `REMOTE_USER`
- `HTTP_HEADER`
- `COOKIE`
- `QUERY_STRING`
- `WEB_SESSION`
- `USER_PRINCIPAL`

Qualsiasi metodo utilizzato per passare il segreto condiviso deve essere personalizzato nelle proprietà globali `Trusted.auth.user.retrieval` per il file `BOE.war`.

9.2.5.1 Uso di Autenticazione affidabile per il Single Sign On SAML

Il linguaggio SAML (Security Assertion Markup Language) è uno standard basato su XML per la comunicazione di informazioni sull'identità che offre una connessione protetta in cui l'identità e l'attendibilità vengono comunicate attraverso l'abilitazione di un meccanismo di Single Sign On che elimina accessi aggiuntivi per utenti attendibili che cercano di accedere alla piattaforma BI.

Abilitazione dell'autenticazione SAML

Se il server delle applicazioni può funzionare come provider di servizi SAML, è possibile utilizzare Autenticazione affidabile per fornire il SSO SAML alla piattaforma BI.

A tale scopo, è necessario innanzitutto configurare il server di applicazioni Web per l'autenticazione SAML.

Per passare il nome utente al client è inoltre necessario utilizzare uno di questi metodi:

- `REMOTE_USER`
- `USER_PRINCIPAL`

Nell'esempio che segue viene utilizzato un file web.xml configurato per l'autenticazione SAML:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>InfoView</web-resource-name>
    <url-pattern>*/</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>j2ee-admin</role-name>
    <role-name>j2ee-guest</role-name>
    <role-name>j2ee-special</role-name>
  </auth-constraint>
  <user-data-constraint>
    <transport-guarantee>NONE</transport-guarantee>
  </user-data-constraint>
</security-constraint>
<login-config>
  <auth-method>FORM</auth-method>
  <realm-name>InfoView</realm-name>
  <form-login-config>
    <form-login-page>/logon.jsp</form-login-page>
    <form-error-page>/logon.jsp</form-error-page>
  </form-login-config>
</login-config>
<security-role>
  <description>Assigned to the SAP J2EE Engine System Administrators</description>
  <role-name>j2ee-admin</role-name>
</security-role>
<security-role>
  <description>Assigned to all users</description>
  <role-name>j2ee-guest</role-name>
</security-role>
<security-role>
  <description>Assigned to a special group of users</description>
  <role-name>j2ee-special</role-name>
</security-role>
```

Per ulteriori istruzioni su come eseguire questa operazione, fare riferimento alla documentazione del server di applicazioni, dal momento che potrebbero essere diverse da un server all'altro.

Uso di Autenticazione affidabile

Dopo aver configurato il server di applicazioni Web affinché funzioni come provider di servizi SAML, è possibile utilizzare Autenticazione affidabile per fornire il SSO SAML.

Nota:

È necessario che gli utenti vengano importati nella piattaforma BI o dispongano di account Enterprise.

Per abilitare il SSO, viene utilizzata la creazione di alias dinamica. Quando un utente accede per la prima volta alla pagina di accesso attraverso SAML, un messaggio chiede di collegarsi manualmente utilizzando le credenziali già esistenti per l'account della piattaforma BI. Dopo aver verificato le credenziali dell'utente, il sistema assegna all'identità SAML dell'utente un alias nell'account della piattaforma BI. I tentativi di accesso successivi per l'utente verranno eseguiti attraverso il SSO in quanto l'alias di identità dell'utente verrà messo automaticamente in corrispondenza con un account esistente.

Nota:

per far sì che il meccanismo funzioni, è necessario abilitare una proprietà specifica per il file war BOE: `trusted.auth.user.namespace.enabled`.

9.2.5.2 Proprietà di Autenticazione affidabile per le applicazioni Web

Nella tabella che segue sono elencate le impostazioni di Autenticazione affidabile nel file `global.properties` predefinito per il file `BOE.war`. Per sovrascrivere le impostazioni, creare un nuovo file in `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Proprietà	Valore predefinito	Descrizione
<code>sso.enabled=true</code>	<code>sso.enabled=false</code>	Abilita e disabilita il Single Sign On (SSO) nella piattaforma BI. Impostare su <code>true</code> per consentire l'autenticazione affidabile.
<code>trusted.auth.shared.secret</code>	Nessuno	Nome di variabile della sessione utilizzato per recuperare il segreto per Autenticazione affidabile. Si applica solo se si utilizza la sessione Web per passare il segreto condiviso.
<code>trusted.auth.user.param</code>	Nessuno	Specifica la variabile utilizzata per recuperare il nome utente per Autenticazione affidabile.
<code>trusted.auth.user.retrieval</code>	Nessuno	<p>Specifica il metodo utilizzato per recuperare il nome utente per Autenticazione affidabile:</p> <ul style="list-style-type: none"> • <code>REMOTE_USER</code> • <code>HTTP_HEADER</code> • <code>COOKIE</code> • <code>QUERY_STRING</code> • <code>WEB_SESSION</code> • <code>USER_PRINCIPAL</code> <p>Non specificare alcun valore per disabilitare Autenticazione affidabile.</p>
<code>trusted.auth.user.namespace.enabled</code>	Nessuna	<p>Abilita e disabilita il collegamento dinamico degli alias ad account utente esistenti. Se impostata su <code>true</code>, Autenticazione affidabile utilizza il collegamento degli alias per autenticare gli utenti nella piattaforma BI. Con il collegamento degli alias, il server di applicazioni può funzionare come un provider di servizi SAML, abilitando Autenticazione affidabile affinché fornisca Single Sign On SAML al sistema.</p> <p>Se questa proprietà è vuota, Autenticazione affidabile utilizzerà un nome corrispondente durante l'autenticazione degli utenti.</p>

9.2.5.3 Configurazione di Autenticazione affidabile per l'applicazione Web

Se si intende memorizzare il segreto condiviso nel file `TrustedPrincipal.conf`, assicurarsi che il file sia memorizzato nella directory della piattaforma appropriata:

Piattaforma	Posizione di TrustedPrincipal.conf
Windows, installazione predefinita	<ul style="list-style-type: none"> <DIRINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\ <DIRINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\
AIX	<DIRINSTALL>/sap_bobj/enterprise_xi40/ aix_rs6000/
Solaris	<DIRINSTALL>/sap_bobj/enterprise_xi40/solaris_sparc/
Linux	<DIRINSTALL>/sap_bobj/enterprise_xi40/linux_x86

Diversi meccanismi popolano la variabile nome utente utilizzata per configurare Autenticazione attendibile per il client che ospita le applicazioni Web. Configurare o impostare il server di applicazioni Web in uso in modo tale che i nomi utente vengano esposti prima di utilizzare i metodi di recupero dei nomi utente. Per ulteriori informazioni vedere <http://java.sun.com/j2ee/1.4/docs/api/javax/servlet/http/HttpServletRequest.html>.

Per configurare Autenticazione affidabile per il client, è necessario accedere e modificare le proprietà per il file `BOE.war`, che includono le proprietà generali e specifiche per le applicazioni Web BI Launch Pad e OpenDocument.

Nota:

potrebbero essere necessari ulteriori passaggi in base a come si intende recuperare il nome utente o il segreto condiviso.

1. Accedere alla cartella personalizzata contenente il file `BOE.war` nel computer che ospita le applicazioni Web:

```
<DIRINSTALL>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\.
```

In un secondo momento, sarà necessario ridistribuire il file `BOE.war` modificato.

2. Creare un nuovo file, utilizzando Blocco note o un'altra utilità di modifica del testo.
3. Immettere le seguenti proprietà Autenticazione affidabile:

```
sso.enabled=true
trusted.auth.user.retrieval=Method for user ID retrieval
trusted.auth.user.param=Variable
trusted.auth.shared.secret=WEB_SESSION
```

Per la proprietà `trusted.auth.shared.secret`, selezionare una delle opzioni seguenti per il recupero del nome utente:

Opzione	Metodo di recupero del nome utente
HTTP_HEADER	Il nome utente viene recuperato dai contenuti di un'intestazione HTTP. Specificare l'intestazione HTTP da utilizzare nella proprietà <code>trusted.auth.user.param</code> .
QUERY_STRING	Il nome utente viene recuperato da un parametro dell'URL di richiesta. Specificare la stringa di query da utilizzare nella proprietà <code>trusted.auth.user.param</code> .
COOKIE	Il nome utente viene recuperato da un cookie specificato. Specificare il cookie da utilizzare nella proprietà <code>trusted.auth.user.param</code> .
WEB_SESSION	Il nome utente viene recuperato dai contenuti di una variabile di sessione specificata. Specificare la variabile della sessione Web da utilizzare nella proprietà <code>trusted.auth.user.param</code> in <code>global.properties</code> .
REMOTE_USER	Il nome utente viene recuperato da una chiamata a <code>HttpServletRequest.getRemoteUser()</code> .
USER_PRINCIPAL	Il nome utente viene recuperato da una chiamata a <code>getUserPrincipal().getName()</code> sull'oggetto <code>HttpServletRequest</code> per la richiesta corrente in un servlet o JSP.

Nota:

- alcuni server di applicazioni Web richiedono che la variabile di ambiente `REMOTE_USER` sia impostata su `true` sul server. Per sapere se è necessario, consultare la documentazione del server di applicazioni Web. In caso affermativo, verificare che la variabile di ambiente sia impostata su `true`.
- se si utilizza `USER_PRINCIPAL` o `REMOTE_USER` per passare il nome utente, lasciare vuoto `trusted.auth.user.param`.

4. Salvare il file con il nome `global.properties`.
5. Riavviare il server di applicazioni Web.

Le nuove proprietà hanno effetto solo dopo la redistribuzione dell'applicazione Web BOE modificata nel computer su cui è in esecuzione il server di applicazioni Web. Utilizzare WDeploy per ridistribuire il file WAR sul server di applicazioni Web. Per ulteriori informazioni sull'utilizzo di WDeploy, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

9.2.5.3.1 Configurazioni di esempio

Passaggio del segreto condiviso attraverso il file TrustedPrincipal.conf

Nella configurazione di esempio che segue si presuppone che nella piattaforma BI sia stato creato un utente denominato "JohnDoe".

Le informazioni utente vengono memorizzate e passate attraverso la sessione Web, mentre il segreto condiviso viene passato tramite il file `TrustedPrincipal.conf`, che per impostazione predefinita si trova nella directory `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. La versione in bundle di Tomcat è il server di applicazioni Web.

1. Nella directory `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` creare un nuovo file utilizzando Blocco note o qualsiasi altra utilità di modifica del testo.
2. Per specificare le proprietà di Autenticazione affidabile, immettere i valori seguenti:

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=
```

3. Salvare il file con il nome `global.properties`.
4. Accedere al file `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp`.
5. Modificare il contenuto del file per includere i valori seguenti:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html; charset=utf-8" %>
<%
//custom Java code
request.getSession().setAttribute("MyUser", "JohnDoe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript" src="noCacheCustomResources/myScript.js"></script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI launch pad</a>
</body>
</html>
```

6. Creare il file `myScript.js` nella directory `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources`.
7. Aggiungere i valori seguenti a `myScript.js`:

```
function goToLogonPage() {
    window.location = "logon.jsp"; }
```

8. Riavviare il server di applicazioni Web.
9. Utilizzare WDeploy per ridistribuire il file WAR sul server di applicazioni Web.

Per ulteriori informazioni sull'utilizzo di WDeploy, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

Per verificare di aver configurato in modo appropriato Autenticazione affidabile, utilizzare l'URL seguente per accedere all'applicazione BI Launch Pad: `http://[nomecms]:8080/BOE/BI/custom.jsp` in cui `[nomecms]` è il nome del computer che ospita il CMS. Viene visualizzato il collegamento seguente: Fare clic su di esso per andare alla pagina di accesso di BI Launch Pad.

Passaggio del segreto condiviso attraverso la variabile di sessione Web

Nella configurazione di esempio che segue si presuppone che nella piattaforma BI sia stato creato un utente denominato *JohnDoe*.

Le informazioni sull'utente verranno memorizzate e passate attraverso la sessione Web, mentre il segreto condiviso verrà passato attraverso la variabile di sessione Web. Si presuppone che il file si trovi nella directory seguente: `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. È necessario aprire e prendere nota del contenuto del file. Nella configurazione di esempio si presuppone che il segreto condiviso sia il seguente:

```
9ecb0778edc9f048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc65773
841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

La versione in bundle di Tomcat è il server di applicazioni Web.

1. Accedere alla directory seguente:


```
<DIRINSTALL>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\
```
2. Creare un nuovo file utilizzando un editor di testo.
3. Specificare le proprietà dell'autenticazione affidabile immettendo quanto segue:

```
sso.enabled=true
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=MySecret
```

4. Salvare il file con questo nome:
proprietà globali
5. Accedere al file seguente:


```
C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\cu
stom.jsp
```
6. Modificare il contenuto del file per includere quanto segue:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html; charset=utf-8" %>
<%
//custom Java code
request.getSession().setAttribute("MySecret", "9ecb0778edc9f048edae0fcdde1a5db82112934
86774a127ec949c1bdb98dae8e0ea388979edc65773841c8ae5d1f675a6bf5d7c66038b6a3f1345
285b55a0a7")
```



```
request.getSession().setAttribute("MyUser", "JohnDoe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript" src="noCacheCustomResources/myScript.js"></script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI launch pad</a>
</body>
</html>
```

7. Creare il file myScript.js nella directory seguente:

C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources

8. Aggiungere la stringa seguente a myScript.js:

```
function goToLogonPage() {
    window.location = "logon.jsp";
}
```

9. Riavviare il server di applicazioni Web.

10. Utilizzare WDeploy per ridistribuire il file WAR sul server di applicazioni Web.

Per ulteriori informazioni sull'utilizzo di WDeploy, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

Per verificare di aver configurato in modo appropriato Autenticazione affidabile, utilizzare l'URL seguente per accedere all'applicazione BI Launch Pad: `http://[nomecms]:8080/BOE/BI/custom.jsp`, dove [nomecms] è il nome del computer che ospita il server CMS. Dovrebbe essere visualizzato il collegamento seguente:

Fare clic su di esso per andare alla pagina di accesso di BI Launch Pad

Passaggio del nome utente attraverso un utente principale

Nella configurazione di esempio che segue si presuppone che nella piattaforma BI sia stato creato un utente denominato "JohnDoe".

Le informazioni utente vengono memorizzate e passate attraverso l'opzione Nome principale utente, mentre il segreto condiviso viene passato tramite il file `TrustedPrincipal.conf`, che per impostazione predefinita si trova nella directory `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`. La versione in bundle di Tomcat è il server di applicazioni Web.

1. Arrestare il server Tomcat.

2. Aprire il file server.xml per Tomcat, che per impostazione predefinita si trova nella directory `C:\Programmi (x86)\SAP BusinessObjects\Tomcat\conf\`.

3. Individuare `<Realm className="org.apache.catalina.realm.UserDatabase Realm" .../>` e sostituirlo con il valore seguente:

```
Realm className="orgapachecatalinarealmMemoryRealm"...
```

4. Aprire il file `tomcat-users.xml` che per impostazione predefinita si trova nella directory `C:\Programmi (x86)\SAP BusinessObjects\Tomcat\conf\`.

5. Individuare il tag `<tomcat-users>` e modificare il valore seguente:

```
<user name="JohnDoe" password="password"
roles="onjavauser"/>
```

6. Aprire il file `web.xml` nella directory `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\`.

7. Prima del tag `</web-app>` aggiungere i valori seguenti:

```
<security-constraint>
  <web-resource-collection>
    <web-resource-name>OnJavaApplication</web-resource-name>
    <url-pattern>*/</url-pattern>
  </web-resource-collection>
  <auth-constraint>
    <role-name>onjavauser</role-name>
  </auth-constraint>
</security-constraint>

<login-config>
  <auth-method>BASIC</auth-method>
  <realm-name>OnJava Application</realm-name>
</login-config>
```

Immettere una pagina specifica per il parametro `<url-pattern></url-pattern>`. In genere questa pagina non rappresenta l'URL predefinito per BI Launch PAD o qualsiasi altra applicazione Web.

8. Nel file personalizzato `global.properties` immettere i valori seguenti:

```
trusted.auth.user.retrieval=USER_PRINCIPAL
trusted.auth.user.namespace.enabled=true
```

Nota:

l'impostazione di `trusted.auth.user.namespace.enabled=true` è facoltativa. Aggiungere il parametro per mappare un nome utente esterno a un nome utente della piattaforma BI diverso.

9. Riavviare il server di applicazioni Web.
10. Utilizzare WDeploy per ridistribuire il file WAR sul server di applicazioni Web.

Per ulteriori informazioni sull'utilizzo di WDeploy, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

Nota:

le configurazioni sul server di applicazioni Web sono le stesse se si utilizza il metodo Remote User.

Per verificare di aver configurato in modo appropriato Autenticazione affidabile, utilizzare l'URL seguente per accedere all'applicazione BI Launch Pad: `http://[nomecms]:8080/BOE/BI`, in cui `[nomecms]` è il nome del computer che ospita il CMS. Dopo qualche minuto viene visualizzata una finestra di dialogo di accesso.

9.3 Autenticazione LDAP

9.3.1 Utilizzo dell'autenticazione LDAP

In questa sezione viene fornita una descrizione generale del funzionamento dell'autenticazione LDAP con la piattaforma BI. Vengono quindi presentati gli strumenti di amministrazione che consentono di gestire e configurare gli account LDAP nella piattaforma.

Quando si installa la piattaforma BI, il plug-in di autenticazione LDAP viene installato automaticamente, ma non viene abilitato per impostazione predefinita. Per utilizzare l'autenticazione LDAP, è necessario accertarsi di aver impostato la rispettiva directory LDAP. Per ulteriori informazioni su LDAP, consultare la documentazione LDAP.

LDAP (Lightweight Directory Access Protocol), è un servizio comune di elenchi in linea indipendenti dalle applicazioni che consente agli utenti di condividere informazioni tra varie applicazioni. Basato su uno standard aperto, LDAP fornisce un metodo per accedere e aggiornare le informazioni all'interno di un elenco in linea.

LDAP si basa sullo standard X.500, che utilizza un protocollo di accesso agli elenchi in linea (DAP) per le comunicazioni tra un client e un server di elenchi in linea. LDAP costituisce una alternativa a DAP in quanto utilizza un numero inferiore di risorse e semplifica e omette alcune operazioni e funzioni dello standard X.500.

Nella struttura di directory di LDAP le voci sono organizzate secondo uno schema specifico. Ciascuna voce è identificata dal relativo nome DN (Distinguished Name) o CN (Common Name). Tra gli altri attributi comuni sono inclusi il nome OU (Organizational Unit) e il nome O (Organization). Un gruppo membro può, ad esempio, essere posizionato in una struttura di directory quale: cn=Utenti piattaforma BI, ou=Utenti A Enterprise, o=Ricerca. Per ulteriori informazioni, consultare la documentazione relativa al protocollo LDAP.

Poiché LDAP è indipendente dalle applicazioni, l'accesso alle relative directory è possibile per qualsiasi client che disponga dei privilegi appropriati. LDAP consente di impostare l'accesso degli utenti alla piattaforma BI tramite l'autenticazione LDAP. Offre agli utenti i diritti di accesso per gli oggetti nel sistema. Se sono in esecuzione uno o più server LDAP e si utilizza LDAP nei sistemi di computer in rete esistenti, è possibile utilizzare l'autenticazione LDAP, oltre all'autenticazione Enterprise, NT e Windows AD.

Se necessario, il plug-in di protezione LDAP fornito con la piattaforma BI può comunicare con il server LDAP utilizzando una connessione SSL stabilita mediante l'autenticazione server o reciproca. Con l'autenticazione server, al server LDAP viene assegnato un certificato di protezione che la piattaforma BI utilizza per verificare l'attendibilità del server, benché il server LDAP consenta connessioni da client anonimi. Con l'autenticazione reciproca, sia il server LDAP che la piattaforma BI vengono dotati di certificati di protezione. Per poter stabilire una connessione, il server LDAP deve inoltre verificare il certificato client.

Il plug-in di protezione LDAP fornito con la piattaforma BI può essere configurato per comunicare con il server LDAP via SSL, ma esegue sempre l'autenticazione di base quando verifica le credenziali degli utenti. Prima di implementare l'autenticazione LDAP in combinazione con la piattaforma BI, è necessario

conoscere a fondo le differenze tra questi tipi di LDAP. Per ulteriori informazioni, vedere la RFC2251, attualmente disponibile all'indirizzo <http://www.faqs.org/rfcs/rfc2251.html>.

Argomenti correlati

- [Configurazione dell'autenticazione LDAP](#)
- [Mappatura di gruppi LDAP](#)

9.3.1.1 Plug-in di protezione LDAP

Il plug-in di protezione LDAP consente di mappare account utente e gruppi dal server di directory LDAP alla piattaforma BI. Consente inoltre al sistema di verificare tutte le richieste di accesso in cui è specificata l'autenticazione LDAP. L'autenticazione degli utenti viene eseguita a fronte del server di elenchi in linea LDAP e l'appartenenza a un gruppo LDAP mappato viene verificata prima che il CMS conceda agli utenti una sessione attiva della piattaforma BI. Gli elenchi di utenti e le appartenenze di gruppo sono gestiti dinamicamente dal sistema. È possibile indicare che la piattaforma BI utilizza una connessione SSL (Secure Sockets Layer) per comunicare con il server di elenchi in linea LDAP, per garantire una maggiore protezione.

L'autenticazione LDAP per la piattaforma BI è simile all'autenticazione Windows AD, in quanto consente di mappare gruppi e di impostare l'autenticazione, i diritti di accesso e la creazione di alias. Come accade con l'autenticazione NT o AD, è possibile creare nuovi account Enterprise per utenti LDAP esistenti e assegnare alias LDAP ad utenti esistenti, se i nomi utente corrispondono ai nomi utente Enterprise. È inoltre possibile:

- Mappare utenti e gruppi dal servizio di elenchi in linea LDAP.
- Mappare LDAP in relazione ad AD. Esistono diverse restrizioni se si configura LDAP rispetto ad AD.
- Specificare più nomi host e le relative porte.
- Configurare LDAP con SiteMinder.

Dopo avere mappato gli utenti e i gruppi LDAP, l'autenticazione LDAP sarà supportata da tutti gli strumenti client della piattaforma BI. Sarà anche possibile creare applicazioni personalizzate che supportino l'autenticazione LDAP.

Argomenti correlati

- [Configurazione delle impostazioni SSL per l'autenticazione del server LDAP o reciproca](#)
- [Mappatura di LDAP a Windows AD](#)
- [Configurazione del plug-in LDAP per SiteMinder](#)

9.3.2 Configurazione dell'autenticazione LDAP

Per semplificare l'amministrazione, la piattaforma BI supporta l'autenticazione LDAP per gli account utente e di gruppo. Affinché gli utenti possano utilizzare i propri nomi utente e password LDAP per accedere al sistema, è necessario mappare gli account LDAP alla piattaforma BI. Quando si mappa un account LDAP, è possibile scegliere di creare un nuovo account o di collegarsi a un account già esistente della piattaforma BI.

Prima di impostare e abilitare l'autenticazione LDAP, accertarsi che la directory LDAP sia impostata. Per ulteriori informazioni, consultare la documentazione LDAP.

La configurazione dell'autenticazione LDAP prevede le attività seguenti:

- Configurazione dell'host LDAP
- Preparazione del server LDAP per SSL (se richiesta)
- Configurazione del plug-in LDAP per SiteMinder (se richiesta)

Nota:

Se si configura LDAP rispetto a AD, sarà possibile mappare gli utenti, ma non sarà possibile configurare la funzionalità Single Sign On AD o Single Sign On per il database. Tuttavia, saranno comunque disponibili i metodi LDAP Single Sign On come SiteMinder e l'autenticazione affidabile.

9.3.2.1 Per configurare l'host LDAP

È consigliabile installare ed eseguire il server LDAP prima di configurare l'host LDAP.

1. Selezionare **Autenticazione** nell'elenco di navigazione per accedere all'area di gestione "Autenticazione" della CMC.
2. Fare doppio clic su **LDAP**.
3. Se si sta configurando l'autenticazione LDAP per la prima volta, fare clic su **Avvia Configurazione guidata LDAP**.
4. Immettere il nome e il numero di porta degli host LDAP nel campo **Aggiungi un host LDAP (nomehost:porta)**, ad esempio "serverutente:123", fare clic su **Aggiungi**, quindi su **Avanti**.

Suggerimento:

ripetere questo passaggio per aggiungere altri host LDAP dello stesso tipo di server, se si desidera aggiungere host che possano fungere da server di failover. Per rimuovere un host, evidenziare il nome dell'host e fare clic su **Elimina**.

5. Selezionare il tipo di server dall'elenco **Tipo di server LDAP**.

Nota:

se si mappa LDAP ad AD, selezionare **Microsoft Active Directory Application Server** per il tipo di server.

6. Se si desidera visualizzare o modificare una mappatura di attributi del server LDAP o gli attributi di ricerca predefiniti LDAP, fare clic su **Mostra mappatura attributi**.

Per impostazione predefinita, le mappature di attributi di server e gli attributi di ricerca di ciascun tipo di server supportato sono già impostati.

7. Fare clic su **Avanti**.

8. Nel campo **Nome distinto LDAP di base** digitare il nome distinto, ad esempio o=SomeBase, per il server LDAP, quindi fare clic su **Avanti**.

9. Nell'area "Credenziali di amministrazione del server LDAP" specificare il nome distinto e la password per un account utente che dispone dell'accesso in lettura alla directory.

Le credenziali di amministratore non sono necessarie.

se il server LDAP consente il collegamento anonimo, lasciare quest'area vuota. I server e i client della piattaforma BI effettueranno il collegamento all'host principale mediante accesso anonimo.

10. Se sono stati configurati riferimenti all'host LDAP, immettere le informazioni di autenticazione nell'area "Credenziali di riferimento LDAP" e specificare il numero di hop di riferimento nel campo **Numero massimo di hop di riferimento**.

È necessario configurare l'area "Credenziali di riferimento LDAP" se sono valide tutte le condizioni seguenti:

- L'host principale è stato configurato per fare riferimento a un altro server di directory che gestisce query relative a voci che si trovano in una base specificata.
- L'host a cui si fa riferimento è stato configurato per non consentire il collegamento anonimo.
- Un gruppo presente nell'host a cui si fa riferimento sarà mappato alla piattaforma BI.

Nota:

- sebbene i gruppi possano essere mappati da più host, è possibile impostare solo una serie di credenziali di riferimento. Quindi, se esistono più host di riferimento, è necessario creare un account utente su ogni host che utilizza lo stesso nome distinto e la stessa password.
- se **Numero massimo di hop di riferimento** è impostato su zero, non verranno utilizzati riferimenti.

11. Fare clic su **Avanti**

12. e selezionare il tipo di autenticazione SSL (Secure Sockets Layer) utilizzato:

- **Di base (senza SSL)**
- **Autenticazione server**
- **Autenticazione reciproca**

Dettagli e prerequisiti per l'autenticazione server e reciproca vengono illustrati in una sezione successiva. Per impostare correttamente l'autenticazione LDAP mediante uno dei tipi di SSL, consultare la sezione *Configurazione delle impostazioni SSL per l'autenticazione del server LDAP o reciproca* nel presente documento prima di procedere oltre in questa procedura.

13. Fare clic su **Avanti** e selezionare un metodo di autenticazione Single Sign On LDAP:

- **Di base (senza SSO)**
- **SiteMinder**

14. Fare clic su **Avanti** e selezionare la modalità in cui alias e utenti vengono mappati negli account della piattaforma BI.

a. Nell'area "Nuove opzioni alias" selezionare la modalità in cui i nuovi alias devono essere mappati agli account Enterprise:

- **Assegna a ciascun alias LDAP aggiunto a un account con lo stesso nome**

Utilizzare questa opzione quando è noto che gli utenti dispongono di un account Enterprise già esistente con lo stesso nome. Ciò significa che gli alias LDAP verranno assegnati a utenti esistenti (la creazione di alias automatici è attivata). Gli utenti che non dispongono di un account Enterprise esistente o che non hanno lo stesso nome nei rispettivi account Enterprise e LDAP, verranno aggiunti come nuovi utenti.

- **Crea un nuovo account per ogni alias LDAP aggiunto**

Utilizzare questa opzione quando si desidera creare un nuovo account per ciascun utente.

b. In "Opzioni di aggiornamento alias" selezionare la modalità di gestione degli aggiornamenti degli alias per gli account Enterprise:

- **Crea nuovi alias all'aggiornamento dell'alias**

Utilizzare questa opzione per creare automaticamente un nuovo alias per ogni utente LDAP mappato alla piattaforma BI. Vengono aggiunti nuovi account LDAP per gli utenti senza account della piattaforma BI o per tutti gli utenti, se è stata selezionata l'opzione **Crea un nuovo account per ogni alias LDAP aggiunto**.

- **Crea nuovi alias solo all'accesso dell'utente**

Utilizzare questa opzione se la directory LDAP che si sta mappando contiene molti utenti, di cui solo alcuni utilizzeranno la piattaforma BI. Il sistema non crea automaticamente alias e account Enterprise per tutti gli utenti. Creerà, invece, alias (e account, se necessario) solo per gli utenti che accedono alla piattaforma.

c. Nell'area "Nuove opzioni utente" specificare la modalità di creazione dei nuovi utenti.

- **I nuovi utenti vengono creati come utenti designati**

I nuovi account utente verranno configurati per utilizzare licenze utente designato. Le licenze utente designato sono associate a utenti specifici e consentono di accedere al sistema in base a nome utente e password. Ciò garantisce agli utenti specifici l'accesso al sistema a prescindere dal numero delle altre persone connesse. È necessario disporre di una licenza utente designato per ciascun account utente creato utilizzando questa opzione.

- **I nuovi utenti vengono creati come utenti simultanei**

I nuovi account utente verranno configurati per utilizzare licenze utente simultaneo. Le licenze di accesso simultaneo specificano il numero di persone che possono connettersi alla piattaforma BI contemporaneamente. Questo tipo di licenza è estremamente flessibile, poiché una licenza di accesso simultaneo di dimensioni ridotte può supportare un'ampia base di

utenti. A seconda della frequenza e della durata dell'accesso alla piattaforma, una licenza di accesso simultaneo per 100 utenti può ad esempio supportare 250, 500 o 700 utenti.

15. Eseguire questo passaggio se si stanno impostando le mappature degli attributi utente o se si ha intenzione di importare gli indirizzi di posta elettronica dal server LDAP. Nell'area "Opzioni di collegamento attributi" è possibile specificare la priorità di collegamento degli attributi per il plug-in LDAP:

- a. Fare clic sulla casella **Importa nome completo, indirizzo di posta elettronica e altri attributi**. I nomi completi e le descrizioni utilizzati negli account LDAP vengono importati e memorizzati con gli oggetti utente nel sistema.
- b. Specificare un'opzione per **Imposta priorità collegamento attributi LDAP relativo ad altri collegamenti attributi**.

Nota:

Se l'opzione è impostata su 1, gli attributi LDAP hanno la priorità in scenari in cui sono abilitati LDAP e altri plug-in (Windows AD e SAP). Se l'opzione è impostata su 3, hanno la priorità gli attributi di altri plug-in abilitati.

16. Fare clic su **Fine**.

Argomenti correlati

- [Configurazione delle impostazioni SSL per l'autenticazione del server LDAP o reciproca](#)
- [Configurazione del plug-in LDAP per SiteMinder](#)

9.3.2.2 Gestione di più host LDAP

Utilizzando LDAP e la piattaforma BI, è possibile aggiungere la tolleranza di errore al sistema aggiungendo più host LDAP. Il sistema utilizza il primo host aggiunto come host LDAP principale. I successivi host vengono considerati host di failover.

L'host LDAP primario e tutti gli host di failover devono essere configurati esattamente nello stesso modo e ogni host LDAP deve fare riferimento a tutti gli altri host da cui si desidera mappare gruppi. Per ulteriori informazioni sugli host e sui riferimenti LDAP, consultare la documentazione LDAP.

Per aggiungere più host LDAP, immettere tutti gli host quando si configura LDAP con la Configurazione guidata LDAP. In alternativa, se si è già configurato LDAP, passare all'area di gestione Autenticazione della Central Management Console e fare clic sulla scheda LDAP. Nell'area Riepilogo della configurazione server LDAP, fare clic sul nome dell'host LDAP per aprire la pagina che consente di aggiungere o eliminare host.

Nota:

- Accertarsi di aggiungere per primo l'host principale, seguito dai rimanenti host di failover.

- Se ci si avvale di host LDAP di failover, non è possibile utilizzare il livello più alto di protezione SSL (in altre parole, non è possibile selezionare “Accetta certificato server se proviene da un'autorità di certificazione attendibile e l'attributo CN del certificato corrisponde al nome host DNS del server”).

Argomenti correlati

- [Configurazione dell'autenticazione LDAP](#)

9.3.2.3 Configurazione delle impostazioni SSL per l'autenticazione del server LDAP o reciproca

Questa sezione contiene informazioni dettagliate sull'autenticazione server o reciproca basata su SSL per LDAP. Per l'impostazione dell'autenticazione basata su SSL sono necessarie delle operazioni preliminari. Vengono inoltre fornite informazioni specifiche per la configurazione di SSL con l'autenticazione server e reciproca LDAP nella console CMC. In questa sezione si presuppone che sia stato configurato l'host LDAP e che sia stata selezionata una delle seguenti opzioni di autenticazione SSL:

Per informazioni aggiuntive sulla configurazione del server host LDAP, consultare la documentazione del fornitore LDAP.

Argomenti correlati

- [Per configurare l'host LDAP](#)

9.3.2.3.1 Per configurare l'autenticazione del server LDAP o reciproca

Risorsa	Azione da eseguire prima dell'avvio dell'attività
Certificato CA	<p>Questo prerequisito riguarda sia l'autenticazione reciproca che server con SSL.</p> <ol style="list-style-type: none"> 1. Ottenere da un'autorità di certificazione (CA) un certificato CA. 2. Aggiungere il certificato al server LDAP in uso. <p>Per ulteriori informazioni, consultare la documentazione del fornitore di LDAP.</p>
Certificato server	<p>Questo prerequisito riguarda sia l'autenticazione reciproca che server con SSL.</p> <ol style="list-style-type: none"> 1. Richiedere e quindi generare un certificato server. 2. Autorizzare il certificato e aggiungerlo al server LDAP.
cert7.db oppure cert8.db, key3.db	<p>Questi file sono necessari sia per l'autenticazione reciproca che server con SSL.</p> <ol style="list-style-type: none"> 1. Scaricare l'applicazione certutil che genera un file cert7.db o cert8.db (a seconda dei requisiti) da ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_6_RTM/. 2. Copiare il certificato CA nella stessa directory dell'applicazione certutil. 3. Utilizzare il seguente comando per generare i file cert7.db o cert8.db, key3.db e secmod.db: <pre>certutil -N -d .</pre> 4. Utilizzare il seguente comando per aggiungere il certificato CA al file cert7.db o cert8.db: <pre>certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer</pre> 5. Archiviare i tre file in una directory del computer che ospita la piattaforma BI.
cacerts	<p>Questo file è necessario per l'autenticazione reciproca o server con SSL per applicazioni Java quale BI Launch Pad.</p> <ol style="list-style-type: none"> 1. Localizzare il file keytool nella directory bin di Java. 2. Utilizzare il comando seguente per creare il file cacerts: <pre>keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore</pre> 3. Archiviare il file cacerts nella stessa directory dei file cert7.db o cert8.db e key3.db.
Certificato client	

Risorsa	Azione da eseguire prima dell'avvio dell'attività
	<ol style="list-style-type: none"> Creare richieste client separate per i file <code>cert7.db</code> o <code>cert8.db</code> e <code>.keystore</code>: <ul style="list-style-type: none"> Per configurare il plug-in LDAP utilizzare l'applicazione <code>certutil</code> per generare una richiesta di certificato client. Utilizzare il seguente comando per generare la richiesta di certificato client: <pre>certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .</pre> <p><code><client_dn></code> include informazioni quali <code>CN=nome_client</code>, <code>OU=unità organizzativa</code>, <code>O=nomesocietà</code>, <code>L=città</code>, <code>ST=provincia</code> e <code>C=paese</code>.</p> Utilizzare la CA per autenticare la richiesta di certificato. Utilizzare il seguente comando per recuperare il certificato e inserirlo nel file <code>cert7.db</code> o <code>cert8.db</code>: <pre>certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name></pre> Per agevolare l'autenticazione Java con SSL: <ul style="list-style-type: none"> Utilizzare l'utilità <code>keytool</code> nella directory <code>bin</code> di Java per generare una richiesta di certificato client. Utilizzare il seguente comando per generare una coppia di chiavi: <pre>keytool -genkey -keystore .keystore</pre> Dopo avere specificato le informazioni relative al client, generare una richiesta di certificato client utilizzando il comando seguente: <pre>keytool -certreq -file <certificate_request_name> -keystore .keystore</pre> Una volta che la CA ha autenticato la richiesta di certificato client, utilizzare il seguente comando per aggiungere il certificato CA al file <code>.keystore</code>: <pre>keytool -import -v -alias <CA_alias_name> -file <ca_certificate_name> -trustcacerts -keystore .keystore</pre> Recuperare la richiesta di certificato client dalla CA e utilizzare il seguente comando per aggiungerlo al file <code>.keystore</code>: <pre>keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore</pre> Archiviare il file <code>.keystore</code> nella stessa directory dei file <code>cert7.db</code> o <code>cert8.db</code> e <code>cacerts</code> sul computer che ospita la piattaforma BI.

1. Scegliere il livello di protezione SSL da utilizzare.

Se si utilizza la Configurazione guidata LDAP per configurare l'autenticazione LDAP per la prima volta, selezionare **Autenticazione reciproca** nell'elenco "Tipo di autenticazione SSL" e fare clic su **Avanti**. In alternativa, se si intende riconfigurare l'autenticazione LDAP, accedere all'area **Autenticazione** della CMC e fare doppio clic su **LDAP**. Viene visualizzata la pagina "Riepilogo della

configurazione server LDAP". Fare clic sul valore **Tipo SSL** e selezionare **Autenticazione reciproca** nell'elenco "Tipo di autenticazione SSL".

- **Accetta sempre certificato server**

Questa è l'opzione con il livello di protezione più basso. Per poter stabilire una connessione SSL con l'host LDAP (per autenticare utenti e gruppi LDAP), è necessario che la piattaforma BI riceva un certificato di protezione inviato dall'host LDAP. La piattaforma BI non verifica il certificato ricevuto.

- **Accetta certificato server se proviene da un'autorità di certificazione attendibile**

Questa è un'opzione con un livello di protezione medio. Prima che la piattaforma BI possa stabilire una connessione SSL con l'host LDAP (per autenticare utenti e gruppi LDAP), deve ricevere e verificare un certificato di protezione inviato dall'host LDAP. Per verificare il certificato, il sistema deve individuare l'autorità di certificazione che lo ha rilasciato nel suo database dei certificati.

- **Accetta il certificato del server se proviene da un'autorità di certificazione attendibile e se l'attributo CN del certificato corrisponde al nome host DNS del server**

Questa è l'opzione con il livello di protezione più alto. Prima che la piattaforma BI possa stabilire una connessione SSL con l'host LDAP (per autenticare utenti e gruppi LDAP), deve ricevere e verificare un certificato di protezione inviato dall'host LDAP. Per verificare il certificato, la piattaforma BI deve trovare l'autorità di certificazione che lo ha emesso nel suo database di certificati ed essere in grado di confermare che l'attributo CN sul certificato del server corrisponde esattamente al nome host LDAP inserito nella casella **Aggiungi un host LDAP** nella prima fase della procedura, se è stato inserito un nome host LDAP come ABALONE.rd.crystald.net:389. L'utilizzo di CN =ABALONE:389 nel certificato non funziona.

il nome host presente sul certificato di protezione server è il nome dell'host LDAP primario. Se si seleziona questa opzione, non è possibile utilizzare un host LDAP di failover.

Nota:

le applicazioni Java ignorano la prima e l'ultima impostazione e accettano il certificato del server solo se proviene da un'autorità di certificazione attendibile.

2. Nella casella **Host SSL** digitare il nome dell'host di ogni computer e quindi fare clic su **Aggiungi**. È quindi necessario aggiungere il nome host di ogni computer nella distribuzione della piattaforma BI che utilizza l'SDK della piattaforma BI. Sono compresi i computer che eseguono Central Management Server e il computer su cui è in esecuzione il server di applicazioni Web.
3. Specificare le impostazioni SSL per ogni host SSL aggiunto alla lista:
 - a. Selezionare **Impostazione predefinita** nell'elenco SSL.
 - b. Deselezionare le caselle di controllo **Usa valore predefinito**.
 - c. Inserire un valore nei campi **Percorso dei file di database dei certificati e delle chiavi e Password per il database dei codici**.
 - d. Se si specificano le impostazioni per l'autenticazione reciproca, inserire un valore nella casella **Nome fittizio per il certificato client nel database di certificati**.

Nota:

Le impostazioni predefinite verranno utilizzate (per qualsiasi impostazione) per qualsiasi host con la casella di controllo **Utilizza valore predefinito** selezionata o per qualsiasi computer il cui nome non viene aggiunto all'elenco degli host SSL.

4. Specificare le impostazioni predefinite per ogni host che non si trova in elenco e fare su **Avanti**.
Per specificare le impostazioni per un altro host, selezionarne il nome nell'elenco a sinistra e inserire i valori nelle caselle a destra.

Nota:

Le impostazioni di default verranno utilizzate per qualsiasi impostazione (per qualsiasi host) con la casella di controllo **Utilizza valore predefinito** selezionata o per qualsiasi computer il cui nome non viene aggiunto all'elenco degli host SSL.

5. Selezionare **Di base (senza SSO)** o **SiteMinder** come metodo di autenticazione Single Sign-On LDAP.
6. Scegliere la modalità con cui verranno creati i nuovi utenti e alias LDAP.
7. Scegliere **Fine**.

Argomenti correlati

- [Configurazione del plug-in LDAP per SiteMinder](#)

9.3.2.4 Per modificare le impostazioni di configurazione LDAP

Dopo aver configurato l'autenticazione LDAP con la Configurazione guidata LDAP, è possibile modificare i parametri di connessione e i gruppi membri LDAP utilizzando la pagina "Riepilogo della configurazione server LDAP".

1. Passare all'area di gestione **Autenticazione** della CMC.
2. Fare doppio clic su **LDAP**.

Se l'autenticazione LDAP è configurata, viene visualizzata la pagina "Riepilogo della configurazione server LDAP". In questa pagina è possibile modificare le aree o i campi dei parametri di connessione e le opzioni nell'area "Membri del gruppo LDAP mappati".

3. Eliminare i gruppi correntemente mappati che non saranno più accessibili con le nuove impostazioni di connessione, quindi fare clic su **Aggiorna**.
È possibile eliminare i gruppi mappati selezionando il gruppo di utenti e facendo clic sul pulsante **Elimina** nella sezione "Membri del gruppo LDAP mappati".
4. Modificare le impostazioni di connessione e fare clic su **Aggiorna**.
5. Modificare le "Nuove opzioni di alias", le "Opzioni di aggiornamento alias" e le "Nuove opzioni utente" se necessario e fare clic su **Aggiorna**.
6. Mappare i nuovi gruppi dei membri LDAP, quindi fare clic su **Aggiorna**.

9.3.2.5 Configurazione del plug-in LDAP per SiteMinder

In questa sezione viene illustrato come configurare la console CMC per l'utilizzo di LDAP con SiteMinder. SiteMinder è uno strumento di terzi per l'autenticazione e l'accesso utente che è possibile utilizzare con il plug-in di protezione per creare il Single Sign On alla piattaforma BI.

Per utilizzare SiteMinder e LDAP con la piattaforma BI è necessario apportare modifiche alla configurazione in due punti:

- Il plug-in LDAP mediante la CMC
- Le proprietà del file `BOE.war`

Nota:

Assicurarsi che l'amministratore di SiteMinder abbia abilitato il supporto per gli agenti 4.x. L'operazione va eseguita a prescindere dalla versione in uso di SiteMinder. Per ulteriori informazioni sul SiteMinder e su come eseguire l'installazione, fare riferimento alla documentazione di SiteMinder.

Argomenti correlati

- [Per configurare l'host LDAP](#)

9.3.2.5.1 Per configurare LDAP per Single Sign-On con SiteMinder

1. Aprire la schermata **Configurare le impostazioni di SiteMinder** utilizzando uno dei seguenti metodi:
 - Selezionare SiteMinder nella schermata "Scegliere un metodo di autenticazione Single Sign-On LDAP" della Configurazione guidata LDAP.
 - Selezionare il collegamento **Tipo di Single Sign-On** nella schermata di autenticazione LDAP disponibile se LDAP è già stato configurato e se si stanno aggiungendo SSO.
2. Digitare il nome di ogni server dei criteri nella casella **Host dei server dei criteri** e fare clic su **Aggiungi**.
3. Per ogni host del server dei criteri specificare i numeri di porta **Accounting**, **Autenticazione** e **Autorizzazione**.
4. Specificare il **Nome dell'agente** e il **Segreto condiviso**. Immettere nuovamente il segreto condiviso nella casella "Conferma segreto condiviso".
5. Fare clic su **Avanti**.
6. Continuare con la configurazione delle opzioni LDAP.

9.3.2.5.2 Abilitazione di LDAP e SiteMinder nel file BOE.war

Oltre che per il plug-in di protezione LDAP, le impostazioni di SiteMinder devono essere specificate anche per le proprietà del file `BOE.war`.

1. Accedere alla directory `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` nell'installazione della piattaforma BI.
2. Creare un nuovo file, utilizzando Blocco note o un'altra utilità di modifica del testo.
3. Immettere l'istruzione seguente:

```
siteminder.authentication=secLDAP
siteminder.enabled=true
```

4. Chiudere il file e salvarlo con il nome `global.properties`, senza un'estensione file.
5. Creare un altro file nella stessa directory.
6. Immettere l'istruzione seguente:

```
authentication.default=secLDAP  
cms.default=[your cms name]:[the CMS port number]
```

Ad esempio:

```
authentication.default=secLDAP  
cms.default=mycms:6400
```

7. Chiudere il file e salvarlo con il nome `bilaunchpad.properties`.

Le nuove proprietà hanno effetto solo dopo la redistribuzione dell'applicazione Web BOE modificata nel computer su cui è in esecuzione il server di applicazioni Web. Utilizzare WDeploy per ridistribuire il file WAR sul server di applicazioni Web. Per ulteriori informazioni sull'utilizzo di WDeploy, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

9.3.3 Mappatura di gruppi LDAP

Una volta configurato l'host LDAP utilizzando la Configurazione guidata LDAP, è possibile mappare i gruppi LDAP ai gruppi Enterprise.

Dopo aver mappato i gruppi LDAP, è possibile visualizzarli facendo clic sull'opzione LDAP nell'area di gestione **Autenticazione**. Se l'autenticazione LDAP è configurata, nell'area Gruppi membri LDAP mappati verranno visualizzati i gruppi LDAP mappati alla piattaforma BI.

Nota:

È inoltre possibile mappare i gruppi Windows AD per l'autenticazione nella piattaforma BI mediante il plug-in di protezione LDAP.

Nota:

se LDAP è stato configurato in base ad AD, questa procedura consente di mappare i gruppi AD.

Argomenti correlati

- [Mappatura di LDAP a Windows AD](#)

9.3.3.1 Mappatura di gruppi LDAP mediante la piattaforma BI

1. Passare all'area di gestione "Autenticazione" della CMC.
2. Fare doppio clic su **LDAP**.

Se l'autenticazione LDAP è configurata, viene visualizzata la pagina di riepilogo LDAP.

3. Nell'area "Membri del gruppo LDAP mappati" specificare il gruppo LDAP (in base al nome comune o al nome distinto) nel campo **Aggiungi un gruppo LDAP (mediante cn o dn)** e fare clic su **Aggiungi**.

Per aggiungere più gruppi LDAP, ripetere questo passaggio. per rimuovere un gruppo, evidenziare il gruppo LDAP quindi fare clic su **Elimina**.

4. Nell'area "Nuove opzioni alias" selezionare un'opzione per specificare come gli alias LDAP devono essere mappati agli account Enterprise:

- **Assegna a ciascun alias LDAP aggiunto un account con lo stesso nome**

Utilizzare questa opzione quando è noto che gli utenti dispongono di un account Enterprise già esistente con lo stesso nome. Ciò significa che gli alias LDAP verranno assegnati a utenti esistenti (la creazione di alias automatici è attivata). Gli utenti che non dispongono di un account Enterprise esistente, o che non hanno lo stesso nome nei rispettivi account Enterprise e LDAP, verranno aggiunti come nuovi utenti LDAP.

- **Crea un nuovo account per ogni alias LDAP aggiunto**

Utilizzare questa opzione quando si desidera creare un nuovo account per ciascun utente.

5. Nell'area "Opzioni di aggiornamento alias" selezionare un'opzione per specificare se gli alias LDAP devono essere creati automaticamente per tutti i nuovi utenti:

- **Crea nuovi alias all'aggiornamento dell'alias**

Utilizzare questa opzione per creare automaticamente un nuovo alias per ogni utente LDAP mappato alla piattaforma BI. I nuovi account LDAP vengono aggiunti per gli utenti che non dispongono di account della piattaforma BI o per tutti gli utenti, se è stata selezionata l'opzione **Crea un nuovo account per ogni alias LDAP aggiunto** ed è stato fatto clic su **Aggiorna**.

- **Crea nuovi alias solo all'accesso dell'utente**

Utilizzare questa opzione se la directory LDAP che si sta mappando contiene molti utenti, di cui solo alcuni utilizzeranno la piattaforma BI. Il sistema non crea automaticamente alias e account Enterprise per tutti gli utenti. Creerà, invece, alias (e account, se necessario) solo per gli utenti che accedono alla piattaforma.

6. Nell'area "Opzioni nuovo utente", se la licenza della piattaforma BI si basa sui ruoli utente, selezionare un'opzione per specificare le proprietà dei nuovi account Enterprise creati per essere mappati agli account LDAP:

- **I nuovi utenti vengono creati come utenti designati**

I nuovi account utente verranno configurati per utilizzare licenze utente designato. Le licenze utente designato sono associate a utenti specifici e consentono di accedere al sistema in base a nome utente e password. Ciò garantisce agli utenti specifici l'accesso al sistema a prescindere dal numero delle altre persone connesse. È necessario disporre di una licenza utente designato per ciascun account utente creato utilizzando questa opzione.

- **I nuovi utenti vengono creati come utenti simultanei**

I nuovi account utente verranno configurati per utilizzare licenze utente simultaneo. Le licenze di accesso simultaneo specificano il numero di persone che possono connettersi alla piattaforma BI contemporaneamente. Questo tipo di licenza è estremamente flessibile, poiché una licenza di accesso simultaneo di dimensioni ridotte può supportare un'ampia base di utenti. A seconda della frequenza e della durata dell'accesso al sistema, una licenza di accesso simultaneo per 100 utenti può ad esempio supportare 250, 500 o 700 utenti.

7. Fare clic su **Aggiorna**.

9.3.3.2 Eliminazione della mappatura di gruppi LDAP mediante la piattaforma BI

1. Passare all'area di gestione **Autenticazione** della CMC.
2. Fare doppio clic su **LDAP**.
Se l'autenticazione LDAP è configurata, viene visualizzata la pagina di riepilogo LDAP.
3. Nell'area Gruppi membri LDAP mappati, selezionare il gruppo LDAP che si desidera rimuovere.
4. Fare clic su **Elimina**, quindi su **Aggiorna**.

Gli utenti del gruppo non saranno in grado di accedere alla piattaforma BI.

Nota:

le uniche eccezioni si applicano se un utente dispone di un alias per l'account Enterprise. Per limitare l'accesso, disabilitare o eliminare l'account Enterprise dell'utente.

per negare l'autenticazione LDAP a tutti i gruppi, deselezionare la casella di controllo "Autenticazione LDAP abilitata", quindi fare clic su **Aggiorna**.

9.3.3.3 Mappatura di LDAP a Windows AD

Se si configura LDAP rispetto a Windows AD, tenere presenti le seguenti limitazioni:

- Se si configura LDAP rispetto a AD, sarà possibile mappare gli utenti, ma non sarà possibile configurare la funzionalità Single Sign On AD o Single Sign On per il database. Tuttavia, saranno comunque disponibili i metodi LDAP Single Sign On come SiteMinder e l'autenticazione affidabile.
- Gli utenti che sono solo membri di gruppi predefiniti di AD non saranno in grado di accedere. Gli utenti devono essere anche membri di un altro gruppo creato in modo esplicito in AD e, inoltre, tale gruppo deve essere mappato. Un esempio di tale gruppo è il gruppo "utenti di dominio".
- Se un gruppo di dominio locale mappato contiene un utente proveniente da un altro dominio della foresta, tale utente non sarà in grado di accedere.

- Gli utenti appartenenti a un gruppo universale di un dominio diverso da quello specificato come host LDAP non saranno in grado di accedere.
- Non è possibile utilizzare il plug-in LDAP per mappare utenti e gruppi dalle foreste AD esterne alla foresta in cui è installata la piattaforma BI.
- Non è possibile mappare nel gruppo Utenti dominio in AD.
- Non è possibile mappare un gruppo locale del computer.
- Se si utilizza il controller di dominio del catalogo globale, la mappatura di LDAP rispetto ad AD richiede ulteriori considerazioni:

Situazione	Considerazioni
Più domini quando si fa riferimento al controller di dominio del catalogo globale	<p>È possibile mappare in:</p> <ul style="list-style-type: none"> • gruppi universali in un dominio secondario. • gruppi nello stesso dominio che contiene gruppi universali da un dominio secondario e • gruppi universali in un dominio trasversale. <p>Non è possibile mappare in:</p> <ul style="list-style-type: none"> • gruppi globali in un dominio secondario, • gruppi locali in un dominio secondario, • gruppi nello stesso dominio che contiene un gruppo globale dal dominio secondario e • gruppi globali tra domini. <p>In genere, se il gruppo è un gruppo universale, supporterà utenti di domini secondari o trasversali. Altri gruppi non verranno mappati se contengono utenti di domini secondari o trasversali. All'interno del dominio a cui si fa riferimento, è possibile mappare gruppi locali, globali e universali del dominio.</p>
Mappatura in gruppi universali	Per mappare in gruppi universali, è necessario fare riferimento al Controller di dominio del catalogo globale. È inoltre possibile utilizzare il numero di porta 3268 anziché quello predefinito 389.

- Se si utilizzano più domini ma non si fa riferimento al Controller di dominio del catalogo globale, non è possibile mappare in nessun tipo di gruppo di domini secondari o trasversali. È possibile mappare tutti i tipi di gruppo solo dal dominio specifico a cui si fa riferimento.

9.3.3.4 Utilizzo del plug-in LDAP per configurare SSO nel database SAP HANA

Questa sezione fornisce agli amministratori le fasi necessarie all'impostazione e configurazione Single Sign On (SSO) fra la piattaforma BI in esecuzione su SUSE Linux 11 e il database SAP HANA. Autenticazione LDAP tramite Kerberos consente agli utenti AD di essere autenticati su una piattaforma BI in esecuzione su Linux, in modo specifico su SUSE. Questo scenario supporta anche la Single Sign On su SAP HANA come database di report.

Nota:

Per informazioni sulla configurazione del database SAP HANA, consultare il *manuale di aggiornamento e installazione server - database SAP HANA*. Per ulteriori informazioni sulla modalità di configurazione del componente Accesso ai dati per SAP HANA, consultare *Manuale dell'accesso ai dati*.

Panoramica dell'implementazione

Affinché Kerberos SSO possa funzionare correttamente, devono essere predisposti i seguenti componenti.

Componente	Requisito
Controller di dominio	Ospitato su un computer che esegue Active Directory impostato per utilizzare l'autenticazione Kerberos.
Central Management Server	Installato e in esecuzione su un computer che esegue SUSE Linux Enterprise 11 (SUSE).
Client Kerberos V5	Installato insieme alle librerie e utilità necessarie sull'host SUSE. Nota: Utilizzare la versione più recente del client Kerberos V5. Aggiungere le cartelle <code>bin</code> e <code>lib</code> alle variabili di ambiente <code>PATH</code> e <code>LD_LIBRARY_PATH</code> .
plug-in per l'autenticazione LDAP	Attivata sull'host SUSE.
File di configurazione di accesso Kerberos	Creato sulla macchina che ospita il server di applicazioni Web.

Workflow di implementazione

È necessario effettuare le seguenti attività per consentire agli utenti della piattaforma BI l'accesso SSO a SAP HANA tramite l'autenticazione Kerberos utilizzando JDBC.

1. Configurazione dell'host AD.
2. Creazione di file di codice e account per l'host SUSE e la piattaforma BI sull'host AD.
3. Installazione delle risorse Kerberos sull'host SUSE.
4. Configurazione dell'host SUSE per l'autenticazione Kerberos.

5. Configurazione delle opzioni di autenticazione Kerberos nel plug-in per autenticazione LDAP.
6. Creazione di un file di configurazione di accesso Kerberos per l'host di applicazioni Web.

9.3.3.4.1 Per impostare il controller del dominio

Potrebbe essere necessario impostare una relazione di trust fra l'host SUSE e il controller del dominio. Se l'host SUSE si trova nel controller del dominio Windows non è necessario configurare la relazione di trust. Tuttavia, se la distribuzione della piattaforma BI e il controller del dominio si trovano in domini differenti, potrebbe essere necessario impostare una relazione di trust fra la macchina SUSE Linux e il controller del dominio. Viene richiesto quanto segue:

1. Creare un account utente per la macchina SUSE che esegue la piattaforma BI.
2. Creare un host Nome principale servizio (SPN).

Nota:

SPN dovrebbe essere formattato in base alle convenzioni Windows AD: `host/nomehost@NOME_DOMINIO_DNS`. Utilizzare, con lettere minuscole, un nome di dominio completamente qualificato per `/nomehost.NOME_DOMINIO_DNS` dovrebbe essere indicato in lettere maiuscole.

3. Eseguire il comando di configurazione keytab Kerberos `ktpass` per associare SPN all'account utente:

```
c:\> ktpass -princ host/hostname@DNS_REALM_NAME-mapuser username -pass Password1 -crypto RC4-HMAC-NT -out usernamebase.keytab
```

Le fasi seguenti devono essere eseguite sulla macchina che ospita il controller del dominio.

1. Creare un account utente per il servizio che esegue la piattaforma BI.
2. Sulla pagina "Account utente", fare clic col tasto destro del mouse sull'account del nuovo servizio e selezionare **Proprietà > Delega**.
3. Selezionare **Utente attendibile per la delega a qualsiasi servizio (solo Kerberos)**.
4. Eseguire il comando di configurazione keytab Kerberos `ktpass` per creare un account SPN per il nuovo account di servizio:

```
c:\>ktpass -princ sianame/service_name@DNS_REALM_NAME -mapuser service_name -pass password -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT -out sianame.keytab
```

Nota:

SPN dovrebbe essere formattato in base alle convenzioni Windows AD: `sianame/nome_servizio@NOME_DOMINIO_DNS`. Specificare il `nome servizio` in lettere minuscole altrimenti la piattaforma SUSE potrebbe non riuscire a risolverlo. `NOME_DOMINIO_DNS` dovrebbe essere indicato in lettere maiuscole.

Parametro	Descrizione
-princ	Specifica il nome principale per l'autenticazione Kerberos.
-out	Specifica il nome del file Kerberos <code>keytab</code> da generare. Dovrebbe corrispondere al <code>nomesia</code> utilizzato in <code>-princ</code> .
-mapuser	Specifica il nome dell'account utente a cui è stato mappato l'SPN. Server Intelligence Agent viene eseguito su questo account.

Parametro	Descrizione
-pass	Specifica la password utilizzata dall'account di servizio.
-ptype	Specifica il tipo principale: <code>-ptype KRB5_NT_PRINCIPAL</code>
-crypto	Specifica il tipo di crittografia da utilizzare con l'account di servizio: <code>-crypto RC4-HMAC-NT</code>

Sono stati creati i file keytab necessari per la relazione di trust fra la macchina SUSE e il controller del dominio.

È necessario trasferire il file keytab alla macchina SUSE e archivarlo nella directory `/etc`.

9.3.3.4.2 Per configurare il computer SUSE Linux Enterprise 11

Sono necessarie le seguenti risorse per la configurazione di Kerberos nel computer SUSE Linux che esegue la piattaforma BI:

- File keytab creati sul controller del dominio. Il file keytab creato per il servizio della piattaforma BI è obbligatorio. Il keytab per l'host SUSE è consigliato in modo specifico per gli scenari in cui l'host della piattaforma BI e il controller del dominio si trovano in domini differenti.
- La libreria Kerberos V5 più recente (incluso il client Kerberos) deve essere installata sull'host SUSE. È necessario aggiungere la posizione dei file binari alle variabili di ambiente `PATH` e `LD_LIBRARY_PATH`. Per verificare l'installazione e configurazione corrette del client Kerberos, controllare che le seguenti utilità e librerie siano presenti sull'host SUSE:

- `kinit`
- `ktutil`
- `kdestroy`
- `klist`
- `/lib64/libgssapi_krb5.so.2.2`
- `/lib64/libkrb5.so.3.3`
- `/lib/libkrb5support.so.0.1`
- `/lib64/libk5crypto.so.3`
- `/lib64/libcom_err.so.2`

Suggerimento:

Eseguire `rpm -qa | grep krb` per verificare la versione di tali librerie. Per ulteriori informazioni sul client Kerberos più recente, librerie e configurazione dell'host Unix, consultare <http://web.mit.edu/Kerberos/krb5-1.9/krb5-1.9.2/doc/krb5-install.html#Installing%20Kerberos%20V5>.

Una volta che tutte le risorse necessarie sono disponibili sull'host SUSE, seguire le istruzioni riportate di seguito per configurare l'autenticazione Kerberos.

Nota:

per eseguire questi passaggi, è necessario disporre di privilegi root.

1. Per unire i file keytab eseguire il seguente comando:

```
> ktutil
ktutil: rkt <susemachine>.keytab
ktutil: rkt <BI platform service>.keytab
ktutil: wkt /etc/krb5.keytab
ktutil:q
```

2. Modificare il file `/etc/kerb5.conf` per fare riferimento al controller del dominio (sulla piattaforma Windows) come al Controller di dominio Kerberos (KDC).

Utilizzare gli esempi seguenti:

```
[domain_realm]
.name.mycompany.corp = DOMAINNAME.COM
.name.mycompany.corp = DOMAINNAME.COM

[libdefaults]
    forwardable = true
    default_realm = DOMAINNAME.COM
    default_tkt_enctypes = rc4-hmac
    default_tgs_enctypes = rc4-hmac

[realms]
    DOMAINNAME.COM = {
        kdc = machinename.domainname.com
    }
```

Nota:

il file `krb5.conf` contiene informazioni di configurazione Kerberos, incluse le posizioni di KDC e server per le aree di interesse Kerberos, applicazioni Kerberos e mappature di nomi host nei domini Kerberos. Di norma, il file `krb5.conf` viene installato nella directory `/etc`.

3. Aggiungere il controller del dominio a `/etc/hosts` in modo che l'host SUSE possa localizzare KDC.
4. Eseguire il programma `kinit` dalla directory `/usr/local/bin` per verificare che Kerberos sia stato configurato correttamente. Verificare che un account utente AD possa eseguire l'accesso al computer SUSE.

Suggerimento:

KDC dovrebbe emettere un ticket di concessione ticket (TGT) che può essere visualizzato nella cache. Utilizzare il programma `klist` per visualizzare il TGT.

Esempio:

```
> kinit <AD user>
Password for <AD user>@<domain>: <AD user password>

> klist
Ticket cache: FILE:/tmp/krb5cc_0Default principal: <AD user>@<domain>
Valid starting Expires Service principal
08/10/11 17:33:43 08/11/11 03:33:46 krbtgt/<domain>@<domain>renew
until 08/11/11 17:33:43
Kerberos 4 ticket cache: /tmp/tkt0klist: You have no tickets cached

>klist -k
Keytab name: FILE:/etc/krb5.keytabKVNO Principal-3hdb/<FQDN>@<Domain>
```

Inoltre, è consigliabile servirsi di `kinit` per verificare SPN.

9.3.3.4.3 Per configurare le opzioni di autenticazione Kerberos per LDAP

Prima di configurare l'autenticazione Kerberos per LDAP, è necessario innanzitutto attivare e configurare il plug-in di autenticazione LDAP della piattaforma BI per eseguire la connessione alla directory AD. Per utilizzare l'autenticazione LDAP, è necessario accertarsi di aver impostato la rispettiva directory LDAP.

Nota:

quando si esegue "Avvia Configurazione guidata LDAP" è necessario specificare **Microsoft Active Directory Application Server** e fornire i dettagli di configurazione richiesti.

Dopo aver abilitato l'autenticazione LDAP ed effettuato la connessione a Microsoft Active Directory Application Server, viene visualizzata l'area "Abilita autenticazione Kerberos" sulla pagina Riepilogo della configurazione server. Utilizzare quest'area per configurare l'autenticazione Kerberos, necessaria per il Single Sign On nel database SAP HANA da una distribuzione della piattaforma BI in SUSE.

1. Passare all'area di gestione **Autenticazione** della CMC.
2. Fare doppio clic su **LDAP**.

Viene visualizzata la pagina "Riepilogo della configurazione server LDAP", in cui è possibile modificare qualsiasi campo o parametro di connessione.

3. Per configurare l'autenticazione Kerberos, eseguire le operazioni illustrate di seguito nell'area "Abilita autenticazione Kerberos":
 - a. Fare clic su **Abilita autenticazione Kerberos**.
 - b. Fare clic su **Contesto di protezione della cache (richiesto per SSO al database)**.

Nota:

l'attivazione del contesto di protezione della cache è richiesto specificatamente per il Single Sign On a SAP HANA.

- c. Specificare Nome principale servizio (SPN) per l'account della piattaforma BI in "Nome principale servizio".

Il formato per specificare SPN è `nomesia/servizio@NOME_DOMINIO_DNS`:

<code>nomesia</code>	Nome dell'agente Server Intelligence Agent
<code>servizio</code>	Nome dell'account di servizio utilizzato per eseguire la piattaforma BI
<code>NOME_DOMINIO_DNS</code>	Il nome del dominio del controller di dominio in lettere maiuscole

Suggerimento:

Alla specifica di SPN, ricordare che `nomesia/servizio` fa distinzione tra minuscole e maiuscole.

- d. Specificare il dominio per il controller di dominio in "Area di autenticazione Kerberos predefinita".
- e. Specificare `userPrincipalName` in **Nome principale utente**.

Questo valore viene utilizzato dall'applicazione di autenticazione LDAP per fornire i valori ID utente richiesti da Kerberos. Il valore specificato dovrebbe corrispondere al nome fornito durante la creazione dei file keytab.

4. Fare clic su **Aggiorna** per inviare e salvare le modifiche.

Sono state configurate le opzioni di autenticazione Kerberos per far riferimento agli account utente nella directory AD.

È necessario creare un file di configurazione degli accessi Kerberos, `bscLogin.conf`, per attivare il Single Sign On e l'accesso di Kerberos.

Argomenti correlati

- [Configurazione dell'autenticazione LDAP](#)

9.3.3.4.4 Per creare un file di configurazione degli accessi Kerberos

Per attivare il Single Sign On e l'accesso di Kerberos è necessario aggiungere un file di configurazione degli accessi sul computer che ospita il server delle applicazioni Web della piattaforma BI.

1. Creare un file denominato `bscLogin.conf` e archivarlo nella directory `/etc`.

Nota:

È possibile memorizzare questo file in un'altra posizione, ma in tal caso sarà necessario specificarla nelle opzioni Java. È consigliabile che i file `bscLogin.conf` e keytab Kerberos si trovino nella stessa directory. In un'implementazione distribuita è necessario aggiungere un file `bscLogin.conf` per ogni computer che ospita un server di applicazioni Web.

2. Aggiungere il codice seguente al file di configurazione degli accessi `bscLogin.conf`:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
com.businessobjects.security.jgss.accept {
com.sun.security.auth.module.Krb5LoginModule required
storeKey=true
useKeyTab=true
keyTab="/etc/krb5.keytab"
principal="principal name";
};
```

Nota:

La sezione seguente è richiesta in modo specifico per il Single Sign On:

```
com.businessobjects.security.jgss.accept {
com.sun.security.auth.module.Krb5LoginModule required
storeKey=true
useKeyTab=true
keyTab="/etc/krb5.keytab"
principal="principal name";
};
```

3. Salvare e chiudere il file.

9.3.3.5 Risoluzione dei problemi relativi ai nuovi account LDAP

- Se si crea un nuovo account utente LDAP che non appartiene a un account di gruppo mappato alla piattaforma BI, mappare il gruppo oppure aggiungere il nuovo account utente LDAP a un gruppo già mappato al sistema.
- Se viene creato un nuovo account utente LDAP e l'account appartiene a un account di gruppo mappato alla piattaforma BI, è necessario aggiornare l'elenco degli utenti.

Argomenti correlati

- [Configurazione dell'autenticazione LDAP](#)
- [Mappatura di gruppi LDAP](#)

9.4 Autenticazione Windows AD

9.4.1 Utilizzo dell'autenticazione Windows AD

9.4.1.1 Requisiti di supporto e impostazione iniziale di Windows AD

In questa sezione viene descritto il processo di configurazione dell'autenticazione Windows Active Directory (AD) per l'utilizzo nella piattaforma BI. Oltre a una descrizione di tutti i workflow end-to-end da eseguire, vengono illustrati anche i test di convalida e le verifiche dei prerequisiti.

Requisiti di supporto

Per semplificare l'autenticazione AD nella piattaforma BI, tenere presenti i seguenti requisiti di supporto.

- Il server CMS deve essere sempre installato su una piattaforma Windows supportata.
- Benché la piattaforma Windows 2008 sia supportata per l'autenticazione Kerberos e NTLM, è possibile che alcune applicazioni della piattaforma BI utilizzino solo metodi di autenticazione particolari. Ad esempio, le applicazioni come BI Launch Pad e Central Management Console supportano solo Kerberos.

Workflow dell'impostazione AD consigliato

Per impostare inizialmente l'autenticazione AD manuale con la piattaforma BI, utilizzare il workflow seguente:

1. Impostare il controller di dominio.
2. Configurare l'autenticazione AD nella console CMC.
3. Configurare l'account utente AD sul SIA (Server Intelligence Agent).
4. Configurare il server di applicazioni Web per l'autenticazione AD con Kerberos.

Nota:

Utilizzare questo workflow, indipendentemente dalla necessità di utilizzare il Single Sign On (SSO). Il workflow descritto nelle sezioni seguenti consentirà innanzitutto di accedere manualmente (mediante un nome utente AD e una password) alla piattaforma BI. Dopo aver configurato l'autenticazione AD manuale, in una sezione vengono fornite istruzioni dettagliate per il completamento dell'impostazione del SSO per l'autenticazione AD.

9.4.2 Preparazione del controller di dominio

9.4.2.1 Impostazione di un account di servizio per l'autenticazione AD con Kerberos

Per configurare la piattaforma BI affinché funzioni con l'autenticazione Windows AD (Kerberos), è necessario disporre di un account di servizio. È possibile creare un nuovo account di dominio o utilizzare un account esistente. L'account di servizio verrà utilizzato per eseguire i server della piattaforma BI. Al termine dell'impostazione, è necessario impostare anche un nome SPN per l'account stesso. Tale nome SPN viene utilizzato per importare i gruppi utente AD nella piattaforma BI.

Nota:

Per utilizzare AD con SSO, sarà necessario rivedere successivamente l'account di servizio impostato per concedere i diritti appropriati dell'account e configurarlo per la delega vincolata.

9.4.2.1.1 Per impostare l'account di servizio in un dominio Windows 2008

È necessario impostare un nuovo account di servizio per abilitare correttamente l'autenticazione Windows AD mediante il protocollo Kerberos. Questo account di servizio verrà utilizzato principalmente per consentire agli utenti di un determinato gruppo AD di accedere a BI Launch Pad. Quest'attività viene eseguita sul computer che rappresenta il controller di dominio AD.

1. Creare un nuovo account di servizio con una password sul controller di dominio principale.

2. Utilizzare il comando `setspn -a` per aggiungere i nomi principali di servizio (SPN) all'account di servizio creato al passaggio 1. Specificare i nomi principali di servizio (SPN) per l'account di servizio, il server di dominio completo e l'indirizzo IP del computer su cui è distribuito BI Launch Pad.

Ad esempio:

```
setspn -a BICMS/service_account_name.domain.com serviceaccountname
setspn -a HTTP/servername servicename
setspn -a HTTP/servername.domain.com servicename
setspn -a HTTP/<ip address of server> servicename
```

BICMS è il nome del computer su cui è in esecuzione il SIA, *nome server* è il nome del server su cui viene distribuito BI Launch Pad e *dominio nome server* è il nome di dominio completo.

3. Eseguire `setspn -l nome servizio` per verificare che i nomi principali di servizio siano stati aggiunti all'account di servizio.

L'output del comando deve includere tutti i nomi SPN registrati, come viene illustrato di seguito:

```
Registered ServicePrincipalNames for
CN=bo.service,OU=boe,OU=BIP,OU=PG,DC=DOMAIN,DC=com:
HTTP/<ip address of server>
HTTP/servername.DOMAIN.com
HTTP/servername
servername/servicenameDOMAIN.com
```

Un output di esempio viene indicato in basso:

```
C:\Users\Admin>setspn -L bossosvcacct

Registered ServicePrincipalNames for
CN=bossosvcacct,OU=svcaccts,DC=domain,DC=com:
    BICMS/bossosvcacct.domain.com
    HTTP/Tomcat HTTP/Tomcat.domain.com
    HTTP/Load_Balancer.domain.com
```

Dopo la creazione, è necessario concedere diritti all'account di servizio e aggiungere quest'ultimo al gruppo degli amministratori locali dei server. Il nome SPN verrà utilizzato per importare gruppi AD nella sezione successiva.

9.4.3 Configurazione dell'autenticazione AD nella CMC

9.4.3.1 Plug-in di protezione di Windows AD

Il plug-in di protezione Windows AD consente di mappare account utente e gruppi dal database utenti AD 2008 alla piattaforma BI. Consente inoltre al sistema di verificare tutte le richieste di accesso che specificano l'autenticazione Windows AD. L'autenticazione degli utenti viene eseguita sul database utente AD e viene verificata l'appartenenza a un gruppo AD mappato prima che il Central Management Server (CMS) conceda agli utenti una sessione attiva. È possibile utilizzare il plug-in per configurare gli aggiornamenti per i gruppi AD importati.

Il plug-in di protezione Windows AD consente di configurare quanto segue:

- Autenticazione Windows AD con Kerberos
- Autenticazione Windows AD con NTLM
- Autenticazione Windows AD con SiteMinder per il Single Sign-On

Il plug-in di protezione AD è compatibile con i domini AD 2008 eseguiti in modalità originale o mista.

Dopo essere stati mappati, gli utenti e i gruppi AD potranno accedere agli strumenti client della piattaforma BI utilizzando l'autenticazione **Windows AD**.

- L'autenticazione Windows AD funziona solo se il CMS viene eseguito su Windows. Per il corretto funzionamento del Single Sign On in un database, è necessario anche che i server per la creazione di report vengano eseguiti in Windows. In caso contrario, tutti gli altri server e servizi possono essere eseguiti su tutte le piattaforme supportate dalla piattaforma BI.
- Il plug-in di Windows AD per la piattaforma BI supporta i domini in più foreste.

9.4.3.2 Per mappare gli utenti e i gruppi AD

Prima di poter importare gruppi di utenti AD nella piattaforma BI, è necessario completare le azioni prerequisite seguenti:

- Avere creato un account di servizio nel controller di dominio per la piattaforma BI. L'account verrà utilizzato per eseguire i server della piattaforma BI.

Nota:

per consentire l'autenticazione AD con il Single Sign On Vintela, è necessario fornire un nome SPN appositamente configurato. Le operazioni descritte di seguito consentono di configurare l'autenticazione AD manuale nella piattaforma BI. Dopo aver configurato l'autenticazione AD manuale, fare riferimento alla sezione *Impostazione del Single Sign On* di questo capitolo per informazioni dettagliate sull'aggiunta del Single Sign On alla configurazione dell'autenticazione AD.

- Avere verificato che il nome SPN contenente il nome del computer su cui è in esecuzione il SIA sia stato aggiunto all'account di servizio.

I passaggi da 1 a 11 descritti di seguito sono obbligatori per importare i gruppi AD nella piattaforma BI.

1. Passare all'area di gestione "Autenticazione" della CMC.
2. Fare doppio clic su **Windows AD**.
3. Selezionare la casella di controllo **Abilita Windows Active Directory (AD)**.
4. Nell'area "Riepilogo configurazione AD" fare clic sul collegamento accanto a **Nome amministrazione AD**.

Nota:

prima di configurare il plug-in di Windows AD, questo collegamento viene visualizzato tra virgolette. Dopo avere salvato la configurazione, il collegamento viene compilato con i nomi degli amministratori AD.

5. Immettere il nome e la password di un account utente di dominio abilitato.

Le credenziali di amministrazione possono utilizzare uno dei formati seguenti:

- Nome NT (NomeDominio\NomeUtente)
- UPN (utente@DNS_dominio_nome)

Questo account viene utilizzato dalla piattaforma BI per richiedere informazioni da AD. La piattaforma non modifica, aggiunge o elimina contenuto da AD. Poiché le informazioni vengono solo lette, sono necessari solo i diritti appropriati per tale operazione.

Nota:

l'autenticazione AD non viene mantenuta se l'account utilizzato per leggere la directory AD non è più valido (ad esempio se la password dell'account viene modificata o è scaduta o se l'account viene disabilitato).

6. Immettere il dominio AD nella casella **Dominio AD predefinito**.

Il dominio deve essere specificato come NOME COMPLETO DEL DOMINIO in MAIUSCOLO o come nome di dominio secondario da cui la maggior parte degli utenti accederà alla piattaforma BI. Tale dominio deve corrispondere al dominio predefinito specificato nei file di configurazione di Kerberos utilizzati per configurare il server di applicazioni. È possibile mappare i gruppi dal dominio predefinito senza specificare il prefisso del nome di dominio. Se si digita un nome di dominio AD predefinito, non è necessario che gli utenti del dominio predefinito specifichino il nome del dominio AD quando accedono alla piattaforma BI tramite l'autenticazione AD.

7. Nell'area "Gruppi membri AD mappati" immettere il dominio\gruppo AD nella casella **Aggiungere il gruppo AD (dominio\gruppo)**, utilizzando uno dei formati seguenti per mappare i gruppi:

- Nome account SAM (Security Account Manager), indicato anche come nome NT (NomeDominio\NomeGruppo)
- DN (cn=NomeGruppo,, dc=NomeDominio, dc=com)

Nota:

per mappare un gruppo locale, utilizzare solo il formato nome NT: \\NomeServer\NomeGruppo. AD non supporta utenti locali. Gli utenti locali che appartengono a un gruppo locale mappato non vengono mappati alla piattaforma BI. Pertanto, non possono accedere al sistema.

Suggerimento:

quando si accede manualmente a BI Launch Pad, gli utenti di altri domini devono aggiungere il nome di dominio in lettere maiuscole dopo il nome utente. Ad esempio, CHILD.PARENTDOMAIN.COM è il dominio in

```
user@CHILD.PARENTDOMAIN.COM
```

8. Fare clic su **Aggiungi**.

Il codice verrà aggiunto all'elenco in "Gruppi membri AD mappati".

9. In "Opzioni di autenticazione", selezionare **Usa autenticazione Kerberos**.

10. Nella casella **Nome principale servizio** inserire il nome SPN mappato all'account di servizio creato per l'esecuzione dei server della piattaforma BI.

Nota:

è necessario specificare il nome SPN per l'account di servizio che esegue il SIA. Ad esempio: `BIC MS/bossosvcacct.domain.com`.

11. Fare clic su **Aggiorna.****Avvertenza:**

non procedere se gli utenti e/o i gruppi non vengono mappati in modo appropriato. Per risolvere problemi di mappatura dei gruppi AD specifici, fare riferimento alla nota SAP 1631734.

Nota:

se gli account del gruppo AD sono stati mappati correttamente e non si desidera configurare opzioni di autenticazione AD o aggiornamenti del gruppo AD, saltare i passaggi da 12 a 19. È possibile configurare queste impostazioni facoltative dopo aver impostato correttamente l'autenticazione Kerberos AD manuale.

12. Se la configurazione richiede SSO a un database, selezionare **Contesto di protezione della cache.****Nota:**

se si tratta della configurazione iniziale dell'autenticazione AD, è consigliabile impostare prima l'autenticazione AD manuale in modo corretto prima di prendere in considerazione la configurazione supplementare richiesta per SSO.

13. Selezionare **Abilita Single Sign On per la modalità di autenticazione selezionata se la configurazione dell'autenticazione AD richiede SSO.****14. Nell'area "Sincronizzazione delle credenziali" selezionare un'opzione per abilitare e aggiornare le credenziali di accesso all'origine dati dell'utente AD.**

Questa opzione sincronizza l'origine dati con le credenziali di accesso correnti dell'utente, consentendo in questo modo di eseguire i report pianificati quando l'utente non è collegato alla piattaforma BI e SSO Kerberos non è disponibile.

15. Nell'area "Opzioni alias AD" specificare in che modo i nuovi alias vengono aggiunti e aggiornati nella piattaforma BI.**a. Nell'area "Nuove opzioni di alias" selezionare un'opzione per la mappatura dei nuovi alias agli account Enterprise:**

- **Assegna ogni nuovo alias AD a un account utente esistente con lo stesso nome**

Utilizzare questa opzione quando è noto che gli utenti possiedono un account Enterprise già esistente con lo stesso nome; in altre parole gli alias AD saranno assegnati a utenti esistenti (la creazione di alias automatici è attivata). Gli utenti che non dispongono di un account Enterprise esistente o che non hanno lo stesso nome nei rispettivi account Enterprise e AD, verranno aggiunti come nuovi utenti.

- **Crea un nuovo account utente per ogni nuovo alias AD**

Utilizzare questa opzione quando si desidera creare un nuovo account per ciascun utente.

b. Nell'area "Opzioni di aggiornamento alias" selezionare un'opzione per la gestione degli aggiornamenti degli alias per gli account Enterprise:

- **Crea nuovi alias all'aggiornamento dell'alias**

Selezionare questa opzione per creare automaticamente un nuovo alias per ogni utente AD mappato alla piattaforma BI. I nuovi account AD vengono aggiunti per gli utenti che non dispongono di account della piattaforma BI o per tutti gli utenti, se è stata selezionata l'opzione **Crea un nuovo account utente per ogni nuovo alias AD** e si è fatto clic su **Aggiorna**.

- **Crea nuovi alias solo all'accesso dell'utente**

Selezionare questa opzione se la directory AD che si sta mappando include molti utenti, di cui solo alcuni utilizzeranno la piattaforma BI. La piattaforma non crea automaticamente alias e account Enterprise per tutti gli utenti. Creerà, invece, alias (e account, se necessario) solo per gli utenti che accedono alla piattaforma.

c. Nell'area "Nuove opzioni utente" selezionare un'opzione per creare nuovi utenti:

- **I nuovi utenti vengono creati come utenti designati**

I nuovi account utente verranno configurati per utilizzare licenze utente designato. Le licenze utente designato sono associate a utenti specifici e consentono di accedere alla piattaforma BI in base a nome utente e password. Ciò garantisce agli utenti designati l'accesso al sistema, indipendentemente dal numero di persone connesse. È necessario disporre di una licenza utente designato per ciascun account utente creato utilizzando questa opzione.

- **I nuovi utenti vengono creati come utenti simultanei**

I nuovi account utente verranno configurati per utilizzare licenze utente simultaneo. Le licenze di accesso simultaneo specificano il numero di persone che possono connettersi alla piattaforma BI contemporaneamente. Questo tipo di licenza è estremamente flessibile, poiché una licenza di accesso simultaneo di dimensioni ridotte può supportare un'ampia base di utenti. A seconda della frequenza e della durata dell'accesso al sistema, una licenza di accesso simultaneo per 100 utenti può ad esempio supportare 250, 500 o 700 utenti.

16. Per configurare come pianificare gli aggiornamenti degli Alias AD, fare clic su **Pianificazione**.

- Nella finestra di dialogo "Pianificazione" selezionare una ricorrenza nell'elenco **Esegui oggetto**.
- Impostare le opzioni e i parametri della pianificazione rimanenti nel modo richiesto.
- Fare clic su **Pianificazione**.

All'aggiornamento degli alias vengono aggiornate anche le informazioni sul gruppo.

17. Nell'area "Opzioni di collegamento attributi" è possibile specificare la priorità di collegamento degli attributi per il plug-in AD:

- Selezionare la casella di controllo **Importa nome completo, indirizzo di posta elettronica e altri attributi**.

I nomi completi e le descrizioni utilizzati negli account AD vengono importati e memorizzati con gli oggetti utente nella piattaforma BI.

- Specificare un'opzione per **Imposta priorità collegamento attributi AD relativo ad altri collegamenti attributi**.

Se l'opzione è impostata su 1, gli attributi AD hanno la priorità negli scenari in cui sono abilitati AD e altri plug-in (LDAP e SAP). Se l'opzione è impostata su 3, hanno la priorità gli attributi di altri plug-in abilitati.

18. Nell'area "Opzioni gruppo AD", configurare gli aggiornamenti del gruppo AD:

- Fare clic su **Pianifica**.

Viene visualizzata la finestra di dialogo "Pianificazione".

- b. Selezionare una ricorrenza dall'elenco a discesa **Esegui oggetto**.
- c. Impostare le opzioni e i parametri della pianificazione rimanenti nel modo richiesto.
- d. Fare clic su **Pianificazione**.

Il sistema pianifica l'aggiornamento e lo esegue in base alla pianificazione specificata.

L'aggiornamento pianificato successivo per gli account del gruppo AD viene visualizzato in "Opzioni gruppo AD".

19. Nell'area "Aggiornamento AD su richiesta" selezionare una delle seguenti opzioni:

- **Aggiorna gruppi AD ora**

Selezionare questa opzione se si desidera avviare l'aggiornamento di tutti i gruppi AD pianificati quando si fa clic su **Aggiorna**. Il prossimo aggiornamento pianificato del gruppo AD è indicato in "Opzioni gruppo AD".

- **Aggiorna alias e gruppi AD ora**

Selezionare questa opzione se si desidera avviare l'aggiornamento di tutti i gruppi e alias utente AD pianificati quando si fa clic su **Aggiorna**. I successivi aggiornamenti pianificati sono elencati in "Opzioni gruppo AD" e "Opzioni alias AD".

- **Non aggiornare alias e gruppi AD ora**

Nessun gruppo o alias utente AD verrà aggiornato quando si fa clic su **Aggiorna**.

20. Fare clic su **Aggiorna**, quindi su **OK**.

Per verificare di aver importato effettivamente gli account utente AD, andare a **CMC > Utenti e gruppi > Gerarchia gruppi** e selezionare il gruppo AD mappato per visualizzare gli utenti al suo interno. Verranno visualizzati gli utenti correnti e nidificati nel gruppo AD.

Argomenti correlati

- [Per creare un file di configurazione Kerberos](#)

9.4.3.3 Pianificazione degli aggiornamenti per i gruppi Windows AD

La piattaforma BI consente agli amministratori di pianificare gli aggiornamenti per gli alias utente e i gruppi AD. Questa caratteristica è disponibile per l'autenticazione AD con Kerberos o NTLM. La console CMC consente inoltre di visualizzare l'ora e la data in cui è stato eseguito l'ultimo aggiornamento.

Nota:

Per consentire il funzionamento dell'autenticazione AD nella piattaforma BI, è necessario configurare la pianificazione degli aggiornamenti per alias e gruppi AD.

Quando si pianifica un aggiornamento, è possibile scegliere tra gli schemi ricorrenti nella seguente tabella.

Criterio di ricorrenza	Descrizione
Ogni ora	L'aggiornamento verrà eseguito ogni ora. È possibile specificare l'ora di inizio nonché una data di inizio e di fine.
Giornaliero	L'aggiornamento verrà eseguito ogni giorno oppure dopo il numero di giorni specificato. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Settimanale	L'aggiornamento verrà eseguito ogni settimana. e può essere eseguito una o più volte a settimana. È possibile specificare in quali giorni e a che ora verrà eseguito nonché una data di inizio e di fine.
Mensile	L'aggiornamento verrà eseguito ogni mese oppure dopo il numero di mesi specificato. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Il N° giorno del mese	L'aggiornamento verrà eseguito in un giorno specifico del mese. È possibile specificare in quale giorno del mese e a che ora verrà eseguito nonché una data di inizio e di fine.
Il primo lunedì del mese	L'aggiornamento verrà eseguito il primo lunedì di ogni mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Ultimo giorno del mese	L'aggiornamento verrà eseguito l'ultimo giorno di ogni mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Giorno X della N° settimana del mese	L'aggiornamento verrà eseguito in un giorno specifico di una settimana specifica del mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Calendario	L'aggiornamento verrà eseguito nelle date specificate all'interno di un calendario creato in precedenza.

Pianificazione degli aggiornamenti dei gruppi AD

La piattaforma BI si basa su AD per le informazioni su utenti e gruppi. Per ridurre il volume delle query inviate ad AD, il plug-in AD memorizza nella cache le informazioni sui gruppi, le relative relazioni e l'appartenenza degli utenti. L'aggiornamento non viene eseguito se non si definisce una pianificazione specifica.

È necessario utilizzare la console CMC per configurare la ricorrenza dell'aggiornamento dei gruppi. Questa dovrebbe essere pianificata in base alla frequenza con cui vengono modificate le informazioni sull'appartenenza ai gruppi.

Pianificazione degli aggiornamenti degli alias utente AD

È possibile creare alias degli oggetti utente in un account AD, consentendo in tal modo agli utenti di utilizzare le proprie credenziali AD per accedere alla piattaforma BI. Gli aggiornamenti apportati agli

account AD vengono propagati nella piattaforma BI mediante il plug-in AD. Gli account creati, eliminati o disabilitati in AD verranno creati, eliminati o disabilitati anche nella piattaforma BI.

Se non si pianificano aggiornamenti agli alias AD, verranno eseguiti solo nei casi seguenti:

- All'accesso di un utente: l'alias AD verrà aggiornato.
- Un amministratore seleziona l'opzione **Aggiorna alias e gruppi AD ora** nell'area **Aggiornamento AD su richiesta** della console CMC.

Nota:

non viene memorizzata alcuna password AD nell'alias utente.

9.4.4 Configurazione del servizio della piattaforma BI per l'esecuzione del SIA

9.4.4.1 Esecuzione del SIA nell'account di servizio della piattaforma BI

Per supportare l'autenticazione AD Kerberos per la piattaforma BI, è necessario assegnare all'account di servizio il diritto di agire come parte del sistema operativo. Questa operazione deve essere eseguita su ogni computer che esegue Server Intelligence Agent (SIA) in cui sia in esecuzione il CMS (Central Management Server).

Per consentire all'account di servizio di eseguire/avviare il SIA, è necessario configurare impostazioni del sistema operativo specifiche descritte in questa sezione.

Nota:

Se si richiede il Single Sign On al database, il SIA deve includere i seguenti server:

- Crystal Reports Processing Server
- Report Application Server
- Server di elaborazione Web Intelligence

9.4.4.2 Per configurare l'esecuzione del SIA nell'account di servizio

Prima di configurare l'esecuzione del SIA nell'account di servizio della piattaforma BI, è necessario completare le azioni prerequisite seguenti:

- È stato creato un account di servizio è stato creato sul controller di dominio per la piattaforma BI.

- È stato verificato che i nomi principali servizio (SPN) sono stati aggiunti all'account di servizio.
- Sono stati mappati i gruppi di utenti AD nella piattaforma BI.

Eseguire quest'attività per qualsiasi agente SIA (Server Intelligence Agent) che esegua servizi utilizzati dall'account del servizio.

1. Per avviare CCM, scegliere **Programmi > SAP Business Intelligence > Piattaforma SAP BusinessObjects BI 4 > Central Configuration Manager**.

Viene visualizzata la home page di CCM.

2. In CCM fare clic con il pulsante destro del mouse su Server Intelligence Agent (SIA) e scegliere **Arresta**.

Nota:

Quando si arresta il SIA, vengono arrestati anche tutti i servizi gestiti dall'agente.

3. Fare clic con il pulsante destro del mouse sul SIA e scegliere **Proprietà**.
4. Deselezionare la casella di controllo **Account sistema**.
5. Immettere le credenziali dell'account di servizio (*DOMAINNAME\nome servizio*) e fare clic su **OK**.

All'account di servizio devono essere concessi i diritti seguenti sul computer su cui è in esecuzione il SIA:

- Deve disporre in modo specifico del diritto "Agire come parte del sistema operativo".
- Deve disporre in modo specifico del diritto "Accesso come servizio".
- Diritti di controllo completo per la cartella in cui è installata la piattaforma BI.
- Diritti di controllo completo per "HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects" nel registro di sistema.

6. Fare clic su **Start > Pannello di controllo > Strumenti di amministrazione > Criteri di protezione locali**.
7. Espandere **Criteri locali**, quindi fare clic su **Assegnazione diritti utente**.
8. Fare doppio clic su **Agisci come parte del sistema operativo**.
9. Fare clic su **Aggiungi** e immettere il nome dell'account di servizio creato, quindi fare clic su **OK**.
10. Ripetere la procedura descritta in precedenza per ogni computer su cui è in esecuzione un server della piattaforma BI.

Nota:

È importante selezionare il diritto valido dopo avere selezionato **Agisci come parte del sistema operativo**. Affinché questa condizione si verifichi, generalmente è necessario riavviare il server. Se, dopo il riavvio del server, l'opzione non è ancora attiva, verrà eseguito l'override delle impostazioni di criterio locale da parte delle impostazioni di criterio dominio.

11. Riavviare il SIA.
12. Se necessario, ripetere i passaggi da 1 a 5 per ogni SIA che esegue un servizio da configurare.

Ora dovrebbe essere possibile accedere al CCM utilizzando le credenziali AD.

9.4.4.3 Per verificare le credenziali AD su CCM

Per eseguire questa attività, è necessario aver mappato un gruppo di utenti AD alla piattaforma BI.

1. Aprire CCM e fare clic sull'icona **Gestisci server**.
2. Assicurarsi che nel campo "Sistema" vengano visualizzate le informazioni corrette.
3. Selezionare **Windows AD** dall'elenco delle opzioni di autenticazione.
Viene visualizzata una finestra di dialogo di connessione.
4. Accedere mediante un account AD esistente dal gruppo AD mappato nella piattaforma BI.

Nota:

Se si utilizza un account AD che non risiede nel dominio predefinito, accedere come `dominio\nomeutente`.

Non verranno visualizzati messaggi di errore. È necessario poter accedere mediante CCM utilizzando un account AD mappato prima di passare alla sezione successiva.

Suggerimento:

Se viene visualizzato un messaggio di errore, passare a **CMC > Autenticazione > Windows AD**. In "Opzioni di autenticazione" modificare **Usa autenticazione Kerberos** in **Usa autenticazione NTLM** e fare clic su **Aggiorna**. Ripetere i passaggi da 1 a 4 sopra descritti. Se il messaggio di errore non viene più visualizzato, il problema dipende dalla configurazione di Kerberos.

9.4.5 Configurazione del server di applicazioni Web per l'autenticazione AD

9.4.5.1 Preparazione del server di applicazioni per l'autenticazione Windows AD (Kerberos)

Il processo di configurazione di Kerberos per un server di applicazioni Web varia leggermente a seconda dello specifico server di applicazioni. Tuttavia, il processo generale di configurazione di Kerberos include i seguenti passaggi:

- Creazione del file di configurazione Kerberos (`krb5.ini`).
- Creazione del file di configurazione per l'accesso JAAS (`bscLogin.conf`).

Nota:

questo passaggio non è necessario per il server di applicazioni Java SAP NetWeaver 7.3. Sarà tuttavia necessario aggiungere LoginModule al server SAP NetWeaver.

- Modifica delle opzioni Java per il server di applicazioni.
- Sovrascrittura delle proprietà del file `BOE.war` per l'autenticazione Windows AD.
- Riavvio del server di applicazioni Java.

In questa sezione vengono fornite informazioni dettagliate sulla configurazione di Kerberos per l'utilizzo con i seguenti server di applicazioni:

- Tomcat
- WebSphere
- WebLogic
- Oracle Application Server
- SAP NetWeaver 7.3

9.4.5.1.1 Creazione di file di configurazione Kerberos

Per creare un file di configurazione Kerberos

Prima di procedere, assicurarsi di avere eseguito le attività prerequisite seguenti:

- È stato creato un account di servizio è stato creato sul controller di dominio per la piattaforma BI.
- È stato verificato che i nomi principali servizio (SPN) sono stati aggiunti all'account di servizio.
- Sono stati mappati i gruppi di utenti AD nella piattaforma BI.
- Le credenziali AD sono state verificate in CCM.

Seguire la procedura seguente per creare il file di configurazione Kerberos se si utilizza SAP NetWeaver 7.3, Tomcat, Oracle Application Server, WebSphere o WebLogic come server di applicazioni Web per la distribuzione della piattaforma BI.

1. Creare il file `krb5.ini`, se non è già presente e memorizzarlo in `C:\Windows` per Windows.

Nota:

- se il server di applicazioni viene installato in UNIX, è necessario utilizzare le directory seguenti:

Solaris: `/etc/krb5/krb5.conf`

Linux: `/etc/krb5.conf`

- è possibile memorizzare questo file in un'altra posizione, ma in tal caso sarà necessario specificarla nelle opzioni Java. Per ulteriori informazioni su `krb5.ini`, vedere <http://docs.oracle.com/app/docs/doc/816-0219/6m6njqb94?a=view>.

2. Aggiungere le seguenti informazioni necessarie nel file di configurazione di Kerberos:

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
```

```

.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
  default_domain = DOMAIN.COM
  kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
  default_domain = DOMAIN2.COM
  kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
  DOMAIN.COM =
}

```

Nota:

i parametri chiave sono descritti nella tabella riportata di seguito.

DOMAIN.COM	Nome DNS del dominio che deve essere immesso in lettere maiuscole nel formato FQDN.
kdc	Nome host del controller di dominio.
[capath]	Definisce l'attendibilità tra i domini che si trovano in un'altra foresta AD. Nell'esempio sopra riportato DOMAIN2.COM è un dominio di una foresta esterna con trust transitivo diretto e bidirezionale a DOMAIN.COM.
default_realm	In una configurazione con più domini, in [lib defaults] il valore default_realm potrebbe corrispondere a uno qualsiasi dei domini di origine. La soluzione migliore consiste nell'utilizzare il dominio con il maggior numero di utenti che verranno autenticati con i propri account AD. Se non viene fornito alcun suffisso UPN durante l'accesso, viene utilizzato il valore predefinito default_realm. Questo valore deve essere coerente con l'impostazione "dominio predefinito" nella console CMC. Tutti i domini devono essere specificati in maiuscolo, come viene mostrato nell'esempio sopra riportato.

9.4.5.1.2 Creazione di un file di configurazione per l'accesso JAAS

Creazione di un file di configurazione degli accessi JAAS Tomcat o WebLogic

Il file `bscLogin.conf` viene utilizzato per caricare il modulo di accesso java ed è necessario per l'autenticazione AD Kerberos sui server di applicazioni Web Java.

Il percorso predefinito per i file è: `C:\Windows`.

1. Creare un file denominato `bscLogin.conf`, se non è già presente, e memorizzarlo in `C:\Windows`.

Nota:

È possibile memorizzare il file in un altro percorso. In tal caso, tuttavia, è necessario specificare il percorso nelle opzioni Java.

2. Aggiungere il codice seguente al file di configurazione `bscLogin.conf` JAAS:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. Salvare e chiudere il file.

Per creare un file di configurazione degli accessi JAAS Oracle

1. Individuare il file `jazn-data.xml`.

Nota:

La posizione predefinita del file è `C:\OraHome_1\j2ee\home\config`. Se Oracle Application Server è stato installato in una posizione diversa, individuare il file specifico per l'installazione.

2. Aggiungere al file il seguente contenuto tra i tag `<jazn-loginconfig>`:

```
<application>
<name>com.businessobjects.security.jgss.initiate</name>
<login-modules>
<login-module>
<class>com.sun.security.auth.module.Krb5LoginModule</class>
<control-flag>required</control-flag>
</login-module>
</login-modules>
</application>
```

3. Salvare e chiudere il file `jazn-data.xml`.

Creazione di un file di configurazione degli accessi JAAS WebSphere

1. Creare un file denominato `bscLogin.conf`, se non è già presente, e memorizzarlo nel percorso predefinito: `C:\Windows`.
2. Aggiungere il codice seguente al file di configurazione degli accessi `bscLogin.conf`:

```
com.businessobjects.security.jgss.initiate {
com.ibm.security.auth.module.Krb5LoginModule required;
};
```

3. Salvare e chiudere il file.

Aggiunta di un LoginModule a SAP NetWeaver

Per utilizzare Kerberos e SAP NetWeaver 7.3, configurare il sistema come se si stesse utilizzando il server di applicazioni Web Tomcat. Non è necessario creare un file `bscLogin.conf`.

Una volta eseguita questa operazione, sarà necessario aggiungere un `LoginModule` e aggiornare alcune impostazioni Java in SAP NetWeaver 7.3.

Per mappare `com.sun.security.auth.module.Krb5LoginModule` a `com.businessobjects.security.jgss.initiate`, è necessario aggiungere manualmente un `LoginModule` a NetWeaver.

1. Aprire NetWeaver Administrator digitando l'indirizzo seguente in un browser Web: `http://<nome computer>:<porta>/nwa`.
2. Fare clic su **Configuration Management > Security > Authentication > Login Modules > Edit**.
3. Aggiungere un nuovo modulo di accesso con le informazioni seguenti:

Nome visualizzato	Krb5LoginModule
Nome classe	com.sun.security.auth.module.Krb5LoginModule

4. Fare clic su **Save**.
NetWeaver crea il nuovo modulo.
5. Fare clic su **Components > Edit**.
6. Aggiungere un nuovo criterio denominato `com.businessobjects.security.jgss.initiate`.
7. In Authentication Stack aggiungere il modulo di accesso creato al passaggio 3 e impostarlo su **Required**.
8. Verificare che non siano presenti altre voci in "Options for Selected Login Module". In caso affermativo, rimuoverle.
9. Fare clic su **Save**.
10. Scollegarsi da NetWeaver Administrator.

9.4.5.1.3 Modifica delle impostazioni Java del server di applicazioni per il caricamento di file di configurazione

Per modificare le opzioni Java per Kerberos su Tomcat

1. Nel menu **Start** selezionare **Programmi > Tomcat > Configurazione Tomcat**.
2. Fare clic sulla scheda **Java**.
3. Aggiungere le seguenti opzioni:

```
-Djava.security.auth.login.config=C:\XXXX\bscLogin.conf
-Djava.security.krb5.conf=C:\XXXX\krb5.ini
```

Sostituire XXXX con il percorso in cui è memorizzato il file `bscLogin.conf`.

4. Chiudere il file di configurazione Tomcat.
5. Riavviare Tomcat.

Per modificare le opzioni Java per SAP NetWeaver 7.3

1. Accedere allo strumento di configurazione Java (che, per impostazione predefinita, si trova nel percorso `C:\usr\sap\<ID NetWeaver>\<istanza>\j2ee\configtool\`) e fare doppio clic su `configtool.bat`.
Viene visualizzato lo strumento di configurazione.
2. Fare clic su **View > Expert Mode**.
3. Espandere **Cluster-Data > Template**.

4. Selezionare l'istanza che corrisponde al server NetWeaver in uso (ad esempio **Istanza - <ID sistema><nome computer>**).
5. Fare clic su **VM Parameters**.
6. Selezionare **SAP** nell'elenco **Vendor** e **GLOBAL** nell'elenco **Platform**.
7. Fare clic su **System** e aggiungere le seguenti informazioni sui parametri personalizzati:

java.security.krb5.conf	<percorso del file krb5.ini incluso il nome file>
javax.security.auth.useSubjectCredsOnly	false

8. Fare clic su **Save**, quindi su **Configuration Editor**.
9. Fare clic su **Configurations > Security > Configurations > com.businessobjects.security.jgss.initiate > Security > Authentication**.
10. Fare clic su **Edit Mode**.
11. Fare clic con il pulsante destro del mouse sul nodo **Authentication** e scegliere **Create sub-node**.
12. Selezionare **Value-Entry** nell'elenco in alto.
13. Immettere quanto segue:

Name	create_security_session
Valore	false

14. Fare clic su **Create**, quindi chiudere la finestra.
15. Fare clic su **Config Tool**, quindi su **Save**.

Dopo avere aggiornato la configurazione, è necessario riavviare il server NetWeaver.

Per modificare le opzioni Java per Kerberos in WebLogic

Se si utilizza Kerberos con WebLogic, è necessario modificare le opzioni Java per specificare il percorso del file di configurazione di Kerberos e del modulo di accesso Kerberos.

1. Arrestare il dominio WebLogic che esegue le applicazioni della piattaforma BI.
2. Aprire lo script che avvia il dominio di WebLogic in cui vengono eseguite le applicazioni della piattaforma BI (`startWeblogic.cmd` per Windows, `startWebLogic.sh` per UNIX).
3. Aggiungere le seguenti informazioni nella sezione `Java_Options` del file:

```
set JAVA_OPTIONS=-Djava.security.auth.login.config=C:/XXXX/bscLogin.conf
-Djava.security.krb5.conf=C:/XXX/krb5.ini
```

Sostituire XXXX con il percorso in cui è memorizzato il file.

4. Riavviare il dominio di WebLogic in cui si eseguono le applicazioni della piattaforma BI.

Per modificare le opzioni Java per Kerberos in Oracle Application Server

Se si utilizza Kerberos con Oracle Application Server, è necessario modificare le opzioni Java per specificare il percorso del file di configurazione di Kerberos.

1. Accedere alla console di amministrazione di Oracle Application Server.
2. Fare clic sul nome dell'istanza OC4J in cui vengono eseguite le applicazioni della piattaforma BI.
3. Selezionare **Proprietà server**.
4. Scorrere verso il basso fino alla sezione relativa alla configurazione VM multipla.
5. Nella sezione Opzioni riga di comando, aggiungere quanto segue alla fine del campo di testo "Opzioni Java": `-Djava.security.krb5.conf=C:/XXXX/krb5.ini` sostituendo XXXX con il percorso in cui è memorizzato il file.
6. Riavviare l'istanza OC4J.

Per modificare le opzioni Java per Kerberos in WebSphere

1. Accedere alla console di amministrazione per WebSphere.
Per IBM WebSphere 5.1, digitare `http://nomeserver:9090/admin` Per IBM WebSphere 6.0, digitare `http://nomeserver:9060/ibm/console`
2. Espandere il server, fare clic su **Server di applicazioni**, quindi sul nome del server di applicazioni creato per l'uso con la piattaforma BI.
3. Passare alla pagina "JVM".

Se si utilizza WebSphere 5.1, seguire questa procedura per accedere alla pagina "JVM".

- a. Nella pagina del server, scorrere verso il basso fino a **Definizione processo** nella colonna **Proprietà supplementari**.
- b. Fare clic su **Definizione processo**.
- c. Scorrere verso il basso e fare clic su **Java Virtual Machine**.

Se si utilizza WebSphere 6.0, seguire questa procedura per accedere alla pagina "JVM".

- a. Nella pagina del server selezionare **Java e Process Management**.
- b. Selezionare **Definizione di processo**.
- c. Selezionare **Java Virtual Machine**.

4. Fare clic su **Argomenti JVM generici**, quindi specificare il percorso del file `Krb5.ini` e del file `bscLogin.conf` come illustrato di seguito.

`-Djava.security.auth.login.config=C:\XXXX\bscLogin.conf`

`-Djava.security.krb5.conf=C:/XXXX/krb5.ini`

Sostituire XXXX con il percorso in cui è memorizzato il file.

5. Fare clic su **Applica**, quindi su **Salva**.
6. Arrestare e riavviare il server.

9.4.5.1.4 Per verificare che Java possa ricevere un ticket Kerberos

Prima di verificare se Java ha ricevuto il ticket Kerberos, è necessario completare le azioni prerequisite seguenti:

- Creare il file `bscLogin.conf` per il server di applicazioni.
- Creare il file `krb5.ini`.

1. Andare al prompt dei comandi e passare alla directory `jdk\bin` nell'installazione della piattaforma BI.

Per impostazione predefinita, si trova nel percorso: `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\jdk\bin`.

2. Eseguire `kinit <nomeutente>`

3. Premere **Invio**.

4. Digitare la password.

Se il file `krb5.ini` è stato configurato correttamente e il modulo di accesso Java è stato caricato, verrà visualizzato il messaggio seguente:

Il nuovo ticket è memorizzato nel file di cache
`C:\Users\Administrator\krb5cc_Administrator`

Non proseguire con l'impostazione AD fino a quando non viene ricevuto correttamente un ticket Kerberos.

Se non è possibile ricevere un ticket, prendere in considerazione le opzioni seguenti:

- Consultare la sezione relativa alla risoluzione dei problemi alla fine del capitolo.
- Per i problemi relativi al KDC, ai file di configurazione Kerberos e alle credenziali utente non disponibili nel database Kerberos, fare riferimento agli articoli della Knowledge Base SAP KBA 1476374 e KBA 1245178.

9.4.5.1.5 Configurazione di BI Launch Pad per l'accesso AD manuale

Prima di configurare le applicazioni della piattaforma BI per l'accesso AD manuale, è necessario completare le seguenti azioni prerequisite:

- È stato creato un account di servizio nel controller di dominio per la piattaforma BI.
- È stato verificato che i nomi principali servizio (SPN) HTTP sono stati aggiunti all'account di servizio.
- Sono stati mappati i gruppi di utenti AD nella piattaforma BI.
- Le credenziali AD sono state verificate in CCM.
- I file di configurazione richiesti sono stati creati, configurati e verificati nel server di applicazioni Web.
- Le impostazioni Java del server di applicazioni sono state modificate per caricare i file di configurazione.

Per abilitare l'opzione di autenticazione di Windows AD per BI Launch Pad, eseguire le seguenti operazioni:

1. Accedere alla cartella personalizzata dell'applicazione Web BOE nel computer che ospita il server di applicazioni Web:

`<DIRINSTALL>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\.`

Apportare le modifiche desiderate nella directory `config\custom` e non nella directory `config\default`. In caso contrario, le modifiche verranno sovrascritte quando alla distribuzione verranno applicate patch future.

Sarà quindi necessario ridistribuire l'applicazione Web BOE.

2. Creare un nuovo file.

Nota:

utilizzare Blocco note o un'altra utilità per la modifica del testo.

3. Salvare il file come `BIlaunchpad.properties`.

4. Digitare quanto segue:

```
authentication.visible=true  
authentication.default=secWinAD
```

5. Salvare e chiudere il file.

6. Riavviare il server di applicazioni Web.

Dovrebbe ora essere possibile accedere manualmente a BI Launch Pad. Accedere all'una o all'altra applicazione e selezionare Windows AD dall'elenco di opzioni di autenticazione.

Nota:

non proseguire con l'impostazione di Windows AD fino a quando non è possibile accedere manualmente a BI Launch Pad con un account AD esistente.

Le nuove proprietà avranno effetto solo dopo la ridistribuzione dell'applicazione Web BOE modificata nel computer su cui è in esecuzione il server di applicazioni Web. Utilizzare WDeploy per ridistribuire BOE sul server di applicazioni Web. Per ulteriori informazioni sull'utilizzo di WDeploy per annullare la distribuzione delle applicazioni Web, vedere il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects BI*.

Nota:

Se nella distribuzione viene utilizzato un firewall, ricordarsi di aprire tutte le porte necessarie. In caso contrario le applicazioni Web non saranno in grado di connettersi ai server della piattaforma BI.

9.4.6 Impostazione del Single Sign On

9.4.6.1 Single Sign On alla piattaforma BI con autenticazione AD

Opzioni per il Single Sign On mediante Windows AD

Sono supportati due metodi per l'impostazione del Single Sign On (SSO) per l'autenticazione Windows AD con la piattaforma BI:

- Vintela - questa opzione può essere utilizzata solo con Kerberos.
- SiteMinder - questa opzione può essere utilizzata solo con Kerberos.

SSO al database

Il SSO al database consente agli utenti collegati di eseguire azioni che richiedono l'accesso al database, in particolare la visualizzazione e l'aggiornamento di report senza dover fornire nuovamente le credenziali di accesso. Sebbene la delega vincolata sia facoltativa per l'autenticazione AD e il Single Sign On Vintela, è necessaria per gli scenari di distribuzione che comportano il Single Sign On al database di sistema.

SSO end-to-end

Nella piattaforma BI il Single Sign On end-to-end è supportato tramite Windows AD e Kerberos. In questo scenario gli utenti dispongono sia dell'accesso Single Sign On alla piattaforma BI al front-end sia dell'accesso SSO ai database nel back-end. Pertanto, per avere accesso alla piattaforma BI ed essere in grado di eseguire azioni che richiedono l'accesso al database, ad esempio la visualizzazione dei report, gli utenti dovranno fornire le proprie credenziali di accesso una sola volta, nel momento in cui accedono al sistema operativo.

Confronto tra la configurazione manuale e l'autenticazione AD SSO

Dopo aver configurato correttamente la distribuzione per consentire agli account AD un accesso manuale a BI Launch Pad, è necessario rivedere l'impostazione dell'autenticazione AD per soddisfare i requisiti specifici del Single Sign On. Tali requisiti variano in base al metodo di Single Sign On scelto.

9.4.6.2 Utilizzo del Single Sign On Vintela

9.4.6.2.1 Lista di controllo per l'impostazione del Single Sign On Vintela

Per impostare la piattaforma BI affinché funzioni con il Single Sign On Vintela, è necessario completare le attività seguenti:

1. Configurare specificamente l'account di servizio per il Single Sign On Vintela.
2. Configurare la delega vincolata (facoltativa).
3. Configurare le opzioni di autenticazione SSO Windows AD nella console CMC.
4. Configurare le proprietà generali quelle e specifiche di BI Launch Pad per il Single Sign On Vintela.
5. Se si sta utilizzando Tomcat come server di applicazioni Web per la distribuzione, è necessario aumentare il limite delle dimensioni dell'intestazione.
6. Configurare i browser Internet per Vintela.

9.4.6.2.2 Per impostare l'account di servizio per il Single Sign On Vintela

Lo strumento da riga di comando `ktpass` configura il nome principale servizio per l'host o il servizio in Active Directory e genera un file "codice" Kerberos contenente la chiave segreta condivisa dell'account

di servizio. Tale strumento in genere si trova sui controller di dominio oppure può essere scaricato dal sito del supporto Microsoft: <http://support.microsoft.com/kb/892777>.

È necessario un account di servizio appositamente configurato per consentire agli utenti di un determinato gruppo Windows AD di eseguire automaticamente l'autenticazione a BI Launch Pad con le rispettive credenziali AD. L'account di servizio creato per l'autenticazione AD Kerberos può essere riconfigurato sul controller di dominio.

Quando un client tenta di accedere a BI Launch Pad, viene avviata una richiesta al server che genera ticket Kerberos. Per facilitare la richiesta, l'account di servizio creato per la piattaforma BI deve avere un nome SPN corrispondente all'URL del server delle applicazioni. Eseguire la procedura seguente sul computer che ospita il controller di dominio.

1. Eseguire il comando di impostazione del codice Kerberos `ktpass` per creare e posizionare un file di codice.

Specificare i parametri `ktpass` elencati nella tabella seguente:

Parametro	Descrizione
<code>-out</code>	Specifica il nome del file Kerberos <code>keytab</code> da generare.
<code>-princ</code>	<p>Specifica il nome principale utilizzato per l'account di servizio, nel formato SPN: <code>MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.COM</code>, dove <code>MYSIAMYSERVER</code> è il nome del SIA (Service Intelligence Agent), specificato in CCM (Central Configuration Manager).</p> <p>Nota: Per il nome dell'account di servizio occorre distinguere tra maiuscole e minuscole. L'SPN include il nome del computer host su cui è in esecuzione l'istanza del servizio.</p> <p>Suggerimento: L'SPN deve essere univoco nella foresta in cui viene registrato. Per effettuare il controllo, utilizzare lo strumento di supporto Windows <code>Ldp.exe</code> per cercare il nome SPN.</p>
<code>-pass</code>	Specifica la password utilizzata dall'account di servizio.
<code>-ptype</code>	<p>Specifica il tipo principale:</p> <pre>-ptype KRB5_NT_PRINCIPAL</pre>
<code>-crypto</code>	<p>Specifica il tipo di crittografia da utilizzare con l'account di servizio:</p> <pre>-crypto RC4-HMAC-NT</pre>

Ad esempio:

```
ktpass -out keytab_filename.keytab -princ MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.COM
-pass password -kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

L'output del comando `ktpass` deve confermare il controller di dominio di destinazione e l'avvenuta creazione del file di `codice` Kerberos contenente il segreto condiviso creato. Il comando mappa anche il nome principale all'account di servizio (locale).

2. Fare clic con il pulsante destro del mouse sull'account di servizio, scegliere **Proprietà > Delega**.
3. Fare clic su **Utente attendibile per la delega a qualsiasi servizio (solo Kerberos)**.
4. Fare clic su **OK** per salvare le modifiche apportate.

L'account di servizio ora dispone di tutti i nomi principali servizio richiesti per il Single Sign On Vintela ed è stato generato un file di codice con la password crittografata per l'account di servizio stesso.

Per configurare la delega vincolata per il Single Sign On Vintela

La delega vincolata è facoltativa per l'impostazione del Single Sign On Vintela. È tuttavia obbligatoria per le distribuzioni che richiedono il Single Sign On (SSO) al database di sistema.

1. Sul computer che rappresenta il controller di dominio aprire lo snap-in "Utenti e computer" Active Directory.
2. Fare clic con il pulsante destro del mouse sull'account di servizio creato nella sezione precedente e scegliere **Proprietà > Delega**.
3. Selezionare **Utente attendibile per delega solo ai servizi specificati**.
4. Selezionare **Utilizza solo Kerberos**.
5. Fare clic su **Aggiungi > Utenti o computer**.
6. Immettere il nome dell'account di servizio e fare clic su **OK**.
Viene visualizzato un elenco di servizi.
7. Selezionare i servizi indicati di seguito e fare clic su **OK**.
 - Il servizio HTTP
 - Il servizio utilizzato per eseguire il Service Intelligence Agent (SIA) sul computer che ospita la piattaforma BI.

I servizi vengono aggiunti all'elenco dei servizi delegabili per l'account di servizio.

Per giustificare questa modifica, è necessario modificare le proprietà dell'applicazione Web.

9.4.6.2.3 Per configurare le impostazioni SSO nella console CMC

1. Passare all'area di gestione "Autenticazione" della CMC.
2. Fare doppio clic su **Windows AD**.
3. Assicurarsi che la casella **Abilita Windows Active Directory (AD)** sia selezionata.
4. In "Opzioni di autenticazione" assicurarsi che l'opzione **Usa autenticazione Kerberos** sia selezionata.
5. Se la configurazione richiede il SSO al database, selezionare **Contesto di protezione della cache**.
6. Selezionare **Abilita Single Sign On per la modalità di autenticazione selezionata**.
7. Fare clic su **Aggiorna**.

9.4.6.2.4 Abilitazione del Single Sign-On Vintela per BI Launch Pad e OpenDocument

Questa procedura viene utilizzata per BI Launch Pad o OpenDocument. Per abilitare il Single Sign On alle applicazioni Web della piattaforma Web, è necessario specificare le proprietà specifiche di Vintela e del Single Sign On nel file `BOE.war`. Ai fini dell'impostazione SSO, è consigliabile concentrarsi sull'abilitazione del Single Sign-On su BI Launch Pad per gli account AD prima di gestire altre applicazioni.

1. Accedere alla cartella personalizzata dell'applicazione Web BOE nel computer che ospita il server di applicazioni Web:

```
<DIRINSTALL>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\.
```

Apportare le modifiche desiderate nella directory `config\custom` e non nella directory `config\default`. In caso contrario, le modifiche verranno sovrascritte quando alla distribuzione verranno applicate patch future.

Sarà quindi necessario ridistribuire l'applicazione Web BOE.

2. Creare un nuovo file utilizzando un editor di testo.
3. Immettere quanto segue:

```
sso.enabled=true
siteminder.enabled=false
vintela.enabled=true
idm.realm=DOMAIN.COM
idm.princ=MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.COM
idm.allowUnsecured=true
idm.allowNTLM=false
idm.logger.name=simple
idm.keytab=C:/WIN/filename.keytab
idm.logger.props=error-log.properties
```

Nota:

- è necessario specificare valori validi per i parametri `idm.realm` e `idm.princ`. Il valore di `idm.realm` deve corrispondere a quello impostato al momento della configurazione di `default_realm` nel file `krb5.ini`. Il valore deve essere in lettere maiuscole. Il parametro `idm.princ` corrisponde all'SPN utilizzato per l'account di servizio creato per l'SSO Vintela.
- Nel percorso del file di codice è necessario inserire le barre.

Se non si desidera utilizzare la delega vincolata per l'autenticazione di Windows AD e SSO Vintela, ignorare il passaggio che segue.

4. Per utilizzare la delega vincolata aggiungere:

```
idm.allowS4U=true
```

5. Chiudere il file e salvarlo con il nome `global.properties`:

Nota:

accertarsi che il nome file non venga salvato con un'estensione diversa da `.txt`.

6. Creare un altro file nella stessa directory. Salvare il file come `OpenDocument.properties` o `BI launchpad.properties`, a seconda dei requisiti.

7. Digitare quanto segue:

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

Ad esempio:

```
authentication.default=secWinAD
cms.default=mycms:6400
```

8. Salvare e chiudere il file.

9. Riavviare il server di applicazioni Web.

Le nuove proprietà avranno effetto solo dopo la ridistribuzione dell'applicazione Web BOE modificata nel computer su cui è in esecuzione il server di applicazioni Web. Utilizzare WDeploy per ridistribuire BOE sul server di applicazioni Web. Per ulteriori informazioni sull'utilizzo di WDeploy per annullare la distribuzione delle applicazioni Web, vedere il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects BI*.

Nota:

Se nella distribuzione viene utilizzato un firewall, ricordarsi di aprire tutte le porte necessarie, altrimenti le applicazioni Web non saranno in grado di connettersi ai server della piattaforma BI.

9.4.6.2.5 Per abilitare il Single Sign-On Vintela per i servizi Web

Alcuni strumenti client richiedono l'autenticazione mediante i servizi Web. Seguire i passaggi indicati di seguito per abilitare il Single Sign-On (SSO) per i servizi Web.

1. Creare una copia di backup di questo file: `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\web.xml` e aprirlo per modificarlo.
2. Rimuovere i commenti dalle sezioni Kerberos Proxy Filter e Kerberos Filter per abilitare l'autenticazione SSO Kerberos per Windows Active Directory (secWinAD).

È necessario specificare le opzioni seguenti (le altre sono facoltative):

- `idm.realm` (corrispondente al valore di `default_realm` specificato nel file `Krb5.ini`).
- `idm.princ` (corrispondente al valore di `idm.princ` specificato nel file `global.properties` che si trova in `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).
- `idm.keytab` (corrispondente al valore di `idm.keytab` specificato nel file `global.properties` che si trova in `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`).

Nota:

Se si utilizza la password codificata impostata nelle opzioni Java di Tomcat, non apportare modifiche alle righe `keytab` nel file `web.xml`.

3. Se insieme al server di applicazioni Java non viene utilizzato SSL, impostare il parametro `idm.allowUnsecured` su `true`.
Per ulteriori informazioni su SSL Tomcat, consultare l'articolo 1484802 della Knowledge Base.
4. Creare una copia di backup di questo file: `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\classes\dsws.properties` e aprirlo per modificarlo.

5. Impostare `kerberos.sso` su `true` e salvare il file.
6. Utilizzare WDeploy per ridistribuire il file WAR sul server di applicazioni Web.
Per ulteriori informazioni sull'utilizzo di WDeploy, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.
7. Riavviare Tomcat.
8. Per verificare le impostazioni, nel computer client in cui sono installati gli strumenti client avviare Query as a Web Service Designer.
9. Aggiungere un nuovo host gestito.
10. Immettere il nome del server di applicazioni.
11. Immettere l'URL dei servizi Web nel formato seguente: `http://<ServerAppWeb>:<NumeroPorta>/dswsbobje/services/Session`.
Esempio: `http://BI4:8080/dswsbobje/services/Session`.
12. Immettere il nome host CMS.
13. Cambiare il tipo di autenticazione in **Windows AD**.
14. Selezionare **Abilita Windows Active Directory Single Sign-On**.
15. Al prompt di accesso lasciare vuoti i campi **Utente** e **Password** e fare clic su **OK**.

9.4.6.2.6 Innalzamento del limite per le dimensioni delle intestazioni in Tomcat

Active Directory crea un token Kerberos utilizzato nel processo di autenticazione. Questo token viene memorizzato nell'intestazione HTTP. Il server applicazioni Java presenterà dimensioni dell'intestazione HTTP predefinite. Per evitare errori, assicurarsi che le dimensioni predefinite minime siano pari a 16384 byte. (Alcune distribuzioni potrebbero richiedere dimensioni superiori. Per ulteriori informazioni, vedere le indicazioni sulle dimensioni di Microsoft sul sito di supporto all'indirizzo <http://support.microsoft.com/kb/327825>).

1. Nel server su cui è installato Tomcat aprire il file `server.xml`.
In Windows, questo file si trova in `<DIRINSTALLTomcat>/conf`
 - Se si utilizza la versione di Tomcat installata con la piattaforma BI in Windows e non è stato modificato
il percorso di installazione predefinito, sostituire `<DIRINSTALLAZTomcat>` con `C:\Programmi (x86)\SAP BusinessObjects\Tomcat\`
 - Se si utilizza qualsiasi altro server di applicazioni Web supportato, consultare la documentazione del server per determinare il percorso appropriato.
2. Individuare il tag `<Connector ...>` corrispondente per il numero della porta configurata.
Se si utilizza la porta predefinita 8080, individuare il tag `<Connector ...>` che contiene `port="8080"`.

Ad esempio:

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
minSpareThreads="25" port="8080" redirectPort="8443"
/>
```

3. Aggiungere il seguente valore all'interno del tag `<Connector ...>`:

```
maxHttpHeaderSize="16384"
```

Ad esempio:

```
<Connector URIEncoding="UTF-8" acceptCount="100"
connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
maxSpareThreads="75" maxThreads="150"
maxHttpHeaderSize="16384" minSpareThreads="25" port="8080" redirectPort="8443" />
```

4. Salvare e chiudere il file `server.xml`.
5. Riavviare Tomcat.

Nota:

Per altri server di applicazioni Java, consultare la relativa documentazione.

9.4.6.2.7 Configurazione dei browser Internet

Per supportare il Single Sign On Vintela per l'autenticazione AD Kerberos, è necessario configurare i client della piattaforma BI. Ciò comporta la configurazione del browser Web nei computer client.

Per configurare Internet Explorer nei computer client

1. Nel computer client aprire una finestra del browser Internet Explorer.
2. Abilitare l'autenticazione Windows integrata.
 - a. Nel menu **Strumenti**, fare clic su **Opzioni Internet**.
 - b. Fare clic sulla scheda **Avanzate**.
 - c. Scorrere fino a **Protezione**, selezionare **Abilita autenticazione Windows integrata**, quindi fare clic su **Applica**.
3. Aggiungere il computer applicazioni Java oppure l'URL dei siti affidabili. È possibile immettere il nome completo di dominio del sito.
 - a. Nel menu **Strumenti**, fare clic su **Opzioni Internet**.
 - b. Fare clic sulla scheda **Protezione**.
 - c. Fare clic su **Siti**, quindi su **Avanzato**.
 - d. Selezionare o immettere il sito e fare clic su **Aggiungi**.
 - e. Fare clic su **OK** fino alla chiusura della finestra di dialogo Opzioni Internet.
4. Chiudere e riaprire la finestra del browser Internet Explorer per rendere effettive queste modifiche.
5. Ripetere l'intera procedura precedente per ogni computer client della piattaforma BI.

Per configurare Firefox nei computer client

1. **Modificare network.negotiate-auth.delegation-uris.**
 - a. Nel computer client aprire un'istanza del browser Firefox.
 - b. Digitare `about:config` nel campo dell'indirizzo URL.
Viene visualizzato un elenco di proprietà configurabili.
 - c. Fare doppio clic su **network.negotiate-auth.delegation-uris** per modificare la proprietà.

- d. Immettere l'URL da utilizzare per l'accesso a BI Launch Pad.

Se ad esempio l'URL di BI Launch Pad è `http://machine.domain.com:8080/BOE/BI`, sarà necessario immettere `http://machine.domain.com`.

Nota:

Per aggiungere più URL, separarli con una virgola. Ad esempio `http://computer.dominio.com, computer2.dominio.com`.

- e. Fare clic su **OK**.

2. Modificare `network.negotiate-auth.trusted-uris`

- a. Nel computer client aprire un'istanza del browser Firefox.
- b. Digitare `about:config` nel campo dell'indirizzo URL.
Viene visualizzato un elenco di proprietà configurabili.
- c. Fare doppio clic su **`network.negotiate-auth.trusted-uris`** per modificare la proprietà.
- d. Immettere l'URL da utilizzare per l'accesso a BI Launch Pad.

Se ad esempio l'URL di BI Launch Pad è `http://machine.domain.com:8080/BOE/BI`, sarà necessario immettere `http://machine.domain.com`.

Nota:

Per aggiungere più URL, separarli con una virgola. Ad esempio `http://computer.dominio.com, computer2.dominio.com`.

- e. Fare clic su **OK**.

3. Chiudere e riaprire la finestra del browser Firefox per rendere effettive queste modifiche.
4. Ripetere l'intera procedura precedente per ogni computer client della piattaforma BI.

9.4.6.2.8 Verifica del Single Sign On Vintela per l'autenticazione AD Kerberos

È necessario verificare l'impostazione del Single Sign On da una workstation client. Assicurarsi che il client si trovi sullo stesso dominio della distribuzione della piattaforma BI e che l'accesso alla workstation sia stato effettuato come un utente AD mappato. Questo account utente deve essere in grado di accedere manualmente a BI Launch Pad.

Per verificare il Single Sign On, aprire un browser e immettere l'URL per BI Launch Pad. Se il Single Sign On è configurato correttamente, non verrà richiesto di immettere le credenziali di accesso.

Suggerimento:

È consigliabile testare diversi scenari di utenti AD nella distribuzione in uso. Se ad esempio l'ambiente include utenti di più sistemi operativi, è necessario testare il Single Sign On per gli utenti provenienti da ciascuno di essi, nonché su tutti i possibili browser supportati nell'organizzazione. Se l'ambiente include utenti provenienti da più foreste o domini, è necessario testare il Single Sign On per un account utente di ciascun dominio o foresta.

9.4.6.2.9 Configurazione di Kerberos e di Single Sign On nel database per i server di applicazioni

Single Sign On nel database è supportato per le distribuzioni che soddisfano tutti i seguenti requisiti:

- La distribuzione della piattaforma BI avviene in un server di applicazioni Web.
- Il server di applicazioni Web è stato configurato per il Single Sign On Vintela per l'autenticazione AD.
- Il database per cui è necessario il Single Sign On è una versione supportata di SQL Server o Oracle.
- Ai gruppi o agli utenti per i quali è necessario l'accesso al database devono essere state concesse autorizzazioni all'interno di SQL Server o Oracle.

Il passaggio finale consiste nel modificare il file `krb5.ini` per supportare il Single Sign On al database per applicazioni Web.

Per abilitare la funzionalità Single Sign On nel database per i server di applicazioni Java

1. Aprire il file `krb5.ini` utilizzato per la distribuzione della piattaforma BI.

La posizione predefinita di questo file è la directory WIN nel server di applicazioni Web.

Nota:

Se non è possibile trovare il file nella directory WIN, controllare il seguente argomento Java per la posizione del file:

```
-Djava.security.auth.login.config
```

Questa variabile viene specificata quando si configura AD con Kerberos nel server di applicazioni Web.

2. Passare alla sezione `[libdefaults]` del file.
3. Immettere la stringa seguente prima dell'inizio della sezione `[realms]` del file:

```
forwardable=true
```

4. Salvare e chiudere il file.
5. Riavviare il server di applicazioni Web.

Il Single Sign-On al database non verrà abilitato fino a quando non si seleziona la casella **Contesto di protezione della cache (richiesto per SSO al database)** nella pagina di autenticazione Windows AD della CMC.

9.4.6.3 Utilizzo di SiteMinder

9.4.6.3.1 Utilizzo di Windows AD con SiteMinder

In questa sezione viene illustrato come utilizzare AD e SiteMinder. SiteMinder è uno strumento di terzi per l'autenticazione e l'accesso utente che è possibile utilizzare con il plug-in di protezione AD per creare il Single Sign On nella piattaforma BI. È possibile utilizzare SiteMinder con Kerberos.

Assicurarsi che le risorse di gestione delle identità SiteMinder siano installate e configurate prima di configurare l'autenticazione Windows AD per l'utilizzo di SiteMinder. Per ulteriori informazioni su SiteMinder e su come eseguirne l'installazione, fare riferimento alla documentazione di SiteMinder.

Per l'abilitazione del Single Sign-On AD con SiteMinder sono richieste due attività:

- Configurare il plug-in AD per il Single Sign-On con SiteMinder
- Configurare le proprietà SiteMinder per l'applicazione Web BOE

Nota:

assicurarsi che l'amministratore di SiteMinder abbia abilitato il supporto per gli agenti 4.x. L'operazione va eseguita a prescindere dalla versione in uso di SiteMinder. Per ulteriori informazioni sulla configurazione di SiteMinder, consultare la documentazione di SiteMinder.

Per abilitare le proprietà di SiteMinder per BI Launch Pad

Oltre che per il plug-in di protezione Windows AD, le impostazioni di SiteMinder devono essere specificate anche per le proprietà war BOE.

1. Individuare la directory `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\` nell'installazione della piattaforma BI.
2. Creare un nuovo file nella directory, utilizzando Blocco note o un'altra utilità di elaborazione testo.
3. Nel nuovo file, immettere i valori seguenti:

```
sso.enabled=true
siteminder.authentication=secWinAD
siteminder.enabled=true
```

4. Salvare il file con il nome `global.properties`.

Nota:

accertarsi che il nome file non venga salvato con un'estensione diversa da `.txt`.

5. Creare un altro file nella stessa directory.
6. Nel nuovo file, inserire i seguenti valori:

```
authentication.default=secWinAD
cms.default=[cms name]:[CMS port number]
```

Ad esempio:

```
authentication.default=LDAP
cms.default=mycms:6400
```

7. Salvare il file con il nome `BIlaunchpad.properties`, quindi chiuderlo.

Le nuove proprietà verranno applicate dopo la redistribuzione di `BOE.war` nel computer su cui è in esecuzione il server di applicazioni Web. Utilizzare WDeploy per ridistribuire il file WAR sul server di applicazioni Web. Per ulteriori informazioni sull'utilizzo di WDeploy per annullare la distribuzione delle applicazioni Web, vedere il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects BI*.

Per configurare le impostazioni SiteMinder nella console CMC

Prima di configurare la console CMC per SiteMinder, è necessario completare le azioni prerequisite presenti:

- Sono stati mappati i gruppi di utenti AD nella piattaforma BI.
- Le credenziali AD sono state verificate in CCM.

1. Passare all'area di gestione "Autenticazione" della CMC.
2. Fare doppio clic su **Windows AD**.
3. Selezionare la casella di controllo **Abilita Windows Active Directory (AD)**.
4. In Opzioni di autenticazione selezionare **Usa autenticazione NTLM** oppure **Usa autenticazione Kerberos**.

Per configurare la piattaforma BI per l'autenticazione Kerberos e AD mediante Kerberos, è necessario un account di servizio. È possibile creare un nuovo account di dominio o utilizzare un account esistente. L'account di servizio verrà utilizzato per eseguire i server della piattaforma BI.

Suggerimento:

Quando si accede manualmente a BI Launch Pad, gli utenti di altri domini devono aggiungere il nome di dominio in lettere maiuscole dopo il nome utente. Ad esempio, in `user@CHILD.PARENT DOMAIN.COM`, "CHILD.PARENTDOMAIN.COM" è il dominio.

5. Se si seleziona **Usa autenticazione Kerberos**:
 - a. Se si desidera configurare il Single Sign On per un database, selezionare **Contesto di protezione della cache**.
 - b. Eliminare qualsiasi informazione nella casella **Nome principale servizio**.
6. Per configurare il Single Sign-On, selezionare **Abilita il Single Sign-On per la modalità di autenticazione selezionata**.

Per abilitare il Single Sign On, è necessario anche configurare le proprietà generali dell'applicazione Web e di BI Launch Pad.
7. Nell'area "Sincronizzazione delle credenziali" selezionare un'opzione per abilitare e aggiornare le credenziali di origine dati dell'utente AD all'accesso.

Questa opzione consente di sincronizzare l'origine dati con le credenziali di accesso correnti dell'utente.
8. Nell'area "Opzioni SiteMinder" configurare SiteMinder come opzione di Single Sign On per l'autenticazione AD mediante Kerberos:
 - a. Fare clic su **Disabilitato**.

Viene visualizzata la pagina "Windows Active Directory".

Se non è stato configurato il plug-in Windows AD, viene visualizzato un avviso in cui viene chiesto se si desidera continuare. Scegliere **OK**.
 - b. Fare clic su **Usa il Single Sign On SiteMinder**.
 - c. Nella casella **Host del server dei criteri** digitare il nome di ogni server dei criteri, quindi scegliere **Aggiungi**.

- d. Per ogni host del server dei criteri, immettere un numero di porta nelle caselle **Contabilità, Autenticazione e Autorizzazione**.
 - e. Nella casella **Nome dell'agente** immettere il nome dell'agente.
 - f. Nelle caselle **Segreto condiviso** immettere il segreto condiviso.

Assicurarsi che l'amministratore di SiteMinder abbia abilitato il supporto per gli agenti 4.x, indipendentemente dalla versione di SiteMinder supportata utilizzata. Per ulteriori informazioni su SiteMinder e su come installarlo, vedere la documentazione di SiteMinder.
 - g. Fare clic su **Aggiorna** per salvare le informazioni e tornare alla pagina di autenticazione AD principale.
9. Nell'area "Opzioni alias AD" specificare in che modo i nuovi alias vengono aggiunti e aggiornati nella piattaforma BI.
- a. Nell'area "Nuove opzioni di alias" selezionare un'opzione per la mappatura dei nuovi alias agli account Enterprise:
 - **Assegna ogni nuovo alias AD a un account utente esistente con lo stesso nome**

Utilizzare questa opzione quando è noto che gli utenti possiedono un account Enterprise già esistente con lo stesso nome; in altre parole gli alias AD saranno assegnati a utenti esistenti (la creazione di alias automatici è attivata). Gli utenti che non dispongono di un account Enterprise esistente o che non hanno lo stesso nome nei rispettivi account Enterprise e AD, verranno aggiunti come nuovi utenti.
 - **Crea un nuovo account utente per ogni nuovo alias AD**

Utilizzare questa opzione quando si desidera creare un nuovo account per ciascun utente.
 - b. Nell'area "Opzioni di aggiornamento alias" selezionare un'opzione per la gestione degli aggiornamenti degli alias per gli account Enterprise:
 - **Crea nuovi alias all'aggiornamento dell'alias**

Selezionare questa opzione per creare automaticamente un nuovo alias per ogni utente AD mappato alla piattaforma BI. I nuovi account AD vengono aggiunti per gli utenti che non dispongono di account della piattaforma BI o per tutti gli utenti, se è stata selezionata l'opzione **Crea un nuovo account utente per ogni nuovo alias AD** e si è fatto clic su **Aggiorna**.
 - **Crea nuovi alias solo all'accesso dell'utente**

Selezionare questa opzione se la directory AD che si sta mappando include molti utenti, di cui solo alcuni utilizzeranno la piattaforma BI. La piattaforma non crea automaticamente alias e account Enterprise per tutti gli utenti. Creerà, invece, alias (e account, se necessario) solo per gli utenti che accedono alla piattaforma.
 - c. Nell'area "Nuove opzioni utente" selezionare un'opzione per creare nuovi utenti:
 - **I nuovi utenti vengono creati come utenti designati**

I nuovi account utente verranno configurati per utilizzare licenze utente designato. Le licenze utente specifico sono associate a utenti specifici e consentono di accedere al sistema in base a nome utente e password. Ciò garantisce agli utenti specifici l'accesso al sistema, indipendentemente dal numero di persone connesse. È necessario disporre di una licenza utente designato per ciascun account utente creato utilizzando questa opzione.

- **I nuovi utenti vengono creati come utenti simultanei**

I nuovi account utente verranno configurati per utilizzare licenze utente simultaneo. Le licenze di accesso simultaneo specificano il numero di persone che possono connettersi alla piattaforma BI contemporaneamente. Questo tipo di licenza è estremamente flessibile, poiché una licenza di accesso simultaneo di dimensioni ridotte può supportare un'ampia base di utenti. A seconda della frequenza e della durata dell'accesso al sistema, una licenza di accesso simultaneo per 100 utenti può ad esempio supportare 250, 500 o 700 utenti.

10. Per configurare come pianificare gli aggiornamenti degli Alias AD, fare clic su **Pianificazione**.

- a. Nella finestra di dialogo "Pianificazione" selezionare una ricorrenza nell'elenco **Esegui oggetto**.
- b. Impostare le opzioni e i parametri della pianificazione rimanenti nel modo richiesto.
- c. Fare clic su **Pianificazione**.

All'aggiornamento degli alias vengono aggiornate anche le informazioni sul gruppo.

11. Nell'area "Opzioni di collegamento attributi" è possibile specificare la priorità di collegamento degli attributi per il plug-in AD:

- a. Selezionare la casella di controllo **Importa nome completo, indirizzo di posta elettronica e altri attributi**.

I nomi completi e le descrizioni utilizzati negli account AD vengono importati e memorizzati insieme agli oggetti utente nella piattaforma BI.

- b. Specificare un'opzione per **Imposta priorità collegamento attributi AD relativo ad altri collegamenti attributi**.

Se l'opzione è impostata su 1, gli attributi AD hanno la priorità negli scenari in cui sono abilitati AD e altri plug-in (LDAP e SAP). Se l'opzione è impostata su 3, hanno la priorità gli attributi di altri plug-in abilitati.

12. Nell'area "Opzioni gruppo AD", configurare gli aggiornamenti del gruppo AD:

- a. Fare clic su **Pianifica**.
Viene visualizzata la finestra di dialogo "Pianificazione".
- b. Selezionare una ricorrenza dall'elenco a discesa **Esegui oggetto**.
- c. Impostare le opzioni e i parametri della pianificazione rimanenti nel modo richiesto.
- d. Fare clic su **Pianificazione**.

Il sistema pianifica l'aggiornamento e lo esegue in base alla pianificazione specificata.

L'aggiornamento pianificato successivo per gli account del gruppo AD viene visualizzato in "Opzioni gruppo AD".

13. Nell'area "Aggiornamento AD su richiesta" selezionare un'opzione per indicare se aggiornare gruppi o utenti AD (o nessuno dei due) quando si fa clic su **Aggiorna**:

- **Aggiorna gruppi AD ora**

Selezionare questa opzione se si desidera avviare l'aggiornamento di tutti i gruppi AD pianificati quando si fa clic su **Aggiorna**. Il prossimo aggiornamento pianificato del gruppo AD è indicato in "Opzioni gruppo AD".

- **Aggiorna alias e gruppi AD ora**

Selezionare questa opzione se si desidera avviare l'aggiornamento di tutti i gruppi e alias utente AD pianificati quando si fa clic su **Aggiorna**. I successivi aggiornamenti pianificati sono elencati in "Opzioni gruppo AD" e "Opzioni alias AD".

- **Non aggiornare alias e gruppi AD ora**

Nessun gruppo o alias utente AD verrà aggiornato quando si fa clic su **Aggiorna**.

14. Fare clic su **Aggiorna**, quindi su **OK**.

Disabilitazione di SiteMinder

Se si desidera impedire la configurazione di SiteMinder o disabilitarlo dopo la configurazione nella console CMC, modificare il file di configurazione Web per BI Launch Pad.

Disabilitazione di SiteMinder per i client Java

Oltre che per il plug-in di protezione Windows AD, è necessario disabilitare le impostazioni di SiteMinder anche per il file war BOE del server di applicazioni Web.

1. Accedere alla seguente directory nell'installazione della piattaforma BI:

```
<DIRINSTALL>\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\
```

2. Aprire il file `global.properties` file.

3. Impostare `siteminder.enabled` su `false`

```
siteminder.enabled=false
```

4. Salvare le modifiche e chiudere il file.

La modifica verrà applicata solo dopo la redistribuzione di `BOE.war` nel computer su cui è in esecuzione il server di applicazioni Web. Utilizzare WDeploy per redistribuire il file WAR sul server di applicazioni Web. Per ulteriori informazioni sull'utilizzo di WDeploy per annullare la distribuzione delle applicazioni Web, vedere il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects BI*.

9.4.7 Risoluzione dei problemi relativi all'autenticazione Windows AD

9.4.7.1 Risoluzione dei problemi relativi alla configurazione

Se si verificano problemi durante la configurazione di Kerberos, attenersi alle seguenti procedure:

- Abilitazione della registrazione
- Verifica della configurazione di Kerberos Java SDK

9.4.7.1.1 Per abilitare la registrazione

1. Nel menu **Start** selezionare **Programmi > Tomcat > Configurazione Tomcat**
2. Fare clic sulla scheda **Java**.
3. Aggiungere le seguenti opzioni:

```
-Dcrystal.enterprise.trace.configuration=verbose
-sun.security.krb5.debug=true
```

Viene creato un file registro nella seguente posizione:

```
C:\Documents and Settings\<user name>\.businessobjects\jce_verbose.log
```

9.4.7.1.2 Per verificare la configurazione di Kerberos

- Per verificare la configurazione di Kerberos, eseguire il comando indicato di seguito dove `servant` è l'account di servizio e il dominio in cui viene eseguito CMS e `password` è la password associata all'account di servizio.

```
<InstallDirectory>\SAP BusinessObjects Enterprise XI 4.0\win64_64\jdk\bin\servact@TESTM03.COM Password
```

Ad esempio:

```
C:\Program Files\SAP BusinessObjects\
SAP Business Objects Enterprise XI 4.0\win64_64\jdk\bin\
servact@TESTM03.COM Password
```

Il nome del dominio e il nome principale di servizio devono corrispondere esattamente al nome di dominio e al nome principale di servizio di Active Directory. Se il problema persiste, verificare se è stato immesso lo stesso nome. Tenere presente che il nome supporta la distinzione tra minuscole e maiuscole.

9.4.7.1.3 Errore di accesso dovuto a nomi AD UPN e SAM diversi

L'ID di Active Directory di un utente è stato mappato alla piattaforma BI. Ciò nonostante, l'utente non è in grado di accedere alla console CMC o a BI Launch Pad con l'autenticazione Windows AD e Kerberos nel formato che segue: DOMAIN\ABC123

Questo problema può essere riscontrato quando l'utente viene impostato in Active Directory con un nome UPN e SAM che in qualche modo non corrispondono. Gli esempi riportati di seguito possono causare un problema:

- L'UPN è abc123@azienda.com ma il nome SAM è DOMINIO\ABC123.
- L'UPN è gricci@azienda ma il nome SAM è DOMINIO\giorgioricci.

È possibile risolvere il problema in due modi:

- Fare accedere gli utenti utilizzando l'UPN anziché il nome SAM.
- Accertarsi che il nome di account SAM e il nome UPN corrispondano.

9.4.7.1.4 Errore di preautenticazione

È possibile che un utente precedentemente in grado di effettuare l'accesso non riesca più ad accedere correttamente. L'utente riceverà questo messaggio di errore: Informazioni sull'account non riconosciute. I registri degli errori Tomcat conterranno un errore analogo al seguente "Informazioni di preautenticazione non valide(24) "

Questo errore si può verificare poiché il database utente di Kerberos non ha ricevuto una modifica da UPN in AD. Ciò potrebbe indicare che il database utente di Kerberos e le informazioni AD non sono sincronizzati.

Per risolvere il problema, reimpostare la password dell'utente in AD. In questo modo le modifiche verranno trasmesse correttamente.

Nota:

Questo problema è stato risolto in J2SE 5.0.

9.5 Autenticazione SAP

9.5.1 Configurazione dell'autenticazione SAP

In questa sezione viene spiegato come configurare l'autenticazione della piattaforma BI per l'ambiente SAP.

L'autenticazione SAP consente agli utenti SAP di accedere alla piattaforma BI con il proprio nome utente e la propria password SAP, senza memorizzare le password nella piattaforma BI. Consente inoltre di preservare le informazioni sui ruoli dell'utente in SAP e utilizzare tali informazioni nella piattaforma per assegnare i diritti per l'esecuzione delle attività amministrative o l'accesso al contenuto.

Accesso all'applicazione di autenticazione SAP

È necessario fornire alla piattaforma BI le informazioni sul sistema SAP. È possibile accedere a un'applicazione Web dedicata tramite lo strumento amministrativo principale della piattaforma BI, ovvero la CMC (Central Management Console). Per accedervi dalla home page della console CMC, fare clic su **Autenticazione**.

Autenticazione degli utenti SAP

I plug-in di protezione espandono e personalizzano le modalità di autenticazione degli utenti della piattaforma BI. La funzionalità di autenticazione SAP include un plug-in di protezione SAP (*secSAPR3.dll*) per il componente Central Management Server (CMS) della piattaforma BI. Questo plug-in di protezione SAP offre diversi vantaggi chiave:

- Funge da provider di autenticazione che verifica le credenziali utente in base al sistema SAP per conto del CMS. Quando gli utenti accedono direttamente alla piattaforma BI, possono scegliere l'autenticazione SAP e immettere il proprio nome utente e la propria password SAP. La piattaforma BI può inoltre convalidare i ticket di accesso Enterprise Portal nei sistemi SAP.
- Consente di mappare i ruoli da SAP alla piattaforma BI per facilitare la creazione di account, nonché di assegnare i diritti agli utenti e ai gruppi in modo coerente all'interno della piattaforma BI.
- Mantiene dinamicamente gli elenchi di ruoli SAP. Ciò significa che, dopo che si è mappato un ruolo SAP nella piattaforma, tutti gli utenti che appartengono a tale ruolo possono accedere al sistema. Quando si apportano modifiche successive all'appartenenza ai ruoli SAP, non è necessario aggiornare l'elenco nella piattaforma BI.
- Il componente Autenticazione SAP include un'applicazione Web per la configurazione del plug-in. È possibile accedere a questa applicazione nell'area "Autenticazione" della CMC.

9.5.2 Creazione di un account utente per la piattaforma BI

Il sistema della piattaforma BI richiede un account utente SAP che sia autorizzato ad accedere agli elenchi di appartenenza ai ruoli SAP e ad autenticare gli utenti SAP. Sarà necessario utilizzare le credenziali dell'account per connettere la piattaforma BI al sistema SAP. Per le istruzioni generali per la creazione di account utente SAP e l'assegnazione delle autorizzazioni tramite i ruoli, consultare la documentazione di SAP BW.

Utilizzare la transazione `SU01` per creare un nuovo account utente SAP detto `CRYSTAL`. Utilizzare la transazione `PFCG` per creare un nuovo ruolo detto `CRYSTAL_ENTITLEMENT`. Questi nomi sono consigliati, ma non obbligatori. Cambiare l'autorizzazione del nuovo ruolo impostando i valori per i seguenti oggetti autorizzazione:

Oggetto autorizzazione	Campo	Valore
Autorizzazione per l'accesso ai file (S_DATASET)	Attività (ACTVT)	Lettura, scrittura (33, 34)
	Nome file fisico (FILENAME)	* (indica Tutti)
	Nome programma ABAP (PROGRAM)	*

Oggetto autorizzazione	Campo	Valore
Verifica autorizzazione per l'accesso RFC (S_RFC)	Attività (ACTVT)	16
	Nome dell'RFC da proteggere (RFC_NAME)	BDCH, STPA, SUSO, BDL5, SUUS, SU_USER, SYST, SUNI, RFC1, SDIFRUNTIME, PRGN_J2EE, /CRYSTAL/SECURITY
	Tipo di oggetto RFC da proteggere (RFC_TYPE)	Gruppo di funzioni (FUGR)
Manutenzione master utente: gruppi di utenti (S_USER_GRP)	Attività (ACTVT)	Crea o Genera, e Visualizza (03)
	Gruppo di utenti nella manutenzione master utente (CLASS)	<p>*</p> <p>Nota: Per maggiore sicurezza, si consiglia di elencare esplicitamente i gruppi di utenti i cui membri richiedono l'accesso alla piattaforma BI.</p>

Infine aggiungere l'utente `CRYSTAL` al ruolo `CRYSTAL_ENTITLEMENT`.

Suggerimento:

se in base ai criteri di sistema gli utenti devono modificare le password quando accedono per la prima volta al sistema, accedervi ora con l'account utente `CRYSTAL` e reimpostare la password.

9.5.3 Connessione ai sistemi di autorizzazione SAP

Per poter importare i ruoli o pubblicare contenuto BW nella piattaforma BI, è necessario fornire informazioni sul sistema di autenticazione SAP in cui si desidera effettuare l'integrazione. Tali informazioni vengono utilizzate dalla piattaforma BI per la connessione al sistema SAP di destinazione quando viene stabilita l'appartenenza ai ruoli e viene effettuata l'autenticazione degli utenti SAP.

9.5.3.1 Aggiunta di un sistema di autorizzazione SAP

1. Passare all'area di gestione "Autenticazione" della CMC.
2. Fare doppio clic sul collegamento **SAP**.

Vengono visualizzate le impostazioni dei sistemi di autorizzazione.

Suggerimento:

se un sistema di autorizzazione è già visualizzato nell'elenco **Nome sistema logico**, fare clic su **Nuovo**.

3. Nel campo **Sistema** immettere l'ID del sistema (SID) SAP a tre caratteri.
4. Nel campo **Client** digitare il numero client che la piattaforma BI deve utilizzare per accedere al sistema SAP.
La piattaforma BI combina le informazioni sul sistema e sul client e aggiunge una voce all'elenco **Nome sistema logico**.
5. Assicurarsi che la casella di controllo **Disattivato** sia deselezionata.

Nota:

selezionare la casella di controllo **Disattivato** per indicare alla piattaforma BI che un particolare sistema SAP non è temporaneamente disponibile.

6. Se il bilanciamento del carico è stato configurato in modo tale che la piattaforma BI deve eseguire l'accesso tramite un server messaggi, è necessario completare i campi **Server messaggi** e **Gruppo di accesso** in modo appropriato.

Nota:

è necessario immettere le voci appropriate nel file `Servizi` sul computer della piattaforma BI per consentire il bilanciamento del carico, soprattutto se la distribuzione non è stata eseguita in un unico computer. Prestare particolare attenzione ai computer in cui è in esecuzione il CMS, al server di applicazioni Web e ai computer che gestiscono gli account di autenticazione e le impostazioni.

7. Se il bilanciamento del carico non è stato configurato (o se si preferisce che la piattaforma BI acceda direttamente al sistema SAP), completare i campi **Server applicazioni** e **Numero sistema** in modo appropriato.
8. Nei campi **Nome utente**, **Password** e **Linguaggio** digitare il nome utente, la password e il codice linguaggio per l'account SAP che si desidera che la piattaforma BI utilizzi quando accede a SAP.

Nota:

queste credenziali devono corrispondere all'account utente creato per la piattaforma BI.

9. Fare clic su **Aggiorna**.

Se si aggiungono più sistemi di autorizzazione, fare clic sulla scheda **Opzioni** per specificare il sistema che la piattaforma BI utilizza per impostazione predefinita (ovvero il sistema che viene contattato per autenticare gli utenti che tentano di accedere con le credenziali SAP ma senza specificare un sistema SAP particolare).

Argomenti correlati

- [Creazione di un account utente per la piattaforma BI](#)

9.5.3.2 Per verificare l'aggiunta corretta di un sistema di autorizzazione

1. Fare clic sulla scheda **Importazione ruolo**.
2. Selezionare il sistema di autorizzazione dall'elenco **Nome sistema logico**.

Se il sistema di autorizzazione è stato aggiunto non correttamente, l'elenco **Ruoli disponibili** contiene un elenco dei ruoli che è possibile importare.

Suggerimento:

Se nell'elenco **Nome sistema logico** non sono visibili ruoli, controllare la presenza di messaggi di errore nella pagina. In questi messaggi potrebbero essere contenute le informazioni necessarie per correggere il problema.

9.5.3.3 Per disabilitare temporaneamente una connessione a un sistema di autorizzazione SAP

Nella CMC è possibile disabilitare temporaneamente una connessione tra la piattaforma BI e un sistema di autorizzazione SAP. Ciò può essere utile per mantenere la capacità di risposta della piattaforma BI, ad esempio nel caso del tempo di inattività pianificato di un sistema di autorizzazione SAP.

1. Nella CMC andare nell'area di gestione **Autenticazione**.
2. Fare doppio clic sul collegamento **SAP**.
3. Nell'elenco **Nome sistema logico** selezionare il sistema che si desidera disabilitare.
4. Selezionare la casella di controllo **Disattivato**.
5. Fare clic su **Aggiorna**.

9.5.4 Impostazione delle opzioni di autenticazione SAP

L'autenticazione SAP comprende numerose opzioni che è possibile specificare quando si integra la piattaforma BI con i sistemi SAP. Le opzioni disponibili sono:

- Abilitazione o disabilitazione dell'autenticazione SAP
- Specifica delle impostazioni di connessione

- Collegamenti di utenti importati a modelli di licenza della piattaforma BI.
- Configurazione di Single-Sign-On nel sistema SAP

9.5.4.1 Per impostare le opzioni di autenticazione SAP

1. Passare all'area di gestione "Autenticazione" della CMC.
2. Fare doppio clic sul collegamento **SAP** e fare clic sulla scheda **Opzioni**.
3. Rivedere e modificare le impostazioni seguenti in base alle esigenze:

Impostazione	Descrizione
Abilita autenticazione SAP	<p>Deselezionare questa casella di controllo se si desidera disabilitare l'autenticazione SAP.</p> <p>Nota: Per disabilitare l'autenticazione SAP per un sistema SAP specifico, selezionare la casella Disabilitato del sistema nella scheda Sistemi di autorizzazione.</p>
Contenuto cartella principale	<p>Specificare dove si desidera che la piattaforma BI dovrà iniziare a replicare la struttura delle cartelle BW nella CMC e in BI Launch Pad.</p> <p>L'impostazione predefinita è <code>/SAP/2.0</code> ma è possibile scegliere una cartella diversa, se necessario. Se si desidera modificare il valore, è necessario apportare la modifica sia nella CMC che nel workbench per l'amministrazione dei contenuti.</p>
Sistema predefinito	<p>Selezionare un sistema di autorizzazione SAP che la piattaforma BI deve contattare per autenticare gli utenti che provano ad accedere con le credenziali SAP ma senza specificare un sistema SAP specifico.</p> <p>Nota: Se si seleziona un sistema predefinito, gli utenti di tale sistema non devono immettere il client o l'ID sistema quando si connettono tramite strumenti client quali Live Office o Universe Designer utilizzando l'autenticazione SAP. Ad esempio, se SYS~100 è impostato come sistema predefinito, SYS~100/user1 potrebbe accedere come user1 quando viene scelta l'autenticazione SAP.</p>
Numero massimo di tentativi di accesso non riusciti al sistema di autorizzazione	

Impostazione	Descrizione
	<p>Digitare il numero di tentativi che la piattaforma BI deve effettuare per tentare di contattare un sistema SAP per soddisfare le richieste di autenticazione.</p> <p>Se si imposta il valore su -1, la piattaforma BI tenta di contattare il sistema di autorizzazione un numero illimitato di volte. Se si imposta il valore su 0, la piattaforma BI può provare a contattare il sistema di autorizzazione una sola volta.</p> <p>Nota: Utilizzare questa impostazione insieme all'opzione Mantieni disabilitato sistema di autorizzazione [secondi] per configurare il modo in cui la piattaforma BI deve gestire i sistemi di autorizzazione SAP che sono temporaneamente non disponibili. Il sistema utilizza le due opzioni per stabilire quando interrompere la comunicazione con un sistema SAP che non è disponibile e quando riprendere la comunicazione con tale sistema.</p>
Mantieni disabilitato sistema di autorizzazione [secondi]	<p>Digitare il numero di secondi che la piattaforma BI deve attendere prima di riprovare ad autenticare gli utenti nel sistema SAP.</p> <p>Se ad esempio si specifica 3 per Numero max. accessi al sistema di autorizzazione non riusciti, la piattaforma BI consente un massimo di tre tentativi mancati per autenticare gli utenti in qualsiasi sistema SAP. Al quarto tentativo non riuscito, l'autenticazione degli utenti da parte del sistema viene interrotta per il periodo di tempo specificato.</p>
Numero max. connessioni simultanee per sistema	<p>Specificare quante connessioni al sistema SAP devono restare aperte contemporaneamente.</p> <p>Se ad esempio si digita 2, la piattaforma BI mantiene aperte due connessioni al sistema SAP.</p>
Numero di utilizzi per connessione	<p>Specificare quante operazioni consentire per ogni connessione al sistema SAP.</p> <p>Se ad esempio Numero max. connessioni simultanee per sistema è impostato su 2 e Numero di utilizzi per connessione è impostato su 3, se in una sola connessione vengono effettuati tre accessi, la piattaforma BI si chiude e riavvia la connessione.</p>

Impostazione	Descrizione
Utenti simultanei e Utenti designati	<p>Specificare se i nuovi account utente utilizzeranno licenze utente simultaneo o designato.</p> <p>Le licenze di accesso simultaneo specificano il numero di persone che possono connettersi alla piattaforma BI contemporaneamente. Questo tipo di licenza è estremamente flessibile, poiché poche licenze di accesso simultaneo possono supportare un'ampia base di utenti. A seconda della frequenza e della durata dell'accesso al sistema, una licenza di accesso simultaneo per 100 utenti può ad esempio supportare 250, 500 o 700 utenti.</p> <p>Le licenze utente designato sono associate a utenti specifici e consentono di accedere al sistema in base a nome utente e password. Ciò garantisce agli utenti specifici l'accesso al sistema a prescindere dal numero delle altre persone connesse.</p> <p>Nota: L'opzione selezionata non modifica il numero o il tipo di licenze utente installate nella piattaforma BI. È necessario che sul sistema siano disponibili le licenze appropriate.</p>
Importa nome completo, indirizzo di posta elettronica e altri attributi	<p>Specificare un livello di priorità per il plug-in di autenticazione SAP.</p> <p>I nomi completi e le descrizioni utilizzati negli account SAP vengono importati e archiviati con gli oggetti utente nella piattaforma BI.</p>
Imposta priorità collegamento attributi SAP relativo ad altri collegamenti attributi	<p>Specifica una priorità per il collegamento degli attributi utente SAP (nome completo e indirizzo di posta elettronica).</p> <p>Se l'opzione è impostata su 1, gli attributi SAP hanno la priorità in situazioni in cui sono abilitati SAP e altri plug-in (Windows AD e LDAP). Se l'opzione è impostata su 3, hanno la priorità gli attributi di altri plug-in abilitati.</p>

Impostare le opzioni seguenti per configurare il servizio Single Sign On SAP:

Impostazione	Descrizione
ID sistema	Identificatore di sistema fornito dalla piattaforma BI al sistema SAP quando si esegue il servizio Single Sign On SAP.
Sfoglia	Fare clic per caricare il file dell' <code>archivio chiavi</code> generato per abilitare il Single Sign On SAP. È possibile immettere il percorso completo del file anche manualmente.
Password archi- vio chiavi	Specificare la password richiesta per l'accesso al file dell' <code>archivio chiavi</code> .
Password chiave privata	Specificare la password richiesta per l'accesso al certificato corrispondente al file dell' <code>archivio chiavi</code> . Il certificato è archiviato nel sistema SAP
Alias chiave pri- vata	Specificare l'alias richiesto per l'accesso al file dell' <code>archivio chiavi</code> .

4. Fare clic su **Aggiorna**.

Argomenti correlati

- [Configurazione dell'autenticazione SAP](#)

9.5.4.2 Modifica della cartella contenuti principale

1. Passare all'area di gestione "Autenticazione" della CMC.
2. Fare doppio clic sul collegamento **SAP**.
3. Fare clic su **Opzioni** e digitare il nome della cartella nel campo **Contenuto cartella principale**.
Il nome della cartella immesso corrisponde alla cartella da cui si desidera che la piattaforma BI inizi a replicare la struttura delle cartelle BW.
4. Fare clic su **Aggiorna**.
5. Nel workbench per l'amministrazione dei contenuti di BW, espandere **Sistema Enterprise**.
6. Espandere **Sistemi disponibili** e fare doppio clic sul sistema a cui la piattaforma BI si sta connettendo.
7. Fare clic sulla scheda **Layout** nella **cartella di base del contenuto** e digitare la cartella che si desidera utilizzare come cartella SAP principale nella piattaforma BI, ad esempio `/SAP/2.0/`.

9.5.5 Importazione dei ruoli SAP

Se si importano ruoli SAP nella piattaforma BI, si consente ai membri dei ruoli di accedere al sistema con le consuete credenziali SAP. È inoltre abilitata l'opzione Single Sign On per consentire agli utenti SAP di accedere automaticamente alla piattaforma BI quando accedono ai report dalla GUI SAP o da SAP Enterprise Portal.

Nota:

spesso è necessario soddisfare molti requisiti per abilitare SSO. Tra questi possono figurare l'utilizzo di un driver e di un'applicazione compatibili con SSO e la garanzia che il server e il server Web siano nello stesso dominio.

Per ciascun ruolo importato, la piattaforma BI genera un gruppo. A ciascun gruppo viene assegnato un nome in base alla seguente convenzione: *IDSistema~NumeroCliente@NomeRuolo*. È possibile visualizzare i nuovi gruppi nell'area di gestione "Utenti e gruppi" della CMC. È inoltre possibile utilizzare questi gruppi per definire la protezione degli oggetti nella piattaforma BI.

Si considerino tre categorie principali di utenti quando si configura la piattaforma BI per la pubblicazione e quando si importano i ruoli nel sistema:

- Amministratori della piattaforma BI

Gli amministratori Enterprise configurano il sistema per la pubblicazione di contenuto proveniente da SAP. Importano i ruoli appropriati, creano le cartelle necessarie e assegnano i diritti ai ruoli e alle cartelle nella piattaforma BI.

- Publisher dei contenuti

I publisher dei contenuti sono gli utenti che dispongono dei diritti per pubblicare i contenuti nei ruoli. Lo scopo di questa categoria di utenti è quello di separare i membri dei ruoli regolari da queglii utenti che dispongono dei diritti per pubblicare i report.

- Membri dei ruoli

I membri dei ruoli sono gli utenti che appartengono ai ruoli che "generano contenuti". In altre parole questi utenti appartengono ai ruoli in cui vengono pubblicati i report. Dispongono dei diritti di **visualizzazione, visualizzazione su richiesta e pianificazione** per tutti i report pubblicati nei ruoli di cui sono membri. Tuttavia, i membri dei ruoli regolari non possono pubblicare nuovi contenuti, né possono pubblicare versioni aggiornate dei contenuti.

È necessario importare tutti i ruoli di pubblicazione e di generazione dei contenuti nella piattaforma BI prima di pubblicare i contenuti per la prima volta.

Nota:

si consiglia vivamente di distinguere le attività dei ruoli. Ad esempio, sebbene sia possibile pubblicare da un ruolo amministrativo, è meglio provare a pubblicare solo dai ruoli di publisher dei contenuti. Inoltre la funzione dei ruoli di pubblicazione dei contenuti è solo quella di definire quali utenti possono pubblicare i contenuti. Ciò significa che i ruoli di pubblicazione dei contenuti non devono contenere alcun contenuto; i publisher dei contenuti devono eseguire la pubblicazione nei ruoli di generazione dei contenuti accessibili ai membri dei ruoli regolari.

Argomenti correlati

- [Funzionamento dei diritti nella piattaforma BI](#)
- [Gestione delle impostazioni di protezione per gli oggetti nella CMC](#)

9.5.5.1 Importazione dei ruoli SAP

1. Passare all'area di gestione "Autenticazione" della CMC.
2. Fare doppio clic sul collegamento **SAP**.
3. Nella scheda **Opzioni** selezionare **Utenti simultanei** o **Utenti designati**, a seconda del contratto di licenza di cui si dispone.
L'opzione selezionata qui non modifica il numero o il tipo di licenze utente installate nella piattaforma BI. È necessario che sul sistema siano disponibili le licenze appropriate.
4. Fare clic su **Aggiorna**.
5. Nella scheda **Importazione ruolo**, selezionare il sistema di autorizzazione appropriato dall'elenco **Nome sistema logico**.
6. Nell'area "Ruoli disponibili" selezionare i ruoli che si desidera importare, quindi fare clic su **Aggiungi**.
7. Fare clic su **Aggiorna**.

9.5.5.2 Verifica della corretta importazione di ruoli e utenti

Prima di iniziare questa attività, prendere nota di nome utente e password di un utente SAP che appartiene a uno dei ruoli mappati alla piattaforma BI.

1. Per Java BI Launch Pad, accedere a `http://serverweb:numeroporta/BOE/BI`.

Sostituire *serverweb* con il nome del server Web e *numeroporta* con il numero di porta impostato per la piattaforma BI. Può essere necessario richiedere all'amministratore il nome del server Web, il numero di porta o l'URL esatto per accedere.

2. Nell'elenco **Tipo autenticazione** selezionare **SAP**.

Nota:

Per impostazione predefinita, l'elenco **Tipo di autenticazione** è nascosto in BI Launch Pad. Se l'elenco non è visibile, chiedere all'amministratore di sistema di abilitare l'elenco **Tipo di autenticazione** nel file `BIlaunchpad.properties` e riavviare il server di applicazioni.

3. Immettere il sistema SAP e il client di sistema a cui si desidera accedere.
4. Immettere il nome utente e la password di un utente mappato.
5. Fare clic su **Accedi**.

L'utente è connesso a BI Launch Pad come utente selezionato.

9.5.5.3 Aggiornamento degli utenti e dei ruoli SAP

Dopo aver abilitato l'autenticazione SAP è necessario pianificare ed eseguire aggiornamenti regolari sui ruoli mappati importati nella piattaforma BI. In questo modo le informazioni sui ruoli SAP verranno riportate esattamente nella piattaforma BI.

Sono disponibili due opzioni per l'esecuzione e la pianificazione degli aggiornamenti per i ruoli SAP:

- **Aggiorna solo ruoli:** l'uso di questa opzione determina l'aggiornamento dei soli collegamenti tra i ruoli attualmente mappati importati nella piattaforma BI. Si consiglia di utilizzare questa opzione se si prevede di eseguire aggiornamenti frequenti e si verificano problemi relativi all'utilizzo delle risorse di sistema. Se si aggiornano solo i ruoli SAP, non vengono creati nuovi account utente.
- **Aggiorna ruoli e alias:** questa opzione determina non solo l'aggiornamento dei collegamenti tra i ruoli, ma anche la creazione di nuovi account utente nella piattaforma BI per gli alias utente aggiunti ai ruoli nel sistema SAP.

Nota:

se non è stata specificata la creazione automatica degli alias utente per gli aggiornamenti quando è stata abilitata l'autenticazione SAP, non verranno creati account per i nuovi alias.

9.5.5.3.1 Pianificazione degli aggiornamenti per i ruoli SAP

Una volta mappati i ruoli nella piattaforma BI, è necessario specificare in che modo vengono aggiornati dal sistema.

1. Fare clic sulla scheda **Aggiornamento utente**.
2. Fare clic su **Pianifica** nella sezione "Aggiorna solo ruoli" o nell'area "Aggiorna ruoli e alias".

Suggerimento:

per eseguire immediatamente un aggiornamento, fare clic su **Aggiorna ora**.

Suggerimento:

Utilizzare l'opzione **Aggiorna solo ruoli** se si desidera eseguire aggiornamenti frequenti e si verificano problemi con le risorse di sistema. Il sistema impiega più tempo per aggiornare sia i ruoli che gli alias.

Viene visualizzata la finestra di dialogo "Ricorrenza".

3. Selezionare un'opzione nell'elenco **Esegui oggetto** e immettere nei campi forniti tutte le informazioni richieste relative alla pianificazione.

Quando si pianifica un aggiornamento, è possibile scegliere tra gli schemi ricorrenti nella seguente tabella.

Criterio di ricorrenza	Descrizione
Ogni ora	L'aggiornamento verrà eseguito ogni ora. È possibile specificare l'ora in cui verrà avviato e le date di inizio e di fine.

Criterio di ricorrenza	Descrizione
Ogni giorno	L'aggiornamento verrà eseguito ogni giorno o ogni n giorni (in cui n è il numero di giorni specificato). È possibile specificare l'ora in cui verrà avviato e le date di inizio e di fine.
Ogni settimana	L'aggiornamento verrà eseguito una volta alla settimana o più volte alla settimana. È possibile specificare i giorni in cui verrà eseguito, l'ora in cui viene avviato e le date di inizio e di fine.
Ogni mese	L'aggiornamento verrà eseguito ogni mese oppure dopo il numero di mesi specificato. È possibile specificare l'ora in cui verrà avviato e le date di inizio e di fine.
N-mo giorno del mese	L'aggiornamento verrà eseguito in un giorno specifico del mese. È possibile specificare in quale giorno del mese e a che ora verrà eseguito nonché una data di inizio e di fine.
Primo lunedì del mese	L'aggiornamento verrà eseguito il primo lunedì di ogni mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Ultimo giorno del mese	L'aggiornamento verrà eseguito l'ultimo giorno di ogni mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Giorno X della N-ma settimana del mese	L'aggiornamento verrà eseguito in un giorno specifico di una settimana specifica del mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Calendario	L'aggiornamento verrà eseguito nelle date specificate all'interno di un calendario creato in precedenza.

4. Fare clic su **Pianifica**.

Nella scheda **Aggiornamento utente** viene visualizzata la data del prossimo aggiornamento di ruolo pianificato.

Suggerimento:

Per annullare il successivo aggiornamento pianificato, fare clic su **Annulla aggiornamenti pianificati** nell'area "Aggiorna solo ruoli" o "Aggiorna ruoli e alias".

9.5.6 Configurazione di Secure Network Communication (SNC)

Questa sezione descrive la procedura di configurazione di SNC come parte del processo di impostazione dell'autenticazione SAP per la piattaforma BI

Prima di impostare l'attendibilità tra il sistema SAP e la piattaforma BI, è necessario assicurarsi che l'agente SIA sia configurato in modo da essere avviato ed eseguito per un account impostato per SNC. È inoltre necessario configurare il sistema SAP in modo che consideri attendibile la piattaforma BI.

Argomenti correlati

- [Panoramica dell'attendibilità lato server SAP](#)

9.5.6.1 Panoramica dell'attendibilità lato server SAP

Questa sezione include le procedure per la configurazione dell'attendibilità lato server tra server di applicazioni Web SAP (versione 6.20 e superiori) e la piattaforma SAP BusinessObjects Business Intelligence. È necessario impostare l'attendibilità lato server se si utilizza il bursting di report multi-pass (per le pubblicazioni nelle quali la query di report dipende dal contesto dell'utente).

L'attendibilità lato server include la rappresentazione senza password. Per rappresentare un utente SAP senza specificare una password, l'utente deve essere identificato con SAP mediante un metodo più sicuro rispetto alle normali credenziali nome utente e password. (Un utente SAP con il profilo di autorizzazione `SAP_ALL` non può rappresentare un altro utente SAP senza conoscere la relativa password).

Abilitazione dell'attendibilità lato server utilizzando la libreria di crittografia SAP

Per abilitare l'attendibilità lato server per la piattaforma BI utilizzando la libreria di crittografia SAP, è necessario eseguire i relativi server con le credenziali autenticate mediante un provider SNC (Secure Network Communication) registrato. Queste credenziali vengono configurate in SAP in modo che sia possibile eseguire la rappresentazione senza utilizzare una password. Per la piattaforma BI, è necessario eseguire i server coinvolti nel report bursting utilizzando le credenziali SNC, ad esempio l'Adaptive Job Server.

Sono necessari file binari SNC a 32 e 64 bit rispettivamente per i processi a 32 e 64 bit. Viene installata una libreria di crittografia SAP insieme alla piattaforma BI. Tenere presente che la libreria di crittografia SAP può essere utilizzata solo per impostare l'attendibilità lato server. La libreria di crittografia è disponibile per Windows e UNIX.

Per ulteriori informazioni sulla libreria di crittografia, consultare le note SAP 711093, 597059 e 397175 sul sito Web SAP.

Al server SAP e alla piattaforma BI devono essere assegnati certificati che dimostrino l'identità reciproca. Ogni server avrà il proprio certificato e un elenco di certificati per i partner attendibili. Per configurare l'attendibilità lato server tra SAP e la piattaforma BI, è necessario creare un set di certificati protetti da password denominato PSE (Personal Security Environment). In questa sezione viene descritto come impostare e gestire gli ambienti PSE e come associarli in modo sicuro ai server di elaborazione della piattaforma BI.

SNC client e SNC server

In SNC client, un identificatore di nome SNC viene mappato a uno (o più) nomi utente SAP in SU01. Quando viene inviata una richiesta di accesso, il nome SNC e il nome SAP vengono trasmessi al sistema SAP, ma senza password. Se il nome SNC è mappato al nome SAP, l'accesso viene consentito. Di seguito è riportata una stringa di accesso lato client per l'accesso a un host applicazione:

```
ASHOST =myserver.mydomain SYSNR=37 CLIENT=066 LANG=EN USER=USER123
SNC_MODE=1 SNC_QOP=9 SNC_LIB="/usr/local/lib/libsapcrypto.so"
SNC_PARTNERNAME="p:CN=TheServer, OU=Dept., O=TheCompany, C=FR"
SNC_MYNAME="p:CN=TheUser, O=TheCompany, C=US"
```

L'utente SAP USER123 deve essere mappato a p:CN=TheUser, O=TheCompany, C=US in SU01 affinché l'accesso venga consentito. In SNC server, non è necessario eseguire una mappatura esplicita tra l'identificatore del nome SNC e il nome utente SAP. Il nome SNC viene invece configurato nella transazione SNC0 in modo da consentire di eseguire un accesso di rappresentazione per "qualsiasi" utente senza dover specificare la password utente. Ad esempio:

```
ASHOST =myserver.mydomain SYSNR=37 CLIENT=066 LANG=EN SNC_MODE=1
SNC_QOP=9 SNC_LIB="/usr/local/lib/libsapcrypto.so"
SNC_PARTNERNAME="p:CN=TheServer, OU=Dept., O=TheCompany, C=FR"
SNC_MYNAME="p:CN=TheUser, O=TheCompany, C=US" EXTIDTYPE=UN EXTIDDATA=USER123
```

L'accesso di rappresentazione o tramite un ID esterno in SNC server è più flessibile della procedura di accesso in SNC client in quanto consente l'accesso a qualsiasi account utente SAP nel sistema. Altre opzioni di accesso con ID esterno includono ticket di accesso e certificati client X.509.

Responsabilità dei server della piattaforma SAP BusinessObjects BI

Il ruolo di specifici server della piattaforma BI è inerente all'integrazione SAP in termini di Single Sign On (SSO). Tali server sono elencati nella tabella seguente insieme al tipo di SNC di cui necessitano per particolari aree di responsabilità.

Server	Tipo SNC	Area di responsabilità
Server di applicazioni Web	client	Elenco di ruoli di autenticazione SAP
Servizio Publisher BW	server	Elenchi di scelta di parametri Crystal Reports e personalizzazione
CMS	client	Elenchi di password, ticket, appartenenza ai ruoli e utenti
Page Server	server	Visualizzazione di Crystal Reports su richiesta
Job Server	server	Pianificazione di Crystal Reports
Server di elaborazione Web Intelligence	server	Visualizzazione e pianificazione di report Web Intelligence e prompt con elenchi di valori
Servizio di analisi multidimensionale	server	Analisi

Nota:

il server di applicazioni Web e CMS utilizzano SNC client e quindi richiedono una mappatura esplicita del nome SNC al nome utente SAP. Ciò è specificato nella transazione SU01 o SM30 per la tabella USRACL.

9.5.6.2 Configurazione SAP per l'attendibilità lato server

L'attendibilità lato server si applica solo ai report Crystal e Web Intelligence basati su Universi (.unv). È necessario impostare SNC per l'utilizzo con la piattaforma BI. Per ulteriori informazioni o per assistenza sulla risoluzione dei problemi, consultare la documentazione SAP fornita con il server SAP.

9.5.6.2.1 Per configurare l'attendibilità lato server SAP

1. Verificare di disporre delle credenziali di amministratore SAP per SAP e per il computer su cui è in esecuzione SAP e delle credenziali di amministratore per la piattaforma BI e per il computer su cui è in esecuzione.
2. Sul computer SAP verificare che la libreria di crittografia SAP e lo strumento SAPGENPSE si trovino nella directory UNITÀ: \usr\sap\SID\SYS\exe\run\ (in Windows).
3. Creare una variabile di ambiente denominata *SECUDIR* che punti alla directory in cui si trova il ticket.

Nota:

Questa variabile deve essere accessibile all'utente che esegue il processo SAP **disp+work**.

4. Nella GUI SAP, passare alla transazione RZ10 modificare il profilo di istanza nella modalità di **gestione estesa**.
5. Nella modalità di modifica del profilo, puntare le variabili di profilo SAP alla libreria di crittografia e assegnare al sistema SAP un nome distinto. Queste variabili dovrebbero seguire la convenzione di denominazione LDAP:

Tag	Significato	Descrizione
CN	Nome comune	Il nome del proprietario del certificato.
OU	Unità societaria	Ad esempio, PG per Product Group.
O	Organizzazione	Il nome dell'organizzazione per la quale è stato emesso il certificato.
C	Paese	Il paese in cui si trova l'organizzazione.

Ad esempio, per R21: p:CN=R21, OU=PG, O=BOBJ, C=CA

Nota:

Il prefisso p: si riferisce alla libreria di crittografia SAP. È necessario quando si fa riferimento al nome distinto in SAP, ma non sarà visibile durante l'esame dei certificati in STRUST oppure utilizzando lo strumento SAPGENPSE.

6. Immettere i valori di profilo seguenti, effettuando, dove necessario, le sostituzioni in base al sistema SAP in uso:

Variabile di profilo	Valore
ssf/name	SAPSECULIB
ssf/ssfapi_lib	Percorso completo alla libreria sapcrypto
sec/libsapsecu	Percorso completo alla libreria sapcrypto
snc/gssapi_lib	Percorso completo alla libreria sapcrypto
snc/identity/as	Il nome distinto del sistema SAP in uso

7. Riavviare l'istanza SAP.
8. Quando il sistema è nuovamente in esecuzione, eseguire l'accesso e passare allo strumento STRUST, che ora dovrebbe avere voci aggiuntive per SNC e SSL.
9. Fare clic con il pulsante destro del mouse sul nodo SNC, quindi fare clic su **Crea**.
L'identità specificata nella transazione RZ10 dovrebbe ora essere visualizzata.
10. Fare clic su **OK**.
11. Per assegnare una password al PSE SNC, fare clic sull'icona di blocco.

Nota:

non perdere la password. Verrà infatti richiesta da STRUST ogni volta che si visualizza o si modifica il PSE SNC.

12. Salvare le modifiche.

Nota:

se le modifiche non vengono salvate, il server di applicazioni non verrà avviato nuovamente quando si abilita l'SNC.

13. Tornare alla transazione RZ10 e aggiungere il resto dei parametri di profilo SNC:

Variabile di profilo	Parametro
snc/accept_insecure_rfc	1
snc/accept_insecure_r3int_rfc	1
snc/accept_insecure_gui	1
snc/accept_insecure_cplic	1
snc/permit_insecure_start	1
snc/data_protection/min	1
snc/data_protection/max	3
snc/enable	1

Il livello di protezione minimo è sola autenticazione (1) e il livello massimo è privacy (3). Il valore snc/data_protection/use indica che in questo caso deve essere utilizzata solo l'autenticazione, ma può anche essere (2) per l'integrità, (3) per la privacy e (9) per il massimo disponibile. I valori

snc/accept_insecure_rfc, snc/accept_insecure_r3int_rfc, snc/accept_insecure_gui e snc/accept_insecure_cplic impostati su (1) garantiscono che i precedenti metodi per le comunicazioni (potenzialmente non sicuri) sono ancora consentiti.

14. Riavviare il sistema SAP.

È ora necessario configurare la piattaforma BI per l'attendibilità lato server.

9.5.6.3 Configurazione della piattaforma BI per l'attendibilità lato server

Attenersi alle procedure seguenti per configurare la piattaforma BI per l'attendibilità lato server. Tenere presente che queste procedure si basano su Windows ma poiché lo strumento SAP si basa sulla riga comandi, i passaggi sono molto simili in UNIX.

1. Impostazione dell'ambiente
2. Generazione di un ambiente PSE (Personal Security Environment)
3. Configurazione dei server della piattaforma BI
4. Configurazione dell'accesso PSE
5. Configurazione delle impostazioni SNC per l'autenticazione SAP
6. Impostazione dei gruppi di server dedicati per SAP

Argomenti correlati

- [Per impostare l'ambiente](#)
- [Per generare un PSE](#)
- [Configurazione dei server della piattaforma BI](#)
- [Per configurare l'accesso al PSE](#)
- [Per configurare le impostazioni SNC di autenticazione SAP](#)
- [Utilizzo di gruppi server](#)

9.5.6.3.1 Per impostare l'ambiente

La piattaforma BI include una libreria di crittografia SAP predefinita. Se si utilizza la libreria predefinita, è necessario eseguire solo gli ultimi due passaggi: creare una sottocartella e aggiungere una variabile di ambiente. In caso contrario, per configurare una copia personalizzata della libreria di crittografia SAP, eseguire tutti i passaggi descritti di seguito.

La libreria di crittografia SAP è disponibile nel percorso seguente:

- Windows: `DIRINSTALL\sap\sapcrypto.dll`
- Unix: `DIRINSTALL/sap/libsapcrypto.so`

Prima di iniziare, verificare che:

- La libreria di crittografia SAP sia stata distribuita sull'host su cui vengono eseguiti i server di elaborazione della piattaforma BI.

- I sistemi SAP appropriati siano stati configurati per l'utilizzo della libreria di crittografia SAP come provider SNC.

Prima dell'inizio della gestione PSE, è necessario impostare la libreria, lo strumento e l'ambiente in cui sono memorizzati i PSE.

1. Copiare la libreria di crittografia SAP (incluso lo strumento di gestione PSE) in una cartella del computer su cui è in esecuzione la piattaforma BI.

Ad esempio: `C:\Programmi\SAP\Crypto`

2. Aggiungere la cartella alla variabile di ambiente `PATH`.
3. Aggiungere una variabile di ambiente di sistema `SNC_LIB` che punti alla libreria di crittografia.

Ad esempio: `C:\Programmi\SAP\Crypto\sapcrypto.dll`

Nota:

La lunghezza massima del percorso è di 100 caratteri.

4. Creare una sottocartella denominata `sec`.
Ad esempio: `C:\Programmi\SAP\Crypto\sec`
5. Aggiungere una variabile di ambiente di sistema `SECUDIR` che punti alla cartella `sec`.

Argomenti correlati

- [Configurazione SAP per l'attendibilità lato server](#)

9.5.6.3.2 Per generare un PSE

SAP accetta un server della piattaforma BI come entità attendibile quando i server della piattaforma BI pertinenti dispongono di un PSE associato a SAP. Questa "attendibilità" tra i componenti SAP e la piattaforma BI viene stabilita mediante la condivisione della versione pubblica dei certificati. Il primo passo consiste nel creare un PSE per la piattaforma BI che generi automaticamente il proprio certificato.

1. Aprire un prompt dei comandi ed eseguire `sapgenpse.exe gen_pse -v -p BOE.pse` nella cartella della libreria di crittografia.
2. Scegliere un PIN e un nome distinto per il sistema della piattaforma BI.
Ad esempio, `CN=MyBOE01, OU=PG, O=BOBJ, C=CA`.
È ora disponibile un PSE predefinito, con il relativo certificato.
3. Utilizzare il comando seguente per esportare il certificato nell'ambiente PSE:
`sapgenpse.exe export_own_cert -v -p BOE.pse -o CertBOE.crt`
4. Nella GUI SAP passare alla transazione `STRUST` e aprire il PSE di sistema associato al proprio sistema SAP.
Potrebbe essere richiesta la password già assegnata al PSE del sistema.
5. Importare il file `MyBOECert.crt` creato in precedenza facendo clic sul pulsante "Importare certificato" in basso a sinistra della schermata della transazione `STRUST`.

I certificati `SAPGENPSE` hanno la codifica Base64. Assicurarsi di selezionare Base64 durante l'importazione.

6. Per aggiungere il certificato della piattaforma BI all'elenco dei certificati PSE del server SAP, fare clic sul pulsante **Aggiungi certificati all'elenco**.
7. Salvare le modifiche in STRUST.
8. Fare clic sul pulsante **Esporta** e specificare un nome file per il certificato.
Ad esempio, CertSAP.crt.

Nota:

Il formato dovrebbe rimanere di tipo Base64.

9. Passare alla transazione SNC0.
10. Aggiungere una nuova voce, dove:
 - L'ID di sistema è arbitrario ma riflette il sistema della piattaforma BI in uso.
 - Il nome SNC dovrebbe essere il nome distinto (con prefisso p:) specificato al momento della creazione del PSE della piattaforma BI (nel passaggio 2).
 - Le caselle di controllo **Voce per RFC attivata** e **Voce per ID est. attivata** sono selezionate entrambe:
11. Per aggiungere il certificato esportato nel PSE della piattaforma BI, eseguire il comando seguente al prompt dei comandi:

```
sapgenpse.exe maintain_pk -v -a MySAPCert.crt -p BOE.pse
```

La libreria di crittografia SAP viene installata sul computer della piattaforma BI. È stato creato un ambiente PSE che verrà utilizzato dai server della piattaforma BI per l'identificazione sui server SAP. SAP e il PSE della piattaforma BI si scambiano i certificati. SAP consente alle entità con accesso al PSE della piattaforma BI di eseguire chiamate RFC e rappresentazioni senza password.

Argomenti correlati

- [Configurazione dei server della piattaforma BI](#)

9.5.6.3.3 Configurazione dei server della piattaforma BI

Dopo aver generato un PSE per la piattaforma BI, è necessario configurare una struttura server appropriata per l'elaborazione SAP. La procedura seguente crea un nodo per i server di elaborazione SAP, in modo che sia possibile impostare le credenziali del sistema operativo a livello di nodo.

Nota:

In questa versione della piattaforma BI i server non vengono più configurati in CCM (Central Configuration Manager). Invece, è necessario creare un nuovo SIA (Server Intelligence Agent).

1. In CCM, creare un nuovo nodo per i server di elaborazione SAP.
Assegnare al nodo un nome appropriato, ad esempio SAPProcessor.
2. In CMC, aggiungere i server di elaborazione necessari nel nuovo nodo, quindi avviare i nuovi server.

9.5.6.3.4 Per configurare l'accesso al PSE

Dopo aver configurato i server e il nodo della piattaforma BI, è necessario configurare l'accesso PSE utilizzando lo strumento SAPGENPSE.

1. Eseguire il comando seguente dal prompt dei comandi:

```
sapgenpse.exe seclogin -p SBOE.pse
```

Nota:

Verrà richiesta l'immissione del PIN PSE. Se lo strumento viene eseguito con le stesse credenziali utilizzate dai server di elaborazione SAP della piattaforma BI, non è necessario specificare un nome utente.

2. Per verificare che sia stato stabilito il collegamento SSO, elencare i contenuti del PSE utilizzando il comando seguente:

```
sapgenpse.exe maintain_pk -l
```

I risultati dovrebbero essere simili ai seguenti:

```
C:\Documents and Settings\username\Desktop\sapcrypto.x86\ntintel>sapgenpse.exe
maintain_pk -l
maintain_pk for PSE "C:\Documents and Settings\username\My Documents\snc\sec\bobjsapproc.pse"
*** Object <PKList> is of the type <PKList_OID> ***

1. -----
Version:                0 (X.509v1-1988)
SubjectName:            CN=R21Again, OU=PG, O=BOBJ, C=CA
IssuerName:             CN=R21Again, OU=PG, O=BOBJ, C=CA
SerialNumber:           00
Validity - NotBefore:   Wed Nov 28 16:23:53 2007 (071129002353Z)
                   NotAfter: Thu Dec 31 16:00:01 2037 (380101000001Z)
Public Key Fingerprint: 851C 225D 1789 8974 21DB 9E9B 2AE8 9E9E
SubjectKey:             Algorithm RSA (OID 1.2.840.113549.1.1.1), NULL

C:\Documents and Settings\username\Desktop\sapcrypto.x86\ntintel>
```

Dopo l'esecuzione regolare del comando seclogin non viene richiesta nuovamente l'immissione del PIN PSE.

Nota:

In caso di problemi di accesso al PSE, utilizzare l'argomento -O per specificare tale accesso. Ad esempio, per consentire l'accesso al PSE a un utente specifico in un determinato dominio, digitare il seguente comando in Windows:

```
sapgenpse seclogin -p SBOE.pse -O SYSTEM
```

9.5.6.3.5 Per configurare le impostazioni SNC di autenticazione SAP

Dopo aver configurato l'accesso PSE, è necessario configurare le impostazioni di autenticazione SAP nella CMC.

1. Passare all'area di gestione "Autenticazione" della CMC.
2. Fare doppio clic sul collegamento **SAP**.

Vengono visualizzate le impostazioni dei sistemi di autorizzazione.

3. Fare clic sulla scheda **Impostazioni SNC** nella pagina di "autenticazione SAP".
4. Selezionare il sistema di autorizzazione dall'elenco **Nome sistema logico**.
5. Selezionare **Abilita Secure Network Communication (SNC)** in "Impostazioni base".
6. Selezionare l'opzione **Usa predefinito** per accettare il percorso predefinito per la libreria o selezionare l'opzione **Definisci percorso personalizzato** per scegliere un'altra posizione.
7. Selezionare un livello di protezione in "Qualità di protezione".
Ad esempio, selezionare **Autenticazione**.

Nota:

Non superare il livello di protezione configurato nel sistema SAP. Il livello di protezione è personalizzabile ed è determinato in base alle necessità dell'organizzazione e alle funzionalità della relativa libreria SNC.

8. Immettere il nome SNC del sistema SAP in "Impostazioni autenticazione reciproca".
Il formato del nome SNC dipende dalla libreria SNC. Se si utilizza la libreria di crittografia SAP, si consiglia di seguire le convenzioni di denominazione LDAP per il nome distinto apponendo `p` : come prefisso.
9. Verificare che il nome SNC delle credenziali sotto cui vengono eseguiti i server della piattaforma BI venga visualizzato nella casella **Nome SNC del sistema Enterprise**.
In scenari in cui vengono configurati diversi nomi SNC, è consigliabile lasciare vuoto questo campo.
10. Fornire il nome distinto (DN) del sistema SAP e del PSE della piattaforma BI.

9.5.6.3.6 Utilizzo di gruppi server

Se i server di elaborazione (Crystal Reports or Web Intelligence) non vengono eseguiti in base a credenziali che hanno accesso a PSE, è necessario creare uno specifico gruppo di server che includa solo quei server e i server di supporto necessari. Per ulteriori informazioni e descrizioni relative ai vari server della piattaforma BI, consultare il capitolo "Architettura".

È possibile eseguire la configurazione dei server di elaborazione di contenuto SAP in tre modi:

1. Utilizzare un singolo SIA, che includa tutti i server della piattaforma BI, eseguito in base a credenziali che hanno accesso a PSE. Questo è il metodo più semplice, in quanto non è necessario creare gruppi di server. Ma è anche quello meno sicuro poiché un numero non necessario di server ha accesso a PSE.
2. Creare un secondo SIA con accesso a PSE e aggiungerlo ai server di elaborazione Crystal Reports o Web Intelligence. Eliminare i server duplicati dal SIA di origine. Non è necessario creare gruppi di server ma l'accesso a PSE è garantito a un numero minore di server.
3. Creare un SIA esclusivamente per SAP con accesso a PSE. Aggiungerlo ai server di elaborazione Crystal Reports o Web Intelligence. Tale opzione prevede che su questi server venga eseguito solo contenuto SAP ma, soprattutto, che il contenuto SAP venga eseguito solo su questi server. Poiché con questo metodo il contenuto deve essere indirizzato a determinati server, è necessario creare gruppi di server per il SIA.

Linee guida per l'utilizzo di un gruppo di server

Il gruppo di server deve fare riferimento al SIA utilizzato esclusivamente per la gestione del contenuto SAP nonché ai seguenti server:

- Adaptive Server
- Adaptive Job Server

Tutto il contenuto SAP, i documenti Web Intelligence e i report Crystal devono essere associati al gruppo di server mediante l'associazione più rigorosa, ovvero devono essere eseguiti sui server del gruppo. Dopo la creazione dell'associazione a un livello oggetto, l'impostazione del gruppo di server deve essere propagata nelle impostazioni per la pianificazione diretta e le pubblicazioni.

Per impedire che altro contenuto (non SAP) venga elaborato nei server di elaborazione specifici di SAP, creare un altro gruppo di server che includa tutti i server nel SIA di origine. È importante creare un'associazione rigorosa tra questo contenuto e il gruppo di server non SAP.

9.5.6.4 Configurazione delle pubblicazioni multi-pass

Risoluzione dei problemi relativi alle pubblicazioni multi-pass

Se si riscontrano problemi con le pubblicazioni multi-pass, abilitare il tracciamento per i driver Crystal Reports (CR) o Multidimensional Data Access (MDA) per SAP ed esaminare la stringa di accesso utilizzata per ogni processo o destinatario. Le stringhe di accesso dovrebbero essere simili alla seguente:

```
SAP: Successfully logged on to SAP server.  
Logon handle: 1. Logon string: CLIENT=800 LANG=en  
ASHOST="vanrdw2k107.sap.crystald.net" SYSNR=00 SNC_MODE=1 SNC_QOP=1  
SNC_LIB="C:\WINDOWS\System32\sapcrypto.dll"  
SNC_PARTNERNAME="p:CN=R21Again, OU=PG, O=BOBJ, C=CA" EXTIDDATA=HENRIKRPT3 EXTIDTYPE=UN
```

La stringa di accesso deve contenere EXTIDTYPE=UN (per il nome utente) e EXTIDDATA dovrebbe essere il nome utente SAP del destinatario. In questo esempio, il tentativo di accesso è riuscito.

9.5.6.5 Workflow per l'integrazione con Secure Network Communication

La piattaforma BI supporta gli ambienti che implementano SNC (Secure Network Communication) per l'autenticazione e per la crittografia dei dati tra componenti SAP. Se è stata distribuita la libreria di crittografia SAP (o un altro prodotto di protezione esterna che utilizza l'interfaccia SNC), è necessario impostare valori aggiuntivi per integrare in modo efficace la piattaforma BI nell'ambiente protetto.

Per configurare la piattaforma BI per l'utilizzo di Secure Network Communication, è necessario eseguire le seguenti attività:

1. Configurare i server della piattaforma BI per consentirne l'avvio e l'esecuzione con un account utente appropriato.
2. Configurare il sistema SAP affinché consideri attendibile la piattaforma BI.
3. Configurare le impostazioni SNC nel collegamento SNC nella Central Management Console.

4. Importare utenti e ruoli SAP nella piattaforma BI.

Argomenti correlati

- [Importazione dei ruoli SAP](#)
- [Configurazione SAP per l'attendibilità lato server](#)
- [Configurazione della piattaforma BI per l'attendibilità lato server](#)

9.5.6.6 Per configurare le impostazioni SNC nella Central Management Console

Per poter configurare le impostazioni SNC, è necessario aggiungere un nuovo sistema di autorizzazione alla piattaforma BI, verificare che il file della libreria SNC si trovi in una directory nota e creare una variabile di ambiente `RFC_LIB` che punti al file.

1. Fare clic sulla scheda **Impostazioni SNC** nella pagina di "autenticazione SAP".
2. Selezionare il sistema di autorizzazione dall'elenco **Nome sistema logico**.
3. Selezionare **Abilita Secure Network Communication (SNC)** in "Impostazioni base".
4. Se si sta configurando l'autenticazione SAP per l'utilizzo di universi `.unx` o di connessioni OLAP BICS e si intende utilizzare STS, selezionare la casella di controllo **Blocca connessioni RFC in entrata non protette**.
5. Selezionare l'opzione **Usa predefinito** per accettare il percorso predefinito per la libreria o selezionare l'opzione **Definisci percorso personalizzato** per scegliere un'altra posizione.

Il server di applicazioni e il server CMS devono trovarsi sullo stesso tipo di sistema operativo con lo stesso percorso della libreria crypto.

6. Selezionare un livello di protezione in "Qualità di protezione".

Ad esempio, selezionare **Autenticazione**.

Nota:

il livello di protezione è personalizzabile ed è determinato in base alle necessità dell'organizzazione e alle funzionalità della relativa libreria SNC.

7. Immettere il nome SNC del sistema SAP in "Impostazioni autenticazione reciproca".

Il formato del nome SNC dipende dalla libreria SNC. Se si utilizza la libreria di crittografia SAP, si consiglia di seguire le convenzioni di denominazione LDAP per il nome distinto apponendo `p` : come prefisso.

8. Verificare che il nome SNC delle credenziali sotto cui vengono eseguiti i server della piattaforma BI venga visualizzato nella casella **Nome SNC del sistema Enterprise**.

In scenari in cui vengono configurati diversi nomi SNC, lasciare vuota questa casella.

9. Fare clic su **Aggiorna**.
10. Fare clic sulla scheda **Sistemi di autorizzazione** nella pagina di "autenticazione SAP".
L'opzione **Nome SNC** viene visualizzata sotto l'opzione **Lingua**.

11. Nella casella **Nome SNC** immettere il nome SNC configurato sul server SAP BW.

Il nome deve essere uguale a quello utilizzato per configurare il sistema SAP affinché la piattaforma BI sia considerata attendibile.

Se si utilizza il framework Insight to Action per abilitare l'interfaccia report-report, potrebbero essere necessari anche 10 minuti per l'abilitazione di SNC o perché le modifiche alle impostazioni SNC diventino effettive. Per attivare un aggiornamento immediato, riavviare il server Adaptive Processing Server su cui è in esecuzione il servizio Insight to Action.

Argomenti correlati

- [Connessione ai sistemi di autorizzazione SAP](#)

9.5.6.7 Per associare l'utente di autorizzazione a un nome SNC

1. Accedere al sistema SAP BW ed eseguire la transazione SU01.
Viene visualizzata la schermata iniziale Manutenzione utente.
2. Nel campo **Utente** digitare il nome dell'account SAP designato come utente di autorizzazione, quindi fare clic sul pulsante **Modifica** sulla barra degli strumenti.
Viene visualizzata la schermata Manutenzione utente.
3. Fare clic sulla scheda SNC.
4. Nel campo **Nome SNC** digitare l'ACCOUNT UTENTE SNC immesso in precedenza al punto 2.
5. Fare clic su **Salva**.

9.5.6.8 Aggiunta di un ID di sistema all'elenco di controllo di accesso SNC

1. Accedere al sistema SAP BW ed eseguire la transazione SNC0.
Viene visualizzata la finestra Cambia vista "SNC: Elenco di controllo di accesso (ACL) per sistemi".
2. Fare clic su **New Entries** sulla barra degli strumenti.
Viene visualizzata la finestra Nuove voci: Dettagli delle voci aggiunte.
3. Digitare il nome del computer della piattaforma BI nel campo **ID sistema**.
4. Digitare p:<NOME UTENTE SNC> nel campo **Nome SNC** dove NOME UTENTE SNC rappresenta l'account utilizzato per la configurazione dei server della piattaforma BI.

Nota:

se il provider SNC è gssapi32.dll, specificare il NOME UTENTE SNC in lettere maiuscole. Quando si specifica l'account utente, è necessario includere il nome di dominio. Ad esempio: dominio\nome utente.

5. Selezionare **Voce per RFC attivata** e **Voce per ID est. attivata**.
6. Deselezionare tutte le altre opzioni e fare clic su **Salva**.

9.5.7 Impostazione del Single Sign On nel sistema SAP

Diversi servizi client ed esterni della piattaforma BI interagiscono con i sistemi esterni NetWeaver ABAP in un ambiente integrato. È utile impostare Single Sign On dalla piattaforma BI a questi sistemi esterni (in genere BW). Dopo avere configurato un sistema ABAP come sistema di autenticazione esterno, vengono utilizzati token SAP proprietari per fornire un meccanismo che supporta Single Sign On per tutti i client e i servizi della piattaforma BI che si collegano ai sistemi NetWeaver ABAP.

Per abilitare il Single Sign On nel sistema SAP, è necessario creare un file `archivio_chiavi` e un certificato corrispondente. Utilizzare il programma da riga di comando `keytool` per generare il file e il certificato. Per impostazione predefinita, il programma `keytool` viene installato nella directory `sdk/bin` per ciascuna piattaforma.

È necessario aggiungere il certificato al sistema ABAP BW SAP e alla piattaforma BI utilizzando la CMC.

Nota:

Per potere impostare il Single Sign On nel database utilizzato da SAP BW, è necessario configurare il plug-in dell'autenticazione SAP.

9.5.7.1 Generazione del file archivio chiavi

Il programma `PKCS12Tool` viene utilizzato per generare i file archivio chiavi e i certificati necessari per l'impostazione di Single Sign On nel database SAP. Nella seguente tabella sono elencati i percorsi predefiniti per il file `PKCS12Tool.jar` per ogni piattaforma supportata:

Piattaforma	Posizione predefinita
Windows	<DIRINSTALL>\SAP BusinessObjects Enterprise XI 4.0\java\lib
Unix	sap_bobj/enterprise_xi40/java/lib

1. Avviare un prompt dei comandi e passare alla directory in cui si trova il programma `PKCS12Tool`

2. Per generare il file archivio chiavi con le impostazioni predefinite, eseguire il seguente comando:

```
java -jar PKCS12Tool.jar
```

I file `cert.der` e `keystore.p12` vengono generati nella stessa directory e contengono i seguenti valori predefiniti:

Parametro	Valore predefinito
-keystore	keystore.p12
-alias	myalias
-storepass	123456
-dname	CN=CA
-validity	365
-cert	cert.der

Suggerimento:

per sostituire i valori predefiniti, eseguire lo strumento insieme al parametro `-?`. Viene visualizzato il seguente messaggio:

```
Usage: PKCS12Tool <options>
  -keystore <filename(keystore.p12)>
  -alias <key entry alias(myalias)>
  -storepass <keystore password(123456)>
  -dname <certificate subject DN(CN=CA)>
  -validity <number of days(365)>
  -cert <filename(cert.der)>
      (No certificate is generated when importing a keystore)
  -disablefips
  -importkeystore <filename>
```

È possibile utilizzare i parametri per sostituire i valori predefiniti.

9.5.7.2 Esportazione del certificato di chiave pubblica

È necessario creare ed esportare un certificato per il file archivio chiavi.

1. Avviare un prompt dei comandi e passare alla directory in cui si trova il programma keytool
2. Per esportare il certificato chiave per il file archivio chiavi, utilizzare il comando seguente:

```
keytool -exportcert -keystore <keystore> -storetype pkcs12 -file <filename>
-alias <alias>
```

Sostituire <keystore> con il nome del file archivio chiavi.
Sostituire <filename> con il nome del certificato.
Sostituire <alias> con l'alias utilizzato per creare il file archivio chiavi.

3. Quando richiesto, immettere la password fornita per il file archivio chiavi.

A questo punto nella directory in cui si trova il programma keytool sono presenti un file archivio chiavi e un certificato.

9.5.7.3 Importazione del file certificato nel sistema ABAP SAP

Per consentire alla distribuzione della piattaforma BI di eseguire l'attività seguente, è necessario disporre di un file archivio chiavi con un certificato associato.

Nota:

questa azione può essere eseguita solo in un sistema ABAP SAP.

1. Connettersi al sistema ABAP BW SAP utilizzando la GUI SAP.

Nota:

è consigliabile connettersi come utente con privilegi amministrativi.

2. Eseguire STRUSTSSO2 nella GUI SAP.
Il sistema è preparato per importare il file di certificato.
3. Accedere alla scheda **Certificate**.
4. Assicurarsi che sia selezionata la casella di controllo **Use Binary option**.
5. Fare clic sul pulsante del percorso del file per individuare il percorso in cui si trova il file di certificato.
6. Fare clic sul segno di spunta verde.
Il file di certificato viene caricato.
7. Fare clic su **Add to Certificate List**.
Il certificato viene visualizzato nell'elenco certificati.
8. Fare clic su **Add to ACL** e specificare un client e un ID di sistema.
L'ID sistema deve corrispondere a quello utilizzato per identificare la piattaforma BI per SAP BW.
Il certificato viene aggiunto all'Elenco di controllo di accesso. Il client deve essere specificato come "000".
9. Salvare le impostazioni e chiudere.
Le modifiche vengono salvate nel sistema SAP.

9.5.7.4 Impostazione di Single Sign On nel database SAP nella CMC

Per eseguire la procedura seguente, è necessario accedere al plug-in di protezione SAP utilizzando un account amministratore.

1. Passare all'area di gestione "Autenticazione" della CMC.
2. Fare doppio clic sulla scheda **SAP** e quindi sulla scheda **Opzioni**.
Se non sono stati importati certificati, nella sezione "Servizio SAP SSO " dovrebbe essere visualizzato il messaggio seguente:
`Non è stato caricato alcun file archivio chiavi`
3. Specificare l'ID sistema per la piattaforma BI nel campo appropriato.
Questo valore dovrebbe essere identico a quello utilizzato per l'importazione del certificato nel sistema ABAP SAP.
4. Fare clic sul pulsante **Sfoglia** per individuare il file archivio chiavi.
5. Specificare i dettagli obbligatori seguenti:

Campo	Informazione richiesta
"Password archivio chiavi"	Specificare la password richiesta per l'accesso al file dell'archivio chiavi. Questa password è stata specificata durante la creazione del file archivio chiavi.
"Password chiave privata"	Specificare la password richiesta per l'accesso al certificato corrispondente al file dell'archivio chiavi. Questa password è stata specificata durante la creazione del certificato per il file archivio chiavi.
"Alias chiave privata"	Specificare l'alias richiesto per l'accesso al file dell'archivio chiavi. L'alias è stato specificato durante la creazione del file archivio chiavi.

6. Fare clic su **Aggiorna** per salvare le impostazioni.
Dopo aver salvato le impostazioni, nel campo ID sistema viene visualizzato il messaggio seguente:
`È stato caricato un file archivio chiavi`

9.5.7.5 Aggiunta del Servizio token di protezione ad Adaptive Processing Server

In un ambiente cluster, i Servizi token di protezione vengono aggiunti separatamente a ogni Adaptive Processing Server.

1. Passare all'area di gestione "Server" della CMC.
2. Fare doppio clic su **Servizi principali**.
In "Servizi principali" viene visualizzato l'elenco dei server.

3. Fare clic con il pulsante destro del mouse su Adaptive Processing Server e selezionare **Arresta server**.
Non continuare fino a quando lo stato del server diventa Interrotto.
4. Fare clic con il pulsante destro del mouse su Adaptive Processing Server e scegliere **Interrompi**.
Viene visualizzata la finestra di dialogo "Seleziona servizi".
5. Utilizzare il pulsante **Aggiungi** per spostare il servizio token di protezione dall'elenco **Servizi disponibili** all'elenco **Servizi**.
6. Fare clic su **OK**.
7. Riavviare l'Adaptive Processing Server.

9.5.8 Configurazione di SSO per SAP Crystal Reports e SAP NetWeaver

Per impostazione predefinita, la piattaforma BI viene configurata per consentire agli utenti di SAP Crystal Reports di accedere ai dati SAP utilizzando il Single Sign On (SSO).

9.5.8.1 Disattivazione di SSO per SAP NetWeaver e SAP Crystal Reports

1. Nella Central Management Console (CMC) fare clic su **Applicazioni**.
2. Fare doppio clic su **Configurazione di Crystal Reports**.
3. Fare clic su **Opzioni Single Sign On**.
4. Selezionare uno dei driver seguenti:

Driver	Nome visualizzato
Driver Operational Data Store	crdb_ods
Driver Open SQL	crdb_opensql
Driver InfoSet	crdb_infoset
Driver BW MDX Query	crdb_bwmdx

5. Fare clic su **Rimuovi**.
6. Fare clic su **Salva e chiudi**.
7. Riavviare SAP Crystal Reports.

9.5.8.2 Riattivazione di SSO per SAP NetWeaver e SAP Crystal Reports

Per riattivare SSO per SAP NetWeaver (ABAP) e SAP Crystal Reports, seguire la procedura riportata di seguito.

1. Nella Central Management Console (CMC) fare clic su **Applicazioni**.
2. Fare doppio clic su **Configurazione di Crystal Reports**.
3. Fare clic su **Opzioni Single Sign On**.
4. In "Utilizza il contesto SSO per accedere al database" digitare:

crdb_ods	Per attivare il driver ODS
crdb_opensql	Per attivare il driver Open SQL
crdb_bwmdx	Per attivare il driver SAP BW MDX Query
crdb_infoset	Per attivare il driver InfoSet

5. Fare clic su **Aggiungi**.
6. Fare clic su **Salva e chiudi**.
7. Riavviare SAP Crystal Reports.

9.6 Autenticazione PeopleSoft

9.6.1 Panoramica

Per utilizzare i dati di PeopleSoft Enterprise con la piattaforma BI, è necessario fornire al programma le informazioni relative alla distribuzione. Tali informazioni consentono alla piattaforma BI di autenticare gli utenti in modo che essi possano accedere al programma utilizzando le credenziali di PeopleSoft.

9.6.2 Abilitazione dell'autenticazione PeopleSoft Enterprise

Per consentire l'uso delle informazioni di PeopleSoft Enterprise nella piattaforma BI, è necessario indicare nella piattaforma BI le modalità di autenticazione per il sistema PeopleSoft Enterprise.

9.6.2.1 Abilitazione dell'autenticazione PeopleSoft Enterprise nella piattaforma BI

1. Eseguire l'accesso alla console CMC (Central Management Console) come amministratore.
 2. Fare clic su **Autenticazione** nell'area Gestisci.
 3. Fare doppio clic su **PeopleSoft Enterprise**.
Viene visualizzata la pagina "PeopleSoft Enterprise". Contiene quattro schede: **Opzioni**, **Domini**, **Ruoli** e **Aggiornamento utente**.
 4. Nella scheda **Opzioni** selezionare la casella di controllo **Abilita autenticazione PeopleSoft Enterprise**.
 5. Apportare le modifiche appropriate in **Nuovo alias**, **Opzioni di aggiornamento** e **Nuove opzioni utente** a seconda della distribuzione della piattaforma BI.
Fare clic su **Aggiorna** per salvare le modifiche prima di passare alla scheda **Domini**.
 6. Fare clic sulla scheda **Domini**.
 7. Nell'area "Utente di sistema PeopleSoft Enterprise" digitare un nome utente di database e una password per la piattaforma BI da utilizzare per l'accesso al database PeopleSoft Enterprise.
 8. Nell'area "Domini PeopleSoft Enterprise" immettere il nome dominio e l'indirizzo QAS utilizzati per connettersi all'ambiente PeopleSoft Enterprise, quindi fare clic su **Aggiungi**.
- Nota:**
nel caso di più domini PeopleSoft, ripetere la procedura per tutti i domini aggiuntivi cui si desidera accedere. Il primo dominio cui si accede diventa il dominio predefinito.
9. Fare clic su **Aggiorna** per salvare le modifiche.

9.6.3 Mappatura di ruoli PeopleSoft alla piattaforma BI

La piattaforma BI crea automaticamente un gruppo per ogni ruolo PeopleSoft mappato. Crea inoltre alias che rappresentano i membri dei ruoli PeopleSoft mappati.

È possibile creare un account utente per ogni alias creato.

Tuttavia, se si utilizzano più sistemi e gli utenti dispongono di account su più di un sistema, è possibile assegnare a ciascun utente un alias con lo stesso nome prima di creare gli account nella piattaforma BI.

In questo modo viene ridotto il numero di account creati per lo stesso utente nella piattaforma BI.

Ad esempio, se si utilizza PeopleSoft HR 8.3 e PeopleSoft Financials 8.4 e 30 utenti possono accedere ad entrambi i sistemi, verranno creati solamente 30 account per tali utenti. Se si decide di non assegnare un alias con lo stesso nome a ciascun utente, verranno creati 60 account per i 30 utenti nella piattaforma BI.

Tuttavia, se vengono eseguiti più sistemi e i nomi utente coincidono, è necessario creare un nuovo account del membro per ciascun alias creato.

Ad esempio, se si utilizza PeopleSoft HR 8.3 con l'account utente di Roberto Antinori (nome utente "rantinori") e PeopleSoft Financials 8.4 con l'account utente di Renato Antinori (nome utente "rantinori"), è necessario creare un account diverso per ogni alias dell'utente. In caso contrario, i due utenti verranno aggiunti allo stesso account della piattaforma BI, potranno accedere alla piattaforma BI con le proprie credenziali PeopleSoft e avranno accesso ai dati da entrambi i sistemi PeopleSoft.

9.6.3.1 Mappatura di un ruolo PeopleSoft alla piattaforma BI

Se la JVM (Java virtual machine) della piattaforma BI non dispone di un certificato per il server PeopleSoft, sarà necessario eseguire questi passaggi aggiuntivi prima dei passaggi principali indicati di seguito:

1. Ottenere il file .cer dal server PeopleSoft.
2. Copiare il file .cer in `DIRINSTALLAZ\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security`.
3. Eseguire il comando riportato di seguito dalla directory di protezione: `"DIRINSTALLAZ\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool.exe" -import -file serverpeoplesoft.cer -keystore cacerts -alias serverpeoplesoft`.
4. Riavviare il server di applicazioni Web.

Passaggi principali:

1. Eseguire l'accesso alla CMC (Central Management Console) come amministratore.
2. Fare clic su **Autenticazione**.
3. Fare doppio clic su **PeopleSoft Enterprise**.
4. Nella scheda **Ruoli**, nell'area Domini PeopleSoft Enterprise, selezionare il dominio associato al ruolo che si desidera mappare nella piattaforma BI.
5. Utilizzare una delle seguenti opzioni per selezionare i ruoli da mappare:
 - Nell'area "Ruoli PeopleSoft Enterprise", nella casella Cerca ruoli, immettere il ruolo da individuare, eseguire la mappatura nella piattaforma BI e fare clic su **>**.
 - Dall'elenco "Ruoli disponibili" selezionare il ruolo che si desidera mappare alla piattaforma BI e fare clic su **>**.

Nota:

- Per la ricerca di un particolare utente o ruolo, è possibile utilizzare il carattere jolly %. Ad esempio, per cercare tutti i ruoli che iniziano con "A", digitare **A%**. La ricerca fa distinzione tra maiuscole e minuscole.

- Se si desidera mappare un ruolo da un altro dominio, è necessario selezionare il nuovo dominio dall'elenco di domini disponibili per individuare la corrispondenza di un ruolo da un dominio diverso.
6. Accedere alla scheda **Aggiornamento utente** e fare clic sul pulsante **Aggiorna** oppure pianificare gli aggiornamenti.
 7. Nella scheda **Opzioni** accedere all'area "Nuove opzioni utente" e selezionare una delle opzioni seguenti:
 - **Assegna ogni alias aggiunto a un account con lo stesso nome**

Selezionare questa opzione se si utilizzano più sistemi PeopleSoft Enterprise con utenti che dispongono di account in più sistemi (due utenti non possono avere lo stesso nome utente per sistemi diversi).
 - **Crea un nuovo account per ogni alias aggiunto**

Selezionare questa opzione se si utilizza solo un sistema PeopleSoft Enterprise, se la maggior parte degli utenti dispone di account su uno solo dei sistemi utilizzati oppure se i nomi utente di diversi utenti coincidono su due o più dei sistemi in uso.
 8. Nell'area "Opzioni di aggiornamento alias" selezionare una delle opzioni seguenti:
 - **Crea nuovi alias all'aggiornamento dell'alias**

Selezionare questa opzione per creare un nuovo alias per ciascun utente mappato nella piattaforma BI. Se è stata selezionata l'opzione Crea nuovo account per ogni alias aggiunto, verranno aggiunti nuovi account per gli utenti senza account della piattaforma BI o per tutti gli utenti.
 - **Crea nuovi alias solo all'accesso dell'utente**

Selezionare questa opzione se il ruolo che si desidera mappare contiene molti utenti, ma solo una parte di essi utilizzerà la piattaforma BI. La piattaforma non crea automaticamente gli alias e gli account per gli utenti. Crea invece alias (e account, se necessario) solo per utenti che accedono alla piattaforma BI per la prima volta. Si tratta dell'opzione predefinita.
 9. Nell'area "Nuove opzioni utente" specificare la modalità di creazione dei nuovi utenti.

Selezionare una delle seguenti opzioni:

 - **I nuovi utenti vengono creati come utenti specifici.**

I nuovi account utente verranno configurati per utilizzare licenze utente designato. Le licenze utente designato sono associate a utenti specifici e consentono di accedere al sistema in base a nome utente e password. Ciò garantisce agli utenti specifici l'accesso al sistema a prescindere dal numero delle altre persone connesse. È necessario disporre di una licenza utente designato per ciascun account utente creato utilizzando questa opzione.
 - **I nuovi utenti vengono creati come utenti simultanei.**

I nuovi account utente verranno configurati per utilizzare licenze utente simultaneo. Le licenze di accesso simultaneo specificano il numero di persone che possono connettersi alla piattaforma BI contemporaneamente. Questo tipo di licenza è estremamente flessibile, poiché una licenza di accesso simultaneo di dimensioni ridotte può supportare un'ampia base di utenti. Ad esempio,

in base alla frequenza e alla durata dell'accesso alla piattaforma BI, una licenza di accesso simultaneo per 100 utenti può supportare 250, 500 o 700 utenti.

I ruoli selezionati vengono ora visualizzati come gruppi nella piattaforma BI.

9.6.3.2 Considerazioni sulla rimappatura

Se si aggiungono utenti a un ruolo che è stato già mappato nella piattaforma BI, sarà necessario rimappare il ruolo per aggiungere gli utenti alla piattaforma BI. Quando si rimappa il ruolo, l'opzione relativa alla mappatura di utenti come utenti titolari o simultanei riguarda solamente i nuovi utenti che sono stati aggiunti al ruolo.

Ad esempio, prima si mappa un ruolo nella piattaforma BI selezionando l'opzione "I nuovi utenti vengono creati come utenti specifici", quindi si aggiungono gli utenti allo stesso ruolo e si rimappa il ruolo selezionando l'opzione "I nuovi utenti vengono creati come utenti simultanei".

In questa situazione, solo i nuovi utenti del ruolo vengono mappati nella piattaforma BI come utenti simultanei; gli utenti mappati in precedenza rimangono utenti specifici. Questo avviene anche quando gli utenti vengono prima mappati come simultanei e, in seguito, vengono modificate le impostazioni per rimappare i nuovi utenti come utenti designati.

9.6.3.3 Eliminazione della mappatura di un ruolo

1. Eseguire l'accesso alla CMC (Central Management Console) come amministratore.
2. Fare clic su **Autenticazione**.
3. Fare clic su **PeopleSoft Enterprise**.
4. Fare clic su **Ruoli**.
5. Selezionare il ruolo che si desidera rimuovere e fare clic su <.
6. Fare clic su **Aggiorna**.

I membri del ruolo non saranno più in grado di accedere alla piattaforma BI finché non disporranno di altri account o alias.

Nota:

è inoltre possibile eliminare singoli account o rimuovere gli utenti dai ruoli prima di eseguire la mappatura nella piattaforma BI, impedendo così l'accesso a determinati utenti.

9.6.4 Pianificazione degli aggiornamenti utente

Per garantire che le modifiche ai dati utente per il sistema ERP vengano riportate nei dati utente della piattaforma BI, è possibile pianificare aggiornamenti utente regolari. Questi aggiornamenti sincronizzeranno automaticamente gli utenti ERP e la piattaforma BI in base alle impostazioni delle mappature configurate nella CMC (Central Management Console).

Sono disponibili due opzioni per l'esecuzione e la pianificazione degli aggiornamenti per i ruoli importati:

- **Aggiorna solo ruoli:** l'uso di questa opzione determina l'aggiornamento dei soli collegamenti tra i ruoli attualmente mappati importati nella piattaforma BI. Utilizzare questa opzione se si prevede di eseguire aggiornamenti frequenti e si desidera evitare problemi di utilizzo delle risorse di sistema. Se si aggiornano solo i ruoli, non vengono creati nuovi account utente.
- **Aggiorna ruoli e alias:** questa opzione determina non solo l'aggiornamento dei collegamenti tra i ruoli, ma anche la creazione di nuovi account utente nella piattaforma BI per i nuovi alias utente aggiunti al sistema ERP.

Nota:

se non è stata specificata la creazione automatica degli alias utente per gli aggiornamenti quando è stata abilitata l'autenticazione, non verranno creati account per i nuovi alias.

9.6.4.1 Pianificazione degli aggiornamenti utente

Una volta mappati i ruoli nella piattaforma BI, è necessario specificare in che modo vengono aggiornati dal sistema.

1. Fare clic sulla scheda **Aggiornamento utente**.
2. Fare clic su **Pianifica** nella sezione "Aggiorna solo ruoli" o "Aggiorna ruoli e alias".

Suggerimento:

se si desidera eseguire immediatamente un aggiornamento, fare clic su **Aggiorna ora**.

Suggerimento:

utilizzare l'opzione "Aggiorna solo ruoli" se si desidera eseguire aggiornamenti frequenti e si verificano problemi con le risorse di sistema. Il sistema impiega più tempo per aggiornare sia i ruoli che gli alias.

Viene visualizzata la finestra di dialogo "Ricorrenza".

3. Selezionare un'opzione nell'elenco "Esegui oggetto" e fornire tutte le informazioni richieste relative alla pianificazione.

Quando si pianifica un aggiornamento, è possibile scegliere tra gli schemi ricorrenti nella seguente tabella.

Criterio di ricorrenza	Descrizione
Ogni ora	L'aggiornamento verrà eseguito ogni ora. È possibile specificare l'ora di inizio nonché una data di inizio e di fine.
Giornaliero	L'aggiornamento verrà eseguito ogni giorno oppure dopo il numero di giorni specificato. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Settimanale	L'aggiornamento verrà eseguito ogni settimana. e può essere eseguito una o più volte a settimana. È possibile specificare in quali giorni e a che ora verrà eseguito nonché una data di inizio e di fine.
Mensile	L'aggiornamento verrà eseguito ogni mese oppure dopo il numero di mesi specificato. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Il N° giorno del mese	L'aggiornamento verrà eseguito in un giorno specifico del mese. È possibile specificare in quale giorno del mese e a che ora verrà eseguito nonché una data di inizio e di fine.
Il primo lunedì del mese	L'aggiornamento verrà eseguito il primo lunedì di ogni mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Ultimo giorno del mese	L'aggiornamento verrà eseguito l'ultimo giorno di ogni mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Giorno X della N° settimana del mese	L'aggiornamento verrà eseguito in un giorno specifico di una settimana specifica del mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Calendario	L'aggiornamento verrà eseguito nelle date specificate all'interno di un calendario creato in precedenza.

4. Fare clic su **Pianifica** dopo aver completato l'inserimento delle informazioni sulla pianificazione. Nella scheda **Aggiornamento utente** viene visualizzata la data del successivo ruolo pianificato.

Nota:

è sempre possibile annullare il successivo aggiornamento pianificato facendo clic su **Annulla aggiornamenti pianificati** nella sezione "Aggiorna solo ruoli" o "Aggiorna ruoli e alias".

9.6.5 Utilizzo del Ponte di protezione PeopleSoft

La funzionalità Ponte di protezione della piattaforma BI consente di importare le impostazioni di protezione di PeopleSoft EPM nella piattaforma BI.

Ponte di protezione funziona in due modalità diverse:

- Modalità di configurazione

In modalità di configurazione fornisce un'interfaccia che consente all'utente di creare un file di risposta. Questo file regola il funzionamento di Ponte di protezione in modalità di esecuzione.

- Modalità di esecuzione

In base ai parametri definiti dall'utente nel file di risposta, Ponte di protezione importa le impostazioni di protezione delle tabelle di dimensioni di PeopleSoft EPM negli universi della piattaforma BI.

9.6.5.1 Importazione delle impostazioni di protezione

Per importare le impostazioni di protezione è necessario eseguire nell'ordine le seguenti attività:

- Definire gli oggetti che dovranno essere gestiti da Ponte di protezione.
- Creare un file di risposta.
- Eseguire l'applicazione Ponte di protezione.

Per informazioni sulla gestione della protezione dopo l'importazione delle impostazioni, vedere [Gestione delle impostazioni di protezione](#).

9.6.5.1.1 Definizione degli oggetti gestiti

Prima di eseguire Ponte di protezione, è importante determinare gli oggetti gestiti dall'applicazione. Ponte di protezione gestisce uno o più ruoli PeopleSoft, un gruppo della piattaforma BI e uno o più universi.

- Ruoli PeopleSoft gestiti

Questi sono i ruoli del sistema PeopleSoft in uso. I membri di questi ruoli utilizzano i dati PeopleSoft mediante PeopleSoft EPM. È necessario selezionare i ruoli che includono i membri per i quali si desidera assegnare o aggiornare i privilegi di accesso agli universi gestiti nella piattaforma BI.

I diritti di accesso definiti per i membri di questi ruoli si basano sui rispettivi diritti in PeopleSoft EPM. Ponte di protezione importa queste impostazioni di protezione nella piattaforma BI.

- Gruppo della piattaforma BI gestito

Quando si esegue Ponte di protezione, il programma crea un utente nella piattaforma BI per ogni membro di un ruolo PeopleSoft gestito.

Il gruppo in cui vengono creati gli utenti è il gruppo della piattaforma BI gestito. I membri di questo gruppo sono utenti i cui diritti di accesso agli universi gestiti sono gestiti da Ponte di protezione.

Poiché gli utenti vengono creati in un solo gruppo, è possibile configurare Ponte di protezione in modo da non eseguire l'aggiornamento delle impostazioni di protezione per alcuni utenti mediante la semplice rimozione di tali utenti dal gruppo della piattaforma BI gestito.

Prima di eseguire Ponte di protezione, è necessario selezionare un gruppo della piattaforma BI, che sarà la posizione in cui verranno creati gli utenti. Se si specifica un gruppo inesistente, Ponte di protezione creerà il gruppo nella piattaforma BI.

- Universi gestiti

Gli universi gestiti sono gli universi in cui Ponte di protezione importa le impostazioni di protezione da PeopleSoft EPM. È necessario selezionare tra gli universi archiviati nella propria piattaforma BI quelli che dovranno essere gestiti da Ponte di protezione. I membri di ruoli PeopleSoft gestiti che sono anche membri del gruppo della piattaforma BI gestito non possono accedere mediante questi universi ai dati il cui accesso è impossibile da PeopleSoft EPM.

9.6.5.1.2 Per creare un file di risposta

1. Accedere alla cartella specificata durante l'installazione del Ponte di protezione ed eseguire il file `crpsepmsecuritybridge.bat` (in Windows) e il file `crpsepmsecuritybridge.sh` (in Unix).

Nota:

Per impostazione predefinita, in Windows il file si trova in `C:\Programmi\Business Objects\Kit di integrazione di BusinessObjects 12.0 per PeopleSoft\epm`

Viene visualizzata la finestra di dialogo Ponte di protezione per PeopleSoft EPM.

2. Selezionare **Nuovo** per creare un file di risposta oppure selezionare **Apri** e fare clic su **Sfoglia** per specificare il file di risposta che si desidera modificare. Selezionare la lingua da utilizzare per il file.
3. Fare clic su **Avanti**.
4. Indicare le posizioni dell'**SDK di PeopleSoft EPM** e dell'**SDK della piattaforma BI**.

Nota:

- L'SDK di PeopleSoft EPM di solito si trova nel server PeopleSoft in `<PS_HOME>/class/com.peoplesoft.epm.pf.jar`.
- L'SDK della piattaforma BI di solito si trova nel percorso `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib`.

5. Fare clic su **Avanti**.

La finestra di dialogo richiede all'utente informazioni relative alla connessione e al driver per il database di PeopleSoft.

6. Dall'elenco Database, selezionare il tipo di database appropriato e fornire le informazioni per i seguenti campi:

Campo	Descrizione
Database	Nome del database PeopleSoft.

Campo	Descrizione
Host	Nome del server sul quale è installato il data-base.
Numero di porta	Il numero della porta per accedere al server.
Posizione classe	Posizione dei file di classe del driver di data-base.
Nome utente	Il nome dell'utente.
Password	La password.

7. Fare clic su **Avanti**.

La finestra di dialogo visualizza un elenco di tutte le classi necessarie per l'esecuzione di Ponte di protezione. Se necessario, è possibile aggiungere o rimuovere classi dall'elenco.

8. Fare clic su **Avanti**.

La finestra di dialogo richiede le informazioni di connessione per la piattaforma BI.

9. Fornire le informazioni appropriate per i seguenti campi:

Campo	Descrizione
Server	Nome del server nel quale è posizionato il Central Management Server (CMS).
Nome utente	Il nome dell'utente.
Password	La password.
Autenticazione	Il tipo di autenticazione.

10. Fare clic su **Avanti**.

11. Scegliere un gruppo della piattaforma BI e fare clic su **Avanti**.

Nota:

- Il gruppo specificato in questo campo è quello in cui Ponte di protezione crea utenti per i membri dei ruoli PeopleSoft gestiti.
- Se viene specificato un gruppo che non esiste ancora, Ponte di protezione procederà alla sua creazione.

La finestra di dialogo visualizza un elenco di ruoli dal sistema PeopleSoft.

12. Selezionare l'opzione **Importato** per i ruoli che il Ponte di protezione deve gestire, quindi fare clic su **Avanti**.

Nota:

Ponte di protezione crea un utente nel gruppo della piattaforma BI gestito (specificato nella fase precedente) per ciascun membro dei ruoli selezionati.

Nella finestra di dialogo è visualizzato un elenco di universi della piattaforma BI.

13. Selezionare gli universi nei quali si desidera che Ponte di protezione importi le impostazioni di protezione, quindi fare clic su **Avanti**.
14. Specificare il nome e la posizione in cui salvare il file di registro di Ponte di protezione. È possibile utilizzare il file di registro per determinare se Ponte di protezione esegue correttamente l'importazione delle impostazioni di protezione da PeopleSoft EPM.
15. Fare clic su **Avanti**.

La finestra di dialogo visualizza un'anteprima del file di risposta che verrà utilizzato da Ponte di protezione in modalità di esecuzione.
16. Fare clic su **Salva** e selezionare la posizione in cui si desidera salvare il file di risposta.
17. Fare clic su **Avanti**.

Il file di risposta per Ponte di protezione è stato creato correttamente.
18. Fare clic su **Esci**.

Nota:

Il file di risposta è un file di proprietà Java che può anche essere creato e/o modificato manualmente. Per ulteriori dettagli, vedere la sezione "File di risposta PeopleSoft".

9.6.5.2 Applicazione delle impostazioni di protezione

Per applicare le impostazioni di protezione, eseguire il file batch `crpsepmsecuritybridge.bat` (in Windows) o `crpsepmsecuritybridge.sh` (in Unix) e utilizzare il file di risposta creato come argomento. Digitare ad esempio `crpsepmsecuritybridge.bat myresponsefile.properties` in Windows o `crpsepmsecuritybridge.sh myresponsefile.properties` in Unix.

Viene eseguita l'applicazione Ponte di protezione, che consente di creare utenti nella piattaforma BI per i membri dei ruoli PeopleSoft specificati nel file di risposta e di importare le impostazioni di protezione da PeopleSoft EPM negli universi appropriati.

9.6.5.2.1 Considerazioni sulla mappatura

In modalità di esecuzione, Ponte di protezione crea un utente nella piattaforma BI per ciascun membro di un ruolo PeopleSoft gestito.

Gli utenti creati dispongono unicamente di alias di autenticazione Enterprise e la piattaforma BI assegna loro le password in modo casuale. In questo modo gli utenti non possono accedere alla piattaforma BI finché l'amministratore non assegna manualmente nuove password oppure mappa i ruoli alla piattaforma

BI mediante il plug-in di protezione PeopleSoft, consentendo così agli utenti di accedere utilizzando le proprie credenziali PeopleSoft.

9.6.5.3 Gestione delle impostazioni di protezione

È possibile gestire le impostazioni di protezione applicate modificando gli oggetti gestiti da Ponte di protezione.

9.6.5.3.1 Utenti gestiti

Ponte di protezione gestisce gli utenti sulla base dei seguenti criteri:

- Appartenenza o meno di un utente ad un ruolo PeopleSoft gestito.
- Appartenenza o meno di un utente al gruppo della piattaforma BI gestito.

Se si desidera consentire a un utente di accedere ai dati PeopleSoft mediante gli universi nella piattaforma BI, assicurarsi che l'utente appartenga sia a un ruolo PeopleSoft gestito sia al gruppo della piattaforma BI gestito.

- Ponte di protezione crea account e assegna in modo casuale le password ai membri di ruoli PeopleSoft gestiti che non dispongono di account nella piattaforma BI. L'amministratore deve decidere se assegnare manualmente o meno nuove password oppure se mappare i ruoli alla piattaforma BI mediante il plug-in di protezione PeopleSoft, in modo da consentire agli utenti di accedere alla piattaforma BI.
- Per i membri di ruoli PeopleSoft che appartengono anche ai gruppi della piattaforma BI gestiti, Ponte di protezione aggiorna le impostazioni di protezione applicate all'utente, consentendo così l'accesso ai dati appropriati dagli universi gestiti.

Se un membro di un ruolo PeopleSoft gestito dispone di un account nella piattaforma BI ma non è membro del gruppo della piattaforma BI gestito, Ponte di protezione non aggiorna le impostazioni di protezione applicate all'utente. In genere questo avviene solo quando l'amministratore rimuove manualmente dal gruppo della piattaforma BI gestito gli account utente creati da Ponte di protezione.

Nota:

Si tratta di un metodo efficace per la gestione della protezione: rimuovendo gli utenti dal gruppo della piattaforma BI gestito, è possibile configurarne le impostazioni di protezione in modo che siano diverse da quelle impostate in PeopleSoft.

Al contrario, se un membro del gruppo della piattaforma BI gestito non è un membro di un ruolo PeopleSoft gestito, Ponte di protezione non fornirà l'accesso agli universi gestiti. In genere questo si verifica solo quando gli amministratori PeopleSoft rimuovono gli utenti precedentemente mappati alla piattaforma BI dai ruoli PeopleSoft gestiti mediante Ponte di protezione.

Nota:

Si tratta di un altro metodo per la gestione della protezione: rimuovendo gli utenti dai ruoli PeopleSoft gestiti, tali utenti non potranno accedere ai dati da PeopleSoft.

9.6.5.3.2 Universi gestiti

Ponte di protezione gestisce gli universi mediante set di restrizioni che limitano i dati ai quali gli utenti gestiti possono accedere dagli universi gestiti.

Queste restrizioni sono gruppi di limitazione (ad esempio, limitazioni a Query Controls, SQL Generation e così via). Ponte di protezione applica/aggiorna le limitazioni di accesso alle righe o agli oggetti degli universi gestiti:

- applica infatti delle limitazioni di accesso alle righe per le tabelle di dimensione definite in PeopleSoft EPM. Queste limitazioni sono specifiche dell'utente e possono essere configurate con una delle seguenti impostazioni:
 - Accesso dell'utente a tutti i dati.
 - Accesso negato a tutti i dati.
 - L'accesso ai dati da parte dell'utente dipende dalle autorizzazioni a livello di riga in PeopleSoft, indicate nelle tabelle SJT (Security Join Tables) definite in PeopleSoft EPM.
- Le limitazioni di accesso agli oggetti sono applicate agli oggetti indicatore sulla base dei campi ai quali è possibile accedere mediante gli indicatori stessi.

Se un oggetto indicatore accede a campi definiti come metriche in PeopleSoft, l'accesso all'oggetto indicatore sarà consentito o meno in base alla possibilità da parte dell'utente di accedere alla metrica di riferimento in PeopleSoft. Se l'utente non può accedere a nessuna metrica, l'accesso all'oggetto indicatore verrà negato. Se l'utente ha accesso a tutte le metriche, sarà possibile accedere all'oggetto indicatore.

L'amministratore può anche decidere di limitare i dati ai quali gli utenti possono accedere dal sistema PeopleSoft riducendo il numero degli universi gestiti da Ponte di protezione.

9.6.5.4 File di risposta PeopleSoft

La funzionalità Ponte di protezione della piattaforma BI opera in base alle impostazioni specificate in un file di risposta.

In genere, il file di risposta viene creato utilizzando l'interfaccia fornita da Ponte di protezione in modalità di configurazione. Inoltre, trattandosi di un file di proprietà Java, è possibile crearlo o modificarlo manualmente.

In questa appendice vengono fornite informazioni circa i parametri da includere nel file di risposta per la creazione manuale.

Nota:

Quando si crea il file, è necessario rispettare i requisiti di escape indicati nel file delle proprietà (ad esempio, l'escape per ':' è '\:').

9.6.5.4.1 Parametri del file di risposta

La seguente tabella contiene una descrizione dei parametri inclusi nel file di risposta:

Parametro	Descrizione
classpath	<p>Il percorso della classe per il caricamento dei file .jar necessari. Più percorsi devono essere separati da un ';' sia in Windows che in UNIX.</p> <p>Sono necessari i percorsi di classe per i file <code>com.peoplesoft.epm.pf.jar</code> e per i file .jar del driver JDBC.</p>
db.driver.name	Il nome del driver JDBC utilizzato per connettersi al database PeopleSoft (ad esempio, <code>com.microsoft.jdbc.sqlserver.SQLServerDriver</code>).
db.connect.str	La stringa di connessione JDBC utilizzata per connettersi al database PeopleSoft (ad esempio, <code>jdbc:microsoft:sqlserver://vanrdpsft01:1433;DatabaseName=PRDMO</code>).
db.user.name	Il nome utente utilizzato per accedere al database PeopleSoft.
db.password	La password utilizzata per accedere al database PeopleSoft.
db.password.encrypted	Il valore di questo parametro determina se il parametro della password nel file di risposta è codificato o meno. Il valore può essere impostato su True o su False. Se non viene specificato alcun valore, viene assunto il valore predefinito False.
enterprise.cms.name	Il CMS in cui vengono posizionati gli universi.
enterprise.user.name	Il nome utente utilizzato per accedere al CMS.
enterprise.password	La password utilizzata per accedere al CMS.

Parametro	Descrizione
enterprise.password.encrypted	Il valore di questo parametro determina se il parametro della password nel file di risposta è codificato o meno. Il valore può essere impostato su True o su False. Se non viene specificato alcun valore, viene assunto il valore predefinito False.
enterprise.authMethod	Il metodo di autenticazione per l'accesso al CMS.
enterprise.role	Il gruppo della piattaforma BI gestito. Per ulteriori informazioni, consultare Definizione degli oggetti gestiti .
enterprise.license	Controlla il tipo di licenza quando si importano gli utenti da Peoplesoft. "0" imposta la licenza utente designato, "1" imposta la licenza di accesso simultaneo.
peoplesoft.role.n	<p>L'elenco dei ruoli PeopleSoft gestiti. Per ulteriori informazioni, consultare Definizione degli oggetti gestiti.</p> <p><i>n</i> è un numero intero e ciascuna voce occupa una proprietà con il prefisso peoplesoft.role.</p> <p>Nota: <i>n</i> è a base 1.</p> <p>È possibile utilizzare '*' per identificare tutti ruoli PeopleSoft disponibili, stabilito che <i>n</i> è 1 ed è l'unica proprietà con il prefisso peoplesoft.role nel file di risposta.</p>

Parametro	Descrizione
mapped.universe.n	<p>L'elenco degli universi che si desidera aggiornare tramite la funzione Ponte di protezione. Per ulteriori informazioni, consultare Definizione degli oggetti gestiti.</p> <p><i>n</i> è un numero intero e ciascuna voce occupa una proprietà con il prefisso mapped.universe.</p> <p>Nota: <i>n</i> è a base 1.</p> <p>È possibile utilizzare '*' per identificare tutti gli universi disponibili, stabilito che <i>n</i> è 1 ed è l'unica proprietà con il prefisso mapped.universe nel file di risposta.</p>
log4j.appender.file.File	Il file di registro scritto dalla funzione Ponte di protezione.
log4j.*	<p>Le proprietà log4j predefinite necessarie per il funzionamento corretto di log4j:</p> <p>log4j.rootLogger=INFO, file, stdout</p> <p>log4j.appender.file=org.apache.log4j.RollingFileAppender</p> <p>log4j.appender.file.layout=org.apache.log4j.PatternLayout</p> <p>log4j.appender.file.MaxFileSize=5000KB</p> <p>log4j.appender.file.MaxBackupIndex=100</p> <p>log4j.appender.file.layout.ConversionPattern=%d [%-5] %c{1} - %m%n</p> <p>log4j.appender.stdout=org.apache.log4j.ConsoleAppender</p> <p>log4j.appender.stdout.layout=org.apache.log4j.PatternLayout</p> <p>log4j.appender.stdout.layout.ConversionPattern=%d [%-5] %c{1} - %m%n</p>

Parametro	Descrizione
peoplesoft classpath	<p>Il percorso della classe per i file .jar API di PeopleSoft EPM.</p> <p>Questo parametro è facoltativo.</p>
enterprise.classpath	<p>Il percorso della classe per i file .jar SDK della piattaforma BI.</p> <p>Questo parametro è facoltativo.</p>
db.driver.type	<p>Il tipo di database PeopleSoft. Questo parametro potrebbe assumere uno dei seguenti valori:</p> <p>Microsoft SQL Server 2000</p> <p>Oracle Database 10.1</p> <p>DB2 UDB 8.2 Fixpack 7</p> <p>Personalizzato</p> <p>Il valore Custom può essere utilizzato per specificare i database, oltre che per distinguerne i tipi o le versioni.</p> <p>Questo parametro è facoltativo.</p>
sql.db.class.location sql.db.host sql.db.port sql.db.database	<p>La posizione dei file .jar del driver JDB, il computer host SQL Server, la porta SQL Server e il nome del database SQL Server.</p> <p>Questi parametri possono essere utilizzati solo se db.driver.type corrisponde a Microsoft SQL Server 2000.</p> <p>Questi parametri sono facoltativi.</p>
oracle.db.class.location oracle.db.host oracle.db.port oracle.db.sid	<p>La posizione dei file .jar del driver JDBC Oracle, il computer host Oracle, la porta e il SID del database Oracle.</p> <p>Questi parametri possono essere utilizzati solo se db.driver.type corrisponde a Oracle Database 10.1.</p> <p>Questi parametri sono facoltativi.</p>

Parametro	Descrizione
db2.db.class.location db2.db.host db2.db.port db2.db.sid	La posizione dei file .jar del driver JDBC DB2, il computer host DB2, la porta e il SID del database DB2. Questi parametri possono essere utilizzati solo se db.driver.type corrisponde a DB2 UDB 8.2 Fixpack 7 Questi parametri sono facoltativi.
custom.db.class.location custom.db.drivename custom.db.connectStr	La posizione, il nome e la stringa di connessione del driver JDBC personalizzato. Questi parametri possono essere utilizzati solo se db.driver.type corrisponde a Custom. Questi parametri sono facoltativi.

9.7 Autenticazione JD Edwards

9.7.1 Panoramica

Per utilizzare i dati JD Edwards con la piattaforma BI, è necessario fornire al sistema le informazioni relative alla distribuzione. Queste informazioni consentono alla piattaforma BI di autenticare gli utenti in modo che essi possano utilizzare le credenziali di JD Edwards EnterpriseOne per accedere alla piattaforma BI.

9.7.2 Abilitazione dell'autenticazione JD Edwards EnterpriseOne

Per fare in modo che nella piattaforma BI vengano utilizzate le informazioni di JD Edwards EnterpriseOne, è necessario configurare l'applicazione per l'autenticazione nel sistema JD Edwards EnterpriseOne.

9.7.2.1 Abilitazione dell'autenticazione JD Edwards nella piattaforma BI

1. Eseguire l'accesso alla console CMC (Central Management Console) come amministratore.
2. Fare clic su **Autenticazione** nell'area Gestisci.
3. Fare doppio clic su **JD Edwards EnterpriseOne**.
Viene visualizzata la pagina "JD Edwards EnterpriseOne".
4. Nella scheda **Opzioni** selezionare la casella di controllo **Abilita autenticazione JD Edwards EnterpriseOne**.
5. Apportare le modifiche appropriate in **Nuovo alias**, **Opzioni di aggiornamento** e **Nuove opzioni utente** a seconda della distribuzione della piattaforma BI. Fare clic su **Aggiorna** per salvare le modifiche prima di passare alla scheda **Sistemi**.
6. Fare clic sulla scheda **Server**.
7. Copiare `jdeutil.jar`, `kernel.jar` e `log4j.jar` dall'installazione di JD Edwards in questi percorsi (in Windows): `<DIRINSTALLAZ>\SAP BusinessObjects Enterprise XI 4.0\java\lib\jdedwards\default\jdedwards\` e `<DIRINSTALLAZ>\Tomcat\lib\`.
8. Riavviare Tomcat e Server Intelligence Agent.
9. Nell'area "Utente di sistema JD Edwards EnterpriseOne" digitare un nome utente e una password per la piattaforma BI da utilizzare per accedere al database JD Edwards EnterpriseOne.
10. Nell'area "Dominio JD Edwards EnterpriseOne" immettere il nome, l'host e la porta utilizzati per la connessione all'ambiente JD Edwards EnterpriseOne, immettere un nome per l'ambiente e fare clic su **Aggiungi**.
11. Fare clic su **Aggiorna** per salvare le modifiche.

9.7.3 Mappatura dei ruoli JD Edwards EnterpriseOne alla piattaforma BI

La piattaforma BI crea automaticamente un gruppo per ogni ruolo JD Edwards EnterpriseOne mappato. Crea inoltre alias che rappresentano i membri dei ruoli JD Edwards EnterpriseOne mappati.

È possibile creare un account utente per ogni alias creato.

Tuttavia, se si utilizzano più sistemi e gli utenti dispongono di account su più di un sistema, è possibile assegnare a ciascun utente un alias con lo stesso nome prima di creare gli account nella piattaforma BI.

In questo modo viene ridotto il numero di account creati per lo stesso utente nella piattaforma BI.

Ad esempio, se si utilizza un ambiente di verifica e un ambiente di produzione JD Edwards EnterpriseOne e 30 utenti possono accedere ad entrambi gli ambienti, per tali utenti verranno creati solo 30 account.

Se si decide di non assegnare un alias con lo stesso nome a ciascun utente, verranno creati 60 account per i 30 utenti nella piattaforma BI.

Tuttavia, se vengono eseguiti più sistemi e i nomi utente coincidono, è necessario creare un nuovo account del membro per ciascun alias creato.

Ad esempio, se si utilizza l'ambiente di verifica con l'account utente di Roberto Antinori (nome utente "rantinori") e l'ambiente di produzione con l'account utente di Renato Antinori (nome utente " rantinori"), è necessario creare un account diverso per ogni alias dell'utente. In caso contrario, i due utenti verranno aggiunti allo stesso account della piattaforma BI e non potranno accedere alla piattaforma BI con le proprie credenziali JD Edwards EnterpriseOne.

9.7.3.1 Mappatura di un ruolo JD Edwards EnterpriseOne

1. Eseguire l'accesso alla console CMC (Central Management Console) come amministratore.
2. Fare clic su "Autenticazione" nell'area **Gestisci**.
3. Fare doppio clic su **JD Edwards EnterpriseOne**.
4. Nell'area **Nuove opzioni di alias**, selezionare una delle seguenti opzioni:

- **Assegna ogni alias aggiunto a un account con lo stesso nome**

Selezionare questa opzione se si utilizzano più sistemi JD Edwards EnterpriseOne Enterprise con utenti che dispongono di account su più sistemi (due utenti non possono avere lo stesso nome utente per sistemi diversi).

- **Crea un nuovo account per ogni alias aggiunto**

Selezionare questa opzione se si utilizza solo un sistema JD Edwards EnterpriseOne, se la maggior parte degli utenti dispone di account su uno solo dei sistemi utilizzati oppure se i nomi utente di diversi utenti coincidono su due o più dei sistemi in esecuzione.

5. Nell'area **Opzioni di aggiornamento**, selezionare una delle seguenti opzioni:

- **Nuovi alias verranno aggiunti e nuovi utenti verranno creati**

Selezionare questa opzione per creare un nuovo alias per ciascun utente mappato nella piattaforma BI. Se è stata selezionata l'opzione Crea nuovo account per ogni alias aggiunto, verranno aggiunti nuovi account per gli utenti senza account della piattaforma BI o per tutti gli utenti.

- **Non verranno aggiunti nuovi alias e non verranno creati nuovi utenti**

Selezionare questa opzione se il ruolo che si desidera mappare contiene molti utenti, ma solo una parte di essi utilizzerà la piattaforma BI. Il sistema non crea automaticamente gli alias e gli account per gli utenti. Crea invece alias (e account, se necessario) solo per utenti che accedono alla piattaforma BI per la prima volta. Si tratta dell'opzione predefinita.

6. Nell'area **Nuove opzioni utente** specificare la modalità di creazione dei nuovi utenti.

Selezionare una delle seguenti opzioni:

- **I nuovi utenti vengono creati come utenti specifici.**

I nuovi account utente verranno configurati per utilizzare licenze utente designato. Le licenze utente designato sono associate a utenti specifici e consentono di accedere al sistema in base a nome utente e password. Ciò garantisce agli utenti specifici l'accesso al sistema a prescindere dal numero delle altre persone connesse. È necessario disporre di una licenza utente designato per ciascun account utente creato utilizzando questa opzione.

- **I nuovi utenti vengono creati come utenti simultanei.**

I nuovi account utente verranno configurati per utilizzare licenze utente simultaneo. Le licenze di accesso simultaneo specificano il numero di persone che possono connettersi alla piattaforma BI contemporaneamente. Questo tipo di licenza è estremamente flessibile, poiché una licenza di accesso simultaneo di dimensioni ridotte può supportare un'ampia base di utenti. Ad esempio, in base alla frequenza e alla durata dell'accesso alla piattaforma BI, una licenza di accesso simultaneo per 100 utenti può supportare 250, 500 o 700 utenti.

I ruoli selezionati vengono ora visualizzati come gruppi nella piattaforma BI.

7. Fare clic sulla scheda **Ruoli**.
8. In **Elenco domini** selezionare il server JD Edwards che contiene i ruoli da mappare.
9. In "Ruoli disponibili" selezionare i ruoli da mappare alla piattaforma BI e fare clic su <.
10. Fare clic su **Aggiorna**.

I ruoli verranno mappati nella piattaforma BI.

9.7.3.2 Considerazioni sulla rimappatura

Se si aggiungono utenti a un ruolo che è stato già mappato nella piattaforma BI, sarà necessario rimappare il ruolo per aggiungere gli utenti alla piattaforma BI. Quando si rimappa il ruolo, l'opzione relativa alla mappatura di utenti come utenti titolari o simultanei riguarda solamente i nuovi utenti che sono stati aggiunti al ruolo.

Ad esempio, prima si mappa un ruolo nella piattaforma BI selezionando l'opzione "I nuovi utenti vengono creati come utenti specifici", quindi si aggiungono gli utenti allo stesso ruolo e si rimappa il ruolo selezionando l'opzione "I nuovi utenti vengono creati come utenti simultanei".

In questa situazione, solo i nuovi utenti del ruolo vengono mappati nella piattaforma BI come utenti simultanei; gli utenti mappati in precedenza rimangono utenti specifici. Questo avviene anche quando gli utenti vengono prima mappati come simultanei e, in seguito, vengono modificate le impostazioni per rimappare i nuovi utenti come utenti designati.

9.7.3.3 Per eliminare la mappatura di un ruolo

1. Eseguire l'accesso alla console CMC (Central Management Console) come amministratore.
2. Fare clic su "Autenticazione" nell'area **Gestisci**.
3. Fare clic sulla scheda relativa a **JD Edwards EnterpriseOne**.
4. Nell'area "Ruoli", selezionare il ruolo che si desidera rimuovere e fare clic su <.
5. Fare clic su **Aggiorna**.

I membri del ruolo non saranno più in grado di accedere alla piattaforma BI finché non disporranno di altri account o alias.

Nota:

è inoltre possibile eliminare singoli account o rimuovere gli utenti dai ruoli prima di eseguire la mappatura nella piattaforma BI, impedendo così l'accesso a determinati utenti.

9.7.4 Pianificazione degli aggiornamenti utente

Per garantire che le modifiche ai dati utente per il sistema ERP vengano riportate nei dati utente della piattaforma BI, è possibile pianificare aggiornamenti utente regolari. Questi aggiornamenti sincronizzeranno automaticamente gli utenti ERP e la piattaforma BI in base alle impostazioni delle mappature configurate nella CMC (Central Management Console).

Sono disponibili due opzioni per l'esecuzione e la pianificazione degli aggiornamenti per i ruoli importati:

- **Aggiorna solo ruoli:** l'uso di questa opzione determina l'aggiornamento dei soli collegamenti tra i ruoli attualmente mappati importati nella piattaforma BI. Utilizzare questa opzione se si prevede di eseguire aggiornamenti frequenti e si desidera evitare problemi di utilizzo delle risorse di sistema. Se si aggiornano solo i ruoli, non vengono creati nuovi account utente.
- **Aggiorna ruoli e alias:** questa opzione determina non solo l'aggiornamento dei collegamenti tra i ruoli, ma anche la creazione di nuovi account utente nella piattaforma BI per i nuovi alias utente aggiunti al sistema ERP.

Nota:

se non è stata specificata la creazione automatica degli alias utente per gli aggiornamenti quando è stata abilitata l'autenticazione, non verranno creati account per i nuovi alias.

9.7.4.1 Pianificazione degli aggiornamenti utente

Una volta mappati i ruoli nella piattaforma BI, è necessario specificare in che modo vengono aggiornati dal sistema.

1. Fare clic sulla scheda **Aggiornamento utente**.
2. Fare clic su **Pianifica** nella sezione "Aggiorna solo ruoli" o "Aggiorna ruoli e alias".

Suggerimento:

se si desidera eseguire immediatamente un aggiornamento, fare clic su **Aggiorna ora**.

Suggerimento:

utilizzare l'opzione "Aggiorna solo ruoli" se si desidera eseguire aggiornamenti frequenti e si verificano problemi con le risorse di sistema. Il sistema impiega più tempo per aggiornare sia i ruoli che gli alias.

Viene visualizzata la finestra di dialogo "Ricorrenza".

3. Selezionare un'opzione nell'elenco "Esegui oggetto" e fornire tutte le informazioni richieste relative alla pianificazione.

Quando si pianifica un aggiornamento, è possibile scegliere tra gli schemi ricorrenti nella seguente tabella.

Criterio di ricorrenza	Descrizione
Ogni ora	L'aggiornamento verrà eseguito ogni ora. È possibile specificare l'ora di inizio nonché una data di inizio e di fine.
Giornaliero	L'aggiornamento verrà eseguito ogni giorno oppure dopo il numero di giorni specificato. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Settimanale	L'aggiornamento verrà eseguito ogni settimana. e può essere eseguito una o più volte a settimana. È possibile specificare in quali giorni e a che ora verrà eseguito nonché una data di inizio e di fine.
Mensile	L'aggiornamento verrà eseguito ogni mese oppure dopo il numero di mesi specificato. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Il N° giorno del mese	L'aggiornamento verrà eseguito in un giorno specifico del mese. È possibile specificare in quale giorno del mese e a che ora verrà eseguito nonché una data di inizio e di fine.
Il primo lunedì del mese	L'aggiornamento verrà eseguito il primo lunedì di ogni mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Ultimo giorno del mese	L'aggiornamento verrà eseguito l'ultimo giorno di ogni mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Giorno X della N° settimana del mese	L'aggiornamento verrà eseguito in un giorno specifico di una settimana specifica del mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Calendario	L'aggiornamento verrà eseguito nelle date specificate all'interno di un calendario creato in precedenza.

4. Fare clic su **Pianifica** dopo aver completato l'inserimento delle informazioni sulla pianificazione. Nella scheda **Aggiornamento utente** viene visualizzata la data del successivo ruolo pianificato.

Nota:

è sempre possibile annullare il successivo aggiornamento pianificato facendo clic su **Annulla aggiornamenti pianificati** nella sezione "Aggiorna solo ruoli" o "Aggiorna ruoli e alias".

9.8 Autenticazione Siebel

9.8.1 Abilitazione dell'autenticazione Siebel

Per fare in modo che nella piattaforma BI vengano utilizzate le informazioni di Siebel, è necessario configurare la piattaforma per l'autenticazione nel sistema Siebel.

9.8.1.1 Abilitazione dell'autenticazione Siebel nella piattaforma BI

1. Eseguire l'accesso alla console CMC (Central Management Console) come amministratore.
2. Fare clic su **Autenticazione** nell'area Gestisci.
3. Fare doppio clic su **Siebel**.
Viene visualizzata la pagina "Siebel". Nella pagina sono presenti quattro schede: **Opzioni**, **Sistemi**, **Responsabilità** e **Aggiornamento utente**.
4. Nella scheda **Opzioni** selezionare la casella di controllo **Abilita autenticazione Siebel**.
5. Apportare le modifiche appropriate in **Nuovo alias**, **Opzioni di aggiornamento** e **Nuove opzioni utente** a seconda della distribuzione della piattaforma BI. Fare clic su **Aggiorna** per salvare le modifiche prima di passare alla scheda **Sistemi**.
6. Fare clic sulla scheda **Domini**.
7. Nel campo **Nome dominio** immettere il nome del dominio del sistema Siebel con cui si desidera stabilire la connessione.
8. In **Connessione** immettere la stringa di connessione per il dominio in questione.
9. Nell'area **Nome utente** digitare un nome utente di database e una password per la piattaforma BI da utilizzare per accedere al database Siebel.
10. Nell'area **Password** immettere la password per l'utente selezionato.
11. Fare clic su **Aggiungi** per aggiungere le informazioni relative al sistema all'elenco "Domini correnti".

12. Fare clic su **Aggiorna** per salvare le modifiche.

9.8.2 Mappatura di ruoli alla piattaforma BI

La piattaforma BI crea automaticamente un gruppo per ogni ruolo Siebel mappato. Crea inoltre alias che rappresentano i membri dei ruoli Siebel mappati.

È possibile creare un account utente per ogni alias creato.

Tuttavia, se si utilizzano più sistemi e gli utenti dispongono di account su più di un sistema, è possibile assegnare a ciascun utente un alias con lo stesso nome prima di creare gli account nella piattaforma BI.

In questo modo, viene ridotto il numero degli account creati per lo stesso utente nel programma.

Ad esempio, se si utilizza un ambiente di verifica e un ambiente di produzione eBusiness Siebel e 30 utenti possono accedere ad entrambi gli ambienti, per tali utenti verranno creati solo 30 account. Se si decide di non assegnare un alias con lo stesso nome a ciascun utente, verranno creati 60 account per i 30 utenti nella piattaforma BI.

Tuttavia, se vengono eseguiti più sistemi e i nomi utente coincidono, è necessario creare un nuovo account del membro per ciascun alias creato.

Ad esempio, se si utilizza l'ambiente di verifica con l'account utente di Roberto Antinori (nome utente "rantinori") e l'ambiente di produzione con l'account utente di Renato Antinori (nome utente "rantinori"), è necessario creare un account diverso per ogni alias dell'utente. In caso contrario, i due utenti verranno aggiunti allo stesso account e non potranno accedere alla piattaforma BI con le proprie credenziali Siebel eBusiness.

9.8.2.1 Mappatura di un ruolo Siebel eBusiness alla piattaforma BI

1. Eseguire l'accesso alla CMC (Central Management Console) come amministratore.
2. Fare clic su **Autenticazione**.
3. Fare doppio clic su **Siebel**.
4. Selezionare la casella di controllo **Abilita autenticazione Siebel**.
5. Nell'area **Nuove opzioni di alias**, selezionare una delle seguenti opzioni:
 - **Assegna ogni alias aggiunto a un account con lo stesso nome**
Selezionare questa opzione se si utilizzano più sistemi Siebel eBusiness con utenti che dispongono di account in più sistemi (due utenti non possono avere lo stesso nome utente per sistemi diversi).
 - **Crea un nuovo account per ogni alias aggiunto**

Selezionare questa opzione se si utilizza solo un sistema Siebel eBusiness, se la maggior parte degli utenti dispone di account su uno solo dei sistemi utilizzati oppure se i nomi utente di diversi utenti coincidono su due o più dei sistemi in uso.

6. Nell'area **Opzioni di aggiornamento alias** selezionare una delle opzioni seguenti:

- **Crea nuovi alias all'aggiornamento dell'alias**

Selezionare questa opzione per creare un nuovo alias per ciascun utente mappato nella piattaforma BI. Se è stata selezionata l'opzione Crea nuovo account per ogni alias aggiunto, verranno aggiunti nuovi account per gli utenti senza account della piattaforma BI o per tutti gli utenti.

- **Crea nuovi alias solo all'accesso dell'utente**

Selezionare questa opzione se il ruolo che si desidera mappare contiene molti utenti, ma solo una parte di essi utilizzerà la piattaforma BI. Il programma non crea automaticamente gli alias e gli account per gli utenti. Crea invece alias (e account, se necessario) solo per utenti che accedono alla piattaforma BI per la prima volta. Si tratta dell'opzione predefinita.

7. Nell'area **Nuove opzioni utente** specificare la modalità di creazione dei nuovi utenti.

Se la licenza della piattaforma BI di cui si dispone si basa sui ruoli utente, selezionare una delle opzioni seguenti:

Selezionare una delle seguenti opzioni:

- **I nuovi utenti vengono creati come utenti designati**

I nuovi account utente verranno configurati per utilizzare licenze utente designato. Le licenze utente designato sono associate a utenti specifici e consentono di accedere al sistema in base a nome utente e password. Ciò garantisce agli utenti specifici l'accesso al sistema a prescindere dal numero delle altre persone connesse. È necessario disporre di una licenza utente designato per ciascun account utente creato utilizzando questa opzione.

- **I nuovi utenti vengono creati come utenti simultanei**

I nuovi account utente verranno configurati per utilizzare licenze utente simultaneo. Le licenze di accesso simultaneo specificano il numero di persone che possono connettersi alla piattaforma BI contemporaneamente. Questo tipo di licenza è estremamente flessibile, poiché una licenza di accesso simultaneo di dimensioni ridotte può supportare un'ampia base di utenti. Ad esempio, in base alla frequenza e alla durata dell'accesso alla piattaforma BI, una licenza di accesso simultaneo per 100 utenti può supportare 250, 500 o 700 utenti.

8. Fare clic sulla scheda **Ruoli**.

9. Selezionare il dominio che corrisponde al server Siebel per il quale si desidera mappare i ruoli.

10. In "Ruoli disponibili" selezionare i ruoli da mappare e fare clic su **>**.

Nota:

- se i ruoli sono molto numerosi, è possibile utilizzare il campo **Cerca ruoli che iniziano con:** per limitare la ricerca. Immettere i caratteri iniziali del ruolo o dei ruoli seguiti dal carattere jolly (%) e fare clic su **Cerca**.
- Per consentire il corretto funzionamento della funzionalità di ricerca, è necessario che sia distribuito un file jar di plug-in nella directory lib Tomcat: `DIRINSTALLAZ\tomcat\webapps\BOE\WEB-`

INF\lib e in DIRINSTALLAZ\SAP BusinessObjects Enterprise XI
4.0\java\lib\siebel\default\siebel. Riavviare quindi il server Tomcat e Server
Intelligence Agent.

11. Fare clic su **Aggiorna**.

I ruoli verranno mappati nella piattaforma BI.

9.8.2.2 Considerazioni sulla rimappatura

Per attivare la sincronizzazione di utenti e gruppi tra la piattaforma BI e Siebel, selezionare la casella di controllo **Imponi sincronizzazione dell'utente**.

Nota:

per selezionare **Imponi sincronizzazione utente**, è necessario selezionare prima **Verranno aggiunti nuovi alias e verranno creati nuovi utenti**.

Quando si rimappa il ruolo, l'opzione relativa alla mappatura di utenti come utenti titolari o simultanei riguarda solamente i nuovi utenti che sono stati aggiunti al ruolo.

Ad esempio, prima si mappa un ruolo nella piattaforma BI selezionando l'opzione "I nuovi utenti vengono creati come utenti specifici", quindi si aggiungono gli utenti allo stesso ruolo e si rimappa il ruolo selezionando l'opzione "I nuovi utenti vengono creati come utenti simultanei".

In questa situazione, solo i nuovi utenti del ruolo vengono mappati nella piattaforma BI come utenti simultanei; gli utenti mappati in precedenza rimangono utenti specifici. Questo avviene anche quando gli utenti vengono prima mappati come simultanei e, in seguito, vengono modificate le impostazioni per rimappare i nuovi utenti come utenti designati.

9.8.2.3 Per eliminare la mappatura di un ruolo

1. Eseguire l'accesso alla console CMC (Central Management Console) come amministratore.
2. Fare clic su "Autenticazione" nell'area **Gestisci**.
3. Fare doppio clic su **Siebel**.
4. Nella scheda **Dominio** selezionare il dominio Siebel corrispondente al ruolo o i ruoli per il quale si desidera annullare la mappatura.
5. Nella scheda **Ruoli** selezionare il ruolo che si desidera rimuovere e fare clic su <.
6. Fare clic su **Aggiorna**.

I membri della responsabilità non saranno più in grado di accedere alla piattaforma BI finché non disporranno di altri account o alias.

Nota:

è inoltre possibile eliminare singoli account o rimuovere gli utenti dai ruoli prima di eseguire la mappatura nella piattaforma BI, impedendo così l'accesso a determinati utenti.

9.8.3 Pianificazione degli aggiornamenti utente

Per garantire che le modifiche ai dati utente per il sistema ERP vengano riportate nei dati utente della piattaforma BI, è possibile pianificare aggiornamenti utente regolari. Questi aggiornamenti sincronizzeranno automaticamente gli utenti ERP e la piattaforma BI in base alle impostazioni delle mappature configurate nella CMC (Central Management Console).

Sono disponibili due opzioni per l'esecuzione e la pianificazione degli aggiornamenti per i ruoli importati:

- **Aggiorna solo ruoli:** l'uso di questa opzione determina l'aggiornamento dei soli collegamenti tra i ruoli attualmente mappati importati nella piattaforma BI. Utilizzare questa opzione se si prevede di eseguire aggiornamenti frequenti e si desidera evitare problemi di utilizzo delle risorse di sistema. Se si aggiornano solo i ruoli, non vengono creati nuovi account utente.
- **Aggiorna ruoli e alias:** questa opzione determina non solo l'aggiornamento dei collegamenti tra i ruoli, ma anche la creazione di nuovi account utente nella piattaforma BI per i nuovi alias utente aggiunti al sistema ERP.

Nota:

se non è stata specificata la creazione automatica degli alias utente per gli aggiornamenti quando è stata abilitata l'autenticazione, non verranno creati account per i nuovi alias.

9.8.3.1 Pianificazione degli aggiornamenti utente

Una volta mappati i ruoli nella piattaforma BI, è necessario specificare in che modo vengono aggiornati dal sistema.

1. Fare clic sulla scheda **Aggiornamento utente**.
2. Fare clic su **Pianifica** nella sezione "Aggiorna solo ruoli" o "Aggiorna ruoli e alias".

Suggerimento:

se si desidera eseguire immediatamente un aggiornamento, fare clic su **Aggiorna ora**.

Suggerimento:

utilizzare l'opzione "Aggiorna solo ruoli" se si desidera eseguire aggiornamenti frequenti e si verificano problemi con le risorse di sistema. Il sistema impiega più tempo per aggiornare sia i ruoli che gli alias.

Viene visualizzata la finestra di dialogo "Ricorrenza".

3. Selezionare un'opzione nell'elenco "Esegui oggetto" e fornire tutte le informazioni richieste relative alla pianificazione.

Quando si pianifica un aggiornamento, è possibile scegliere tra gli schemi ricorrenti nella seguente tabella.

Criterio di ricorrenza	Descrizione
Ogni ora	L'aggiornamento verrà eseguito ogni ora. È possibile specificare l'ora di inizio nonché una data di inizio e di fine.
Giornaliero	L'aggiornamento verrà eseguito ogni giorno oppure dopo il numero di giorni specificato. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Settimanale	L'aggiornamento verrà eseguito ogni settimana. e può essere eseguito una o più volte a settimana. È possibile specificare in quali giorni e a che ora verrà eseguito nonché una data di inizio e di fine.
Mensile	L'aggiornamento verrà eseguito ogni mese oppure dopo il numero di mesi specificato. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Il N° giorno del mese	L'aggiornamento verrà eseguito in un giorno specifico del mese. È possibile specificare in quale giorno del mese e a che ora verrà eseguito nonché una data di inizio e di fine.
Il primo lunedì del mese	L'aggiornamento verrà eseguito il primo lunedì di ogni mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Ultimo giorno del mese	L'aggiornamento verrà eseguito l'ultimo giorno di ogni mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Giorno X della N° settimana del mese	L'aggiornamento verrà eseguito in un giorno specifico di una settimana specifica del mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Calendario	L'aggiornamento verrà eseguito nelle date specificate all'interno di un calendario creato in precedenza.

4. Fare clic su **Pianifica** dopo aver completato l'inserimento delle informazioni sulla pianificazione. Nella scheda **Aggiornamento utente** viene visualizzata la data del successivo ruolo pianificato.

Nota:

è sempre possibile annullare il successivo aggiornamento pianificato facendo clic su **Annulla aggiornamenti pianificati** nella sezione "Aggiorna solo ruoli" o "Aggiorna ruoli e alias".

9.9 Autenticazione Oracle EBS

9.9.1 Abilitazione dell'autenticazione Oracle EBS

Per fare in modo che nella piattaforma BI vengano utilizzate le informazioni di Oracle EBS, è necessario configurare il sistema per l'autenticazione nel sistema Oracle EBS.

9.9.1.1 Abilitazione dell'autenticazione Oracle E-Business Suite

Prima di eseguire la procedura, è necessario distribuire i file DLL Oracle e JAR nella piattaforma BI:

1. Scaricare `ojdbc11.dll` dall'applicazione client del database Oracle.
2. Copiare il file in questa posizione:
 - Windows: `<DIRINSTALLAZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`
 - UNIX: `<DIRINSTALLAZ>/sap_bobj/enterprise_xi40/platform`
3. Scaricare `ojdbc5.jar` dall'applicazione client del database Oracle.
4. Copiare il file in questa posizione:
 - Windows: `<DIRINSTALLAZ>\Tomcat\lib`
 - UNIX: `<DIRINSTALLAZ>/sap_bobj/tomcat/lib`

1. Eseguire l'accesso alla console CMC (Central Management Console) come amministratore.
2. Fare clic su **Autenticazione** nell'area Gestisci.
3. Fare clic su **Oracle EBS**.

Viene visualizzata la pagina "Oracle EBS". Nella pagina sono presenti quattro schede: **Opzioni**, **Sistemi**, **Responsabilità** e **Aggiornamento utente**.

4. Nella scheda **Opzioni**, selezionare la casella di controllo **L'autenticazione Oracle EBS è abilitata**.
5. Apportare le modifiche appropriate in **Nuovo alias**, **Opzioni di aggiornamento** e **Nuove opzioni utente** a seconda della distribuzione della piattaforma BI. Fare clic su **Aggiorna** per salvare le modifiche prima di passare alla scheda **Sistemi**.
6. Fare clic sulla scheda **Sistemi**.
7. Nell'area "Utente di sistema Oracle EBS" digitare un nome utente di database e una password per la piattaforma BI da utilizzare per accedere al database Oracle E-Business Suite.
8. Nell'area "Servizi Oracle EBS", immettere il nome del servizio utilizzato dall'ambiente Oracle EBS e fare clic su **Aggiungi**.

9. Fare clic su **Aggiorna** per salvare le modifiche.

A questo punto è necessario mappare i ruoli Oracle EBS al sistema.

Argomenti correlati

- [Mappatura di ruoli Oracle E-Business Suite](#)

9.9.2 Mappatura dei ruoli Oracle E-Business Suite alla piattaforma BI

La piattaforma BI crea automaticamente un gruppo per ciascun ruolo Oracle E-Business Suite (EBS) mappato. Il sistema crea anche alias che rappresentano i membri dei ruoli Oracle E-Business Suite mappati.

È possibile creare un account utente per ogni alias creato. Tuttavia, se si utilizzano più sistemi e gli utenti dispongono di account su più di un sistema, è possibile assegnare a ciascun utente un alias con lo stesso nome prima di creare gli account nella piattaforma BI.

In questo modo viene ridotto il numero degli account creati per lo stesso utente nel sistema.

Ad esempio, se si utilizza un ambiente di verifica e un ambiente di produzione EBS e 30 utenti possono accedere ad entrambi gli ambienti, per tali utenti verranno creati solo 30 account. Se si decide di non assegnare un alias con lo stesso nome a ciascun utente, verranno creati 60 account per i 30 utenti nella piattaforma BI.

Tuttavia, se vengono eseguiti più sistemi e i nomi utente coincidono, è necessario creare un nuovo account del membro per ciascun alias creato.

Ad esempio, se si utilizza l'ambiente di verifica con l'account utente di Roberto Antinori (nome utente "rantinori") e l'ambiente di produzione con l'account utente di Renato Antinori (nome utente "rantinori"), è necessario creare un account diverso per ogni alias dell'utente. In caso contrario, i due utenti verranno aggiunti allo stesso account della piattaforma BI, potranno accedere al sistema con le proprie credenziali Oracle EBS e avranno accesso ai dati da entrambi i sistemi EBS.

9.9.2.1 Mappatura di ruoli Oracle E-Business Suite

1. Eseguire l'accesso alla console CMC (Central Management Console) come amministratore.
2. Fare clic su **Autenticazione** nell'area Gestisci.
3. Fare clic su **Oracle EBS**.
Nella pagina "Oracle EBS" viene visualizzata la scheda **Opzioni**.
4. Nell'area "Nuove opzioni di alias", selezionare una delle seguenti opzioni:
 - **Assegna ciascun alias Oracle EBS aggiunto a un account con lo stesso nome**

Selezionare questa opzione se si utilizzano più sistemi Oracle E-Business Suite con utenti che dispongono di account in più sistemi (e se non ci sono utenti che utilizzano lo stesso nome utente per sistemi diversi).

- **Crea un nuovo account per ciascun alias Oracle EBS aggiunto**

Selezionare questa opzione se si utilizza solo un sistema Oracle E-Business Suite, se la maggior parte degli utenti dispone di account in uno solo dei sistemi utilizzati oppure se i nomi utente di diversi utenti coincidono in due o più dei sistemi in uso.

5. Nell'area "Opzioni di aggiornamento", selezionare una delle seguenti opzioni:

- **Crea nuovi alias all'aggiornamento dell'alias**

Selezionare questa opzione per creare un nuovo alias per ciascun utente mappato nella piattaforma BI. Se è stata selezionata l'opzione **Crea un nuovo account per ciascun alias Oracle EBS aggiunto**, verranno aggiunti nuovi account per gli utenti senza account della piattaforma BI o per tutti gli utenti.

- **Crea nuovi alias solo all'accesso dell'utente**

Selezionare questa opzione se il ruolo che si desidera mappare contiene molti utenti, ma solo una parte di essi utilizzerà la piattaforma BI. La piattaforma non crea automaticamente gli alias e gli account per gli utenti. Crea invece alias (e account, se necessario) solo per utenti che accedono alla piattaforma BI per la prima volta. Si tratta dell'opzione predefinita.

6. In "Nuove opzioni utente" specificare la modalità di creazione dei nuovi utenti, quindi fare clic su **Aggiorna**.

Selezionare una delle seguenti opzioni:

- **I nuovi utenti vengono creati come utenti specifici.**

I nuovi account utente verranno configurati per utilizzare licenze utente designato. Le licenze utente designato sono associate a utenti specifici e consentono di accedere al sistema in base a nome utente e password. Ciò garantisce agli utenti specifici l'accesso al sistema a prescindere dal numero delle altre persone connesse. È necessario disporre di una licenza utente designato per ciascun account utente creato utilizzando questa opzione.

- **I nuovi utenti vengono creati come utenti simultanei.**

I nuovi account utente verranno configurati per utilizzare licenze utente simultaneo. Le licenze di accesso simultaneo specificano il numero di persone che possono connettersi alla piattaforma BI contemporaneamente. Questo tipo di licenza è estremamente flessibile, poiché una licenza di accesso simultaneo di dimensioni ridotte può supportare un'ampia base di utenti. A seconda della frequenza e della durata dell'accesso alla piattaforma, una licenza di accesso simultaneo per 100 utenti può ad esempio supportare 250, 500 o 700 utenti.

I ruoli selezionati vengono ora visualizzati come gruppi nella piattaforma BI.

7. Fare clic sulla scheda **Responsabilità**.

8. In **Servizi Oracle EBS correnti**, selezionare il servizio Oracle EBS che contiene i ruoli da mappare.

9. È possibile specificare i filtri per gli utenti Oracle EBS in "Ruoli Oracle EBS mappati".

- a. Selezionare le applicazioni che gli utenti possono utilizzare per il nuovo ruolo dall'elenco **Applicazione**.
- b. Nell'elenco **Responsabilità**, selezionare le applicazioni, le funzioni, i report e i programmi simultanei Oracle che gli utenti possono utilizzare.
- c. Nell'elenco **Gruppo di protezione** selezionare il gruppo di protezione a cui è assegnato il nuovo ruolo.
- d. Utilizzare i pulsanti **Aggiungi** ed **Elimina** in "Ruolo corrente" per modificare le assegnazioni del gruppo di protezione del ruolo.

10. Fare clic su **Aggiorna.**

I ruoli verranno mappati nella piattaforma BI.

Una volta mappati i ruoli nella piattaforma BI, è necessario specificare in che modo vengono aggiornati dal sistema.

9.9.2.1.1 Aggiornamento degli utenti e dei ruoli Oracle EBS

Dopo aver abilitato l'autenticazione Oracle EBS, è necessario pianificare ed eseguire aggiornamenti regolari sui ruoli mappati importati nella piattaforma BI. In questo modo le informazioni sui ruoli Oracle EBS aggiornate verranno riportate con precisione nella piattaforma BI.

Sono disponibili due opzioni per l'esecuzione e la pianificazione degli aggiornamenti per i ruoli Oracle EBS:

- **Aggiorna solo ruoli:** l'uso di questa opzione determina l'aggiornamento dei soli collegamenti tra i ruoli attualmente mappati importati nella piattaforma BI. Si consiglia di utilizzare questa opzione se si prevede di eseguire aggiornamenti frequenti e si verificano problemi relativi all'utilizzo delle risorse di sistema. Se si aggiornano solo ruoli Oracle EBS, non vengono creati nuovi account utente.
- **Aggiorna ruoli e alias:** questa opzione determina non solo l'aggiornamento dei collegamenti tra i ruoli, ma anche la creazione di nuovi account utente nella piattaforma BI per gli alias utente aggiunti ai ruoli nel sistema Oracle EBS.

Nota:

se non è stata specificata la creazione automatica degli alias utente per gli aggiornamenti quando è stata abilitata l'autenticazione Oracle EBS, non verranno creati account per i nuovi alias.

9.9.2.1.2 Pianificazione degli aggiornamenti per i ruoli Oracle EBS

Una volta mappati i ruoli nella piattaforma BI, è necessario specificare in che modo vengono aggiornati dal sistema.

1. Fare clic sulla scheda **Aggiornamento utente**.
2. Fare clic su **Pianifica** nella sezione "Aggiorna solo ruoli" o "Aggiorna ruoli e alias".

Suggerimento:

Se si desidera eseguire immediatamente un aggiornamento, fare clic su **Aggiorna ora**.

Suggerimento:

Utilizzare l'opzione "Aggiorna solo ruoli" se si desidera eseguire aggiornamenti frequenti e si verificano problemi con le risorse di sistema. Il sistema impiega più tempo per aggiornare sia i ruoli che gli alias.

Viene visualizzata la finestra di dialogo "Ricorrenza".

3. Selezionare un'opzione dall'elenco a discesa "Esegui oggetto" e fornire tutte le informazioni richieste relative alla pianificazione nei campi disponibili.

Quando si pianifica un aggiornamento, è possibile scegliere tra gli schemi ricorrenti nella seguente tabella.

Criterio di ricorrenza	Descrizione
Ogni ora	L'aggiornamento verrà eseguito ogni ora. È possibile specificare l'ora di inizio nonché una data di inizio e di fine.
Giornaliero	L'aggiornamento verrà eseguito ogni giorno oppure dopo il numero di giorni specificato. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Settimanale	L'aggiornamento verrà eseguito ogni settimana. Può essere eseguito una o più volte a settimana. È possibile specificare in quali giorni e a che ora verrà eseguito nonché una data di inizio e di fine.
Mensile	L'aggiornamento verrà eseguito ogni mese oppure dopo il numero di mesi specificato. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Il N° giorno del mese	L'aggiornamento verrà eseguito in un giorno specifico del mese. È possibile specificare in quale giorno del mese e a che ora verrà eseguito nonché una data di inizio e di fine.
Il primo lunedì del mese	L'aggiornamento verrà eseguito il primo lunedì di ogni mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Ultimo giorno del mese	L'aggiornamento verrà eseguito l'ultimo giorno di ogni mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Giorno X della N° settimana del mese	L'aggiornamento verrà eseguito in un giorno specifico di una settimana specifica del mese. È possibile specificare l'ora in cui verrà eseguito nonché una data di inizio e di fine.
Calendario	L'aggiornamento verrà eseguito nelle date specificate all'interno di un calendario creato in precedenza.

4. Fare clic su **Pianifica** dopo aver completato l'inserimento delle informazioni sulla pianificazione. Nella scheda **Aggiornamento utente** viene visualizzata la data del successivo ruolo pianificato.

Nota:

è sempre possibile annullare il successivo aggiornamento pianificato facendo clic su **Annulla aggiornamenti pianificati** nella sezione "Aggiorna solo ruoli" o "Aggiorna ruoli e alias".

9.9.3 Eliminazione mappatura ruoli

Per impedire a determinati gruppi di utenti di accedere alla piattaforma BI, è possibile eliminare la mappatura dei ruoli ai quali appartengono.

9.9.3.1 Per eliminare la mappatura di un ruolo

1. Eseguire l'accesso alla console CMC (Central Management Console) come amministratore.
2. Fare clic su **Autenticazione** nell'area Gestisci.
3. Fare doppio clic sul nome del sistema ERP di cui si desidera annullare la mappatura dei ruoli. Nella pagina del sistema ERP viene visualizzata la scheda **Opzioni**.
4. Fare clic sulla scheda **Responsabilità**.
5. Selezionare **Servizi Oracle EBS correnti**.
6. In "Ruolo corrente" selezionare un ruolo, quindi fare clic sul pulsante **Elimina**.
7. Fare clic su **Aggiorna**.

I membri del ruolo non saranno più in grado di accedere alla piattaforma BI finché non disporranno di altri account o alias.

Nota:

è inoltre possibile eliminare singoli account o rimuovere gli utenti dai ruoli prima di eseguire la mappatura nella piattaforma BI, impedendo così l'accesso a determinati utenti.

9.9.4 Personalizzazione dei diritti per gruppi e utenti Oracle EBS mappati

Quando si mappano ruoli alla piattaforma BI, è possibile impostare i diritti o concedere autorizzazioni per i gruppi e gli utenti creati.

9.9.4.1 Per assegnare i diritti di amministrazione

Per consentire agli utenti di gestire la piattaforma BI, è necessario renderli membri del gruppo Amministratori predefinito. I membri di questo gruppo hanno il pieno controllo di tutti gli aspetti del sistema, quali account, server, cartelle, oggetti, impostazioni e altro ancora.

1. Eseguire l'accesso alla Central Management Console come amministratore.
2. Nell'area "Organizza" fare clic su **Utenti e gruppi**.
3. Nella colonna "Nome" fare clic con il pulsante destro del mouse su **Amministratori** e scegliere **Aggiungi membri a gruppi**.
Viene visualizzata la pagina "Utenti o gruppi disponibili".
4. Dall'area **Elenco utenti** o **Elenco gruppi**, selezionare il ruolo mappato al quale si desidera concedere diritti amministrativi.
5. Fare clic su **>** per rendere il ruolo un sottogruppo del gruppo Administrators, quindi fare clic su **OK**.

I membri del ruolo dispongono ora di diritti di amministrazione nella piattaforma BI.

Nota:

È anche possibile creare un ruolo in Oracle EBS, aggiungere a tale ruolo gli utenti appropriati, mappare il ruolo nella piattaforma BI e rendere il ruolo mappato un sottogruppo del gruppo Amministratori predefinito, concedendo così i diritti amministrativi ai membri del ruolo.

9.9.4.2 Per assegnare i diritti di pubblicazione

Se nel sistema utilizzato sono presenti utenti designati come creatori di contenuti all'interno dell'organizzazione, è possibile concedere loro le autorizzazioni per la pubblicazione di oggetti nella piattaforma BI.

1. Eseguire l'accesso alla console CMC (Central Management Console) come amministratore.
2. Dall'area "Organizza", fare clic su **Cartelle**.
3. Accedere alla cartella nella quale gli utenti sono autorizzati ad aggiungere oggetti.
4. Fare clic su **Gestisci, Protezione livello principale**, quindi su **Tutte le cartelle**.
5. Fare clic su **Aggiungi principali**.
Viene visualizzata la finestra Aggiungi principali.
6. Nell'elenco **Utenti o gruppi disponibili** selezionare il gruppo che include i membri ai quali si desidera concedere i diritti di pubblicazione.
7. Fare clic su **>** per consentire ai gruppi di accedere alla cartella, quindi fare clic su **Aggiungi e assegna protezione**.
Viene visualizzata la pagina Assegna protezione.
8. Nell'elenco **Livelli di accesso disponibili** selezionare il livello di accesso desiderato e fare clic su **>** per assegnare esplicitamente il livello di accesso.
9. Se le opzioni **Eredita da cartella principale** ed **Eredita da gruppo principale** sono selezionate, deselezionarle e fare clic su **Applica**.

10. Fare clic su OK.

I membri dei ruoli dispongono ora delle autorizzazioni per aggiungere oggetti nella cartella e in tutte le relative sottocartelle. Per rimuovere le autorizzazioni assegnate, selezionare un gruppo e fare clic su **Rimuovi**.

9.9.5 Configurazione del Single Sign On (SSO) per SAP Crystal Reports e Oracle EBS

Per impostazione predefinita, la piattaforma BI verrà configurata in modo da consentire agli utenti di SAP Crystal Reports di accedere ai dati di Oracle EBS mediante il Single Sign On (SSO).

9.9.5.1 Disattivazione di SSO per Oracle EBS e SAP Crystal Reports

1. Nella CMC (Central Management Console), fare clic su **Applicazioni**.
2. Fare doppio clic su **Configurazione di Crystal Reports**.
3. Fare clic su **Opzioni Single Sign On**.
4. Selezionare **crdb_oraapps**.
5. Fare clic su **Rimuovi**.
6. Fare clic su **Salva e chiudi**.
7. Accedere alla pagina "Server" nella CMC e selezionare **Servizi Crystal Reports**.
8. Fare clic sul pulsante **Riavvia server**.

9.9.5.2 Riattivazione di SSO per Oracle EBS e SAP Crystal Reports

Seguire la procedura riportata di seguito per riattivare SSO per Oracle EBS e SAP Crystal Reports.

1. Nella CMC (Central Management Console) fare clic su **Applicazioni**.
2. Fare doppio clic su **Configurazione di Crystal Reports**.
3. Fare clic su **Opzioni Single Sign On**.
4. In "Utilizza il contesto SSO per accedere al database con i driver seguenti" digitare **crdb_oraapps**.
5. Fare clic su **Aggiungi**.
6. Fare clic su **Salva e chiudi**.
7. Accedere alla pagina "Server" nella CMC e selezionare **Servizi Crystal Reports**.
8. Fare clic sul pulsante **Riavvia server**.

Amministrazione del server

10.1 Utilizzo dell'area di gestione Server della console CMC

L'area di gestione Server della console CMC è lo strumento principale per i task di gestione dei server. Viene fornito un elenco di tutti i server della distribuzione. Per la maggior parte dei task di gestione e configurazione, è necessario selezionare un server nell'elenco e scegliere un comando dal menu Gestisci o Azioni.

Informazioni sull'albero di spostamento

L'albero di spostamento sul lato sinistro dell'area di gestione Server offre diversi modi per visualizzare l'elenco Server. Selezionare gli elementi nell'albero di spostamento per modificare le informazioni visualizzate nel riquadro "Dettagli".

Opzione dell'albero di spostamento	Descrizione
Elenco Server	Viene visualizzato un elenco completo di tutti i server nella distribuzione.
Elenco gruppi server	Visualizza un elenco semplice di tutti i gruppi di server disponibili nel riquadro Dettagli. Selezionare questa opzione per configurare la protezione o le impostazioni dei gruppi server.
Gruppi server	Vengono elencati i gruppi server e i server in ogni gruppo. Quando si seleziona un gruppo di server, i relativi server e gruppi vengono visualizzati nel riquadro Dettagli in una vista gerarchica.
Nodi	Viene visualizzato un elenco dei nodi presenti nella distribuzione. I nodi vengono configurati in CCM. È possibile selezionare un nodo facendo clic su di esso per visualizzare o gestire i relativi server.

Opzione dell'albero di spostamento	Descrizione
<p>Categorie di servizio</p>	<p>Viene fornito un elenco dei tipi di servizi disponibili nella distribuzione. Le categorie di servizio si suddividono in servizi della piattaforma BI principali e servizi associati a componenti SAP Business Objects specifici. Di seguito sono elencate le categorie di servizio:</p> <ul style="list-style-type: none"> • Servizi di connessione • Servizi principali • Servizi Crystal Reports • Servizi Data Federation • Servizi Lifecycle Management • Servizi Analysis • Servizi Web Intelligence • Servizi Dashboard Design <p>Selezionare una categoria di servizio nell'elenco di navigazione per visualizzare o gestire i relativi server.</p> <p>Nota: un server può ospitare servizi appartenenti a più categorie di servizio. È quindi possibile che un server venga visualizzato in diverse categorie di servizio.</p>
<p>Stato server</p>	<p>Vengono visualizzati i server in base al relativo stato corrente. Si tratta di uno strumento importante per individuare i server in esecuzione e quelli interrotti. Se le prestazioni del sistema non sono ottimali, è possibile utilizzare l'elenco "Stato server" per determinare rapidamente gli eventuali server che presentano uno stato anomalo. Gli stati del server includono:</p> <ul style="list-style-type: none"> • Interrotto • Avvio in corso • Inizializzazione in corso • In esecuzione • Interruzione • Avviato con errori • Terminato in errore • In attesa delle risposte (per informazioni dettagliate, vedere Gestione delle connessioni di database di sistema CMS)

Informazioni sul riquadro Dettagli

A seconda delle opzioni selezionate nell'albero di navigazione, il riquadro "Dettagli" sul lato destro dell'area di gestione Server mostra un elenco di server, gruppi server, stati, categorie o nodi. Nella seguente tabella vengono descritte le informazioni elencate per i server nel riquadro "Dettagli".

Nota:

per nodi, gruppi server, categorie e stati, il riquadro "Dettagli" mostra in genere nomi e descrizioni.

Colonna del riquadro Dettagli	Descrizione
Nome server o Nome	Visualizza il nome del server.
Stato	Visualizza lo stato corrente del server. È possibile ordinare in base allo stato del server utilizzando l'elenco "Stato server" nell'albero di navigazione. Gli stati del server includono: <ul style="list-style-type: none"> • Interrotto • Avvio in corso • Inizializzazione in corso • In esecuzione • Interruzione • Avviato con errori • Terminato in errore • In attesa delle risorse
Attivato	Indica se il server è abilitato o meno.
Non aggiornato	Se il server è contrassegnato come Non aggiornato , è necessario riavviarlo. Ad esempio, se si modificano determinate impostazioni del server nella schermata "Proprietà del server", potrebbe essere necessario riavviare il server per rendere effettive le modifiche.
Tipo	Visualizza il tipo di server.
Nome host	Visualizza il nome host del server.

Colonna del riquadro Dettagli	Descrizione
Stato	<p>Indica lo stato generale del server.</p> <p>Gli stati del server includono:</p> <ul style="list-style-type: none"> • Verde (integro) • Ambra (attenzione) • Rosso (pericolo) <p>Lo stato di integrità di un server dipende direttamente dallo stato del controllo del server. Lo stato di integrità del Central Management Server dipende ad esempio dallo stato di <NOMENODO>.CentralManagementServer Watch.</p> <p>È possibile accedere ai dettagli dei controlli nella pagina "Monitoraggio" della CMC: nella scheda "Elenco di controlli" selezionare il controllo e fare clic su Modifica. Vengono visualizzate la "Regola di attenzione" e la "Regola di pericolo" del controllo, mappate rispettivamente agli stati di integrità giallo e rosso.</p>
PID	Visualizza il numero ID di processo univoco del server.
Descrizione	Visualizza una descrizione del server. È possibile modificare questa descrizione nella pagina "Proprietà del server".
Data ultima modifica	Visualizza la data dell'ultima modifica apportata al server o dell'ultima modifica dello stato del server. Questa colonna è molto utile per verificare lo stato dei server modificati di recente.

Argomenti correlati

- [Gestione di gruppi di server](#)
- [Utilizzo dei nodi](#)
- [Visualizzazione dello stato dei server](#)
- [Avvio, arresto e riavvio dei server](#)
- [Per modificare le proprietà di un server](#)

10.2 Gestione dei server mediante gli script in Windows

Il file eseguibile `ccm.exe` consente di avviare, arrestare, riavviare, abilitare e disabilitare i server nella distribuzione Windows mediante la riga di comando.

Argomenti correlati

- [ccm.exe](#)

10.3 Gestione dei server in Unix

Il file eseguibile `ccm.sh` consente di avviare, arrestare, riavviare, abilitare e disabilitare i server nella distribuzione Unix mediante la riga di comando.

Argomenti correlati

- [ccm.sh](#)

10.4 Visualizzazione e modifica dello stato del server

10.4.1 Visualizzazione dello stato dei server

Lo stato di un server è lo stato operativo corrente: un server può essere in esecuzione, in avvio, in arresto, arrestato, non riuscito, in stato di inizializzazione, avviato con errori o in attesa di risorse. Per rispondere alle richieste della piattaforma BI, un server deve essere in esecuzione e abilitato. Un server disabilitato è ancora in esecuzione come processo; tuttavia, non accetta richieste dal resto della piattaforma BI. Un server in arresto non è più in esecuzione come processo.

In questa sezione viene illustrato come modificare lo stato dei server utilizzando la console CMC.

Argomenti correlati

- [Per visualizzare lo stato di un server](#)
- [Per visualizzare lo stato dei servizi](#)
- [Avvio, arresto e riavvio dei server](#)
- [Abilitazione e disabilitazione dei server](#)
- [Arresto di Central Management Server](#)
- [Per avviare automaticamente un server](#)

10.4.1.1 Per visualizzare lo stato di un server

1. Passare all'area di gestione "Server" della CMC.

Nel riquadro "Dettagli" sono visualizzate le categorie di servizi della distribuzione.

2. Per visualizzare l'elenco dei server di un gruppo di server, un nodo o una categoria di servizi specifici, selezionare il gruppo, il nodo o la categoria nell'albero di spostamento.

Nel riquadro "Dettagli" viene visualizzato l'elenco dei server nella propria distribuzione. La colonna **Stato** indica lo stato di ciascun server nell'elenco.

3. Per visualizzare un elenco di tutti i server con uno stato particolare, espandere l'opzione **Stato server** nella struttura di spostamento e selezionare lo stato desiderato.

Nel riquadro Dettagli viene visualizzato un elenco dei server aventi lo stato selezionato.

Nota:

Questo può essere particolarmente utile per visualizzare rapidamente un elenco di server che non si avviano correttamente o si sono arrestati in modo imprevisto.

Argomenti correlati

- [Per visualizzare lo stato dei servizi](#)

10.4.1.2 Per visualizzare lo stato dei servizi

In caso di errore di un servizio, lo stato del server host viene impostato su "Avviato con errori" (a indicare che almeno un servizio è stato avviato correttamente) o su "Non riuscito" (a indicare che nessuno dei servizi è stato avviato correttamente). È possibile visualizzare gli stati del server nella CMC e in CCM. Tuttavia, è anche possibile visualizzare lo stato di singoli servizi nella pagina "Proprietà" del server nella CMC.

1. Passare all'area di gestione "Server" della CMC.

Nel riquadro "Dettagli" sono visualizzate le categorie di servizi della distribuzione.

2. Per visualizzare l'elenco dei server di un gruppo di server, un nodo o una categoria di servizi specifici, selezionare il gruppo, il nodo o la categoria nell'albero di spostamento.

Nel riquadro "Dettagli" viene visualizzato l'elenco dei server nella propria distribuzione.

3. Fare doppio clic su un server per aprirne la pagina "Proprietà".

Nella pagina "Proprietà" vengono visualizzate le proprietà del server e dei servizi che ospita. Per i servizi in errore vengono visualizzati anche i messaggi di errore.

Argomenti correlati

- [Visualizzazione dello stato dei server](#)

10.4.2 Avvio, arresto e riavvio dei server

L'avvio, l'interruzione e il riavvio dei server sono azioni comuni che vengono eseguite quando si configurano server o si disattiva la modalità in linea. Se si desidera modificare il nome di un server, è necessario innanzitutto arrestare il server. Una volta apportate le modifiche, occorre riavviare il server per renderle effettive. Se si apportano modifiche alle impostazioni di configurazione di un server, sulla console CMC verrà visualizzato un prompt in cui viene chiesto di riavviare il server.

Nella parte restante della sezione viene indicato quando una determinata modifica alla configurazione richiede l'interruzione e il riavvio del server. Tuttavia, poiché queste attività sono estremamente frequenti, vengono descritti per primi i concetti e le differenze, quindi vengono indicate le procedure generali per riferimento.

Azione	Descrizione
Arresto di un server	Può essere necessario arrestare i server della piattaforma BI prima di poter modificare alcune proprietà e impostazioni.
Avvio di un server	Se si è arrestato un server per configurarlo, per rendere effettive le modifiche è necessario riavviarlo prima che riprenda l'elaborazione delle richieste.
Riavvio di un server	Riavviare un server è un'azione più rapida che arrestare un server completamente per poi avviarlo di nuovo. Se è necessario riavviare un server dopo averne modificato un'impostazione, viene visualizzato un prompt sulla console CMC.
Avvio automatico di un server	È possibile impostare i server per l'avvio automatico all'avvio di Server Intelligence Agent.

Azione	Descrizione
Forza terminazione	Arresta il server immediatamente (mentre quando è l'utente ad arrestarlo, il server si arresta solo dopo avere completato le attività di elaborazione correnti). Arrestare forzatamente un server solo quando l'arresto del server non è riuscito ed è necessario arrestarlo immediatamente.

Suggerimento:

Quando si interrompe (o riavvia) un server, si interrompe anche il processo del server, arrestando completamente il server. Prima di arrestare un server, si consiglia di

- disabilitare il server in modo che possa terminare l'elaborazione di eventuali processi in corso e
- assicurarsi che non siano rimasti in coda eventi di controllo. Per visualizzare il numero di eventi di controllo rimasti in coda, passare alla schermata "Metriche" del server e visualizzare la metrica "Numero corrente degli eventi di controllo in coda".

Argomenti correlati

- [Abilitazione e disabilitazione dei server](#)

10.4.2.1 Avvio, arresto o riavvio dei server con la console CMC

1. Passare all'area di gestione "Server" della CMC.

Nel riquadro "Dettagli" sono visualizzate le categorie di servizi della distribuzione.

2. Per visualizzare un elenco dei server di un gruppo di server, un nodo o una categoria di servizi specifici, selezionare il gruppo, il nodo o la categoria nel pannello di spostamento.

Nel riquadro "Dettagli" viene visualizzato un elenco di server.

3. Per visualizzare un elenco di tutti i server con uno stato particolare, espandere l'opzione **Stato server** nella struttura di spostamento e selezionare lo stato desiderato.

Nel riquadro "Dettagli" viene visualizzato un elenco dei server aventi lo stato selezionato.

Nota:

Questo può essere particolarmente utile per visualizzare rapidamente un elenco di server che non si avviano correttamente o si sono arrestati in modo imprevisto.

4. Fare clic con il pulsante destro del mouse sul server di cui si desidera modificare lo stato e, a seconda dell'azione che si intende eseguire, scegliere **Avvia server**, **Riavvia server**, **Arresta server** o **Forza terminazione**.

Argomenti correlati

- [Visualizzazione dello stato dei server](#)

10.4.2.2 Per avviare, interrompere o riavviare un server Windows con il CCM

1. In CCM, fare clic sul pulsante **Gestisci server** nella barra degli strumenti.
2. Quando viene richiesto, accedere al CMS con un account di amministratore.
3. Nella finestra di dialogo "Gestisci server", selezionare il server da avviare, interrompere o riavviare.
4. Fare clic su **Avvia**, **Arresta**, **Riavvia** o **Imponi chiusura**.
5. Fare clic su **Chiudi** per tornare a CCM.

10.4.2.3 Per avviare automaticamente un server

Per impostazione predefinita, i server della distribuzione vengono avviati automaticamente all'avvio di Server Intelligence Agent. Questa attività mostra dove impostare l'opzione di avvio automatico.

1. Passare all'area di gestione "Server" della CMC.
2. Fare doppio clic sul server da avviare automaticamente.
Viene visualizzata la schermata "Proprietà".
3. In "Impostazioni comuni" selezionare la casella di controllo **Avvia automaticamente questo server all'avvio di Server Intelligence Agent** e fare clic su **Salva** o su **Salva e chiudi**.

Nota:

Se la casella di controllo **Avvia automaticamente questo server all'avvio di Server Intelligence Agent** è deselezionata per tutti i CMS del cluster, è necessario riavviare il sistema con CCM. Dopo aver utilizzato CCM per arrestare l'agente SIA, fare clic con il pulsante destro del mouse su tale agente e scegliere **Proprietà**. Nella scheda **Avvio** fare clic su **Proprietà** per aprire la pagina Proprietà server per il CMS. Selezionare **Avvio automatico**, fare clic su **OK** per chiudere la pagina Proprietà server e quindi di nuovo su **OK**. Riavviare il SIA. L'opzione **Avvio automatico** è disponibile solo se la casella di controllo **Avvia automaticamente questo server all'avvio di Server Intelligence Agent** è deselezionata per tutti i CMS del cluster.

10.4.3 Arresto di Central Management Server

Se l'installazione della piattaforma BI prevede più Central Management Server (CMS) attivi, è possibile spegnere un singolo CMS senza perdere dati o influire sul funzionamento del sistema. Un altro server CMS nel nodo acquisirà il carico di lavoro del server arrestato. Il clustering di più CMS consente di eseguire la manutenzione sui singoli Central Management Server in sequenza senza arrestare la piattaforma BI.

Tuttavia, se la distribuzione della piattaforma BI prevede un solo CMS e questo viene arrestato, la piattaforma non sarà disponibile per gli utenti e l'elaborazione di report e programmi verrà interrotta. Per evitare questo problema, il Server Intelligence Agent di ogni nodo assicura che almeno un server CMS sia sempre in esecuzione. È comunque possibile arrestare un server CMS arrestando il relativo agente SIA, ma prima di arrestare l'agente SIA è necessario disabilitare i server di elaborazione mediante la console CMC in modo che possano terminare gli eventuali processi in esecuzione prima dell'arresto della piattaforma BI, a causa del quale anche tutti gli altri server nel nodo verranno arrestati.

Nota:

È possibile che si verifichino situazioni in cui il server CMS è stato arrestato e occorre riavviare il sistema da CCM. Ad esempio, se si arrestano tutti i CMS di un nodo e al momento dell'avvio dell'agente SIA la casella di controllo **Avvia automaticamente questo server all'avvio di Server Intelligence Agent** è deselezionata per tutti i CMS del cluster, è necessario riavviare il sistema con CCM. In CCM fare clic con il pulsante destro del mouse sull'agente SIA e scegliere **Proprietà**. Nella scheda **Avvio** fare clic su **Proprietà** per aprire la pagina Proprietà server per il CMS. Selezionare **Avvio automatico**, fare clic su **OK** per chiudere la pagina Proprietà server e quindi di nuovo su **OK**. Riavviare il SIA. L'opzione **Avvio automatico** è disponibile solo se la casella di controllo **Avvia automaticamente questo server all'avvio di Server Intelligence Agent** è deselezionata per tutti i CMS del cluster.

Se si desidera configurare il sistema in modo da poter avviare e arrestare il server CMS nel cluster senza avviare e arrestare altri server, inserire il CMS in un altro nodo. Creare un nuovo nodo e duplicare il server CMS sul nodo. Con il CMS sul rispettivo nodo, è possibile arrestare con semplicità il nodo senza influenzare altri server.

Argomenti correlati

- [Utilizzo dei nodi](#)
- [Duplicazione di server](#)
- [Cluster di Central Management Server](#)

10.4.4 Abilitazione e disabilitazione dei server

Quando si disabilita un server della piattaforma BI, si evita che tale server riceva e risponda a nuove richieste della piattaforma BI, senza tuttavia arrestarne realmente il processo. Questa possibilità si rivela utile se si desidera consentire a un server di portare a termine l'elaborazione di tutte le richieste correnti prima che venga interrotto del tutto.

Ad esempio, può verificarsi la necessità di interrompere un Job Server prima di riavviare il computer in cui è in esecuzione. Tuttavia, si desidera che il server soddisfi prima tutte le richieste di report in coda. In questo caso, si disabilita il Job Server in modo che non possa accettare altre richieste. Quindi,

utilizzare Central Management Console per verificare quando il server completa i processi in corso (Nell'area di gestione "Server", fare clic con il pulsante destro del mouse sul server e scegliere "Metrica"). Quindi, una volta terminata l'elaborazione delle richieste correnti, si può arrestare il server in modo sicuro.

Nota:

- il server CMS deve essere in esecuzione affinché sia possibile abilitare e/o disabilitare gli altri server.
- Non è possibile abilitare o disabilitare un server CMS.

10.4.4.1 Abilitazione e disabilitazione dei server con la console CMC

1. Passare all'area di gestione "Server" della CMC.
2. Fare clic con il pulsante destro del mouse sul server di cui si desidera modificare lo stato e, in base all'azione che si intende eseguire, fare clic su **Abilita server** oppure su **Disabilita server**.

10.4.4.2 Per abilitare o disabilitare un server Windows con CCM.

1. In CCM, fare clic su **Gestisci server**.
2. Quando richiesto, accedere al CMS con le credenziali che garantiscono privilegi amministrativi per la piattaforma BI.
3. Nella finestra di dialogo "Gestione server", selezionare il server che si desidera abilitare o disabilitare.
4. Fare clic su **Abilita** o su **Disabilita**.
5. Fare clic su **Chiudi** per tornare a CCM.

10.5 Aggiunta, duplicazione o eliminazione di server

10.5.1 Aggiunta, duplicazione ed eliminazione di server

Se si desidera aggiungere nuovo hardware alla piattaforma BI installando componenti server su nuovi computer supplementari, eseguire il programma di installazione della piattaforma BI su tali computer. Il programma di installazione consente di eseguire un'installazione personalizzata. Durante l'installazione personalizzata, specificare il server CMS per la distribuzione esistente e selezionare i componenti che

si desidera installare sul computer locale. Per informazioni dettagliate sulle opzioni di installazione personalizzata, consultare il *Manuale d'installazione della piattaforma SAP BusinessObjects Business Intelligence*.

10.5.1.1 Aggiunta di un server

È possibile eseguire più istanze dello stesso server della piattaforma BI nel medesimo computer. Per aggiungere un server:

1. Passare all'area di gestione "Server" della CMC.
2. Nel menu **Gestisci**, fare clic su **Nuovo > Nuovo server**.
Viene visualizzata la finestra di dialogo "Crea nuovo server".
3. Scegliere la **Categoria di servizio**.
4. Scegliere un tipo di servizio necessario dall'elenco **Selezionare un servizio**, quindi fare clic su **Avanti**.
5. Per aggiungere un servizio aggiuntivo al server, selezionare il servizio nell'elenco **Servizi aggiuntivi disponibili** e fare clic su **>**.

Nota:

i servizi aggiuntivi non sono disponibili per tutti i tipi di server.

6. Dopo aver aggiunto i servizi aggiuntivi desiderati, fare clic su **Avanti**.
7. Se l'architettura della piattaforma BI è composta da più nodi, scegliere il nodo in cui si desidera aggiungere il nuovo server dall'elenco **Nodo**.
8. Digitare un nome per il server nella casella **Nome server**.
Ogni server nel sistema deve avere un nome univoco. La convenzione di denominazione predefinita è *NOMENODO.tiposerver* (se esiste più di un server dello stesso tipo nel medesimo computer host, viene aggiunto un numero).
9. Se si desidera includere una descrizione per il server, digitarla nella casella **Descrizione**.
10. Se si sta aggiungendo un nuovo Central Management Server, specificare il numero di una porta nel campo **Porta server dei nomi**.
11. Fare clic su **Crea**.
Il nuovo server viene visualizzato nell'elenco dei server nell'area **Server** della CMC, ma non viene avviato né abilitato.
12. Utilizzare la CMC per avviare e abilitare il nuovo server quando si desidera che inizi a rispondere alle richieste della piattaforma BI.

Argomenti correlati

- [Server, servizi, nodi e host](#)
- [Configurazione delle impostazioni server](#)
- [Configurazione dei numeri di porta](#)
- [Visualizzazione dello stato dei server](#)

10.5.1.2 Duplicazione di server

Se si desidera aggiungere una nuova istanza di server per la distribuzione, è possibile duplicare un server esistente. Il server duplicato mantiene le impostazioni di configurazione del server originale. Può essere particolarmente utile se si desidera espandere la distribuzione e si desidera creare nuove istanze di server che utilizzano quasi tutte le stesse impostazioni di configurazione di un server esistente.

La duplicazione semplifica il processo di spostamento dei server tra nodi. Per spostare un CMS esistente in un altro nodo, è possibile duplicarlo nel nodo desiderato. Il CMS duplicato comparirà nel nuovo nodo e manterrà tutte le impostazioni di configurazione del CMS originale.

Per duplicare server è necessario fare alcune considerazioni. Se non si desidera duplicare tutte le impostazioni, è opportuno verificare il server duplicato per assicurarsi che soddisfi le esigenze. Se ad esempio si desidera duplicare un server CMS nello stesso computer, assicurarsi di modificare le impostazioni dei numeri di porta copiate dal server CMS originale al server CMS duplicato.

Nota:

- prima di duplicare i server, assicurarsi che tutti i computer della distribuzione presentino la stessa versione della piattaforma SAP BusinessObjects Business Intelligence (ed eventuali aggiornamenti, se presenti).
- è possibile duplicare i server da qualsiasi computer. È tuttavia possibile duplicare i server solo su computer in cui sono installati i binari richiesti per il server.
- Quando si duplica un server, non significa necessariamente che il nuovo server utilizzi le stesse credenziali del sistema operativo. L'account utente è controllato da Server Intelligence Agent in cui viene eseguito il server.

10.5.1.2.1 Utilizzo di segnaposto per le impostazioni del server

I segnaposto sono variabili a livello di nodo utilizzate dai server in esecuzione nel nodo. I segnaposto sono elencati in una pagina dedicata nella console CMC. Quando si fa doppio clic su un server elencato in "Server" nella console CMC, viene fornito un collegamento sul riquadro di spostamento sinistro per "Segnaposto". Nella pagina "Segnaposto" sono elencati tutti i nomi di segnaposto disponibili e i valori associati per il server selezionato. I segnaposto contengono valori di sola lettura e i nomi dei segnaposto iniziano e terminano con il carattere percentuale %.

Nota:

È sempre possibile sovrascrivere un'impostazione segnaposto con una stringa specifica nella pagina "Proprietà server" della console CMC.

Esempio:

I segnaposto sono utili per duplicare i server. Ad esempio, nel computer A, che dispone di più unità, la piattaforma BI è installata in `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0`. Quindi il segnaposto `%DefaultAuditingDir%` sarà

D:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\.

Su un altro computer, il computer B, è invece presente una sola unità disco (non esiste l'unità D) e la piattaforma BI è installata in C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0. In questo caso, il segnaposto %DefaultAuditingDir% sarà C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\.

Per duplicare Event Server dal computer A al computer B, l'utilizzo dei segnaposto per Directory temporanea di controllo garantisce il funzionamento corretto di Event Server, poiché i segnaposto si risolvono automaticamente. Se invece non si utilizzano i segnaposto, Event Server non funzionerà a meno che non si sovrascriva manualmente l'impostazione Directory temporanea di controllo.

10.5.1.2.2 Duplicazione di un server

1. Nel computer sul quale si desidera aggiungere il server duplicato, andare all'area di gestione "Server" della CMC.
2. Fare clic con il pulsante destro del mouse sul server che si desidera duplicare e selezionare **Duplica Server**.
Verrà visualizzata la finestra di dialogo "Duplica server".
3. Digitare un nome per il server nel campo **Nuovo nome server** oppure utilizzare il nome predefinito.
4. Se si sta duplicando un Central Management Server, specificare il numero di una porta nel campo **Porta server dei nomi**.
5. Nell'elenco **Duplica su nodo** scegliere il nodo in cui si desidera aggiungere il server duplicato, quindi fare clic su **OK**.

Il nuovo server verrà visualizzato nell'area di gestione "Server" della CMC.

Nota:

Anche le impostazioni dei numeri di porta vengono duplicate. In molti casi, ad esempio quando si duplica un server CMS, potrebbe essere necessario modificare il numero di porta per evitare conflitti di porte tra il server originale e il relativo duplicato.

10.5.1.3 Eliminazione di un server

1. Passare all'area di gestione "Server" della CMC.
2. Arrestare il server che si desidera eliminare.
3. Fare clic con il pulsante destro del mouse sul server e selezionare **Elimina**.
4. Quando viene richiesto di confermare l'operazione, fare clic su **OK**.

10.6 Cluster di Central Management Server

10.6.1 Cluster di Central Management Server

Se si dispone di un'implementazione della piattaforma SAP BusinessObjects Business Intelligence di grandi dimensioni o mission-critical è probabile che si desideri eseguire diversi computer CMS contemporaneamente in un cluster. Un cluster è costituito da due o più server CMS che operano insieme rispetto a un database di sistema CMS. Se si verifica un errore in un computer in cui è in esecuzione un CMS, il computer con un altro CMS continuerà a rispondere alle richieste della piattaforma BI. Questo supporto "a disponibilità elevata" garantisce che gli utenti della piattaforma BI possano accedere alle informazioni anche quando si verifica un guasto delle apparecchiature.

In questa sezione viene illustrato come aggiungere un nuovo membro del cluster CMS a un sistema di produzione già in funzione. Quando un nuovo CMS viene aggiunto a un cluster esistente, si indica al nuovo CMS di connettersi al database di sistema CMS esistente e di condividere il carico di lavoro di elaborazione con tutti gli altri computer in uso. Per informazioni sul CMS corrente, accedere all'area di gestione "Server" della CMC.

Prima di eseguire il clustering dei computer CMS, è necessario verificare che ogni server CMS sia installato in un sistema conforme ai dettagliati requisiti (inclusi i livelli di versione e di patch) per il sistema operativo, il server del database, il metodo di accesso al database, il driver di database e il client di database indicato nella Product Availability Matrix.

Inoltre, è necessario soddisfare i seguenti requisiti di clustering:

- Per garantire prestazioni ottimali, è necessario che il server del database scelto per l'hosting del database di sistema sia in grado di elaborare le query di piccole dimensioni in modo estremamente rapido. Il server CMS comunica frequentemente con il database di sistema per inviare numerose query di piccole dimensioni. Se il server di database non è in grado di elaborare queste richieste in modo tempestivo, le prestazioni della piattaforma BI verranno ridotte in modo significativo.
- Per ottenere prestazioni ottimali, eseguire ogni membro del cluster CMS in un computer con la stessa quantità di memoria e lo stesso tipo di CPU.
- Configurare ogni computer in modo simile:
 - Installare lo stesso sistema operativo, inclusa la stessa versione dei service pack e delle patch del sistema operativo.
 - Installare la stessa versione della piattaforma BI (incluse le patch, se necessario).
 - Accertarsi che ogni CMS sia connesso al database di sistema CMS nello stesso modo a prescindere dal fatto che si utilizzino driver nativi o driver ODBC. Accertarsi che i driver siano gli stessi su ogni computer e che la relativa versione sia supportata.

- Accertarsi che ogni CMS utilizzi lo stesso client del database per connettersi al relativo database di sistema e che la versione in uso sia supportata.
- Verificare che ogni CMS utilizzi lo stesso account utente e la stessa password per la connessione al database di sistema CMS. Questo account deve disporre di diritti di creazione, eliminazione e aggiornamento nel database di sistema.
- Assicurarci che i nodi in cui si trova ogni server CMS siano in esecuzione nello stesso account del sistema operativo. In Windows l'account predefinito è "LocalSystem".
- Verificare che la data e l'ora correnti siano impostati correttamente in ogni computer CMS (incluse le impostazioni dell'ora legale).
- Assicurarci che tutti i computer di un cluster (inclusi quelli che ospitano il CMS) siano impostati sulla stessa ora di sistema. Per ottenere i risultati migliori, sincronizzare i computer con un server di riferimento orario, ad esempio `time.nist.gov`, o utilizzare una soluzione di monitoraggio centrale.
- Assicurarci che in tutti i server di applicazioni Web del cluster siano installati gli stessi file WAR. Per ulteriori informazioni sulla distribuzione del file WAR, consultare il *Manuale di installazione della piattaforma SAP BusinessObjects Business Intelligence*.
- Assicurarci che ogni CMS di un cluster sia connesso alla stessa rete LAN.
- I thread fuori banda (-oobthreads) sono utilizzati dai ping e dalle notifiche di clustering. Entrambe le operazioni sono molto rapide (le notifiche sono asincrone), di conseguenza la piattaforma BI non deve più disporre di più oobthreads e viene creato un solo oobthread.

Se un cluster dispone di più di otto membri del cluster CMS, assicurarsi che la riga di comando per ogni CMS includa l'opzione `-oobthreads numCMS`, in cui `numCMS` è il numero di server CMS collegati nel cluster. Questa opzione assicura che il cluster sia in grado di gestire carichi di lavoro rilevanti. Per informazioni sulla configurazione delle righe di comando del server, consultare l'appendice sulle righe di comando del server nel *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

- Se si desidera abilitare il controllo, è necessario configurare ogni CMS affinché utilizzi lo stesso database di controllo e stabilisca la connessione a tale database nello stesso modo. I requisiti per il database di controllo sono gli stessi del database di sistema per quanto riguarda i server del database, i client, i metodi di accesso, i driver e gli ID utente.

Suggerimento:

Per impostazione predefinita, il nome di un cluster riproduce il nome host del primo CMS installato.

Argomenti correlati

- [Modifica del nome di un cluster CMS](#)

10.6.1.1 Aggiunta di un CMS a un cluster

Sono disponibili diversi modi per aggiungere un nuovo membro del cluster CMS. Eseguire la procedura appropriata:

- È possibile installare un nuovo nodo con una CMC in un nuovo computer.
- Se si dispone già di un nodo con file binari CMS, è possibile aggiungere un nuovo server CMS dalla console CMC.
- Se si dispone già di un nodo con file binari CMS, è possibile aggiungere un nuovo server CMS duplicando un server CMS esistente.

Nota:

prima di apportare qualsiasi modifica, eseguire il backup del database di sistema CMS corrente, della configurazione del server e dei contenuti di Input File Repository e di Output File Repository. Se necessario, contattare l'amministratore del database.

Argomenti correlati

- [Aggiunta di un nuovo nodo a un cluster](#)
- [Aggiunta di un server](#)
- [Duplicazione di server](#)
- [Panoramica di backup e ripristino](#)

10.6.1.2 Aggiunta di un nuovo nodo a un cluster

Quando si aggiunge un nodo, ovvero una raccolta di server della piattaforma BI gestiti da un unico Server Intelligence Agent (SIA), viene richiesto di creare un nuovo CMS o di creare il cluster del nodo in un CMS esistente.

Per aggregare un nodo a un CMS esistente, è anche possibile utilizzare il programma di installazione. Eseguire il programma di installazione e configurazione della piattaforma BI sul computer in cui si desidera installare il nuovo membro del cluster CMS. Il programma di installazione consente di eseguire un'installazione personalizzata. Durante l'installazione personalizzata, specificare il CMS esistente di cui si desidera espandere il sistema e selezionare i componenti da installare nel computer locale. In questo caso, specificare il nome del CMS in esecuzione nel sistema esistente quindi scegliere di installare un nuovo CMS nel computer locale e fornire al programma di installazione le informazioni necessarie per collegarsi al database di sistema CMS esistente. Quando programma di installazione installa il nuovo CMS nel computer locale aggiunge automaticamente il server al cluster esistente.

Nota:

Prima di creare il cluster di un nuovo nodo in un CMS esistente, se il nodo è un nuovo server, assicurarsi che l'installazione della piattaforma BI in tale server sia allo stesso livello di patch dell'ambiente esistente della piattaforma BI.

Argomenti correlati

- [Utilizzo dei nodi](#)

10.6.1.3 Aggiunta di cluster ai file delle proprietà delle applicazioni Web

Se sono stati aggiunti ulteriori CMS alla distribuzione e si utilizza un server di applicazioni Java, è necessario modificare il file `PlatformServices.properties` nella directory `\webapps\BOE\WEB-INF\config\custom` della distribuzione dell'applicazione Web.

10.6.1.3.1 Definizione delle proprietà dei cluster per l'applicazione Web BOE

1. Accedere alla cartella personalizzata contenente il file `BOE.war` nel computer che ospita le applicazioni Web.

```
<DIR_INSTALLAZ>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\.
```

Successivamente sarà necessario ridistribuire il file `BOE.war` modificato.

2. Creare un nuovo file in un editor di testo.
3. Specificare le proprietà del cluster CMS.

La proprietà `cms.clusters` consente di specificare tutti i cluster della distribuzione. I nomi dei cluster devono essere preceduti da caratteri `@` e separati da virgole. Ad esempio, `cms.clusters=@samplecluster,@samplecluster2, @samplecluster3`. Utilizzare la proprietà `cms.clusters.[nome cluster]` per specificare ciascun CMS incluso nel cluster. Ad esempio:

```
cms.clusters=@samplecluster,@samplecluster2, @samplecluster3
cms.clusters.samplecluster=cmsone:6400,cmstwo
cms.clusters.samplecluster2=cms3,cms4, cms5
cms.clusters.samplecluster3=aps05
```

Nota:

Il numero della porta è separato dal nome del CMS con i due punti e si suppone sia 6400 se non specificato.

4. Salvare il file con questo nome:
`PlatformServices.properties`
5. Riavviare il server delle applicazioni.

Le nuove proprietà vengono applicate solo dopo che l'applicazione Web `BOE` viene ridistribuita nel computer su cui è in esecuzione il server di applicazioni Web. Utilizzare `WDeploy` per ridistribuire il file `WAR` sul server di applicazioni Web. Per ulteriori informazioni sull'utilizzo di `WDeploy`, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

10.6.1.4 Modifica del nome di un cluster CMS

Questa procedura consente di modificare il nome di un cluster già installato. Dopo aver modificato il nome del cluster CMS, Server Intelligence Agent riconfigura automaticamente ogni server SAP Business Objects in modo che esegua la registrazione con il cluster CMS, piuttosto che con un solo server CMS.

Nota:

Per gli amministratori con esperienza della piattaforma BI, non è più possibile utilizzare l'opzione `-ns` sulla riga di comando del server per stabilire con quale CMS un server deve effettuare la registrazione. Questa operazione viene ora eseguita automaticamente dal SIA.

10.6.1.4.1 Per modificare il nome del cluster in Windows

1. Utilizzare CCM per interrompere Server Intelligence Agent per il nodo che contiene un Central Management Server membro del cluster di cui si desidera modificare il nome.
2. Fare clic con il pulsante destro del mouse su Server Intelligence Agent e scegliere **Proprietà**.
3. Nella finestra di dialogo Proprietà, fare clic sulla scheda **Configurazione**.
4. Selezionare la casella di controllo **Cambia nome cluster in**.
5. Digitare il nuovo nome per il cluster.
6. Fare clic su **OK**, quindi riavviare Server Intelligence Agent.

Il nome del cluster CMS viene modificato. A tutti gli altri membri del cluster CMS verrà dinamicamente notificato il nuovo nome del cluster (sebbene è possibile che siano necessari diversi minuti prima che le modifiche vengano propagate ai membri del cluster).

7. Visualizzare l'area di gestione **Server** di CMC e verificare che tutti i server restino abilitati. Se necessario, abilitare eventuali server disabilitati durante le modifiche effettuate.

10.6.1.4.2 Per modificare il nome del cluster in UNIX

Utilizzare lo script `cmsdbsetup.sh`. Per informazioni, consultare il capitolo relativo agli strumenti Unix del *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

10.7 Gestione di gruppi di server

I gruppi di server rappresentano un modo di organizzare i server della piattaforma BI che consente di semplificare le attività di gestione. In altre parole, quando si gestisce un gruppo di server, è necessario visualizzare solo un sottoinsieme di tutti i server del sistema. Inoltre, rappresentano uno strumento efficace per personalizzare la piattaforma BI al fine di ottimizzare il sistema per gli utenti situati in località diverse o per gli oggetti di tipi diversi.

Se si raggruppano i server per regione, è possibile configurare senza alcuna difficoltà impostazioni di elaborazione predefinite, pianificazioni ricorrenti e destinazioni di pianificazione appropriate agli utenti che lavorano in un particolare ufficio regionale. È possibile associare un oggetto a un singolo gruppo di server, in modo che sia sempre elaborato dagli stessi server. Inoltre, è possibile associare oggetti pianificati a un particolare gruppo di server per garantire che tali oggetti siano inviati, ad esempio, alle

stampanti e ai file server corretti. Quindi, i gruppi di server si rivelano particolarmente utili quando si gestiscono sistemi che si estendono su più località e più fusi orari.

Se i server vengono raggruppati per tipo, è possibile configurare oggetti che devono essere elaborati da server ottimizzati per gli oggetti in questione. Ad esempio, i server di elaborazione devono comunicare frequentemente con il database che contiene i dati per i report pubblicati. Se si posizionano i server di elaborazione vicino al server del database a cui devono accedere, migliorano le prestazioni del sistema e si riduce al minimo il traffico di rete. Se si disponeva di diversi report eseguiti a fronte di un database DB2, poteva essere opportuno creare un gruppo di Processing Server per l'elaborazione dei report solo a fronte del server di database DB2. Configurando i report appropriati in modo che vengano visualizzati mediante questo gruppo di server di elaborazione, si otterrebbe un miglioramento delle prestazioni del sistema per la visualizzazione di tali report.

Dopo aver creato gruppi di server, configurare oggetti perché siano utilizzati specifici gruppi di server per la pianificazione o per la visualizzazione e la modifica di report. Utilizzare l'albero di spostamento nell'area di gestione Server della console CMC per visualizzare i gruppi di server. L'opzione Elenco gruppi server visualizza un elenco di gruppi di server nel riquadro dei dettagli e l'opzione Gruppi di server consente di visualizzare i server nel gruppo.

10.7.1 Creazione di un gruppo di server

Per creare un gruppo di server, è necessario specificare il nome e la descrizione del gruppo e aggiungerli, quindi, i server.

10.7.1.1 Per creare un gruppo di server

1. Passare all'area di gestione "Server" della CMC.
2. Scegliere **Gestisci > Nuovo > Crea gruppo server**.
Verrà visualizzata la finestra di dialogo "Crea gruppo server".
3. Nel campo **Nome**, digitare un nome per il nuovo gruppo di server.
4. È possibile aggiungere altre informazioni sul gruppo di server nel campo **Descrizione**.
5. Fare clic su **OK**.
6. Nell'area di gestione "Server", fare clic su **Gruppi server** nell'albero di spostamento e selezionare il nuovo gruppo di server.
7. Scegliere **Aggiungi membri** dal menu **Azioni**.
8. Selezionare i server che si desidera aggiungere a questo gruppo, quindi fare clic su **>**.
Suggerimento:
è possibile selezionare più server utilizzando **CTRL + clic**.
9. Fare clic su **OK**.

Si torna all'area di gestione "Server" che ora elenca tutti i server aggiunti al gruppo. È possibile modificare lo stato, visualizzare le specifiche dei server e modificare le proprietà dei server del gruppo.

Argomenti correlati

- [Visualizzazione dello stato dei server](#)

10.7.2 Utilizzo di sottogruppi di server

I sottogruppi di server rappresentano un modo di ulteriore organizzazione dei server. Un sottogruppo è un gruppo di server appartenente a un altro gruppo di server.

Ad esempio, se si raggruppano i server per regione e paese, ogni gruppo regionale diventa un sottogruppo di un gruppo nazionale. Per organizzare i server in questo modo, prima di tutto creare un gruppo per ogni regione e aggiungere i server appropriati a ciascun gruppo regionale. Quindi, creare un gruppo per ogni paese e aggiungere ciascun gruppo regionale al gruppo nazionale corrispondente.

È possibile impostare i sottogruppi in due modi: modificando i sottogruppi di un gruppo di server o rendendo un gruppo di server membro di un altro gruppo. Il risultato è lo stesso, quindi utilizzare il metodo più conveniente.

10.7.2.1 Per aggiungere sottogruppi a un gruppo di server

1. Passare all'area di gestione degli "Server" della CMC.
2. Fare clic su **Gruppi server** nell'albero di spostamento e selezionare il gruppo di server a cui si desidera aggiungere i sottogruppi.
Questo sarà il gruppo principale.
3. Scegliere **Aggiungi membri** dal menu **Azioni**.
4. Fare clic su **Gruppi server** nell'albero di spostamento e selezionare i gruppi di server che si desidera aggiungere a questo gruppo, quindi fare clic su **>**.

Suggerimento:

è possibile selezionare più gruppi di server utilizzando **CTRL + clic**.

5. Fare clic su **OK**.

Si torna all'area di gestione "Server" che ora elenca i gruppi di server aggiunti al gruppo principale.

10.7.2.2 Per rendere un gruppo di server membro di un altro gruppo

1. Passare all'area di gestione degli "Server" della CMC.
2. Fare clic sul gruppo che si desidera aggiungere a un altro gruppo.
3. Scegliere **Aggiungi a un gruppo server** dal menu **Azioni**.
4. Nell'elenco **Gruppi server disponibili**, selezionare gli altri gruppi a cui si desidera aggiungere il gruppo, quindi fare clic su **>**.

Suggerimento:

è possibile selezionare più gruppi di server utilizzando **CTRL + clic**.

5. Fare clic su **OK**.

10.7.3 Modifica dell'appartenenza di gruppo di un server

È possibile modificare l'appartenenza di gruppo di un server per aggiungere rapidamente il server a qualsiasi gruppo o sottogruppo (o per rimuoverlo da esso) già stato creato nel sistema.

Ad esempio, si supponga di avere creato gruppi di server per diverse regioni. Può essere opportuno utilizzare un solo Central Management Server(CMS) per più regioni. Invece di dover aggiungere il CMS singolarmente a ogni gruppo di server regionale, è possibile fare clic sul collegamento **Membro di** del server per aggiungerlo a tutte e tre le regioni contemporaneamente.

10.7.3.1 Per modificare l'appartenenza di gruppo di un server

1. Passare all'area di gestione "Server" della CMC.
2. Fare clic con il pulsante destro del mouse sul server di cui si desidera modificare le informazioni di appartenenza e scegliere **Gruppi server esistenti**.
Nel pannello dei dettagli, l'elenco **Gruppi server disponibili** visualizza i gruppi a cui è possibile aggiungere il server. L'elenco **Membro dei gruppi di server** visualizza tutti i gruppi di server a cui appartiene il server.
3. Per modificare i gruppi di cui è membro il server, utilizzare le frecce per spostare gruppi di server tra gli elenchi, quindi fare clic su **OK**.

10.7.4 Accesso degli utenti a server e gruppi di server

È possibile utilizzare diritti per concedere l'accesso a server e gruppi di server, consentendo di eseguire attività quali l'avvio o l'arresto di server.

A seconda della configurazione del sistema e dei problemi di protezione, può essere opportuno limitare la gestione dei server all'amministratore della piattaforma BI. Tuttavia, può essere necessario fornire l'accesso alle persone che utilizzano tali server. Molte organizzazioni hanno un gruppo di esperti IT dedicato alla gestione dei server. Se il team dei server deve eseguire regolari attività di manutenzione che richiedono l'arresto e l'avvio di server, è necessario concedere i diritti relativi ai server. Può inoltre essere opportuno delegare le attività di amministrazione dei server della piattaforma BI ad altre persone oppure consentire a gruppi diversi dell'organizzazione di controllare la propria gestione server.

10.7.4.1 Per concedere l'accesso a un server o a un gruppo di server

1. Passare all'area di gestione "Server" della CMC.
2. Fare clic con il pulsante destro del mouse sul server o sul gruppo di server cui si desidera concedere l'accesso e scegliere **Protezione utente**.
3. Fare clic su **Aggiungi principali** per aggiungere gli utenti o i gruppi che si desidera possano accedere al server o al gruppo di server selezionato.

Viene visualizzata la finestra di dialogo "Aggiungi principali".

4. Selezionare l'utente o il gruppo cui si desidera consentire l'accesso al server o al gruppo di server specificato, quindi fare clic su **>**.
5. Fare clic su **Aggiungi e assegna protezione**.
6. Nella schermata "Assegna protezione", scegliere le impostazioni di protezione desiderate per il gruppo di utenti e fare clic su **OK**.

Argomenti correlati

- [Funzionamento dei diritti nella piattaforma BI](#)

10.7.4.2 Diritti degli oggetti per il Report Application Server

Per consentire agli utenti di creare o modificare i report sul Web tramite il Report Application Server (RAS), è necessario che nel sistema siano disponibili licenze di modifica report RAS. È inoltre necessario

concedere agli utenti una serie minima di diritti sugli oggetti. Quando si concedono tali diritti per un oggetto report, gli utenti possono selezionare il report come origine dati per un nuovo report o modificare il report in modo diretto:

- Visualizzare oggetti (o “Visualizzare istanze documento”, a seconda delle necessità)
- Modifica oggetti
- Aggiorna i dati del report
- Esporta i dati del report

Gli utenti devono inoltre disporre dell'autorizzazione per aggiungere oggetti ad almeno una cartella prima di poter salvare i nuovi report nella piattaforma BI.

Per garantire che gli utenti conservino la possibilità di eseguire attività aggiuntive relative ai report (come la copia, la pianificazione, la stampa e così via), è consigliabile innanzitutto assegnare il livello di accesso appropriato e aggiornare le modifiche. Quindi, impostare il livello di accesso su Avanzato e aggiungere i diritti necessari non ancora concessi. Ad esempio, se gli utenti dispongono già di diritti di visualizzazione su richiesta per un oggetto report, è possibile consentire loro di modificare il report impostando il livello di accesso su Avanzato e concedendo esplicitamente il diritto aggiuntivo Modifica oggetti.

Quando gli utenti visualizzano i report tramite il visualizzatore DHTML avanzato e il RAS, il livello di accesso Visualizzazione è sufficiente a visualizzare il report, ma, per utilizzare le funzioni di ricerca avanzate, è necessario il livello di accesso Visualizzazione su richiesta. Il diritto aggiuntivo Modifica oggetti non è necessario.

10.8 Configurazione degli Adaptive Processing Server per i sistemi di produzione

Il programma di installazione installa un solo APS (Adaptive Processing Server) per sistema host. In base alle funzionalità installate, il server APS può ospitare un numero elevato di servizi, tra cui il servizio di monitoraggio, il servizio Lifecycle Management, il servizio di analisi multidimensionale (MDAS), quello di pubblicazione e altri ancora.

Per i sistemi di produzione o di test, la procedura consigliata consiste nel creare ulteriori APS e nel configurarli in base alle specifiche esigenze aziendali.

È possibile creare ulteriori APS in due modi:

- Eseguire la Configurazione guidata del sistema.

La procedura guidata consente di definire le configurazioni di base del sistema della piattaforma BI, inclusa la configurazione degli APS in base ai modelli di distribuzione predefiniti. La configurazione degli APS fornita dalla procedura guidata è un valido punto di partenza. È comunque necessario eseguire il ridimensionamento del sistema.

La procedura guidata è disponibile nella Central Management Console (CMC). Per ulteriori informazioni sulla procedura guidata, consultare [Introduzione alla Configurazione guidata del sistema](#). Per ulteriori informazioni sui modelli di distribuzione predefiniti, consultare il documento *SAP*

BusinessObjects BI platform Deployment Templates, disponibile all'interno della procedura guidata e anche all'indirizzo <http://help.sap.com/bobip41>.

- Utilizzare la CMC per creare e configurare manualmente ulteriori APS. Per ulteriori informazioni, consultare [Aggiunta, duplicazione ed eliminazione di server](#).

Promemoria:

La selezione di un modello di distribuzione nella procedura guidata o la creazione manuale di ulteriori APS non sostituisce il ridimensionamento del sistema. Accertarsi di eseguire il ridimensionamento: <http://www.sap.com/bisizing>.

10.9 Valutazione delle prestazioni del sistema

10.9.1 Monitoraggio dei server della piattaforma BI

L'applicazione di monitoraggio consente di acquisire le metriche cronologiche e di runtime dei server della piattaforma BI per la creazione di report e notifiche. Consente inoltre agli amministratori del sistema di stabilire se i server funzionano normalmente e se i tempi di risposta sono quelli previsti.

Argomenti correlati

- [Informazioni sul monitoraggio](#)

10.9.2 Analisi delle specifiche dei server

La console CMC (Central Management Console) consente di visualizzare le metriche per i server del sistema. Tali specifiche includono informazioni generali su ciascun computer, insieme a dettagli specifici del tipo di server. La CMC consente inoltre di visualizzare le specifiche di sistema, che includono informazioni sulla versione del prodotto, il CMS e l'attività corrente del sistema.

Nota:

è possibile visualizzare solo le metriche per i server attualmente in esecuzione.

10.9.2.1 Visualizzazione delle metriche del server

1. Passare all'area di gestione "Server" della CMC.
2. Fare clic con il pulsante destro del mouse sul server di cui si desidera visualizzare le metriche, quindi scegliere **Metriche**.

Nella scheda "Metriche" viene visualizzato un elenco delle metriche del server.

Argomenti correlati

- [Per modificare le proprietà di un server](#)
- [Informazioni sull'appendice sulle metriche server](#)

10.9.3 Visualizzazione delle specifiche del sistema

Nell'area di gestione "Impostazioni" della CMC vengono visualizzate metriche di sistema contenenti informazioni generali sull'installazione della piattaforma BI. La sezione "Proprietà" include informazioni sulla versione e la build del prodotto. Riporta, inoltre, l'origine dati, il nome di database e il nome utente di database del database CMS. La sezione "Visualizza le metriche di sistema globali" indica l'attività corrente dell'account e visualizza le statistiche sui processi correnti ed elaborati. La sezione "Cluster" riporta il nome del CMS a cui si è connessi, il nome del cluster CMS e i nomi degli altri membri del cluster.

10.9.3.1 Visualizzazione delle metriche del sistema

1. Passare all'area di gestione "Impostazioni" di CMC.
2. Fare clic su una freccia per espandere e visualizzare le impostazioni nell'area **Proprietà**, **Visualizza metriche di sistema globali**, **Cluster** o **Backup a caldo**.

10.9.4 Registrazione dell'attività dei server

La piattaforma BI consente di registrare informazioni specifiche sulla relativa attività Web.

- Inoltre, ogni server della piattaforma BI è progettato per registrare i messaggi nel registro di sistema standard del sistema operativo.
 - In Windows, la piattaforma BI esegue la registrazione nel servizio Registro eventi. È possibile visualizzare i risultati con il Visualizzatore eventi (nel Registro applicazione).

- In UNIX, la piattaforma BI esegue la registrazione nel daemon syslog come applicazione utente. Ogni server aggiunge il proprio nome e PID all'inizio di qualsiasi messaggio registrato.

Ogni server registra inoltre messaggi assertivi nella directory di registrazione dell'installazione del prodotto. Le informazioni a livello di programmazione registrate in questi file sono in genere utili solo al personale di supporto di SAP Business Objects per svolgere le attività di debug avanzato. Il percorso dei file di registro dipende dal sistema operativo:

- In Windows, la directory di registrazione predefinita è `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\Logging`.
- In UNIX la directory di registrazione predefinita è `DIRINSTALL/sap_bobj/logging`, ovvero la directory di installazione.

È importante notare che questi file di registro vengono puliti automaticamente, quindi non conterranno mai più di circa 1 MB di dati registrati per server.

Nota:

Per abilitare la funzione di registrazione nei computer UNIX che ospitano i server della piattaforma BI, è necessario impostare e configurare la registrazione di sistema in modo che tutti i messaggi registrati nella funzionalità "user" a livello "info" o superiore vengano registrati. È necessario inoltre configurare `SYSLOGD` in modo che accetti la registrazione in remoto.

Le procedure di impostazione variano da un sistema a un altro. Per istruzioni specifiche, consultare la documentazione del sistema operativo.

10.10 Configurazione delle impostazioni server

In questa sezione sono incluse informazioni tecniche e procedure che illustrano come modificare le impostazioni per i server della piattaforma BI.

La maggior parte delle impostazioni qui descritte consentono di integrare più efficacemente la piattaforma BI con l'hardware, il software e le configurazioni di rete correnti. Di conseguenza, le impostazioni scelte dipenderanno ampiamente da requisiti specifici.

È possibile modificare le impostazioni del server tramite la console CMC (Central Management Console) in due modi:

- Nella schermata "Proprietà" del server.
- Nella schermata "Modifica servizi comuni" relativa al server.

È importante notare che non tutte le modifiche si verificano immediatamente. Se un'impostazione non viene modificata immediatamente, le schermate "Proprietà" e "Modifica servizi comuni" visualizzano sia l'impostazione corrente (in rosso) che quella desiderata. Quando si torna all'area di gestione Server, il server verrà contrassegnato come Non aggiornato. Dopo essere stato riavviato, il server utilizza le impostazioni desiderate e il contrassegno Non aggiornato viene rimosso.

Nota:

In questa sezione non viene illustrato come configurare il server di applicazioni Web per distribuire le applicazioni della piattaforma BI. Questa attività viene eseguita in genere quando si installa il prodotto. Per ulteriori informazioni consultare il *Manuale di installazione della piattaforma SAP BusinessObjects Business Intelligence*.

Argomenti correlati

- [Configurazione dei numeri di porta](#)
- [Per modificare le proprietà di un server](#)
- [Ricreazione del database di sistema CMS](#)
- [Selezione di un database CMS nuovo o esistente](#)

10.10.1 Per modificare le proprietà di un server

1. Passare all'area di gestione "Server" della CMC.
2. Fare doppio clic sul server di cui si desidera modificare le impostazioni.
Viene visualizzata la schermata "Proprietà".
3. Apportare le modifiche desiderate e fare clic su **Salva** o su **Salva e chiudi**.

Nota:

Non tutte le modifiche si verificano immediatamente. Se un'impostazione non viene modificata immediatamente, la finestra di dialogo Proprietà visualizza l'impostazione corrente (in rosso) e quella desiderata. Quando si torna all'area di gestione Server, il server verrà contrassegnato come Non aggiornato. Dopo essere stato riavviato, il server utilizza le impostazioni desiderate dalla finestra di dialogo Proprietà e il contrassegno Non aggiornato viene rimosso.

10.10.2 Applicazione delle impostazioni dei servizi a più server

È possibile applicare la stessa impostazione ai servizi ospitati in più server.

1. Passare all'area di gestione "Server" della CMC.
2. Tenendo premuto **CTRL**, fare clic su ogni server che ospita servizi per il quale si desidera modificare le impostazioni, quindi fare clic con il pulsante destro del mouse e selezionare **Modifica servizi comuni**.
Verrà visualizzata la finestra di dialogo "Modifica servizi comuni" con l'elenco dei servizi ospitati dai server selezionati per i quali è possibile modificare impostazioni.
3. Se nella finestra di dialogo "Modifica servizi comuni" sono elencati più servizi, selezionare il servizio che si desidera modificare e fare clic su **Continua**.

4. Apportare le modifiche necessarie e fare clic su **OK**.

Nota:

Viene visualizzata l'area di gestione dei "server" della console CMC. Se è necessario riavviare un server, quest'ultimo viene contrassegnato come non aggiornato. Dopo il riavvio, il server utilizzerà le nuove impostazioni e il contrassegno Non aggiornato verrà rimosso.

10.10.3 Utilizzo di modelli di configurazione

I modelli di configurazione consentono di configurare con facilità più istanze dei server. I modelli di configurazione archiviano un elenco di impostazioni per ogni tipo di servizio che è possibile utilizzare per configurare istanze di server aggiuntive. Se ad esempio si dispone di dodici server di elaborazione Web Intelligence da configurare in modo identico, è necessario configurare le impostazioni per uno solo di essi. Sarà quindi possibile utilizzare il servizio configurato per definire il modello di configurazione per i server di elaborazione Web Intelligence e quindi applicare il modello alle altre 11 istanze di server.

Ogni tipo di servizio della piattaforma BI dispone di un proprio modello di configurazione. Esiste ad esempio un modello di configurazione per il tipo di servizio di elaborazione di Web Intelligence, uno per il tipo di servizio di pubblicazione e così via. Il modello di configurazione è definito nelle proprietà del server in Central Management Console (CMC).

Quando si configura un server per l'utilizzo di un modello di configurazione, le impostazioni esistenti per il server vengono sovrascritte dai valori del modello. Se successivamente si decide di non utilizzare più il modello, le impostazioni originali non vengono ripristinate. Le modifiche successive apportate al modello di configurazione non hanno più effetto sul server.

È buona norma utilizzare i modelli di configurazione nel modo seguente:

1. Impostare il modello di configurazione in un server.
2. Se si desidera applicare la stessa configurazione a tutti i server dello stesso tipo, selezionare **Usa modello configurazione** per tutti i server dello stesso tipo, incluso quello in cui è stato impostato il modello di configurazione.
3. Se in seguito si desidera modificare la configurazione di tutti i servizi di questo tipo, visualizzare le proprietà di tali servizi, deselezionare la casella di controllo **Usa modello configurazione**. Modificare le impostazioni desiderate, quindi selezionare **Imposta modello configurazione** per il server e fare clic su **Salva**. Tutti i servizi di quel tipo vengono aggiornati. Non avendo un server sempre impostato come modello di configurazione, non si rischia di modificare inavvertitamente le impostazioni di configurazione per tutti i server di quel tipo.

Argomenti correlati

- [Per impostare un modello di configurazione](#)
- [Per applicare un modello di configurazione a un server](#)

10.10.3.1 Per impostare un modello di configurazione

È possibile impostare un modello di configurazione per ogni tipo di servizio. Non è possibile impostare più modelli di configurazione per un servizio. È possibile utilizzare la pagina "Proprietà" di qualsiasi server per configurare le impostazioni che verranno utilizzate dal modello di configurazione per un tipo di servizio ospitato nel server.

1. Passare all'area di gestione "Server" della CMC.
2. Fare doppio clic sul server che ospita servizi di cui si desidera impostare il modello di configurazione. Viene visualizzata la schermata "Proprietà".
3. Configurare le impostazioni server da utilizzare nel modello, selezionare la casella di controllo **Imposta modello configurazione** e fare clic su **Salva** o **Salva e chiudi**.

Il modello di configurazione per il tipo di servizio selezionato viene definito in base alle impostazioni del server corrente. Altri server dello stesso tipo che ospitano gli stessi servizi verranno automaticamente e immediatamente riconfigurati in base al modello di configurazione se nelle relative proprietà l'opzione **Usa modello configurazione** è abilitata.

Nota:

Se non si definiscono esplicitamente le impostazioni per il modello di configurazione, vengono utilizzate le impostazioni predefinite del servizio.

Argomenti correlati

- [Per applicare un modello di configurazione a un server](#)

10.10.3.2 Per applicare un modello di configurazione a un server

Prima di applicare un modello di configurazione, assicurarsi di avere definito le impostazioni del modello di configurazione per il tipo di server a cui applicare il modello. Se non si definiscono esplicitamente le impostazioni del modello di configurazione, vengono utilizzate le impostazioni predefinite per il servizio.

Nota:

I server per i quali l'impostazione Usa modello configurazione non è abilitata non verranno aggiornati quando si modificano le impostazioni del modello di configurazione.

1. Passare all'area di gestione degli "Server" della CMC.
2. Fare doppio clic sul server che ospita un servizio a cui applicare il modello di configurazione. Viene visualizzata la schermata "Proprietà".
3. Selezionare la casella di controllo **Usa modello configurazione** e fare clic su **Salva** o **Salva e chiudi**.

Nota:

Se per rendere effettive le nuove impostazioni è necessario riavviare il server, nell'elenco dei server è contrassegnato come "Non aggiornato".

Il modello di configurazione appropriato viene applicato al server corrente. Qualsiasi modifica successiva apportata al modello di configurazione comporta il cambiamento della configurazione di tutti i server che ne fanno uso.

Con la deselezione dell'opzione **Usa modello configurazione** la configurazione del server non viene ripristinata sui valori precedenti all'applicazione del modello di configurazione. Le modifiche apportate successivamente al modello di configurazione non hanno effetto sulla configurazione dei server che utilizzano il modello.

Argomenti correlati

- [Per impostare un modello di configurazione](#)

10.10.3.3 Per ripristinare i valori predefiniti di sistema

È possibile ripristinare la configurazione di un servizio alle impostazioni originali, ad esempio in caso di errata configurazione dei server o di problemi di prestazioni.

1. Passare all'area di gestione degli "Server" della CMC.
2. Fare doppio clic sul server che ospita un servizio per il quale si desidera ripristinare i valori predefiniti di sistema.

Viene visualizzata la schermata "Proprietà".

3. Selezionare la casella di controllo **Ripristina valori predefiniti di sistema** e selezionare **Salva o Salva e chiudi**.

Vengono ripristinate le impostazioni predefinite per il tipo di servizio specifico.

10.11 Configurazione delle impostazioni di rete del server

Le impostazioni di rete per i server della piattaforma BI vengono gestite tramite la CMC. Queste impostazioni sono divise in due categorie: impostazioni porta e identificazione host.

impostazioni predefinite

Durante l'installazione, gli identificatori host del server sono impostati su **Assegna automaticamente**. A ogni server può tuttavia essere assegnato un nome host o un indirizzo IP specifico. Il numero di porta CMS predefinito è 6400. Gli altri server della piattaforma BI vengono associati in modo dinamico alle

porte disponibili. I numeri di porta vengono gestiti automaticamente dalla piattaforma BI, tuttavia è possibile utilizzare la CMC per specificare i numeri di porta.

10.11.1 Opzioni dell'ambiente di rete

La piattaforma BI supporta il traffico di rete basato su Internet Protocol versione 6 (IPv6) e Internet Protocol versione 4 (IPv4). È possibile utilizzare i componenti client e server in qualsiasi dei seguenti ambienti:

- Rete IPv4: tutti i componenti client e server vengono eseguiti solo con il protocollo IPv4.
- Rete IPv6: tutti i componenti client e server vengono eseguiti solo con il protocollo IPv6.
- Rete mista IPv6/IPv4: i componenti client e server possono essere eseguiti con entrambi i protocolli IPv6 e IPv4.

Nota:

La configurazione della rete dovrebbe essere eseguita dal sistema e dall'amministratore di rete. La piattaforma BI non fornisce un meccanismo per la definizione di un ambiente di rete. È possibile utilizzare la CMC per creare un'associazione a uno specifico indirizzo IPv6 o IPv4 per un server della piattaforma BI.

10.11.1.1 Ambiente IPv6/IPv4 misto

L'ambiente di rete IPv6/IPv4 consente:

- I server della piattaforma BI possono soddisfare sia le richieste IPv6 che IPv4 se vengono eseguiti in modalità IPv6/IPv4 mista.
- I componenti client possono interagire con i server come nodi solo IPv6, solo IPv4 o nodi IPv6/IPv4.

La modalità mista è particolarmente utile nei seguenti scenari:

- Spostamento da un ambiente di nodo solo IPv4 a un ambiente di nodo solo IPv6. Tutti i componenti client e server continueranno a interagire senza interruzioni fino al completamento della transizione. È quindi possibile disattivare le impostazioni IPv4 per tutti i server.
- Il software di terze parti non compatibile con IPv6 continuerà a funzionare nell'ambiente di nodo IPv6/IPv4.

10.11.2 Opzioni di identificazione host del server

È possibile specificare le opzioni di identificazione host nella console CMC per tutti i server della piattaforma BI. Nella seguente tabella sono riepilogate le opzioni disponibili nell'area "Impostazioni comuni":

Opzione	Descrizione
Assegna automaticamente	<p>Impostazione predefinita per tutti i server. Quando si seleziona questa casella di controllo, il server associa automaticamente la porta richiesta del server alla prima interfaccia di rete nel computer.</p> <p>Nota: È consigliabile selezionare la casella di controllo Assegna automaticamente per il nome host. Tuttavia, in alcuni casi, ad esempio quando il server viene eseguito in un computer multi-home o quando il server deve interagire con una determinata configurazione di firewall, è necessario considerare l'utilizzo di un indirizzo IP o di un nome host specifico. Consultare le informazioni relative alla configurazione di un computer multi-home e all'utilizzo dei firewall nel <i>Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence</i>.</p>
Nome host	<p>Specifica il nome host dell'interfaccia di rete su cui il server resta in ascolto delle richieste. Per il server CMS, questa impostazione specifica il nome host dell'interfaccia di rete cui il server CMS associa la porta richiesta e la porta del server dei nomi.</p>
Indirizzo IP	<p>Specifica l'indirizzo IP dell'interfaccia di rete su cui il server resta in ascolto delle richieste. Per il server CMS, specifica l'indirizzo dell'interfaccia di rete che il server CMS utilizza per associare la porta del server dei nomi alla porta richiesta. Per tutti i server, vengono forniti campi separati per specificare gli indirizzi IP IPv4 e/o IPv6.</p>

Avvertenza:

Se si seleziona la casella di controllo **Assegna automaticamente** su un computer multi-home, il server CMS potrebbe associarsi automaticamente all'interfaccia di rete errata. Per evitare questo problema, assicurarsi che le interfacce di rete sul computer host siano elencate nell'ordine corretto (utilizzando gli strumenti del sistema operativo del computer). È necessario specificare il nome host del server CMS nella CMC.

Nota:

Se si utilizzano computer multi-home o alcune configurazioni firewall NAT, potrebbe essere necessario specificare il nome host tramite nomi di dominio completi anziché nomi host.

Argomenti correlati

- [Per configurare il sistema per i firewall](#)
- [Configurazione di un computer multi-home](#)
- [Per risolvere i problemi relativi a più interfacce di rete](#)

10.11.2.1 Per modificare un'identificazione host di un server

1. Passare all'area di gestione degli "Server" della CMC.
2. Selezionare il server, quindi scegliere **Arresta server** dal menu **Azioni**.
3. Scegliere **Proprietà** dal menu **Gestisci**.
4. In **Impostazioni comuni** selezionare una delle seguenti opzioni:

Opzione	Descrizione
Assegna automaticamente	Il server verrà associato a una delle interfacce di rete disponibili.
Nome host	Immettere il nome host dell'interfaccia di rete su cui il server rimane in attesa delle richieste.
Indirizzo IP	<p>Immettere nei campi forniti un indirizzo IP IPv4 o IPv6 per l'interfaccia di rete su cui il server rimane in attesa di richieste.</p> <p>Nota: Per fare in modo che il server possa funzionare come nodo IPv4/IPv6 doppio, immettere un indirizzo IP valido in entrambi i campi.</p>

5. Fare clic su **Salva** o su **Salva e chiudi**.
Le modifiche vengono riflesse nella riga di comando visualizzata nella scheda "Proprietà".
6. Avviare e abilitare il server.

10.11.3 Configurazione di un computer multi-home

Un computer multi-home dispone di più indirizzi di rete. È possibile realizzare questa configurazione con più interfacce di rete, ciascuna con uno o più indirizzi IP, o con una sola interfaccia di rete a cui sono stati assegnati più indirizzi IP.

Se si dispone di più interfacce di rete, ciascuna con un solo indirizzo IP, modificare l'ordine di associazione in modo che l'interfaccia di rete al primo posto in tale ordine sia quella a cui si desidera vengano associati i server della piattaforma BI. Se l'interfaccia ha più indirizzi IP, utilizzare l'opzione **Identificatori host** nella console CMC per specificare una scheda di interfaccia di rete per il server della piattaforma BI. È possibile specificarla con nome host o indirizzo IP. Per ulteriori informazioni sulla configurazione dell'impostazione **Identificatori host**, consultare "Per risolvere i problemi relativi a più interfacce di rete".

Suggerimento:

questa sezione illustra come limitare tutti i server allo stesso indirizzo di rete, ma è possibile associare singoli server a indirizzi diversi. Ad esempio, può essere opportuno associare i File Repository Server a un indirizzo privato che non sia instradabile dai computer degli utenti. Configurazioni avanzate come questa richiedono che la configurazione DNS instradi in modo efficace le comunicazioni tra tutti i componenti server della piattaforma BI. In questo esempio, il DNS deve instradare le comunicazioni dagli altri server della piattaforma BI all'indirizzo privato dei File Repository Server.

Argomenti correlati

- [Per risolvere i problemi relativi a più interfacce di rete](#)

10.11.3.1 Per configurare il server CMS da associare a un indirizzo di rete

Nota:

in una macchina multi-homed, è possibile impostare l'identificatore host sul nome di dominio completo o sull'indirizzo IP dell'interfaccia a cui associare il server.

1. Passare all'area di gestione **Server** della CMC.
2. Fare doppio clic sul CMS.
3. In "Impostazioni comuni" selezionare una delle seguenti opzioni:
 - **Nome host**
 - Immettere il nome host dell'interfaccia di rete a cui verrà associato il server.
 - **Indirizzo IP**
 - Immettere nei campi forniti un indirizzo IP IPv4 o IPv6 per l'interfaccia di rete a cui verrà associato il server.

Nota:

Per fare in modo che il server possa funzionare come nodo IPv4/IPv6 doppio, immettere un indirizzo IP valido in entrambi i campi.

Avvertenza:

Non selezionare **Assegna automaticamente**.

4. Per **Porta richiesta** è possibile effettuare una delle operazioni seguenti:
 - Selezionare l'opzione **Assegna automaticamente**.
 - Immettere un numero di porta valido nel campo **Porta richiesta**.
5. Assicurarsi che sia specificato un numero di porta nella finestra di dialogo Porta server dei nomi.

Nota:

Il numero di porta predefinito è 6400.

10.11.3.2 Configurazioni degli altri server da associare a un indirizzo di rete

Gli altri server della piattaforma BI selezionano le porte in modo dinamico per impostazione predefinita. Per informazioni sulla disabilitazione dell'impostazione Assegna automaticamente, che propaga dinamicamente questa informazione, consultare "Modifica di una porta utilizzata da un server per l'accettazione di richieste."

Argomenti correlati

- [Per modificare la porta utilizzata da un server per accettare le richieste](#)

10.11.3.3 Per risolvere i problemi relativi a più interfacce di rete

In un computer multi-home, è possibile che il server CMS venga associato automaticamente all'interfaccia di rete errata. Per evitare questa situazione, assicurarsi che le interfacce di rete sull'host siano elencate nell'ordine corretto (utilizzando gli strumenti del sistema operativo) o che l'impostazione Nome host sia abilitata per il server CMS nella console CMC. Se l'interfaccia di rete primaria non è instradabile, è possibile utilizzare la seguente procedura per configurare la piattaforma BI per l'associazione a un'interfaccia di rete instradabile non primaria. Eseguire questi passaggi immediatamente dopo l'installazione della piattaforma BI nel computer locale, prima di installare la piattaforma BI in altri computer.

1. Aprire CCM e arrestare SIA per il nodo nel computer che dispone di più interfacce di rete.
2. Fare clic con il pulsante destro del mouse sul SIA e scegliere **Proprietà**.
3. Nella finestra di dialogo "Proprietà" fare clic sulla scheda "Configurazione".
4. Per associare il SIA a una specifica interfaccia di rete, digitare il numero di porta dell'interfaccia di rete di destinazione nel campo **Porta**.
5. Fare clic su **OK** e selezionare la scheda "Avvio".
6. Nell'elenco "Server CMS locali" selezionare il CMS e fare clic su **Proprietà**.
7. Per associare il CMS a una specifica interfaccia di rete, digitare il numero di porta dell'interfaccia di rete di destinazione nel campo **Porta**.
8. Fare clic su **OK** per applicare le nuove impostazioni.
9. Avviare SIA e attendere l'avvio dei server.
10. Avviare Central Management Console (CMC) e accedere all'area di gestione "Server". Ripetere i passaggi 11-14 per ogni server.
11. Selezionare il server, quindi scegliere **Arresta server** dal menu **Azioni**.
12. Scegliere **Proprietà** dal menu **Gestisci**.
13. In **Impostazioni comuni** selezionare una delle seguenti opzioni:

- Nome host: immettere il nome host dell'interfaccia di rete a cui verrà associato il server.
- Indirizzo IP: immettere nei campi forniti un indirizzo IP IPv4 o IPv6 per l'interfaccia di rete a cui verrà associato il server.

Nota:

Per fare in modo che il server possa funzionare come nodo IPv4/IPv6 doppio, immettere un indirizzo IP valido in entrambi i campi.

Avvertenza:

Non selezionare Assegna automaticamente.

14. Fare clic su **Salva** o su **Salva e chiudi**.

15. Tornare a CCM e riavviare SIA.

SIA riavvia tutti i server nel nodo. Tutti i server nel computer sono ora associati all'interfaccia di rete corretta.

10.11.4 Configurazione dei numeri di porta

Durante l'installazione, il CMS viene impostato per utilizzare i numeri di porta predefiniti. Il numero di porta CMS predefinito è 6400. Questa porta rientra nell'intervallo di porte riservato da SAP BusinessObjects (da 6400 a 6410). La comunicazione su queste porte non dovrebbe entrare in conflitto con applicazioni di terze parti.

Quando viene avviato e abilitato, ciascuno degli altri server della piattaforma BI viene associato dinamicamente a una porta disponibile (con un numero superiore a 1024), viene registrato con questa porta sul CMS e attende le richieste della piattaforma BI. Se necessario, è possibile indicare a ciascun componente server di restare in attesa su una porta specifica (piuttosto che selezionare dinamicamente qualsiasi porta disponibile). Sarà, ad esempio, necessario configurare manualmente una porta di richiesta per ogni server della piattaforma BI che deve comunicare attraverso un firewall.

I numeri delle porte possono essere specificati nella scheda Proprietà di ogni server nella console CMC. In questa tabella vengono riepilogate le opzioni in "Impostazioni comuni", relative all'utilizzo delle porte per tipi di server specifici:

Impostazione	CMS	Altri server
Porta richiesta	Specifica la porta utilizzata dal server CMS per accettare tutte le richieste da altri server (tranne le richieste del server dei nomi). Utilizza la stessa interfaccia di rete come porta del server dei nomi. Quando si seleziona Assegna automaticamente , il server utilizza automaticamente un numero di porta assegnato dal sistema operativo.	Specifica la porta su cui il server resta in ascolto di tutte le richieste. Quando si seleziona Assegna automaticamente , il server utilizza automaticamente un numero di porta assegnato dal sistema operativo.
Porta server dei nomi	Specifica la porta della piattaforma BI su cui il server CMS resta in ascolto delle richieste del servizio dei nomi. Il numero di porta predefinito è 6400.	Non applicabile.

10.11.4.1 Per modificare la porta CMS predefinita nella console CMC

Se un server CMS è già in esecuzione nel cluster, è possibile utilizzare la console CMC per modificare il numero della porta CMS predefinita. Se non sono presenti CMS in esecuzione nel cluster, sarà necessario utilizzare il CCM su Windows o lo script `serverconfig.sh` su UNIX, per modificare il numero di porta.

Nota:

Il CSM utilizza la stessa scheda di interfaccia di rete per la porta richiesta e la porta del server dei nomi.

1. Passare all'area di gestione "Server" della CMC.
2. Fare doppio clic sul server CMS nell'elenco dei server.
3. Sostituire il numero **Porta server dei nomi** con la porta su cui si desidera che resti in ascolto il server CMS. Il numero di porta predefinito è 6400.
4. Fare clic su **Salva e chiudi**.
5. Riavviare CMS.

Il server CMS inizia l'ascolto sul numero di porta specificato. Il Server Intelligence Agent propaga dinamicamente le nuove impostazioni agli altri server nel nodo, se tali server dispongono dell'opzione **Assegna automaticamente** selezionata per la porta richiesta. Potrebbero occorrere alcuni minuti per la visualizzazione delle modifiche nelle impostazioni Proprietà di tutti i membri del nodo.

Le impostazioni scelte nella pagina "Proprietà" vengono riflesse nella riga di comando del server, che viene anche visualizzata nella pagina "Proprietà".

10.11.4.2 Modifica della porta CMS predefinita in CCM su Windows

Se non sono presenti CMS accessibili nel cluster e si desidera modificare la porta CMS predefinita per uno o più CMS nella distribuzione, è necessario utilizzare il CCM per modificare il numero di porta CMS.

1. Aprire CCM e arrestare il SIA per il nodo.
2. Fare clic con il pulsante destro del mouse sul SIA e scegliere **Proprietà**.
3. Nella finestra di dialogo "Proprietà" fare clic sulla scheda "Avvio".
4. Dall'elenco "Server CMS locali", selezionare il CMS per il quale si desidera modificare il numero di porta e fare clic su **Proprietà**.
5. Per associare il CMS a una porta specifica, digitare il numero di porta nel campo **Porta**.
6. Fare clic su **OK** per applicare le nuove impostazioni.
7. Avviare SIA e attendere l'avvio dei server.

10.11.4.3 Modifica della porta CMS predefinita in CCM su Unix

Se non sono presenti CMS accessibili nel cluster e si desidera modificare la porta CMS predefinita per uno o più CMS nella distribuzione, utilizzare lo script `serverconfig.sh` per modificare il numero di porta CMS.

1. Utilizzare lo script `ccm.sh` per interrompere l'agente SIA (Server Intelligence Agent) che ospita il CMS di cui si desidera modificare il numero di porta.
2. Eseguire lo script `serverconfig.sh`.
Per impostazione predefinita, questo script risiede nella directory `<DirInstallaz>/sap_bobj`.
3. Selezionare **3 - Modifica nodo** e premere **Invio**.
4. Selezionare il nodo che ospita il CMS che si desidera modificare e premere **Invio**.
5. Selezionare **3 - Modifica un CMS locale** e premere **Invio**.
Verrà visualizzato un elenco di CMS ospitati nel nodo.
6. Selezionare il CMS da modificare, quindi premere **Invio**.
7. Digitare il nuovo numero di porta per il CMS, quindi premere **Invio**.
8. Specificare se si desidera che il CMS si avvii automaticamente all'avvio dell'agente SIA e premere **Invio**.
9. Digitare gli argomenti della riga di comando per il CMS o accettare gli argomenti correnti e premere **Invio**.
10. Digitare `esci` per uscire dallo script.
11. Avviare il SIA con lo script `ccm.sh` e attendere l'avvio dei server.

10.11.4.4 Per modificare la porta utilizzata da un server per accettare le richieste

Nota:

non è possibile utilizzare questa procedura per modificare la porta per le richieste del CMS (Central Management Server). Consultare invece "Per modificare la porta utilizzata da un CMS per accettare le richieste".

1. Passare all'area di gestione degli "Server" della CMC.
2. Selezionare il server, quindi scegliere **Arresta server** dal menu **Azioni**.
3. Fare doppio clic sul server.
Viene visualizzata la schermata "Proprietà".
4. In "Impostazioni comuni", deselezionare la casella di controllo **Assegna automaticamente** per **Porta richiesta**, quindi digitare il numero di porta su cui si desidera che il server resti in ascolto.
5. Fare clic su **Salva** o su **Salva e chiudi**.
6. Avviare e abilitare il server.

Il server viene associato alla nuova porta, esegue la registrazione con il server CMS e inizia l'ascolto per le richieste della piattaforma BI sulla nuova porta.

10.12 Gestione dei nodi

10.12.1 Utilizzo dei nodi

Un nodo è un gruppo di server della piattaforma BI eseguiti sullo stesso host e gestiti dallo stesso agente SIA (Server Intelligence Agent). Tutti i server di un nodo vengono eseguiti con lo stesso account utente. In un computer possono essere presenti molti nodi, pertanto è possibile eseguire i processi con account utente diversi. La gestione e il controllo di tutti i server di un nodo, a garanzia del corretto funzionamento di questi, viene eseguita da un unico agente SIA.

Nota:

è necessario utilizzare un account Administrator con l'autenticazione Enterprise per eseguire correttamente tutte le procedure di gestione dei nodi. Se tuttavia è abilitata la comunicazione SSL tra i server, è necessario disabilitare SSL per eseguire qualsiasi attività di gestione dei nodi.

Nota:

Verificare che tutti i driver di database necessari per la connessione dei server della piattaforma BI alle rispettive origini dati, ad esempio per la connessione del CMS al database CMS, siano presenti e che sia già stato configurato l'ambiente corretto, ad esempio che siano state configurate le variabili di ambiente appropriate.

Argomenti correlati

- [Configurazione dei server per SSL](#)
- [Per preparare un computer Unix per SQL Anywhere](#)

10.12.1.1 Variabili

Variabile	Descrizione
<DIRINSTALL>	Directory in cui viene installato SAP BusinessObjects Business Intelligence Platform. In Windows: C:\Programmi (x86)\SAP BusinessObjects
<DIRSCRIPT>	La directory in cui si trovano gli script di gestione dei nodi. <ul style="list-style-type: none"> In Windows: <DIRINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts In Unix: <DIRINSTALL>/sap_bobj/enterprise_xi40/<PLATFORM64>/scripts
<PLATFORM32>	Nome del sistema operativo Unix. I valori accettabili sono: <ul style="list-style-type: none"> aix_rs6000 linux_x86 solaris_sparc win32_x86
<PIATTAFORMA64>	Nome del sistema operativo Unix. I valori accettabili sono: <ul style="list-style-type: none"> aix_rs6000_64 linux_x64 solaris_sparcv9 win64_x64

10.12.1.2 Per preparare un computer Unix per SQL Anywhere

Per potere utilizzare SQL Anywhere come origine dati ODBC su un computer Unix, è necessario creare un file `odbc.ini` ed eseguire il comando `source` su di esso.

Nota:

Questa procedura non è necessaria se si utilizza il server SQL Anywhere in bundle installato con la piattaforma BI.

1. Creare il file `odbc.ini` in `DIRINSTALL/sap_bobj/enterprise_xi40/PIATTAFORMA64`.
2. Immettere il nome DSN (Database Source Name), il nome di database e il nome server per SQL Anywhere, nonché l'indirizzo IP e il numero di porta del computer che ospita il server di database SQL Anywhere.
3. Salvare `odbc.ini`.
4. Importare l'ambiente SQL Anywhere nel proprio ambiente corrente.

Se, ad esempio, si utilizza Bash come shell della riga di comando, specificare la versione a 64 bit del file `sa_config.sh` come origine.

5. Definire una variabile di ambiente denominata `ODBCINI` che punti alla posizione in cui è stato creato il file `odbc.ini`.

Configurare la variabile di ambiente in modo che i processi secondari possano visualizzare la variabile di ambiente `ODBCINI`.

Esempio:

File `odbc.ini` di esempio:

```
[ODBC Data Sources]
SampleDatabase=SQLAnywhere 12.0

[SampleDatabase]
UID=Administrator
PWD=password
DatabaseName=SampleDatabase
ServerName=SampleDatabase
CommLinks=tcpip(host=192.0.2.0;port=2638)
Driver=/build/bo/sqlanywhere12/lib64/libdbodbc12.so
```

Comando `source` di esempio:

```
source /build/bo/sqlanywhere12/bin64/sa_config.sh
ODBCINI=/build/bo/sap_bobj/enterprise_xi40/linux_x64/odbc.ini;export ODBCINI
```

Argomenti correlati

- [Variabili](#)

10.12.2 Aggiunta di un nuovo nodo

Il programma di installazione crea un singolo nodo quando si installa per la prima volta la piattaforma BI.

Se si desidera eseguire i server utilizzando account utente differenti, potrebbero essere necessari nodi aggiuntivi.

È possibile aggiungere un nuovo nodo utilizzando CCM (Central Configuration Manager) oppure uno script di gestione dei nodi. Se si utilizza un firewall, assicurarsi che le porte del SIA (Server Intelligence Agent) e del server CMS (Central Management Server) siano aperte.

Nota:

Utilizzare CCM o lo script di gestione dei nodi sul computer sul quale si desidera aggiungere un nodo. Non è possibile aggiungere un nodo su un computer remoto.

Un'installazione della piattaforma BI rappresenta un'istanza univoca dei file della piattaforma BI creati dal programma di installazione su un computer. È possibile utilizzare un'istanza di un'installazione della piattaforma BI solo all'interno di un singolo cluster. I nodi appartenenti a cluster differenti che condividono

la stessa installazione della piattaforma BI non sono supportati perché questo tipo di distribuzione non può essere corretto né aggiornato. Solo le piattaforme Unix supportano più installazioni del software sullo stesso computer, a condizione che ogni installazione venga eseguita con un account utente univoco e venga installata in una cartella separata in modo da non condividere file con le altre installazioni.

Tenere presente che tutti i computer nel cluster devono presentare versione e livello patch identici.

10.12.2.1 Aggiunta di un nodo a un nuovo computer in una distribuzione esistente

È possibile creare automaticamente il primo nodo in un computer quando si utilizza il programma di installazione per aggiungere un nuovo computer a una distribuzione esistente.

Suggerimento:

durante l'installazione, fare clic su **Espandi** e specificare il Central Management Server esistente.

Se si desidera creare altri nodi, utilizzare Central Configuration Manager o lo script `serverconfig.sh`.

Per ulteriori informazioni sull'installazione, consultare il *Manuale di installazione della piattaforma SAP BusinessObjects Business Intelligence*.

10.12.2.2 Aggiunta di un nodo in Windows

Avvertenza:

eseguire una copia di backup della configurazione del server per l'intero cluster prima e dopo l'aggiunta di un nodo.

1. In CCM (Central Configuration Manager), sulla barra degli strumenti, fare clic su **Aggiungi nodo**.
2. Nell'"Aggiunta guidata nodo" immettere il nome nodo e il numero di porta per il nuovo SIA (Server Intelligence Agent).
3. Scegliere se si desidera creare server nel nuovo nodo.
 - **Aggiungi nodo senza server**
 - **Aggiungi nodo con CMS**
 - **Aggiungi nodo con server predefiniti**

Questa opzione crea solo i server installati in questa macchina. Non include tutti i server possibili.

4. Selezionare un CMS.
 - Se la distribuzione in esecuzione, selezionare **Utilizza CMS esistente in esecuzione** e fare clic su **Avanti**.

Se richiesto, immettere il nome host e il numero di porta per il CMS esistente, le credenziali dell'amministratore, il nome dell'origine dati, le credenziali per il database di sistema e la chiave cluster.

- Se la distribuzione viene interrotta, selezionare **Avvia un nuovo CMS temporaneo** e fare clic su **Avanti**.

Se richiesto, immettere il nome host e il numero di porta per il CMS temporaneo, le credenziali dell'amministratore, il nome dell'origine dati, le credenziali per il database di sistema e la chiave cluster. Viene avviato un CMS temporaneo che viene interrotto al termine di questo processo.

Avvertenza:

evitare di utilizzare la distribuzione mentre è in esecuzione il CMS temporaneo. Assicurarsi che il CMS esistente e quello nuovo utilizzino porte diverse.

5. Rivedere la pagina di conferma e premere **Fine**.

CCM crea un nodo. Se si verificano errori, esaminare il file di registro.

A questo punto è possibile utilizzare CCM per avviare il nuovo nodo.

10.12.2.2.1 Aggiunta di un nodo a Windows mediante uno script

Avvertenza:

eseguire una copia di backup della configurazione del server per l'intero cluster prima e dopo l'aggiunta di un nodo.

È possibile utilizzare `AddNode.bat` per aggiungere un nodo in un computer Windows. Per ulteriori informazioni, consultare la sezione "Parametri script per l'aggiunta, la ricreazione e l'eliminazione di nodi".

Esempio:

A causa delle limitazioni del prompt dei comandi, è necessario utilizzare l'accento circonflesso (^) per eseguire l'escape degli spazi, del segno di uguale (=) e del punto e virgola (;) in questi parametri, a meno che il testo non venga racchiuso tra virgolette.

```
<SCRIPTDIR>\AddNode.bat -name mynode2
-siapiport 6415
-cms mycms:6400
-username Administrator
-password My^ Password
-cmsport 7400
-dbdriver mysqldatabasesubsystem
-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
-dbkey abc1234
-noservers
-createcms
```

Nota:

per evitare l'utilizzo dell'accento circonflesso nelle stringhe lunghe, è possibile scrivere il nome dello script e tutti i relativi parametri in un file `response.bat` temporaneo, quindi eseguire nuovamente il file `response.bat` senza parametri.

Argomenti correlati

- [Variabili](#)
- [Parametri script per l'aggiunta, la ricreazione e l'eliminazione di nodi](#)

10.12.2.3 Aggiunta di un nodo in Unix

Avvertenza:

eseguire una copia di backup della configurazione del server per l'intero cluster prima e dopo l'aggiunta di un nodo.

1. Eseguire `DIRINSTALL/sap_bobj/serverconfig.sh`
 2. Selezionare **1 - Add node** e premere **Invio**.
 3. Digitare il nome del nuovo nodo e premere **Invio**.
 4. Immettere il numero di porta del nuovo SIA e premere **Invio**.
 5. Scegliere se si desidera creare server nel nuovo nodo.
 - **no servers**
Crea un nodo che non contiene alcun server.
 - **cms**
Crea un CMS sul nodo senza creare altri server.
 - **default servers**
Crea solo i server installati in questa macchina. Non include tutti i server possibili.
 6. Selezionare un CMS.
 - Se la distribuzione è in esecuzione, selezionare **existing** e premere **Invio**.
Se richiesto, immettere il nome host e il numero di porta per il CMS esistente, le credenziali dell'amministratore, le informazioni di connessione al database, le credenziali per il database di sistema e la chiave cluster.
 - Se la distribuzione viene interrotta, selezionare **temporary** e premere **Invio**.
Se richiesto, immettere il nome host e il numero di porta per il CMS temporaneo, le credenziali dell'amministratore, le informazioni di connessione al database, le credenziali per il database di sistema e la chiave cluster. Viene avviato un CMS temporaneo che viene interrotto al termine di questo processo.
- Avvertenza:**
evitare di utilizzare la distribuzione mentre è in esecuzione il CMS temporaneo. Assicurarsi che il CMS esistente e quello nuovo utilizzino porte diverse.
7. Rivedere la pagina di conferma e premere **Invio**.
CCM crea un nodo. Se si verificano errori, esaminare il file di registro.

A questo punto è possibile eseguire `DIRINSTALL/sap_bobj/ccm.sh -start NomeNodo` per avviare il nuovo nodo.

10.12.2.3.1 Aggiunta di un nodo a Unix mediante uno script

Avvertenza:

eseguire una copia di backup della configurazione del server per l'intero cluster prima e dopo l'aggiunta di un nodo.

È possibile utilizzare `addnode.sh` per aggiungere un nodo in un computer Unix. Per ulteriori informazioni, consultare la sezione “Parametri script per l'aggiunta, la ricreazione e l'eliminazione di nodi”.

Esempio:

```
<SCRIPTDIR>/addnode.sh -name mynode2
-siaport 6415
-cms mycms:6400
-username Administrator
-password Password1
-cmsport 7400
-dbdriver mysqldatabasesubsystem
-connect "DSN=BusinessObjects CMS 140;UID=Administrator;PWD=Password1;HOSTNAME=myDatabase;PORT=3306"
-dbkey abc1234
-noservers
-creatcms
```

Argomenti correlati

- [Variabili](#)
- [Parametri script per l'aggiunta, la ricreazione e l'eliminazione di nodi](#)

10.12.3 Ricreazione di un nodo

È possibile ricreare un nodo utilizzando il CCM (Central Configuration Manager) o uno script di gestione dei nodi dopo aver ripristinato la configurazione per l'intero cluster o se il computer che ospita la distribuzione viene arrestato, viene danneggiato o presenta un file system corrotto. Utilizzare le seguenti indicazioni:

- Non è necessario ricreare un nodo se si reinstalla la distribuzione in un computer sostitutivo con opzioni di installazione e nome del nodo identici. Il nodo viene ricreato automaticamente dal programma di installazione.
- È consigliabile ricreare un nodo solo in un computer con una distribuzione esistente che presenti opzioni di installazione e livello di patch identici.
- È consigliabile ricreare solo i nodi che non esistono in computer della distribuzione. Assicurarsi che nessun altro computer ospiti lo stesso nodo.
- Sebbene la distribuzione consenta l'esecuzione dei nodi su sistemi operativi diversi, è necessario ricreare i nodi solo in computer che utilizzano lo stesso sistema operativo.

- Se si utilizza un firewall, verificare che le porte del SIA (Server Intelligence Agent) e del CMS (Central Management Server) siano aperte.

Promemoria:

è possibile ricreare un nodo solo sul computer in cui risiede.

Argomenti correlati

- [Ripristino del sistema](#)

10.12.3.1 Ricreazione di un nodo in Windows

1. Nel CCM (Central Configuration Manager) fare clic su **Aggiungi nodo** sulla barra degli strumenti.
2. Nell'"Aggiunta guidata nodo" immettere il nome del nodo e il numero di porta per il SIA (Server Intelligence Agent) ricreato.

Nota:

i nomi del nodo di origine e di quello ricreato devono essere identici.

3. Selezionare **Ricrea nodo** e fare clic su **Avanti**.
 - Se il nodo esiste nel database di sistema del Central Management Server (CMS), viene ricreato sull'host locale.

Avvertenza:

utilizzare questa opzione solo se il nodo non esiste in nessun host del cluster.

- Se il nodo non esiste nel database di sistema CMS (Central Management System), viene aggiunto un nuovo nodo con i server predefiniti che includono tutti i server installati nell'host.
4. Selezionare un CMS.
 - Se il CMS è in esecuzione, selezionare **Utilizza CMS esistente in esecuzione** e fare clic su **Avanti**.

Se richiesto, immettere il nome host e il numero di porta per il CMS esistente, le credenziali dell'amministratore, il nome dell'origine dati, le credenziali per il database di sistema e la chiave cluster.

- Se il CMS è stato interrotto, selezionare **Avvia un nuovo CMS temporaneo** e fare clic su **Avanti**.

Se richiesto, immettere il nome host del CMS temporaneo, le credenziali dell'amministratore, il nome dell'origine dati, le credenziali del database di sistema e la chiave cluster. Viene avviato un CMS temporaneo che viene interrotto al termine di questo processo.

Avvertenza:

Evitare di utilizzare la distribuzione mentre è in esecuzione il CMS temporaneo.

5. Verificare la pagina di conferma e premere **Fine**.

Il CCM ricrea il nodo e aggiunge informazioni ad esso relative al computer locale. Se si verificano errori, esaminare il file di registro.

È ora possibile eseguire il CCM per avviare il nodo ricreato.

10.12.3.1.1 Ricreazione di un nodo in Windows mediante uno script

Per ricreare un nodo in un computer Windows è possibile utilizzare `AddNode.bat`. Per ulteriori informazioni, consultare la sezione “Parametri script per l'aggiunta, la ricreazione e l'eliminazione di nodi”.

Esempio:

A causa delle limitazioni del prompt dei comandi, è necessario utilizzare l'accento circonflesso (^) per eseguire l'escape degli spazi, del segno di uguale (=) e del punto e virgola (;) in questi parametri, a meno che il testo non venga racchiuso tra virgolette.

```
<SCRIPTDIR>\AddNode.bat -name mynode2
-siaport 6415
-cms mycms:6400
-username Administrator
-password Password1
-cmsport 7400
-dbdriver mysqldatabasesubsystem
-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
-dbkey abc1234
-adopt
```

Nota:

per evitare l'utilizzo dell'accento circonflesso nelle stringhe lunghe, è possibile scrivere il nome dello script e tutti i relativi parametri in un file `response.bat` temporaneo, quindi eseguire nuovamente il file `response.bat` senza parametri.

Argomenti correlati

- [Variabili](#)
- [Parametri script per l'aggiunta, la ricreazione e l'eliminazione di nodi](#)

10.12.3.2 Ricreazione di un nodo in Unix

1. Eseguire `DIRINSTALL/sap_bobj/serverconfig.sh`
2. Selezionare **1 - Add node** e premere **Invio**.
3. Digitare il nome del nuovo nodo e premere **Invio**.

Nota:

i nomi del nodo di origine e di quello ricreato devono essere identici.

4. Digitare il numero di porta del nuovo SIA, quindi premere **Invio**.
5. Selezionare **Ricrea nodo**, quindi premere **Invio**.
 - Se il nodo esiste nel database di sistema del server CMS, viene ricreato nell'host locale.

Avvertenza:

utilizzare questa opzione solo se il nodo non esiste in nessun host del cluster.

- Se il nodo non esiste nel database di sistema CMS (Central Management System), viene aggiunto un nuovo nodo con i server predefiniti che includono tutti i server installati nell'host.

6. Selezionare un CMS.

- Se la distribuzione è in esecuzione, selezionare **existing** e premere **Invio**.

Se richiesto, immettere il nome host e il numero di porta per il CMS esistente, le credenziali dell'amministratore, le informazioni di connessione al database, le credenziali per il database di sistema e la chiave cluster.

- Se la distribuzione viene interrotta, selezionare **temporary** e premere **Invio**.

Se richiesto, immettere il nome host del CMS temporaneo, le credenziali dell'amministratore, le informazioni sulla connessione al database, le credenziali del database di sistema e la chiave cluster. Viene avviato un CMS temporaneo che viene interrotto al termine di questo processo.

Avvertenza:

Evitare di utilizzare la distribuzione mentre è in esecuzione il CMS temporaneo.

7. Verificare la pagina di conferma e premere **Invio.**

Il CCM ricrea il nodo e aggiunge informazioni ad esso relative al computer locale. Se si verificano errori, esaminare il file di registro.

È ora possibile eseguire `DIRINSTALL/sap_bobj/ccm.sh -start NomeNodo` per avviare il nodo ricreato.

10.12.3.2.1 Ricreazione di un nodo in Unix mediante uno script

Per ricreare un nodo in un computer Unix è possibile utilizzare `addnode.sh`. Per ulteriori informazioni, consultare la sezione "Parametri script per l'aggiunta, la ricreazione e l'eliminazione di nodi".

Esempio:

```
SCRIPTDIR/addnode.sh -name mynode2
-siport 6415
-cms mycms:6400
-username Administrator
-password Password1
-cmsport 7400
-dbdriver mysqldatabasesubsystem
-connect "DSN=BusinessObjects CMS 140;UID=Administrator;PWD=Password1;HOSTNAME=database;PORT=3306"
-dbkey abc1234
-adopt
```

Argomenti correlati

- [Variabili](#)
- [Parametri script per l'aggiunta, la ricreazione e l'eliminazione di nodi](#)

10.12.4 Eliminazione di un nodo

È possibile eliminare un nodo interrotto utilizzando un CCM (Central Configuration Manager) in esecuzione o uno script di gestione dei nodi. Utilizzare le seguenti indicazioni:

- L'eliminazione di un nodo determina anche la cancellazione permanente dei server in esso contenuti.
- Se il cluster comprende più computer, eliminare i nodi prima di rimuovere un computer dal cluster e disinstallare il software da esso. Se si rimuove un computer da un cluster prima di eliminare un nodo o il file system di un computer non funziona correttamente, è necessario ricreare il nodo in un altro computer con gli stessi server all'interno dello stesso cluster, quindi eliminare il nodo.

Promemoria:

è possibile eliminare un nodo solo sul computer in cui risiede.

Argomenti correlati

- [Ricreazione di un nodo](#)

10.12.4.1 Eliminazione di un nodo in Windows

Avvertenza:

eseguire il backup della configurazione server per l'intero cluster prima e dopo l'eliminazione di un nodo.

1. Eseguire il CCM (Central Configuration Manager).
2. Nel CCM interrompere il nodo da eliminare.
3. Selezionare il nodo, quindi fare clic su **Elimina nodo** sulla barra degli strumenti.
4. Se richiesto, immettere il nome host, la porta e le credenziali dell'amministratore per il CMS.

CCM elimina il nodo e tutti i server in esso contenuti.

10.12.4.1.1 Eliminazione di un nodo in Windows mediante uno script

Avvertenza:

eseguire il backup della configurazione server per l'intero cluster prima e dopo l'eliminazione di un nodo.

Per eliminare un nodo in un computer Windows è possibile utilizzare `RemoveNode.bat`. Per ulteriori informazioni, consultare la sezione "Parametri script per l'aggiunta, la ricreazione e l'eliminazione di nodi".

Esempio:

```
SCRIPTDIR\RemoveNode.bat -name mynode2  
-cms mycms:6400
```

```
-username Administrator  
-password Password1
```

Argomenti correlati

- [Variabili](#)
- [Parametri script per l'aggiunta, la ricreazione e l'eliminazione di nodi](#)

10.12.4.2 Eliminazione di un nodo in Unix

Prima e dopo aver eliminato un nodo, eseguire il backup della configurazione server per l'intero cluster.

1. Eseguire `DIRINSTALL/sap_bobj/ccm.sh -stop NomeNodo` per arrestare il nodo da eliminare.
2. Eseguire `DIRINSTALL/sap_bobj/serverconfig.sh`
3. Selezionare **2 - Elimina nodo**, quindi premere **Invio**.
4. Selezionare il nodo da eliminare, quindi premere **Invio**.
5. Se richiesto, immettere il nome host, il numero di porta e le credenziali dell'amministratore per il CMS.

Vengono eliminati il nodo e tutti i server in esso contenuti.

10.12.4.2.1 Eliminazione di un nodo in Unix mediante uno script

Avvertenza:

eseguire il backup della configurazione server per l'intero cluster prima e dopo l'eliminazione di un nodo.

Per eliminare un nodo in un computer Unix è possibile utilizzare `removenode.sh`. Per ulteriori informazioni, consultare la sezione "Parametri script per l'aggiunta, la ricreazione e l'eliminazione di nodi".

Esempio:

```
SCRIPTDIR\removenode.sh -name mynode2  
-cms mycms:6400  
-username Administrator  
-password Password1
```

Argomenti correlati

- [Variabili](#)
- [Parametri script per l'aggiunta, la ricreazione e l'eliminazione di nodi](#)

10.12.5 Ridenominazione di un nodo

È possibile rinominare un nodo utilizzando il CCM (Central Configuration Manager). Per rinominare un nodo, è necessario creare un nuovo nodo con un nuovo nome, clonare i server dal nodo originale nel nuovo nodo, quindi eliminare il nodo originale. Utilizzare le seguenti indicazioni:

- Se si rinomina il computer in cui è presente un nodo, non è necessario rinominare il nodo. È possibile continuare a utilizzare il nome del nodo esistente.
- Se si utilizza un firewall, verificare che le porte del SIA (Server Intelligence Agent) e del CMS (Central Management Server) siano aperte.

Promemoria:

è possibile rinominare un nodo solo sul computer in cui risiede.

Argomenti correlati

- [Aggiunta di un nuovo nodo](#)
- [Duplicazione di server](#)
- [Eliminazione di un nodo](#)

10.12.5.1 Ridenominazione di un nodo in Windows

Avvertenza:

eseguire il backup della configurazione server per l'intero cluster prima e dopo la ridenominazione di un nodo.

1. Avviare il Central Configuration Manager (CCM).
2. Nel CCM (Central Configuration Manager) fare clic su **Aggiungi nodo** sulla barra degli strumenti.
3. Nell'"Aggiunta guidata nodo" immettere il nome del nodo e il numero di porta per il nuovo SIA (Server Intelligence Agent), le credenziali dell'amministratore, le informazioni sulla connessione al database, le credenziali del database di sistema e la chiave cluster.
4. Selezionare **Aggiungi nodo senza server**.
5. Una volta creato il nodo, utilizzare la pagina "Gestione server" della Central Management Console per clonare tutti i server dal nodo di origine nel nuovo nodo.

Nota:

verificare che i server clonati non presentino conflitti di porta con i server del nodo precedente.

6. Nel CCM avviare il nuovo nodo.
7. Dopo almeno cinque minuti di esecuzione del nuovo nodo, utilizzare il CCM per eliminare quello di origine.

Argomenti correlati

- [Aggiunta di un nuovo nodo](#)
- [Duplicazione di server](#)
- [Eliminazione di un nodo](#)

10.12.5.2 Ridenominazione di un nodo in Unix

Avvertenza:

eseguire il backup della configurazione server per l'intero cluster prima e dopo la ridenominazione di un nodo.

1. Eseguire `DIRINSTALL/sap_bobj/serverconfig.sh`.
2. Selezionare **1 - Add node** e premere **Invio**.
3. Digitare il nome del nuovo nodo e premere **Invio**.
4. Immettere il numero di porta del nuovo SIA e premere **Invio**.
5. Se necessario, immettere le credenziali dell'amministratore, le informazioni sulla connessione al database, le credenziali del database di sistema e la chiave cluster.
6. Selezionare **nessun server** e premere **Invio**.
7. Una volta creato il nodo, utilizzare la pagina "Gestione server" della Central Management Console per clonare tutti i server dal nodo di origine nel nuovo nodo.

Nota:

verificare che i server clonati non presentino conflitti di porta con i server del nodo precedente.

8. Eseguire `DIRINSTALL/sap_bobj/ccm.sh -start NomeNodo` per avviare il nuovo nodo.
9. Dopo almeno cinque minuti di esecuzione del nuovo nodo, utilizzare `serverconfig.sh` per eliminare quello di origine.

Argomenti correlati

- [Aggiunta di un nuovo nodo](#)
- [Duplicazione di server](#)
- [Eliminazione di un nodo](#)

10.12.6 Spostamento di un nodo

È possibile spostare un nodo interrotto da un cluster in un altro utilizzando il CCM (Central Configuration Manager) o uno script di gestione dei nodi. Utilizzare le seguenti indicazioni:

- Verificare che il cluster di destinazione non presenti un nodo con lo stesso nome.
- Verificare che tutti i tipi di server installati nel computer in cui si trova il nodo di origine siano installati anche nel cluster di destinazione.
- Se si desidera aggiungere un nuovo computer a un cluster di produzione senza che tuttavia venga utilizzato prima di completarne il test, installare la piattaforma BI in un computer autonomo, eseguire il test del computer, quindi spostare il nodo in un cluster di produzione.
- Il livello del service pack e della versione della piattaforma BI di questo computer devono essere coerenti con il resto del cluster.

Promemoria:

è possibile spostare un nodo solo sul computer in cui risiede.

10.12.6.1 Spostamento di un nodo esistente in Windows

In questo esempio il nodo da spostare viene installato nel sistema di origine. Il computer del sistema di origine, inizialmente installazione autonoma, viene aggiunto al cluster di destinazione.

Avvertenza:

eseguire il backup della configurazione server per l'intero cluster prima e dopo lo spostamento di un nodo.

1. Interrompere il nodo nel CCM (Central Configuration Manager).
2. Fare clic con il pulsante destro del mouse sul nodo e scegliere **Sposta**.
3. Se richiesto, selezionare il nome dell'origine dati e immettere il nome host, la porta, le informazioni sulla connessione al database, le credenziali dell'amministratore per il CMS di destinazione e la chiave cluster.
4. Selezionare un CMS.
 - Se la distribuzione di origine è in esecuzione, selezionare **Utilizza CMS esistente in esecuzione** e premere **Avanti**.

Se richiesto, immettere il nome host e il numero di porta del CMS esistente del sistema di origine e le credenziali dell'amministratore.
 - Se la distribuzione di origine è stata interrotta, selezionare **Avvia un nuovo CMS temporaneo** e fare clic su **Avanti**.

Se richiesto, immettere il nome host e il numero di porta del CMS temporaneo del sistema di origine, le credenziali dell'amministratore, il nome dell'origine dati, le credenziali del database di sistema di origine e la chiave cluster. Viene avviato un CMS temporaneo che viene interrotto al termine di questo processo.

Avvertenza:

Evitare di utilizzare la distribuzione mentre è in esecuzione il CMS temporaneo.

5. Verificare la pagina di conferma e premere **Fine**.

Il CCM crea un nuovo nodo nel cluster di destinazione con lo stesso nome e gli stessi server del nodo del cluster di origine. Nel cluster di origine rimane una copia del nodo. Non vengono spostati i modelli di configurazione dei server del nodo. Se si verificano errori, esaminare il file di registro.

Avvertenza:

non utilizzare il cluster di origine dopo aver spostato il nodo.

6. Nel CCM avviare il nodo spostato.

10.12.6.1.1 Spostamento di un nodo in Windows mediante uno script

Avvertenza:

eseguire il backup della configurazione server per l'intero cluster prima e dopo lo spostamento di un nodo.

Per spostare un nodo in un computer Windows è possibile utilizzare `MoveNode.bat`. Per ulteriori informazioni, consultare la sezione "Parametri di script per lo spostamento di nodi".

Esempio:

A causa delle limitazioni del prompt dei comandi, è necessario utilizzare l'accento circonflesso (^) per eseguire l'escape degli spazi, del segno di uguale (=) e del punto e virgola (;) in questi parametri, a meno che il testo non venga racchiuso tra virgolette.

```
SCRIPTDIR\MoveNode.bat -cms sourceMachine:6409
-username Administrator
-password Password1
-dbdriver mysqldatabasesubsystem
-connect "DSN=Source BOEXI40;UID=username;PWD=Password1;HOSTNAME=databasel;PORT=3306"
-dbkey abc1234
-destcms destinationMachine:6401
-destusername Administrator
-destpassword Password2
-destdbdriver sybasedatabasesubsystem
-destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
-destdbkey def5678
```

Nota:

per evitare l'utilizzo dell'accento circonflesso nelle stringhe lunghe, è possibile scrivere il nome dello script e tutti i relativi parametri in un file `response.bat` temporaneo, quindi eseguire nuovamente il file `response.bat` senza parametri.

Argomenti correlati

- [Variabili](#)
- [Parametri script per lo spostamento di nodi](#)

10.12.6.2 Spostamento di un nodo esistente in Unix

In questo esempio il nodo da spostare viene installato nel sistema di origine. Il computer del sistema di origine, inizialmente installazione autonoma, viene aggiunto al cluster di destinazione.

Avvertenza:

eseguire il backup della configurazione server per l'intero cluster prima e dopo lo spostamento di un nodo.

1. Eseguire `DIRINSTALL/sap_bobj/ccm.sh -stop NomeNodo` per arrestare il nodo.
2. Eseguire `DIRINSTALL/sap_bobj/serverconfig.sh`
3. Selezionare **4 - Sposta nodo**, quindi premere **Invio**.
4. Selezionare il nodo da spostare, quindi premere **Invio**.
5. Quando richiesto, selezionare le informazioni sulla connessione al database e immettere il nome host, la porta, le credenziali dell'amministratore per il CMS di destinazione e la chiave cluster.
6. Selezionare un CMS.
 - Se la distribuzione di origine è in esecuzione, selezionare **existing** e premere **Invio**.
Se richiesto, immettere il nome host e il numero di porta del CMS esistente del sistema di origine e le credenziali dell'amministratore.
 - Se la distribuzione di origine è stata interrotta, selezionare **temporary** e premere **Invio**.
Se richiesto, immettere il nome host e la porta del CMS temporaneo del sistema di origine, le credenziali dell'amministratore, le informazioni sulla connessione al database, le credenziali del database di sistema di origine e la chiave cluster. Viene avviato un CMS temporaneo che viene interrotto al termine di questo processo.

Avvertenza:

evitare di utilizzare la distribuzione mentre è in esecuzione il CMS temporaneo. Verificare che il CMS esistente e quello temporaneo utilizzino porte diverse.

7. Verificare la pagina di conferma e premere **Invio**.
Il CCM crea un nuovo nodo nel cluster di destinazione con lo stesso nome e gli stessi server del nodo del cluster di origine. Nel cluster di origine rimane una copia del nodo. Non vengono spostati i modelli di configurazione dei server del nodo. Se si verificano errori, esaminare il file di registro.

Avvertenza:

non utilizzare il cluster di origine dopo aver spostato il nodo.

8. Eseguire `DIRINSTALL/sap_bobj/ccm.sh -start NomeNodo` per avviare il nodo spostato.

10.12.6.2.1 Spostamento di un nodo in Unix mediante uno script

Avvertenza:

eseguire il backup della configurazione server per l'intero cluster prima e dopo lo spostamento di un nodo.

Per spostare un nodo in un computer Unix è possibile utilizzare `movenode.sh`. Per ulteriori informazioni, consultare la sezione "Parametri di script per lo spostamento di nodi".

Esempio:

```
SCRIPTDIR/movenode.sh -cms sourceMachine:6409
-username Administrator
-password Password1
-dbdriver mysqldatabasesubsystem
-connect "DSN=Source BOEXI40;UID=username;PWD=Password1;HOSTNAME=database1;PORT=3306"
-dbkey abc1234
-destcms destinationMachine:6401
-destusername Administrator
-destpassword Password2
-destdbdriver sybasedatabasesubsystem
-destconnect "DSN=Destin BOEXI40;UID=username;PWD=Password2;"
-destdbkey def5678
```

Argomenti correlati

- [Variabili](#)
- [Parametri script per lo spostamento di nodi](#)

10.12.7 Parametri script

10.12.7.1 Parametri script per l'aggiunta, la ricreazione e l'eliminazione di nodi

Parametro	Descrizione	Esempio
-adopt	Ricrea il nodo se è già presente nel server CMS.	-adopt
-cms	<p>Il nome e la porta del server CMS (Central Management Server).</p> <p>Avvertenza: non utilizzare questo parametro se si utilizza <code>-usetempcms</code></p> <p>Nota: è necessario specificare un numero di porta se il server CMS non viene eseguito sulla porta predefinita 6400.</p>	-cms mycms:6409

Parametro	Descrizione	Esempio
-cmsport	<ul style="list-style-type: none"> Il numero di porta del server CMS quando si avvia un CMS temporaneo. <p>Limitazione: è inoltre necessario utilizzare i parametri -usetempcms, -dbdriver, -connect e -dbkey.</p> <ul style="list-style-type: none"> Il numero di porta del server CMS quando si crea un nuovo CMS. <p>Limitazione: inoltre, è necessario utilizzare i parametri -dbdriver, -connect e -dbkey.</p>	-cmsport 6401
-connect	<p>La stringa di connessione del database di sistema del server CMS o del server CMS temporaneo.</p> <p>Nota: omettere gli attributi NOMEHOST e PORTA per eseguire la connessione ai database DB2, Oracle, SQL Anywhere, SQL Server o Sybase.</p>	-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=password;HOSTNAME=database;PORT=3306"
-dbdriver	<p>Il driver di database del server CMS.</p> <p>Valori accettati:</p> <ul style="list-style-type: none"> db2databasesubsystem maxdbdatabasesubsystem mysqldatabasesubsystem oracledatabasesubsystem sqldatabasesubsystem sqlserverdatabasesubsystem sybasedatabasesubsystem newdbdatabasesubsystem 	-dbdriver mysqldatabasesubsystem
-dbkey	La chiave cluster.	-dbkey abc1234
-name	Il nome di un nodo.	-name mynode2

Parametro	Descrizione	Esempio
-noservers	Crea un nodo senza server. Nota: il parametro <code>-createcms</code> aggiuntivo crea un nodo con un server CMS, ma nessun altro server. Omettere questi parametri per creare un nodo con tutti i server predefiniti.	-noservers
-password	La password dell'account Administrator.	-password Password1
-siaport	Il numero di porta dell'agente SIA per il nodo.	-siaport 6409
-username	Il nome utente dell'account Administrator.	-username Administrator
-usetempcms	Avvertenza: non utilizzare questo parametro se si utilizza <code>-cms</code> Avvia e utilizza il server CMS temporaneo. Nota: utilizzare un server CMS temporaneo quando la distribuzione non è in esecuzione.	-usetempcms

Argomenti correlati

- [Aggiunta di un nodo a Windows mediante uno script](#)
- [Aggiunta di un nodo a Unix mediante uno script](#)
- [Ricreazione di un nodo in Windows mediante uno script](#)
- [Ricreazione di un nodo in Unix mediante uno script](#)
- [Eliminazione di un nodo in Windows mediante uno script](#)
- [Eliminazione di un nodo in Unix mediante uno script](#)

10.12.7.2 Parametri script per lo spostamento di nodi

Parametro	Descrizione	Esempio
-cms	<p>Il nome del server CMS (Central Management Server) di origine.</p> <p>Avvertenza: non utilizzare questo parametro se si utilizza <code>-usetempcms</code></p> <p>Nota: è necessario specificare un numero di porta se il server CMS non viene eseguito sulla porta predefinita 6400.</p>	-cms sourceMachine:6409
-cmsport	<ul style="list-style-type: none"> Il numero di porta del server CMS quando si avvia un CMS temporaneo. <p>Limitazione: è inoltre necessario utilizzare i parametri <code>-usetempcms</code>, <code>-dbdriver</code>, <code>-connect</code> e <code>-dbkey</code>.</p> <ul style="list-style-type: none"> Il numero di porta del server CMS quando si crea un nuovo CMS. <p>Limitazione: inoltre, è necessario utilizzare i parametri <code>-dbdriver</code>, <code>-connect</code> e <code>-dbkey</code>.</p>	-cmsport 6401
-connect	<p>La stringa di connessione del database di sistema del server CMS di origine o del server CMS temporaneo.</p> <p>Nota: omettere gli attributi <code>NOMEHOST</code> e <code>PORTA</code> per eseguire la connessione ai database DB2, Oracle, SQL Anywhere, SQL Server o Sybase.</p>	-connect "DSN=Source BOEXI40;UID=username;PWD=password;HOSTNAME=data base;PORT=3306"

Parametro	Descrizione	Esempio
-dbdriver	<p>Il driver di database del server CMS di origine.</p> <p>Valori accettati:</p> <ul style="list-style-type: none"> • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqldatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem • newdbdatabasesubsystem 	-dbdriver mysqldatabasesubsystem
-dbkey	La chiave cluster di origine.	-dbkey abc1234
-destcms	<p>Il nome del server CMS di destinazione.</p> <p>Nota: è necessario specificare un numero di porta se il server CMS non viene eseguito sulla porta predefinita 6400.</p>	-destcms destinationMachine:6401
-destconnect	<p>La stringa di connessione del database di sistema CMS di destinazione.</p> <p>Nota: omettere gli attributi <code>NOMEHOST</code> e <code>PORTA</code> per eseguire la connessione ai database DB2, Oracle, SQL Anywhere, SQL Server o Sybase.</p>	-destconnect "DSN=Destin BOEXI40;UID=username;PWD=password;HOSTNAME=database;PORT=3306"
-destdbdriver	<p>Il driver di database del server CMS di destinazione.</p> <p>Valori accettati:</p> <ul style="list-style-type: none"> • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqldatabasesubsystem • sybasedatabasesubsystem • newdbdatabasesubsystem 	-destdbdriver sybasedatabasesubsystem
-destdbkey	La chiave cluster di destinazione.	-destdbkey def5678

Parametro	Descrizione	Esempio
-destpassword	La password dell'account Administrator nel server CMS di destinazione.	-destpassword Password2
-destusername	Il nome utente dell'account Administrator nel server CMS di destinazione.	-destusername Administrator
-password	La password dell'account Administrator nel server CMS di origine.	-password Password1
-username	Il nome utente dell'account Administrator nel server CMS di origine.	-username Administrator
-usetempcms	<p>Avvertenza: non utilizzare questo parametro se si utilizza <code>-cms</code></p> <p>Avvia e utilizza il server CMS temporaneo.</p> <p>Nota: utilizzare un server CMS temporaneo quando la distribuzione non è in esecuzione.</p>	-usetempcms

Argomenti correlati

- [Spostamento di un nodo in Windows mediante uno script](#)
- [Spostamento di un nodo in Unix mediante uno script](#)

10.12.8 Aggiunta di dipendenze dei server Windows

In un ambiente Windows ogni istanza del SIA (Server Intelligence Agent) dipende dai servizi Registro eventi e RPC (Remote Procedure Call).

Se un SIA non funziona correttamente, verificare che entrambi i servizi vengano visualizzati sulla scheda "Dipendenza" del SIA.

10.12.8.1 Aggiunta di dipendenze dei server Windows

1. Utilizzare il CCM per arrestare il SIA (Server Intelligence Agent).
2. Fare clic con il pulsante destro del mouse sul SIA e scegliere **Proprietà**.
3. Fare clic sulla scheda **Dipendenza**.
4. Fare clic su **Aggiungi**.
Viene visualizzata la finestra di dialogo "Aggiungi dipendenza" che riporta un elenco di tutte le dipendenze disponibili.
5. Selezionare una dipendenza e fare clic su **Aggiungi**.
6. Fare clic su **OK**.
7. Utilizzare il CCM per avviare il SIA.

10.12.9 Modifica delle credenziali utente per un nodo

È possibile utilizzare CCM (Central Configuration Manager) per specificare o aggiornare le credenziali utente per il SIA (Server Intelligence Agent) se la password del sistema operativo viene modificata oppure se si desidera eseguire tutti i server di un nodo con un account utente diverso.

Tutti i server gestiti dal SIA vengono eseguiti con lo stesso account. Per eseguire un server utilizzando un account non di sistema, assicurarsi che l'account sia membro del gruppo di amministratori locali sul server e che disponga del diritto "Sostituzione di token a livello di processo".

Limitazione:

in un computer Unix è necessario eseguire la piattaforma BI con lo stesso account utilizzato per installarla. Per utilizzare un account diverso, reinstallare la distribuzione con un altro account.

10.12.9.1 Modifica delle credenziali utente per un nodo in Windows

1. Utilizzare CCM (Central Configuration Manager) per arrestare il SIA (Server Intelligence Agent).
2. Fare clic con il pulsante destro del mouse sul SIA e scegliere **Proprietà**.
3. Deselezionare la casella di controllo **Account sistema**.
4. Immettere nome utente e password, quindi fare clic su **OK**.
5. Utilizzare CCM per riavviare il SIA.

I processi del SIA e del server accedono al computer locale con il nuovo account utente.

10.13 Assegnazione di un nuovo nome a un computer in una distribuzione della piattaforma BI

10.13.1 Modifica dei nomi dei cluster

Di seguito sono riportate le azioni consigliate per l'assegnazione di un nuovo nome ai cluster:

Avvertenza:

non distribuire mai più cluster con lo stesso nome.

Condizione	Azione
Il nome del cluster viene modificato.	Informare gli utenti del nuovo nome del cluster e chiedere loro di utilizzarlo (dopo la prima connessione al CMS mediante la sintassi <i>nome host:porta</i>). Al livello Web aggiornare il nome del cluster nel file delle proprietà di tutti i server di applicazioni Web.
Viene installata una versione diversa della piattaforma BI in un computer in cui in precedenza veniva eseguito un CMS oppure il computer viene aggiunto a un cluster diverso.	<ul style="list-style-type: none">• Verificare che il nuovo CMS venga eseguito tramite una porta diversa.• Utilizzare password diverse per cluster diversi, per evitare che gli utenti accedano a un cluster non corretto.

10.13.2 Modifica di indirizzi IP

Per evitare modifiche di configurazione dovute alla modifica dell'indirizzo IP del computer, selezionare **Proprietà server** nella scheda **Server** della console CMC, quindi verificare che tutti i server siano associati a nomi host, oppure utilizzare l'opzione **Assegna automaticamente**. Seguire inoltre queste azioni consigliate:

Condizione	Azione
Si utilizza ODBC con il database CMS o il database di controllo.	Verificare che il DNS utilizzi il nome host del server di database CMS.
Si utilizza un altro tipo di connessione al database con il database CMS o il database di controllo.	Utilizzare il CCM per aggiornare il database in modo che utilizzi il nome host del server di database.
Il database CMS o il database di controllo si trova nello stesso host del CMS.	Utilizzare <code>localhost</code> come nome computer.
Si utilizza l'URL per le applicazioni Web della piattaforma BI a cui gli utenti accedono tramite browser, ad esempio la console CMC.	Utilizzare nomi host anziché indirizzi IP per l'URL predefinito. Per aggiornare l'URL del visualizzatore predefinito, selezionare Impostazioni di elaborazione per l'applicazione selezionata.
L'URL per i client della piattaforma BI si basa sui servizi Web, ad esempio Crystal Reports for Java o LiveOffice).	Ad esempio, per Open Document, fare clic sulla scheda Applicazioni nella CMC, fare clic con il pulsante destro del mouse su Open Document e scegliere Impostazioni di elaborazione .
Si utilizza OpenDocument.	

Linee guida alternative

Nota:

seguire queste linee guida solo se non è possibile eseguire le azioni consigliate sopra descritte.

Tabella 10 - 9: Per i computer che ospitano server

Condizione	Azione
L'host contiene server della piattaforma BI e i server devono essere associati a indirizzi IP specifici.	Modificare gli indirizzi IP nella scheda Server della CMC, ma non riavviare i server finché tutti i componenti del computer non saranno stati aggiornati. Riavviare quindi il computer e non i singoli server della piattaforma BI.
Una connessione a database deve utilizzare un indirizzo IP.	Modificare l'indirizzo IP.
È necessaria la modifica di un indirizzo IP in una rete IP statica.	Modificare l'indirizzo IP del computer della piattaforma BI. Suggerimento: Accedere alla console CMC per verificare che la piattaforma BI sia operativa.

Promemoria:

dopo aver eseguito un'azione, riavviare il computer.

Tabella 10 - 10: Per i computer che ospitano il server di applicazioni Web

Condizione	Azione
L'URL del visualizzatore predefinito per OpenDocument deve utilizzare un indirizzo IP.	Aggiornare l'indirizzo IP nel campo Imposta URL del visualizzatore predefinito nella sezione Impostazioni di elaborazione della scheda Applicazioni della console CMC.
Gli utenti accedono alle applicazioni Web della piattaforma BI (ad esempio alla console CMC) specificando un URL con un indirizzo IP nel browser.	Informare gli utenti del nuovo indirizzo IP.
I client della piattaforma BI basati su servizi Web, ad esempio Crystal Reports for Java o LiveOffice, devono utilizzare indirizzi IP.	Configurare tutti i client in modo che utilizzino il nuovo indirizzo IP.

Argomenti correlati

- [Selezione di un database CMS nuovo o esistente](#)

10.13.3 Assegnazione di nuovi nomi ai computer

In qualsiasi momento è possibile rinominare i computer di una distribuzione della piattaforma BI dopo avere arrestato tutti i server della piattaforma BI all'interno del computer. Di seguito sono riportate le azioni consigliate per l'assegnazione di un nuovo nome ai computer:

Condizione	Azione
Si effettua l'accesso per la prima volta.	Utilizzare il nome del computer CMS anziché il nome del cluster.
La distribuzione interessa più computer.	Verificare che durante l'operazione di assegnazione del nuovo nome i server CMS in tutti gli altri computer siano in esecuzione.

10.13.3.1 Livello server

Nota:

prima di rinominare il computer CMS, nella scheda “Gestione server” della console CMC esaminare la configurazione di tutti i server situati nel computer che si desidera rinominare. Se la proprietà "Nome host" utilizza il nome host CMS precedente, aggiornarla con il nuovo nome host CMS.

Promemoria:

riavviare i server solo dopo aver completato tutte le procedure di assegnazione del nuovo nome al computer.

Per rinominare i computer del livello server, seguire queste istruzioni:

Condizione	Azione
Il computer rinominato ospita un CMS e alcuni utenti sono già connessi con il nome precedente del computer.	Informare gli utenti del nome del computer CMS e chiedere loro di utilizzarlo.
Il computer rinominato ospita un CMS e la proprietà <code>cms.default</code> dei file delle proprietà predefiniti delle applicazioni Web della piattaforma BI contiene il nome host CMS precedente.	<p>Aggiornare il nome del computer CMS nella proprietà <code>cms.default</code> di tutti i file delle proprietà personalizzati di tutti i computer del livello Web. Per impostazione predefinita, in Tomcat i file delle proprietà creati dall'utente si trovano in <code>DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom</code></p> <p>Nota: se non sono presenti file delle proprietà personalizzati, crearne di nuovi. Copiare i file delle proprietà predefiniti in una cartella personalizzata e rimuoverne tutto il contenuto ad eccezione della riga <code>cms.default</code>.</p>

Condizione	Azione
Il computer rinominato ospita un CMS e in tutti i computer del cluster è installato SAP BusinessObjects Explorer.	Sostituire il nome host CMS precedente con quello nuovo nella proprietà <code>default.cms.name</code> del file <code>default.settings.properties</code> di tutti i computer che ospitano server di applicazioni Web. Per impostazione predefinita, in Tomcat il file <code>default.settings.properties</code> si trova in <code>DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\explorer\WEB-INF\classes\</code> Promemoria: dopo aver eseguito questa operazione, riavviare l'applicazione Web Explorer o il server di applicazioni Web.
Si utilizza SSO con Explorer	Aggiornare il valore <code>cms</code> in <code>jsp-sso-provider.jsp</code> e aggiornare i valori <code>sso.global.cms</code> e <code>sso.trusted.auth.x509.cms</code> in <code>sso.properties</code> con il nuovo nome host CMS.
Si utilizzano Portal Integration Kit o applicazioni personalizzate.	Configurare i Portal Integration Kit o le applicazioni personalizzate in modo che utilizzino il nuovo nome host CMS.
La distribuzione soddisfa tutte le condizioni seguenti: <ul style="list-style-type: none"> • Un cluster è costituito da più nodi. • Tutti i server CMS sono in esecuzione solo all'interno del computer rinominato. • Almeno un nodo non ospita il CMS. • Il computer che si desidera rinominare contiene almeno un nodo. • L'indirizzo IP viene modificato durante il processo di assegnazione del nuovo nome. 	Utilizzare CCM per eseguire il workflow "Ricrea nodo" in tutti i nodi ad eccezione del nodo che ospita il CMS, quindi avviare tutti i nodi della piattaforma BI all'interno della distribuzione. Per ulteriori informazioni, consultare il capitolo "Gestione dei nodi".

Promemoria:

dopo aver eseguito un'operazione, riavviare l'applicazione o il server di applicazioni Web.

Argomenti correlati

- [Ricreazione di un nodo](#)

10.13.3.2 Livello Web

Se si rinomina il computer che ospita il server di applicazioni Web della piattaforma BI, seguire queste istruzioni:

Condizione	Azione
Si modifica il nome del computer che ospita il server di applicazioni Web della piattaforma BI e l'URL del visualizzatore OpenDocument predefinito utilizza il nome host del server di applicazioni Web.	Accedere alla console CMC e aggiornare l'URL del visualizzatore predefinito in Applicazioni > CMC > Impostazioni di elaborazione .
Si modifica il nome del computer che ospita il server di applicazioni Web della piattaforma BI e gli utenti accedono alle applicazioni Web della piattaforma BI utilizzando un URL che include il nome host del server di applicazioni Web.	Chiedere agli utenti di accedere alle applicazioni Web della piattaforma BI utilizzando un URL che includa il nuovo nome host del server di applicazioni Web.
Si modifica il nome del computer che ospita il server di applicazioni Web della piattaforma BI e i client della piattaforma BI basati su servizi Web utilizzano nomi host di server di applicazioni Web nell'URL.	Riconfigurare tutti i client della piattaforma BI basati su servizi Web in modo che utilizzino il nuovo nome host del server di applicazioni Web.

10.13.3.3 Database

Se si desidera rinominare il computer che ospita il database di sistema CMS o il database di controllo, eseguire queste azioni consigliate:

Condizione	Azione
Evitare di aggiornare l'indirizzo IP.	Utilizzare il nome computer del database CMS o del database di controllo nel nome origine dati (DSN, Data Source Name).
Il database CMS o il database di controllo si trova nello stesso host del CMS.	Utilizzare <code>localhost</code> nel DSN per evitare di doverlo aggiornare in caso di modifica del nome host.

Database di sistema CMS

Condizione	Azione
Si desidera rinominare un computer che ospita il database di sistema CMS e si utilizza ODBC.	Aggiornare il DSN del database CMS con il nuovo nome host del server di database.
Si desidera rinominare un computer che ospita il database di sistema CMS e si utilizza un tipo di connessione non ODBC.	Utilizzare CCM per aggiornare il database CMS con il nuovo nome host del server di database in ogni nodo del cluster.

Database di controllo

Condizione	Azione
Si desidera rinominare un computer che ospita il database di controllo e si utilizza ODBC.	Aggiornare il DSN del database di controllo con il nuovo nome host del server di database.
Si desidera rinominare un computer che ospita il database di controllo e si utilizza un tipo di connessione non ODBC.	Aggiornare il nome del computer del server di database con il nuovo nome host del server di database nella scheda Controllo della console CMC.

10.13.3.4 File Repository Server

Se si desidera rinominare il computer che ospita l'archivio file FRS, è necessario aggiornare l'"Input File Repository Server" e l'"Output File Repository Server" nella pagina "Gestione server" della console CMC. È inoltre necessario verificare che le proprietà "Directory archivio file" e "Directory temporanea" utilizzino il nuovo percorso dell'archivio file, quindi riavviare i server.

10.14 Utilizzo di librerie a 32 e a 64 bit con la piattaforma BI

I server della piattaforma BI sono una combinazione di processi a 32 e 64 bit. Alcuni server avviano inoltre processi secondari a 32 e 64 bit. Per utilizzare la versione corretta delle librerie di terze parti (a 32 bit o a 64 bit) con i processi della piattaforma BI, è necessario impostare variabili di ambiente separate per ogni versione sul computer che ospita la piattaforma BI. È quindi necessario impostare una variabile di ambiente aggiuntiva contenente un elenco separato da virgole delle variabili di ambiente che includono versioni a 32 e 64 bit. Quando si avvia un processo dalla piattaforma BI, viene selezionata la variabile appropriata a seconda che il processo sia a 32 o 64 bit.

- `PRIMA_VAR_AMB`=il valore da utilizzare con i processi della piattaforma BI a 64 bit.

- `PRIMA_VAR_AMB32`=il valore da utilizzare con i processi a 32 bit.
- `SECONDA_VAR_AMB`=il valore da utilizzare con i processi a 64 bit.
- `SECONDA_VAR_AMB`=il valore da utilizzare con i processi a 32 bit.
- `BOE_USE_32BIT_ENV_FOR`=`PRIMA_VAR_AMB,SECONDA_VAR_AMB`

Se, ad esempio, la piattaforma BI è stata installata in un computer AIX insieme a client Oracle a 32 e 64 bit ed è necessario impostare la variabile `LIBPATH`, procedere all'impostazione delle variabili seguenti:

- `ORACLE_HOME`=versione a 64 bit del client Oracle
- `ORACLE_HOME32`=versione a 32 bit
- `LIBPATH`=versione a 64 bit
- `LIBPATH32`=versione a 32 bit
- `BOE_USE_32BIT_ENV_FOR`=`ORACLE_HOME,LIBPATH`

Nota:

In Linux e in Solaris non utilizzare `BOE_USE_32BIT_ENV_FOR=LD_LIBRARY_PATH` per separare i percorsi a 32 e 64 bit, ma aggiungere entrambi i percorsi a 32 e 64 bit a `LD_LIBRARY_PATH`.

10.15 Gestione dei segnaposto per server e nodi

10.15.1 Visualizzazione dei segnaposto server

- Nell'area di gestione dei "Server" della CMC fare clic con il pulsante destro del mouse su un server e scegliere **Segnaposto**.

Nella finestra di dialogo "Segnaposto" viene visualizzato un elenco di segnaposto per tutti i server dello stesso cluster del server selezionato. Se si desidera modificare il valore di un segnaposto, modificare il segnaposto del nodo.

Argomenti correlati

- [Segnaposto server e nodo](#)

10.15.2 Visualizzazione e modifica dei segnaposto per un nodo

1. Nell'area di gestione dei "Server" della Central Management Console fare clic con il pulsante destro del mouse sul nodo per il quale si desidera modificare i segnaposto e scegliere **Segnaposto**.

2. Se si desidera modificare le impostazioni dei segnaposto, apportare le modifiche appropriate e fare clic su **Salva** per continuare.

Argomenti correlati

- [Segnaposto server e nodo](#)

Gestione dei database CMS (Central Management Server)

11.1 Gestione delle connessioni di database di sistema CMS

Se il database di sistema CMS non è disponibile, ad esempio a causa di un problema hardware, software o della rete, il server CMS entra nello stato "In attesa delle risorse". Se la distribuzione della piattaforma BI utilizza più server CMS, le richieste successive da altri server vengono inoltrate ai server CMS del cluster che dispongono di una connessione attiva al database di sistema. Quando un server CMS si trova nello stato "In attesa delle risorse", qualsiasi richiesta corrente che non richiede l'accesso al database continua a essere elaborata, mentre le richieste che richiedono l'accesso al database CMS avranno esito negativo.

Per impostazione predefinita, un server CMS nello stato "In attesa delle risorse" tenta periodicamente di ristabilire il numero di connessioni specificate nella proprietà "Connessioni richieste al database di sistema". Non appena viene stabilita almeno una connessione al database, il CMS sincronizza tutti i dati necessari, entra nello stato "In esecuzione" e riprende le normali operazioni.

Talvolta, può essere utile impedire al server CMS di ristabilire automaticamente una connessione al database. Ad esempio, può essere utile verificare l'integrità del database prima di ristabilire le connessioni al database. A tale scopo, nella pagina "Proprietà" del server CMS deselezionare **Riconnessione automatica al database di sistema**.

Argomenti correlati

- [Per modificare le proprietà di un server](#)

11.1.1 Selezione di SQL Anywhere come database CMS

Per utilizzare SQL Anywhere come database CMS, eseguire le operazioni seguenti:

1. Arrestare tutti i nodi del sistema.
2. Eseguire l'applicazione appropriata:
 - In Unix, eseguire `./cmsdbsetup.sh`.
 - In Windows avviare Central Configuration Manager (CCM).

3. Copiare i dati dal database CMS predefinito, selezionando SQL Anywhere come database di destinazione. Per ulteriori informazioni, consultare l'argomento correlato "Copia dei dati da un database di sistema CMS a un altro".
4. Nelle distribuzioni a più nodi, aggiornare l'origine dati CMS in ogni nodo, tranne quello su cui si copia il database, con il nuovo database SQL Anywhere. Per ulteriori informazioni, consultare l'argomento correlato "Selezione di un database CMS nuovo o esistente".
5. Assicurarsi che la distribuzione sia operativa, ad esempio accedere al CMC e visualizzare un report.

Argomenti correlati

- [Copia dei dati da un database di sistema CMS a un altro](#)
- [Selezione di un database CMS nuovo o esistente](#)

11.1.2 Selezione di SAP HANA come database CMS

Per utilizzare SAP HANA come database CMS, eseguire le operazioni seguenti:

1. Installare la piattaforma BI con il database CMS predefinito.
2. Installare il client SAP HANA.
3. Creare una connessione a SAP HANA.
 - In Unix verificare la presenza della variabile di ambiente `ODBCINI`. Se la variabile esiste e punta a un file `odbc.ini` esistente, aggiungere le righe seguenti a tale file:

```
[ODBC Data Sources]
NewDB=<New_DB_version>
```

```
[NewDB]
SERVERNODE=<HANA Server IP address>:<HANA server port #>
```

<Nuova_versione_DB> è la versione SAP HANA; ad esempio "NewDB 1.0", <indirizzo IP server HANA> è l'indirizzo IP del server SAP HANA e <n porta server HANA> è il numero di porta del server SAP HANA.

Se la variabile di ambiente `ODBCINI` non esiste, creare un file `odbc.ini` nella directory `DIRINSTALL/sap_bobj/enterprise_xi40/`, aggiungere le righe sopra riportate al file e impostare la variabile di ambiente `ODBCINI` come indicato di seguito:

```
ODBCINI=INSTALDIR/sap_bobj/enterprise_xi40/odbc.ini
```

- In Windows creare una connessione ODBC a SAP HANA.

Nota:

Per le modifiche alla connessione ODBC, accertarsi di eseguire la versione a 64 bit di Amministrazione origine dati ODBC: **Start > Pannello di controllo > Strumenti di amministrazione > Origini dati (ODBC)**.

4. Assicurarsi che sia possibile eseguire le connessioni al server SAP HANA.

- In Unix è possibile verificare la connessione al server SAP HANA eseguendo il comando seguente. Le variabili nell'esempio seguente si riferiscono all'installazione SAP HANA:

```
INSTALLDIR/odbcereg SERVER:HDBINDEXSERVERPORT SYSTEMID NONADMINUSER NONADMINPASSWORD
```

- In Windows è possibile utilizzare Amministrazione origine dati ODBC per verificare la connessione ODBC SAP HANA.
5. In Unix copiare `libodbcHDB.so` dalla directory di installazione SAP HANA in `DIRINSTALL/sap_bobj/enterprise_xi40/PLATFORM`
 6. Arrestare tutti i nodi del sistema.
 7. Eseguire l'applicazione appropriata:
 - In Unix, eseguire `./cmsdbsetup.sh`.
 - In Windows avviare Central Configuration Manager (CCM).
 8. Copiare i dati dal database CMS predefinito, selezionando SAP HANA come database di destinazione. Per ulteriori informazioni, consultare l'argomento correlato "Copia dei dati da un database di sistema CMS a un altro".
 9. Nelle distribuzioni a più nodi aggiornare l'origine dati CMS in ogni nodo, tranne quello su cui si copia il database, con il nuovo database SAP HANA. Per ulteriori informazioni, consultare l'argomento correlato "Selezione di un database CMS nuovo o esistente".
 10. Assicurarsi che la distribuzione sia operativa, ad esempio accedere al CMC e visualizzare un report.

Argomenti correlati

- [Copia dei dati da un database di sistema CMS a un altro](#)
- [Selezione di un database CMS nuovo o esistente](#)

11.2 Selezione di un database CMS nuovo o esistente

È possibile utilizzare CCM o `cmsdbsetup.sh` per specificare un database di sistema CMS nuovo o esistente per un nodo. In genere il completamento della procedura risulta indispensabile solo in un numero limitato di casi:

- Se si è modificata la password per il database di sistema CMS corrente, questi passaggi consentiranno di disconnettersi e riconnettersi al database corrente. Quando viene richiesto, è possibile fornire al CMS la nuova password.
- Se si desidera selezionare e inizializzare un database vuoto per la piattaforma BI, attenersi alla procedura illustrata per selezionare la nuova origine dati.
- Se si è ripristinato un database di sistema CMS da un backup (utilizzando gli strumenti e le procedure standard di amministrazione del database) con una procedura che ha reso non valida la connessione al database originale, sarà necessario riconnettere il CMS al database ripristinato. Questa situazione può verificarsi, ad esempio, se il database CMS originale è stato ripristinato in un server del database installato di recente.

Nota:

- Se come database CMS si utilizza IBM DB2 e lo si aggiorna da una versione precedente a 9.5 Fix Pack 5 alla versione 9.5 Fix Pack 5 o più recente (per la linea 9.5), oppure si esegue l'aggiornamento da una versione precedente a 9.7 Fix Pack 1 alla versione 9.7 Fix Pack 1 o più recente (per la linea 9.7), durante il riavvio successivo del nodo della piattaforma BI o di CMS, lo schema del database CMS verrà aggiornato automaticamente da CMS in modo da supportare lo schema compatibile con HADR.

Questo può essere un processo lungo, durante il quale il sistema della piattaforma BI non sarà disponibile per l'uso. Non interrompere il processo di aggiornamento per evitare di danneggiare il database CMS. Si consiglia vivamente di eseguire il backup del database CMS prima di eseguire questa operazione. Non provare inoltre a utilizzare IBM HADR con un database CMS IBM DB2 di una versione precedente a 9.5 Fix Pack 5 (per la linea 9.5) o a 9.7 Fix Pack 1 (per la linea 9.7).

- Non configurare un'installazione della piattaforma BI per l'utilizzo di un database di sistema CMS appartenente a un cluster diverso, a meno che non si stia eseguendo un workflow di copia di sistema.

Il sistema potrebbe essere danneggiato se le versioni e i livelli di patch delle installazioni della piattaforma BI e i database CMS sono diversi o se differiscono i percorsi di installazione o i componenti installati e così via.

Per evitare che il sistema venga danneggiato, non provare a migrare il contenuto BI da un sistema all'altro puntando la distribuzione della piattaforma BI a un database CMS di un altro sistema della piattaforma BI, soprattutto se la versione e il livello di patch sono diversi.

11.2.1 Selezione di un database CMS nuovo o esistente in Windows

1. Utilizzare CCM per arrestare Server Intelligence Agent (SIA).
2. Selezionare il SIA e fare clic sul pulsante **Specifica origine dati CMS**.
3. Selezionare **Aggiorna impostazioni origine dati** e fare clic su **OK**.
4. Selezionare un driver di database e fare clic su **OK**.
5. Questi passaggi dipendono dal tipo di connessione selezionato:
 - Se si seleziona ODBC, viene visualizzata la finestra di dialogo di Windows "Seleziona origine dati". Selezionare l'origine dati ODBC che si desidera utilizzare come database CMS, quindi fare clic su **OK**. Fare clic su **Nuovo** per configurare un nuovo DSN. Se richiesto, fornire le credenziali del database e fare clic su **OK**.
 - Se si seleziona un driver originale, viene richiesto di indicare il nome del server, l'ID di accesso e la password. Fornire tali informazioni e fare clic su **OK**.
6. Specificare la chiave cluster.
7. Riavviare Server Intelligence Agent.

11.2.2 Per selezionare un database CMS nuovo o esistente in UNIX

Utilizzare lo script `cmsdbsetup.sh`. Come riferimento, consultare il capitolo relativo agli strumenti UNIX.

1. Eseguire lo script `cmsdbsetup.sh` (disponibile per impostazione predefinita in `DIRINS` `TALL/sap_bobj/`).
2. Selezionare l'azione di aggiornamento (opzione 6).
3. Se richiesto, fornire il tipo di database del nuovo database CMS.
4. Fornire le informazioni del database (nome host, nome utente, password e chiave cluster).
Viene visualizzato un messaggio di notifica quando il database CMS viene puntato al nuovo percorso.
5. Se viene richiesto di ricreare Server Intelligence Agent (SIA), fornire la password di amministratore e il numero di porta di comunicazione del server CMS.

Nota:

Queste informazioni vengono richieste solo se si fa riferimento a un database CMS vuoto.

11.3 Ricreazione del database di sistema CMS

Questa procedura descrive come ricreare (reinizializzare) il database di sistema CMS corrente. Eseguendo questa attività si eliminano tutti i dati già presenti nel database. Questa procedura è utile, ad esempio, se si è installata la piattaforma BI in un ambiente di sviluppo per progettare e testare applicazioni Web personalizzate. È possibile reinizializzare il database di sistema CMS nell'ambiente di sviluppo ogni volta che è necessario cancellare dal sistema tutti i dati.

Avvertenza:

Con l'implementazione dei passaggi indicati in questo workflow, verranno eliminati tutti i dati del database CMS nonché gli oggetti come report e utenti. Non eseguire questi passaggi in una distribuzione di produzione.

È molto importante eseguire il backup di tutte le impostazioni di configurazione del server prima di reinizializzare il database di sistema CMS. Quando si ricrea il database, le impostazioni di configurazione del server verranno cancellate e per ripristinarle è necessario disporre di un backup.

Quando si ricrea il database di sistema, i codici di licenza esistenti devono essere conservati nel database. Tuttavia, se si rende necessario immettere nuovamente i codici di licenza, accedere alla console CMC con l'account Administrator predefinito. Passare all'area di gestione Autorizzazione e immettere le informazioni nella scheda Codici di licenza.

Nota:

Se si reinizializza il database di sistema CMS, tutti i dati nel database di sistema CMS corrente verranno eliminati. Valutare l'ipotesi di eseguire un backup del database corrente prima di iniziare. Se necessario, contattare l'amministratore del database.

Argomenti correlati

- [Backup delle impostazioni server](#)

11.3.1 Nuova creazione del database di sistema CMS in Windows

1. Utilizzare CCM per arrestare Server Intelligence Agent (SIA).

Nota:

Per questa procedura, non è possibile eseguire il CCM in un computer remoto; è necessario che venga eseguito in un computer con almeno un nodo valido. È inoltre necessario che nel computer siano installati i file binari CMS.

2. Fare clic con il pulsante destro del mouse su SIA e scegliere **Proprietà**.
3. Nella finestra di dialogo **Proprietà** accedere alla scheda "Configurazione" e fare clic su **Specifica**.
4. Nella finestra di dialogo **Impostazione database CMS** fare clic su **Crea di nuovo origine dati corrente**.

Nota:

Verranno anche ricreati tutti i server e gli oggetti del computer in cui si è eseguito CCM nel passaggio 1. Non verranno tuttavia ricreati tutti gli oggetti, ma solo quelli principali predefiniti. Ad esempio non vengono ricreati i report di esempio.

5. Fare clic su **OK**. Per confermare, fare clic su **Sì**.
6. Specificare la password per il database di sistema CMS e fare clic su **OK**.

Nota:

Assicurarsi di avere impostato una nuova password amministratore. Per impostazione predefinita l'account amministratore non prevede la password.

Il CCM avviserà del completamento dell'installazione del database di sistema CMS.

7. Fare clic su **OK**.
Si verrà riportati al CCM.
8. Riavviare Server Intelligence Agent e abilitare i servizi.
Durante l'avvio di Server Intelligence Agent, viene anche avviato il server CMS. Il server CMS scrive i dati di sistema richiesti nell'origine dati appena svuotata.
9. Se la distribuzione contiene più computer, è necessario ricreare i nodi negli altri computer.

11.3.2 Per creare nuovamente il database di sistema CMS in UNIX

Utilizzare lo script `cmsdbsetup.sh`. Per informazioni, consultare il capitolo relativo agli strumenti UNIX del *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

1. Eseguire `cmsdbsetup.sh` (per impostazione predefinita è disponibile in `DIRINSTALL/sap_bobj/`).
2. Selezionare l'opzione "reinizializza" (opzione 5), quindi confermare la scelta.

Lo script `cmsdbsetup.sh` avvia la ricreazione del database di sistema CMS.

3. Specificare la password del database di sistema.
4. Al termine della creazione del database, chiudere lo script `cmsdbsetup.sh`.
5. Fornire le informazioni del database (nome host, nome utente e password).
Viene visualizzato un messaggio di notifica quando il database CMS viene puntato al nuovo percorso.
6. Se viene richiesto di ricreare Server Intelligence Agent (SIA), fornire la password di amministratore e il numero di porta attraverso il quale il server CMS deve comunicare.

Nota:

Queste informazioni vengono richieste solo se si fa riferimento a un database CMS vuoto.

7. Nella directory `DIINSTALL/sap_bobj/` utilizzare il comando seguente per avviare il nodo.

```
ccm.sh -start nodename
```

8. Per abilitare i servizi, utilizzare il seguente comando:

```
ccm.sh -enable all -cms CMSNAME:PORT -username administrator -password password
```

Nota:

Poiché il database CMS è stato appena ricreato, la password di amministratore non è ancora stata specificata.

11.4 Copia dei dati da un database di sistema CMS a un altro

È possibile utilizzare CCM (Central Configuration Manager) o `cmsdbsetup.sh` per copiare i dati di sistema da un server di database a un altro. Se ad esempio si desidera sostituire il database con un altro dopo un aggiornamento o un passaggio da un tipo di database all'altro, è possibile copiare il contenuto del database esistente nel nuovo prima di rimuoverlo.

Il database di destinazione viene inizializzato prima che i nuovi dati vi siano copiati, quindi il contenuto esistente del database di destinazione viene definitivamente eliminato (tutte le tabelle della piattaforma BI vengono eliminate in modo permanente e quindi ricreate). Una volta copiati i dati, il database di destinazione diventa il database corrente per il CMS.

Nota:

Se si desidera importare utenti, gruppi, cartelle e report da una versione principale precedente della piattaforma BI alla versione principale corrente, utilizzare Upgrade Management Tool della piattaforma SAP BusinessObjects Business Intelligence. Per ulteriori informazioni, fare riferimento alla *guida sull'aggiornamento della piattaforma SAP BusinessObjects Business Intelligence*.

11.4.1 Preparazione per la copia di un database di sistema CMS

Prima di eseguire la copia di un database di sistema CMS, attivare la modalità non in linea per gli ambienti di origine e di destinazione disabilitando e successivamente arrestando tutti i server. Eseguire il backup di entrambi i database CMS, quindi delle directory principali utilizzate dagli Input e Output File Repository Server. Se necessario, contattare l'amministratore del database o di rete.

Accertarsi di disporre di un account utente per il database con autorizzazione alla lettura di tutti i dati del database di origine e un account utente per il database con diritti di creazione, eliminazione e aggiornamento per il database di destinazione. Verificare inoltre di potersi connettere a entrambi i database, mediante il software client di database o ODBC, in base alla configurazione in uso, dal computer CMS di cui si sta sostituendo il database.

Se si copia un database CMS dalla posizione corrente in un server di database diverso, il database CMS corrente costituirà l'ambiente di origine. Il suo contenuto viene copiato nel database di destinazione, che si stabilisce diventi il database attivo per il CMS corrente. Si tratta della procedura da seguire per spostare il database CMS predefinito dal database predefinito esistente a un server del database dedicato, quale Microsoft SQL Server, Informix, Oracle, DB2 o Sybase. Accedere con un account amministrativo al computer che esegue CMS di cui si desidera spostare il database.

Nota:

- quando si copiano i dati da un database all'altro, il database di destinazione viene inizializzato prima che i nuovi dati siano copiati. Di conseguenza, se il database di destinazione non contiene le tabelle di sistema della piattaforma BI, si procederà alla relativa creazione. Se il database di destinazione contiene le tabelle di sistema della piattaforma BI, queste verranno eliminate definitivamente, ne verranno create delle nuove e vi verranno copiati dati dal database di origine. Le altre tabelle nel database non saranno interessate.
- se si copia un database di sistema CMS in un database di destinazione MaxDB su Windows, è necessario verificare che il percorso del client MaxDB sia stato aggiunto alla variabile di ambiente *PATH*. Ad esempio, ;C:\Programmi\sdb\MAXDB1\pgm.

11.4.2 Copia di un database di sistema CMS in Windows

Prima di copiare il contenuto del database CMS, assicurarsi di poter accedere al database di destinazione con un account che disponga di autorizzazioni per l'aggiunta o l'eliminazione di tabelle o per l'aggiunta, l'eliminazione o la modifica dei dati in tali tabelle.

1. Aprire il CCM e arrestare il Server Intelligence Agent (SIA).
2. Fare clic con il pulsante destro del mouse sul SIA e scegliere **Proprietà**.
3. Fare clic sulla scheda **Configurazione** e quindi su **Specifica**.
4. Scegliere **Copia** e fare clic su **OK**.
5. Selezionare il tipo di database per il database CMS di origine, quindi specificarne le relative informazioni (inclusi il nome host, il nome utente e la password).
6. Selezionare il tipo di database per il database CMS di destinazione, quindi specificarne le relative informazioni (inclusi il nome host, il nome utente e la password).
7. Una volta completata la copia del database CMS, fare clic su **OK**.

11.4.3 Copia di dati da un database di sistema CMS in Unix

Prima di copiare il contenuto del database CMS, assicurarsi di poter accedere al database di destinazione con un account che disponga di autorizzazioni per l'aggiunta o l'eliminazione di tabelle o per l'aggiunta, l'eliminazione o la modifica dei dati in tali tabelle.

Nota:

In UNIX non è possibile eseguire una migrazione direttamente da un ambiente di origine che utilizza una connessione ODBC al database CMS. Se il database CMS di origine utilizza ODBC, è innanzitutto necessario aggiornare il sistema a un driver originale supportato.

1. Arrestare il server CMS digitando il seguente comando:
`./ccm.sh -stop nomenodo`
 2. Eseguire `cmsdbsetup.sh` (per impostazione predefinita è disponibile in `DIRINSTALL/sap_bobj/`).
 3. Selezionare l'opzione 4 ("copia"), quindi confermare la scelta.
 4. Selezionare il tipo di database per il database CMS di origine, quindi specificarne le relative informazioni (inclusi il nome host, il nome utente e la password).
 5. Selezionare il tipo di database per il database CMS di destinazione, quindi specificarne le relative informazioni (inclusi il nome host, il nome utente e la password).
- Il database CMS viene copiato nel database di destinazione. Al termine della copia, viene visualizzato un messaggio.

Gestione dei server del contenitore di applicazioni Web (WACS)

12.1 WACS

12.1.1 Server contenitore applicazioni Web (WACS)

I server del contenitore di applicazioni Web (WACS) forniscono una piattaforma per l'host delle applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence. Ad esempio, una console CMC può essere ospitata in un server WACS.

WACS semplifica l'amministrazione del sistema rimuovendo diversi flussi di lavoro in precedenza richiesti per la configurazione dei server di applicazioni e la distribuzione delle applicazioni Web e offrendo un'interfaccia amministrativa coerente e semplificata.

Le applicazioni Web vengono distribuite automaticamente in WACS. Il server WACS non supporta la distribuzione manuale o WDeploy della piattaforma BI o di applicazioni Web esterne.

12.1.1.1 Necessità dei server WACS

Se non si desidera utilizzare un server di applicazioni Java per ospitare le applicazioni Web SAP BusinessObjects, è possibile ospitarle sul WACS.

Se si intende utilizzare un server di applicazioni Java supportato per distribuire le applicazioni Web della piattaforma BI o se si installa la piattaforma BI in un sistema UNIX, non è necessario installare né utilizzare i server WACS.

12.1.1.2 Vantaggi dell'utilizzo di un server WACS

L'utilizzo di WACS per ospitare la console CMC offre numerosi vantaggi:

- Il server WACS richiede interventi minimi per l'installazione, la manutenzione e la configurazione.
- Tutte le applicazioni ospitate sono predistribuite nel server WACS, in modo da evitare ulteriori operazioni manuali.
- WACS è supportato da SAP.
- Con il server WACS non occorre avere competenze di amministrazione e manutenzione di server di applicazioni Java.
- Il server WACS offre un'interfaccia amministrativa coerente con quella di altri server della piattaforma BI.

12.1.1.3 Operazioni comuni

Attività	Descrizione	Argomento
Come migliorare le prestazioni delle applicazioni Web o dei servizi Web ospitati sul server WACS.	Per migliorare le prestazioni delle applicazioni Web o dei servizi Web installando il server WACS su più computer.	<ul style="list-style-type: none"> • Aggiunta o rimozione di WACS aggiuntivi alla distribuzione • Clonazione di un Server del contenitore di applicazioni Web
Come migliorare la disponibilità del livello Web	Creare WACS aggiuntivi nella distribuzione in modo che, in caso di errore hardware o software in un server, un altro possa continuare a servire le richieste.	Aggiunta o rimozione di WACS aggiuntivi alla distribuzione
Come creare un ambiente in cui sia possibile recuperare facilmente in caso di console CMC configurata in modo errato.	Creare un secondo WACS, non avviato, e utilizzarlo per definire un modello di configurazione. Qualora il primo WACS perda la configurazione corretta, utilizzare il secondo WACS finché non si configura il primo server oppure applicare il modello di configurazione al primo server.	Aggiunta o rimozione di WACS aggiuntivi alla distribuzione
Come migliorare la protezione della comunicazione tra client e WACS	Configurare HTTPS su WACS.	<ul style="list-style-type: none"> • Configurazione di HTTPS/SSL • Utilizzo dei WACS con i firewall

Attività	Descrizione	Argomento
Come migliorare la protezione della comunicazione tra WACS e altri server della piattaforma BI nella distribuzione corrente	Configurare la comunicazione SSL tra WACS e altri server della piattaforma BI nella distribuzione.	<ul style="list-style-type: none"> • Configurazione dei server per SSL • Utilizzo dei WACS con i fire-wall
È possibile utilizzare WACS con HTTPS e un proxy inverso?	È possibile utilizzare il WACS con HTTPS e un proxy inverso se si crea due WACS e si configurano entrambi i server con HTTPS. Utilizzare il primo WACS per la comunicazione nella rete interna e l'altro WACS per la comunicazione con una rete esterna attraverso un proxy inverso.	Per configurare il WACS affinché supporti HTTPS con un proxy inverso
Come inserire il WACS in un ambiente IT	È possibile distribuire il WACS in un ambiente IT con server Web esistenti, bilanciatori del carico hardware, proxy inversi e firewall.	<ul style="list-style-type: none"> • Utilizzo del WACS con altri server Web • Utilizzo del WACS con un bilanciatore di carico • Utilizzo del WACS con un proxy inverso • Utilizzo dei WACS con i fire-wall
È possibile utilizzare WACS in una distribuzione con un bilanciatore di carico?	È possibile utilizzare il WACS in una distribuzione che utilizza un bilanciatore del carico hardware. Il server WACS stesso non può essere utilizzato come bilanciatore di carico.	Utilizzo del WACS con un bilanciatore di carico
È possibile utilizzare il WACS in una distribuzione con un proxy inverso?	È possibile utilizzare il WACS in una distribuzione con un proxy inverso. Il server WACS stesso non può essere utilizzato come proxy inverso.	Utilizzo del WACS con un proxy inverso
Come risolvere i problemi relativi ai server WACS installati?	Per determinare la causa di prestazioni non ottimali del server WACS, è possibile esaminare i file di registro e visualizzare le metriche di sistema.	<ul style="list-style-type: none"> • Configurazione dell'analisi sul server WACS • Per visualizzare le specifiche del server

Attività	Descrizione	Argomento
Non viene servita alcuna pagina su una determinata porta. Errore	<p>Numerose possono essere le ragioni dell'impossibilità di connettersi a un server WACS. Verificare se:</p> <ul style="list-style-type: none"> Le porte HTTP, HTTP su proxy e HTTPS specificate per il WACS sono occupate da altre applicazioni. La memoria allocata al WACS è sufficiente. Il WACS consente un numero di richieste simultanee sufficiente. Se necessario, ripristinare i valori predefiniti di sistema per il server WACS. 	<ul style="list-style-type: none"> Per risolvere i conflitti tra porte HTTP Per modificare le impostazioni di memoria Per modificare il numero di richieste simultanee Per ripristinare i valori predefiniti di sistema
Come configurare le proprietà delle applicazioni Web ospitate sul server WACS.	La procedura per la configurazione delle proprietà delle applicazioni Web dipende dalla proprietà e dall'applicazione Web specifica. Per ulteriori informazioni, consultare la sezione "Configurazione delle proprietà delle applicazioni Web" di questo capitolo.	Configurazione delle proprietà delle applicazioni Web
Dove sono elencate le proprietà del WACS?	Nella sezione "Appendice sulle proprietà dei server" di questo manuale è contenuto un elenco delle proprietà dei server WACS.	Proprietà dei servizi principali

12.1.2 Aggiunta o rimozione di WACS aggiuntivi alla distribuzione

L'aggiunta di un WACS alla distribuzione può comportare numerosi vantaggi:

- Recupero più rapido da un server configurato in modo errato.
- Disponibilità server più elevata.
- Bilanciamento del carico migliorato.
- Prestazioni complessive ottimali.

Sono disponibili tre modi per aggiungere ulteriori WACS alla distribuzione:

- Installazione di un WACS in un computer.
- Creazione di un nuovo WACS.
- Duplicazione di un WACS.

Nota:

È consigliabile eseguire un solo WACS nello stesso computer in un determinato momento a causa dell'elevato consumo di risorse. È tuttavia possibile distribuire più di un WACS nello stesso computer ed eseguirne uno solo per consentire il recupero in caso di WACS configurato in modo errato.

12.1.2.1 Installazione dei server WACS

L'installazione di WACS in computer separati può fornire alla distribuzione migliori prestazioni, un migliore bilanciamento del carico e una disponibilità server più elevata. Se la distribuzione contiene due o più WACS in computer separati, la disponibilità delle applicazioni e dei servizi Web non sarà interessata dagli errori hardware o software di un computer specifico, in quanto l'altro server WACS continuerà a fornire i servizi.

È possibile installare un Server del contenitore applicazioni Web utilizzando il programma di installazione della piattaforma BI. Sono disponibili due modi per installare WACS:

- Nella schermata "Seleziona server di applicazioni Web Java" di un'installazione completa scegliere **Installare il server del contenitore applicazioni Web e distribuire automaticamente le applicazioni Web**.

Se si seleziona un server di applicazioni Java in una nuova installazione, il WACS non viene installato.

- In un'installazione personalizzata o espansa è possibile scegliere di installare il server WACS nella schermata "Seleziona funzionalità" espandendo **Server > Servizi piattaforma** e selezionando **Server del contenitore applicazioni Web**.

Se si installa un WACS, il programma di installazione crea automaticamente un server denominato `NODE.WebApplicationContainerServer`, dove `NODE` è il nome del nodo. Le applicazioni e i servizi Web della piattaforma BI vengono quindi distribuiti in tale server. Non sono richieste operazioni manuali per distribuire o configurare CMC. Il sistema è pronto all'uso.

Quando si installa un WACS, il programma di installazione chiede di fornire un numero di porta HTTP per il WACS. Assicurarsi di specificare un numero di porta non utilizzato. Il numero di porta predefinito è 6405. Se si intende consentire agli utenti di connettersi al WACS dall'esterno di un firewall, è necessario assicurarsi che la porta HTTP del server sia aperta sul firewall.

WACS è supportato solo nei sistemi operativi Windows.

Nota:

Le applicazioni Web ospitate dal server WACS vengono automaticamente distribuite quando si installa il server WACS o quando si applicano aggiornamenti o hot fix al server WACS o alle applicazioni Web

ospitate su server WACS. La distribuzione delle applicazioni Web richiede alcuni minuti. Fino al completamento della distribuzione dell'applicazione Web, il server WACS si trova nello stato "Inizializzazione in corso". Gli utenti non saranno in grado di accedere alle applicazioni Web ospitate su server WACS fino al completamento della distribuzione di tali applicazioni. Non arrestare il server finché la distribuzione iniziale non sarà stata completata. È possibile visualizzare lo stato del server WACS da Central Configuration Manager (CCM).

Questo ritardo si verifica solo al primo avvio del server WACS dopo l'installazione o l'applicazione di aggiornamenti. I successivi riavvii del server WACS non richiedono tempi prolungati.

Non è possibile distribuire manualmente le applicazioni Web in un server WACS. Non è possibile utilizzare WDeploy per distribuire le applicazioni Web nel server WACS.

12.1.2.2 Aggiunta di un nuovo Server del contenitore di applicazioni Web

Nota:

È consigliabile eseguire un solo WACS nello stesso computer in un determinato momento a causa dell'elevato consumo di risorse. È tuttavia possibile distribuire più di un WACS nello stesso computer ed eseguirne uno solo per consentire il recupero in caso di WACS configurato in modo errato.

1. Passare all'area di gestione "Server" della CMC.
2. Selezionare **Gestisci > Nuovo > Nuovo server**.
Viene visualizzata la schermata "Crea nuovo server".
3. Nell'elenco **Categoria di servizio** selezionare **Servizi principali**.
4. Nell'elenco **Selezionare un servizio** selezionare i servizi che devono essere ospitati da WACS e fare clic su **Avanti**.
 - Se si desidera che il server WACS ospiti applicazioni Web quali CMC, BI Launch Pad oppure Open Document, selezionare **Servizio applicazione Web BOE**.
 - Se si desidera che il server WACS ospiti servizi Web quali Live Office o Query come servizio Web (QaaWS), selezionare **SDK di servizi Web e servizio QaaWS**.
 - Se si desidera che il server WACS ospiti i servizi Web Business Process BI, selezionare **Servizio Web Business Process BI**.
5. Nella schermata successiva "Crea nuovo server" selezionare eventuali servizi aggiuntivi che devono essere ospitati da WACS e fare clic su **Avanti**.
6. Nella schermata successiva "Crea nuovo server" selezionare un nodo a cui aggiungere il server, digitare un nome, una porta e una descrizione per il server, quindi fare clic su **Crea**.

Nota:

solo i nodi in cui è installato il WACS figureranno nell'elenco **Nodo**.

7. Nella schermata "Server" fare doppio clic sul nuovo WACS.
Viene visualizzata la schermata "Proprietà".

8. Se non si desidera che il server WACS venga avviato automaticamente al riavvio del sistema, nel riquadro "Impostazioni comuni" verificare che la casella di controllo **Avvia automaticamente questo server all'avvio di Server Intelligence Agent** non sia selezionata.

9. Fare clic su **Salva e chiudi**.

Viene creato un nuovo WACS. Le impostazioni predefinite e le proprietà vengono applicate al server.

12.1.2.3 Clonazione di un Server del contenitore di applicazioni Web

Come alternativa all'aggiunta di un nuovo WACS alla distribuzione, è anche possibile duplicare un WACS, nello stesso computer o in uno diverso. Se l'aggiunta di un nuovo WACS comporta la creazione di un server con le impostazioni predefinite, la duplicazione di un WACS comporta l'applicazione delle impostazioni del WACS di origine nel nuovo WACS.

I server possono essere duplicati solo nei computer in cui è già installato un WACS.

Nota:

È consigliabile eseguire un solo WACS nello stesso computer in un determinato momento a causa dell'elevato consumo di risorse. È tuttavia possibile distribuire più di un WACS nello stesso computer ed eseguirne uno solo per consentire il recupero in caso di WACS configurato in modo errato.

1. Passare all'area di gestione "Server" della CMC.
2. Selezionare il WACS che si desidera duplicare, fare clic con il pulsante destro del mouse e selezionare **Duplica server**.

Nella schermata "Duplica server" viene visualizzato un elenco di nodi nella distribuzione in cui è possibile duplicare il WACS. Solo i nodi in cui sono installati WACS sono visualizzati nell'elenco **Duplica su nodo**.

3. Nella schermata "Duplica server" digitare un nuovo nome di server, selezionare il nodo in cui duplicare il server e fare clic su **OK**.

Viene creato un nuovo WACS. Il nuovo server contiene gli stessi servizi del server da cui è stato duplicato. Il nuovo server e i servizi che ospita presentano le stesse impostazioni del server da cui è stato duplicato, ad eccezione del nome del server.

Nota:

Se un WACS è stato duplicato nello stesso computer, è possibile che si verifichino conflitti di porta con il WACS utilizzato per la duplicazione. In questo caso, è necessario modificare i numeri di porta nell'istanza del WACS appena creata.

Argomenti correlati

- [Per risolvere i conflitti tra porte HTTP](#)

12.1.2.4 Eliminazione di WACS dalla distribuzione

È possibile eliminare un WACS solo se non ospita attualmente il servizio CMC. Se si desidera eliminare un WACS dalla distribuzione, è necessario accedere al servizio CMC da un altro WACS o server di applicazioni Java. Non è possibile eliminare un WACS se attualmente ospita il servizio CMC.

1. Passare all'area di gestione "Server" della CMC.
2. Arrestare il server che si desidera eliminare facendo clic con il pulsante destro del mouse su di esso e facendo clic su **Arresta server**.
3. Fare clic con il pulsante destro del mouse sul server e selezionare **Elimina**.
4. Quando viene richiesto di confermare l'operazione, fare clic su **OK**.

12.1.3 Aggiunta o rimozione di servizi dal server WACS

12.1.3.1 Aggiunta di un'applicazione Web o di un servizio Web a un server WACS

L'aggiunta di ulteriori applicazioni o servizi Web della piattaforma BI a un server WACS richiede l'arresto del server in questione. È pertanto necessario disporre di almeno una console CMC aggiuntiva ospitata in un server WACS nella distribuzione in grado di fornire il servizio applicazione Web BOE durante l'arresto e l'aggiunta di un servizio Web all'altro server WACS.

Quando si aggiunge un servizio al WACS, il servizio viene distribuito automaticamente nel WACS al riavvio del server.

1. Passare all'area di gestione "Server" della CMC.
2. Fare doppio clic sul WACS a cui si desidera aggiungere il servizio e visualizzare le proprietà del server per assicurarsi che il servizio da aggiungere non sia già presente.
3. Fare clic su **Annulla** per tornare alla schermata "Server".
4. Arrestare il server facendo clic con il pulsante destro del mouse e selezionando **Arresta server**.
Se si tenta di arrestare il WACS che ospita il servizio CMC, viene visualizzato un messaggio di avviso. Non procedere a meno che non sia presente almeno un altro servizio applicazione Web BOE aggiuntivo in esecuzione in un altro WACS all'interno della distribuzione. Se si esegue questa operazione, fare clic su **OK**, accedere a un altro WACS e avviare la procedura dall'inizio.
5. Fare clic con il pulsante destro del mouse sul server e scegliere **Seleziona servizi**.
Verrà visualizzata la schermata "Seleziona servizi".

6. Selezionare il servizio da aggiungere al server, aggiungerlo facendo clic su **>**, quindi su **OK**.
7. Avviare il WACS facendo clic con il pulsante destro del mouse sul server e selezionando **Avvia server**.

Il servizio viene aggiunto al WACS. Vengono applicate le impostazioni e le proprietà predefinite del servizio.

12.1.3.2 Rimozione di un'applicazione Web o di un servizio Web da un server WACS

Per poter rimuovere un'applicazione o un servizio Web da un server WACS, è necessario accedere a una CMC su un altro server WACS o su un server di applicazioni Java. Non è possibile arrestare il WACS che sta fornendo il servizio CMC.

Non è possibile eliminare l'ultimo servizio da un WACS. Se pertanto si rimuove un servizio Web da un server WACS, è necessario assicurarsi che il server ospiti almeno un altro servizio.

Se si desidera rimuovere l'ultimo servizio da un server WACS, eliminare il server WACS stesso.

1. Passare all'area di gestione "Server" della CMC.
2. Fare doppio clic sul WACS da cui si desidera rimuovere il servizio Web e visualizzare le proprietà del server per assicurarsi che il servizio Web da rimuovere sia presente.
3. Fare clic su **Annulla** per tornare alla schermata "Server".
4. Arrestare il WACS facendo clic con il pulsante destro del mouse sul server e selezionando **Arresta server**.

Se si tenta di arrestare il WACS che ospita il servizio CMC, viene visualizzato un messaggio di avviso. Non procedere a meno che non sia presente almeno un altro servizio applicazione Web BOE aggiuntivo in esecuzione in un altro WACS all'interno della distribuzione. Se si esegue questa operazione, fare clic su **OK**, accedere a un altro WACS e avviare la procedura dall'inizio.

5. Fare clic con il pulsante destro del mouse sul server WACS e scegliere **Seleziona servizi**.
Verrà visualizzata la schermata "Seleziona servizi".
6. Selezionare il servizio da rimuovere, fare clic su **<** e quindi su **OK**.
7. Avviare il WACS facendo clic con il pulsante destro del mouse sul server e selezionando **Avvia server**.

Il servizio viene rimosso dal WACS.

12.1.4 Configurazione di HTTPS/SSL

È possibile utilizzare il protocollo Secure Sockets Layer (SSL) e HTTP per la comunicazione di rete tra client e WACS nella distribuzione della piattaforma BI. SSL/HTTPS crittografa il traffico di rete e fornisce una protezione migliorata.

Esistono due tipi di SSL:

- SSL utilizzato tra i server della piattaforma BI, inclusi il server WACS e altri server della piattaforma BI nella distribuzione. Questo protocollo è noto come CORBA SSL. Per ulteriori informazioni sull'utilizzo di SSL tra i server della piattaforma BI nella distribuzione, consultare la sezione relativa alle "comunicazioni tra i componenti della piattaforma SAP BusinessObjects Business Intelligence" del capitolo sull'"utilizzo dei firewall" nel *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.
- HTTP su SSL, tra WACS e client (ad esempio, browser) che comunicano con WACS.

Nota:

Se si distribuisce il server WACS in una distribuzione con un proxy o un proxy inverso e si desidera utilizzare SSL per proteggere la comunicazione in rete nella distribuzione, è necessario creare due WACS. Per ulteriori informazioni, consultare la sezione relativa all'*utilizzo dei WACS con un proxy inverso*.

Per configurare HTTPS/SSL in un server WACS, è necessario eseguire la procedura seguente:

- Generare o ottenere un archivio di certificati PKCS12 o un archivio di chiavi JKS contenente certificati e chiavi private. È possibile utilizzare Microsoft Internet Information Service (IIS) e Microsoft Management Console (MMC) per generare un file PCKS12 oppure utilizzare openssl o lo strumento da riga di comando Java keytool per generare un file dell'archivio di chiavi.
- Se si desidera che solo alcuni client si connettano a un WACS, è necessario generare un file dell'elenco di certificati attendibili.
- Quando si dispone di un archivio di certificati e, se necessario, di un file di elenco di certificati attendibili, copiare i file nel computer WACS.
- Configurare HTTPS nel WACS.

Argomenti correlati

- [Informazioni sulla comunicazione tra componenti della piattaforma BI](#)
- [Utilizzo del WACS con un proxy inverso](#)

12.1.4.1 Per generare un archivio di file di certificati PKCS12

Esistono diversi modi per generare un archivio di chiavi Java o di file di certificati PKCS12, nonché diversi strumenti. Il metodo da utilizzare dipende dagli strumenti accessibili e conosciuti.

In questo esempio viene illustrato come generare un file PKCS12 tramite Microsoft Internet Information Services (IIS) e Microsoft Management Console (MMC) per Windows Server 2008.

1. Accedere al computer che ospita il WACS come amministratore.

2. In IIS richiedere un certificato a un'autorità di certificazione. Per informazioni, vedere la Guida di IIS.
 3. Avviare MMC facendo clic sul pulsante **Start > Esegui**, digitando mmc.exe e facendo clic su **OK**.
 4. Aggiungere lo snap-in Certificati alla MMC:
 - a. Dal menu **File** fare clic su **Aggiungi/Rimuovi snap-in**.
Viene visualizzata la schermata "Aggiungi o rimuovi snap-in".
 - b. Dall'elenco "Snap-in disponibili" selezionare **Certificati** e fare clic su **Aggiungi**.
 - c. Selezionare **Account computer** e fare clic su **Avanti**.
 - d. Selezionare **Computer locale** e fare clic su **Fine**.
 - e. Fare clic su **OK**.Lo snap-in Certificati viene aggiunto a MMC.
 5. In MMC, espandere **Certificati** e selezionare il certificato che desideri utilizzare.
 6. Nel menu **Azione** selezionare **Tutti i task > Esporta**.
Viene avviata l'"Esportazione guidata certificati".
 7. Fare clic su **Avanti**.
 8. Selezionare **Esporta la chiave privata** e fare clic su **Avanti**.
 9. Selezionare **Personal Information Exchange - PKCS #12 (.PFX)** e fare clic su **Avanti**.
 10. Immettere la password utilizzata per la creazione del certificato e fare clic su **Avanti**. È necessario specificare questa password nel campo **Password accesso chiave privata** quando si configura HTTPS per il WACS.
- Viene creato un archivio di certificati PKCS12.

12.1.4.2 Per generare un elenco di certificati attendibili

1. Accedere al computer che ospita il WACS come amministratore.
2. Avviare Microsoft Management Console (MMC).
3. Aggiungere lo snap-in Internet Information Services:
 - a. Dal menu **File** selezionare **Aggiungi/Rimuovi snap-in**.
 - b. Nell'elenco "Snap-in disponibili" selezionare **Gestione Internet Information Services (IIS)** e fare clic su **Aggiungi**.
 - c. Fare clic su **OK**.Lo snap-in IIS viene aggiunto a MMC.
4. Seguire la procedura qui descritta per creare un elenco degli scopi consentiti ai certificati:
<http://www.iis.net/learn/install/installing-iis-7/compatibility-and-feature-requirements-for-windows-vista#NoWizard>.

12.1.4.3 Per configurare HTTPS/SSL

Prima di configurare HTTPS/SSL sul WACS, assicurarsi di avere già creato un file PKCS12 o un archivio di chiavi JKS e di avere copiato o spostato il file nel computer che ospita il WACS.

1. Passare all'area di gestione "Server" della CMC.
2. Fare doppio clic sul server WACS per il quale abilitare HTTPS.
Viene visualizzata la schermata "Proprietà".
3. Nella sezione "Configurazione HTTPS" selezionare la casella di controllo **Abilita HTTPS**.
4. Nel campo **Associa a nome host o indirizzo IP** specificare l'indirizzo IP per cui sono stati emessi i certificati e a cui verrà associato il WACS.
I servizi HTTPS verranno forniti tramite un indirizzo IP specificato.
5. Nel campo **Porta HTTPS** specificare un numero di porta per il WACS per fornire il servizio HTTPS. È necessario assicurarsi che questa porta sia libera. Se si intende consentire agli utenti di connettersi al WACS dall'esterno di un firewall, è necessario assicurarsi che questa porta sia aperta sul firewall.
6. Se si configura SSL con un proxy inverso, specificare la porta e il nome host del server proxy nei campi **Nome host proxy** e **Porta proxy**.
7. Nell'elenco **Protocollo** selezionare un protocollo. Le opzioni disponibili sono:
 - **SSL**
SSL è il protocollo Secure Sockets Layer, un protocollo per la crittografia del traffico di rete.
 - **TLS**
TLS è il protocollo Transport Layer Security, un protocollo migliorato e più avanzato. Le differenze tra SSL e TLS sono minime, ma in TLS sono inclusi algoritmi di crittografia più potenti.
8. Nel campo **Tipo di archivio certificati** specificare il tipo di file per il certificato. Le opzioni disponibili sono:
 - **PKCS12**
Selezionare PKCS12 se si preferisce utilizzare gli strumenti Microsoft.
 - **JKS**
Selezionare JKS se si preferisce utilizzare gli strumenti Java.
9. Nel campo **Percorso file archivio certificati** specificare il percorso in cui è stato copiato o spostato il file dell'archivio chiavi Java o l'archivio di certificati.
10. Nel campo **Password accesso chiave privata** specificare la password.
Gli archivi certificati PKCS12 e gli archivi di chiavi JKS presentano chiavi private protette con password per impedire accessi non autorizzati. È necessario specificare la password per l'accesso alle chiavi private in modo che il WACS possa accedere alle chiavi private.

11. È consigliabile utilizzare un archivio certificati o un archivio di chiavi che contenga un singolo certificato o in cui il certificato che si desidera utilizzare sia elencato per primo. Se si utilizza un archivio certificati o un archivio di chiavi che contiene più di un certificato e quel certificato non è il primo nell'archivio, nel campo **Alias certificato** è necessario specificare l'alias per il certificato.
12. Se si desidera che il WACS accetti unicamente le richieste HTTPS da determinati client, abilitare l'autenticazione client.
L'autenticazione client non autentica gli utenti. Assicura che il WACS serva unicamente le richieste HTTPS a determinati client.
 - a. Selezionare **Abilita autenticazione client**.
 - b. In **Percorso file elenco certificati attendibili** specificare il percorso del file PKCS12 o dell'archivio chiavi JKS contenente il file dell'elenco di certificati attendibili.
Nota:
Il tipo di elenco di certificati attendibili deve corrispondere al tipo di archivio certificati.
 - c. Nel campo **Password accesso chiave privata elenco certificati attendibili** digitare la password che protegge l'accesso alle chiavi private nel file dell'elenco di certificati attendibili.
Nota:
Se si abilita l'autenticazione client e un servizio Web o browser non è autenticato, la connessione HTTPS viene rifiutata.
13. Fare clic su **Salva e chiudi**.
14. Accedere alla schermata "Metriche" e assicurarsi che il connettore HTTPS sia visualizzato nell'elenco Connettori WACS in esecuzione. Se HTTPS non figura, assicurarsi che il connettore HTTPS sia configurato correttamente.

12.1.5 Metodi di autenticazione supportati

Il server WACS supporta i seguenti metodi di autenticazione:

- Enterprise
- LDAP
- AD Kerberos

Il server WACS non supporta i seguenti metodi di autenticazione:

- NT
- AD NTLM
- LDAP con Single Sign On

12.1.6 Configurazione di AD Kerberos per server WACS

Per configurare l'autenticazione AD Kerberos per i server WACS, è necessario prima configurare il computer per il supporto di AD. È necessario eseguire le operazioni riportate di seguito.

- Abilitare il plug-in di protezione di Windows AD.
- Mappare utenti e gruppi.
- Impostare un account di servizio.
- Impostare la delega con restrizioni.
- Abilitare l'autenticazione Kerberos nel plug-in Windows AD per WACS.
- Creare file di configurazione.

Dopo avere configurato il computer che ospita il server WACS per l'utilizzo dell'autenticazione AD Kerberos, è necessario eseguire altre operazioni di configurazione dalla console CMC.

Se si configura Single Sign On tramite AD Kerberos per SDK e QaaWS di servizi Web, è anche necessario configurare sia il server WACS sia il computer che ospita WACS.

Argomenti correlati

- [Plug-in di protezione di Windows AD](#)
- [Per mappare gli utenti e i gruppi AD](#)
- [Impostazione di un account di servizio per l'autenticazione AD con Kerberos](#)
- [Esecuzione del SIA nell'account di servizio della piattaforma BI](#)
- [Abilitazione dell'autenticazione Kerberos nel plug-in Windows AD per WACS](#)
- [Creazione di file di configurazione](#)
- [Configurazione di WACS per AD Kerberos](#)
- [Configurazione del Single Sign On AD Kerberos](#)

12.1.6.1 Abilitazione dell'autenticazione Kerberos nel plug-in Windows AD per WACS

Per supportare Kerberos è necessario configurare il plug-in di protezione di Windows AD nella console CMC per l'utilizzo dell'autenticazione Kerberos. Le operazioni richieste sono:

- Verifica dell'attivazione dell'autenticazione Windows AD.
- Immissione dell'account dell'amministratore AD

Nota:

Questo account richiede accesso in lettura solo per Active Directory, nessun'altra autorizzazione è necessaria.

- Abilitazione dell'autenticazione Kerberos e Single Sign On, se richiesto.
- Immissione del nome principale di servizio (SPN) per l'account di servizio

12.1.6.1.1 Prerequisiti

Prima di configurare il plug-in di protezione di Windows AD per Kerberos, è necessario completare le seguenti attività:

- [Impostazione di un account di servizio per l'autenticazione AD con Kerberos](#)
- [Esecuzione del SIA nell'account di servizio della piattaforma BI](#)
- [Per mappare gli utenti e i gruppi AD](#)

12.1.6.1.2 Per configurare il plug-in di protezione Windows AD per Kerberos

1. Passare all'area di gestione **Autenticazione** della CMC.
2. Fare doppio clic su **Windows AD**.
3. Verificare che la casella di controllo **Abilita Windows Active Directory (AD)** sia selezionata.
4. In **Opzioni di autenticazione**, selezionare **Usa autenticazione Kerberos**.
5. Per configurare il Single Sign On in un database, selezionare la casella di controllo **Contesto di protezione della cache** (richiesto per SSO al database).
6. Nel campo **Nome principale servizio**, immettere l'account e il dominio dell'account di servizio o il mapping SPN all'account di servizio.

Utilizzare il formato riportato di seguito, dove *svcacct* è il nome dell'account di servizio o SPN creato in precedenza e *DNS.COM* è il nome del dominio completo in lettere maiuscole. Ad esempio, l'account di servizio sarà *svcacct@DNS.COM* e l'SPN sarà *BOBJCentralMS/nome@DOMINIO.COM*.

Nota:

- Se si intende consentire l'accesso a utenti che non appartengono al dominio predefinito, è necessario fornire l'SPN mappato in precedenza.
 - L'account di servizio rileva la distinzione tra lettere maiuscole e minuscole. L'ortografia dell'account deve corrispondere esattamente a quanto impostato nel dominio Active Directory.
 - Questo nome deve corrispondere allo stesso account utilizzato per eseguire i server della piattaforma BI o all'SPN mappato a questo account.
7. Per configurare il Single Sign-On, selezionare **Abilita il Single Sign-On per la modalità di autenticazione selezionata**.

Nota:

Se si è scelto di abilitare il Single Sign-On sarà necessario configurare il server WACS.

Argomenti correlati

- [Configurazione del Single Sign On AD Kerberos](#)

12.1.6.2 Creazione di file di configurazione

Il processo generale di configurazione di Kerberos nel server di applicazioni include i seguenti passaggi:

- Creazione del file di configurazione di Kerberos.
- Creazione del file di configurazione per l'accesso JAAS.

Nota:

- Il dominio predefinito Active Directory deve essere nel formato DNS in lettere maiuscole.
- Non è necessario scaricare e installare MIT Kerberos per Windows. Non è più necessario neanche il codice per l'account di servizio.

12.1.6.2.1 Per creare il file di configurazione di Kerberos

Attenersi alla procedura seguente per creare il file di configurazione di Kerberos.

1. Creare il file `krb5.ini`, se non è già presente, e memorizzarlo in `C:\Windows` per Windows.

Nota:

È possibile memorizzare il file in un altro percorso. In questo caso, tuttavia, è necessario specificare il percorso nel campo **Posizione file Krb5.ini** nella pagina "Proprietà" per il server WACS nella console CMC.

2. Aggiungere le seguenti informazioni necessarie nel file di configurazione di Kerberos:

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_enctypes = rc4-hmac
default_tgs_enctypes = rc4-hmac
[domain_realm]
.domain.com = DOMAIN.COM
domain.com = DOMAIN.COM
.domain2.com = DOMAIN2.COM
domain2.com = DOMAIN2.COM
[realms]
DOMAIN.COM = {
default_domain = DOMAIN.COM
kdc = HOSTNAME.DOMAIN.COM
}
DOMAIN2.COM = {
default_domain = DOMAIN2.COM
kdc = HOSTNAME.DOMAIN2.COM
}
[capaths]
DOMAIN2.COM = {
DOMAIN.COM =
```

Nota:

- `DNS.COM` è il nome DNS del dominio che deve essere immesso in lettere maiuscole nel formato FQDN.
- `kdc` è il nome host del controller di dominio.
- È possibile aggiungere più domini nella sezione `[realms]` nel caso in cui gli utenti eseguano l'accesso da domini diversi. Per un esempio di questo file con più domini consultare [Esempio di file Krb5.ini](#).
- In una configurazione con più domini, in `[libdefaults]` il valore `default_realm` potrebbe essere qualsiasi dominio desiderato. La soluzione migliore consiste nell'utilizzare il dominio con il maggior numero di utenti che verranno autenticati con i propri account AD.

12.1.6.2.2 Per creare il file di configurazione degli accessi JAAS

1. Creare un file denominato `bscLogin.conf`, se non è già presente, e memorizzarlo nel percorso predefinito: `C:\Windows`.

Nota:

È possibile memorizzare il file in un altro percorso. In questo caso, tuttavia, è necessario specificare il percorso nel campo **Posizione file bscLogin.conf** nella pagina "Proprietà" per il server WACS nella console CMC.

2. Aggiungere il codice seguente al file di configurazione `bscLogin.conf` JAAS:

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
```

3. Salvare e chiudere il file.

12.1.6.2.3 Esempio di file Krb5.ini

Esempio di file Krb5.ini con più domini

Di seguito viene riportato un esempio di file con più domini.

```
[domain_realm]
.domain03.com = DOMAIN03.COM
domain03.com = DOMAIN03.com
.child1.domain03.com = CHILD1.DOMAIN03.COM
child1.domain03.com = CHILD1.DOMAIN03.com
.child2.domain03.com = CHILD2.DOMAIN03.COM
child2.domain03.com = CHILD2.DOMAIN03.com
.domain04.com = DOMAIN04.COM
domain04.com = DOMAIN04.com
[libdefaults]
default_realm = DOMAIN03.COM
dns_lookup_kdc = true
dns_lookup_realm = true
[realms]
DOMAIN03.COM = {
admin_server = testvmw2k07
kdc = testvmw2k07
default_domain = domain03.com
}
CHILD1.DOMAIN03.COM = {
admin_server = testvmw2k08
kdc = testvmw2k08
default_domain = child1.domain03.com
}
CHILD2.DOMAIN03.COM = {
admin_server = testvmw2k09
kdc = testvmw2k09
default_domain = child2.domain03.com
}
DOMAIN04.COM = {
admin_server = testvmw2k011
kdc = testvmw2k011
default_domain = domain04.com
}
```

Esempio di file Krb5.ini con un dominio

Di seguito viene riportato un esempio di file con un dominio.

```
[libdefaults]
default_realm = ABCD.MFROOT.ORG
dns_lookup_kdc = true
dns_lookup_realm = true
```

```
[realms]
ABCD.MFROOT.ORG = {
    kdc = ABCDIR20.ABCD.MFROOT.ORG
    kdc = ABCDIR21.ABCD.MFROOT.ORG
    kdc = ABCDIR22.ABCD.MFROOT.ORG
    kdc = ABCDIR23.ABCD.MFROOT.ORG
    default_domain = ABCD.MFROOT.ORG
}
```

12.1.6.3 Configurazione di WACS per AD Kerberos

Dopo avere configurato il computer che ospita il server WACS per l'autenticazione AD Kerberos, è necessario configurare il server WACS stesso tramite la Central Management Console (CMC).

12.1.6.3.1 Per configurare il server WACS per AD Kerberos

1. Passare all'area di gestione "Server" della CMC.
2. Fare doppio clic sul server WACS per il quale configurare AD.
Viene visualizzata la schermata "Proprietà".
3. Nel campo **Posizione file Krb5.ini** specificare il percorso del file di configurazione `krb5.ini`.
4. Nel campo **Posizione file bscLogin.conf** specificare il percorso del file di configurazione `bscLogin.conf`.
5. Fare clic su **Salva e chiudi**.
6. Riavviare il WACS.

12.1.6.4 Risoluzione dei problemi di Kerberos

Se si verificano problemi durante la configurazione di Kerberos, attenersi alle seguenti procedure:

- Abilitazione della registrazione
- Verifica della configurazione di Kerberos

12.1.6.4.1 Per abilitare la registrazione Kerberos

1. Avviare Central Configuration Manager (CCM) e fare clic su **Gestisci server**.
2. Specificare le credenziali di accesso.
3. Nella schermata "Gestisci server", arrestare il WACS.
4. Fare clic su **Configurazione livello Web**.

Nota:

L'icona **Configurazione livello Web** è disponibile solo quando si seleziona un WACS arrestato.

Viene visualizzata la schermata "Configurazione livello Web".

5. In Parametri riga di comando, copiare il testo seguente alla fine dei parametri:

```
"-Dcrystal.enterprise.trace.configuration=verbose
-Djcsi.Kerberos.debug=true"
```

6. Fare clic su OK.**7. Nella schermata "Gestisci server" avviare il WACS.****12.1.6.4.2 Per verificare la configurazione di Kerberos**

- Per verificare la configurazione di Kerberos, eseguire il comando indicato di seguito dove `servact` è l'account di servizio e il dominio in cui viene eseguito CMS e `password` è la password associata all'account di servizio.

```
INSTALLDIR\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM Password
```

Ad esempio:

```
C:\Program Files\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM Password
```

Se il problema persiste, controllare che il dominio e il nome principale di servizio immessi corrispondano esattamente a quanto impostato in Active Directory.

12.1.6.4.3 Un utente AD mappato non è in grado di accedere alla piattaforma BI su WACS

Anche se gli utenti sono stati mappati alla piattaforma BI, si potrebbero verificare i due problemi seguenti:

Errore di accesso dovuto a nomi AD UPN e SAM diversi

L'ID di Active Directory di un utente è stato correttamente mappato alla piattaforma BI. Nonostante ciò, l'utente non è in grado di accedere alla console CMC con l'autenticazione AD e Kerberos nel formato che segue: `DOMAIN\ABC123`

Questo problema può essere riscontrato quando l'utente viene impostato in Active Directory con un nome UPN e SAM che in qualche modo non corrispondono. Di seguito sono riportati due esempi in cui si può verificare un problema:

- L'UPN è `abc123@azienda.com` ma il nome SAM è `DOMINIO\ABC123`.
- L'UPN è `gricci@azienda` ma il nome SAM è `DOMINIO\giorgioricci`.

È possibile risolvere il problema in due modi:

- Fare accedere gli utenti utilizzando l'UPN anziché il nome SAM.
- Accertarsi che il nome di account SAM e il nome UPN corrispondano.

Errore di preautenticazione

È possibile che un utente precedentemente in grado di effettuare l'accesso non riesca più ad accedere correttamente. L'utente riceverà questo messaggio di errore: Informazioni sull'account non riconosciute. I registri di WACS conterranno un errore analogo al seguente "Informazioni di preautenticazione non valide(24) "

Questo errore si può verificare poiché il database utente di Kerberos non ha ricevuto una modifica da UPN in AD. Ciò potrebbe indicare che il database utente di Kerberos e le informazioni AD non sono sincronizzati.

Per risolvere il problema, reimpostare la password dell'utente in AD. In questo modo le modifiche verranno trasmesse correttamente.

12.1.7 Configurazione del Single Sign On AD Kerberos

Se si sta configurando il Single Sign On AD Kerberos per l'SDK di BI Launch Pad o Servizi Web e il servizio QaaWS, è necessario assicurarsi di aver configurato sia il server WACS che il computer che ospita WACS per l'autenticazione AD Kerberos.

Per configurare WACS per Single Sign-On AD Kerberos, è necessario configurare prima il computer che ospita WACS, quindi configurare il server WACS stesso:

Nota:

Se si intende utilizzare il Single Sign On in un ambiente proxy inverso, leggere le informazioni sulla protezione nel presente manuale.

Argomenti correlati

- [Panoramica della protezione](#)
- [Configurazione di AD Kerberos per server WACS](#)
- [Configurazione del computer per il Single Sign On AD Kerberos](#)
- [Configurazione di WACS per il Single Sign On AD Kerberos](#)

12.1.7.1 Configurazione del computer per il Single Sign On AD Kerberos

Per configurare Single Sign-On AD Kerberos per SDK di servizi Web e servizio QaaWS, è necessario configurare prima il computer che ospita WACS:

- [Per configurare la delega vincolata per il Single Sign On Vintela](#)
- [Per impostare l'account di servizio per il Single Sign On Vintela](#)
- [Impostazione di più SPN](#)
- [Aumento del limite delle dimensioni dell'intestazione per il server WACS](#)

Nelle sezioni riportate di seguito viene descritto come completare ciascuno dei passaggi.

12.1.7.1.1 Impostazione di più SPN

L'utilizzo di più SPN non è supportato.

12.1.7.1.2 Aumento del limite delle dimensioni dell'intestazione per il server WACS

Active Directory crea un token Kerberos utilizzato nel processo di autenticazione. Questo token viene memorizzato nell'intestazione HTTP. Le dimensioni predefinite dell'intestazione HTTP del server WACS sono sufficienti per la maggior parte degli utenti. Tali dimensioni possono essere configurate.

1. Passare all'area di gestione "Server" della CMC.
2. Fare doppio clic sul WACS per cui si desidera modificare le dimensioni dell'intestazione HTTP. Viene visualizzata la schermata "Proprietà".
3. Nella sezione "Configurazione HTTP", "Configurazione di HTTP tramite proxy" o "Configurazione HTTPS" specificare un valore nel campo **Dimensioni massime intestazione HTTP (in byte)**.
4. Fare clic su **Salva e chiudi**.
5. Riavviare il server.

12.1.7.2 Configurazione di WACS per il Single Sign On AD Kerberos

È possibile configurare un server del contenitore applicazioni Web per l'utilizzo di Single Sign-On AD Kerberos. Single Sign-On per AD Kerberos è supportato. NTLM AD non è supportato.

Prima di configurare WACS, è necessario configurare Single Sign-On AD Kerberos per il computer che ospita WACS.

1. Passare all'area di gestione "Server" della CMC.
2. Fare doppio clic sul WACS che si desidera configurare. Viene visualizzata la schermata "Proprietà".
3. Selezionare **Abilita Single Sign On per Kerberos Active Directory**.
4. Specificare i valori per le proprietà Dominio AD predefinito, Nome principale servizio e File di codice, quindi fare clic su **Salva e chiudi**.
5. Riavviare il WACS.

Single Sign-On per Active Directory è ora disponibile.

12.1.7.3 Configurazione di Kerberos e Single Sign-On nel database

Single Sign On nel database è supportato per le distribuzioni che soddisfano tutti i seguenti requisiti:

- La distribuzione della piattaforma BI viene eseguita su WACS.
- WACS è stato configurato con AD con Kerberos.
- Il database per cui è necessaria l'autenticazione Single Sign On è una versione supportata di SQL Server o Oracle.
- Ai gruppi o agli utenti per i quali è necessario l'accesso al database devono essere state concesse autorizzazioni all'interno di SQL Server o Oracle.
- La casella di controllo Contesto di protezione della cache (necessaria per il Single Sign-On al database) nella pagina Autenticazione AD di CMC è selezionata.

Il passaggio finale consiste nella modifica del file `krb5.ini` per supportare la funzionalità Single Sign-On nel database.

Nota:

Queste istruzioni spiegano come configurare Single Sign-On nel database. Se si desidera configurare la funzionalità Single Sign On end-to-end nel database, è necessario eseguire anche i passaggi di configurazione per Vintela Single Sign-On. Per ulteriori informazioni, consultare [Configurazione del Single Sign On AD Kerberos](#).

12.1.7.3.1 Per abilitare Single Sign-On nel database

1. Aprire il file `krb5.ini` utilizzato per la distribuzione della piattaforma BI.
La posizione predefinita di questo file è la directory `C:\Windows` nel server di applicazioni Web.
2. Passare alla sezione `[libdefaults]` del file.
3. Immettere la stringa seguente prima dell'inizio della sezione `[realms]` del file:

```
forwardable = true
```
4. Salvare e chiudere il file.
5. Riavviare WACS.

12.1.8 Configurazione di servizi Web RESTful

L'SDK dei servizi Web RESTful della piattaforma Business Intelligence consente di accedere alla piattaforma BI mediante il protocollo HTTP. In questo modo, gli utenti possono esplorare il repository della piattaforma BI e pianificare oggetti utilizzando qualsiasi linguaggio di programmazione che supporta le richieste HTTP. I servizi Web RESTful sono installati come parte di WACS.

Questa sezione illustra come amministrare i servizi Web RESTful. Per ulteriori informazioni sui servizi Web RESTful, vedere il *Manuale dello sviluppatore dei servizi Web RESTful della piattaforma Business Intelligence*.

12.1.8.1 Applicazioni

12.1.8.1.1 Configurazione dell'URL di base per i servizi Web RESTful

Se la distribuzione della piattaforma BI utilizza un server proxy o contiene più di un'istanza del server WACS (Web Application Container Server), potrebbe essere necessario configurare l'URL di base da utilizzare con i servizi Web RESTful. Prima di configurare l'URL di base è necessario conoscere il nome del server e il numero di porta sui cui avviene l'ascolto delle richieste di servizio Web RESTful.

L'URL di base viene utilizzato per ogni richiesta di servizio Web RESTful. Gli sviluppatori rilevano sistematicamente l'URL di base e lo utilizzano per indirizzare le richieste di servizio Web RESTful al server e alla porta corretti. L'URL viene inoltre utilizzato per le risposte del servizio Web RESTful per definire i collegamenti ipertestuali ad altre risorse RESTful.

Nota:

Nelle installazioni predefinite della piattaforma BI, l'URL di base è definito come `http://<servername>:6405/biprws`. Sostituire `<servername>` con il nome del server che ospita i servizi Web RESTful.

1. Effettuare l'accesso alla CMC (Central Management Console) come amministratore.
2. Nella CMC fare clic su **Applicazioni**.
Viene visualizzato un elenco di applicazioni.
3. Fare clic con il pulsante destro del mouse su **Servizio Web RESTful > Proprietà**.
Viene visualizzata la finestra di dialogo "Proprietà".
4. Nella casella di testo **URL di accesso**, digitare il nome dell'URL di base per i servizi Web RESTful.
Digitare ad esempio `http://<servername>:<portnumber>/biprws`. Sostituire `<servername>` e `<portnumber>` con il nome del server e con la porta su cui avviene l'ascolto del servizio Web RESTful.
5. Fare clic su **Salva e chiudi**.

12.1.8.2 Proprietà del server WACS

12.1.8.2.1 Configurazione dei parametri della riga di comando per metodi e intestazioni

Gli amministratori possono definire quali metodi e intestazioni possono essere utilizzati dai servizi Web RESTful aggiungendo le opzioni appropriate a "Parametri riga di comando" nelle proprietà del Servizio contenitore applicazioni (WACS). Le modifiche ai parametri richiedono il riavvio del servizio WACS.

1. Accedere alla Central Management Console come amministratore.
2. Fare clic su **Server**, quindi su **Elenco server**.
3. Fare clic con il pulsante destro del mouse sul Server del contenitore applicazioni Web (WACS), ad esempio `MySIA.WebApplicationContainerServer` e scegliere **Proprietà**.

Viene visualizzata la scheda **Proprietà** del server WACS.

4. Nell'area "Parametri riga di comando" immettere i metodi e le intestazioni consentiti.
Ogni gruppo di opzioni è racchiuso tra virgolette. Utilizzare metodi diversi da `GET`, `HEAD` e `POST`. Utilizzare le virgole per separare i valori di opzioni quali `PUT` e `DELETE`, come illustrato nel seguente esempio.

```
"-Dcom.sap.bip.rs.cors.extra.methods= PUT, DELETE"
"-Dcom.sap.bip.rs.cors.extra.headers= X-SAP-LogonToken, X-SAP-PVL, WWW-Authenticate"
```

Nota:

Il valore predefinito per consentire tutti i metodi e le intestazioni è `*` (asterisco). La totale omissione dei parametri della riga di comando ha lo stesso effetto.

5. Fare clic su **Salva e chiudi**.
6. Riavviare il servizio facendo clic con il pulsante destro del mouse sul nome del server WACS, ad esempio `MySIA.WebApplicationContainerServer`, e scegliendo **Riavvia server**.

12.1.8.2.2 Configurazione delle proprietà del sistema

Abilitazione dello stack dei messaggi di errore

Un amministratore ha la facoltà di configurare i messaggi di errore restituiti dai servizi Web RESTful in modo che venga incluso lo stack errori. Lo stack errori offre informazioni di debug extra utilizzabili per scoprire il punto in cui si sono verificati gli errori.

Nota:

non è consigliabile abilitare lo stack errori negli scenari di produzione, in quanto potrebbe fornire informazioni sulla piattaforma BI che non si desidera rivelare agli utenti finali. Si consiglia invece di abilitare lo stack errori negli scenari di produzione quando necessario per il debug, e di disabilitarlo quando non è più necessario.

1. Effettuare l'accesso alla Central Management Console come amministratore.
2. Fare clic su **Server**, quindi su **Elenco server**.
3. Fare clic con il pulsante destro del mouse sul Server del contenitore applicazioni Web (WACS); ad esempio, fare clic con il pulsante destro del mouse su `MySIA.WebApplicationContainerServer` e scegliere **Proprietà**.

Viene visualizzata la scheda **Proprietà** del server WACS.

4. Nell'area **Servizio Web RESTful**, selezionare **Mostra stack errori**.
5. Fare clic su **Salva e chiudi**.

Le informazioni sullo stack errori vengono incluse nei messaggi di errore del servizio Web RESTful.

Impostazione del numero predefinito di voci visualizzate in ogni pagina

Quando una risposta del servizio Web RESTful contiene un feed con un grande numero di voci, tale risposta può essere divisa in pagine. È possibile configurare il numero predefinito di voci visualizzate in ciascuna pagina. Quando gli sviluppatori creano richieste di servizio Web RESTful, possono specificare il numero di voci da visualizzare in ogni pagina. Se, tuttavia, questo valore non viene specificato, vengono utilizzate le dimensioni di pagina predefinite.

1. Effettuare l'accesso alla Central Management Console come amministratore.
2. Fare clic su **Server**, quindi su **Elenco server**.
3. Fare clic con il pulsante destro del mouse sul Server del contenitore applicazioni Web (WACS); ad esempio, fare clic con il pulsante destro del mouse su `MySIA.WebApplicationContainerServer` e scegliere **Proprietà**.

Viene visualizzata la scheda **Proprietà** del server WACS.

4. Nell'area **Servizio Web RESTful**, digitare le dimensioni predefinite di pagina nell'area di testo **Numero predefinito di oggetti in una pagina**.
5. Fare clic su **Salva e chiudi**.

Impostazione del valore di timeout di un token di accesso

I token di accesso scadono se non vengono utilizzati per un determinato periodo di tempo. È possibile impostare la durata della validità di un token di accesso inutilizzato.

Nota:

per impostazione predefinita, il valore di timeout di un token di accesso è un'ora.

1. Effettuare l'accesso alla Central Management Console come amministratore.
2. Fare clic su **Server**, quindi su **Elenco server**.
3. Fare clic con il pulsante destro del mouse sul Server del contenitore applicazioni Web (WACS); ad esempio, fare clic con il pulsante destro del mouse su `MySIA.WebApplicationContainerServer` e scegliere **Proprietà**.

Viene visualizzata la scheda **Proprietà** del server WACS.

4. Nell'area **Servizio Web RESTful**, digitare la durata di validità di un token di accesso, in minuti, nell'area di testo **Timeout token sessione Enterprise (minuti)**.
5. Fare clic su **Salva e chiudi**.

Configurazione delle impostazioni del pool sessioni

Un pool sessioni consente di migliorare le prestazioni del server. Il pool sessioni memorizza nella cache le sessioni di servizio Web RESTful attive, cosicché queste possano essere riutilizzate quando un utente invia un'altra richiesta che utilizza lo stesso token di accesso nell'intestazione della richiesta HTTP. Le dimensioni del pool sessioni specificano il numero di sessioni memorizzate nella cache da archiviare in una volta, mentre il valore di timeout della sessione controlla il tempo per il quale quella sessione rimarrà memorizzata nella cache.

Per impostare le dimensioni del pool sessioni e il valore di timeout sessione:

1. Effettuare l'accesso alla CMC (Central Management Console) come amministratore.
2. Fare clic su **Server**, quindi su **Elenco server**.
3. Fare clic con il pulsante destro del mouse sul Server del contenitore applicazioni Web (WACS); ad esempio, fare clic con il pulsante destro del mouse su `MySIA.WebApplicationContainerServer` e scegliere **Proprietà**.
Viene visualizzata la scheda **Proprietà** del server WACS.
4. Nella casella di testo **Dimensioni pool sessioni** dell'area **Servizio Web RESTful**, digitare il numero massimo di sessioni da memorizzare nella cache.
5. Nella casella di testo **Timeout pool sessioni (in minuti)** dell'area **Servizio Web RESTful**, digitare il valore di timeout del pool sessioni.
6. Fare clic su **Salva e chiudi**.
7. Fare clic con il pulsante destro del mouse sul server WACS, ad esempio `MySIA.WebApplicationContainerServer`, quindi fare clic su **Riavvia server**.

Abilitazione dell'autenticazione di base HTTP

L'autenticazione di base HTTP consente agli utenti di creare richieste di servizio Web RESTful senza dover fornire un token di accesso. Se l'autenticazione di base HTTP è abilitata, agli utenti viene richiesto di indicare nome utente e password alla prima creazione di una richiesta di servizio Web RESTful.

Nota:

I nomi utente e le password non vengono trasmessi in modo protetto con l'autenticazione di base HTTP, a meno che questa non sia utilizzata insieme al protocollo HTTPS.

Quando si abilita l'autenticazione di base HTTP, il tipo predefinito deve essere impostato su SAP, Enterprise, LDAP o WinAD. Gli utenti possono ignorare il tipo di autenticazione di base HTTP predefinito all'accesso.

L'accesso alla piattaforma BI mediante l'autenticazione di base HTTP consuma una licenza. Se viene utilizzata la memorizzazione nella cache del pool sessioni, la richiesta si serve della licenza associata alla sessione memorizzata nella cache. Se non viene utilizzata la memorizzazione nella cache del pool sessioni, viene consumata una licenza mentre la richiesta è in corso, per poi essere rilasciata una volta che la richiesta viene portata a termine.

1. Effettuare l'accesso alla CMC (Central Management Console) come amministratore.
2. Fare clic su **Server > Elenco server**.
3. Fare clic con il pulsante destro del mouse sul Server del contenitore applicazioni Web (WACS); ad esempio, fare clic con il pulsante destro del mouse su `MySIA.WebApplicationContainerServer` e scegliere **Proprietà**.
Viene visualizzata la scheda **Proprietà** del server WACS.
4. Nell'area "Servizio Web RESTful", selezionare **Abilita autenticazione di base HTTP**.
5. (Facoltativo) Nell'elenco **Schema di autenticazione predefinito per HTTP di base**, selezionare il tipo predefinito di autenticazione di base HTTP.
6. Fare clic su **Salva e chiudi**.

Nota:

Un utente finale che effettua l'accesso utilizzando l'autenticazione di base HTTP può specificare il tipo di autenticazione da utilizzare. A tal fine, nel prompt del nome utente del browser digitare `<auth type>\<username>, <password>` nel prompt della password.

Per accedere utilizzando sistematicamente l'autenticazione di base HTTP, aggiungere l'attributo `Authorization` all'intestazione della richiesta HTTP, quindi impostare il valore in modo che sia `Basic <auth type>\<username>:<password>`.

Sostituire `<auth type>` con il tipo di autenticazione, `<username>` con il nome utente e `<password>` con la password. Il tipo di autenticazione, nome utente e password devono essere provvisti di codifica base64, come stabilito da RFC 2617. I nomi utente che contengono il carattere `:` non possono essere utilizzati con l'autenticazione di base HTTP.

Argomenti correlati

- [Configurazione delle impostazioni del pool sessioni](#)

12.1.8.2.3 Condivisione di risorse con diverse origini*Configurazione della condivisione di risorse con diverse origini*

L'impostazione **Configurazione della condivisione di risorse con diverse origini** consente di aggiungere un elenco di nomi di dominio, per permettere agli utenti di recuperare dati da più origini in pagine Web basate su JavaScript. Ciò è necessario per aggirare il criterio di protezione che i linguaggi JavaScript e Ajax utilizzano per impedire l'accesso interdominio. Per evitare di compromettere la sicurezza, vengono aggiunti alle proprietà del server WACS **Consenti origini** nella CMC solo i siti Web a cui è possibile accedere.

È inoltre disponibile un'impostazione **Durata max (minuti)** per regolare l'ora di scadenza della cache, in cui si imposta il numero massimo di minuti per cui i browser possono conservare le richieste HTTP.

Nota:

per impostazione predefinita, l'accesso a tutti i domini è consentito con `*` (asterisco).

1. Effettuare l'accesso alla Central Management Console come amministratore.
2. Fare clic su **Server > Elenco server**.
3. Fare clic con il pulsante destro del mouse sul Server del contenitore applicazioni Web (WACS), ad esempio `MySIA.WebApplicationContainerServer` e scegliere **Proprietà**.
Viene visualizzata la scheda **Proprietà** del server WACS.
4. Nell'area **Servizio Web RESTful** passare alla casella di testo **Configurazione della condivisione di risorse con diverse origini** accanto a **Consenti origini**: e sostituire `*` (asterisco) con l'elenco dei nomi di dominio separati da una virgola. Ad esempio: `http://origine1.server:8080, http://origine2.server:8080`
5. Nella casella di testo **Durata max (minuti)**: digitare il numero massimo di minuti per cui si desidera che i browser memorizzino le richieste HTTP.
6. Fare clic su **Salva e chiudi**.

12.1.8.2.4 Autenticazione

Configurazione di web.xml per abilitare l'SSO WinAD

La configurazione dei servizi Web RESTful per il riconoscimento del Single Sign On di Windows Active Directory (SSO WinAD) richiede modifiche al file di configurazione `web.xml`, disponibile nel server della piattaforma BI. Per ulteriori informazioni, vedere "Using the SDK > Authentication > To get a logon token using an Active Directory Single Sign-On (AD SSO) account" nel manuale *Business Intelligence Platform RESTful Web Service Developer Guide*.

Per fare in modo che il server della piattaforma BI riconosca le credenziali di accesso SSO WinAD del computer client, è necessario rimuovere il commento alla sezione `Kerberos Proxy filter` del file `web.xml` e aggiornare i valori relativi a `idm.realm`, `idm.princ` e `idm.keytab` che riflettono l'ambiente Active Directory utilizzato.

1. Individuare la configurazione di `web.xml` in `<directory principale boe>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\RestWebService\biprws\WEB-INF\`. Il seguente percorso file è un esempio.

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\RestWebService\biprws\WEB-INF\web.xml
```

2. Nel file `web.xml`, rimuovere il commento alla sezione `Kerberos Proxy Filter` aggiungendo un tag di chiusura commento `-->` prima del tag `<filter>` e rimuovere il tag commento di chiusura `-->`

```
<!-- Kerberos Proxy Filter
- Uncomment this filter and the corresponding filter-mapping to enable Kerberos SSO
- for Windows AD (secWinAD) authentication.
- The following options must be specified (the rest are optional):
-   idm.realm
-   idm.princ
-   idm.keytab (unless using password, see below)
-->

<filter>
  <filter-name>WrappedResponseAuthFilter</filter-name>
  .
  .
  .
</filter>

<filter-mapping>
  <filter-name>WrappedResponseAuthFilter</filter-name>
  <url-pattern>/logon/adsso</url-pattern>
</filter-mapping>

</web-app>
```

3. Aggiornare il `<param-value>` per ogni impostazione di `idm.realm`, `idm.princ` e `idm.keytab` con i valori utilizzati nell'ambiente Active Directory.

```
<init-param>
  <param-name>idm.realm</param-name>
  <param-value>ADDOM.COM</param-value>
  <description>
    Required: Set this value to the Kerberos realm to use.
  </description>
</init-param>

<init-param>
  <param-name>idm.princ</param-name>
  <param-value>BOE120SIAVMB0ESRVR/bo.service.addom.com</param-value>
  <description>
    Set this value to the Kerberos service principal to use.
  </description>
```



```

        This will be a name of the form HTTP/fully-qualified-host.
        For example, HTTP/example.vintela.com
        If not set, defaults to the server's hostname and the
        idm.realm property above.
    </description>
</init-param>

<init-param>
    <param-name>idm.kdc</param-name>
    <param-value></param-value>
    <description>
        The KDC against which secondary credentials must be validated
        This can be used for BASIC fallback or credential delegation.
        By default the KDC will be discovered automatically and this
        parameter must only be used if automatic discovery fails, or
        if a different KDC to the one discovered must automatically be used.
    </description>
</init-param>

<init-param>
    <param-name>idm.keytab</param-name>
    <param-value>C:/winnt/BOE120STAVMBOESVR.keytab</param-value>
    <description>
        The file containing the keytab that Kerberos will use for
        user-to-service authentication. If unspecified, SSO will default
        to using an in-memory keytab with a password specified in the
        com.wedgetail.idm.sso.password environment variable.
    </description>
</init-param>

```

Nota:

Il valore `idm.keytab` si riferisce a un percorso file sul server della piattaforma BI. I valori di `idm.realm` e `idm.prince` possono essere visualizzati dalla Central Management Console. Nella scheda **Autenticazione** della CMC fare doppio clic su **Windows AD**. Il valore di `idm.realm` viene impostato con il parametro "Dominio AD predefinito" in "Riepilogo configurazione AD". Il valore di `idm.prince` viene impostato con il parametro "Nome principale servizio" in "Opzioni di autenticazione".

4. Riavviare il servizio WACS in modo che le modifiche apportate a `web.xml` vengano riconosciute.
5. Utilizzare un computer client per verificare che sia possibile recuperare un token di accesso SSO AD con l'API servizi Web RESTful (ad esempio, `http://<host boe>:6405/biprws/logon/ad sso`).
6. Verificare il token utilizzando una query GET, includendo `X-SAP-LoginToken` nell'intestazione e utilizzando l'API `/infostore`.

Abilitazione e configurazione dell'autenticazione affidabile

L'autenticazione affidabile viene attivata e configurata dalla Central Management Console (CMC), in aree che includono **Autenticazione > Enterprise**, in cui viene abilitata l'autenticazione affidabile e viene generato un file di chiave privata condivisa; **Utenti e gruppi > Elenco utenti**, in cui viene creato un account per un utente affidabile; e **Server > Elenco server > WACS > Proprietà**, in cui viene selezionata l'opzione "Metodo di recupero" per le richieste del token di accesso API `/logon/trusted`.

1. Effettuare l'accesso alla Central Management Console come amministratore.
2. Passare ad **Autenticazione > Enterprise** e fare clic su **Autenticazione affidabile attivata**.
3. Fare clic su **Nuova chiave privata condivisa** e quindi su **Scarica chiave privata condivisa**.
4. Fare clic su **Salva** e posizionare il file `TrustedPrincipal.conf` nel percorso predefinito, ovvero `<DirEnterprise>\<piattaforma>`.

Di seguito è riportato un percorso di esempio:

```
"C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjectsEnterprise XI 4.0\win64_x64\"
```

Nota:

- è possibile modificare il percorso predefinito del file di chiave condivisa `TrustedPrincipal.conf` aggiungendo una voce della riga di comando nella CMC, in **Server > Elenco server > WACS > Proprietà > Parametri riga di comando**, e riavviando il servizio WACS. Ad esempio, una voce della riga di comando che utilizza `-Dbobj.trustedauth.home=` e la cartella `SharedSecrets`, posizionata nella directory principale dell'unità `C:\` del server della piattaforma BI, avrà il seguente aspetto:

```
"-Dbobj.trustedauth.home=C:\SharedSecrets"
```

- è possibile lasciare l'opzione **Validità chiave privata condivisa (giorni)** impostata sul valore predefinito di zero (0), in modo che non scada. L'opzione **La richiesta di accesso affidabile raggiunge il timeout dopo N millisecondi (0 significa che non ci sono limiti)** può essere lasciata sul valore predefinito di zero (0), in modo che non ci sia alcun limite di tempo per le richieste di accesso affidabili.
5. Fare clic su **Aggiorna** per salvare la modifica.
 6. Aggiungere un nuovo utente e password, ad esempio `bob` e `Passw0rd`, in **Utenti e gruppi > Elenco utenti** utilizzando **Gestisci > Nuovo > Nuovo utente**. Deselezionare **Cambiamento obbligatorio della password all'accesso successivo**, quindi fare clic su **Crea e chiudi**.

Nota:

è possibile creare un nuovo utente anche facendo clic sull'icona **Crea un nuovo utente** o facendo clic con il pulsante destro del mouse in un'area aperta della finestra in cui sono elencati i nomi utente e scegliendo **Nuovo > Nuovo utente**.

7. Passare a **Server > Servizi principali > WACS > Proprietà**, scorrere fino alla sezione "Configurazione autenticazione affidabile" e utilizzare il menu "Metodo di recupero" per selezionare **HTTP_HEADER, QUERY_STRING** o **COOKIE**.

Nota:

è possibile modificare il valore di "Parametro nome utente" passando dall'etichetta predefinita `X-SAP-TRUSTED-USER` a un'altra etichetta utile (ad esempio `UserName`, `bankteller` o `nurse`), che gli sviluppatori di servizi Web RESTful dovranno utilizzare.

8. Riavviare il servizio facendo clic con il pulsante destro del mouse sul nome del server WACS, ad esempio `MySIA.WebApplicationContainerServer`, e scegliendo **Riavvia server**.

Nota:

La successiva modifica dell'opzione in "Metodo di recupero", come illustrato al passaggio 7, non richiede il riavvio di WACS.

9. Verificare di poter recuperare un token di accesso utilizzando l'API `.../biprsw/logon/trusted/` e inviando una richiesta `GET` con l'etichetta di intestazione predefinita di `X-SAP-TRUSTED-USER` con il nome utente creato al passaggio 5.

Configurazione del parametro della riga di comando per ricollocare il file di configurazione della chiave privata condivisa `TrustedPrincipal.conf`

I servizi Web RESTful includono un parametro della riga di comando per scegliere un percorso diverso per il file `TrustedPrincipal.conf` dell'autenticazione affidabile.

Il file `TrustedPrincipal.conf` contiene una chiave privata condivisa generata tramite CMC:

Autenticazione > Enterprise facendo clic sul pulsante **Nuova chiave privata condivisa** e salvando il file facendo clic su **Scarica chiave privata condivisa**, quindi salvando il file nel percorso predefinito.

Aggiornare la riga di comando del Server del contenitore applicazioni (WACS) con un percorso personalizzato per il file `TrustedPrincipal.conf`, come illustrato di seguito:

1. Accedere alla Central Management Console come amministratore.
2. Fare clic su **Server**, quindi su **Elenco server**.
3. Fare clic con il pulsante destro del mouse sul servizio WACS, ad esempio `MySIA.WebApplicationContainerServer`, e scegliere **Proprietà**.
Viene visualizzata la scheda **Proprietà** del server WACS.
4. Nell'area "Parametri riga di comando" immettere il percorso della directory che conterrà il file `TrustedPrincipal.conf`.

La stringa è racchiusa tra virgolette, come illustrato nel seguente esempio.

```
"-Dbobj.trustedauth.home=C:\SharedSecrets"
```

Nota:

la posizione predefinita del file `TrustedPrincipal.conf` è `<DirEnterprise>\<piattaforma>`. Di seguito è riportato un percorso di esempio:

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64
"
```

5. Fare clic su **Salva e chiudi**.
6. Riavviare il servizio facendo clic con il pulsante destro del mouse sul nome del server WACS, ad esempio `MySIA.WebApplicationContainerServer`, e scegliendo **Riavvia server**.

12.1.9 WACS e ambiente IT

In questa sezione viene descritto come configurare un WACS in un ambiente complesso.

12.1.9.1 Utilizzo del WACS con altri server Web

Quando è installato un Server del contenitore di applicazioni Web (WACS), funziona come server di applicazioni e server Web senza richiedere ulteriore configurazione. È possibile configurare server Web supportati come Internet Information Services (IIS) e Apache per eseguire l'inoltro degli URL al server WACS.

Nota:

Non è consentito inoltrare le richieste tramite un filtro ISAPI da IIS a un WACS.

Il WACS non supporta lo scenario di distribuzione in cui un server Web ospita contenuto statico e il WACS ospita contenuto dinamico. Il contenuto statico e il contenuto dinamico devono entrambi risiedere nel server WACS.

12.1.9.2 Utilizzo del WACS con un bilanciatore di carico

Per utilizzare il WACS in una distribuzione con un bilanciatore del carico hardware, è necessario configurare il bilanciatore di carico in modo che utilizzi i cookie attivi o il routing IP. In questo modo, dopo avere stabilito una sessione utente in un WACS, tutte le richieste successive dello stesso utente verranno inviate allo stesso WACS.

Non è previsto il supporto dei WACS con bilanciatori del carico hardware che utilizzano cookie passivi.

Se il bilanciatore del carico hardware inoltra le richieste HTTPS crittografate tramite SSL al WACS, è necessario configurare HTTPS nel WACS e installare i certificati SSL su ogni WACS.

Se il bilanciatore del carico hardware decrittografa il traffico HTTPS e inoltra le richieste HTTP decrittografate al WACS, non è necessaria alcuna ulteriore configurazione del WACS.

Argomenti correlati

- [Configurazione di HTTPS/SSL](#)

12.1.9.3 Utilizzo del WACS con un proxy inverso

È possibile utilizzare un WACS in una distribuzione con un server proxy normale o inverso. Non è possibile utilizzare il WACS come server proxy.

12.1.9.3.1 Per configurare il WACS affinché supporti HTTP con un proxy inverso

Per utilizzare il WACS in una distribuzione con un proxy inverso, configurarlo in modo che la porta HTTP venga utilizzata per la comunicazione all'interno di un firewall (ad esempio in una rete protetta) e che la porta HTTP tramite proxy venga utilizzata per la comunicazione all'esterno (Internet ad esempio).

1. Passare all'area di gestione "Server" della CMC.

2. Fare doppio clic sul WACS che si desidera configurare.
Viene visualizzata la schermata "Proprietà".
3. Nella sezione "Configurazione HTTP su proxy":
 - a. Selezionare **Abilita HTTP su proxy**.
 - b. Specificare la porta HTTP del WACS da utilizzare per la comunicazione attraverso il proxy.
 - c. Specificare il nome host e la porta del server proxy.
4. Fare clic su **Salva e chiudi**.

12.1.9.3.2 Per configurare il WACS affinché supporti HTTPS con un proxy inverso

È possibile configurare alcuni bilanciatori di carico e server proxy inverso per decrittografare il traffico HTTPS e quindi inoltrarlo ai server di applicazioni. In questo caso, è possibile configurare il WACS per l'utilizzo di HTTP o HTTP su proxy.

Se il bilanciatore di carico o il proxy inverso inoltra il traffico HTTPS e si desidera configurare HTTPS con un proxy inverso, creare due WACS. Configurare un WACS per HTTPS per il traffico esterno attraverso il proxy inverso e l'altro WACS per comunicare con i client nella rete interna tramite HTTPS.

12.1.9.4 Utilizzo dei WACS con i firewall

La distribuzione di WACS in un ambiente IT con i firewall è supportata.

Per impostazione predefinita, il WACS associa tutti gli indirizzi IP nel computer su cui è installato. Se intendi utilizzare un firewall tra client e il WACS, è necessario imporre al WACS di eseguire l'associazione a un indirizzo IP specifico per HTTP o HTTP attraverso il proxy. A tale scopo, deselezionare **Associa a tutti gli indirizzi IP**, quindi specificare un nome host o un indirizzo IP a cui eseguire l'associazione.

Se si prevede di utilizzare un firewall tra un server WACS e gli altri server della piattaforma BI della distribuzione, consultare la sezione relativa alle "comunicazioni tra componenti della piattaforma SAP BusinessObjects Business Intelligence" nel *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

Argomenti correlati

- [Informazioni sulla comunicazione tra componenti della piattaforma BI](#)

12.1.9.5 Configurazione di un WACS in un computer multi-home

Un computer multi-home ha più indirizzi di rete. Per impostazione predefinita, le istanze del Server del contenitore di applicazioni Web associano la porta HTTP a tutti gli indirizzi IP. Per associare il WACS

a una scheda NIC (Network Interface Card) specifica, ad esempio quando si desidera associare la porta HTTP del WACS a una scheda NIC e la porta di richiesta a un'altra scheda NIC:

1. Passare all'area di gestione "Server" della CMC.
2. Fare doppio clic sul WACS che si desidera configurare.
Viene visualizzata la schermata "Proprietà".
3. Nella sezione "Configurazione di HTTP tramite proxy" del riquadro "Servizio contenitore applicazioni Web", deselezionare **Associa a tutti gli indirizzi IP** e digitare un indirizzo IP al quale associare il WACS.
4. Nella sezione "Configurazione HTTP" deselezionare **Associa a tutti gli indirizzi IP** e digitare un indirizzo IP o un nome host al quale associare il WACS.
5. In "Impostazioni comuni" deselezionare **Assegna automaticamente**, quindi specificare il nome host o l'indirizzo IP della scheda NIC utilizzata per la comunicazione tra i WACS e gli altri server della piattaforma BI della distribuzione.
6. Fare clic su **Salva e chiudi**.
7. Riavviare il WACS.

12.1.10 Configurazione delle proprietà delle applicazioni Web

Le proprietà delle applicazioni Web ospitate su un server WACS possono essere configurate nei modi seguenti:

- Le proprietà modificate spesso vengono esposte come proprietà di servizio configurabili per il server WACS. Per modificarle, aprire la pagina "Proprietà" del server WACS nella CMC (Central Management Console), modificare il valore della proprietà appropriata e fare clic su **Salva**.
- Per modificare i timeout della sessione per le applicazioni Web ospitate su WACS, stabilire innanzitutto se l'applicazione Web dispone di proprietà configurabili nella CMC.

Se l'applicazione Web presenta proprietà modificabili nella CMC, modificare il file `web_xml.ino` di tale applicazione. Il file si chiama `NomeAppWeb_web_xml.ino`, dove `NomeAppWeb` è il nome dell'applicazione Web ed è disponibile nella directory `DirectoryEnterprise/java/pjs/services/NomeAppWeb`.

Se invece l'applicazione Web non dispone di proprietà modificabili nella CMC, modificare il file `web.xml` di tale applicazione. Il file si trova nel percorso `DirectoryEnterprise/warfile/webapps/NomeAppWeb`, dove `NomeAppWeb` è il nome dell'applicazione Web.

- Per modificare proprietà diverse dal timeout della sessione o dalle proprietà visualizzate nella schermata "Proprietà" del server WACS nella CMC, modificare il file `.properties` dell'applicazione Web. Per ulteriori informazioni, consultare la sezione relativa alla "gestione delle applicazioni mediante le proprietà del file `BOE.war`" nel *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

Nota:

- Non modificare il file `web.xml`, `web_xml.ino` o `.properties` nella directory `DirectoryEnterprise/java/pjs/container/work/NomeDescrittivoServer`, in quanto le modifiche apportate verranno sovrascritte a ogni avvio o riavvio di WACS.
- dopo aver modificato le proprietà di un server WACS, è sempre necessario riavviarlo.

Argomenti correlati

- [Per modificare le proprietà di un server](#)
- [File WAR BOE](#)

12.1.11 Risoluzione dei problemi

12.1.11.1 Configurazione dell'analisi sul server WACS

Per configurare l'analisi per il server WACS, consultare [Registrazione delle analisi dei componenti](#)

12.1.11.2 Per visualizzare le specifiche del server

È possibile visualizzare le metriche del sistema di un server WACS dalla Central Management Console (CMC).

1. Passare all'area di gestione "Server" della CMC.
2. Fare clic con il pulsante destro del mouse sul WACS e fare clic su **Metriche**.

Argomenti correlati

- [Metriche del server del contenitore di applicazioni Web](#)

12.1.11.3 Per visualizzare lo stato di un WACS

Per visualizzare lo stato di un WACS, accedere all'area "Server" di CMC. Nell'**Elenco server** è inclusa una colonna **Stato** che fornisce lo stato di ogni server nell'elenco.

I WACS presentano un stato server definito "Avviato con errori". Questo stato indica che il WACS è in esecuzione, ma presenta una o più delle seguenti condizioni di errore:

- Errata configurazione di un connettore HTTP, HTTP tramite proxy o HTTPS.
- Errata esecuzione di un servizio in funzione sul WACS, ad esempio il servizio log analisi.
- Errore di distribuzione di un'applicazione Web nel WACS.

Per identificare i servizi non riusciti, vedere la pagina "Proprietà" del WACS.

12.1.11.4 Risoluzione dei conflitti tra porte

Se non è possibile ottenere alcuna pagina mentre si tenta di accedere al servizio CMC attraverso una determinata porta, assicurarsi che un'altra applicazione non abbia occupato le porte HTTP, HTTP su proxy o HTTPS specificate per il WACS.

Sono disponibili due modi per determinare la presenza di conflitti tra porte con il WACS. Se nella distribuzione sono presenti più WACS, accedere alla CMC e controllare le metriche Elenco di connettori WACS in esecuzione ed Errori connettori WACS all'avvio. Se i connettori HTTP, HTTP tramite proxy o HTTP non figurano nell'Elenco di connettori WACS in esecuzione, non è possibile avviarli a causa di un conflitto tra porte.

Se la distribuzione contiene un solo WACS o se non è possibile accedere al servizio CMC tramite alcun WACS, utilizzare un'utilità quale netstat per determinare se un'altra applicazione ha occupato una porta WACS.

12.1.11.4.1 Per risolvere i conflitti tra porte HTTP

1. Avviare Central Configuration Manager (CCM) e fare clic sull'icona **Gestisci server**.
2. Specificare le credenziali di accesso.
3. Nella schermata "Gestisci server", arrestare il WACS.
4. Fare clic sull'icona **Configurazione livello Web**.

Nota:

L'icona **Configurazione livello Web** è disponibile solo quando si seleziona un WACS arrestato.

Viene visualizzata la schermata "Configurazione livello Web".

5. Nel campo **Porta HTTP** specificare una porta HTTP libera che possa essere utilizzata dal WACS e fare clic su **OK**.
6. Nella schermata "Gestisci server" avviare il WACS.

12.1.11.4.2 Per risolvere i conflitti tra porte HTTP su proxy o HTTPS

Se non è possibile accedere a un WACS attraverso le porte HTTP su proxy o HTTPS, ma è ancora possibile connettersi a Central Management Console (CMC) attraverso la porta HTTP, modificare i numeri di porta attraverso CMC.

1. Passare all'area di gestione "Server" della CMC.
2. Per arrestare il WACS che si desidera configurare, fare clic con il pulsante destro del mouse sul server e scegliere **Arresta server**.
3. Fare doppio clic sul WACS che si desidera configurare.
Viene visualizzata la schermata "Proprietà".
4. Nella sezione "Configurazione HTTP attraverso proxy" specificare una nuova porta HTTP.
5. Per modificare la porta HTTPS, nella sezione "Configurazione HTTPS" digitare un nuovo valore nel campo **Porta HTTPS**.
6. Fare clic su **Salva e chiudi**.
7. Per avviare il WACS, fare clic con il pulsante destro del mouse sul server, quindi scegliere **Avvia server**.

12.1.11.5 Per modificare le impostazioni di memoria

Per migliorare le prestazioni di un WACS, è possibile modificare la quantità di memoria allocata al server tramite Central Configuration Manager (CCM).

1. Avviare CCM e fare clic sull'icona **Gestisci server**.
2. Specificare le credenziali di accesso per la console CMC.
3. Nella schermata "Gestisci server", arrestare il WACS.
4. Fare clic sull'icona **Configurazione livello Web**.

Nota:

L'icona **Configurazione livello Web** è disponibile solo quando si seleziona un WACS arrestato.

Viene visualizzata la schermata "Configurazione livello Web".

5. In "Parametri riga di comando" specificare un nuovo valore di memoria modificando la riga di comando:
 - a. Trovare l'opzione -Xmx. Per questa opzione è in genere specificato un valore.
Ad esempio "-Xmx1g". Questa impostazione alloca un gigabyte di memoria al server.
 - b. Specificare un nuovo valore per il parametro.
 - Per specificare un valore in megabyte, utilizzare "m". Ad esempio, "-Xmx640m" alloca 640 megabyte di memoria al WACS.
 - Per specificare un valore in gigabyte, utilizzare "g". Ad esempio, "-Xmx2g" alloca due gigabyte di memoria al WACS.

- c. Fare clic su **OK**.
- 6. Nella schermata "Gestisci server" avviare il WACS.

12.1.11.6 Per modificare il numero di richieste simultanee

Il numero predefinito di richieste HTTP simultanee che un WACS per gestire è 150. Questo valore dovrebbe essere accettabile per la maggior parte degli scenari di distribuzione. Per migliorare le prestazioni del WACS, è possibile aumentare il numero massimo di richieste HTTP simultanee. Sebbene l'aumento del numero di richieste possa migliorare le prestazioni, l'impostazione di un valore eccessivamente elevato potrebbe compromettere negativamente le prestazioni. L'impostazione ideale dipende dall'hardware, dal software e dai requisiti IT.

1. Passare all'area di gestione "Server" della CMC.
2. Per arrestare il WACS che si desidera configurare, fare clic con il pulsante destro del mouse sul server e scegliere **Arresta server**.
3. Fare doppio clic sul WACS che si desidera configurare.
Viene visualizzata la schermata "Proprietà".
4. In "Impostazioni di concorrenza (per connettore)", nel campo **N. massimo richiesta simultanee** digitare il numero desiderato di richieste simultanee e fare clic su **Salva e chiudi**.
5. Per avviare il WACS, fare clic con il pulsante destro del mouse sul server, quindi scegliere **Avvia server**.

12.1.11.7 Per ripristinare i valori predefiniti di sistema

Se un WACS è stato configurato in modo errato, è possibile ripristinare la configurazione di sistema predefinita attraverso Central Configuration Manager (CCM).

1. Avviare CCM e fare clic sull'icona **Gestisci server**.
2. Specificare le credenziali di accesso.
3. Nella schermata "Gestisci server", arrestare il WACS.
4. Fare clic sull'icona **Configurazione livello Web**.

Nota:

l'icona **Configurazione livello Web** è disponibile solo quando si seleziona un WACS arrestato.

Viene visualizzata la schermata "Configurazione livello Web".

5. Fare clic su **Ripristina valori predefiniti sistema**.
6. Se necessario, specificare una porta HTTP libera e fare clic su **OK**.
7. Nella schermata "Gestisci server" avviare il WACS.

12.1.11.8 Per impedire agli utenti di connettersi al WACS attraverso HTTP

In alcuni casi, si desidera solo consentire agli utenti di connettersi dal computer locale al WACS attraverso HTTP o HTTPS. È il caso ad esempio in cui, sebbene non sia possibile chiudere la porta HTTP, è possibile configurare il WACS in modo che accetti unicamente le richieste HTTP dai client che si trovano nello stesso computer del WACS. In questo modo, è possibile eseguire le operazioni di manutenzione o configurazione nel WACS attraverso un browser dallo stesso computer del WACS, mentre si impedisce ad altri di accedere al server.

1. Passare all'area di gestione "Server" della CMC.
2. Fare doppio clic sul WACS che si desidera modificare.
Viene visualizzata la schermata "Proprietà".
3. Nella sezione "Servizio contenitore applicazioni Web" deselezionare la casella di controllo **Associa a tutti gli indirizzi IP**.
4. Nel campo **Associa a nome host o indirizzo IP** digitare 127.0.0.1 e fare clic su **Salva e chiudi**.
5. Per avviare il WACS, fare clic con il pulsante destro del mouse sul server, quindi scegliere **Avvia server**.

Il WACS così configurato accetta unicamente le connessioni dal computer locale.

12.1.12 Proprietà del server WACS

Per un elenco completo delle proprietà di configurazione generali, HTTP, HTTP tramite proxy e HTTPS che è possibile configurare per i server WACS, consultare la sezione "Impostazioni dei server principali" dell'"Appendice sulle proprietà dei server".

Argomenti correlati

- [Proprietà dei servizi principali](#)

Backup e ripristino del sistema

13.1 Panoramica di backup e ripristino

In questo capitolo viene illustrata la procedura per eseguire il backup della piattaforma BI e per ripristinare il sistema da un guasto hardware, da un guasto software e dalla perdita di dati. Per eseguire un piano di backup e di ripristino, è necessario un professionista esperto SAP BusinessObjects, un amministratore di sistema e un amministratore del database.

Argomenti correlati

- [Backup dell'intero sistema](#)
- [Backup del contenuto BI](#)
- [Backup delle impostazioni server mediante CCM in Windows](#)
- [Backup delle impostazioni del server in UNIX](#)
- [Panoramica della copia del sistema](#)

13.2 Terminologia

Termine	Definizione
Replica dei dati	La replica dei dati è il processo di creazione di una o più copie dei dati. Le copie vengono aggiornate in tempo reale, ad esempio quando si utilizzano unità con mirroring. Offre protezione dei dati dai danni fisici in tempo reale ma, dal momento che le unità sono sottoposte continuamente ad aggiornamento, non è possibile ripristinare uno stato precedente del sistema se i dati vengono danneggiati o accidentalmente rimossi.

Termine	Definizione
Controllo delle versioni	<p>Il controllo versione crea diverse versioni di uno o più file specifici sul sistema. Ciò consente di riportare il sistema a uno stato precedente.</p> <p>Questa procedura, tuttavia, prevede l'archiviazione di tutte le versioni dei dati nello stesso sistema host. Pertanto, se quest'ultimo viene compromesso o danneggiato, si rischia di perdere sia la versione corrente che le versioni precedenti. Analogamente, la funzione di annullamento dell'eliminazione consente di conservare copie dei file "eliminati" per successive operazioni di ripristino. Tali copie però vengono anch'esse archiviate sullo stesso sistema host dei dati originali. Non garantisce il danneggiamento dei dati fisici (ad esempio, guasto del disco).</p>
Backup di sistema bare metal	<p>Un backup di sistema bare metal è il backup di un intero file system, incluso il sistema operativo. Questo tipo di backup viene utilizzato per ripristinare un sistema di cui è stato eseguito il backup allo stato di hardware che non contiene alcun software o sistema operativo.</p> <p>Per i backup di sistema bare metal, in caso di errore, l'intero file system (incluso il sistema operativo) viene ripristinato allo stesso hardware o, se gli strumenti di ripristino supportano il ripristino indipendente dall'hardware, a qualsiasi hardware.</p>
Backup di sistema bare metal e backup di applicazione	<p>Un backup di sistema bare metal crea una copia dell'intero sistema, incluso il sistema operativo. Ciò consente di ripristinare una versione precedente dell'intero sistema.</p> <p>Un backup di applicazione crea una copia di backup dei file correlati alle singole applicazioni.</p> <p>La piattaforma BI supporta i backup di sistema bare metal ma non i backup di applicazione.</p> <p>Per i backup di sistema bare metal, in caso di errore, l'intero file system (incluso il sistema operativo) viene ripristinato allo stesso hardware o, se gli strumenti di ripristino supportano il ripristino indipendente dall'hardware, a qualsiasi hardware.</p> <p>Il backup di sistema completo della piattaforma BI viene definito set di backup.</p>

Termine	Definizione
Set di backup	<p>Un set di backup comprende i backup singoli seguenti, che vengono creati contemporaneamente:</p> <ul style="list-style-type: none"> • Un backup del database di sistema CMS. • Un backup bare metal dell'intero file system, incluso il sistema operativo, di tutti i computer inclusi nella distribuzione della piattaforma BI • Il backup degli archivi dei file FRS di input e di output, se non incluso nel file system della piattaforma BI. • Un backup dei componenti del livello Web (se non incluso come parte del file system della piattaforma BI). • Un backup del database di controllo.
Backup a freddo e backup a caldo	<p>Il backup a freddo viene eseguito quando il sistema è arrestato e non disponibile per gli utenti. I backup a caldo vengono invece eseguiti mentre il sistema è in esecuzione e disponibile per gli utenti, pertanto è possibile che durante l'esecuzione del backup i dati vengano modificati. Inoltre, a differenza del backup a freddo, per il backup a caldo è necessario eseguire i passaggi nell'ordine corretto.</p> <p>La piattaforma BI supporta sia il backup a caldo che quello a freddo.</p> <p>Il backup a caldo viene talvolta denominato "backup online".</p>

13.3 Casi d'uso per il backup e il ripristino

Nella tabella che segue sono descritti gli obiettivi che si possono raggiungere con le risorse disponibili e viene indicata la soluzione di backup più appropriata.

Obiettivo	Risorse necessarie	Soluzione
<p>Obiettivo: ripristinare un sistema</p> <ol style="list-style-type: none"> 1. La piattaforma BI è danneggiata. È necessario ripristinare lo stato in cui si trovava quando è stato eseguito l'ultimo backup. 2. Un computer che ospita la piattaforma BI è danneggiato. È necessario sostituirlo con un nuovo computer. 	<ul style="list-style-type: none"> • Un sistema di destinazione con hardware identico nel sistema di origine <p>AND</p> <ul style="list-style-type: none"> • Backup del sistema di origine 	<p>Utilizzare il workflow di backup e ripristino del sistema descritto in dettaglio in questo manuale. Consultare la procedura Backup dell'intero sistema. Ricreare il sistema di destinazione da backup del sistema di origine.</p>
<p>Obiettivo: ripristinare oggetti</p> <p>Si desidera recuperare un documento o un altro oggetto eliminato per errore.</p>	<ul style="list-style-type: none"> • Backup di file e database del sistema di origine <p>AND</p> <ul style="list-style-type: none"> • Informazioni di sistema dettagliate descritte in Per eseguire l'esportazione da un sistema di origine 	<p>Utilizzando i backup, creare una copia del sistema in un altro computer seguendo le indicazioni del workflow relativo alla copia del sistema fornite nel capitolo relativo alla "copia della distribuzione della piattaforma BI". Utilizzare gli strumenti di gestione della promozione per promuovere dal nuovo sistema gli oggetti eliminati per errore. Fare riferimento al workflow relativo alla copia del sistema, iniziando con Pianificazione della copia del sistema, e seguire le istruzioni per il resto del capitolo</p> <p>Nota:</p> <p>è possibile creare il sistema di destinazione all'interno di un computer con una distribuzione esistente della piattaforma BI con la stessa versione, lo stesso pacchetto di supporto e lo stesso livello patch, oppure in un computer "pulito" senza piattaforma BI installata.</p>
<p>Obiettivo: ripristinare oggetti 2</p> <p>Si desidera recuperare un documento o un altro oggetto eliminato per errore.</p>	<p>Un sistema in cui sia in uso il controllo delle versioni di Promotion Management</p>	<p>Utilizzare l'applicazione Promotion Management per ripristinare una versione precedente del documento. Per i dettagli, consultare l'argomento correlato sulla gestione delle promozioni.</p>

Obiettivo	Risorse necessarie	Soluzione
<p>Obiettivo: creare copie di backup di oggetti</p> <p>Si desidera creare copie di backup di un numero limitato di oggetti (ad esempio documenti, cartelle, utenti).</p>	<p>Un sistema in cui sia in uso il controllo delle versioni di Promotion Management</p>	<p>Utilizzare l'applicazione Promotion Management per eseguire il backup del contenuto BI e quindi esportarlo nei file Business Intelligence Archive (LCMBIAR). Se il contenuto è danneggiato o mancante, è possibile ripristinarlo in un secondo momento, senza ripristinare l'intero sistema.</p> <p>Per i dettagli, consultare l'argomento correlato sulla gestione delle promozioni.</p>

Argomenti correlati

- [Backup](#)
- [Pianificazione della copia del sistema](#)
- [Panoramica](#)

13.4 Backup

Un piano di backup e recupero consiste in alcuni passaggi da eseguire in caso di errori del sistema dovuti a un disastro naturale o a un guasto imprevisto. Lo scopo del piano è ridurre al minimo gli effetti del disastro sulle attività quotidiane, in modo da potere continuare a utilizzare o riprendere rapidamente le funzioni più importanti.

Quando si esegue il backup della distribuzione della piattaforma BI, sono disponibili le tre opzioni indicate di seguito.

- Eseguire il backup dell'intero sistema per ripristinarlo. In questo caso, non è possibile ripristinare solo una parte del sistema. Se si desidera rigenerare la piattaforma BI anziché ripristinarla da un backup, consultare l'argomento correlato che descrive la procedura di copia del sistema.
- Eseguire il backup solo delle impostazioni del server e non di altri oggetti mantenendo lo stato corrente del contenuto BI del sistema.
- Eseguire il backup del contenuto BI (ad esempio documenti), ovvero ripristinare in modo selettivo parti del contenuto BI senza ripristinare tutti gli oggetti.

Consultare gli argomenti correlati per i dettagli sui tre tipi di backup.

Suggerimento:

- Per evitare la perdita dei dati, eseguire regolarmente i backup.

- È possibile eseguire il backup di un sistema della piattaforma BI e quindi ripristinarlo nello stesso computer host o in un computer host diverso per creare una copia del sistema.

Argomenti correlati

- [Backup dell'intero sistema](#)
- [Backup delle impostazioni server](#)
- [Backup del contenuto BI](#)
- [Panoramica della copia del sistema](#)

13.4.1 Backup dell'intero sistema

Eseguire il backup a caldo o a freddo dell'intero sistema della piattaforma BI. Questa operazione crea un set di backup. Se si conservano più set di backup che si riferiscono a momenti diversi, si ha a disposizione un numero maggiore di opzioni in fase di ripristino del sistema. Eseguire il backup del sistema con la frequenza richiesta dalle esigenze aziendali dell'organizzazione.

È possibile scegliere di arrestare il sistema della piattaforma BI e di eseguire un backup a freddo. In alternativa, è possibile eseguire un backup a caldo. Con il backup a caldo, il sistema rimane attivo e disponibile per gli utenti durante il processo di backup. Il vantaggio di questo approccio è l'assenza di tempi di inattività.

Nota:

- è consigliabile scrivere il registro delle transazioni in un file system diverso dal sistema di server di database principale eseguendo regolarmente il backup del registro delle transazioni e salvandolo insieme agli altri file nel set di backup.
- se si esegue la copia di backup dei dati di controllo, verificare che nel set di file di backup sia incluso il registro delle transazioni del database di controllo. Non è necessario includere nel backup anche i file temporanei di controllo.

13.4.1.1 Backup a caldo

La funzionalità di backup a caldo consente di eseguire il backup del sistema della piattaforma BI consentendo agli utenti di continuare a utilizzare normalmente il sistema. Se si ha necessità di non interrompere le attività aziendali durante il backup a caldo, abilitare e configurare il backup a caldo nella Central Management Console.

L'impostazione **Durata massima del backup a caldo** specifica la quantità massima di tempo previsto per l'esecuzione del backup, a partire dall'inizio del backup del CMS fino al termine del backup del server FRS. Se la durata specificata è troppo breve, è possibile che i file vengano eliminati prima che il programma di backup abbia l'opportunità di copiarli. Per evitare che ciò accada, è più sicuro inserire

un valore superiore a quello previsto. Bilanciare questo problema con le risorse del sistema perché un elevato valore potrebbe aumentare sensibilmente la capacità di memorizzazione dei file FRS.

Nota:

Il backup a caldo viene abilitato fintantoché la casella di controllo **Abilitare backup a caldo** è selezionata nella CMC. L'abilitazione del backup a caldo non dipende dall'impostazione **Durata massima del backup a caldo**.

È più semplice ripristinare lo stato in cui si trovava il sistema a un'ora di backup specifica. Ad esempio, se i backup del sistema vengono eseguiti ogni giorno alle ore 15:00, è possibile ripristinare facilmente il sistema allo stato in cui si trovava al momento dell'inizio del backup del sistema CMS (alle ore 15:00 del giorno prescelto). Se è stata abilitata la registrazione delle transazioni di un database CMS o di un database di controllo, in caso di guasto è possibile ripristinare il sistema allo stato in cui si trovava immediatamente prima.

Per la massima sicurezza, salvare i record di registrazione delle transazioni in un percorso diverso rispetto ai record di backup del database primario. Ciò garantisce che, in caso di errore del database, è possibile ripristinare lo stato in cui si trovava prima dell'errore.

Nota:

- a causa di una limitazione delle dimensioni del registro delle transazioni nelle versioni precedenti di IBM DB2, le attività correlate al backup a caldo e al registro delle transazioni sono supportate solo se il database di sistema CMS è ospitato nel server di database DB2 versione 9.5 Fix Pack 5 o successiva (per la linea 9.5) e 9.7 Fix Pack 1 o successiva (per la linea 9.7).
- è consigliabile scrivere il registro delle transazioni in un file system diverso dal sistema di server di database principale eseguendo regolarmente il backup del registro delle transazioni e salvandolo insieme ad altri file nel set di backup.

I client Crystal Reports 2011 Designer, Web Intelligence Rich e Universe Design Tool precedenti alla versione 4.0 FP3 e le applicazioni thick client sviluppate personalizzate compilate con SDK precedenti alla versione 4.0 FP3 potrebbero non supportare la modifica dei file durante il backup a caldo. Se queste applicazioni client modificano il contenuto BI durante i backup, la qualità dei dati modificati potrebbe essere compromessa durante il backup. È possibile impedire che le applicazioni client modifichino i documenti per garantire la coerenza dei dati di backup. Aggiornare le applicazioni client con la versione 4.0 FP3 ove possibile. In caso contrario, è possibile adottare soluzioni alternative. È ad esempio possibile avvisare gli utenti che le applicazioni client eliminano gli oggetti esistenti e consigliare loro di salvare le nuove versioni anziché modificare gli oggetti.

13.4.1.1.1 Per abilitare i backup a caldo

1. Aprire Central Management Console (CMC).
2. Nell'area "Gestisci" aprire la pagina **Impostazioni**.
3. Nella sezione "Backup a caldo" selezionare **Abilitare backup a caldo**.
4. Immettere il numero massimo di minuti previsto per il backup in **Durata massima del backup a caldo (minuti)**.

Specificare il tempo richiesto per eseguire il backup sia del database CMS che del file system del computer host della piattaforma BI.

Nota:

se la durata effettiva del backup supera il limite immesso in questo campo, possono verificarsi incongruenze nei dati di backup. Per evitare che ciò accada, è più sicuro inserire un valore superiore a quello previsto.

5. Per consentire ai client Web Intelligence Rich, Crystal Reports Designer o ad applicazioni thick client SDK personalizzate precedenti (anteriori alla versione 4.0 FP3) di modificare i documenti del sistema, selezionare la casella di controllo **Abilita supporto di applicazioni precedenti (restrizioni di backup)**.

se si consente a queste applicazioni client precedenti di modificare i documenti durante le operazioni di backup, è possibile che si verifichino incongruenze nei documenti modificati durante il backup. Per informazioni sulle restrizioni di backup, consultare il collegamento correlato che riguarda i backup a caldo.

6. Fare clic su **Aggiorna**.

Il backup a caldo è abilitato.

Una volta abilitato il supporto del backup a caldo, è possibile eseguire backup utilizzando gli strumenti di backup del fornitore del database e del file system.

Argomenti correlati

- [Backup a caldo](#)
- [Per eseguire un backup di sistema a caldo o a freddo](#)

13.4.1.2 Per eseguire un backup di sistema a caldo o a freddo

Se si desidera eseguire un backup a caldo, consultare prima l'argomento correlato per conoscere i prerequisiti e ottenere altre informazioni. Se si intende eseguire un backup a freddo, arrestare tutti i nodi nella distribuzione della piattaforma BI.

Avvertenza:

Se si esegue un backup senza abilitare il backup a caldo e senza arrestare tutti i nodi, potrebbe risultare un'incoerenza di dati tra il database CMS e l'archivio file FRS.

Nota:

Per i backup a caldo, è importante che le procedure vengano avviate nella sequenza descritta. Per i backup a freddo, le procedure possono essere eseguite in qualsiasi ordine. In entrambi i casi, non è necessario attendere il completamento di ciascun passaggio della procedura di backup prima di passare a quello successivo.

1. Utilizzare gli strumenti del fornitore di database per eseguire il backup del database di sistema CMS (Central Management Server).

Nota:

Per backup a caldo, utilizzare gli strumenti di backup del fornitore di database in modalità atomica online.

2. Utilizzare gli strumenti del fornitore di database in modalità atomica online per eseguire il backup del database di controllo della piattaforma BI.
3. Eseguire il backup dell'intero file system, incluso il sistema operativo, di tutti i computer inclusi nella distribuzione della piattaforma BI.
 - a. Se gli archivi file FRS di input e di output non sono inclusi nel backup della piattaforma BI (computer host separati), creare una copia di backup di entrambi utilizzando gli strumenti di backup dei file.
 - b. Se i componenti del livello Web non sono inclusi nel backup della piattaforma BI (computer host separati), creare una copia di backup di tali componenti utilizzando gli strumenti di backup dei file.

Per i backup a caldo, utilizzare gli strumenti per il backup atomico dei file, se possibile.

Se è stato eseguito un backup a freddo, attendere il completamento di tutti i backup, quindi avviare i nodi della piattaforma BI.

Argomenti correlati

- [Backup a caldo](#)

13.4.2 Backup delle impostazioni server

Per proteggere il sistema dall'errata configurazione delle impostazioni server, eseguire il backup regolare di tali impostazioni in un file BIAR. La disponibilità di backup dei server consente di ripristinare le impostazioni senza ripristinare il database di sistema CMS, i file repository o il contenuto di Business Intelligence.

È essenziale eseguire il backup delle impostazioni server ogni volta che si apportano modifiche alla distribuzione del sistema, che comprende la creazione, la ridenominazione, lo spostamento e l'eliminazione di nodi, nonché la creazione o l'eliminazione di server. È consigliabile eseguire il backup delle impostazioni server prima di modificare le impostazioni e di nuovo dopo aver verificato le modifiche apportate.

Utilizzare CCM (Central Configuration Manager) o uno script per effettuare il backup delle impostazioni server della piattaforma BI in un file BIAR, quindi archiviare il file in un computer o un supporto di archiviazione separato.

Nota:

se si esegue il backup o il ripristino delle impostazioni in una distribuzione in cui è abilitato il SSL, è necessario innanzitutto disabilitare quest'ultimo attraverso il CCM, quindi riabilitarlo al termine dell'operazione.

In Windows lo script `BackupCluster.bat` si trova nella directory `DIRINSTALLAZ\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

In UNIX lo script `backupcluster.sh` si trova nella directory `/DIRINSTALLAZ/sap_bobj/enterprise_xi40/platform64/scripts`.

Argomenti correlati

- [Configurazione del protocollo SSL](#)

13.4.2.1 Backup delle impostazioni server mediante CCM in Windows

La seguente procedura è relativa al backup delle impostazioni server di un intero cluster. Non è possibile eseguire il backup delle impostazioni di singoli server.

Nota:

se si utilizza un CMS temporaneo, è necessario utilizzare il CCM su un computer sul quale siano installati i file binari del CMS locale.

1. Avviare CCM e fare clic su **Esegui backup configurazione server** nella barra degli strumenti.
Viene visualizzato il "Backup guidato configurazione server".
2. Fare clic su **Avanti** per avviare la procedura guidata.
3. Specificare se utilizzare un server CMS esistente per il backup delle impostazioni di configurazione del server o creare un CMS temporaneo.
 - Per eseguire il backup delle impostazioni server da un sistema in esecuzione, selezionare **Utilizza CMS esistente in esecuzione**, quindi fare clic su **Avanti**.
 - Per eseguire il backup delle impostazioni server da un sistema non in esecuzione, selezionare **Avvia un nuovo CMS temporaneo**, quindi fare clic su **Avanti**.
4. Se si utilizza un CMS temporaneo, selezionare un numero di porta per il CMS da utilizzare e specificare le informazioni sulla connessione al database.
Per ridurre il rischio che altri utenti accedano al sistema durante il ripristino, specificare un numero di porta diverso da quelli utilizzati per i CMS esistenti.
5. Inserire la chiave cluster e fare clic su **Avanti** per continuare.
6. Quando richiesto, accedere al CMS specificando il sistema nonché il nome utente e la password di un account con privilegi amministrativi, quindi fare clic su **Avanti**.
7. Specificare la posizione e il nome di un file BIAR in cui eseguire il backup delle impostazioni di configurazione del server, quindi fare clic su **Avanti** per continuare.
Nella pagina "Conferma" vengono visualizzate le informazioni fornite.
8. Verificare che le informazioni fornite nella pagina "Conferma" siano corrette e fare clic su **Fine** per continuare.
CCM esegue il backup delle impostazioni di configurazione del server per l'intero cluster sul file BIAR specificato. I dettagli relativi alla procedura di backup vengono scritti in un file di registro. Il nome e il percorso del file di registro vengono visualizzati in una finestra di dialogo.
9. Se l'operazione di backup non riesce, verificare il file di registro per identificare il motivo.

10. Fare clic su **OK** per chiudere la procedura guidata.

13.4.2.2 Backup delle impostazioni del server in UNIX

In UNIX utilizzare lo script `serverconfig.sh` per eseguire il backup delle impostazioni del server della distribuzione in un file BIAR.

1. Selezionare **5 - Esegui backup configurazione server** e premere **Invio**.
2. Specificare se utilizzare un server CMS esistente per il backup delle impostazioni di configurazione del server o creare un CMS temporaneo.
 - Per eseguire il backup delle impostazioni del server da un sistema in esecuzione, selezionare **esistente** e premere **Invio**.
 - Per eseguire il backup delle impostazioni del server da un sistema non in esecuzione o per ripristinare le impostazioni del server, selezionare **temporaneo** e premere **Invio**.
3. se si utilizza un server CMS temporaneo per il backup delle impostazioni del server, nelle schermate successive selezionare un numero di porta per il CMS temporaneo da utilizzare e le informazioni di connessione al database di sistema CMS.

Per ridurre il rischio che altri utenti accedano al sistema durante il ripristino, specificare un numero di porta diverso da quelli utilizzati per i CMS esistenti.
4. Quando richiesto, accedere al server CMS specificando il sistema, il nome utente e la password di un account con privilegi di amministratore, quindi premere **Invio**.
5. Quando richiesto, specificare il percorso e il nome di un file BIAR in cui eseguire il backup delle impostazioni di configurazione e premere **Invio**.

Le informazioni fornite vengono visualizzate in una pagina di riepilogo.
6. Verificare che le informazioni visualizzate siano corrette e premere **Invio** per continuare.

Lo script `serverconfig.sh` esegue il backup delle impostazioni di configurazione del server per l'intero cluster nel file BIAR specificato. I dettagli della procedura di backup vengono scritti in un file di registro. Vengono visualizzati il nome e il percorso del file di registro.
7. Se il backup non viene eseguito, verificare il file di registro per identificare il motivo.

13.4.2.3 Per eseguire il backup delle impostazioni del server mediante script

Per creare un backup delle impostazioni del server nella distribuzione, è possibile eseguire il file `BackupCluster.bat` in Windows o lo script `backupcluster.sh` in UNIX.

In Windows il file `BackupCluster.bat` si trova nella directory `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

In UNIX `backupcluster.sh` si trova nella directory `/DIRINSTALL/sap_bobj/enterprise_xi40/platform64/scripts`.

Argomenti correlati

- [Script BackupCluster e RestoreCluster](#)

13.4.3 Backup del contenuto BI

È consigliabile utilizzare l'applicazione Promotion Management per eseguire regolarmente il backup del contenuto Business Intelligence, ad esempio report, utenti e gruppi e universi. Disporre di backup aggiornati dei contenuti consente di ripristinare Business Intelligence senza dover ripristinare tutto il sistema o le impostazioni del server.

Per ulteriori informazioni sull'utilizzo dell'applicazione Promotion Management, consultare il capitolo "Promotion Management" di questa guida.

Se con l'applicazione Promotion Management si utilizza Subversion, vedere il capitolo "Gestione delle versioni".

13.5 Ripristino del sistema

Se il sistema è danneggiato, è possibile ripristinarlo interamente, ripristinando di conseguenza anche la piattaforma BI. A seconda delle condizioni del sistema, il ripristino completo potrebbe non essere necessario. Se il sistema funziona normalmente ma parte del contenuto è stata persa o danneggiata, è possibile scegliere di ripristinare solo il contenuto Business Intelligence (BI). Se il contenuto BI è valido ma i server della piattaforma sono stati configurati in modo non corretto, è possibile ripristinare solo le impostazioni del server.

La procedura è la stessa che si segue per eseguire un ripristino da un back a caldo o a freddo.

Argomenti correlati

- [Ripristino dell'intero sistema](#)
- [Ripristino delle impostazioni server](#)
- [Ripristino del contenuto BI](#)

13.5.1 Ripristino dell'intero sistema

Quando viene ripristinato l'intero sistema, viene ripristinato anche il cluster della piattaforma BI. A seconda del tipo di errore che si è verificato nel sistema, potrebbe ancora essere possibile eseguire un ripristino parziale.

Se uno dei componenti seguenti riporta errori o viene perso, è necessario ripristinare l'intero sistema:

- Database CMS

Nota:

Se la piattaforma BI funziona normalmente ma il database CMS è stato arrestato in modo anomalo, è possibile ripristinarlo senza dover ripristinare l'intero sistema.

- Archivio file FRS
- File system del computer

Nota:

Per un ripristino dell'intero sistema, il sistema di destinazione non richiede che la piattaforma BI sia già installata.

Se viene corrotto o perso soltanto il database di controllo, è possibile ripristinarlo, senza dover ripristinare l'intero sistema.

Se il contenuto a livello Web viene corrotto o perso, è possibile ripristinarlo senza dover ripristinare l'intero sistema.

Argomenti correlati

- [Ripristino dell'intero sistema](#)
- [Ripristino del solo database di controllo](#)
- [Ripristino del contenuto a livello Web](#)
- [Ripristino del solo database CMS](#)

13.5.1.1 Ripristino dell'intero sistema

Prima ripristinare il sistema, è necessario utilizzare Central Configuration Manager (CCM) per arrestare tutti i nodi della distribuzione della piattaforma BI e scegliere il momento preciso in cui si intende ripristinare il sistema.

Nota:

se si intende ripristinare il sistema al suo stato corrente, eseguire il backup del sistema prima di eseguire l'operazione.

1. Individuare i file di backup seguenti:

- Backup del database CMS
- Backup dell'archivio file FRS di input e di output
- Backup dei file system per ogni macchina host inclusa nel cluster della piattaforma BI

Nota:

assicurarsi di convalidare i backup e verificare che tutti i file elencati sopra provengano dallo stesso di set di backup. Se il backup impostato è stato ottenuto come backup a caldo, verificare che la data/ora di inizio del backup del database CMS sia precedente alla data/ora del file system del computer host, del livello Web e dell'archivio file FRS corrispondente. Saranno necessari tutti questi file anche se il problema riguarda un solo componente.

2. Utilizzare gli strumenti di ripristino file per ripristinare il file system di tutti i computer host nel cluster della piattaforma BI.
3. Utilizzare gli strumenti di ripristino file per ripristinare gli archivi file FRS di input e di output.
4. Utilizzare gli strumenti del database per ripristinare il database CMS.
5. Se la password del database CMS è stata modificata dopo la creazione del backup, utilizzare CCM per aggiornare la password del database CMS su tutti i nodi e i computer host della piattaforma BI.
6. Se si utilizza la funzionalità di controllo:
 - a. Individuare gli ultimi backup e registri delle transazioni relativi al database di controllo.
 - b. Utilizzare gli strumenti del database per ripristinare il database di controllo.
 - c. Eseguire un rollforward sul database di controllo, riproducendo il registro delle transazioni.
7. Per il ripristino dell'indice di ricerca, scegliere una delle opzioni seguenti:
 - Se si desidera eseguire lo script di recupero dell'indice di ricerca, consultare l'argomento [Esecuzione dello script di recupero dell'indice di ricerca](#) e seguire le istruzioni in esso contenute. In questo modo si otterrà più velocemente un indice completo.
 - Se si desidera rigenerare l'indice di ricerca anziché utilizzare lo script di recupero, utilizzare CCM per riavviare i nodi della piattaforma BI. Questa procedura è più semplice ma durante la rigenerazione dell'indice si potrà accedere solo parzialmente ai dati della piattaforma per le ricerche.
8. Avviare il sistema e annotare l'ora per utilizzarla durante la procedura conclusiva richiesta.
9. Verificare che il sistema stia funzionando nel modo previsto ed eseguire un test di integrità.

Dopo aver verificato il sistema, intraprendere le azioni seguenti:

- Eseguire il Repository Diagnostic Tool per rimuovere gli eventuali file temporanei inutilizzati e verificare la coerenza del repository. Consultare la sezione relativa allo Strumento di diagnostica del repository di questo manuale.
- Se lo script di recupero dell'indice non è stato utilizzato, rigenerare l'indice di ricerca della piattaforma.
- I processi di pubblicazione in esecuzione al momento del backup del sistema verranno visualizzati come non riusciti. Non rieseguire queste istanze ma avviare nuovi processi di pubblicazione.
- Se il database di controllo è stato ripristinato, è necessario eseguire una query SQL per rimuovere tutti gli eventi che si sono verificati tra l'errore del database e l'ora di riavvio (l'ora annotata al passaggio 8). Ad esempio: `delete from [NOME_DB].ADS_EVENT where Start_Time > '[ora errore DB]' and Start_Time < '[ora ripristino DB]'`

Argomenti correlati

- [Indicizzazione del contenuto nel repository CMS](#)

13.5.1.2 Ripristino del solo database di controllo

Prima di ripristinare il sistema di controllo, è necessario utilizzare Central Configuration Manager (CCM) per arrestare tutti i nodi della distribuzione della piattaforma BI. È inoltre necessario scegliere il momento preciso in cui si intende ripristinare il database.

Nota:

Eseguire questa attività solo se si è certi che il database di controllo è l'unico componente compromesso della piattaforma BI. Se anche altri componenti sono danneggiati, è necessario ripristinare l'intero sistema.

1. Individuare gli ultimi backup e registri delle transazioni relativi al database di controllo.
2. Utilizzare gli strumenti del database per ripristinare il database di controllo.
3. Eseguire un rollforward sul database di controllo, riproducendo il registro delle transazioni.

Argomenti correlati

- [Ripristino dell'intero sistema](#)

13.5.1.3 Ripristino del contenuto a livello Web

Prima di ripristinare il contenuto a livello Web, è necessario arrestare tutti i nodi inclusi nella distribuzione della piattaforma BI utilizzando Central Configuration Manager (CCM). Sarà inoltre necessario decidere in quale momento specifico eseguire il ripristino.

Se si desidera avere la possibilità di tornare allo stato corrente del sistema, è necessario eseguire un backup del sistema prima del ripristino.

Se il livello Web è corrotto è possibile ripristinarlo in modo individuale.

1. Utilizzare gli strumenti di ripristino dei file per ripristinare le cartelle a livello Web sulla macchina host a livello Web.
2. Utilizzare CCM per riavviare tutti i nodi per la distribuzione della piattaforma BI.

13.5.1.4 Ripristino del solo database CMS

Nota:

Eseguire questa procedura se l'unico componente che si è arrestato è il database CMS. Se il database si è danneggiato o il funzionamento di altri componenti è compromesso, è necessario eseguire il ripristino di tutto il sistema.

Riparare o sostituire la macchina host del database CMS. In caso di sostituzione, assicurarsi che abbia lo stesso nome di sistema della macchina host precedente, nonché impostazioni della porta e credenziali del database identiche.

Nota:

se non è possibile ripristinare la macchina utilizzando lo stesso nome e le stesse credenziali, sarà necessario utilizzare CCM per aggiornare le informazioni sulla connessione del database per ogni nodo del cluster e riavviare i nodi.

1. Arrestare tutti i nodi della piattaforma BI utilizzando CCM.
2. Individuare il set di backup del database CMS più recente.
3. Utilizzando gli strumenti del database, ripristinare il database CMS.
4. Individuare il registro transazioni del database CMS più recente, ossia il registro contenente le transazioni eseguite dopo l'ultimo backup.
5. Riprodurre l'intero registro delle transazioni per il database CMS.
6. Utilizzare CCM per avviare i nodi della piattaforma BI.

Dopo aver verificato il corretto funzionamento del sistema, effettuare le operazioni seguenti:

- Eseguire il Repository Diagnostic Tool per rimuovere gli eventuali file temporanei inutilizzati e verificare la coerenza del repository. Consultare la sezione relativa allo Strumento di diagnostica del repository di questo manuale.
- I processi di pubblicazione in esecuzione al momento del backup del sistema verranno visualizzati come non riusciti. Non rieseguire queste istanze ma avviare nuovi processi di pubblicazione.

Argomenti correlati

- [Indicizzazione del contenuto nel repository CMS](#)

13.5.1.5 Recupero dell'indice di ricerca

La funzionalità di ricerca della piattaforma gestisce una serie di file di indice e di informazioni in tutto il sistema per consentire ricerche più efficienti. Se è necessario ripristinare il sistema, tali file di informazioni

possono generare incoerenze. È possibile riparare tali incoerenze utilizzando lo script di recupero dell'indice o rigenerando l'indice.

La ricreazione dell'indice è un processo diretto, ma richiede una notevole quantità di risorse e molto tempo per essere completato. Inoltre le ricerche eseguite durante la ricreazione restituiranno solo risultati per le parti indicizzate del database. Lo script di recupero prevede una procedura più complicata, ma che garantisce un indice completo e funzionante in breve tempo.

Se si sta ripristinando una distribuzione con più computer, eseguire lo script su tutti i computer che ospitano il servizio di ricerca. Per il primo computer in un cluster, utilizzare l'opzione `-Both`, quindi su tutti gli altri computer del cluster utilizzare l'opzione `-ContentStore`.

Argomenti correlati

- [Indicizzazione del contenuto nel repository CMS](#)

13.5.1.5.1 Esecuzione dello script di recupero dell'indice di ricerca

- Verificare che CMS sia in esecuzione e arrestare tutti gli Adaptive Processing Server (APS) in cui è installato il servizio di ricerca.

Nota:

È necessario arrestare tali APS subito dopo l'avvio del nodo.

- Impostare `JAVA_HOME` sul percorso `sapjvm/bin` nella directory di installazione della piattaforma BI.
- La directory dei dati di ricerca piattaforma è accessibile dal computer in cui si esegue lo script.

1. Sulla macchina host CMS o APS aprire una finestra della riga di comando (se si utilizza un sistema operativo Windows).

2. Passare alla directory seguente `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\java\lib\`.

I computer Unix utilizzano il percorso file Unix equivalente.

3. Digitare `java -jar platformSearchOnlineHotbackupRestore.jar` e premere **Invio**.

4. Alla richiesta, immettere le informazioni seguenti e premere **Invio**:

- Il percorso dell'installazione della piattaforma BI (ad esempio, `DIRINSTALL/SAP businessObjects Enterprise XI 4.0`)
- Le credenziali di accesso CMS, incluso il nome CMS, l'ID e la password utente e il tipo di autenticazione. Il tipo di autenticazione presenta le seguenti opzioni:
 - `SecEnterprise`
 - `secLDAP`
 - `secWinAD`
 - `secSAPR3`

5. Quando viene richiesto il tipo di ripristino dell'indice, digitare una delle opzioni seguenti e premere **Invio**.

Valore	Descrizione
-Both	Questa opzione deve essere utilizzata per distribuzioni di server singoli oppure nelle distribuzioni in più computer, per il primo computer host APS con il servizio di ricerca. In un sistema con più APS di ricerca, la prima volta che lo script viene eseguito, utilizzare il valore <code>-Both</code> (per aggiornare il database e l'archivio contenuti). Se lo script viene eseguito per tutti gli altri APS di ricerca, utilizzare il valore <code>-ContentStore</code> (per aggiornare solo l'archivio contenuti).
-ContentStore	Questa opzione deve essere utilizzata quando si esegue lo script su computer host APS in cui è installato il servizio di ricerca, a meno che non si tratti del primo computer nel cluster in cui viene eseguito lo script.
-Exit	Questa opzione consente di chiudere lo script senza eseguire un ripristino dell'indice.

- Al termine dell'esecuzione dello script, chiudere la finestra della riga di comando (per le macchine Windows).

Avviare tutte le istanze di APS arrestate.

13.5.2 Ripristino delle impostazioni server

Per ripristinare le impostazioni server del sistema da un file BIAR, è possibile utilizzare CCM (Central Configuration Manager) o lo script `RestoreCluster`. Il ripristino del contenuto del server da un file BIAR non influenza contenuto Business Intelligence quali report, utente e gruppi o impostazioni di protezione.

Nota:

- quando si ripristinano le impostazioni server, è supportato il ripristino delle impostazioni di un intero cluster. Non è possibile ripristinare solo le impostazioni di una parte dei server del cluster.
- se si intende eseguire il backup o il ripristino delle impostazioni del server in una distribuzione in cui SSL è abilitato, è necessario prima disabilitare SSL mediante CCM, quindi abilitarlo nuovamente al completamento del backup o del ripristino.

Argomenti correlati

- [Configurazione dei server per SSL](#)

13.5.2.1 Ripristino delle impostazioni server mediante CCM in Windows

È possibile utilizzare CCM (Central Configuration Manager) per ripristinare le impostazioni server. Dopo aver ripristinato le impostazioni server, è necessario creare nuovamente i nodi del sistema in ogni computer del cluster di sistema.

1. Arrestare tutti i nodi su tutti i computer del cluster per i quali è in corso il ripristino delle impostazioni di configurazione server, arrestando Server Intelligence Agent per ogni nodo.
2. Avviare CCM in un computer che utilizza un CMS.
3. Fare clic su **Ripristina configurazione server** sulla barra degli strumenti.
Viene visualizzato il "Ripristino guidato configurazione server".
4. Fare clic su **Avanti** per avviare la procedura guidata.
5. Quando viene richiesto, fornire il numero di porta del CMS (Central Management Server) temporaneo da utilizzare e le informazioni necessarie per connettersi al database di sistema CMS, quindi fare clic su **Avanti** per continuare.
6. Inserire la chiave cluster e fare clic su **Avanti** per continuare.
7. Quando richiesto, accedere a CMS immettendo il nome CMS e il nome utente e la password di un account con privilegi amministrativi e fare clic su **Avanti** per continuare.
8. Specificare la posizione e il nome del file BIAR che contiene le impostazioni di configurazione server da ripristinare, quindi fare clic su **Avanti** per continuare.
In una pagina di riepilogo vengono visualizzati i contenuti del file BIAR.
9. Fare clic su **Avanti** per continuare.
In una pagina di riepilogo vengono visualizzate le informazioni immesse dall'utente.
10. Fare clic su **Fine** per continuare.
Un messaggio di avviso indica che le impostazioni server esistenti verranno sovrascritte con i valori contenuti nel file BIAR e, nel caso in cui si scelga di procedere, le impostazioni server correnti saranno perse.
11. Fare clic su **Sì** per ripristinare le impostazioni di configurazione del server.
CCM esegue il ripristino delle impostazioni di configurazione del server per l'intero cluster dal file BIAR. I dettagli relativi al ripristino vengono scritti in un file di registro. Il nome e il percorso del file di registro vengono visualizzati in una finestra di dialogo.
12. Se l'operazione di ripristino non riesce, verificare il file di registro per identificare il motivo.
13. Fare clic su **OK** per chiudere la procedura guidata.

Le impostazioni server presenti nel file BIAR vengono ripristinate sul sistema. Vengono creati i nodi e i server esistenti nel file BIAR che non erano presenti nel sistema prima del ripristino.

Nota:

i nodi e i server esistenti nel sistema ma non nel file BIAR vengono rimossi dal repository. I nodi e i server vengono ancora visualizzati in CCM, ma è possibile cancellare manualmente i file `dbinfo` e `bootstrap` in un nodo.

È necessario creare nuovamente i nodi del sistema in ogni computer del cluster.

Argomenti correlati

- [Utilizzo dei nodi](#)

13.5.2.2 Ripristino delle impostazioni server in Unix con CCM

Nei computer Unix, utilizzare lo script `serverconfig.sh` per ripristinare le impostazioni del server di distribuzione da un file BIAR.

1. Selezionare **6 - Ripristina configurazione server** e premere **Invio**.
2. Immettere un numero di porta per il server Central Management Server (CMS) temporaneo da utilizzare e premere **Invio**.
3. Nelle schermate successive, specificare le informazioni di connessione al database di sistema CMS.
4. Quando richiesto, accedere a CMS specificando il sistema, il nome utente e la password di un account con privilegi amministrativi e premere **Invio**.
5. Quando richiesto, specificare il percorso e il nome del file BIAR da cui si desidera eseguire il ripristino delle impostazioni della configurazione server quindi premere **Invio**.

Le informazioni fornite vengono visualizzate in una schermata di riepilogo.

6. Verificare che le informazioni visualizzate siano corrette e premere **Invio** per continuare.

Lo script `serverconfig.sh` ripristina le impostazioni di configurazione del server per l'intero cluster dal file BIAR specificato. I dettagli della procedura di ripristino vengono scritti in un file di registro. Il nome e il percorso del file di registro vengono visualizzati sullo schermo.

7. Se l'operazione di ripristino non riesce, controllare il file di registro per determinare il motivo.

13.5.2.3 Ripristino delle impostazioni del server con uno script

Se si preferisce, è possibile ripristinare le impostazioni server della distribuzione eseguendo lo script `RestoreCluster.bat` in Windows o lo script `restorecluster.sh` in Unix.

In Windows `RestoreCluster.bat` si trova nella directory `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts`.

In Unix `restorecluster.sh` si trova nella directory `/DIRINSTALL/sap_bobj/enterprise_xi40/PLATFORM64/scripts`.

Argomenti correlati

- [Script BackupCluster e RestoreCluster](#)

13.5.3 Ripristino del contenuto BI

Se il backup del contenuto Business Intelligence (BI) è stato eseguito in file LCMBIAR, è possibile utilizzare Lifecycle Management Console per ripristinare il contenuto BI, senza dover ripristinare l'intero sistema. Per ulteriori informazioni consultare il *Manuale dell'utente di Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0*.

13.6 Script BackupCluster e RestoreCluster

Nella tabella che segue sono riportati i parametri della riga di comando utilizzati con lo script `BackupCluster`.

Nota:

questo script consente di eseguire il backup solo delle impostazioni server di un cluster. È necessario eseguire il backup degli altri dati separatamente.

Tabella 13 - 2: Parametri di BackupCluster

Nome	Descrizione	Esempio
-backup	Nome e percorso del file BIAR in cui si desidera creare il backup delle impostazioni del server del sistema per il ripristino.	-backup "C:\Users\Administrator\Desktop\my.biar"
-cms	Nome host del computer in cui si trova il server CMS del sistema. Se il server CMS viene eseguito su una porta diversa da quella predefinita (6400), è necessario specificare anche il numero di porta.	-cms mycms:6400
-username	Nome utente di un account Administrator.	-username Administrator
-password	Password di un account Administrator.	-password Password1

Nella tabella che segue sono riportati i parametri della riga di comando utilizzati con lo script `RestoreCluster`.

Tabella 13 - 3: Parametri di RestoreCluster

Nome	Descrizione	Esempio
-restore	Il nome e il percorso del file BIAR che contiene le impostazioni di configurazione del server che si desidera ripristinare.	-restore "C:\Users\Administrator\Desktop\my.biar"
-username	Nome utente di un account Administrator.	-username Administrator
-password	Password di un account Administrator.	-password Password1
-displaycontents	Visualizza un elenco di nodi e server contenuti nel file BIAR.	-displaycontents "C:\Users\Administrator\Desktop\my.biar"

Nota:

eseguire lo script `RestoreCluster` con il parametro `-displaycontents` per visualizzare i contenuti del file BIAR prima di ripristinare le impostazioni del server.

I parametri riportati di seguito sono necessari se si esegue il backup delle impostazioni server da un sistema non in esecuzione oppure se si stanno ripristinando le impostazioni server.

Tabella 13 - 4: Parametri utilizzati con un server CMS temporaneo

Nome	Descrizione	Esempio
-usetempcms	Crea un CMS temporaneo per l'operazione specificata. Al termine dell'operazione, il CMS temporaneo viene arrestato.	-usetempcms
-cmsport	Numero della porta del CMS temporaneo.	-cmsport 6700

Nome	Descrizione	Esempio
-dbdriver	<p>Il driver di database del data base di sistema CMS. I valori accettati sono:</p> <ul style="list-style-type: none"> • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem • sqlanywheredatabasesubsystem • newdbdatabasesubsystem <p>Nota: il parametro newdbdatabase subsystem viene utilizzato con i database SAP HANA.</p>	-dbdriver sqlserverdatabasesubsystem
-connect	La stringa di connessione al database di sistema CMS.	-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"
-dbkey	La chiave cluster.	-dbkey abc1234

Esempio:

Nell'esempio che segue, viene eseguito il backup delle impostazioni del server su un file BIAR, utilizzando un server CMS esistente.

```
-backup "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
```

Esempio:

L'esempio che segue mostra in che modo viene visualizzato il contenuto di un file BIAR.

```
-displaycontents "C:\Users\Administrator\Desktop\mybiar.biar"
```

Esempio:

L'esempio che segue mostra in che modo vengono ripristinate le impostazioni dal file BIAR. Utilizzare sempre un CMS temporaneo quando si ripristinano le impostazioni del server.

```
-restore "C:\Users\Administrator\Desktop\my.biar"  
-cms mycms:6400  
-username Administrator  
-password Password1  
-usetempcms  
-cmsport 6400  
-dbdriver sqlserverdatabasesubsystem  
-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=Password1;HOSTNAME=database;PORT=3306"  
-dbkey abc1234
```

Copia della distribuzione della piattaforma BI

14.1 Panoramica della copia del sistema

In questo capitolo è descritto come creare un duplicato della distribuzione della piattaforma BI a scopo di test o standby o per altri scopi.

Argomenti correlati

- [Panoramica di backup e ripristino](#)

14.2 Terminologia

Termine	Definizione
Sistema di origine	La distribuzione della piattaforma BI originale.
Sistema di destinazione	La nuova distribuzione che si desidera creare.
Copia del sistema	La creazione di un duplicato di una distribuzione della piattaforma BI esistente.
Copia del sistema omogenea	La creazione di un duplicato del sistema in cui il sistema di origine e quello di destinazione utilizzano sistema operativo e database dello stesso tipo. La piattaforma BI supporta solo copie di sistema omogenee.
Copia del sistema eterogenea	La creazione di un duplicato del sistema in cui il sistema di origine e quello di destinazione utilizzano sistemi operativi e database diversi ma si basano sugli stessi dati.
Copia del database	La creazione di un duplicato del database di sistema CMS o del database di controllo mediante gli strumenti del fornitore del database.

14.3 Casi di utilizzo per la copia del sistema

Nella tabella seguente vengono descritti gli obiettivi che l'utente potrebbe voler raggiungere in base alle risorse a sua disposizione, con l'indicazione delle soluzioni più appropriate.

Obiettivo	Risorse necessarie	Soluzione
<p>Obiettivo: copia identica</p> <p>Creazione di un sistema duplicato a scopo di standby o test con una configurazione hardware e indirizzi IP/nomi computer identici.</p>	<ul style="list-style-type: none"> Una soluzione di destinazione con hardware identico a quello del sistema di origine E Backup del sistema di origine o accesso al sistema di origine da cui creare un backup. 	<p>Utilizzare il workflow di backup e ripristino del sistema descritto in dettaglio in questo manuale. Consultare la procedura Backup dell'intero sistema. Ricreare il sistema di destinazione da backup del sistema di origine.</p>
<p>Obiettivo: copia</p> <p>Creazione di un sistema duplicato a scopo di standby, test o formazione con hardware e indirizzi IP/nomi computer diversi da quelli del sistema di origine.</p>	<ul style="list-style-type: none"> Sistema di origine (in esecuzione o arrestato) O backup dei database e dei file del sistema di origine. E Informazioni dettagliate sul sistema descritte in Per eseguire l'esportazione da un sistema di origine 	<p>Utilizzare il workflow della copia del sistema, iniziando con Pianificazione della copia del sistema e seguire le istruzioni per il resto del capitolo.</p> <p>Nota:</p> <p>È possibile creare il sistema di destinazione su un computer con una distribuzione esistente della piattaforma BI con la stessa versione, lo stesso pacchetto di supporto e lo stesso livello patch oppure in un computer pulito senza piattaforma BI installata.</p>

Argomenti correlati

- [Backup](#)
- [Pianificazione della copia del sistema](#)

14.4 Pianificazione della copia del sistema

Una copia del sistema non deve riflettere il sistema corrente. È possibile creare una copia del sistema e attendere un po' prima di procedere alla ricreazione della copia sul sistema di destinazione o in alternativa è possibile utilizzare un backup precedente del sistema di origine come base per il sistema di destinazione. La copia corrisponderà al sistema così com'era nel momento in cui la copia è stata creata. Se ad esempio si attende un mese, la copia ricreerà il sistema nelle condizioni in cui questo si trovava un mese prima.

Dopo aver esaminato gli esempi di utilizzo nella sezione precedente ed aver scelto il più adatto alle proprie esigenze, è necessario sviluppare un piano per la copia del sistema.

Creazione di una copia del sistema

Quando si pianifica la copia di un sistema, è consigliabile stabilire preventivamente i seguenti punti:

- Se il sistema di origine deve essere arrestato o attivo durante la creazione della copia. La procedura può essere effettuata in entrambi i casi.
 - Se il sistema deve essere arrestato, quanto tempo di inattività sarà necessario.
 - Pianificare del tempo per il test in modo da garantire l'integrità del sistema di destinazione.
- Quali strumenti utilizzare per il backup e il ripristino del database.
- In quali computer distribuire il sistema di destinazione e dove verrà ospitato ciascun nodo.
- Quali componenti facoltativi copiare.
- Il tipo di database da utilizzare per il database CMS di destinazione ed eventuali altri database facoltativi da copiare.

È inoltre necessario considerare gli aspetti seguenti:

- Quali componenti della piattaforma BI sono installati nel sistema di origine. È inoltre possibile utilizzare la funzione **Aggiungi/Rimuovi > Modifica** del programma di installazione per visualizzare l'elenco dei componenti attualmente installati.
- Se il sistema di destinazione è installato in un'installazione hardware differente dal sistema di origine, potrebbe essere necessario ottimizzare il sistema di destinazione per ottenere prestazioni migliori. Consultare le informazioni relative al miglioramento delle prestazioni del sistema nel manuale *SAP BusinessObjects Business Intelligence sizing companion guide*.
- Se si desidera, è possibile fare in modo che per il sistema di destinazione i report vengano creati da database diversi da quelli del sistema di origine. In questo caso sarà necessario modificare le informazioni di connessione per i database di creazione report. A tale scopo, è possibile mantenere lo stesso nome DNS per il sistema di destinazione, modificando però il database a cui il DNS fa riferimento.

Componenti del sistema di origine richiesti

- Database di sistema CMS
- Archivio file FRS
- File di configurazione del livello semantico
- Database di controllo (facoltativo)
- Database di monitoraggio (facoltativo)
- Database di Subversion di Lifecycle Management (facoltativo)

14.5 Considerazioni e limitazioni

Durante la creazione di una copia della distribuzione della piattaforma BI è necessario tenere conto delle considerazioni seguenti.

Ad area	Considerazione
Integrazioni con SAP Business Warehouse	Se si utilizzano la piattaforma BI e SAP ERP o BW in un ambiente integrato, prima di eseguire la copia del sistema leggere la documentazione relativa alla copia di sistemi SAP. I manuali relativi alla copia del sistema sono disponibili all'indirizzo http://www.sdn.sap.com/irj/sdn/systemcopy (è richiesto l'accesso a SMP). Scegliere la versione di SAP NetWeaver. I relativi manuali sono disponibili nella cartella dei manuali di installazione.
Versione dei programmi	Il sistema di origine e quello di destinazione devono avere la stessa versione, lo stesso pacchetto di supporto e lo stesso livello patch.
Impostazioni relative al contenuto e alla configurazione	È possibile copiare solo l'intero sistema. Non è possibile copiare selettivamente il contenuto o le impostazioni di configurazione del sistema.
Percorso di installazione	I percorsi di installazione di origine e di destinazione devono essere identici. Ad esempio, se il sistema di origine è installato in <code>C:\SAP BusinessObjects Enterprise XI 4.0</code> , è necessario installare anche il sistema di destinazione in <code>C:\SAP BusinessObjects Enterprise XI 4.0</code> .
Sistema operativo host	I sistemi operativi di origine e di destinazione devono essere identici.
Tipo di software di database CMS	I database di origine e destinazione CMS devono essere dello stesso tipo. È possibile scegliere se passare a un altro tipo di database supportato, dopo aver copiato il sistema.
Tipo di software di database di controllo	Se si desidera effettuare la copia di dati di controllo, i database di controllo di origine e di destinazione devono essere dello stesso tipo. Dopo la creazione della copia, sarà possibile stabilire un nuovo database di tipo diverso. Nota: se si stabilisce un nuovo database, gli eventi esistenti non verranno copiati all'interno di esso. Nel nuovo database verranno registrati solo i nuovi eventi.
Personalizzazione del livello Web	La procedura di copia non consente di copiare i componenti del livello Web dal sistema di origine. Se il livello Web è stato personalizzato (ad esempio modificando i file <code>.properties</code> nella cartella <code>custom</code>) è necessario applicare manualmente le stesse personalizzazioni alla destinazione.
Argomenti non trattati in queste istruzioni	Il workflow illustrato non descrive come esportare o importare un database. Per la copia e il ripristino del database utilizzare gli strumenti del fornitore del database.

Durante la procedura di copia del sistema vengono copiati i dati seguenti:

- Database del repository CMS (contiene report, analitiche, cartelle, diritti, utenti e gruppi di utenti, impostazioni del server e altro contenuto della piattaforma BI e di sistema).
- Database di controllo (contiene eventi di controllo attivati dai server della piattaforma BI o da applicazioni client).
- Database di monitoraggio (contiene dati di tendenza da metriche, probe e controlli).
- Database di Lifecycle Management (contiene versioni diverse di report, analitiche, altre risorse BI e informazioni sulla versione).

Nota:

per una descrizione dei database e del relativo contenuto, consultare la sezione [Database](#) di questo manuale.

- File di configurazione del livello semantico

La configurazione dei livelli Web, l'indice di ricerca e i dati non citati esplicitamente in precedenza non vengono copiati.

Considerazioni sulle copie per il recupero dei file

Se lo scopo specifico dell'esecuzione della copia del sistema è il recupero di un file eliminato per errore, è inoltre necessario tenere conto delle considerazioni seguenti.

Utilizzando il backup, eseguire i passaggi della procedura [Per eseguire l'importazione in un sistema di destinazione](#) sul sistema di produzione.

- Non installare tutti i nodi, ma solo il primo, che conterrà il CMS e il relativo database.
- Non installare i database di controllo, LCM e di monitoraggio.
- Non ricreare le connessioni ai database di controllo o di creazione report.

Utilizzare LCM per promuovere l'oggetto che si desidera recuperare dal sistema di destinazione al sistema di origine.

14.6 Procedura di copia del sistema

Le procedure seguenti consentono di eseguire le due fasi relative alla copia della distribuzione della piattaforma BI.

14.6.1 Per eseguire l'esportazione da un sistema di origine

È necessario prendere nota delle informazioni seguenti relative al sistema di origine: Se si desidera scrivere queste informazioni, è disponibile un foglio di lavoro in [Foglio di lavoro della copia del sistema](#).

Proprietà	Posizione
Chiave cluster CMS. Assicurarsi che questa informazione sia protetta.	Creata dall'amministratore di sistema al momento dell'installazione della piattaforma BI.
Nome dei nodi.	Passare alla scheda Server della console CMC. Nella struttura a sinistra espandere Nodi .
Nome computer e cartella di installazione della piattaforma BI di ogni computer della distribuzione.	Passare alla scheda Server della console CMC, fare clic con il pulsante destro del mouse sul CMS e scegliere Segnaposto . Cercare il valore del segnaposto <code>%INSTALLROOTDIR%</code> .
Password dell'amministratore della piattaforma BI. Assicurarsi che questa informazione sia protetta.	Creata dall'amministratore di sistema al momento dell'installazione della piattaforma BI.
<p>Tutte le connessioni ai database che possono essere utilizzate dal CMS, nonché nomi utente e password associati a tali connessioni. Sono comprese le connessioni al database di controllo, se si desidera copiare tali informazioni. Verificare di recuperare queste informazioni per tutti i computer del cluster.</p> <p>Nota: se si desidera copiare il database di controllo, sono inoltre necessari i nomi e le credenziali di connessione a questo.</p>	<p>Passare alla scheda Server della console CMC, fare clic con il pulsante destro del mouse sul CMS e scegliere Metriche.</p> <p>Verificare le metriche seguenti:</p> <ul style="list-style-type: none"> • "Nome connessione database di sistema" • "Nome server database di sistema" • "Nome utente database di sistema" • "Nome origine dati" • "Nome connessione database di controllo" (facoltativo) • "Nome utente database di controllo" (facoltativo)
Per ogni computer del cluster, i dettagli (tipo di client, versione) delle altre connessioni a database, ad esempio quelle utilizzate da universi e report. Non dimenticare di includere nomi utente e password.	Per i report Crystal generati direttamente dai database, verificare le informazioni di connessione utilizzando le applicazioni di progettazione di SAP Crystal Reports 2011 o SAP Crystal Reports for Enterprise. Per le informazioni di connessione a universi, utilizzare Information Design Tool (.unx) o Universe Design Tool (.unv).
Versione, pacchetto di supporto e livello patch del sistema di origine.	<p>In Windows queste informazioni sono individuabili all'interno dello strumento "Installazione applicazioni".</p> <p>In Unix è possibile utilizzare l'utilità <code>modifyOrRemoveProducts.sh</code> disponibile nella directory di installazione della piattaforma BI.</p>

Proprietà	Posizione
<p>I percorsi degli archivi file per ogni FRS di input e di output nella distribuzione.</p>	<p>Passare alla scheda Server della console CMC, fare clic con il pulsante destro del mouse sull'FRS di input o di output e scegliere Proprietà. Verificare la proprietà "Directory archivio file".</p> <p>Nota: Se il valore inizia con %, si tratta di un segnaposto ed è necessario fare clic su Segnaposto e prendere nota della directory riportata nel segnaposto.</p>

Proprietà	Posizione
Se si intende copiare LCM (Lifecycle Management), il percorso della cartella del database LCM e le cartelle di Subversion di LCM.	<p>La cartella predefinita per il database LCM nelle installazioni Windows è <i>DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOVERRIDE</i>, mentre in Unix è <i>DIRINSTALL/sap_bobj/data/LCM/LCMOverride</i>.</p> <p>Le cartelle predefinite per i file Subversion di LCM nelle installazioni Windows sono:</p> <ul style="list-style-type: none"> <i>DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\CheckOut</i> <i>DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository</i> <p>mentre in Unix sono:</p> <ul style="list-style-type: none"> <i>DIRINSTALL/check_out</i> (questa directory viene creata solo dopo avere utilizzato Subversion per l'estrazione dei file). <i>\$HOME/LCM_Repository</i>
Se si intende copiare il database di monitoraggio, la cartella di quest'ultimo.	<p>Questa è impostata nella console CMC. Passare all'area di gestione Applicazioni della console CMC, selezionare Applicazione di monitoraggio > Proprietà e verificare la "Directory di backup del database di tendenza".</p> <p>La cartella predefinita nelle installazioni Windows è <i>DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB</i>, mentre in Unix è <i>DIRINSTALL/sap_bobj/Data/TrendingDB</i>.</p>
Percorso della cartella di livello semantico.	Per impostazione predefinita, il percorso della cartella nelle installazioni Windows è <i>DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionsServer\</i> .

Dopo aver registrato le informazioni sopra descritte:

1. Utilizzare gli strumenti di backup del fornitore del database per creare una copia di backup dei database seguenti:
 - Il database di sistema CMS
 - Il database di controllo (facoltativo)
2. Utilizzando gli strumenti per il backup dei file, eseguire il backup dei set di file seguenti:
 - Gli archivi di file di input e di output FRS.

- Il database di tendenza di monitoraggio (facoltativo). A questo scopo, eseguire il backup dei file della cartella di monitoraggio registrati nel foglio di lavoro. Per impostazione predefinita, in Windows è: *DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB*. In Unix: *DIRINSTALL/sap_bobj/Data/TrendingDB*.
- Il database di Lifecycle Management (facoltativo). A questo scopo, eseguire il backup dei file della cartella di monitoraggio registrati nel foglio di lavoro. Per impostazione predefinita, in Windows è: *DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOVERRIDE*. In Unix: *DIRINSTALL/sap_bobj/data/LCM/LCMOverride*.
- Il database di Subversion di Lifecycle Management (facoltativo). A questo scopo, eseguire il backup dei file delle cartelle di Subversion registrate nel foglio di lavoro. Per impostazione predefinita, in Windows sono:
 - *DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\CheckOut*
 - *DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository*.

Mentre in Unix sono:

- *DIRINSTALL/check_out* (questa directory viene creata solo dopo avere utilizzato Subversion per l'estrazione dei file).
- *\$HOME/LCM_Repository*
- I file di configurazione della cartella di livello semantico: il file *cs.cfg* nella cartella *connectionServer* e i file *.sbo* e *.prm* nelle relative sottocartelle.

Nota:

per i vincoli e per una descrizione dettagliata di questo workflow, consultare la sezione [Backup a caldo](#).

3. I file elencati di seguito possono essere personalizzati dall'utente. Se personalizzati, eseguirne il backup dal sistema di origine e successivamente ripristinarli nella stessa cartella nel sistema di origine:

- *BO_trace.ini* installato in:
 - *[DIRINSTALLAZ]SAP BusinessObjects Enterprise XI 4.0/conf*
- *clientsDKOptions.xml* installato in:
 - *[DIRINSTALLAZ]SAP BusinessObjects Enterprise XI 4.0/java/lib*
 - *[DIRINSTALLAZ]SAP BusinessObjects Enterprise XI 4.0/win32_x86*
 - *[DIRINSTALLAZ]SAP BusinessObjects Enterprise XI 4.0/win64_x64*
- *CRConfig.xml* installato in:
 - *[DIRINSTALLAZ]SAP BusinessObjects Enterprise XI 4.0/java*
- *mdas.properties* installato in:
 - *[DIRINSTALLAZ]/SAP BusinessObjects Enterprise XI 4.0/java/pjs/services/MDAS/resources/com/businessobjects/multidimensional/services*
- I file di configurazione di WDeploy installati in *[DIRINSTALLAZ]SAP BusinessObjects Enterprise XI 4.0/wdeploy/conf*:
 - *config.apache*
 - *config.jboss7*
 - *config.sapappsvr73*
 - *config.tomcat6*

- config.tomcat7
- config.weblogic11
- config.websphere7
- config.websphere8
- wdeploy.conf

4. I file a livello Web elencati di seguito possono essere personalizzati dall'utente. Se sono state apportate modifiche a tali file, eseguirne il backup dal sistema di origine. Successivamente, sarà necessario ripristinarli o riapplicare le modifiche al sistema di destinazione.

- **BO_trace.ini installato in:**
 - [DIRINSTALLAZ]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/BOE/WEB-INF/TraceLog
 - [DIRINSTALLAZ]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/conf
 - **clientaccesspolicy.xml installato in:**
 - [DIRINSTALLAZ]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT
 - **clientSDKOptions.xml installato in:**
 - [DIRINSTALLAZ]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/clientapi/WEB-INF/lib
 - [DIRINSTALLAZ]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/lib
 - **crossdomain.xml installato in:**
 - [DIRINSTALLAZ]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT
 - [DIRINSTALLAZ]tomcat/webapps/ROOT
 - Eventuali file personalizzati nella cartella `config/custom` (livello Web). Eseguire il backup di questi file per trasferire la personalizzazione nel sistema di destinazione.
5. Eseguire il backup delle estensioni personalizzate aggiunte manualmente al sistema di origine, ad esempio le estensioni di pubblicazione, le librerie personalizzate e così via.

Conservare le informazioni registrate in precedenza con la copia dei database e dei file. È consigliabile conservare una seconda copia da aggiornare quando necessario per le procedure future di copia del sistema.

14.6.2 Per eseguire l'importazione in un sistema di destinazione

Questa procedura è basata sul presupposto che siano state create copie di backup dei database della distribuzione e dei file di sistema che si intende utilizzare nel sistema di destinazione. Tutti i file di backup devono provenire dallo stesso set di backup. Saranno inoltre necessarie le informazioni (ad

esempio chiave cluster e credenziali per il database) annotate durante la procedura “Per eseguire l'esportazione da un sistema di origine”.

Se il sistema di destinazione risiederà in un percorso di rete con accesso alle risorse del sistema di origine, è necessario assicurarsi che il sistema di destinazione non provi ad accedere a tali risorse fino a quando non sarà stato riconfigurato. A tale scopo, inserire un firewall tra il sistema di destinazione e le risorse del sistema di origine oppure lasciare spento il sistema di origine durante l'avvio del sistema di destinazione. Dopo il primo avvio del sistema di destinazione è possibile rimuovere il firewall o avviare il sistema di origine.

Se nel sistema di origine è già installata la piattaforma BI, assicurarsi che la versione, il pacchetto di supporto e il livello patch di questa siano gli stessi del sistema di origine al momento della creazione della copia. Verificare inoltre che il percorso di installazione del sistema di destinazione sia lo stesso del sistema di origine.

1. Nel sistema di destinazione creare le connessioni al database o ai database in cui si desidera installare il repository CMS e i database di controllo e di creazione report.

Nota:

le connessioni possono fare riferimento a database diversi, ma devono avere lo stesso nome o DSN e utilizzare le stesse credenziali del sistema di origine.

2. Utilizzare gli strumenti per i database per ripristinare il database di sistema CMS e il database di controllo (se necessario) dal backup del sistema di origine nel database di destinazione.

Se per gli universi o i report del sistema di destinazione è necessario utilizzare un database di creazione report diverso, modificare la connessione in modo che faccia riferimento a tale database.

Per ulteriori istruzioni su questo passaggio, consultare l'argomento [Ripristino del sistema](#).

3. Se la piattaforma BI è installata nel sistema host di destinazione, andare al passaggio 4. Se la piattaforma BI non è installata, installarla nel sistema host di destinazione tenendo conto di quanto segue:
 - a. Installare la stessa versione di programma, lo stesso pacchetto di supporto e lo stesso livello patch del sistema di origine.
 - b. Utilizzare lo stesso percorso di installazione del sistema di origine.
 - c. Selezionare gli stessi componenti installati nel sistema di origine.
 - d. Quando il programma di installazione richiede di creare il database CMS (e il database di controllo, se applicabile), scegliere l'opzione **Utilizza un database esistente** e immettere il nome della connessione e le credenziali impostate nel passaggio 1.

Nota:

non scegliere di reinizializzare il database CMS.

- e. Quando viene richiesto il **Nome nodo**, utilizzare gli stessi nomi, gli stessi numeri di porta, la stessa password dell'amministratore e la stessa chiave cluster del sistema di origine.

Per le istruzioni di installazione complete, consultare il *Manuale di installazione della piattaforma SAP BusinessObjects Business Intelligence*. Al termine dell'installazione, andare al passaggio 6.

Nota:

se non si desidera copiare i dati di controllo dal sistema di origine, è possibile creare un nuovo database di controllo configurando questa funzione durante la procedura di installazione.

- f. Arrestare tutti i nodi della console CCM.
4. Se la piattaforma BI è già installata nel sistema di destinazione, arrestare tutti i nodi della console CCM. Nel computer host CMS del sistema di destinazione avviare CCM.
5. Se la piattaforma BI è già installata, aggiungere un nuovo nodo utilizzando l'opzione **Ricrea nodo**.
 - a. Utilizzare **Nome nodo** e **Porta SIA** del sistema di origine.
 - b. Scegliere **Avvia un nuovo CMS temporaneo**.
 - c. Selezionare un nuovo **Numero porta CMS** (una qualsiasi porta libera) e un nuovo **Tipo di database CMS** (corrispondente al tipo di database ripristinato).
 - d. Immettere i dettagli per la connessione al database CMS ripristinato nel passaggio 1.
 - e. Immettere la chiave cluster del sistema di origine.
 - f. Immettere la password dell'amministratore del sistema di origine.
6. Ripristinare gli archivi file FRS di input e output nell'archivio file del sistema di destinazione. Utilizzare la stessa cartella del sistema di origine.
7. Ripristinare la cartella del database di monitoraggio (se si desidera copiare le informazioni di monitoraggio) nella stessa cartella del sistema di origine.
8. Ripristinare la cartella del database LCM (se si desidera copiare le informazioni LCM) nella stessa cartella del sistema di origine.
9. Ripristinare i file di Subversion di LCM (se si desidera copiare le informazioni LCM) nella stessa cartella del sistema di origine.
10. Ripristinare i file del server di configurazione del livello semantico/della connessione nella stessa cartella del sistema di origine.
11. Riavviare i computer host del sistema di destinazione.
12. Se la piattaforma BI è stata installata nel sistema di destinazione durante il passaggio 3, applicare eventuali pacchetti di supporto o patch necessarie per ottenere la corrispondenza con il sistema di origine.
13. Se il sistema di destinazione viene eseguito in più computer host, ripetere i passaggi 1–11 per ciascun computer.

Per l'installazione di ulteriori nodi della piattaforma BI, utilizzare l'opzione Espandi. Tenere presente che per i nodi aggiuntivi del sistema di destinazione è necessario utilizzare gli stessi nomi utilizzati nel sistema di origine.
14. Se il database CMS del sistema di destinazione deve essere di tipo diverso rispetto al sistema di origine, utilizzare CCM per eseguire [Copia dei dati da un database di sistema CMS a un altro](#), specificando come destinazione il database che si desidera utilizzare per la copia.
15. Ripristinare i file personalizzabili dall'utente di cui è stato eseguito il backup al passaggio 3 della procedura "Per eseguire l'esportazione da un sistema di origine".
16. Ripristinare i file a livello Web di cui è stato eseguito il backup al passaggio 4 della procedura "Per eseguire l'esportazione da un sistema di origine".

Il termine "livello Web" si riferisce all'area di gestione temporanea WDeploy nella quale è possibile eseguire le personalizzazioni e al contenuto a livello Web distribuito nel server di applicazioni.

Quando si apportano modifiche al sistema di destinazione, non applicarle alla directory del server di applicazioni ma all'area di gestione temporanea WDeploy e quindi ridistribuire il livello Web nel server di applicazioni mediante WDeploy.

L'area di gestione temporanea WDeploy corrisponde a questo percorso di Windows: *DIRINSTALL/SAP BusinessObjects Enterprise XI 4.0/warfiles*.

17. Ripristinare le estensioni di cui è stato eseguito il backup al passaggio 5 della procedura "Per eseguire l'esportazione da un sistema di origine".

Dopo avere eseguito la copia di sistema della piattaforma BI:

1. Durante l'installazione del primo nodo nella destinazione viene creato un CMS temporaneo, che verrà arrestato al termine dell'installazione. Utilizzando la console CMC, passare alla pagina Server ed eliminare questo CMS.

Promemoria:

se non si rimuove il sistema di origine o lo si utilizza simultaneamente al sistema di destinazione, si consiglia di rinominare il cluster nel sistema di destinazione.

2. Eseguire lo strumento di diagnostica del repository sul database CMS di destinazione.
3. Se applicabile, configurare il Single Sign-On (SSO) di Windows AD nel sistema di destinazione. Vedere [Single Sign On alla piattaforma BI con autenticazione AD](#).
4. Se applicabile, configurare SLD nel sistema di destinazione. Per informazioni dettagliate, vedere la nota SAP 1508421: "SAP SLD Data Supplier for Apache Tomcat".
5. Eseguire un test di integrità funzionale sul sistema di destinazione.
6. Eseguire una rigenerazione completa dell'indice di ricerca.

Gestione delle versioni

15.1 Gestione di diverse versioni delle risorse BI

L'applicazione Promotion Management consente di gestire versioni diverse delle risorse BI presenti nel repository della piattaforma BI. Per favorire l'esecuzione di questa funzionalità, lo strumento include i sistemi di controllo delle versioni SubVersion e ClearCase.


Per gestire versioni differenti di processi o infoobject, completare la procedura seguente:

1. Accedere alla CMC (Central Management Console) e selezionare **Gestione delle versioni**.
2. Dal pannello sinistro della finestra "Gestione delle versioni" selezionare la cartella per visualizzare il processo o gli infoobject di cui si desidera gestire le versioni.
3. Selezionare gli infoobject e fare clic su **Aggiungi a gestione versioni**.

Nota:

se si fa clic su "Aggiungi a gestione versioni" viene creata una versione di base dell'oggetto nel repository VMS (Sistema di gestione delle versioni). È necessaria una versione di base per le successive archiviazioni.

4. Alle successive modifiche del documento e delle versioni incrementali del documento modificato, fare clic su **Archivia**. In questo modo verrà aggiornato il documento esistente nel repository VMS. Viene visualizzata la finestra di dialogo "Commenti di archiviazione".
5. Immettere i commenti e fare clic su **OK**.
La modifica nel numero di versione dell'infoobject selezionato viene visualizzata nelle colonne Sistema di gestione delle versioni e Sistema di gestione del contenuto.
6. Per ottenere la versione più recente di un documento dal VMS, selezionare l'infoobject richiesto e fare clic su **Ottieni versione più recente**.
L'ultima versione dal repository VMS viene importata nel CMS (Central Management System).
7. Per creare una copia della versione più recente, fare clic su **Crea copia**.
Viene creata una copia della versione selezionata nel repository VMS.
8. Selezionare **Cronologia** per visualizzare tutte le versioni disponibili per l'infoobject selezionato. Viene visualizzata la finestra "Cronologia". Vengono visualizzate le seguenti opzioni:
 - **Ottieni versione**: se sono presenti più versioni della risorsa BI ed è necessario utilizzarne una particolare, è possibile selezionare l'infoobject necessario e fare clic su **Ottieni versione**.
 - **Ottieni copia della versione**: questa opzione consente di ottenere una copia della versione selezionata.

- **Esporta copia della versione:** questa opzione consente di ottenere una copia della versione selezionata e di salvarla nel sistema locale.
 - **Confronta:** questa opzione consente di confrontare le informazioni dei metadati delle due versioni di un processo. Per ulteriori informazioni, vedere “Confronto tra versioni diverse dello stesso processo”.
9. Selezionare un infoobject e fare clic su **Blocca** per bloccare l'infoobject, o su **Sblocca** per sbloccare l'infoobject, o su **Elimina** per eliminare tutte le versioni di contenuto dal repository VMS. Il contenuto del CMS rimane intatto.
- Nota:**
se si blocca un infoobject, non è possibile eseguire alcuna azione su tale infoobject.
10. Quando la versione presente nel CMS è più recente di quella presente nel sistema di gestione delle versioni accanto all'infoobject aggiornato viene visualizzato un indicatore. Posizionando il cursore sull'indicatore viene visualizzata una descrizione che informa che l'infoobject nel CMS è stato aggiornato.
11. Per visualizzare l'elenco di tutte le risorse archiviate presenti nel VMS ma non nel CMS, fare clic su **Visualizza risorse eliminate**.
Fare clic su una qualsiasi risorsa eliminata per visualizzarne la relativa cronologia. È possibile selezionare una risorsa eliminata e fare clic su **Ottieni versione** per visualizzare quella specifica versione della risorsa. È possibile fare clic su **Ottieni copia della versione** per ottenere una copia della risorsa selezionata.
Fare clic su **Elimina** per rimuovere definitivamente dal repository VMS anche l'oggetto.
- Nota:**
se si utilizza **Ottieni versione** o **Ottieni copia della versione**, la risorsa viene spostata dall'elenco dei file mancanti del VMS al CMS.
12. Selezionare un infoobject e fare clic su  per visualizzare le proprietà dell'infoobject.
In alternativa, è possibile fare clic con il pulsante destro del mouse sull'infoobject ed eseguire i passaggi da 4 a 16.

15.2 Utilizzo dell'opzione Impostazioni sistema gestione versioni

È possibile specificare le impostazioni del sistema di gestione delle versioni dalla Central Management Console. È possibile configurare i parametri SubVersion e ClearCase.

Per impostare il sistema di gestione SubVersion, attenersi alla seguente procedura:

1. Nella pagina iniziale della CMC selezionare **Applicazioni**.
2. Fare doppio clic su **VMS**. Viene visualizzata la schermata Impostazione di gestione delle versioni.
3. Selezionare **Impostazioni VMS**.
4. Dall'elenco a discesa **Sistemi di gestione delle versioni**, selezionare **SubVersion**.

Il numero di porta del server, la password il nome del repository, il nome del server, il nome utente, il nome della directory dello spazio di lavoro e quello della directory di installazione forniti durante il processo di installazione dello strumento Promotion Management vengono visualizzati nei campi appropriati.

5. Modificare i campi, se necessario.

Assicurarsi di immettere il percorso di installazione esteso fino al file `.exe`. In Windows: `DIRINSTALLAZ\SAP BusinessObjects Enterprise XI 4.0\subversion` o in Unix: `DIRINSTALLAZ/sap_bobj/enterprise_40/subversion/bin`

6. È possibile utilizzare i protocolli http oppure svn per accedere al repository Subversion facendo clic rispettivamente sui pulsanti di opzione http o svn.
7. È possibile convalidare le impostazioni del sistema di gestione delle versioni specificate facendo clic su **Test VMS**.
8. Fare clic su **Salva**.

Nota:

- Se si desidera impostare SubVersion come VMS predefinito, selezionare **Usa come sistema di gestione delle versioni predefinito**.
- Se sono stati modificati i campi come indicato al passaggio 3, riavviare il Server Intelligence Agent.

15.2.1 Impostazione del sistema di gestione delle versioni ClearCase in Windows

Per impostare il sistema di gestione delle versioni ClearCase, attenersi alla seguente procedura:

1. Nella finestra "Opzioni di amministrazione", fare clic su **Impostazioni sistema gestione versioni**.
2. Dall'elenco a discesa **Sistemi di gestione delle versioni**, selezionare **ClearCase**.
3. Immettere i dettagli seguenti:
 - Unità mappa ClearCase: immettere il nome dell'unità. Per impostazione predefinita, corrisponde all'unità M. Ad esempio: M:
 - Nome tag VOB: immettere il nome VOB (Versioned Object Base). Ad esempio: FridayVB
 - Visualizza directory di archiviazione: immettere il percorso alla cartella condivisa. Ad esempio: \\HostName\FolderName

Nota:

Il nome host non deve essere scritto come localhost.

4. Fare clic su **Salva**.

15.2.2 Impostazione del sistema di gestione delle versioni ClearCase in Unix

Per impostare il sistema di gestione delle versioni ClearCase in Unix, attenersi alla seguente procedura:

1. Nella finestra Opzioni di amministrazione, fare clic su **Impostazioni sistema gestione versioni**.
2. Dall'elenco a discesa Sistemi di gestione delle versioni, selezionare **ClearCase**.
3. Immettere i dettagli seguenti:
 - Unità mappa ClearCase: immettere il nome della cartella in cui si trova MVFS. Per impostazione predefinita, è /view
 - Nome tag VOB: immettere il nome VOB e la cartella in cui si trova il VOB. Ad esempio: CartellaVob/NomeVob
 - Visualizza directory di archiviazione: immettere il percorso alla directory in cui vengono create le viste.

È possibile selezionare **Usa come sistema di gestione delle versioni predefinito** se si desidera utilizzare ClearCase come sistema di gestione delle versioni predefinito.

15.3 Confronto tra versioni diverse dello stesso processo

È possibile visualizzare le differenze tra due versioni dello stesso processo attenendosi alla procedura indicata di seguito.

1. Accedere all'applicazione CMC.
2. Nella pagina iniziale della CMC selezionare **Gestione delle versioni**.
3. Nella schermata Gestione delle versioni selezionare l'infoobject di cui si desidera confrontare le versioni.
4. Fare clic su **Cronologia**.
Viene visualizzata la pagina Cronologia, in cui sono presenti tutte le versioni dell'infoobject selezionato.
5. Selezionare due versioni da confrontare.
6. Fare clic su **Confronta**.
Il processo di confronto viene avviato e le differenze vengono evidenziate in arancione, mentre gli oggetti mancanti vengono evidenziati in rosso.
7. Fare clic su **Salva** per salvare il report sulle differenze.

15.4 Aggiornamento del contenuto di Subversion

È possibile aggiornare eventuale contenuto di Subversion meno recente che è stato creato con una versione precedente della piattaforma BI alla versione più recente attenendosi alla procedura indicata di seguito.

1. Accedere al VMS nel computer in cui è installato SAP BusinessObjects Platform Enterprise 3.x.

2. Archiviare gli oggetti. Ad esempio archiviare due volte gli oggetti amministratore e guest.
3. Nella CMC fare clic su **Utenti** e verificare che 2 sia visualizzato nel numero di versione di VMS e CMS.
4. Disconnettersi da VMS.
5. Accedere al prompt dei comandi, passare alla cartella `C:\Programmi\Subversion\bin` ed eseguire il comando di esportazione: `svnadmin dump c:/LCM_repository/svn_repository > dumrepo`.
6. Copiare il file `dumrepo` nel computer in cui è installata la piattaforma BI.
7. Accedere al prompt dei comandi nel computer con la piattaforma BI, passare alla cartella `C:\Programmi (x)\SAP` ed eseguire i comandi indicati di seguito.

```
svnadmin.exe load "C:/Programmi (x86)/SAP BusinessObjects/SAPBusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository" < c:/dumrepo  
svnadmin.exe upgrade "C:/Programmi (x86)/SAP BusinessObjects/SAP BusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository"
```
8. Dopo la corretta esecuzione dei comandi, riavviare il SIA.
9. Accedere alla console CMC e fare clic su **Gestione delle versioni**.
10. Fare clic su **Utenti** e verificare che la versione del VMS sia 2.
11. Selezionare l'oggetto **Amministratore**, quindi fare clic su **Ottieni versione più recente**.
12. I numeri di versione di VMS e CMS ora corrispondono.

Promotion Management

16.1 Promotion Management

16.1.1 Panoramica

L'applicazione Promotion Management consente di spostare le risorse di Business Intelligence (BI) da un repository a un altro, di gestire le dipendenze delle risorse e, se necessario, anche di eseguire il rollback delle risorse promosse nel sistema di destinazione. L'applicazione supporta anche la gestione di diverse versioni della stessa risorsa di BI.

L'applicazione Promotion Management è integrata con la Central Management Console. È possibile promuovere una risorsa BI da un sistema a un altro solo se la stessa versione della piattaforma BI è installata sia nel sistema di origine che nel sistema di destinazione.

16.1.2 Funzionalità

L'applicazione gestione promozioni supporta le funzionalità seguenti:

- **Promozione:** questa funzionalità consente di creare o aggiornare infoobject nel sistema di destinazione. Oltre alla promozione di infoobject, questa funzionalità consente di effettuare le seguenti attività:
 - Creare un nuovo processo
 - Copiare da un processo esistente
 - Modificare un processo
 - Pianificare la promozione di un processo
 - Visualizzare la cronologia di un processo
 - Esporta come LCMBIAR
 - Importare sia BIAR sia LCMBIAR
- **Gestisci dipendenze:** questa funzionalità consente di selezionare, filtrare e gestire gli oggetti dipendenti degli infoobject presenti nel processo che si desidera promuovere.

- Pianificazione: questa funzionalità consente di specificare un'ora per la promozione di un processo, anziché promuoverlo non appena creato. Per pianificare la promozione del processo è possibile utilizzare uno qualsiasi dei seguenti parametri: Ogni ora, Ogni giorno, Ogni settimana o Ogni mese.
- Protezione: questa funzionalità consente di promuovere infoobject insieme ai diritti di protezione associati e, se necessario, di promuovere infoobject associati a diritti applicazione.
- Prova promozione: questa funzionalità consente di controllare o provare la promozione per verificare che tutte le misure preventive siano state prese prima di eseguire l'effettiva promozione degli infoobject.
- Rollback: questa funzionalità consente di ripristinare il sistema di destinazione allo stato precedente, dopo la promozione di un processo. È possibile effettuare il rollback di un intero processo o di parte di esso.
- Controllo: gli eventi generati dallo strumento Promotion Management vengono memorizzati nel database di controllo. Questa funzionalità consente di monitorare gli eventi registrati nel database di controllo.
- Impostazioni di sostituzione LCM: questa funzionalità consente di analizzare e promuovere le sostituzioni mediante la promozione di un processo.

16.1.3 Diritti di accesso per l'applicazione

In questa sezione vengono descritti i diritti di accesso relativi all'applicazione Promotion Management.

- È possibile impostare i diritti di accesso per l'applicazione Promotion Management nella CMC.
- Si possono impostare diritti granulari di applicazione per diverse funzioni all'interno dell'applicazione Promotion Management.

Per impostare diritti specifici nell'applicazione Promotion Management, attenersi alla procedura illustrata di seguito.

1. Accedere alla console CMC e selezionare **Applicazioni**.
2. Fare doppio clic su **Promotion Management**.
3. Fare clic su **Protezione utente** e selezionare un utente. È possibile visualizzare o assegnare diritti di protezione per l'utente.
4. Sono disponibili i diritti specifici di Promotion Management indicati di seguito.
 - Consentire l'accesso per modificare le sostituzioni
 - Consenti accesso per includere protezione
 - Consenti accesso ad amministrazione LCM
 - Consenti accesso per gestire dipendenze
 - Crea processo
 - Elimina processo
 - Modifica processo
 - Modifica LCMBIAR
 - Esporta come LCMBIAR
 - Importa LCMBIAR
 - Promuovi processo

- Processo di rollback
 - Visualizza e seleziona oggetti BOMM (BusinessObjects Metadata)
 - Visualizza e seleziona viste aziendali
 - Visualizza e seleziona calendari
 - Visualizza e seleziona connessioni
 - Visualizza e seleziona profili
 - Visualizza e seleziona QaaWS
 - Visualizza e seleziona oggetti report
 - Visualizzazione e selezione di impostazioni di protezione
 - Visualizzazione e selezione di universi
5. Se si desidera assegnare diritti a un utente selezionato, selezionare il diritto appropriato e fare clic su **Assegna protezione**.

I diritti di accesso per l'applicazione Promotion Management sono ora impostati all'interno della CMC.

16.1.4 Supporto di WinAD in Promotion Management

Per consentire il funzionamento corretto dell'applicazione Promotion Management, è necessario aggiungere quanto segue a tutti gli argomenti `javaargs` per tutti gli Adaptive Job Server:

```
Djava.security.auth.login.config=<path>\bsclogin.conf,Djava.security.krb5.conf=<path>\krb5.ini
```

Promemoria:

Specificare il percorso corretto per `bsclogin.conf` e `krb5.ini` nella distribuzione.

16.2 Introduzione allo strumento Promotion Management

16.2.1 Accesso all'applicazione Promotion Management

Per accedere all'applicazione Promotion Management, selezionare **Promotion Management** dalla pagina iniziale della CMC (Central Management Console).

qualsiasi utente con autorizzazioni di visualizzazione alla cartella **Processi di promozione** può avviare l'applicazione Promotion Management. Tuttavia, per creare, pianificare o promuovere un processo è necessario disporre di diritti aggiuntivi assegnati dall'amministratore.







16.2.2 Componenti dell'interfaccia utente


In questo capitolo vengono descritti i componenti GUI dello strumento Promotion Management.

- Barra degli strumenti dello spazio di lavoro di Promotion Management
- Pannello dello spazio di lavoro
- Pannello struttura
- Pannello Dettagli
- Pagina Carrello degli acquisti e Visualizzatore processi

Barra degli strumenti dello spazio di lavoro di Promotion Management

Nella tabella seguente sono elencate le opzioni presenti nella barra degli strumenti dello spazio di lavoro di Promotion Management e vengono esaminate le attività che è possibile eseguire utilizzando tali opzioni:

Opzione	Descrizione
	Consente di creare una nuova cartella. La nuova cartella viene creata come sottocartella nella cartella Processi di promozione .
	Consente di copiare e rimuovere il processo o la cartella selezionati dal percorso corrente.
	Consente di copiare il processo o la cartella dal percorso corrente.
	Consente di incollare il processo o la cartella copiati in un nuovo percorso.
	Consente di eliminare un processo esistente.
	Consente di aggiornare la pagina iniziale, per ottenere l'elenco aggiornato dei processi o delle cartelle disponibili per la promozione.
Proprietà	Consente di modificare le proprietà del processo selezionato. È possibile modificare titolo, descrizione e parole chiave del processo selezionato.
Cronologia	Consente di visualizzare la cronologia del processo selezionato.
Nuovo processo	Consente di creare un nuovo processo.
Importa	Consente di importare file BIAR o Override.

Opzione	Descrizione
Modifica	Consente di modificare il processo selezionato.
Promuovi	Consente di promuovere il processo selezionato.
Rollback	Consente di recuperare il processo promosso dal sistema di destinazione.
	Consente di spostarsi tra le pagine di un elenco di processi. È possibile utilizzare questa opzione per spostarsi all'interno di una singola pagina o per passare a una pagina specifica immettendone il numero.
Ricerca	Consente di ricercare processi specifici. È possibile ricercare un processo in base al nome, alle parole chiave, alla descrizione o a tutti e tre i parametri.
Processi di promozione	Consente di visualizzare i processi promossi.
Stato promozione	Visualizza i processi promossi in base allo stato, ad esempio Operazione riuscita, Operazione non riuscita o Operazione parzialmente riuscita.

Pannello Spazio di lavoro

Il pannello Spazio di lavoro della pagina iniziale di Promotion Management riporta l'elenco dei nuovi processi creati. È possibile utilizzare il pannello per visualizzare il nome del processo, lo stato del processo, le informazioni di creazione del processo, il riepilogo della promozione, il riepilogo della verifica della promozione, le schermate per la gestione delle dipendenze e le informazioni relative al sistema di destinazione.

Pannello struttura

Nel pannello struttura della pagina iniziale di Promotion Management viene visualizzata la struttura ad albero, che contiene le cartelle **Processo di promozione** e **Stato promozione**. I nuovi processi creati vengono visualizzati in una struttura gerarchica sotto la cartella **Processi di promozione**. La cartella **Stato promozione** riporta i processi promossi in base allo stato.

Pannello Dettagli

Il pannello include inoltre il collegamento **Preferenze** che consente all'amministratore e agli utenti di impostare le preferenze dello strumento. I collegamenti **?** e **Informazioni su** consentono di ottenere ulteriori informazioni sull'utilizzo dello strumento Promotion Management.

Pagina Carrello degli acquisti e Visualizzatore processi

Un carrello degli acquisti è una struttura ad albero dinamicamente generata che contiene un elenco di infoobject da promuovere classificati in gruppi utenti, universi, connessioni e così via. La pagina Visualizzatore processi consente di visualizzare gli infoobject aggiunti a un processo.

16.2.3 Utilizzo delle opzioni di impostazione

L'opzione Impostazioni consente di configurare le impostazioni prima di promuovere gli infoobject da una distribuzione della piattaforma BI a un'altra distribuzione della piattaforma BI e un'altra distribuzione SAP. In questa sezione viene spiegato come utilizzare le opzioni di impostazione.

Fare clic sul menu a discesa **Impostazioni** della schermata "Processi di promozione". In questo menu a discesa sono presenti le opzioni di seguito:

- **Gestisci sistemi:** questa opzione consente di aggiungere tutti i sistemi necessari per le attività di Promotion Management.
- **Impostazioni rollback:** questa opzione consente di selezionare un sistema per il quale è abilitato il rollback.
- **Impostazioni processo:** questa opzione consente di selezionare la visualizzazione di istanze completate nella pagina Dipendenze. Consente inoltre di gestire le attività di pulizia delle istanze di processo.
- **Impostazioni CTS:** questa opzione consente di aggiungere il servizio Web e le informazioni di sistema di SAP BW per l'integrazione di Enhanced Change Transport System.
- **Impostazioni di sostituzione LCM:** questa opzione consente di analizzare, promuovere e modificare le informazioni di connessione al database per le connessioni di Crystal Reports e dell'universo. Qui è anche possibile modificare URL QAAWA.

16.2.3.1 Per utilizzare l'opzione Gestisci sistemi

In questa sezione viene descritto come utilizzare l'opzione Gestisci sistemi. Questa opzione consente di aggiungere o rimuovere sistemi host.

Per aggiungere un sistema host, attenersi alla seguente procedura:

1. Nella finestra "Opzioni di amministrazione" fare clic sull'opzione **Gestisci sistemi**.

Viene visualizzata la finestra "Gestisci sistemi" con gli elenchi dei nomi host, dei numeri di porta, dei nomi visualizzati e delle relative descrizioni.

2. Fare clic su **Aggiungi**.

Viene visualizzata la finestra di dialogo "Aggiungi sistema".

3. Aggiungere il nome host, il numero di porta, il nome visualizzato e la descrizione nei campi appropriati.

Nota:

selezionare l'opzione **Contrassegna come 'Origine'** per identificare il sistema come sistema di origine, ovvero come il sistema da cui hanno origine le informazioni di connessione.

4. Fare clic su **OK** per aggiungere il sistema.

Il sistema host viene aggiunto all'elenco.

Nota:

per rimuovere un sistema host, selezionarlo e fare clic su **Rimuovi**.

Argomenti correlati

- [Per utilizzare l'opzione Impostazioni rollback](#)
- [Per utilizzare l'opzione Impostazioni processo](#)

16.2.3.2 Per utilizzare l'opzione Impostazioni rollback

Per impostazione predefinita, il processo di rollback viene abilitato a livello di sistema. L'opzione **Impostazioni rollback** consente di disabilitare il processo di rollback a livello di sistema.

Per disabilitare il processo di rollback a livello di sistema, attenersi alla procedura seguente:

1. Nella finestra "Rollback", dall'elenco di sistemi host, selezionare il sistema host per disabilitare il processo di rollback.
2. Fare clic su **Salva e chiudi** per salvare le modifiche.

Argomenti correlati

- [Per utilizzare l'opzione Impostazioni processo](#)

16.2.3.3 Per utilizzare l'opzione Impostazioni processo

L'opzione Impostazioni processo consente di specificare il numero di istanze processo che possono esistere nel sistema. È possibile specificare una delle seguenti opzioni:

- Elimina istanze processo quando sono presenti più di N istanze di un processo: questa opzione consente di specificare il numero massimo di istanze per processo che possono esistere nel sistema.
- Eliminare le istanze per il processo dopo N giorni: questa opzione consente di specificare che tutte le istanze di processo create prima del numero di giorni indicato devono essere eliminate.
- Dall'elenco a discesa **Mostra processi creati** selezionare l'intervallo di tempo per visualizzare i processi creati durante un periodo specifico.

Per impostare l'opzione **Impostazioni processo**, attenersi alla seguente procedura:

1. Selezionare l'opzione e immettere il valore preferito.
2. Fare clic su **Salva** per salvare le modifica aggiornate.

È possibile fare clic su **Impostazioni predefinite** per impostare i valori predefiniti e su **Chiudi** per chiudere la finestra.

Nota:

le vecchie istanze processo vengono eliminate solo alla successiva esecuzione del processo.

Argomenti correlati

- [Utilizzo dell'opzione Impostazioni sistema gestione versioni](#)

16.2.3.4 Utilizzo dell'opzione Impostazioni di sostituzione LCM

L'opzione Impostazioni di sostituzione LCM consente di promuovere le sostituzioni in una promozione di processi oppure in file BIAR.

Nota:

- nelle procedure seguenti verrà utilizzato il termine "sistema". Esistono tre tipi di sistema:
 - Origine: è il sistema di origine per tutte le informazioni di connessione.
 - LCM centrale: è il sistema al quale si è connessi per impostazione predefinita.
 - Destinazione: è il sistema finale sul quale sono state promosse le risorse BI.
- Nella versione 4.0 SP4 della piattaforma BI i dati di sostituzione sono archiviati in un database centralizzato locale creato nel computer su cui è in esecuzione il servizio PJS. Per evitare che vengano immessi dati duplicati e dati di sostituzione non coerenti derivanti dalla manutenzione di più database, è possibile impostare un'unica posizione per la sostituzione di tutti i server PJS. Nella CMC, nella pagina "Applicazioni" fare clic con il pulsante destro del mouse su "Promotion Management" e scegliere Impostazioni di sostituzione LCM. Quando viene visualizzato un elenco di tutti i server PJS che ospitano il servizio LCM, verificare che tutte le directory puntino alla stessa posizione.

16.2.3.4.1 Per promuovere le sostituzioni

Aggiungere un sistema host prima di promuovere le sostituzioni. Per informazioni sull'aggiunta di oggetti esistenti, consultare [Per utilizzare l'opzione Gestisci sistemi](#).

Per promuovere le sostituzioni, attenersi alla procedura seguente:

1. Nella finestra "Opzioni di amministrazione" fare clic sull'opzione **Impostazioni di sostituzione**. Viene visualizzata la finestra "Impostazioni di sostituzione".
2. Se è stato eseguito l'accesso al sistema centrale di gestione delle promozioni, disconnettersi.
3. Fare clic su **Accedi** per connettersi al sistema di origine. Viene visualizzata la finestra "Accedi al sistema".
4. Selezionare il sistema di origine contrassegnato come **Origine** in modo da analizzare gli oggetti e accedere al sistema utilizzando credenziali valide.

5. Nell'elenco a discesa **Avvia**, accanto a **Esamina**, selezionare l'opzione **Avvia**.
Viene avviato il processo di scansione. Viene visualizzato l'"elenco delle connessioni univoche".

Nota:

per pianificare la scansione in base alle proprie preferenze, selezionare l'opzione **Impostazioni di ricorrenza** nell'elenco a discesa.

6. Nell'elenco di sostituzioni modificare lo stato in Attivo per gli oggetti da promuovere e fare clic su **Salva**.
 7. Fare clic su **Promuovi sostituzioni**.
Viene visualizzata la schermata "Promuovi sostituzioni" con l'elenco dei sistemi di destinazione.
 8. Fare clic su **Accedi** per accedere al sistema di destinazione utilizzando credenziali valide.
È possibile specificare più sistemi di destinazione.
 9. Fare clic su **Promuovi**.
La promozione delle sostituzioni è completa.
- Nota:**
se le sostituzioni non riescono nel sistema di destinazione durante la promozione degli infoobject, il sistema imposta lo stato del processo su "Operazione parzialmente riuscita" e imposta anche lo stato di avviso "Overrides Failed" sull'oggetto.
10. Disconnettersi dal sistema di origine.
 11. Dalla schermata "Impostazioni di sostituzione" fare clic su **Accedi**.
Viene visualizzata la finestra Accedi al sistema.
 12. Accedere a uno dei sistemi di destinazione utilizzando credenziali valide.
In "Elenco di sostituzioni" viene visualizzato un elenco con tutti gli oggetti promossi. Lo stato di questi oggetti è Inattivo.
 13. Fare clic sulla casella di controllo **Seleziona** per gli oggetti da modificare e quindi su **Modifica**.
 14. Aggiornare i valori richiesti e fare clic su **Fine**.
 15. Modificare lo stato degli oggetti in Attivo e fare clic su **Salva**.

16.2.3.4.2 Per promuovere le sostituzioni utilizzando i file BIAR

Aggiungere un sistema host prima di promuovere le sostituzioni. Per informazioni sull'aggiunta di oggetti esistenti, consultare [Per utilizzare l'opzione Gestisci sistemi](#).

Per promuovere le sostituzioni mediante i file BIAR, attenersi alla procedura seguente:

1. Nella finestra "Opzioni di amministrazione" fare clic sull'opzione **Impostazioni di sostituzione**.
Viene visualizzata la finestra "Impostazioni di sostituzione".
2. Se è stato eseguito l'accesso al sistema LCM centrale, disconnettersi.
3. Fare clic su **Accedi** per connettersi al sistema di origine.
Viene visualizzata la finestra "Accedi al sistema".
4. Nella schermata "Impostazioni di sostituzione" selezionare il sistema di origine contrassegnato come **Origine** in modo da analizzare gli oggetti e accedere al sistema utilizzando credenziali valide.

5. Dall'elenco a discesa **Avvia** accanto ad **Esamina** selezionare l'opzione **Avvia**.
Il processo di analisi viene avviato e viene visualizzato l'Elenco di sostituzioni.

Nota:

per pianificare la scansione in base alle proprie preferenze, selezionare l'opzione **Impostazioni di ricorrenza** nell'elenco a discesa.

6. Nell'elenco di sostituzioni modificare lo stato degli oggetti appropriati in Attivo e fare clic su **Salva**.
7. Fare clic su **Promuovi sostituzioni**.
Viene visualizzata la schermata "Promuovi sostituzioni" con l'elenco dei sistemi di destinazione.
8. Per crittografare il file BIAR utilizzando una password, fare clic sulla casella di controllo **Crittografia password**.
I campi **Password** e **Conferma password** vengono abilitati.
9. Immettere una password nel campo **Password**. Reimmettere la stessa password nel campo **Conferma password**.
10. Fare clic su **Esporta** e salvare il file BIAR delle sostituzioni in un file system.
11. Accedere al sistema di destinazione mediante lo strumento LCM e fare clic su **Importa > Ignora file**.
Viene visualizzata la finestra di dialogo "Importa file LCMBIAR".
12. Fare clic su **Sfoglia** per individuare il file BIAR.
13. Immettere la password del file BIAR nel campo **Password**.

Nota:

il campo **Password** viene visualizzato solo se il file BIAR selezionato viene crittografato utilizzando una password.

14. Fare clic su **OK**. La promozione delle sostituzioni è completa.
15. Disconnettersi dal sistema di origine.
16. Dalla schermata "Impostazioni di sostituzione" fare clic su **Accedi**.
Viene visualizzata la finestra "Accedi al sistema".
17. Accedere al sistema di destinazione utilizzando credenziali valide.
Nell'Elenco di sostituzioni viene visualizzato un elenco di oggetti importati con lo stato Inattivo.
18. Fare clic sulla casella di controllo **Seleziona** per gli oggetti da modificare e quindi su **Modifica**. Gli oggetti modificati verranno indicati da un'icona.

Nota:

è possibile eliminare gli oggetti di sostituzione facendo clic sull'icona.

19. Aggiornare i valori richiesti e fare clic su **Fine**.
20. Modificare lo stato degli oggetti in "Attivo" e fare clic su **Salva**.

16.2.3.4.3 Per promuovere le sostituzioni utilizzando CTS+

Aggiungere un sistema host prima di promuovere le sostituzioni. Per informazioni sull'aggiunta di oggetti esistenti, consultare [Per utilizzare l'opzione Gestisci sistemi](#).

Per promuovere le sostituzioni mediante CTS+, attenersi alla procedura seguente:

Nota:

avviare lo strumento Promotion Management utilizzando l'autenticazione SAP per rendere disponibile questa opzione.

1. Nella finestra "Opzioni di amministrazione" fare clic sull'opzione **Impostazioni di sostituzione**.
Viene visualizzata la finestra "Impostazioni di sostituzione".
2. Se è stato eseguito l'accesso al sistema LCM centrale, disconnettersi.
3. Fare clic su **Accedi** per connettersi al sistema di origine.
Viene visualizzata la finestra "Accedi al sistema".
4. Selezionare il sistema di origine contrassegnato come **Origine** in modo da analizzare gli oggetti e accedere al sistema utilizzando credenziali valide.
5. Dall'elenco a discesa **Avvia** accanto ad **Esamina** selezionare l'opzione **Avvia**.
Viene avviato il processo di scansione. Viene visualizzato l'"Elenco di sostituzioni".

Nota:

per pianificare la scansione in base alle proprie preferenze, selezionare l'opzione **Impostazioni di ricorrenza** nell'elenco a discesa.

6. Nell'elenco di sostituzioni modificare lo stato in Attivo per gli oggetti da promuovere e fare clic su **Salva**.
7. Fare clic su **Promuovi sostituzioni**.
Viene visualizzata la schermata "Promuovi sostituzioni" con l'elenco dei sistemi di destinazione.
8. Nell'elenco a discesa **Opzioni di promozione** selezionare **Promuovi con CTS+**.
9. Fare clic su **Promuovi**.
10. Rilasciare le sostituzioni nel sistema di destinazione effettuando le operazioni seguenti:
 - a. Accedere al controller di dominio di CTS+ e aprire l'interfaccia utente Web di "Transport Organizer". Per ulteriori informazioni sull'interfaccia utente Web di Transport Organizer, consultare http://help.sap.com/saphelp_nw70ehp1/helpdata/en/b5/6d03660d3745938cd46d6f5f9cef2e/frameaset.htm.
 - b. Se lo stato della richiesta è **Modifiable**, fare clic su **Release** per rilasciare la richiesta di trasporto delle sostituzioni. Per ulteriori informazioni sul rilascio delle richieste di trasporto con oggetti non ABAP, vedere http://help.sap.com/saphelp_nw70ehp1/helpdata/en/55/07c497db8140ef8176715d4728eec1/frameaset.htm
 - c. Chiudere l'interfaccia utente di "Transport Organizer".
11. Importare le sostituzioni nel sistema di destinazione effettuando le operazioni seguenti:
 - a. Accedere al controller di dominio di CTS+.
 - b. Chiamare la transazione STMS per accedere al sistema di gestione dei trasporti.
 - c. Fare clic sull'icona **Panoramica importazione**.

Viene visualizzata la schermata "Panoramica importazione" nella quale è possibile visualizzare le voci della coda di importazione di tutti i sistemi.
 - d. Fare clic sull'ID del sistema LCM di destinazione.
L'utente può visualizzare l'elenco di richieste di trasporto che è possibile importare nel sistema.

- e. Fare clic su **Aggiorna**.
 - f. Importare le richieste di trasporto pertinenti. Per ulteriori informazioni consultare http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a39e7acc11d1899e0000e829fbbd/fra/meset.htm.
12. La promozione delle sostituzioni è completa.
 13. Accedere a uno dei sistemi di destinazione utilizzando credenziali valide.
In "Elenco di sostituzioni" viene visualizzato un elenco di tutti gli oggetti promossi. Lo stato di questi oggetti è Inattivo.
 14. Fare clic sulla casella di controllo **Seleziona** per gli oggetti da modificare e quindi su **Modifica**.
 15. Aggiornare i valori richiesti e fare clic su **Fine**.
 16. Modificare lo stato degli oggetti in Attivo e fare clic su **Salva**.

16.2.3.5 Utilizzo dell'opzione Impostazioni CTS

Questa opzione consente di aggiungere servizi Web e di gestire sistemi BW nell'ambiente di lavoro. Fare riferimento alla sezione [Per configurare le impostazioni CTS+ nello strumento Promotion Management](#) per ulteriori informazioni sull'utilizzo dell'opzione Impostazioni CTS e per la configurazione di CTS per l'utilizzo con l'applicazione Promotion Management.

16.3 Utilizzo dello strumento Promotion Management

All'avvio dell'applicazione Promotion Management, per impostazione predefinita si apre la pagina "Processi di promozione".

La schermata della home page "Processi di promozione" include varie schede che consentono di eseguire le seguenti attività:

- Selezionare **Nuovo processo** per selezionare i processi correlati al processo. È anche possibile fare clic con il pulsante destro del mouse sulla home page e scegliere i processi secondari correlati al processo principale dall'elenco.
- Selezionare **Importa > Importa file** per importare un file BIAR o LCMBIAR direttamente dal file system, invece di eseguire l'intera procedura di creazione di un nuovo processo.
- Selezionare **Importa > Ignora file** per importare le sostituzioni.
- Selezionare **Modifica** per modificare i processi esistenti.
- Selezionare **Promuovi** per promuovere il processo dal sistema di origine al sistema di destinazione o esportare il processo in un file BIAR.
- Selezionare **Rollback** per ripristinare i processi promossi dal sistema di destinazione.
- Selezionare **Cronologia** per visualizzare le istanze di promozione precedenti del processo.

- Selezionare **Proprietà** per visualizzare le proprietà dell'istanza del processo selezionata, quali il titolo, l'ID, il nome file, la descrizione e così via.

L'area dell'applicazione "Processi di promozione" riporta l'elenco dei processi presenti nel sistema, insieme alle seguenti informazioni per ciascun processo:

- **Nome:** visualizza il nome del processo creato.
- **Stato:** visualizza lo stato del processo, ad esempio Creato, Operazione riuscita, Operazione parzialmente riuscita, In esecuzione o Operazione non riuscita.
- **Creato:** visualizza la data e l'ora di creazione del processo.
- **Ultima esecuzione:** visualizza la data e l'ora in cui il processo è stato promosso l'ultima volta.
- **Sistema di origine:** visualizza il nome del sistema da cui viene promosso il processo.
- **Sistema di destinazione:** visualizza il nome del sistema in cui viene promosso il processo.
- **Creato da:** riporta il nome dell'utente che ha creato il processo in questione.

Nota:

L'applicazione Promotion Management si serve dell'SDK della piattaforma SAP BusinessObjects Business Intelligence per tutte le sue attività.


16.3.1 Creazione ed eliminazione di cartelle

In questa sezione viene descritto come creare ed eliminare una cartella nella home page dei processi di promozione.

16.3.1.1 Per creare una cartella

In questa sezione viene descritto come creare una cartella.

Per creare una cartella, attenersi alla seguente procedura:

1. Nella barra degli strumenti di Promotion Management, fare clic su .
2. Nella finestra di dialogo "Crea cartella" immettere il nome della cartella.
3. Fare clic su **OK**.

Viene creata una nuova cartella.


Argomenti correlati

- [Per creare un processo](#)
- [Per eliminare una cartella](#)

16.3.1.2 Per eliminare una cartella

In questa sezione viene descritto come eliminare una cartella.

Per eliminare una cartella, attenersi alla seguente procedura:

1. Selezionare una cartella o un processo nella home page "Processi di promozione".
2. Fare clic su .

Viene visualizzata la finestra di dialogo "Elimina".

3. Scegliere **OK**.

La cartella selezionata viene eliminata.

Argomenti correlati

- [Per creare un processo](#)

16.3.2 Per creare un processo

In questa sezione viene descritto come creare un nuovo processo utilizzando lo strumento Promotion Management.

Nella seguente tabella vengono descritti gli elementi GUI e i campi utilizzabili per creare un nuovo processo:

Campo	Descrizione
Nome	Nome del processo che si desidera creare.
Descrizione	Descrizione del processo che si desidera creare.
Parole chiave	Parole chiave per il contenuto del processo che si desidera creare.
Salva processo in	Viene visualizzata la cartella selezionata predefinita.
Sistema di origine	Il nome del sistema della piattaforma BI da cui si desidera promuovere un processo.
Sistema di destinazione	Il nome del sistema della piattaforma BI a cui si desidera promuovere un processo.

Campo	Descrizione
Nome utente	ID di accesso che è necessario utilizzare per accedere al sistema di origine o di destinazione.
Password	Password che è necessario utilizzare per accedere al sistema di origine o di destinazione.
Autenticazione	<p>Tipo di autenticazione utilizzato per accedere al sistema di origine o di destinazione.</p> <p>Lo strumento Promotion Management supporta i seguenti tipi di autenticazione:</p> <ul style="list-style-type: none"> • Enterprise • Windows AD • LDAP • SAP

Nota:

prima di creare un processo, assicurarsi che le sostituzioni, se presenti, siano state modificate e aggiornate nel sistema di destinazione, cosicché il contenuto della piattaforma BI venga aggiornato automaticamente. Per ulteriori informazioni vedere Utilizzo dell'opzione Impostazioni di sostituzione.

Per creare un nuovo processo utilizzando Promotion Management, completare la procedura seguente:

1. Avviare lo strumento Promotion Management.
2. Nella home page "Processi di promozione" fare clic sulla scheda **Nuovo processo**.
3. Immettere nome, descrizione e parole chiave del processo nei campi appropriati.

Nota:

l'inserimento di informazioni nei campi Descrizione, Parole chiave e Sistema di destinazione è facoltativo.

4. Nel campo **Salva processo in** individuare la cartella in cui si desidera salvare il processo e selezionarla.

Nota:

per impostazione predefinita, il campo **Salva processo in** viene compilato con il nome della cartella evidenziata nel riquadro delle cartelle prima di fare clic su **Nuovo processo**.

5. Dall'elenco a discesa **Seleziona dipendenze** selezionare le opzioni per aggiungere gli oggetti dipendenti al processo. È necessario selezionare esplicitamente gli oggetti dipendenti da promuovere. Ad esempio, selezionando Tutti gli universi dall'elenco a discesa Seleziona dipendenze, verranno selezionati tutti gli universi inclusi nell'elenco degli oggetti dipendenti. È quindi possibile selezionare singolarmente gli oggetti dipendenti.
6. Selezionare il sistema di origine e quello di destinazione dai rispettivi elenchi a discesa.
Se il nome del sistema non è incluso nell'elenco a discesa, fare clic sull'opzione **Accedi a nuovo CMS**. Viene aperta una nuova finestra. Immettere il nome del sistema, il nome utente e la password.
7. Fare clic su **Crea**.

Il nuovo processo creato viene memorizzato nel repository CMS del sistema di origine.

Nota:

se si crea un processo con una cartella come oggetto principale e tale processo è di tipo ricorrente, questo includerà eventuale contenuto aggiunto alla cartella all'esecuzione successiva.

Argomenti correlati

- [Utilizzo dell'opzione Impostazioni di sostituzione LCM](#)

16.3.2.1 Per accedere a un nuovo CMS

In questa sezione viene descritto come accedere a un nuovo CMS.

Per accedere a un nuovo CMS, attenersi alla seguente procedura:

1. Avviare l'applicazione Promotion Management.
2. Creare un nuovo processo.
Per ulteriori informazioni sulla creazione di un nuovo processo, consultare [Per creare un processo](#).
3. Dall'elenco a discesa **Sistema di origine** selezionare **Accedi a nuovo CMS**.
Viene visualizzata la finestra di dialogo "Accedi al sistema".
4. Immettere le credenziali utente, selezionare il tipo di autenticazione appropriato e fare clic su **Accedi**.
5. Dall'elenco a discesa **Sistema di destinazione** selezionare **Accedi a nuovo CMS**.
6. Immettere le credenziali utente, selezionare il tipo di autenticazione appropriato e fare clic su **Accedi**.

Argomenti correlati

- [Per modificare un processo](#)
- [Per aggiungere un infoobject a un processo](#)
- [Per promuovere un processo quando i repository sono connessi](#)
- [Per pianificare la promozione di un processo](#)

16.3.3 Per creare un nuovo processo copiando un processo esistente

In questa sezione viene descritto come creare un nuovo processo copiando un processo esistente.

Per creare un nuovo processo copiando un processo esistente, attenersi alla procedura seguente:

1. Avviare l'applicazione Promotion Management.
2. Nella home page "Processi di promozione" fare clic su **Nuovo processo**.

3. Fare clic sull'opzione **Copia da un processo esistente**.

Verrà visualizzata la finestra "Copia da un processo esistente" con l'elenco dei processi disponibili nella cartella **Processi di promozione**.

4. Selezionare il processo richiesto nell'elenco e fare clic su **Crea**.

Vengono visualizzati il nome, le parole chiave e la descrizione relativi al processo. Se necessario, è possibile modificare questi campi. Non è però possibile modificare il nome del sistema di origine.

5. Nel campo **Salva processo in** specificare la cartella in cui si desidera salvare il processo e fare clic su **Crea**.

Viene creato un nuovo processo e viene visualizzata la pagina "Aggiungi oggetti - Nome processo".

Argomenti correlati

- [Per aggiungere un infoobject a un processo](#)
- [Per modificare un processo](#)
- [Per promuovere un processo quando i repository sono connessi](#)

16.3.4 Per eseguire la ricerca di un processo

La funzionalità di ricerca dello strumento Promotion Management consente di individuare un processo disponibile nel repository.

Per cercare un processo, attenersi alla procedura seguente:

1. Nel campo **Cerca** della pagina iniziale, immettere il testo che si desidera individuare.
2. Fare clic sull'elenco che viene visualizzato accanto al campo **Cerca** per specificare i parametri di ricerca. È possibile specificare i seguenti parametri di ricerca:
 - Cerca titolo: questa opzione consente di ricercare un processo in base al nome.
 - Cerca parola chiave: questa opzione consente di ricercare un processo in base a parole chiave.
 - Cerca nella descrizione: questa opzione consente di ricercare un processo in base alla descrizione.
 - Cerca in tutti i campi: questa opzione consente di ricercare un processo in base a titolo, parole chiave e descrizione.
3. Fare clic sull'icona di ricerca.

Argomenti correlati

- [Per aggiungere un infoobject a un processo](#)
- [Per modificare un processo](#)

16.3.5 Per modificare un processo

In questa sezione viene descritto come modificare un processo.

Nota:

modificare un processo non significa crearne uno nuovo.

Per modificare un processo, attenersi alla seguente procedura:

1. Avviare l'applicazione Promotion Management.
2. Nella home page "Processi di promozione" selezionare il processo che si desidera modificare.
3. Fare clic su **Modifica**.

Vengono visualizzati i dettagli del processo selezionato. In base alle proprie esigenze, è possibile aggiungere o rimuovere infoobject, gestire dipendenze o promuovere il processo.

durante la modifica di un processo non è possibile cambiare il nome del sistema di origine.

Argomenti correlati

- [Per aggiungere un infoobject a un processo](#)
- [Per promuovere un processo quando i repository sono connessi](#)
- [Per pianificare la promozione di un processo](#)

16.3.6 Per aggiungere un infoobject a un processo

Ogni processo deve includere un insieme di infoobject e di relativi oggetti dipendenti. Prima di promuovere un processo nel sistema di destinazione è quindi necessario aggiungervi degli infoobject.

Nota:

Quando si promuove un report Crystal in base agli Inoobject della vista aziendale (Connessione dati, Base dati, Elementi aziendali e Vista aziendale) è necessario includere informazioni sulla protezione (il diritto DataAccess per Connessione dati e il diritto ViewDataField per Base dati ed Elementi aziendali) per visualizzare i dati di un report sul sistema di destinazione.

Nota:

durante l'aggiunta di un infoobject a un processo è necessario accedere al sistema di destinazione.

Per aggiungere un infoobject a un processo, attenersi alla seguente procedura:

1. Avviare lo strumento Promotion Management.
2. Creare un nuovo processo.

Per informazioni sulla creazione di un nuovo processo, consultare [Per creare un processo](#).

3. Fare clic su **Aggiungi oggetti**.

Verrà visualizzata la finestra di dialogo "Aggiungi oggetti" con l'elenco degli oggetti disponibili.

4. Passare alla cartella da cui si desidera selezionare l'infoobject.

Verrà visualizzato l'elenco degli infoobject presenti nella cartella selezionata.

5. Selezionare l'infoobject che si desidera aggiungere al processo e fare clic su **Aggiungi**.

Se si desidera aggiungere un infoobject e uscire dalla finestra di dialogo "Aggiungi oggetti - Nome del sistema di origine" fare clic su **Aggiungi e chiudi**. L'infoobject viene aggiunto al processo e la finestra di dialogo "Aggiungi oggetti - Nome del sistema di origine" viene chiusa.

Dopo avere aggiunto un infoobject a un processo, è possibile fare clic con il pulsante destro del mouse sulla pagina "Visualizzatore processi" e selezionare i processi secondari correlati al processo principale per continuare l'attività di promozione. È possibile gestire gli oggetti dipendenti dell'infoobject selezionato utilizzando l'opzione **Gestisci dipendenze** della pagina "Visualizzatore processi".

Nota:

- Il carrello degli acquisti, che viene visualizzato nel pannello sinistro della pagina "Visualizzatore processi", riporta il processo, insieme ai relativi oggetti dipendenti, in una semplice struttura ad albero.
- Dopo avere aggiunto gli infoobject, fare clic sull'opzione **Salva** per salvare le modifiche. In caso contrario, verrà richiesto di salvare il processo al momento della chiusura della scheda.

Procedura consigliata: SAP Business Objects consiglia di selezionare un numero ridotto di infoobject da promuovere contemporaneamente, ovvero non più di 100 alla volta, al fine di garantire le migliori prestazioni possibili da parte dello strumento Promotion Management.

Argomenti correlati

- [Per gestire le dipendenze di un processo](#)
- [Per promuovere un processo quando i repository sono connessi](#)
- [Per pianificare la promozione di un processo](#)

16.3.7 Per gestire le dipendenze di un processo

In questa sezione viene descritto come gestire gli oggetti dipendenti di un infoobject.

Per gestire gli oggetti dipendenti di un infoobject, attenersi alla seguente procedura:

1. Avviare lo strumento Promotion Management.

2. Creare un nuovo processo.

Per informazioni sulla creazione di un nuovo processo, consultare [Per creare un processo](#).

3. Aggiungere gli infoobject richiesti al nuovo processo.


Viene visualizzata la schermata "Processi di promozione".

4. Fare clic su **Gestisci dipendenze**.

Viene visualizzata la finestra "Gestisci dipendenze" con l'elenco degli infoobject e relativi oggetti dipendenti. Per visualizzare solo gli oggetti dipendenti che non sono stati selezionati, fare clic sulla casella di controllo **Visualizzare solo i dipendenti non selezionati**.

5. Dall'elenco a discesa **Seleziona dipendenze** selezionare le opzioni per aggiungere gli oggetti dipendenti al processo. Gli oggetti dipendenti non sono selezionati per impostazione predefinita; è necessario selezionare esplicitamente quelli che si desidera promuovere.

Se ad esempio si seleziona **Tutti gli universi** nell'elenco a discesa **Visualizzare solo i dipendenti non selezionati**, vengono selezionati tutti gli universi inclusi nell'elenco dei dipendenti. Gli oggetti dipendenti possono essere selezionati anche singolarmente.

È possibile fare clic su **Tipo**  per visualizzare le opzioni di filtro supportate per gli infoobject. Viene visualizzato un elenco a discesa con le opzioni di filtro supportate. Selezionare l'opzione di filtro e fare clic su **OK**. Vengono visualizzati gli infoobject filtrati.

Gli oggetti dipendenti selezionati dalla colonna **Dipendenti** vengono automaticamente spostati nella colonna **Oggetti in processo**.

Per ricercare un oggetto dipendente, è inoltre possibile digitarne il nome nel campo **Cerca dipendenti**.

Per ulteriori informazioni sulla ricerca di oggetti dipendenti, consultare [Per eseguire la ricerca di oggetti dipendenti](#)

6. Fare clic su **Applica modifiche** per aggiornare l'elenco degli oggetti dipendenti e fare clic su **Applica modifiche e chiudi** per salvare le modifiche.

Gli oggetti dipendenti vengono elaborati automaticamente dallo strumento in base alle relazioni o alle proprietà degli infoobject. Gli oggetti dipendenti non qualificabili in base ai suddetti parametri non vengono elaborati in questa versione dello strumento.

Nota:

se si seleziona una cartella per la promozione, i contenuti presenti in essa vengono considerati risorse primarie.

Argomenti correlati

- [Per promuovere un processo quando i repository sono connessi](#)

16.3.8 Per eseguire la ricerca di oggetti dipendenti

La funzionalità di ricerca avanzata nello strumento Promotion Management consente di individuare gli oggetti dipendenti degli infoobject disponibili nel repository.

Per cercare gli oggetti dipendenti di un infoobject, attenersi alla procedura seguente:

1. Avviare Promotion Management.
2. Creare un nuovo processo o modificare un processo esistente.

Se è stato creato un nuovo processo, aggiungervi infoobject. Se si sta modificando un processo esistente, è possibile aggiungere gli oggetti, se necessario.

3. Fare clic su **Gestisci dipendenze**.
4. Nel campo **Cerca dipendenti** immettere il nome dell'oggetto dipendente che si desidera individuare.
5. Fare clic sull'icona di ricerca.

Argomenti correlati

- [Per gestire le dipendenze di un processo](#)

16.3.9 Per promuovere un processo quando i repository sono connessi

In questa sezione viene descritto come promuovere un processo dal sistema di origine a quello di destinazione se i repository sono connessi.

Nella tabella seguente sono elencati i tipi di infoobject che è possibile promuovere utilizzando lo strumento Promotion Management:

Categoria	Tipi di oggetto che si possono promuovere
Report	Crystal Reports, Web Intelligence, Cruscotti, QaaWS, Explorer
Oggetti di terze parti	Testo formattato, documento di testo, Microsoft Excel, Microsoft Power Point, Microsoft Word, Flash, Adobe Acrobat
Utenti	Utenti e gruppi di utenti
Server	Gruppi di server
Piattaforma BI	Cartella, programma, eventi, profili, pacchetto oggetti, collegamento ipertestuale, categorie, avvisi, documento posta in arrivo, cartella personale e cartella Preferiti
Universo, spazio di lavoro	Universi UNV, connessioni
EPM Dashboard	Universi, connessioni, report, cruscotto e analitiche
BusinessView	DataFoundation

Categoria	Tipi di oggetto che si possono promuovere
Federation <ul style="list-style-type: none"> • Elenco di replica • Processi di replica 	Elenco di replica promuove i seguenti oggetti: Flash, .txt, discussioni, cruscotti, .pdf, collegamenti ipertestuali, .xls, ObjectPackage, Crystal Reports, documenti Web Intelligence, universi, programmi, connessioni, DataFoundation, Business Views, .rtf, profili, eventi, utenti e gruppi di utenti. Le connessioni di replica promuovono processi di replica, connessione remota, pubblicazioni, discussione, connessione Pioneer
Servizi BI	Documenti Web Intelligence, universi e connessioni
Nuovi Infoobject	Report Crystal (rpt/rptr), Pioneer, Dashboard Design, DSL Universe (UNX), WEBI, Explorer, Data Federator, Data Steward, Spazio di lavoro BI e così via.

Per promuovere un processo, attenersi alla procedura seguente:

1. Avviare Promotion Management.
2. Nella home page "Processi di promozione" selezionare il processo che si desidera promuovere.
È anche possibile fare clic con il pulsante destro del mouse sulla schermata home page e scegliere **Promuovi**.
3. Dagli elenchi a discesa dei sistemi **Origine** e **Destinazione** selezionare i sistemi di origine e di destinazione.

Nota:

prima di procedere al processo di promozione, assicurarsi di avere eseguito l'accesso sia al sistema di origine che a quello di destinazione.

4. Nel campo **ID gestione modifiche** immettere il valore appropriato e fare clic su **Salva**.

Nota:

L'ID gestione modifiche viene utilizzato per ottenere informazioni relative ad accesso, controllo, cronologia dei processi e così via. Lo strumento Promotion Management consente di mappare tutte le istanze della creazione di processi a un ID gestione modifiche. L'ID gestione modifiche è un attributo che viene impostato dall'utente nella definizione del processo durante la creazione di un nuovo processo. Lo strumento genera automaticamente un ID per ogni processo.

5. Selezionare **Impostazioni di protezione**, se necessario. Vengono visualizzate le seguenti opzioni:
 - Non promuovere protezione: opzione predefinita.
 - Promuovi protezione: opzione da utilizzare per promuovere i processi con i diritti di protezione associati.
 - Promuovi protezione oggetto: utilizzare questa opzione per promuovere la protezione di oggetti e cartelle.
 - Promuovi protezione utente: consente di promuovere i diritti degli utenti che sono parte del processo.

- **Includi diritti applicazione:** questa opzione è abilitata solo quando si seleziona **Promuovi protezione**. Se gli oggetti nel processo ereditano diritti applicazione, il processo viene promosso insieme a tali diritti.

È anche possibile fare clic su **Visualizza protezione** per visualizzare le dipendenze di protezione degli infoobject nel processo.

6. Fare clic su **Prova promozione** per assicurarsi che non ci siano conflitti tra i CUID degli infoobject nei sistemi di origine e di destinazione. I dettagli della promozione sono visualizzati nelle schede **Operazione riuscita**, **Operazione non riuscita** e **Avviso**. La prima colonna riporta gli oggetti da promuovere, mentre la seconda lo stato di promozione di ogni infoobject. Lo strumento Promotion Management classifica gli oggetti selezionati in utenti, gruppi, universi e così via.

Nota:

questa opzione non consente di salvare alcun infoobject per la promozione.

La prova della promozione può produrre uno dei seguenti risultati:

- **Sovrascritto:** l'infoobject nel sistema di destinazione viene sovrascritto dall'infoobject nel sistema di origine.
- **Copiato:** l'infoobject nel sistema di origine viene copiato nel sistema di destinazione.
- **Rimosso:** l'infoobject non viene promosso dal sistema di origine al sistema di destinazione.
- **Avviso:** l'infoobject nel sistema di destinazione è la versione più recente ed è possibile rimuovere l'infoobject dal processo. Tuttavia, se si desidera eseguire la promozione, l'infoobject viene promosso.

7. Fare clic su **Pianifica processo** se si desidera pianificare la promozione di un'istanza di un processo.
8. Fare clic su **Promuovi**.

Il processo selezionato viene promosso.

se non si desidera promuovere il processo, è possibile utilizzare l'opzione **Salva** per salvare le modifiche apportate ad esempio alle impostazioni Protezione, ID gestione modifiche e Pianifica.

16.3.10 Promozione di un processo mediante un file BIAR

Per promozione si intende l'attività di trasferimento di una risorsa BI da un repository all'altro. Se i sistemi di origine e di destinazione sono connessi, lo strumento Promotion Management utilizza la WAN o la LAN per promuovere l'infoobject. Tuttavia, Promotion Management semplifica la promozione di infoobject anche se i sistemi di origine e di destinazione non sono connessi.

Negli scenari in cui i sistemi di origine e di destinazione non sono connessi, lo strumento Promotion Management supporta la promozione dei processi nel sistema di destinazione consentendo di esportare il processo presente nel sistema di origine in un file BIAR, per poi importarlo dal file BIAR al sistema di destinazione.

In questa sezione viene descritto come esportare un processo in un file BIAR e quindi importarlo dal file BIAR al sistema di destinazione.

Nota:

non è possibile utilizzare un file BIAR creato mediante lo strumento Importazione guidata.

Argomenti correlati

- [Esportazione di un processo in un file BIAR](#)
- [Importazione di un processo da un file BIAR](#)

16.3.10.1 Esportazione di un processo in un file BIAR

In questa sezione viene descritto come esportare un processo in un file BIAR.

Per esportare un processo in un file BIAR, attenersi alla seguente procedura:

1. Avviare lo strumento Promotion Management e creare un nuovo processo.
Per ulteriori informazioni sulla creazione di un nuovo processo, consultare [Per creare un processo](#)
2. Nell'elenco a discesa **Destinazione** selezionare l'opzione **Output nel file LCMBIAR** e fare clic su **Crea**.
3. Fare clic su **Aggiungi oggetti** per aggiungere gli infoobject al processo.
È possibile utilizzare l'opzione **Gestisci dipendenze** per gestire le dipendenze del processo selezionato.
4. Fare clic su **Promuovi**.
Viene visualizzata la finestra di dialogo "Promuovi".
5. Modificare le opzioni come desiderato e fare clic su **Esporta**.
Viene creato il file BIAR. È possibile salvare un file BIAR in un file system o in una posizione FTP.
6. Nell'elenco a discesa **Destinazione** selezionare l'opzione **Output nel file LCMBIAR** e fare clic su **Destinazione file LCMBiar**.
Viene visualizzato il riquadro **Destinazione file LCMBiar**.
7. Eseguire una delle seguenti operazioni:
 - Selezionare **File System**.
 - Selezionare **FTP**, immettere i dettagli appropriati nei campi host, porta, nome utente, password, directory e nome file.
8. Per crittografare il file LCMBIAR mediante una password, fare clic sulla casella di controllo **Crittografia password**.
9. Immettere una password nel campo **Password**.
10. Immettere di nuovo la password nel campo **Verify Password**.
11. Fare clic su **Esporta**.
Il file BIAR viene esportato nel file system o in un percorso FTP, a seconda dell'opzione selezionata nel passaggio 7.

12. È possibile pianificare l'esportazione di un processo in un file BIAR. Per ulteriori informazioni su questo argomento, fare riferimento alla sezione [Per pianificare la promozione di un processo](#).

Argomenti correlati

- [Per aggiungere un infoobject a un processo](#)
- [Per gestire le dipendenze di un processo](#)

16.3.10.2 Importazione di un processo da un file BIAR

È possibile importare un processo dai classici file BIAR o da un file LCMBIAR. Il file BIAR viene copiato dal dispositivo di archiviazione al sistema di destinazione.

Per importare un file BIAR, attenersi alla procedura seguente:

1. Avviare l'applicazione Promotion Management.
2. Nella pagina iniziale di "Processi di promozione", fare clic su **Importa > Importa file**.
Viene visualizzata la finestra "Importa da file".
3. È possibile importare un file BIAR dal computer locale o da un'altro computer di origine qualsiasi.
 - Per importare un file BIAR dal computer locale, eseguire la procedura seguente:
 - a. Selezionare **File System**.
 - b. Fare clic su **Sfoglia** e selezionare un file BIAR dal file system.
Nota:
se esiste un processo con lo stesso nome, viene visualizzata la finestra a comparsa Conferma salvataggio. Fare clic su "Sì" per sovrascrivere il processo esistente, su "No" per creare un processo con un nuovo CUID e il nome Nomeprocesso_copia.
 - c. Nel campo **Password** immettere la password del file LCMBIAR.
Nota:
il campo Password viene visualizzato solo se il file LCMBIAR viene crittografato con una password.
 - d. Fare clic su **Crea**. Viene creato il processo.
 - Per importare il file BIAR da un qualsiasi computer di origine sul quale è abilitato l'FTP, completare la procedura seguente:
 - a. Selezionare **FTP**.
 - b. Immettere le informazioni appropriate nei campi host, porta, nome utente, password, directory e nome file e fare clic su **OK**.
4. Fare clic su **Promuovi**.

Viene visualizzata la finestra "Promuovi - Nome processo".

5. Nell'elenco a discesa **Destinazione** selezionare il sistema di destinazione. Se si seleziona **Accedi a nuovo CMS**, verrà richiesto di immettere le credenziali. Confermare le credenziali di accesso del sistema di destinazione.
6. Fare clic su **Promuovi** per promuovere i contenuti nel sistema di destinazione.
È anche possibile scegliere l'opzione **Prova promozione** per visualizzare gli oggetti da promuovere e il relativo stato della promozione.

Argomenti correlati

- [Per gestire le dipendenze di un processo](#)

16.3.11 Per pianificare la promozione di un processo

In questa sezione viene descritto come pianificare la promozione di un'istanza processo. Viene inoltre descritto come specificare le opzioni di ricorrenza e i parametri.

Per pianificare la promozione di un'istanza processo, attenersi alla procedura seguente:

1. Nella finestra di dialogo "Promuovi" fare clic sull'opzione **Pianifica**.
2. Impostare l'opzione di pianificazione necessaria e fare clic su **Pianifica**.

Se si aggiungono infoobject a una cartella esistente dopo aver pianificato il processo per la promozione, questi verranno promossi anche nella destinazione all'ora pianificata.

La pianificazione in una destinazione è possibile durante l'esportazione di un processo in un file BIAR.

Suggerimento:

Una volta completata la promozione di un infoobject, è possibile visualizzare tutte le istanze in esecuzione dell'infoobject facendo clic su di esso con il pulsante destro del mouse e scegliendo **Cronologia**.

La promozione di un processo può avvenire anche in base ad attivazioni di eventi.

È possibile selezionare le notifiche di posta elettronica in base allo stato della promozione del processo (come operazione riuscita/operazione parzialmente riuscita/operazione non riuscita). Per informazioni dettagliate sulle diverse opzioni di pianificazione e di configurazione delle notifiche, fare riferimento alla sezione Pianificazione.

Argomenti correlati

- [Esportazione di un processo in un file BIAR](#)




16.3.11.1 Per aggiornare le istanze di promozione dei processi ricorrenti e in sospeso

Lo strumento Promotion Management consente di rilevare e aggiornare lo stato della promozione pianificata di un'istanza di processo mediante le opzioni **Ricorrente e Istanze in sospeso**.

Per tenere traccia e aggiornare le istanze di promozione di un processo pianificato, attenersi alla procedura seguente:

1. Avviare lo strumento Promotion Management.
2. Nella home page "Processi di promozione" selezionare un processo.
3. Fare clic su **Cronologia**.
Viene visualizzata la finestra "Cronologia processo".
4. Fare clic su **Ricorrente e Istanze in sospeso**.
Viene visualizzata la finestra "Cronologia processo per ricorrenze e Istanze in sospeso" con l'elenco delle istanze di promozione del processo ricorrenti e in sospeso.

In base alle esigenze, è possibile utilizzare le seguenti opzioni:

- Fare clic su **Istanze promosse** per visualizzare l'elenco delle istanze di promozione del processo.
- Fare clic sull'opzione **Sospendi** per sospendere la promozione pianificata.
- Fare clic sull'opzione **Riprendi** per riprendere l'istanza di promozione del processo pianificata sospesa.
- Fare clic sull'opzione **Ripianifica** per ripianificare un'istanza di promozione del processo.
- Fare clic su  per eliminare un'istanza di promozione del processo pianificata.
- Fare clic su  per aggiornare lo stato di un'istanza di promozione del processo pianificata.
- È possibile utilizzare l'opzione  per spostarsi all'interno di una singola pagina o passare a una pagina specifica immettendone il numero.

Nota:

la colonna Stato nella finestra "Cronologia processo per ricorrenze e Istanze in sospeso" riporta lo stato dell'istanza di promozione del processo, ad esempio Ricorrente, In sospeso e così via.

Argomenti correlati

- [Per eseguire il rollback di un processo](#)

16.3.12 Per visualizzare la cronologia di un processo

In questa sezione viene descritto come visualizzare la cronologia di un processo.

Nota:

Per visualizzare la cronologia di un processo, assicurarsi che il relativo stato sia uno dei seguenti:

- Esito positivo
- Operazione non riuscita
- Operazione parzialmente riuscita

Per visualizzare la cronologia di un processo, attenersi alla seguente procedura:

1. Avviare lo strumento Promotion Management.

Viene visualizzata la home page "Processi di promozione".

2. Eseguire una delle operazioni riportate di seguito:

- Fare clic con il pulsante destro del mouse sul processo di cui si desidera visualizzare la cronologia e selezionare **Cronologia**.
- Selezionare il processo di cui si desidera visualizzare la cronologia e fare clic sulla scheda **Cronologia**.

Vengono visualizzati l'istanza del processo, il nome del processo, i nomi dei sistemi di origine e destinazione, l'ID dell'utente che ha promosso il processo e lo stato (Operazione riuscita, Operazione non riuscita o Operazione parzialmente riuscita) del processo.

È possibile visualizzare lo stato del processo utilizzando il collegamento visualizzato nella colonna **Stato**.

16.3.13 Per eseguire il rollback di un processo

L'opzione Rollback consente di ripristinare lo stato precedente del sistema di destinazione dopo la promozione di un processo.

Per eseguire il rollback di un processo, attenersi alla seguente procedura:

1. Avviare lo strumento Promotion Management.

Viene visualizzata la home page "Processi di promozione".

2. Eseguire una delle operazioni riportate di seguito:

- Fare clic con il pulsante destro del mouse sul processo di cui si desidera eseguire il rollback e scegliere **Rollback**.
- Selezionare il processo per il quale eseguire il rollback e fare clic sulla scheda **Rollback**.

Viene visualizzata la finestra "Rollback".

3. Selezionare il processo di cui si desidera eseguire il rollback e fare clic su **Rollback completo**.

Il processo viene sottoposto a rollback.

È possibile eseguire il rollback solo dell'istanza più recente di una promozione di processo. Non è possibile eseguire il rollback di due istanze processo alla volta.

16.3.13.1 Per utilizzare l'opzione Rollback parziale

Lo strumento Promotion Management consente di eseguire il rollback completo o parziale degli infoobject in un processo dal sistema di destinazione.

Per eseguire il rollback parziale degli infoobject, attenersi alla procedura seguente:

1. Avviare lo strumento Promotion Management.
Viene visualizzata la home page "Processi di promozione".
2. Eseguire una delle operazioni riportate di seguito:
 - Fare clic con il pulsante destro del mouse sul processo di cui si desidera eseguire il rollback e scegliere **Rollback**.
 - Selezionare il processo per il quale eseguire il rollback e fare clic sulla scheda **Rollback**.
Viene visualizzata la finestra "Rollback".
3. Selezionare il processo dall'elenco e fare clic su **Rollback parziale**.
L'elenco degli infoobject nel processo selezionato viene visualizzato nella pagina "Visualizzatore processi".
4. Selezionare gli infoobject di cui si desidera eseguire il rollback e fare clic su **Rollback**.

Nota:

è necessario assicurarsi di avere eseguito il rollback di tutti gli infoobject di un processo prima di eseguire il rollback degli infoobject del successivo processo.

Avvertenza:

Se un processo viene promosso con la protezione, durante il rollback parziale degli infoobject, la protezione degli infoobject dipendenti selezionati potrebbe non essere riportata allo stato precedente.

Argomenti correlati

- [Gestione di diverse versioni delle risorse BI](#)

16.3.13.2 Per eseguire il rollback di un processo infoobject dopo la scadenza della password

In questa sezione viene descritto come eseguire il rollback di un processo dopo la scadenza della password utilizzata per promuoverlo.

Per eseguire il rollback di un processo dopo la scadenza della password, attenersi alla seguente procedura:

1. Selezionare il processo di cui si desidera eseguire il rollback e fare clic su **Rollback**.

2. Nella finestra "Rollback" selezionare **Rollback completo**.

Viene visualizzato un messaggio di errore in cui si informa che il processo non può essere sottoposto a rollback. Viene inoltre richiesto di accedere al sistema di origine o di destinazione.

3. Immettere le nuove credenziali di accesso e fare clic su **Accedi**.

Viene visualizzata una finestra di dialogo che indica che il processo di rollback è stato completato.

Nota:

I processi promossi utilizzando le credenziali per il sistema di origine o di destinazione vengono aggiornati automaticamente.

Argomenti correlati

- [Per eseguire il rollback degli infoobject dopo la scadenza della password](#)
- [Per utilizzare l'opzione Rollback parziale](#)

16.3.13.2.1 Per eseguire il rollback degli infoobject dopo la scadenza della password

In questa sezione viene descritto come eseguire il rollback di infoobject dopo la scadenza della password del sistema di origine o di destinazione.

Per eseguire il rollback di infoobject dopo la scadenza della password, attenersi alla seguente procedura:

1. Selezionare il processo di cui si desidera eseguire il rollback e fare clic su **Rollback**.

Viene visualizzata la finestra "Rollback".

2. Selezionare l'opzione **Rollback parziale**.

Viene visualizzato un messaggio di errore che informa che non è possibile eseguire il rollback degli infoobject. Viene inoltre richiesto di accedere al sistema di origine o di destinazione.

3. Immettere le nuove credenziali di accesso e fare clic su **Accedi**.

Viene visualizzata la pagina "Visualizzatore processi". In questa pagina viene visualizzato l'elenco degli infoobject.

4. Selezionare gli infoobject necessari e fare clic su **Rollback**.

Nota:

i processi promossi utilizzando le credenziali del sistema di origine o di destinazione vengono automaticamente aggiornati.

Argomenti correlati

- [Per eseguire il rollback di un processo](#)
- [Per utilizzare l'opzione Rollback parziale](#)
- [Per eseguire il rollback di un processo infoobject dopo la scadenza della password](#)

16.4 Per gestire versioni diverse di un infoobject

L'applicazione Gestione delle versioni consente di gestire versioni diverse delle risorse BI presenti nel repository della piattaforma BI. Sono supportati i sistemi di gestione delle versioni Subversion e ClearCase. In questa sezione viene spiegato come utilizzare la funzionalità Gestione delle versioni nello strumento Console Promotion Management.


Per creare e gestire diverse versioni di un infoobject, attenersi alla seguente procedura:

1. Avviare l'applicazione Promotion Management.
2. Nella home page selezionare **Gestione delle versioni** nell'elenco a discesa.
Viene visualizzata la finestra di dialogo "Accedi al sistema".

3. Immettere le credenziali di accesso e fare clic su **Accedi**.
Viene visualizzata la finestra "Gestione delle versioni".

Nota:


È possibile accedere al sistema di gestione delle versioni (VMS, Version Management System) solo se è già stato configurato.

4. Se si desidera cambiare il sistema host, fare clic su .
Viene visualizzata la finestra di dialogo "Accedi al sistema".
5. Immettere le credenziali utente e fare clic su **Accedi**.
6. Dal pannello sinistro della finestra "Gestione delle versioni" selezionare la cartella per visualizzare gli infoobject dei quali si desidera gestire le versioni.
7. Selezionare gli infoobject e fare clic su **Aggiungi a gestione versioni**.

Nota:

facendo clic su "Aggiungi a gestione delle versioni", viene creata una versione di base dell'oggetto nel repository VMS. È necessaria una versione di base per le successive archiviazioni.

8. Fare clic su **Archivia** per aggiornare il documento esistente nel repository VMS.
Viene visualizzata la finestra di dialogo "Commenti di archiviazione".
9. Immettere i commenti e fare clic su **OK**.
Il cambiamento nel numero di versione dell'infoobject selezionato viene visualizzato nelle colonne Sistema di gestione delle versioni e Sistema di gestione dei contenuti.
10. Per ottenere la versione più recente di un documento dal VMS, selezionare l'infoobject richiesto e fare clic su **Ottieni versione più recente**.
11. Per creare una copia della versione più recente, fare clic su **Crea copia**.
Viene creata una copia della versione selezionata.
12. Selezionare **Cronologia** per visualizzare tutte le versioni disponibili per la risorsa selezionata.
Viene visualizzata la finestra "Cronologia". Vengono visualizzate le seguenti opzioni:

- **Ottieni versione:** se esistono più versioni e si desidera una versione particolare di una risorsa BI, è possibile selezionare la risorsa richiesta e fare clic su **Ottieni versione**.
 - **Ottieni copia della versione:** questa opzione consente di ottenere una copia della versione selezionata.
 - **Esporta copia della versione:** questa opzione consente di ottenere una copia della versione selezionata e di salvarla nel sistema locale.
13. Selezionare un infoobject e fare clic su **Blocca** per bloccare l'infoobject; fare clic su **Sblocca** per sbloccarlo.
- Nota:**
se si blocca un infoobject, non è possibile eseguire alcuna azione su di esso.
14. Sincronizzazione di CMS e VMS: quando la versione del CMS dell'infoobject viene aggiornata, viene visualizzato un indicatore accanto all'infoobject aggiornato. Posizionando il cursore sull'indicatore, viene visualizzata una descrizione che informa che l'infoobject nel CMS è stato aggiornato.
15. Per visualizzare l'elenco di tutte le risorse archiviate che esistono in VMS, ma non nel CMS, fare clic su **Visualizza risorse eliminate**.
Fare clic su una qualsiasi risorsa eliminata per visualizzarne la relativa cronologia. È possibile selezionare una risorsa eliminata e fare clic su **Ottieni versione** per visualizzare quella specifica versione della risorsa. È possibile fare clic su **Ottieni copia della versione** per ottenere una copia della risorsa selezionata.
- Nota:**
se si utilizzano le opzioni **Ottieni versione** o **Ottieni copia della versione**, la risorsa viene spostata dall'elenco dei file mancanti di VMS nel CMS.
- Avvertenza:**
se si elimina una cartella principale, le cartelle gli oggetti secondari in essa contenuti non potranno essere recuperati.
16. Selezionare una risorsa e fare clic su  per visualizzare le proprietà di tale risorsa.
In alternativa, è possibile fare clic con il pulsante destro del mouse sull'infoobject ed eseguire i passaggi da 4 a 16.

16.4.1 Diritti di accesso dell'applicazione Gestione delle versioni

In questa sezione vengono descritti i diritti di accesso dell'applicazione relativi all'applicazione Gestione delle versioni.

- È possibile impostare i diritti di accesso all'applicazione Gestione delle versioni nella CMC.
- È possibile impostare diritti granulari di applicazione per diverse funzioni nell'applicazione Gestione delle versioni.

Per impostare diritti specifici nell'applicazione Gestione delle versioni, attenersi alla procedura illustrata di seguito.

1. Accedere alla CMC e selezionare **Applicazioni**.

2. Fare doppio clic su **Gestione delle versioni**.
3. Fare clic su **Protezione utente** e selezionare un utente. È possibile visualizzare o assegnare diritti di protezione per l'utente selezionato.
4. Ora sono disponibili i diritti specifici della gestione delle versioni seguenti:
 - Consenti archiviazione
 - Consenti creazione copia
 - Consenti eliminazione revisione
 - Consenti acquisizione revisione
 - Consenti blocco e sblocco
 - Visualizza oggetti BOMM e aggiungi a gestione delle versioni
 - Visualizza viste aziendali e aggiungi a gestione delle versioni
 - Visualizza calendari e aggiungi a gestione delle versioni
 - Visualizza connessioni e aggiungi a gestione delle versioni
 - Visualizza profili e aggiungi a gestione delle versioni
 - Visualizza QaaWS e aggiungi a gestione delle versioni
 - Visualizza oggetti report e aggiungi a gestione delle versioni
 - Visualizza oggetti di protezione e aggiungi a gestione delle versioni
 - Visualizza universi e aggiungi a gestione delle versioni
 - Visualizza risorse eliminate
5. Se si desidera assegnare diritti a un utente selezionato, selezionare il diritto appropriato e fare clic su **Assegna protezione**.

16.4.2 Backup e ripristino di file Subversion

In questa sezione vengono descritte le procedure consigliate per eseguire backup e ripristino dei file Subversion. Un piano di backup e recupero consiste in alcune precauzioni da prendere in caso di errori del sistema dovuti a un disastro naturale o un evento catastrofico.

16.4.2.1 Per eseguire il backup dei file Subversion

Per eseguire il backup dei file Subversion, effettuare le operazioni seguenti:

1. In Windows, accedere a `DIRINSTALLAZ\SAP BusinessObjects Enterprise 4.0\Checkout` o in Unix, accedere a `DIRINSTALLAZ/sap_bobj/enterprise_40/subversion/checkout`
2. Copiare la cartella `Checkout` e salvarla su dispositivo di backup.
3. Copiare l'intero `Repository_LCME` salvarlo su qualsiasi dispositivo di backup.

16.4.2.2 Per ripristinare i file Subversion

Per eseguire il ripristino dei file Subversion, effettuare le operazioni seguenti:

1. Ripristinare la cartella di estrazione dal percorso in cui è stato eseguito il backup.

Nota:

Nella CMC fare clic su **Applicazioni > Gestione delle versioni > Impostazioni sistema gestione versioni** e verificare che nel campo **Directory spazio di lavoro** sia specificato il percorso di estrazione corretto.

2. Ripristinare LCM_Repository dal percorso in cui è stato eseguito il backup.

Nota:

Nella CMC fare clic su **Applicazioni > Gestione delle versioni > Impostazioni sistema gestione versioni** e verificare che nel campo **Percorso di installazione** sia specificato il percorso di estrazione corretto.

16.5 Utilizzo dell'opzione della riga di comando

L'opzione Riga di comando dello strumento Promotion Management consente di promuovere gli oggetti mediante input dalla riga di comando da una distribuzione della piattaforma BI a un'altra distribuzione della piattaforma BI.

Lo strumento Promotion Management supporta la promozione di processo seguente mediante l'opzione della riga di comando:

- Esportazione di un modello di processo LCM esistente in LCMBIAR con crittografia della password
- Esportazione di un modello di processo LCM esistente in LCMBIAR senza crittografia della password
- Promozione con il modello di processo esistente
- Importazione e promozione di un LCMBIAR esistente
- Esportazione di query di piattaforma singole/multiple
- Promozione di query di piattaforma multiple
- Esecuzione della promozione Live-Live

16.5.1 Per eseguire lo strumento da riga di comando in Windows

Per eseguire lo strumento da riga di comando, attenersi alla procedura seguente:

1. Avviare una shell o una finestra della riga di comando.

2. Spostarsi nella directory appropriata.

Ad esempio, il percorso della directory per Windows è -C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib

3. Eseguire una delle operazioni seguenti:

- Eseguire l'applicazione LCMCLI. Verificare che il percorso java venga impostato prima di eseguire il programma.

Comando: `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <file proprietà>`

- Eseguire il file BAT da C:\Programmi (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts\lcm_cli.bat

Comando: `lcm_cli.bat -lcmproperty <file proprietà>`

Nota:

immettere le password valide quando richiesto.

Lo strumento da riga di comando Promotion Management accetta come parametro un file *properties*. Il file *properties* include i parametri richiesti per indicare allo strumento Promotion Management le azioni da eseguire, la distribuzione della piattaforma BI a cui connettersi, i metodi di connessione, gli oggetti da promuovere e così via.

Il formato del file deve essere <Nome File>.properties

Ad esempio: *Proprietà.properties*

16.5.2 Per eseguire lo strumento da riga di comando in UNIX

Per eseguire lo strumento da riga di comando, attenersi alla procedura seguente:

1. Avviare la shell.

2. Spostarsi nella directory appropriata.

Ad esempio, `/usr/u/qaunix/Aurora604/sap_bobj/enterprise_40/java/lib`

3. Eseguire una delle operazioni seguenti:

- Eseguire l'applicazione LCMCLI. Verificare che il percorso java venga impostato prima di eseguire il programma.

Comando: `java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <file proprietà>`

- Eseguire il file BAT da `<installdir_path>\sap_bobj\lcm_cli.sh`

Comando: `lcm_cli.sh -lcmproperty <file proprietà>`

Nota:

immettere le password valide quando richiesto.

16.5.3 Parametri degli strumenti della riga di comando

Nella tabella seguente sono riportati i parametri e i valori consentiti per le opzioni della riga di comando dell'applicazione Promotion Management.

Parametro	Valori consentiti	Descrizione	Obbligatorio o facoltativo
<code>action</code>	Export, Promote Esempio: <code>action=export</code>	Questa opzione consente di specificare l'operazione che deve essere eseguita dalla CLI. Questa procedura può eseguire una delle operazioni seguenti: <ul style="list-style-type: none"> Promozione di oggetti di un file LCMBIAR o un processo di Promotion Management a un sistema della piattaforma BI. Esportazione di oggetti da un sistema della piattaforma BI o un file LCMBIAR. 	Obbligatorio
<code>consolelog</code>	true o false	Questo parametro viene utilizzato per visualizzare il log completo del comando eseguito dall'utente nel log dei comandi.	Facoltativo

Parametro	Valori consentiti	Descrizione	Obbligatorio o facoltativo
Destination_authentication	secEnterprise, secWinAD, secLDAP, secSAPR3 Esempio: Destination_authentication=<autenticazione>	Questo parametro indica il tipo di autenticazione da utilizzare.	Facoltativo. Se il tipo di autenticazione non è specificato, viene utilizzato secEnterprise
Destination_clientID	ID client Esempio: Destination_clientID=<ID sistema>	Questo parametro viene utilizzato esclusivamente per l'autenticazione SAP.	Obbligatorio per l'autenticazione SAP.
Destination_CMS	Testo in formato libero. Esempio: Destination_CMS=<NomeCMS: n. porta>	Questo parametro consente all'utente di specificare il CMS al quale deve connettersi lo strumento.	Obbligatorio se action=export
Destination_password	Testo in formato libero. Esempio: Destination_password=<password>	Questo parametro specifica la password associata dell'account utente.	Obbligatorio se action=promote
Destination_systemID	ID sistema Esempio: Destination_systemID=<ID sistema>	Questo parametro viene utilizzato esclusivamente per l'autenticazione SAP.	Obbligatorio per l'autenticazione SAP.

Parametro	Valori consentiti	Descrizione	Obbligatorio o facoltativo
Destination_username	<p>Testo in formato libero.</p> <p>Esempio: Destination_username=<nomeutente></p>	<p>Questo parametro consente di specificare l'account utente che deve essere utilizzato dallo strumento per la connessione al server CMS della piattaforma BI.</p> <p>Nota: è supportato l'amministratore delegato.</p>	Obbligatorio se action=promote
exportLocation	<p>Testo in formato libero. Deve avere estensione .lcmbar</p> <p>Esempio: exportLocation=C:/Backup/New.lcmbar</p>	<p>Questo parametro consente all'utente di specificare la posizione in cui inserire il file LC-MBIAR dopo l'esportazione e l'inserimento di oggetti in un pacchetto.</p>	Obbligatorio se action=export
exportDependencies	<p>false, true</p> <p>Esempio: exportDependencies=<true o false></p>	<p>Questo parametro specifica le dipendenze degli oggetti raccolte dallo strumento per l'esportazione. È valido solo se utilizzato insieme al flag Source_CMS.</p>	<p>Facoltativo, utilizzato se action=promote o export</p> <p>Se non è specificato, il valore predefinito è false.</p>

Parametro	Valori consentiti	Descrizione	Obbligatorio o facoltativo
exportQuery	<p>Testo in formato libero. Utilizzare il formato del linguaggio di query del server CMS.</p> <p>Esempio: <code>exportQuery1=select*from ci_Infoobjects where si_name='Xtreme Employees' and si_kind='Webi'</code></p> <p>Nota: in un file delle proprietà può essere presente qualsiasi numero di query che tuttavia devono essere denominate <code>exportQuery1</code>, <code>exportQuery2</code> e così via.</p>	Si tratta delle query che devono essere eseguite dallo strumento per raccogliere gli oggetti che si desidera esportare.	Facoltativo. Utilizzato se <code>action=export</code>
exportQueriesTotal	<p>Numeri interi positivi</p> <p><code>exportQueriesTotal=<numero intero></code></p>	Questo parametro consente all'utente di specificare il numero di query di esportazione da eseguire. Se sono presenti x query di esportazione e si desidera eseguirle tutte, impostare questo valore di parametro su x.	<p>Facoltativo. Utilizzato se <code>action=export</code></p> <p>Se non è specificato, il valore predefinito è 1.</p>
importLocation	<p>Testo in formato libero. Deve avere estensione <code>.lcmbiar</code></p> <p>Esempio: <code>importLocation=C:/Backup/New.lcmbiar</code></p>	Questo parametro consente all'utente di specificare la posizione del file LCMBIAR contenente gli oggetti da promuovere.	Obbligatorio se <code>action=promote</code>

Parametro	Valori consentiti	Descrizione	Obbligatorio o facoltativo
<code>includeApplicationSecurity</code>	<p>false, true</p> <p>Esempio: <code>includeApplicationSecurity=<true o false></code></p>	Questo parametro indica allo strumento di esportare o importare la protezione associata alle applicazioni selezionate.	<p>Facoltativo. Se non è specificato, il valore predefinito è false.</p> <p>Utilizzato se <code>action=promote o export</code></p>
<code>includeSecurity</code>	<p>false, true</p> <p>Esempio: <code>includeSecurity=<true o false></code></p>	Questo parametro indica allo strumento di esportare o importare la protezione associata agli oggetti e agli utenti selezionati. Se vengono utilizzati i livelli di accesso, anche questi verranno esportati o importati.	<p>Facoltativo. Se non è specificato, il valore predefinito è false.</p> <p>Utilizzato se <code>action=promote o export</code></p>
<code>JOB_CUID</code>	Il CUID del processo LCM salvato.	Questo parametro indica allo strumento di esportare tutti gli oggetti del processo nel file LCMBIAR.	Facoltativo. Utilizzato se <code>action=export o promote</code>
<code>lcmbiarpassword</code>	<p>Testo in formato libero.</p> <p>Esempio: <code>java -jar upgradeManagementTool.jar -mode livetobiart -biarfile "C:\TEMP\abc.biar" -lcmbiarpassword "testpassword"</code></p>	Questo parametro consente la crittografia e la decrittazione dei file BIAR mediante una password.	Facoltativo. Se non è specificato o la stringa è vuota, implica l'assenza di crittografia.

Parametro	Valori consentiti	Descrizione	Obbligatorio o facoltativo
lcmproperty	<p>Percorso completo della posizione in cui è stato salvato il file delle proprietà.</p> <p>lcm_cli.bat -lcm property <percorso file del file delle proprietà></p>	Questo parametro fa riferimento ai valori necessari per l'esecuzione di un comando, che vengono salvati in un file.	Obbligatorio
LCM_authentication	<p>secEnterprise, secWinAD, secLDAP, secSAPR3</p> <p>Esempio: LCM_authentication=<autenticazione></p>	Questo parametro indica il tipo di autenticazione da utilizzare.	Facoltativo. Se il tipo di autenticazione non è specificato, viene utilizzato secEnterprise
LCM_clientID	<p>ID client</p> <p>Esempio: LCM_clientID=<IDclient></p>	Questo parametro viene utilizzato per l'autenticazione SAP.	Obbligatorio per l'autenticazione SAP.
LCM_CMS	<p>Testo in formato libero.</p> <p>Esempio: LCM_CMS=<NomeCMS:n.porta></p>	Questo parametro consente all'utente di specificare il CMS per l'applicazione Promotion Management.	Obbligatorio se action=promote o export
LCM_password	<p>Testo in formato libero.</p> <p>Esempio: LCM_password=<password></p>	Questo parametro consente all'utente di specificare la password dell'account utente.	Obbligatorio se action=promote o export
LCM_systemID	<p>ID sistema</p> <p>Esempio: LCM_systemID=<IDSistema></p>	Questo parametro viene utilizzato per l'autenticazione SAP.	Obbligatorio per l'autenticazione SAP.

Parametro	Valori consentiti	Descrizione	Obbligatorio o facoltativo
LCM_userName	<p>Testo in formato libero.</p> <p>Esempio: LCM_userName=<nomeutente></p>	<p>Questo parametro consente all'utente di specificare il nome utente dell'account che lo strumento deve utilizzare per il collegamento al CMS dell'applicazione Promotion Management.</p> <p>Nota: è supportato l'amministratore delegato</p>	Obbligatorio se action=promote o export
Source_authentication	<p>secEnterprise, secWinAD, secLDAP, secSAPR3</p> <p>Esempio: Source_authentication=<autenticazione></p>	Questo parametro indica il tipo di autenticazione da utilizzare.	Facoltativo. Se il tipo di autenticazione non è specificato, viene utilizzato secEnterprise
Source_clientID	<p>ID client SAP</p> <p>Esempio: Source_clientID=<IDSistema></p>	Questo parametro viene utilizzato esclusivamente per l'autenticazione SAP.	Obbligatorio per l'autenticazione SAP.
Source_CMS	<p>Testo in formato libero.</p> <p>Esempio: Source_CMS=<NomeCMS: n.porta></p>	Questo parametro consente all'utente di specificare il CMS al quale deve connettersi lo strumento.	Obbligatorio se action=export
Source_password	<p>Testo in formato libero.</p> <p>Esempio: Source_password=<password></p>	Questo parametro specifica la password associata dell'account utente.	Obbligatorio se action=export

Parametro	Valori consentiti	Descrizione	Obbligatorio o facoltativo
Source_systemID	ID sistema SAP Esempio: Source_systemID=<IDSistema>	Questo parametro viene utilizzato esclusivamente per l'autenticazione SAP.	Obbligatorio per l'autenticazione SAP.
Source_userName	Testo in formato libero. Esempio: Source_username=<nomeutente>	Questo parametro consente di specificare l'account utente che deve essere utilizzato dallo strumento per la connessione al server CMS della piattaforma BI. Nota: è supportato l'amministratore delegato.	Obbligatorio se action=export
stacktrace	true o false Esempio: stacktrace=<true o false>	Questo parametro consente all'utente di tenere traccia di tutte le chiamate.	Facoltativo. Se non è specificato, il valore predefinito è false

Nota:

- Analoga alla creazione di un processo prima dell'esportazione, l'opzione della riga di comando crea rapidamente un processo temporaneo. Il nome di questo processo potrebbe essere una combinazione di `Query_<UTENTE>_<Indicazione data e ora>` ed è specifico solo di `exportQuery`.
- La convenzione di denominazione del file LCMBIAR esportato può essere una combinazione di `<NomeProcesso>_<IndicazioneDataOra>.lcmbar` per garantire l'univocità quando il nome di LCMBIAR non è specificato nel file `exportLocation`.
- È possibile eseguire il rollback del processo solo mediante l'applicazione Promotion Management. Non è disponibile alcun supporto della riga di comando per il rollback dei processi.

16.5.4 File delle proprietà di esempio

Quello che segue è un file delle proprietà di esempio:

Esempio:

```
importLocation=C:/Backup/CR.lcmbiar
action=promote
LCM_CMS=<nome CMS:numero porta>
LCM_userName=<nomeutente>
LCM_password=<password>
LCM_authentication=<autenticazione>
LCM_systemID=<ID>
LCM_clientID=<ID client>
Destination_CMS=<nome CMS:numero porta>
Destination_userName=<nomeutente>
Destination_password=<password>
Destination_authentication=<autenticazione>
Destination_systemID=<ID>
Destination_clientID=<ID client>
lcmbiarpassword=<password>
```

Nota:

se il file delle proprietà non contiene informazioni personali, la CLI dell'LCM richiederà lo stesso file nella console.

16.6 Utilizzo di Enhanced Change and Transport System

Change and Transport System (CTS) consente di organizzare e personalizzare i progetti di sviluppo in ABAP Workbench, quindi di trasportare le modifiche tra i sistemi SAP presenti nel System Landscape. Enhanced Change and Transport System (CTS+) è un componente aggiuntivo di CTS che consente la promozione dei contenuti ABAP nei repository non ABAP abilitati per CTS+.

Gli infobject della piattaforma BI possono utilizzare il contenuto SAP Business Warehouse come origine dati. L'integrazione di CTS+ con lo strumento Promotion Management consente di gestire il repository della piattaforma BI in modo analogo al repository SAP Business Warehouse (BW), utilizzando le richieste di trasporto CTS per promuovere i processi. CTS+ consente di trasportare oggetti non SAP

in un ambiente di sistema. Ad esempio, gli oggetti creati nel sistema di sviluppo possono essere allegati a una richiesta di trasporto e inoltrati ad altri sistemi dell'ambiente.

Per ulteriori informazioni su Change and Transport System, vedere http://help.sap.com/saphelp_nw70ehp1/helpdata/en/3b/dfba3692dc635ce10000009b38f839/frameset.htm

Per ulteriori informazioni su CTS+ e il trasporto di contenuti non ABAP, vedere http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bb/6fab6036a146baa58e42fac032ab7b/frameset.htm

16.6.1 Prerequisiti

Di seguito vengono elencati i prerequisiti per il trasporto di contenuto Business Intelligence da un sistema all'altro tramite CTS+:

1. La piattaforma SAP BusinessObjects Business Intelligence 4.0 (piattaforma BI) è installata.
2. SAP Solution Manager 7.1 o SAP Solution Manager 7.0 EHP1 (a partire da SP25) è installato e utilizzato come controller di dominio per CTS+, almeno per la configurazione dei sistemi SAP BusinessObjects.

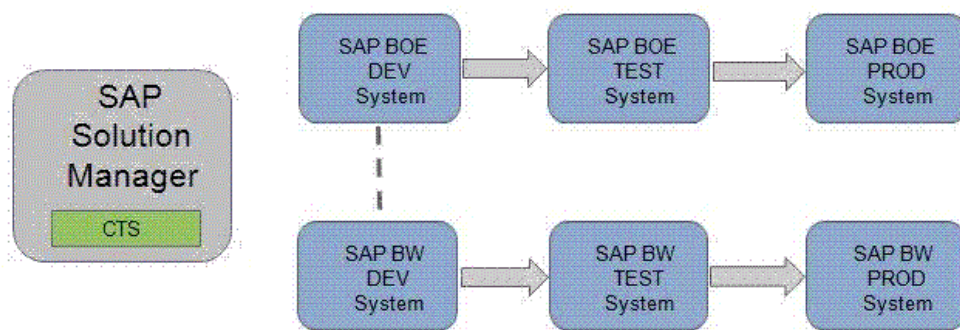
Per ulteriori informazioni sulla configurazione del dominio di trasporto, vedere http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a0a77acc11d1899e0000e829fbbd/frameset.htm

3. Il plug-in CTS è installato in SAP Solution Manager (il plug-in CTS è estratto dal SL Toolset 1.0 SP02. Si consiglia di utilizzare il plug-in CTS più recente disponibile).

Per ulteriori informazioni sull'installazione del plug-in CTS richiesto, vedere la Nota SAP: <https://service.sap.com/sap/support/notes/1533059>

4. Sistemi *SAP Business Warehouse 7.0* (SPS 24 o successivo) installati. Per ulteriori informazioni, consultare la nota SAP <https://service.sap.com/sap/support/notes/1369301>
5. L'ambiente di trasporto di SAP Business Warehouse (SAP BW) è configurato in Change and Transport System (CTS).

16.6.2 Per configurare la piattaforma BI e l'integrazione con CTS+



Transport Management System (TMS), che fa parte di Change and Transport System, consente di trasportare le modifiche tra sistemi SAP all'interno di un ambiente. Gestisce i sistemi connessi, i relativi percorsi e le importazioni nei sistemi. Per ulteriori informazioni su Transport Management System, consultare http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a0137acc11d1899e0000e829fbbd/frameset.htm

CTS+ consente la raccolta di file dall'esterno e la distribuzione degli stessi in un ambiente di trasporto. L'interfaccia utente Web di Transport Organizer, che fa parte di CTS+, gestisce le richieste di trasporto e gli oggetti in esse contenuti. Per ulteriori informazioni consultare http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a0137acc11d1899e0000e829fbbd/frameset.htm.

È possibile integrare Promotion Management della piattaforma BI con CTS+ e SAP BW utilizzando le richieste di trasporto CTS.

Nota:

per consentire l'integrazione della piattaforma BI con SAP Solution Manager, è necessario definire il tipo di applicazione "BOLM" nell'ambiente SAP Solution Manager.

Per integrare la piattaforma BI e CTS+, effettuare le seguenti operazioni:

1. Attivare il servizio Web di esportazione CTS.
2. Configurare le impostazioni CTS nello strumento Promotion Management.
3. Configurare il sistema di importazione della piattaforma BI in SAP Solution Manager.

Argomenti correlati

- [Per attivare il servizio Web di esportazione CTS](#)
- [Per configurare le impostazioni CTS+ nello strumento Promotion Management](#)
- [Per configurare la piattaforma BI e l'integrazione con CTS+](#)

16.6.2.1 Per attivare il servizio Web di esportazione CTS

Per configurare il sistema della piattaforma BI, è necessario attivare il servizio Web di esportazione CTS nello strumento Web SOA Management.

1. Per avviare l'applicazione, immettere il codice di transazione SOAMANAGER in SAP Solution Manager.

Per ulteriori informazioni su SOA Management e sulla configurazione di un endpoint di un servizio, fare riferimento a SAP Help Portal all'indirizzo: http://help.sap.com/saphelp_nw70ehp1/helpdata/en/33/06820d9d174c2884576bd78ac5629d/frameset.htm

Dopo aver completato l'autenticazione richiesta, la console di SOA Management si apre in un browser Web.

2. Nella scheda **Service Administration** scegliere **Single Service Configuration**.

Il servizio Web di esportazione CTS viene denominato EXPORT_CTS_WS

3. Nella scheda **Configuration** creare o modificare l'endpoint del servizio.
4. Nella scheda **Security** configurare il protocollo di trasporto e il metodo di autenticazione.
5. Nella scheda **Transport Settings** definire l'URL di accesso alternativo per un accesso agevole dell'endpoint del servizio.

16.6.2.2 Per configurare le impostazioni CTS+ nello strumento Promotion Management

Nella sezione che segue viene illustrata la procedura di configurazione da eseguire nell'applicazione CMC in ciascun sistema per impostare CTS+ per l'utilizzo con lo strumento Promotion Management.

1. Nella pagina "Processi di promozione", fare clic su **Impostazioni CTS** e quindi su **Sistemi BW**.
2. Nella pagina "Sistemi BW" fare clic su **Aggiungi** per aggiungere un sistema BW all'ambiente.
3. Nella pagina "Aggiungi sistema" inserire i dettagli seguenti:
 - **SID BW host** : specificare l'ID sistema (SID) del computer SAP BW/ABAP host.
 - **Nome host**: specificare l'indirizzo IP del computer host.
 - **Numero sistema**: inserire il numero di sistema del sistema host.
 - **Client**: si riferisce ai dettagli di sistema del computer client.
 - **Utente e Password**: specificare il nome utente e la password del computer client in questi campi.
 - **Lingua**: specificare la lingua scelta in questo campo.
4. Fare clic su **Salva** per aggiungere il sistema all'ambiente.

Nota:

Dopo aver aggiunto un sistema BW all'ambiente, è possibile utilizzare **Modifica** o **Elimina** nella pagina "Sistemi BW" per modificare i sistemi dell'ambiente.

5. Nella pagina "Processi di promozione" fare clic su **Impostazioni CTS**, quindi su **Impostazioni servizio Web**.
6. Nella pagina "Impostazioni servizio Web" inserire l'URL del servizio Web e i dettagli utente.

Nota:

Se non si conoscono tali dettagli, rivolgersi all'amministratore di Solution Manager per richiederli.

7. Fare clic su **Salva e Chiudi** per completare l'aggiunta di impostazioni del servizio Web.

8. Creare a un file di mappatura sul servizio di origine BI.

Completare i passaggi che seguono nel sistema di sviluppo della piattaforma BI per creare un file di testo con dettagli sulla connettività per abilitare la mappatura:

- a. Nel CMS di Promotion Management della piattaforma BI accedere alla directory principale e creare una cartella con il nome LCM nel percorso <percorsoinstallazionepiattaformaSAP BusinessObjects Business Intelligence>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/
- b. Creare un file di testo denominato LCM_SOURCE_CMS_SID_MAPPING.properties e immettere uno dei seguenti elementi nel file:
 - <nome completo del sistema di origine della piattaforma SAP BusinessObjects Business Intelligence con dominio>@<numero porta CMS> = <nome logico per sistema di origine utilizzato nella configurazione del CTS>
 - <numero IP del sistema di origine della piattaforma SAP BusinessObjects Business Intelligence>@<numero porta CMS> = <nome logico per sistema di origine utilizzato nella configurazione del CTS>

Ad esempio:

DEWDFTH04171S@6400=WJ3

10.208.112.177@6400=WJ3

DEWDFTH04171S.pgdev.sap.corp@6400=WJ3

Nota:

Nel caso di un ambiente cluster copiare i file LCM_SOURCE_CMS_SID_MAPPING.properties e LCM_SID_RFC_MAPPING.properties sul sistema in cui è in esecuzione Adaptive Processing Server.

Per ulteriori informazioni sull'esecuzione delle procedure di configurazione per sistemi non ABAP, consultare http://help.sap.com/saphelp_nw70/helpdata/en/d4/3bab83106941f08ad1f2e1ec14375e/fra/meset.htm

16.6.2.3 Per configurare il sistema di importazione della piattaforma BI in SAP Solution Manager.

1. Accedere al sistema SAP Solution Manager.
2. Immettere la transazione **stms** e premere **Invio**.
3. Configurare BOLM come tipo di applicazione.
 - a. Passare a **Overview > Systems**.
 - b. Passare a **Extras > Application Type > Configure**.

- c. Scegliere **New Entries**.
 - d. Nel campo **Application Type** immettere BOLM.
 - e. Immettere la descrizione.
 - f. Nel campo **Support Details** immettere <http://service.sap.com> (ACH: BOJ-BIP-DEP)
 - g. Scegliere **Table View > Save**.
 - h. Confermare la richiesta scegliendo **Yes**.
4. Per utilizzare diverse lingue, è possibile utilizzare del testo tradotto nel modo seguente:
- a. Scegliere **Goto > Translation**.
 - b. Selezionare le lingue in cui si desidera tradurre il testo.
 - c. Immettere i valori tradotti nei campi **Description** e **Support Details**.
 - d. Confermare la scelta nella finestra di dialogo.
 - e. Scegliere **Continue**.
 - f. Scegliere **Table View > Save**.
 - g. Confermare il prompt.

Il dominio TMS è ora pronto a supportare l'utilizzo del contenuto BI in CTS.

5. In CTS+, definire il sistema della piattaforma BI di origine come sistema di esportazione.

Nota:

Per ulteriori informazioni sulla creazione di un sistema non ABAP come sistema di origine, consultare http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2f1abeeaf4f8e4/frameset.htm (http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2f1abeeaf4f8e4/frameset.htm)

6. In CTS+, configurare il sistema di importazione della piattaforma BI completando la procedura seguente:

Nota:

È possibile definire un SID come riferimento al sistema di importazione della piattaforma BI.

- a. Creare un sistema non ABAP come sistema di importazione.
Per ulteriori informazioni consultare http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2f1abeeaf4f8e4/frameset.htm (http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2f1abeeaf4f8e4/frameset.htm).
- b. Impostare il metodo di distribuzione su **Others** e deselezionare tutte le altre opzioni.
- c. Scegliere **Salva**.
- d. Confermare la distribuzione nella finestra di dialogo.
Viene mostrata la visualizzazione tabella per configurare le impostazioni del sistema di importazione.
- e. Scegliere **Edit > New Entries**.
- f. Nella schermata "Change View CTS: System details for handling of application types" procedere come segue:
 - 1. Nel campo **Deploy Method** selezionare **application specific Deployer (EJB)**.
 - 2. Nel campo **Deploy URI** immettere l'URI seguente: `http://<BOE (http://%3cboe/) nome server web>:<porta server Web>/BOE/LCM/CTSServlet?&cmsName=<nome destinazione BOE>:<CMSport>&authType=<tipo di autenticazione BOE>`

dove

- "nome server Web BOE" è il nome o l'indirizzo IP del computer in cui è in esecuzione il server Web della piattaforma BI.
- "porta server Web" è il numero di porta del server di applicazioni della piattaforma BI.
- "nome destinazione BOE" è il nome del computer in cui è in esecuzione Central Management Server (CMS) della piattaforma BI.
- "porta CMS" è il numero della porta del CMS.
- "tipo autenticazione BOE" è il tipo di autenticazione utente utilizzato per l'importazione di contenuto BI. I tipi di autenticazione supportati sono secEnterprise, secLDAP, secWinAD e secSAPR3.

3. Nel campo **User** immettere il nome utente per la piattaforma BI.
4. Nel campo **Password** immettere la password per la piattaforma BI.
5. Scegliere **Save** per salvare le impostazioni.

Se è necessario più di un sistema di importazione, ripetere i passaggi precedenti per creare tutti i sistemi di destinazione richiesti. Per configurare i percorsi di trasporto tra il sistema di origine e di destinazione dopo la creazione dei sistemi di destinazione, consultare http://help.sap.com/sa/phelp_nw70ehp1/helpdata/en/44/b4a1df7acc11d1899e0000e829fbbd/frameset.htm

16.6.2.4 Per eseguire l'esportazione dalla piattaforma BI a CTS+

16.6.2.4.1 Per configurare SSL per CTS+

Per configurare SSL per CTS+, è necessario configurare SSL nel sistema ABAP del server delle applicazioni.

Promemoria:

Verificare che sia installata la libreria di crittografia SAP nel server delle applicazioni

1. Utilizzare il codice di transazione rz10, quindi configurare il parametro di "profilo" per l'utilizzo di SSL.

- a. Aggiungere i parametri seguenti al profilo di istanza SM1_DVWEBMGS00_PAPGVMWIN044:

```
ssf/name=SAPSECULIB
# HTTPS port
icm/server_port_1=PROT=HTTPS,PORT=8443,TIMEOUT=30,PROCTIMEOUT=600
# 0: Do not use certificates 1: Allow certificates (default) 2: Require certificates
icm/HTTPS/verify_client=1
```

2. Se non esiste già un PSE per il server SSL, crearne uno dalla riga di comando.

- a. Impostare la variabile SECUDIR:

```
set SECUDIR=D:\usr\sap\SM1\DVEBMGS00\sec
```

- b. Eseguire `sapgenpse` utilizzando i parametri seguenti:

```
sapgenpse get_pse -p SAPSSLS.pse
```

Nota:

Non specificare un PIN e utilizzare il nome di dominio completo del server delle applicazioni come nome comune (CN) nel nome distinto (DN).

Promemoria:

Verificare che l'utente del sistema operativo che esegue ICM disponga delle autorizzazioni in lettura per PSE.

3. Inviare la richiesta di certificato a un'autorità di certificazione (CA).
 - a. Selezionare SAPNetCA PKCS#7 come CA e `certify the cert. req.` come comando.
 - b. Allegare la richiesta di certificato.
 - c. Salvare la risposta alla richiesta di certificato in un file, ad esempio `smlsslcert.crt`.

4. Importare la risposta alla richiesta di certificato nel PSE del server SSL utilizzando i parametri seguenti:

```
sapgenpse import_own_cert -c smlsslcert.crt -p SAPSSLS.pse
```

5. Utilizzare il codice di transazione `smicm` e fare clic su **Administration > ICM > Exit Soft > Global** per riavviare ICM.

Nota:

È possibile anche utilizzare SAP MMC per riavviare l'intero sistema SM1.

6. Utilizzare la scheda "ICM Monitor - Service Display" per verificare che il servizio HTTPS sia in esecuzione su ICM.
7. Verificare la connessione SSL.

16.6.2.4.2 Per configurare il certificato SSL del lato client

Per configurare il certificato SSL lato client, è necessario importare il certificato server o il certificato CA attendibile nell'archivio chiavi JVM.

1. Eseguire il backup dei file `cacerts` dalla directory `<DIRINSTALL>\win64_x64\sapjvm\jre\lib\security`.
2. Importare il certificato SAPNetCA nella JVM Tomcat che ospita il file `BOE.war` utilizzando i parametri seguenti:

```
<INSTALLDIR>\win64_x64\sapjvm\jre\bin\keytool.exe -import -file SAPNetCA.cer -keystore cacerts
```

Nota:

È possibile scaricare il certificato SAPNetCA dall'archivio CA attendibile SAP. La password predefinita dell'archivio chiavi è `changeit`.

3. Riavviare Tomcat.

16.6.2.4.3 Per configurare il servizio Web di esportazione CTS+

Per configurare il servizio Web di esportazione CTS+ (`EXPORT_CTS_WS`) è necessario creare un nuovo endpoint HTTPS.

1. Utilizzare il codice di transazione soamanager e, nella scheda "Provider Security", in "Communication Security", selezionare **SSL over HTTP (Transport Channel Security)** e in "Transport Channel Authentication" selezionare **User ID/Password**.
2. Nella scheda "Transport settings", in "Transport Binding", selezionare **HTTPS** per "Calculated Protocol".

16.6.2.4.4 Per configurare la funzionalità di gestione della promozione per SSL

Promemoria:

Importare il certificato server o la certificazione CA attendibile nell'archivio chiavi JVM.

1. Nella CMC, nella scheda "Promotion Management", fare clic su **Impostazioni > Impostazioni CTS > Impostazioni servizio Web**.
2. Verificare che il parametro "URL servizio Web" includa `https://`

Nota:

Se non è possibile accedere all'URL specificato, **Promote via CTS** non verrà visualizzato nel menu **Job destination** o nella finestra "Overrides". Se l'handshake SSL tra la gestione delle promozioni e CTS+ non riesce, verrà visualizzato un errore.

16.6.2.5 Per eseguire l'importazione da CTS+ alla piattaforma BI

16.6.2.5.1 Per configurare CTS+ per SSL

Per configurare CTS+ per SSL, è necessario creare un PSE del server SSL e importarvi un certificato CA SAP. Per ulteriori informazioni, vedere "Per configurare SSL per CTS+".

Nota:

Se il PSE del client SSL non esiste, per impostazione predefinita viene utilizzato il PSE del server SSL.

Argomenti correlati

- [Per configurare SSL per CTS+](#)

16.6.2.5.2 Per configurare il componente Tomcat nella piattaforma BI per l'uso di HTTPS

Per configurare Tomcat nella piattaforma BI per l'uso di HTTPS, è necessario eseguire la procedura seguente nel computer in cui è installata la piattaforma BI.

1. Creare una coppia di chiavi del server, un certificato e un archivio chiavi.

- a. Eseguire `<DIRINSTALL>\win64_x64\sapjvm\jre\bin\keytool.exe` con i parametri seguenti:

```
keytool -genkey -alias server -keyalg RSA -keysize 1024 -keystore serverkeystore.jks -storetype JKS
keytool -certreq -keyalg RSA -alias server -file server.csr -keystore serverkeystore.jks
```

- b. Quando viene richiesto, immettere le informazioni seguenti:

- Nome e cognome
- Nome dell'unità organizzativa di appartenenza
- Nome dell'organizzazione
- Città o località
- Stato
- Codice paese a due lettere relativo all'unità

Verrà visualizzata una stringa formattata (ad esempio, CN=John Smith, OU=Accounting, O=SAP, L=Vancouver, ST=BC, C=CA). Digitare **yes** e premere **Invio** per confermare.

2. Inviare la richiesta di certificato server a un'autorità di certificazione (CA). Per ulteriori informazioni, vedere "Per configurare SSL per CTS+".
3. Importare il certificato server con firma nell'archivio chiavi del server utilizzando i parametri seguenti:

```
keytool -import -alias server -keystore serverkeystore.jks -trustcacerts -file server.crt
```

4. Configurare il file di configurazione Tomcat `server.xml` per abilitare HTTPS e per l'uso dell'archivio chiavi del server creato.
5. Riavviare Tomcat e verificare la connessione accedendo all'URL seguente in un browser:
`https://<NOMESERVER>:8443`

Argomenti correlati

- [Per configurare SSL per CTS+](#)

16.6.2.5.3 Per aggiornare i sistemi di test e di produzione per l'uso di HTTPS

Per abilitare HTTPS nei sistemi di test e di produzione, nella visualizzazione "CTS: System details for handling of application types" di CTS+ verificare che il parametro "Deploy URI" includa `https://`

16.6.3 Per promuovere un processo utilizzando CTS

In questa sezione viene illustrato il workflow supportato dall'applicazione Promotion Management per la promozione degli oggetti CMS (Central Management Server) della piattaforma BI dal sistema di origine al sistema di destinazione mediante il sistema CTS (Change Transport System). Per utilizzare CTS per promuovere un processo, attenersi alla seguente procedura:

1. Avviare l'applicazione Promotion Management utilizzando l'autenticazione SAP e creare un processo.
Per ulteriori informazioni sulla creazione di un nuovo processo, vedere la sezione "Creazione di un nuovo processo" nei collegamenti correlati riportati più avanti.

Nota:

accertarsi di selezionare "SAP" come tipo di autenticazione nella schermata di accesso del sistema di origine.

2. Dall'elenco a discesa **Destinazione** selezionare l'opzione **Promuovi con**

The screenshot shows a web-based form. At the top, there is a label 'Destination:' followed by a dropdown menu. The dropdown menu is open, showing 'Promote via CTS' as the selected option. Below the dropdown, there are two buttons: 'Create' and 'Cancel'.

CTS+.

3. Fare clic su **Crea**.

Viene visualizzata la schermata "Aggiungi oggetti dal sistema". Le cartelle e le sottocartelle vengono visualizzate in una struttura ad albero.

4. Passare alla cartella dalla quale si desidera selezionare l'infoobject.
5. Selezionare l'infoobject da aggiungere al processo e fare clic su **Aggiungi**. Se si desidera aggiungere un infoobject e uscire dalla schermata "Aggiungi oggetti", fare clic su **Aggiungi e chiudi**. L'infoobject viene aggiunto al processo e viene visualizzata la schermata "Processi di promozione".

Nota:

nella scheda Processi di promozione possono essere eseguite le seguenti operazioni:

- Utilizzare l'opzione **Aggiungi oggetti** per aggiungere altri infoobject al processo. Per ulteriori informazioni, consultare Aggiunta di un infoobject a un processo.
- Utilizzare l'opzione **Gestisci dipendenze** per gestire le dipendenze dell'infoobject selezionato. Le dipendenze SAP BW dell'oggetto verranno visualizzate nell'interfaccia utente e potranno essere selezionate dall'utente.

Per ulteriori informazioni, consultare Gestione delle dipendenze di un processo.

6. Fare clic su **Promuovi**.

Viene visualizzata la schermata "Promuovi" in cui sono mostrati l'ID, il proprietario e una breve descrizione della richiesta di trasporto predefinita attualmente impostata.

7. È possibile utilizzare il collegamento ipertestuale **Richieste di trasporto** per eseguire le operazioni seguenti:
 - Visualizzare i dettagli della richiesta di trasporto.
 - Modificare le impostazioni della richiesta di trasporto predefinita.
 - Scegliere una richiesta di trasporto diversa.
 - Creare una richiesta di trasporto.
- a. Fare clic sul collegamento ipertestuale **Richieste di trasporto** per aprire l'interfaccia utente Web di "Transport Organizer".
- b. Se viene richiesto di fornire le credenziali di accesso, utilizzare credenziali utente valide per il sistema del controller di dominio CTS.
- c. Aggiornare la schermata "Promuovi" per visualizzare gli aggiornamenti.

Per ulteriori informazioni sull'interfaccia utente Web di "Transport Organizer", consultare http://help.sap.com/saphelp_nw70ehp1/helpdata/en/b5/6d03660d3745938cd46d6f5f9cef2e/frame set.htm

8. Per visualizzare i dettagli relativi alle dipendenze degli oggetti SAP BW, fare clic sul collegamento ipertestuale **Dipendenze di secondo livello**.

Nota:

quando si fa clic sul collegamento ipertestuale **Dipendenze di secondo livello** vengono visualizzati solo gli oggetti bloccati in una richiesta. Se la richiesta è stata rilasciata, non è possibile visualizzarne le dipendenze. Questo collegamento ipertestuale è inoltre disattivato se non sono presenti dipendenze di secondo livello.

9. Fare clic su **Promuovi**.

10. Chiudere il processo.

Viene visualizzata la schermata principale di Promotion Management. Lo stato del processo creato è ora **Esportato in CTS+**.

11. Rilasciare l'oggetto della piattaforma BI nel sistema di destinazione effettuando le operazioni seguenti:

- a. Fare clic sul collegamento visualizzato nella colonna di stato del processo da promuovere.
Viene visualizzata la finestra "Stato promozione".
- b. Fare clic sull'opzione **Stato della richiesta**.
Viene visualizzata l'interfaccia utente di "Transport Organizer".
- c. Se lo stato della richiesta è **Modifiable**, fare clic su **Release** per rilasciare la richiesta di trasporto dell'oggetto della piattaforma BI. Per ulteriori informazioni sul rilascio delle richieste di trasporto contenenti oggetti non ABAP, vedere http://help.sap.com/saphelp_nw70ehp1/helpdata/en/55/07c497db8140ef8176715d4728eec1/frameset.htm
- d. Chiudere l'interfaccia utente di "Transport Organizer".

12. Per visualizzare le dipendenze degli oggetti SAP BW, fare clic sul collegamento ipertestuale **Elenco di dipendenze BW**.

Nota:

è consigliabile consultare il team SAP BW per ottenere gli aggiornamenti delle dipendenze SAP BW e il rilascio di tali oggetti mentre vengono utilizzati dal team.

13. Chiudere la finestra "Stato promozione".

14. Importare l'oggetto della piattaforma BI nel sistema di destinazione effettuando le operazioni seguenti:

- a. Accedere al controller di dominio CTS+.
- b. Chiamare la transazione STMS per accedere al sistema di gestione dei trasporti.
- c. Fare clic sull'icona **Panoramica importazione**.
Viene visualizzata la schermata "Panoramica importazione" nella quale è possibile visualizzare le voci della coda di importazione di tutti i sistemi.
- d. Scegliere l'ID del sistema LCM di destinazione.
L'utente può visualizzare l'elenco di richieste di trasporto che è possibile importare nel sistema.
- e. Fare clic su **Aggiorna**.

- f. Importare le richieste di trasporto pertinenti. Per ulteriori informazioni consultare http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a39e7acc11d1899e0000e829fbbd/frameset.htm.

Per informazioni generali sull'importazione delle richieste di trasporto con contenuto BOLM, vedere http://help.sap.com/saphelp_nw70ehp1/helpdata/en/09/ca0f3a878f46e9a5a32e666131d2ba/frameset.htm

15. Se l'oggetto selezionato presenta dipendenze SAP BW, eseguire la procedura seguente:
- Rilasciare le dipendenze SAP BW nel sistema di destinazione effettuando le operazioni seguenti:
 - Accedere al sistema SAP BW.
 - Chiamare la transazione SE09. Viene visualizzata la schermata "Transport Organizer".
 - Fare clic su **Visualizza** per visualizzare la richiesta SAP BW.
 - Fare clic sulla richiesta SAP BW ed espanderla per visualizzare le attività create per le dipendenze.
 - Fare clic con il pulsante destro del mouse sulla richiesta associata all'oggetto SAP BW primario e selezionare **Rilascia direttamente**. Ripetere questo passaggio per rilasciare tutte le attività associate a ciascuna dipendenza separatamente.
 - Fare clic con il pulsante destro del mouse sulla richiesta associata all'oggetto BW primario e scegliere **Rilascia direttamente**.
 - Aggiornare la schermata finché non saranno state rilasciate tutte le richieste.

Nota:

è possibile visualizzare i registri di una richiesta facendo doppio clic su di essa.

- Importare le dipendenze SAP BW nel sistema di destinazione effettuando le operazioni seguenti:
 - Accedere al sistema SAP BW di destinazione.
 - Chiamare la transazione SIMS per accedere al sistema di gestione dei trasporti.
 - Fare clic sull'icona **Panoramica importazione**. Viene visualizzata la schermata "Panoramica importazione".
 - Fare doppio clic sull'ID del sistema SAP BW di destinazione. È possibile visualizzare l'elenco di richieste di trasporto che è possibile importare nel sistema.
 - Importare le richieste di trasporto pertinenti. Per ulteriori informazioni consultare http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a39e7acc11d1899e0000e829fbbd/frameset.htm.

Per ulteriori informazioni sul trasporto con le code di importazione, consultare http://help.sap.com/saphelp_nw70ehp1/helpdata/en/65/8a99386185c064e10000009b38f8cf/frameset.htm

16. Accedere al sistema di destinazione per visualizzare lo stato del processo promosso.

Per informazioni sulla documentazione in linea relativa al CTS generico, consultare http://help.sap.com/saphelp_ctsplug100/helpdata/en/52/700dbe608e4752a8e2e96a1876f865/frameset.htm

Argomenti correlati

- [Per creare un processo](#)
- [Per gestire le dipendenze di un processo](#)

Differenza visiva

17.1 Differenza visiva nello strumento Promotion Management

Differenza visiva consente di visualizzare le differenze tra due versioni di un tipo di file supportato (LCM BIAR) e/o di un tipo di oggetto supportato (Processo LCM). È possibile utilizzare questa funzionalità per determinare la differenza tra i file o gli oggetti al fine di sviluppare e gestire diversi tipi di report. Questa funzionalità fornisce uno stato del confronto tra le versioni di origine e quelle di destinazione. Ad esempio, se una versione precedente del report utente è accurata, a differenza della versione corrente, è possibile confrontare e analizzare il file per valutare l'entità esatta del problema.

Di seguito sono riportati i tre tipi di differenza visiva da cui è possibile esaminare un file o un oggetto:

- **Rimosso:** in un report, se un elemento manca in una delle versioni del file, il tipo di differenza indicato è Rimosso. Ad esempio, l'elemento può essere una riga, un'istanza di sezione o anche un blocco.
- **Modificato:** in un report, se è presente un valore differente tra la versione di origine e la versione di destinazione, il tipo di differenza indicato è Modificato. Ad esempio, il valore può essere il contenuto delle celle o il risultato di una variabile locale.
- **Inserito:** in un report, se un elemento è presente nella versione di destinazione ma non nella versione di origine, il tipo di differenza indicato è Inserito.

Di seguito sono riportati i tipi di oggetto che supportano la differenza visiva:

- LCMBIAR
- Processo LCM

È possibile eseguire il confronto delle seguenti combinazioni:

- Processo LCM con un altro processo LCM
- Processo LCM con un file LCMBIAR
- File LCMBIAR con un altro file LCMBIAR
- File LCMBIAR con un processo LCM

Preferenze

Nella pagina iniziale della differenza visiva, è possibile impostare preferenze quali impostazioni internazionali dei prodotti, impostazioni internazionali di visualizzazione, numero massimo di oggetti per pagina, fuso orario e prompt per i dati non salvati.

Pagina iniziale

La pagina iniziale della funzione di differenza visiva è costituita dai seguenti riquadri e tabelle:

- **Nuovo confronto:** questa scheda consente di creare un nuovo confronto tra oggetti

- Cerca confronti: questo campo consente di cercare gli oggetti già confrontati
- Confronti: questo riquadro contiene le schede di filtri e differenze
- Confronti: Differenze: in questo riquadro sono riportati gli oggetti confrontati con il nome del confronto, la data e l'ora, lo stato delle differenze

17.1.1 Confronto di oggetti o file mediante la differenza visiva

L'opzione Differenza visiva consente di confrontare i file e gli oggetti BIAR.

Per confrontare i file utilizzando la differenza visiva, completare la procedura seguente:

1. Accedere all'applicazione CMC.
2. Nella home page di CMC, sotto la scheda "Gestisci", fare clic sul collegamento **Differenza visiva**. Viene visualizzata la pagina Differenza visiva. I file sottoposti a confronto vengono archiviati nella cartella "Differenze" o in una delle sottocartelle create dall'utente.

Nota:

Per creare una nuova sottocartella, fare clic sull'icona Cartella.

3. Fare clic su **Nuovo confronto**. Viene visualizzata la schermata "Confronti".
4. Selezionare il sistema di riferimento dall'elenco a discesa **Seleziona sistema** sotto Riferimento. È possibile connettersi a uno dei seguenti sistemi di riferimento:
 - CMS
 - VMS
 - File system locale
5. Fare clic su **Sfoglia** per selezionare l'oggetto o un file dal sistema locale per il confronto.
6. Selezionare il sistema di destinazione dall'elenco **Seleziona sistema** sotto Destinazione. È possibile connettersi a uno dei seguenti sistemi di riferimento:
 - CMS
 - VMS
 - File system locale

Nota:

Se si accede a CMS o VMS, l'oggetto selezionato nel sistema di riferimento può inoltre essere automaticamente associato a un oggetto con lo stesso nome nel sistema di riferimento.

7. Fare clic su **Sfoglia** per selezionare l'oggetto o un processo dal sistema locale per il confronto.
8. Fare clic su **Aggiungi**.

Gli oggetti selezionati per il confronto vengono aggiunti al carrello degli acquisti.

Se al carrello degli acquisti è stata aggiunta più di una coppia di oggetti, il confronto tra oggetti può essere pianificato per essere eseguito in un secondo momento. Tuttavia, se il carrello degli acquisti contiene solo una coppia di oggetti, è possibile eseguire subito il confronto.

Per confrontare i file, continuare con il passaggio successivo. Per pianificare il confronto, vedere [Pianificazione del confronto](#).

9. Fare clic sul pulsante **Confronta** per confrontare gli oggetti o le cartelle.

Nota:

Il confronto tra file di processo LCMBIAR/LCM include:

- Metadati LCMBIAR: confronto dei dettagli del processo come nome, autore, ora e così via.
- Oggetti principali: confronto di ogni oggetto selezionato in modo esplicito nel LCMBIAR con un oggetto simile nel LCMBIAR di destinazione in base al CUID.
- Oggetti dipendenti: confronto dell'oggetto dipendente selezionato nel file con un oggetto simile presente nella destinazione in base al CUID.

Se sono selezionati oggetti diversi dai processi LCMBIAR o LCM, viene visualizzato il seguente messaggio di errore: `Plug-in non trovato`.

Il processo di confronto inizia immediatamente e le eventuali differenze vengono visualizzate nel "visualizzatore Differenza visiva". Le differenze vengono evidenziate in arancione e gli oggetti mancanti vengono evidenziati in rosso.

È inoltre possibile utilizzare l'opzione di filtro per visualizzare gli oggetti confrontati in base al tipo, con le differenze o con gli attributi comuni.

10. Fare clic su **Salva** per salvare il report sulle differenze.
11. Specificare il percorso in cui si desidera salvare il report quindi fare clic su **OK**.

17.1.2 Confronto di oggetti o file nel sistema di gestione delle versioni

È possibile confrontare i processi o le cartelle di Promotion Management in un sistema di gestione delle versioni utilizzando la funzione di differenza visiva.

Per confrontare gli oggetti in un sistema di gestione delle versioni, completare i seguenti passaggi:

1. Accedere all'applicazione CMC.
2. Nella home page di CMC, sotto la scheda "Gestisci", fare clic sul collegamento **Differenza visiva**.

Viene visualizzata la pagina Differenza visiva. I file sottoposti a confronto vengono archiviati nella cartella "Differenze" o in una delle sottocartelle create dall'utente.

Nota:

Per creare una nuova sottocartella, fare clic sull'icona Cartella.

3. Fare clic su **Nuovo confronto**.

Viene visualizzata la schermata "Confronti".

4. Selezionare **Accedi al sistema di gestione delle versioni** da **Seleziona sistema** in Riferimento.
5. Immettere le credenziali di accesso al sistema di gestione delle versioni e fare clic su **Accedi**.

Viene visualizzata la finestra di dialogo "Selezione automatica sistema di destinazione"

6. Fare clic su **No** se si desidera impostare un sistema di destinazione diverso oppure su **Sì** se si desidera impostare il nome del sistema di destinazione come sistema di riferimento.
7. Fare clic sul pulsante **Sfoglia** per selezionare gli oggetti o i processi che si desidera confrontare sia dai sistemi di riferimento che dai sistemi di destinazione.
8. Fare clic su **Aggiungi**.

Gli oggetti selezionati per il confronto vengono elencati nel riquadro Nuovo confronto.

È possibile confrontare subito i file oppure pianificare il confronto per un momento successivo. Per confrontare i file, continuare con il passaggio successivo. Per pianificare il confronto, vedere [Pianificazione del confronto](#).

9. Fare clic sul pulsante **Confronta** per confrontare i processi o le cartelle.

Il processo di confronto inizia immediatamente e le eventuali differenze vengono visualizzate nel "visualizzatore Differenza visiva". Le differenze vengono evidenziate in arancione e gli oggetti mancanti vengono evidenziati in rosso.

È inoltre possibile utilizzare l'opzione di filtro per visualizzare gli oggetti confrontati in base al tipo, con le differenze o con gli attributi comuni.

10. Fare clic su **Salva** per salvare il report sulle differenze.
11. Specificare il percorso in cui si desidera salvare il report quindi fare clic su **OK**.

17.1.3 Pianificazione del confronto

Per pianificare il confronto di file o oggetti, completare la procedura seguente:

1. Fare clic su **Pianifica**.
Viene visualizzata la finestra di dialogo "Pianifica".
2. Selezionare la frequenza per pianificare il confronto dall'elenco a discesa **Esegui confronto**.
3. Specificare il numero di tentativi consentiti e l'intervallo tra i tentativi nei rispettivi campi.

Nota:

è possibile specificare l'intervallo tra i tentativi solo se si specifica il numero di tentativi.

4. Specificare il nome del report e fare clic su **Sfoglia** per selezionare la posizione in cui si desidera salvare il report.
Viene visualizzata la finestra "Salva processo in".
5. Selezionare la cartella in cui si desidera salvare il report e fare clic su **OK**.

Nota:

In base all'opzione selezionata dall'elenco **Esegui confronto**, è necessario specificare la data e l'ora per il confronto.

6. Fare clic su **Pianifica**.

L'utente può visualizzare l'oggetto del confronto o il report sulle differenze nel visualizzatore della differenza visiva in una fase successiva. Viene aperta la pagina "Confrontato: Differenze" con l'elenco delle cartelle e dei file o i report sul confronto.

La pagina contiene anche le seguenti opzioni:

- **Cronologia:** l'opzione **Cronologia** consente di visualizzare la cronologia del confronto.
- **Riesegui:** l'opzione **Riesegui** consente di eseguire di nuovo il confronto.
- **Pianifica:** l'opzione **Pianifica** consente di pianificare il confronto.

Gestione delle applicazioni

18.1 Gestione delle applicazioni mediante CMC

18.1.1 Panoramica

L'area di gestione "Applicazioni" della console CMC consente di cambiare l'aspetto e la funzionalità delle applicazioni Web, ad esempio la console CMC e BI Launch Pad, senza eseguire operazioni di programmazione. È inoltre possibile modificare l'accesso alle applicazioni per utenti, gruppi e amministratori modificando i diritti associati a ognuno.

In questa sezione sono disponibili informazioni contestuali, procedure e istruzioni relative alla gestione di varie impostazioni. Le seguenti applicazioni presentano impostazioni che possono essere modificate tramite la CMC:

- SAP BusinessObjects Analysis versione per OLAP
- Applicazione di gestione degli avvisi
- BI Launch Pad
- Spazi di lavoro BI
- Central Management Console
- Collaborazione (con SAP Jam o SAP StreamWork)
- Configurazione Crystal Reports
- Cruscotti
- Discussioni
- Information Designer
- Applicazione di monitoraggio
- Multi-tenancy
- OpenDocument
- Applicazione di ricerca piattaforma
- Promotion Management
- Strumento di conversione dei report
- SAP BusinessObjects Mobile
- Translation Management Tool
- Universe Design Tool

- Upgrade Management Tool
- Differenza visiva
- Web Intelligence
- Servizio Web
- Widget

18.1.2 Impostazioni comuni per le applicazioni

18.1.2.1 Impostazione dei diritti sulle applicazioni

È possibile utilizzare i diritti per controllare l'accesso utente a determinate funzionalità delle applicazioni. L'area "Applicazioni" della CMC consente di assegnare principali all'elenco di controllo dell'accesso per un'applicazione, visualizzare i diritti di un principale e modificare i diritti di un principale per un'applicazione. Per ulteriori informazioni sull'amministrazione dei diritti, consultare il *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

18.1.2.2 Impostazione del livello del registro di analisi delle applicazioni Web nella CMC

Per analizzare altre applicazioni Web, è necessario configurare manualmente il file `BO_trace.ini` corrispondente.

1. Nell'area "Applicazioni" della CMC, fare clic con il pulsante destro del mouse su un'applicazione e scegliere **Impostazioni registro di analisi**.

Nota:

Queste applicazioni includono impostazioni del registro di analisi: BI Launch Pad, CMC, Open Document, Promotion Management, Gestione delle versioni, Differenza visiva e Servizio Web.

Viene visualizzata la finestra di dialogo "Impostazioni registro di analisi".

2. Selezionare un'impostazione nell'elenco **Livello di registrazione**.
3. Fare clic su **Salva e chiudi**.

Il nuovo livello del registro di analisi sarà effettivo al successivo accesso all'applicazione Web.

Argomenti correlati

- [Livelli del registro di analisi](#)

18.1.2.2.1 Livelli del registro di analisi

Per i componenti della piattaforma BI sono disponibili i livelli del registro di analisi seguenti:

Livello	Descrizione
Non specificato	Il livello del registro di analisi viene specificato mediante altri meccanismi, in genere un file con estensione <code>ini</code> .
Nessuno	L'analisi non viene eseguita.
Basso	Il filtro del registro di analisi consente di registrare i messaggi di errore ignorando nel contempo i messaggi di avviso e di stato. Vengono registrati messaggi di stato importanti che si riferiscono a messaggi di richiesta di inizio e fine, di arresto e avvio dei componenti. l'impostazione di questo livello non è consigliata per le finalità di debug.
Medio	Il filtro del registro di analisi è impostato in modo da includere i messaggi di errore, avviso e la maggior parte dei messaggi di stato. I messaggi di stato meno importanti o eccessivamente dettagliati vengono esclusi. Questo livello non è sufficientemente dettagliato per le finalità di debug.
Alto	Non viene escluso alcun messaggio. L'impostazione di questo livello è consigliata per le finalità di debug. Avvertenza: Questo livello del registro di analisi influisce in modo significativo sulle risorse di sistema, sull'aumento dell'utilizzo della CPU e sull'impiego della spazio di archiviazione.

18.1.3 Impostazioni specifiche dell'applicazione

18.1.3.1 Gestione delle impostazioni dell'applicazione CMC

18.1.3.1.1 Autenticazione e oggetti programma

L'aggiunta di oggetti programma al repository può comportare rischi alla protezione potenziale di cui è necessario tenere conto. Il livello di autorizzazioni file per l'account con cui viene eseguito un oggetto programma determinerà le modifiche che il programma può apportare ai file, nel caso siano necessarie.

È possibile controllare i tipi di oggetti programma eseguibili dagli utenti e configurare le credenziali necessarie per eseguire tali oggetti.

Abilitazione o disabilitazione di un tipo di oggetto programma

Come primo livello di protezione è possibile configurare i tipi di oggetti programma utilizzabili.

Autenticazione su tutte le piattaforme

Nell'area di gestione "Cartelle" della CMC, è necessario specificare le credenziali per l'account con cui eseguire il programma. Questa funzionalità consente di impostare uno specifico account utente per il programma, a cui assegnare i diritti appropriati, all'interno del quale rendere possibile l'esecuzione dell'oggetto programma.

In alternativa, gli utenti che aggiungono oggetti programma alla piattaforma BI possono assegnare le proprie credenziali a un oggetto programma per concedere a quest'ultimo l'accesso al sistema. In questo modo, il programma verrà eseguito con l'account utente specificato e i suoi diritti saranno limitati a quelli dell'utente. Se si sceglie di non specificare un account utente per un oggetto programma, l'oggetto verrà eseguito con l'account di sistema predefinito, che, in genere, possiede diritti locali ma non per la rete.

Nota:

per impostazione predefinita, quando si pianifica un oggetto programma, il processo ha esito negativo se non vengono specificate le credenziali. Per fornire le credenziali predefinite, selezionare **CMC** nell'area di gestione "Applicazioni". Selezionare **Azioni > Diritti oggetto programma**, selezionare **Pianifica con le seguenti credenziali del sistema operativo** e immettere un nome utente e una password predefiniti.

Autenticazione per programmi Java

La piattaforma BI consente di impostare la protezione per tutti gli oggetti programma. Per i programmi Java, la piattaforma BI impone l'utilizzo di un file dei criteri Java, che ha un'impostazione predefinita coerente con l'impostazione predefinita Java per il codice non protetto. Utilizzare lo strumento dei criteri Java (disponibile nel Java Development Kit) per modificare il file dei criteri Java e adeguarlo ad esigenze specifiche.

Lo strumento dei criteri Java ha due voci di base di codice. La prima voce punta all'SDK Java della piattaforma BI e concede agli oggetti programma diritti completi per tutti i file JAR della piattaforma. La seconda voce di base di codice si applica a tutti i file locali. Utilizza le stesse impostazioni di protezione per il codice non sicuro delle impostazioni predefinite Java per lo stesso tipo di codice.

Nota:

- Le impostazioni dei criteri Java sono identiche per tutti gli Adaptive Job Server in esecuzione sullo stesso computer.
- Per impostazione predefinita, il file dei criteri Java viene installato nella directory dell'SDK Java all'interno della directory principale di installazione della piattaforma BI. Ad esempio, quello di seguito è un percorso tipico in Windows `C:\Programmi\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\conf\crystal-program.policy`.

Abilitazione o disabilitazione di un tipo di oggetto programma

1. Nell'area "Applicazioni" selezionare **Central Management Console**.

2. Scegliere **Azioni > Diritti oggetto programma**.

Verrà visualizzata la finestra di dialogo "Diritti oggetto programma".

3. Nell'area "Consenti agli utenti di", selezionare i tipi di oggetto programma che gli utenti devono essere in grado di eseguire.

È possibile selezionare **Eseguire script/binari** o **Eseguire programmi Java**.

Se si seleziona **Eseguire programmi Java**, è possibile selezionare o deselezionare la casella di controllo **Utilizzare la rappresentazione**. Questa opzione fornisce al programma Java un token con cui accedere alla piattaforma Business Intelligence.

4. Fare clic su **Salva e chiudi**.

18.1.3.1.2 Registrazione delle estensioni di elaborazione nel sistema

Nota:

Questa funzionalità non si applica ai documenti Web Intelligence.

Prima di poter applicare le estensioni di elaborazione a determinati oggetti, è necessario rendere disponibile la libreria di codice a ogni computer in cui verranno elaborate le richieste di pianificazione o di visualizzazione rilevanti. L'installazione della piattaforma BI crea una directory predefinita per le estensioni di elaborazione su ciascun Job Server, Processing Server e Report Application Server (RAS). Si consiglia di copiare le estensioni di elaborazione nella directory predefinita di ciascun server. In Windows, la directory predefinita è `C:\Programmi\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win32_x86\ProcessExt`. In UNIX, invece, la directory è `sap_bobj/ProcessExt`.

Suggerimento:

è possibile condividere un file di estensioni di elaborazione.

A seconda della funzionalità inserita nell'estensione, copiare la libreria nei seguenti computer:

- Se l'estensione di elaborazione intercetta solo richieste di pianificazione, copiare la libreria su ciascun computer in esecuzione come Adaptive Job Server.
- Se l'estensione di elaborazione intercetta solo le richieste di visualizzazione, copiare la libreria su ogni computer in esecuzione come Server di elaborazione Crystal Reports o RAS.
- Se l'estensione di elaborazione intercetta le richieste di pianificazione e di visualizzazione, copiare la libreria su ogni computer in esecuzione come Adaptive Job Server, Server di elaborazione Crystal Reports o RAS.

Nota:

Se l'estensione di elaborazione è necessaria solo per le richieste di pianificazione/visualizzazione inviate a un particolare gruppo di server, è sufficiente copiare la libreria su ciascun server di elaborazione del gruppo.

Registrazione di un'estensione di elaborazione nel sistema

1. Accedere all'area di gestione "Applicazioni" della CMC (Central Management Console).
2. Selezionare **Central Management Console**.

3. Scegliere Azioni > Estensioni di elaborazione.

Viene visualizzata la finestra di dialogo "Estensioni di elaborazione: CMC".

4. Nel campo Nome immettere un nome per la visualizzazione dell'estensione di elaborazione.**5. Nel campo Posizione digitare il nome file dell'estensione di elaborazione ed eventuali informazioni di percorso aggiuntive.**

- Se l'estensione di elaborazione è stata copiata nella directory predefinita su ciascuno dei computer appropriati, è sufficiente digitare il nome file senza l'estensione.
- Se l'estensione di elaborazione è stata copiata in una sottocartella della cartella principale, digitare il seguente percorso: `{sottocartella/nomefile}`

6. Il campo Descrizione consente di aggiungere informazioni sull'estensione di elaborazione.**7. Fare clic su Aggiungi.****Suggerimento:**

per eliminare un'estensione di elaborazione, selezionarla dall'elenco **Estensioni esistenti** e fare clic su **Elimina**. Verificare che nessun processo ricorrente sia basato su questa estensione di elaborazione, poiché tutti i processi futuri basati su di essa avranno esito negativo.

8. Fare clic su Salva e chiudi.

L'estensione di elaborazione viene registrata con la CMC.

A questo punto è possibile selezionare l'estensione di elaborazione per applicarne la logica a oggetti particolari.

*Condivisione delle estensioni di elaborazione tra più server***Nota:**

questa funzionalità non si applica ai documenti o ai report Web Intelligence creati in SAP Crystal Reports for Enterprise.

Per inserire tutte le estensioni di elaborazione in una singola posizione, è possibile eseguire l'override delle estensioni predefinite di elaborazione per ciascun Adaptive Job Server, Server di elaborazione Crystal Reports e RAS. In primo luogo è necessario copiare le estensioni di elaborazione in una directory condivisa su un'unità in rete che sia accessibile a tutti i server. Mappare, quindi, (o collegare) l'unità di rete di ciascun computer server.

Nota:

le unità mappate in Windows sono valide solo fino al riavvio del computer.

Se i server sono in esecuzione sia in Windows sia in UNIX, copiare la versione DLL e SO di ciascuna estensione di elaborazione nella directory condivisa. L'unità di rete condivisa deve essere inoltre visibile nei computer Windows e UNIX tramite Samba o un altro sistema di condivisione dei file.

Modificare infine la riga di comando di ciascun server per modificare la directory predefinita delle estensioni di elaborazione. Per modificare la riga di comando, passare alla scheda Server della CMC, selezionare un server e aprire la relativa pagina Proprietà. Aggiungere `-report_ProcessExtPath percorso assoluto` alla riga di comando. Sostituire *percorso assoluto* con il percorso della nuova cartella, utilizzando le convenzioni di percorso appropriate per il sistema operativo in esecuzione sul server (ad esempio `M:\code\extensions`, `/home/shared/code/extensions` e così via).

Per modificare la directory delle estensioni di elaborazione personalizzata, utilizzare la console CMC per arrestare il server. Aprire la pagina delle proprietà del server per modificare la riga di comando. Dopo avere completato queste operazioni, avviare nuovamente il server.

18.1.3.1.3 Gestione dell'accesso alle schede CMC

Amministrazione delegata e accesso alle schede CMC

Un amministratore del sistema della piattaforma BI generalmente gestisce un numero elevato di documenti, cartelle, utenti, server e altri oggetti. In ambienti aziendali di ampie dimensioni, tuttavia la quantità di risorse può superare quello gestibile da un solo amministratore. Un amministratore di sistema che intenda concentrarsi solo sulle attività ad alta priorità può creare amministratori delegati cui assegnare sottoinsiemi di attività di gestione (ad esempio l'amministrazione di un reparto o di un database). A differenza degli amministratori di sistema, gli amministratori delegati eseguono un insieme limitato di attività e dispongono di un numero inferiore di diritti sugli oggetti del sistema.

La configurazione predefinita della Central Management Console consente agli utenti di accedere a tutte le schede CMC disponibili. L'amministratore di sistema può gestire l'accesso alle schede CMC per controllare le schede visibili per i principali (utenti o gruppi di utenti). Per migliorare l'esperienza utente e il workflow dell'amministratore delegato, un amministratore di sistema può inoltre nascondere le schede CMC che l'amministratore delegato non dovrà utilizzare.

Avvertenza:

la gestione dell'accesso alle schede CMC influisce solo sull'aspetto visivo dell'interfaccia utente CMC. Nascondere le schede CMC non rappresenta una misura di protezione, in quanto non imposta né modifica i diritti di protezione sugli oggetti interni alle schede. Per garantire che gli utenti non eseguano operazioni non autorizzate su oggetti non autorizzati (ad esempio gestire server tramite Central Configuration Manager o software di terze parti basato sull'SDK della piattaforma BI), è necessario impostare i diritti di protezione appropriati sugli oggetti (ad esempio gli oggetti server).

Argomenti correlati

- [Gestione dell'accesso alle schede CMC per altri utenti](#)
- [Gestione dell'autorizzazione per la configurazione dell'accesso alle schede CMC per altri utenti o altri gruppo di utenti](#)

Utilizzo dell'accesso alle schede CMC

Gestione dell'accesso alle schede CMC per altri utenti

Un amministratore di sistema ha sempre accesso a tutte le schede CMC. Di seguito sono riportate le linee guida per l'amministrazione delle schede CMC cui possono accedere i principali.

- Per un processo di gestione semplificato e per ridurre gli interventi di manutenzione e risoluzione dei problemi, è consigliabile che gli amministratori gestiscano l'accesso alle schede CMC a livello di gruppo di utenti anziché a livello utente.
- Per le schede CMC che presentano cartelle di livello superiore, un amministratore deve concedere l'accesso a una scheda, nonché il diritto di "Visualizzazione" per la cartella di livello superiore della scheda. Di seguito sono elencate le schede CMC che supportano le cartelle di livello superiore:

- **Livelli di accesso**
 - **Calendari**
 - **Categorie**
 - **Connessioni (agli universi) Connessioni**
 - **Chiavi di crittografia**
 - **Eventi**
 - **Federazioni**
 - **Cartelle**
 - **Inboxes**
 - **Connessione OLAP**
 - **Categorie personali**
 - **Cartelle personali**
 - **Profili**
 - **Elenchi di replica**
 - **Server e gruppi**
 - **Memoria temporanea**
 - **Universi**
 - **Utenti e gruppi**
 - **Query servizio Web**
- Per una maggiore protezione del sistema, l'accesso alle schede CMC riportate di seguito è consentito solo ai membri del gruppo Amministratori. In quanto amministratori di sistemi, i membri del gruppo Amministratori possono accedere a qualsiasi scheda CMC indipendentemente dalle autorizzazioni di accesso alle schede CMC. Le autorizzazioni di accesso alle schede CMC sono state progettate per controllare l'accesso alle schede CMC per gli amministratori delegati, ovvero gli utenti che non sono membri del gruppo Amministratori.
 - **Controllo**
 - **Autenticazioni**
 - **Chiavi di crittografia**
 - **Codici di licenza**
 - **Monitoraggio**
 - **Sessioni**
 - **Impostazioni**
 - **Gestione attributi utente**

Avvertenza:

la gestione dell'accesso alle schede CMC influisce solo sull'aspetto visivo dell'interfaccia utente CMC. Nascondere le schede CMC non rappresenta una misura di protezione, in quanto non imposta né modifica i diritti di protezione sugli oggetti interni alle schede. Per garantire che gli utenti non eseguano operazioni non autorizzate su oggetti non autorizzati (ad esempio gestire server tramite Central Configuration Manager o software di terze parti basato sull'SDK della piattaforma BI), è necessario impostare i diritti di protezione appropriati sugli oggetti (ad esempio gli oggetti server).

Gestione dell'accesso alle schede CMC per altri utenti

1. Accedere alla CMC.

2. Nella scheda "Utenti e gruppi" fare clic con il pulsante destro del mouse su un principale e scegliere **Configurazione scheda CMC**.

Nota:

Se l'accesso alla scheda CMC non ha restrizioni, viene visualizzato il seguente messaggio: Avviso: l'accesso alla scheda CMC non è al momento limitato. Per limitare l'accesso alla CMC, fare clic sulla scheda "Applicazione", selezionare "CMC" e impostare l'accesso alla scheda CMC su limitato. Queste impostazioni avranno effetto solo dopo che l'accesso alla scheda CMC sarà limitato. È comunque possibile configurare l'accesso alle schede CMC, tuttavia la configurazione avrà effetto solo dopo che verranno definiti limiti per l'accesso.

Nella finestra di dialogo "Configurazione accesso scheda CMC" viene visualizzata una tabella:

- ✓ o ✗ indica le schede CMC a cui può accedere il principale.
 - "Ereditato" indica che l'accesso alla scheda è stato ereditato dai rispettivi gruppi di utenti principali.
 - "Esplicito" indica che l'accesso alla scheda è stato specificato esplicitamente sul livello principale.
3. Rivedere i diritti di accesso alle schede CMC. Per modificare i diritti, è possibile utilizzare i pulsanti sulla barra degli strumenti indicati di seguito.
 - Fare clic su **Concedi** per concedere esplicitamente l'accesso a una scheda.
 - Fare clic su **Nega** per negare esplicitamente l'accesso a una scheda.
 - Fare clic su **Eredita** per utilizzare un diritto di accesso ereditato.

Nota:

facendo clic sui pulsanti, le modifiche vengono applicate immediatamente al principale.

4. Al termine, fare clic su **Chiudi**.

Nella colonna "Autorizzazione" della tabella viene visualizzato il nuovo accesso alle schede valido.

Argomenti correlati

- [Restrizione dell'accesso alla scheda CMC](#)

Ereditarietà dell'accesso alle schede CMC

I diritti di accesso alle schede CMC e l'autorizzazione per la configurazione dell'accesso alle schede CMC per altri utenti o gruppi vengono applicati ed ereditati allo stesso modo degli altri diritti di protezione della piattaforma BI. Se per i principali non sono stati specificati esplicitamente diritti di accesso alle schede, questi li ereditano dai gruppi di utenti cui appartengono.

Se un utente è membro di due gruppi di utenti, l'accesso alle schede viene calcolato allo stesso modo di tutti gli altri diritti della piattaforma BI. Se ad esempio l'accesso a una scheda CMC viene concesso per uno dei gruppi e negato per l'altro, il principale non sarà in grado di accedere alla scheda CMC.

Nota:

- Se si modifica il diritto di accesso alle schede CMC per un gruppo di utenti, viene modificato anche l'accesso per tutti gli utenti che ereditano i diritti da tale gruppo, se il rispettivo accesso alle schede CMC è impostato su **Ereditato**.

- L'accesso impostato a livello di utente ha sempre la priorità rispetto a quello ereditato dai gruppi di utenti.

Gruppi di utenti amministratori delegati

È possibile creare un insieme di gruppi di utenti amministratori delegati per semplificare la gestione delle schede CMC. Per evitare di configurare singolarmente l'accesso alle schede CMC, è possibile rendere un utente o un gruppo di utenti esistente membro di un gruppo di utenti amministratore delegato. Di seguito viene illustrata la configurazione consigliata, che può tuttavia essere modificata per soddisfare esigenze aziendali specifiche.

Nota:

l'appartenenza a più gruppi comporta l'aggiunta di diritti, se questi sono impostati su **Ereditato**.

Gruppo di utenti amministratori delegati	Diritti consigliati
Amministratori di sistema	Concedere l'accesso a Tutte le schede
Amministratori di utenti	Concedere l'accesso a Livelli di accesso, Cartelle, Caselle di posta in arrivo, Cartelle personali, Categorie personali, Risultati query, Sessioni e Utenti e gruppi . Impostare tutte le altre schede su Ereditato .
Amministratori di contenuto	Concedere l'accesso a Calendari, Categorie, Eventi, Cartelle, Gestione delle istanze, Categorie personali, Cartelle personali, Profili, Risultati query e Universi . Impostare tutte le altre schede su Ereditato .
Amministratori di server	Concedere l'accesso a Server e Applicazioni . Impostare tutte le altre schede su Ereditato .

Gestione dell'autorizzazione per la configurazione dell'accesso alle schede CMC per altri utenti o altri gruppi di utenti

In un ambiente aziendale di ampie dimensioni un amministratore di sistema potrebbe avere la necessità di delegare la gestione dell'accesso alle schede CMC a un amministratore delegato. In alternativa, in un sistema multi-tenant per ciascun database potrebbe essere disponibile un amministratore delegato responsabile della gestione dell'accesso alle schede CMC per altri utenti e gruppi di utenti.

1. Accedere alla CMC.
2. Nella scheda "Utenti e gruppi" fare clic con il pulsante destro del mouse su un principale e scegliere **Configurazione scheda CMC**.

Nella finestra di dialogo "Configurazione accesso scheda CMC" per il principale è visualizzata l'opzione **Autorizzazione a configurare l'accesso alla scheda CMC per altri utenti o gruppi di utenti**.

Nota:

se questa autorizzazione viene concessa, il principale potrà gestire l'accesso alle schede CMC (solo per le schede cui ha accesso) per gli utenti su cui esercita il diritto "Modificare in modo sicuro i diritti

degli utenti sugli oggetti". Il principale potrà inoltre delegare ad altri utenti la gestione dell'accesso alle schede CMC concedendo l'**Autorizzazione a configurare l'accesso alla scheda CMC per altri utenti o gruppi di utenti** agli utenti sui quali esercita il diritto "Modificare in modo sicuro i diritti degli utenti sugli oggetti".

- ✓ o ✗ indica se il principale dispone dell'autorizzazione per configurare le schede CMC per altri utenti o gruppi di utenti.
 - "Ereditato" indica che l'autorizzazione è stata ereditata dai rispettivi gruppi di utenti principali.
 - "Esplicito" indica che l'autorizzazione è stata specificata esplicitamente sul livello principale.
3. Rivedere le autorizzazioni per la configurazione dell'accesso alle schede CMC per altri utenti o altri gruppo di utenti. È possibile modificare le autorizzazioni selezionando una delle impostazioni elencate di seguito nell'elenco.
- Fare clic su **Concedi** per concedere esplicitamente l'autorizzazione per la gestione dell'accesso alle schede CMC per altri utenti o gruppi di utenti.
 - Fare clic su **Nega** per negare esplicitamente l'autorizzazione per la gestione dell'accesso alle schede CMC per altri utenti o gruppi di utenti.
 - Fare clic su **Eredita** per ereditare l'autorizzazione per la gestione dell'accesso alle schede CMC per altri utenti o gruppi di utenti.

Nota:

selezionando un'opzione nell'elenco, viene modificata immediatamente l'autorizzazione del principale.

4. Al termine, fare clic su **Chiudi**.

Viene visualizzata la nuova autorizzazione valida.

Argomenti correlati

- [Amministrazione delegata e accesso alle schede CMC](#)
- [Ereditarietà dell'accesso alle schede CMC](#)

Per aggiungere una scheda Personalizzazione per un utente o un gruppo di utenti

Per poter aggiungere una scheda "Personalizzazione" per un utente o un gruppo di utenti, è necessario impostare l'accesso alle schede CMC su **Protetto**.

1. Nella CMC accedere all'area di gestione **Utenti e gruppi**.
2. Fare clic con il pulsante destro del mouse su un utente o un gruppo di utenti e scegliere **Configurazione scheda CMC**.

Viene visualizzata la finestra di dialogo "Configura schede CMC", in cui sono elencati i titoli delle singole schede CMC con il rispettivo livello di autorizzazione per il gruppo di utenti.

Se nella parte alta della finestra di dialogo viene visualizzato il messaggio di avviso seguente in rosso, per poter aggiungere una scheda **Personalizzazione**, è necessario impostare su Protetto l'accesso alle schede CMC:

Avviso: l'accesso alla scheda CMC non è al momento limitato. Per limitare l'accesso alla CMC, fare clic sulla scheda "Applicazione", selezionare

"CMC" e impostare l'accesso alla scheda CMC su limitato. Queste impostazioni avranno effetto solo dopo che l'accesso alla scheda CMC sarà limitato:

3. Per impostare l'accesso alle schede CMC su Protetto (se necessario):
 - a. Nell'area di gestione **Applicazioni** della CMC fare clic con il pulsante destro del mouse su **Central Management Console** e scegliere **Configurazione accesso scheda CMC**.
 - b. In **Accesso alla scheda CMC** selezionare l'opzione **Protetto** e fare clic su **Salva e chiudi**.
4. Nella finestra di dialogo "Configura schede CMC" per il gruppo di utenti selezionare per ciascuna scheda CMC dell'elenco **Concesso**, **Negato** o **Ereditato**.

Ogni volta che si modifica l'impostazione dell'autorizzazione per una scheda, la finestra di dialogo Configura schede CMC aggiorna l'autorizzazione del gruppo di utenti per configurare l'accesso alle schede per altri utenti o gruppi di utenti.
5. Fare clic su **Chiudi**.

Restrizione dell'accesso alla scheda CMC

È consigliabile configurare innanzitutto l'accesso alla scheda CMC per i principali e quindi limitare tale accesso. Se si limita l'accesso alla scheda prima di configurarla, gli utenti non potranno accedere alle schede CMC finché un amministratore non avrà concesso loro l'accesso.

Per garantire la coerenza con le versioni precedenti della piattaforma BI, inizialmente l'accesso alla scheda CMC è illimitato dopo l'installazione della piattaforma BI e qualsiasi utente con diritto di accesso alla CMC potrà accedere a tutte le schede disponibili. Per impedire che gli utenti accedano alle schede per le quali non dispongono dei diritti di accesso, un amministratore di sistema può limitare l'accesso alla scheda CMC.

È possibile rimuovere la restrizione di accesso alla scheda CMC in un caso urgente o per risolvere i problemi di configurazione dell'accesso alla scheda CMC, ad esempio se un amministratore delegato non può accedere a una scheda CMC essenziale.

1. Accedere alla CMC.
2. Nella scheda "Applicazioni" fare clic con il pulsante destro del mouse su **Central Management Console** e scegliere **Configurazione accesso scheda CMC**.

Viene visualizzata la finestra di dialogo "Accesso alla scheda CMC".
3. Configurare la regola di accesso alla scheda CMC.
 - Per limitare l'accesso degli utenti alle schede per le quali non dispongono dei diritti necessari, selezionare **Limitato**.
 - Per consentire agli utenti l'accesso a tutte le schede, selezionare **Non limitato**.
4. Al termine, fare clic su **Salva e chiudi**.

La regola di accesso alla scheda CMC viene applicata al sistema.

Argomenti correlati

- [Risoluzione dei problemi di accesso alla scheda CMC](#)

Risoluzione dei problemi di accesso alla scheda CMC

Per impedire l'accesso non autorizzato o per risolvere i problemi di accesso limitato di un utente alle schede CMC, è possibile risolvere i problemi relativi ai diritti di accesso alla scheda CMC di un utente.

1. Accedere alla CMC come amministratore.

Nota:

assicurarsi di disporre di accesso alla scheda di cui si desidera risolvere i problemi e di disporre del diritto "Modificare in modo sicuro i diritti degli utenti sugli oggetti" sull'utente.

2. Nella scheda "Utenti e gruppi" fare clic con il pulsante destro del mouse su un principale e scegliere **Configurazione accesso scheda CMC**.

Viene visualizzata la finestra "Configura schede CMC".

3. Controllare l'accesso effettivo alla scheda CMC. È possibile concedere o negare esplicitamente l'accesso alle schede disponibili.

Se l'accesso alla scheda CMC viene ereditato ma l'accesso effettivo alla scheda non corrisponde alle esigenze dell'utente:

- a. Compilare un elenco di tutti i gruppi di utenti di cui è membro il principale selezionato.
- b. Ripetere i passaggi da 1 a 3 per ogni gruppo dal quale l'utente eredita l'accesso alla scheda.
- c. Correggere l'accesso alla scheda CMC al livello del principale o del gruppo, come necessario.

Nota:

l'esecuzione di questa attività al livello del gruppo influisce sull'accesso alla scheda CMC per tutti gli utenti che sono membri di questo gruppo di utenti e per tutti gli utenti che sono membri dei gruppi di utenti ereditati da questo gruppo di utenti, a condizione che l'accesso degli utenti alla scheda CMC sia impostato su **Ereditato**.

4. Al termine, fare clic su **Chiudi**.

Argomenti correlati

- [Gestione dell'accesso alle schede CMC per altri utenti](#)
- [Ereditarietà dell'accesso alle schede CMC](#)

18.1.3.2 Gestione delle impostazioni delle discussioni

Nell'area "Applicazioni" della CMC della piattaforma BI è possibile specificare le impostazioni del livello di sistema per i thread di discussione.

L'applicazione "Discussioni" consente di gestire i thread di discussione e di interagire con essi in diversi modi, tra cui i seguenti:

- Ricerca dei thread di discussione in base ai criteri di ricerca specificati.
- Ordinamento dei risultati di ricerca dei thread di discussione.

- Eliminazione dei thread di discussione.

Nota:

Le impostazioni dei diritti utente non sono disponibili per l'applicazione Discussioni. È tuttavia possibile impostare diritti sui singoli report.

18.1.3.2.1 Ricerca di un thread di discussione

Per impostazione predefinita, nella pagina "Discussioni" vengono visualizzati i titoli di tutti i thread di discussione. Vengono visualizzati solo i thread del livello principale.

Per scorrere l'elenco dei thread di discussione, utilizzare i pulsanti Precedente e Successivo. È inoltre possibile cercare un thread o un gruppo di thread specifico.

1. Andare all'area "Applicazioni" della CMC e selezionare **Discussioni**.

2. Fare clic su **Gestisci > Gestisci thread**.

Viene visualizzata la finestra di dialogo **Amministrazione note**.

3. Nell'elenco **Nome campo** selezionare un'opzione.

Opzione	Descrizione
Titolo thread	Ricerche per titolo di thread.
Data di creazione	Ricerche per data di creazione.
Data ultima modifica	Ricerche per data dell'ultima modifica.
Autore	Ricerche per autore.

4. Mediante il secondo elenco è possibile perfezionare la ricerca.

Nota:

per le ricerche non viene fatta distinzione tra lettere maiuscole e minuscole.

- Se è stata selezionata l'opzione **Titolo thread** o **Autore**, scegliere tra le opzioni seguenti nel secondo campo.

Opzione	Descrizione
è	Vengono cercati thread di discussione in cui il titolo del thread o il nome dell'autore corrispondono esattamente al testo digitato nel terzo campo.
non è	Vengono cercati thread di discussione in cui il titolo del thread o il nome dell'autore non corrispondono esattamente al testo digitato nel terzo campo.
contiene	Vengono cercati thread di discussione contenenti la stringa di testo da ricercare nel titolo del thread o nel nome dell'autore.
non contiene	Vengono cercati thread di discussione che non contengono la stringa di testo nel titolo del thread.

- Se si è scelto **Data creazione** o **Data ultima modifica**, scegliere una delle seguenti opzioni e specificare una data di ricerca.

Opzione	Descrizione
prima	Vengono cercati thread di discussione creati o modificati prima della data di ricerca.
dopo	Vengono cercati thread di discussione creati o modificati dopo la data di ricerca.
tra	Vengono cercati thread di discussione creati o modificati tra due date di ricerca.

5. Per definire ulteriormente la ricerca, utilizzare il terzo campo.
 - Se si è selezionata una ricerca basata sul testo nei primi due campi, digitare la stringa di testo.
 - Se è stata scelta una ricerca basata sulla data, immettere la data o le date nei campi appropriati.
6. Fare clic su **Cerca**.

18.1.3.2.2 Ordinamento dei risultati della ricerca dei thread di discussione

Quando si cercano thread di discussione, è possibile selezionare la modalità di visualizzazione dei risultati di ricerca. Ad esempio, è possibile ordinarli in ordine alfabetico crescente e scegliere quanti risultati visualizzare per pagina.

1. Andare all'area "Applicazioni" della CMC e selezionare **Discussioni**.
2. Fare clic su **Gestisci > Gestisci thread**.
Viene visualizzata la finestra di dialogo "Amministrazione note".
3. Selezionare un'opzione di ordinamento dall'elenco **Ordina per**.

Opzione	Descrizione
Titolo thread	Ordinamento in base al titolo di un thread di discussione.
Data di creazione	Ordinamento in base alla data di creazione del thread.
Data ultima modifica	Ordinamento in base alla data in cui un thread è stato modificato per l'ultima volta.
Autore	Ordinamento in base all'autore di un thread di discussione specifico.

4. Nel secondo elenco, scegliere se si desidera che i record vengano visualizzati in ordine crescente o decrescente.
5. Nel terzo campo di testo, immettere quanti risultati dei thread di discussione visualizzare in ciascuna pagina.
Il valore predefinito è 10 risultati ogni pagina.
6. Fare clic su **Cerca**.

18.1.3.2.3 Per eliminare un thread di discussione

È possibile eliminare qualsiasi thread di discussione nell'area "Applicazioni" della console CMC della piattaforma BI.

1. Andare all'area "Applicazioni" della CMC e selezionare **Discussioni**.
2. Fare clic su **Gestisci > Gestisci thread**.
Viene visualizzata la finestra di dialogo "Amministrazione note".
3. Nell'elenco dei risultati cercare il thread di discussione che si desidera eliminare e selezionarlo.
4. Fare clic su **Elimina**.

18.1.3.3 Gestione delle impostazioni di BI Launch Pad

Nell'area **Applicazioni** della console CMC nella piattaforma BI selezionare **Gestisci > Proprietà** per mostrare le opzioni di visualizzazione di BI Launch Pad.

Per BI Launch Pad è possibile concedere a utenti o gruppi le seguenti capacità:

- Modifica delle preferenze
- Organizzazione delle cartelle
- Ricerca
- Filtraggio degli elenchi di oggetti per tipo di oggetto
- Visualizzazione della cartella *Preferiti*

Se ad esempio sono state create cartelle degli utenti utilizzando una convenzione di denominazione standard, è possibile negare agli utenti la possibilità di organizzare le proprie cartelle.

Nota:

per impostazione predefinita, tutti gli utenti hanno accesso a queste funzioni.

18.1.3.3.1 Modifica delle impostazioni di visualizzazione di BI Launch Pad

1. Passare all'area **Applicazioni** della CMC e fare doppio clic su **BI Launch Pad**.
Viene visualizzata la finestra di dialogo "Proprietà di BI Launch Pad".
2. Per consentire discussioni agli utenti di BI Launch Pad, selezionare **Abilita discussioni**.
3. Per abilitare i filtri per la pianificazione, selezionare la casella di controllo **Mostra scheda "Filtri" nella pagina di pianificazione**.
Questa impostazione controlla se gli utenti possono immettere formule di selezione di record o gruppi quando pianificano un report Crystal.
4. Fare clic su **Salva e chiudi**.

18.1.3.4 Gestione delle impostazioni di Web Intelligence

È possibile stabilire quali funzionalità rendere accessibili agli utenti per i documenti di Web Intelligence impostando le proprietà dell'applicazione Web Intelligence.

18.1.3.4.1 Modifica delle impostazioni di visualizzazione per Web Intelligence

1. Andare nell'area "Applicazioni" della console CMC e selezionare **Web Intelligence**.
2. Fare clic su **Gestisci > Proprietà**.
Viene visualizzata la finestra di dialogo "Proprietà".
3. Definire tutte le opzioni di visualizzazione seguenti desiderate.

Opzione	Descrizione
"Dimensioni e dettagli"	Utilizzare le opzioni in questa area per definire la modalità di visualizzazione dei dati nei report. È possibile modificare lo stile del carattere, il colore del testo e quello dello sfondo. Un'anteprima mostra automaticamente le modifiche apportate. Al termine, scegliere OK .
"Valori fluttuanti (misure numeriche)"	Utilizzare le opzioni di quest'area per modificare e formattare l'intestazione della pagina. È possibile modificare lo stile del carattere, il colore del testo e quello dello sfondo. Un'anteprima mostra automaticamente le modifiche apportate. Al termine, scegliere OK .
"Proprietà immagini incorporate"	: specificare le dimensioni massime delle immagini incorporate.
"Proprietà della modalità Visualizzazione rapida"	Nei campi appropriati specificare i valori per il numero massimo di record verticali e orizzontali, la larghezza minima della pagina, l'altezza minima della pagina, la spaziatura destra e la spaziatura inferiore.
"Impostazioni salvataggio automatico"	Impostare l'intervallo con cui vengono salvati automaticamente i documenti. Questo intervallo viene reimpostato ogni volta che si salva manualmente o automaticamente un documento. Inoltre, il documento salvato automaticamente viene eliminato quando il documento viene salvato manualmente.
"Aggiornamento automatico"	Abilita l'aggiornamento automatico dei documenti Web quando si seleziona la proprietà Aggiorna automaticamente di tali documenti. Per informazioni dettagliate, consultare il <i>Manuale dell'utente di SAP BusinessObjects Web Intelligence</i> .

Opzione	Descrizione
"Unisci automaticamente"	<p>Abilita l'unione automatica delle dimensioni quando è selezionata la proprietà Unisci automaticamente dimensioni dei documenti Web Intelligence.</p> <p>Per informazioni dettagliate, consultare il <i>Manuale dell'utente di SAP BusinessObjects Web Intelligence</i>.</p>
"Impostazione del diritto di protezione per l'aggiornamento automatico all'apertura di un documento"	<p>Deselezionare questa opzione per abilitare in Web Intelligence l'aggiornamento automatico dei documenti all'apertura, senza abilitare Aggiornamento all'apertura nelle proprietà dei documenti Web Intelligence. La selezione di questa opzione implica anche quella del diritto di protezione Documenti - disabilita l'aggiornamento automatico all'apertura.</p>
"Smart View"	<p>Questa opzione determina quale versione dei documenti viene visualizzata alla loro apertura in Web Intelligence.</p> <ul style="list-style-type: none"> • Visualizza ultima istanza <p>Viene aperta l'ultima istanza dell'oggetto. Se ad esempio un documento viene pianificato per essere aggiornato ogni ora e l'ultimo salvataggio del documento è stato effettuato cinque ore prima, viene aperta l'ultima istanza. Quando un utente salva tale istanza, il documento originale viene aggiornato di conseguenza.</p> • Visualizza oggetto <p>Il documento viene aperto nello stesso stato in cui era quando è stato salvato l'ultima volta, indipendentemente dagli aggiornamenti pianificati che potrebbero essere stati effettuati.</p>

4. Fare clic su **Salva e chiudi**.

Nota:

Per riselectare le variabili di visualizzazione predefinite, scegliere **Reimposta**.

18.1.3.5 Gestione delle impostazioni di avviso

Nell'area "Applicazioni" della console CMC nella piattaforma BI è possibile specificare le impostazioni del livello di sistema per gli avvisi.

Per l'applicazione "Avvisi" è possibile controllare e definire le modalità di accesso agli avvisi degli utenti di sistema con:

- Abilitazione della cartella **Avvisi personali** per i sottoscrittori a un avviso
- Abilitazione e formattazione dei messaggi di avviso inviati tramite posta elettronica
- Impostazione di un limite per il numero di avvisi nel sistema
- Impostazione di un periodo di scadenza per i messaggi di avviso

Argomenti correlati

- [Impostazione dei diritti sulle applicazioni](#)

18.1.3.5.1 Per modificare le proprietà della destinazione di avviso

1. Nell'area **Applicazioni** della CMC fare doppio clic su **Applicazione di gestione degli avvisi**.
2. Fare clic su **Gestisci > Proprietà**.
Viene visualizzata la finestra di dialogo "Avvisi".
3. (Obbligatorio) Eseguire una delle azioni seguenti:
 - Per consentire ai sottoscrittori a un avviso di ricevere notifiche selezionare **Abilita avvisi personali** al di sotto di **Avvisi personali** in BI Launch Pad.
 - Selezionare **Abilita posta elettronica** per consentire ai sottoscrittori a un avviso di ricevere notifiche tramite posta elettronica.

Vengono visualizzate le opzioni di posta elettronica globale degli avvisi.

4. Se è stato selezionato **Abilita posta elettronica**, eseguire le azioni seguenti:
 - Nella casella **Da** immettere l'indirizzo di posta elettronica da cui verranno inviate le notifiche di avviso.

I sottoscrittori riceveranno messaggi di posta elettronica di avviso da questo indirizzo di posta elettronica. Utilizzare un indirizzo di posta elettronica valido, riconosciuto dal sistema.
 - Nella casella **A** immettere l'indirizzo di posta elettronica del sottoscrittore all'avviso.

Per impostazione predefinita, tutti gli avvisi di sistema verranno inviati a questo indirizzo di posta elettronica.

Suggerimento:

Non specificare un indirizzo di posta elettronica o un destinatario. Utilizzare il segnaposto **%INDIRIZZO_POSTALETTRONICA_SI%**.

- Nella casella **Cc** immettere l'indirizzo di posta elettronica di ogni destinatario che deve ricevere le copie per conoscenza degli avvisi.
- Nella casella **Oggetto** immettere un'intestazione predefinita per l'oggetto da utilizzare nei messaggi di posta elettronica contenenti avvisi.
- Nella casella **Messaggio** immettere un messaggio predefinito da includere nei messaggi di posta elettronica contenenti avvisi.
- Selezionare **Aggiungi allegato** per consentire l'inclusione predefinita degli allegati nei messaggi di posta elettronica contenenti avvisi.

Selezionare ad esempio questa opzione per includere i report Crystal associati con gli avvisi attivati.

- Se è stato selezionato **Aggiungi allegato**, in **Nome file** selezionare **Generato automaticamente** o **Nome specifico** per indicare in che modo assegnare i nomi agli allegati dei messaggi di posta elettronica.

5. Fare clic su **Salva e chiudi**.

Argomenti correlati

- [Impostazione dei diritti sulle applicazioni](#)
- [Gestione delle impostazioni di avviso](#)

18.1.3.5.2 Modifica delle proprietà predefinite di avviso

1. Passare all'area "Applicazioni" della CMC e selezionare **Applicazione di gestione degli avvisi**.
2. Scegliere **Gestisci > Proprietà > Impostazioni predefinite**.
3. Impostare i valori appropriati per le proprietà seguenti.

Opzione	Descrizione
"Periodo di scadenza"	Specifica per quanto tempo i messaggi di avviso verranno conservati nel sistema prima di essere cancellati.
"Numero massimo di messaggi di avviso"	Specifica il numero massimo di messaggi di avviso supportato dal sistema. Quando viene raggiunta la soglia, il sistema rimuove il 20% dei messaggi di avviso, iniziando da quelli più vecchi.

4. Fare clic su **Salva e chiudi**.

Argomenti correlati

- [Gestione delle impostazioni di avviso](#)

18.1.3.6 Gestione delle impostazioni dei widget

Widget per SAP BusinessObjects Enterprise è un'applicazione desktop che consente agli utenti di aggiungere mini-applicazioni al proprio desktop per facilitare l'accesso al contenuto di business intelligence nelle applicazioni della piattaforma BI e Web Dynpro sui SAP NetWeaver Application Server.

Dall'area "Applicazioni" della CMC è possibile controllare l'accesso degli utenti per la creazione e l'utilizzo dei widget nei desktop, nonché la loro capacità di eseguire ricerche nel repository della piattaforma BI dall'applicazione widget sul proprio desktop.

È possibile concedere a utenti o gruppi la capacità di:

- Utilizzare i widget
- Modificare gli oggetti creati tramite i widget
- Modificare i diritti utente per l'accesso agli oggetti

Nota:

Per impostazione predefinita, tutti gli utenti generali possono accedere a queste funzionalità.

18.1.3.7 Gestione delle impostazioni di SAP BusinessObjects Explorer

È possibile definire le funzionalità cui hanno accesso gli utenti in SAP BusinessObjects Explorer impostando i diritti di protezione nell'area Applicazioni della console CMC.

18.1.3.7.1 Modifica delle proprietà delle applicazioni SAP BusinessObjects Explorer

1. Accedere all'area "Applicazioni" della console CMC.
2. Fare clic su **Gestisci > Proprietà**.
Viene visualizzata la finestra di dialogo "Proprietà".
3. Definire tutte le impostazioni SAP BusinessObjects Explorer seguenti desiderate:
 - Validità dei segnalibri
 - Configurazione avanzata
4. Fare clic su **Salva e chiudi**.

18.1.3.8 Cronologia del documento

La seguente tabella contiene una panoramica delle modifiche principali apportate al documento.

Versione	Data	Descrizione
Piattaforma SAP BusinessObjects Business Intelligence 4.1	Maggio 2013	<p>È stato aggiunto il supporto per SAP Jam. Quando è integrato, SAP Jam aggiunge le funzionalità social media e di collaborazione a BI Launch Pad.</p> <p>Sono stati aggiunti ulteriori diritti di accesso SAP StreamWork per utenti e gruppi. Il pannello dei feed di SAP StreamWork include un elenco a discesa delle istanze e degli orari e un pulsante che consente di seguire o non seguire un feed. Seguire automaticamente tutte le istanze correlate quando si segue un documento modello in SAP StreamWork. I commenti sulle istanze vengono pubblicati solo per l'istanza in SAP StreamWork.</p> <p>È possibile aprire i collegamenti OpenDocument a documenti e istanze su una scheda o mediante il link. Quando si visualizza un documento o un'istanza mediante un collegamento OpenDocument, aprire il pannello dei feed di SAP StreamWork per monitorare o rispondere a un feed di documenti.</p> <p>È stata aggiunta la casella di controllo Aggiungi estensione file alla finestra di dialogo "Destinazioni".</p>

Versione	Data	Descrizione
Piattaforma SAP BusinessObjects Business Intelligence 4.1 pacchetto di supporto 1	Agosto 2013	<p>Questo manuale è stato aggiornato in modo da includere le informazioni seguenti:</p> <p>Nota: È possibile eseguire una sola sessione di BI Launch Pad alla volta. Utilizzare le schede (o le finestre a seconda della propria configurazione) per visualizzare più oggetti e applicazioni.</p>

18.1.3.9 Gestione dell'integrazione con le applicazioni di collaborazione

Utilizzare l'area **Applicazioni** della console CMC nella piattaforma BI per abilitare e configurare la collaborazione con SAP Jam o SAP StreamWork.

Nell'agente Enterprise dell'applicazione di collaborazione è necessario eseguire ulteriori attività di configurazione:

- Stabilire la connessione HTTPS con il provider di servizi
- Soddisfare i prerequisiti di autenticazione

Poiché vengono applicate diverse procedure di autenticazione (SAML 2.0 e OAuth 1.0a), la descrizione occupa la maggior parte del documento. Una volta configurata l'applicazione di collaborazione, i feed SAP Jam o SAP StreamWork sono disponibili in BI Launch Pad.

Destinatari

Gli amministratori della piattaforma BI impegnati nell'integrazione di tale piattaforma con l'applicazione di collaborazione SAP Jam o SAP StreamWork.

18.1.3.10 Prerequisiti di collaborazione

Sono riepilogati i requisiti per la piattaforma BI e le applicazioni di collaborazione.

- La piattaforma BI deve essere installata con almeno un Central Management Server (CMS).
- È necessario configurare l'applicazione di collaborazione (SAP Jam o SAP StreamWork) nella CMC.

- È necessario definire un'organizzazione Enterprise per l'applicazione di collaborazione (SAP Jam o SAP StreamWork).
- Gli utenti SAP Jam o SAP StreamWork devono appartenere all'organizzazione Enterprise.

Nota:

Un agente Enterprise di SAP StreamWork è necessario solo per il provisioning degli utenti mediante un servizio directory LDAP/AD on-premise.

18.1.3.11 Configurazione della piattaforma BI

18.1.3.11.1 Opzioni di configurazione della collaborazione

In questa tabella sono riepilogate le opzioni della console CMC nella piattaforma BI per l'integrazione di SAP Jam o SAP StreamWork.

Nella finestra di dialogo "Proprietà: Collaborazione" della CMC vengono visualizzate le opzioni riportate di seguito. Per accedere a queste opzioni, passare alla scheda **Applicazioni**, fare clic su **Collaborazione**, quindi dal menu **Gestisci** selezionare **Proprietà**.

Opzione	Descrizione
Abilita collaborazione	Selezionare questa casella di controllo e SAP Jam o SAP StreamWork .
URL di connessione	Digitare l'URL dell'applicazione di collaborazione.
ID provider di identità univoco	<p>Immettere un valore da utilizzare per la distribuzione della piattaforma BI. Questo valore sarà associato al certificato utilizzato per configurare l'integrazione sulla console di amministrazione dell'applicazione di collaborazione.</p> <p>Nota: è necessario configurare l'applicazione per eseguire l'asserzione di un'identità per un Single Sign On come un'applicazione amministrativa OAuth.</p>

Opzione	Descrizione	
Certificato Base64 provider di identità	Se si fa clic su Genera , viene creato un certificato nel campo Certificato Base64 provider di identità . Utilizzare questo certificato nella console di amministrazione di SAP StreamWork per generare una OAuth Consumer Key. Questo certificato stabilisce la relazione di attendibilità tra l'applicazione di collaborazione e la piattaforma BI. Lo stesso provider di identità esterno viene identificato mediante un certificato X509, che viene utilizzato per firmare tutte le asserzioni di identità. È necessario che il certificato sia codificato Base64.	
Chiave utente OAuth	Utilizzare questo campo per immettere una chiave utente OAuth valida generata dalla console di amministrazione dell'applicazione di amministrazione.	
Connessione tramite proxy	<p>Selezionare la casella di controllo se si desidera abilitare la connessione tramite proxy. È necessario fornire informazioni sull'host proxy nei campi Host proxy HTTP e Porta.</p> <p>Suggerimento: Per autorizzare le connessioni in entrata dai server dell'applicazione di collaborazione alla rete aziendale, è necessario disporre di un proxy inverso nella DMZ.</p> <p>Nota: Per aggiungere un certificato attendibile di un provider di certificati SSL al proxy inverso, è necessario disporre di un nome del dominio o del sottodominio del proxy inverso.</p>	
	Host proxy HTTP	<p>Nella configurazione del proxy inverso digitare l'indirizzo esterno accessibile all'applicazione di collaborazione. È ad esempio possibile utilizzare <code>https://ProxyInverso/</code>, in cui <i>ProxyInverso</i> è il nome del dominio o del sottodominio del proxy inverso.</p> <p>L'applicazione di collaborazione utilizza questo indirizzo per inviare informazioni alla piattaforma BI. Il proxy inverso utilizza l'indirizzo per reindirizzare le informazioni ricevute dall'applicazione di collaborazione al computer in cui si trova l'agente Enterprise dell'applicazione di collaborazione.</p>
	Porta	L'agente Enterprise dell'applicazione di collaborazione è configurato per ascoltare dalla porta 8443.

18.1.3.11.2 Per abilitare e configurare la collaborazione nella CMC

Questa attività richiede una valida connessione alla console di amministrazione dell'applicazione di collaborazione (SAP Jam o SAP StreamWork). Sarà infatti necessario passare e recuperare dettagli di protezione dalla console.

Per motivi di protezione, i seguenti account predefiniti non possono inviare o pianificare contenuto per SAP Jam o SAP StreamWork:

- Guest
- SMAdmin
- Amministratore
- WaaWSServletPrincipal

1. Nella Central Management Console (CMC) della piattaforma BI passare all'area **Applicazioni**, quindi fare doppio clic su **Collaborazione**
2. Nella finestra di dialogo "Proprietà: Collaborazione" selezionare la casella di controllo **Abilita collaborazione**, quindi selezionare **SAP Jam** o **SAP StreamWork**.
3. Nella casella **URL di connessione** digitare l'URL dell'applicazione di collaborazione.
4. Nella casella **ID provider di identità univoco** digitare un valore del provider di identità univoco per la distribuzione della piattaforma BI.
Prendere nota del valore del provider di identità: verrà utilizzato per configurare l'applicazione di collaborazione.
5. Fare clic su **Genera** (o **Rigenera**, se è già stato creato un certificato).
Viene creato un certificato nella casella **Certificato Base64 provider di identità**. Il valore del certificato viene utilizzato per configurare l'applicazione di collaborazione.
6. Nella casella **Chiave utente OAuth** digitare una chiave utente OAuth valida.
La chiave utente OAuth viene creata nell'applicazione di collaborazione.
7. Se si è connessi tramite proxy al server con SAP Jam o SAP StreamWork, eseguire le seguenti azioni:
 - a. Selezionare la casella di controllo **Connessione tramite proxy**.
 - b. Nella casella **Host proxy HTTP** digitare il nome dell'host proxy del server.
 - c. Nella casella **Porta** digitare il numero di porta del server.
8. Fare clic su **Salva e chiudi**.

18.1.3.12 Configurazione SAP Jam

18.1.3.12.1 Per registrare un nuovo certificato IDP attendibile SAML per SAP Jam

Per poter registrare un nuovo provider di identità attendibile SAML:

- La società deve essere aggiunta e configurata in SAP Jam.

- Alla società deve essere associato un account utente valido in SAP Jam.
- È necessario disporre di diritti di amministrazione della società in SAP Jam e di diritti di amministrazione completa nella piattaforma BI e in BI Launch Pad.
- È necessario registrare BI Launch Pad con SAP Jam come client OAuth che funge da rappresentante di BI Launch Pad all'interno di SAP Jam.

Nota:

Ogni utente deve essere registrato in SAP Jam con un indirizzo di posta elettronica univoco corrispondente all'indirizzo di posta elettronica Enterprise dell'utente in BI Launch Pad. Viene eseguita la mappatura degli indirizzi di posta elettronica tra la piattaforma BI e SAP Jam.

1. In SAP Jam selezionare **Admin** dal menu **Administrator** nell'angolo superiore destro.
In SAP Jam vengono visualizzate le informazioni sulla società, inclusa la licenza SAP Jam. Prendere nota di queste informazioni.
2. Dal menu **Admin** selezionare **SAML Trusted IDPs**, quindi fare clic su **Register your identity provider**.
È necessario registrare il provider di identità creato in BI Launch Pad.
3. (Obbligatorio) Nella casella **IDP ID** immettere il valore del provider di identità univoco creato quando SAP Jam è stato configurato nella piattaforma BI.
Se non si dispone del valore, contattare l'amministratore dell'applicazione esterna.
Digitare ad esempio *NomeSocietà_IDSistema_Client*
4. Nella casella **Single Sign-On URL** immettere l'URL che consente di accedere direttamente a SAP Jam.
SAP Jam utilizza questo URL per il singolo accesso con il provider di identità univoco.
5. Nella casella **Single Log-Out URL** immettere l'URL da visualizzare dopo la disconnessione da SAP Jam.
SAP Jam utilizza questo URL per la singola disconnessione con il provider di identità univoco.
6. Nella casella **Default Name ID Format** immettere il formato dell'ID nome da utilizzare nelle richieste di autenticazione.
7. Nella casella **Default Name ID Policy SP Name Qualifier** digitare il qualificatore del nome SP da utilizzare nelle richieste di autenticazione.
8. (Obbligatorio) Nell'elenco **Allowed Assertion Scope** selezionare **Users in my company**.
Questa opzione specifica l'insieme di utenti per cui SAP Jam accetterà le asserzioni dal provider di identità.
9. (Obbligatorio) Nella casella **X509 Certificate (Base64)** immettere il valore del certificato Base64 generato quando SAP Jam è stato configurato nella piattaforma BI.
Se non si dispone del valore, contattare l'amministratore dell'applicazione esterna.
10. Fare clic su **Registra**.

18.1.3.12.2 Per creare un client OAuth per SAP Jam

Per poter creare una chiave utente OAuth:

- La società deve essere aggiunta e configurata in SAP Jam.
- Alla società deve essere associato un account utente valido in SAP Jam.
- È necessario disporre di diritti di amministrazione della società in SAP Jam e di diritti di amministrazione completa nella piattaforma BI e in BI Launch Pad.
- È necessario registrare BI Launch Pad con SAP Jam come client OAuth che funge da rappresentante di BI Launch Pad all'interno di SAP Jam.

Nota:

Ogni utente deve essere registrato in SAP Jam con un indirizzo di posta elettronica univoco corrispondente all'indirizzo di posta elettronica Enterprise dell'utente in BI Launch Pad. Viene eseguita la mappatura degli indirizzi di posta elettronica tra la piattaforma BI e SAP Jam.

1. In SAP Jam selezionare **Admin** dal menu **Administrator** nell'angolo superiore destro.
In SAP Jam vengono visualizzate le informazioni sulla società, inclusa la licenza SAP Jam.
2. Dal menu **Admin** selezionare **OAuth Clients**, quindi fare clic su **Add OAuth Client**.
3. Nella finestra di dialogo "Register a new OAuth Client", nella casella **Name** immettere il valore del provider di identità univoco creato quando SAP Jam è stato configurato nella piattaforma BI.
Se non si dispone del valore, contattare l'amministratore dell'applicazione esterna.
SAP Jam visualizza il nome dell'applicazione come collegamento ipertestuale all'URL immesso quando esegue azioni per conto di un utente.
Digitare ad esempio *NomeSocietà_IDSistema_Client_Applicazione*
4. Nella casella **URL di integrazione** immettere l'URL che consente di accedere direttamente a BI Launch Pad.
SAP Jam visualizza il nome dell'applicazione come collegamento ipertestuale a questo URL quando esegue azioni per conto di un utente.
5. Nella casella **X509 Certificate (Base64)** immettere il valore del certificato Base64 generato quando SAP Jam è stato configurato nella piattaforma BI.
Se non si dispone del valore, contattare l'amministratore dell'applicazione esterna.
Se questa casella viene lasciata vuota, SAP Jam fornisce un segreto utente.
6. Fare clic su **Salva**.
Viene generata la chiave utente OAuth. Prendere nota del valore della chiave utente OAuth in modo che l'amministratore della piattaforma BI possa utilizzarla.

18.1.3.13 Configurazione SAP StreamWork

18.1.3.13.1 Illustrazione dell'integrazione SAP StreamWork

Questo diagramma mostra i componenti piattaforma BI, SAP StreamWork e agente Enterprise di SAP StreamWork necessari per l'integrazione con SAP StreamWork.

Il flusso di lavoro descrive i passaggi coinvolti nell'integrazione dei sistemi e offre una panoramica delle azioni che gli utenti possono eseguire dopo l'integrazione:

- Nell'agente Enterprise di SAP StreamWork gli utenti possono eseguire il provisioning degli utenti Enterprise da LDAP a SAP StreamWork.
- Nella CMC della piattaforma BI gli amministratori possono creare utenti e mapparli agli utenti Enterprise.
- In BI Launch Pad gli utenti possono creare attività e visualizzarle in un browser, senza creare un account o accedere a SAP StreamWork.
- In BI Launch Pad gli utenti possono visualizzare e rispondere ai feed SAP StreamWork.

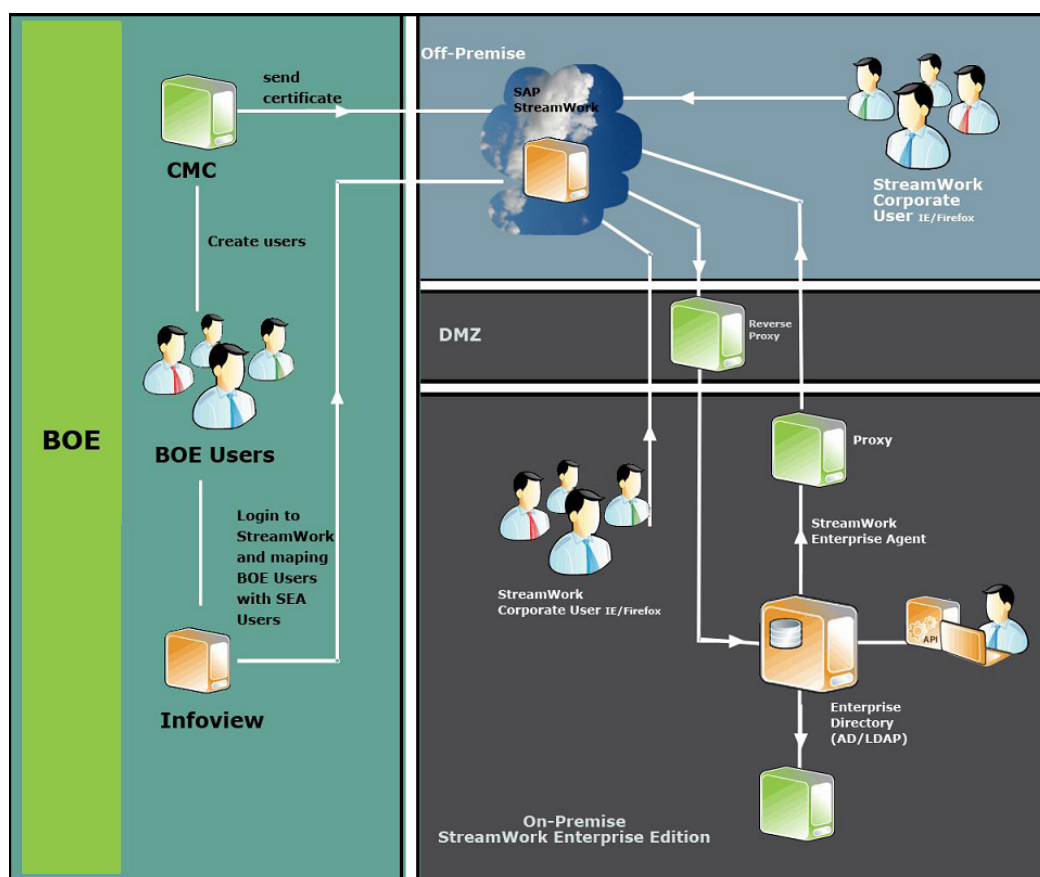


Figura 18 - 1: System Landscape

18.1.3.13.2 Per creare una chiave utente OAuth per SAP StreamWork

Per poter creare una chiave utente OAuth, è necessario disporre di diritti di amministratore per l'organizzazione Enterprise SAP StreamWork.

1. Nella console di amministrazione di SAP StreamWork, nella scheda **Admin** selezionare **SAML Trusted IDPs**, quindi accedere a SAP StreamWork utilizzando un account designato come amministratore dell'organizzazione Enterprise.
2. Fare clic su **Register your identity provider**.
3. Selezionare **Click here to create a new administrative OAuth application**, quindi accettare il contratto dei termini di utilizzo.
4. Nella finestra **Register a new Application OAuth application** eseguire le seguenti azioni:
 - a. Nella casella **Application Name** immettere il nome dell'istanza dell'applicazione da utilizzare nell'integrazione.
Questa informazione identifica l'applicazione necessaria per eseguire azioni per conto di un utente, ad esempio per pubblicare feed SAP StreamWork per un utente. Gli utenti devono essere in grado di riconoscere questo nome di applicazione.
 - b. Nella casella **Integration URL** immettere l'URL che consente di accedere direttamente a BI Launch Pad.
 - c. Nella casella **Base64 X509 Certificate** immettere il valore del certificato Base64 generato durante la configurazione di SAP StreamWork nella console CMC (Central Management Console) della piattaforma BI.
Se non si dispone del valore, contattare l'amministratore dell'applicazione esterna.
5. Fare clic su **Registra**.
Viene generata la chiave utente OAuth. Prendere nota del valore della chiave utente OAuth in modo che l'amministratore della piattaforma BI possa utilizzarla.
6. Fare clic su **Back** per visualizzare i provider di identità attendibili SAML.
7. Nella finestra "Register a new SAML Trusted Identity Provider" eseguire le seguenti azioni:
 - a. Nella casella **Display Name** immettere un nome per la distribuzione della piattaforma BI.
Questo nome viene visualizzato agli utenti in SAP StreamWork.
 - b. Nella casella **IDP ID** immettere il valore del provider di identità univoco creato durante la configurazione di SAP StreamWork nella piattaforma BI.
Se non si dispone del valore, contattare l'amministratore dell'applicazione esterna.
 - c. Nella casella **Base64 X509 Certificate** immettere il valore del certificato Base64 generato durante la configurazione di SAP StreamWork nella piattaforma BI.
Se non si dispone del valore, contattare l'amministratore dell'applicazione esterna.
8. Fare clic su **Registra**.

18.1.3.13.3 Per aggiungere SAP StreamWork a uno spazio di lavoro BI

SAP StreamWork è nascosto e deve essere reso visibile manualmente nell'elenco di moduli BI Launch Pad che è possibile aggiungere a uno spazio di lavoro BI.

1. Individuare il file `home-analyticlist.xml` nel percorso `C:\BusinessObjects\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.PerformanceManagement\web\WEB-INF\lib\asdk-ivdm_ext.jar\conf-syst\conf-syst\`.

Il contenuto del file deve iniziare con il testo seguente:

```
<?xml version="1.0" encoding="UTF-8"?>

<CHOICE>

<!--<SW_ACTIVITIES NAME="$MSG_SW_ACTIVITIES$" DESCRIPTION="$MSG_SW_ACTIVITIESDESC$" />-->

<!--SW_FEED NAME="$MSG_SW_FEED$" DESCRIPTION="$MSG_SW_ACTIVITIESDESC$" />-->

<HOMEINBOX NAME="$MSG_HOMEINBOX$" DESCRIPTION="$MSG_HOMEINBOXDESC$" />

<HOMEAPPLICATIONS NAME="$MSG_HOMEAPPLICATIONS$" DESCRIPTION="$MSG_HOMEAPPLICATIONSDESC$" />

<HOMERECENTLYRUNDOCS NAME="$MSG_HOMERECENTLYRUNDOCS$" DESCRIPTION="$MSG_HOMERECENTLYRUNDOCSDESC$" />

<HOMERECENTDOCS NAME="$MSG_HOMERECENTDOCS$" DESCRIPTION="$MSG_HOMERECENTDOCSDESC$" />

<HOMEALERTS NAME="$MSG_ALERTNOTIFICATIONS$" DESCRIPTION="$MSG_ALERTNOTIFICATIONSDESC$" />

</CHOICE>
```

2. Rimuovere `!--` dalle righe `SW_ACTIVITIES NAME=` e `SW_FEED NAME=`.
3. Riavviare il server Tomcat.

Il feed **SAP StreamWork** viene visualizzato nell'elenco di **Moduli BI Launch Pad** nella libreria di moduli per gli spazi di lavoro BI in BI Launch Pad.

18.1.3.14 Gestione delle impostazioni di Ricerca piattaforma

Nell'area "Applicazioni" della console CMC nella piattaforma BI è possibile specificare le impostazioni al livello di sistema per l'applicazione Ricerca piattaforma.

Argomenti correlati

- [Elenco errori di indicizzazione](#)
- [Configurazione delle proprietà dell'applicazione nella CMC](#)

18.1.3.14.1 Configurazione delle proprietà dell'applicazione nella CMC

Per configurare le proprietà dell'applicazione Ricerca piattaforma, attenersi alla procedura seguente:

1. Accedere all'area "Applicazioni" della console CMC.
2. Selezionare **Applicazione di ricerca piattaforma**.
3. Fare clic su **Gestisci > Proprietà**. Viene visualizzata la finestra di dialogo "Proprietà".
4. Configurare le impostazioni di Ricerca piattaforma:

Opzione	Descrizione
Statistiche della ricerca	<p>L'applicazione di ricerca piattaforma fornisce le seguenti statistiche della ricerca:</p> <ul style="list-style-type: none"> • Stato indicizzazione: visualizza lo stato del processo di indicizzazione. • Numero di documenti indicizzati: visualizza il numero di documenti indicizzati. • Ultima indicazione data e ora: visualizza la data e l'ora in cui è stata eseguita l'ultima indicizzazione del documento.
Interrompi / Avvia indicizzazione	<p>Le opzioni Avvia indicizzazione e Interrompi indicizzazione consentono di avviare o arrestare il processo di indicizzazione quando si desidera passare dalla ricerca per indicizzazione continua alla ricerca per indicizzazione pianificata o a scopo di manutenzione.</p> <p>Per interrompere l'indicizzazione, fare clic su Interrompi indicizzazione.</p>
Impostazioni internazionali indice predefinite	<p>Ricerca piattaforma si serve delle impostazioni locali specificate nella CMC per indicizzare tutti i documenti BI non localizzati. Una volta localizzato un documento, viene utilizzato l'Analyzer della lingua corrispondente per l'indicizzazione.</p> <p>La ricerca si basa sulle impostazioni locali del prodotto del client che vengono configurate nelle proprietà di configurazione della CMC.</p>

Opzione	Descrizione
Frequenza di ricerca per indicizzazione	<p>È possibile indicizzare l'intero repository della piattaforma BI utilizzando le seguenti opzioni:</p> <ul style="list-style-type: none"> • Ricerca per indicizzazione continua: questa opzione implica un'indicizzazione continua, ovvero il repository viene indicizzato ogni volta che si aggiunge, si modifica o si elimina un oggetto. Consente di visualizzare o utilizzare i contenuti della piattaforma BI più aggiornati. La ricerca per indicizzazione continua costituisce l'impostazione predefinita e aggiorna in modo continuativo il repository in base alle azioni eseguite. La ricerca per indicizzazione continua agisce senza intervento dell'utente e riduce il tempo richiesto per l'indicizzazione di un documento. • Ricerca per indicizzazione pianificata: con questa opzione l'indicizzazione avviene in base alla pianificazione impostata tramite le opzioni specifiche. <p>Per ulteriori informazioni sulla pianificazione di un oggetto, consultare la sezione <i>Pianificazione di un oggetto</i> di Ricerca piattaforma nella <i>Guida in linea CMC della piattaforma SAP BusinessObjects Business Intelligence</i>.</p> <p>Nota:</p> <ul style="list-style-type: none"> • Se si seleziona Ricerca per indicizzazione pianificata e si imposta la Ricorrenza su un'opzione diversa da Ora, Ricerca piattaforma visualizza la data e l'ora in cui è pianificata l'indicizzazione successiva del documento. • Se si seleziona Ricerca per indicizzazione pianificata, il pulsante Avvia indicizzazione viene abilitato mentre il pulsante Interrompi indicizzazione viene disabilitato. • Al termine della pianificazione, il pulsante Interrompi indicizzazione viene disabilitato.

Opzione	Descrizione
Posizione indice	

Opzione	Descrizione
	<p>Gli indici vengono archiviati in cartelle condivise nelle posizioni seguenti:</p> <ul style="list-style-type: none"> • Posizione indice principale (indici, correttori ortografici): gli indici principale e correttore ortografico archiviati in questa posizione. Durante una ricerca, i risultati iniziali vengono recuperati mediante l'indice principale, mentre per recuperare i suggerimenti vengono utilizzati gli indici correttore ortografico. In una distribuzione della piattaforma BI in cluster questa posizione dovrebbe corrispondere al file system condiviso accessibile da tutti i nodi del cluster. • Posizione dati persistenti (archivi contenuti): in questa posizione si trova l'archivio contenuti. Viene creata dalla posizione dell'indice principale con cui rimane sincronizzata. L'archivio contenuti viene utilizzato per generare facet ed elabora i riscontri iniziali generati da Posizione indice principale. In una distribuzione della piattaforma BI in cluster, gli archivi di contenuti vengono generati in corrispondenza di ciascun nodo. <p>La posizione dei dati persistenti è l'unica posizione di indice interessata dall'ambiente cluster, poiché contiene le cartelle degli archivi contenuti. Se un computer utilizza un solo servizio di ricerca, esisterà solo una posizione dell'archivio contenuti. Ad esempio, {boj.enterprise.home}\data\PlatformSearchData\workspace\<Nome server>\ContentStores.</p> <p>Tuttavia, in un ambiente cluster, se sono presenti più servizi di ricerca, ognuno di essi avrà una sola posizione dell'archivio contenuti. Se ad esempio sono in esecuzione due istanze di un server, le posizioni dell'archivio contenuti saranno le seguenti:</p> <ol style="list-style-type: none"> a. {boj.enterprise.home}\data\PlatformSearchData\workspace\<Nome server>\ContentStores. b. {boj.enterprise.home}\data\PlatformSearchData\workspace\<Nome server 1>\ContentStores. <ul style="list-style-type: none"> • Posizione dati non persistenti (file surrogati temporanei, Delta indexes): in questa posizione gli indici delta vengono creati e archiviati temporaneamente prima di essere uniti all'indice principale. Una volta uniti all'indice principale, gli indici vengono eliminati da questa posizione. Inoltre in questa posizione vengono creati e archiviati temporaneamente i file surrogati (output degli estrattori) fino a quando non vengono convertiti in indici delta. <p>Nota:</p> <ul style="list-style-type: none"> • Tutte le posizioni degli indici devono essere percorsi condivisi. • È necessario fare clic su Interrompi indicizzazione per modificare la posizione dell'indice. • Se si modifica la posizione di un indice, copiare il contenuto in una nuova posizione. In caso contrario, le informazioni relative all'indice

Opzione	Descrizione
	esistente verranno perdute.
Livello di indicizzazione	<p>È possibile regolare il contenuto della ricerca impostando il livello di indicizzazione nei seguenti modi:</p> <ul style="list-style-type: none"> • Metadati piattaforma: viene creato un indice solo per le informazioni sui metadati della piattaforma, ad esempio titoli, parole chiave e descrizioni dei documenti. • Metadati piattaforma e documento: questo indice include i metadati della piattaforma e del documento. I metadati del documento includono la data di creazione, la data di modifica e il nome dell'autore. • Contenuto completo: questo indice include i metadati della piattaforma, i metadati del documento e altri contenuti quali: <ul style="list-style-type: none"> • il contenuto effettivo del documento • il contenuto dei prompt e degli elenchi di valori • grafici ed etichette <p>Nota: quando si modifica il livello di indicizzazione, l'indicizzazione viene reinizializzata per l'intero repository della piattaforma BI.</p>
Tipi contenuto	<p>È possibile selezionare i seguenti tipi di contenuto per l'indicizzazione:</p> <ul style="list-style-type: none"> • Crystal Reports • Web Intelligence • Universo • Spazio di lavoro BI • Microsoft PowerPoint • Adobe Acrobat • Rich Text • Testo • Microsoft Word • Microsoft Excel

Opzione	Descrizione
Rigenera indice	<p>Questa opzione elimina l'indice esistente e reindicizza l'intero repository.</p> <p>È possibile selezionare l'opzione Rigenera indice indipendentemente dal fatto che l'indicizzazione sia in esecuzione o sia stata interrotta. L'indice esistente viene eliminato quando si salvano le modifiche alla pagina delle proprietà. Se invece l'indicizzazione è attualmente interrotta, la rigenerazione dell'indice non ha inizio fino a quando non viene riavviata l'indicizzazione.</p> <p>Se non si desidera che Ricerca piattaforma indicizzi nuovamente i documenti, deselegnare l'opzione Rigenera indice prima di fare clic su Avvia indicizzazione.</p>
Documenti esclusi dall'indicizzazione	<p>L'opzione Documenti esclusi dall'indicizzazione consente di escludere documenti dall'indicizzazione. Ad esempio, può essere opportuno escludere dalla ricerca i report Crystal di dimensioni molto elevate per evitare eccessivi carichi di lavoro delle risorse del Report Application Server. Analogamente, è possibile evitare che le pubblicazioni con centinaia di report personalizzati vengano indicizzate.</p> <p>Escludendo documenti specifici, è possibile evitare che vengano aperti in Ricerca piattaforma. È importante notare che, se un documento è stato indicizzato prima di essere inserito in questo gruppo, potrebbe ancora essere accessibile per le ricerche. Per essere sicuri che i documenti del gruppo Documenti esclusi dall'indicizzazione non siano accessibili, è necessario generare nuovamente l'indice.</p> <p>Per impostazione predefinita, solo l'account Administrator ha il controllo completo dell'opzione Documenti esclusi dall'indicizzazione. Gli altri utenti con i diritti seguenti possono solo aggiungere documenti al gruppo Documenti esclusi dall'indicizzazione:</p> <ul style="list-style-type: none"> • Diritti di visualizzazione e modifica per la categoria • Modifica diretta del documento

5. Fare clic su **Salva e chiudi**.

Nota:

Se un utente non seleziona l'opzione **Rigenera indice** e cambia il livello di indicizzazione oppure seleziona o deselegnare gli estrattori, l'indice viene aggiornato in modo incrementale senza che venga eliminato l'indice esistente.

18.1.3.15 Configurazione dell'integrazione Web BEx

Le applicazioni Web BEx sono applicazioni basate sul Web di Business Explorer (BEx) in SAP NetWeaver Business Warehouse (BW), utilizzate per l'analisi dei dati, la creazione di report e le applicazioni analitiche sul Web.

Business Explorer è la suite di SAP NetWeaver Business Intelligence che fornisce strumenti flessibili per la creazione di report e l'analisi a supporto delle attività legate all'analisi strategica e al decision making. Tali strumenti includono funzioni di query, creazione di report e analisi. Come dipendente che dispone di diritti di accesso, l'utente può valutare i dati cronologici o correnti a vari livelli di dettaglio e da prospettive diverse, sia sul Web che in Microsoft Excel.

Gli utenti possono accedere ai dati da SAP NetWeaver Portal o da BI Launch Pad della piattaforma SAP BusinessObjects Business Intelligence. Gli autori delle applicazioni Web BEx possono eseguire le applicazioni Web direttamente in BI Launch Pad da BEx Web Application Designer.

Per integrare le applicazioni Web BEx nella piattaforma BI, è necessario seguire questa procedura di configurazione:

1. Impostare un server per le applicazioni Web BEx nella console CMC (Central Management Console). È possibile utilizzare un server generale o autonomo per le applicazioni Web BEx.

Suggerimento:

È consigliabile impostare un server autonomo per le applicazioni Web BEx, poiché il server generale normalmente viene utilizzato da molti altri servizi.

2. Configurare le impostazioni del server.
3. Verificare la connessione al sistema BW.
4. Per garantire che gli autori possano eseguire le applicazioni Web BEx direttamente in BI Launch Pad da BEx Web Application Designer, definire le impostazioni rilevanti nella tabella **Connected Portals** (RSPOR_T_PORTAL) nel sistema BW.

Eseguita la configurazione del server della piattaforma BI, gli utenti possono aprire le applicazioni Web BEx in BI Launch Pad. Possono quindi spostarsi tra i dati e salvare le applicazioni Web BEx come segnalibri nei Preferiti del browser.

Limitazione:

L'integrazione è supportata nelle versioni di SAP NetWeaver seguenti:

- SAP NetWeaver 7.0 Enhancement Package 1 Support Package Stack 8
- SAP NetWeaver 7.3 Support Package Stack 1

poiché lo stack SAP NetWeaver Java non è necessario per questa integrazione, si applicano le limitazioni riportate di seguito.

- Information Broadcasting non è supportato.

- Poiché il portale e Knowledge Management di SAP NetWeaver non sono necessari, le operazioni che richiedono l'integrazione dei documenti e l'uso del portale non sono supportate nelle applicazioni Web BEx.
- La voce **Web Report** non è supportata. È consigliabile utilizzare SAP Crystal Reports per la creazione di report formattati.
- Per creare versioni stampate delle applicazioni Web BEx, viene utilizzata la libreria di esportazione per SAP Business Explorer. I servizi ADS (Adobe Document Services) non sono disponibili.
- Le applicazioni Web BEx integrate nella piattaforma BI possono contenere solo origini dati archiviate nel sistema BW principale. Nell'amministrazione del sistema viene definito il sistema configurato come sistema BW principale nella piattaforma BI.
- Il Single Sign On tra la piattaforma BI e il sistema SAP NetWeaver BW non è abilitato. Per ogni sessione della piattaforma BI, gli utenti delle applicazioni Web BEx devono accedere al sistema principale BW corrispondente.
- L'interfaccia report/report da e verso applicazioni Web BEx non è supportata. I comandi corrispondenti non verranno eseguiti.
- Non sono supportati i cruscotti basati sulle query BEx o sulle viste delle query e create con SAP BusinessObjects Dashboards.

Per ulteriori informazioni sulle funzionalità delle applicazioni Web BEx, consultare il SAP Help Portal all'indirizzo <http://help.sap.com>: **SAP NetWeaver 7.3 > SAP NetWeaver Library: Function-Oriented View > Business Warehouse > SAP Business Explorer > BEx Web > Analysis & Reporting: BEx Web Applications.**

Per ulteriori informazioni sull'accesso e il salvataggio delle applicazioni Web BEx in BI Launch Pad, consultare il *Manuale dell'utente di BI Launch Pad* all'indirizzo <http://help.sap.com>.

Argomenti correlati

- [Avvio di un server per le applicazioni Web BEx](#)
- [Avvio di un server autonomo per le applicazioni Web BEx](#)
- [Configurazione delle impostazioni server](#)
- [Verifica della connessione al sistema BW](#)
- [Configurazione di una connessione tra BEx Web Application Designer e la piattaforma BI](#)

18.1.3.15.1 Avvio di un server per le applicazioni Web BEx

Prima di potere eseguire questa attività, Adaptive Processing Server deve essere in stato di arresto.

1. Collegarsi alla Central Management Console (CMC).
2. Scegliere **Server**.
3. Espandere il nodo **Categorie di servizio** e scegliere **Servizi di analisi**.
4. Selezionare **Adaptive Processing Server** e scegliere **Seleziona servizi** nel menu di scelta rapida.
5. Spostare il **Servizio applicazioni Web BEx** dall'elenco **Servizi disponibili** all'elenco Servizi a destra.
6. Riavviare il Servizio applicazioni Web BEx riavviando l'Adaptive Processing Server.

18.1.3.15.2 Avvio di un server autonomo per le applicazioni Web BEx

1. Collegarsi alla Central Management Console (CMC).
2. Scegliere **Server**.
3. Espandere il nodo **Categorie di servizio** e scegliere **Servizi di analisi**.
4. Selezionare **Adaptive Processing Server** e scegliere **Duplica server** nel menu di scelta rapida.
5. Immettere un nome per il server (ad esempio AdaptiveProcessingServer) e selezionare il nodo richiesto nella casella **Duplica su nodo**.
6. Selezionare il server duplicato e scegliere **Seleziona servizi** nel menu di scelta rapida.
7. Selezionare il **Servizio applicazioni Web BEx** nell'elenco **Servizi disponibili** e spostarlo nell'elenco Servizi a destra.
8. Avviare il Servizio applicazioni Web BEx avviando il nuovo Adaptive Processing Server.

18.1.3.15.3 Configurazione delle impostazioni server

1. Collegarsi alla Central Management Console (CMC).
2. Scegliere **Server**.
3. Espandere il nodo **Categorie di servizio** e scegliere **Servizi di analisi**.
4. Selezionare il server che ospita le applicazioni Web BEx e scegliere **Proprietà** nel menu di scelta rapida.
5. In **Configurazione del servizio applicazioni Web BEx**, nell'area "Servizio applicazioni Web BEx", definire le impostazioni seguenti:
 - a. Verificare e modificare se necessario il numero massimo di sessioni client.
 - b. In **SAP BW Master System** immettere il nome della connessione OLAP al sistema BW creato nella piattaforma BI. Il nome predefinito è **SAP_BW**.
 - c. Immettere il nome della **Destinazione RFC server JCo** specificato nel sistema BW nell'area **Configuration of RFC Connections** (codice transazione sm59).
 - d. Immettere il nome dell'**Host gateway server JCo** definito nel sistema BW nell'area **Configuration of RFC Connections** (codice transazione sm59).
 - e. Immettere il nome del **Servizio gateway server JCo** definito nel sistema BW nell'area **Configuration of RFC Connections** (codice transazione sm59).
 - f. Verificare e modificare se necessario il **Conteggio connessione server JCo**.
6. Scegliere **Salva e chiudi**.
7. Selezionare il server che ospita le applicazioni Web BEx e scegliere **Riavvia server** nel menu di scelta rapida.

Per applicare le impostazioni selezionate, è necessario riavviare il server.

Nota:

prima di riavviare il server, è necessario che sia stata creata la destinazione RFC nel sistema ABAP.

Argomenti correlati

- [Creazione di una destinazione RFC nel sistema ABAP](#)

18.1.3.15.4 Verifica della connessione al sistema BW

1. Collegarsi alla Central Management Console (CMC).
2. Scegliere **Connessioni OLAP**.
3. Verificare se è stata stabilita una connessione al sistema BW. Se non è stata abilitata, fare clic sul pulsante **Nuova connessione** per impostarne una. Il nome predefinito della connessione è SAP_BW. È possibile immettere un nome diverso.
4. Verificare di aver selezionato **Predefinita** in **Autenticazione** e di aver definito le voci necessarie per l'utente e la password.

Nota:

Questo account utente è necessario per la destinazione RFC del server JCo che consente l'integrazione di BEx Web Application Designer, del sistema BW e della piattaforma BI.

Suggerimento:

per rendere sicura la connessione, accertarsi che solo gli amministratori dispongano dei diritti di accesso necessari.

- a. A tale scopo, selezionare con il pulsante destro del mouse la connessione al sistema BW (nome predefinito SAP_BW) e scegliere **Protezione utente**.
- b. Definire le impostazioni di protezione necessarie e assegnare i diritti di accesso solo agli amministratori.

18.1.3.15.5 Configurazione di una connessione tra BEx Web Application Designer e la piattaforma BI

Per garantire che gli autori possano eseguire le applicazioni Web BEx direttamente in BI Launch Pad da BEx Web Application Designer, è necessario definire le impostazioni rilevanti nella tabella **Connected Portals** (RSPOR_T_PORTAL) presente nel sistema BW.

1. Nel sistema BW chiamare la transazione SM30 (**Table View Maintenance**).
2. Al di sotto di **Table/View** immettere RSPOR_T_PORTAL.
3. Scegliere **Maintain**.
4. Per creare una nuova voce, scegliere **New Entries**.
5. Definire le seguenti impostazioni:
 - a. Per garantire l'integrazione tra il sistema BW e la piattaforma BI, è necessario creare una destinazione RFC nella transazione SM59. Immettere questa destinazione RFC al di sotto di **Destination**.
 - b. Selezionare **Standard Portal**. In questo modo le applicazioni Web in Web Application Designer vengono sempre chiamate nella piattaforma BI.
 - c. Sotto **URL Prefix** immettere l'URL del server del contenitore applicazioni Web (WACS) della piattaforma BI, inclusi il protocollo, la porta e il nome host come nell'esempio `http://<wacs><dominio>:<porta>`.
 - d. In **Platform** selezionare **BOE**.
 - e. Selezionare **Use SAP Export Lib (PDF)** se si desidera attivare la libreria di esportazione di SAP Business Explorer per consentire l'esportazione dei file PDF, PostScript e PCL dalle applicazioni Web BEx.

6. Salvare le voci.

Argomenti correlati

- [Creazione di una destinazione RFC nel sistema ABAP](#)

Creazione di una destinazione RFC nel sistema ABAP

Per integrare il sistema BW e la piattaforma BI, è necessario creare una destinazione RFC, che consente la comunicazione tra il sistema BW e la piattaforma BI.

1. Chiamare **Configuration of RFC Connections** (codice transazione SM59).
2. Scegliere **Create**.
3. Mantenere la destinazione RFC:
 - a. Immettere un nome per la destinazione RFC.
 - b. Selezionare **T for TCP/IP connection** come tipo di connessione.
 - c. Immettere una descrizione.
È possibile mantenere la descrizione della lingua di destinazione RFC.
 - d. In **Technical Settings** selezionare **Registered Server Program** come tipo di attivazione.
 - e. In **Technical Settings** immettere l'ID del programma.
L'ID del programma deve essere identico a quello (destinazione RFC del server JCo) specificato per la creazione della destinazione di questo sistema BW nel server della piattaforma BI.
 - f. In **Technical Settings**, nell'area **Gateway Options**, immettere l'host gateway e il servizio gateway che il server della piattaforma BI utilizza per comunicare con il sistema BW.
4. Nella pagina della scheda **Logon & Security** attivare l'opzione **Send SAP Logon Ticket**.
5. Salvare le voci.

Argomenti correlati

- [Configurazione delle impostazioni server](#)

18.1.3.16 Configurazione di Single Sign On per SAP HANA

Nell'area "Applicazioni" della CMC nella piattaforma BI, è possibile configurare Single Sign On (SSO) per le connessioni ai database SAP HANA. SSO viene implementato utilizzando SAML (Security Assertion Markup Language).

Una volta stabilita una sessione della piattaforma BI, sarà possibile generare un ticket SAML che potrà essere utilizzato dall'utente per accedere a SAP HANA senza fornire una password.

Di seguito è illustrato il workflow di base implicato nella connessione alle origini dati SAP HANA:

1. Un amministratore configura una relazione di trust tra SAP HANA e la piattaforma BI nella CMC.

2. Un utente accede alla piattaforma BI con uno dei provider di autenticazione supportati.
3. Se gli ID utente di SAP HANA e della piattaforma BI corrispondono, la piattaforma BI può generare un'asserzione SAML che SAP HANA può accettare per stabilire una connessione per l'utente corrente. L'ID utente passato a SAP HANA è l'ID utente della piattaforma BI dell'utente che ha effettuato l'accesso.
4. Un'applicazione client della piattaforma BI crea una connessione SAP HANA.

Nota:

Prima di configurare Single Sign On per SAP HANA con SAML, è necessario configurare SSL nel computer SAP HANA. Per informazioni dettagliate, consultare la documentazione relativa a SAP HANA.

18.1.3.16.1 Per creare una connessione SAP HANA

1. Recuperare i parametri del database SAP HANA.
 - a. Aprire l'applicazione SAP HANA Studio.
 - b. Aprire la pagina delle proprietà del sistema e individuare l'URL per la connessione al database.
 - c. Registrare il nome del computer host e il numero di porta.
Queste informazioni saranno necessarie nel passaggio 2.
2. Configurare una connessione SAP HANA nella piattaforma BI.
 - a. Passare all'area "Applicazioni" della CMC e fare doppio clic su **Autenticazione HANA**.
 - b. Nella finestra di dialogo "Autenticazione HANA" fare clic sul pulsante **Crea una connessione**.
Viene visualizzata la finestra di dialogo "Crea connessione di autenticazione HANA".
 - c. Immettere il nome del computer host e il numero di porta registrati nel passaggio 1.
 - d. Nel campo "ID provider di identità univoco" specificare un valore che verrà utilizzato per la distribuzione della piattaforma BI.
 - e. Fare clic su **Genera**.
Viene creato un certificato nella casella "Certificato Base64 provider di identità".
3. Configurare la distribuzione SAP HANA.
 - a. Utilizzando l'applicazione SAP HANA Studio eseguire il comando SQL seguente per abilitare la piattaforma BI come provider ID:


```
CREATE SAML PROVIDER UNIQUE ID WITH SUBJECT 'C=CA, ST=BC, O=SAP, OU=BOE, CN=UNIQUE ID' ISSUER 'C=CA, ST=BC, O=SAP, OU=BOE, CN=UNIQUE ID'
```

UNIQUE ID è l'"ID provider di identità univoco" specificato nel passaggio 2.
 - b. Copiare il certificato dalla CMC nel file `trust.pem` all'interno della directory `~/ .ssl` dell'utente creato quando è stato installato SAP HANA.
Il nome utente è `<Codice3caratteri>adm`. Se ad esempio l'identificativo dell'istanza di SAP HANA è `xyz`, il nome utente è `xyzadm`.

Nota:

A questo punto è possibile verificare se il file `key.pem` è presente nella directory `~/ .ssl`. Se non è presente, SAP HANA non è stato configurato correttamente per l'utilizzo di SSL. Prima di configurare Single Sign On per SAP HANA con SAML, è necessario configurare SSL nel computer SAP HANA. Per informazioni dettagliate, consultare la documentazione relativa a SAP HANA.

- c. Riavviare SAP HANA.
- d. Utilizzare i comandi seguenti per creare un utente in SAP HANA per cui la piattaforma BI possa generare ticket:

```
CREATE USER HANAUserName PASSWORD HANAUserPassword;
ALTER USER HANAUserName ENABLE SAML;
ALTER USER HANAUserName ADD IDENTITY 'BIPUserName' FOR SAML PROVIDER BIPUniqueIdentityProviderID;
```

BIPUserName è il nome completo dell'utente della piattaforma BI.

Esempio:

```
CREATE USER Administrator PASSWORD Abcd1234;
ALTER USER Administrator ENABLE SAML;
ALTER USER Administrator ADD IDENTITY 'Administrator' FOR SAML PROVIDER BIPDeployment1;
```

In alternativa, è possibile utilizzare un utente esistente ed eseguire solo i comandi **ALTER** precedenti.

4. Verificare la configurazione SAP HANA.

- a. Passare all'area "Applicazioni" della CMC e fare doppio clic su **Autenticazione HANA**.
- b. Nella finestra di dialogo "Autenticazione HANA" aprire la connessione creata nel passaggio 2. Viene visualizzata la finestra di dialogo "Modifica connessione di autenticazione HANA".
- c. Al di sotto di "Verifica la connessione per questo utente" immettere un nome utente e fare clic sul pulsante **Verifica connessione** per verificare che le impostazioni della connessione siano valide.

Immettere ad esempio il nome utente Administrator. Se le impostazioni non sono valide, viene visualizzato un messaggio di errore. È possibile provare a eseguire i seguenti passaggi per risolvere il problema segnalato:

- Verificare che nessun altro certificato del file `trust.pem` contenga un componente Subject o Issuer che presenta lo stesso valore per la proprietà CN. Per visualizzare i componenti del certificato, cercare in Internet "decodificatore certificati x509" per individuare un decodificatore di certificati.
- Provare a eseguire i comandi seguenti per verificare la configurazione sul lato HANA:

```
select * from "SAML_PROVIDERS"
select user_name, is_saml_enabled from users where user_name = '<UserName>'
select * from "PUBLIC"."SAML_USER_MAPPINGS"
```

Nota:

Se il file `key.pem` non è presente nella directory `.ssl`, SAP HANA non è stato configurato correttamente per l'utilizzo di SSL.

18.1.3.16.2 Impostazioni della connessione SAP HANA

Nella tabella di seguito sono riportate le impostazioni disponibili nella CMC per la configurazione delle connessioni SAP HANA.

Impostazione	Descrizione
"Nome host HANA"	Fornire il nome dell'host SAP HANA.
"Porta HANA"	Fornire il numero di porta per l'host SAP HANA.
"ID provider di identità univoco"	Nome univoco in una determinata installazione di HANA. Per gli accessi l'installazione di HANA accetta i ticket firmati correttamente da questo nome di provider di identità.
"Certificato Base64 provider di identità"	Se si fa clic su Genera , viene creato un certificato nel campo "Certificato Base64 provider di identità". Copiare il certificato nel file <code>trust.pem</code> della distribuzione di SAP HANA. Il certificato stabilisce la relazione di trust tra SAP HANA e la piattaforma BI. Lo stesso provider di identità esterno viene identificato mediante un certificato X509, che viene utilizzato per firmare tutte le asserzioni di identità. È necessario che il certificato sia codificato Base64.

18.2 Gestione delle applicazioni mediante le proprietà BOE.war

18.2.1 File WAR BOE

È possibile modificare le impostazioni delle applicazioni Web della piattaforma BI sovrascrivendo le proprietà predefinite del file BOE.war. Questo file viene distribuito sul computer che ospita il server di applicazioni Web. Per informazioni dettagliate sulla distribuzione del file, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

Le proprietà contenute nel file BOE.war controllano le specifiche relative al comportamento di accesso predefinito, i metodi di autenticazione predefiniti e le impostazioni di Single Sign On. È possibile specificare due tipi di proprietà:

- Proprietà globali: influenzano tutte le applicazioni Web contenute nel file BOE.war.
- Proprietà specifiche dell'applicazione: impostazioni delle proprietà che influenzano una specifica applicazione Web.

Per modificare le proprietà predefinite, utilizzare la directory di configurazione personalizzata per salvare le nuove impostazioni relative alle proprietà globali o specifiche dell'applicazione. Per impostazione

predefinita la directory si trova in C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom.

Non modificare le proprietà nella directory config\default.

Nota:

In alcuni server di applicazioni Web, come la versione di Tomcat inclusa nella piattaforma BI, è possibile accedere al file BOE.war direttamente. In tale scenario è possibile specificare direttamente le impostazioni personalizzate senza annullare la distribuzione del file WAR. Quando non è possibile accedere direttamente alle applicazioni Web distribuite, è necessario annullare la distribuzione del file, personalizzarlo e ridistribuirlo. Per ulteriori informazioni consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

18.2.1.1 Proprietà BOE.war globali

Nella tabella che segue sono elencate le impostazioni incluse nel file `global.properties` predefinito per BOE.war. Per sovrascrivere le impostazioni, creare un nuovo file in C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom.

Impostazione	Valori predefiniti	Descrizione
<code>persistentcookies.enabled</code>	<code>persistentcookies.enabled=true</code>	Abilita o disabilita i cookie permanenti nella pagina di accesso all'applicazione Web.
<code>siteminder.authentication</code>	<code>siteminder.authentication=secLDAP</code>	Specifica il metodo di autenticazione da utilizzare con SiteMinder. Le uniche opzioni sono <code>secLDAP</code> e <code>secwinAD</code> .
<code>siteminder.enabled</code>	<code>siteminder.enabled=false</code>	Abilita e disabilita l'autenticazione con SiteMinder.
<code>sso.enabled</code>	<code>sso.enabled=false</code>	Abilita e disabilita il Single Sign On (SSO) nella piattaforma BI.
<code>sso.sap.primary</code>	<code>sso.sap.primary=false</code>	Impostare su <code>true</code> se si desidera utilizzare il SSO SAP come meccanismo di Single Sign On principale dell'applicazione. Si applica solo a casi in cui sia utilizza sia il SSO SAP che quello SiteMinder.
<code>max.tree.children.threshold</code>	<code>max.tree.children.threshold=200</code>	Specifica la soglia in corrispondenza della quale il controllo dell'elenco strutturato non visualizza tutti i nodi e visualizza invece un messaggio "Troppi elementi secondari".

Impostazione	Valori predefiniti	Descrizione
trus ted.auth.sha red.secret	Nessuno	Specifica il nome di variabile della sessione utilizzato per recuperare il segreto per Autenticazione affidabile. Si applica solo se si utilizza la sessione Web per passare il segreto condiviso.
trus ted.auth.user.pa ram	Nessuno	Specifica la variabile utilizzata per recuperare il nome utente per Autenticazione affidabile. Può essere impostato su uno dei valori seguenti: <ul style="list-style-type: none"> • Header • URL Parameter • Cookie • Session
trus ted.auth.user.re trieval	Nessuno	Specifica il metodo utilizzato per recuperare il nome utente per Autenticazione affidabile. Può essere impostato su uno dei valori seguenti: <ul style="list-style-type: none"> • "REMOTE_USER" • "HTTP_HEADER" • "COOKIE" • "QUERY_STRING" • "WEB_SESSION" • "USER_PRINCIPAL" Impostare su empty per disabilitare Autenticazione affidabile.
trus ted.auth.user.na mespace.en abled	trusted.auth.user.namespace.enabled=false	Abilita e disabilita il collegamento dinamico degli alias ad account utente esistenti. Se la proprietà è impostata su <code>true</code> , Autenticazione affidabile utilizza il collegamento degli alias per autenticare gli utenti nella piattaforma BI. Con il collegamento degli alias, il server di applicazioni può funzionare come un provider di servizi SAML e abilitare quindi Autenticazione affidabile a fornire il SSO SAML al sistema. Se la proprietà è impostata su <code>false</code> , Autenticazione affidabile utilizza la corrispondenza dei nomi per autenticare gli utenti.

Impostazione	Valori predefiniti	Descrizione
vintela.enabled	<pre>vintela.enabled=false idm.realm=YOUR_REALM idm.princ=YOUR_PRINCIPAL idm.allowUnsecured=true idm.allowNTLM=false idm.logger.name=simple idm.logger.props=error-log.properties</pre>	Utilizzato per abilitare o disabilitare le impostazioni Vintela per l'autenticazione Windows AD.
pinger.showWarningDialog.cmc	<pre>pinger.showWarningDialog.cmc=true</pre>	Specifica se visualizzare o meno la finestra di dialogo di avviso con il messaggio che indica che la sessione corrente scadrà presto nella CMC.
pinger.showWarningDialog.bi-launchpad	<pre>pinger.showWarningDialog.bi-launchpad=true</pre>	Specifica se visualizzare o meno la finestra di dialogo di avviso con il messaggio che indica che la sessione corrente scadrà presto in BI Launch Pad.
pinger.warningPeriod.pingIncrementsInSeconds	<pre>pinger.warningPeriod.pingIncrementsInSeconds=15</pre>	Specifica la frequenza di invio di una richiesta del server Web durante la visualizzazione del messaggio di avviso della scadenza della sessione. Questo è importante per la sincronizzazione della finestra di dialogo di avviso in diverse applicazioni.
pinger.warningPeriod.lengthInMinutes	<pre>pinger.warningPeriod.lengthInMinutes=5</pre>	Specifica con quanto anticipo visualizzare l'avviso prima della scadenza della sessione.
logoff.on.websession.expiry	<pre>logoff.on.websession.expiry=true</pre>	Specifica se tutte le sessioni dell'applicazione vengono scollegate allo scadere della sessione Web.
pinger.enabled	<pre>pinger.enabled=true</pre>	Abilita o disabilita il meccanismo di invio di messaggi di avviso relativi alla scadenza della sessione.
system.com.sap.bip.jcomanager.destinations.maxsize	<pre>system.com.sap.bip.jcomanager.destinations.maxsize=1000</pre>	Specifica il numero massimo di connessioni Java nella cache.
httpproxy.username	<pre>httpproxy.username=myusername</pre>	Specifica il nome utente per accedere al server proxy HTTP.
httpproxy.password	<pre>httpproxy.password=mypassword</pre>	Specifica la password per accedere al server proxy HTTP.

Impostazione	Valori predefiniti	Descrizione
<code>logon.embed.secret</code>	Nessuno	Segreto condiviso tra un portale che incorpora le applicazioni della piattaforma BI e il server di applicazioni della piattaforma BI, utilizzato per determinare se le applicazioni della piattaforma BI possono essere incorporate in modo sicuro in altre pagine.
<code>logon.embed.timeout</code>	<code>logon.embed.timeout=300</code>	Numero di secondi dopo il quale le applicazioni della piattaforma BI, come BI Launch Pad, rifiuteranno di essere incorporate in un portale. Verificare che i clock di sistema sui computer del server Web della piattaforma BI e del server del portale rientrino nel numero di secondi indicato.
<code>iview.autologoff</code>	<code>iview.autologoff=true</code>	Impostare su <code>true</code> per consentire la disconnessione automatica immediata per SAP NetWeaver iViews.
<code>pinger.showWarningDialog</code>	<code>pinger.showWarningDialog=true</code>	Specifica se visualizzare o meno la finestra di dialogo di avviso con il messaggio che indica che la sessione corrente scadrà presto. Non si applica alla CMC e a BI Launch Pad.

18.2.1.2 Proprietà di BI Launch Pad

Nella tabella che segue sono elencate le impostazioni incluse nel file `bilaunchpad.properties` predefinito per il file `BOE.war`. Per sovrascrivere le impostazioni, creare un nuovo file in `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Impostazione	Descrizione																		
app.name	Specifica il nome di visualizzazione dell'applicazione. Il nome appare sulla pagina del titolo dell'applicazione Web e sulla schermata di accesso. Impostazione predefinita: app.name=BI launch pad																		
app.name.short	Specifica il nome di visualizzazione dell'applicazione. Il nome appare sulla pagina del titolo dell'applicazione Web e sulla schermata di accesso. Impostazione predefinita: app.name.short=BI launch pad																		
app.url.name	Specifica il nome dell'URL dell'applicazione, preceduto dal carattere "/". Impostazione predefinita: app.url.name=/BI																		
authentication.default	<p>Specifica il metodo di autenticazione predefinito utilizzato per autenticare gli utenti nell'applicazione. È possibile utilizzare uno dei valori seguenti per questa impostazione:</p> <table> <tr> <th>Autenticazione</th><th>Valore di impostazione</th></tr> <tr> <td>Enterprise</td><td>SecEnterprise</td></tr> <tr> <td>LDAP</td><td>secLDAP</td></tr> <tr> <td>Windows AD</td><td>secWinAD</td></tr> <tr> <td>SAP</td><td>secSAPR3</td></tr> <tr> <td>PeopleSoft</td><td>secpsenterprise</td></tr> <tr> <td>JD Edwards</td><td>secPSE1</td></tr> <tr> <td>Siebel</td><td>secSiebel7</td></tr> <tr> <td>Oracles EBS</td><td>secOraApps</td></tr> </table> <p>Impostazione predefinita: authentication.default=secEnterprise</p>	Autenticazione	Valore di impostazione	Enterprise	SecEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpsenterprise	JD Edwards	secPSE1	Siebel	secSiebel7	Oracles EBS	secOraApps
Autenticazione	Valore di impostazione																		
Enterprise	SecEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpsenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel7																		
Oracles EBS	secOraApps																		
authentication.visible	Specifica se gli utenti che accedono a BI Launch Pad hanno la possibilità di visualizzare e modificare il metodo di autenticazione. Impostazione predefinita: authentication.visible=false																		
cms.default	Specifica il nome CMS predefinito. Impostazione predefinita: cms.default=[name of host machine]																		
cms.visible	Specifica se gli utenti che accedono a BI Launch Pad hanno la possibilità di visualizzare e modificare il nome CMS. Impostazione predefinita: cms.visible=true																		
dialogue.prompt.enabled	Specifica se visualizzare un messaggio di avviso quando gli utenti escono da una pagina di input in una finestra di dialogo. Impostazione predefinita: dialogue.prompt.enabled=false																		

Impostazione	Descrizione
<code>logontoken.enabled</code>	Specifica se abilitare o meno la creazione dei token per la sessione dopo l'accesso di un utente a BI Launch Pad. Il token verrà memorizzato in un cookie. Impostazione predefinita: <code>logontoken.enabled=false</code>
<code>SMTPFrom</code>	<p>Abilita o disabilita il campo "From" durante la pianificazione di un oggetto in una destinazione. Impostazione predefinita: <code>SMTPFrom=true</code></p> <p>Se il valore è impostato su <code>false</code> il campo "Da" non viene visualizzato e il sistema cercherà di recuperare il valore di posta elettronica "Da" nell'ordine seguente:</p> <ol style="list-style-type: none">1. primo: dal report predefinito per un oggetto report.2. Secondo: dall'indirizzo di posta elettronica sul profilo utente dell'utente registrato.3. Infine, dal server del processo predefinito.
<code>url.exit</code>	Specifica l'URL a cui reindirizzare gli utenti dopo aver terminato la sessione BI Launch Pad. Questa impostazione si applica solo agli utenti che hanno ottenuto l'accesso all'applicazione attraverso un processo di verifica esterna.
<code>disable.locale.preference</code>	Abilita o disabilita la visualizzazione e la conseguente modifica delle preferenze di visualizzazione locali dell'utente relative a BI Launch Pad. Impostazione predefinita: <code>disable.locale.preference=false</code>

Impostazione	Descrizione
<code>extlogon.allow.logoff</code>	Abilita o disabilita automaticamente la disconnessione degli utenti dalle sessioni dopo aver chiuso la sessione BI Launch Pad. Impostare su false se si desidera che le sessioni non terminino automaticamente quando l'utente accede a BI Launch Pad. Impostazione predefinita: <code>extlogon.allow.logoff=true</code>
<code>logon.allowInsecureEmbedding</code>	Specifica se consentire di incorporare questa applicazione (come frame) in altre pagine senza passare un token incorporato valido. Impostazione predefinita: <code>logon.allowInsecureEmbedding=false</code>
<code>sso.types.and.order</code>	<p>Specifica un elenco delimitato da virgola dei tipi SSO da abilitare e l'ordine con cui vengono eseguiti.</p> <p>Un elenco vuoto indica che deve essere utilizzato l'ordinamento legacy.</p> <p>Se l'elenco è specificato, vengono ignorate le opzioni legacy.</p> <p>Opzioni valide: <code>vintela</code>, <code>trustedIIS</code>, <code>trustedHeader</code>, <code>trustedParameter</code>, <code>trustedCookie</code>, <code>trustedSession</code>, <code>trustedUserPrincipal</code>, <code>trustedVintela</code>, <code>trustedX509</code>, <code>sapSSO</code> e <code>siteminder</code>.</p> <p>Se nessuna delle opzioni desiderate è adatta, specificare: <code>none</code></p>

18.2.1.3 Proprietà OpenDocument

Nella tabella che segue sono elencate le impostazioni incluse nel file `opendocument.properties` predefinito per il file `BOE.war`. Per sovrascrivere le impostazioni, creare un nuovo file in `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Impostazione	Descrizione																		
app.name	Specifica il nome di visualizzazione dell'applicazione. Il nome appare sulla pagina del titolo dell'applicazione Web e sulla schermata di accesso. Impostazione predefinita: app.name=SAP BusinessObjects OpenDocument																		
app.name.short	Specifica il nome di visualizzazione dell'applicazione. Il nome appare sulla pagina del titolo dell'applicazione Web e sulla schermata di accesso. Impostazione predefinita: app.name.short=OpenDocument																		
authentication.default	<p>Specifica il metodo di autenticazione predefinito utilizzato per autenticare gli utenti nell'applicazione. È possibile utilizzare uno dei valori seguenti per questa impostazione:</p> <table> <tr> <th>Autenticazione</th><th>Valore di impostazione</th></tr> <tr> <td>Enterprise</td><td>SecEnterprise</td></tr> <tr> <td>LDAP</td><td>secLDAP</td></tr> <tr> <td>Windows AD</td><td>secWinAD</td></tr> <tr> <td>SAP</td><td>secSAPR3</td></tr> <tr> <td>PeopleSoft</td><td>secpssenterprise</td></tr> <tr> <td>JD Edwards</td><td>secPSE1</td></tr> <tr> <td>Siebel</td><td>secSiebel17</td></tr> <tr> <td>Oracles EBS</td><td>secOraApps</td></tr> </table> <p>Impostazione predefinita: authentication.default=secEnterprise</p>	Autenticazione	Valore di impostazione	Enterprise	SecEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpssenterprise	JD Edwards	secPSE1	Siebel	secSiebel17	Oracles EBS	secOraApps
Autenticazione	Valore di impostazione																		
Enterprise	SecEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpssenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel17																		
Oracles EBS	secOraApps																		
authentication.visible	Specifica se gli utenti che accedono a OpenDocument hanno la possibilità di visualizzare e modificare il metodo di autenticazione. Impostazione predefinita: authentication.visible=false																		
cms.default	Specifica il nome CMS predefinito. Impostazione predefinita: cms.default=[name of host machine]																		
cms.visible	Specifica se gli utenti che accedono a OpenDocument hanno la possibilità di visualizzare e modificare il nome CMS. Impostazione predefinita: cms.visible=true																		
logontoken.enabled	Specifica se abilitare o meno la creazione dei token per la sessione dopo l'accesso di un utente a OpenDocument. Il token verrà memorizzato in un cookie. Impostazione predefinita: logontoken.enabled=false																		
extlogon.allow.logoff	Abilita o disabilita automaticamente la disconnessione degli utenti dalle sessioni utente dopo aver chiuso la sessione OpenDocument. Impostare su false se si desidera che le sessioni utente non vengano terminate automaticamente quando l'utente si scollega da OpenDocument. Impostazione predefinita: extlogon.allow.logoff=true																		

Impostazione	Descrizione
<code>SAPLogonToken.enabled</code>	Specifica se consentire ai token di accesso SAP del servizio Web RESTful di eseguire l'autenticazione nella piattaforma BI. Il token di accesso SAP viene specificato dal valore X-SAP-LogonToken nell'intestazione richiesta dopo un accesso eseguito correttamente con l'URL del servizio Web RESTful. Impostazione predefinita: <code>SAPLogonToken.enabled=true</code>
<code>logon.allowInsecureEmbedding=false</code>	Specifica se consentire di incorporare questa applicazione (come frame) in altre pagine senza passare un token incorporato valido. Impostazione predefinita: <code>logon.allowInsecureEmbedding=false</code>
<code>sso.types.and.order</code>	<p>Specifica un elenco delimitato da virgola dei tipi SSO da abilitare e l'ordine con cui vengono eseguiti.</p> <p>Un elenco vuoto indica che deve essere utilizzato l'ordinamento legacy.</p> <p>Se l'elenco è specificato, vengono ignorate le opzioni legacy.</p> <p>Opzioni valide: <code>serializedSession</code>, <code>sapLogonToken</code>, <code>trustedIIS</code>, <code>trustedHeader</code>, <code>trustedParameter</code>, <code>trustedCookie</code>, <code>trustedSession</code>, <code>trustedUserPrincipal</code>, <code>trustedVintela</code>, <code>vintela</code>, <code>infoview</code>, <code>trustedX509</code>, <code>sapSSO</code> e <code>siteminder</code>.</p> <p>Se nessuna delle opzioni desiderate è adatta, specificare: <code>none</code></p>

18.2.1.4 Proprietà CMC

Nella tabella che segue sono elencate le impostazioni incluse nel file `cmc.properties` predefinito per BOE.war. Per sovrascrivere le impostazioni, creare un nuovo file in `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom`.

Impostazione	Descrizione																		
app.url.name	Specifica il nome dell'URL dell'applicazione, preceduto dal carattere "/". Impostazione predefinita: app.url.name=/CMC																		
authentication.default	<p>Specifica il metodo di autenticazione predefinito utilizzato per autenticare gli utenti nell'applicazione. È possibile utilizzare uno dei valori seguenti per questa impostazione:</p> <table> <tr> <th>Autenticazione</th><th>Valore di impostazione</th></tr> <tr> <td>Enterprise</td><td>SecEnterprise</td></tr> <tr> <td>LDAP</td><td>secLDAP</td></tr> <tr> <td>Windows AD</td><td>secWinAD</td></tr> <tr> <td>SAP</td><td>secSAPR3</td></tr> <tr> <td>PeopleSoft</td><td>secpsenterprise</td></tr> <tr> <td>JD Edwards</td><td>secPSE1</td></tr> <tr> <td>Siebel</td><td>secSiebel7</td></tr> <tr> <td>Oracles EBS</td><td>secOraApps</td></tr> </table> <p>Impostazione predefinita: authentication.default=secEnterprise</p>	Autenticazione	Valore di impostazione	Enterprise	SecEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpsenterprise	JD Edwards	secPSE1	Siebel	secSiebel7	Oracles EBS	secOraApps
Autenticazione	Valore di impostazione																		
Enterprise	SecEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpsenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel7																		
Oracles EBS	secOraApps																		
authentication.visible	Specifica se gli utenti che accedono alla CMC hanno la possibilità di visualizzare e modificare il metodo di autenticazione. Impostazione predefinita: authentication.visible=false																		
cms.default	Specifica il nome CMS predefinito. Impostazione predefinita: cms.default=[name of host machine]																		
cms.visible	Specifica se gli utenti che accedono alla CMC hanno la possibilità di visualizzare e modificare il nome CMS. Impostazione predefinita: cms.visible=true																		

Impostazione	Descrizione
<code>dialogue.prompt.enabled</code>	Specifica se visualizzare un messaggio di avviso quando gli utenti escono da una pagina di input in una finestra di dialogo. Impostazione predefinita: <code>dialogue.prompt.enabled=false</code>
<code>logontoken.enabled</code>	Specifica se abilitare o meno la creazione dei token per la sessione dopo l'accesso di un utente alla CMC. Il token verrà memorizzato in un cookie. Impostazione predefinita: <code>logontoken.enabled=false</code>
<code>SMTPFrom</code>	<p>Abilita o disabilita il campo "From" durante la pianificazione di un oggetto in una destinazione. Impostazione predefinita: <code>SMTPFrom=true</code></p> <p>Se il valore è impostato su <code>false</code> il campo "Da" non viene visualizzato e il sistema cercherà di recuperare il valore di posta elettronica "Da" nell'ordine seguente:</p> <ol style="list-style-type: none"> 1. primo: dal report predefinito per un oggetto report. 2. Secondo: dall'indirizzo di posta elettronica sul profilo utente dell'utente registrato. 3. Infine, dal server del processo predefinito.

18.3 Personalizzazione dei punti di ingresso per l'accesso a BI Launch Pad e OpenDocument

È possibile personalizzare la pagina di accesso delle applicazioni Web BI Launch Pad e OpenDocument. È ad esempio possibile personalizzare la pagina di accesso con un logo di società o un foglio di stile professionale oppure è possibile creare una pagina di accesso personalizzata che consenta l'autenticazione affidabile.

Per personalizzare la pagina di accesso, modificare il file `custom.jsp` archiviato nelle aree di applicazione di BI Launch Pad e OpenDocument dell'applicazione Web `BOE.war`, quindi ridistribuire l'applicazione Web `BOE.war` nel sistema della piattaforma BI. Gli utenti accedono al punto di ingresso per l'accesso personalizzato utilizzando un unico URL.

Per poter utilizzare questi esempi, è necessario avere familiarità con la distribuzione delle applicazioni Web della piattaforma BI. Per ulteriori informazioni consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

18.3.1 Percorsi dei file BI Launch Pad e OpenDocument

Le applicazioni Web BI Launch Pad e OpenDocument vengono incluse nel pacchetto all'interno del file dell'archivio Web BOE.war. Il percorso del file di archivio BOE.war viene definito nel file BOE.properties.

Nei sistemi Windows il file BOE.properties si trova nel percorso:

- `DIR_INSTALL_BOE\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf\apps\BOE.properties`

Nei sistemi UNIX il file BOE.properties si trova nel percorso:

- `DIR_INSTALL_BOE/sap_bobj/enterprise_xi40/wdeploy/conf/apps/BOE.properties`

Nelle tabelle seguenti viene definito il percorso dei file comuni all'interno del file dell'archivio Web BOE.war per entrambe le applicazioni, BI Launch Pad e OpenDocument.

Tabella 18 - 5: Percorsi dei file in BI Launch Pad

Nota:

l'applicazione Web BI Launch Pad veniva precedentemente chiamata InfoView.

Tipo di file	Posizione
Script di accesso personalizzato	WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp
Directory per i file aggiuntivi	WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources
URL di accesso personalizzato	http://<nomeserver>:<porta>/BOE/BI/custom.jsp

Tabella 18 - 6: Percorsi dei file in OpenDocument

Tipo di file	Posizione
Script di accesso personalizzato	WEB-INF\eclipse\plugins\webpath.OpenDocument\web\opendoc\custom.jsp
Directory per i file aggiuntivi	WEB-INF\eclipse\plugins\webpath.OpenDocument\web\noCacheCustomResources
URL di accesso personalizzato	http://<nomeserver>:<porta>/BOE/OpenDocument/opendoc/custom.jsp

18.3.2 Per definire una pagina di accesso personalizzata

È possibile personalizzare il punto di ingresso nella pagina di accesso della piattaforma BI. È ad esempio possibile creare una pagina di accesso personalizzata in cui viene visualizzato il logo di una società e viene utilizzato un foglio di stile professionale.

Modificare il file `custom.jsp` per personalizzare l'esperienza di accesso per gli utenti e inserire i file di supporto nella cartella `noCacheCustomResources`.

In questo esempio viene mostrato come creare una pagina di accesso personalizzata che reindirizza l'utente alla pagina di accesso standard.

1. Creare un file contenente il codice di accesso personalizzato e salvarlo con il nome `custom.js` nella cartella `noCacheCustomResources`.

In questo esempio viene definita una funzione che reindirizza l'utente alla pagina di accesso standard, `logon.jsp`.

```
function load() {window.location = "logon.jsp";}
```

2. Modificare il file `custom.jsp` per personalizzare la pagina di accesso.

In questo esempio viene visualizzato un messaggio di benvenuto e un collegamento ipertestuale che chiama il metodo `load` definito nel file `custom.js`.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">

<%@ page language= "java" contentType= "text/html; charset=utf-8"%>
<html>
<head> <title>Welcome</title>
</head>
<body>
<script type= "text/javascript" src= "noCacheCustomResources/custom.js"></script>
<p>Welcome to ABC corporation.</p>
<a href= "javascript:load()" ">Enter</a>
</body>
</html>
```

3. Ridistribuire l'applicazione Web `BOE.war` e riavviare il server Web.

18.3.3 Aggiunta di un'autenticazione affidabile all'accesso

Per abilitare l'autenticazione affidabile, impostare l'utente attendibile come attributo di sessione nel file `custom.jsp` e modificare le impostazioni di autenticazione in una copia del file `global.properties`. I valori della copia personalizzata del file `global.properties` hanno la precedenza sui valori predefiniti.

1. Modificare il file `custom.jsp` in modo da impostare un attributo di sessione che definisce l'utente attendibile.

```
request.getSession().setAttribute("TrustedUserAttribute", "TrustedUser");
```

2. Creare una copia personalizzata del file `global.properties` copiando `WEB-INF\config\default\global.properties` in `WEB-INF\config\custom\global.properties`.
3. Modificare `WEB-INF\config\custom\global.properties` in modo da abilitare SSO (Single Sign-On).

```
sso.enabled=true
```

4. Modificare `WEB-INF\config\custom\global.properties` in modo da impostare i parametri di autenticazione affidabile, inclusa la variabile della sessione utente e il segreto condiviso. Sostituire "..." con il segreto condiviso del sistema.

```
trusted.auth.user.param=TrustedUserAttribute
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.shared.secret="..."
```

Per ulteriori dettagli, consultare l'argomento correlato che riguarda la configurazione dell'autenticazione attendibile per le applicazioni Web.

5. Ridistribuire l'applicazione Web e riavviare il server Web.
6. Nella CMC abilitare l'autenticazione attendibile.
Nella scheda "Autenticazione" fare doppio clic su **Enterprise**, quindi selezionare la casella di controllo **Autenticazione affidabile attivata**.

Argomenti correlati

- [Abilitazione dell'Autenticazione affidabile](#)
- [Configurazione di Autenticazione affidabile per l'applicazione Web](#)

18.4 Personalizzazione dell'interfaccia Web Intelligence

Nella CMC è possibile personalizzare l'aspetto degli elementi dell'interfaccia Web Intelligence per i gruppi di utenti, ad esempio elementi specifici di barre degli strumenti o barre degli strumenti intere, e personalizzare l'accesso a specifiche modalità dei documenti.

Per impostazione predefinita, vengono visualizzati tutti gli elementi dell'interfaccia. Se non si desidera visualizzare determinati elementi, deselezionarli nella CMC: nella scheda **Utenti e gruppi** selezionare un utente o un gruppo, quindi fare clic su **Azioni > Personalizzazione**.

La sezione Personalizzazione contiene le schede seguenti:

- Funzionalità
In questa scheda è possibile scegliere di nascondere i pulsanti correlati a una funzione, ad esempio Aggiorna.
- Elementi dell'interfaccia utente

In questa scheda è possibile selezionare singoli elementi dell'interfaccia utente, come una barra degli strumenti o una scheda, oppure i relativi elementi secondari, ad esempio un pulsante di comando.

Nota:

La personalizzazione è applicabile a tutti i client di applicazioni Web Intelligence: Web, applet Java e Rich Client.

18.4.1 Scheda Funzionalità


Singola funzionalità	Descrizione	Influenza gli elementi di interfaccia seguenti
Aggiorna	Gli utenti possono aggiornare i documenti per aggiornare i dati dell'origine dati.	Il pulsante Aggiorna nella barra degli strumenti Gruppo azioni standard utilizzata nelle modalità Lettura e Progettazione.
Drill	Gli utenti possono eseguire il drill up e il drill down sui dati di un documento.	Il pulsante Drill disponibile nelle posizioni seguenti: <ul style="list-style-type: none"> La barra degli strumenti Gruppo analisi in modalità Lettura. La sottoscheda Interagisci della scheda Analisi in modalità Progettazione.
Modalità Lettura	Gli utenti possono visualizzare un documento in modalità Lettura.	Il pulsante Lettura disponibile nelle posizioni seguenti: <ul style="list-style-type: none"> Menu di scelta rapida Applicazione Barra degli strumenti Controllo applicazione
Modalità Progettazione	Gli utenti possono visualizzare un documento in modalità Progettazione.	Il pulsante Progettazione disponibile nelle posizioni seguenti: <ul style="list-style-type: none"> Menu di scelta rapida Applicazione Barra degli strumenti Controllo applicazione
Modalità Dati	Gli utenti possono visualizzare un documento in modalità Dati.	Il pulsante Dati disponibile nelle posizioni seguenti: <ul style="list-style-type: none"> Menu di scelta rapida Applicazione Barra degli strumenti Controllo applicazione

18.4.2 Scheda Elementi dell'interfaccia utente

Alcuni elementi dell'interfaccia personalizzabili sono identificati nei diagrammi presenti nelle sottosezioni che seguono. Utilizzare la tabella seguente per identificare le voci degli elementi nei diagrammi.

Voce dell'elemento dell'interfaccia utente	Voce dell'elemento secondario	Descrizione	Numero nel diagramma
Schermata di avviso		Selezionare questa voce per nascondere la schermata visualizzata quando si apre Web Intelligence.	
Menu di scelta rapida Applicazione		Selezionare questa voce per nascondere il menu visualizzato quando si fa clic con il pulsante destro del mouse nella schermata Web Intelligence.	1
	Modalità Applicazione	Selezionare questa voce per nascondere l'opzione di modifica della modalità di applicazione nel menu di scelta rapida Applicazione.	1a
	Barra filtro	Selezionare questa voce per nascondere l'opzione Barra filtro nel menu di scelta rapida Applicazione.	1b
	Struttura	Selezionare questa voce per nascondere l'opzione Struttura nel menu di scelta rapida Applicazione.	1c
	Barra delle formule	Selezionare questa voce per nascondere l'opzione Barra delle formule nel menu di scelta rapida Applicazione.	1d
	Pannello laterale	Selezionare questa voce per nascondere l'opzione Pannello laterale nel menu di scelta rapida Applicazione.	1e
	Schede del report	Selezionare questa voce per nascondere l'opzione Schede del report nel menu di scelta rapida Applicazione.	1f
	Barra di stato	Selezionare questa voce per nascondere l'opzione Barra di stato nel menu di scelta rapida Applicazione.	1g
Pannello laterale		Selezionare questa voce per nascondere il pannello laterale accanto al pannello dei report che consente agli utenti di accedere a diverse schede di informazioni.	2
	Riepilogo dei documenti	Selezionare questa voce per nascondere la scheda Riepilogo dei documenti nel pannello laterale.	2a
	Mappa di spostamento	Selezionare questa voce per nascondere la scheda Mappa di spostamento (denominata Mappa dei report nell'interfaccia HTML) nel pannello laterale.	2b

Voce dell'elemento dell'interfaccia utente	Voce dell'elemento secondario	Descrizione	Numero nel diagramma
	Controlli di input	Selezionare questa voce per nascondere la scheda Controlli di input nel pannello laterale.	2c
	Immissione prompt utente	Selezionare questa voce per nascondere la scheda Immissione prompt utente nel pannello laterale.	2d
	Oggetti disponibili	Selezionare questa voce per nascondere la scheda Oggetti disponibili nel pannello laterale.	2e
	Struttura e filtri del documento	Selezionare questa voce per nascondere la scheda Struttura e filtri del documento nel pannello laterale.	2f
	Web Service Publisher	Selezionare questa voce per nascondere la scheda Web Service Publisher nel pannello laterale.	2g
	Dati	Selezionare questa voce per nascondere la scheda Dati nel pannello laterale.	2h
Barra di stato		Selezionare questa voce per nascondere la barra di stato, in cui l'utente può trovare informazioni sullo stato delle azioni relative ai documenti ed eseguire attività di zoom, spostamento tra le pagine e di attivazione della barra delle formule.	3
	Elenco a discesa del report	Selezionare questa voce per nascondere l'elenco a discesa del report nella barra di stato.	3a
	Icona di stato di stampa	Selezionare questa voce per nascondere l'icona dello stato di stampa nella barra di stato.	3b
	Rileva modifiche dei dati	Selezionare questa voce per nascondere lo stato di Rileva modifiche dei dati nella barra di stato.	3c
	Spostamento tra le pagine	Selezionare questa voce per nascondere la barra Spostamento tra le pagine nella barra di stato.	3d
	Modalità impaginazione	Selezionare questa voce per nascondere i pulsanti della Modalità impaginazione nella barra di stato.	3e
	Ingrandisci elenco	Selezionare questa voce per nascondere l'elenco a discesa delle percentuali di zoom nella barra di stato.	3f
	Dispositivo di scorrimento dello zoom	Selezionare questa voce per nascondere la barra Dispositivo di scorrimento dello zoom nella barra di stato.	3g

Voce dell'elemento dell'interfaccia utente	Voce dell'elemento secondario	Descrizione	Numero nel diagramma
	Stato spazio di lavoro	<p>Selezionare questa voce per nascondere l'indicatore Stato spazio di lavoro nella barra di stato.</p> <p>Nota: L'indicatore Stato spazio di lavoro () viene visualizzato tra il dispositivo di scorrimento dello zoom e la data dell'ultimo aggiornamento se si verifica un problema nello spazio di lavoro.</p>	Non visualizzato
	Data ultimo aggiornamento	Selezionare questa voce per nascondere la data dell'ultimo aggiornamento nella barra di stato.	3i
	Stato della connessione	Selezionare questa voce per nascondere lo stato della connessione di Web Intelligence Rich Client nella barra di stato.	3j
Zona del report		Selezionare questa voce per nascondere la zona del report in Web Intelligence.	4
	Schede del report	Selezionare questa voce per nascondere le schede del report nella zona del report.	4a
	Scorrimento pagina bidirezionale	Selezionare questa voce per nascondere la funzionalità di scorrimento della pagina bidirezionale nell'angolo in basso della pagina della zona del report.	4b
	Barra delle formule	Selezionare questa voce per nascondere la barra delle formule nella parte superiore della zona del report.	4c
Barra degli strumenti Modalità Lettura		Selezionare questa voce per nascondere le barre degli strumenti visualizzate in modalità Lettura.	5
	Elenco a discesa Web Intelligence	Selezionare questa voce per nascondere l'elenco a discesa Web Intelligence in modalità Lettura.	5a
	Gruppo file	Selezionare questa voce per nascondere la barra degli strumenti Gruppo file in modalità Lettura.	5b
	Gruppo azioni standard	Selezionare questa voce per nascondere la barra degli strumenti Gruppo azioni standard in modalità Lettura.	5c

Voce dell'elemento dell'interfaccia utente	Voce dell'elemento secondario	Descrizione	Numero nel diagramma
	Gruppo analisi	Selezionare questa voce per nascondere la barra degli strumenti Gruppo analisi in modalità Lettura.	5d
Barra degli strumenti Modalità progettazione		Selezionare questa voce per nascondere le barre degli strumenti e le schede visualizzate in modalità Progettazione.	6
	Scheda File	Selezionare questa voce per nascondere la scheda File in modalità Lettura.	6a
	Scheda Proprietà	Selezionare questa voce per nascondere la scheda Proprietà in modalità Lettura.	6b
	Gruppo azioni standard	Selezionare questa voce per nascondere la barra degli strumenti Gruppo azioni standard in modalità Lettura.	6c
	Scheda Elementi del report	Selezionare questa voce per nascondere la scheda Elementi del report in modalità Lettura.	6d
	scheda Formato	Selezionare questa voce per nascondere la scheda Formato in modalità Lettura.	6e
	Scheda Accesso ai dati	Selezionare questa voce per nascondere la scheda Accesso ai dati in modalità Lettura.	6f
	Scheda Analisi	Selezionare questa voce per nascondere la scheda Analisi in modalità Lettura.	6g
	Scheda Imposta pagina	Selezionare questa voce per nascondere la scheda Imposta pagina in modalità Lettura.	6h
Barra degli strumenti iniziale		Selezionare questa voce per nascondere le barre degli strumenti iniziali visualizzate quando un utente apre l'applicazione Web Intelligence.	7
	Elenco a discesa di Web Intelligence	Selezionare questa voce per nascondere l'elenco a discesa di Web Intelligence nella barra degli strumenti iniziale.	7a
	Gruppo file	Selezionare questa voce per nascondere la barra degli strumenti Gruppo file nella barra degli strumenti iniziale.	7b

Voce dell'elemento dell'interfaccia utente	Voce dell'elemento secondario	Descrizione	Numero nel diagramma
Barra degli strumenti Controllo applicazione		Selezionare questa voce per nascondere la barra degli strumenti Controllo applicazione, visualizzata nella barra degli strumenti superiore di Web Intelligence.	8
	Pulsanti Modalità applicazione	Selezionare questa voce per nascondere i pulsanti della modalità Applicazione (Lettura, Progettazione e Dati) nella barra degli strumenti superiore di Web Intelligence.	8a
	Strumenti	Selezionare questa voce per nascondere l'icona Strumenti nella barra degli strumenti superiore di Web Intelligence.	8b
	Guida in linea	Selezionare questa voce per nascondere l'icona della Guida in linea nella barra degli strumenti superiore di Web Intelligence.	8c
	Chiudi	Selezionare questa voce per nascondere l'icona Chiudi nella barra degli strumenti superiore di Web Intelligence.	8d

Schermata iniziale

Nella personalizzazione di utenti e gruppi della CMC, è possibile scegliere di nascondere la schermata iniziale di Web Intelligence visualizzata. Nell'immagine seguente viene mostrata la schermata iniziale visualizzata per impostazione predefinita quando un utente apre Web Intelligence.



Figura 18 - 2: Schermata iniziale (esempio in inglese)

Menu di scelta rapida Applicazione

Nei diagrammi seguenti vengono mostrate le voci che possono essere nascoste nel menu di scelta rapida.

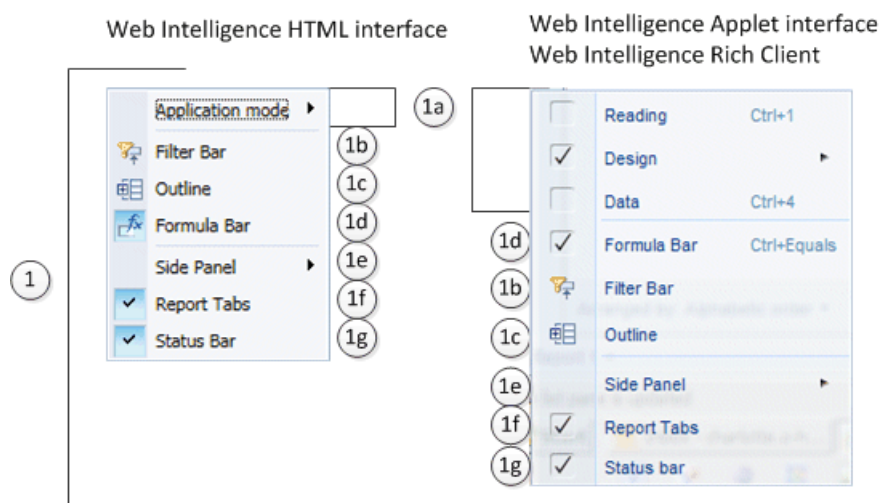
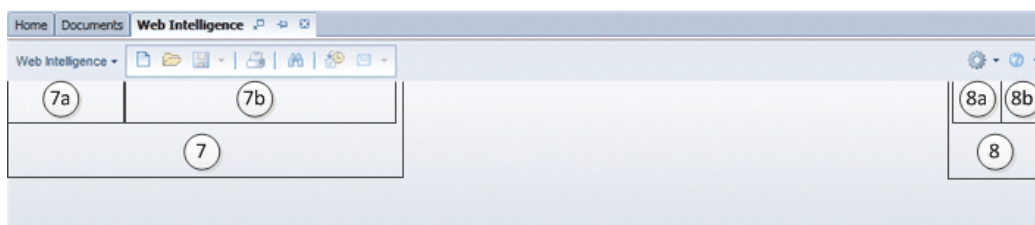


Figura 18 - 3: Menu di scelta rapida Applicazione (esempio in inglese)

Barra degli strumenti iniziale

Nei diagrammi seguenti vengono mostrate le voci che è possibile nascondere nelle barre degli strumenti visualizzate in Web Intelligence in assenza di documenti aperti.

Web Intelligence Applet interface
Web Intelligence Rich Client



Web Intelligence HTML interface

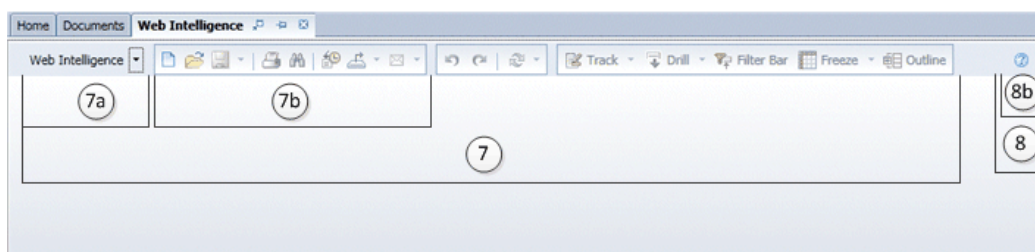
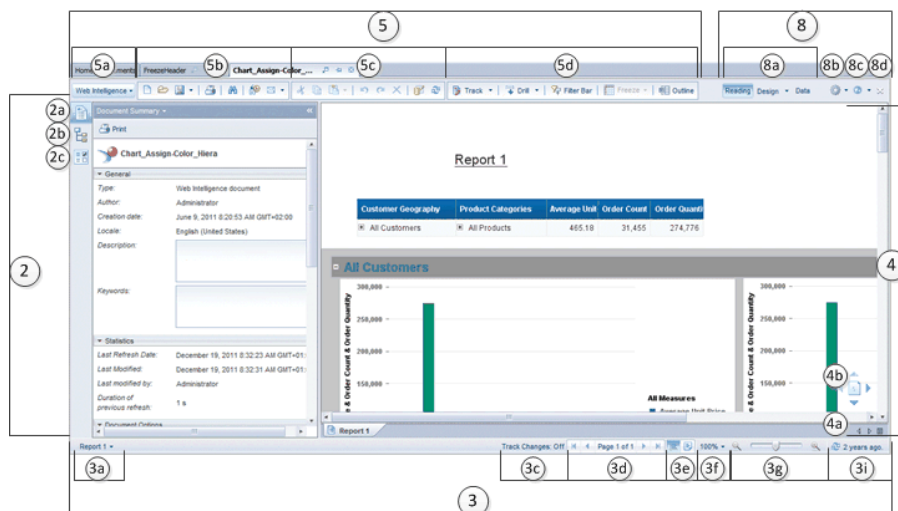


Figura 18 - 4: Barra degli strumenti in inglese (esempio in inglese)

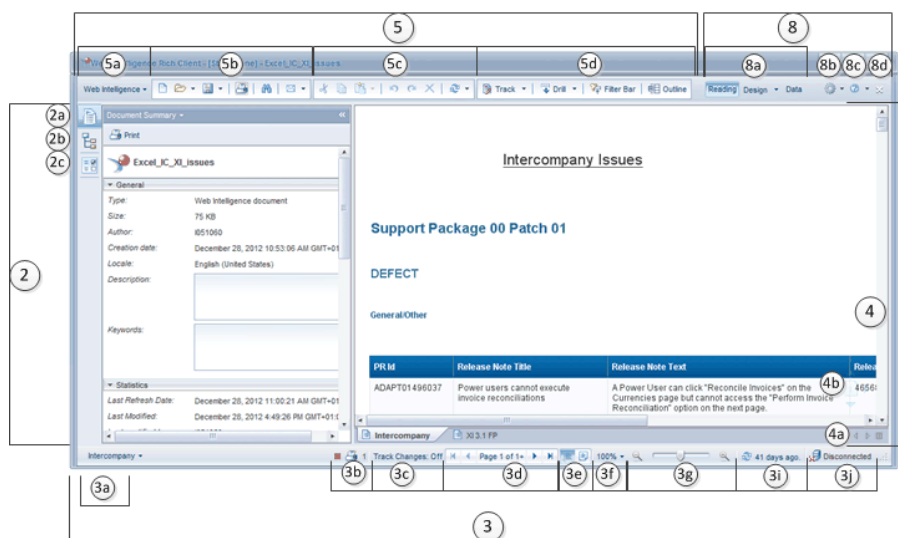
Modalità Lettura

Nei diagrammi seguenti vengono mostrate le voci che è possibile nascondere nella modalità Lettura di Web Intelligence.

Web Intelligence Applet interface



Web Intelligence Rich Client



Web Intelligence HTML interface

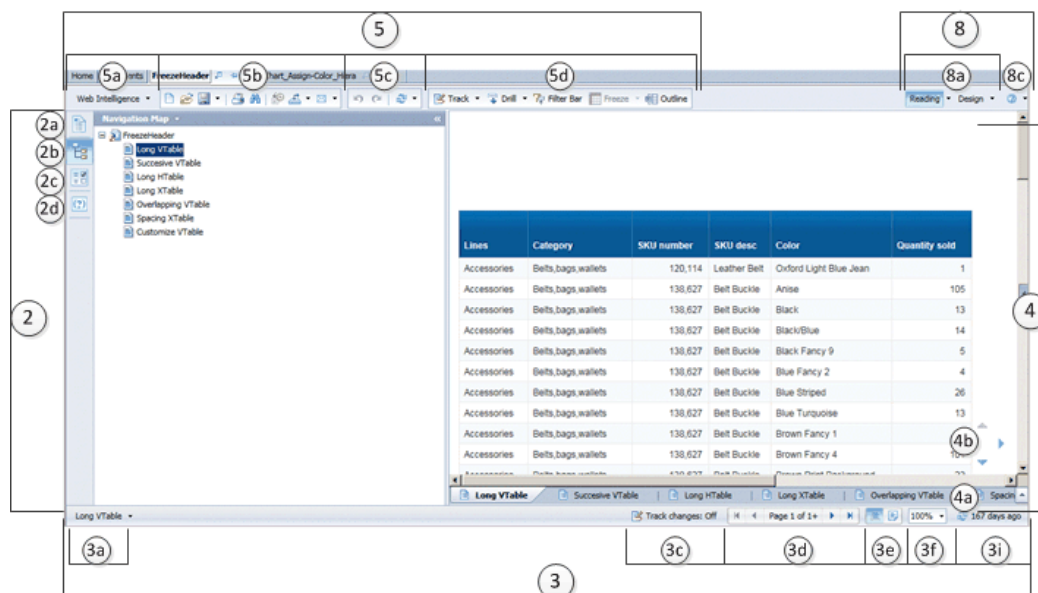
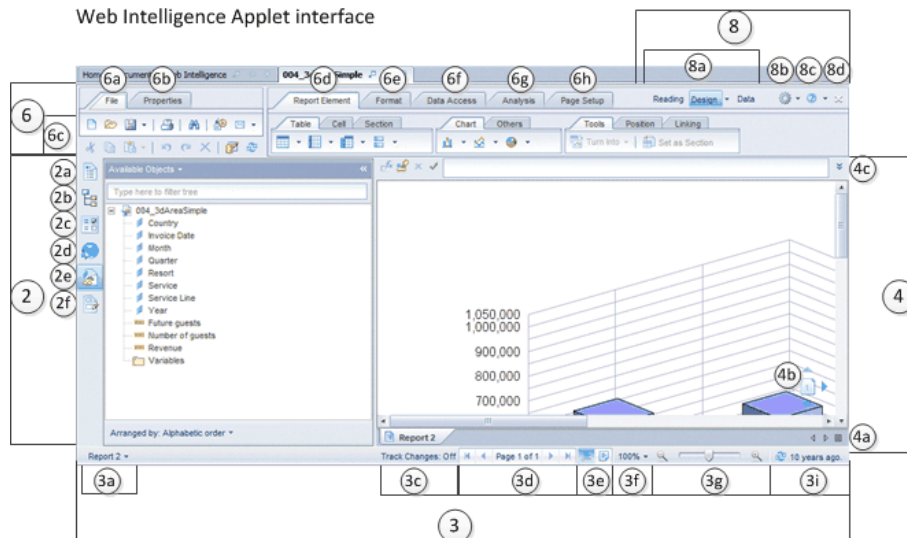


Figura 18 - 5: Modalità Reading (esempio in inglese)

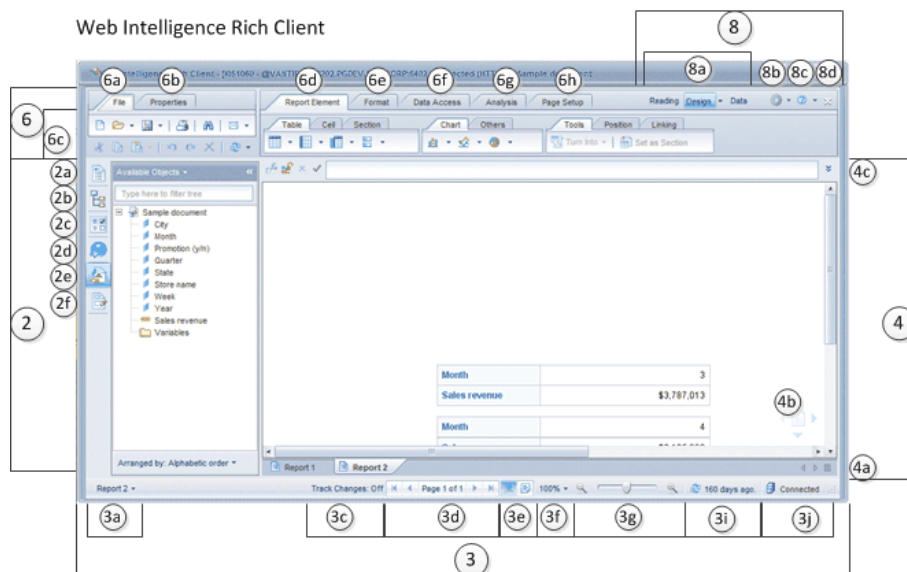
Modalità Progettazione

Nei diagrammi seguenti vengono mostrate le voci che è possibile nascondere nella modalità Progettazione di Web Intelligence.

Web Intelligence Applet interface



Web Intelligence Rich Client



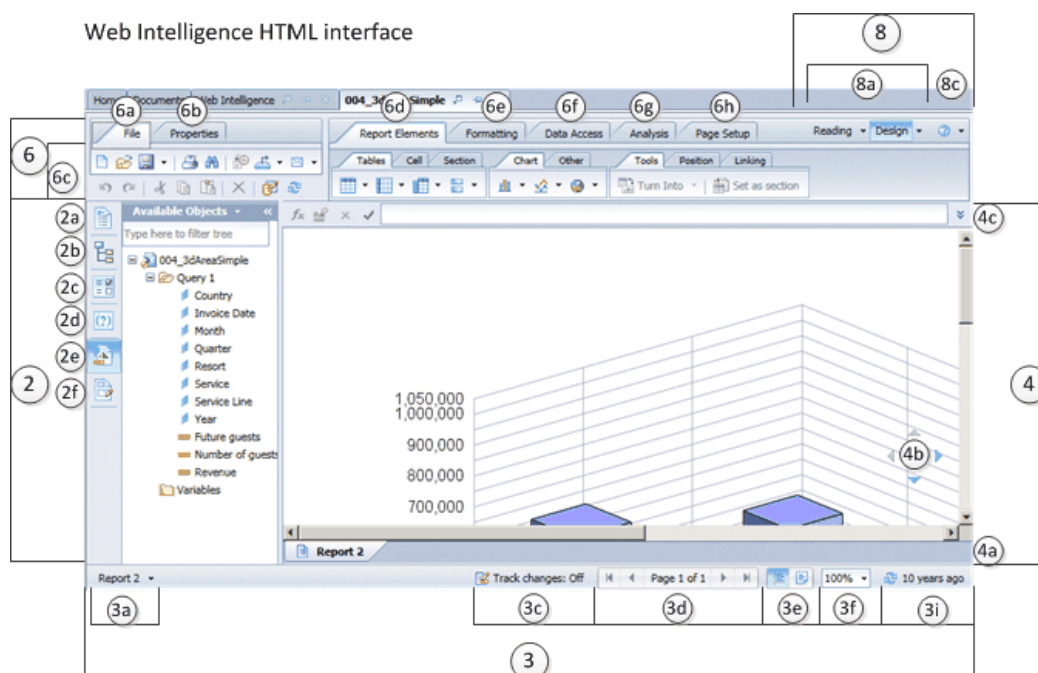
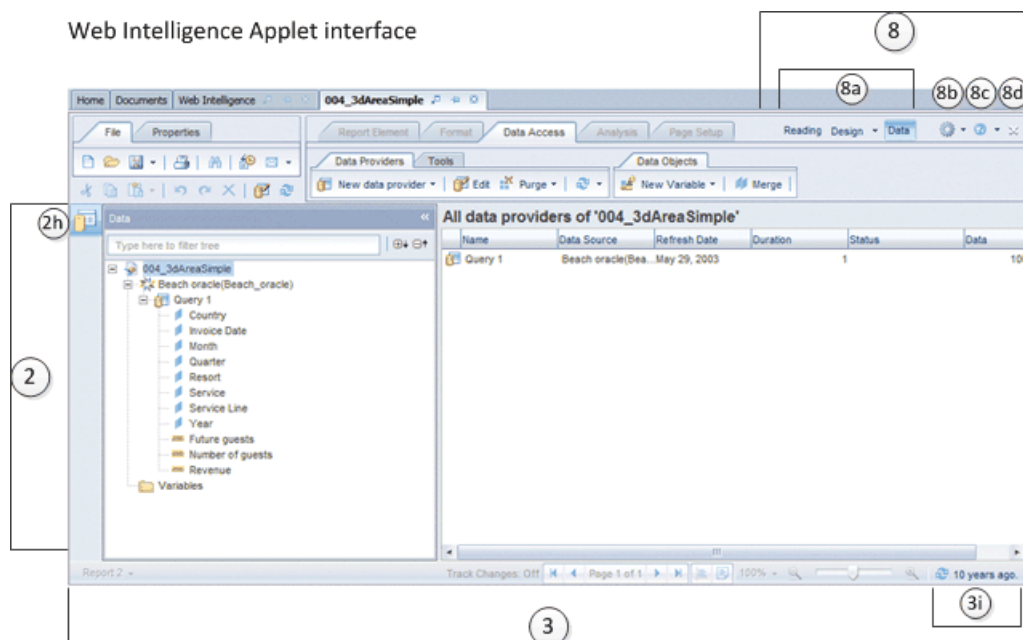


Figura 18 - 6: Modalità Design (esempio in inglese)

Modalità Dati

Nei diagrammi seguenti vengono mostrate le voci che è possibile nascondere nella modalità Dati di Web Intelligence.

Web Intelligence Applet interface



Web Intelligence Rich Client

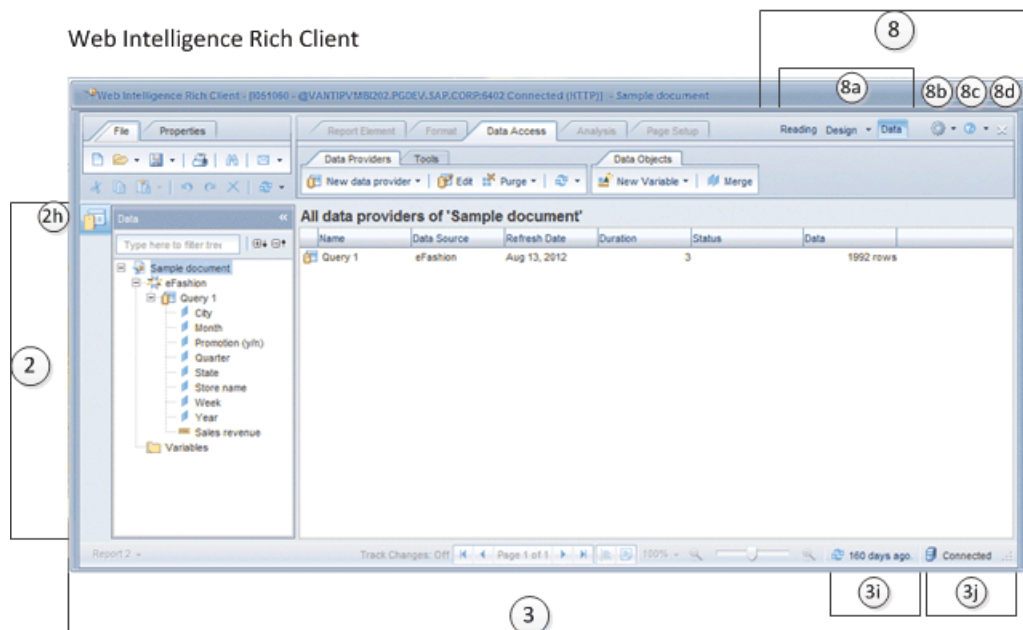


Figura 18 - 7: Modalità Data (esempio in inglese)

18.4.3 Per personalizzare l'aspetto dell'interfaccia Web Intelligence

È possibile personalizzare l'aspetto dell'interfaccia utente Web Intelligence nascondendo voci di menu, voci secondarie e funzionalità a tutti i membri di un gruppo di utenti selezionato.

1. Accedere alla CMC come amministratore.
2. Nell'elenco "Organizza" selezionare **Utenti e gruppi**.
3. Nell'elenco "Gerarchia gruppi" selezionare un gruppo di utenti.
4. Nell'elenco "Gestisci" selezionare **Proprietà**.
5. Nel pannello laterale selezionare **Personalizzazione**.
6. Effettuare una delle operazioni seguenti:
 - Per nascondere elementi dell'interfaccia in Web Intelligence, selezionarli nella scheda Elementi dell'interfaccia utente o Funzionalità.
 - Per visualizzare gli elementi dell'interfaccia nascosti in Web Intelligence, deselezionarli nella scheda Elementi dell'interfaccia utente o Funzionalità.
7. Fare clic su **Salva e chiudi**.

Una volta salvata la personalizzazione, tutti gli utenti del gruppo selezionato vedranno le modifiche la volta successiva in cui accederanno a BI Launch Pad e apriranno Web Intelligence.

Nota:

Si consiglia di accedere a BI Launch Pad come utente dal gruppo appena personalizzato, di avviare Web Intelligence e di verificare che l'interfaccia corrisponda alle impostazioni di personalizzazione configurate.

Gestione di connessioni e universi

19.1 Gestione delle connessioni

La connessione è un insieme denominato di parametri che definiscono in che modo una o più applicazioni SAP BusinessObjects possono accedere ai database relazionali o OLAP. I dettagli delle connessioni, ad esempio nome del server, database, nome utente e password, possono essere archiviati nel repository della piattaforma BI all'interno della cartella delle connessioni.

I progettisti definiscono gli universi in base alle connessioni. Gli utenti delle applicazioni per le query, l'analisi e la creazione di report accedono al database tramite l'universo senza necessariamente conoscere le strutture di dati sottostanti all'interno del database.

È possibile creare connessioni utilizzando le seguenti applicazioni:

- Universe Design Tool: le connessioni vengono archiviate nel repository.
- Information Design Tool: le connessioni possono essere create in locale e successivamente pubblicate nel repository oppure create e modificate direttamente nel repository.

Nota:

Per informazioni su come gestire le connessioni alle origini dati OLAP, consultare il *Manuale dell'amministratore di SAP BusinessObjects Analysis, versione per OLAP*.

È possibile concedere diritti agli utenti per consentirgli di creare, modificare ed eliminare le connessioni.

È possibile concedere l'accesso agli utenti per le connessioni agli universi in modo da consentirgli di creare e visualizzare documenti che utilizzano universi e connessioni.

Argomenti correlati

- [Gestione delle impostazioni di protezione per gli oggetti nella CMC](#)
- [Diritti di connessione](#)

19.1.1 Eliminazione di una connessione universo

Suggerimento:

è anche possibile eliminare le connessioni in Universe Design Tool e in Information Design Tool.

1. Nell'area "Connessioni" scegliere una connessione all'universo dall'elenco.

2. Scegliere **Gestisci > Elimina**.

19.2 Gestione degli universi

L'universo è una raccolta organizzata di oggetti metadati che consente agli utenti aziendali di analizzare e creare report utilizzando i dati aziendali in un linguaggio non tecnico. Tali oggetti includono dimensioni, indicatori, gerarchie, attributi, calcoli predefiniti, funzioni e query. Il livello degli oggetti metadati viene creato su uno schema di database relazionale o un cubo OLAP: gli oggetti vengono pertanto mappati direttamente alle strutture del database. Un universo include connessioni alle origini dati in modo che gli utenti di strumenti di query e di analisi possano connettersi ad esso per eseguire query e creare report utilizzando gli oggetti al suo interno senza necessariamente conoscere le strutture di dati sottostanti del database.

È possibile creare universi con i seguenti strumenti:

- Universe Design Tool: gli universi creati con questo strumento vengono denominati universi .unv dall'estensione .unv che li caratterizza. Gli universi .unv vengono definiti su una connessione protetta e archiviati nella cartella degli universi.
- Information Design Tool: gli universi creati con questo strumento sono basati sul nuovo livello semantico. Vengono denominati universi .unx dall'estensione .unx che li caratterizza. Gli universi .unx vengono creati in locale e pubblicati nella cartella degli universi del repository. I progettisti possono definire la protezione a livello di oggetto utilizzando l'editor di protezione di Information Design Tool.

È possibile concedere agli utenti diritti per le applicazioni e gli universi in modo da consentirgli di creare, modificare ed eliminare gli universi, nonché progettare la protezione su di essi.

È possibile concedere agli utenti diritti per gli universi in modo da consentirgli di creare e visualizzare documenti che utilizzano universi.

Argomenti correlati

- [Gestione delle impostazioni di protezione per gli oggetti nella CMC](#)
- [Diritti di Universe Design Tool](#)
- [Diritti sugli universi \(.unv\)](#)
- [Diritti di Information Design Tool](#)
- [Diritti sugli universi \(.unx\)](#)

19.2.1 Eliminazione di universi

Suggerimento:

è anche possibile eliminare gli universi in Universe Design Tool e in Information Design Tool.

1. Nell'area "Universi" della console CMC selezionare un universo dall'elenco.
2. Scegliere **Gestisci > Elimina**.
3. Quando viene richiesto di confermare l'operazione, fare clic su **OK**.

Monitoraggio

20.1 Informazioni sul monitoraggio

L'applicazione di monitoraggio consente di acquisire le metriche cronologiche e di runtime dei server della piattaforma BI, per la creazione di report e per le notifiche. Consente inoltre agli amministratori del sistema di stabilire se un'applicazione funziona normalmente e se i tempi di risposta sono quelli previsti. Grazie alle metriche aziendali chiave fornite dall'applicazione di monitoraggio, è possibile avere una visione più approfondita della piattaforma BI.

Il monitoraggio consente di eseguire le attività seguenti:

- Controllare le prestazioni di ciascun server: per questa attività vengono utilizzati i controlli che mostrano lo stato di ciascun server tramite i semafori. L'amministratore di sistema può impostare delle soglie per i controlli e ricevere avvisi nel caso in cui vengano violate. Ciò consente di intraprendere azioni proattive in caso di interruzioni o errori improvvisi.
- Visualizzare i KPI (Key Performance Indicator) critici di sistema: supporta il monitoraggio delle attività e delle risorse. I KPI vengono visualizzati nella pagina del cruscotto dell'applicazione di monitoraggio.
- Visualizzare l'intera distribuzione della piattaforma BI in base a gruppi di server, categorie di servizi e nodi Enterprise, sia in formato grafico che tabulare.
- Visualizzare gli errori recenti nella schermata del cruscotto.
- Controllare la disponibilità del sistema e il tempo di risposta: con le probe è possibile simulare i workflow per verificare se i server e i servizi nella distribuzione della piattaforma BI funzionano come previsto. Analizzando la cronologia di andata e ritorno delle probe a intervalli regolari, l'amministratore di sistema può valutare i criteri di utilizzo del sistema.
- Analizzare il carico massimo e il periodo di picco per il CMS: questa funzionalità consente all'amministratore di sistema di determinare se occorrono altre licenze o risorse di sistema.
- Eseguire l'integrazione con altre applicazioni Enterprise: è possibile integrare l'applicazione di monitoraggio della piattaforma BI con altre applicazioni Enterprise, ad esempio SAP Solution Manager e IBM Tivoli Monitoring.

Argomenti correlati

- [Informazioni sull'appendice sulle metriche server](#)

20.2 Termini relativi al monitoraggio

Nel seguente elenco vengono forniti i termini correlati all'applicazione di monitoraggio:

Tendenza

Registrare o visualizzare dati cronologici allo scopo di individuare le tendenze.

Cruscotto

La pagina Cruscotto fornisce all'amministratore di sistema una vista centralizzata che consente di monitorare le prestazioni di tutti i server. Fornisce informazioni in tempo reale su KPI di sistema, avvisi recenti, controlli e relativi grafici basati sullo stato del controllo.

Controllo

I controlli forniscono lo stato in tempo reale e trend cronologici dei server e dei workflow all'interno dell'ambiente della piattaforma BI. Gli utenti possono associare soglie e avvisi ai controlli. È possibile creare un controllo utilizzando i dati di probe, server, SAPOSCOL o metriche derivate.

Metrica derivata

Le metriche derivate sono metriche che si creano mediante la combinazione di due o più metriche esistenti in un'equazione matematica. È possibile creare una metrica in base ai requisiti dell'utente, quindi creare un controllo utilizzando la metrica creata.

Metrica topologica

Le metriche topologiche forniscono informazioni chiare sullo stato di ogni categoria di servizi nella piattaforma BI. Ad esempio, il servizio Crystal Reports restituisce lo stato di integrità combinato di tutti i controlli relativi ai server Crystal Reports.

Stato di integrità

I valori dello stato di integrità possono essere i seguenti:

- "0" - indica che lo stato d'integrità della metrica non è buono.
- "1" - indica che lo stato d'integrità della metrica si sta deteriorando e richiede attenzione immediata.
- "2" - indica che lo stato d'integrità della metrica è buono.

KPI

I KPI (Key Performance Indicator, indicatori di prestazioni chiave) sono metriche standard della piattaforma BI. Forniscono informazioni sulle pianificazioni e sulle sessioni di accesso. Ad esempio, un valore più elevato per **RunningJobs** indica buone prestazioni dei server. Al contrario, un valore più elevato per **PendingJobs** indica che le prestazioni sono scarse e il sistema è sovraccarico.

Probe

Le probe monitorano vari servizi e simulano le diverse funzionalità dei componenti della piattaforma BI. Pianificando l'esecuzione delle probe a intervalli specificati, l'amministratore di sistema è in grado di tracciare la disponibilità e le prestazioni dei servizi chiave forniti dalla piattaforma BI. Questi dati possono essere utilizzati anche per la pianificazione della capacità.

Semaforo

Il semaforo è un'icona che visualizza il colore verde, giallo o rosso per indicare lo stato di un controllo in un dato momento. Gli utenti possono impostare due o tre stati per un controllo.

Grafico di tendenza

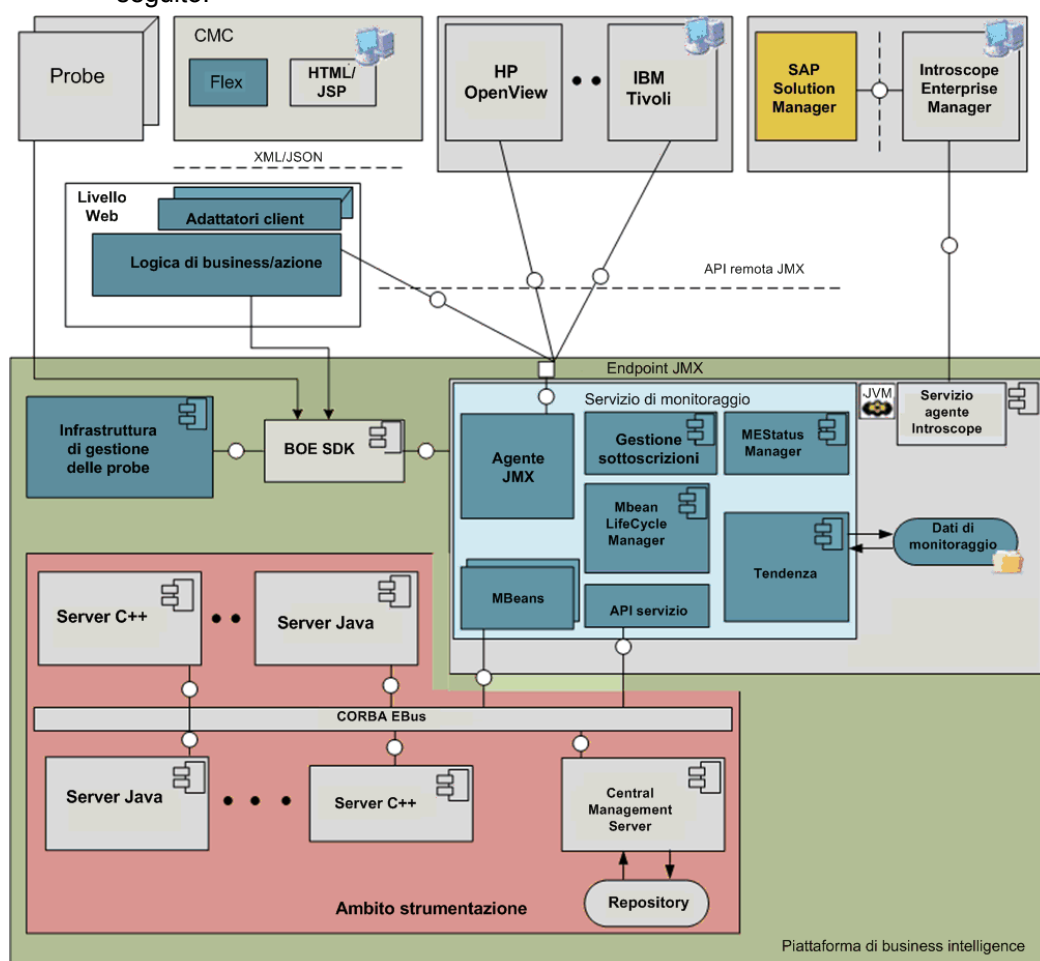
Il grafico di tendenza è una rappresentazione grafica dei dati metrici cronologici generati da probe e server. Consente all'amministratore di sistema di monitorare il sistema a intervalli di tempo diversi e di valutare i criteri di utilizzo del sistema.

Avviso

Un avviso corrisponde a una notifica generata dall'applicazione di monitoraggio quando viene violato un valore di soglia definito dall'utente, impostato per metriche diverse applicate a un controllo. È possibile specificare se ricevere avvisi tramite posta elettronica o nella pagina "Cruscotto".

20.2.1 Architettura

Questa sezione fornisce una panoramica di alto livello dell'architettura di monitoraggio e spiega brevemente il ruolo dei componenti. L'architettura di monitoraggio è rappresentata graficamente di seguito:



I componenti di alto livello nell'architettura sono elencati di seguito:

- Adaptive Processing Server (APS)
- Agente/server Java Management Extensions (JMX)
- MBeans
- Client JMX
- Console di gestione
- Database di tendenza

Il servizio di monitoraggio viene ospitato sull'Adaptive Processing Server. L'applicazione è basata sulla tecnologia JMX.

Il servizio di monitoraggio fornisce i servizi principali disponibili nell'applicazione di monitoraggio. I servizi offerti sono i seguenti:

- Fornisce il servizio dell'agente JMX.
- Crea dinamicamente gli MBean per i server SAP BusinessObjects.
- Fornisce la gestione del ciclo di vita per gli MBean.
- Fornisce un meccanismo per la registrazione di nuove probe.
- Consente agli utenti di creare condizioni di soglia complesse utilizzando le metriche dei server.
- Fornisce un meccanismo di notifica di soglia e invia avvisi.
- Archivia i dati cronologici.

Il servizio di pianificazione probe ospitato su Adaptive Job Server gestisce l'esecuzione e la pianificazione delle probe. Quindi, è necessario che Adaptive Job Server sia in esecuzione per poter eseguire le probe.

L'applicazione di monitoraggio espone inoltre un endpoint dell'URL JMX o Remote Method Invocation (RMI). Altre applicazioni aziendali, quale IBM Tivoli Monitoring, possono connettersi all'applicazione di monitoraggio e accedere alle metriche della piattaforma BI utilizzando un'API remota JMX. L'applicazione di monitoraggio utilizza un database Derby dedicato per l'archiviazione dei dati cronologici per la funzionalità di tendenza. Per informazioni sullo schema del database di tendenza, vedere [Schema del database di tendenza](#).

20.3 Configurazione del supporto di database per il monitoraggio

In questa sezione viene illustrato come configurare il monitoraggio e creare report in base ai dati a esso relativi.

Nota:

Solo i controlli per i quali è stata selezionata l'impostazione **Scrivi nel database di tendenza** registrano informazioni di monitoraggio nel database di tendenza.

Sono disponibili due opzioni di database per la registrazione delle informazioni di monitoraggio:

- Registrare informazioni nel database Derby incorporato (opzione predefinita).

L'applicazione di monitoraggio include un database Apache Derby incorporato, spesso definito "database di tendenza", in cui vengono archiviate le informazioni di monitoraggio per impostazione predefinita. Gli utenti possono creare report dal database Derby. Tale database non fornisce invece gli strumenti per il backup e il recupero tradizionali del database relazionale o il failover. Il database Derby deve inoltre essere aggiornato manualmente per fare in modo che vengano restituite le informazioni più aggiornate.

- Registrare le informazioni nel database di controllo (il database relazionale in cui CMS archivia i dati di controllo).

Aniché utilizzare il database Derby predefinito, è possibile scegliere di utilizzare l'archivio dati di controllo, spesso definito database di controllo. È possibile utilizzare il database di controllo incluso nella piattaforma BI o un altro database supportato che sia stato configurato come database di controllo. L'utilizzo del database di controllo consente agli utenti di creare report dall'insieme dei dati di controllo e delle informazioni di monitoraggio. L'acquisizione dei dati in un database relazionale fornisce funzionalità di backup e recupero, e disponibilità dei dati in tempo reale.

Argomenti correlati

- [Configurazione per l'utilizzo del database Derby](#)
- [Configurazione per l'utilizzo del database di controllo](#)

20.3.1 Configurazione per l'utilizzo del database Derby

L'applicazione di monitoraggio archivia i dati di monitoraggio nel database Derby incorporato per impostazione predefinita. Se si desidera utilizzare il database Derby, confermare le impostazioni di database seguenti nella CMC:

1. Nell'area "Gestisci" della home page della CMC fare clic su **Applicazioni**.
2. Fare doppio clic su **Applicazione di monitoraggio** per aprire la pagina delle proprietà.
3. Nell'area "Impostazioni database di tendenza" verificare che sia selezionato **Utilizza database incorporato**.

Per eseguire le query nel database Derby per la creazione di report ed eseguire analisi dei dati, è necessario un universo per il database Derby. Viene fornito un universo con la distribuzione della piattaforma BI nel percorso seguente all'interno della CMC: **Universes > Monitoring TrendData Universes**.

20.3.2 Configurazione per l'utilizzo del database di controllo

Se si desidera utilizzare il database di controllo per i dati di monitoraggio, è necessario eseguire ulteriori passaggi di configurazione, come indicato di seguito.

- Se il database di tendenza Derby contiene già dati, è necessario migrarlo nel database di controllo, quindi configurare la piattaforma BI per registrare le informazioni di monitoraggio nel database di controllo. Di seguito è riportata la procedura generale da eseguire. Per informazioni dettagliate, vedere gli argomenti correlati.
 1. Migrare il database Derby.
 2. Configurare i file SBO e aggiungere i nomi alias.
 3. Passare al database di controllo.
 4. Riavviare l'Adaptive Processing Server che ospita il servizio di monitoraggio.
 5. Nel cruscotto di monitoraggio verificare che tutto funzioni come previsto. Verificare che nel database siano state create le tabelle di monitoraggio seguenti:
 - MOT_MES_DETAILS
 - MOT_MES_METRICS
 - MOT_TREND_DATA
 - MOT_TREND_DETAILS
- Se il database di tendenza non contiene dati, ovvero è stata eseguita una nuova installazione, non è necessario migrarlo. È sufficiente configurare la piattaforma BI per registrare le informazioni di monitoraggio nel database di controllo. Di seguito è riportata la procedura generale da eseguire. Per informazioni dettagliate, vedere gli argomenti correlati.
 1. Verificare che il database di controllo funzioni e che il controllo sia in esecuzione.
 2. Creare le tabelle di monitoraggio nell'ADS.
 3. Configurare i file SBO e aggiungere i nomi alias.
 4. Passare al database di controllo.
 5. Riavviare l'Adaptive Processing Server che ospita il servizio di monitoraggio.
 6. Nel cruscotto di monitoraggio verificare che tutto funzioni come previsto. Verificare che nel database siano state create le tabelle di monitoraggio seguenti:
 - MOT_MES_DETAILS
 - MOT_MES_METRICS
 - MOT_TREND_DATA
 - MOT_TREND_DETAILS

Nota:

Se si registrano dati di monitoraggio nel database di controllo e si desidera creare report da questi dati, è necessario sviluppare un universo personalizzato. L'universo incluso nella piattaforma BI deve essere utilizzato solo con il database Derby incorporato.

Argomenti correlati

- [Migrazione del database Derby al database di controllo](#)
- [Configurazione dei file SBO](#)
- [Aggiunta di nomi di alias nel file SBO](#)
- [Per passare al database di controllo](#)
- [Per creare le tabelle di monitoraggio nell'ADS](#)

20.3.2.1 Migrazione del database Derby al database di controllo

Se si desidera utilizzare il database di controllo per i dati di monitoraggio e nel database di tendenza Derby sono già presenti dati, è necessario migrare il database Derby al database di controllo.

Prima di procedere alla migrazione dei dati, verificare la presenza dei prerequisiti seguenti:

- Il database di controllo deve funzionare e il controllo deve essere in esecuzione.
- È necessario disporre delle autorizzazioni sufficienti e di applicazioni client di database sul database di destinazione per creare nuove tabelle, importare dump CSV e così via.
- Il database di controllo deve supportare l'importazione di file CSV (Comma-Separated Value).

Attenersi alla procedura seguente per eseguire la migrazione del database:

1. [Per eseguire il backup del database Derby](#)
2. [Per esportare i dati in file CSV](#)
3. [Per creare le tabelle di monitoraggio nell'ADS](#)
4. [Per ripristinare il contenuto nel database di destinazione](#)

Nota:

in uno scenario cluster si prevede che gli utenti utilizzino la stessa istanza del database Derby per tutte le istanze di monitoraggio. Se l'utente dispone di più istanze del database Derby in uno scenario cluster, deve importare solo i dati di un'istanza. L'importazione di dati da più istanze del database Derby comporta l'incoerenza dei dati e quindi non è consigliata.

20.3.2.1.1 Per eseguire il backup del database Derby

1. Nell'area "Gestisci" della home page della CMC fare clic su **Applicazioni**.
2. Fare doppio clic su **Applicazione di monitoraggio** per aprire la pagina delle proprietà.
3. Nell'area "Impostazioni database di tendenza" immettere una posizione file in cui eseguire il backup del database di tendenza Derby, quindi fare clic su **Salva**.
4. Accanto a "Esegui attività di backup del database" fare clic su **Ora**.

Se il backup del database riesce, viene visualizzato un messaggio di conferma. Verificare inoltre la posizione di cartella immessa per il backup e verificare che i file di backup siano stati inseriti in questa posizione.

20.3.2.1.2 Per esportare i dati in file CSV

In questa sezione viene illustrato come generare i file dump CSV necessari per eseguire la migrazione. I file CSV contengono valori separati da virgola del contenuto di dati del database Derby incorporato.

1. Nell'area "Gestisci" della home page della CMC fare clic su **Applicazioni**.
2. Fare doppio clic su **Applicazione di monitoraggio** per aprire la pagina delle proprietà.
3. Nell'area "Impostazioni database di tendenza", accanto a "Esporta dati da database incorporato come file CSV" fare clic su **Esporta**.

Vengono generati i quattro file CSV elencati di seguito nella posizione predefinita del database di tendenza, in < BOE_Install_Dir>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB:

- Mot_Mes_Details.csv
- Mot_Trend_Data.csv
- Mot_Trend_Details.csv
- Mot_Mes_Metrics.csv

20.3.2.1.3 Per creare le tabelle di monitoraggio nell'ADS

Attenersi alla procedura seguente per preparare il database di controllo di destinazione:

1. Dopo avere installato la piattaforma BI, le DDL correlate a tutti i database di controllo CMS supportati sono disponibili nel percorso <Dir install>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB. Qui saranno contenuti sette file diversi (estensione .sql) con il rispettivo nome database. Ad esempio: Oracle.sql per Oracle, Sybase ASE.sql per Sybase ASE Database e così via.
2. Passare al database di destinazione (in questo caso, il database di destinazione è quello in cui è stato configurato il controllo CMS) ed eseguire il file .sql. Vengono create le quattro tabelle di monitoraggio seguenti: MOT_TREND_DETAILS, MOT_TREND_DATA, MOT_MES_DETAILS e MOT_MES_METRICS. Insieme alle tabelle vengono creati anche gli indici richiesti.

Se tutte le tabelle sono create con i tipi di dati corretti, come riportato nel file .sql, viene creato lo schema del database richiesto per l'applicazione di monitoraggio.

20.3.2.1.4 Per ripristinare il contenuto nel database di destinazione

È necessario eseguire i passaggi seguenti per ripristinare il contenuto nel database di destinazione:

1. Abilitare l'inserimento di identità.

Le tabelle di monitoraggio contengono una serie di colonne IDENTITY. I valori contenuti in queste colonne sono generati automaticamente. Alcuni database (ad esempio MS SQL Server e SYBASE ASE) non consentono l'inserimento esplicito dei valori in queste colonne. Tuttavia, durante la migrazione dei dati, è necessario migrare anche i valori contenuti nelle colonne IDENTITY. Pertanto, gli utenti devono abilitare l'inserimento esplicito di questi valori, utilizzando il comando SQL seguente:

```
SET IDENTITY_INSERT <NOME TABELLA> ON.
```

2. Importare il file dump CSV nella tabella di destinazione.

Tutto il software fornito con i client di database consente agli utenti di importare i dati dal formato CSV nella tabella, mediante un'opzione di menu o un comando. L'utente deve utilizzare questa opzione per importare i dati dal file CSV nella tabella corrispondente. Importare i file di dati nelle nuove tabelle nell'ordine seguente:

- a. MOT_TREND_DETAILS
- b. MOT_TREND_DATA
- c. MOT_MES_DETAILS
- d. MOT_MES_METRICS

3. Disabilitare l'inserimento di identità.

Al termine dell'importazione dei dati, è necessario disabilitare l'inserimento di identità nella tabella, mediante il comando SQL seguente: `SET IDENTITY_INSERT <NOME TABELLA> OFF`.

Al termine dell'importazione dei dati, è necessario disabilitare l'inserimento d'identità in una tabella per poter abilitare l'opzione nella tabella successiva. Questo è necessario perché è possibile abilitare l'operazione di inserimento d'identità soltanto in una tabella alla volta.

Nota:

i passaggi per abilitare e disabilitare l'inserimento di identità sono applicabili solamente per MS SQL Server e Sybase ASE. Per gli altri database, ad esempio Oracle, MaxDb, DB2, MySQL o SQL Anywhere, non sono necessari. Infatti, è possibile importare direttamente i dati nelle tabelle.

20.3.2.2 Configurazione dei file SBO

L'applicazione di monitoraggio utilizza al suo interno le librerie di Connection Server. Per consentire la connessione di Connection Server al driver del database è richiesta la configurazione SBO. Per stabilire tale connettività è necessario specificare il driver del database e la relativa posizione nel file SBO.

Esempio:

- Se il campo Nome della connessione configurato nella pagina Controllo della CMC è impostato su ODBC DSN, è necessario configurare il driver in: `<Dir_Installaz>\dataAccess\connectionServer\odbc\<Tipodb>.sbo`.
- Se il database utilizzato per il controllo è SAP HANA, il file nel quale è necessario configurare il driver è: `<Dir_Installaz>\dataAccess\connectionServer\odbc\newdb.sbo`.
- Se il database utilizzato per il controllo è MS SQL Server, il file nel quale è necessario configurare il driver è: `<Dir_Installaz>\dataAccess\connectionServer\odbc\sqlsrv.sbo`.
- Se il database utilizzato per il controllo è DB2, il file nel quale è necessario configurare il driver è: `<Dir_Installaz>\dataAccess\connectionServer\odbc\db2iseries.sbo`.
- Se il campo Nome della connessione configurato nella pagina Controllo della CMC corrisponde a `<Nomehost><Numporta><Nomedb>`, è necessario configurare il driver JAR in: `dataAccess\connectionServer\jdbc\<Tipodb>.sbo`.

Configurazione dei file SBO

In genere, le librerie ODBC sono già configurate nei file SBO ed è solo necessario aggiungere i nomi degli alias. In caso contrario, attenersi agli esempi seguenti per eseguire la configurazione nel file SBO:

Esempio:

- Se la versione di database utilizzata per il controllo è SAP HANA, la configurazione nel file SBO deve essere:

```
<DataBase Active="Yes" Name="SAP HANA database 1.0" Platform="MSWindows">
  <Aliases>
    <Alias>SAP High-Performance Analytic Appliance (SAP HANA) 1.0</Alias>
    <Alias>Hana</Alias>
  </Aliases>
```

```
<Libraries>
  <Library Platform="MSWindows">dbd_wnewdb</Library>
  <Library Platform="MSWindows">dbd_newdb</Library>
</Libraries>
<Parameter Name="Driver Name">HDBODBC</Parameter>
</DataBase>
```

- Se la versione di database utilizzata per il controllo è MS SQL Server 2008, la configurazione nel file SBO deve essere:

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
  <Libraries>
    <Library>dbd_wmssql</Library>
    <Library>dbd_mssql</Library>
  </Libraries>
  <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
  <Parameter Name="CharSet Table" Platform="Unix">datadirect</Parameter>
  <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
  <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
</DataBase>
```

- Se la versione di database utilizzata per il controllo è DB2, la configurazione nel file SBO deve essere:

```
<DataBase Active="Yes" Name="DB2 UDB for iSeries v5">
  <!-- You can add an alias here if you are using some connections that are defined with an older database engine -->
  <Alias>DB2/400 V5</Alias>
  <Alias>DB2/400 V4</Alias>
  <Alias>DB2 for iSeries v4</Alias>
  <Alias>DB2</Alias>
</Aliases>
```

- Se la versione di database utilizzata per il controllo è MySQL 5, nel file SBO deve essere inclusa la voce seguente:

```
<DataBase Active="Yes" Name="MySQL 5">
  <JDBCdriver>
    <ClassPath>
      <Path>C:\mysqljdbcdriver.jar</Path>
    </ClassPath>
    <Parameter Name="JDBC Class">com.mysql.jdbc.Driver</Parameter>
    <Parameter Name="URL Format">jdbc:mysql://$DATASOURCE/$DATABASE$</Parameter>
  </JDBCdriver>
  <Parameter Name="Driver Capabilities">Query,Procedures</Parameter>
  <Parameter Name="Force Execute">Always</Parameter>
  <Parameter Name="Extensions">mysql5,mysql,jdbc</Parameter>
</DataBase>
```

Per ulteriori informazioni sulla configurazione del driver nei file SBO, fare riferimento al *Manuale di accesso ai dati*.

20.3.2.3 Aggiunta di nomi di alias nel file SBO

Oltre alla configurazione del driver, è necessario aggiungere anche un alias nel file SBO incluso nella versione di database utilizzata per il controllo. Nella tabella seguente sono elencati i nomi di alias da utilizzare per i database specificati.

Nome DB	Nome alias da utilizzare nel file SBO
SAP HANA	Hana
Microsoft SQL Server	MS SQL Server
My SQL	MySQL
SAP Max DB	MaxDB
IBM DB2	DB2
Sybase SQL Anywhere	Sybase SQL Anywhere
Sybase Adaptive Server Enterprise	Sybase Adaptive Server Enterprise
Oracle	Oracle

È necessario utilizzare i nomi specificati poiché l'applicazione di monitoraggio cerca tali nomi nel file SBO.

Esempio:

Se il database utilizzato per il controllo è MS SQL Server 2008, è necessario aggiungere l'alias al file SBO come indicato:

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
  <Aliases>
    <Alias>MS SQL Server</Alias>
  </Aliases>
  <Libraries>
    <Library>dbd_wmssql</Library>
    <Library>dbd_mssql</Library>
  </Libraries>
  <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
  <Parameter Name="CharSet Table" Platform="Unix">datadirect</Parameter>
  <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
  <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
</DataBase>
```

20.3.2.4 Per passare al database di controllo

Cambiare il database in modo da archiviare le informazioni di tendenza di monitoraggio nel database di controllo.

1. Nell'area "Gestisci" della home page della CMC fare clic su **Applicazioni**.
2. Fare doppio clic su **Applicazione di monitoraggio** per aprire la pagina delle proprietà.
3. Nell'area "Impostazioni database di tendenza" selezionare **Utilizza database di controllo**.

20.4 Proprietà di configurazione

Questa sezione descrive le proprietà dell'applicazione di monitoraggio e come modificarle.

Per visualizzare le proprietà di configurazione dell'applicazione di monitoraggio:

1. Accedere alla scheda **Applicazioni** della CMC.
2. Fare clic con il pulsante destro del mouse su **Applicazione di monitoraggio** e scegliere **Proprietà**. Viene visualizzata la finestra "Proprietà dell'applicazione di monitoraggio". Le proprietà configurabili vengono descritte nella seguente tabella:

Sezione	Campo	Descrizione
	Abilita applicazione di monitoraggio	Selezionare questa opzione per abilitare le funzionalità di monitoraggio. Se si deseleziona questa opzione, verranno disabilitate tutte le funzioni di monitoraggio, tranne le probe. Verrà disabilitata anche la funzionalità di tendenza della probe.
	URL endpoint predefinito dell'agente JMX (IIOP)	Contiene l'URL dell'endpoint predefinito dell'agente JMX che utilizza il protocollo IIOP. Questo URL viene generato automaticamente se si abilita il monitoraggio e si riavvia il server. Questo è il protocollo predefinito per il servizio di monitoraggio. Questo campo è di sola lettura.
RMI	Abilita protocollo RMI per JMX	Per impostazione predefinita, questa opzione è disabilitata. Per abilitarla, è necessario fornire il numero di porta RMI. Questa porta può essere utilizzata sia per la voce del Registro di sistema RMI che per la porta del connettore RMI. La porta deve essere disponibile per il servizio, in caso contrario non sarà possibile avviare il servizio. Una volta fornito il numero di porta RMI, riavviare il server. Una volta riavviato il server, viene generato l'URL dell'endpoint dell'agente JMX RMI. Si tratta di una proprietà di sola lettura che contiene l'URL dell'endpoint dell'agente JMX che utilizza il protocollo RMI. Utilizzare questo URL per connettersi al monitoraggio da altri client.

Sezione	Campo	Descrizione
Metriche host	Abilita metriche host	<p>Per impostazione predefinita, questa opzione è disabilitata. Se si abilita questa opzione, è necessario fornire il percorso dell'installazione dei file binari SAPOSCOL.</p> <p>Per abilitare le metriche host, è necessario installare SAPOSCOL. Per ulteriori informazioni su come installare SAPOSCOL, consultare Installazione di SAPOSCOL.</p>

Sezione	Campo	Descrizione
Impostazioni database di tendenza	Utilizza database di controllo	Selezionare questa opzione per archiviare la cronologia della tendenza delle metriche nel database di controllo del CMS. Nota: per questo lavoro è necessario configurare l'applicazione di controllo di CMS.
	Utilizza database incorporato	Selezionare questa opzione per archiviare la cronologia della tendenza delle metriche e dei controlli nel database incorporato incluso nell'applicazione di monitoraggio.
	Elimina i dati più datati quando le dimensioni del database sono maggiori di (MB)	I dati del database di tendenza verranno eliminati quando le dimensioni del database superano il limite specificato. Un buffer del 30% viene creato per il database. Ad esempio, se questa proprietà è stata impostata su 100 MB e la verifica di sistema rileva che il database supera i 100 MB, verranno eliminati dati dal database fino a raggiungere i 70 MB.
	Esegui attività di pulizia del database ogni giorno alle	L'attività di pulizia del database viene avviata nell'ora specificata. La pulizia del database viene eseguita quando le sue dimensioni superano il limite massimo specificato.
	Backup del database di tendenza ogni	Specifica il numero di ore tra un backup e l'altro del database di tendenza. Se si imposta questo valore, viene eseguito un backup quando si avvia il sistema o ogni volta che viene riavviato l'APS e anche a ogni intervallo specificato.
	Directory di backup del database di tendenza	Per impostazione predefinita, il percorso non viene specificato. È possibile specificare una posizione, tuttavia è necessario utilizzare un percorso assoluto e non relativo. Nel caso di una posizione condivisa, è necessario autorizzare l'accesso a tale posizione.

Sezione	Campo	Descrizione
	Esegui attività di backup del database	L'attività di backup del database inizia quando si fa clic su questa opzione. Specificare il percorso della directory di backup del database prima di scegliere questa opzione.
	Esporta dati da database incorporato come file CSV	Fare clic sul pulsante Esporta per esportare il database come file con valori separati da virgola (CSV).
	Posizione database di tendenza	Per impostazione predefinita, il percorso del database di tendenza è <i>DIRINSTALL\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0/Data/TrendingDB</i> . È possibile specificare una posizione diversa, tuttavia, è necessario utilizzare un percorso assoluto e non relativo. Per gli ambienti cluster, la posizione può essere condivisa ed è necessario concedere l'autorizzazione di accesso alla posizione condivisa.

Sezione	Campo	Descrizione
Altre impostazioni	Intervallo di aggiornamento metrica (secondi)	<p>L'intervallo minimo che è possibile specificare è di 15 secondi. Tale intervallo si applica a quanto segue:</p> <ul style="list-style-type: none"> • Calcolo delle sottoscrizioni per i controlli: le regole di attenzione e di pericolo vengono calcolate costantemente con l'intervallo di tempo specificato. • Calcolo dello stato del controllo: lo stato del controllo viene calcolato costantemente con l'intervallo di tempo specificato se l'impostazione Evento del controllo è selezionata con l'opzione: Modifica stato di controllo ogni volta che la regola di attenzione o di pericolo restituisce true. • Periodo di tendenza: la modalità Cronologia dei grafici viene registrata continuamente con l'intervallo di tempo specificato.
	Intervallo di aggiornamento automatico UI di monitoraggio (secondi)	<p>Questo intervallo viene utilizzato nell'interfaccia utente di monitoraggio (inclusi cruscotto, elenco di controlli e probe) per l'aggiornamento automatico. L'intervallo minimo è di 15 secondi. L'aggiornamento automatico non interessa la durata in modalità Live nei grafici, impostata sul valore predefinito di 15 secondi.</p>
	Frequenza promemoria avviso (giorni)	<p>Specifica il numero di giorni prima della generazione di un promemoria avviso.</p>

3. Fare clic su **Salva**.

Nota:

Quando si modifica una di queste proprietà, ad eccezione di quella relativa all'abilitazione e alla disabilitazione dell'applicazione di monitoraggio, è necessario riavviare gli Adaptive Processing Server che ospitano i servizi di monitoraggio.

Installazione di SAPOSCOL

Attenersi alla seguente procedura per installare SAPOSCOL:

1. Scaricare SAPHOSTAGENT710_XX.SAR dal sito SAP Marketplace (<http://service.sap.com>).

2. Estrarre SAPHOSTAGENT710_XX.SAR eseguendo il comando `SAPCAR.EXE -xvf SAPHOSTAGENT710_XX.SAR`.
3. Installare saphostexec eseguendo il comando `saphostexec.exe -install`. Una volta installato saphostexec come servizio, viene avviato SAPOSCOL.
4. Verificare lo stato di SAPOSCOL eseguendo il comando `saposcol -s`.

20.4.1 URL dell'endpoint JMX

L'applicazione di monitoraggio espone un URL dell'endpoint JMX tramite il quale gli altri client possono eseguire la connessione utilizzando l'API remota JMX. Per impostazione predefinita, la connettività JMX viene fornita utilizzando il trasporto IIOP (Internet Inter-Orb Protocol) o CORBA (Common Object Request Broker Architecture). Questo URL di connessione viene visualizzato nella pagina delle proprietà dell'applicazione di monitoraggio. La possibilità di connettersi tramite IIOP risolve il problema dell'utilizzo di firewall e dell'esposizione delle porte. Le porte CORBA sono disponibili per impostazione predefinita. I file jar elencati nella seguente tabella sono necessari per la connessione del client JMX:

File Jar
activation-1.1.jar
axiom-api-1.2.5.jar
axiom-impl-1.2.5.jar
axis2-adb-1.3.jar
axis2-kernel-1.3.jar
cecore.jar
celib.jar
cesession.jar
commons-logging-1.1.jar
corbaidl.jar
ebus405.jar
log4j.jar
logging.jar
monitoring-plugins.jar
monitoring-sdk.jar
stax-api-1.0.1.jar
wsdl4j-1.6.2.jar

File Jar
wstx-asl-3.2.1.jar
XmlSchema-1.3.2.jar
TraceLog.jar
ceaspect.jar
aspectjrt.jar

Un'altra soluzione prevede la connessione tramite la porta predefinita RMI. Per ulteriori informazioni su come connettersi tramite la porta RMI, vedere [Proprietà di configurazione](#).

20.4.2 Autenticazione HTTPS per le probe di monitoraggio

È supportata l'autenticazione server HTTPS per le probe di monitoraggio. Prima di utilizzarla è necessaria la configurazione seguente:

1. Importare il certificato del server nel truststore del client. Ciò consente di verificare l'identità del server sul lato client (la probe). Eseguire il comando seguente:

```
<DIR_PRINCIPALE_INSTALLAZ>\SAP BusinessObjects Enterprise XI
4.0\win64_x64\sapjvm\lib> keytool -import -alias ca -keystore
"<DIR_PRINCIPALE_INSTALLAZ>\SAP BusinessObjects Enterprise XI
4.0\win64_x64\sapjvm\jre\lib\security\cacerts" -file ca.cer
```

ca.cer è il certificato con firma automatica del server o il certificato dell'autorità di certificazione (in genere una CA interna) che ha generato il certificato del server. Se il certificato del server viene generato da una CA ben nota, non è necessario importarlo ed è possibile ignorare questo passaggio. Il motivo di ciò è che il certificato del server verrà verificato con la CA, la cui chiave pubblica è già presente nel truststore per impostazione predefinita.
2. Cambiare la "base URL" nelle impostazioni della probe di BI Launch Pad in `https://<URL>/BOE/BI`, in cui <URL> fa riferimento all'host con il nome utilizzato nel certificato.

Non è supportata l'autenticazione client HTTPS per le probe di monitoraggio.

20.4.3 Crittografia delle password per le probe

Quando si utilizzano le probe, per verificare che le password siano crittografate, è necessario aggiungere il parametro `true` al parametro `password` delle singole probe di monitoraggio quando queste vengono create tramite la riga di comando. Per ulteriori informazioni e un esempio di sintassi, consultare l'argomento *Managing Probes Through the Command Line* nella Guida in linea della CMC.

20.5 Integrazione con altre applicazioni

Soluzioni Enterprise, come IBM Tivoli Monitoring, si integrano con l'applicazione di monitoraggio come client JMX che si connettono mediante l'URL dell'endpoint JMX. Dopo l'integrazione, le metriche di SAP BusinessObjects possono essere visualizzate dall'interfaccia utente del client.

20.5.1 Integrazione dell'applicazione di monitoraggio con IBM Tivoli

Per integrare l'applicazione di monitoraggio con IBM Tivoli, è necessario creare, installare e configurare un agente di monitoraggio IBM Tivoli. Attenersi alla seguente procedura per creare un agente di monitoraggio IBM Tivoli:

1. Installare il software IBM Tivoli Monitoring Agent Builder versione 6.2.1.
2. Creare un nuovo agente. Per informazioni sulla creazione di un nuovo agente, consultare il Manuale dell'utente di IBM Tivoli Monitoring Agent.
3. Nel passaggio "Defining data monitoring types" selezionare **Data from a server** nell'area "Monitoring Data Categories" e selezionare **JMX** nell'area "Data Sources".
4. Fare clic su **Avanti**.
5. Nella finestra "JMX Information", fare clic su **Browse** per visualizzare tutti gli MBean JMX sul server MBean.

Nota:

Se si esegue il browser per la prima volta, è necessario aggiungere una nuova connessione.

6. Nella finestra "Java Management Extensions (JMX) Browser" fare clic su + accanto a **Connection Name** per aggiungere una nuova connessione.
7. Nella finestra "MBean Server Connection Wizard", selezionare **Standard JMX Connections (JSR-160)**.
8. Inserire le informazioni seguenti nella finestra "Connection Properties":

Campo	Descrizione
Nome connessione	Server conforme a JSR-160
ID utente	Nome utente utilizzato per accedere alla piattaforma BI
Password	Password utilizzata per accedere alla piattaforma BI
URL servizio	Fornire l'URL dell'endpoint JMX

9. Fare clic su **Fine**.
10. Nell'area "MBean Key Properties", selezionare **Domain** e **Type**.

Tutti gli MBean vengono visualizzati nel campo di testo seguente.

11. Selezionare tutti gli MBean con il dominio Server, selezionandone uno alla volta affinché vengano elencati gli attributi. Scegliere un attributo chiave nel caso in cui siano presenti più MBean dello stesso tipo. Ad esempio, se esistono due istanze di un server in esecuzione, il PID di ciascuna istanza può essere un attributo chiave.
12. Selezionare un server e selezionare le opzioni per il gruppo di attributi JMX nella finestra "JMX Agent-Wide Options".
13. Nella finestra "Data Source Definition", selezionare l'agente aggiunto e fare clic su **Add to Selected**. Con questa azione si torna all'inizio del ciclo di creazione dell'agente ed è necessario ripetere i passi precedenti per aggiungere un altro server da monitorare.
14. Dopo aver creato l'agente, è necessario installarlo. Per ulteriori informazioni sulle modalità di installazione di un agente, consultare il Manuale dell'utente di IBM Tivoli Monitoring Agent dalla figura 154 in avanti. In questa sezione vengono fornite informazioni sull'installazione locale dell'agente, nonché sulla creazione di una soluzione installabile dell'agente.

Nota:

Se si sta creando un agente per la piattaforma BI mediante Agent Builder, è necessario che la piattaforma BI sia installata nello stesso sistema. Se tuttavia si esegue l'installazione di un agente già esistente utilizzando il relativo file di installazione, non è necessario che il monitoraggio della piattaforma BI sia installato poiché al momento della configurazione è possibile fornire i dettagli di un qualsiasi sistema con un endpoint JMX.

Per configurare un agente esistente, attenersi alla seguente procedura:

1. Aprire "Manage Tivoli Enterprise Monitoring Services" in modalità TEMS. Verrà visualizzato l'agente installato.
2. Fare clic con il pulsante destro del mouse sul modello dell'agente e selezionare **Configure using defaults**.
3. Selezionare il nome di un'istanza.

L'agente può essere configurato utilizzando due diversi protocolli: RMI e BOEIIOP.

Per utilizzare il protocollo RMI:

- Fare clic su **Avanti**. Non apportare alcuna modifica ai parametri Java.
- Fornire i valori per le credenziali JMX, ad esempio ID utente, Password e URL servizio. Per ulteriori informazioni, vedere *Proprietà di configurazione* negli argomenti correlati.
- Fare clic su **OK**.

Per utilizzare il protocollo BOEIIOP:

- Copiare i file `bcm.jar` e `cryptojFIPS.jar` da `%DirInstall%\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib` a una cartella nel sistema.
- Copiare i file jar elencati nella seguente tabella in un'altra cartella.
- Nei parametri Java, impostare gli argomenti JVM nel percorso della cartella
`-Djmx.remote.protocol.provider.pkgs = com.businessobjects.sdk.monitoring`
e `-Djmx.boeiiop.bcm.dir=<` in cui sono stati copiati i file `bcm.jar` e `cryptojFIPS.jar`.
- Selezionare **Avanti**.
- Fornire i valori per le credenziali JMX, ad esempio ID utente, Password e URL servizio. Per ulteriori informazioni, vedere *Proprietà di configurazione* negli argomenti correlati.

- Impostare il valore **<Jar Directories>** come posizione della cartella in cui è stato copiato l'elenco di file jar forniti nella tabella.
- Fare clic su **OK**.

File Jar
activation-1.1.jar
axiom-api-1.2.5.jar
axiom-impl-1.2.5.jar
axis2-adb-1.3.jar
axis2-kernel-1.3.jar
cecore.jar
celib.jar
cesession.jar
commons-logging-1.1.jar
corbaidl.jar
ebus405.jar
log4j.jar
logging.jar
monitoring-plugins.jar
monitoring-sdk.jar
stax-api-1.0.1.jar
wsdl4j-1.6.2.jar
wstx-asl-3.2.1.jar
XmlSchema-1.3.2.jar
TraceLog.jar
ceaspect.jar
aspectjrt.jar

4. Fare clic con il pulsante destro del mouse sull'agente e scegliere **Start** nella finestra "Manage Tivoli Enterprise Monitoring Services".
5. Aprire IBM Tivoli Enterprise Portal Desktop/Browser Client. Viene visualizzato un pulsante nella finestra "Navigator".
6. Fare clic sul pulsante **Navigator**.
L'agente viene aggiunto a Navigator.

Argomenti correlati

- [Proprietà di configurazione](#)

20.5.2 Integrazione dell'applicazione di monitoraggio con SAP Solution Manager

Per integrare l'applicazione di monitoraggio con SAP Solution Manager, è necessario che [Wily Introscope](#) sia installato e in esecuzione sul sistema. SAP Solution Manager deve essere configurato per la workstation Introscope. Eseguire i passaggi seguenti durante l'installazione della piattaforma BI:

1. Nel passaggio "Configure Connectivity to Introscope Enterprise Manager" fornire il nome host e i dettagli della porta. Introscope Agent viene installato in `C:\Programmi (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\Wiley` durante l'installazione della piattaforma BI.
2. Avviare la workstation Introscope e fare clic su **New Investigator**. È possibile visualizzare le metriche server di SAP BusinessObjects e le metriche virtuali delle probe nella sezione JMX dell'agente configurato.

Nota:

È possibile configurare l'agente Introscope (IS) scegliendo **CMC > Servers > Server node > Placeholders**. Seguendo questo percorso è anche possibile configurare la porta e l'host di IS Enterprise Manager per consentire la comunicazione tra l'agente IS e l'applicazione di monitoraggio. Per ulteriori informazioni, vedere l'argomento *Managing Servers* nella Guida in linea della CMC.

Per rendere le metriche JMX disponibili in IS, verificare che i servizi dell'agente IS e il servizio di monitoraggio siano disponibili nell'istanza di AdaptiveProcessingServer.

Se si abilita la strumentazione IS, la strumentazione del codice viene abilitata automaticamente.

20.6 Supporto cluster per il server di monitoraggio

L'applicazione di monitoraggio supporta il clustering, che offre funzionalità di failover.

Con il supporto cluster, solo un servizio sarà attivo in un dato momento e tutti gli altri servizi saranno passivi. Se in un ambiente cluster sono presenti i due servizi di monitoraggio s1 e s2, solo uno dei essi sarà disponibile. Sia s1 che s2 tentano di attivarsi, ma quando uno di essi ci riesce, l'altro diventa inattivo o passivo.

Il servizio passivo verifica periodicamente la disponibilità del servizio attivo (ogni minuto). Se il servizio attivo risulta non disponibile, il servizio passivo tenta immediatamente di passare allo stato attivo.

Nota:

È consigliabile che il servizio di monitoraggio venga ospitato in un'istanza separata di Adaptive Processing Server (APS) per evitare errori o la riduzione delle prestazioni del server APS.

20.7 Risoluzione dei problemi

In questa sezione vengono fornite soluzioni passo passo per un'ampia gamma di problemi che possono verificarsi con l'applicazione di monitoraggio.

20.7.1 Cruscotto

Il collegamento del cruscotto di monitoraggio non è visualizzato sulla pagina CMC

- Verificare se l'utente dispone di diritti di accesso adeguati.
- Assicurarci che l'utente venga aggiunto ai gruppi Monitoring User or Administrator o a qualsiasi altro gruppo che faccia parte di quelli appena citati.

Gli indicatori di prestazioni chiave non sono visibili sul cruscotto di monitoraggio

- Verificare se le metriche richieste sono visibili scegliendo **Proprietà server > Metriche**.
- Verificare che il Central Management Server risponda nel modo previsto.

Impossibile avviare l'applicazione di monitoraggio

Scaricare e installare l'ultima versione del lettore Flash.

20.7.2 Avvisi

Impossibile ricevere avvisi nella pagina Avvisi

- Verificare che sia selezionata l'opzione **Abilita avvisi personali** nelle proprietà dell'applicazione Avvisi.
- Assicurarci di disporre di diritti di accesso adeguati per ricevere avvisi.
- Verificare se gli avvisi recenti sono visibili sul cruscotto di monitoraggio.

Nota:

È possibile inviare un documento Crystal Reports all'ID di posta elettronica impostato per verificare che il protocollo SMTP funzioni come previsto.

Impossibile ricevere notifiche di posta elettronica

- Verificare che sia selezionata l'opzione **Abilita posta elettronica** nelle proprietà dell'applicazione Avvisi.

- Verificare che le impostazioni dell'indirizzo di posta elettronica per la ricezione degli avvisi siano appropriate.
- Verificare se il server SMTP funziona.
- Assicurarci che sia abilitata l'istanza Adaptive Job Server.
- Verificare le impostazioni SMTP nella destinazione dell'istanza Adaptive Job Server.

20.7.3 Elenco di controlli

Impossibile ricevere dati cronologici per Controllo

- Verificare l'intervallo di polling nella pagina **Proprietà** dell'applicazione di monitoraggio.
- Controllare il file di traccia nella cartella logging.
- Verificare se la **Posizione del database di tendenza** è specificata nella pagina **Applicazioni** della CMC. Per un ambiente cluster, verificare che l'utente disponga delle autorizzazioni necessarie per accedere alla posizione condivisa. Per ulteriori informazioni, vedere *Proprietà di configurazione* negli argomenti correlati.
- Assicurarci che l'orario di sistema del server e del client sia lo stesso in un fuso orario specifico.

Si è verificato un errore durante il recupero dei dati live sincronizzati

Verificare che l'istanza Adaptive Processing Server sia in esecuzione.

La scheda Elenco di controlli è disabilitata

- Verificare che il servizio di monitoraggio sia in esecuzione.
- Verificare la presenza di messaggi di errore nei registri del servizio di monitoraggio.
- Verificare che i server e le relative metriche siano visibili in jConsole.

Argomenti correlati

- [Proprietà di configurazione](#)

20.7.4 Probe

Impossibile pianificare i probe

- Verificare che l'istanza AdaptiveJobServer che ospita il Servizio di pianificazione probe sia in esecuzione.
- Assicurarci che il CUID del report, utilizzato per i documenti Crystal Reports e Web Intelligence, sia appropriato.
- Verificare che l'utente disponga di diritti di amministrazione o che sia un membro del gruppo Administrator.

- Verificare se l'utente dispone di diritti adeguati per aprire, aggiornare ed esportare documenti Crystal Reports o Web Intelligence utilizzati nelle probe corrispondenti.

Lo stato della pianificazione della probe è in sospeso

- Verificare se l'istanza di ProbeSchedulingService è installata.
- Verificare che l'istanza AdaptiveJobServer che ospita il Servizio di pianificazione probe sia in esecuzione.

Si è verificato un errore durante il recupero dei dati di tendenza dal database

Verificare se l'istanza di AdaptiveProcessingServer è in esecuzione.

Impossibile eseguire correttamente probeRun.bat

- Verificare se `java_home` è stato impostato.
- Verificare se al prompt dei comandi sono stati immessi i parametri corretti.

Nota:

immettere `probeRun.bat -help` al prompt dei comandi per verificare se tutti i parametri sono appropriati.

20.7.5 Metriche

Le metriche dell'host non sono elencate

- Assicurarsi che SAPOSCOL sia in esecuzione.
- Verificare che l'opzione **Abilita metriche host** sia selezionata sulla pagina **Proprietà** dell'applicazione di monitoraggio.
- Riavviare l'istanza di AdaptiveProcessingServer per applicare le modifiche.
- Verificare che il **Percorso dell'installazione dei file binari SAPOSCOL** sia appropriato.

Si è verificato un errore durante il recupero del client JMX

Verificare se l'istanza di AdaptiveProcessingServer è in esecuzione.

Il valore della metrica SAPOSCOL è zero sulla pagina Metrica

- Assicurarsi che SAPOSCOL sia in esecuzione.
- Eseguire i comandi seguenti sull'host in cui è installato SAPOSCOL:
 1. `saposcol -s` per controllare lo stato
 2. `saposcol -m` per ottenere un'istantanea dei dati raccolti da SAPOSCOL

20.7.6 Grafico

I grafici mostrano orari diversi per le modalità live e cronologia

Assicurarsi che l'orario di sistema del server e del client sia lo stesso in un fuso orario specifico.

I dati del grafico non vengono visualizzati in modalità cronologia per uno scenario di cluster

Assicurarsi che tutte le istanze di AdaptiveProcessingServer puntino alla stessa posizione del database Derby.

Controllo

21.1 Panoramica

La funzionalità di controllo consente di tenere traccia degli eventi significativi sui server e sulle applicazioni; ciò fornisce un quadro di insieme sulle informazioni cui si accede, sulle relative modalità di accesso e di modifica, nonché sull'utente che esegue tali operazioni. Le informazioni vengono registrate in un database denominato archivio dati di controllo (ADS). Una volta inseriti i dati nel database ADS, è possibile progettare report personalizzati in base alle proprie esigenze. È possibile trovare report e universi di esempio nella SAP Community Network <http://scn.sap.com/>.

Ai fini di questo capitolo, per sistema di controllo si intende qualsiasi sistema responsabile della registrazione o dell'archiviazione delle informazioni su un evento mentre per sistema controllato si intende qualsiasi sistema responsabile dell'esecuzione di un evento controllabile. In alcune circostanze un singolo sistema può svolgere entrambe le funzioni.

Funzionamento delle attività di controllo

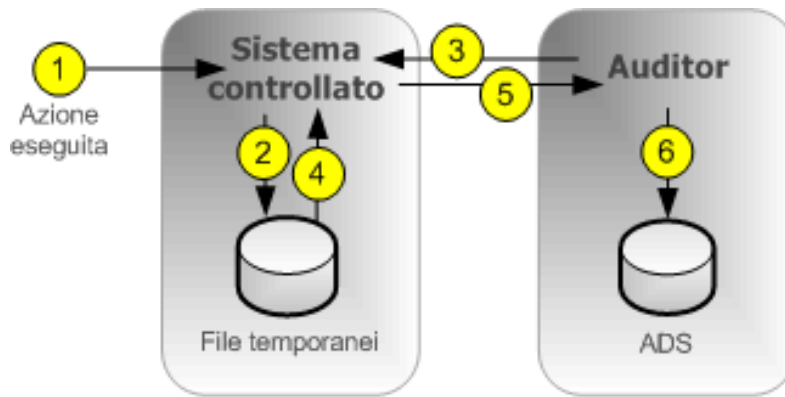
Central Management Server (CMS) riveste il ruolo di sistema di controllo, mentre ogni server o applicazione che attiva un evento controllabile funge da sistema controllato. Quando viene attivato un evento controllato, il sistema controllato genera un record e lo archivia in un file temporaneo locale. A intervalli regolari CMS comunica con i sistemi controllati per richiedere tali record e inserisce i dati nel database ADS.

CMS controlla inoltre la sincronizzazione degli eventi di controllo che si verificano su computer diversi. Ogni sistema controllato fornisce un'indicazione data e ora per gli eventi di controllo registrati. Per assicurarsi che le indicazioni data e ora degli eventi su server diversi siano coerenti, CMS trasmette periodicamente la propria ora di sistema ai sistemi controllati. I sistemi controllati confrontano quindi quest'orario con gli orologi interni. Se vengono rilevate differenze, correggono la data e l'ora registrate per gli eventi di controllo successivi.

A seconda del tipo di sistema controllato, verrà utilizzato uno dei seguenti workflow per registrare gli eventi.

Controllo dei server

In caso di eventi generati dal server, CMS può fungere sia da sistema controllato che da sistema di controllo.

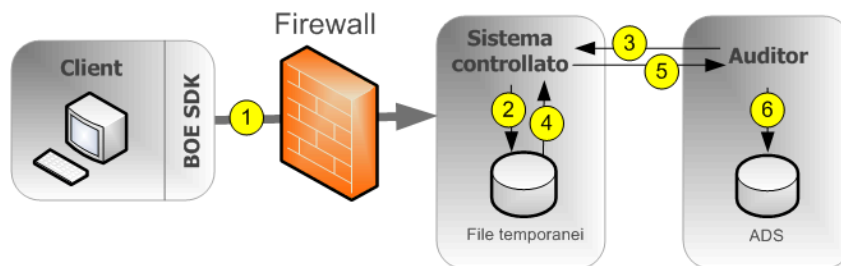


NOTA: l'Auditor e il sistema controllato possono coesistere sullo stesso server CMS.

1. Un evento controllabile è eseguito dal server.
2. Il sistema controllato scrive gli eventi in un file temporaneo. I passaggi 1 e 2 possono verificarsi più volte prima del passaggio 3.
3. A intervalli regolari il sistema di controllo interroga il sistema controllato e richiede un batch di eventi di controllo.
4. Il sistema controllato recupera gli eventi dai file temporanei.
5. Il sistema controllato trasmette gli eventi al sistema di controllo.
6. Il sistema di controllo scrive gli eventi nell'ADS e indica al sistema controllato di eliminare gli eventi dai file temporanei.

Controllo dell'accesso client per i client che si connettono tramite Corba

Riguarda applicazioni come SAP BusinessObjects Web Intelligence.



NOTA: l'Auditor e il sistema controllato possono coesistere sullo stesso server CMS.

1. Il client si connette a CMS, che funge da sistema controllato. Il client fornisce l'indirizzo IP e il nome del computer che verranno verificati dal sistema controllato.

Nota:

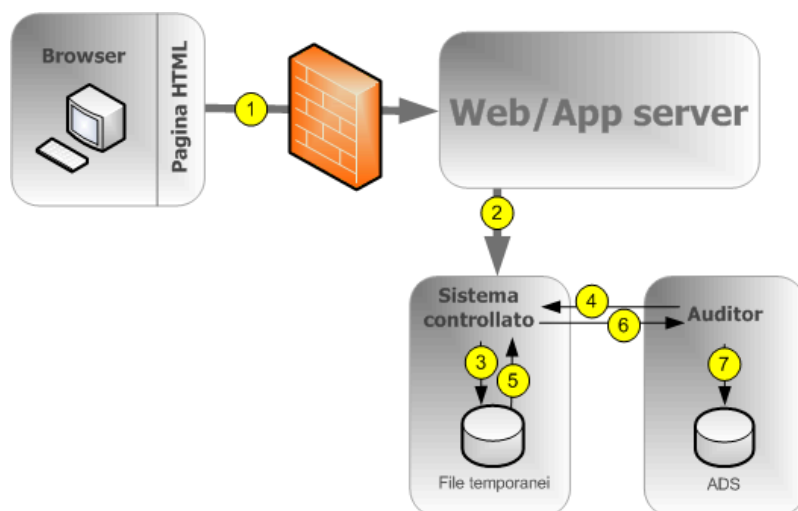
è necessario aprire una porta nel firewall tra il client e CMS. Per ulteriori informazioni sui firewall, consultare il capitolo relativo alla protezione del *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

2. Il sistema controllato scrive gli eventi in un file temporaneo. I passaggi 1 e 2 possono verificarsi più volte prima del passaggio 3.

3. A intervalli regolari il sistema di controllo interroga il sistema controllato e richiede un batch di eventi di controllo.
4. Il sistema controllato recupera gli eventi dai file temporanei.
5. Il sistema controllato trasmette gli eventi al sistema di controllo.
6. Il sistema di controllo scrive gli eventi nell'ADS e indica al sistema controllato di eliminare gli eventi dai file temporanei.

Controllo dell'accesso client per i client che si connettono tramite HTTP

Riguarda applicazioni online come BI Launch Pad, Central Management Console, SAP BusinessObjects Web Intelligence e così via.

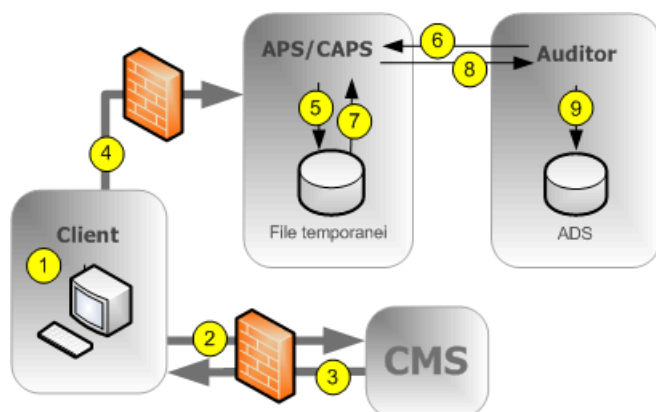


NOTA: l'Auditor e il sistema controllato possono coesistere sullo stesso server CMS.

1. Il browser si connette al server di applicazioni Web cui vengono inoltrati i dati di accesso.
2. L'SDK della piattaforma BI inoltra la richiesta di accesso al sistema controllato (CMS), insieme all'indirizzo IP e al nome del computer in cui è presente il browser.
3. Il sistema controllato scrive gli eventi in un file temporaneo. I passaggi da 1 a 3 possono verificarsi più volte prima del passaggio 4.
4. A intervalli regolari il sistema di controllo interroga il sistema controllato e richiede un batch di eventi di controllo.
5. Il sistema controllato recupera gli eventi dai file temporanei.
6. Il sistema controllato invia gli eventi al sistema di controllo.
7. Il sistema di controllo scrive gli eventi nell'ADS e indica al sistema controllato di eliminare gli eventi dai file temporanei.

Controllo non all'accesso per i client che si connettono tramite CORBA

Questo flusso di lavoro si applica agli eventi di controllo SAP BusinessObjects Web Intelligence durante la connessione tramite CORBA.



1. L'utente esegue un'operazione che può essere controllata.
2. Il client contatta CMS per verificare se l'operazione è configurata per il controllo.
3. Se l'azione è impostata per il controllo, CMS comunica l'informazioni al client.
4. Il client invia le informazioni sugli eventi al servizio proxy di controllo client, ospitato in Adaptive Processing Server.

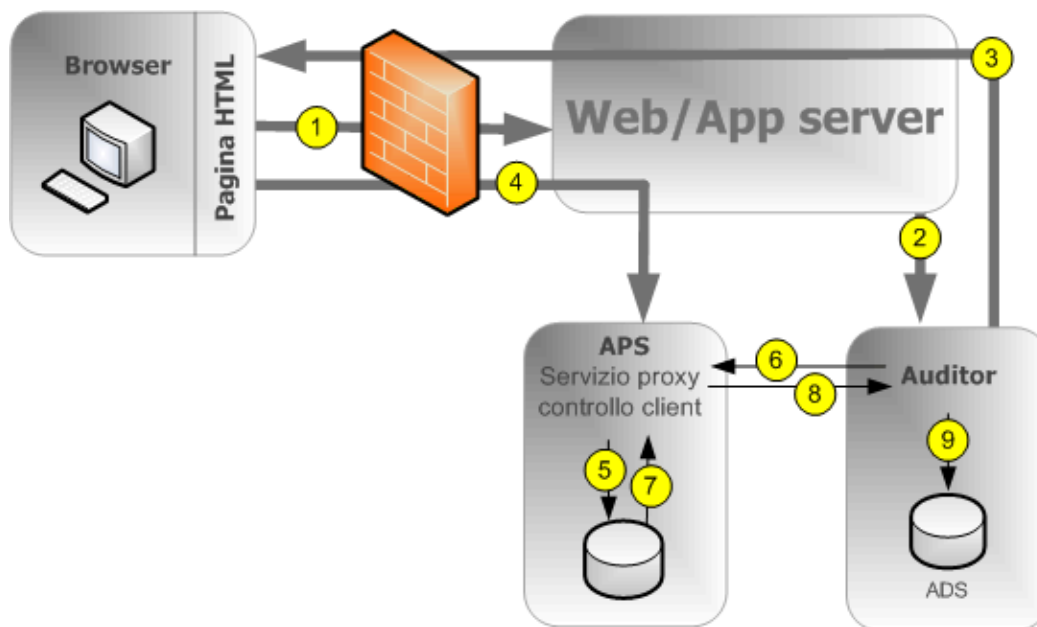
Nota:

è necessario aprire una porta nel firewall tra ogni client e ogni Adaptive Processing Server che ospiti CAP e tra ogni client e CMS. Per ulteriori informazioni sui firewall, consultare il capitolo relativo alla protezione del *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

5. Il CAPS scrive gli eventi in un file temporaneo. I passaggi da 1 a 5 possono verificarsi più volte prima del passaggio 6.
6. A intervalli regolari il sistema di controllo interroga il CAPS e richiede un batch di eventi di controllo.
7. Il CAPS recupera gli eventi dai file temporanei.
8. Il CAPS invia le informazioni sugli eventi al sistema di controllo.
9. Il sistema di controllo scrive gli eventi nell'ADS e indica al CAPS di eliminare gli eventi dai file temporanei.

Controllo non all'accesso per i client che si connettono tramite HTTP

Questo flusso di lavoro si applica agli eventi di controllo SAP BusinessObjects Web Intelligence (ad eccezione di quelli di accesso) durante la connessione tramite HTTP.



NOTA: l'Auditor e il sistema controllato possono coesistere sullo stesso server CMS.

1. L'utente avvia un evento potenzialmente controllabile. L'applicazione client contatta il server di applicazioni Web.
 2. L'applicazione Web verifica se l'evento è configurato per essere controllato.
- Nota:**
anche se il diagramma mostra il sistema di controllo CMS oggetto del contatto, qualsiasi CMS del cluster può essere contattato per queste informazioni.
3. CMS restituisce le informazioni di configurazione del controllo al server di applicazioni Web, che le passa all'applicazione client.
 4. Se l'evento è configurato per il controllo, il client invia le informazioni sugli eventi al server di applicazioni Web, il quale le passa al servizio proxy di controllo client (CAPS), ospitato in un Adaptive Processing Server (APS).
 5. Il CAPS scrive gli eventi in un file temporaneo. I passaggi da 1 a 5 possono verificarsi più volte prima del passaggio 6.
 6. A intervalli regolari il sistema di controllo interroga il CAPS e richiede un batch di eventi di controllo.
 7. Il CAPS recupera gli eventi dai file temporanei.
 8. Il CAPS invia le informazioni sugli eventi al sistema di controllo.
 9. Il sistema di controllo scrive gli eventi nell'ADS e indica al CAPS di eliminare gli eventi dai file temporanei.

Client che supportano il controllo

Le applicazioni client che supportano il controllo sono le seguenti:

- Central Management Console (CMC)
- BI Launch Pad
- OpenDocument
- Analisi

- Provider dei servizi Web Live Office
- Web Intelligence Rich Client

Nota:

Almeno un'istanza di CAPS deve essere in esecuzione per raccogliere eventi di controllo dai client sopra elencati.

I client non elencati non generano direttamente eventi, ma è possibile controllare alcune azioni eseguite dai server come risultato delle operazioni dell'applicazione client.

Coerenza del controllo

Nella maggior parte dei casi, se il controllo è stato installato, configurato e protetto correttamente e se vengono utilizzate le versioni corrette di tutte le applicazioni client, il controllo registrerà in modo corretto e coerente tutti gli eventi di sistema indicati. È importante ricordare, tuttavia, che alcune condizioni di sistema e ambiente possono compromettere il controllo.

C'è sempre un ritardo tra l'ora in cui si verifica un evento e il suo trasferimento finale nell'ADS. Tali ritardi possono essere incrementati da condizioni quali la mancata disponibilità di CMS o del database di controllo oppure la perdita di connettività della rete.

Come amministratore di sistema, è consigliabile evitare tutte le seguenti condizioni, in quanto potrebbero originare record di controllo incompleti:

- Un'unità in cui vengono archiviati i dati di controllo raggiunge la capacità massima. Occorre verificare la totale disponibilità dello spazio su disco per il database di controllo e i file temporanei del sistema controllato.
- Un server controllato viene rimosso in modo non corretto dalla rete, prima che abbia trasmesso tutti gli eventi di controllo: è necessario assicurarsi che durante la rimozione di un server dalla rete, si conceda il tempo necessario per l'invio degli eventi di controllo al database di controllo.
- Eliminazione o modifica dei file temporanei del sistema controllato.
- Errore dell'hardware o del disco.
- Danneggiamento fisico di un computer host controllato o di controllo

Esistono, inoltre, alcune condizioni per le quali gli eventi di controllo non sono in grado di raggiungere l'auditor CMS. Essi includono:

- Utenti con versioni client precedenti.
- La trasmissione di informazioni di controllo potrebbe essere bloccata da firewall configurati in modo non corretto.

Nota:

- gli eventi generati da applicazioni client contengono informazioni inviate dal lato cliente, ovvero esterne all'area del sistema ritenuta affidabile. Pertanto, in determinate condizioni queste informazioni potrebbero non essere attendibili come quelle registrate dai server di sistema.
- se si desidera rimuovere un server dalla distribuzione, è innanzitutto necessario disabilitarlo mantenendolo in esecuzione e connesso alla rete finché non sia stato possibile inserire tutti gli eventi dei file temporanei nel database di controllo. La metrica "Numero corrente degli eventi di controllo in coda" del server mostra il numero di eventi di controllo in attesa di essere trasferiti. Quando tale metrica raggiunge il valore zero, è possibile arrestare il server. La posizione dei file temporanei è definita nei segnaposto %DefaultAuditingDir% relativi al nodo in questione. Consultare il capitolo relativo all'amministrazione dei server per ulteriori dettagli sui segnaposto.

- se si intende utilizzare la funzionalità di controllo client, è consigliabile creare un Adaptive Processing Server dedicato per il Servizio proxy controllo client. In questo modo sarà possibile garantire prestazioni ottimali del sistema. Per aumentare la tolleranza agli errori del sistema è anche possibile eseguire il CAPS in più APS.

Collegamenti correlati

[Segnaposto server e nodo](#)

21.2 Pagina di controllo CMC

La pagina "Controllo" della console CMC è costituita dalle seguenti aree:

- " Riepilogo stato"
- "Imposta eventi"
- " Dettagli imposta eventi"
- "Configurazione"

21.2.1 Stato del controllo

Nel "riepilogo dello stato" del controllo è riportato un insieme di metriche che consente di ottimizzare la configurazione del controllo e di segnalare eventuali problemi che possono compromettere l'integrità dei dati di controllo. Il riepilogo dello stato è visualizzato nella parte superiore della pagina "Controllo" della console CMC.

Il riepilogo visualizza inoltre degli avvisi nelle seguenti circostanze:

- La connessione al database ADS non è disponibile.
- Non è in funzione o non è abilitato il servizio proxy controllo client, quindi è impossibile raccogliere gli eventi dei client.
- Un sistema controllato contiene eventi che non possono essere recuperati (il server o i server interessati verranno identificati). Ciò di solito indica che un server non è stato arrestato o spento in modo appropriato e contiene ancora eventi nei file temporanei.

Nota:

Le metriche del riepilogo dello stato sono contrassegnate in verde, in giallo o in rosso a indicare lo stato della funzionalità di controllo.

Metriche dello stato del controllo

Metrica	Dettagli
ADS Last Updated on	Data e ora dell'ultima volta in cui il CMS di controllo ha terminato la richiesta di eventi ai sistemi controllati.
Auditing Thread Utilization	<p>Percentuale del ciclo di polling utilizzata dal CMS di controllo per raccogliere i dati dai sistemi controllati, il tempo rimanente è quello che trascorre tra una richiesta e l'altra.</p> <p>Se il valore raggiunge il 100%, l'immagine sarà visualizzata in giallo, a indicare che lo strumento di controllo sta ancora raccogliendo dati dai sistemi controllati al momento in cui dovrebbe iniziare il prossimo ciclo di polling. Questo potrebbe causare ritardi negli eventi relativi all'ADS.</p> <p>Se questa circostanza si verifica di frequente o continuamente, si consiglia di aggiornare la distribuzione per consentire al database ADS di ricevere i dati a una velocità superiore (ad esempio, connessioni di rete più veloci o hardware di database più potente) o ridurre il numero di eventi di controllo registrati dal sistema.</p>
Last Polling Cycle Duration	<p>Durata dell'ultimo ciclo di polling in secondi. Indica il ritardo massimo con cui i dati dell'evento possono raggiungere l'ADS durante il ciclo di polling precedente.</p> <ul style="list-style-type: none"> Se il valore è inferiore a 20 minuti (1200 secondi), apparirà su uno sfondo verde. Se è compreso tra 20 minuti e 2 ore (7200 secondi), apparirà su uno sfondo giallo. Se è superiore a 2 ore, apparirà su uno sfondo rosso. <p>Se questo stato persiste e si ritiene che il ritardo sia eccessivo, si consiglia di aggiornare la distribuzione per consentire al database ADS di ricevere i dati a una velocità superiore (ad esempio, connessioni di rete più veloci o hardware di database più potente) o ridurre il numero di eventi di controllo registrati dal sistema.</p>
CMS Auditor	Nome del server CMS che attualmente funziona come strumento di controllo.
ADS Database Connection Name	Nome della connessione al database attualmente utilizzata dal CMS di controllo per collegarsi all'ADS. Per SQL Anywhere, SQL Server e i server SAP HANA, è il nome della connessione ODBC. Per altri tipi di database, sarà il nome del database e la porta di connessione, seguiti dal nome del server.
	Nome utente utilizzato dal CMS di controllo per accedere al database ADS.

Metrica	Dettagli
ADS Database User Name	

21.2.2 Configurazione del controllo eventi

La pagina Controllo della console CMC consente di attivare il controllo e di selezionare gli eventi che verranno controllati in tutto il sistema.

Se non si è interessati ad alcuni eventi o dettagli di eventi, è possibile lasciarli deselezionati per ottimizzare le prestazioni del sistema.

Nota:

se si è scelto di non configurare la connessione all'ADS durante l'installazione della piattaforma BI, sarà necessario impostare una connessione al database prima di configurare gli eventi per il controllo. Senza una connessione, gli eventi verranno comunque raccolti ma, una volta stabilita la connessione, verranno scritti nell'ADS. Per disattivare il controllo, dovrebbe essere disattivato il livello. Vedere *Impostazioni di configurazione ADS*.

21.2.2.1 Configurazione degli eventi di controllo

1. Selezionare la scheda **Controllo** nella console CMC.

Viene visualizzata la pagina **Controllo**.

2. Impostare l'indicatore **Imposta eventi** sul livello desiderato.

La tabella che segue indica le diverse impostazioni dell'indicatore e gli eventi acquisiti a ciascun livello.

Livello di controllo	Eventi acquisiti
Disattivato	Nessuna
Minimo	<ul style="list-style-type: none"> • Accesso • Logout • Modifica dei diritti • Livello di accesso personalizzato modificato • Modifica di controllo
Predefinito	Eventi contrassegnati con Minimo più: <ul style="list-style-type: none"> • Visualizza • Aggiorna • Prompt • Crea • Elimina • Modifica • Salva • Cerca • Modifica • Esegui • Fornitura
Completa	Eventi contrassegnati con Minimo e Predefinito più: <ul style="list-style-type: none"> • Attiva • Drill fuori dal livello • Pagina recuperata • Configurazione LCM • Rollback • Aggiungi VMS • Recupera VMS • Archivia nel sistema di gestione delle versioni • Estrai VMS • Esporta VMS • Blocca VMS • Sblocca VMS • Eliminazione VMS • Connessione cubo • Sessione MDAS <p>Nota: Se vengono installati componenti aggiuntivi, potrebbero verificarsi altri eventi.</p>
Personalizzata	Viene selezionato un insieme personalizzato di eventi.

3. Se è stata selezionata l'opzione **Personalizzato**, fare clic sugli eventi che si desidera acquisire

nell'elenco sotto l'indicatore **Imposta eventi**.

4. In "Dettagli imposta eventi" fare clic sui dettagli facoltativi che si desidera registrare con gli eventi. Registrando un numero minore di dettagli si migliorano le prestazioni del sistema .

Dettaglio	Descrizione
Query	Se impostato, il dettaglio eventi "Query" (ID dettaglio 25) verrà registrato per tutti gli eventi che eseguono una query sul database.
Dettagli percorso cartella	Se il valore viene impostato, verranno acquisiti i seguenti dettagli. <ul style="list-style-type: none"> • " Percorso cartella oggetto (ID dettaglio 71)" • "Nome cartella superiore (ID dettaglio 72)" • " Percorso cartella contenitore (ID dettaglio 64)"
Dettagli diritti	Se il valore viene impostato, verranno acquisiti i seguenti dettagli. <ul style="list-style-type: none"> • "Diritto aggiunto (ID dettaglio 55)" • "Diritto rimosso (ID dettaglio 56)" • "Diritto modificato (ID dettaglio 57)"
Dettagli gruppo utenti	Se il valore viene impostato, verranno acquisiti i seguenti dettagli. <ul style="list-style-type: none"> • "Nome gruppo utenti (ID dettaglio 16)" • "ID gruppo utenti (ID dettaglio 15)"
Dettagli valore proprietà	Se impostato, il dettaglio evento "Valore proprietà" (ID dettaglio 29) verrà acquisito quando le proprietà di un oggetto vengono aggiornate. Viene generato solo per eventi di CMC, BI Launch Pad o Sharepoint.

5. Fare clic su **Salva**.

Nota:

Per il controllo dei client, dopo aver apportato le modifiche potrebbe essere necessario attendere fino a due minuti prima che il sistema inizi a registrare i dati per i nuovi eventi. Assicurarsi di consentire questo ritardo quando si implementano modifiche al sistema.

21.2.3 Impostazioni di configurazione dell'archivio dati di controllo (ADS)

Se si è scelto di non impostare un database di controllo durante l'installazione della piattaforma BI o si desidera modificare il percorso o le impostazioni del database, è possibile eseguire le operazioni indicate di seguito per configurare la connessione all'ADS.

Questa è anche la posizione in cui è possibile configurare la durata di retention degli eventi di controllo nel database.

Se è stato eseguito un aggiornamento da una versione precedente di SAP BusinessObjects Enterprise XI 3.x ed è stata installata la versione 3.x di Business Objects Metadata Manager (BOMM), si consiglia di configurare l'ADS in modo tale che utilizzi lo stesso database o spazio tabelle di BOMM.

Nota:

se si utilizza un gruppo di lavoro DB2 9.7 esistente come database di controllo, verificare che l'account del database sia configurato per dimensioni di pagina maggiori di 8 KB.

21.2.3.1 Configurazione delle impostazioni del database ADS

1. Selezionare la scheda **Controllo** nella console CMC.
2. Nell'area "Configurazione", sotto l'intestazione "Database ADS", selezionare il tipo di database configurato per i dati di controllo.
3. Nel campo "Nome connessione " immettere il nome della connessione configurata per il database di controllo.

Tipo di data-base	Nome connessione
IBM DB2	nome servizio
Microsoft SQL Server	ODBC DSN
MySQL	<i>nomehostserver,porta,nomedatabase</i>
Oracle	Nome servizio TNS
SAP HANA	ODBC DSN
SAP MaxDB	<i>nomehostserver,porta,nomedatabase</i>
Sybase Adaptive Server Enterprise	nome servizio
Sybase SQL Anywhere	ODBC DSN

- a. Se si utilizza un database Microsoft SQL con autenticazione Windows, abilitare l'opzione **Autenticazione Windows**.
4. Nei campi **Nome utente** e **Password**, immettere il nome utente e la password che il CMS di controllo dovrà utilizzare per l'accesso al database.
Quando viene installato IBM DB2 come database predefinito nella piattaforma BI, lasciare vuoti i campi **Nome utente** e **Password**.

5. Nel campo **Elimina eventi più vecchi di (giorni)** immettere il numero di giorni in cui si desidera che le informazioni rimangano nel database (valore minimo 1, valore massimo 109,500).

Avvertenza:

I dati più vecchi rispetto al numero di giorni impostato verranno definitivamente eliminati dall'ADS e non potranno essere recuperati. Può essere opportuno spostare periodicamente i record in un database di archivio se si desidera utilizzare i record a lungo termine.

6. Nel caso in cui la connessione al database si interrompa, se si desidera ricollegare manualmente il CMS di controllo al database, deselezionare l'opzione **Riconnessione automatica ADS**.

Nota:

Se l'opzione non è selezionata, sarà necessario ristabilire manualmente una connessione all'ADS se si perde la connessione. L'operazione può essere eseguita riavviando il CMS o abilitando la **Riconnessione automatica ADS**. Gli eventi vengono registrati e restano memorizzati nei file temporanei finché l'ADS non viene riconnesso.

7. Fare clic su **Salva**.
8. Riavviare tutti i CMS del cluster.

Nota:

Il "Riepilogo stato" in alto nella pagina mostra i valori ADS correnti, che possono essere diversi da quelli presenti nella sezione "Database ADS", fino a quando non vengono riavviati i CMS.

21.3 Eventi di controllo

Nella tabella che segue sono riportati tutti gli eventi di controllo presenti nel sistema con una breve descrizione di ciascuno. Di seguito sono elencati i tipi di servizio che creano gli eventi.

Evento	Descrizione, server e client che generano il tipo di evento
Modifica di controllo	Le impostazioni di controllo del sistema vengono modificate. <ul style="list-style-type: none"> • Servizio Central Management
Crea	Un nuovo oggetto viene aggiunto al sistema. <ul style="list-style-type: none"> • Central Management Service • Servizio di modifica e visualizzazione Crystal Reports • Desktop Intelligence • Servizio Information Engine • Lifecycle Management • Web Intelligence • Servizio comune di Web Intelligence • Servizio principale di Web Intelligence • Servizio di elaborazione di Web Intelligence
Connessione cubo	Viene eseguita un'operazione di connessione al cubo OLAP. <ul style="list-style-type: none"> • Servizio di analisi multidimensionale
Livello di accesso personalizzato modificato	Le informazioni relative ai privilegi vengono modificate. <ul style="list-style-type: none"> • Servizio Central Management
Elimina	Un oggetto viene rimosso dal sistema. <ul style="list-style-type: none"> • Servizio Central Management • Servizio Lifecycle Management
Fornitura	Un oggetto viene inviato/consegnato a una destinazione. <ul style="list-style-type: none"> • Servizio di pianificazione aggiornamento autenticazione • Central Management Service • Servizio di pianificazione di Crystal Reports for Enterprise • Servizio di pianificazione Crystal Reports • Desktop Intelligence • Servizio di pianificazione consegna di destinazione • Servizio di pianificazione ricerca piattaforma • Servizio di pianificazione metriche • Servizio di pianificazione programma • Servizio di pianificazione query di protezione • Servizio di pianificazione importazione gruppi e utenti • Servizio di pubblicazione e pianificazione di Web Intelligence

Evento	Descrizione, server e client che generano il tipo di evento
Drill fuori dal livello	<p>Un utente di un documento Web Intelligence ha eseguito il drill down fino a un livello di dettaglio esterno ai dati precaricati del report.</p> <ul style="list-style-type: none"> • Web Intelligence • Servizio di elaborazione di Web Intelligence • Servizi comuni di Web Intelligence • Servizio principale di Web Intelligence • Servizio Information Engine
Modifica	<p>Il contenuto di un oggetto è stato modificato.</p> <ul style="list-style-type: none"> • Applicazione spazi di lavoro BI • Desktop Intelligence • Servizio Information Engine • Web Intelligence • Servizio comune di Web Intelligence • Servizio principale di Web Intelligence • Servizio di elaborazione di Web Intelligence
Configurazione LCM	<p>I dettagli di configurazione della console LCM (Lifecycle Management Console) sono cambiati.</p> <ul style="list-style-type: none"> • Lifecycle Management
Accesso	<p>Un utente ha eseguito l'accesso al sistema.</p> <ul style="list-style-type: none"> • Servizio Central Management
Logout	<p>Un utente ha eseguito la disconnessione dal sistema.</p> <ul style="list-style-type: none"> • Servizio Central Management
Modifica	<p>Le proprietà di file di un oggetto sono state modificate.</p> <ul style="list-style-type: none"> • Web Intelligence • Lifecycle Management • Servizio Central Management
Sessione MDAS	<p>Viene eseguita un'operazione da parte dei servizi di analisi multidimensionali</p> <ul style="list-style-type: none"> • Servizio di analisi multidimensionale
Pagina recuperata	<p>Un client SAP BusinessObjects Web Intelligence recupera informazioni aggiuntive dal repository.</p> <ul style="list-style-type: none"> • Servizio di elaborazione di Web Intelligence • Servizi comuni di Web Intelligence • Servizio principale di Web Intelligence • Servizio Information Engine

Evento	Descrizione, server e client che generano il tipo di evento
Prompt	<p>Vengono immesse informazioni per un prompt di oggetto.</p> <ul style="list-style-type: none"> • Servizio cache Crystal Reports • Servizio di pianificazione di Crystal Reports for Enterprise • Servizio di pianificazione Crystal Reports • Servizio cache Dashboards • Desktop Intelligence • Servizio Information Engine • Live Office • Web Intelligence • Servizio comune di Web Intelligence • Servizio principale di Web Intelligence • Servizio di elaborazione di Web Intelligence
Aggiorna	<p>I dati di un oggetto vengono aggiornati dal database su richiesta di un utente.</p> <ul style="list-style-type: none"> • Servizio cache Crystal Reports • Servizio di pianificazione di Crystal Reports for Enterprise • Servizio di pianificazione Crystal Reports • Servizio cache Dashboards • Desktop Intelligence • Servizio Information Engine • Live Office • Web Intelligence • Servizio comune di Web Intelligence • Servizio principale di Web Intelligence • Servizio di elaborazione di Web Intelligence
Recupera	<p>Viene recuperato un oggetto dal repository.</p> <ul style="list-style-type: none"> • Servizio Central Management • Desktop Intelligence
Modifica dei diritti	<p>Vengono modificate le informazioni sulla protezione per un utente, un gruppo o un oggetto.</p> <ul style="list-style-type: none"> • Servizio Central Management
Rollback	<p>Viene utilizzato Lifecycle Manager per riportare un oggetto a una versione precedente.</p> <ul style="list-style-type: none"> • Lifecycle Management

Evento	Descrizione, server e client che generano il tipo di evento
Esegui	<p>Viene eseguito un processo.</p> <ul style="list-style-type: none"> • Servizio di pianificazione aggiornamento autenticazione • Servizio di pianificazione di Crystal Reports for Enterprise • Servizio di pianificazione Crystal Reports • Desktop Intelligence • Servizio di pianificazione consegna di destinazione • Servizio di pianificazione LCM • Lifecycle Management • Servizio di pianificazione ricerca piattaforma • Servizio di pianificazione metriche • Servizio di pianificazione programma • Servizio di pianificazione pubblicazione • Servizio di replica • Servizio di pianificazione query di protezione • Servizio di pianificazione importazione gruppi e utenti • Servizio di pianificazione differenza visiva • Servizio di pubblicazione e pianificazione di Web Intelligence
Salva	<p>Un oggetto viene salvato dopo essere stato aggiornato o modificato.</p> <ul style="list-style-type: none"> • Analysis versione per OLAP • Servizio cache Crystal Reports • Servizio di pianificazione di Crystal Reports for Enterprise • Servizio di pianificazione Crystal Reports • Servizio di modifica e visualizzazione Crystal Reports • Dashboards • Desktop Intelligence • Servizio Information Engine • Lifecycle Management • Servizio di analisi multidimensionale • SAP BusinessObjects Mobile • Web Intelligence • Servizio comune di Web Intelligence • Servizio principale di Web Intelligence • Servizio di elaborazione di Web Intelligence
Cerca	<p>Viene eseguita una ricerca.</p> <ul style="list-style-type: none"> • Servizio di ricerca • Explorer • Lifecycle Management
Attiva	<p>Viene attivato un evento di file.</p> <ul style="list-style-type: none"> • Servizio eventi • Servizio Central Management

Evento	Descrizione, server e client che generano il tipo di evento
Visualizza	Viene visualizzato un oggetto. <ul style="list-style-type: none"> • Analysis versione per OLAP • BI Launch Pad • Applicazione spazi di lavoro BI • CMC • Servizio cache Crystal Reports • Servizio di modifica e visualizzazione Crystal Reports • Servizio cache Dashboards • Desktop Intelligence • Servizio Information Engine • OpenDocument • SAP BusinessObjects Mobile • Web Intelligence • Servizio comune di Web Intelligence • Servizio principale di Web Intelligence • Servizio di elaborazione di Web Intelligence
Aggiungi VMS	Un oggetto viene aggiunto al sistema di gestione delle versioni di LCM. <ul style="list-style-type: none"> • Lifecycle Management
Archiviazione in VMS	Un oggetto viene archiviato nel sistema di gestione delle versioni di LCM. <ul style="list-style-type: none"> • Lifecycle Management
Estrazione da VMS	Un oggetto viene estratto dal sistema di gestione delle versioni di LCM. <ul style="list-style-type: none"> • Lifecycle Management
Esporta VMS	Una risorsa viene esportata dal sistema VMS. <ul style="list-style-type: none"> • Lifecycle Management
Blocca VMS	Una risorsa in VMS è bloccata. <ul style="list-style-type: none"> • Lifecycle Management

Evento	Descrizione, server e client che generano il tipo di evento
Sblocca VMS	Una risorsa in VMS viene sbloccata. <ul style="list-style-type: none"> • Lifecycle Management
Recupera VMS	Un oggetto viene recuperato dal sistema di gestione delle versioni di LCM. <ul style="list-style-type: none"> • Lifecycle Management
Eliminazione VMS	Un oggetto viene eliminato dal sistema di gestione delle versioni di LCM. <ul style="list-style-type: none"> • Lifecycle Management

Eventi per tipo di servizio

Tipo di servizio	Tipi di evento generati
Servizio di pianificazione aggiornamento autenticazione	<ul style="list-style-type: none"> • Fornitura • Esegui
BI Launch Pad	Visualizza
Servizio Central Management	<ul style="list-style-type: none"> • Modifica di controllo • Crea • Livello di accesso personalizzato modificato • Elimina • Fornitura • Accesso • Logout • Modifica • Recupera • Modifica dei diritti • Attiva
Central Management Console	Visualizzazione
Servizio di pianificazione Crystal Reports	<ul style="list-style-type: none"> • Fornitura • Prompt • Aggiorna • Esegui • Salva
Servizio cache Crystal Reports	<ul style="list-style-type: none"> • Prompt • Aggiorna • Salva • Visualizza

Tipo di servizio	Tipi di evento generati
Servizio di pianificazione di Crystal Reports for Enterprise	<ul style="list-style-type: none"> • Fornitura • Prompt • Aggiorna • Esegui • Salva
Servizio di pianificazione Crystal Reports	<ul style="list-style-type: none"> • Fornitura • Prompt • Aggiorna • Esegui • Salva
Servizio di modifica e visualizzazione Crystal Reports	<ul style="list-style-type: none"> • Crea • Salva • Visualizza
Servizio cache Dashboards	<ul style="list-style-type: none"> • Prompt • Aggiorna • Visualizza
Applicazione Dashboards	<ul style="list-style-type: none"> • Salva
Desktop Intelligence (client)	<ul style="list-style-type: none"> • Fornitura • Prompt • Recupera • Esegui
Processo di pianificazione di Desktop Intelligence	<ul style="list-style-type: none"> • Fornitura • Esegui
Servizio di pianificazione consegna di destinazione	<ul style="list-style-type: none"> • Fornitura • Esegui
Servizio eventi	Attiva
Servizio Information Engine	<ul style="list-style-type: none"> • Crea • Drill fuori dal livello • Modifica • Pagina recuperata • Prompt • Aggiorna • Salva • Visualizza

Tipo di servizio	Tipi di evento generati
Servizio di pianificazione LCM	Esegui
Servizio LCM	<ul style="list-style-type: none"> • Crea • Elimina • Configurazione LCM • Modifica • Rollback • Esegui • Salva • Aggiungi VMS • Archivia nel sistema di gestione delle versioni • Estrai VMS • Eliminazione VMS • Esporta VMS • Blocca VMS • Recupera VMS • Sblocca VMS • Ricerca
Live Office	<ul style="list-style-type: none"> • Prompt • Aggiorna
Servizio di analisi multidimensionale	<ul style="list-style-type: none"> • Connessione cubo • Sessione MDAS • Salva
OpenDocument	Visualizzazione
Servizio di pianificazione ricerca piattaforma	<ul style="list-style-type: none"> • Fornitura • Esegui
Servizio di ricerca piattaforma	Ricerca
Servizio di pianificazione metriche	<ul style="list-style-type: none"> • Fornitura • Esegui
Servizio di pianificazione programma	<ul style="list-style-type: none"> • Fornitura • Esegui
Servizio di pianificazione pubblicazione	Esegui
Servizio di replica	Esegui
Servizio di pianificazione query di protezione	<ul style="list-style-type: none"> • Esegui • Fornitura

Tipo di servizio	Tipi di evento generati
Servizio di pianificazione importazione gruppi e utenti	<ul style="list-style-type: none">• Esegui• Fornitura
Servizio di pianificazione differenza visiva	Esegui
Applicazione Web Intelligence	<ul style="list-style-type: none">• Crea• Drill fuori dal livello• Modifica• Modifica• Prompt• Aggiorna• Salva• Visualizza
Servizio comune di Web Intelligence	<ul style="list-style-type: none">• Crea• Drill fuori dal livello• Modifica• Pagina recuperata• Prompt• Aggiorna• Salva• Visualizza

Tipo di servizio	Tipi di evento generati
Servizio principale di Web Intelligence	<ul style="list-style-type: none"> • Crea • Drill fuori dal livello • Modifica • Pagina recuperata • Prompt • Aggiorna • Salva • Visualizza
Servizio di elaborazione di Web Intelligence	<ul style="list-style-type: none"> • Crea • Drill fuori dal livello • Modifica • Pagina recuperata • Prompt • Aggiorna • Salva • Visualizza
Servizio di pubblicazione e pianificazione di Web Intelligence	<ul style="list-style-type: none"> • Fornitura • Esegui

Proprietà e dettagli degli eventi

Ogni evento registrato dalla piattaforma BI include un insieme di proprietà e dettagli dell'evento.

Le proprietà dell'evento vengono sempre generate con un evento, benché talvolta qualcuna non contiene valori se le informazioni non sono valide per un evento specifico. Nell'archivio dati di controllo, le proprietà dell'evento sono incluse nella tabella che contiene l'evento, quindi possono essere utilizzate per ordinare o raggruppare gli eventi quando si creano i report.

Nei dettagli dell'evento sono riportate informazioni aggiuntive sull'evento, che non sono incluse nelle proprietà dell'evento. Se un dettaglio di evento non è pertinente per un evento specifico, non verrà generato. Esiste un gruppo di dettagli di eventi comuni che possono essere generati per tutti i tipi di evento quando sono pertinenti. Esistono inoltre gruppi di dettagli di eventi aggiuntivi che vengono generati per tipi specifici di evento. Ad esempio, gli eventi di prompt indicano i valori immessi per il prompt in un dettaglio di evento, ma nessun altro tipo di evento genera un dettaglio di evento con valore di prompt. Nell'archivio dati di controllo, i dettagli vengono memorizzati in una tabella separata collegata all'evento principale.

In alcuni casi i dettagli evento possono includere più valori. Tali dettagli possono essere raggruppati utilizzando l'ID di gruppo. Per ulteriori informazioni sugli ID di gruppo, consultare gli argomenti correlati.

Eventuali dati multilingua, ad esempio nomi di oggetti o cartelle, verranno restituiti nella lingua predefinita in base alle impostazioni locali del server CMS di controllo.

Argomenti correlati

- [Tabelle dell'archivio dati di controllo](#)

21.3.1 Eventi di controllo e dettagli

Nelle sezioni che seguono sono indicati tutti i tipi di evento, seguiti da una descrizione delle proprietà e dei dettagli specifici di ciascun evento. All'inizio della sezione è riportato un elenco delle proprietà e dei dettagli comuni a tutti i tipi di evento.

Nota:

Alcuni programmi client non dispongono di propri eventi esclusivi e si affidano agli eventi comuni e della piattaforma per acquisire le informazioni necessarie per l'esecuzione delle operazioni.

Proprietà e dettagli degli eventi universali

Le seguenti tabelle indicano quali sono le proprietà e i dettagli degli eventi che vengono registrati per tutti gli eventi.

Nota:

Le proprietà di questa tabella rappresentano le colonne della tabella ADS_EVENT nell'archivio dati di controllo.

Proprietà dell'evento	Descrizione
Event_ID	Identificatore univoco per l'evento.
Client_Type_ID	Identificatore per il tipo di applicazione che ha eseguito l'evento
Service_Type_ID	Indica l'ID del tipo di servizio o applicazione che ha attivato l'evento.
Start_Time	La data e l'ora di inizio in cui l'evento è iniziato (GMT).
Durata	Durata dell'evento in millisecondi.
Session_ID	ID della sessione durante la quale l'evento è stato attivato.
Event_Type_ID	Tipo di evento, ad esempio 1002 per visualizzazione.
Status_ID	Registra l'esito positivo o negativo dell'azione ("0" = positivo, "1" = negativo). Alcuni eventi presentano tipi di stato aggiuntivi, i cui dettagli vengono forniti insieme alle descrizioni degli eventi.

Proprietà dell'evento	Descrizione
Object_ID	CUID dell'oggetto interessato (se applicabile). CUID dell'evento di avviso per gli eventi di attivazione. Nota: tutti gli oggetti non salvati nel repository CMS avranno come ID 0. Tali oggetti possono essere, ad esempio, documenti che non sono ancora stati salvati nel database CMS oppure sono archiviati localmente su un computer client. Sarà necessario utilizzare la proprietà Object_Name per differenziare gli oggetti.
User_ID	CUID dell'utente che ha eseguito l'evento.
User_Name	Nome utente dell'utente che ha eseguito l'evento.
Object_Name	Nome dell'oggetto interessato (se applicabile). Nome dell'evento di avviso per gli eventi di attivazione.
Object_Type_ID	CUID del tipo di oggetto (ad esempio, documento, cartella e così via).
Object_Folder_Path	Percorso completo della cartella in cui è situato l'oggetto interessato nel repository CMS. Ad esempio, Vendite/Nord America/Costa orientale
Folder_ID	CUID della cartella in cui è memorizzato l'oggetto.
Top_Folder_Name	Nome della cartella di livello superiore in cui è memorizzato l'oggetto interessato. Ad esempio, se l'oggetto si trova in Vendite/Nord America/Costa orientale, il valore è Vendite.
Top_Folder_ID	CUID della cartella di livello superiore in cui si trova l'oggetto interessato. Ad esempio, se l'oggetto si trova in Vendite/Nord America/Costa orientale, il valore è il CUID della cartella Vendite.
Cluster_ID	CUID del cluster CMS che ha registrato l'evento.
Action_ID	Identificatore univoco che può essere utilizzato per raggruppare una sequenza di eventi avviati da un'unica azione utente.

Nota:

Le proprietà di questa tabella rappresentano le colonne della tabella ADS_EVENT_DETAIL_TYPE_STR nell'archivio dati di controllo.

Dettagli dell'evento	ID	Descrizione
Errore	1	Viene utilizzato solo se l'azione ha esito negativo; testo di eventuali messaggi di errore generati dal tentativo.
ID elemento	2	Nome di un oggetto che risiede in un oggetto contenitore (ad esempio, un documento Live Office o cruscotto).
Nome elemento	3	ID generato per un oggetto che risiede in un oggetto contenitore (ad esempio, un documento Live Office o cruscotto).
ID tipo di elemento	5	Tipo di oggetto in un oggetto contenitore che viene visualizzato o modificato. Viene generato solo se applicabile.
ID documento principale	12	<ul style="list-style-type: none"> • Per un'istanza di documento: il CUID del documento principale. • Per i documenti principali: il relativo CUID.
ID universo	13	CUID dell'universo utilizzato dal documento o oggetto. Se si utilizzano più universi, verrà generato un dettaglio di evento per ciascuno di essi.
Nome dell'universo	14	Nome dell'universo utilizzato dal documento o oggetto. Se si utilizzano più universi, verrà generato un dettaglio di evento per ciascuno di essi.
Nome gruppo utenti	15	Nome del gruppo utenti a cui appartiene l'utente che esegue l'azione. Se l'utente appartiene a più gruppi, verrà generato un dettaglio di evento per ogni gruppo.
ID gruppo utenti	16	ID del gruppo utenti a cui appartiene l'utente che esegue l'azione. Se l'utente appartiene a più gruppi, verrà generato un dettaglio di evento per ogni gruppo.

Eventi comuni

I seguenti tipi di eventi sono comuni a tutti i server e client di SAP BusinessObjects.

Visualizza

L'utente ha visualizzato un documento o oggetto.

- ID tipo di evento: 1002

Dettagli dell'evento	ID	Descrizione
Dimensioni	17	Dimensione dell'oggetto (in byte) a cui si riferisce l'evento.
ID contenitore	32	CUID dell'oggetto contenitore, ad esempio un cruscotto, in cui risiede l'oggetto (se applicabile).
Tipo di contenitore	33	Tipo di applicazione del contenitore per l'oggetto (se applicabile).

Nota:

se si utilizza un servizio di ricerca, durante l'indicizzazione dei documenti è possibile che venga generato un numero elevato di eventi di visualizzazione dall'utente "Account sistema". Ciò è determinato dal servizio di indicizzazione della ricerca che apre i documenti allo scopo di creare l'indice di ricerca.

Aggiorna

Un oggetto è stato aggiornato dal database.

- ID tipo di evento: 1003

Dettagli dell'evento	ID	Descrizione
Dimensioni	17	Dimensione dell'oggetto (in byte) a cui si riferisce l'evento. Nota: per Crystal Reports con visualizzazione su richiesta questa impostazione è 0.
Numero di righe	63	Numero di record restituiti dal server di database. Nota: per Crystal Reports con visualizzazione su richiesta questa impostazione è 0.
Query	25	Indica la query SQL utilizzata per aggiornare i dati (facoltativo, impostato nella CMC).
Nome oggetto universo	31	Nome dell'universo utilizzato dal documento o dall'oggetto. Verrà generato un dettaglio di evento per ogni universo a cui accede il documento o l'oggetto.

Dettagli dell'evento	ID	Descrizione
Ambito documento	36	Indica le informazioni relative all'ambito previsto del documento in base alle impostazioni di pubblicazione (ad esempio: Paese=USA, Ruolo=Manager). Applicabile solo ai workflow di pubblicazione.
ID istanza pubblicazione	37	ID di questa istanza della pubblicazione. Applicabile solo ai workflow di pubblicazione.
Tipo di oggetto Live Office	10701	Identifica il tipo di oggetto che viene aggiornato in un documento Live Office (ad esempio, un report Crystal). Viene generato solo per i documenti Live Office.

Prompt

È stato immesso un valore per un prompt.

- ID tipo di evento: 1004

Dettagli dell'evento	ID	Descrizione
Nome del prompt	26	Nome assegnato al prompt, ad esempio "Data". Verrà generato un dettaglio separato per ogni prompt in un documento o oggetto e i dettagli verranno raggruppati.
Valore prompt	27	Il valore immesso per un prompt. Verrà generato un dettaglio separato per ogni valore immesso. I dettagli possono essere raggruppati insieme e messi in relazione con il nome del prompt.
Ambito documento	36	Informazioni sull'ambito previsto del documento, ad esempio: Paese=USA, Ruolo=Manager.
ID istanza pubblicazione	37	ID di questa istanza della pubblicazione. Applicabile solo ai workflow di pubblicazione.
Nome al momento della progettazione	90	Nome del documento Dashboards al momento della progettazione. Viene generato solo per aggiornamenti di Dashboards o per un documento Live Office che include un prompt.
Tipo di oggetto Live Office	10701	Identifica il tipo di oggetto che viene aggiornato in un documento Live Office (ad esempio, un report Crystal). Viene generato solo per i documenti Live Office in cui l'oggetto incorporato include un prompt.

Crea

L'utente ha creato un oggetto.

- ID tipo di evento: 1005

Dettagli dell'evento	ID	Descrizione
Dimensioni	17	Dimensione dell'oggetto (in byte) a cui si riferisce l'evento.
Sovrascrivi	21	Indica se il documento o l'oggetto è nuovo o sovrascrive un oggetto esistente (0=nuovo documento o oggetto, 1=sovrascrive un documento o oggetto esistente).
Aggiornamento all'apertura	23	Indica se il documento o oggetto è impostato in modo da essere automaticamente aggiornato all'apertura (0=nessun aggiornamento, 1=aggiornamento all'apertura). Viene generato solo se applicabile.
Descrizione	24	Restituisce le informazioni presenti nel campo della descrizione del documento o oggetto.

Elimina

L'utente ha eliminato un oggetto.

- ID tipo di evento: 1006

Modifica

L'utente ha modificato una proprietà di un file o le proprietà dei file di un oggetto.

- ID tipo di evento: 1007

Dettagli dell'evento	ID	Descrizione
Nome proprietà	28	Nome della proprietà modificata. Verrà generato un dettaglio di evento per ogni proprietà modificata.
Valore di proprietà	29	Nuovo valore per una proprietà modificata del documento o oggetto. Verrà generato un dettaglio di evento per ogni proprietà modificata.

Salva

Salvataggio o esportazione di un documento o oggetto a livello locale, remoto o nel repository CMS, nel formato già esistente o in un altro formato.

- ID tipo di evento: 1008
- Stati:
 - "0" indica che l'oggetto è stato correttamente salvato localmente
 - "1" indica che il tentativo non è riuscito
 - "2" indica che l'oggetto è stato correttamente salvato o esportato in un repository
 - "3" indica che l'oggetto è stato correttamente salvato o esportato in un nuovo formato

Dettagli dell'evento	ID	Descrizione
Dimensioni	17	Dimensioni in byte dell'oggetto salvato o esportato.
Nome file	18	Nome completo utilizzato per salvare il documento o l'oggetto. Se il file è stato salvato localmente da un'applicazione client, il nome include anche il percorso del file.
Sovrascrivi	21	Indica se il documento o l'oggetto è nuovo o sovrascrive un file già esistente. "0"=nuovo documento o oggetto, "1"=sovrascrive il documento o oggetto esistente.
Formato	22	Specifica il formato del documento salvato/esportato, visualizzato con la normale estensione di file di tre lettere, ad esempio "doc" per un file Microsoft Word o "pdf" per un file Adobe PDF.
Aggiornamento all'apertura	23	Indica se il documento o oggetto è impostato in modo da essere automaticamente aggiornato all'apertura ("0"=nessun aggiornamento, "1"=aggiornamento all'apertura). Viene generato solo se applicabile.

Cerca

Viene eseguita una ricerca.

- ID tipo di evento: 1009

Dettagli dell'evento	ID	Descrizione
Parola chiave	19	Parole chiave della ricerca eseguita.
Categoria	20	Categoria utilizzata nella ricerca (se applicabile).
Numero di righe	63	Numero di righe restituite dalla ricerca.

Modifica

L'utente ha modificato il contenuto di un oggetto.

- ID tipo di evento: 1010

Dettagli dell'evento	ID	Descrizione
Dimensioni	17	Dimensione dell'oggetto (in byte) a cui si riferisce l'evento.
Query	25	Se viene modificata una query SQL, indica la nuova query. Questa impostazione è facoltativa e può essere selezionata nella pagina Controllo della console CMC.
Nome oggetto universo	31	Nome dell'universo utilizzato dal documento o dall'oggetto. Verrà generato un dettaglio separato per ogni universo a cui accede il documento o l'oggetto.
ID contenitore	32	CUID del contenitore, ad esempio un cruscotto, in cui risiede l'oggetto (se applicabile).
Tipo di contenitore	34	Tipo di applicazione del contenitore per l'oggetto (se applicabile).
Percorso cartella contenitore	64	Percorso della cartella per il contenitore dell'oggetto (se applicabile).

Run

È stato eseguito un processo.

- ID tipo di evento: 1011
- Stati:
 - "0" indica che il processo ha avuto esito positivo
 - "1" indica che il processo ha avuto esito negativo
 - "2" indica che il processo ha avuto esito negativo ma che verrà nuovamente tentata l'esecuzione
 - "3" indica che il processo è stato annullato

Dettagli dell'evento	ID	Descrizione
Dimensioni	17	Dimensioni del documento (in byte) che è stato eseguito.
Ambito documento	36	Informazioni sull'ambito previsto del documento, ad esempio: Paese=USA, Ruolo=Manager.

Consegna

È stato consegnato un oggetto.

- ID tipo di evento: 1012

Dettagli dell'evento	ID	Descrizione
Dimensioni	17	Dimensioni del documento (in byte) che è stato consegnato.
Tipo di destinazione	35	Destinazione dell'istanza di documento o oggetto, ad esempio posta elettronica, FTP, disco non gestito, Posta in arrivo o stampante.
Ambito documento	36	Informazioni sull'ambito previsto del documento, ad esempio: Paese=USA, Ruolo=Manager
ID istanza pubblicazione	37	ID dell'istanza del documento o oggetto.
Dominio	38	Indica il nome di dominio del server SMTP per i documenti/oggetti distribuiti via posta elettronica (se applicabile).
Nome host	39	Indica il nome dell'host SMTP o FTP per i documenti/oggetti distribuiti via posta elettronica o FTP (se applicabile).
Porta	40	Indica la porta del dominio del server SMTP o FTP per i documenti/oggetti distribuiti via posta elettronica o FTP (se applicabile).
Indirizzo di invio	41	Indica l'indirizzo del mittente per i documenti/oggetti distribuiti via posta elettronica (se applicabile).
Indirizzo di destinazione	42	Indica l'indirizzo del destinatario per i documenti/oggetti distribuiti via posta elettronica (se applicabile). Viene inoltre specificato se l'indirizzo è incluso nei campi A, Cc o Ccn. Verrà generato un dettaglio di evento per ogni destinatario previsto.
Nome file	18	Indica il nome file dei documenti/oggetti distribuiti via posta elettronica o FTP oppure scritti direttamente su un disco che non fa parte dell'implementazione di Business Objects.
Account Name	45	Restituisce uno dei seguenti elementi: <ul style="list-style-type: none"> Per gli oggetti consegnati nella Posta in arrivo, un elenco di nomi di account utente di BusinessObjects. Per gli oggetti consegnati su FTP, il nome dell'account FTP. Per gli oggetti consegnati su un disco non gestito, l'account utilizzato per l'accesso. Per gli oggetti consegnati su SMTP, l'account utilizzato per l'accesso al server SMTP.
Nome stampante	46	Nome della stampante a cui è stato inviato il documento o l'oggetto (se applicabile).
Numero di copie	47	Numero di copie stampate del documento o oggetto (se applicabile).
Nome destinatario	48	Nome o nomi utente del destinatario o dei destinatari del documento o oggetto. Verrà generato un dettaglio di evento per ogni destinatario previsto.

Dettagli dell'evento	ID	Descrizione
ID evento di avviso	92	CUID dell'evento di avviso. Viene generato solo se l'evento è stato richiesto da un avviso.
Nome evento di avviso	93	Nome dell'evento di avviso. Viene generato solo se l'evento è stato richiesto da un avviso.
Tipo di consegna	75	Indica in che modo la consegna è stata avviata: <ul style="list-style-type: none"> "0" indica che è stata pianificata "1" indica che è stata inviata a una destinazione "2" indica che è stata pubblicata "3" indica che è stato attivato un avviso

Recupero

È stato recuperato un oggetto dal server CMS.

- ID tipo di evento: 1013

Accesso

Un utente effettua l'accesso.

- ID tipo di evento: 1014
- Stati:
 - "0" indica che l'accesso con licenza utente simultaneo ha avuto esito positivo
 - "1" indica un tentativo di accesso non riuscito
 - "2" indica che l'accesso con licenza utente designato ha avuto esito positivo
 - "3" indica che è stato eseguito correttamente un accesso non di utente (sistema)

Dettagli dell'evento	ID	Descrizione
Conteggio utenti simultanei	50	Numero di utenti connessi al sistema nel momento in cui l'evento è stato attivato.
Nome host del client segnalato dal client	51	Nome host del client restituito dal client.
Nome host del client risolto dal server	52	Nome host del client risolto dal server. Se non è possibile risolvere il nome host, non verrà restituito alcun valore.
Indirizzo IP del client segnalato dal client	53	Indirizzo IP del client restituito dal client.
Indirizzo IP del client risolto dal server	54	Indirizzo IP del client risolto dal server. Se non è possibile risolvere l'indirizzo IP del client, non verrà restituito alcun valore.

Disconnetti

Un utente effettua la disconnessione.

- ID tipo di evento: 1015

Dettagli dell'evento	ID	Descrizione
Conteggio utenti simultanei	50	Numero di utenti connessi simultaneamente al sistema nel momento in cui l'evento è stato attivato.

Attivazione

Viene attivato un evento di file.

- ID tipo di evento: 1016

Dettagli dell'evento	ID	Descrizione
Nome file	18	Nome del file che ha monitorato e attivato l'evento.

21.3.1.1 Eventi piattaforma

Gli eventi indicati di seguito sono specifici per la piattaforma BI.

Modifica dei diritti

I diritti relativi a un oggetto sono stati modificati.

- ID tipo di evento: 10003

Dettagli dell'evento	ID	Descrizione
Diritto aggiunto	55	Il tipo di diritto aggiunto, l'ambito del nuovo diritto, ovvero gli oggetti, e il tipo di oggetto cui si applica. Le informazioni verranno strutturate in base all'esempio seguente: diritto aggiunto=Esporta; nuovo valore=Concesso; ambito=Oggetto corrente; tipo di oggetto applicabile=tutti i tipi di oggetto.
Diritto rimosso	56	Il tipo di diritto rimosso, l'ambito del nuovo diritto, ovvero gli oggetti, e il tipo di oggetto cui si applica. Le informazioni verranno strutturate in base all'esempio seguente: diritto rimosso=Esporta; valore precedente=Negato; ambito=Oggetto corrente; tipo di oggetto applicabile=tutti i tipi di oggetto.
Diritto modifica- to	57	Il tipo di diritto modificato, l'ambito del nuovo diritto, ovvero gli oggetti, e il tipo di oggetto cui si applica. Le informazioni verranno strutturate in base all'esempio seguente: diritto modificato=Esporta; valore precedente=Concesso; ambito=Oggetto corrente; tipo di oggetto applicabile=tutti i tipi di oggetto.
Principale	118	L'ID di un utente o di un gruppo di utenti (principale) per cui sono stati modificati i diritti di protezione.
Nome princi- pale	119	Il nome di un utente o di un gruppo di utenti (principale) per cui sono stati modificati i diritti di protezione.

Livello di accesso personalizzato modificato

Un livello di accesso personalizzato è stato modificato.

- ID tipo di evento: 10004

Dettagli dell'evento	ID	Descrizione
Diritto aggiunto	55	Il tipo di diritto aggiunto, l'ambito del nuovo diritto, ovvero gli oggetti, e il tipo di oggetto cui si applica. Le informazioni verranno strutturate in base all'esempio seguente: diritto aggiunto=Esporta; nuovo valore=Concesso; ambito=Oggetto corrente; tipo di oggetto applicabile=tutti i tipi di oggetto.
Diritto rimosso	56	Il tipo di diritto rimosso, l'ambito del nuovo diritto, ovvero gli oggetti, e il tipo di oggetto cui si applica. Le informazioni verranno strutturate in base all'esempio seguente: diritto rimosso=Esporta; valore precedente=Negato; ambito=Oggetto corrente; tipo di oggetto applicabile=tutti i tipi di oggetto.
Diritto modifica- to	57	Il tipo di diritto modificato, l'ambito del nuovo diritto, ovvero gli oggetti, e il tipo di oggetto cui si applica. Le informazioni verranno strutturate in base all'esempio seguente: diritto modificato=Esporta; valore precedente=Concesso; ambito=Oggetto corrente; tipo di oggetto applicabile=tutti i tipi di oggetto.
Principale	118	L'ID di un utente o di un gruppo di utenti (principale) per cui sono stati modificati i diritti di protezione.

Modifica controllo

È stata apportata una modifica alle impostazioni di controllo del sistema.

- ID tipo di evento: 10006

Dettagli dell'evento	ID	Descrizione
ID tipo di evento	58	Indica l'ID del tipo di evento di controllo che è stato abilitato o disabilitato. Se vengono abilitati o disabilitati più tipi di evento in una sola azione, verrà generato un dettaglio dell'evento per ciascun tipo di evento.
Azione	59	Indica gli eventi di controllo abilitati e quelli disabilitati.
Nuovo livello di controllo	60	Se il livello di controllo del dettaglio viene modificato, registra l'impostazione del nuovo livello (ad esempio disattivo, minimo o predefinito).
Livello di controllo precedente	61	Se il livello di controllo del dettaglio viene modificato, registra l'impostazione del livello precedente (ad esempio disattivo, minimo o predefinito).

Dettagli dell'evento	ID	Descrizione
Opzione di controllo	62	Se viene abilitato o disabilitato un dettaglio facoltativo, viene indicato il dettaglio modificato e se è stato abilitato o disabilitato. Se vengono abilitati o disabilitati più dettagli in un'unica azione, verrà generato un record dettagliato per ciascun dettaglio modificato.
Connessione ADS	78	Se la connessione all'archivio dati di controllo viene modificata, registra le nuove impostazioni di connessione utilizzando il formato seguente: DBType=Oracle, DBName=MyADS, Username=USR1, Password="*****", SSO=off, DBReconnect=on. Verranno registrati solo i dettagli modificati. Se, ad esempio, il nome utente è l'unico elemento aggiornato, verrà registrato solo Username="new". Nota: le informazioni relative alla password saranno sempre oscurate mediante asterischi * nel database.
Intervallo di eliminazione automatica	105	Questo dettaglio registra le modifiche al campo Elimina eventi più vecchi di nella pagina Controllo della CMC. Questa impostazione determina il numero di giorni in cui le informazioni di controllo verranno conservate nel database ADS.

21.3.1.2 eventi SAP BusinessObjects Web Intelligence

Gli eventi seguenti sono specifici del componente SAP BusinessObjects Web Intelligence.

Drill fuori dal livello

L'utente ha eseguito il drill al di fuori del livello del report.

- ID tipo di evento: 10201

Dettagli dell'evento	ID	Descrizione
Istanza oggetto	11	Indica se l'evento è il risultato di un aggiornamento pianificato o di un utente che visualizza l'oggetto ("0" = indica che è il risultato di un utente che visualizza l'oggetto, "1" = indica che è il risultato di un aggiornamento pianificato dell'oggetto)
Numero di righe	63	Il numero di righe restituito dal server di database.
Query	25	Indica la query utilizzata per aggiornare i dati (facoltativo, impostato nella CMC).
Nome oggetto universo	31	Nome dell'universo utilizzato dal documento. Verrà registrata un'istanza per ciascun universo cui accede il documento.
ID universo	32	CUID dell'universo utilizzato dal documento. Verrà registrata un'istanza per ciascun universo cui accede il documento.

Pagina recuperata

È stata recuperata la pagina del documento Web Intelligence.

- ID tipo di evento: 10202

21.3.1.3 Eventi SAP BusinessObjects Analysis, versione per OLAP

Sessione MDAS

Viene eseguita un'operazione relativa alla sessione MDAS

- ID tipo di evento: 10300
- Stati:
 - "0" = è stata aperta una nuova sessione.
 - "1" = non è stato possibile aprire una nuova sessione.
 - "2" = è stata chiusa una sessione esistente.

Connessione cubo MDAS

È stata eseguita un'operazione relativa alla connessione cubo.

- ID tipo di evento: 10301
- Stati:
 - "0" = è stata aperta una nuova connessione.
 - "1" = non è stato possibile aprire una nuova connessione.
 - "2" = è stata chiusa una connessione esistente.

Dettagli dell'evento	ID	Descrizione
ID di connessione	94	Identificativo univoco della connessione.
Nome connessione	95	Nome della connessione.
Tipo di provider	96	Il tipo di provider per il cubo.
Nome cubo	97	Nome completo del cubo utilizzato.

21.3.1.4 Eventi di Lifecycle Management Console per SAP BusinessObjects

Gli eventi seguenti riguardano esclusivamente il componente Lifecycle Management per SAP BusinessObjects.

Dettagli comuni di SAP BusinessObjects Lifecycle Management Console

Di seguito sono indicati i dettagli aggiuntivi degli eventi di Lifecycle Management.

Dettagli dell'evento	ID	Descrizione
Cluster elemento	6	Il CUID o i cluster interessati quando Lifecycle Management Console esegue un'operazione sugli oggetti che si trovano in cluster diversi. Verrà generato un dettaglio eventi per ogni cluster interessato.
Commento elemento	7	Informazioni aggiuntive sull'oggetto.
Elemento primario	8	Se l'elemento è un elemento primario, questo dettaglio verrà impostato su "1", se invece è un elemento dipendente, verrà impostato su "0".
Stato elemento	9	Se l'elemento dell'operazione restituisce un errore, questo dettaglio verrà impostato su "1". In caso contrario, sarà "0".
Operazione	10	Descrive il tipo di operazione eseguita, ad esempio Aggiungi, Elimina o Modifica.

Configurazione di SAP BusinessObjects Lifecycle Management Console

La configurazione di Lifecycle Management è cambiata.

- ID tipo di evento: 10900

Dettagli dell'evento	ID	Descrizione
Configurazione	100	Un utente visualizza la configurazione di Lifecycle Management Console. La configurazione viene visualizzata sotto forma di coppie di valori separate da virgole, ad esempio: impostazioni rollback=abilite, porta=900.
Configurazione prima	101	Se le impostazioni di Lifecycle Management Console per un oggetto vengono modificate, registra le impostazioni di configurazione precedenti. Utilizza lo stesso formato di Configurazione.
Configurazione dopo	102	Se le impostazioni di Lifecycle Management Console per un oggetto vengono modificate, registra le nuove impostazioni di configurazione. Utilizza lo stesso formato di Configurazione.
Tipo VMS	10900	Il tipo di sistema di gestione delle versioni.

Rollback

È stata ripristinata la versione precedente di VMS (Version Management System) per un oggetto.

- ID tipo di evento: 10901

Aggiungi VMS

Una risorsa viene aggiunta al sistema VMS.

- ID tipo di evento: 10902

Dettagli dell'evento	ID	Descrizione
Versione	104	Indica il numero di versione del documento nel sistema VMS.

Recupera VMS

Una risorsa viene recuperata dal sistema VMS.

- ID tipo di evento: 10903

Dettagli dell'evento	ID	Descrizione
Ripristina oggetto eliminato	103	Indica se un oggetto recuperato è stato eliminato dal sistema. "0" indica che l'oggetto non è stato eliminato, "1" indica il contrario.
Versione	104	Indica il numero di versione del documento nel sistema VMS.

Archivia nel sistema di gestione delle versioni

Una risorsa viene archiviata nel sistema VMS.

- ID tipo di evento: 10904

Dettagli dell'evento	ID	Descrizione
Versione	104	Indica il numero di versione del documento nel sistema VMS.

Estrai VMS

Una risorsa viene estratta dal sistema VMS.

- ID tipo di evento: 10905

Dettagli dell'evento	ID	Descrizione
Versione	104	Indica il numero di versione del documento nel sistema VMS.

Esporta VMS

Una risorsa viene esportata dal sistema VMS.

- ID tipo di evento: 10906

Dettagli dell'evento	ID	Descrizione
Versione	104	Indica il numero di versione del documento nel sistema VMS.

Blocca VMS

Una risorsa del sistema VMS viene bloccata per impedire agli utenti di modificarla.

- ID tipo di evento: 10907

Dettagli dell'evento	ID	Descrizione
Versione	104	Indica il numero di versione del documento nel sistema VMS.
Bloccato da	10901	Il nome utente dell'utente che ha eseguito l'azione.

Sblocca VMS

Una risorsa del sistema VMS viene sbloccata per consentire agli utenti di modificarla.

- ID tipo di evento: 10908

Dettagli dell'evento	ID	Descrizione
Versione	104	Indica il numero di versione del documento nel sistema VMS.
Sbloccato da	10902	Il nome dell'utente che ha eseguito l'azione.

Eliminazione VMS

Una risorsa viene eliminata dal sistema VMS.

- ID tipo di evento: 10909

Dettagli dell'evento	ID	Descrizione
Versione	104	Indica il numero di versione del documento nel sistema VMS.

Ricerca piattaforma

22.1 Informazioni sul servizio di ricerca piattaforma

Ricerca piattaforma consente agli utenti di eseguire ricerche sul contenuto all'interno del repository della piattaforma SAP BusinessObjects Business Intelligence. Affina i risultati della ricerca raggruppandoli in categorie e classificandoli in ordine di rilevanza.

In questa versione della piattaforma BI, Ricerca piattaforma è stata potenziata con le funzionalità seguenti:

- Ricerca di contenuti della piattaforma BI ed Explorer.
- Suggerimento di una query per la creazione di un documento, se non riesce a trovare un documento esistente.
- Supporto dell'indicizzazione continua e basata su pianificazione
- Supporto dell'indicizzazione in un ambiente cluster
- Impostazione e modifica del livello di indicizzazione
- Opzioni di configurazione della ricerca avanzate
- Supporto della ricerca e dell'indicizzazione multilingue
- Sintassi di ricerca avanzata
- Supporto di metadati, contenuti e facet dinamici
- Supporto della riparazione automatica in base al carico del sistema

Nota:

se si esegue la migrazione dalla versione precedente alla nuova versione, l'indice non verrà migrato.

22.1.1 SDK applicazione di ricerca piattaforma

La ricerca piattaforma supporta un SDK pubblico che funziona come interfaccia tra l'applicazione client e il servizio di ricerca piattaforma. Viene esposto pubblicamente allo scopo di consentire la personalizzazione del servizio di ricerca e l'integrazione di questo con l'applicazione.

Quando un parametro di richiesta ricerca viene inviato tramite l'applicazione client al livello SDK, il livello SDK converte il parametro di richiesta in un formato codificato XML e lo passa al servizio Ricerca piattaforma.

Per ulteriori informazioni sull'API di Ricerca piattaforma, consultare il manuale *Business Intelligence platform Java API Reference*.

22.1.2 Ambiente cluster

Ricerca piattaforma consente di suddividere il carico su più nodi di un ambiente cluster. La distribuzione in un ambiente cluster assicura un utilizzo ottimale delle risorse del sistema e migliora le prestazioni del server.

Ricerca piattaforma supporta il clustering orizzontale e verticale per le funzionalità di ricerca e di indicizzazione. Con gli ambienti cluster, ottimizza le prestazioni dei processi sia di ricerca che di indicizzazione.

Bilanciamento del carico

Il servizio ricerca piattaforma supporta il bilanciamento del carico sia per l'indicizzazione che per la ricerca. In un ambiente cluster, le richieste di indicizzazione e di ricerca possono essere eseguite su più nodi per suddividere il carico. Ciascun nodo elabora indipendentemente l'indicizzazione del contenuto e la creazione di indici delta. Tuttavia, solo un nodo del cluster funge da indice principale e unisce gli indici delta nell'indice principale. Tutti i nodi possono accedere all'indice master. In questo modo si consentono richieste di ricerca simultanee.

Failover

Il meccanismo di failover garantisce la continuità delle operazioni di ricerca e di indicizzazione degli utenti. Quando un nodo nel cluster non è più disponibile a causa di un errore tecnico o di attività di manutenzione, un altro nodo elabora automaticamente le richieste di indicizzazione e ricerca.

22.2 Impostazione della ricerca piattaforma

22.2.1 Distribuzione di OpenSearch

Ricerca piattaforma supporta lo standard OpenSearch, consentendo la comunicazione con le applicazioni client mediante tale standard o il rispettivo formato. Per impostazione predefinita, OpenSearch non viene installato con la suite SAP BusinessObjects Business Intelligence, pertanto gli utenti devono distribuirlo manualmente come file WAR separato (`opensearch.war`) in un server di applicazioni come Tomcat oppure mediante lo strumento WDeploy. Tale file viene copiato nella directory `DIRINS` `TALL\warfiles\OpenSearch` dal programma di installazione.

Nota:

- È necessario che i programmi client seguano gli standard OpenSearch per comunicare con Ricerca piattaforma.
- Quando si installa la piattaforma BI, il server di applicazioni Tomcat viene installato per impostazione predefinita.

22.2.1.1 Distribuzione manuale

Per distribuire OpenSearch in un ambiente della piattaforma BI, effettuare le operazioni seguenti:

1. Passare al percorso seguente: `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\`.
2. Copiare la cartella OpenSearch in `DIRINSTALL\tomcat\webapps\`.
3. Modificare i parametri di configurazione nel file `\OpenSearch\WEB-INF\config.properties`:
 - CMS: nome del CMS con il numero di porta: `<Nome CMS>:<Numero porta>`.
 - OpenDocURL: URL dell'applicazione OpenDocument: `http://<host tomcat>:<porta connettore>/BOE/OpenDocument/opendoc/openDocument.jsp`.
 - Proxy.rpurl: il nome del server proxy inverso è necessario se si desidera utilizzare un proxy inverso.
 - Proxy.opendoc.rpurl: il nome del server proxy inverso opendoc è necessario se si desidera utilizzare un proxy inverso.
4. Riavviare il server di applicazioni Tomcat per distribuire OpenSearch.

22.2.1.2 Distribuzione mediante WDeploy

Per distribuire OpenSearch utilizzando WDeploy, effettuare le operazioni seguenti:

Nota:

Per Windows e UNIX, i comandi vengono indicati come `wdeploy.bat <parametri>` e `wdeploy.sh <parametri>`, rispettivamente.

1. Aggiornare il file `config.server applicazioni` che si trova in `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf` con i parametri del server di applicazioni Web richiesti, ad esempio directory di installazione, nome istanza, porta ammin, nome utente ammin e password ammin.
2. Modificare i parametri di configurazione nel file `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\OpenSearch\WEB-INF\config.properties`:
 - CMS: nome del CMS con il numero di porta: `<Nome CMS>:<Numero porta>`.

- OpenDocURL: l'URL dell'applicazione OpenDocument: `http://<Host server applicazione Web>:<portaconnettore>/BOE/OpenDocument/opensdoc/openDocument.jsp`.
 - Proxy.rpurl: il nome del server proxy inverso è necessario se si desidera utilizzare un proxy inverso.
 - Proxy.opendoc.rpurl: il nome del server proxy inverso opensdoc è necessario se si desidera utilizzare il proxy inverso.
3. Eseguire il comando `wdeploy.bat` <server applicazioni Web>
`-Dapp_source_tree=<cartella principale webapp OpenSearch> -DAPP=OpenSearch`
 deploy dal percorso `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\wdeploy`.
 Ad esempio, il comando seguente distribuisce OpenSearch in un server di applicazioni Web WebSphere 7:
- ```
wdeploy.bat websphere7 -Dapp_source_tree="INSTALLDIR\SAP BusinessObjects Enterprise XI 4.0\warfiles" -DAPP=OpenSearch deploy
```
4. Riavviare il server delle applicazioni.

## 22.2.2 Configurazione del proxy inverso

Per distribuire applicazioni Web in un server di applicazioni Web protetto da un server proxy inverso, configurare il server proxy inverso in modo da mappare le richieste URL in entrata al file WAR corretto.

per illustrare la procedura di configurazione, come esempio viene utilizzato il server proxy inverso Apache 2.2. Per configurare il server proxy inverso Apache 2.2 per OpenSearch:

1. Impostare il proxy inverso e apportare le modifiche nel file `WEB-INF\config.properties` di OpenSearch.
2. Abilitare i seguenti parametri di contesto e modificare i valori di conseguenza.
  - `proxy.rpurl`: URL del proxy inverso per OpenSearch, ad esempio `http://machineIPAddress/RP/OpenSearch/`.
  - `proxy.opendoc.rpurl`: URL del proxy inverso per Open Doc, ad esempio `http://machineIPAddress/RP/BOE/`.
3. Aggiornare il file `httpd.conf`, presente nella cartella di installazione del proxy inverso Apache, con le impostazioni seguenti:
  - `ProxyPass /RP/BOE/OpenDocument/ http://<Host Tomcat>:<Porta connettore>/BOE/OpenDocument/`
  - `ProxyPass /RP/OpenSearchRP/ http://<Host Tomcat>:<Porta connettore>/OpenSearch/`
  - `ProxyPassReverseCookiePath /BOE /RP/BOE`
  - `ProxyPassReverseCookiePath /OpenSearchRP /RP/OpenSearchRP`
4. Riavviare il server proxy inverso Apache 2.2.

### 22.2.3 Configurazione delle proprietà dell'applicazione nella CMC

Per configurare le proprietà dell'applicazione Ricerca piattaforma, attenersi alla procedura seguente:

1. Accedere all'area "Applicazioni" della console CMC.
2. Selezionare **Applicazione di ricerca piattaforma**.
3. Fare clic su **Gestisci > Proprietà**. Viene visualizzata la finestra di dialogo "Proprietà".
4. Configurare le impostazioni di Ricerca piattaforma:

| Opzione                                        | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Statistiche della ricerca                      | <p>L'applicazione di ricerca piattaforma fornisce le seguenti statistiche della ricerca:</p> <ul style="list-style-type: none"> <li>• Stato indicizzazione: visualizza lo stato del processo di indicizzazione.</li> <li>• Numero di documenti indicizzati: visualizza il numero di documenti indicizzati.</li> <li>• Ultima indicazione data e ora: visualizza la data e l'ora in cui è stata eseguita l'ultima indicizzazione del documento.</li> </ul> |
| Interrompi / Avvia indicizzazione              | <p>Le opzioni Avvia indicizzazione e Interrompi indicizzazione consentono di avviare o arrestare il processo di indicizzazione quando si desidera passare dalla ricerca per indicizzazione continua alla ricerca per indicizzazione pianificata o a scopo di manutenzione.</p> <p>Per interrompere l'indicizzazione, fare clic su <b>Interrompi indicizzazione</b>.</p>                                                                                   |
| Impostazioni internazionali indice predefinite | <p>Ricerca piattaforma si serve delle impostazioni locali specificate nella CMC per indicizzare tutti i documenti BI non localizzati. Una volta localizzato un documento, viene utilizzato l'Analyzer della lingua corrispondente per l'indicizzazione.</p> <p>La ricerca si basa sulle impostazioni locali del prodotto del client che vengono configurate nelle proprietà di configurazione della CMC.</p>                                              |

| Opzione                                 | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Frequenza di ricerca per indicizzazione | <p>È possibile indicizzare l'intero repository della piattaforma BI utilizzando le seguenti opzioni:</p> <ul style="list-style-type: none"> <li>• Ricerca per indicizzazione continua: questa opzione implica un'indicizzazione continua, ovvero il repository viene indicizzato ogni volta che si aggiunge, si modifica o si elimina un oggetto. Consente di visualizzare o utilizzare i contenuti della piattaforma BI più aggiornati. La ricerca per indicizzazione continua costituisce l'impostazione predefinita e aggiorna in modo continuativo il repository in base alle azioni eseguite. La ricerca per indicizzazione continua agisce senza intervento dell'utente e riduce il tempo richiesto per l'indicizzazione di un documento.</li> <li>• Ricerca per indicizzazione pianificata: con questa opzione l'indicizzazione avviene in base alla pianificazione impostata tramite le opzioni specifiche.</li> </ul> <p>Per ulteriori informazioni sulla pianificazione di un oggetto, consultare la sezione <i>Pianificazione di un oggetto</i> di Ricerca piattaforma nella <i>Guida in linea CMC della piattaforma SAP BusinessObjects Business Intelligence</i>.</p> <p><b>Nota:</b></p> <ul style="list-style-type: none"> <li>• Se si seleziona <b>Ricerca per indicizzazione pianificata</b> e si imposta la <b>Ricorrenza</b> su un'opzione diversa da <b>Ora</b>, Ricerca piattaforma visualizza la data e l'ora in cui è pianificata l'indicizzazione successiva del documento.</li> <li>• Se si seleziona <b>Ricerca per indicizzazione pianificata</b>, il pulsante <b>Avvia indicizzazione</b> viene abilitato mentre il pulsante <b>Interrompi indicizzazione</b> viene disabilitato.</li> <li>• Al termine della pianificazione, il pulsante <b>Interrompi indicizzazione</b> viene disabilitato.</li> </ul> |

| Opzione          | Descrizione |
|------------------|-------------|
| Posizione indice |             |

| Opzione | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | <p>Gli indici vengono archiviati in cartelle condivise nelle posizioni seguenti:</p> <ul style="list-style-type: none"> <li>• Posizione indice principale (indici, correttori ortografici): gli indici principali e correttore ortografico archiviati in questa posizione. Durante una ricerca, i risultati iniziali vengono recuperati mediante l'indice principale, mentre per recuperare i suggerimenti vengono utilizzati gli indici correttore ortografico. In una distribuzione della piattaforma BI in cluster questa posizione dovrebbe corrispondere al file system condiviso accessibile da tutti i nodi del cluster.</li> <li>• Posizione dati persistenti (archivi contenuti): in questa posizione si trova l'archivio contenuti. Viene creata dalla posizione dell'indice principale con cui rimane sincronizzata. L'archivio contenuti viene utilizzato per generare facet ed elabora i riscontri iniziali generati da Posizione indice principale. In una distribuzione della piattaforma BI in cluster, gli archivi di contenuti vengono generati in corrispondenza di ciascun nodo.</li> </ul> <p>La posizione dei dati persistenti è l'unica posizione di indice interessata dall'ambiente cluster, poiché contiene le cartelle degli archivi contenuti. Se un computer utilizza un solo servizio di ricerca, esisterà solo una posizione dell'archivio contenuti. Ad esempio, {bobj.enterprise.home}\data\PlatformSearchData\workspace\&lt;Nome server&gt;\ContentStores.</p> <p>Tuttavia, in un ambiente cluster, se sono presenti più servizi di ricerca, ognuno di essi avrà una sola posizione dell'archivio contenuti. Se ad esempio sono in esecuzione due istanze di un server, le posizioni dell'archivio contenuti saranno le seguenti:</p> <ol style="list-style-type: none"> <li>a. {bobj.enterprise.home}\data\PlatformSearchData\workspace\&lt;Nome server&gt;\ContentStores.</li> <li>b. {bobj.enterprise.home}\data\PlatformSearchData\workspace\&lt;Nome server 1&gt;\ContentStores.</li> </ol> <ul style="list-style-type: none"> <li>• Posizione dati non persistenti (file surrogati temporanei, DeltaIndexes): in questa posizione gli indici delta vengono creati e archiviati temporaneamente prima di essere uniti all'indice principale. Una volta uniti all'indice principale, gli indici vengono eliminati da questa posizione. Inoltre in questa posizione vengono creati e archiviati temporaneamente i file surrogati (output degli estrattori) fino a quando non vengono convertiti in indici delta.</li> </ul> <p><b>Nota:</b></p> <ul style="list-style-type: none"> <li>• Tutte le posizioni degli indici devono essere percorsi condivisi.</li> <li>• È necessario fare clic su <b>Interrompi indicizzazione</b> per modificare la posizione dell'indice.</li> <li>• Se si modifica la posizione di un indice, copiare il contenuto in una nuova posizione. In caso contrario, le informazioni relative all'indice</li> </ul> |



| Opzione                   | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           | esistente verranno perdute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Livello di indicizzazione | <p>È possibile regolare il contenuto della ricerca impostando il livello di indicizzazione nei seguenti modi:</p> <ul style="list-style-type: none"> <li>• Metadati piattaforma: viene creato un indice solo per le informazioni sui metadati della piattaforma, ad esempio titoli, parole chiave e descrizioni dei documenti.</li> <li>• Metadati piattaforma e documento: questo indice include i metadati della piattaforma e del documento. I metadati del documento includono la data di creazione, la data di modifica e il nome dell'autore.</li> <li>• Contenuto completo: questo indice include i metadati della piattaforma, i metadati del documento e altri contenuti quali: <ul style="list-style-type: none"> <li>• il contenuto effettivo del documento</li> <li>• il contenuto dei prompt e degli elenchi di valori</li> <li>• grafici ed etichette</li> </ul> </li> </ul> <p><b>Nota:</b><br/>quando si modifica il livello di indicizzazione, l'indicizzazione viene reinitializzata per l'intero repository della piattaforma BI.</p> |
| Tipi contenuto            | <p>È possibile selezionare i seguenti tipi di contenuto per l'indicizzazione:</p> <ul style="list-style-type: none"> <li>• Crystal Reports</li> <li>• Web Intelligence</li> <li>• Universo</li> <li>• Spazio di lavoro BI</li> <li>• Microsoft PowerPoint</li> <li>• Adobe Acrobat</li> <li>• Rich Text</li> <li>• Testo</li> <li>• Microsoft Word</li> <li>• Microsoft Excel</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Opzione                               | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rigenera indice                       | <p>Questa opzione elimina l'indice esistente e reindicizza l'intero repository.</p> <p>È possibile selezionare l'opzione <b>Rigenera indice</b> indipendentemente dal fatto che l'indicizzazione sia in esecuzione o sia stata interrotta. L'indice esistente viene eliminato quando si salvano le modifiche alla pagina delle proprietà. Se invece l'indicizzazione è attualmente interrotta, la rigenerazione dell'indice non ha inizio fino a quando non viene riavviata l'indicizzazione.</p> <p>Se non si desidera che Ricerca piattaforma indicizzi nuovamente i documenti, deselezionare l'opzione <b>Rigenera indice</b> prima di fare clic su <b>Avvia indicizzazione</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Documenti esclusi dall'indicizzazione | <p>L'opzione <b>Documenti esclusi dall'indicizzazione</b> consente di escludere documenti dall'indicizzazione. Ad esempio, può essere opportuno escludere dalla ricerca i report Crystal di dimensioni molto elevate per evitare eccessivi carichi di lavoro delle risorse del Report Application Server. Analogamente, è possibile evitare che le pubblicazioni con centinaia di report personalizzati vengano indicizzate.</p> <p>Escludendo documenti specifici, è possibile evitare che vengano aperti in Ricerca piattaforma. È importante notare che, se un documento è stato indicizzato prima di essere inserito in questo gruppo, potrebbe ancora essere accessibile per le ricerche. Per essere sicuri che i documenti del gruppo <b>Documenti esclusi dall'indicizzazione</b> non siano accessibili, è necessario generare nuovamente l'indice.</p> <p>Per impostazione predefinita, solo l'account Administrator ha il controllo completo dell'opzione <b>Documenti esclusi dall'indicizzazione</b>. Gli altri utenti con i diritti seguenti possono solo aggiungere documenti al gruppo <b>Documenti esclusi dall'indicizzazione</b>:</p> <ul style="list-style-type: none"> <li>• Diritti di visualizzazione e modifica per la categoria</li> <li>• Modifica diretta del documento</li> </ul> |

##### 5. Fare clic su **Salva e chiudi**.

##### **Nota:**

Se un utente non seleziona l'opzione **Rigenera indice** e cambia il livello di indicizzazione oppure seleziona o deseleziona gli estrattori, l'indice viene aggiornato in modo incrementale senza che venga eliminato l'indice esistente.

## 22.3 Utilizzo della ricerca piattaforma

### 22.3.1 Indicizzazione del contenuto nel repository CMS

L'indicizzazione è un processo continuo che comprende le seguenti attività sequenziali:

1. Ricerca per indicizzazione: la ricerca per indicizzazione è un meccanismo che consente il polling del repository CMS e l'identificazione di oggetti pubblicati, modificati o eliminati. Può essere eseguita in due modalità: continua e pianificata.

Per ulteriori informazioni sulla ricerca per indicizzazione continua e pianificata, consultare l'argomento *Configurazione delle proprietà delle applicazioni* negli Argomenti correlati.

2. Estrazione: meccanismo che richiama gli esperti in base al tipo di documento. Esiste un esperto dedicato per ciascun tipo di documento disponibile nel repository: I nuovi tipi di documento possono essere resi ricercabili definendo nuovi plug-in per l'esperto. Ciascun esperto ha un grado di scalabilità sufficiente a estrarre contenuti da documenti di grandi dimensioni che comprendono molti record.

Sono supportati i seguenti esperti:

- Esperto metadati
- Esperto di Crystal Reports
- Esperto Web Intelligence
- Esperto Universo
- Esperti generali (MS Office 2003 e 2007 e documenti pdf)

Per ulteriori informazioni sui tipi di documenti in cui è possibile eseguire ricerche, consultare l'argomento *Tipi di contenuto in cui è possibile eseguire ricerche* negli Argomenti correlati.

3. Indicizzazione: è un meccanismo che indicizza tutti i contenuti estratti mediante una libreria di terze parti, denominata Apache Lucene Engine. Il tempo necessario per l'indicizzazione varia in base al numero di oggetti nel sistema, nonché alle dimensioni e al tipo dei documenti.

Per eseguire correttamente l'indicizzazione, i server seguenti devono essere in esecuzione e abilitati:

- Input File Repository Server (IFRS)
- Output File Repository Server (OFRS)
- Central Management Server (CMS)
- L'Adaptive Processing Server (APS) che ospita il servizio di ricerca piattaforma

Se il tipo di oggetto viene selezionato come report di Web Intelligence o Crystal Reports, è necessario che il server Web Intelligence Processing Server o Crystal Reports Application Server corrispondente sia abilitato e in esecuzione per i rispettivi tipi di oggetto selezionati.

4. Archivio contenuti: l'archivio contenuti contiene informazioni quali ID, CUID, nome, tipo e istanza, estratte dall'indice master in un formato di facile lettura. Contente di velocizzare il processo di ricerca.

**Argomenti correlati**

- [Configurazione delle proprietà dell'applicazione nella CMC](#)
- [Tipi di contenuto in cui è possibile eseguire ricerche](#)

## 22.3.2 Elenco errori di indicizzazione

L'elenco degli errori di indicizzazione è un elenco di documenti in cui si è verificato un errore durante l'indicizzazione. Ricerca piattaforma offre tre tentativi di indicizzazione per un documento. I documenti di cui non viene completata l'indicizzazione vengono inseriti nell'elenco degli errori di indicizzazione.

Per visualizzare l'elenco degli errori di indicizzazione, attenersi alla seguente procedura:

1. Accedere all'area "Applicazioni" della console CMC.
2. Selezionare **Applicazione di ricerca piattaforma**.
3. Scegliere **Azioni > Elenco errori di indicizzazione**.

Viene visualizzata la finestra di dialogo "Applicazione di ricerca piattaforma" contenente un elenco di documenti con i seguenti dettagli:

- Titolo: visualizza il titolo del documento in cui si è verificato un errore durante l'indicizzazione.
- Tipo: visualizza il nome del tipo di documento, ad esempio Crystal Report e Web Intelligence, insieme alla posizione.
- Tipo di errore: visualizza il codice di errore e il motivo dell'errore di indicizzazione del documento. Fare clic sul collegamento ipertestuale Ulteriori informazioni per ottenere altre informazioni sull'analisi dello stack della causa dell'errore.
- Ora ultimo tentativo: visualizza l'indicatore data e ora dell'ultimo tentativo di indicizzazione di un documento.

## 22.3.3 Risultati della ricerca

### 22.3.3.1 Pre-ricerca

#### 22.3.3.1.1 Query suggerite

Quando utilizza l'applicazione Ricerca piattaforma, un utente può tentare di trovare le risposte a una domanda specifica anziché cercare un oggetto specifico. Le risposte alle domande possono essere presenti o meno nei report disponibili nel repository della piattaforma BI.

Ricerca piattaforma analizza la struttura degli universi e dei report esistenti nel repository e confronta queste informazioni con la richiesta di ricerca fornita dall'utente per suggerire nuove query di SAP BusinessObjects Web Intelligence che potrebbero aiutare gli utenti a trovare le risposte alle loro domande.

Per creare report potenziali, Ricerca piattaforma trova la corrispondenza delle parole in tutti gli universi con i valori di dimensione, indicatore, condizione e filtro.

Ricerca piattaforma cerca le corrispondenze nelle seguenti informazioni sugli universi o nei documenti esistenti di Web Intelligence.

- Indicatori negli universi che corrispondono alle parole immesse per la ricerca.

Quando un indicatore corrisponde a uno dei termini di ricerca, tale indicatore verrà utilizzato nel documento Web intelligence risultante.

- Nomi di dimensioni negli universi che corrispondono a parole nell'input di ricerca.

Quando il nome di una dimensione corrisponde a uno dei termini di ricerca, il documento Web Intelligence risultante scompone le informazioni in questa dimensione.

- Il filtri di query possono essere utilizzati per concentrarsi sui dati nel documento. Tali filtri vengono generati analizzando l'input della ricerca.
  - Se il nome di una condizione di universo corrisponde a uno dei termini di ricerca, la condizione viene utilizzata come filtro.
  - Se i nomi dei valori di campo presenti in documenti Web Intelligence esistenti corrispondono ai termini di ricerca, verrà creato un filtro dalla dimensione del report cronologico con il valore con corrispondenza, utilizzando "uguale a" come operatore di condizione.

Se Ricerca piattaforma rileva un numero di corrispondenze tale che il documento risultante conterrà due campi di risultati e un filtro, la query verrà considerata pronta per essere eseguita. In questo caso, l'utente può fare clic per visualizzare il report completato.

Se non è stato trovato un numero sufficiente di corrispondenze tra gli universi e il documento, è possibile modificare la query prima di eseguirla.

Ricerca piattaforma suggerisce più query se più universi corrispondono all'input di ricerca o se la stessa parola viene visualizzata in due diverse corrispondenze, ad esempio nel nome di una dimensione e come valore filtro.

#### 22.3.3.1.2 Tipi di contenuto in cui è possibile eseguire ricerche

È possibile effettuare ricerche nel contenuto pubblicato nella piattaforma BI mediante Ricerca piattaforma. Di seguito sono elencati i tipi di oggetto con il contenuto indicizzato corrispondente:

| Tipo di oggetto                                                                                                                                                                                                                    | Contenuto indicizzato                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Crystal Reports (2008 e 2011)                                                                                                                                                                                                      | Titolo, descrizione, formula di selezione, dati salvati, campi di testo in ogni sezione, valori dei parametri e sottoreport.                                                                                                                                                                                                                                                                                                                          |
| Documenti Web Intelligence                                                                                                                                                                                                         | Titolo, descrizione, nome dei filtri dell'universo utilizzati nel report, dati salvati, costanti della condizione di filtro definita in locale nel report, nome degli indicatori dell'universo utilizzati nel report, nome degli oggetti dell'universo utilizzati nel report, dati dell'insieme di record e testo statico nelle celle.                                                                                                                |
| Documenti Microsoft Excel (2003 e 2007)                                                                                                                                                                                            | <p>Dati in tutte le celle non vuote, campi nella pagina di riepilogo delle proprietà del documento (titolo, oggetto, autore, azienda, categoria, parole chiave e commenti) e testo nelle intestazioni e nei piè di pagina del documento.</p> <p>Per le celle che utilizzano un calcolo o una formula, è possibile cercare il valore dopo la valutazione. Per valori numero o data/ora, i dati non elaborati possono essere sottoposti a ricerche.</p> |
| Documenti Microsoft Word (2003 e 2007)                                                                                                                                                                                             | Testo in tutti i paragrafi e in tutte le tabelle, campi nella Pagina di riepilogo delle proprietà del documento (titolo, oggetto, autore, azienda, categoria, parole chiave e commenti), testo nelle intestazioni e nei piè di pagina del documento e testo numerico.                                                                                                                                                                                 |
| File RTF, PDF, PPT e TXT                                                                                                                                                                                                           | È possibile effettuare ricerche in tutto il testo contenuto in questi file.                                                                                                                                                                                                                                                                                                                                                                           |
| LCMJob, AFDashboard Page, Dashboards, ObjectPackage, Web service query (QaaWS), Profile, Discussions, InformationDesigner, widget per la piattaforma SAP BusinessObjects BI, MDAnalysis, Publications, Flash, Analytic e Hyperlink | È possibile effettuare ricerche nel contenuto dei metadati.                                                                                                                                                                                                                                                                                                                                                                                           |

| Tipo di oggetto     | Contenuto indicizzato                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Eventi              | <p>È possibile effettuare ricerche per tutti gli eventi, quali gli eventi personalizzati, di sistema, Crystal Reports e di monitoraggio. Se un evento è associato a un'origine, Ricerca piattaforma visualizza l'origine insieme all'evento.</p> <p><b>Nota:</b><br/>Ricerca piattaforma supporta eventi per Crystal Reports for Enterprise.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Spazio di lavoro BI | <ul style="list-style-type: none"> <li>• Vengono indicizzati il titolo, la descrizione e il contenuto dei moduli BIW seguenti: <ul style="list-style-type: none"> <li>• Modulo di testo</li> <li>• Modulo pagina Web</li> <li>• Modulo Elenco navigazione</li> <li>• Modulo Visualizzatore</li> </ul> </li> <li>• Vengono indicizzati il titolo e la descrizione di un modulo composito.</li> <li>• Viene indicizzato solo il titolo di un modulo di modello Spazio di lavoro.</li> <li>• Nel caso di un modulo Gruppo, vengono indicizzati il titolo e i metadati dei moduli al suo interno.</li> <li>• Vengono indicizzati il titolo, la descrizione e il CUID dei moduli InfoObject in BIW.</li> </ul> <p><b>Nota:</b><br/>poiché vengono indicizzati solo il titolo e la descrizione di un modulo InfoObject incorporato, i tentativi di ricerca nel contenuto InfoObject non restituiranno riferimenti al modulo incorporato. Se, ad esempio, si inserisce un CR in BIW, ne vengono indicizzati il titolo e la descrizione. Qualsiasi tentativo di ricerca nel contenuto del CR non restituirà riferimenti al modulo incorporato.</p> <ul style="list-style-type: none"> <li>• Se un BIW contiene più schede e schede secondarie, vengono indicizzati anche il titolo e il contenuto di ogni scheda e scheda secondaria.</li> </ul> |

| Tipo di oggetto         | Contenuto indicizzato                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CR con formato Next Gen | <p>Titolo, descrizione, formula di selezione, dati salvati, campi di testo in ogni sezione, valori dei parametri e sottoreport.</p> <p>In un report CR Next Gen non sono supportati gli oggetti seguenti:</p> <ul style="list-style-type: none"> <li>• Report a campi incrociati</li> <li>• Estrazione dati grafico</li> <li>• Estrazione immagini e metadati associati</li> <li>• OLE incorporato, ad esempio un documento Word incorporato in CR</li> <li>• Estrazione oggetti Flash</li> </ul> <p>Inoltre, non è consentita la lettura pagina per pagina di un report CR Next Gen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Universo                | <p>È possibile effettuare ricerche nel contenuto dei dati.</p> <p><b>Nota:</b></p> <p>Per impostazione predefinita, l'opzione di indicizzazione dell'universo è abilitata. Se si nota che l'esecuzione delle query utilizzate da Ricerca piattaforma per indicizzare il contenuto dell'universo richiede molto tempo e influisce sulle prestazioni del server di database, si consiglia di disabilitare l'opzione di indicizzazione dell'universo nella console CMC (Central Management Console). Un esempio di query utilizzata da Ricerca piattaforma durante l'indicizzazione del contenuto dell'universo è <b>Select distinct SampleColumnName from SampleTableName LIMIT 1000</b>.</p> <p>Attenersi alla procedura seguente per disabilitare l'indicizzazione dell'universo:</p> <ol style="list-style-type: none"> <li>1. Accedere alla Central Management Console (CMC).</li> <li>2. Scegliere <b>Applicazioni</b>.</li> <li>3. Passare a Applicazione di ricerca piattaforma e scegliere <b>Proprietà</b>.</li> <li>4. Passare ai tipi di contenuto e deselezionare <b>Universo</b>.</li> <li>5. Scegliere <b>Salva e chiudi</b>.</li> </ol> |



**Nota:**

la dimensione massima supportata per i documenti generali (documenti MS Office 2003 e 2007 e PDF) è 15 MB.

### **22.3.3.2 Cerca**

Quando un utente cerca una parola chiave da BI Launch Pad o da un'altra applicazione che utilizza l'SDK di Ricerca piattaforma, è l'indice master a essere verificato in base ai termini della ricerca. In base ai diritti di visualizzazione dell'utente, il motore di ricerca visualizza solo i documenti per i quali l'utente dispone di diritti di accesso.

### **22.3.3.3 Post-ricerca**

#### **22.3.3.3.1 Facet**

Ricerca piattaforma affina i risultati della ricerca raggruppandoli in categorie o facet di tipi di oggetti simili e classificandoli per il numero di occorrenze della categoria tra i risultati restituiti per un termine di ricerca. I facet consentono di spostarsi fino ad arrivare al risultato esatto.

Ricerca piattaforma genera facet da metadati di InfoObject, metadati di documenti e contenuto di documenti. Visualizza solo i facet per i quali vi sono più di due documenti corrispondenti a una query specificata. I facet vengono visualizzati dinamicamente in base ai documenti che corrispondono alla query di ricerca e vengono ordinati in base al conteggio dei documenti.

I documenti vengono raggruppati nei facet o nelle categorie generiche elencate di seguito:

- Personale o pubblico (ad esempio HR, Aziendale e Finanziario): basato sulle categorie di documenti della piattaforma BI.
- Tipo di documento: in base al tipo di documento, ad esempio Web Intelligence, Crystal Reports, Microsoft Word (2003 e 2007), Microsoft Excel (2003 e 2007) e Dashboards.
- Universo e Connessioni: basato sull'origine del contenuto.
- Data: include la data dell'ultimo aggiornamento: (anno, trimestre e mese).
- Ora: include l'ora dell'ultimo aggiornamento (ad esempio, ultime 24 ore e ultima settimana).
- Autore: nome dell'utente che ha creato il documento.

#### **22.3.3.3.2 Normalizzazione della classificazione dei risultati della ricerca**

Il servizio di ricerca piattaforma tiene in considerazione il punto in cui compare il termine ricercato quando viene classificato un documento. Raggruppa il contenuto nelle seguenti categorie sulla base delle relative occorrenze nel documento:

1. Metadati piattaforma
2. Metadati documento
3. Metadati contenuto
4. Contenuto

Il peso per le suddette categorie può essere configurato nella CMC.

#### *Personalizzazione del peso per la classificazione dei risultati della ricerca*

Il servizio di ricerca piattaforma consente di impostare pesi per il contenuto raggruppato in categorie sulla base delle occorrenze dello stesso nel documento, in modo che sia possibile impostare un valore più alto per la categoria desiderata, per recuperare più velocemente i risultati della ricerca correlati.

Per impostare il peso, utilizzare la seguente procedura:

1. Nell'area "Gestisci" della CMC fare clic su **Applicazioni**.
2. Aprire **Applicazione di ricerca piattaforma**.
3. Scegliere **Classifica**.

Verranno visualizzati i pesi delle diverse categorie di contenuto, ad esempio Metadati piattaforma, Metadati documento, Metadati contenuto e Contenuto. Le "Impostazioni internazionali utente" sono le impostazioni internazionali configurate nelle Preferenze di BI Launch Pad.

4. Impostare i pesi in base alle proprie esigenze.
5. Scegliere **Salva**.

In uno scenario di aggiornamento, se si applica una classificazione a documenti già indicizzati, sarà necessario rigenerare l'indice. Per ulteriori informazioni, fare riferimento alle informazioni sulla rigenerazione dell'indice nella sezione [Configurazione delle proprietà dell'applicazione nella CMC](#).

#### **22.3.3.3.3 Supporto multilingue**

Ricerca piattaforma offre il supporto multilingua per l'indicizzazione del contenuto, il recupero dei risultati delle ricerche e la visualizzazione di suggerimenti nella lingua preferita. Per indicizzare tutti i documenti non localizzati della piattaforma BI, utilizza le impostazioni internazionali configurate nelle **Impostazioni internazionali indice predefinite** nella CMC.

Una volta localizzato l'InfoObject, il servizio utilizza l'analizzatore di lingue corrispondente per indicizzare il documento.

La ricerca si basa sulle impostazioni internazionali configurate in Impostazioni internazionali prodotto nel client. Il servizio di ricerca piattaforma assegna più peso alle impostazioni internazionali del prodotto client durante il recupero dei risultati della ricerca. I pesi possono essere configurati nella CMC.

#### **22.3.3.3.4 Suggerimenti**

Ricerca piattaforma offre suggerimenti per le query di ricerca digitate in modo non corretto. Se la query di ricerca originale non restituisce alcun risultato, Ricerca piattaforma suggerisce i termini che risultano più appropriati in base al contenuto indicizzato.

I suggerimenti vengono visualizzati come parole chiave con collegamento ipertestuale. Fare clic su un collegamento ipertestuale per visualizzare un elenco di documenti contenenti la parola chiave che potrebbe corrispondere alla query originale. I suggerimenti vengono determinati algebricamente in base a vari fattori oggettivi.

Nel caso in cui vi siano più termini che possono corrispondere alla richiesta originale, Ricerca piattaforma indica i primi tre suggerimenti nella lingua impostata in **Impostazioni internazionali indice predefinite** nella CMC.

**Nota:**

Ricerca piattaforma non genera suggerimenti in questi casi:

- se le query di ricerca contengono meno di tre lettere
- per le ricerche con attributi, ad esempio Tipo: Crystal Reports
- per contenuto e metadati di universi
- per le lingue a più byte quali cinese, giapponese e coreano

#### 22.3.3.3.5 Raggruppamento dei risultati della ricerca di SAP BusinessObjects Explorer

In Ricerca piattaforma viene eseguito il raggruppamento delle richieste di ricerca SAP BusinessObjects Explorer e vengono visualizzati gli Infospace insieme al contenuto della piattaforma BI.

I risultati della ricerca di SAP BusinessObjects Explorer vengono raggruppati in base alle categorie di metadati. Tra i facet supportati per gli infospace figurano il tipo, la posizione e l'ora di aggiornamento.

SAP BusinessObjects Explorer invia la frequenza del termine a Ricerca piattaforma per ogni termine di ricerca della query di ricerca. Ricerca piattaforma calcola la rilevanza utilizzando la somma della radice quadrata delle frequenze dei termini. Il valore risultante viene assegnato come punteggio a ogni infospace. I risultati vengono quindi ordinati in base al punteggio e inviati al client.

## 22.4 Integrazione del servizio di ricerca piattaforma con la funzionalità di ricerca di SAP NetWeaver Enterprise

La funzionalità di ricerca di SAP NetWeaver Enterprise 7.20 e versioni successive può utilizzare un servizio di ricerca basato su OpenSearch (RSS e ATOM). Questa funzionalità può delegare le richieste di ricerca ai sistemi di provider dei servizi di ricerca in remoto. In questo caso, OpenSearch è il provider dei servizi, la funzionalità di ricerca di NetWeaver Enterprise è il consumer dei risultati della ricerca e Ricerca piattaforma di SAP BusinessObjects è il provider dei servizi di ricerca.

Se un utente invia una richiesta di ricerca, la funzionalità di ricerca di SAP NetWeaver Enterprise inoltra tale richiesta direttamente al provider OpenSearch. Il provider risponde alla richiesta di ricerca e invia la risposta alla funzionalità di ricerca di SAP NetWeaver Enterprise. Questa viene unita, insieme ai risultati ricevuti da altri connettori oggetto di ricerca, a un risultato della ricerca e visualizzata in un'interfaccia utente.

Per integrare il servizio di ricerca di SAP NetWeaver Enterprise e Ricerca piattaforma, è necessari attenersi alla procedura seguente:

1. Creare un connettore nella funzionalità di ricerca di SAP NetWeaver Enterprise.
2. Importazione del ruolo di un utente nella piattaforma BI.

### 22.4.1 Creazione di un connettore nella funzionalità di ricerca di SAP NetWeaver Enterprise

È possibile utilizzare un connettore oggetto di ricerca di tipo OpenSearch per integrare i provider di ricerca esterni che offrono una funzione di ricerca disponibile mediante OpenSearch.

Per creare un connettore nella funzionalità di ricerca di SAP NetWeaver Enterprise, sono necessari i prerequisiti seguenti:

1. L'URL del servizio di descrizione OpenSearch.
2. Il servizio di descrizione OpenSearch deve essere disponibile esclusivamente in formato RSS o ATOM.

Per creare un connettore nella funzionalità di ricerca di SAP NetWeaver Enterprise, attenersi alla procedura riportata di seguito:

1. Avviare il pannello di controllo di amministrazione e scegliere Crea.
2. Selezionare OpenSearch come tipo di connettore dell'oggetto di ricerca.
3. Scegliere **Next**.
4. Specificare l'URL del servizio di descrizione OpenSearch del provider OpenSearch.
5. Selezionare una delle impostazioni di autenticazione seguenti per avviare l'URL del servizio di descrizione:
  - No Authentication: non viene effettuata alcuna autenticazione.
  - SAP Authentication Assertion Ticket: questo utente viene utilizzato per l'autenticazione mediante SSO.
  - User/Password: per l'autenticazione viene utilizzato un utente predefinito.
6. Selezionare l'URL di ricerca nelle impostazioni relative agli URL OpenSearch.  
Il servizio di descrizione OpenSearch viene convalidato. Viene immesso automaticamente un valore per il modello dell'URL di ricerca con la descrizione associata.
7. Selezionare una delle impostazioni di autenticazione seguenti per configurare un connettore:
  - No authentication: non viene effettuata alcuna autenticazione.
  - SAP Authentication Assertion Ticket: questo utente viene utilizzato per l'autenticazione mediante SSO.
  - User/Password: per l'autenticazione viene utilizzato un utente predefinito.
8. Scegliere **Next**.  
Viene visualizzata una finestra di dialogo di riepilogo con i valori immessi per questo connettore oggetto di ricerca.
9. Scegliere **Precedente** per modificare le impostazioni oppure **Annulla** per annullare i dati immessi.
10. Scegliere **Fine** per salvare le impostazioni.

## 22.4.2 Importazione del ruolo di un utente nella piattaforma BI

Per importare il ruolo di un utente nella piattaforma BI, attenersi alla procedura riportata di seguito:

**Nota:**

È necessario che l'amministratore disponga di dettagli relativi all'utente, informazioni di sistema, credenziali utente e informazioni relative all'host applicazione.

1. Accedere all'area "Autenticazione" della console CMC.
2. Scegliere **SAP**.
3. Specificare le informazioni seguenti nella scheda "Sistemi di autorizzazione":
  - Sistema
  - Client
  - Server di applicazioni
  - Numero di sistema
  - Nome utente
  - Password
  - Lingua
4. Scegliere **Aggiorna**.
5. Scegliere la scheda "Importazione ruolo" e importare ruoli utente.
6. Scegliere **Aggiorna**.
7. Scegliere **Gestisci > funzioni di protezione dell'utente** nella CMC per assegnare i diritti utente appropriati.

## 22.5 Ricerca dalla funzionalità di ricerca di NetWeaver Enterprise

Per cercare risultati dalla funzionalità di ricerca di SAP NetWeaver Enterprise, attenersi alla procedura seguente:

1. Accedere all'applicazione di ricerca SAP NetWeaver Enterprise.
2. Scegliere **Ricerca avanzata**.
3. Selezionare il connettore creato per Ricerca piattaforma.
4. Eseguire la ricerca di una parola chiave.

I risultati consolidati per la parola chiave contengono quelli derivanti da Ricerca piattaforma, nel caso in cui ci sia una corrispondenza con la parola chiave.

## 22.6 Controllo

Tutti gli eventi delle richieste di ricerca inviate da un'applicazione client che utilizzi il servizio Ricerca piattaforma e la risposta alla ricerca vengono controllati. Per Ricerca piattaforma, il controllo viene implementato al livello di servizio.

Per poter inviare eventi di controllo, è necessario eseguire il servizio di ricerca piattaforma con un Servizio proxy controllo client sullo stesso server.

Esistono un ID tipo di evento 1009 per Ricerca piattaforma e quattro ID tipo dettagli evento specifici di Ricerca piattaforma:

- Parola chiave cercata (ID: 19)
- Numero di risultati della ricerca (ID: 63)
- Ricerca facet (ID: 20)
- Eccezione di ricerca (ID: 1)

Tranne che per i dettagli evento descritti in precedenza, esistono alcuni dettagli evento standard come sessionCuid e userCuid supportati per qualsiasi tipo di controllo nei moduli della piattaforma BI.

Il funzionamento del controllo in Ricerca piattaforma viene spiegato di seguito con un esempio.

Se si esegue una ricerca con una parola chiave, ad esempio "Vendite", il numero totale di risultati della ricerca potrebbe essere 5: In questo caso, vengono controllati i seguenti eventi:

- ID tipo di evento 1009
- ID tipo dettagli evento 19 con valore vendite
- ID tipo dettagli evento 63 con valore 5
- Cuid sessione
- Cuid utente
- Stato con valore 0, che rappresenta lo stato riuscito
- Ora di inizio
- Durata
- ID oggetto con valore 0 poiché si tratta di un controllo del lato servizio

Quando vengono generati dei facet e se ne seleziona uno o più di uno, vengono controllati i seguenti eventi:

- ID tipo di evento 1009
- ID tipo dettagli evento 19 con valore vendite
- ID tipo dettagli evento 63 con valore 5
- ID tipo dettagli evento 20 con stringa di facet separata da virgola
- Cuid sessione
- Cuid utente
- Stato con valore 0, che rappresenta lo stato riuscito
- Ora di inizio
- Durata

- ID oggetto con valore 0 poiché si tratta di un controllo del lato servizio

Se si verifica un'eccezione di ricerca a causa di una voce non valida, ad esempio "\*"a", vengono controllati i seguenti dettagli evento:

- ID tipo di evento 1009
- ID tipo dettagli evento 19 con valore vendite
- ID tipo dettagli evento 63 con valore 0
- ID tipo dettagli evento 1 con messaggio di eccezione
- Cuid sessione
- Cuid utente
- Stato con valore 1, che rappresenta lo stato non riuscito
- Ora di inizio
- Durata
- ID oggetto con valore 0 poiché si tratta di un controllo del lato servizio

## **22.7 Risoluzione dei problemi**

### **22.7.1 Riparazione automatica**

Ricerca piattaforma dispone di un proprio meccanismo di riparazione automatica, che monitora continuamente l'utilizzo della memoria del servizio di ricerca e interrompe automaticamente l'indicizzazione quando l'utilizzo della memoria supera il valore di soglia. Viene avviato automaticamente quando il livello di utilizzo della memoria raggiunge un limite minimo ragionevole. Tuttavia, gli utenti possono continuare a effettuare la ricerca durante questo processo ma non possono eseguire indicizzazioni per un periodo di tempo specifico. Per impostazione predefinita, Ricerca piattaforma configura il numero di documenti che possono essere indicizzati in qualsiasi momento in base al tipo di documento. L'indicizzazione viene avviata in base a risorse di sistema come la CPU e la memoria.

### **22.7.2 Scenari di problemi**

In questa sezione vengono fornite soluzioni passo passo per un'ampia gamma di problemi che possono verificarsi durante il recupero dei risultati della ricerca con Ricerca piattaforma.

### **Impossibilità di recuperare i risultati della ricerca dal documento appena aggiunto contenente la parola chiave**

- Verificare se la Ricerca piattaforma supporta il tipo di documento del documento inviato. Se il tipo di documento non è supportato, l'indicizzazione del documento non riesce.

Per ulteriori informazioni sui tipi di documento supportati, fare riferimento all'argomento *Tipi di documento in cui è possibile eseguire ricerche* negli argomenti correlati elencati di seguito.

- Verificare l'opzione selezionata per **Frequenza di ricerca per indicizzazione**. Se l'opzione **Frequenza di ricerca per indicizzazione** è impostata su **Ricerca per indicizzazione continua**, i documenti vengono selezionati immediatamente per l'indicizzazione. Se l'opzione **Frequenza di ricerca per indicizzazione** è impostata su **Ricerca per indicizzazione pianificata**, l'indicizzazione viene eseguita solo durante il periodo pianificato.

Per ulteriori informazioni sull'opzione *Frequenza di ricerca per indicizzazione*, fare riferimento all'argomento *Configurazione delle proprietà delle applicazioni* negli argomenti correlati elencati di seguito.

- Verificare l'elenco degli errori di indicizzazione per verificare se il documento è stato indicizzato. Se il documento viene visualizzato in questo elenco, è necessario modificarlo e inviarlo nuovamente in modo da consentire a Ricerca piattaforma di utilizzarlo per l'indicizzazione.

#### **Nota:**

È possibile modificare il documento aggiungendo o eliminando un campo e quindi salvandolo nuovamente. In questo modo viene aggiornata l'indicazione di data e ora del documento nel repository della piattaforma BI e viene avviata la reindicizzazione del documento.

Per ulteriori informazioni sui documenti di cui non si riesce a eseguire l'indicizzazione, fare riferimento all'argomento *Elenco degli errori di indicizzazione* negli argomenti correlati riportati di seguito.

- Verificare i registri di analisi di Adaptive Processing Server contenenti le informazioni relative all'errore di indicizzazione.
  1. Passare alla directory `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\logging\` contenente il registro di analisi APS con estensione .glf.
  2. Aprire il file del registro di analisi e cercare il SI\_ID del documento che deve essere indicizzato.

#### **Nota:**

Il SI\_ID del documento si trova nelle proprietà del documento.

### **Impossibile recuperare documenti Crystal Reports**

Ricerca piattaforma indicizza il contenuto Crystal Reports solo per le versioni 2008 e 2011. Non indicizza il contenuto per Crystal Reports for Enterprise.

Nel caso di Crystal Reports for Enterprise è tuttavia possibile cercare metadati documento, quali titolo, descrizione e parola chiave, che rappresentano proprietà del documento.

Se il documento include contenuto indicizzabile, è necessario seguire la stessa procedura elencata nella sezione sopra indicata *Impossibilità di recuperare i risultati della ricerca dal documento appena aggiunto contenente la parola chiave*.



**Impossibile recuperare infospace SAP BusinessObjects Explorer**

Controllare i server di SAP BusinessObjects Explorer per verificare se sono spenti o disattivati. Abilitare i server per consentire a Ricerca piattaforma di recuperare i risultati della ricerca dal repository SAP BusinessObjects Explorer.

**La funzionalità di ricerca di SAP NetWeaver Enterprise non consente di recuperare i risultati dal repository della piattaforma BI**

- Controllare Ricerca piattaforma per verificare se recupera i risultati della ricerca utilizzando BI Launch Pad allo scopo di stabilire se il problema è dovuto all'integrazione di Ricerca piattaforma con la funzionalità di ricerca di SAP NetWeaver Enterprise.
- Verificare che OpenSearch sia distribuito correttamente nel server di applicazioni Web. I passaggi specifici per la convalida della distribuzione di OpenSearch dipendono dal tipo di server di applicazioni Web in uso.
- Verificare che il connettore venga creato o configurato correttamente nella configurazione della funzionalità di ricerca di SAP NetWeaver Enterprise. È necessario utilizzare il connettore corretto per la funzionalità di ricerca di SAP NetWeaver Enterprise per eseguire la federazione dei risultati da Ricerca piattaforma.
- Verificare che la comunicazione tra i computer su cui sono in esecuzione rispettivamente la funzionalità di ricerca di SAP NetWeaver Enterprise e la piattaforma BI funzioni correttamente. In caso di problemi di rete in un ambiente distribuito, è possibile che la funzionalità di ricerca di SAP NetWeaver Enterprise non riesca a eseguire la federazione dei risultati.
- Verificare che gli utenti della funzionalità di ricerca di SAP NetWeaver Enterprise vengano aggiunti alla piattaforma BI con i diritti appropriati. Per convalidare i diritti degli utenti, accedere all'area **Autenticazione** della CMC e selezionare **SAP**.

**Argomenti correlati**

- [Elenco errori di indicizzazione](#)
- [Configurazione delle proprietà dell'applicazione nella CMC](#)
- [Tipi di contenuto in cui è possibile eseguire ricerche](#)



# Federazione

## 23.1 Federation

Federation è uno strumento di replica tra siti per l'utilizzo di più distribuzioni della piattaforma BI in un ambiente globale.

È possibile creare e gestire contenuto da una distribuzione della piattaforma BI e replicarlo in altre distribuzioni della piattaforma BI tra siti geografici in base a una pianificazione ricorrente. Gli utenti possono completare i processi di replica unilaterale e replica bilaterale.

Grazie a Federation gli utenti possono:

- Ridurre il traffico di rete
- Creare e gestire il contenuto da un'unica posizione
- Migliorare le prestazioni per gli utenti finali

Quando si replicano contenuti mediante Federation è possibile:

- Semplificare le esigenze di amministrazione per più distribuzioni
- Fornire criteri coerenti relativi ai diritti tra più uffici per organizzazioni globali
- Ottenere informazioni in modo più rapido ed elaborare i report presso i siti remoti dove risiedono i dati
- Risparmiare tempo recuperando in modo più rapido i dati locali e dispersi
- Sincronizzare il contenuto da più distribuzioni senza scrivere codice personalizzato

Federation consente di disporre di modelli di protezione, di cicli di vita, test e orari di distribuzione separati, nonché di amministratori e di titolari aziendali diversi. Ad esempio, è possibile delegare le funzionalità amministrative che impediscono all'amministratore dell'applicazione delle vendite di modificare l'applicazione delle risorse umane.

È possibile replicare diversi oggetti con Federation, come illustrato nella tabella seguente.

| Categoria              | Tipi di oggetto che è possibile replicare                                                                                                                         | Note aggiuntive                                                    |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Viste aziendali        | Business View Manager, DataConnection, LOV, base dati e così via.                                                                                                 | tutti gli oggetti sono supportati anche se non al singolo livello. |
| Report                 | Report Crystal, Web Intelligence e Dashboard Design                                                                                                               | Sono supportati componenti aggiuntivi client e modelli completi.   |
| Oggetti di terze parti | File Excel, PDF, PowerPoint, Flash, Word, di testo, RTF e Shockwave Flash                                                                                         |                                                                    |
| Utenti                 | Utenti, Gruppi, Posta in arrivo, Preferiti e Categoria personale                                                                                                  |                                                                    |
| Piattaforma BI         | Cartelle, eventi, categorie, calendari, livelli di accesso, collegamenti ipertestuali, collegamenti, programmi, profili, pacchetti di oggetti, documenti generali |                                                                    |
| Universo               | Universo, Connessioni e Overload universo                                                                                                                         |                                                                    |

Negli scenari seguenti vengono illustrati due esempi dell'utilizzo di Federation da parte di un'organizzazione.

#### Scenario 1: Vendita al dettaglio (progettazione centralizzata)

Il negozio ACME desidera inviare un rapporto mensile sulle vendite a tutte le diverse sedi attraverso il metodo di replica unilaterale. L'amministratore del sito di origine crea un report che gli amministratori di ogni sito di destinazione replicheranno ed eseguiranno rispetto al database di quel negozio.

#### **Suggerimento:**

Le istanze localizzate possono essere inviate al sito di origine che mantiene ogni informazione replicata dell'oggetto. Ad esempio, applicherà il logo appropriato, le informazioni di connessione al database e così via.

#### Scenario 2: Pianificazione remota (accesso distribuito)

I dati si trovano presso il sito di origine. I processi di replica in sospeso vengono inviati al sito di origine per l'esecuzione. I processi di replica completati vengono quindi inviati ai siti di destinazione per la visualizzazione. Ad esempio, i dati per un report potrebbero non essere disponibili nel sito di destinazione, ma l'utente può impostare i report per l'esecuzione nel sito di origine prima che il report completato venga inviato al sito di destinazione.

## 23.2 Termini correlati a Federation

Nel seguente elenco di termini vengono introdotte parole e frasi correlate a Federation con istruzioni per l'utilizzo:

#### **&Riprova**

Sistema che non è locale per un utente. Ad esempio, il sito di origine viene considerato "Remoto" per gli utenti e gli amministratori del sito di destinazione.

**Aggiornamento della replica**

Tutti gli oggetti inclusi in un elenco di replica vengono aggiornati a prescindere dall'ultima versione modificata.

**Applicazione BI**

Raggruppamento logico di contenuto Business Intelligence (BI) correlato con scopo e utenti specifici. Un'applicazione BI non è un oggetto. Una distribuzione della piattaforma BI può ospitare più applicazioni BI, ognuna delle quali può presentare un modello di protezione, un ciclo di vita, scadenze di test e distribuzione diversi, nonché amministratori e proprietari separati.

**Connessione remota**

Oggetto che contiene informazioni utilizzate per connettersi a una distribuzione della piattaforma BI, inclusi nome utente e password, nome CMS, URL WebService e opzioni di eliminazione.

**Elenco di replica**

Elenco degli oggetti da replicare. Un elenco di replica fa riferimento ad altro contenuto quali utenti, gruppi, report e così via nella distribuzione della piattaforma BI da replicare insieme.

**Istanze completate eseguite localmente**

Istanze elaborate nel sito di destinazione e inviate nuovamente al sito di origine.

**Local**

Sistema locale a cui è connesso un utente o un amministratore. Ad esempio, l'amministratore di un sito di destinazione viene considerato "Locale" nel sito di destinazione.

**Oggetto di replica**

Oggetto replicato da un sito di origine a un sito di destinazione. Tutti gli oggetti replicati in un sito di destinazione verranno contrassegnati da un'icona di replica. Se si verifica un conflitto, gli oggetti verranno contrassegnati da un'icona di conflitto.

**Pacchetto di replica**

Creato durante il trasferimento, il pacchetto di replica contiene gli oggetti del processo di replica. Può contenere tutti gli oggetti definiti nell'elenco di replica, come nel caso di un ambiente mutevole o di una replica iniziale. In alternativa, può contenere un sottoinsieme dell'elenco di replica se gli oggetti cambiano raramente rispetto alla pianificazione del processo di replica. Il pacchetto di replica viene implementato come file BI Application Resource (BIAR).

**Pianificazione remota**

Richieste di pianificazione inviate dal sito di destinazione al sito di origine. È possibile pianificare in remoto i report sui siti di destinazione, affinché l'istanza di report venga inviata nuovamente al sito di origine per l'elaborazione. L'istanza completata verrà quindi restituita al sito di destinazione.

**Processo di replica**

Oggetto che contiene informazioni sulla pianificazione della replica, sul contenuto replicare e sulle eventuali condizioni speciali da eseguire durante la replica del contenuto.

**Replica**

Processo di copia del contenuto da un sistema della piattaforma BI a un altro.

**Replica bilaterale**

Funziona come la replica unilaterale, ma la replica bilaterale invia le modifiche in entrambe le direzioni. Gli aggiornamenti del sito di origine vengono replicati in ogni sito di destinazione. Gli aggiornamenti e i nuovi oggetti in un sito di destinazione vengono inviati al sito di origine.

**Replica unilaterale**

Gli oggetti vengono replicati in una sola direzione, dal sito di origine al sito di destinazione. Eventuali aggiornamenti effettuati nel sito di destinazione rimangono in tale sito.

**Siti di origine multipli**

Più di un sito può servire da sito di origine. Ad esempio, più centri di sviluppo hanno in genere più siti di origine. Può tuttavia esistere un solo sito di origine per replica.

**Sito di destinazione**

Un sistema della piattaforma BI che estrae il contenuto replicato della piattaforma da un sito di origine.

**Sito di origine**

Il sistema della piattaforma BI in cui ha origine il contenuto.

## **23.3 Gestione dei diritti di protezione**

Federation replica il contenuto tra distribuzioni separate e richiede la collaborazione con altri amministratori, pertanto è necessario comprendere come viene eseguita la protezione prima di cominciare ad utilizzare Federation.

È necessario che gli amministratori in distribuzioni separate si coordinino prima di attivare Federation. Una volta replicato, il contenuto può essere modificato dagli amministratori.

I diritti specifici nelle distribuzioni di origine e destinazione sono richiesti per eseguire determinate attività:

- Diritti richiesti sul sito di origine
- Diritti richiesti nel sito di destinazione
- Diritti richiesti negli oggetti specifici di Federation
- Scenari di Federation

**Suggerimento:**

si consiglia di leggere questo capitolo prima di abilitare Federation.

### **23.3.1 Diritti richiesti sul sito di origine**

In questa sezione vengono descritte le azioni nel sito di origine e i diritti richiesti dell'account utente per la connessione al sito di origine. Si tratta dell'account immesso nell'oggetto Connessione remota nel sito di destinazione.

| Azione              | Descrizione                                                                                                                                                                                                                                          | Diritti richiesti                                                                                                                                                                                                                                                                                    |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Replica unilaterale | Esegue la replica solo dal sito di origine al sito di destinazione.<br><b>Nota:</b><br>i diritti "Visualizzazione" e "Replica" sono necessari su tutti gli oggetti da replicare, inclusi quelli replicati automaticamente dai calcoli di dipendenza. | <ul style="list-style-type: none"> <li>• "Visualizza" e "Replica" su tutti gli oggetti che si desidera replicare.</li> <li>• Diritto di "Visualizzazione" nell'elenco di replica.</li> </ul>                                                                                                         |
| Replica bilaterale  | Esegue la replica dal sito di origine al sito di destinazione e viceversa.                                                                                                                                                                           | <ul style="list-style-type: none"> <li>• "Visualizza" e "Replica" su tutti gli oggetti che si desidera replicare.</li> <li>• Diritto di "Visualizzazione" nell'elenco di replica.</li> <li>• "Modifica i diritti" sugli oggetti dell'utente per replicare qualsiasi modifica di password.</li> </ul> |
| Pianificazione      | Consente l'esecuzione della pianificazione remota nel sito di origine dal sito di destinazione.                                                                                                                                                      | <ul style="list-style-type: none"> <li>• Diritto "Pianifica" per tutti gli oggetti che si desidera pianificare in modo remoto</li> </ul>                                                                                                                                                             |

#### Argomenti correlati

- [Diritti richiesti nel sito di destinazione](#)

### 23.3.2 Diritti richiesti nel sito di destinazione

In questa sezione vengono descritte le azioni applicate al sito di destinazione e i diritti richiesti dell'account utente che esegue il processo di replica. Si tratta dell'account dell'utente che ha creato il processo di replica.

**Nota:**

come per altri oggetti pianificabili, è possibile pianificare il processo di replica per conto di altri.

| Azione            | Descrizione                                                                                                                                                                                                                                                                                                                                        | Diritti richiesti                                                                                                                                                                                          |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tutti gli oggetti | Replica gli oggetti indipendentemente dal tipo di replica, ovvero unilaterale o bilaterale.                                                                                                                                                                                                                                                        | <ul style="list-style-type: none"> <li>• “Visualizza,” “Aggiungi,” “Modifica” e “Modifica i diritti” su tutti gli oggetti</li> <li>• Diritto “Modifica password utente”, per gli oggetti utente</li> </ul> |
| Prima replica     | Al momento della prima esecuzione del processo di replica, non esistono ancora oggetti nel sito di destinazione. Di conseguenza, è necessario che l'account utente con cui viene eseguito il processo di replica disponga di diritti specifici in tutte le cartelle di livello superiore e in tutti gli oggetti a cui verrà aggiunto un contenuto. | <ul style="list-style-type: none"> <li>• Diritti “Visualizza”, “Aggiungi”, “Modifica” e “Modifica diritti” in tutte le cartelle di livello superiore e in tutti gli oggetti predefiniti</li> </ul>         |

#### Argomenti correlati

- [Diritti richiesti sul sito di origine](#)

### 23.3.3 Diritti specifici di Federation

In questa sezione vengono descritti dettagliatamente gli scenari specifici di Federation.



| Azione                                                  | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Diritti richiesti                                                                                                                                                                                           |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Eliminazione oggetto                                    | Eliminazione oggetto cancella gli oggetti nel sito di destinazione.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <ul style="list-style-type: none"> <li>L'account in cui è in esecuzione il processo di replica richiede i diritti "Elimina" su tutti gli oggetti che potrebbero essere potenzialmente eliminati.</li> </ul> |
| Disabilitare l'eliminazione per determinati oggetti     | <p>Se determinati oggetti vengono replicati dal sito di origine, è possibile evitare che vengano eliminati dal sito di destinazione anche se vengono eliminati nel sito di origine. È possibile ottenere questo risultato tramite i diritti. È ad esempio consigliabile scegliere questa opzione quando gli utenti nel sito di destinazione utilizzano un oggetto indipendentemente dagli utenti nel sito di origine.</p> <p>Ad esempio, in un universo replicato da cui gli utenti nel sito di destinazione creano i propri report locali, è possibile evitare di perdere l'universo nel sito di destinazione anche se viene eliminato dal sito di origine.</p> | <ul style="list-style-type: none"> <li>Negare i diritti "Elimina" dell'account utente con cui è in esecuzione il processo di replica per gli oggetti che si desidera mantenere.</li> </ul>                  |
| Replica bilaterale, senza modifiche nel sito di origine |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <ul style="list-style-type: none"> <li>Negare i diritti "Modifica" dell'account utente utilizzato per la connessione nell'oggetto connessione remota.</li> </ul>                                            |

| Azione | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Diritti richiesti |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
|        | <p>In determinate circostanze è possibile che si preferisca la replica bilaterale ma non si desideri che vengano modificati alcuni oggetti nel sito di origine, anche se sono cambiati nel sito di destinazione. Uno dei motivi di questa preferenza potrebbe essere un oggetto speciale che deve essere modificato solo dagli utenti nel sito di origine oppure il caso in cui si desideri abilitare la pianificazione remota senza propagare le modifiche in senso contrario.</p> <p><b>Nota:</b><br/>per la pianificazione remota, è possibile creare un processo che gestisca solo gli oggetti per la pianificazione remota. Tuttavia, in questo caso gli oggetti an-tenati vengono ancora replicati, inclusi il report, la cartella contenente il report e la cartella di livello superiore di tale cartella. Qualsiasi modifica apportata nel sito di destinazione viene replicata nel sito di origine e le modifiche apportate nel sito di origine vengono replicate nel sito di destinazione.</p> |                   |

### 23.3.4 Replica della protezione per un oggetto

Per mantenere i diritti di protezione per un oggetto, è necessario replicare l'oggetto e il relativo utente o gruppo contemporaneamente. Altrimenti, è necessario che siano già esistenti nel sito in cui si replica e che dispongano di identificatori univoci e identici (CUID) in ogni sito.

Se un oggetto viene replicato e l'utente o il gruppo non viene replicato o non esiste ancora nel sito in cui si replica, i diritti verranno ignorati.

#### Esempio:

Il Gruppo A e il Gruppo B hanno diritti assegnati sull'oggetto A. Il Gruppo A dispone di diritti "Visualizza" e il Gruppo B dispone di diritti "Nega Visualizza". Se il processo di replica esegue la replica solo per il Gruppo A e l'Oggetto A, nel sito di destinazione l'Oggetto A disporrà solamente dei diritti "Visualizza" per il Gruppo A associato ad esso.

Quando si replica un oggetto vi sono potenziali rischi per la protezione se non si replicano tutti i gruppi con diritti espliciti sull'oggetto. L'esempio precedente evidenzia un potenziale rischio per la protezione. Se l'Utente A appartiene a entrambi i Gruppi A e B, l'utente non disporrà dell'autorizzazione per visualizzare l'Oggetto A nel sito di origine. Tuttavia l'Utente A verrà replicato nel sito di destinazione perché appartiene a entrambi i gruppi. A questo punto, poiché il Gruppo B non è stato replicato, l'Utente A disporrà del diritto di visualizzare l'Oggetto A nel sito di destinazione, ma non potrà visualizzare l'Oggetto A nel sito di origine.

Gli oggetti che fanno riferimento ad altri oggetti non inclusi in un processo di replica o quelli che non si trovano già nel sito di destinazione, vengono visualizzati in un file di registro. Tale file mostra che l'oggetto faceva riferimento all'oggetto non replicato e ha eliminato il riferimento.

La protezione su un oggetto per un utente o gruppo particolare viene replicata solo dal sito di origine al sito di destinazione. È possibile impostare la protezione sugli oggetti replicati nel sito di destinazione, ma tali impostazioni non verranno replicate nel sito di origine.

### **23.3.5 Replica della protezione mediante i livelli di accesso**

Per essere resi permanenti, i diritti devono essere definiti dai livelli di accesso. È necessario che l'oggetto, utente o gruppo e il livello di accesso siano replicati contemporaneamente oppure che siano già esistenti nel sito in cui si replica.

Gli oggetti che assegnano diritti espliciti a un utente o un gruppo non inclusi nel processo di replica o non ancora presenti nel sito di destinazione vengono visualizzati nel relativo file di registro che indica che all'oggetto erano stati assegnati diritti non replicati che sono stati quindi eliminati.

Inoltre, è possibile scegliere di replicare automaticamente i “Livelli di accesso” utilizzati su un oggetto importato. Questa opzione è disponibile nell'elenco di replica.

#### **Nota:**

i livelli di accesso predefiniti non vengono replicati, ma i riferimenti vengono mantenuti.

## **23.4 Opzioni di tipi e modalità di replica**

A seconda della selezione per Tipo di replica e Modalità replica, è possibile creare una tra quattro diverse opzioni di processo di replica:

- Replica unilaterale
- Replica bilaterale
- Aggiorna da origine
- Aggiorna da destinazione

### 23.4.1 Replica unilaterale

Con la replica unilaterale, è possibile replicare il contenuto in una sola direzione, dal sito di origine a quello di destinazione. Eventuali modifiche agli oggetti nell'elenco di replica del sito di origine vengono inviate al sito di destinazione. Tuttavia, le modifiche apportate agli oggetti in un sito di destinazione non vengono inviate al sito di origine.

La replica unilaterale è ideale per distribuzioni con una sola distribuzione centrale della piattaforma BI in cui vengono creati, modificati e amministrati gli oggetti. Altre distribuzioni utilizzano il contenuto della distribuzione centrale.

Per creare la replica unilaterale, selezionare le opzioni seguenti:

- Tipo di replica = Replica unilaterale
- Modalità replica = Replica normale

### 23.4.2 Replica bilaterale

La replica bilaterale consente di replicare il contenuto in entrambe le direzioni tra il sito di origine e quello di destinazione. Eventuali modifiche apportate agli oggetti nel sito di origine vengono replicate nel sito di destinazione, mentre le modifiche apportate in un sito di destinazione vengono replicate nel sito di origine.

**Nota:**

per eseguire la pianificazione remota e replicare le istanze eseguite localmente al sito di origine, è necessario selezionare la modalità di replica bilaterale.

Se si dispone di più distribuzioni della piattaforma BI in cui il contenuto viene creato, modificato, amministrato e utilizzato in entrambe le posizioni, la replica bilaterale è la modalità più efficiente. Contribuisce inoltre alla sincronizzazione delle distribuzioni.

Per creare la replica bilaterale, selezionare le opzioni seguenti:

- Tipo di replica = Replica bilaterale
- Modalità replica = Replica normale

**Argomenti correlati**

- [Pianificazione remota e istanze eseguite localmente](#)

### 23.4.3 Aggiornamento da origine o da destinazione

Quando si replica il contenuto nella modalità Replica unilaterale o Replica bilaterale, gli oggetti nell'elenco di replica vengono replicati in un sito di destinazione. È possibile tuttavia che non tutti gli oggetti vengano replicati a ogni esecuzione del processo di replica.

Federation dispone di un motore di ottimizzazione progettato per velocizzare il completamento dei processi di replica. Utilizza una combinazione di timestamp e versione dell'oggetto per stabilire se l'oggetto è già stato modificato dopo l'ultima replica. Questo controllo viene eseguito su oggetti specificatamente selezionati nell'elenco di replica ed eventuali oggetti replicati durante la verifica della dipendenza.

In alcuni casi, tuttavia, è possibile che il motore di ottimizzazione perda alcuni oggetti, che non verranno replicati. In questi casi, è possibile utilizzare "Aggiorna da origine" e "Aggiorna da destinazione" per forzare il processo di replica a replicare il contenuto e le relative dipendenze, indipendentemente dalle indicazioni data e ora.

"Aggiorna da origine" invia il contenuto unicamente dal sito di origine a quelli di destinazione. "Aggiorna da destinazione" invia il contenuto unicamente dai siti di destinazione a quello di origine.

#### Esempio:

Nei tre esempi seguenti vengono illustrati alcuni scenari in cui vengono utilizzate le opzioni "Aggiorna da origine" e "Aggiorna da destinazione" e in cui alcuni oggetti potrebbero essere persi a causa dell'ottimizzazione.

Scenario 1: aggiunta di oggetti che contengono altri oggetti in un'area che viene replicata.

La Cartella A viene replicata dal sito di origine a quello di destinazione. Ora è presente in entrambi i siti. Un utente sposta o copia la Cartella B con il Report B nella Cartella A nel sito di origine. Durante la replica successiva, Federation rileverà che l'indicazione data e ora della Cartella B è stata modificata e la replicherà nel sito di destinazione. Il timestamp del Report B tuttavia non è cambiato. Pertanto il report verrà saltato da un normale processo di replica unilaterale o bilaterale.

Per assicurarsi che il contenuto della Cartella B sia replicato correttamente, è necessario utilizzare una volta un processo di replica con "Aggiorna da origine." Dopodiché, il normale processo di replica unilaterale o bilaterale funzionerà correttamente. Se questo esempio viene invertito e la Cartella B viene spostata o copiata nel sito di destinazione, utilizzare "Aggiorna da destinazione."

Scenario 2: aggiunta di nuovi oggetti utilizzando LifeCycle Manager o la riga di comando BIAR.

Quando si aggiungono oggetti a un'area che viene replicata utilizzando LifeCycle Manager o la riga di comando BIAR, l'oggetto potrebbe venire ignorato da un normale processo di replica unilaterale o bilaterale. Questa situazione può essere dovuta al fatto che i clock interni nei sistemi di origine e di destinazione non sono sincronizzati quando si utilizza LifeCycle Manager o la riga di comando BIAR.

**Nota:**

dopo l'importazione di nuovi oggetti in un'area replicata nel sito di origine, è consigliabile eseguire un processo di replica con l'opzione "Aggiorna da origine." Dopo l'importazione di nuovi oggetti in un'area replicata nel sito di destinazione, è consigliabile eseguire un processo di replica con l'opzione "Aggiorna da destinazione."

Scenario 3: orari di replica pianificati intermedi.

Se si aggiungono oggetti a un'area che viene replicata e non è possibile aspettare la successiva replica pianificata, è possibile utilizzare processi di replica con le opzioni "Aggiorna da origine" e "Aggiorna da destinazione". È possibile replicare rapidamente il contenuto selezionando l'area in cui sono stati aggiunti gli oggetti.

---

**Nota:**

- questo scenario può essere oneroso per elenchi di replica di grandi dimensioni, pertanto è consigliabile non utilizzare spesso questa opzione. Ad esempio, non è necessario creare processi di replica che eseguono l'aggiornamento dal sito di origine a quello di destinazione, pianificati ogni ora. Queste modalità devono essere utilizzate con la pianificazione "Esegui ora" o con scarsa frequenza.
- in alcuni casi, non è possibile utilizzare la risoluzione dei conflitti, ad esempio con "Aggiorna da origine:" l'opzione Risoluzione conflitti a favore del sito di destinazione è bloccata e con "Aggiorna da destinazione:" l'opzione Risoluzione conflitti a favore del sito di origine è bloccata.

## 23.5 Replica di utenti e gruppi di terze parti

In Federation è possibile replicare utenti e gruppi di terze parti, specificamente utenti e gruppi Active Directory (AD) e LDAP.

**Suggerimento:**

se si intende replicare questi tipi di utenti e gruppi o il contenuto personale, ad esempio le cartelle Preferiti o Posta in arrivo, consultare questa sezione.

**Mappatura di utenti e gruppi**

1. Mappare gli utenti e i gruppi nel sito di origine affinché vengano replicati correttamente in Federation.
2. È quindi necessario replicare gli utenti e i gruppi mappati nel sito di destinazione.

**Nota:**

non mappare gruppi e utenti separatamente nel sito di destinazione. In caso contrario, avranno identificatori univoci (CUID) diversi nel sito di destinazione e in quello di origine e non sarà possibile stabilirne correttamente la corrispondenza in Federation.

**Esempio:**

L'amministratore mappa il Gruppo A all'Utente A nei siti di origine e di destinazione. Sia il Gruppo A sia l'Utente A hanno identificatori univoci diversi nei siti di origine e di destinazione. Durante la replica,

Federation non può trovare la corrispondenza e il Gruppo A o l'Utente A non vengono replicati a causa di un conflitto di alias.

---

**Nota:**

- prima di replicare utenti e gruppi di terze parti, il sito di destinazione deve essere impostato per l'utilizzo dell'autenticazione AD o LDAP. È tuttavia necessario configurare il sito di destinazione per l'utilizzo di AD o LDAP in modo da consentire la comunicazione con il server di directory o il controller di dominio.
- dopo la prima replica di un gruppo AD o LDAP, gli utenti di tale gruppo non saranno in grado di accedere finché non verrà aggiornato il grafico del gruppo AD/LDAP. Questa operazione viene eseguita automaticamente ogni 15 minuti circa. Per aggiornare manualmente il grafico del gruppo AD/LDAP, andare alla pagina "Autenticazione" della console CMC, fare doppio clic su **Windows AD o LDAP**, quindi fare clic su **Aggiorna**.
- prestare attenzione durante la replica di gruppi di terze parti. Quando si aggiungono nuovi utenti al gruppo nel server di directory, tali utenti potranno accedere a entrambi i siti. Questo problema di protezione dell'autenticazione AD o LDAP non dipende da Federation.

Se si accede separatamente ai siti di destinazione e di origine o se l'appartenenza al gruppo viene aggiornata in entrambi i siti tramite il pulsante di aggiornamento nella pagina di autenticazione della CMC, verrà creato un account utente in entrambi i siti. Gli account avranno identificatori univoci diversi e Federation non sarà in grado di replicarli correttamente.

**Nota:**

è importante creare l'account in un sito, quindi replicarlo nell'altro.

## 23.6 Replica di universi e connessioni agli universi

Se si intende utilizzare Federation per replicare gli universi tra le distribuzioni della piattaforma BI, è importante pianificarlo in anticipo. Un oggetto Universo non può funzionare senza un oggetto Connessione all'universo sottostante.

Gli oggetti connessione all'universo contengono informazioni necessarie per la connessione a un database di reporting. Per funzionare correttamente, gli oggetti connessione all'universo devono contenere informazioni valide e consentire che venga stabilita una connessione al database.

**Nota:**

se si utilizza la replica bidirezionale e si replica un universo dal sito di origine a quello di destinazione senza la relativa connessione all'universo, è possibile che nelle repliche successive la relazione dell'universo di origine con la Connessione all'universo nell'origine venga sovrascritta o rimossa. Per evitare questa situazione, replicare sempre le connessioni agli universi con gli universi stessi.

Per assicurarsi che le connessioni agli universi dipendenti vengano replicate insieme agli universi, selezionare sempre le opzioni seguenti quando si crea o si modifica l'elenco repliche che contiene gli universi:

- **Includi connessioni utilizzate dagli universi selezionati**

- **Includi universi richiesti dagli universi selezionati**

**Nota:**

se la relazione di un universo con la relativa connessione viene sovrascritta o rimossa, aprire l'universo in Universe Designer e in **File > Parametri**, modificare le informazioni sulla connessione.

Nei due esempi seguenti viene illustrato il processo di replica degli universi e delle relative connessioni agli universi.

**Esempio:**

Quando si replicano gli universi e le connessioni agli universi, è necessario assicurarsi che l'ambiente di connettività del sito di origine corrisponda all'ambiente di connettività del sito di destinazione.

Se ad esempio la connessione all'universo utilizza una connessione ODBC denominata "TestODBC", è necessario che nell'ambiente di destinazione sia presente una connessione ODBC configurata correttamente denominata "TestODBC." La connessione ODBC può essere risolta nello stesso database o in un altro database. Per evitare problemi di connettività per gli universi che utilizzano questa connessione, è necessario che lo schema dei database sia lo stesso.

---

**Esempio:**

Se si desidera che l'universo replicato nella destinazione utilizzi un database diverso da quello utilizzato per l'universo nel sito di origine, replicare la connessione all'universo ma impostare le informazioni di connettività del sito di destinazione affinché facciano riferimento al database desiderato.

Se ad esempio la connessione all'universo del sito di origine utilizza una connessione ODBC denominata "Test" che fa riferimento al "DatabaseA", impostare nel sito di destinazione una connessione ODBC denominata anch'essa "Test" ma con riferimento al "DatabaseB".

---

## 23.7 Gestione degli elenchi di replica

Gli elenchi di replica includono contenuti, quali utenti, gruppi e report nella distribuzione della piattaforma BI, che possono essere replicati insieme. È possibile accedere agli elenchi di replicare dalla CMC.

I tipi di contenuto che possono essere replicati sono descritti nella seguente tabella.



| Categoria              | Oggetti supportati                                                                                                                                                                       |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Oggetti del repository | Gli oggetti che includono viste aziendali, connessioni dati, Elenchi di valori, basi dati e altro.<br><b>Nota:</b><br>tutti gli oggetti sono supportati anche se non al singolo livello. |
| Report                 | Report Crystal, documenti Web Intelligence e oggetti di Cruscotti.<br><b>Nota:</b><br>sono supportati componenti aggiuntivi e modelli Full Client.                                       |
| Oggetti di terze parti | Excel, PDF, Powerpoint, Flash, Word, file di testo, file RTF, file Shockwave Flash.                                                                                                      |
| Utenti                 | Utenti, gruppi, Posta in arrivo, Preferiti, categoria personale.                                                                                                                         |
| Piattaforma BI         | Cartelle, eventi, categorie, calendari, ruoli personalizzati, collegamenti ipertestuali, collegamenti, programmi, profili, pacchetti di oggetti, documenti generali.                     |
| Universi               | Universi, connessioni, overload di universi.                                                                                                                                             |

**Nota:**

i seguenti oggetti devono essere creati nel sito di origine e replicati nel sito di destinazione. Se si creano questi oggetti nel sito di destinazione e successivamente si replicano nel sito di origine, in quest'ultimo sito non funzioneranno.

- Viste aziendali
- Elementi aziendali
- Basi dati
- Connessioni dati
- Elenchi dei valori
- Overload di universi

## 23.7.1 Creazione di elenchi di replica

Gli elenchi di replica si trovano nell'area Elenchi di replica della CMC. È possibile organizzare gli elenchi di replica in cartelle e sottocartelle create dall'utente.

### 23.7.1.1 Creazione di una cartella Elenco di replica

1. Accedere all'area "Elenchi di replica" della console CMC.
2. Fare clic su **Elenchi di replica**.

3. Scegliere **Gestisci > Nuova > cartella**.

Verrà visualizzata la finestra di dialogo "Crea cartella".

4. Immettere un nome per la cartella e fare clic su **OK**.

A questo punto è possibile creare elenchi di replica in questa cartella.

### 23.7.1.2 Creazione di un elenco di replica

1. Accedere all'area "Elenchi di replica" della console CMC.

2. Selezionare la cartella in cui si desidera salvare il nuovo elenco di replica.

3. Fare clic su **Gestisci > Nuovo > Nuovo elenco di replica**.

Verrà visualizzata la finestra di dialogo "Nuovo elenco di replica".

4. Immettere il titolo e la descrizione dell'elenco di replica.

5. Per accedere a opzioni avanzate, fare clic sul collegamento **Proprietà elenco di replica**.

In questo modo sarà possibile specificare le dipendenze che devono essere replicate automaticamente dal sito di origine al sito di destinazione.

6. Selezionare le opzioni desiderate come descritto nella tabella.

| Opzioni di dipendenza oggetti                                  | Definizione                                                                                                    |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Includi cartelle personali per gli utenti selezionati          | Replica le cartelle personali di un utente selezionato e il relativo contenuto.                                |
| Includi categorie personali per gli utenti selezionati         | Replica le categorie personali di un utente selezionato.                                                       |
| Includi universi per i report selezionati                      | Replica qualsiasi universo da cui dipendono gli oggetti report selezionati.                                    |
| Includi membri dei gruppi di utenti selezionati                | Replica gli utenti all'interno di un gruppo selezionato.                                                       |
| Includi universi richiesti dagli universi selezionati          | Replica qualsiasi universo che dipende da altri universi.                                                      |
| Includi caselle di Posta in arrivo per gli utenti selezionati  | Replica la casella di Posta in arrivo di un utente selezionato e il relativo contenuto.                        |
| Includi gruppi di utenti per gli universi selezionati          | Replica i gruppi di utenti associati agli overload di un universo.                                             |
| Includi livelli di accesso impostati sugli oggetti selezionati | Replica qualsiasi livello di accesso utilizzato su uno o più oggetti selezionati.                              |
| Includi documenti per categorie selezionate                    | Replica qualsiasi documento, inclusi file di Word, Excel, PDF e così via, incluso nelle categorie selezionate. |

| Opzioni di dipendenza oggetti                                   | Definizione                                                                                                                        |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Includi dipendenze supportate per gli oggetti Flash selezionati | Replica qualsiasi report Crystal, collegamento ipertestuale, documento o universo Web Intelligence da cui dipende l'oggetto Flash. |
| Includi profili per utenti e gruppi di utenti selezionati       | Replica qualsiasi profilo associato a utenti o gruppi selezionati.                                                                 |
| Includi connessioni utilizzate dagli universi selezionati       | Replica qualsiasi oggetto connessione universo utilizzato dagli oggetti selezionati.                                               |

**Nota:**

alcuni oggetti nella piattaforma BI dipendono da altri oggetti. Ad esempio: un documento Web Intelligence dipende dall'universo sottostante per quanto riguarda struttura e contenuto. Se si replica un documento Web Intelligence ma non si seleziona l'universo che utilizza, la replica non funzionerà nel sito di destinazione a meno che tale universo non sia già stato replicato. Se tuttavia si abilita "Includi universi per i report selezionati", Federation replicherà automaticamente gli universi da cui dipende il report.

7. Fare clic su **Avanti**.
8. Selezionare uno o più oggetti da aggiungere all'elenco di replica.
  - Utilizzare i tasti freccia per aggiungere o rimuovere gli oggetti dalla cartella "Oggetti disponibili".
  - In alternativa, fare clic su **Replica tutto** in "Oggetti repository" per replicare tutte le visualizzazioni aziendali, gli elementi aziendali, la base dati, la connessione dati e gli oggetti repository, incluse funzioni e immagini di report.

**Nota:**

non è possibile replicare le cartelle di livello superiore, che si trovano sotto la cartella "Oggetti disponibili".

9. Fare clic su **Salva e chiudi**.

## 23.7.2 Modifica degli elenchi di replica

Dopo avere creato un elenco di replica, è possibile modificarne le proprietà o gli oggetti.

### 23.7.2.1 Modifica delle proprietà in un elenco di replica

1. Accedere all'area "Elenchi di replica" della console CMC.
2. Selezionare l'**Elenco di replica** da modificare.
3. Fare clic su **Gestisci > Proprietà**.

Verrà visualizzata la finestra di dialogo **Proprietà generali**.

4. Modificare il titolo e la descrizione. È anche possibile modificare altre aree dell'elenco di replica mentre la finestra di dialogo **Proprietà** è aperta.
5. Se si desidera modificare le opzioni di dipendenza, fare clic su **Proprietà elenco replica** nell'elenco di spostamento.
6. Fare clic su **Salva e chiudi**.

#### **Argomenti correlati**

- [Creazione di elenchi di replica](#)

### **23.7.2.2 Modifica di oggetti in un elenco di replica**

1. Accedere all'area "Elenchi di replica" della console CMC.
2. Selezionare un **Elenco di replica**.
3. Fare clic su **Azioni > Gestisci elenco replica**.  
Verrà visualizzata la finestra di dialogo "Gestisci elenco replica" con un elenco degli oggetti inclusi nell'elenco di replica.
4. Aggiungere o rimuovere oggetti nel modo desiderato.
5. Fare clic su **Salva e chiudi**.

#### **Argomenti correlati**

- [Creazione di elenchi di replica](#)

## **23.8 Gestione delle connessioni remote**

Gli oggetti connessione remota contengono le informazioni necessarie per la connessione a una distribuzione della piattaforma BI remota.

#### **Nota:**

l'oggetto connessione remota viene creato in una distribuzione della piattaforma BI del sito di destinazione. La connessione remota è il sito di origine.

È possibile visualizzare le connessioni remote nell'area "Federazione" della CMC.

## 23.8.1 Creazione di connessioni remote

Una connessione remota in Federation si connette a una distribuzione remota della piattaforma BI. Per stabilire una connessione al sito di origine in cui si trova il contenuto da replicare, è necessario creare una connessione remota sul sito di destinazione.

È possibile creare cartelle e sottocartelle per organizzare le connessioni remote.

### 23.8.1.1 Creazione di una cartella di connessione remota

1. Accedere all'area "Federazione" della console CMC.
2. Fare clic su **Connessioni remote**.
3. Scegliere **Gestisci > Nuova > cartella**.  
Verrà visualizzata la finestra di dialogo **Crea cartella**.
4. Immettere un nome per la cartella e fare clic su **OK**.  
A questo punto è possibile creare connessioni remote in questa cartella.

### 23.8.1.2 Creazione di una connessione remota

Per connettersi a una distribuzione remota della piattaforma BI, è necessario creare una connessione remota in Federation.

1. Accedere all'area "Federazione" della console CMC.
2. Fare clic su **Connessioni remote**.
3. Fare clic su **Gestisci > Nuovo > Nuova connessione remota**.  
Verrà visualizzata la finestra di dialogo "Nuova connessione al sistema remoto".
4. Immettere un titolo, una descrizione e campi correlati, secondo le esigenze:

**Nota:**

tutti i campi sono obbligatori, ad eccezione di "Descrizione" e "Limitare il numero di oggetti eliminati a."

| Campo  | Descrizione                           |
|--------|---------------------------------------|
| Titolo | Nome dell'oggetto Connessione remota. |

| Campo                                     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Descrizione                               | Descrizione dell'oggetto Connessione remota. (Facoltativo)                                                                                                                                                                                                                                                                                                                                                                                                   |
| URI servizio Web sul sistema remoto       | <p>URL di Servizi Web di Federation, distribuiti automaticamente sul server delle applicazioni Java. È possibile utilizzare qualsiasi servizio Web Federation disponibile nella piattaforma BI, sia sul sito di origine sia su quello di destinazione, o un'altra distribuzione. Utilizzare questo formato:</p> <p><code>http://nome_server_applicazioni:porta/dswsbobje</code>.</p> <p>Esempio: <code>http://computer.dominio.com:8080/dswsbobje</code></p> |
| CMS sistema remoto                        | <p>Nome del CMS a cui ci si desidera collegare, accessibile attraverso i Servizi Web di Federation. Questo verrà considerato come il CMS del sito di origine. Il formato è: Nome_CMS:porta.</p> <p>Esempio: <code>mymachine:6400</code></p> <p><b>Nota:</b><br/>se si utilizza la porta predefinita 6400, la specifica della porta è facoltativa.</p>                                                                                                        |
| Nome utente                               | <p>Nome utente che verrà utilizzato per connettersi al sito di origine.</p> <p><b>Nota:</b><br/>assicurarsi che il nome utente utilizzato disponga dei diritti di visualizzazione per l'elenco di replica nella distribuzione del sito di origine.</p>                                                                                                                                                                                                       |
| Password                                  | Password dell'account utente utilizzato per connettersi al sito di origine.                                                                                                                                                                                                                                                                                                                                                                                  |
| Autenticazione                            | Tipo di autenticazione utilizzata per connettersi al sito di origine. Le opzioni sono: Enterprise, NT, AD o LDAP.                                                                                                                                                                                                                                                                                                                                            |
| Frequenza di eliminazione (in ore)        | Frequenza con cui verranno eliminati gli oggetti dai processi di replica che utilizzano questo oggetto Connessione remota. Immettere solo numeri interi positivi. L'unità di misura è l'ora. Impostazione predefinita = 24.                                                                                                                                                                                                                                  |
| Limitare il numero di oggetti eliminati a | Numero di oggetti eliminati da un processo di replica. (Facoltativo)                                                                                                                                                                                                                                                                                                                                                                                         |

##### 5. Scegliere **OK**.

**Argomenti correlati**

- [Gestione dell'eliminazione di oggetti](#)

## 23.8.2 Modifica delle connessioni remote

Dopo avere creato una connessione remota, è possibile modificarne le proprietà e le opzioni di protezione.



Per modificare una connessione remota:

1. Accedere all'area "Federazione" della console CMC.
2. Fare clic su **Connessioni remote**.
3. Fare doppio clic sulla connessione remota che si desidera modificare.  
Verrà visualizzata la finestra di dialogo "Proprietà connessione remota". È possibile utilizzare le seguenti proprietà:
  - **Titolo**
  - **Descrizione**
  - **URI servizio Web sul sistema remoto**
  - **CMS sistema remoto**
  - **Nome utente**
  - **Password**
  - **Autenticazione**
  - **Frequenza di eliminazione (in ore)**
  - **Limitare il numero di oggetti eliminati a**
4. Specificare le modifiche.
5. Fare clic su **Salva e chiudi**.

## 23.9 Gestione dei processi di replica

Un processo di replica è un tipo di oggetto eseguito in base a una pianificazione che viene utilizzato per replicare il contenuto tra due distribuzioni della piattaforma BI in Federation.

**Nota:**

gli oggetti replicati in un sito di destinazione verranno contrassegnati con un'icona di replica, come illustrato di seguito:  In caso di conflitto, un oggetto verrà contrassegnato con un'icona di conflitto, come illustrato di seguito: 

È possibile visualizzare un elenco dei processi di replica nella cartella **Connessione remota** nell'area "Federazione" della CMC.

## 23.9.1 Creazione di processi di replica

Un processo di replica è necessario per replicare il contenuto tra due distribuzioni della piattaforma BI in Federation. A ogni processo di replica devono essere associati una sola connessione remota e un solo elenco di replica.

### 23.9.1.1 Creazione di un processo di replica

1. Accedere all'area "Federazione" della console CMC.
2. Fare clic su **Connessioni remote**.
3. Selezionare una **Connessione remota** in cui inserire il nuovo processo di replica.

**Avvertenza:**

per proseguire con la procedura guidata, è necessario che la console CMC possa connettersi ai Servizi Web nell'URI di connessione remota.

4. Fare clic su **Gestisci > Nuovo > Nuovo processo di replica**.  
Verrà visualizzata la finestra di dialogo "Nuovo processo di replica".
5. Immettere un titolo e una descrizione per il processo di replica.
6. Fare clic su **Avanti**.  
Verrà visualizzato un elenco degli elenchi di replica disponibili nel sito di origine.
7. Selezionare l'**Elenco replica** che si desidera utilizzare con il processo di replica.
8. Fare clic su **Avanti**.
9. Selezionare le opzioni di configurazione come descritto nella tabella riportata di seguito.



| Opzione                                                                                       | Descrizione                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Attiva eliminazione oggetto sulla destinazione</b>                                         | <p>Impone al processo di replica l'eliminazione di qualsiasi oggetto replicato sul sito di destinazione se l'oggetto originale sul sito di origine è stato rimosso.</p> <p><b>Nota:</b><br/>con l'eliminazione di oggetti non verranno eliminati oggetti replicati utilizzando dipendenze o oggetti selezionati nell'elenco di replica.</p> |
| <b>Replica unilaterale</b>                                                                    | Specifica che un oggetto venga replicato solo dal sito di origine a quello di destinazione. Le modifiche apportate all'oggetto sul sito di origine dopo la replica verranno replicate sul sito di destinazione, mentre quelle apportate sul sito di destinazione non verranno replicate sul sito di origine.                                |
| <b>Replica bilaterale</b>                                                                     | Specifica che gli oggetti vengano replicate in entrambe le direzioni, ovvero dal sito di origine al sito di destinazione e viceversa. Le modifiche apportate a questi oggetti su un sito dopo la replica vengono replicate automaticamente nell'altro sito.                                                                                 |
| <b>Precedenza del sito di origine</b>                                                         | Specifica che, quando viene rilevato un conflitto tra un oggetto sul sito di origine e la versione replicata sul sito di destinazione, la priorità spetta alla versione sul sito di origine.                                                                                                                                                |
| <b>Nessuna risoluzione conflitti automatica</b>                                               | Specifica che non venga eseguita alcuna azione per risolvere eventuali conflitti rilevati.                                                                                                                                                                                                                                                  |
| <b>Precedenza del sito di destinazione</b> (disponibile unicamente con la replica bilaterale) | Specifica che, quando viene rilevato un conflitto tra un oggetto sul sito di origine e la versione replicata sul sito di destinazione, la priorità spetta alla versione sul sito di destinazione.                                                                                                                                           |
| <b>Replica normale</b>                                                                        | Specifica che il processo di replica venga eseguito normalmente.                                                                                                                                                                                                                                                                            |
| <b>Aggiorna da origine</b>                                                                    | Replica tutto il contenuto dal sito di origine al sito di destinazione indipendentemente dal fatto che il contenuto sia stato modificato o meno. È possibile replicare l'intero elenco di replica o solo una parte di esso.                                                                                                                 |
| <b>Aggiorna da destinazione</b> (disponibile unicamente con la replica bilaterale)            | Replica tutto il contenuto dal sito di destinazione al sito di origine indipendentemente dal fatto che il contenuto sia stato modificato o meno. È possibile replicare l'intero elenco di replica o solo una parte di esso.                                                                                                                 |

| Opzione                                                                                 | Descrizione                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Replica tutti gli oggetti</b> (disponibile unicamente con la replica bilaterale)     | Replica l'intero elenco di replica.<br><b>Nota:</b><br>si tratta dell'opzione più completa, ma anche più lunga.                                                                   |
| <b>Replica pianificazioni remote</b> (disponibile unicamente con la replica bilaterale) | Replica le istanze remote in sospeso dal sito di destinazione al sito di origine e impone istanze complete dal sito di origine a quello di destinazione.                          |
| <b>Replica modelli documento</b>                                                        | Replica tutti gli oggetti che non sono istanze (eseguiti localmente o report selezionati per la pianificazione remota). Sono inclusi utenti, gruppi, cartelle, report e così via. |
| <b>Replica istanze completate eseguite localmente</b>                                   | Replica le istanze completate solo dal sito di destinazione al sito di origine.                                                                                                   |

10. Fare clic su **OK**.

#### Argomenti correlati

- [Gestione dell'eliminazione di oggetti](#)
- [Gestione del rilevamento e della risoluzione dei conflitti](#)
- [Pianificazione remota e istanze eseguite localmente](#)

## 23.9.2 Pianificazione dei processi di replica

Dopo avere creato un processo di replica, è possibile pianificarlo per la singola esecuzione o su base ricorrente. È inoltre possibile pianificare più processi di replica in un sito di destinazione da un sito di origine.

#### Nota:

se si pianificano più processi di replica in un sito di destinazione, al sito di origine può connettersi solo un processo di replica alla volta. Tutti gli altri processi di replica che tentano di connettersi verranno posti in uno stato sospeso dove vi rimarranno finché non saranno in grado di connettersi automaticamente al sito di origine.

### 23.9.2.1 Pianificazione di un processo di replica

1. Accedere all'area "Federazione" della console CMC.
2. Selezionare il **Processo di replica** da pianificare.
3. Fare clic su **Azioni > Pianificazioni**.
4. Selezionare le opzioni di pianificazione desiderate.

### 23.9.3 Modifica dei processi di replica

Dopo avere creato un processo di replica in Federation, è possibile modificarne le proprietà.

#### 23.9.3.1 Modifica di un processo di replica

1. Accedere all'area "Federazione" della console CMC.
2. Fare clic sulla cartella **Connessioni remote**.
3. Selezionare l'oggetto **Connessione remota** che contiene il **processo di replica** da modificare.
4. Selezionare il **processo di replica** da modificare.
5. Fare clic su **Gestisci > Gestisci proprietà oggetto**.
6. Visualizzare e modificare le **Proprietà**, la **Pianificazione**, la **Cronologia**, l'**Elenco di replica** e la **Protezione utente** nel modo desiderato.

| Sezioni           | Descrizione                                                                                      |
|-------------------|--------------------------------------------------------------------------------------------------|
| Proprietà         | Modificare il nome, la descrizione e altre proprietà generali e opzioni del processo di replica. |
| Pianificazione    | Impostare il processo di replica affinché venga eseguito secondo una pianificazione ricorrente.  |
| Cronologia        | Visualizzare e amministrare tutte le istanze del processo di replica.                            |
| Elenco di replica | Modificare l'elenco di replica selezionato.                                                      |
| Protezione utente | Impostare i diritti sul processo di replica.                                                     |

#### 23.9.4 Visualizzazione di un registro dopo un processo di replica

Ogni volta che si esegue un processo di replica, Federation genera automaticamente un file di registro nel sito di destinazione. I file di registro si basano sugli standard XML 1.1 e richiedono un browser che supporti tali standard.

Per visualizzare un registro di replica:

1. Accedere all'area "Federation" della CMC.
2. Fare clic su **Tutti i processi di replica**.
3. Selezionare un **Processo di replica** dall'elenco.
4. Fare clic su **Proprietà**.  
Verrà aperta la pagina "Proprietà" del processo di replica.
5. Fare clic su **Cronologia**.
6. Fare clic su **Ora istanza** del file di registro per visualizzare i processi di replica completati oppure fare clic sullo stato **Non riuscito** per visualizzare un file di registro dei processi di replica non riusciti.
7. Selezionare l'istanza desiderata per visualizzare il file di registro.

Il file di registro viene generato in formato XML e un form XSL viene utilizzato per formattare le informazioni in una pagina HTML.

È possibile accedere al registro XML dal computer che esegue Server Intelligence Agent contenente Adaptive Job Server. Il file di registro è reperibile in questo percorso:

- In Windows, `DirInstallaz\SAP BusinessObjects Enterprise XI 4.0\logging`.
- In Unix: `DirInstall/sap_bobj/logging`

## 23.10 Gestione dell'eliminazione di oggetti

In Federation, è necessario eseguire l'attività di eliminazione di oggetti durante il ciclo del processo di replica, per assicurarsi che tutti gli oggetti eliminati dal sito di origine vengano eliminati anche dal sito di destinazione.

L'eliminazione di oggetti implica una connessione remota e un processo di replica. L'oggetto Connessione remota definisce le opzioni generali di eliminazione, mentre il processo di replica esegue l'eliminazione al termine dell'intervallo appropriato.

### 23.10.1 Modalità di utilizzo dell'eliminazione di oggetti

I processi di replica separati che utilizzano la stessa connessione remota funzionano insieme durante l'eliminazione di oggetti. Ciò significa che il processo di replica eliminerà gli oggetti all'interno del proprio elenco di replica, nonché gli oggetti all'interno di altri elenchi di replica che utilizzano la stessa connessione remota. Una connessione remota è considerata uguale solo se l'elemento principale del processo di replica è lo stesso oggetto Connessione remota.

**Esempio:**

I processi di replica A e B replicano l'oggetto A e l'oggetto B. Entrambi i processi replicano gli oggetti dallo stesso sito di origine e utilizzano la stessa connessione remota. Se il sito di origine elimina l'oggetto B, il processo di replica A rileverà che l'oggetto B è stato eliminato. Anche se la replica viene eseguita dal processo di replica B, verrà rimosso dal sito di destinazione anche l'oggetto B. Quando viene eseguito il processo di replica B non sarà necessaria un'operazione di eliminazione di oggetti.

---

**Nota:**

durante un'eliminazione di oggetti vengono eliminati solo gli oggetti nel sito di destinazione. Se si rimuove un oggetto dal sito di origine che fa parte di una replica, l'oggetto verrà rimosso dal sito di destinazione. Se tuttavia un oggetto viene rimosso dal sito di destinazione, non verrà rimosso dal sito di origine durante l'eliminazione di oggetti, anche se il processo di replica si trova in modalità Replica bilaterale.

Gli oggetti che vengono eliminati o rimossi dall'elenco di replica non vengono eliminati dal sito di destinazione. Per rimuovere correttamente un oggetto specificato in modo esplicito in un elenco di replica, è necessario eliminarlo sia dal sito di destinazione sia da quello di origine. Gli oggetti che vengono replicati tramite calcoli di dipendenza non vengono eliminati.

## 23.10.2 Limiti dell'eliminazione di oggetti

Nell'oggetto Connessione remota, è possibile definire il numero di oggetti che un processo di replica elimina in una sola operazione. In Federation viene automaticamente rilevato il punto in cui termina il processo di eliminazione. In questo modo, alla successiva esecuzione di un processo di replica, il processo di eliminazione successivo viene avviato da tale punto.

**Suggerimento:**

per completare più rapidamente un processo di replica, limitare il numero di oggetti per ogni eliminazione.

**Esempio:**

I processi di replica A e B replicano l'oggetto A e l'oggetto B. Entrambi gli oggetti vengono replicati dallo stesso sito di origine e utilizzano la stessa connessione remota.

Se il sito di origine elimina l'oggetto B e il limite di oggetti è impostato su 1, alla successiva esecuzione il processo di replica A verificherà se l'oggetto A è stato eliminato. In questo modo, l'oggetto B non viene controllato, né eliminato.

A questo punto, viene eseguito il processo di replica B e viene avviata l'eliminazione di oggetti dal punto in cui è terminato il processo di replica A. Viene controllato se l'oggetto B è stato eliminato e quest'ultimo viene rimosso dal sito di destinazione. Questa opzione è disponibile nella proprietà dell'oggetto Connessione remota "Limitare il numero di oggetti eliminati a:".

**Nota:**

se non si seleziona questa opzione, tutti i processi di replica che utilizzano questa connessione remota controlleranno tutti gli oggetti per l'eventuale eliminazione.

---

### 23.10.3 Frequenza di eliminazione degli oggetti

È possibile impostare la frequenza con la quale un processo di replica esegue l'eliminazione degli oggetti nel campo "Frequenza di eliminazione" della connessione remota.

**Nota:**

è necessario immettere un numero intero positivo che rappresenta il numero di ore di attesa tra le elaborazioni di eliminazione di oggetti.

**Esempio:**

I processi di replica A e B replicano l'oggetto A e l'oggetto B. Entrambi gli oggetti vengono replicati dallo stesso sito di origine e utilizzano la stessa connessione remota.

Se l'oggetto B viene cancellato dal sito di origine e tutte le condizioni seguenti sono vere, il processo di replica verificherà se l'oggetto A è stato cancellato.

- Il Limite oggetto è 1
- La Frequenza di eliminazione è di 150 ore
- Viene eseguito il processo di replica A

Dato che il Limite oggetto è 1, l'oggetto B non verrà controllato o cancellato dal sito di destinazione.

L'eliminazione successiva viene eseguita 150 ore dopo il controllo iniziale effettuato dal processo di replica A. Sebbene sia possibile che i processi di replica A e B vengano eseguiti molte volte prima del limite delle 150 ore, non verranno eseguiti tentativi di eliminazione di oggetti. Trascorse le 150 ore, il processo di replica successivo tenterà di eseguire l'eliminazione, Determina quindi che l'Oggetto B è stato eliminato nel sito di origine e lo elimina quindi nel sito di destinazione.

---

**Abilitazione e disabilitazione delle opzioni**

Ogni processo di replica può partecipare a una eliminazione di oggetti. Tramite l'opzione "Attiva eliminazione oggetto sulla destinazione" in un processo di replica, è possibile indicare se eseguire o meno un'eliminazione di oggetti. In alcuni casi, potrebbero essere presenti processi di replica con priorità elevata che non si desidera partecipino all'eliminazione di oggetti in modo che sia possibile eseguirli con la massima rapidità. A tale scopo, disabilitare l'eliminazione degli oggetti.

**Argomenti correlati**

- [Limiti dell'eliminazione di oggetti](#)

## 23.11 Gestione del rilevamento e della risoluzione dei conflitti

In Federation, si verifica un conflitto quando le proprietà di un oggetto vengono modificate sul sito di origine e sul sito di destinazione. Le proprietà di livello superiore e le proprietà nidificate di un oggetto vengono verificate per rilevare eventuali conflitti. Ad esempio, può verificarsi un conflitto se un report o il nome di un report viene modificato sia sul sito di origine sia su quello di destinazione.

Alcune istanze non creano un conflitto. Ad esempio, se il nome di un report viene modificato nel sito di origine e la descrizione della versione replicata viene modificata nel sito di destinazione, le modifiche si uniscono e non si verificano conflitti.

### 23.11.1 Risoluzione di conflitti di replica unilaterale

Nella replica unilaterale sono disponibili due opzioni per la risoluzione del conflitto.

#### **Precedenza del sito di origine**

Se si verifica un conflitto durante la replica unilaterale, l'oggetto del sito di origine avrà la precedenza. Qualsiasi modifica apportata agli oggetti in un sito di destinazione verrà sovrascritta dalle informazioni del sito di origine. Ad esempio, se un report viene modificato sia sul sito di origine sia su quello di destinazione, le modifiche apportate al sito di destinazione verranno sovrascritte dalla versione del sito di origine dopo il successivo processo di replica.

#### **Nota:**

poiché il conflitto viene risolto automaticamente, non viene generato nel file di registro e non è visualizzato nell'elenco degli oggetti in conflitto.

#### **Nessuna risoluzione conflitti automatica**

Se si verifica un conflitto e si seleziona "Nessuna risoluzione conflitti automatica", il conflitto non viene risolto, non viene generato un file di registro e il conflitto non viene inserito nell'elenco degli oggetti in conflitto.

Gli amministratori possono accedere a un elenco di tutti gli oggetti replicati in conflitto nell'area Federation della CMC. Gli oggetti in conflitto sono raggruppati insieme dalla connessione remota utilizzata per connettersi al sito di origine. Per accedere a questi elenchi, passare alla cartella Errori di replica nell'area Federation della CMC e selezionare la connessione remota desiderata. Tutti gli oggetti replicati in un sito di destinazione verranno contrassegnati da un'icona di replica. Se si verifica un conflitto, gli oggetti verranno contrassegnati da un'icona di conflitto. Nella pagina "Proprietà" viene visualizzato un messaggio di avviso.

**Nota:**

- l'elenco viene aggiornato quando viene completato un processo di replica che utilizza una connessione remota. Contiene tutti gli oggetti in conflitto per tutti i processi di replica che utilizzano la relativa connessione remota specifica.
- qualsiasi utente con accesso alla CMC e alle istanze del processo di replica può accedere al registro XML salvato nella directory del file di registro. L'icona di un oggetto del sito di destinazione è contrassegnata per indicare un conflitto. Durante l'elaborazione, viene creato un registro dei conflitti.

Giorgio modifica il Report A nel sito di origine. Maria modifica la versione replicata nel sito di destinazione. Alla successiva esecuzione del processo di replica, il report sarà in conflitto poiché è stato modificato in entrambi i siti e non verrà risolto il conflitto.

Il report di destinazione viene mantenuto e le modifiche apportate al report di origine non vengono replicate. Lo stesso vale per i processi di replica successivi finché non verrà risolto il conflitto. Qualsiasi modifica apportata nel sito di origine non viene replicata finché il conflitto non viene risolto manualmente.

**Nota:**

in questo caso, non viene replicato l'intero oggetto. Le altre modifiche che potrebbero non essere in conflitto non vengono replicate.

Per risolvere manualmente un conflitto sono disponibili tre opzioni:

1. Creare un processo di replica per la replica dei soli oggetti in conflitto. Deve utilizzare lo stesso oggetto connessione remota e lo stesso elenco di replica.

Per mantenere le modifiche del sito di origine, creare un processo di replica. Impostare Modalità replica su "Aggiorna da origine" e Risoluzione conflitti automatica su "Precedenza del sito di origine."

Per mantenere le modifiche del sito di destinazione, creare un processo di replica con Tipo di replica = "Replica bilaterale", Modalità replica = "Aggiorna da destinazione" e Risoluzione conflitti automatica = "Precedenza del sito di destinazione."

**Nota:**

in Modalità replica, impostare "Aggiorna da origine" o "Aggiorna da destinazione" per selezionare solo gli oggetti in conflitto nell'elenco di replica. In questo modo gli altri oggetti non vengono replicati. Successivamente, pianificare l'esecuzione del processo di replica. Verranno replicati gli oggetti selezionati e risolto il conflitto nel modo specificato.

2. Creare un processo di replica per la replica dei soli oggetti in conflitto. Deve utilizzare lo stesso oggetto connessione remota. A differenza dell'opzione 1, tuttavia, è possibile creare un nuovo elenco di replica nel sito di origine. Utilizzare solo gli oggetti in conflitto e creare un nuovo processo di replica che utilizzi questo elenco di replica.

Per mantenere le modifiche del sito di origine, impostare Risoluzione conflitti automatica su "Precedenza del sito di origine."

Per mantenere le modifiche del sito di destinazione, impostare Risoluzione conflitti automatica su "Precedenza del sito di destinazione" e Tipo di replica su "Replica bilaterale."

3. Per processi di replica unilaterale, è possibile eliminare l'oggetto sul sito di destinazione. Alla successiva esecuzione del processo di replica, verrà replicato l'oggetto dal sito di origine al sito di destinazione.



**Nota:**

quando si elimina un oggetto occorre prestare attenzione poiché è possibile che altri oggetti che dipendono dall'oggetto eliminato vengano rimossi, smettano di funzionare o perdano la protezione. Sono consigliate le opzioni 1 e 2.

### **23.11.2 Risoluzione conflitti di replica bilaterale**

Per la replica bilaterale sono disponibili tre opzioni per rilevare i conflitti:

- Precedenza del sito di origine
- Precedenza del sito di destinazione
- Nessuna risoluzione conflitti automatica

**Precedenza del sito di origine**

Se si verifica un conflitto, il sito di origine avrà la precedenza e sovrascriverà qualsiasi modifica apportata al sito di destinazione.

**Esempio:**

Liliana modifica il nome di un report in Report A. Mario modifica il nome della versione replicata nel sito di destinazione in Report B. Dopo l'esecuzione del successivo processo di replica, la versione replicata nel sito di destinazione verrà rinominata Report A.

Non verrà generato alcun conflitto nel file di registro e non vi sarà segnalazione nell'elenco degli oggetti in conflitto perché il conflitto è stato risolto secondo le istruzioni dell'utente nel sito di origine.

---

**Precedenza del sito di destinazione**

Se si verifica un conflitto, il sito di destinazione manterrà le modifiche e le sovrascriverà nel sito di origine.

**Esempio:**

Giacomo modifica il nome di un report in Report A. Pietro modifica il nome della versione replicata nel sito di destinazione in Report B. Quando si esegue il processo di replica, viene rilevato un conflitto. Il nome del report di destinazione resta Report B.

Nella replica bilaterale, le modifiche vengono reinviare al sito di origine. In questo scenario, il sito di origine viene aggiornato e il nome del report viene modificato in Report B. Non verrà generato alcun conflitto nel file di registro e non vi sarà segnalazione nell'elenco degli oggetti perché il conflitto è stato risolto secondo le istruzioni dell'utente.

---

**Nessuna risoluzione conflitti automatica**

Quando si seleziona "Nessuna risoluzione conflitti automatica", il conflitto non verrà risolto. Il conflitto verrà segnalato in un file di registro per l'amministratore che potrà risolverlo manualmente.

**Nota:**

- l'icona di un oggetto viene contrassegnata per indicare un conflitto.
- sebbene le modifiche vengano replicate sia nel sito di origine sia in quello di destinazione nella replica bilaterale, solo le versioni del sito di destinazione verranno contrassegnate da un'icona di conflitto.

**Nota:**

qualsiasi utente con accesso alla CMC e alle istanze del processo di replica può accedere al registro XML creato nella directory del file di registro. L'icona di un oggetto del sito di destinazione è contrassegnata per indicare un conflitto. Durante l'elaborazione, viene creato un registro dei conflitti.

L'amministratore può accedere a un elenco di tutti gli oggetti replicati in conflitto nell'area Federation della Central Management Console (CMC). Gli oggetti in conflitto sono raggruppati insieme dalla connessione remota utilizzata per connettersi al sito di origine. Per accedere a questi elenchi, andare a **CMC > Federation > Errori di replica > Connessione remota**.

**Nota:**

l'elenco viene aggiornato quando viene completato un processo di replica che utilizza una connessione remota. Contiene tutti gli oggetti in conflitto per tutti i processi di replica che utilizzano la relativa connessione remota specifica. Tutti gli oggetti replicati in un sito di destinazione verranno contrassegnati da un'icona di replica. Se si verifica un conflitto, gli oggetti verranno contrassegnati da un'icona di conflitto.

**Esempio:**

Michele modifica il Report A nel sito di origine. Daniele modifica la versione replicata nel sito di destinazione. Alla successiva esecuzione del processo di replica, il report sarà in conflitto poiché è stato modificato in entrambi i siti e non verrà risolto il conflitto.

Il report di destinazione viene mantenuto e le modifiche apportate al report di origine non vengono replicate. Lo stesso vale per i processi di replica successivi finché non verrà risolto il conflitto. Qualsiasi modifica del sito di origine non verrà replicata finché il conflitto non verrà risolto manualmente dall'amministratore o dall'amministratore con delega.

**Nota:**

- in questo caso, non viene replicato l'intero oggetto. Le altre modifiche non in conflitto non vengono replicate.
- qualsiasi utente con accesso alla CMC e alle istanze del processo di replica può accedere al registro XML creato nella directory del file di registro. L'icona di un oggetto del sito di destinazione è contrassegnata per indicare un conflitto. Durante l'elaborazione, viene creato un registro dei conflitti.

L'amministratore può accedere a un elenco di tutti gli oggetti replicati in conflitto nell'area Federation della Central Management Console (CMC). Gli oggetti in conflitto sono raggruppati insieme dalla connessione remota utilizzata per connettersi al sito di origine. Per accedere a questi elenchi, andare a **CMC > Federation > Errori di replica > Connessione remota**.

**Nota:**

l'elenco viene aggiornato quando viene completato un processo di replica che utilizza una connessione remota. Contiene tutti gli oggetti in conflitto per tutti i processi di replica che utilizzano la relativa

connessione remota specifica. Tutti gli oggetti replicati in un sito di destinazione verranno contrassegnati da un'icona di replica. Se si verifica un conflitto, gli oggetti verranno contrassegnati da un'icona di conflitto.

---

Per risolvere manualmente un conflitto sono disponibili tre opzioni:

1. Creare un processo di replica per la replica dei soli oggetti in conflitto. Deve utilizzare lo stesso oggetto connessione remota e lo stesso elenco di replica.

Per mantenere le modifiche del sito di origine, creare un processo di replica. Impostare Modalità replica su "Aggiorna da origine" e impostare Risoluzione conflitti automatica su "Precedenza del sito di origine".

Per mantenere le modifiche del sito di destinazione, creare un processo di replica e impostare Tipo di replica su "Replica bilaterale", Modalità replica su "Aggiorna da destinazione" e Risoluzione conflitti automatica su "Precedenza del sito di destinazione."

**Nota:**

in Modalità replica, impostare "Aggiorna da origine" o "Aggiorna da destinazione" per selezionare solo gli oggetti in conflitto nell'elenco di replica. In questo modo gli altri oggetti non vengono replicati. Successivamente, pianificare l'esecuzione del processo di replica. Verranno replicati gli oggetti selezionati e risolto il conflitto nel modo specificato.

2. Creare un processo di replica per la replica dei soli oggetti in conflitto. Deve utilizzare lo stesso oggetto connessione remota. A differenza dell'opzione 1, tuttavia, è possibile creare un nuovo elenco di replica nel sito di origine. Utilizzare solo gli oggetti in conflitto e creare un nuovo processo di replica che utilizzi questo elenco di replica.

Per mantenere le modifiche del sito di origine, impostare Risoluzione conflitti automatica su "Precedenza del sito di origine."

Per mantenere le modifiche del sito di destinazione, impostare Risoluzione conflitti automatica su "Precedenza del sito di destinazione" e Tipo di replica su "Replica bilaterale".

3. Eliminare l'oggetto dal sito in cui non si desidera posizionarlo.

**Nota:**

quando si elimina un oggetto occorre prestare attenzione poiché è possibile che altri oggetti che dipendono dall'oggetto eliminato vengano rimossi, smettano di funzionare o perdano la protezione. Sono consigliate le opzioni 1 e 2.

Per mantenere le modifiche del sito di destinazione, è possibile eliminare l'oggetto nel sito di origine. Alla successiva esecuzione del processo di replica, verrà replicato l'oggetto dal sito di destinazione a quello di origine.

**Nota:**

prestare attenzione nell'eliminare una copia dal sito di origine poiché altri siti di destinazione che replicano tale oggetto potrebbero eseguire il processo di replica prima che la copia sia stata nuovamente replicata. In questo caso, gli altri siti di destinazione eliminerebbero la rispettiva copia che non sarebbe più disponibile fino alla restituzione della copia.

Per mantenere le modifiche del sito di origine, è possibile eliminare l'oggetto nel sito di destinazione.

## 23.12 Utilizzo dei Servizi Web in Federation

Federation utilizza Servizi Web per inviare oggetti e relative modifiche tra il sito di origine e i siti di destinazione. I servizi Web specifici di Federation vengono automaticamente installati e distribuiti nell'installazione della piattaforma BI. Può tuttavia essere utile modificare le proprietà o personalizzare le distribuzioni di Servizi Web per migliorare le funzionalità, come illustrato in questa sezione.

### **Suggerimento:**

per migliorare la funzionalità e la gestione dei file, abilitare la memorizzazione dei file nella cache in Federation.

### 23.12.1 Variabili di sessione

Se si trasferiscono molti file di contenuto in un processo di replica, può essere utile aumentare il periodo di timeout della sessione dei Servizi Web di Federation.

La proprietà si trova nel file `dsws.properties`:

*Directory di installazione server applicazioni\dswebobje\Web-INF\classes*

Ad esempio:

```
C:\Programmi\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswebobje\WEB-INF\classes
```

Per attivare una variabile di sessione, immettere:

```
session.timeout = x
```

Dove “x” è il tempo desiderato, “x” è misurato in secondi. Se non viene specificato, il valore predefinito è 1200 secondi o 20 minuti.

Le nuove proprietà hanno effetto solo dopo la ridistribuzione dell'applicazione Web modificata nel computer su cui è in esecuzione il server di applicazioni Web. Utilizzare WDeploy per ridistribuire il file WAR sul server di applicazioni Web. Per ulteriori informazioni sull'utilizzo di WDeploy, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

### 23.12.2 Memorizzazione di file nella cache

la memorizzazione di file nella cache consente ai Servizi Web di gestire allegati di grandi dimensioni senza memorizzarli nel buffer di memoria. Se non viene abilitata durante i trasferimenti di file di grandi dimensioni, è possibile che venga utilizzata tutta la memoria di Java Virtual Machine e che la replica non riesca.

**Nota:**

La memorizzazione di file nella cache incide negativamente sulle prestazioni poiché l'elaborazione di Servizi Web viene effettuata nei file anziché in memoria. È possibile utilizzare una combinazione di entrambe le opzioni e inviare trasferimenti di grandi dimensioni in un file e quelli più piccoli in memoria.

Per abilitare la memorizzazione di file nella cache, modificare il file `Axix2.xml` che si trova in:

*Directory di installazione server applicazioni\dswsbobje\Web-Inf\conf*

Ad esempio:

`C:\Programmi\SAP BusinessObjects\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`

Immettere quanto segue:

`<parameter name="allegatiCache" locked="false">true</parameter>`

`<parameter name="DIRallegati" locked="false">temp directory</parameter>`

`<parameter name="sogliaDimensioni" locked="false">4000</parameter>`

**Nota:**

le dimensioni di soglia sono espresse in byte.

Le nuove proprietà hanno effetto solo dopo la ridistribuzione dell'applicazione Web modificata nel computer su cui è in esecuzione il server di applicazioni Web. Utilizzare WDeploy per ridistribuire il file WAR sul server di applicazioni Web. Per ulteriori informazioni sull'utilizzo di WDeploy, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

### 23.12.3 Distribuzione personalizzata

I servizi Web di Federation possono essere distribuiti automaticamente e richiedono i servizi “federation”, “biplatform” e “session” per essere attivati. Per disattivare Federation o qualsiasi altro servizio Web, modificare il file `service.xml` corrispondente dei servizi Web.

I servizi Web della piattaforma BI si trovano in:

*Directory di installazione server applicazioni\dswsbobje\WEB-INF\services*

Esempio:

`C:\Programmi\SAP BusinessObjects\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps\dswsbobje\WEB-INF\services`

Per disattivare i Servizi Web:

- aggiungere la proprietà "activate" nel tag del nome del servizio nel file `service.xml` e impostarla su false.
- riavviare il server delle applicazioni Java.

Ad esempio, per disabilitare Federation:

Il file `services.xml` si trova in:

```
C:\Programmi\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\war
files\webapps\dswebobje\WEB-INF\services\federator\META-INF
```

Modificare il nome del servizio da:

```
<service name="Federator">
```

A:

```
<service name="Federator" activate="false">
```

Le nuove proprietà hanno effetto solo dopo la ridistribuzione dell'applicazione Web modificata nel computer su cui è in esecuzione il server di applicazioni Web. Utilizzare WDeploy per ridistribuire il file WAR sul server di applicazioni Web. Per ulteriori informazioni sull'utilizzo di WDeploy, consultare il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

## 23.13 Pianificazione remota e istanze eseguite localmente

In questa sezione vengono descritte la pianificazione remota, le istanze eseguite localmente e la condivisione delle istanze. Queste funzionalità consentono l'esecuzione dei report dove risiedono i dati e al termine inviano le istanze alle posizioni appropriate.

### 23.13.1 Pianificazione remota

Con Federation, è possibile pianificare un report nel sito di destinazione ed elaborarlo nel sito di origine. L'istanza completa verrà restituita al sito di destinazione.

Per abilitare la pianificazione remota, pianificare un report nel modo consueto e abilitare l'opzione "Esegui su sito di origine". Per abilitare questa opzione, fare clic su **Pianificazione > Pianificazione gruppo di server > Esegui su sito di origine**. Dopo la creazione, lo stato delle istanze pianificate è in sospeso.

Durante la pianificazione remota, le informazioni inviate al sito di destinazione vengono ignorate e l'istanza del report rimane in sospeso.

Quando il processo di replica successivo che gestisce il report viene abilitato per la pianificazione remota, l'istanza viene copiata nel sito di origine per l'elaborazione. L'istanza rimane in attesa finché non viene elaborata dallo Scheduler. Nel frattempo, il processo di replica che l'ha inviata restituirà eventuali istanze completate in precedenza e le modifiche apportate agli oggetti.

Una volta che l'istanza è stata elaborata nel sito di origine, passa allo stato completato. Quando il processo di replica successivo che gestisce il report viene abilitato per le pianificazioni remote, l'istanza completata verrà utilizzata per aggiornare la copia nel sito di destinazione. Dopo essere stata aggiornata, l'istanza nel sito di destinazione è completata.

**Nota:**

è necessario che un processo di replica venga eseguito due volte per restituire un'istanza completa.

**Esempio:**

1. Giovanni pianifica il Report A per la pianificazione remota.
2. Il Report A viene creato nel sito di destinazione e si trova nello stato In sospeso.
3. Viene eseguito il Processo di replica A. Vengono innanzitutto replicate le modifiche dal sito di origine a quello di destinazione, incluse le istanze completate in precedenza. In seguito, viene copiata l'istanza nello stato In sospeso nel sito di origine e vengono copiate le modifiche da replicare dal sito di destinazione a quello di origine.
4. Lo Scheduler del sito di origine seleziona l'istanza nello stato In sospeso e la invia al Job Server appropriato affinché venga elaborata. L'istanza viene quindi elaborata e impostata sullo stato Completato nel sito di origine.
5. Viene di nuovo eseguito il processo di replica A. Quando il contenuto viene replicato dal sito di origine al sito di destinazione, l'istanza completata del Report A viene selezionata e le modifiche vengono applicate alla versione della destinazione.
6. Al termine di questa attività, la versione di destinazione è completa.

---

La pianificazione remota funziona solamente con un processo di replica bilaterale ed è necessario abilitare "Replica pianificazioni remote". Questa opzione è disponibile nella pagina "Proprietà processo di replica" nell'area "Filtri di replica". In alcuni scenari, può essere opportuno replicare in modalità remota processi di pianificazione più frequentemente rispetto ad altri oggetti presenti nell'elenco di replica. A tale scopo, creare due processi di replica. Abilitarne uno con "Replica pianificazioni remote" per un processo di replica riguardante unicamente la pianificazione remota. Abilitare l'altro con "Replica modelli documento" o "Replica tutti gli oggetti (nessun filtro)".

**Nota:**

quando si abilita la pianificazione remota, le istanze completate e non riuscite vengono visualizzate sia nel sito di origine sia in quello di destinazione.

Se un utente nel sito di destinazione pianifica un report per la pianificazione remota e nel sito di origine l'utente non esiste, l'istanza avrà esito negativo nel sito di origine. Il proprietario dell'istanza non riuscirà a essere l'account utente dell'oggetto connessione remota utilizzato per la connessione all'origine.

Sebbene sia possibile configurare un processo di replica solo per la pianificazione remota, gli oggetti antenati dell'istanza del report vengono sempre replicati. Ciò significa che se esistono modifiche tra le repliche, il report effettivo, la cartella dei report e così via vengono sempre replicati. Se si desidera che queste modifiche nel sito di destinazione non vengano replicate nel sito di origine, è possibile utilizzare i diritti di protezione per controllare quali modifiche vengono replicate.

**Argomenti correlati**

- [Gestione dei diritti di protezione](#)

### 23.13.2 Istanze eseguite localmente

Le istanze eseguite localmente sono istanze di un report elaborate dai report nel sito di destinazione. Con Federation, è possibile replicare le istanze completate dal sito di destinazione a quello di origine.

Per consentire a un processo di replica di replicare le istanze completate e quelle non riuscite dal sito di destinazione a quello di origine, fare clic su **Proprietà processo di replica > Filtri di replica > Replica istanze completate eseguite localmente**.

In alcuni casi, potrebbe essere opportuno che un processo di replica replichi solo le istanze eseguite localmente. A tale scopo, abilitare “Replica istanze completate eseguite localmente”.

**Nota:**

quando si abilita l'opzione Istanze eseguite localmente in un processo di replica, le istanze completate e quelle non riuscite verranno entrambe replicate nel sito di origine. In questo modo le copie saranno presenti sia nel sito di origine sia in quello di destinazione.

Le istanze in sospeso non vengono mai replicate.

Se il proprietario di un'istanza eseguita localmente non esiste nel sito di origine, il proprietario sarà l'account utente utilizzato per la connessione nell'oggetto connessione remota.

### 23.13.3 Condivisione di istanze

Quando si abilitano la pianificazione remota e le istanze eseguite localmente in un processo di replica, è possibile che si verifichi la condivisione di istanze se un sito di origine dispone di più siti di destinazione che replicano lo stesso report.

**Esempio:**

Il Report A ha origine nel sito di origine e viene replicato nei siti di destinazione A e B. La condivisione di istanze ha luogo in entrambi i siti di destinazione:

- Processi di replica attivati con “Replica pianificazioni remote” e/o “Replica istanze completate eseguite localmente”. Replicare il Report A con lo stesso processo di replica indicato sopra
- Pianificare il Report A nel sito di destinazione per “essere eseguito nel sito di origine” e/o localmente

Se entrambi i siti di destinazione A e B replicano il Report A e i processi di replica corrispondenti replicano le pianificazioni remote e/o le istanze eseguite localmente, qualsiasi istanza elaborata nel



sito di destinazione A e/o nel sito di origine per conto del sito di destinazione A verrà condivisa nel sito di destinazione B.

Analogamente, qualsiasi istanza elaborata nel sito di destinazione B e/o nel sito di origine verrà anche condivisa nel sito di destinazione A. Di conseguenza, il sito di origine e i siti di destinazione A e B avranno un insieme identico di istanze.

---

La condivisione di istanze è ottimale in molti casi. Ad esempio quando gli utenti di altri siti hanno esigenza di accedere a informazioni da distribuzioni di pari livello. In questo caso, per evitare che le istanze vengano visualizzate dagli utenti nel sito locale, accertarsi che i diritti di protezione appropriati siano impostati. Ad esempio, in un oggetto report è possibile applicare i diritti in modo che gli utenti possano vedere solo le istanze di cui sono proprietari.

**Nota:**

tutti gli oggetti seguono le regole di protezione della piattaforma BI. Per assicurarsi che gli utenti e i gruppi possano visualizzare solo le istanze previste, è consigliabile impostare i diritti in modo che possano visualizzare solo le istanze di loro proprietà. Ad esempio, in un oggetto report è possibile applicare i diritti in modo che gli utenti possano vedere solo le istanze di cui sono proprietari.

**Argomenti correlati**

- [Gestione dei diritti di protezione](#)

## **23.14 Importazione e promozione di contenuto replicato**

In alcuni casi è possibile scegliere di importare o promuovere il contenuto replicato da una piattaforma BI a un'altra. In questa sezione vengono illustrate queste funzionalità in Federation.

**Nota:**

le migrazioni di oggetti vengono eseguite al meglio da membri del gruppo Amministratori, in particolare dall'account utente Administrator. La migrazione di un oggetto potrebbe implicare la migrazione anche di molti oggetti correlati. Un account amministratore delegato potrebbe non ottenere i diritti di protezione richiesti per tutti gli oggetti.

### **23.14.1 Importazione di contenuto replicato**

Se si utilizza LifeCycle Manager per importare il contenuto da una distribuzione della piattaforma BI a un'altra, LifeCycle Manager non importerà alcuna informazione specifica di replica associata agli oggetti replicati in fase di importazione. In questo modo, dopo l'importazione, l'oggetto agirà come se non fosse mai stato replicato. Questa condizione è specifica degli oggetti replicati nel sito di destinazione è descritta nello scenario seguente.

**Esempio:**

La piattaforma BI A è un sito di destinazione in un processo di Federation. Il Report A, un report replicato sul Sistema A, viene importato dal Sistema A alla piattaforma BI B mediante LifeCycle Manager.

Risultato: quando il Report A viene copiato nella piattaforma BI B non contiene alcuna informazione replicata. Il Report A non è più contrassegnato con l'icona di replica. Se l'oggetto era in conflitto nella piattaforma BI A non sarà in conflitto nel Sistema B. Verrà sostanzialmente trattato come un oggetto originato dal Sistema B.

**Nota:**

è possibile che il CUID sia lo stesso oppure no, in base alle opzioni di importazione selezionate in LifeCycle Manager.

---

### 23.14.2 Importazione del contenuto replicato e continuazione della replica

Dopo avere importato il contenuto replicato, può essere utile includere gli oggetti importati in un processo di Federation. Gli scenari possibili sono due: trattare come sito di origine o come sito di destinazione il sistema in cui risiedono gli oggetti importati. Per trattare tale sistema come sito di origine, eseguire la normale procedura di Federation.

Per trattare il sistema come sito di destinazione e replicare gli oggetti importati come sito di origine, è necessario:

- Assicurarci che il CUID degli oggetti venga mantenuto quando si utilizza LifeCycle Manager.
- Assicurarci che per il primo processo di replica la risoluzione dei conflitti sia impostata su "Risoluzione conflitti a favore del sito di origine" o su "Risoluzione conflitti a favore del sito di destinazione."

**Suggerimento:**

anziché importare l'oggetto da un sito di destinazione all'altro tramite LifeCycle Manager, è consigliabile e più efficiente utilizzare solo Federation per replicare l'oggetto.

**Esempio:**

Il Report A è stato creato nel Sistema A della piattaforma BI. Il Sistema X ha utilizzato Federation per replicare il Report A dal Sistema A al Sistema X. Il Report A è stato quindi importato tramite LifeCycle Manager dal Sistema X al Sistema Y.

Piano: il Sistema Y desidera impostare Federation sul Sistema A e mantenere il Report A come parte della replica. Il Sistema Y è la destinazione e il Sistema A è l'origine.

Azione: quando si importa il Report A dal Sistema X al Sistema Y, il CUID del Report A deve essere mantenuto. Inoltre, quando viene eseguito, il primo processo di replica tenta di replicare il Report A. Poiché l'oggetto esiste già nel Sistema Y, la replica genera un conflitto. Per specificare quale versione utilizzare, è necessario impostare la modalità Risoluzione conflitti su "Risoluzione conflitti a favore del sito di origine" o "Risoluzione conflitti a favore del sito di destinazione".

**Nota:**

in questo esempio, anziché importare l'oggetto utilizzando LifeCycle Manager da un sito di destinazione a un altro, è consigliabile utilizzare solo Federation per replicare l'oggetto. Il Report A verrà replicato dal Sistema A al Sistema Y e non occorrerà utilizzare LifeCycle Manager per l'importazione dal Sistema X al Sistema Y.

---

### 23.14.3 Promozione del contenuto da un ambiente di test

In qualsiasi organizzazione, i test vengono spesso eseguiti prima della distribuzione di un componente all'ambiente di produzione. È normale testare Federation tra i sistemi della piattaforma BI in un ambiente di sviluppo o di test prima dell'installazione nei computer del reparto produzione. Una volta creati i siti di origine e di destinazione e il contenuto in un ambiente di test, è possibile promuovere questa configurazione ai computer del reparto produzione effettuando i seguenti passaggi:

1. Utilizzare LifeCycle Manager per promuovere il contenuto dal sito di origine dell'ambiente di test al computer del reparto produzione che avrà al funzione di sito di origine.

**Nota:**

l'oggetto dell'elenco di replica non è selezionabile quando si utilizza LifeCycle Manager.

2. Creare l'elenco di replica nel sito di origine dell'ambiente di produzione e includere il contenuto desiderato.
3. Scegliere tra le due seguenti opzioni:
  - A) Creare un oggetto connessione remota e i processi di replica appropriati nei computer di produzione che avranno la funzione di siti di destinazione.
  - B) Utilizzare LifeCycle Manager per importare la connessione remota e i processi di replica dal sito di destinazione in Dev/QA ai computer di produzione che avranno la funzione di siti di destinazione. Modificare quindi le connessioni remote importate affinché puntino al computer nel reparto produzione con funzione di sito di origine.

### 23.14.4 Puntamento a un sito di destinazione

Attualmente, dopo essere stato replicato da un sito di origine, un oggetto deve sempre essere replicato da quella origine e non può essere replicato da un'altra piattaforma BI. Se l'oggetto connessione remota viene modificato in modo da fare riferimento a un nuovo sistema, qualsiasi tentativo di replicare un oggetto replicato da un altro sistema della piattaforma BI che non sia l'oggetto connessione remota avrà esito negativo. Per replicare un oggetto da un sito di origine diverso, è necessario eliminarlo prima dal sito di destinazione.

**Nota:**

una volta copiato un oggetto replicato, il CUID della copia verrà modificato e la copia non conterrà alcuna informazione di replica.

## 23.15 Procedure consigliate

È possibile utilizzare Federation per ottimizzare le prestazioni di un processo di replica.

Se in un unico processo di replica è presente un numero elevato di oggetti, è possibile eseguire ulteriori passaggi per assicurarsi che il processo venga eseguito correttamente. In genere, dovrebbe essere possibile replicare fino a 32.000 oggetti in ciascun processo di replica. Tuttavia, alcune distribuzioni potrebbero richiedere configurazioni con repliche di dimensioni maggiori o minori.

### 1) Ottenere un fornitore di servizi Web dedicato

In Federation, il contenuto replicato viene inviato tramite servizi Web. In un'installazione predefinita della piattaforma BI tutti i servizi Web utilizzano lo stesso provider di servizi Web. Ciò significa che i processi di replica di dimensioni maggiori potrebbero richiedere un utilizzo prolungato del provider di servizi Web e rallentare le risposte ad altre richieste di servizi Web nonché ad altre applicazioni.

Se viene pianificata la replica di un numero elevato di oggetti o l'esecuzione in sequenza di più processi di replica, considerare la distribuzione dei servizi Web di Federation sul server di applicazioni Java utilizzando il proprio fornitore di servizi Web.

Per eseguire questa operazione, utilizzare il programma di installazione della piattaforma BI per installare i servizi Web. Java Application Server deve essere già in esecuzione. In caso contrario, installare l'opzione completa Componenti di livello Web che installerà i servizi Web e Tomcat.

**Nota:**

- è necessario fornire informazioni relative a un CMS esistente (ad esempio nome host, porta e password dell'amministratore).
- è necessario utilizzare l'URI di questo nuovo fornitore di servizi Web nel campo URI della connessione remota.

### 2) Aumentare la memoria disponibile di Java Application Server

Aumentare la memoria disponibile del server di applicazioni Java se il singolo processo di replica esegue la replica di più oggetti o se il server di applicazioni viene condiviso con altre applicazioni.

Se la piattaforma BI e Tomcat sono stati distribuiti, la memoria disponibile predefinita è 1 GB. Per aumentare la memoria disponibile per Tomcat:

In Windows:

1. Fare clic sul pulsante **Start > Programmi > Tomcat > Configurazione di Tomcat**.
2. Selezionare **Java**.
3. Nella casella **Opzioni Java**, individuare `-Xmx1024M`
4. Impostare `-Xmx1024M` sul valore desiderato.

**Esempio:**

Per aumentare la memoria fino a 2GB, immettere: `-Xmx2048M`

---

In Unix:

1. In `<DIR_INSTALL_BOE>/setup/`, aprire `env.sh` con l'editor di testo desiderato. Impostare il parametro `-Xmx1024m` sul valore desiderato.
2. Individuare le seguenti righe

```
if [-d "$BOBJEDIR"/tomcat]; then
set the JAVA_OPTS for Tomcat
JAVA_OPTS="-Dbojbj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"

if ["$SOFTWARE" = "AIX" -o "$SOFTWARE" =
"SunOS" -o "$SOFTWARE" = "Linux"];
then
 JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
fi
export JAVA_OPTS
fi
```

3. Impostare il parametro `-Xmx1024m` sul valore desiderato.

**Esempio:**

Per aumentare la memoria fino a 2GB, immettere: `-Xmx2048m`

---

**Suggerimento:**

per altri server di applicazioni Java, consultare la relativa documentazione per aumentare la memoria disponibile.

- 3) Ridurre le dimensioni dei file BIAR creati.

Federation utilizza i Servizi Web per replicare il contenuto tra il sito di origine e quello di destinazione. Gli oggetti vengono raggruppati insieme e compressi in file BIAR affinché possano essere più facilmente trasportati.

Quando si replica un numero elevato di oggetti, configurare il server di applicazioni Java per creare file BIAR di dimensioni ridotte. Federation raggrupperà e comprimerà oggetti tra più file BIAR di dimensioni ridotte affinché il numero di oggetti da replicare non venga limitato.

Per ridurre le dimensioni dei file BIAR creati, aggiungere i seguenti parametri Java al server di applicazioni Java:

```
Dbojbj.biar.suggestSplit
and
Dbojbj.biar.forceSplit
```

`bojbj.biar.suggestSplit` suggerisce una dimensione appropriata per il file BIAR, che cercherà di raggiungere e mantenere. Il nuovo valore suggerito è 90 MB.

`bojbj.biar.forceSplit` obbligherà un file BIAR ad arrestarsi una volta raggiunta una determinata dimensione. Il nuovo valore suggerito è 100 MB.

**Nota:**

non è necessario modificare le impostazioni della dimensione dei file BIAR a meno che il server di applicazioni non esaurisca la memoria e la dimensione heap massima non possa essere ulteriormente aumentata.

Per Tomcat Windows:

1. Per aprire lo strumento **Configurazione Tomcat** fare clic su **Start > Programmi > Tomcat > Configurazione Tomcat**.
2. Selezionare **Java**.
3. Nella casella **Opzioni Java** aggiungere alla fine le seguenti righe:

```
-Dbobj.biar.suggestSplit=90
-Dobj.biar.forceSplit=100
```

Per Tomcat Unix/Linux:

1. Aprire env.sh con l'editor di testo preferito. Si trova in <DIR\_INSTALL\_BOE>/setup/
2. Individuare le seguenti righe:

```
if [-d "$BOBJEDIR"/tomcat]; then
set the JAVA_OPTS for tomcat
JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120 -Djava.awt.headless=true"

if ["$SOFTWARE" = "AIX" -o "$SOFTWARE" = "SunOS" -o "$SOFTWARE" = "Linux"]; then
 JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
fi
export JAVA_OPTS
fi
```

Aggiungere i parametri relativi alla dimensione dei file BIAR desiderati.

Esempio: JAVA\_OPTS="\$JAVA\_OPTS -Xmx1024m -XX:MaxPermSize=256m  
-Dbobj.biar.suggestSplit=90 -Dbobj.biar.forceSplit=100"

Per altri server di applicazioni Java, consultare la documentazione per aggiungere proprietà di sistema Java.

- 4) Aumentare il timeout del socket.

Adaptive Job Server è responsabile dell'esecuzione del processo di replica. Durante l'esecuzione del processo di replica, Adaptive Job Server stabilisce una connessione al sito di origine. Quando si ricevono grandi quantità di informazioni dal sito di origine, è importante che il socket utilizzato da Adaptive Job Server per ricevere informazioni non scada.

Il valore predefinito è 90 minuti. Se necessario, è possibile aumentare il timeout del socket.

Per aumentare il timeout del socket in Adaptive Job Server:

1. Aprire Central Management Console (CMC)
2. Spostarsi nella sezione **Server** e selezionare **Adaptive Job Server**.
3. Fare clic su **Proprietà**.
4. Aggiungere "Parametri riga di comando" alla fine di:
  - Windows: -javaArgs Xmx1000m,Xincgc,server,Dbobj.federation.WSTimeout=<timeout in minuti>
  - Unix: -javaArgs Xmx512m,Dbobj.federation.WSTimeout=<timeout in minuti>

**Argomenti correlati**

- [Risoluzione dei messaggi di errore](#)
- [Utilizzo dei Servizi Web in Federation](#)
- [Limitazioni della release corrente](#)

**23.15.1 Limitazioni della release corrente**

Benché Federation sia uno strumento flessibile, è possibile che alcune limitazioni influiscano sulle prestazioni durante la produzione. In questa sezione vengono evidenziate aree modificabili per ottimizzare le operazioni di Federation.

- Numero massimo di oggetti

Ogni processo di replica esegue la replica di oggetti tra le distribuzioni della piattaforma BI. È consigliabile che il numero massimo di oggetti replicati in un singolo processo di replica venga stabilito a 100.000. Sebbene un processo di replica possa funzionare con più di 100.000 oggetti, Federation supporta unicamente la replica di non più di 100.000 oggetti.

- Diritti

In Federation, i diritti vengono replicati solo dal sito di origine a quello di destinazione. È consigliabile che i diritti utente comuni a entrambe le distribuzioni vengano impostati sul sito di origine e replicati su quelli di destinazione utilizzando la replica bilaterale. I diritti utente per un sito specifico verranno amministrati come di consueto in una distribuzione della piattaforma BI nel sito in cui risiedono gli utenti.

- Viste aziendali e oggetti associati

La piattaforma BI può archiviare viste aziendali, elementi aziendali, basi dati, connessioni dati ed elenchi di valori. Questi oggetti vengono utilizzati per migliorare la funzionalità Crystal Reports.

Se questi oggetti vengono creati prima nel sito di destinazione e quindi replicati nel sito di origine utilizzando la replica bilaterale, potrebbero non funzionare correttamente e i dati potrebbero non essere visualizzati in Crystal Reports.

È consigliabile creare viste aziendali, elementi aziendali, basi dati, connessioni dati ed elenchi di valori sul sito di origine e quindi replicarli nel sito di destinazione. Effettuare gli aggiornamenti sugli oggetti nel sito di destinazione o in quello di origine, diritti permettendo, e le modifiche verranno replicate bilateralmente nel modo appropriato.

- Overload di universi

La piattaforma BI è in grado di archiviare overload di universi. Se vengono creati overload di universi nel sito di destinazione e quindi replicati in quello di origine utilizzando la replica bilaterale, è possibile che si verifichino degli errori.

Per risolvere questo problema, creare innanzitutto gli overload di universi nel sito di origine e replicarli nel sito di destinazione. Successivamente, impostare la protezione sugli overload di universi nel sito di origine e replicarli nel sito di destinazione.

- Eliminazione oggetto

Vengono eliminati gli oggetti che sono stati eliminati sull'altro sito. L'eliminazione degli oggetti viene attualmente eseguita unicamente dal sito di origine al sito di destinazione.

- File di registro di Federation

I file di registro di Federation sono scritti in file XML basati sugli standard XML 1.1. Per visualizzare i file di registro in un browser, è necessario che il browser supporti XML 1.1.

### **Argomenti correlati**

- [Gestione dell'eliminazione di oggetti](#)

## **23.15.2 Risoluzione dei messaggi di errore**

In questa sezione sono contenuti i messaggi di errore che possono venire visualizzati in rare circostanze durante l'utilizzo di Federation. Questi messaggi vengono visualizzati nei registri dei processi di replica o nell'area Funzionalità di un report.

### **1) GUID non valido**

**Esempio di errore:** ERROR 2008-01-10T00:31:08.234Z The GUID ASXOOFyvy0FJnRcD0dZNTZg (trovato nella proprietà SI\_PARENT\_CUID numero oggetto 1285) non è un GUID valido

Questo errore indica che viene eseguita la replica di un oggetto senza che anche il relativo oggetto principale venga replicato e che non esiste ancora nel sito di destinazione. Ad esempio, viene replicato un oggetto, ma non la cartella che lo contiene. L'oggetto principale non viene replicato perché l'account che replica gli oggetti non dispone di diritti sufficienti per l'oggetto principale.

### **2) I Crystal Reports non mostrano dati nel sito di origine**

Questo errore può verificarsi se il report Crystal utilizza una vista aziendale, un elemento aziendale, una base dati, una connessione dati o un elenco di valori originariamente creato nel sito di destinazione e successivamente replicato nel sito di origine.

### **3) Gli overload di universi non vengono applicati correttamente.**

Questo errore può verificarsi se il report utilizza un universo che contiene un overload di universi creato nel sito di destinazione e replicato nel sito di origine.

### **4) Errore di memoria Java.**

**Esempio di errore:** java.lang.OutOfMemoryError.

Questo errore può verificarsi se il server di applicazioni Java ha esaurito la memoria durante l'elaborazione di un processo di replica. Il processo di replica potrebbe essere di dimensioni troppo elevate oppure il server di applicazioni Java potrebbe disporre di una quantità di memoria insufficiente.



Aumentare la memoria disponibile del server di applicazioni Java spostando i Servizi Web di Federation in un computer dedicato oppure ridurre la quantità di oggetti replicati in un processo di replica.

#### **5) Timeout del socket.**

**Esempio di errore:** Errore durante la comunicazione con il sito di origine. Timeout di lettura.

Le informazioni inviate dal sito di origine ad Adaptive Job Server nel sito di destinazione sono maggiori del timeout allocato. Aumentare il timeout del socket in Adaptive Job Server oppure ridurre il numero di oggetti replicati nel processo di replica.

#### **6) Limite di query.**

**Esempio di errore:** errore SDK verificatosi nel sito di destinazione. Non una query valida. (FWB 00025) .....Stringa della query maggiore del limite di lunghezza.

Questo errore può verificarsi se si replicano molti oggetti e Federation inoltra una query troppo lunga per poter essere gestita da CMS. Gli oggetti del sito di origine verranno salvati nel sito di destinazione. Tuttavia, eventuali modifiche che devono essere salvate nel sito di origine non verranno invece salvate. I conflitti vengono risolti nel modo specificato, anche se l'oggetto non viene contrassegnato con il flag di risoluzione conflitti. Gli oggetti salvati nel sito di destinazione continueranno a funzionare correttamente.

Per risolvere questo problema, ridurre il numero di oggetti replicati in un processo di replica.

#### **7) Timeout del processo di replica.**

**Esempio di errore:** Impossibile pianificare l'oggetto entro l'intervallo di tempo specificato.

È possibile ricevere questo messaggio se si verifica il timeout del processo di replica prima che un altro processo di replica sia stato completato. Questa situazione può verificarsi se più processi di replica sono connessi contemporaneamente allo stesso sito di origine. Il processo di replica non riuscito verrà nuovamente eseguito all'ora pianificata successiva.

Per risolvere questo problema, pianificare il processo di replica non riuscito per un orario che non sia in conflitto con altri processi di replica connessi allo stesso sito di origine.

#### **8) Limite di replica.**

**Esempio di errore:** errore SDK verificatosi nel sito di destinazione. Errore di accesso al database. .... Errore dell'elaboratore di query: spazio di stack esaurito nell'elaboratore di query durante l'ottimizzazione della query. Errore nell'esecuzione della query in ExecWithDeadlockHandling.

È possibile ricevere questo messaggio se si supera il numero di oggetti supportati che è possibile replicare in un determinato momento. Per risolvere questo problema, ridurre il numero di oggetti replicati nel processo di replica ed eseguire di nuovo il processo.

#### **9) Oggetto eliminato.**

**Esempio di errore:** Errore riscontrato durante il controllo dei diritti di protezione 0 Errore durante la creazione del pacchetto per l'oggetto.

È possibile che questo messaggio venga visualizzato se viene eliminato un oggetto dal pacchetto di replica. Ciò può accadere quando in Federation viene eseguita una query per un oggetto che deve essere replicato, prima che ne vengano controllati i diritti e ne venga creato il pacchetto.

### 10) Adaptive Processing Server

Esempio di errore: Si è verificato un errore in Job Processing Server.

Questo errore può verificarsi quando vengono caricate troppe classi in Federation e la memoria disponibile non è sufficiente per elaborare il processo di replica.

Per risolvere il problema, è necessario eseguire le operazioni riportate di seguito:

1. Negli argomenti della riga di comando di Adaptive Processing Server, aggiungere la riga seguente:  
`-javaArgs "XX:MaxPermSize=256m".`
2. Aggiungere i parametri seguenti al server di applicazioni Java a cui si effettua la connessione per Federation, per ridurre le dimensioni dei file BIAR in uso.
  - `-Dbobj.biar.suggestSplit=100m`
  - `-Dbobj.biar.forceSplit=100m`

### 11) Spazio di Object Manager

Esempio di errore: Impossibile generare il pacchetto push. Si è verificata un'eccezione di input/output: "Spazio esaurito sul dispositivo".

Questo errore si verifica quando lo spazio su disco disponibile per la directory temporanea utilizzata da Federation non è sufficiente. Per risolvere questo problema, creare spazio aggiuntivo nella directory temporanea o utilizzare un percorso diverso per tale directory.

Per specificare un percorso diverso per la directory temporanea nel sito di origine, aggiungere la riga seguente nei file di configurazione di Java Application Server: `-Dbobj.tmp.dir=TempDir`.

Per specificare un percorso diverso per la directory temporanea nel sito di destinazione, aggiungere la riga seguente agli argomenti della riga di comando di Adaptive Processing Server: `-javaArgs "-Dbobj.tmp.dir=TempDir"`.

Negli esempi precedenti *TempDir* rappresenta il percorso della directory temporanea da utilizzare.

### 12) Errore dell'universo

Esempio di errore: Si è verificato un errore interno durante la chiamata all'API `processDPCommands`.

Questo errore si verifica quando un universo replicato contiene una relazione di connessione universo-universo non valida o mancante. Per risolvere il problema, eseguire il processo di replica con l'opzione **Aggiorna da origine** selezionata e verificare che la connessione all'universo venga replicata.

In alternativa è possibile aprire l'universo in Universe Designer, modificarne la connessione all'universo e salvarlo nuovamente.

### Argomenti correlati

- [Procedure consigliate](#)
- [Limitazioni della release corrente](#)

# Configurazioni supplementari per gli ambienti ERP

## 24.1 Configurazioni per l'integrazione di SAP NetWeaver

### 24.1.1 Integrazione con SAP Netweaver Business Warehouse (BW)

#### 24.1.1.1 Panoramica

In questa sezione viene illustrato come configurare BW per abilitare e amministrare la pubblicazione dei report da SAP NetWeaver Business Warehouse nella piattaforma BI.

Prima di iniziare questa sezione, assicurarsi di avere completato la configurazione del plug-in di autenticazione SAP nella console CMC.

#### **Argomenti correlati**

- [Configurazione dell'autenticazione SAP](#)

#### 24.1.1.1.1 Configurazione delle cartelle e della protezione nella piattaforma BI

Quando si definisce un sistema di autorizzazione nella piattaforma BI, il sistema crea una struttura di cartelle logiche in base al sistema SAP. Quando si importano i ruoli e si pubblica il contenuto nella piattaforma BI, vengono create le cartelle corrispondenti. Non è l'amministratore che deve creare queste cartelle. Vengono infatti create in seguito alla definizione di un sistema di autorizzazione durante la configurazione del plug-in di autenticazione SAP, importando i ruoli nella console CMC e pubblicando il contenuto nella piattaforma BI.

#### **Nota:**

L'amministratore della piattaforma BI è responsabile dell'assegnazione dei diritti appropriati per queste cartelle:

- Cartella di livello principale SAP

Verificare che il gruppo Tutti abbia accesso limitato alla cartella di livello principale SAP.

- Cartelle ID sistema

Assegnare i diritti seguenti Publisher nella CMC:

- Aggiungi oggetti alla cartella
- Visualizza oggetti
- Modifica oggetti
- Modificare i diritti che gli utenti hanno sugli oggetti
- Elimina oggetti

**Suggerimento:**

Per facilitare la gestione dei diritti, è possibile creare un livello di accesso Publisher personalizzato che includa tali diritti, quindi concedere al Publisher principale tale livello di accesso per le cartelle ID sistema pertinenti.

**Argomenti correlati**

- [Utilizzo di livelli di accesso](#)
- [Funzionamento dei diritti nella piattaforma BI](#)

#### 24.1.1.1.2 Comprensione dei modelli di protezione predefiniti delle cartelle

Quando si esegue la pubblicazione del contenuto nella piattaforma BI da SAP, la piattaforma crea automaticamente la gerarchia rimanente dei ruoli, delle cartelle e dei report. Il sistema organizza i report in cartelle i cui nomi si basano sull'ID di sistema e sul numero client, in base al nome del ruolo.

- Il sistema crea le cartelle di livello principale, ovvero le cartelle SAP, 2.0 e di sistema (*SID*), quando si definisce un sistema di autorizzazione.
- Se necessario, il sistema crea le cartelle dei ruoli (importate come gruppi nella piattaforma BI) quando viene pubblicato un ruolo da BW.
- Viene creata una cartella dei contenuti per ogni ruolo in cui viene pubblicato del contenuto.
- La protezione è impostata per ciascun oggetto report in modo che gli utenti possano visualizzare solo i report che appartengono ai rispettivi ruoli.

L'amministratore è responsabile dell'assegnazione dei diritti ai membri dei differenti ruoli. L'area di lavoro per l'amministrazione dei contenuti viene utilizzata per amministrare la funzione di pubblicazione da SAP BW. È possibile identificare i ruoli dal sistema SAP BW con determinati sistemi della piattaforma BI, pubblicare report e sincronizzare questi ultimi tra una distribuzione SAP BW e della piattaforma BI.

**Cartelle dei contenuti**

La piattaforma BI importa un gruppo per ogni ruolo che viene aggiunto al sistema di autorizzazione come definito nella CMC.

Per garantire che siano concessi i diritti predefiniti adatti a tutti i membri di un ruolo di generazione dei contenuti, assegnare i diritti appropriati nel workbench per l'amministrazione dei contenuti per ogni sistema di autorizzazione definito nella piattaforma BI. Per avviare il workbench per l'amministrazione dei contenuti, eseguire la transazione `/CRYSTAL/RPTADMIN`:

1. Nel workbench per l'amministrazione dei contenuti, espandere **Sistema Enterprise** e quindi espandere **Sistemi disponibili**.
2. Fare doppio clic sul sistema desiderato.
3. Fare clic sulla scheda **Layout**.
4. Impostare **Criteri di protezione standard per report** su **View**.
5. Impostare **Criteri di protezione standard per cartelle ruoli** su **View su richiesta**.
6. Fare clic su **OK**.

Le impostazioni vengono applicate nella piattaforma BI per tutti i ruoli di contenuti. I ruoli, quindi, che hanno contenuto pubblicato. I membri di tali ruoli potranno a questo punto visualizzare le istanze di pianificazione dei report pubblicati in altri ruoli e potranno aggiornare i report pubblicati nei ruoli di cui sono membri.

**Nota:**

si consiglia vivamente di distinguere le attività dei ruoli. Ad esempio, sebbene sia possibile pubblicare da un ruolo amministrativo, è meglio provare a pubblicare solo dai ruoli di publisher. Inoltre, la funzione dei ruoli di pubblicazione è solo quella di definire quali utenti possono pubblicare i contenuti. Ciò significa che i ruoli di pubblicazione non devono contenere alcun contenuto; i publisher devono eseguire la pubblicazione nei ruoli di generazione dei contenuti accessibili ai membri dei ruoli regolari.

### **24.1.1.2 Configurazione di Publisher BW**

Publisher BW consente di pubblicare i report Crystal (file .rpt) separatamente o in batch da BW nella piattaforma BI.

In Windows è possibile configurare Publisher BW in uno dei due modi seguenti:

- Avviare Publisher BW utilizzando un servizio su un computer che ospita la piattaforma BI. Il servizio Publisher BW avvierà istanze di Publisher BW in base alle esigenze.
- Avviare Publisher BW utilizzando un gateway SAP locale per creare istanze di Publisher BW.

È necessario selezionare il metodo di configurazione in base ai requisiti del sito, dopo avere considerato i vantaggi e gli svantaggi di ciascuna configurazione. Una volta configurato Publisher BW nella piattaforma BI, è necessario configurare la pubblicazione nel workbench per l'amministrazione dei contenuti.

### **24.1.1.3 Configurazione di Publisher BW come servizio**

In questa sezione viene illustrato come abilitare la pubblicazione dei report da BW nella piattaforma BI, utilizzando Publisher BW come un servizio.

#### 24.1.1.3.1 Distribuzione dell'installazione di Publisher BW

In questa sezione viene illustrata la distribuzione del servizio Publisher BW e come separare Publisher BW da altri componenti della piattaforma BI.

È possibile eseguire il bilanciamento del carico della pubblicazione da BW mediante l'installazione dei servizi Publisher BW su due computer separati nello stesso sistema della piattaforma BI.

Quando si installa Publisher BW sui computer che ospitano la piattaforma BI, configurare i computer in modo che utilizzino gli stessi ID programma, host gateway SAP e servizio gateway. Dopo aver creato una destinazione RFC che utilizza questo ID del programma, BW esegue il bilanciamento del carico della pubblicazione tra i computer che ospitano la piattaforma BI. Inoltre, se Publisher BW diventa non disponibile, BW continua a utilizzare i servizi Publisher BW rimanenti.

È possibile aggiungere un altro livello di ridondanza di sistema a qualsiasi configurazione che includa più server di applicazioni BW. Configurare ciascun server di applicazioni BW in modo che esegua un gateway SAP. Per ciascun computer installare un servizio Publisher BW distinto in un computer che ospita la piattaforma BI. Configurare ciascun servizio Publisher BW in modo che utilizzi l'host gateway e il servizio gateway di un server di applicazioni BW separato. In questa configurazione, se un Publisher BW o un server di applicazioni non funziona, la pubblicazione può continuare da BW.

Se si desidera separare Publisher BW da altri componenti della piattaforma BI, installarlo utilizzando un gateway SAP autonomo.

In questo caso è necessario installare un gateway SAP locale sullo stesso computer su cui è installato Publisher BW. Inoltre, Publisher BW richiede l'accesso all'SDK della piattaforma BI e al motore di stampa di SAP Crystal Reports. Quindi, se si installa Publisher BW e il gateway SAP locale in un computer dedicato, è necessario installare anche il server SIA.

#### 24.1.1.3.2 Avvio di Publisher BW: UNIX

Eseguire lo script di Publisher BW per creare una o più istanze del publisher per gestire le richieste di pubblicazione. Si consiglia di avviare un'istanza del publisher.

Dopo l'avvio di Publisher BW, viene stabilita una connessione con il servizio gateway SAP specificato al momento dell'esecuzione del programma di installazione della piattaforma BI.

#### 24.1.1.3.3 Avvio di Publisher BW: Windows

In Windows utilizzare il CCM (Central Configuration Manager) per avviare il servizio Publisher BW. Quando si avvia il servizio Publisher BW, viene creata un'istanza del publisher che consente di gestire le richieste di pubblicazione dal sistema BW. Se il volume delle richieste di pubblicazione aumenta, Publisher BW crea automaticamente altri publisher per soddisfare la domanda.

#### 24.1.1.3.4 Configurazione di una destinazione per il servizio Publisher BW

Per abilitare Publisher BW, è necessario configurare una destinazione RFC sul server BW in modo che comunichi con il servizio Publisher BW. Se si dispone di un cluster BW, configurare la destinazione RFC su ciascun server, usando sempre l'istanza centrale di BW come host gateway.

Se si desidera eseguire la pubblicazione in più sistemi della piattaforma BI da BW, creare una destinazione RFC separata per il servizio Publisher BW in ciascuna distribuzione della piattaforma BI. È necessario utilizzare ID di programma univoci per ciascuna destinazione, ma gli stessi host e servizio gateway.

#### 24.1.1.3.5 Configurazione di Publisher BW con un gateway SAP locale

**Nota:**

Non utilizzare questa configurazione se la piattaforma BI è installata in UNIX. L'utilizzo di questo metodo in UNIX potrebbe restituire un comportamento di sistema imprevedibile.

Per abilitare la pubblicazione dei report da BW nella piattaforma BI utilizzando un gateway SAP locale, attenersi alla procedura seguente:

- [Installazione di un gateway SAP locale.](#)
- [Configurazione di una destinazione per Publisher BW.](#)

#### 24.1.1.3.6 Installazione di un gateway SAP locale

Nel computer dove è installato il Publisher BW è necessario installare un gateway SAP locale. Si consiglia di fare eseguire l'installazione di uno di questi gateway SAP a un amministratore BASIS SAP.

Per le istruzioni aggiornate per l'installazione di un gateway SAP locale, consultare le istruzioni per l'installazione SAP incluse nel CD di presentazione di SAP.

Per un elenco dettagliato degli ambienti sottoposti a test, consultare il file `platforms_EN.txt` fornito insieme al prodotto. Questo file include la versione specifica e i requisiti del service pack per i server di applicazioni, i sistemi operativi, i componenti SAP e così via.

Dopo aver installato il gateway SAP, utilizzare `regedit` per verificare le voci di registro `TMP` e `TEMP` nella sottochiave `HKEY_CURRENT_USER\Environment`. Entrambe le voci di registro devono contenere lo stesso valore di stringa, che deve essere un percorso di directory assoluto valido. Se il valore della voce contiene la variabile `%USERPROFILE%`, sostituirla con un percorso di directory assoluto. Solitamente entrambe le voci di registro sono impostate su `C:\WINDOWS\TEMP`.

#### 24.1.1.4 Configurazione di una destinazione per Publisher BW

Per abilitare Publisher BW, è necessario configurare una destinazione RFC in modo che fornisca a BW il percorso del computer su cui sono installati il gateway SAP locale e Publisher BW.

### **24.1.1.5 Configurazione della pubblicazione nel workbench per l'amministrazione dei contenuti**

L'area di lavoro per l'amministrazione dei contenuti viene utilizzata per amministrare la funzione di pubblicazione da SAP BW. È possibile identificare i ruoli dal sistema SAP BW con determinati sistemi della piattaforma BI, pubblicare report e sincronizzare questi ultimi tra una distribuzione SAP BW e della piattaforma BI. Dopo avere impostato l'autenticazione SAP e configurato Publisher BW, eseguire le funzioni descritte in questa sezione per abilitare la pubblicazione. Queste istruzioni consentono di:

- Impostare le autorizzazioni appropriate per utenti diversi del workbench per l'amministrazione dei contenuti.
- Impostare le connessioni per la piattaforma BI in cui è pubblicato il contenuto.
- Definire i ruoli che possono eseguire la pubblicazione in ciascuna piattaforma BI.
- Pubblicare il contenuto da BW nella piattaforma BI.

### **24.1.1.6 Utenti che possono accedere al workbench per l'amministrazione dei contenuti**

Esistono tre tipi di utenti che possono accedere al workbench per l'amministrazione dei contenuti:

- I consumatori dei contenuti, che appartengono ai ruoli di generazione dei contenuti e che possono visualizzare i report. Non dispongono dell'autorizzazione per attività diverse dalla visualizzazione dei report.
- I publisher dei contenuti della piattaforma BI, che possono visualizzare, pubblicare, modificare e (facoltativamente) eliminare i report da BW.
- Gli amministratori della piattaforma BI, che sono in grado di eseguire tutte le attività nell'area di lavoro per l'amministrazione dei contenuti. Tra queste attività figurano la definizione dei sistemi della piattaforma BI, la pubblicazione dei report e l'esecuzione della manutenzione dei report.

### **24.1.1.7 Creazione dei ruoli in BW per i publisher dei contenuti designati**

Quando si configura BW per l'integrazione con la piattaforma BI, valutare se la struttura di ruoli corrente consente di designare rapidamente utenti BW particolari come amministratori di sistema o publisher di contenuti per i sistemi della piattaforma BI.



Si consiglia di contrassegnare ogni nuovo ruolo creato in modo descrittivo. Esempi di nomi di ruolo descrittivi potrebbero essere `BOE_CONTENT_PUBLISHERS` e `BOE_SYSTEM_ADMINISTRATORS`.

**Suggerimento:**

è possibile assegnare a un utente amministrativo tutti i diritti di amministrazione di sistema o un sottoinsieme di tali diritti.

Per modificare i diritti che vengono concessi a questi nuovi ruoli (o a uno dei ruoli esistenti) nella piattaforma BI, è innanzitutto necessario impostare l'autenticazione SAP e importare i ruoli. È quindi possibile modificare i diritti di ciascun ruolo importato utilizzando la Central Management Console.

Per i dettagli della creazione dei ruoli, consultare la documentazione di SAP. Per ulteriori informazioni sull'utilizzo dei ruoli nell'amministrazione dei contenuti, consultare le seguenti sezioni:

- [Importazione dei ruoli SAP](#).
- [Configurazione delle cartelle e della protezione nella piattaforma BI](#).
- [Comprensione dei modelli di protezione predefiniti delle cartelle](#).

### 24.1.1.8 Configurazione dell'accesso al workbench per l'amministrazione dei contenuti

Per ogni tipo di utente che può accedere al workbench per l'amministrazione dei contenuti, è necessario applicare l'insieme di autorizzazioni appropriato in BW. Le autorizzazioni sono elencate nelle seguenti tabelle.

Tabella 24 - 1: Autorizzazioni per gli utenti amministrativi

Oggetto autorizzazione	Campo	Valori
S_RFC S_TCODE	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	Esegui (16)
	TCD	/CRYSTAL/RPTADMIN, RS-CR_MAINT_PUBLISH
S_TABU_CLI	CLIIDMAINT	X

Oggetto autorizzazione	Campo	Valori
S_TABU_DIS	ACTVT	Modifica, Visualizza (02, 03)
	DICBERCLS	&NC&
	JOB ACTION	DELE, RELE
	JOB GROUP	' '
S_RS_ADMWB	ACTVT	Esegui (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	Crea nuovo, Modifica, Visualizza, Elimina (01, 02, 03, 06)
ZCNTADMJOB	ACTVT	Create new, Elimina (01, 06)
ZCNTADMRPT	ACTVT	Visualizza, Elimina, Attiva, Mantieni, Verifica (03, 06, 07, 23, 39)

Tabella 24 - 2: Autorizzazioni per i publisher dei contenuti

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH, SH3A, SUNI
	ACTVT	Esegui (16)
	TCD	/CRYSTAL/RPTADMIN

Oggetto autorizzazione	Campo	Valori
S_BTCH_JOB	JOB ACTION	DELE, RELE
	JOB GROUP	' '
	ACTVT	Esegui (16)
	RSADMWBOBJ	WORKBENCH
ZCNTADMCES	ACTVT	Visualizza (03)
ZCNTADMJOB	ACTVT	(Nuovo, Elimina) 01, 06
ZCNTADMRPT	ACTVT	Visualizza, Attiva, Maintain, Verifica (03, 07, 23, 39) Elimina (facoltativo) (06) Modifica (facoltativo) (02)

Concedere ai publisher dei contenuti il diritto di eliminare i report nel workbench per l'amministrazione dei contenuti BW è facoltativo. Si tenga tuttavia presente che quando si elimina un report in BW, lo si elimina anche nella piattaforma BI. Se i publisher non dispongono di diritti sufficienti per eliminare i report nella piattaforma, viene generato un errore.

#### Autorizzazioni per i consumatori dei contenuti

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SH3A, SUNI
	ACTVT	Esegui (16)
	TCD	/CRYSTAL/RPTADMIN

Oggetto autorizzazione	Campo	Valori
S_RS_ADMWB	ACTVT	Esegui (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	Visualizza (03)

### 24.1.1.9 Definizione di un sistema della piattaforma BI

È necessario creare una definizione di sistema nel workbench per l'amministrazione dei contenuti per ciascun sistema della piattaforma BI in cui si desidera pubblicare i report.

#### 24.1.1.9.1 Aggiunta di un sistema della piattaforma BI

1. Eseguire la transazione `/crystal/rptadmin` per accedere al workbench per l'amministrazione dei contenuti.
2. Nel riquadro **Operazioni**, selezionare **Sistema Enterprise**.
3. Fare doppio clic su **Aggiungi nuovo sistema**.
4. Sulla scheda **Sistema**:
  - Digitare un nome descrittivo nel campo **Alias**. Evitare di utilizzare spazi o caratteri speciali, in quanto questi caratteri richiedono un trattamento speciale quando il nome alias viene utilizzato durante la configurazione di Enterprise Portal.
  - Digitare il nome del computer su cui è in esecuzione il CMS. Se si è configurato il CMS in modo che ascolti su una porta diversa da quella predefinita, digitare CMSNAME:PORT.
  - Selezionare **Sistema predefinito** se si desidera pubblicare i report in questo sistema da qualsiasi ruolo che non è stato esplicitamente assegnato a un sistema della piattaforma BI. Solo un sistema della piattaforma BI può essere impostato come predefinito.

Nell'elenco di tutti i sistemi disponibili il sistema predefinito è contrassegnato da un segno di spunta verde.
5. Fare clic su **Salva**.
6. Nella scheda **Destinazioni RFC** aggiungere ciascuna destinazione RFC associata a questo sistema. Per aggiungere una destinazione, fare clic sul pulsante **Inserisci riga**. Nell'elenco visualizzato fare doppio clic sul nome della destinazione RFC.

**Nota:**

un sistema della piattaforma BI può avere più destinazioni per aggiungere ridondanza di sistema. Consultare “Distribuzione dell'installazione di Publisher BW”.

7. Selezionare la casella di controllo accanto al nome della destinazione aggiunta e fare clic su **Verify BOE definition**.

In questa prova viene verificato se BW può contattare il Publisher BW specificato e può accedere a questo sistema mediante l'account utente di autorizzazione Crystal.

8. Sulla scheda **HTTP**:

- Nel campo **Protocol** digitare http o https, se il server Web connesso alla piattaforma BI è configurato per HTTPS.
- Nel campo **Web server host and port** digitare il nome del dominio o l'indirizzo IP completo del server Web che ospita BI Launch Pad. Per un'installazione che utilizza un server di applicazioni Java, includere il numero di porta. Ad esempio digitare boserver01.businessobjects.com:8080.
- Nel campo **Path** digitare SAP

Questo percorso è fondamentalmente il percorso virtuale che il server Web utilizza quando fa riferimento alla sottocartella `sap` del contenuto Web della piattaforma BI. Fornire un valore alternativo solo se sono stati personalizzati l'ambiente Web e il percorso dei file del contenuto Web della piattaforma.

Non includere una barra rovesciata all'inizio o alla fine della voce.

- Nel campo **Viewer application** digitare il nome dell'applicazione del visualizzatore.

Per utilizzare il visualizzatore della piattaforma BI predefinito che utilizza la versione Java di BI Launch Pad, digitare `openDocument.jsp`

Se la piattaforma BI è stata installata in Windows utilizzando la configurazione `ASP.NET` predefinita, per utilizzare il browser predefinito digitare `report/report_view.aspx`

9. Nella scheda **Languages** selezionare le lingue dei report che verranno pubblicati in questo sistema.
10. Nella scheda **Roles** aggiungere i ruoli di generazione dei contenuti che si desidera associare a questo sistema della piattaforma BI.  
Consultare “Importazione di ruoli SAP”.
11. Fare clic sul pulsante **Insert Row**.

Viene visualizzato un elenco dei ruoli disponibili da aggiungere a questo sistema.

**Nota:**

ciascun ruolo può eseguire la pubblicazione solo in un sistema della piattaforma BI. Se i ruoli che si desidera aggiungere a questo sistema della piattaforma BI non appaiono nell'elenco, fare clic su **Cancel** per tornare alla scheda **Roles**, quindi su **Reassign Roles**.

12. Selezionare i ruoli che si desidera pubblicare in questo sistema e fare clic su **OK**.
13. Nella scheda **Layout** selezionare le impostazioni di protezione predefinite per i report e le cartelle di ruoli pubblicate in questo sistema della piattaforma BI.

**Nota:**

- Per ogni ruolo pubblicato nel sistema viene automaticamente creata una cartella nella piattaforma BI. Tale cartella contiene i collegamenti dei report pubblicati in tale ruolo.
- Se dopo la configurazione di un sistema della piattaforma BI si modificano i livelli di protezione predefiniti, questa modifica non incide sui livelli di protezione dei report o delle cartelle dei ruoli pubblicati. Per modificare i livelli di protezione predefiniti per tutti i ruoli e i contenuti pubblicati nella piattaforma, eliminare le cartelle dei ruoli e i collegamenti nel sistema. Si tenga presente che non vengono eliminati i report effettivi. Modificare le impostazioni di protezione e pubblicare di nuovo i ruoli e i report.

14. Fare clic su **OK** in basso per salvare le impostazioni e creare il sistema della piattaforma BI nel workbench per l'amministrazione dei contenuti.

È ora possibile pubblicare i report nella piattaforma BI da BW.

**Argomenti correlati**

- [Distribuzione dell'installazione di Publisher BW](#)
- [Importazione dei ruoli SAP](#)

### **24.1.1.10 Pubblicazione dei report mediante il workbench per l'amministrazione dei contenuti**

Dopo che si è salvato un report in BW, è possibile pubblicarlo mediante il workbench per l'amministrazione dei contenuti. È possibile utilizzare il workbench per l'amministrazione dei contenuti per pubblicare i singoli report oppure è possibile pubblicare tutti i report salvati in un ruolo particolare. Solo un utente che dispone delle autorizzazioni per un publisher di contenuti Crystal (vedere [Creazione e applicazione delle autorizzazioni](#)) può utilizzare il workbench per l'amministrazione dei contenuti per pubblicare e gestire i report.

### **24.1.1.11 Pubblicazione dei ruoli o dei report**

1. Eseguire la transazione `/crystal/rptadmin` per accedere al workbench per l'amministrazione dei contenuti.
2. Nel riquadro **Operazioni** selezionare **Pubblica report**.
3. Per trovare il contenuto salvato nel sistema BW, fare doppio clic su **Seleziona report e ruoli da pubblicare**.

Viene visualizzata una finestra di dialogo nella quale è possibile filtrare i ruoli e i report disponibili.

4. Nell'elenco, selezionare il sistema o i sistemi in cui è disponibile il contenuto che si desidera visualizzare.

**Nota:**

l'elenco contiene tutti i sistemi disponibili definiti nel sistema BW.

5. Quindi filtrare i risultati per limitare il numero di report e ruoli che verranno visualizzati. Utilizzare queste opzioni:

- **Versione oggetto**

Selezionando "A: attiva", vengono visualizzati tutti i report che possono essere pubblicati. Se si seleziona l'opzione vuota, vengono visualizzati tutti i report. Le opzioni rimanenti sono termini riservati SAP.

- **Stato oggetto**

Selezionare "ACT Attivo, eseguibile" per visualizzare solo i report che sono stati pubblicati. Selezionare "INA Inattivo, non eseguibile" per visualizzare solo i report che non sono stati pubblicati. Lasciare il campo vuoto per visualizzare tutti i report. Le opzioni rimanenti sono termini riservati SAP.

- **Filtro ruoli**

Se si digita del testo in questa casella, vengono visualizzati solo i ruoli che corrispondono a quanto digitato. Utilizzare \* come carattere jolly. Ad esempio, per visualizzare tutti i ruoli che iniziano con la lettera d, digitare d\*.

- **Descrizione report**




Se si digita del testo in questa casella, vengono visualizzati solo i report le cui descrizioni corrispondono a quanto digitato. Utilizzare \* come carattere jolly per trovare un numero qualsiasi di caratteri. Utilizzare + come carattere jolly per trovare nessun carattere o 1 carattere. Ad esempio, per visualizzare tutti i report le cui descrizioni contengono la parola reddito, digitare \*reddito\*.

6. Fare clic su **OK**.

Nel pannello destro viene visualizzato l'elenco dei report che soddisfano i criteri.

I report sono disposti in base a una gerarchia: Sistema della piattaforma BI > Ruoli in quel sistema > Report salvati nel ruolo.

Ciascun elemento della gerarchia è contrassegnato con un punto rosso, giallo o verde. Gli elementi più alti nella gerarchia riflettono lo stato degli elementi in essi contenuti, con la condizione meno favorevole filtrata al livello più alto della gerarchia. Ad esempio, se un report in un ruolo è giallo (attivo), ma tutti gli altri sono verdi (pubblicati), il ruolo viene visualizzato in giallo (attivo).

-  Verde: l'elemento è pubblicato completamente. Se l'elemento è un ruolo o un sistema della piattaforma BI, tutti i report presenti nell'elemento vengono pubblicati.
-  Giallo: l'elemento è attivo, ma non pubblicato. Se l'elemento è un report, può essere pubblicato. Se l'elemento è un ruolo o un sistema della piattaforma BI, tutti i contenuti sono attivi e almeno un elemento del ruolo o del sistema non è stato pubblicato.
-  Rosso: l'elemento è un contenuto SAP e non può essere pubblicato mediante il workbench per l'amministrazione dei contenuti. Il contenuto non è disponibile per la pubblicazione finché non viene attivato utilizzando il workbench per l'amministrazione dei contenuti.

#### 7. Selezionare i report che si desidera pubblicare.

Per pubblicare tutti i report in un ruolo, selezionare il ruolo. Per pubblicare tutti i ruoli di un sistema della piattaforma BI, selezionare il sistema.

##### **Nota:**

quando si seleziona un ruolo (o un sistema), vengono selezionati tutti i report in esso contenuti. Per cancellare questa selezione, deselezionare la casella di controllo corrispondente al ruolo (o al sistema), quindi fare clic su **Aggiorna**.

#### 8. Fare clic su **Pubblica**.

##### **Nota:**

i report pubblicati in background vengono elaborati man mano che le risorse del sistema diventano disponibili. Per utilizzare questa opzione, fare clic su **In background** e non su **Pubblica**.

#### 9. Fare clic su **Aggiorna** per aggiornare la visualizzazione dello stato dei sistemi della piattaforma BI, dei ruoli e dei report nel workbench per l'amministrazione dei contenuti.

##### **Suggerimento:**

per visualizzare un report, fare clic con il pulsante destro del mouse sul report, quindi selezionare **Visualizza**. Per vedere le query utilizzate dal report, fare clic con il pulsante destro del mouse sul report e selezionare **Query usate**.

##### **Nota:**

Dopo avere pubblicato un report nella piattaforma BI, per sovrascrivere il report pubblicato, fare clic su **Sovrascrivi**.

#### **Argomenti correlati**

- [Pianificazione della pubblicazione in background](#)

### **24.1.1.12 Pianificazione della pubblicazione in background**



Se si pubblicano i report in background, immediatamente o come processo pianificato, si risparmiano le risorse del sistema. Si consiglia di pubblicare i report in background per migliorare la capacità di risposta del sistema.

Se si pubblicano i report regolarmente, come processi pianificati, si sincronizzano le informazioni sui report tra BW e la distribuzione della piattaforma BI. Si consiglia di pianificare tutti i report (o i ruoli che contengono questi report). È inoltre possibile sincronizzare manualmente i ruoli e i report mediante l'opzione Aggiorna stato dell'operazione Manutenzione report. Per ulteriori informazioni vedere [Aggiornamento dello stato dei report](#).

### **24.1.1.13 Aggiornamento delle informazioni sul sistema per i report pubblicati**

Publisher BW utilizza le informazioni sul sistema SAP immesse qui per aggiornare l'origine dati dei report pubblicati. È possibile scegliere di utilizzare il server di applicazioni BW locale o l'istanza BW centrale se si preferisce una configurazione del bilanciamento del carico.

### **24.1.1.14 Manutenzione dei report**

Le attività di manutenzione dei report includono la sincronizzazione delle informazioni sui report tra la piattaforma BI e BW (Aggiorna stato), l'eliminazione dei report indesiderati (Elimina report) e l'aggiornamento dei report di cui si è eseguita la migrazione da versioni precedenti della piattaforma (Post-migrazione).

#### **24.1.1.14.1 Aggiornamento dello stato dei report**

Se si apporta una modifica a un report pubblicato in un sistema della piattaforma BI (ad esempio, si modifica il ruolo in cui è pubblicato un report), la modifica non viene riflessa in BW fino a quando non si sincronizzano la piattaforma BI e BW. È possibile pianificare un processo di pubblicazione in modo che sincronizzi regolarmente la piattaforma BI e BW (vedere [Pianificazione della pubblicazione in background](#)). In alternativa è possibile aggiornare manualmente lo stato del report mediante lo strumento di manutenzione dei report.

#### **24.1.1.14.2 Eliminazione di report**

Se si elimina un report pubblicato da BW mediante il workbench per l'amministrazione dei contenuti, lo si elimina anche dalla piattaforma BI. Solo gli utenti a cui sono state concesse le autorizzazioni necessarie per eliminare i report su BW e sul sistema della piattaforma BI possono rimuovere i report.

**Nota:**

se un utente dispone dei diritti per eliminare un report su BW, ma non sul sistema della piattaforma BI in cui è pubblicato il report, è possibile che si verifichi un errore.

### 24.1.1.15 Configurazione del gestore di richieste http SAP

Per abilitare la visualizzazione dei report in BW, è necessario configurare BW in modo che utilizzi il gestore di richieste http che fa parte del workbench per l'amministrazione dei contenuti. Quindi, quando un utente BW apre un report Crystal nella GUI SAP, BW può instradare la richiesta di visualizzazione sul Web in modo appropriato.

Utilizzare la transazione SICF per accedere all'elenco di servizi e host virtuali attivi sul sistema BW. Creare un nuovo nodo detto `ce_url` in BW nella gerarchia `default_host` e aggiungere `/CRYSTAL/CL_BW_HTTP_HANDLER` all'elenco dei gestori. È possibile che sia necessario attivare manualmente questo servizio dopo averlo creato.

### 24.1.1.16 Configurazioni per l'elaborazione di dati SAP

#### 24.1.1.16.1 Elaborazione dei report pianificati nella modalità batch di SAP

Per le installazioni Windows, è possibile eseguire i report pianificati nella piattaforma BI nella modalità batch di SAP. I driver InfoSet e Open SQL possono eseguire i report nella modalità batch o background di SAP quando determinate variabili di ambiente sono impostate su 1. Le variabili di ambiente rilevanti sono:

- `CRYSTAL_INFOSET_FORCE_BATCH_MODE` (per il driver InfoSet)
- `CRYSTAL_OPENSQ_L_FORCE_BATCH_MODE` (per il driver Open SQL)

Si consiglia, tuttavia, di utilizzare questa funzione solo quando si dispone di un'installazione distribuita della piattaforma BI. Quando queste variabili di ambiente sono impostate su 1, i driver eseguono i report nella modalità batch di SAP, indipendentemente dal componente per la creazione di report che sta effettivamente eseguendo il report. Pertanto, se si creano queste variabili di ambiente come variabili di ambiente di sistema in un computer su cui è in esecuzione una combinazione di server della piattaforma BI, i driver eseguono tutti i report nella modalità batch (comprese le richieste di report su richiesta del server di elaborazione Crystal Reports e del Report Application Server).

Per garantire che i driver eseguano solo i report pianificati nella modalità batch (ovvero i report eseguiti da Adaptive Job Server), evitare di impostare le variabili di ambiente di sistema nei computer su cui sono in esecuzione combinazioni di server della piattaforma BI. Eseguire invece queste operazioni per personalizzare le variabili di ambiente per ciascun Adaptive Job Server.

**Nota:**

Gli utenti SAP che pianificano i report nella piattaforma BI possono richiedere ulteriori autorizzazioni in SAP.

**Argomenti correlati**

- [Pianificazione di un report in modalità batch con una query Open SQL](#)

**24.1.1.16.2 Per elaborare i report pianificati nella modalità batch di SAP**

1. Creare uno script batch (file `.bat`) in un editor di testo, ad esempio Blocco note, con il seguente contenuto:

```
@echo off
set CRYSTAL_INFOSET_FORCE_BATCH_MODE=1
set CRYSTAL_OPENSQ_L_FORCE_BATCH_MODE=1
%*
```

Questo script imposta le variabili di ambiente su 1, quindi esegue i parametri trasmessi allo script dalla riga di comando.

2. Salvare il file con il nome `jobserver_batchmode.bat` in una cartella su ciascun computer su cui è in esecuzione Adaptive Job Server.
3. Collegarsi alla Central Management Console (CMC).
4. Scegliere **Server**.
5. Espandere il nodo **Categorie di servizio** e scegliere **Servizi di analisi**.
6. Selezionare **Adaptive Processing Server** e scegliere **Proprietà** nel menu di scelta rapida. Viene visualizzata la pagina "Proprietà".
7. Nella pagina "Proprietà" individuare il campo **Parametri riga di comando**.

Si tratta del comando di avvio per l'Adaptive Job Server. Ad esempio:

```
"\\SERVER01\C$\Program Files\SAO Business Objects\SAP BusinessObjects Enterprise\win32_x86\JobServer.exe" -service -name SERVER01.report -ns SERVER01 -objectType BusinessObjects Enterprise.Report -lib procReport -restart
```

8. Utilizzare come prefisso del comando predefinito il percorso completo del file `jobserver_batchmode.bat` salvato sul computer su cui è in esecuzione l'Adaptive Job Server.

In questo esempio il file batch viene salvato su un computer detto SERVER01 con il nome:

```
C:\Crystal Scripts\jobserver_batchmode.bat
```

Pertanto il nuovo comando di avvio per l'Adaptive Job Server è:

```
"\\SERVER01\C$\Crystal Scripts\jobserver_batchmode.bat" "\\SERVER01\C$\Program Files\SAP Business Objects\SAP BusinessObjects Enterprise 12.0\win32_x86\JobServer.exe" -service -name SERVER01.report -ns SERVER01 -objectType BusinessObjects Enterprise.Report -lib procReport -restart
```

Questo nuovo comando di avvio consente di avviare prima il file batch. A sua volta il file batch imposta le variabili di ambiente necessarie prima di eseguire il comando di avvio originale per l'Adaptive Job Server. In questo modo le variabili di ambiente disponibili per Adaptive Job Server differiscono dalle variabili di ambiente disponibili nei server responsabili della creazione di report su richiesta (il server di elaborazione Crystal Reports e il Report Application Server).

9. Fare clic su **Salva e chiudi**.

10. Fare clic con il pulsante destro del mouse sull'Adaptive Job Server e scegliere **Avvia** nel menu di scelta rapida.

**Nota:**

Se l'Adaptive Job Server non viene avviato, verificare il nuovo comando di avvio.

## 24.1.1.17 Configurazioni per trasporti SAP

### 24.1.1.17.1 Panoramica

La piattaforma BI include i trasporti seguenti:

- Trasporto Connettività Open SQL
- Trasporto Connettività InfoSet
- Trasporto Definizione protezione a livello di riga
- Trasporto Definizione cluster
- Trasporto Workbench per l'amministrazione dei contenuti
- Trasporto per la personalizzazione dei parametri BW Query
- Trasporto MDX
- Trasporto ODS

Esistono due set diversi di trasporti: trasporti compatibili con Unicode e trasporti ANSI. Se si esegue un sistema BASIS 6.20 o versione successiva, utilizzare i trasporti compatibili con Unicode. Se si esegue un sistema BASIS precedente alla versione 6.20, utilizzare i trasporti ANSI. Tutti i trasporti installati si trovano nella directory seguente nel supporto di distribuzione del prodotto: `\Collaterals\Add-Ons\SAP\Transports\`.

**Nota:**

quando si cercano possibili conflitti di installazione, assicurarsi che nessuno dei nomi oggetto esista già nel sistema SAP. Gli oggetti utilizzano per impostazione predefinita uno spazio dei nomi `/crystal/`, pertanto non è necessario crearne uno manualmente. Se si crea manualmente uno spazio dei nomi `/crystal/`, verranno richieste le chiavi di ripristino della licenza a cui non è possibile accedere.

### 24.1.1.17.2 Configurazione dei trasporti

Per configurare i componenti Accesso ai dati o BW Publisher della piattaforma BI, è necessario importare i trasporti appropriati nel sistema SAP. Tali file utilizzano il contenuto di questi file di trasporto durante la comunicazione con il sistema SAP.

Le procedure di installazione e configurazione che è necessario eseguire sul sistema SAP devono essere eseguite da un esperto BASIS che abbia dimestichezza con il sistema di modifica e trasporto e che disponga dei diritti amministrativi per il sistema SAP. La procedura esatta per l'importazione dei file di trasporto varia a seconda della versione di BASIS in esecuzione. Per i dettagli procedurali specifici, fare riferimento alla documentazione di SAP.

Quando si distribuisce il componente Accesso ai dati per la prima volta, tutti gli utenti possono accedere a tutte le tabelle SAP per impostazione predefinita. Per proteggere i dati SAP a cui possono accedere gli utenti, utilizzare l'Editor definizione Protezione.

Dopo che si sono importati i trasporti, è necessario configurare i livelli appropriati dell'accesso dell'utente. Creare le autorizzazioni necessarie e applicarle tramite i profili o i ruoli agli utenti SAP che progetteranno, eseguiranno o pianificheranno i report Crystal.

### **Argomenti correlati**

- [Creazione e applicazione delle autorizzazioni](#)

### ***Tipi di trasporti***

Esistono due set diversi di trasporti: trasporti compatibili con Unicode e trasporti ANSI. Se si esegue un sistema BASIS 6.20 o versione successiva, utilizzare i trasporti compatibili con Unicode. Se si esegue un sistema BASIS precedente alla versione 6.20, utilizzare i trasporti ANSI. Tutti i trasporti installati si trovano nella directory seguente nel supporto di distribuzione del prodotto: `\Collaterals\Add-Ons\SAP\Transports\`. Il file `transports.txt` elenca i file di trasporto ANSI e compatibili con Unicode.

Di seguito sono descritti i tipi di trasporto:

- Trasporto Connettività Open SQL

Il trasporto Connettività Open SQL consente al driver Open SQL di connettersi a e creare report dal sistema SAP.

- Trasporto Definizione protezione a livello di riga

Questo trasporto fornisce l'Editor definizione Protezione, uno strumento che funge da interfaccia grafica per le tabelle `/crystal/auth` nel trasporto Connettività Open SQL.

- Trasporto Definizione cluster

Questo trasporto fornisce lo strumento Cluster Definition, che consente di creare un repository di metadati per le definizioni dei cluster di dati ABAP. Queste definizioni forniscono al driver Open SQL le informazioni necessarie per creare report da questi cluster di dati.

#### **Nota:**

i cluster di dati ABAP non coincidono con le tabelle di cluster. Le tabelle di cluster sono già definite in DDIC.

- Trasporto Connettività InfoSet

Il trasporto Connettività InfoSet consente al driver InfoSet di accedere a set informazioni e a query SAP.

- Workbench per l'amministrazione dei contenuti

Questo trasporto fornisce la funzionalità di amministrazione dei contenuti per i sistemi BW. È disponibile solo come trasporto compatibile con UNICODE.

- Trasporto per la personalizzazione dei parametri BW Query

Questo trasporto fornisce il supporto per i valori dei parametri personalizzati e predefiniti nei report basati sulle query BW.

- Trasporto Connettività BW MDX

Questo trasporto consente al driver MDX Query di accedere ai cubi e alle query BW. Questo trasporto è compatibile con BW 3.0B patch 27 o superiore e BW 3.1C patch 21 o superiore.

- Trasporto Connettività ODS

Questo trasporto consente al driver ODS Query di accedere ai dati ODS. Questo trasporto è compatibile con BW 3.0B patch 27 o superiore e BW 3.1C patch 21 o superiore.

### *Verifica dei conflitti*

Il contenuto dei file di trasporto viene registrato automaticamente nello spazio dei nomi SAP BusinessObjects quando si importano i file. Lo spazio dei nomi SAP BusinessObjects è riservato a questo scopo nelle versioni recenti di R/3 e MYSAP ERP. Tuttavia, per alcuni oggetti quali oggetti di autorizzazione, classi di autorizzazioni e oggetti legacy, i relativi nomi possono non contenere i prefissi appropriati. Prima di eseguire l'importazione dei file di trasporto, si consiglia di controllare eventuali conflitti per questi tipi di oggetto.

Se il gruppo di funzioni, uno dei moduli di funzione o uno degli altri oggetti esiste già nel sistema SAP, è necessario risolvere lo spazio dei nomi prima di importare i file di trasporto di SAP BusinessObjects. Fare riferimento alla documentazione di SAP NetWeaver per le procedure appropriate alla versione di SAP in possesso.

### *Importazione dei file di trasporto*

Leggere il file `transports_EN.txt` che si trova nella directory seguente nel supporto di distribuzione del prodotto: `\Collaterals\Add-Ons\SAP\Transports\`. In questo file di testo sono elencati i nomi esatti dei file che costituiscono ciascun trasporto. Le directory `cofiles` e `data` nella directory `transports` corrispondono alle directory `../trans/cofiles` e `../trans/data` sul server SAP.

È necessario importare il trasporto Connettività Open SQL prima di importare i trasporti Definizione protezione a livello di riga o Definizione cluster. Gli altri trasporti possono essere importati in qualsiasi ordine.

#### **Nota:**

- dopo avere copiato i file dal CD sul server, assicurarsi che tutti i file siano scrivibili prima di importare i trasporti. Se i file di importazione sono a sola lettura, le importazioni non riescono.
- dato che i trasporti sono file binari, nelle installazioni UNIX è necessario aggiungere i file tramite FTP in modalità binaria (per evitare che vengano danneggiati). È inoltre necessario disporre delle autorizzazioni di scrittura per il server UNIX.

*Trasporti**Trasporto Connettività Open SQL*

Il trasporto Connettività Open SQL consente ai driver di connettersi a e creare report dal sistema SAP.

Oggetto	Tipo	Descrizione
/CRYSTAL/BC	Pacchetto	Classe di sviluppo
/CRYSTAL/OPENSQL	Gruppo di funzioni	Funzioni Open SQL
/CRYSTAL/OSQL_AUTH_FORMS	Programma	Programma di supporto
/CRYSTAL/OSQL_EXECUTE	Programma	Programma di supporto
/CRYSTAL/OSQL_TYPEPOOL PROG	Programma	Programma di supporto
/CRYSTAL/OSQL_TYPE POOLS	Programma	Programma di supporto
/CRYSTAL/OSQL_UTILS	Programma	Programma di supporto
ZSSI	Classe di oggetti autorizzazione	Oggetti autorizzazione per la creazione di report
ZSEGREPORT	Oggetto autorizzazione	Oggetto autorizzazione per la creazione di report
/CRYSTAL/OSQL_CLU_ACT KEY_ENTRY	Tabella	Metadati cluster
/CRYSTAL/OSQL_FCN_PARAMETER	Tabella	Metadati funzione

Oggetto	Tipo	Descrizione
/CRYSTAL/OSQL_FCN_P RAM_FIELD	Tabella	Metadati funzione
/CRYSTAL/OSQL_FIELD_E NTRY	Tabella	Metadati tabella
/CRYSTAL/OSQL_OBJECT_E NTRY	Tabella	Metadati tabella
/CRYSTAL/OS QL_RLS_CHK_ENTRY	Tabella	Metadati RLS
/CRYSTAL/OS QL_RLS_FCN_ENTRY	Tabella	Metadati RLS
/CRYSTAL/OS QL_RLS_VAL_ENTRY	Tabella	Metadati RLS
ZCLUSTDATA	Tabella	Metadati cluster
ZCLUSTID	Tabella	Metadati cluster
ZCLUSTKEY	Tabella	Metadati cluster
ZCLUSTKEY2	Tabella	Metadati cluster
/CRYSTAL/AUTHCHK	Tabella	Metadati RLS
/CRYSTAL/AUTHFCN	Tabella	Metadati RLS
/CRYSTAL/AUTHKEY	Tabella	Metadati RLS
/CRYSTAL/AUTHOBJ	Tabella	Metadati RLS



Oggetto	Tipo	Descrizione
/CRYSTAL/AUTHREF	Tabella	Metadati RLS
ZSSAUTHCHK	Tabella	Metadati RLS precedenti
ZSSAUTHOBJ	Tabella	Metadati RLS precedenti
ZSSAUTHKEY	Tabella	Metadati RLS precedenti
ZSSAUTHREF	Tabella	Metadati RLS precedenti
ZSSAUTH FCN	Tabella	Metadati RLS precedenti

### *Trasporto Connettività InfoSet*

Il trasporto Connettività InfoSet consente al driver InfoSet di accedere a set informazioni. Questo trasporto è compatibile con R/3 4.6c e versioni successive. Non importarlo se si esegue SAP R/3 4.6a o una versione precedente.

Oggetto	Tipo	Descrizione
/CRYSTAL/BC	Pacchetto	Classe di sviluppo
/CRYSTAL/FLAT	Gruppo di funzioni	Funzioni wrapper InfoSet
/CRYSTAL/QUERY_BATCH	Programma	Esecuzione in modalità batch
/CRYSTAL/QUERY_BATCH_STREAM	Programma	Flusso dell'esecuzione in modalità batch.

### *Trasporto Definizione protezione a livello di riga*

Questo trasporto fornisce l'Editor definizione Protezione, uno strumento che funge da interfaccia grafica per le tabelle /CRYSTAL/AUTH nel trasporto Connettività Open SQL.

Oggetto	Tipo	Descrizione
/CRYSTAL/BC	Pacchetto	Classe di sviluppo
/CRYSTAL/TABMNT	Gruppo di funzioni	Gruppo di funzioni per la visualizzazione della manutenzione della tabella per le limitazioni delle funzioni
/CRYSTAL/RLSDEF	Programma	Programma principale
/CRYSTAL/RLS_INCLUDE1	Programma	Include il programma contenente le definizioni dei moduli
/CRYSTAL/RLS_INCLUDE2	Programma	Include il programma contenente le definizioni delle sottoroutine
TDDAT [/CRYSTAL/AUTHFCN]	Contenuto tabella	Definizione manutenzione tabella
TVDIR [/CRYSTAL/AUTHFCN]	Contenuto tabella	Definizione manutenzione tabella
/CRYSTAL/AUTHFCNS	Definizione oggetto trasporto e manutenzione	Definizione manutenzione tabella
/CRYSTAL/RLS	Transazione	Transazione programma principale
/CRYSTAL/RLSFCN	Transazione	Transazione di supporto richiamata internamente dal programma principale.

**Trasporto Definizione cluster**

Questo trasporto fornisce lo strumento Cluster Definition, che consente di creare un repository di metadati per le definizioni dei cluster di dati ABAP. Queste definizioni forniscono al driver Open SQL le informazioni necessarie per creare report da questi cluster di dati.

**Nota:**

i cluster di dati ABAP non coincidono con le tabelle di cluster. Le tabelle di cluster sono già definite in DDIC.

Oggetto	Tipo	Descrizione
ZCIMPRBG	Programma	Programma principale
ZCRBGTOP	Programma	Include il programma
ZCDD	Transazione	Transazione programma principale

**Trasporto Workbench per l'amministrazione dei contenuti**

Questo trasporto fornisce la funzionalità di amministrazione dei contenuti per i sistemi BW. È disponibile solo come trasporto compatibile con Unicode.

Oggetto	Tipo	Descrizione
/CRYSTAL/BC	Pacchetto	Classe di sviluppo
/CRYSTAL/CL_BW_HTTP_HANDLER	Classe	Gestore di richieste HTTP compatibile con più CE
/CRYSTAL/OBJECT_STATUS_DOM	Dominio	Attività di report
/CRYSTAL/OBJ_POLICY_DOM	Dominio	Protezione oggetto CE
/CRYSTAL/OBJECT_STATUS	Elemento dati	Attività di report

Oggetto	Tipo	Descrizione
/CRYSTAL/OBJ_POLICY	Elemento dati	Protezione oggetto CE
/CRYSTAL/CE_SYNCH	Gruppo di funzioni	Stub publisher
/CRYSTAL/CA_MSG	Classe di messaggi	Messaggi di stato
/CRYSTAL/CE_SYNCH_FORMS	Programma	Componente programma
/CRYSTAL/CONTENT_ADMIN	Programma	Componente programma
/CRYSTAL/CONTENT_ADMIN_CLASS_D	Programma	Componente programma
/CRYSTAL/CONTENT_ADMIN_CLASS_I	Programma	Componente programma
/CRYSTAL/CONTENT_ADMIN_CTREE	Programma	Componente programma
/CRYSTAL/CONTENT_ADMIN_FORMS	Programma	Componente programma
/CRYSTAL/CONTENT_ADMIN_MODULES	Programma	Componente programma
/CRYSTAL/CONTENT_ADMIN_PAIS	Programma	Componente programma
/CRYSTAL/CONTENT_ADMIN_PBOS	Programma	Componente programma
/CRYSTAL/CONTENT_ADMIN_TAB_FRM	Programma	Componente programma

Oggetto	Tipo	Descrizione
/CRYSTAL/CONTENT_ADMIN_TOP	Programma	Componente programma
/CRYSTAL/PUBLISH_WORKER	Programma	Componente programma
/CRYSTAL/PUBLISH_WORKER_DISP	Programma	Componente programma
/CRYSTAL/PUBLISH_WORKER_DISP_I	Programma	Componente programma
/CRYSTAL/PUBLISH_WORKER_FORMS	Programma	Componente programma
/CRYSTAL/PUBLISH_WORKER_PROC	Programma	Componente programma
/CRYSTAL/PUBLISH_WORKER_PROC_I	Programma	Componente programma
/CRYSTAL/PUBLISH_WORKER_SCREEN	Programma	Componente programma
/CRYSTAL/CA_DEST	Tabella	Stato applicazione
/CRYSTAL/CA_JOB	Tabella	Stato applicazione
/CRYSTAL/CA_JOB2	Tabella	Stato applicazione
/CRYSTAL/CA_LANG	Tabella	Stato applicazione
/CRYSTAL/CA_PARM	Tabella	Stato applicazione
/CRYSTAL/CA_ROLE	Tabella	Stato applicazione

Oggetto	Tipo	Descrizione
/CRYSTAL/CA_SYST	Tabella	Stato applicazione
/CRYSTAL/MENU_TREE_ITEMS	Struttura	Stato applicazione
/CRYSTAL/REPORT_ID	Tabella	Stato applicazione
/CRYSTAL/RPTADMIN	Transazione	Transazione programma principale
/CRYSTAL/EDIT_REPORT	Programma	Wrapper per modifica report
/CRYSTAL/EDIT_REPORT	Gruppo di funzioni	Funzioni di modifica dei report
ZSSI	Classe di oggetti autorizzazione	Autorizzazioni Crystal
ZCNTADMCES	Oggetto autorizzazione	Operazioni CE
ZCNTADMRPT	Oggetto autorizzazione	Operazioni report
ZCNTADMJOB	Oggetto autorizzazione	Operazioni processo in background

### *Trasporto Connettività ODS*

Questo trasporto consente al driver ODS Query di accedere ai dati ODS. Questo trasporto è compatibile con BW 3.0B patch 27 o superiore e BW 3.1C patch 21 o superiore.

Oggetto	Tipo	Descrizione
/CRYSTAL/BC	Pacchetto	Classe di sviluppo
/CRYSTAL/ODS_REPORT	Gruppo di funzioni	Funzioni ODS

**Trasporto per la personalizzazione dei parametri BW Query**

Questo trasporto fornisce il supporto per i valori dei parametri personalizzati e predefiniti nei report basati sulle query BW.

Oggetto	Tipo	Descrizione
/CRYSTAL/BC	Pacchetto	Classe di sviluppo
/CRYSTAL/PERS_VAR	Struttura	Definizione della variabile
/CRYSTAL/PERS_VALUE	Struttura	Definizione valore
/CRYSTAL/PERS	Gruppo di funzioni	Funzioni di personalizzazione

**Trasporto Connettività BW MDX**

Questo trasporto consente al driver MDX Query di accedere ai cubi e alle query BW. Questo trasporto è compatibile con BW 3.0B patch 27 o superiore e BW 3.1C patch 21 o superiore.

Oggetto	Tipo	Descrizione
/CRYSTAL/BC	Pacchetto	Classe di sviluppo
/CRYSTAL/MDX	Gruppo di funzioni	Funzioni MDX
/CRYSTAL/MDX_STREAM_LAYOUT	Definizione tabella	Struttura di insieme di dati
/CRYSTAL/CX_BAPI_ERROR	Classe	Eccezione
/CRYSTAL/CX_METADATA_ERROR	Classe	Eccezione
/CRYSTAL/CX_MISSING_STREAMINFO	Classe	Eccezione

Oggetto	Tipo	Descrizione
/CRYSTAL/CX_NO_MORE_CELLS	Classe	Eccezione
/CRYSTAL/CX_NO_MORE_MEMBERS	Classe	Eccezione
/CRYSTAL/CX_NO_MORE_PROPERTIES	Classe	Eccezione
/CRYSTAL/CX_SAVE_SESSION_STATE	Classe	Eccezione
/CRYSTAL/MDX_APPEND_DATA	Classe	Processore di insieme di dati
/CRYSTAL/MDX_READER_BASE	Classe	Processore di insieme di dati
/CRYSTAL/MDX_READ_DIMENSIONS	Classe	Processore di insieme di dati
/CRYSTAL/MDX_READ_MEASURES	Classe	Processore di insieme di dati
/CRYSTAL/MDX_READ_PROPERTIES	Classe	Processore di insieme di dati
/CRYSTAL/MDX_AXIS_LEVELS	Tipo di tabella	Struttura di metadati
/CRYSTAL/MDX_PROPERTY_KEYS	Tipo di tabella	Struttura di metadati
/CRYSTAL/MDX_PROPERTY_VALUES	Tipo di tabella	Struttura di metadati



Oggetto	Tipo	Descrizione
/CRYS TAL/MDX_STREAM_LAYOUT_TAB	Tipo di tabella	Struttura di metadati

### 24.1.1.18 Panoramica sulle autorizzazioni

In questa sezione è riportato un elenco delle autorizzazioni SAP che, secondo la nostra esperienza e nel nostro ambiente di test, sono necessarie per eseguire le attività comuni della piattaforma BI in un ambiente SAP integrato. A seconda dell'implementazione individuale è possibile che siano necessari ulteriori oggetti o campi autorizzazione.

A partire da ciascun oggetto autorizzazione è necessario creare un'autorizzazione e definire i valori appropriati del campo. È quindi necessario applicare le appropriate autorizzazioni ai profili (o ruoli) degli utenti SAP. Nelle sezioni seguenti vengono descritte le autorizzazioni richieste e vengono forniti i valori necessari del campo. Per i dettagli procedurali specifici della versione di SAP, fare riferimento alla documentazione di SAP.

#### **Nota:**

- Le informazioni riportate in questa sezione vengono fornite solo a titolo indicativo.
- L'oggetto di autorizzazione ZSEGREPORT appartiene alla classe di oggetti ZSSI, installata quando si importano i file di trasporto dell'integrazione SAP necessari per il supporto delle query Open SQL.

#### 24.1.1.18.1 Creazione e applicazione delle autorizzazioni

A questo punto è necessario creare e applicare le autorizzazioni richieste da ciascun utente per accedere alle informazioni mediante Desktop Intelligence Integration for SAP. Le procedure esatte per la creazione, la configurazione e l'applicazione delle autorizzazioni dipendono dalla versione di SAP installata. In questa sezione viene fornito un elenco di autorizzazioni SAP che, in base all'esperienza pregressa e agli ambienti di prova, si sono rivelate necessarie per l'esecuzione di alcune attività standard quando si utilizza la piattaforma BI integrata in un ambiente SAP NetWeaver ABAP. A seconda dell'implementazione individuale è possibile che siano necessari ulteriori oggetti o campi autorizzazione.

#### **Argomenti correlati**

- [Configurazione della pubblicazione nel workbench per l'amministrazione dei contenuti](#)

### 24.1.1.19 Azioni in BW

In queste sezione vengono illustrate una serie di azioni eseguibili in BW.

#### 24.1.1.19.1 Azioni all'interno di Crystal Reports

*Creazione di un nuovo report da una query in un ruolo BW*

Oggetto autorizzazione	Campo	Valori
S_USER_AGR	ACT_GROUP	USER_ROLE*
	ACTVT	01, 02, 06
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	RS_PERS_BOD
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**

Oggetto autorizzazione	Campo	Valori
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16

\* *USER\_ROLE* indica il nome dei ruoli ai quali appartiene l'utente. È possibile immettere in questo campo più valori.

\* *QUERY\_OWNER* indica il nome del proprietario della query. Se si specifica un nome, è possibile creare report solo dalle query con quel proprietario. Immettere \* per creare report da query con qualsiasi proprietario.

\*\*Per *INFO\_AREA*, *INFO\_CUBE* o *COMP\_ID* immettere \* per indicare un qualsiasi valore. Se si specifica un valore, sarà possibile generare report solo dalle query che contengono tali aree di informazioni, cubi e ID componente.

#### Apertura di un report esistente da un ruolo BW

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SUSO, SUNI, RSCR, SH3A, RFC1, RZX0, RZX2, RS_PERS_BOD, /CRYSTAL/PERS, RSOB
	ACTVT	16

Oggetto autorizzazione	Campo	Valori
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16

\* *QUERY\_OWNER* indica il nome del proprietario della query da cui viene creato il report. Se si immette il nome del proprietario della query, è possibile creare report solo dalle query con questo proprietario. Immettere \* per indicare qualsiasi proprietario di query.

\*\* Per *INFO\_AREA*, *INFO\_CUBE* o *COMP\_ID* immettere \* per indicare un qualsiasi valore. Se si immette un valore specifico, è possibile creare report solo dalle query che contengono tali aree di informazioni, cubi di informazioni e ID componente.

**Anteprima o aggiornamento di un report**

Oggetto autorizzazione	Campo	Valori
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16

\* *QUERY\_OWNER* indica il nome del proprietario della query da cui viene creato il report. Se si immette il nome del proprietario della query, è possibile creare report solo dalle query con questo proprietario. Immettere \* per indicare qualsiasi proprietario di query.

\*\* Per *INFO\_AREA*, *INFO\_CUBE* o *COMP\_ID* immettere \* per indicare un qualsiasi valore. Se si immette un valore specifico, è possibile creare report solo dalle query che contengono tali aree di informazioni, cubi di informazioni e ID componente.

**Verifica del database (aggiornamento delle definizioni della tabella in un report)**

Oggetto autorizzazione	Campo	Valori
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16

\* *QUERY\_OWNER* indica il nome del proprietario della query da cui viene creato il report. Se si immette il nome del proprietario della query, è possibile creare report solo dalle query con questo proprietario. Immettere \* per indicare qualsiasi proprietario di query.

\*\* Per *INFO\_AREA*, *INFO\_CUBE* o *COMP\_ID* immettere \* per indicare un qualsiasi valore. Se si immette un valore specifico, è possibile creare report solo dalle query che contengono tali aree di informazioni, cubi di informazioni e ID componente.

*Impostazione del percorso dell'origine dati*

Oggetto autorizzazione	Campo	Valori
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16

\* *QUERY\_OWNER* indica il nome del proprietario della query da cui viene creato il report. Se si immette il nome del proprietario della query, è possibile creare report solo dalle query con questo proprietario. Immettere \* per indicare qualsiasi proprietario di query.

\*\* Per *INFO\_AREA*, *INFO\_CUBE* o *COMP\_ID* immettere \* per indicare un qualsiasi valore. Se si immette un valore specifico, è possibile creare report solo dalle query che contengono tali aree di informazioni, cubi di informazioni e ID componente.

*Salvataggio di un report in un ruolo BW*

Oggetto autorizzazione	Campo	Valori
S_USER_AGR	ACT_GROUP	USER_ROLE*
	ACTVT	01, 02, 06
S_CTS_ADMI	CTS_ADMFCT	TABL

\* *USER\_ROLE* indica il nome dei ruoli ai quali appartiene l'utente. È possibile immettere in questo campo più valori.

**Preparazione di un report per la traduzione durante il salvataggio in BW**

Oggetto autorizzazione	Campo	Valori
S_USER_AGR	ACT_GROUP	<i>USER_ROLE</i> *
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL

\* *USER\_ROLE* indica il nome dei ruoli ai quali appartiene l'utente. È possibile immettere in questo campo più valori.

**Salvataggio di un report e pubblicazione simultanea nella piattaforma BI**

Oggetto autorizzazione	Campo	Valori
S_USER_AGR	ACT_GROUP	<i>USER_ROLE</i> *
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL
S_RS_COMP	RSINFOAREA	<i>INFO_AREA</i> ***
	RSINFOCUBE	<i>INFO_CUBE</i> ***
	RSZCOMPTP	REP
	RSZCOMPID	<i>COMP_ID</i> ***



Oggetto autorizzazione	Campo	Valori
S_RS_COMP1	RSZCOMPID	COMP_ID ***
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER **
	ACTVT	16

\* *USER\_ROLE* indica il nome dei ruoli ricoperti dall'utente. È possibile immettere in questo campo più valori.

\*\* *QUERY\_OWNER* indica il nome del proprietario della query da cui viene creato il report. Se si immette il nome del proprietario della query, è possibile creare report solo dalle query con questo proprietario. Immettere \* per indicare qualsiasi proprietario di query.

\*\*\* Per *INFO\_AREA*, *INFO\_CUBE*, o *COMP\_ID* immettere \* per indicare un qualsiasi valore. Se si specifica un valore, sarà possibile generare report solo dalle query che contengono tali aree di informazioni, cubi e ID componente.

#### Avvio di BEx Query Designer

Oggetto autorizzazione	Campo	Valori
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**

Oggetto autorizzazione	Campo	Valori
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16
S_CTS_ADMI	CST_ADMFCT	TABL

\* *QUERY\_OWNER* indica il nome del proprietario della query da cui viene creato il report. Se si immette il nome del proprietario della query, è possibile creare report solo dalle query con questo proprietario. Immettere \* per indicare qualsiasi proprietario di query.

\*\* Per *INFO\_AREA*, *INFO\_CUBE* o *COMP\_ID* immettere \* per indicare un qualsiasi valore. Se si immette un valore specifico, è possibile creare report solo dalle query che contengono tali aree di informazioni, cubi di informazioni e ID componente.

#### 24.1.1.19.2 Azioni all'interno di BI Launch Pad

##### Accesso alla piattaforma BI con le credenziali SAP

Oggetto autorizzazione	Campo	Valori
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M

## Visualizzazione di un report SAP BW su richiesta

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16
S_RS_ODSO	RSINFOAREA	INFO_AREA**
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

\* *QUERY\_OWNER* indica il nome del proprietario della query da cui viene creato il report. Se si immette il nome del proprietario della query, è possibile creare report solo dalle query con questo proprietario. Immettere \* per indicare qualsiasi proprietario di query.

\*\* Per *INFO\_AREA*, *INFO\_CUBE* o *COMP\_ID* immettere \* per indicare un qualsiasi valore. Se si immette un valore specifico, è possibile creare report solo dalle query che contengono tali aree di informazioni, cubi di informazioni e ID componente.

### Aggiornamento di un report dal visualizzatore

Oggetto autorizzazione	Campo	Valori
S_RS_COMP	RSINFOAREA	<i>INFO_AREA</i> **
	RSINFOCUBE	<i>INFO_CUBE</i> **
	RSZCOMPTP	REP
	RSZCOMPID	<i>COMP_ID</i> **
S_RS_COMP1	RSZCOMPID	<i>COMP_ID</i> **
	RSZCOMPTP	REP
	RSZOWNER	<i>QUERY_OWNER</i> *
	ACTVT	16
S_RS_ODSO	RSINFOAREA	<i>INFO_AREA</i> **
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

\* *QUERY\_OWNER* indica il nome del proprietario della query da cui viene creato il report. Se si immette il nome del proprietario della query, è possibile creare report solo dalle query con questo proprietario. Immettere \* per indicare qualsiasi proprietario di query.

\*\* Per *INFO\_AREA*, *INFO\_CUBE* o *COMP\_ID* immettere \* per indicare un qualsiasi valore. Se si immette un valore specifico, è possibile creare report solo dalle query che contengono tali aree di informazioni, cubi di informazioni e ID componente.

### Pianificazione di un report

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB, SUNI
	ACTVT	16
S_RS_COMP	RSINFOAREA	<i>INFO_AREA</i> **
	RSINFOCUBE	<i>INFO_CUBE</i> **
	RSZCOMPTP	REP
	RSZCOMPID	<i>COMP_ID</i> **
S_RS_COMP1	RSZCOMPID	<i>COMP_ID</i> **
	RSZCOMPTP	REP
	RSZOWNER	<i>QUERY_OWNER</i> *
	ACTVT	16

Oggetto autorizzazione	Campo	Valori
S_RS_ODSO	RSINFOAREA	INFO_AREA**
	RSODSOBJ	0CRM_OLVM
	RSODSPART	DATA
	ACTVT	03

\* *QUERY\_OWNER* indica il nome del proprietario della query da cui viene creato il report. Se si immette il nome del proprietario della query, è possibile creare report solo dalle query con questo proprietario. Immettere \* per indicare qualsiasi proprietario di query.

\*\* Per *INFO\_AREA*, *INFO\_CUBE* o *COMP\_ID* immettere \* per indicare un qualsiasi valore. Se si immette un valore specifico, è possibile creare report solo dalle query che contengono tali aree di informazioni, cubi di informazioni e ID componente.

#### *Lettura di elenchi di scelta dinamici nei parametri del report*

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RSOB
	ACTVT	16

#### 24.1.1.19.3 Azioni all'interno di SAP Netweaver (ABAP)

##### *Da Crystal Reports mediante il driver Open SQL*

In questa sezione vengono illustrate diverse azioni eseguibili in SAP NetWeaver (ABAP) dall'interfaccia di Crystal Reports mediante il driver Open SQL.

*Connessione a un server SAP*

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQ
	ACTVT	16

*Creazione di un nuovo report*

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQ
	ACTVT	16
ZSEGREPORT	ACTVT	01

*Apertura o anteprima di un report esistente*

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQ
	ACTVT	16
ZSEGREPORT	ACTVT	02

*Verifica del database (aggiornamento delle definizioni della tabella in un report)*

Oggetto autorizzazione	Campo	Valori
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQ
	ACTVT	16

*Impostazione del percorso dell'origine dati*

Oggetto autorizzazione	Campo	Valori
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQ
	ACTVT	16



#### 24.1.1.19.4 Azioni all'interno di Crystal Reports mediante il driver InfoSet e la creazione di report InfoSet

##### Connessione a un server SAP

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

##### Creazione di un nuovo report da un InfoSet su SAP Netweaver (ABAP)

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/FLAT, SKBW, AQRC
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL

##### **Nota:**

aggiungere inoltre un numero sufficiente di autorizzazioni per visualizzare le righe di dati. Ad esempio P\_ORIG o P\_APAP.

##### **Argomenti correlati**

- [Impostazione del percorso dell'origine dati](#)

*Verifica del database (aggiornamento delle definizioni della tabella in un report)*

Oggetto autorizzazione	Campo	Valori
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M

*Impostazione del percorso dell'origine dati*

Oggetto autorizzazione	Campo	Valori
P_ABAP	REPID	AQTGSYSTGENERATESY, SAPDBPNP
	COARS	2

## 24.1.1.19.5 Azioni all'interno di Crystal Reports mediante il driver InfoSet e la creazione di report da una query ABAP

*Connessione a un server SAP*

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

*Creazione di un nuovo report da una query ABAP su SAP Netweaver*

Oggetto autorizzazione	Campo	Valori
P_ABAP	REPID	AQTG02=====P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
S_TABU_DIS	ACTVT	03
	GROUP	Nome del gruppo di tabelle

*Verifica del database*

Oggetto autorizzazione	Campo	Valori
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16

*Impostazione del percorso dell'origine dati*

Oggetto autorizzazione	Campo	Valori
P_ABAP	REPID	AQTG02=====P6, SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	ST0R, ST0M
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16
S_TABU_DIS	ACTVT	03
	GROUP	Nome del gruppo di tabelle

## 24.1.1.19.6 Azioni all'interno della piattaforma BI

*Pianificazione di un report in modalità di dialogo (con una query Open SQL)*

Oggetto autorizzazione	Campo	Valori
S_USER_GRP	CLASS	
	ACTVT	03

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPE- NSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

**Nota:**

il valore per CLASS è BLANK.

*Pianificazione di un report in modalità batch con una query Open SQL*

Oggetto autorizzazione	Campo	Valori
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, RFC1, /CRYSTAL/OPE- NSQL, SH3A
	ACTVT	16
S_BTCH_JOB	JOBGROUP	' '
	JOBACTION	RELE
ZSEGREPORT	ACTVT	02
S_BTCH_ADM	BTCADMIN	Y

**Nota:**

il valore per CLASS è BLANK.

*Sistema di autorizzazione Crystal*

Oggetto autorizzazione	Campo	Valore
Autorizzazione per l'accesso ai file (S_DATASET)	Attività (ACTVT)	Lettura, scrittura (33, 34)
	Nome file fisico (FILENAME)	* (indica Tutti)
	Nome programma ABAP (PROGRAM)	*
Verifica autorizzazione per l'accesso RFC (S_RFC)	Attività (ACTVT)	16
	Nome dell'RFC da proteggere (RFC_NAME)	BDCH, STPA, SUSO, SUUS, SU_USER, SYST, SUNI, PRGN_J2EE, /CRYSTAL/SECURITY
	Tipo di oggetto RFC da proteggere (RFC_TYPE)	Gruppo di funzioni (FUGR)
Manutenzione master utente: gruppi di utenti (S_USER_GRP)	Attività (ACTVT)	Crea o Genera, e Visualizza (03)
	Gruppo di utenti nella manutenzione master utente (CLASS)	<p>*</p> <p><b>Nota:</b> Per maggiore sicurezza, si consiglia di elencare esplicitamente i gruppi di utenti i cui membri richiedono l'accesso alla piattaforma BI.</p>

*Esecuzione e progettazione di query BW BEx*

Quando si crea un report da un universo basato su una query BW BEx, se si include una dimensione data, l'amministratore di sistema deve concedere l'autorizzazione S\_RS\_IOBJ sia all'utente che progetta l'universo che all'utente che esegue il report.

Oggetto autorizzazione	Campo	Valori
S_RS_IOBJ	ACTVT	03
	RSIOBJ	
	RSIOBJ_CAT	
	RSIOBJ_PART	

## 24.2 Configurazione per l'integrazione JD Edwards

### 24.2.1 Configurazione del Single Sign On (SSO) per SAP Crystal Reports

Per impostazione predefinita, la piattaforma BI verrà configurata per consentire agli utenti di SAP Crystal Reports di accedere ai dati JD Edwards EnterpriseOne mediante il Single Sign On (SSO).

#### 24.2.1.1 Disattivazione di SSO per JD Edwards e SAP Crystal Reports

1. Nella CMC (Central Management Console), fare clic su **Applicazioni**.
2. Fare doppio clic su **Configurazione di Crystal Reports**.
3. Fare clic su **Opzioni Single Sign On**.
4. Selezionare **crdb\_pseone**.

5. Fare clic su **Rimuovi**.
6. Fare clic su **Salva e chiudi**.
7. Nella pagina **Server** della CMC selezionare **Crystal Reports Services**, quindi fare clic su **Riavvia il server**.

### 24.2.1.2 Attivazione di SSO per JD Edwards e SAP Crystal Reports

Se è stato disattivato il SSO per JD Edwards e SAP Crystal Reports e si desidera riattivarlo, seguire la procedura seguente.

1. Nella CMC (Central Management Console), fare clic su **Applicazioni**.
2. Fare doppio clic su **Configurazione di Crystal Reports**.
3. Fare clic su **Opzioni Single Sign On**.
4. Al di sotto di "Utilizza il contesto SSO per accedere al database con i driver seguenti" digitare **crdb\_pseone**.
5. Fare clic su **Aggiungi**.
6. Fare clic su **Salva e chiudi**.
7. Nella pagina **Server** della CMC selezionare **Crystal Reports Services**, quindi fare clic su **Riavvia il server**.

### 24.2.2 Configurazione delle integrazioni di Secure Socket Layer per JD Edwards

È possibile utilizzare il protocollo SSL (Secure Sockets Layer) per tutte le comunicazioni di rete tra i client e i server nella distribuzione della piattaforma BI e JD Edwards EnterpriseOne.

L'utilizzo dei dati di JD Edwards EnterpriseOne con la piattaforma BI comporta alcune modifiche alla configurazione SSL. Come per la configurazione SSL per gli altri server e client della piattaforma BI, memorizzare i seguenti file di chiavi e certificati in una posizione sicura (nella stessa directory) a cui possono accedere i computer della distribuzione della piattaforma BI.

- Il file del certificato attendibile (cacert.der).
- Il file del certificato del server generato (servercert.der).
- Il file delle chiavi del server (server.key).
- Il file della passphrase (passphrase.txt).

#### 24.2.2.1 Per abilitare la connettività dati JD Edwards EnterpriseOne con SSL



**Nota:**

Tutti i valori descritti nella procedura seguente fanno distinzione tra maiuscole e minuscole.

1. Avviare il Central Configuration Manager (CCM).
2. Interrompere il Server Intelligence Agent.
3. Fare doppio clic sul SIA per aprire la finestra di dialogo "Proprietà".
4. Fare clic sulla scheda **Protocollo**.
5. Selezionare **Abilita SSL**.
6. Per "Cartella certificati SSL" scegliere la directory che contiene i certificati SSL.
7. Per "File di certificato SSL server" scegliere `servercert.der`.
8. Per "File dei certificati SSL attendibili" scegliere `cacert.der`.
9. Per "File chiave privata SSL" scegliere `server.key`.
10. Per "File della password lunga di chiave privata" scegliere `passphrase.txt`.
11. Fare clic su **Applica**.
12. Avviare Server Intelligence Agent.

Riavviare i server di report della piattaforma BI (ad esempio, Adaptive Job Server) per applicare le modifiche.

#### 24.2.2.2 File delle proprietà di configurazione SSL

Il file delle proprietà `sslconf.properties` contiene tutte le informazioni per i certificati e le chiavi richiesti utilizzati dalla piattaforma BI. Ad esempio:

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

Il file `sslconf.properties` deve essere inserito nella cartella di installazione della piattaforma BI, ovvero `C:\Programmi\Business Objects\BusinessObjects 13.0` per impostazione predefinita.

### 24.3 Configurazione per l'integrazione PeopleSoft Enterprise

### 24.3.1 Configurazione di Single Sign-On (SSO) per SAP Crystal Reports e PeopleSoft Enterprise

Per impostazione predefinita, la piattaforma BI verrà configurata per consentire agli utenti di SAP Crystal Reports di accedere ai dati PeopleSoft Enterprise mediante il Single Sign On (SSO).

#### 24.3.1.1 Disattivazione di SSO per PeopleSoft Enterprise e SAP Crystal Reports

1. Nella Central Management Console (CMC) fare clic su **Applicazioni**.
2. Fare doppio clic su **Configurazione di Crystal Reports**.
3. Fare clic su **Opzioni Single Sign On**.
4. Selezionare **crdb\_psenterprise**.
5. Fare clic su **Rimuovi**.
6. Fare clic su **Salva e chiudi**.
7. Nella pagina **Server** della CMC selezionare **Crystal Reports Services**, quindi fare clic su **Riavvia il server**.

#### 24.3.1.2 Attivazione di SSO per PeopleSoft Enterprise e SAP Crystal Reports

Se SSO per PeopleSoft Enterprise e SAP Crystal Reports è stato disattivato e si desidera riattivarlo, procedere come descritto di seguito.

1. Nella Central Management Console (CMC) fare clic su **Applicazioni**.
2. Fare doppio clic su **Configurazione di Crystal Reports**.
3. Fare clic su **Opzioni Single Sign On**.
4. Al di sotto di "Utilizza il contesto SSO per accedere al database con i driver seguenti" digitare **crdb\_psenterprise**.
5. Fare clic su **Aggiungi**.
6. Fare clic su **Salva e chiudi**.
7. Nella pagina **Server** della CMC selezionare **Crystal Reports Services**, quindi fare clic su **Riavvia il server**.

## 24.3.2 Configurazione per le comunicazioni Secure Sockets Layer

È possibile utilizzare il protocollo Secure Sockets Layer (SSL) per tutte le comunicazioni di rete tra client e server nella distribuzione della piattaforma BI.

Come per la configurazione SSL per gli altri server e client della piattaforma BI, memorizzare i seguenti file di chiavi e certificati in una posizione sicura (nella stessa directory) a cui possono accedere i computer della distribuzione della piattaforma BI.

- Il file del certificato attendibile (cacert.der).
- Il file del certificato del server generato (servercert.der).
- Il file delle chiavi del server (server.key).
- Il file della passphrase (passphrase.txt).

### 24.3.2.1 File delle proprietà di configurazione SSL

Il file delle proprietà `sslconf.properties` contiene tutte le informazioni per le chiavi e i certificati richiesti utilizzati dai componenti della piattaforma BI. Ad esempio:

```
[default]
businessobjects.ora.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

Il file `sslconf.properties` deve essere inserito nella cartella in cui è installata la piattaforma BI. Per impostazione predefinita, la cartella è `C:\Programmi\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\`.

### 24.3.2.2 Per abilitare PeopleSoft Query Server con SSL

#### **Nota:**

Tutti i valori descritti nella procedura seguente fanno distinzione tra maiuscole e minuscole.

- Configurare i due valori del registro sotto la chiave del registro per ogni server di query, ad esempio:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Business
Objects\Suite 12.0\Integration Kit for
PeopleSoft\QRY\Instances\noname]
"CommunicationProtocol"="ssl"
"SSL Configuration File"="C:\Program
```

```
Files\Business Objects\BusinessObjects 12.0 Integration Kit for
PeopleSoft\sslconf.properties"
```

Riavviare i server di report della piattaforma BI (ad esempio, Adaptive Job Server) per applicare le modifiche.

### 24.3.2.3 Per abilitare il ponte di protezione con SSL

#### Nota:

Tutti i valori descritti nella procedura seguente fanno distinzione tra maiuscole e minuscole.

- Eseguire `crpsepmsecuritybridge.bat` con gli argomenti seguenti aggiungendoli al file `.bat`.

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir="d:\ssl"
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
```

Assicurarsi che gli argomenti vengano aggiunti nella posizione corretta nel file `.bat`, a destra dopo `java.exe` e prima degli argomenti `-jar`. Ad esempio:

```
@ECHO OFF
SETLOCAL
SET PATH=%PATH%;C:\Program Files\Business
Objects\BusinessObjects Enterprise 12.0\win32_x86\;C:\Program
Files\Business Objects\BusinessObjects 12.0 Integration Kit for
PeopleSoft\epm;
"C:\Program Files\Business Objects\javasdk\bin\java.exe" -Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir="C:\!test" -DtrustedCert=cacert.der
-DsslCert=servercert.der -DsslKey=server.key
-Dpassphrase=passphrase.txt -jar "C:\Program Files\Business
Objects\BusinessObjects 12.0 Integration Kit for
PeopleSoft\epm\crpsepmsecuritybridge.jar" %1 "language"
"C:\Program Files\Business
Objects\LanguagePacks.xml\LanguagePacks.xml"
```

La tabella seguente mostra le descrizioni degli esempi riportati:

DcertDir=d:\ssl	La directory in cui memorizzare tutti i certificati e le chiavi.
DtrustedCert=cacert.der	File del certificato sicuro. Se si specificano più file, utilizzare il punto e virgola come separatore.
DsslCert=clientcert.der	Certificato utilizzato dall'SDK.
DsslKey=client.key	Chiave privata del certificato SDK.

Dpassphrase=passphrase.txt	Il file che memorizza la passphrase per la chiave privata.
----------------------------	------------------------------------------------------------

### 24.3.3 Regolazione delle prestazioni per i sistemi PeopleSoft

Per assicurare prestazioni ottimali durante la creazione di query PeopleSoft, è importante comprendere come vengono eseguite le query in Crystal Reports e nella piattaforma BI.

Ogni volta che si aggiorna o si esegue un report basato su una query PeopleSoft, viene stabilita una connessione con un server PeopleSoft:

- Negli ambienti PeopleSoft Enterprise (PeopleTools 8.46 o versione successiva), viene stabilita una connessione a PeopleSoft Analytic Server.
- Negli ambienti PeopleSoft Enterprise (PeopleTools 8.21-8.45), viene stabilita una connessione a PeopleSoft Application Server.

#### 24.3.3.1 Suggerimenti

In una distribuzione ottimale vengono impostati uno o più PeopleSoft Analytic/Application Server per gestire esclusivamente le richieste di report. In ciascuno di questi server le impostazioni relative al numero minimo e massimo di istanze consentono di controllare il numero delle richieste di report che possono essere elaborate ogni volta. Questa impostazione offre i seguenti vantaggi:

- Nessuna disputa tra le richieste di report e le richieste transazionali nel server PeopleSoft.
- Possibilità di eseguire attività di gestione sul server che gestisce le richieste di report senza disabilitare il server che gestisce le richieste transazionali.

In un ambiente in cui sia le richieste di report che quelle transazionali vengono gestite da un unico server PeopleSoft Analytic/Application Server, è necessario configurare la piattaforma BI in modo che non venga eseguito più di un report alla volta. In caso contrario, se tutti i processi PSANALYTICSRV o PSAPPSRV vengono utilizzati per l'esecuzione dei report, gli utenti non saranno in grado di effettuare richieste transazionali.

#### **Nota:**

- Per informazioni su come limitare il numero di processi report pianificati e di processi di visualizzazione di report su richiesta, consultare la sezione "Gestione e configurazione dei server" nel *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

- non è possibile configurare il sistema per limitare il numero di utenti Crystal Reports che tentano di accedere contemporaneamente al server.

In caso di problemi relativi alle prestazioni, utilizzare lo strumento di configurazione Psadmin per stabilire se le richieste vengono messe in coda. È anche possibile monitorare le risorse del sistema sul computer PeopleSoft Analytic/Application Server. Se in mancanza di memoria fisica viene utilizzata la memoria virtuale, anche l'elaborazione può risultare rallentata.

### 24.3.3.2 Server PeopleSoft

In un PeopleSoft Analytic Server il processo che aggiorna o esegue i report è il processo PSANALYTICSRV. In un PeopleSoft Application Server il processo che aggiorna o esegue i report è il processo PSAPPSRV. Il numero di processi PSANALYTICSRV o PSAPPSRV disponibili determina il numero di report che è possibile eseguire contemporaneamente.

Un file di configurazione PeopleSoft Analytic/Application Server tipico contiene le informazioni seguenti:

```
Min Instances=3
Max Instances=5
```

In questo esempio sono sempre disponibili da un minimo di tre a un massimo di cinque processi PSANALYTICSRV o PSAPPSRV. Ciò non significa necessariamente che è possibile eseguire contemporaneamente cinque report; inoltre, i processi possono essere utilizzati per gestire altre attività del sistema. Se non è disponibile alcun processo PSANALYTICSRV o PSAPPSRV per gestire una richiesta, questa viene messa in coda finché non ne risulterà disponibile uno.

#### **Nota:**

In genere il file di configurazione dei PeopleSoft Application Server include anche il parametro `Service Timeout`, che specifica il tempo di attesa per un processo disponibile. Se nessun processo diventa disponibile entro il periodo di tempo indicato dal parametro, la richiesta scade.

## 24.4 Configurazione per l'integrazione Siebel

### 24.4.1 Configurazione di Siebel per l'integrazione con la piattaforma SAP BusinessObjects Business Intelligence

L'integrazione della piattaforma BI rende disponibile un collegamento a Crystal Reports che consente di incorporare il contenuto della suite SAP BusinessObjects Business Intelligence in un'applicazione

Siebel. Dopo l'installazione e la configurazione, la nuova voce di menu consente agli utenti di avviare BI Launch Pad dall'applicazione Siebel.

Per impostazione predefinita, i file necessari vengono installati nella cartella seguente: C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\.

**Nota:**

le sottocartelle Siebel 7.7 e Siebel 8.0 contengono file diversi da utilizzare con le due diverse versioni.

### 24.4.1.1 Importazione del progetto di integrazione Siebel della piattaforma BI

1. Avviare Siebel Tools.
2. Fare clic su **Tools > Import from Archive**.
3. Alla richiesta di indicare un file archivio, passare alla cartella Siebel Files dell'installazione del prodotto Integration.  
Per impostazione predefinita, si tratta della cartella: *DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\*.
4. Passare alla sottocartella appropriata (Siebel 7.7 o Siebel 8.0) e selezionare il file *BusinessObjectsEnterprise.sif*.  
Viene visualizzata l'Importazione guidata.
5. Fare clic su **Unisci la definizione dell'oggetto nel file di archivio con la definizione nel repository**.
6. Seguire le istruzioni contenute nelle varie schermate della procedura guidata per completare l'importazione del progetto di integrazione.  
Il progetto di integrazione viene aggiunto al repository.
7. Bloccare il progetto **BusinessObjects Integration**.

### 24.4.2 Creazione della voce di menu Crystal Reports

1. In Siebel Tools, bloccare il progetto **Menu**.
2. In Explorer oggetti selezionare l'oggetto **Menu Item**.

**Nota:**

se l'oggetto Menu non viene visualizzato in Explorer oggetti, fare clic su **View > Options** in Siebel Tools, fare clic sulla scheda **Object Explorer** e selezionare l'oggetto **Menu**.

3. Nell'elenco **Menus** selezionare il menu **Generic Web**.
4. Fare clic sull'intestazione **Menu Items**.
5. Fare clic su **Edit > New Record**.

6. Definire appropriatamente la nuova voce di menu. I valori consigliati sono i seguenti:
    - Name: Vista - Crystal Reports
    - Command: Crystal Reports
    - Comments: Menu Report integrati di SAP BusinessObjects
    - Inactive: Falso
  7. Utilizzare un numero per selezionare una posizione per la voce di menu nel menu View.  
Per facilitare la scelta di un numero di posizione, ordinare le voci di menu per posizione.
  8. A questo punto è possibile aggiungere record di impostazioni locali per localizzare la didascalia in base alle preferenze.
- Ricompilare l'applicazione Siebel. Consultare [Ricompilazione dell'applicazione Siebel](#).

### 24.4.2.1 Ricompilazione dell'applicazione Siebel

Una volta installata la piattaforma BI e aver reso disponibile per gli utenti il relativo comando mediante una voce di menu Siebel, è necessario ricompilare l'applicazione Siebel attenendosi alle procedure consuete. Per ulteriori informazioni, consultare Siebel Bookshelf.

Dopo avere ricompilato l'applicazione Siebel, rigenerarne i file JavaScript. In Siebel 7.7 e versioni successive è possibile rigenerare automaticamente i file JavaScript nell'ambito del processo di ricompilazione.

Poiché le operazioni necessarie per compilare il repository Siebel vengono eseguite nella workstation Siebel Tools, è necessario distribuire i file JavaScript risultanti dalla workstation Siebel Tools al server Siebel in uso. Di solito, a seconda della posizione di installazione di Siebel, i file JavaScript generati si trovano nella posizione seguente:

```
C:\sea77\tools\PUBLIC\ENU\srf1096416329_444
```

Il nome della cartella, nell'esempio *srf1096416329\_444*, viene generato da Siebel Tools e corrisponde in modo univoco al file repository risultante.

I file JavaScript devono essere distribuiti nel server Siebel, generalmente nella posizione seguente, a seconda della posizione di installazione di Siebel:

```
C:\sea77\SWEApp\PUBLIC\ENU\srf1096416329_444
```

È importante non modificare il nome della cartella generato da Siebel Tools.

Per abilitare il servizio, è inoltre necessario aggiornare il file di configurazione di Siebel nel computer che ospita il server Siebel. Individuare il file di configurazione appropriato nel computer che esegue il server Siebel. Se ad esempio si esegue una versione inglese di Siebel Call Center, utilizzare *uagent.nt.cfg*. Per impostazione predefinita il file si trova in *C:\sea77\siebsrvr\bin\ENU\* per Siebel 7.7.



Quindi aggiungere la riga seguente alla fine della sezione SWE del file di configurazione:

```
ClientBusinessServiceNUMBER = BusinessObjects Integration Service
```

I numeri `ClientBusinessService` sono sequenziali. Se nella sezione SWE non vi sono altri numeri `ClientBusinessService`, impostare `NUMBER` su 0. In caso contrario impostare `NUMBER` sul valore maggiore successivo.

Per Siebel 8.x o versioni successive:

1. Accedere a Siebel Tools e individuare l'oggetto applicazione **Siebel Universal Agent** in Explorer oggetti.
2. Espandere gli oggetti applicazione per visualizzare l'oggetto **Application User Prop**.
3. Creare un nuovo record per ogni servizio aziendale da dichiarare, impostando le proprietà Name e Value come indicato di seguito:
  - Name = ClientBusinessServiceX
  - Value = BusinessObjects Integration

A questo punto è possibile creare la voce di menu Crystal Reports che richiama il comando Siebel importato.

### 24.4.3 Contextual Awareness

Contextual Awareness è una funzionalità che presenta all'utente i report potenzialmente pertinenti rispetto all'attività corrente. In tal caso agli utenti che accedono a Crystal Reports direttamente da un'applicazione client Siebel vengono visualizzati automaticamente i report predisposti per contenere i dati Siebel.

#### 24.4.3.1 Configurazione di Contextual Awareness

Prima di configurare la sensibilità contestuale, verificare di avere eseguito le operazioni seguenti:

- installazione del prodotto Integration per Siebel
- configurazione di Siebel per l'integrazione con la piattaforma BI

1. Aprire Central Management Console (CMC).

2. Fare clic su **Autenticazione**.

3. Fare doppio clic su **Siebel**.

Viene visualizzata l'interfaccia di mappatura Siebel.

4. Fare clic su **Domini**.

Viene visualizzata l'interfaccia di mappatura domini.

5. Prendere nota del nome del dominio che corrisponde al server Siebel che si desidera utilizzare.

6. Chiudere l'interfaccia di mappatura Siebel.
7. Aprire BI Launch Pad.
8. Creare una nuova cartella in `PublicFolders\Siebel` con lo stesso nome del dominio Siebel nella CMC.
9. Copiare in questa cartella i report designati per incorporare i dati Siebel.

### 24.4.3.2 Indicazione dell'URL del componente Contextual Awareness

1. Una volta rigenerati i file JavaScript dell'applicazione, aprire la cartella Siebel Files dell'installazione della piattaforma BI, il cui percorso predefinito è `C:\Programmi\Business Objects\SAP BusinessObjects Enterprise XI\Siebel Files\`.
2. Copiare il file `BusinessObjectsEnterpriseServer.html`. Individuare quindi la cartella pubblica in cui il programma `genbscript` ha generato i nuovi file JavaScript e inserire una copia di `BusinessObjectsEnterpriseServer.html` nella sottocartella della lingua appropriata.

Se ad esempio i file JavaScript di un'applicazione sono stati generati nella cartella `c:\sea752\SWEApp\PUBLIC\ENU` del server Siebel, copiare il file `BusinessObjectsEnterpriseServer.html` nella cartella `c:\sea752\SWEApp\PUBLIC\ENU`.

3. Aprire il file `BusinessObjectsEnterpriseServer.html` dalla cartella pubblica in un editor di testo come Blocco note e individuare le righe seguenti:

```
Var userDomain = "SIEB78"

var destAddr = "http://server SAP
BusinessObjects:8080/BOE/BI/logon/siebelStart.do"
```

#### **Nota:**

- se si modifica la variabile `userDomain` o `destAddr`, cancellare le pagine Web memorizzate nella cache del browser per avere la certezza che il browser farà riferimento all'indirizzo di destinazione corretto.
- la variabile `userDomain` fa la distinzione tra maiuscole e minuscole.

### 24.4.3.3 Verifica della funzionalità Contextual Awareness

1. In Siebel Tools fare clic su **Debug > Start**.
2. Visualizzare uno schermo qualsiasi e fare clic sul menu **View**.  
Il menu conterrà la nuova voce Crystal Reports.
3. Fare clic sulla voce di menu **Crystal Reports**.

Nella piattaforma BI si apre la finestra BI Launch Pad che richiede nome utente e password per la connessione. L'immissione di nome utente e password è necessaria solo al primo accesso in seguito a un timeout di sessione. Il nome di dominio configurato in html e l'autenticazione Siebel sono già impostati.

**Nota:**

questo passaggio ha esclusivamente lo scopo di verificare l'installazione fino a questo punto. Non è possibile accedere alla piattaforma BI con l'autenticazione Siebel se le responsabilità Siebel non sono state prima mappate alla piattaforma BI.

#### 24.4.3.4 Aggiunta delle cartelle alla piattaforma BI

L'integrazione della piattaforma BI per Siebel richiede l'aggiunta di alcune cartelle a BI Launch Pad per abilitare completamente la funzionalità Contextual Awareness.

La cartella della funzionalità deve infatti presentare la struttura seguente: *Cartelle pubbliche\Siebel\Nome dominio*. Solo i report memorizzati nella sottocartella *Nome dominio* e configurati nel sistema Siebel per l'associazione allo specifico componente business di SAP Business Objects verranno visualizzati nell'ambito della funzionalità Contextual Awareness. Il *Nome dominio* utilizzato qui deve essere uguale al nome di dominio configurato per Siebel nella configurazione dell'autenticazione e corrispondere al valore configurato nel file *BusinessObjectsEnterpriseServer.html* in Siebel.

**Nota:**

per completare la procedura di questa sessione è necessario disporre di Siebel Tools.

#### 24.4.4 Configurazione di Single Sign-On (SSO) per SAP Crystal Reports e Siebel

Per impostazione predefinita, la piattaforma BI viene configurata per consentire agli utenti di SAP Crystal Reports di accedere ai dati Siebel utilizzando il Single Sign On (SSO).

##### 24.4.4.1 Disattivazione di SSO per Siebel e SAP Crystal Reports

1. Nella Central Management Console (CMC) fare clic su **Applicazioni**.
2. Fare doppio clic su **Configurazione di Crystal Reports**.
3. Fare clic su **Opzioni Single Sign On**.
4. Selezionare **crdb\_siebel**.

5. Fare clic su **Rimuovi**.
6. Fare clic su **Salva e chiudi**.
7. Riavviare SAP Crystal Reports.

#### 24.4.4.2 Attivazione di SSO per Siebel e SAP Crystal Reports

Se SSO per Siebel e SAP Crystal Reports è stato disattivato e si desidera riattivarlo, procedere come descritto di seguito.

1. Nella Central Management Console (CMC) fare clic su **Applicazioni**.
2. Fare doppio clic su **Configurazione di Crystal Reports**.
3. Fare clic su **Opzioni Single Sign On**.
4. "In Utilizza il contesto SSO per accedere al database..." digitare **crdb\_siebel**.
5. Fare clic su **Aggiungi**.
6. Fare clic su **Salva e chiudi**.
7. Riavviare i server SAP Crystal Reports.

#### 24.4.5 Configurazione per le comunicazioni Secure Sockets Layer

È possibile utilizzare il protocollo Secure Sockets Layer (SSL) per tutte le comunicazioni di rete tra client e server presenti nelle distribuzioni Siebel e della piattaforma BI.

Come per la configurazione SSL eseguita per gli altri server e client della piattaforma BI, memorizzare i seguenti file di chiavi e certificati in una directory sicura, accessibile ai computer della distribuzione Siebel.

- Il file del certificato attendibile (cacert.der).
- Il file del certificato del server generato (servercert.der).
- Il file delle chiavi del server (server.key).
- Il file della passphrase (passphrase.txt).

##### File delle proprietà di configurazione SSL

Il file delle proprietà `sslconf.properties` contiene tutte le informazioni per i certificati e le chiavi necessari utilizzati dai componenti di Integration for Siebel. Ad esempio:

```
businessobjects.orb.ocj.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

**Il file `sslconf.properties` deve essere inserito nella cartella in cui è installata la piattaforma BI, ovvero `C:\Programmi\Business Objects\SAP BusinessObjects Enterprise XI\` per impostazione predefinita.**



# Gestione e configurazione dei registri

## 25.1 Registrazione delle analisi dei componenti

### File di registro

La piattaforma BI genera messaggi a livello di sistema e li scrive nei file di registro. Gli amministratori di sistema possono utilizzare questi file di registro per monitorare le prestazioni o per eseguire il debug degli errori.

### Analisi

La piattaforma BI genera inoltre analisi (registrazioni di eventi che si verificano durante il funzionamento di un componente monitorato) e le raccoglie in file di registro con l'estensione `.glf`. Gli eventi analizzati variano da messaggi di stato a errori di eccezione gravi. Gli sviluppatori e il personale di supporto SAP possono utilizzare le analisi per creare report sulle prestazioni dei componenti della piattaforma BI (server e applicazioni Web) e sull'attività dei componenti monitorati.

Quando si imposta il livello del registro di analisi per un componente, si stabilisce il tipo e il dettaglio delle informazioni inviate al file di registro. Il livello del registro di traccia è un filtro che sopprime le analisi che si trovano sotto una determinata soglia. Grazie al monitoraggio del registro di analisi di un componente, è possibile stabilire se è necessario modificare l'istanza corrente del componente o la relativa configurazione per poter gestire un aumento del carico di lavoro.

### **Nota:**

È possibile visualizzare i file di registro della piattaforma BI con qualsiasi editor di testo.

## 25.2 Livelli del registro di analisi

Per i componenti della piattaforma BI sono disponibili i livelli del registro di analisi seguenti:

Livello	Descrizione
Non specificato	Il livello del registro di analisi viene specificato mediante altri meccanismi, in genere un file con estensione <code>ini</code> .
Nessuno	L'analisi non viene eseguita.
Basso	Il filtro del registro di analisi consente di registrare i messaggi di errore ignorando nel contempo i messaggi di avviso e di stato. Vengono registrati messaggi di stato importanti che si riferiscono a messaggi di richiesta di inizio e fine, di arresto e avvio dei componenti. L'impostazione di questo livello non è consigliata per le finalità di debug.
Medio	Il filtro del registro di analisi è impostato in modo da includere i messaggi di errore, avviso e la maggior parte dei messaggi di stato. I messaggi di stato meno importanti o eccessivamente dettagliati vengono esclusi. Questo livello non è sufficientemente dettagliato per le finalità di debug.
Alto	Non viene escluso alcun messaggio. L'impostazione di questo livello è consigliata per le finalità di debug.  <b>Avvertenza:</b> Questo livello del registro di analisi influisce in modo significativo sulle risorse di sistema, sull'aumento dell'utilizzo della CPU e sull'impiego della spazio di archiviazione.

## 25.3 Configurazione dell'analisi per i server

Un messaggio di registro è un record permanente relativo agli eventi e allo stato di un sistema software. Le analisi relative a una distribuzione monitorata della piattaforma BI vengono scritte in un file di registro `.glf` specifico e archiviate nella directory di registrazione.

- In Windows il percorso predefinito è `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\logging`
- In Unix il percorso predefinito è `DIRINSTALL/sap_bobj/logging`

Il nome del file di registro `.glf` include un identificatore abbreviato, il nome del server e un numero di riferimento, ad esempio `aps_mysia.AdaptiveProcessingServer_trace.000012.glf`. Quando la dimensione del file di registro si avvicina alla soglia di 1 MB viene creato un nuovo file di registro di analisi per il server monitorato. Vengono inoltre mantenuti cinque file di registro alla volta; via via che i file di registro vengono creati, vengono eliminati quelli vecchi.

È possibile valutare la gravità e l'importanza delle analisi raccolte nel file di registro impostando il livello del registro di analisi per un determinato server o gruppo di server.



**Nota:**

Per modificare i livelli dei registri di analisi per specifici server o per un gruppo di server, utilizzare il servizio registro di analisi nella CMC (Central Management Console). Per modificare altri parametri, cambiare manualmente il livello del registro di analisi e altre impostazioni nel file `BO_trace.ini`.

### 25.3.1 Per impostare il livello del registro nella console CMC

È possibile regolare il livello del registro di analisi per un server senza influire sulle altre impostazioni di analisi.

1. Nell'area "Server" della CMC, accedere a un server.
  - Selezionare un server da una categoria specifica.
  - Fare clic su **Elenco server** nel pannello di spostamento per accedere all'elenco completo di server e selezionare un server.
2. Fare clic con il pulsante destro del mouse sul server selezionato e scegliere **Proprietà**. Viene visualizzata la finestra di dialogo "Proprietà".
3. Nell'area del "servizio Registro di analisi" selezionare un'impostazione nell'elenco **Livello di registrazione**.
4. Fare clic su **Salva e chiudi**.

Il nuovo livello del registro di analisi ha effetto immediatamente.

Per specificare un'altra directory di output per i file di registro, includere il parametro `-loggingPath directory_destinazione` nell'area "Parametri riga di comando". Riavviare il server per rendere effettiva questa impostazione.

**Argomenti correlati**

- [Livelli del registro di analisi](#)

### 25.3.2 Per impostare il livello del registro per più server nella console CMC

1. Nell'area "Server" della CMC accedere a più server.
  - Selezionare i server da una categoria specifica.
  - Fare clic su **Elenco server** nel pannello di spostamento per accedere all'elenco completo dei server. Tenere premuto **Ctrl** e fare clic su più server per selezionarli.
2. Fare clic con il pulsante destro del mouse sui server selezionati e scegliere **Modifica servizi comuni**. Viene visualizzata la finestra di dialogo "Modifica servizi comuni".

3. Nell'area del "servizio Registro di analisi" selezionare un'impostazione nell'elenco **Livello di registrazione**.
4. Fare clic su **OK**.

Il nuovo livello del registro di analisi ha effetto immediatamente.

Per specificare un'altra directory di output per i file di registro, includere il parametro `-loggingPath directory_destinazione` nell'area "Parametri riga di comando". Riavviare il server per rendere effettiva questa impostazione.

#### **Argomenti correlati**

- [Livelli del registro di analisi](#)

### **25.3.3 Per configurare l'analisi del server tramite il file BO\_trace.ini**

Per impostazione predefinita, il file `BO_trace.ini` registra solo errori e asserzioni.

1. Aprire il file `BO_trace.ini`.
  - In Windows il percorso predefinito è `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\conf\`
  - In Unix il percorso predefinito è `DIRINSTALL/sap_bobj/enterprise_xi40/conf/`
2. Rimuovere il commento relativo alle righe nella sezione "Trace Syntax and Setting".
3. Modificare i parametri di analisi del server. Per la configurazione dell'analisi del server vengono utilizzati i parametri seguenti:

Parametro	Valori possibili	Descrizione
sap_log_level	log_information log_warning log_error log_fatal log_none	<p>Determina la gravità dei messaggi registro. La gravità predefinita è log_error.</p> <p>La gravità dei registri segue una gerarchia, con log_information al livello più alto e log_none a quello più basso. Quando si imposta un livello di gravità dei registri, vengono visualizzati tutti i messaggi di tale livello e dei livelli inferiori. Se, ad esempio, si imposta la gravità dei registri su log_warning, i messaggi che includono log_warning, log_error e log_fatal vengono scritti nel file di registro.</p> <p><b>Nota:</b> log_information e log_warning possono essere abbreviati in log_info e log_warn.</p>
sap_trace_level	trace_debug trace_path trace_information trace_error trace_none	<p>Determina la gravità dei messaggi di analisi. La gravità predefinita è trace_error.</p> <p>La gravità dei messaggi di analisi segue una gerarchia, con trace_debug al livello più alto e trace_none a quello più basso. Quando si imposta un livello di gravità dell'analisi, vengono visualizzati tutti i messaggi di tale livello e dei livelli inferiori. Se, ad esempio, si imposta la gravità dell'analisi su trace_path, i messaggi che includono trace_path, trace_information e trace_error vengono scritti nel file di registro.</p> <p><b>Nota:</b> trace_information può essere abbreviato in trace_info.</p>

#### 4. Salvare e chiudere il file BO\_trace.ini.

Il file BO\_trace.ini viene letto spesso. Le modifiche apportate al file BO\_trace.ini avranno effetto entro cinque minuti dal salvataggio. Se si riavvia il CMS, le modifiche al file BO\_trace.ini avranno effetto immediatamente.

#### Esempio:

BO\_trace.ini

```
sap_log_level=log_warning;
sap_trace_level=trace_path;
```

### 25.3.3.1 Per configurare l'analisi per un server specifico

Il file `BO_trace.ini` specifica i parametri di analisi per i server della piattaforma BI. Le impostazioni interessano tutti i server gestiti. Gli amministratori possono utilizzare il file `BO_trace.ini` per impostare determinati parametri di analisi per un server specifico.

#### Avvertenza:

Le nuove impostazioni del registro di analisi specificate nella CMC per un determinato server sovrascriveranno le impostazioni nel file `BO_trace.ini`.

#### 1. Aprire il file `BO_trace.ini`.

- In Windows il percorso predefinito è `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\conf\`
- In Unix il percorso predefinito è `DIRINSTALL/sap_bobj/enterprise_xi40/conf/`

#### 2. Utilizzare un'istruzione `if` per specificare le impostazioni di analisi di un determinato server. Ad esempio:

```
if (process == "aps_MySIA.ProcessingServer") {
 sap_log_level=log_warning;
 sap_trace_level=trace_path;
}
```

#### Suggerimento:

È necessario specificare il processo per consentire l'applicazione dell'impostazione di analisi a un determinato server.

#### 3. Salvare e chiudere il file `BO_trace.ini`.

Le impostazioni modificate verranno implementate entro cinque minuti.

## 25.4 Configurazione dell'analisi per le applicazioni Web

Le analisi per una distribuzione della piattaforma BI monitorata vengono scritte in un file di registro `.glf` specifico e archiviate in una directory sul computer che ospita la cartella delle applicazioni Web.

- In Windows il percorso predefinito è `C:\SBOPWebapp_APPLICAZIONE_INDIRIZZOIP_PORTA\`  
Ad esempio, `C:\SBOPWebapp_BIlaunchpad_192.0.2.0_8080\`
- In Unix il percorso predefinito è `$userHome/SBOPWebapp_APPLICAZIONE_INDIRIZZOIP_PORTA/`  
Ad esempio, `$userHome/SBOPWebapp_CMC_192.0.2.0_8080/`

Per impostazione predefinita, il livello del registro di analisi per le applicazioni Web nella CMC è impostato su **Non specificato**. Nella CMC le impostazioni del registro di analisi sono disponibili per le applicazioni seguenti:

- Central Management Console

- BI Launch Pad
- OpenDocument
- Servizio Web

**Nota:**

Per modificare i livelli dei registri di analisi per specifici server o per un gruppo di server, utilizzare il servizio registro di analisi nella CMC (Central Management Console). Per modificare altri parametri, cambiare manualmente il livello del registro di analisi e altre impostazioni nel file `BO_trace.ini`. Questo file viene distribuito insieme ai file `BOE.war` e `dswsbobje.war` nel server di applicazioni Web.

Prima di configurare il file `BO_trace.ini`, è necessario utilizzare lo strumento WDeploy per annullare la distribuzione delle applicazioni Web esistenti dal server di applicazioni Web. Dopo averlo configurato, è necessario ridistribuirlo insieme alle applicazioni Web sul server di applicazioni Web. Per ulteriori informazioni sull'utilizzo di Wdeploy per preparare, distribuire e annullare la distribuzione delle applicazioni Web, vedere il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

## 25.4.1 Impostazione del livello del registro di analisi delle applicazioni Web nella CMC

Per analizzare altre applicazioni Web, è necessario configurare manualmente il file `BO_trace.ini` corrispondente.

1. Nell'area "Applicazioni" della CMC, fare clic con il pulsante destro del mouse su un'applicazione e scegliere **Impostazioni registro di analisi**.

**Nota:**

Queste applicazioni includono impostazioni del registro di analisi: BI Launch Pad, CMC, Open Document, Promotion Management, Gestione delle versioni, Differenza visiva e Servizio Web.

Viene visualizzata la finestra di dialogo "Impostazioni registro di analisi".

2. Selezionare un'impostazione nell'elenco **Livello di registrazione**.
3. Fare clic su **Salva e chiudi**.

Il nuovo livello del registro di analisi sarà effettivo al successivo accesso all'applicazione Web.

**Argomenti correlati**

- [Livelli del registro di analisi](#)

## 25.4.2 Per configurare le impostazioni di analisi utilizzando il file `BO_trace.ini`

Il file `BO_trace.ini` viene distribuito con i file `BOE` e `dswsbobje.war` sul server di applicazioni Web. È possibile utilizzare il file `BO_trace.ini` per specificare i parametri di analisi per le applicazioni Web della piattaforma BI. Poiché questo file non è sempre accessibile, è necessario annullare la distribuzione dell'applicazione Web interessata dal server di applicazioni Web.

1. Utilizzare Wdeploy per annullare la distribuzione dell'applicazione Web dal server di applicazioni Web. Per ulteriori informazioni sull'utilizzo di Wdeploy per annullare la distribuzione delle applicazioni Web, vedere il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.
  - Se si utilizza il server di applicazioni Web Tomcat fornito con l'installazione della piattaforma BI, non è necessario annullare la distribuzione delle applicazioni Web. È possibile modificare i file direttamente.
    - Il file di configurazione dell'analisi per il file `BOE.war` è disponibile in `DIRINSTALL\Tomcat\webapps\BOE\WEB-INF\TraceLog`
    - Il file di configurazione dell'analisi per il file `dswsbobje.war` è disponibile in `DIRINSTALL\Tomcat\webapps\dswsbobje\WEB-INF\conf`

**Nota:**

Se si utilizza il server di applicazioni Web Tomcat in bundle, saltare il passaggio 2.

2. Accedere a una versione predistribuita del file `BO_trace.ini`:
  - Il percorso predefinito di una versione predistribuita del file di configurazione per il file `BOE.war` è `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
  - Il percorso predefinito di una versione predistribuita del file di configurazione per il file `dswsbobje.war` è `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`
3. Aprire il file `BO_trace.ini`.
  - In Windows il percorso predefinito è `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\conf\`
  - In Unix il percorso predefinito è `DIRINSTALL/sap_bobj/enterprise_xi40/conf/`
4. Modificare i parametri di analisi del server. Per la configurazione dell'analisi del server vengono utilizzati i parametri seguenti:

Parametro	Valori possibili	Descrizione
sap_log_level	log_information log_warning log_error log_fatal log_none	<p>Determina la gravità dei messaggi registro. La gravità predefinita è log_error.</p> <p>La gravità dei registri segue una gerarchia, con log_information al livello più alto e log_none a quello più basso. Quando si imposta un livello di gravità dei registri, vengono visualizzati tutti i messaggi di tale livello e dei livelli inferiori. Se, ad esempio, si imposta la gravità dei registri su log_warning, i messaggi che includono log_warning, log_error e log_fatal vengono scritti nel file di registro.</p> <p><b>Nota:</b> log_information e log_warning possono essere abbreviati in log_info e log_warn.</p>
sap_trace_level	trace_debug trace_path trace_information trace_error trace_none	<p>Determina la gravità dei messaggi di analisi. La gravità predefinita è trace_error.</p> <p>La gravità dei messaggi di analisi segue una gerarchia, con trace_debug al livello più alto e trace_none a quello più basso. Quando si imposta un livello di gravità dell'analisi, vengono visualizzati tutti i messaggi di tale livello e dei livelli inferiori. Se, ad esempio, si imposta la gravità dell'analisi su trace_path, i messaggi che includono trace_path, trace_info e trace_error vengono scritti nel file di registro.</p> <p><b>Nota:</b> trace_information può essere abbreviato in trace_info.</p>

5. Salvare e chiudere il file `BO_trace.ini`.

6. Utilizzare WDeploy per distribuire il file `.war` sul computer che ospita il server di applicazioni Web.

Le impostazioni di analisi modificate diventano effettive al successivo accesso all'applicazione Web.

### 25.4.2.1 Configurazione dell'analisi per un'applicazione Web specifica

Il file `BO_trace.ini` viene distribuito insieme ai file `BOE` e `dswsbobje.war` nel server di applicazioni Web. È possibile utilizzare il file `BO_trace.ini` per specificare i parametri di analisi per le applicazioni Web della piattaforma BI. Poiché questo file non è sempre accessibile, è necessario annullare la distribuzione dell'applicazione Web interessata dal server di applicazioni Web. Di seguito sono elencate le applicazioni Web e i file `.war` a esse associate:

Applicazione Web	File WAR	Posizione predefinita
Central Management Console	BOE.war	<code>DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog</code>
BI Launch Pad	BOE.war	<code>DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog</code>
OpenDocument	BOE.war	<code>DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog</code>
Servizio Web	dsws bobje.war	<code>DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf</code>

1. Utilizzare Wdeploy per annullare la distribuzione dell'applicazione Web dal server di applicazioni Web. Per ulteriori informazioni sull'utilizzo di Wdeploy per annullare la distribuzione delle applicazioni Web, vedere il *Manuale della distribuzione in rete di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence*.

- Se si utilizza il server di applicazioni Web Tomcat fornito con l'installazione della piattaforma BI, non è necessario annullare la distribuzione delle applicazioni Web. È possibile modificare direttamente il file.
  - Il file di configurazione dell'analisi per il file `BOE.war` è disponibile in `DIRINSTALL\Tomcat\webapps\BOE\WEB-INF\TraceLog`
  - Il file di configurazione dell'analisi per il file `dswsbobje.war` è disponibile in `DIRINSTALL\Tomcat\webapps\dswsbobje\WEB-INF\conf`

**Nota:**

Se si utilizza il server di applicazioni Web Tomcat in bundle, saltare il passaggio 2.

2. Accedere a una versione predefinita del file `BO_trace.ini`:

- Il percorso predefinito di una versione predefinita del file di configurazione per il file `BOE.war` è `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`
- Il percorso predefinito di una versione predefinita del file di configurazione per il file `dswsbobje.war` è `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`

3. Aprire il file `BO_trace.ini`.

- In Windows il percorso predefinito è `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\conf\`
- In Unix il percorso predefinito è `DIRINSTALL/sap_bobj/enterprise_xi40/conf/`

4. Utilizzare un'istruzione `if` per specificare le impostazioni di analisi di un'applicazione Web specifica. Ad esempio:

```
if (device_name == "Webapp_opendocument_trace") {
 sap_log_level=log_warning;
 sap_trace_level=trace_path;
}
```



È necessario specificare il processo per consentire l'applicazione dell'impostazione di analisi a un server di applicazioni Web specifico. Dopo l'installazione iniziale sono disponibili le applicazioni Web seguenti:

Applicazione Web	Nome dispositivo
BI Launch Pad	WebApp_BIlaunchpad
Central Management Server	WebApp_CMC
OpenDocument	WebApp_OpenDocument

Per configurare l'analisi del server di applicazioni Web vengono utilizzati i parametri seguenti:

Parametro	Valori possibili	Descrizione
sap_log_level	log_information log_warning log_error log_fatal log_none	<p>Determina la gravità dei messaggi registro. La gravità predefinita è log_error.</p> <p>La gravità dei messaggi registro segue una gerarchia, con log_information al livello più alto e log_none a quello più basso. Quando si imposta un livello di gravità dei registri, vengono visualizzati tutti i messaggi di tale livello e dei livelli inferiori. Se, ad esempio, si imposta la gravità dei registri su log_warning, i messaggi che includono log_warning, log_error e log_fatal vengono scritti nel file di registro.</p> <p><b>Nota:</b> log_information e log_warning possono essere abbreviati in log_info e log_warn.</p>
sap_trace_level	trace_debug trace_path trace_information trace_error trace_none	<p>Determina la gravità dei messaggi di analisi. La gravità predefinita è trace_error.</p> <p>La gravità dei messaggi di analisi segue una gerarchia, con trace_debug al livello più alto e trace_none a quello più basso. Quando si imposta un livello di gravità dell'analisi, vengono visualizzati tutti i messaggi di tale livello e dei livelli inferiori. Se, ad esempio, si imposta la gravità dell'analisi su trace_path, i messaggi che includono trace_path, trace_info e trace_error vengono scritti nel file di registro.</p> <p><b>Nota:</b> trace_information può essere abbreviato in trace_info.</p>

##### 5. Salvare e chiudere il file BO\_trace.ini.

6. Utilizzare WDeploy per distribuire il file `.war` sul computer che ospita il server di applicazioni Web.

## 25.5 Configurazione dell'analisi per Upgrade Management Tool

Non è possibile configurare l'analisi per lo strumento Upgrade Management Tool tramite la CMC. A questo scopo, è necessario utilizzare il file `BO_trace.ini`.

- In Windows il percorso predefinito è `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\conf\`
- In Unix il percorso predefinito è `DIRINSTALL/sap_bobj/enterprise_xi40/conf/`

### 25.5.1 Configurazione dell'analisi per Upgrade Management Tool

1. Aprire il file `BO_trace.ini`.
  - In Windows il percorso predefinito è `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\conf\`
  - In Unix il percorso predefinito è `DIRINSTALL/sap_bobj/enterprise_xi40/conf/`
2. Rimuovere il commento alle righe richieste nella sezione "Trace Syntax and Setting".
3. Per specificare le impostazioni di analisi, utilizzare un'istruzione `if`. Ad esempio:

```
if (process == "upgrademanagementtool") {
 sap_log_level=log_warning;
 sap_trace_level=trace_path;
}
```

#### **Suggerimento:**

Per applicare l'impostazione di analisi allo strumento Upgrade Management Tool, è necessario specificare il processo come `upgrademanagementtool`.

4. Salvare e chiudere il file `BO_trace.ini`.

Le impostazioni modificate verranno implementate entro cinque minuti.

## 25.6 Configurazione dell'analisi per le applicazioni client della piattaforma BI

È possibile attivare l'analisi nei seguenti client:

- Universe Design Tool
- Information Design Tool
- Web Intelligence Rich Client

Per configurare l'analisi per questi componenti, modificare i file .ini per ognuno dei tipi di client. Questi file .ini operano in modo identico al file BO\_trace.ini descritto in altre sezioni di questo capitolo. Per ulteriori informazioni sulla modifica del file .ini, consultare [Per configurare l'analisi del server tramite il file BO\\_trace.ini](#).

I file devono trovarsi nelle directory di lavoro configurate per le applicazioni (per impostazione predefinita, <DIRINSTALLAZ>\SAP BusinessObjects). Se non esistono già, potrebbe essere necessario crearle. Di seguito sono elencati i nomi dei file:

- Universe Design Tool: designer\_trace.ini.
- Information Design Tool: BO\_Trace.ini
- Web Intelligence Rich Client: WebIRichClient\_trace.ini

Per ulteriori informazioni, consultare la documentazione relativa a questi prodotti.



# Integrazione con SAP Solution Manager

## 26.1 Panoramica sull'integrazione

Alla piattaforma BI sono state aggiunte funzionalità di supportabilità che consentono l'integrazione in SAP Solution Manager. È possibile utilizzare i componenti SAP Solution Manager seguenti per fornire supporto per la distribuzione della piattaforma BI:

- Solution Landscape Directory
- Solution Manager Diagnostics
- CA Wily Introscope
- SAP Passport

**Nota:**

è possibile accedere a SAP Support Portal per SAP BusinessObjects all'indirizzo: <https://websmp205.sap-ag.de/bosap-support>

## 26.2 Elenco di controllo dell'integrazione di SAP Solution Manager

Nella tabella seguente sono riepilogati i componenti richiesti per abilitare SAP Solution Manager a fornire supporto per la piattaforma BI.

Supporto SAP Solution Manager	Richiesto per la piattaforma BI
Registrazione SLD	<ul style="list-style-type: none"> <li>• È necessario installare SAPHOSTAGENT per abilitare la registrazione dei server della piattaforma BI.</li> </ul> <p><b>Nota:</b> Il programma di installazione della piattaforma BI registrerà automaticamente i server se SAPHOSTAGENT è già installato.</p> <ul style="list-style-type: none"> <li>• È necessario creare un file connect.key per il fornitore di dati che crea report sui server di back-end.</li> <li>• (Facoltativo) Per la registrazione SLD con WebSphere 6.1 o 7, è necessario installare lo strumento di registrazione SLDREG in tutti i server di applicazioni Web WebSphere. Per ulteriori informazioni, fare riferimento alla nota SAP 1482727.</li> <li>• (Facoltativo) Per la registrazione SLD con SAP NetWeaver 7.2, installare SLDREG in tutti gli host NetWeaver. Per ulteriori informazioni, fare riferimento alla nota SAP 1018839.</li> <li>• (Facoltativo) Per la registrazione SLD con Apache Tomcat, è necessario che SLDREG sia installato in ogni server Tomcat. Per ulteriori informazioni, consultare la nota SAP 1508421.</li> </ul>
Integrazione SMD	<ul style="list-style-type: none"> <li>• È necessario scaricare e installare l'agente SMD (DIAGNOSTICS.AGENT) su tutti gli host dei server della piattaforma BI.</li> <li>• È necessario abilitare l'account utente SMAAdmin nella piattaforma BI.</li> </ul>
Strumentazione delle prestazioni	<ul style="list-style-type: none"> <li>• È necessario configurare Introscope Agent per la connessione a Enterprise Manager. Utilizzare il programma di installazione della piattaforma BI o i segnaposto del nodo CMC per configurare le connessioni.</li> <li>• È necessario installare l'agente SMD.</li> <li>• È necessario configurare la piattaforma BI per la connessione all'agente SMD. Utilizzare il programma di installazione della piattaforma BI o i segnaposto del nodo CMC per configurare le connessioni.</li> </ul>
SAP Passport	<ul style="list-style-type: none"> <li>• È necessario scaricare e installare lo strumento client SAP Passport.</li> </ul>

## 26.3 Gestione della registrazione di System Landscape Directory

## 26.3.1 Registrazione della piattaforma BI in System Landscape

System Landscape Directory (SLD) è un repository centrale delle informazioni di System Landscape rilevanti per la gestione del ciclo di vita del software. SLD include una descrizione di System Landscape, ovvero dei sistemi e dei componenti software correntemente installati. I fornitori di dati SLD registrano i sistemi nel server SLD e mantengono aggiornate le informazioni. Le applicazioni business e di gestione accedono alle informazioni archiviate in SLD per eseguire attività in un ambiente di elaborazione collaborativo.

Il fornitore di dati System Landscape Directory (SLD-DS) è l'applicazione responsabile della registrazione dei server della piattaforma BI nel server SLD. Per ciascuna installazione della piattaforma viene specificato un fornitore di dati specifico per la creazione di report sui componenti seguenti:

- Server della piattaforma BI
- Applicazioni Web e servizi ospitati nel server di applicazioni Web WebSphere.

### **Nota:**

SAP NetWeaver include un fornitore SLD-DS incorporato che registra il server di applicazioni NetWeaver, nonché servizi e applicazioni Web ospitati. Questo SLD-DS è rilevante per le distribuzioni della piattaforma BI integrate in un ambiente SAP NetWeaver.

Il fornitore SLD-DS che crea report sui server della piattaforma BI richiede l'installazione e la configurazione del programma SLDREG. Il programma SLDREG viene installato durante l'installazione dello strumento SAPHOSTAGENT. Per ulteriori informazioni su come accedere a SAPHOSTAGENT e installarlo, consultare la sezione relativa alla preparazione nel *Manuale di installazione della piattaforma SAP BusinessObjects Business Intelligence*. Una volta installato SLDREG, è necessario creare un file `connect.key` per abilitarlo a connettersi al server SLD.

Per informazioni su come configurare il fornitore di dati specifico per WebSphere, consultare il *Manuale della distribuzione in rete di applicazioni Web*.

Durante l'installazione della piattaforma BI, le informazioni necessarie per la registrazione della piattaforma vengono memorizzate in un file di configurazione. Questo file include informazioni utilizzate dal fornitore di dati SLD DS per connettersi al database della piattaforma BI.

### 26.3.1.1 Creazione di un file `connect.key` per il fornitore di dati SLD

Prima di creare un file `connect.key` per il fornitore di dati SLD, è necessario scaricare e installare SAPHOSTAGENT. Per informazioni dettagliate, fare riferimento al *Manuale di installazione della piattaforma SAP BusinessObjects Business Intelligence*.

**Nota:**

Il file `connect.key` è necessario per la registrazione SLD con il fornitore di dati che crea report sui server della piattaforma BI.

1. Aprire una console della riga di comando.
2. Passare al percorso di installazione predefinito di SAPHOSTAGENT.
  - In Windows: `Programmi\SAP\hostctrl\exe`
  - In Unix: `/usr/sap/hostctrl/exe`

3. Eseguire il seguente comando:

```
sldreg -configure connect.key
```

4. Immettere i dettagli di configurazione seguenti

- Nome utente
- Password
- Host
- Numero di porta
- Specificare l'utilizzo di HTTP

Lo strumento `sldreg` crea un file `connect.key` che verrà utilizzato automaticamente dal fornitore di dati per il push delle informazioni al server SLD.

### 26.3.2 Quando viene attivata la registrazione SLD?

Il processo di registrazione SLD viene richiamato dal fornitore di dati che crea report sui server di back-end della piattaforma BI negli scenari seguenti:

- Viene riavviato un nodo server della distribuzione della piattaforma BI.
- Alla distribuzione viene aggiunto un nuovo server o un nodo.
- Viene eliminato un server o un nodo

**Nota:**

se viene eliminato un server o un nodo, il processo di registrazione SLD non modifica il contenuto del server SLD. Per aggiornare il server SLD quando viene rimosso un server o un nodo, eliminare il sistema dal server SLD e inviarlo di nuovo riavviando la piattaforma BI.

Il fornitore di dati per la registrazione di WebSphere SLD può essere richiamato manualmente o impostato per l'esecuzione in un intervallo specificato, ad esempio ogni 24 ore. Per ulteriori informazioni sulla configurazione di questo fornitore di dati, fare riferimento alla nota SAP 482727.

### 26.3.3 Registrazione della connettività SLD



### File di configurazione del fornitore di dati

Per le distribuzioni della piattaforma BI viene creato un file di configurazione utilizzato per la registrazione SLD. Il file, `sldparserconfig.properties`, si trova nella directory seguente: `<DIRINSTALL>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/`.

### Registrazione della connettività SLD

La connettività tra il server SLD e il fornitore di dati nella distribuzione della piattaforma BI viene controllata mediante lo strumento `sldreg` e il file `connect.key`.

#### Nota:

il nome del file di registro viene specificato come proprietà nel file `sldparserconfig.properties`.

Il file di registro per il fornitore di dati SLD che crea report sui server di back-end della piattaforma BI si trova per impostazione predefinita nel percorso seguente: `<DIRINSTALL>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/bobjsldds.log`. Il file viene sovrascritto ogni volta che viene eseguito il fornitore di dati.

I file di registro per `sldreg` si trovano per impostazione predefinita nel percorso seguente: `<DIRINSTALL>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/log`. I nomi dei file di registro `sldreg` non possono essere modificati e utilizzano il formato seguente: `sldreg_Indicazione data e ora.log`.

Viene creato un nuovo file di registro ogni volta che il fornitore di dati chiama `sldreg`.

## 26.4 Gestione degli agenti di Solution Manager Diagnostics

### 26.4.1 Panoramica di Solution Manager Diagnostics (SMD)

Il componente SMD (Solution Manager Diagnostics) di SAP Solution Manager offre tutte le funzionalità per l'analisi e il monitoraggio centralizzati di un sistema completo. La piattaforma BI può essere monitorata dal server SMD, se è installato un agente SMD. L'agente SMD (`DIAGNOSTICS.AGENT`) raccoglie informazioni per il componente SMD che può essere quindi utilizzato a scopo di analisi della causa principale. Le informazioni raccolte e inviate al server SMD includono le configurazioni dei server di back-end e il percorso dei file di registro del server.

### 26.4.2 Utilizzo degli agenti SMD

La piattaforma BI non installa l'agente SMD. È possibile scaricare l'agente, `DIAGNOSTICS.AGENT`, al seguente indirizzo: <http://service.sap.com/swdc>.

Informazioni sull'installazione e la configurazione dell'agente sono disponibili all'indirizzo: <http://service.sap.com/diagnostics>

### Linee guida per l'utilizzo dell'agente SMD

Di seguito vengono fornite linee guida per l'utilizzo degli agenti SMD per monitorare la piattaforma BI:

- L'ordine di installazione dell'agente e del sistema monitorato non è importante. È possibile decidere di installare l'agente SMD prima o dopo l'installazione e la distribuzione della piattaforma BI.
- Durante l'installazione di un agente SMD, prendere nota del nome host e della porta di attesa. Si tratta infatti di informazioni critiche per la configurazione della piattaforma BI come sistema monitorato. Se l'agente è stato installato prima del sistema monitorato, è possibile fornire le informazioni di configurazione durante la procedura di installazione della piattaforma BI. Tali informazioni possono essere fornite anche in una fase successiva mediante segnaposto per i nodi della Central Management Console all'interno della distribuzione.
- Se i server di back-end vengono distribuiti in un sistema distribuito, è consigliabile installare un agente SMD in ciascun computer che ospita un server di back-end.
- L'agente SMD è richiesto per la strumentazione delle prestazioni dei server non java.
- È necessario attivare l'account utente SMAAdmin per abilitare l'accesso del server SMD al server CMS.

## 26.4.3 Account utente SMAAdmin

Per ogni distribuzione della piattaforma BI viene creato un account utente per semplificare l'integrazione SMD. Questo account in sola lettura viene utilizzato dal server SMD per accedere al CMS e raccogliere informazioni sulla configurazione server e altre informazioni sulla distribuzione.

L'account SMAAdmin è disattivato per impostazione predefinita.

### 26.4.3.1 Attivazione dell'account SMAAdmin

1. Nell'area di gestione "Utenti e gruppi" della console CMC selezionare **Elenco utenti**.  
Viene visualizzato l'elenco degli utenti.
2. Individuare l'account utente "SMAAdmin".
3. Fare clic su **Gestisci > Proprietà**.  
Viene visualizzata la finestra di dialogo "Proprietà".
4. Deselezionare la casella **Account disattivato**.
5. Fare clic su **Salva e chiudi**.

## 26.5 Gestione della strumentazione delle prestazioni

### 26.5.1 Strumentazione delle prestazioni per la piattaforma BI

È possibile utilizzare CA Wily Introscope come parte di SAP Solution Manager per la misurazione della strumentazione delle prestazioni della piattaforma BI. Quando si installa la piattaforma, per la distribuzione vengono fornite le risorse seguenti

- **Agente Introscope:** l'agente Introscope raccoglie metriche di prestazioni dai server di back-end Java della piattaforma BI. Gli agenti raccolgono inoltre informazioni dall'ambiente di elaborazione circostante, quindi comunicano tali metriche a Enterprise Manager.
- **File forniti per semplificare il processo di strumentazione.** Vengono forniti due insiemi di file, uno per la strumentazione dei server non Java e uno per la strumentazione dei server Java. Per SAP Solution Manager è richiesto il componente EM (Enterprise Manager). EM funge da repository centrale per tutti i dati e le metriche delle prestazioni di Introscope raccolti in un ambiente di applicazione. EM elabora i dati relativi alle prestazioni e li rende disponibili agli utenti per il monitoraggio e la diagnosi della produzione.

### 26.5.2 Impostazione della strumentazione delle prestazioni per la piattaforma BI

È possibile configurare in due modi la strumentazione delle prestazioni per i workflow in esecuzione sui server di back-end della piattaforma BI.

1. Durante l'installazione della piattaforma BI. In questo caso è necessario conoscere il nome host e la porta di attesa dell'agente SMD. Per ulteriori informazioni, consultare il *Manuale di installazione della piattaforma SAP BusinessObjects Business Intelligence*. Se si sceglie questa opzione, la strumentazione verrà eseguita per impostazione predefinita al termine della distribuzione del sistema monitorato.
2. Dopo l'installazione della piattaforma BI è possibile fornire le informazioni di configurazione per l'agente SMD mediante i segnaposto nelle proprietà dei nodi nella CMC (Central Management Console).

**Nota:**

per la strumentazione dei workflow nei server non Java, è necessario che sia installato l'agente SMD (DIAGNOSTICS.AGENT).

**Argomenti correlati**

- [Utilizzo degli agenti SMD](#)

### 26.5.2.1 Configurazione dei nodi per la strumentazione

Di seguito sono riportate istruzioni utili per gli utenti che non hanno specificato informazioni di configurazione per l'agente SMD ed Enterprise Manager durante la procedura di installazione della piattaforma BI.

1. Accedere all'area "Server" della console CMC.
2. Nel riquadro di spostamento fare clic su **Nodi**.  
Vengono visualizzati tutti i nodi disponibili.
3. Fare clic con il pulsante destro del mouse sul nodo in cui si desidera eseguire la strumentazione e scegliere **Segnaposto**.  
Verrà visualizzata la finestra di dialogo Segnaposto.
4. Modificare i valori dei segnaposto seguenti.

Segnaposto	Descrizione
%IntroscopeAgentEnableInstrumentation%	Abilita o disabilita la strumentazione nei server Java. Sarà impostato su abilitato se sono stati forniti dettagli di configurazione per Enterprise Manager durante la procedura di installazione. Impostare questo valore su <code>true</code> per abilitare la strumentazione.
%IntroscopeAgentEnterpriseManagerHost%	Nome host della macchina in cui è installato Enterprise Manager.
%IntroscopeAgentEnterpriseManagerPort%	La porta di attesa utilizzata da Enterprise Manager.
%IntroscopeAgentEnterpriseManagerTransport%	Il protocollo di autenticazione utilizzato da Enterprise Manager. Tra i protocolli supportati sono inclusi TCP, SSL, HTTP Tunnel e HTTPS.
%NCSInstrumentLevelThreshold%	Consente di impostare il livello di strumentazione per i server non Java. Impostare questo valore su "0" se si desidera disattivare la strumentazione. Se invece si desidera attivarla, impostarlo su qualsiasi valore superiore a "0."
%SMDAgentHost%	Nome host della macchina in cui è installato l'agente SMD ( <code>DIAGNOSTICS.AGENT</code> ).
%SMDAgentPort%	La porta di attesa utilizzata dall'agente SMD.

5. Fare clic su **Salva e chiudi**.
6. Riavviare il nodo.

Una volta riavviato il nodo, i nuovi valori specificati verranno propagati in tutti i server gestiti.

### 26.5.3 Strumentazione delle prestazioni per il livello Web

I dati di strumentazione per i componenti del livello Web non sono inclusi nella piattaforma BI.

### 26.5.4 File di registro di strumentazione

Una volta configurata la distribuzione della piattaforma BI per l'esecuzione della strumentazione, i messaggi vengono registrati in posizioni specifiche. È possibile verificare lo stato della strumentazione analizzando i file di registro.

Per la strumentazione nei server di back-end Java, il file di registro si trova nella directory seguente: `DIRINSTALL/SAP BusinessObjects Enterprise XI 4.0/java/wily/logs`. Per ciascun processo java viene creato un file `.log` separato. Nella cartella saranno inoltre inclusi file `Auto Probe.log` che specificano i metodi caricati per la strumentazione.

Per la strumentazione nei server di back-end non Java i file di registro si trovano nella directory seguente: `<DIRINSTALL>/SAP BusinessObjects Enterprise XI 4.0/logging/`. In Unix i file si trovano nella directory `<sap_bobj>\logging\`. I file di registro correlati alla strumentazione per i server non Java vengono salvati come file `.trc`.

Per la strumentazione nei server di applicazioni Web il file di registro si trova nella directory seguente: `<DIRINSTALL>/SAP BusinessObjects Enterprise XI 4.0/java/wily/webapp/logs`. In questa cartella sono presenti due tipi di file di registro: `Introscope.log` e `Autoprobe.log`.

## 26.6 Analisi con SAP Passport

Oltre all'analisi di componenti della piattaforma BI, quali server e applicazioni Web, il meccanismo di analisi è in grado di supportare l'analisi di un'azione specifica. In un'analisi end-to-end vengono analizzate le prestazioni di una singola transazione. Il consolidamento di tutte le informazioni di analisi per un'azione specifica consente al personale di supporto SAP di esaminare tutti i dati di analisi senza essere distratto dalle informazioni relative ad altre azioni.

### SAP Passport

Il meccanismo che supporta l'analisi end-to-end per la piattaforma BI è uno strumento denominato SAP Passport. Lo strumento client SAP Passport inserisce un identificatore univoco in tutte le richieste HTTP per un determinato workflow e tale identificatore viene inoltrato a tutti i server utilizzati nel workflow. Il personale di supporto SAP può raccogliere le informazioni di un'analisi end-to-end per il workflow utilizzando l'identificatore univoco.

**Nota:**

Vengono utilizzati i livelli del registro di analisi specificati nella console CMC e nel file di configurazione `BO_trace.ini`, se superiori a quelli specificati nello strumento client SAP Passport, `SAPClientPlugin.exe`.

Passport si trova nei registri dei server di back-end, nelle applicazioni Web e nei registri dei servizi Web.

Lo strumento client SAP Passport non viene installato come parte della piattaforma BI. È possibile accedere allo strumento e scaricarlo all'indirizzo <http://service.sap.com/swdc>.

# Amministrazione della riga di comando

## 27.1 Script UNIX

In questa sezione sono descritti in dettaglio tutti gli strumenti e gli script amministrativi inclusi nella distribuzione UNIX della piattaforma SAP BusinessObjects Business Intelligence. Questa sezione viene fornita principalmente a scopo di riferimento. I concetti e le procedure di configurazione sono illustrati in maggiore dettaglio in questa Guida.

La distribuzione UNIX della piattaforma BI include una serie di script che, insieme, forniscono tutte le opzioni di configurazione disponibili nella versione Windows del Central Configuration Manager (CCM). Esistono diversi altri script che forniscono opzioni specifiche di UNIX o fungono da modelli per gli script dell'utente. Esistono inoltre alcuni script secondari che vengono utilizzati dalla piattaforma BI. Ogni script viene descritto di seguito e vengono fornite, laddove possibile, le opzioni della riga di comando.

### 27.1.1 Utilità per gli script

In questa sezione vengono descritti gli script amministrativi che assistono l'utente nell'utilizzo della piattaforma BI in UNIX. Nella parte restante di questa guida vengono illustrati i concetti sottostanti a ciascuna attività che è possibile eseguire con tali script. In questa sezione di riferimento vengono forniti le principali opzioni della riga di comando e i relativi argomenti.

#### 27.1.1.1 `ccm.sh`

Lo script `ccm.sh` viene installato nella directory `DIRINSTALL/sap_bobj` dell'installazione. Questo script fornisce una versione da riga di comando del Central Configuration Manager. Questa sezione elenca le opzioni della riga di comando e fornisce alcuni esempi.

**Nota:**

- Gli argomenti in parentesi quadre [ ] sono opzionali.
- Se non si conosce con sicurezza il nome di un agente SIA, osservare le proprietà Command nel file `ccm.config` e utilizzare il valore che viene visualizzato dopo l'opzione `-name`.

- Lo script `ccm.sh` può essere avviato solo dall'utente che ha eseguito l'installazione della piattaforma BI.
- Gli argomenti identificati da *altre informazioni di autenticazione* vengono forniti nella seconda tabella.

Opzione CCM	Argomenti validi	Descrizione
<code>-help</code>	N/D	Consente di visualizzare la guida della riga di comando.
<code>-start</code>	<code>all</code> o <i>sianame</i>	Avviare ogni Server Intelligence Agent come processo. L'opzione <code>all</code> avvia tutti i nodi presenti nel computer, inclusi quelli appartenenti a cluster diversi.
<code>-stop</code>	<code>all</code> o <i>sianame</i>	Arrestare ogni Server Intelligence Agent terminando il relativo ID di processo. L'opzione <code>all</code> avvia tutti i nodi presenti nel computer, inclusi quelli appartenenti a cluster diversi.
<code>-restart</code>	<code>all</code> o <i>sianame</i>	Arrestare ogni Server Intelligence Agent terminando il relativo ID processo, dopodiché viene avviato ogni SIA. L'opzione <code>all</code> avvia tutti i nodi presenti nel computer, inclusi quelli appartenenti a cluster diversi.
<code>-managedstart</code>	<i>nome server completo[altre informazioni di autenticazione]</i>	Avvia un server.
<code>-managedstop</code>	<i>nome server completo[altre informazioni di autenticazione]</i>	Arresta un server.



Opzione CCM	Argomenti validi	Descrizione
-managedrestart	<i>nome server completo[altre informazioni di autenticazione]</i>	Arresta un server, quindi avvia il server.
-managedforceterminate	<i>nome server completo[altre informazioni di autenticazione]</i>	Arresta il server immediatamente senza completare le richieste di elaborazione correnti.
-enable	<i>nome server completo[altre informazioni di autenticazione]</i>	Consente di abilitare un server avviato in modo che si registri con il sistema e inizi ad attendere in corrispondenza della porta appropriata. Utilizzare la forma completa del nome server.
-disable	<i>nome server completo[altre informazioni di autenticazione]</i>	Disabilitare un server in modo che non risponda più alle richieste della piattaforma BI ma rimanga avviato come processo. Utilizzare la forma completa del nome server.
-display	<i>[altre informazioni di autenticazione]</i>	Indica lo stato corrente di tutti i server del cluster, inclusi i nomi dei server, i nomi host, gli ID processo, le descrizioni, se i server sono in esecuzione e se sono abilitati o disabilitati.

Nella tabella riportata di seguito vengono descritte le opzioni che compongono l'argomento indicato da *[altre informazioni di autenticazione]*.

**Nota:**

per garantire una maggiore sicurezza, è necessario fornire sempre le credenziali di un account con autenticazione Enterprise. Non sono supportati altri tipi di autenticazione.

Opzione di autenticazione	Argomenti validi	Descrizione
-cms	<i>cmsname:port#</i>	Consente di specificare il CMS a cui si desidera accedere. Se non specificato, l'impostazione predefinita del CCM corrisponde al computer locale e alla porta predefinita (6400).
-username	<i>username</i>	Specificare un account che fornisca diritti amministrativi per la piattaforma BusinessObjects Business Intelligence. Se non specificato, si tenta con l'account Administrator predefinito.
-password	<i>password</i>	Consente di specificare la password corrispondente. Se non specificata, si tenta con una password vuota.  <b>Nota:</b> Per specificare l'argomento -password, è necessario specificare anche l'argomento -username.

CCM legge le stringhe di avvio e altri valori di configurazione dal file `ccm.config`.

### Argomenti correlati

- [ccm.config](#)

#### 27.1.1.1.1 Esempi

Questi due comandi consentono di avviare e abilitare tutti i server della piattaforma BI. Il Central Management Server(CMS) viene avviato sul computer locale e sulla porta predefinita (6400):

```
ccm.sh -start all
ccm.sh -enable all
```

Questi due comandi consentono di avviare e abilitare tutti i server della piattaforma BI. CCM abiliterà tutti i server inclusi nel cluster, dove CMS viene eseguito sul computer MACHINE01, porta 6701:

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701
```

Questi due comandi consentono di avviare e abilitare tutti i server della piattaforma BI per i quali è stato specificato l'account amministrativo `SysAdmin` ed è stata fornita la password:

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

Questo singolo comando accede con un account amministrativo specificato per disabilitare un Job Server adattivo in esecuzione in un secondo computer:

```
ccm.sh -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

#### 27.1.1.1.2 ccm.config

Questo file di configurazione definisce le stringhe di avvio e altri valori che vengono utilizzati da CCM quando vengono eseguiti i relativi comandi. Questo file è gestito da CCM e dalle altre utilità di script della piattaforma BI. Questo file viene in genere modificato solo quando è necessario modificare la riga di comando di Server Intelligence Agent. È fortemente consigliato eseguire il backup di questo file prima di modificarlo manualmente.

##### Argomenti correlati

- [Panoramica sulle righe di comando](#)

### 27.1.1.2 cmsdbsetup.sh

Lo script `cmsdbsetup.sh` viene installato nella directory `sap_bobj` dell'installazione. Lo script fornisce un programma basato su testo che consente di effettuare le operazioni seguenti.

- Configurare un database di sistema CMS
- Inizializzare nuovamente un database di sistema CMS
- Copiare i dati da un'altra origine dati
- Modificare la chiave cluster
- Modificare il nome del cluster

##### Nota:

prima di eseguire lo script, creare una copia di backup del database di sistema CMS corrente e dei contenuti di Input e Output File Repository. Per ulteriori informazioni, vedere "Backup e ripristino del sistema". Consultare inoltre la sezione relativa ai cluster di server CMS nel capitolo "Manutenzione del server" del *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence* per maggiori dettagli sui cluster CMS e sulla configurazione del database CMS.

Lo script chiederà il nome di Server Intelligence Agent (SIA). Per verificare il nome del SIA, visualizzare le proprietà dei comandi del SIA nel file `ccm.config`. Il nome corrente del SIA viene visualizzato dopo l'opzione `-name`. In alternativa, è possibile utilizzare l'opzione 8 con il file `serverconfig.sh`.

##### Argomenti correlati

- [Cluster di Central Management Server](#)

- [Panoramica di backup e ripristino](#)

### 27.1.1.3 serverconfig.sh

Lo script `serverconfig.sh` viene installato nella directory `sap_bobj` dell'installazione. Lo script fornisce un programma basato su testo che consente di effettuare le operazioni seguenti.

- Aggiungere un nodo
- Eliminare un nodo
- Modificare un nodo
- Spostare un nodo
- Eseguire un backup della configurazione del server
- Ripristinare la configurazione del server
- Modificare la configurazione a livello Web
- Elencare tutti i nodi

#### 27.1.1.3.1 Aggiunta/eliminazione/modifica/elenco di nodi in UNIX

1. Andare alla directory `DIRINSTALL/sap_bobj` dell'installazione.
2. Eseguire il seguente comando:

```
./serverconfig.sh
```

Lo script richiede all'utente un elenco di opzioni:

- a. Aggiungere un nodo
  - b. Eliminare un nodo
  - c. Modificare un nodo
  - d. Spostare un nodo
  - e. Eseguire un backup della configurazione del server
  - f. Ripristinare la configurazione del server
  - g. Modificare la configurazione a livello Web
  - h. Elencare tutti i nodi
3. Digitare il numero che corrisponde all'azione che si desidera eseguire.
  4. Se si aggiunge, elimina o modifica un server, fornire allo script tutte le informazioni aggiuntive che richiede.

### 27.1.2 Modelli di script

### 27.1.2.1 startservers

Lo script `startservers` viene installato nella directory `DIRINSTALL/sap_bobj` dell'installazione. Questo script può essere utilizzato come modello per i propri script: viene fornito come esempio per mostrare come impostare uno script per l'avvio dei server della piattaforma BI eseguendo una serie di comandi CCM. Per informazioni dettagliate sulla scrittura di comandi CCM per i server, consultare [ccm.sh](#).

### 27.1.2.2 stopservers

Lo script `stopservers` viene installato nella directory `DIRINSTALL/sap_bobj` dell'installazione. Questo script può essere utilizzato come modello per i propri script: viene fornito come esempio per mostrare come impostare uno script per l'arresto dei server della piattaforma BI eseguendo una serie di comandi CCM. Per informazioni dettagliate sulla scrittura di comandi CCM per i server, consultare [ccm.sh](#).

## 27.1.3 Script utilizzati nella piattaforma BI

Questi script secondari vengono spesso eseguiti in background durante l'esecuzione delle principali utilità per gli script della piattaforma BI, pertanto non è necessario eseguirli manualmente.

### **bobjrestart.sh**

Questo script viene eseguito internamente da CCM per gestire i nodi di Server Intelligence Agent. Non eseguire questo script manualmente.

### **env.sh**

Lo script `env.sh` viene installato nella directory `sap_bobj/setup` dell'installazione. Questo script imposta le variabili di ambiente della piattaforma BI richieste da alcuni degli altri script. Gli script della piattaforma BI eseguono `env.sh` in base alle esigenze. Per ulteriori dettagli, consultare il *Manuale di installazione della piattaforma SAP BusinessObjects Business Intelligence*.

### **env-locale.sh**

Lo script `env-locale.sh` viene utilizzato per convertire le stringhe di linguaggio degli script tra differenti tipi di codifica (ad esempio, UTF8, EUC o Shift-JIS). Questo script viene eseguito da `env.sh` se necessario.

**initlaunch.sh**

Lo script `initlaunch.sh` esegue `env.sh` per impostare le variabili di ambiente della piattaforma BI, quindi esegue tutti i comandi che sono stati aggiunti come argomento della riga di comando per lo script. Questo script è destinato principalmente all'utilizzo come strumento di debug da parte di SAP BusinessObjects.

**postinstall.sh**

Lo script `postinstall.sh` è installato nella directory `SCRIPTDIR` dell'installazione, e non deve essere eseguito manualmente.

**setup.sh**

Lo script `setup.sh` è installato nella directory principale dell'installazione. Fornisce un programma basato su testo che consente di impostare l'installazione della piattaforma BI. Lo script viene eseguito automaticamente quando si installa la piattaforma BI e richiede all'utente le informazioni necessarie per impostare la piattaforma BI per la prima volta.

Per informazioni complete su come rispondere allo script di impostazione quando si installa la piattaforma BI, consultare il *Manuale di installazione della piattaforma SAP BusinessObjects Business Intelligence*.

**setupinit.sh**

Lo script `setupinit.sh` viene installato nella directory `/sap_bobj/init` dell'installazione. Questo script copia gli script di controllo dell'esecuzione nelle directory `rc#` per un avvio automatico. Se si desidera che i server della piattaforma BI vengano avviati e arrestati con il computer in cui sono installati, eseguire questo script dopo aver completato lo script `setup.sh`.

**Nota:**

per eseguire questo script, è necessario disporre di privilegi principali.

## 27.2 Script Windows

In questa sezione sono descritti in dettaglio tutti gli strumenti e gli script amministrativi inclusi nella distribuzione Windows della piattaforma BI. Questa sezione viene fornita principalmente a scopo di riferimento. I concetti e le procedure di configurazione sono illustrati in maggiore dettaglio in questa Guida.

La distribuzione Windows della piattaforma BI include la versione Windows di Central Configuration Manager (CCM). Oltre a interagire con la GUI, è possibile decidere di eseguire il file eseguibile di CCM dalla riga di comando con le opzioni che consentono di gestire i server.

### 27.2.1 ccm.exe

Il file eseguibile `ccm.exe` è installato nella directory `DIRINSTALL\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64` dell'installazione. È possibile eseguire tale file dalla riga di comando per eseguire determinate operazioni. Questa sezione elenca le opzioni della riga di comando e fornisce alcuni esempi.

**Nota:**

- per poter utilizzare le opzioni da riga di comando di `ccm.exe` per interagire con un server singolo, è necessario che siano in esecuzione un agente SIA (Server Intelligence Agent) e un server CMS (Central Management Server).
- Gli argomenti in parentesi quadre [ ] sono opzionali.
- Gli argomenti identificati da *altre informazioni di autenticazione* vengono forniti nella seconda tabella.

Opzione CCM	Argomenti validi	Descrizione
-help	N/D	Consente di visualizzare la guida della riga di comando.
-managedstart	<code>all oppure nome server completo[altre informazioni di autenticazione]</code>	Avvia un server.
-managedstop	<code>all oppure nome server completo[altre informazioni di autenticazione]</code>	Arresta un server.
-managedrestart	<code>all oppure nome server completo[altre informazioni di autenticazione]</code>	Arresta un server, quindi avvia il server.
-managedforceterminate	<code>all oppure nome server completo[altre informazioni di autenticazione]</code>	Arresta il server immediatamente senza completare le richieste di elaborazione correnti.

Opzione CCM	Argomenti validi	Descrizione
-enable	<i>all oppure nome server completo [altre informazioni di autenticazione]</i>	Consente di abilitare un server avviato in modo che si registri con il sistema e inizi ad attendere in corrispondenza della porta appropriata.
-disable	<i>all oppure nome server completo [altre informazioni di autenticazione]</i>	Disabilitare un server in modo che non risponda più alle richieste della piattaforma BI ma rimanga avviato come processo.
-display	<i>[altre informazioni di autenticazione]</i>	Indica lo stato corrente di tutti i server del cluster, inclusi i nomi dei server, i nomi host, gli ID processo, le descrizioni, se i server sono in esecuzione e se sono abilitati o disabilitati.

Nella tabella riportata di seguito vengono descritte le opzioni che compongono l'argomento indicato da *[altre informazioni di autenticazione]*.

**Nota:**

È necessario fornire sempre le credenziali di un account con autenticazione Enterprise.

Opzione di autenticazione	Argomenti validi	Descrizione
-cms	<i>cmsname:port#</i>	Consente di specificare il CMS a cui si desidera accedere. Se non specificato, l'impostazione predefinita del CCM corrisponde al computer locale e alla porta predefinita (6400).
-username	<i>username</i>	Specificare un account che fornisce diritti amministrativi per la piattaforma BI. Se non specificato, si tenta con l'account Administrator predefinito.



Opzione di autenticazione	Argomenti validi	Descrizione
<code>-password</code>	<code>password</code>	Specificare la password corrispondente. Se non specificata, si tenta con una password vuota.  <b>Nota:</b> Per specificare l'argomento <code>-password</code> , è necessario specificare anche l'argomento <code>-username</code> .
<code>-authentication</code>	<code>tipo autenticazione</code>	Specificare il tipo di autenticazione. È supportato solamente <code>secEnterprise</code> .

CCM legge le stringhe di avvio e altri valori di configurazione dal file `ccm.config`.

### 27.2.1.1 Esempi

Nell'esempio seguente si presuppone che siano stati avviati e che siano in esecuzione un Server Intelligence Agent (SIA) e Central Management Server (CMS). Prima di utilizzare le opzioni da riga di comando di `ccm.exe` per interagire con un server singolo, è possibile utilizzare il comando Windows seguente per avviare il servizio SIA:

```
net start "Server Intelligence Agent (NODENAME)"
```

È anche possibile arrestare il SIA specificando `net stop "Server Intelligence Agent (NODENOME)"`.

Questo comando avvia tutti i server della piattaforma BI:

```
ccm.exe -managedstart all
```

Questo comando avvia un Adaptive Job Server. Il CMS è stato avviato sulla porta 6701 anziché sulla porta predefinita:

```
ccm.exe -managedstart MACHINE01.AdaptiveJobServer -cms MACHINE01:6701
```

Questo comando abilita un Adaptive Job Server con un account amministrativo specifico denominato `SysAdmin`:

```
ccm.exe -enable MACHINE01.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

Questo comando consente l'accesso con un account amministrativo specificato per disabilitare un Adaptive Job Server in esecuzione in un secondo computer:

```
ccm.exe -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

## 27.3 Righe di comando server

### 27.3.1 Panoramica sulle righe di comando

In questa sezione sono elencate le opzioni della riga di comando che controllano il funzionamento di ciascun server della piattaforma BI.

Quando si avvia o si configura un server tramite la console CMC, il server viene avviato o riavviato con una riga di comando predefinita che include una serie tipica di opzioni e valori. Nella maggioranza dei casi, non è necessario modificare direttamente le righe di comando predefinite. È inoltre possibile manipolare la maggior parte delle impostazioni comuni tramite diverse schermate di configurazione server della CMC. Per riferimento, questa sezione fornisce un elenco completo delle opzioni della riga di comando supportate da ciascun server. È possibile modificare la riga di comando di ogni server direttamente, se è necessario personalizzare ulteriormente il comportamento della piattaforma BI.

In questa sezione i valori riportati tra parentesi quadre [ ] sono opzionali.

#### **Nota:**

Nelle tabelle seguenti sono elencate le opzioni della riga di comando supportate. I server della piattaforma BI utilizzano una serie di opzioni interne non elencate in queste tabelle. Tali opzioni non devono essere modificate.

#### 27.3.1.1 Per visualizzare o modificare la riga di comando di un server

1. Utilizzare la console CMC (Central Management Console) per arrestare il server.
2. Fare clic con il pulsante destro del mouse sul server e scegliere **Proprietà**.
3. Nella schermata "Proprietà" modificare la riga di comando per il server e fare clic su **Salva e chiudi**.
4. Avviare il server.

## 27.3.2 Opzioni standard per tutti i server

Le opzioni della riga di comando descritte di seguito sono valide per tutti i server della piattaforma SAP BusinessObjects Business Intelligence, se non indicato altrimenti. Per informazioni sulle opzioni specifiche di ciascun tipo di server, fare riferimento al resto di questa sezione.

Opzione	Argomenti validi	Comportamento
<code>-requestPort</code>	<i>port</i>	<p>Specificare la porta su cui il server è in ascolto. Il server registra questa porta nel CMS. Se non è specificato alcun valore, viene scelta automaticamente una porta libera superiore a 1024.</p> <p><b>Nota:</b> questa porta viene utilizzata per scopi diversi da server diversi. Prima di apportare modifiche, consultare la sezione relativa alla configurazione dei numeri di porta nel <i>Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence</i>.</p>
<code>-loggingPath</code>	<i>percorso assoluto</i>	Specificare il percorso in cui vengono creati i file di registro.

### 27.3.2.1 Gestione dei segnali UNIX

In UNIX, i daemon della piattaforma BI gestiscono i segnali seguenti:

- `SIGTERM` provoca un normale arresto del server (codice di uscita = 0).
- `SIGSEGV`, `SIGBUS`, `SIGSYS`, `SIGFPE` e `SIGILL` causano un arresto rapido (codice di uscita = 1).

### 27.3.3 Central Management Server

Questa sezione riporta le opzioni della riga di comando specifiche del CMS. Il percorso predefinito del server in Windows è `DIRINSTALL\BusinessObjects Enterprise XI 4.0\win64_x64\CMS.exe`.

Il percorso predefinito del server in UNIX è `DIRINSTALL/bobje/enterprise40/piattaforma/boe_cmsd`.

Opzione	Argomenti validi	Comportamento
<code>-threads</code>	<i>number</i>	Specifica il numero di thread di lavoro inizializzati e utilizzati dal server CMS. Il valore può essere compreso tra 12 e 150 e 50 è l'impostazione predefinita.
<code>-reinitializedb</code>		Fare in modo che il CMS elimini il database di sistema e lo crei nuovamente solo con gli oggetti di sistema predefiniti. Tutti i dati esistenti nel database si perdono quando viene ricreato.
<code>-quit</code>		Imporre la chiusura del CMS dopo l'elaborazione dell'opzione <code>-reinitializedb</code> .
<code>-receiverPool</code>	<i>number</i>	Specificare il numero di thread che il CMS crea per ricevere le richieste client. Un client può essere un altro server SAP BusinessObjects, la Pubblicazione guidata report, Crystal Reports o un'applicazione client personalizzata creata dall'utente. Il valore predefinito è 5. In genere, non è necessario aumentare tale valore, a meno di non creare un'applicazione personalizzata con molti client.

Opzione	Argomenti validi	Comportamento
<code>-maxobjectsincache</code>	<i>number</i>	Specificare il numero massimo di oggetti che il CMS archivia nella cache. Se si aumenta il numero di oggetti, si riduce il numero di chiamate al database necessarie e migliorano significativamente le prestazioni del CMS. Tuttavia, inserire troppi oggetti in memoria può ridurre eccessivamente la memoria che il CMS ha a disposizione per elaborare le query. Il limite superiore è 100000.
<code>-ndbqthreads</code>	<i>number</i>	Specificare il numero dei thread di lavoro CMS che inviano richieste al database. Ogni thread ha una connessione al database, quindi è necessario fare attenzione a non superare la capacità del database. Nella maggior parte dei casi, il valore massimo da impostare è 20.
<code>-oobthreads</code>	<i>number</i>	Se il cluster include più di otto membri di cluster CMS, assicurarsi che la riga di comando per ogni CMS includa questa opzione. Specificare il numero di servizi CMS nel cluster. Questa opzione assicura che il cluster possa sostenere il carico pesante.

**Argomenti correlati**

- [Opzioni standard per tutti i server](#)

**27.3.4 Server di elaborazione Crystal Reports e Crystal Reports Cache Server**

Il server di elaborazione Crystal Reports e Crystal Reports Cache Server sono entrambi controllati dalla riga di comando. Le opzioni della riga di comando determinano se il server viene avviato come server di elaborazione, come cache server o come entrambi. Le opzioni valide solo per un tipo di server sono riportate in basso.

I percorsi predefiniti dei server in Windows sono:

- `DIRINSTALL\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\cacheserver.exe.`
- `DIRINSTALL\BusinessObjects Business Intelligence platform XI 4.0\win64_x64\pageserver.exe.`

I percorsi predefiniti dei server in UNIX sono:

- `DIRINSTALL/sap_bobj/enterprise_xi40/PIATTAFORMA/boe_cachesd.`
- `DIRINSTALL/sap_bobj/enterprise_xi40/PIATTAFORMA/boe_procd.`

Opzione	Argomenti validi	Comportamento
-cache		Abilitare la funzionalità Cache Server.
-deleteCache		Eliminare la directory cache ogni volta che il server viene avviato e interrotto.
-report_ProcessExtPath	<i>absolute path</i>	Specificare la directory predefinita per le estensioni di elaborazione. Per ulteriori informazioni consultare il <i>Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence</i> .

#### Argomenti correlati

- [Opzioni standard per tutti i server](#)

## 27.3.5 Server di elaborazione di Dashboards e Server cache di Dashboards

Il Server di elaborazione di Dashboards e il Server cache di Dashboards vengono controllati in modo molto simile dalla riga di comando. Le opzioni della riga di comando determinano se il server viene

avviato come server di elaborazione, come cache server o come entrambi. Le opzioni valide solo per un tipo di server sono riportate in basso.

I percorsi predefiniti dei server in Windows sono:

- `DIRINSTALL\SAP BusinessObjects\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\xccache.exe.`
- `DIRINSTALL\SAP BusinessObjects\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\xcproc.exe.`

I percorsi predefiniti dei server in UNIX sono:

- `DIRINSTALL/sap_bobj/enterprise_xi40/<piattaforma>_64/boe_xccached.`
- `DIRINSTALL/sap_bobj/enterprise_xi40/<piattaforma>_64/xcprocd.`

Opzione	Argomenti validi	Comportamento
<code>-cache</code>		Abilitare la funzionalità Cache Server.
<code>-dir</code>	<i>absolutePath</i>	Specificare la directory di cache per Cache Server e la directory temporanea per il server di elaborazione. Le directory create sono <i>absolutePath/cache</i> e <i>absolutePath/temp</i>
<code>-deleteCache</code>		Eliminare la directory cache ogni volta che il server viene avviato e interrotto.
<code>-psdir</code>	<i>absolutePath</i>	Specificare la directory temporanea per il server di elaborazione. Questa opzione sostituisce <code>-dir</code> .
<code>-refresh</code>	<i>minutes</i>	Condividere le pagine memorizzate nella cache per il numero specificato di minuti.

Opzione	Argomenti validi	Comportamento
<code>-auditMaxEventsPerFile</code>	<i>number</i>	Nel Cache Server, specifica il numero massimo di azioni di controllo registrate nel file di registro di controllo. Il valore predefinito è 500. Se questo numero massimo di record viene superato, il server apre un nuovo file di registro.

**Argomenti correlati**

- [Opzioni standard per tutti i server](#)

**27.3.6 Job Server**

Questa sezione riporta le opzioni della riga di comando specifiche per i Job Server adattivi.

Il percorso predefinito del server in Windows è `DIRINSTALL\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\JobServer.exe`.

Il percorso predefinito del server in UNIX `DIRINSTALL/sap_bobj/enterprise_xi40/PIATTAFORMA/boe_jobds`.

Opzione	Argomenti validi	Comportamento
<code>-dir</code>	<i>absolute path</i>	Specificare la directory dei dati del Job Server.
<code>-maxJobs</code>	<i>number</i>	Impostare il numero massimo di processo simultanei che il server gestirà. Il valore predefinito è 5.



Opzione	Argomenti validi	Comportamento
<code>-requestJSChildPorts</code>	<i>lowerbound-upperbound</i>	<p>Specificare l'intervallo di porte che i processi secondari devono utilizzare in un ambiente firewall. Ad esempio, 6800-6805 limita i processi secondari a sei porte.</p> <p><b>Nota:</b> Affinché questa opzione diventi operativa, è inoltre necessario specificare l'impostazione <code>-requestPort</code>.</p>
<code>-report_ProcessExtPath</code>	<i>absolute path</i>	<p>Specificare la directory predefinita per le estensioni di elaborazione. Per ulteriori informazioni consultare il <i>Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence</i>.</p>

**Argomenti correlati**

- [Opzioni standard per tutti i server](#)

## 27.3.7 Adaptive Processing Server

Adaptive Processing Server utilizza parametri definiti per SAP Java Virtual Machine (SAP JVM). Per ulteriori informazioni, fare riferimento alla documentazione di SAP JVM.

## 27.3.8 Report Application Server

Questa sezione riporta le opzioni della riga di comando specifiche Report Application Server.

Il percorso predefinito del server in Windows è `DIRINSTALL\SAP BusinessObjects Business Intelligence platform 4.0\win32_x86\crystalras.exe`.

Il percorso predefinito del server in UNIX è *DIRINSTALL/sap\_bobj/enterprise\_xi40/PIATTA  
FORMA/ras/boe\_crystalrasd*.

Opzione	Argomenti validi	Comportamento
<code>-ipport</code>	<i>port</i>	Specificare il numero di porta per la ricezione delle richieste TCP/IP durante l'esecuzione in modalità autonoma (all'esterno della piattaforma BI).
<code>-report_ProcessExtPath</code>	<i>absolute path</i>	Specificare la directory predefinita per le estensioni di elaborazione. Per ulteriori informazioni consultare il <i>Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence</i> .

Opzione	Argomenti validi	Comportamento
<code>-ProcessAffinityMask</code>	<code>mask</code>	<p>Utilizzare una maschera per specificare esattamente quali CPU utilizzerà il RAS quando viene eseguito in un computer multiprocessore.</p> <p>La maschera presenta il formato <code>0xffffffff</code>, dove ogni <code>f</code> rappresenta un processore e l'elenco dei processori viene letto da destra a sinistra (in altre parole, l'ultima <code>f</code> rappresenta il primo processore). Per ogni <code>f</code>, sostituire 0 (utilizzo della CPU non consentito) o 1 (utilizzo della CPU consentito).</p> <p>Ad esempio, se si esegue il RAS su un computer a 4 processori e si desidera utilizzare il terzo e il quarto processore, specificare la maschera <code>0x1100</code>. Per utilizzare il secondo e il terzo processore, specificare <code>0x0110</code>.</p> <p><b>Nota:</b></p> <ul style="list-style-type: none"> <li>• RAS utilizza i primi processori consentiti nella stringa, fino al numero massimo specificato dalla licenza. Se si dispone di una licenza per due processori, <code>0x1110</code> ha lo stesso effetto di <code>0x0110</code>.</li> <li>• Il valore predefinito della maschera è <code>-1</code>, che ha lo stesso significato di <code>0x1111</code>.</li> </ul>

**Argomenti correlati**

- [Opzioni standard per tutti i server](#)

## 27.3.9 Server di elaborazione Web Intelligence

In questa sezione sono elencate le opzioni della riga di comando specifiche di Server di elaborazione Web Intelligence.

Il percorso predefinito del server in Windows è `DIRINSTALL\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\WIReportServer.exe`.

Il percorso predefinito del server in UNIX è `DIRINSTALL/sap_bobj/enterprise_xi40/PIATTA FORMA/WIReportServer`.

Opzione	Argomenti validi	Comportamento
<code>-ConnectionTimeout Minutes</code>	<i>minutes</i>	Specifica il numero di minuti prima del timeout del server.
<code>-MaxConnections</code>	<i>number</i>	Specifica il numero massimo di connessioni simultanee che il server consente in una volta.
<code>-DocExpressEnable</code>		Abilita la memorizzazione dei documenti Web Intelligence durante la visualizzazione dei documenti stessi.
<code>-DocExpressRealTime CachingEnable</code>		Abilita la cache in tempo reale dei documenti Web Intelligence.
<code>-DocExpressCache DurationMinutes</code>	<i>minutes</i>	Specifica il tempo (in minuti) per il quale il contenuto è memorizzato nella cache.
<code>-DocExpressMaxCache SizeKB</code>	<i>kilobytes</i>	Specifica la dimensione della cache dei documenti.
<code>-EnableListOfValues Cache</code>		Abilita la cache per sessioni utente degli elenchi di valori

Opzione	Argomenti validi	Comportamento
-ListOfValuesBatchSize	<i>number</i>	Il numero massimo di valori che possono essere restituiti per ogni batch di elenco dei valori.
-UniverseMaxCacheSize	<i>number</i>	Specifica il numero di universi da memorizzare.
-WIDMaxCacheSize	<i>number</i>	Specifica il numero di documenti Web Intelligence che possono essere memorizzati nella cache.

**Argomenti correlati**

- [Opzioni standard per tutti i server](#)

### 27.3.10 Input e Output File Repository Server

Questa sezione riporta le opzioni della riga di comando specifiche dell'Input e dell'Output File Repository Server.

Il percorso predefinito dei server in Windows è `DIRINSTALL\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\fileserver.exe`

Il percorso predefinito del programma che fornisce entrambi i server in UNIX è `DIRINSTALL/sap_bobj/enterprise_xi40/piattaforma/boe_filesd`. Per impostazione predefinita, il Server Intelligence Agent avvierà un'istanza di `boe_filesd` per l'Input File Repository Server e un'istanza per l'Output File Repository Server.

Opzione	Argomenti validi	Comportamento
-rootDir	<i>absolutePath</i>	<p>Impostare la directory principale delle sottocartelle e dei file gestiti dal server. I percorsi file utilizzati per fare riferimento ai file del File Repository Server vengono interpretati come relativi a questa directory principale.</p> <p><b>Nota:</b> tutti gli Input File Repository Server e tutti gli Output File Repository Server devono condividere la stessa directory principale (altrimenti c'è il rischio produrre istanze incoerenti). Inoltre, la directory principale di input non deve coincidere con la directory principale di output. È consigliabile replicare le directory principali utilizzando una matrice RAID o una soluzione hardware alternativa.</p>
-tempDir	<i>absolutePath</i>	<p>Impostare il percorso della directory temporanea che il FRS utilizza per il trasferimento di file. Utilizzare questa opzione della riga di comando se si desidera controllare il percorso della directory temporanea del server FRS o se il nome della directory temporanea predefinita generato dal server FRS supera il limite di percorso del file system, impedendo l'avvio del server FRS.</p> <p><b>Nota:</b> Non specificare una directory esistente per questa opzione. La directory specificata verrà svuotata all'avvio di FRS e rimossa all'arresto di FRS. Se si utilizza una directory esistente, verrà svuotata e rimossa.</p>

Opzione	Argomenti validi	Comportamento
-maxidle	<i>minutes</i>	Specificare il numero di minuti trascorsi i quali una sessione inattiva viene eliminata.

**Argomenti correlati**

- [Opzioni standard per tutti i server](#)

**27.3.11 Event Server**

Questa sezione riporta le opzioni della riga di comando specifiche dell'Event Server.

Il percorso predefinito del server in Windows è `DIRINSTALL\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\EventServer.exe`

Il percorso predefinito del server in Unix è `DIRINSTALL/sap_bobj/enterprise_xi40/<piattaforma>/boe_eventsd`

Opzione	Argomenti validi	Comportamento
-cleanup	<i>minutes</i>	Specificare la frequenza (in minuti) con cui il server elimina i proxy listener. Il valore rappresenta la quantità di tempo richiesto per eseguire due eliminazioni. Se ad esempio si specifica un valore pari a 10, i proxy verranno puliti ogni cinque minuti.

**Argomenti correlati**

- [Opzioni standard per tutti i server](#)





# Repository diagnostic tool

## 28.1 Panoramica dello Strumento di diagnostica del repository

Lo Strumento di diagnostica del repository è uno strumento da riga di comando che esegue scansioni, diagnosi e riparazioni delle incoerenze che si possono verificare tra il database di sistema di Central Management Server (CMS) e il servizio archivio di File Repository Server (FRS) o nei metadati degli InfoObject archiviati nel database CMS.

Durante le normali operazioni, si verificano raramente conflitti nel database di sistema CMS. Tuttavia, è possibile che si verifichino conflitti durante gli eventi imprevisti, come ripristino di emergenza, ripristino di backup o interruzioni di rete. Durante questi eventi, il database di sistema CMS può essere interrotto durante l'esecuzione di un'attività. Questo può causare conflitti con gli oggetti nel database di sistema CMS.

Lo Strumento di diagnostica del repository esegue la scansione del database di sistema CMS e individua le incoerenze in report, utenti, gruppi di utenti, cartelle, server, universi, connessioni agli universi e altri oggetti.

Tale strumento esegue la scansione di due tipi di incoerenze.

- Conflitti tra oggetti e file.

Si tratta di incoerenze che si possono verificare tra InfoObject nel database CMS e i file corrispondenti nei file repository. Ad esempio, un file archiviato nel file repository server potrebbe non disporre di un oggetto corrispondente nel database di sistema CMS.

- Incoerenze nei metadati di InfoObject.

Si tratta di incoerenze che possono essere presenti in una definizione di oggetto di InfoObject (metadati) nel database CMS. Ad esempio, un InfoObject può fare riferimento a un altro InfoObject che non esiste nel database CMS.

Lo Strumento di diagnostica del repository esegue due funzioni, a seconda dei parametri specificati durante l'esecuzione:

- Esegue la scansione del database di sistema CMS e dei servizi archivi FRS, segnala le incoerenze e produce un file di registro in formato XML con le azioni consigliate per riparare le incoerenze.
- Esegue la scansione e ripara le incoerenze individuate nel database di sistema CMS e nel FRS e segnala le azioni eseguite in un file di registro in formato XML.

## 28.2 Utilizzo dello strumento di diagnostica del repository

Lo Strumento di diagnostica del repository (RDT) è disponibile su qualsiasi computer in cui sia installato Central Configuration Manager (CCM). Questo strumento da riga di comando consente di eseguire la scansione, diagnosticare e riparare le incoerenze che possono verificarsi tra il database di sistema CMS e il servizio archivio FRS o le incoerenze presenti nei metadati di InfoObject.

È invece consigliabile eseguire il backup del database CMS e del servizio archivio FRS ed eseguire lo strumento RDT sulla versione di backup con i servizi della piattaforma SAP BusinessObjects Business Intelligence inattivi. Se ciò non è possibile, lo strumento RDT può essere eseguito su un database attivo.

Se si desidera eseguire RDT su un database attivo, considerare quanto segue:

- RDT utilizza una sola connessione di database durante l'esecuzione.
- Lo strumento RDT verifica solo la coerenza del database rispetto al momento in cui ne è stata avviata l'esecuzione. Tutte le incoerenze che si verificano durante l'esecuzione dello strumento RDT non vengono registrate né corrette.
- La memoria del computer host su cui è in esecuzione RDT deve essere superiore ai valori normalmente consigliati per il sistema per l'elaborazione delle transazioni RDT:
  - Un database con un massimo di 50.000 InfoObject deve presentare una quantità aggiuntiva di 350 MB disponibile per l'elaborazione
  - Un database con un numero di InfoObject compreso tra 50.000 e 400.000 deve presentare una quantità aggiuntiva di 1,7 GB disponibile per l'elaborazione
  - Un database con un numero di InfoObject compreso tra 400.000 e 1.000.000 deve presentare una quantità aggiuntiva di 4 GB disponibile per l'elaborazione
- RDT non deve essere eseguito dal server CMS. Se viene eseguito su un computer separato, si riduce l'impatto sulle prestazioni del sistema.
- Lo strumento può avere un impatto moderato sulle prestazioni del database mentre è in esecuzione.

Lo strumento RDT non richiede che il servizio CMS sia in esecuzione. Viene eseguito direttamente sul database CMS.

### 28.2.1 Per utilizzare lo strumento Repository Diagnostic Tool

1. Se si esegue lo strumento in un computer Windows, aprire una finestra di comando ed eseguire il comando seguente:

```
DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\win64_x64\reposcan.exe
argomenti, dove argomenti è l'elenco dei parametri che si desidera specificare.
```

2. Se si esegue lo strumento in un computer Unix, aprire una shell compatibile /usr/bin/sh ed eseguire il comando seguente.

`.DIRINSTALL/sap_bobj/enterprise_xi40/piattaforma/boe_reposcan.sh argomenti`  
dove *piattaforma* è "linux\_x64", "solaris\_sparcv9", "hpux\_ia64" o "aix\_rs6000\_64" e *argomenti* è l'elenco di parametri che si desidera specificare.

Lo strumento Repository Diagnostic Tool esegue la scansione del repository per individuare incoerenze. A seconda dei parametri specificati, lo strumento esegue la diagnosi e la registrazione delle incoerenze oppure ripara le incoerenze e registra le azioni eseguite.

In `Repo_Scan_yyyy_mm_dd_hh_mm_ss.xml` vengono elencate le incoerenze individuate dallo strumento. Se lo strumento viene configurato per riparare le incoerenze riscontrate, viene creato anche il file `Repo_Repair_yyyy_mm_dd_hh_mm_ss.xml`. In questo file sono indicati in dettaglio gli oggetti riparati e i file orfani eliminati. Sono anche elencate le incoerenze che non possono essere riparate.

Il percorso dei file di registro può essere specificato dal parametro `outputdir`. Se il parametro non viene specificato, la directory predefinita per i file di registro è `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\reposcan` in Windows e `./sap_bobj/enterprise_xi40/reposcan` in Unix.

**Nota:**

L'applicazione fornisce un file XSL predefinito che può essere utilizzato con il file XML per creare una pagina HTML. Il file XSL viene memorizzato nella directory `DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\reposcan` in Windows e `./sap_bobj/enterprisexi_40/reposcan` in Unix.

Per un elenco dei messaggi di avviso e di azioni consigliate eseguite dallo strumento RDT quando rileva incoerenze, vedere *Incoerenze nei metadati CMS* e *Incoerenze tra CMS e FRS*.

**Argomenti correlati**

- [Incoerenze nei metadati CMS](#)
- [Incoerenze tra CMS e FRS](#)

## 28.2.2 Parametri di Repository Diagnostic Tool

Questo strumento accetta i parametri riportati nella tabella seguente:

**Nota:**

Durante l'esecuzione, le voci dei file di parametro vengono sovrascritte dagli argomenti della riga di comando.

Tabella 28 - 1: Parametri generali

Parametro	Facoltativi o obbligatori	Descrizione
dbdriver	Obbligatorio	<p>Tipo di driver utilizzato per connettersi al database CMS. I valori accettati sono:</p> <ul style="list-style-type: none"> <li>• db2databasesubsystem</li> <li>• maxdbdatabasesubsystem</li> <li>• mysqldatabasesubsystem</li> <li>• oracledatabasesubsystem</li> <li>• sqlserverdatabasesubsystem</li> <li>• sybasedatabasesubsystem</li> <li>• sqlanywheredatabasesubsystem</li> </ul>
connect	Obbligatorio	<p>Dettagli di connessione utilizzati per connettersi al database CMS.</p> <p>Ad esempio: <code>-connect "UID=root;PWD=password;DSN=dsn;HOSTNAME=nomehost;PORT=numeroporta"</code></p>

Parametro	Facoltativi o obbligatori	Descrizione
dbkey	Obbligatorio	<p>Immettere la chiave cluster per la distribuzione della piattaforma BI.</p> <p>Se non si conosce la chiave cluster, reimpostarla procedendo come indicato di seguito:</p> <p><b>Nota:</b></p> <p>Se il computer si trova in un cluster, sarà necessario eseguire questa procedura per tutti i membri del cluster. Eseguire il backup dell'archivio file e del database CMS prima di procedere.</p> <ol style="list-style-type: none"> <li>1. Avviare Central Configuration Manager (CCM).</li> <li>2. In CCM fare clic con il pulsante destro del mouse su Server Intelligence Agent (SIA) e scegliere <b>Interrompi</b>. Non procedere al passaggio 3 fino a quando lo stato SIA non è contrassegnato come "Interrotto".</li> <li>3. Fare clic con il pulsante destro del mouse sul SIA e scegliere <b>Proprietà</b>.</li> <li>4. Nella scheda Configurazione fare clic su <b>Cambia</b> accanto a "Configurazione chiave cluster CMS".</li> <li>5. Viene visualizzato un messaggio di avviso. Fare clic su Sì per continuare.</li> <li>6. Nella finestra di dialogo "Modifica chiave cluster" immettere la stessa chiave a otto caratteri in entrambi i campi "Nuova chiave cluster" e "Conferma nuova chiave cluster".</li> </ol> <p><b>Nota:</b></p> <ul style="list-style-type: none"> <li>• Lo Strumento di diagnostica del repository non verrà eseguito se il parametro dbkey viene omissso o se la chiave cluster non è corretta.</li> <li>• La chiave cluster visualizzata nel CCM viene crittografata e non può essere utilizzata nel parametro dbkey.</li> </ul> <p>Per ulteriori informazioni sulle chiavi cluster, vedere "Protezione della piattaforma BI" nel <i>Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence</i>.</p>

Parametro	Facoltativi o obbligatori	Descrizione
inputfrsdir	Obbligatorio	<p>Il percorso file di Input File Repository Server.</p> <p><b>Nota:</b> L'account utente con cui è stato eseguito l'accesso viene utilizzato per eseguire lo strumento da riga di comando. È necessario che disponga del controllo completo sul percorso di file.</p>
outputfrsdir	Obbligatorio	<p>Il percorso file di Output File Repository Server.</p> <p><b>Nota:</b> L'account utente con cui è stato eseguito l'accesso viene utilizzato per eseguire lo strumento da riga di comando. È necessario che disponga del controllo completo sul percorso di file.</p>
outputdir	Facoltativo	<p>Percorso del file in cui lo strumento RDT scrive i file di registro.</p> <p>Il valore predefinito è <code>DIRINSTALL\SAP BusinessObjects Enterprise XI 4.0\reposcan in Windows</code> e <code>./sap_bobj/enterprise_xi40/reposcan in Unix</code>.</p>
count	Facoltativo	<p>Numero di errori approssimativi di cui eseguire la scansione. Assicura prestazioni ottimali. Il conteggio superiore è <math>2e31 - 1</math>. Un valore 0 viene interpretato come l'intero repository.</p> <p>Il valore predefinito è 0.</p>
repair	Facoltativo	<p>Indica allo strumento RDT di riparare tutte le incoerenze riscontrate. Il comportamento predefinito è quello di segnalare solo le incoerenze senza eseguirne la riparazione. Se il parametro <code>-repair</code> esiste nella riga di comando, RDT segnala e corregge tutte le incoerenze.</p> <p><b>Avvertenza:</b> Questo processo eliminerà gli oggetti o i file orfani nel database del repository.</p>

Parametro	Facoltativi o obbligatori	Descrizione
scanfrs	Facoltativo	<p>Specifica se lo strumento RDT esegue la scansione dei server CMS e FRS per individuare le incoerenze. I valori accettabili sono True e False.</p> <p>Il valore predefinito è True.</p>
scancms	Facoltativo	<p>Specifica se lo strumento RDT esegue la scansione del server CMS per individuare le incoerenze tra InfoObject. I valori accettabili sono True e False.</p> <p>Il valore predefinito è True.</p>
submitterid	Facoltativo	<p>Specifica l'ID utente da utilizzare in sostituzione di ID mancanti o non validi per gli oggetti pianificati. Se non viene fornito alcun valore, lo strumento RDT non sostituisce gli ID non validi. Se l'ID utente fornito non esiste nel server CMS, lo strumento RDT richiede un ID valido.</p> <p>Questo parametro viene utilizzato solo quando lo strumento RDT viene eseguito in modalità di riparazione.</p>
startid	Facoltativo	<p>Specifica l'oggetto nel database CMS per il quale avviare la scansione. Ad esempio, se è già stata eseguita la scansione dei primi 500 oggetti nel repository, è possibile impostare -startid=501 per avviare una nuova scansione in corrispondenza del 501° oggetto.</p> <p>Il valore predefinito è 1.</p>
optionsfile	Facoltativo	<p>Specifica il percorso di un file di parametro. Il file di parametro è un file di testo che elenca ogni opzione della riga di comando con i relativi valori. Il file deve riportare un parametro per riga.</p> <p><b>Nota:</b> Con questa opzione, è possibile impostare tutti i parametri in un file di testo come descritto in precedenza. Utilizzare questa opzione per puntare al file di parametro senza immettere i parametri nella riga di comando.</p>

Parametro	Facoltativi o obbligatori	Descrizione
syscopy	Facoltativo	<p>Questo parametro viene utilizzato quando si copia il database di repository. È necessario eseguire lo strumento sulla copia appena creata, per aggiornarla ed evitarne il clustering con i server di sistema di origine. Ciò non sarà necessario, se la copia non è in grado di comunicare con il sistema di origine. Lo strumento deve essere utilizzato solo con i parametri obbligatori e non deve essere combinato con altri parametri facoltativi presenti nell'elenco.</p> <p><b>Nota:</b> prestare attenzione a non eseguire lo strumento RDT con il parametro syscopy nel sistema di origine.</p>

Se lo strumento di diagnostica del repository è in esecuzione su un CMS cluster attivo, verranno utilizzati i seguenti parametri.

Tabella 28 - 2: Utilizzo dello strumento RDT in un server CMS cluster

Parametro	Facoltativi o obbligatori	Descrizione
requestport	Facoltativo	Il numero della porta utilizzata dallo strumento RDT per comunicare con il server CMS. Accetta numeri interi positivi. Per impostazione predefinita, lo strumento utilizza il valore del sistema operativo del computer in cui viene eseguito.
numericip	Facoltativo	<p>Se lo strumento RDT utilizza l'indirizzo IP numerico anziché il nome host per la comunicazione tra il server CMS e il computer in cui viene eseguito. I valori accettabili sono True e False.</p> <p>L'impostazione predefinita è False.</p>
ipv6	Facoltativo	<p>Il nome ipv6 del computer in cui viene eseguito lo strumento RDT. Accetta una stringa.</p> <p>Il valore predefinito è il nome host del computer in cui viene eseguito lo strumento RDT.</p>



Parametro	Facoltativi o obbligatori	Descrizione
port	Facoltativo	Il nome ipv4 del computer in cui viene eseguito lo strumento RDT. Accetta una stringa. Il valore predefinito è il nome host del computer in cui viene eseguito lo strumento RDT.
threads	Facoltativo	Numero di thread da utilizzare. Accetta numeri interi positivi. Il valore predefinito è 12.

I parametri seguenti vengono utilizzati quando lo strumento RDT utilizza SSL per comunicare con il database CMS di cui esegue la scansione.

Tabella 28 - 3: Utilizzo dello strumento RDT con SSL

Parametro	Facoltativi o obbligatori	Descrizione
protocol	Facoltativo	Specifica se lo strumento viene eseguito in modalità SSL. L'unico valore accettato è ssl.
ssl_certdir	Facoltativo	Directory che contiene i certificati SSL.
ssl_trustedcertificate	Facoltativo	Nome file del certificato.
ssl_mycertificate	Facoltativo	Nome file del certificato firmato.
ssl_mykey	Facoltativo	Nome del file che contiene la chiave SSL privata.
ssl_mykey_passphrase	Facoltativo	Nome del file che contiene la chiave di accesso SSL.

**Esempio:**

Nell'esempio seguente viene eseguita la scansione dei server CMS e FRS per entrambi i tipi di incoerenze e vengono riparate le incoerenze riscontrate.

```
reposcan.exe
-dbdriver mysqldatabasesubsystem
-connect "UID=root;PWD=Password1;DSN=myDsn;HOSTNAME=myHostname;PORT=3306"
-inputfrsdir "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\FileStore\Input"
-outputfrsdir "C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\FileStore\Output"
-dbkey cluster key
-repair
```

---

## 28.3 Incoerenze tra CMS e FRS

Nella tabella seguente vengono descritte le incoerenze che possono esistere tra un database Central Management Server (CMS) e i File Repository Server (FRS) riconosciuti dallo Strumento di diagnostica del repository. La tabella è composta da quattro colonne:

- Messaggio di avviso

Il messaggio di avviso viene scritto nei file di registro di scansione e di riparazione.

- Conflitto

Spiegazione dell'incoerenza riscontrata dallo strumento RDT per l'oggetto.

- Suggerimento

Azione consigliata dallo Strumento di diagnostica del repository quando rileva un'incoerenza. Ciò è indicato nel file di registro di scansione.

- Azione

Azione eseguita dallo strumento RDT per riparare un'incoerenza. Ciò è indicato nel file di registro di riparazione.

Messaggio di avviso	Conflitto	Suggerimento	Azione
L'oggetto <i>nome oggettotipo oggetto</i> (ID oggetto = <i>ID</i> ) fa riferimento a file che non esistono in FRS ( <i>nome file</i> ).	L'oggetto esiste nel database CMS, ma non è presente un file corrispondente nel server FRS.	Consentire all'applicazione l'eliminazione di questo oggetto. Verranno eliminati anche gli oggetti che discendono da questo oggetto.	Eliminazione dell'oggetto dal repository.
Il file <i>nome file</i> è presente in Input FRS o Output FRS, ma non è presente InfoObject nel repository.	Il file esiste nel server FRS, ma non esiste un file corrispondente nel database CMS.	Consentire la rimozione del file non collegato nell'applicazione.	Nessuna azione eseguita.
L'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) ha il file <i>nome file</i> . La dimensione del file archiviato è <i>dimensione</i> , che non corrisponde alla dimensione effettiva del file <i>dimensione</i> .	La dimensione del file non corrisponde alla dimensione del file InfoObject.	Consentire l'aggiornamento dell'oggetto con la dimensione file corretta nell'applicazione.	Aggiornamento dell'oggetto con la dimensione file corretta.
Questa directory non contiene file.	La cartella FRS è vuota.	Consentire la rimozione della directory nell'applicazione.	Rimozione della cartella vuota.

## 28.4 Incoerenze nei metadati CMS

Nella tabella seguente vengono illustrate le incoerenze che si possono verificare nei metadati degli oggetti presenti nel database di un sistema CMS (Central Management Server) riconosciute dallo Strumento di diagnostica del repository. La tabella è composta da quattro colonne:

- Messaggio di avviso

Il messaggio di avviso viene scritto nei file di registro di scansione e di riparazione.

- Conflitto

Spiegazione dell'incoerenza riscontrata dallo strumento RDT per l'oggetto.

- Suggerimento

Azione consigliata dallo Strumento di diagnostica del repository quando rileva un'incoerenza. Ciò è indicato nel file di registro di scansione.

- Azione

Azione eseguita dallo strumento RDT per riparare un'incoerenza. Ciò è indicato nel file di registro di riparazione.

Messaggio di avviso	Conflitto	Suggerimento	Azione
L'oggetto principale dell'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) non è disponibile (ID oggetto principale = <i>ID</i> ).	Un ID oggetto principale dell'oggetto non è disponibile o non è valido.	Consentire lo spostamento dell'oggetto nella cartella "Riparazione BOE" nell'applicazione.	Spostamento dell'oggetto e dei relativi oggetti secondari nella cartella Riparazione BOE.
L'oggetto proprietario dell'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) non è disponibile (ID oggetto proprietario = <i>ID</i> ).	Un ID oggetto proprietario dell'oggetto non è disponibile o non è valido.	Consentire all'applicazione di assegnare l'oggetto all'amministratore.	Assegnazione dell'oggetto all'amministratore.
L'oggetto mittente dell'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) non è disponibile (ID oggetto mittente = <i>ID</i> ).	Un ID oggetto mittente dell'oggetto non è disponibile o non è valido.	<p>Il suggerimento visualizzato dallo strumento RDT dipende dal fatto che sia stato fornito un valore per il parametro -submitterid.</p> <ul style="list-style-type: none"> <li>Se si fornisce tale parametro, il suggerimento è "Consentire l'aggiornamento dell'oggetto con la dimensione file corretta nell'applicazione".</li> <li>Se non si fornisce questo parametro, il suggerimento è "Ripianificare l'oggetto o utilizzare la riga di comando -submitterid per sostituire l'ID mittente non valido".</li> </ul>	<p>Se si fornisce un valore per il parametro -submitterid, lo strumento RDT applica tale valore per l'ID mittente dell'oggetto.</p> <p>Se non si fornisce un valore per tale parametro, lo strumento RDT non esegue alcuna azione. Quando si ripianifica l'oggetto, il server CMS applica un nuovo ID.</p>
La proprietà dell'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) dell'ultima istanza completata fa riferimento a un oggetto mancante (ID oggetto ultima istanza completata = <i>ID</i> ).	L'ultima istanza completata dell'oggetto non è disponibile o non è valida.	Consentire il ricalcolo della proprietà nell'applicazione.	Ricalcolo della proprietà.

Messaggio di avviso	Conflitto	Suggerimento	Azione
L'oggetto calendario dell'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) non è disponibile (ID oggetto calendario = <i>ID</i> ).	L'oggetto fa riferimento a un calendario che non esiste.	Ripianificare l'oggetto con un calendario esistente. Non è possibile eseguire alcuna azione nell'applicazione.	Nessuna azione eseguita.
Il gruppo di server di pianificazione obbligatorio dell'oggetto <i>tipo oggettonome oggetto'</i> (ID oggetto = <i>ID</i> ) è mancante (ID oggetto gruppo server = <i>ID</i> ).	Il server preferito non esiste.	Ripianificare l'oggetto e scegliere un gruppo di server esistente. Non è possibile eseguire alcuna azione nell'applicazione.	Nessuna azione eseguita.
Uno o più oggetti mancanti dall'elenco di eventi in sospeso dell'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) (ID oggetto/i evento = <i>ID</i> ).	Uno o più degli eventi che l'oggetto attende non esistono.	Ripianificare l'oggetto in modo che attenda oggetti evento esistenti. Non è possibile eseguire alcuna azione nell'applicazione.	Nessuna azione eseguita.
Uno o più oggetti mancanti dall'elenco di eventi da attivare dell'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) (ID oggetto/i evento = <i>ID</i> ).	Questo oggetto attiva un evento inesistente.	Consentire la rimozione degli eventi mancanti dall'elenco di eventi da attivare dell'oggetto nell'applicazione.	Rimozione degli eventi mancanti dall'elenco di eventi da attivare dell'oggetto.
L'elenco di controllo di accesso dell'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) fa riferimento a un oggetto principale mancante (ID oggetto principale = <i>ID</i> ).	Voce di controllo di accesso orfana.	Consentire la rimozione dell'oggetto principale mancante dall'elenco di controllo di accesso dell'oggetto nell'applicazione.	Rimozione dell'oggetto principale mancante dall'elenco di controllo di accesso dell'oggetto.
L'elenco di controllo di accesso dell'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) fa riferimento a un livello di accesso mancante (ID livello di accesso = <i>ID</i> ).	Voce di controllo di accesso orfana.	Consentire la rimozione del livello di accesso mancante dall'elenco di controllo di accesso dell'oggetto nell'applicazione.	Rimozione del livello di accesso mancante dall'elenco di controllo di accesso dell'oggetto.

Messaggio di avviso	Conflitto	Suggerimento	Azione
L'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) ha più cartelle Preferiti.	Un account utente specifico ha più cartelle Preferiti.	Consentire il consolidamento di più cartelle in una singola cartella Preferiti nell'applicazione.	Tutte le cartelle Preferiti sono state consolidate in una singola cartella Preferiti.
L'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) contiene voci del file di input non valide ( <i>File</i> ).	L'oggetto contiene voci non valide nell'elenco di file di input.	Consentire la rimozione delle voci non valide dell'oggetto dall'elenco di file di input tramite lo strumento.	Rimozione delle voci non valide dall'elenco di file di input dell'oggetto.
L'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) contiene voci del file di input non valide ( <i>File</i> ).	L'oggetto contiene voci non valide nell'elenco di file di output.	Consentire la rimozione delle voci non valide dell'oggetto dall'elenco di file di output tramite lo strumento.	Rimozione delle voci non valide dall'elenco di file di output dell'oggetto.
Il gruppo di server di pianificazione obbligatorio dell'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) è mancante (ID oggetto gruppo server = <i>ID</i> ).	Il gruppo server cache obbligatorio non è disponibile nell'oggetto.	Ripianificare l'oggetto e scegliere un gruppo di server esistente.	Nessuna azione eseguita.
Il gruppo di server di pianificazione obbligatorio dell'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) è mancante (ID oggetto gruppo server = <i>ID</i> ).	Il gruppo server di elaborazione obbligatorio non è disponibile nell'oggetto.	Ripianificare l'oggetto e scegliere un gruppo di server esistente.	Nessuna azione eseguita.
Uno o più oggetti mancanti dall'elenco di profili dell'oggetto <i>tipo oggettonome oggetto</i> (ID oggetto = <i>ID</i> ) (ID profilo/i = <i>ID</i> ).	Nell'elenco di profili dell'oggetto non sono disponibili uno o più oggetti.	Aggiornare la pubblicazione con i profili esistenti. Non è possibile eseguire alcuna azione nell'applicazione.	Nessuna azione eseguita.

## Appendice sui diritti

### 29.1 Appendice sui diritti

In questa appendice sui diritti è elencata e descritta la maggior parte dei diritti che è possibile impostare su oggetti diversi nel sistema della piattaforma BI. Nei casi in cui sia necessario più di un diritto per eseguire un task su un oggetto, vengono fornite informazioni sui diritti aggiuntivi necessari e sugli oggetti su cui è necessario impostare tale diritti. Per ulteriori informazioni sull'impostazione dei diritti, consultare il capitolo *Impostazione dei diritti* del *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

### 29.2 Diritti generali

I diritti descritti in questa sezione sono applicabili a più tipi di oggetto. Molti di questi diritti hanno anche diritti del proprietario equivalenti. I diritti del proprietario sono validi solo per il proprietario dell'oggetto di cui vengono verificati i diritti.

I diritti seguenti sono applicabili solo agli oggetti che è possibile pianificare.

- Diritto "Pianificare il documento da eseguire".
- Diritto "Pianifica per conto degli utenti".
- Diritto "Pianificare in destinazioni".
- Diritto "Visualizzare istanze documento".
- Diritto "Eliminare istanze".
- Diritto "Interrompere e riprendere istanze del documento".
- Diritto "Ripianificare istanze".

Diritto	Descrizione
"Visualizzare oggetti"	Consente di visualizzare gli oggetti e le relative proprietà. Se non si dispone di questo diritto su un oggetto, l'oggetto viene nascosto nel sistema della piattaforma BI. Si tratta di un diritto di base necessario per tutte le attività.
"Aggiungere oggetti alla cartella"	Consente di aggiungere oggetti a una cartella. Questo diritto è anche applicabile agli oggetti che si comportano come cartelle, ad esempio le cartelle Posta in arrivo e <i>Preferiti</i> o i pacchetti di oggetti.
"Modificare oggetti"	Consente di modificare il contenuto e le proprietà di oggetti e cartelle.
"Modificare i diritti che gli utenti hanno sugli oggetti"	Consente di modificare le impostazioni di protezione per un oggetto.
"Modificare in modo sicuro i diritti degli utenti sugli oggetti"	Consente di concedere ad altri utenti diritti o livelli di accesso di cui si dispone per un oggetto. A tale scopo, è necessario questo diritto sull'utente e sull'oggetto stesso. Per ulteriori informazioni su questo diritto, consultare il capitolo "Impostazione dei diritti" del <i>Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence</i> .
"Definire gruppi di server per elaborare i lavori"	Consente di specificare quale gruppo di server utilizzare per l'elaborazione degli oggetti. Questo diritto è applicabile solo agli oggetti per i quali è possibile specificare server di elaborazione.  Per specificare un gruppo di server, è anche necessario disporre del diritto "Modificare oggetti" sull'oggetto.
"Eliminare oggetti"	Consente di eliminare gli oggetti e le relative istanze.
"Copia oggetti in un'altra cartella"	Consente di creare copie di oggetti in altre cartelle nel server CMS. A tale scopo, è necessario disporre del diritto "Aggiungere oggetti alla cartella" per la cartella di destinazione.  <b>Nota:</b> Quando viene copiato un oggetto, la protezione esplicita su quell'oggetto non viene copiata; il nuovo oggetto eredita le impostazioni di protezione dalla cartella di destinazione, ma è necessario reimpostare la protezione esplicita.



Diritto	Descrizione
"Replica contenuto"	Consente di replicare gli oggetti in un altro sistema in una distribuzione federata.
"Pianificare il documento da eseguire"	Consente di pianificare gli oggetti.
"Pianifica per conto degli utenti"	<p>Consente di pianificare gli oggetti per altri utenti o gruppi. L'utente o il gruppo per il quale si pianifica l'oggetto diventa il proprietario dell'istanza dell'oggetto.</p> <p>Per pianificare un oggetto per altri utenti o gruppi, è anche necessario disporre dei diritti seguenti:</p> <ul style="list-style-type: none"> <li>• Questo diritto sull'utente o il gruppo.</li> <li>• Diritto "Pianificare il documento da eseguire" sull'oggetto.</li> </ul>
"Pianificare in destinazioni"	<p>Consente di eseguire le operazioni seguenti:</p> <ul style="list-style-type: none"> <li>• Pianificare gli oggetti in destinazioni diversa dal percorso Enterprise predefinito.</li> <li>• Modificare le destinazioni predefinite specificate per la pianificazione.</li> </ul> <p>Per pianificare l'oggetto in destinazioni, è anche necessario disporre dei diritti seguenti:</p> <ul style="list-style-type: none"> <li>• Diritto "Pianificare il documento da eseguire" sull'oggetto da pianificare.</li> <li>• Diritto "Aggiungere oggetti alla cartella" nella Posta in arrivo del destinatario, per pianificare in una destinazione Posta in arrivo.</li> <li>• Diritto "Copia oggetti in un'altra cartella" sull'oggetto da pianificare, per inviare una copia in una destinazione Posta in arrivo anziché un collegamento.</li> </ul>
"Visualizzare istanze documento"	Consente di visualizzare le istanze di oggetti. Si tratta di un diritto di base necessario per tutte le attività eseguite sulle istanze di oggetti.

Diritto	Descrizione
"Eliminare istanze"	Consente di eliminare solo le istanze di oggetti. Se si dispone del diritto "Eliminare oggetti", non è necessario questo diritto per eliminare le istanze.
"Interrompere e riprendere istanze del documento"	Consente di interrompere e riprendere le istanze di oggetti in esecuzione.
"Ripianificare istanze"	Consente di ripianificare le istanze di oggetti.

#### Argomenti correlati

- [Diritti del proprietario](#)
- [Scelta tra le opzioni Modificare i diritti che gli utenti hanno sugli oggetti](#)

## 29.3 Diritti per tipi di oggetti specifici

### 29.3.1 Diritti sulla cartella

Per semplificare l'amministrazione dei diritti, è consigliabile impostare i diritti sulle cartelle in modo che il relativo contenuto erediti le impostazioni di protezione. I diritti sulle cartelle includono i seguenti:

- Diritti generali applicabili all'oggetto cartella.
- Diritti specifici dei tipi correlati al contenuto della cartella, ad esempio il diritto **Stampa i dati del report** sui report Crystal.

#### Argomenti correlati

- [Diritti specifici del tipo](#)

### 29.3.2 Categorie

I diritti in questa sezione sono diritti generali con un significato specifico nel contesto delle categorie pubbliche e personali.

**Nota:**

Gli oggetti nelle categorie non ereditano diritti impostati sulle categorie.

Diritto	Descrizione
"Aggiungere oggetti alla cartella"	Consente di creare nuove categorie nelle categorie. Questo diritto non è necessario per aggiungere oggetti a una categoria.
"Modificare oggetti"	<p>Consente di eseguire le seguenti operazioni:</p> <ul style="list-style-type: none"> <li>• Modificare le proprietà delle categorie.</li> <li>• Spostare la categoria in un'altra categoria come categoria secondaria.</li> <li>• Aggiungere oggetti alla categoria.</li> <li>• Rimuovere oggetti dalla categoria.</li> </ul> <p>Per spostare una categoria in un'altra categoria come categoria secondaria, sono necessari i seguenti diritti:</p> <ul style="list-style-type: none"> <li>• Il diritto "Eliminare oggetti" nella categoria originale.</li> <li>• Il diritto "Aggiungere oggetti alla cartella" nella categoria di destinazione.</li> </ul>
"Eliminare oggetti"	Consente di eliminare la categoria.

### 29.3.3 Documenti Desktop Intelligence

I diritti in questa sezione sono applicabili unicamente ai documenti Desktop Intelligence.

Diritto	Descrizione
"Usa elenchi di valori"	Consente agli utenti di utilizzare elenchi di valori.
"Scarica file associati all'oggetto"	Consente agli utenti di scaricare i file associati all'oggetto.
"Esporta dati del report"	Consente agli utenti di esportare i dati dei documenti nei formati Excel, PDF e CSV. Se non si dispone di questo diritto, è necessario disporre del diritto "Salva in formato CSV", "Salva in formato Excel" o "Salva in formato PDF"; questi diritti consentono di esportare documenti solo nel formato specificato.
"Visualizza SQL"	Consente agli utenti di visualizzare le istruzioni SQL generate per la query.
"Aggiorna dati del report"	Consente agli utenti di aggiornare i dati dei documenti.
"Aggiorna elenco di valori"	Consente agli utenti di aggiornare gli elenchi di valori per i prompt quando si crea il prompt o si visualizza il documento. A tale scopo, è necessario disporre anche del diritto "Usa elenchi di valori" sul documento.

Di seguito sono riportati i diritti dei documenti specifici dei formati PDF, XLS, RTF e di testo:

Diritto	Descrizione
"Aggiungere oggetti alla cartella"	Consente agli utenti di aggiungere oggetti a una cartella. Questo diritto è anche applicabile agli oggetti che si comportano come cartelle, ad esempio le cartelle Posta in arrivo e Preferiti o i pacchetti di oggetti.
"Copia oggetti in un'altra cartella"	Consente agli utenti di creare copie di oggetti in altre cartelle del CMS. A tale scopo, è necessario disporre anche del diritto "Aggiungere oggetti alla cartella" per la cartella di destinazione.
"Eliminare istanze"	Consente agli utenti di eliminare solo le istanze degli oggetti. Se si dispone del diritto "Eliminare oggetti", non è necessario questo diritto per eliminare le istanze.
"Eliminare oggetti"	Consente agli utenti di eliminare questa categoria.
"Modificare oggetti"	Consente agli utenti di modificare le proprietà delle categorie, di spostare una categoria in un'altra come sottocategoria, nonché di aggiungere e rimuovere oggetti da una categoria.

Diritto	Descrizione
"Modificare i diritti che gli utenti hanno sugli oggetti"	Consente agli utenti di modificare qualsiasi diritto, per qualsiasi utente su un determinato oggetto.
"Interrompere e riprendere istanze del documento"	Consente agli utenti di sospendere o riprendere le istanze degli oggetti in esecuzione.
"Replica contenuto"	Consente agli utenti di replicare gli oggetti in un altro sistema all'interno di una distribuzione federata.
"Ripianificare istanze"	Consente agli utenti di ripianificare le istanze degli oggetti.
"Modificare in modo sicuro i diritti degli utenti sugli oggetti"	Consente agli utenti di concedere, negare o reimpostare su non specificato solo i diritti già concessi.
"Visualizzare istanze documento"	Consente agli utenti di visualizzare le istanze degli oggetti. Si tratta di un diritto di base necessario per tutte le attività eseguite sulle istanze di oggetti.
"Visualizzare oggetti"	Consente agli utenti di visualizzare la categoria e le sottocategorie che contiene.

### 29.3.4 Note

Le note consentono agli utenti di aggiungere commenti su altri oggetti tramite l'applicazione Discussions. Le note sono collegate insieme in thread di discussione; tali thread sono considerati oggetti secondari degli oggetti presi in considerazione nella discussione. È possibile impostare diritti al livello di oggetto o di cartella per controllare l'utilizzo dei thread di discussione.

I diritti in questa sezione sono applicabili unicamente alle note.

Diritto	Descrizione
Consenti thread di discussione	<p>Questo diritto consente di eseguire le seguenti operazioni:</p> <ul style="list-style-type: none"> <li>• Avviare e rispondere ai thread di discussione.</li> <li>• Visualizzare le note in un thread di discussione.</li> <li>• Modificare o eliminare le note pubblicate.</li> </ul>

### 29.3.5 Report Crystal

I diritti in questa sezione sono applicabili unicamente ai report Crystal.

**Nota:**

Questi diritti sono applicabili unicamente quando i report Crystal si trovano nell'ambiente della piattaforma BI. Quando si scaricano i report Crystal sul disco locale, questi diritti non hanno efficacia. Per evitare questo problema, è possibile negare il diritto "Scarica file associati all'oggetto" per il report Crystal.

Diritto	Descrizione
"Stampa i dati del report"	Consente di stampare il report.
"Aggiorna dati del report"	Consente di aggiornare i dati del report.
"Esporta dati del report"	<p>Consente di esportare dati del report in qualsiasi formato quando si visualizza il report in linea nel visualizzatore Crystal Reports.</p> <p>Per esportare dati del report nel formato RPT, è necessario disporre anche del diritto "Scarica file associati all'oggetto".</p>
"Scarica file associati all'oggetto"	<p>Questo diritto consente di eseguire le seguenti operazioni:</p> <ul style="list-style-type: none"> <li>• Esportare il report nel formato RPT.</li> <li>• Aprire il report in Crystal Reports Designer.</li> <li>• Pianificare il report nel formato RPT in destinazioni esterne.</li> </ul>

### 29.3.6 Documenti Web Intelligence

I diritti in questa sezione sono applicabili unicamente ai documenti Web Intelligence.

Diritto	Descrizione
"Usa elenchi di valori"	Consente di utilizzare gli elenchi di valori.
"Esporta dati del report"	Consente di esportare i dati del documento nei formati Excel, PDF e CSV. Se non si dispone di questo diritto, è necessario disporre del diritto "Salva in formato CSV", "Salva in formato Excel" o "Salva in formato PDF"; questi diritti consentono di esportare documenti solo nel formato specificato.
"Script query - abilita visualizzazione (SQL, MDX...)"	Consente la visualizzazione degli script di query (SQL e MDX).
"Aggiorna dati del report"	Consente di aggiornare i dati del documento.
"Modifica query"	Consente di modificare le query nel documento.
"Aggiorna elenco di valori"	Consente di aggiornare gli elenchi di valori per i prompt quando si crea il prompt o si visualizza il documento. A tale scopo, è necessario disporre anche del diritto "Usa elenchi di valori" sul documento.
"Salva in formato CSV"	Consente di esportare i documenti solo come file CSV. Se si dispone già del diritto "Esporta dati del report" su un documento, questo diritto non è necessario.
"Salva in formato Excel"	Consente di esportare documenti solo come file Excel. Se si dispone già del diritto "Esporta dati del report" su un documento, questo diritto non è necessario.
"Salva in formato PDF"	Consente di esportare documenti solo come file PDF. Se si dispone già del diritto "Esporta dati del report" su un documento, questo diritto non è necessario.
"Invia a"	Consente di inviare documenti allo Scheduler, alla Posta in arrivo della piattaforma BI o come collegamenti ipertestuali nei messaggi di posta elettronica. Questo diritto consente anche agli utenti di Web Intelligence Rich Client di inviare documenti come allegati di posta elettronica.

## 29.3.7 Utenti e gruppi

È possibile impostare diritti su utenti e gruppi come per qualsiasi oggetto presente nell'ambiente della piattaforma BI. I diritti in questa sezione sono diritti specifici del tipo applicabili unicamente agli oggetti utente e gruppo oppure diritti generali aventi un significato specifico nel contesto di utenti e gruppi.

**Nota:**

- Gli utenti e i sottogruppi possono ereditare diritti dall'appartenenza al gruppo.
- L'autore di un account utente è considerato il proprietario dell'account. Tuttavia, dopo la creazione dell'account, anche l'utente a cui è destinato tale account verrà considerato un proprietario.



Diritto	Descrizione
"Modificare oggetti"	<p>Consente di eseguire le seguenti operazioni:</p> <ul style="list-style-type: none"> <li>• Modificare le proprietà per l'utente o il gruppo.</li> <li>• Gestire l'appartenenza al gruppo.</li> </ul> <p>Per aggiungere un utente o un gruppo a un altro gruppo, è necessario disporre di questo diritto sull'utente o il gruppo e sul gruppo di destinazione.</p>
"Modifica password utente"	<p>Consente di eseguire le seguenti operazioni:</p> <ul style="list-style-type: none"> <li>• Modificare la password per l'account utente. A tale scopo, è necessario disporre del diritto "Modificare oggetti" per l'account utente.</li> <li>• Modificare la password per un altro account utente. A tale scopo, è necessario disporre dei diritti "Modificare oggetti" e "Modificare i diritti che gli utenti hanno sugli oggetti" per l'account utente.</li> </ul> <p><b>Nota:</b></p> <ul style="list-style-type: none"> <li>• Questo diritto non influisce sulle seguenti impostazioni della password utente: <ul style="list-style-type: none"> <li>• "Nessuna scadenza password"</li> <li>• "Modifica obbligatoria password all'accesso successivo"</li> <li>• "Modifica password non consentita"</li> </ul> </li> <li>• Questo diritto non è applicabile alle credenziali delle origini dati per gli universi SAP Business Objects.</li> </ul>
"Sottoscrivi a pubblicazioni"	<p>Consente di aggiungere l'utente alle pubblicazioni come destinatario.</p>
"Pianifica per conto degli utenti"	<p>Consente di pianificare oggetti per conto dell'utente affinché l'utente diventi il proprietario dell'istanza dell'oggetto. A tale scopo, è necessario disporre anche del diritto "Pianifica per conto degli utenti" sull'oggetto.</p>
"Aggiungi o modifica attributi utente"	<p>Consente di modificare il valore di un indirizzo di posta elettronica dell'utente o gli attributi utente personalizzati.</p> <p>Questo diritto è applicabile solo agli utenti.</p>
"Aggiungi o modifica attributi utente (diritto proprietario)"	

Diritto	Descrizione
	<p>Consente al proprietario di un oggetto utente di modificare il valore di un indirizzo di posta elettronica dell'utente o gli attributi utente personalizzati.</p> <p>Questo diritto è applicabile solo agli utenti.</p>

### 29.3.8 Livelli di accesso

I diritti in questa sezione sono applicabili unicamente ai livelli di accesso.

Diritto	Descrizione
"Utilizza livello di accesso per l'assegnazione della protezione"	<p>Consente di assegnare il livello di accesso quando si aggiungono principali per accedere agli elenchi di controllo per gli oggetti. A tale scopo, è necessario disporre del diritto "Modificare i diritti che gli utenti hanno sugli oggetti" o "Modificare in modo sicuro i diritti che gli utenti hanno sugli oggetti" per il principale e l'oggetto. Qualora venga concesso il diritto "Modificare in modo sicuro i diritti che gli utenti hanno sugli oggetti", è necessario disporre dello stesso livello di accesso per l'oggetto.</p>

#### Argomenti correlati

- [Scelta tra le opzioni Modificare i diritti che gli utenti hanno sugli oggetti](#)

### 29.3.9 Diritti sugli universi (.unv)

I diritti in questa sezione sono applicabili agli universi creati con Universe Design Tool o agli universi .unv. I diritti elencati in questa sezione sono diritti specifici del tipo e applicabili solo agli universi oppure diritti generali con un significato specifico nel contesto degli universi.

#### Nota:

i diritti sugli universi si applicano solo quando si importano universi dal server CMS nell'applicazione Universe Design Tool. Questi diritti non si applicano quando l'universo viene salvato sul disco locale.

Diritto	Descrizione
"Aggiungere oggetti alla cartella"	Consente di aggiungere oggetti o insiemi di restrizioni all'universo. A tale scopo, è anche necessario il diritto "Modifica restrizioni di accesso".
"Visualizzare oggetti"	Consente di accedere all'universo e di visualizzarlo.
"Modificare oggetti"	Questo diritto consente di eseguire le seguenti operazioni: <ul style="list-style-type: none"> <li>• Modificare l'universo nella console CMC o in Universe Design Tool.</li> <li>• Bloccare o sbloccare l'universo.</li> </ul> Per sbloccare un universo, è anche necessario il diritto "Sblocca universo".
"Eliminare oggetti"	Consente di eliminare l'universo.
"Traduci oggetti"	Consente di salvare i nomi degli oggetti universo tradotti utilizzando Translation Management Tool.  <b>Nota:</b> è inoltre possibile salvare le traduzioni se all'utente è stato concesso esplicitamente il diritto "Modifica oggetti" ma non è stato negato esplicitamente il diritto "Traduci oggetti".
"Nuovo elenco di valori"	Questo diritto consente di: <ul style="list-style-type: none"> <li>• Associare nuovi elenchi di valori agli oggetti.</li> <li>• Modificare gli elenchi di valori esistenti.</li> </ul> <b>Nota:</b> Questo diritto non impedisce la creazione di elenchi sovrapposti di valori.
"Stampa universo"	Consente di stampare l'universo.
"Mostra valori di tabella o oggetto"	Consente di visualizzare i valori associati alle tabelle o agli oggetti nell'universo.
"Modifica restrizioni di accesso"	Consente di modificare le restrizioni di accesso (overload) per l'universo.

Diritto	Descrizione
"Sblocca universo"	<p>Consente di:</p> <ul style="list-style-type: none"> <li>• Sbloccare l'universo se è bloccato da un altro utente.</li> <li>• Esportare l'universo dal server CMS.</li> </ul> <p>Per sbloccare un universo, è anche necessario il diritto "Modificare oggetti".</p>
"Accesso ai dati"	<p>Consente di recuperare dati dall'universo e aggiornare i documenti in base all'universo. A tale scopo, è anche necessario questo diritto per l'applicazione Universe Design Tool, il documento e la connessione all'universo.</p>
"Crea e modifica query in base all'universo"	<p>Consente di creare documenti e modificare query basate sull'universo.</p>

### 29.3.10 Diritti sugli universi (.unx)

I diritti in questa sezione sono applicabili agli universi creati con Information Design Tool o agli universi .unx. I diritti elencati in questa sezione sono diritti specifici del tipo e applicabili solo agli universi oppure diritti generali con un significato specifico nel contesto degli universi.

**Nota:**

i diritti sugli universi si applicano solo agli universi pubblicati in un repository. Questi diritti non si applicano quando l'universo viene salvato in una cartella locale.

Diritto	Descrizione
"Visualizzare oggetti"	<p>Consente di accedere all'universo e di visualizzarlo.</p>
"Modificare oggetti"	<p>Consente di ripubblicare l'universo.</p>
"Eliminare oggetti"	<p>Consente di eliminare l'universo.</p>
"Recuperare universi"	<p>Consente di recuperare un universo pubblicato e di modificare le risorse sottostanti (livello aziendale e base dati) in Information Design Tool.</p> <p><b>Nota:</b> il diritto Recuperare universi è necessario anche per l'applicazione "Information Design Tool".</p>

Diritto	Descrizione
"Modificare profili di protezione"	Consente di inserire, modificare ed eliminare i profili di protezione per l'universo nell'editor di protezione di Information Design Tool.  <b>Nota:</b> questo diritto non è necessario per visualizzare i profili di protezione o modificare le opzioni di aggregazione dei profili di protezione.
"Assegnare profili di protezione"	Consente di assegnare e annullare l'assegnazione dei profili di protezione a utenti e gruppi nell'editor di protezione di Information Design Tool.
"Accesso ai dati"	Consente di recuperare dati dall'universo e aggiornare i documenti in base all'universo.  In Information Design Tool questo diritto consente di visualizzare in anteprima il set di risultati nel pannello delle query.
"Creare e modificare le query basate su questo universo"	Consente di creare e modificare query basate sull'universo.  In Information Design Tool questo diritto consente di aprire il pannello delle query e di eseguire una query sull'universo.
"Salva per tutti gli utenti"	Consente di salvare l'universo per tutti gli utenti.  <b>Nota:</b> il diritto Salva per tutti gli utenti è anche necessario per l'applicazione "Information Design Tool".

### 29.3.11 Livelli di accesso agli oggetti universo

Quando i progettisti creano un universo utilizzando Universe Design Tool o un livello aziendale utilizzando Information Design Tool, assegnano un livello di accesso agli oggetti per ogni oggetto dell'universo. I livelli di accesso agli oggetti disponibili sono:

- Pubblico (predefinito)
- Controllato
- Protetto
- Riservato
- Privato

Dopo aver pubblicato l'universo nel repository, è possibile concedere l'accesso agli oggetti che lo compongono in base ai livelli di accesso agli oggetti assegnati nell'applicazione. È ad esempio possibile concedere l'accesso Pubblico al gruppo Everyone. In questo modo gli utenti di tale gruppo potranno visualizzare gli oggetti dell'universo designati come pubblici.

Ogni livello di accesso agli oggetti concede un grado maggiore di accesso agli oggetti rispetto al precedente. Il livello minimo è Pubblico. I principali cui viene concesso l'accesso di tipo Pubblico possono visualizzare solo gli oggetti designati come pubblici. I principali cui viene concesso l'accesso di tipo Controllato possono visualizzare gli oggetti designati come pubblici e controllati. Privato è l'impostazione di massimo livello e consente ai principali l'accesso a tutti i livelli di accesso agli oggetti, ovvero a tutti gli oggetti presenti nell'universo.

**Nota:**

- le impostazioni di protezione dei livelli di accesso agli oggetti hanno la precedenza su eventuali impostazioni di protezione ereditate dall'universo.
- per gli universi .unx le impostazioni di protezione dei livelli di accesso agli oggetti vengono prese in considerazione con la protezione degli oggetti definita dal profilo di protezione. Per ulteriori informazioni sui profili di protezione, consultare il *Manuale dell'utente di Information Design Tool*.

**Argomenti correlati**

- [Assegnazione dei livelli di accesso agli oggetti universo](#)

### 29.3.11.1 Assegnazione dei livelli di accesso agli oggetti universo

Per impostare la protezione dei livelli di accesso agli oggetti universo, è necessario disporre del diritto **Modifica i diritti che gli utenti hanno sugli oggetti** per l'universo.

1. Nell'area "Universi" del CMS selezionare l'universo.
2. Fare clic su **Azione > Protezione universo**.
3. Nella finestra di dialogo "Protezione universo" selezionare il livello di accesso agli oggetti per l'utente o il gruppo nell'elenco **Livello di protezione dell'oggetto**.

### 29.3.12 Diritti di connessione

I diritti in questa sezione sono diritti specifici dei tipi e sono applicabili alle connessioni agli universi oppure sono diritti generali con un significato specifico nel contesto delle connessioni agli universi. Tali diritti si applicano alle connessioni pubblicate nel repository.

### Diritti di connessioni relazionali

Diritto	Descrizione
"Visualizzare oggetti"	Consente di visualizzare la connessione.
"Modificare oggetti"	Consente di modificare i parametri di connessione.
"Scarica connessione in locale"	<p>Consente di utilizzare in modalità offline gli universi creati per la connessione in Web Intelligence Rich Client.</p> <p>Consente di utilizzare il driver del middleware locale nello strumento Information Design Tool. A tale scopo, selezionare l'opzione relativa al middleware locale nelle preferenze di Information Design Tool, per evitare che le query del database utilizzino il middleware del server.</p> <p>Questo diritto è necessario anche per modificare una connessione protetta nello strumento Information Design Tool.</p>
"Eliminare oggetti"	Consente di eliminare la connessione.

Diritto	Descrizione
"Copia oggetti in un'altra cartella"	Consente di copiare la connessione da una cartella in un'altra.
"Accesso ai dati"	Consente di recuperare contenuto dal database specificato nella connessione.  In Information Design Tool questo diritto consente di esplorare i dati delle tabelle dagli editor delle connessioni e delle basi dati. Consente inoltre di visualizzare l'anteprima del set di risultati nel pannello delle query.
"Usa connessione per stored procedure"	Consente di utilizzare le stored procedure nel database specificato per la connessione all'universo.  <b>Nota:</b> Questo diritto è applicabile solo agli universi .unv.

#### Diritti di connessioni OLAP

Diritto	Descrizione
"Visualizzare oggetti"	Consente di visualizzare la connessione.
"Modificare oggetti"	Consente di modificare i parametri di connessione nell'editor delle connessioni di Information Design Tool.
"Eliminare oggetti"	Consente di eliminare la connessione.
"Copia oggetti in un'altra cartella"	Consente di copiare la connessione da una cartella in un'altra.

### 29.3.13 Applicazioni

#### 29.3.13.1 CMC

I diritti in questa sezione sono applicabili unicamente alla console CMC.



Diritto	Descrizione
"Accedere a CMC e visualizzare questo oggetto in CMC"	Consente di accedere alla console CMC.
"Consenti l'accesso a gestione delle istanze"	Consente di accedere a Gestione delle istanze.
"Consenti l'accesso a query di relazione"	Consente di eseguire query di relazione nella console CMC.
"Consenti l'accesso a query protezione"	Consente di eseguire query di protezione nella console CMC.

### 29.3.13.2 BI Launch Pad

I diritti elencati in questa sezione sono applicabili unicamente a BI Launch Pad.

Diritto	Descrizione
"Organizza"	Consente di eseguire le seguenti operazioni: <ul style="list-style-type: none"> <li>• Spostare e copiare oggetti.</li> <li>• Aggiungere oggetti alla cartella Preferiti.</li> <li>• Creare collegamenti agli oggetti.</li> </ul>
"Invia a posta in arrivo Business Objects"	Consente di inviare oggetti ai destinatari della Posta in arrivo BI.
"Invia a destinazione di posta elettronica"	Consente di inviare oggetti ai destinatari della Posta in arrivo BI.
"Invia a una posizione file"	Consente di salvare oggetti in una posizione file.
"Invia a una posizione FTP"	Consente di salvare oggetti in una posizione FTP.

#### 29.3.13.2.1 Diritti per le applicazioni di collaborazione

I diritti riportati in questa sezione si applicano a SAP Jam o SAP StreamWork, quando l'applicazione è configurata nella piattaforma BI.

Diritto	Descrizione
Commento su documenti	Consente di commentare documenti e istanze
Commento su documenti di proprietà dell'utente	Consente di commentare documenti e istanze di proprietà dell'utente
Visualizza commenti su documenti di proprietà dell'utente	Consente di visualizzare i commenti su documenti e istanze di proprietà dell'utente
Visualizza commenti su documenti	Consente di visualizzare i commenti su documenti e istanze

### 29.3.13.3 Spazi di lavoro BI

I diritti elencati in questa sezione sono applicabili unicamente agli spazi di lavoro BI.

Diritto	Descrizione
"Crea e modifica spazi di lavoro BI"	Consente all'utente di creare nuovi spazi di lavoro BI e di modificare quelli esistenti.
"Crea e modifica moduli"	Consente all'utente di creare nuovi moduli e di modificare quelli esistenti.
"Modificare spazi di lavoro BI"	Consente all'utente di modificare gli spazi di lavoro BI esistenti. Gli utenti non possono creare nuovi spazi di lavoro BI.

### 29.3.13.4 Desktop Intelligence

I diritti contenuti in questa sezione si applicano a SAP BusinessObjects Desktop Intelligence.

<b>Diritto</b>	<b>Descrizione</b>
"Crea e modifica connessioni"	Consente agli utenti di creare una nuova connessione o di modificarne una esistente.
"Gestione dei fornitori di dati"	Consente agli utenti di modificare una query o l'universo su cui è basata.
"Modifica Free-hand SQL"	Consente agli utenti di modificare una query che utilizza script Free-hand SQL come fornitore di dati. Per eseguire questa azione è necessario disporre anche del diritto "Usa Free-hand SQL".
"Usa Free-hand SQL"	Consente agli utenti di creare una query utilizzando script Free-hand SQL come fornitore di dati.
"Aggiorna l'elenco dei documenti e le categorie"	Quando è abilitato, consente agli utenti di aggiornare l'elenco di documenti.
"Invia documenti al repository"	Consente agli utenti di pubblicare un documento nel CMS, all'interno delle cartelle pubbliche o delle cartelle personali.
"Invia documenti alla posta"	Consente agli utenti di inviare documenti come posta elettronica da Desktop Intelligence.
"Recupera i documenti"	Consente agli utenti di importare il documento dal CMS.
"Esegui codice VBA"	Consente agli utenti di eseguire il codice VBA.
"Installa componenti aggiuntivi"	Consente agli utenti di installare o disinstallare componenti aggiuntivi VBA.
"Gestisci tutte le categorie aziendali"	Consente agli utenti di creare, modificare o eliminare i documenti della categoria.
"Gestisci le categorie aziendali personali"	Consente agli utenti di creare, modificare o eliminare qualsiasi categoria aziendale dall'applicazione Desktop Intelligence.
"Modifica ambito di analisi"	Consente agli utenti di modificare l'ambito di analisi

<b>Diritto</b>	<b>Descrizione</b>
"Lavora in modalità Drill"	Consente agli utenti di eseguire il drill down verso un livello più dettagliato di analisi nei report.
"Lavora in modalità Slice and Dice"	Consente agli utenti di utilizzare il pannello Slice and Dice.
"Modifica codice VBA"	Consente agli utenti di modificare le macro VBA utilizzate nei report.
"Convertitore euro"	Consente agli utenti di convertire le cifre di valuta presenti nei report in euro e viceversa.
"Copia negli Appunti"	Consente agli utenti di tagliare o copiare il contenuto dei documenti.
"Drill through"	Consente agli utenti di eseguire un ulteriore drill in un report mediante il recupero di nuovi dati.
"Modifica tasso del convertitore euro"	Consente agli utenti di modificare i tassi di scambio in euro utilizzati dalla funzione del convertitore euro.
"Interazioni tra report Desktop Intelligence"	Consente agli utenti di selezionare singoli elementi di un report da tagliare, copiare, cancellare, duplicare o eliminare.
"Interazioni tra documenti Desktop Intelligence"	Consente agli utenti di rinominare, duplicare, inserire o eliminare un report in un documento.
"Stampa documenti"	Consente agli utenti di stampare documenti.
"Aggiorna contenuto Desktop Intelligence"	Consente agli utenti di aggiornare il contenuto di Desktop Intelligence.
"Usa modelli"	Consente agli utenti di creare report con modelli o di applicare modelli al contenuto esistente.
"Crea modelli"	Consente agli utenti di salvare documenti come modelli.
"Salva i documenti per tutti gli utenti"	Consente agli utenti di salvare documenti senza vincoli di protezione per l'uso offline in modo da consentire a tutti di visualizzare il documento salvato in locale.

<b>Diritto</b>	<b>Descrizione</b>
"Crea documenti Desktop Intelligence"	Consente agli utenti di creare un nuovo documento.
"Salva documenti Desktop Intelligence"	Consente agli utenti di salvare documenti in locale.
"Invia documenti alla Posta in arrivo"	Consente agli utenti di inviare documenti alle caselle di posta in arrivo di BI Launch Pad.
"Usa oggetti utente"	Consente agli utenti di creare, modificare o eliminare oggetti utente.
"Aggiorna elenco di valori"	Se concesso, questo diritto consente agli utenti di aggiornare gli elenchi di valori.
"Usa elenco di valori"	Consente agli utenti di utilizzare e aggiornare gli elenchi di valori nel documento.
"Modifica elenco di valori"	Consente agli utenti di modificare gli elenchi di valori definiti negli universi.
"Usa query"	Consente agli utenti di creare nuove query basate sugli universi.
"Modifica query"	Consente agli utenti di modificare le query basate sugli universi.
"Visualizza SQL"	Consente agli utenti di visualizzare le istruzioni SQL generate per la query.
"Modifica SQL della query"	Consente agli utenti di modificare le istruzioni SQL delle query.
"Rigenera sistematicamente SQL"	Consente la rigenerazione delle query a ogni aggiornamento.
"Usa stored procedure"	Consente agli utenti di creare un report utilizzando una stored procedure come fornitore di dati.
"Modifica stored procedure"	Consente agli utenti di modificare i parametri delle stored procedure.

Diritto	Descrizione
"Usa file di dati personali"	Consente agli utenti di creare un report utilizzando file Excel, dBase o di testo ASCII come fornitore di dati.
"Modifica file di dati personali"	Consente agli utenti di modificare il fornitore di dati personali.
"Modificare in modo sicuro i diritti degli utenti sugli oggetti"	Consente agli utenti di concedere, negare o reimpostare su non specificato solo i diritti già concessi.
"Modificare i diritti degli utenti per questo oggetto"	Consente agli utenti di modificare qualsiasi diritto, per qualsiasi utente su un determinato oggetto.
"Modificare l'oggetto"	Consente agli utenti di modificare le proprietà dell'applicazione nella CMC.
"Accedere a Desktop Intelligence e visualizzare questo oggetto in CMC"	Consente agli utenti di accedere a Desktop Intelligence e visualizzare l'oggetto nella CMC.

### 29.3.13.5 Web Intelligence

I diritti in questa sezione sono applicabili unicamente a SAP BusinessObjects Web Intelligence (inclusa l'interfaccia Rich Client) e possono influire sui visualizzatori e sui pannelli di query di tali applicazioni.

Diritto	Descrizione
"Dati: abilita rilevamento dati"	Consente il rilevamento dei dati modificati.
"Dati: abilita formattazione di dati modificati"	Consente di scegliere il formato dei dati modificati.
"Interfaccia Rich Client - abilita Web Intelligence Rich Client"	Consente l'utilizzo dell'interfaccia Rich Client.
"Interfaccia Rich Client - abilita fornitori di dati locali"	Consente l'utilizzo di fornitori di dati personali nell'interfaccia Rich Client.
"Interfaccia Rich Client - esporta documenti"	Consente l'esportazione di documenti nel CMS nell'interfaccia Rich Client.

<b>Diritto</b>	<b>Descrizione</b>
"Interfaccia Rich Client - importa documenti"	Consente l'importazione di documenti dal CMS nell'interfaccia Rich Client.
"Interfaccia Rich Client - installa da BI Launch Pad"	Consente il download dell'interfaccia Rich Client da BI Launch Pad.
"Interfaccia Rich Client - stampa documenti"	Consente la stampa di documenti dall'interfaccia Rich Client.
"Interfaccia Rich Client - rimuovi protezione documento"	Consente la rimozione della protezione dei documenti dall'interfaccia Rich Client.
"Interfaccia Rich Client - salva documento per tutti gli utenti"	Consente il salvataggio dei documenti per tutti gli utenti dall'interfaccia Rich Client.
"Interfaccia Rich Client - salva documenti in locale"	Consente il salvataggio dei documenti sul disco locale nell'interfaccia Rich Client.
"Interfaccia Rich Client - invia tramite posta elettronica"	Consente l'invio dei documenti tramite posta elettronica nell'interfaccia Rich Client.
"Interfaccia Rich Client - abilita fornitori di dati locali"	Consente l'utilizzo di fornitori di dati personali nell'interfaccia Rich Client.
"Documenti: disabilita l'aggiornamento automatico all'apertura"	Interrompe l'aggiornamento automatico dei documenti all'apertura.
"Documenti: abilita il salvataggio automatico"	Consente il salvataggio automatico dei documenti (se il salvataggio automatico viene attivato nella CMC dall'amministratore).
"Documenti: abilita creazione"	Consente la creazione di nuovi documenti.
"Documenti: abilita pubblicazione e gestione contenuto"	Consente la pubblicazione dei documenti nel CMS.
"Interattivo: creazione di report - Crea e modifica segnalatori"	Consente di creare e modificare i segnalatori nel visualizzatore interattivo.

<b>Diritto</b>	<b>Descrizione</b>
"Interfacce: abilita Rich Internet Application"	Consente l'utilizzo dell'interfaccia di visualizzazione e modifica di Rich Internet Application (pannello dei report Java nelle versioni precedenti).
"Interfacce: abilita interfaccia di visualizzazione Web"	Consente l'utilizzo dell'interfaccia di visualizzazione Web (visualizzatore DHTML nelle release precedenti).
"Interfacce: abilita pannello query Web"	Consente l'utilizzo del pannello delle query Web (Query - HTML nelle release precedenti).
"Generale - Modifica 'Preferenze personali'"	Consente la modifica delle preferenze in BI Launch Pad.
"Generale - Abilitazione del menu a comparsa"	Consente l'utilizzo di menu a comparsa.
"Riquadro a sinistra - Abilitazione del riepilogo dei documenti"	Consente la visualizzazione del riepilogo dei documenti nel riquadro a sinistra.
"Riquadro a sinistra - Abilitazione della struttura e dei filtri del documento"	Consente la visualizzazione della struttura e dei filtri dei documenti nel riquadro a sinistra.
"Script query - abilita modifica (SQL, MDX...)"	Consente la modifica degli script di query (SQL e MDX).
"Script query - abilita visualizzazione (SQL, MDX...)"	Consente la visualizzazione degli script di query (SQL e MDX).
"Creazione report: crea e modifica interruzioni"	Consente la creazione e la modifica delle interruzioni.
"Creazione report: crea e modifica regole di formattazione condizionale"	Consente la creazione e la modifica delle regole di formattazione condizionale.
"Creazione report: crea e modifica calcoli predefiniti"	Consente la creazione e la modifica dei calcoli predefiniti.
"Creazione di report - Creazione e modifica di controlli di input"	Consente la creazione e la modifica dei controlli di input.
"Creazione report: crea e modifica filtri report e utilizza controlli di input"	Consente la creazione e la modifica dei filtri di report e dei controlli di input. I controlli di input nel riquadro a sinistra non vengono visualizzati se disabilitati.
"Creazione report: crea e modifica ordinamenti"	Consente la creazione e la modifica degli ordinamenti.



Diritto	Descrizione
"Creazione report: crea formule e variabili"	Consente la creazione di formule e variabili.
"Creazione report: abilita la formattazione"	Consente la modifica della formattazione dei report. Se questo diritto viene negato, la modalità Progettazione e dati non sarà disponibile per l'utente, ovvero sarà disattivata.
"Creazione report: abilita dimensioni unite"	Consente la sincronizzazione dei dati mediante l'utilizzo di dimensioni unite nei report e nel gestore dei dati.
"Creazione report: inserisci e rimuovi report, tabelle, grafici e celle"	Consente l'inserimento e la rimozione di report, tabelle, grafici e celle. Regola inoltre il workflow dei duplicati (Copia/Incolla).

### 29.3.13.6 Strategy Builder

Strategy Builder è uno strumento correlato a Performance Management. I diritti in questa sezione sono applicabili unicamente a Strategy Builder e possono influire sulla gestione degli obiettivi in Performance Manager o funzionalità specifiche in Strategy Builder.

Diritto	Descrizione
"Crea, modifica o elimina obiettivi"	Consente di aggiungere, modificare o rimuovere obiettivi in Performance Manager.
"Visualizza obiettivi"	Consente di visualizzare gli obiettivi in analitiche che contengono obiettivi.
"Accesso alla gestione obiettivi"	Consente di visualizzare gli obiettivi nella pagina "Gestione obiettivi" in Performance Manager.
"Pubblica obiettivi"	Consente di pubblicare obiettivi in Performance Manager.

Diritto	Descrizione
"Accesso a Strategy Builder"	Consente di accedere allo strumento Strategy Builder in Performance Manager.
"Crea, modifica o elimina ruoli"	Consente di amministrare i ruoli utilizzati per pubblicare obiettivi o metriche in audience specifiche in Strategy Builder.
"Crea, modifica o elimina strategie"	Consente di creare strategie che collegano ruoli e pubblicano obiettivi e metriche in Strategy Builder.

### 29.3.13.7 Diritti di Universe Design Tool

I diritti in questa sezione sono validi per l'applicazione Universe Design Tool.

Diritto	Descrizione
"Verifica l'integrità dell'universo"	Consente di verificare l'integrità dell'universo.
"Aggiorna la finestra della struttura"	Consente di aggiornare la finestra della struttura.
"Usa il browser delle tabelle"	Consente di visualizzare i dati del database utilizzando il relativo browser.
"Applica vincoli di universo"	Consente di applicare vincoli di universo predefiniti agli utenti di un universo importato.
"Collega universo"	Consente di collegare due universi e di condividere i componenti.
"Creare, modificare o eliminare connessioni"	Consente di creare, modificare ed eliminare connessioni agli universi archiviate nel repository o come connessioni personali o condivise.

### 29.3.13.8 Diritti di Information Design Tool

I diritti in questa sezione sono validi per l'applicazione Information Design Tool.

Diritto	Descrizione
"Amministra profili di protezione"	<p>Consente di aprire l'editor di protezione.</p> <p><b>Nota:</b> Per utilizzare i profili di protezione, è necessario che siano stati concessi diritti per l'universo.</p>
"Condividi progetti"	Consente di condividere un progetto locale e di aprire la vista Sincronizza progetto per sincronizzare un progetto condiviso con quello locale.
"Creare, modificare o eliminare connessioni"	<p>Consente di eseguire le seguenti operazioni:</p> <ul style="list-style-type: none"> <li>• creare ed eliminare le connessioni protette dalla vista Risorse pubblicate</li> <li>• modificare le connessioni nell'editor delle connessioni</li> <li>• pubblicare le connessioni in un repository</li> </ul>
"Pubblica universo"	Consente di pubblicare universi in un repository.
"Recupera universo"	Consente di recuperare gli universi pubblicati in un progetto locale da modificare.
"Salva per tutti gli utenti"	Consente di utilizzare l'opzione Salva per tutti gli utenti durante il recupero degli universi.
"Statistiche di calcolo"	Consente di selezionare le tabelle e le colonne sulle quali calcolare e pubblicare le statistiche.

### 29.3.13.9 Widget per la piattaforma SAP BusinessObjects Business Intelligence

I diritti in questa sezione sono applicabili unicamente ai widget dell'applicazione della piattaforma SAP BusinessObjects Business Intelligence.

Diritto	Descrizione
"Utilizza Explorer"	Consente agli utenti di cercare il contenuto in tutti i server della piattaforma BI connessi utilizzando Esplora elenco documenti.
"Utilizza Posta in arrivo degli avvisi"	(Obsoleto) Consente di utilizzare la Posta in arrivo degli avvisi.
"Utilizza ricerca"	Consente agli utenti di eseguire ricerche contemporaneamente in tutti i repository della piattaforma BI connessi utilizzando Ricerca di contenuti.

### 29.3.13.10 Avvisi

I diritti in questa sezione sono applicabili unicamente all'applicazione Avvisi.

Diritto	Descrizione
""Attiva avvisi""	<p>Consente di attivare gli eventi di avviso.</p> <p>Per attivare un avviso per un documento, è necessario disporre dei seguenti diritti:</p> <ul style="list-style-type: none"> <li>• Diritti di visualizzazione e di pianificazione sul documento</li> <li>• Diritti visualizzazione e attivazione sull'evento corrispondente</li> </ul>
""Sottoscrivi oggetti""	<p>Consente di sottoscrivere un evento di avviso.</p> <p>Per sottoscrivere un evento, è necessario disporre dei seguenti diritti:</p> <ul style="list-style-type: none"> <li>• Diritto di visualizzazione sull'evento corrispondente</li> <li>• Diritto di sottoscrizione sull'account utente</li> </ul> <p>Per sottoscrivere un avviso per un documento, è necessario disporre dei seguenti diritti:</p> <ul style="list-style-type: none"> <li>• Diritto di visualizzazione sul documento</li> <li>• Diritto di visualizzazione istanza sul documento</li> <li>• Diritto di visualizzazione sull'evento corrispondente</li> <li>• Diritto di sottoscrizione sull'account utente</li> </ul>

### 29.3.13.11 Explorer

I diritti elencati in questa sezione sono applicabili unicamente a Explorer.

Diritto	Descrizione
"Accedere a Explorer e visualizzare questo oggetto nella CMC"	Consente di accedere a Explorer. Questo diritto è necessario per eseguire altre attività con Explorer.
"Esplora spazi informazioni"	<p>Consente di esplorare uno spazio informazioni.</p> <p>Per eseguire questa attività, è necessario disporre anche del diritto "Accedere a Explorer e visualizzare questo oggetto nella CMC".</p>
"Esplora spazi informazioni: Esporta in segnalibro/posta elettronica"	<p>Consente di utilizzare segnalibri e segnalibri di posta elettronica.</p> <p>Per eseguire questa attività, è necessario disporre anche dei seguenti diritti:</p> <ul style="list-style-type: none"> <li>• "Accedere a Explorer e visualizzare questo oggetto nella CMC"</li> <li>• "Esplora spazi informazioni"</li> </ul>
"Esplora spazi informazioni: Esporta in CSV"	<p>Consente di esportare i risultati di un'esplorazione in un file CSV o Excel.</p> <p>Per eseguire questa attività, è necessario disporre anche dei seguenti diritti:</p> <ul style="list-style-type: none"> <li>• "Accedere a Explorer e visualizzare questo oggetto nella CMC"</li> <li>• "Esplora spazi informazioni"</li> </ul>
"Esplora spazi informazioni: Esporta in immagine"	<p>Consente di esportare i risultati di un'esplorazione come immagine.</p> <p>Per eseguire questa attività, è necessario disporre anche dei seguenti diritti:</p> <ul style="list-style-type: none"> <li>• "Accedere a Explorer e visualizzare questo oggetto nella CMC"</li> <li>• "Esplora spazi informazioni"</li> </ul>

Diritto	Descrizione
"Esplora spazi informazioni: Esporta in Web Intelligence"	<p>Consente di esportare i risultati di un'esplorazione come query.</p> <p>Per eseguire questa attività, è necessario disporre anche dei seguenti diritti:</p> <ul style="list-style-type: none"> <li>• "Accedere a Explorer e visualizzare questo oggetto nella CMC"</li> <li>• "Esplora spazi informazioni"</li> </ul>
"Gestione spazi informazioni"	<p>Consente di accedere al menu Gestione spazi e ad eseguire le attività associate.</p> <p>Per eseguire questa attività, è necessario disporre anche del diritto "Accedere a Explorer e visualizzare questo oggetto nella CMC".</p>
"Gestione spazi informazioni: Crea nuovo spazio"	<p>Consente di creare un nuovo spazio informazioni</p> <p>Per eseguire questa attività, è necessario disporre anche dei seguenti diritti:</p> <ul style="list-style-type: none"> <li>• "Accedere a Explorer e visualizzare questo oggetto nella CMC"</li> <li>• "Gestione spazi informazioni"</li> </ul>

Diritto	Descrizione
"Gestione spazi informazioni: Modifica spazio"	<p>Consente di modificare o eliminare uno spazio informazioni.</p> <p>Per eseguire questa attività, è necessario disporre anche dei seguenti diritti:</p> <ul style="list-style-type: none"> <li>• "Accedere a Explorer e visualizzare questo oggetto nella CMC"</li> <li>• "Gestione spazi informazioni"</li> </ul>
"Gestione spazi informazioni: Pianifica indicizzazione"	<p>Consente di pianificare l'indicizzazione per i dati degli spazi informazioni.</p> <p>Per eseguire questa attività, è necessario disporre anche dei seguenti diritti:</p> <ul style="list-style-type: none"> <li>• "Accedere a Explorer e visualizzare questo oggetto nella CMC"</li> <li>• "Gestione spazi informazioni"</li> </ul>
"Gestione spazi informazioni: Avvia indicizzazione"	<p>Consente di eseguire l'indicizzazione per i dati degli spazi informazioni.</p> <p>Per eseguire questa attività, è necessario disporre anche dei seguenti diritti:</p> <ul style="list-style-type: none"> <li>• "Accedere a Explorer e visualizzare questo oggetto nella CMC"</li> <li>• "Gestione spazi informazioni"</li> </ul>

### 29.3.13.12 SAP BusinessObjects Mobile

I diritti in questa sezione sono validi unicamente per l'applicazione SAP BusinessObjects Mobile.

Diritto	Descrizione
"Accedere all'applicazione SAP BusinessObjects Mobile"	Concede l'accesso alla piattaforma BI tramite l'applicazione Mobile e visualizzare i documenti
"Sottoscrivere gli avvisi del documento"	<p>Concede l'accesso per la sottoscrizione di avvisi su documenti/ricorrenza.</p> <p><b>Nota:</b></p> <ul style="list-style-type: none"> <li>• se a un utente è stato precedentemente concesso il diritto "Sottoscrizione ad avvisi sui documenti" e poi gli è stato negato, continuerà comunque a ricevere gli avvisi sottoscritti. Se non si desidera ricevere gli avvisi, è necessario eseguire esplicitamente l'annullamento della sottoscrizione.</li> <li>• per effettuare la sottoscrizione agli avvisi sui documenti (o le istanze ricorrenti) per le pianificazioni, l'utente deve disporre dell'accesso protetto "Controllo completo" alla cartella "Eventi di sistema" in "Eventi" nella Central Management Console (CMC).</li> </ul>
"Salvare i documenti nella memoria locale di un dispositivo"	<p>Concede l'accesso per il salvataggio di documenti sul dispositivo Mobile.</p> <p><b>Nota:</b></p> <p>se sono stati salvati documenti sul dispositivo quando si disponeva del diritto "Salvataggio dei documenti in locale sul dispositivo", i documenti continueranno a esistere sul dispositivo anche se si viene privati di tale diritto. Tuttavia, non saranno più sincronizzati durante il processo di sincronizzazione.</p>
"Inviare i documenti dal dispositivo come messaggi di posta elettronica"	Concede l'accesso per l'invio di report tramite posta elettronica.

Per ulteriori informazioni, consultare il *Manuale d'installazione e distribuzione di SAP BusinessObjects Mobile*.



## Appendice sulle proprietà dei server

### 30.1 Informazioni sull'appendice sulle proprietà dei server

In questa appendice sulle proprietà dei server sono elencate e descritte le proprietà che è possibile impostare per ogni server della piattaforma BI.

#### 30.1.1 Proprietà comuni dei server

Le proprietà dei server descritte in questa sezione si applicano a tutti i tipi di server.

Tabella 30 - 1: Proprietà della porta richiesta

Proprietà	Descrizione	Valore predefinito
<b>Nome server</b>	Il nome del server.	Il valore predefinito è il nome del nodo in cui si trova il server, cui si aggiunge il nome del server.
<b>ID, CUID</b>	L'ID abbreviato e l'ID univoco del cluster del server. Valori in sola lettura.	Questi valori vengono generati automaticamente.
<b>Nodo</b>	Nome del nodo in cui si trova il server.	Questo valore viene specificato durante l'installazione.
<b>Descrizione</b>	Descrizione del server	Il valore predefinito è il nome del server.
<b>Parametri della riga di comando</b>	Parametri della riga di comando relativi al server.	Il valore predefinito dipende dal tipo di server.

Proprietà	Descrizione	Valore predefinito
<b>Porta richiesta</b>	<p>Specifica la porta dalla quale il server riceve richieste. In un ambiente con firewall è possibile configurare il server per ascoltare solo le richieste sulle porte aperte nel firewall. Se si specifica una porta per il server, verificare che non sia già assegnata a un altro processo.</p> <p><b>Nota:</b> se si seleziona <b>Assegna automaticamente</b>, il server viene associato a una porta allocata in modo dinamico. Questo significa che al server viene assegnato un numero di porta casuale ogni volta che viene riavviato.</p>	Per impostazione predefinita, l'opzione <b>Assegna automaticamente</b> è impostata su TRUE e l'opzione <b>Porta richiesta</b> è vuota.
<b>Assegna automaticamente</b>	<p>Specifica se il server viene associato a una porta assegnata dinamicamente ogni volta che viene riavviato. Per associare il server a una porta specifica, impostare <b>Assegna automaticamente</b> su FALSE e specificare una <b>Porta richiesta</b> valida.</p>	Il valore predefinito è TRUE.

Tabella 30 - 2: Proprietà di avvio automatico

Proprietà	Descrizione	Valore predefinito
<b>Avvia automaticamente questo server all'avvio di Server Intelligence Agent</b>	<p>Specifica se il server viene avviato automaticamente all'avvio o al riavvio di Server Intelligence Agent (SIA).</p> <p>Se il valore viene impostato su FALSE e l'agente SIA viene avviato o riavviato, il server non viene avviato.</p>	Il valore predefinito è TRUE.

Tabella 30 - 3: Proprietà degli identificatori host

Proprietà	Descrizione	Valore predefinito
<b>Assegna automaticamente</b>	<p>Specifica se il server viene associato a un'interfaccia di rete assegnata automaticamente. Se impostata su FALSE, il server viene associato a un'interfaccia di rete specifica. Se impostata su TRUE, il server accetta le richieste inviate al primo indirizzo IP disponibile. Nei computer multi-home è possibile specificare una determinata interfaccia di rete per l'associazione impostando il valore su FALSE e specificando un nome host o un indirizzo IP valido.</p>	Il valore predefinito è TRUE.

Proprietà	Descrizione	Valore predefinito
<b>Nome host</b>	Nome host dell'interfaccia di rete cui viene associato il server. Se si specifica un nome host, il server accetta le richieste inviate a tutti gli indirizzi IP associati a tale nome.	Per impostazione predefinita, l'opzione <b>Assegna automaticamente</b> è impostata su TRUE e l'opzione <b>Nome host</b> è vuota.
<b>Indirizzo IP</b>	L'indirizzo IP dell'interfaccia di rete al quale è associato il server. Sono supportati i protocolli IPv4 e IPv6. Se si specifica un indirizzo IP, il server accetta le richieste inviate solo a tale indirizzo.	Per impostazione predefinita, l'opzione <b>Assegna automaticamente</b> è impostata su TRUE e l'opzione <b>Indirizzo IP</b> è vuota.

Tabella 30 - 4: Proprietà dei modelli di configurazione

Proprietà	Descrizione	Valore predefinito
<b>Usa modello configurazione</b>	Specifica se utilizzare un modello di configurazione.	Il valore predefinito è FALSE.
<b>Ripristina valori predefiniti di sistema</b>	Specifica se ripristinare le impostazioni predefinite originali per questo server.	Il valore predefinito è FALSE.
<b>Imposta modello configurazione</b>	Specifica se utilizzare le impostazioni del servizio corrente come modello di configurazione per tutti i servizi dello stesso tipo. Se questa opzione viene impostata su TRUE, tutti i servizi dello stesso tipo per cui è stata selezionata l'opzione <b>Usa modello configurazione</b> vengono immediatamente riconfigurati per l'utilizzo delle impostazioni del servizio corrente.	Il valore predefinito è FALSE.

Tabella 30 - 5: Proprietà del Servizio log analisi

Proprietà	Descrizione	Valore predefinito
<b>Livello di registrazione</b>	<p>Specifica il livello di gravità minimo di messaggi che si desidera registrare e determina quante informazioni vengono registrate nel file di registro del server.</p> <p>I livelli della soglia di registrazione possibili sono:</p> <ul style="list-style-type: none"> <li>• <b>Non specificato</b></li> <li>• <b>Nessuno</b></li> <li>• <b>Bassa</b></li> <li>• <b>Media</b></li> <li>• <b>Alta</b></li> </ul>	Il valore predefinito è Non specificato.

#### Argomenti correlati

- [Utilizzo di modelli di configurazione](#)
- [Livelli del registro di analisi](#)

## 30.1.2 Proprietà dei servizi principali

La categoria Servizi principali include i server seguenti:

- Adaptive Job Server
- Adaptive Processing Server
- Central Management Server
- Dashboard Server
- Dashboard Analytics Server
- Event Server
- Input File Repository Server
- Output File Repository Server
- Web Application Container Server

## Proprietà di Adaptive Job Server

Tabella 30 - 6: Proprietà generali

Proprietà	Descrizione	Valore predefinito
<b>Directory temporanea</b>	<p>Specifica la directory in cui vengono creati i file temporanei quando necessario. Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni. Per ottenere prestazioni migliori, verificare che questa directory si trovi su un disco locale.</p> <p><b>Nota:</b> È necessario riavviare il server per rendere effettive le modifiche.</p>	%DefaultDataDir%

Adaptive Job Server può ospitare alcuni servizi differenti. Ogni servizio ha le proprietà seguenti:

Tabella 30 - 7: Proprietà servizio

Proprietà	Descrizione	Valore predefinito
<b>Numero max. processi simultanei</b>	<p>Specifica il numero di processi indipendenti simultanei (processi secondari) consentiti dal server. È possibile adattare il numero massimo di processi in base all'ambiente di creazione report.</p> <p>L'impostazione predefinita è accettabile per la maggior parte degli scenari di reporting. L'impostazione ideale per un ambiente di reporting dipende dalla configurazione hardware, dal software di database e dai requisiti di reporting.</p>	5
<b>Numero max. richieste secondarie</b>	Specifica il numero di processi che l'elemento secondario elaborerà prima di essere riavviato.	100

## Proprietà di Adaptive Processing Server

Tabella 30 - 8: Proprietà generali

Proprietà	Descrizione	Valore predefinito
<b>Timeout di avvio servizio (secondi)</b>	<p>Specifica, in secondi, per quanto tempo il server rimane in attesa dell'avvio dei servizi.</p> <p>Se un servizio non viene avviato nel periodo di tempo specificato, i motivi possibili sono due:</p> <ul style="list-style-type: none"> <li>Il servizio non è stato avviato, ad esempio, perché non è stata trovata una risorsa richiesta, quale un database, oppure il servizio ha riscontrato un conflitto di porta.</li> <li>Il servizio non è stato attivato nel periodo di tempo specificato, ad esempio, perché il sistema è troppo lento.</li> </ul> <p>Per individuare il motivo del problema, consultare il file di registro del server. Se il servizio non viene avviato nel periodo di tempo specificato, può essere opportuno aumentare il valore.</p>	1500

Tabella 30 - 9: Proprietà del servizio proxy controllo client

Proprietà	Descrizione	Valore predefinito
Nessuna proprietà di configurazione		

Tabella 30 - 10: Proprietà del servizio token di protezione

Proprietà	Descrizione	Valore predefinito
Nessuna proprietà di configurazione		

Tabella 30 - 11: Proprietà del servizio Insight to Action

Metrica	Descrizione	
<b>Numero massimo di connessioni attive per sessione utente</b>	Il numero massimo di connessioni con il server SAP disponibili per un utente in un determinato momento. Quando un utente apre un report o un cruscotto che supporta RRI, viene stabilita una connessione con il server SAP per determinare le destinazioni RRI disponibili.	20
<b>Numero massimo di connessioni inattive per sessione utente</b>	Il numero di connessioni inattive da mantenere aperte e riutilizzare per le richieste RRI successive. Aumentando questa impostazione si allocheranno ulteriori risorse di sistema.	20
<b>Tempo massimo di attesa per connessione (in secondi)</b>	Il periodo di tempo in cui il framework informazioni per azione deve attendere una risposta dal server SAP prima del timeout (in secondi).	30

Tabella 30 - 12: Proprietà del servizio di pubblicazione

Proprietà	Descrizione	Valore predefinito
<b>Dimensione pool di thread</b>	Specifica quanti thread di elaborazione dei batch ambito possono essere eseguiti contemporaneamente. Se il valore di questa proprietà è impostato su "0", la dimensione del pool di thread viene determinata utilizzando una formula basata sul numero di core di CPU nel computer corrente.	0

Tabella 30 - 13: Proprietà del servizio di traduzione

Proprietà	Descrizione	Valore predefinito
Nessuna proprietà di configurazione		

Tabella 30 - 14: Proprietà del servizio di monitoraggio

Proprietà	Descrizione	Valore predefinito
Nessuna proprietà di configurazione		

Tabella 30 - 15: Proprietà del servizio di ricerca piattaforma

Proprietà	Descrizione	Valore predefinito
Nessuna proprietà di configurazione		

Tabella 30 - 16: Proprietà del servizio di post-elaborazione pubblicazione

Proprietà	Descrizione	Valore predefinito
Nessuna proprietà di configurazione		

### Proprietà di Central Management Server

**Nota:**

quando si modifica una di queste proprietà del server, è necessario riavviare il server per rendere effettive le modifiche.

Tabella 30 - 17: Proprietà di Servizio Central Management

Proprietà	Descrizione	Valore predefinito
<b>Porta server dei nomi</b>	Specifica la porta di attesa del server CMS per le richieste iniziali del servizio dei nomi.	6400
<b>Connessioni richieste al database di sistema</b>	Specifica il numero di connessioni al database di sistema CMS che il CMS tenta di stabilire. Se il server non riesce a stabilire tutte le connessioni al database richieste, il CMS continua a funzionare ma con prestazioni ridotte, in quanto è possibile eseguire simultaneamente un numero inferiore di richieste concorrenti. Il CMS tenterà di stabilire altre connessioni, finché non ne verrà stabilito il numero necessario.  La metrica <b>Connessioni database di sistema stabilite</b> del CMS mostra il numero corrente di connessioni stabilite.	14
<b>Riconnessione automatica al database di sistema</b>	Specifica se il server CMS tenta automaticamente di ristabilire la connessione al database CMS nel caso di interruzione del servizio. Se il valore viene impostato su FALSE è possibile controllare l'integrità del database CMS prima di riprendere le operazioni. Per ristabilire la connessione al database, è necessario riavviare il server CMS.	TRUE



Tabella 30 - 18: Proprietà del servizio Single Sign On

Proprietà	Descrizione	Valore predefinito
<b>Scadenza Single Sign-On (secondi)</b>	Specifica il tempo, in secondi, di validità di una connessione SSO a un'origine dati prima della scadenza. Questa opzione è applicabile agli utenti di Windows AD che eseguono report configurati per la connessione SSO di Windows AD a un'origine dati.	86400

### Proprietà di Event Server

Tabella 30 - 19: Proprietà del servizio eventi

Proprietà	Descrizione	Valore predefinito
<b>Intervallo di polling eventi (minuti)</b>	Specifica la frequenza con cui il server esegue il polling di un file che attiva un evento, in secondi.	10 L'intervallo di valori consentiti è tra 1 e 1200 secondi.
<b>Intervallo di svuotamento (minuti)</b>	Specifica la frequenza con cui viene eseguita l'utilità di pulizia, in minuti.	20

### Proprietà dell'Input File Repository Server

Tabella 30 - 20: Proprietà del servizio archivio file di input

Proprietà	Descrizione	Valore predefinito
<b>Directory archivio file</b>	Specifica la directory in cui vengono archiviati gli oggetti repository dei file. <b>Nota:</b> Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni.	%DefaultInputFRS Dir/%
<b>Directory temporanea</b>	Specifica la directory in cui vengono creati i file temporanei quando necessario. <b>Nota:</b> Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni. Per garantire prestazioni migliori, è preferibile che la <b>Directory temporanea</b> si trovi nello stesso file system della <b>Directory archivio file</b> .	%DefaultInputFRS Dir/temp%

Proprietà	Descrizione	Valore predefinito
<b>Tempo massimo di inattività (in minuti)</b>	Specifica il periodo di tempo di attesa del server prima della chiusura delle connessioni inattive. L'impostazione di un valore troppo basso può causare la chiusura prematura della richiesta di un utente. L'impostazione di un valore troppo alto può causare un consumo eccessivo delle risorse del sistema, ad esempio il tempo di elaborazione e lo spazio su disco.	10
<b>Numero max. tentativi per l'accesso file</b>	Specifica il numero di tentativi effettuati dal server per accedere a un file.	1

### Proprietà dell'Output File Repository Server

Tabella 30 - 21: Proprietà del servizio archivio file di output

Proprietà	Descrizione	Valore predefinito
<b>Directory archivio file</b>	Specifica la directory in cui vengono archiviati gli oggetti repository dei file. <b>Nota:</b> Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni.	%DefaultOutputFRS Dir/%
<b>Directory temporanea</b>	Specifica la directory in cui vengono creati i file temporanei quando necessario. <b>Nota:</b> Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni.	%DefaultOutputFRS Dir/temp%
<b>Tempo massimo di inattività (in minuti)</b>	Specifica il periodo di tempo di attesa del server prima della chiusura delle connessioni inattive. L'impostazione di un valore troppo basso può causare la chiusura prematura della richiesta di un utente. L'impostazione di un valore troppo alto può causare un consumo eccessivo delle risorse del sistema, ad esempio il tempo di elaborazione e lo spazio su disco.	10
<b>Numero max. tentativi per l'accesso file</b>	Specifica il numero di tentativi effettuati dal server per accedere a un file.	1

## Proprietà del server del contenitore di applicazioni Web

Tabella 30 - 22: Proprietà generali

Proprietà	Descrizione	Valore predefinito
<b>Timeout di avvio servizio (secondi)</b>	<p>Tempo di attesa dell'avvio dei servizi ospitati da parte del server WACS prima del timeout. Se il timeout scade, il WACS non fornirà servizi non ancora avviati. In un computer più lento, è opportuno specificare un valore più lungo.</p> <p>Se si specifica un valore troppo piccolo e il server WACS non viene avviato prima del timeout, ripristinare le impostazioni predefinite del server WACS tramite Central Configuration Manager (CCM).</p>	1500

Tabella 30 - 23: Proprietà del servizio log analisi

Proprietà	Descrizione	Valore predefinito
<b>Livello di registrazione</b>	<p>Consente la registrazione e imposta il livello di gravità e dettaglio su Nessuno (registrazione dei soli eventi più importanti), Bassa (avvio, chiusura, messaggi di richiesta di avvio e chiusura), Media (messaggi di errore, avviso e la maggior parte dei messaggi di stato) o Alta (include tutti i casi. Utilizzare solo per finalità di debug. L'utilizzo della CPU potrebbe risultare più intenso, rallentando le prestazioni).</p> <p>Di seguito sono elencate le opzioni a disposizione:</p> <ul style="list-style-type: none"> <li>• <b>Non specificato</b></li> <li>• <b>Nessuno</b></li> <li>• <b>Bassa</b></li> <li>• <b>Media</b></li> <li>• <b>Alta</b></li> </ul>	Non specificato

Tabella 30 - 24: Proprietà del servizio BI Business Process

Proprietà	Descrizione	Valore predefinito
Nessuna proprietà di configurazione		

Tabella 30 - 25: Proprietà del servizio Query Builder

Proprietà	Descrizione	Valore predefinito
Nessuna proprietà di configurazione		

Tabella 30 - 26: Servizio Web RESTful - Proprietà di configurazione delle proprietà di sistema

Proprietà	Descrizione	Valore predefinito
<b>Mostra stack errori</b>	Quando è attivo, il registro errori include i messaggi di errore del servizio Web RESTful a scopo di debug. Non dovrebbe essere utilizzato per altre finalità o quando si verifica un problema a livello di protezione per cui le informazioni della piattaforma BI sono divulgate.	Non selezionato
<b>Numero predefinito di oggetti in una pagina</b>	Il numero di voci che verranno elencate per pagina. Gli sviluppatori possono sovrascrivere questa impostazione con il parametro &pageSize=<m> nell'SDK del servizio Web RESTful.	50
<b>Timeout token sessione Enterprise (minuti)</b>	Il tempo per cui un token di accesso rimarrà valido. Terminato questo lasso di tempo, dovrà essere generato un nuovo token di accesso.	60
<b>Dimensioni pool sessioni</b>	Il numero di sessioni memorizzate da archiviare contemporaneamente utilizzate per migliorare le prestazioni del server. Il pool sessioni memorizza le sessioni attive del servizio Web RESTful in modo che possano essere riutilizzate quando un utente invia un'altra richiesta che utilizza lo stesso token di accesso nell'intestazione della richiesta HTTP.	1000
<b>Timeout pool sessioni (in minuti)</b>	Il lasso di tempo espresso in minuti in cui le sessioni memorizzate scadranno.	2

Proprietà	Descrizione	Valore predefinito
<b>Abilita autenticazione di base HTTP</b>	Se questa impostazione non è abilitata, le richieste del servizio Web RESTful dovranno utilizzare un token di accesso. Quando questa impostazione è attiva, gli utenti devono fornire il nome e la password alla prima richiesta del servizio Web RESTful. Quando è attiva, viene visualizzato il menu a discesa <b>Schema di autenticazione predefinito per HTTP di base</b> .	Non selezionato
<b>Schema di autenticazione predefinito per HTTP di base</b>	Quando l'opzione <b>Abilita autenticazione di base HTTP</b> è selezionata, è possibile scegliere uno dei quattro tipi di autenticazione. I nomi e le password vengono trasmessi in testo non crittografato a meno che non vengano utilizzate le opzioni HTTPS.  I valori accettati sono: <ul style="list-style-type: none"> <li>• <b>SecEnterprise</b></li> <li>• <b>secDAP</b></li> <li>• <b>SAPR3</b></li> <li>• <b>secWinAD</b></li> </ul>	Vuoto. Se, tuttavia, è selezionato <b>Abilita autenticazione di base HTTP</b> , come valore predefinito viene utilizzato <b>secEnterprise</b> .

Tabella 30 - 27: Servizio Web RESTful - Proprietà di configurazione della condivisione di risorse con diverse origini

Proprietà	Descrizione	Valore predefinito
<b>Consenti origini</b>	Questa impostazione ha lo scopo di consentire agli utenti con browser che supportano la configurazione della condivisione di risorse con diverse origini di accedere alle pagine con script Java che devono accedere a più nomi di dominio. Aggiungere i singoli nomi di dominio e separarli con virgole. Ad esempio http://origin1.server.com:8080, http://origin2.server.com:8080. Per impostazione predefinita, ai browser è consentito l'accesso a tutti i domini (*).	* (un asterisco)
<b>Durata max (minuti)</b>	Si tratta della durata massima di mantenimento delle richieste HTTP nella cache dei browser.	1440

Tabella 30 - 28: Servizio Web RESTful - Proprietà di configurazione autenticazione affidabile

Proprietà	Descrizione	Valore predefinito
<b>Metodo di recupero</b>	<p>Questa impostazione è un menu che consente di specificare il metodo query da utilizzare per il recupero dei token di accesso con autenticazione affidabile quando si utilizza l'API del servizio Web RESTful /logon/trusted.</p> <ul style="list-style-type: none"> <li>• <b>HTTP_HEADER</b> viene utilizzato per le query GET con l'intestazione di richiesta accept=application/xml (o application/json).</li> <li>• <b>QUERY_STRING</b> viene utilizzato per aggiungere un nome di accesso alla fine di una query URL quando si utilizza l'API del servizio Web RESTful, ad esempio /logon/trusted/?user=johndoe.</li> <li>• <b>COOKIE</b> viene utilizzato quando si recupera il nome di accesso da un cookie del browser. Nel cookie devono essere memorizzati il dominio, il nome, il valore e il percorso.</li> </ul>	HTTP_HEADER
<b>Parametro nome utente</b>	Questa è l'etichetta utilizzata per identificare un utente attendibile allo scopo di recuperare un token di accesso.	X-SAP-TRUSTED-USER

Tabella 30 - 29: Proprietà del servizio applicazione Web BOE

Tipo di proprietà	Descrizione	Valore predefinito
<b>Tipo di autenticazione</b>	<p>Il tipo di autenticazione utilizzato per autenticare gli utenti per l'accesso a BI Launch Pad.</p> <p>I valori accettati sono:</p> <ul style="list-style-type: none"> <li>• <b>AD Kerberos</b></li> <li>• <b>AD Kerberos SSO</b></li> <li>• <b>Enterprise</b></li> <li>• <b>LDAP</b></li> </ul>	Enterprise
<b>Dominio AD predefinito</b>	Il dominio Active Directory predefinito viene utilizzato in modo che gli utenti non debbano fornire un dominio al momento dell'accesso. Ad esempio, se il dominio predefinito è impostata su "dominio" e un utente accede con il nome utente "utente", l'autorità di accesso Active Directory tenta di autenticare "utente@dominio.com".	Vuoto

Tipo di proprietà	Descrizione	Valore predefinito
<b>Nome principale servizio</b>	Nome principale servizio (SPN) utilizzato dai client per identificare in modo univoco un'istanza di un servizio. Il servizio di autenticazione Kerberos utilizza un SPN per autenticare un servizio.	Vuoto
<b>File di codice</b>	Percorso completo a un file di codice. Un file di codice consente di configurare i filtri Kerberos senza esposizione della password dell'account utente sul computer di applicazioni Web.	Vuoto

Tabella 30 - 30: Proprietà di SDK e QaaWS di servizi Web

Proprietà	Descrizione	Valore predefinito
<b>Abilita Single Sign On per Kerberos Active Directory</b>	Se abilitare Single Sign On di Kerberos AD per SDK e QaaWS di servizi Web.	FALSE
<b>Dominio AD predefinito</b>	Il dominio Active Directory predefinito viene utilizzato in modo che gli utenti non debbano fornire un dominio al momento dell'accesso.	Vuoto
<b>Nome principale servizio</b>	Nome principale servizio (SPN) utilizzato dai client per identificare in modo univoco un'istanza di un servizio. Il servizio di autenticazione Kerberos utilizza un SPN per autenticare un servizio.	Vuoto
<b>File di codice</b>	Percorso completo a un file di codice. Un file di codice consente di configurare i filtri Kerberos senza esposizione della password dell'account utente sul computer di applicazioni Web.	Vuoto

Tabella 30 - 31: Proprietà di configurazione HTTP

Proprietà	Descrizione	Valore predefinito
<b>Associa a tutti gli indirizzi IP</b>	Se eseguire o meno l'associazione a tutte le interfacce di rete. Se il server dispone di più schede NIC e si desidera stabilire un'associazione a un'interfaccia di rete specifica, deselezionare questa proprietà.	TRUE
<b>Associa a nome host o a indirizzo IP</b>	Specifica in quale interfaccia di rete (indirizzo IP o nome host) viene fornito il servizio HTTP. È possibile specificare un valore solo se si deseleziona <b>Associa a tutti gli indirizzi IP</b> .	localhost

Proprietà	Descrizione	Valore predefinito
<b>Porta HTTP</b>	Porta su cui viene fornito il servizio HTTP.	6405 L'intervallo di valori consentiti è tra 1 e 65535.
<b>Dimensioni massime intestazione HTTP</b>	La massima dimensione consentita, in byte, dell'intestazione HTTP di richiesta e risposta.	32768

Tabella 30 - 32: Proprietà della configurazione di HTTP tramite proxy

Proprietà	Descrizione	Valore predefinito
<b>Abilita HTTP su proxy</b>	Se abilitare il connettore HTTP tramite proxy sul server WACS. Questa opzione è in genere selezionata nelle distribuzioni con proxy inverso.	FALSE
<b>Associa a tutti gli indirizzi IP</b>	Se associare o meno la porta HTTP su proxy a tutte le interfacce di rete.	TRUE
<b>Associa a nome host o a indirizzo IP</b>	Specifica in quale interfaccia di rete (indirizzo IP o nome host) viene fornito il servizio HTTP tramite proxy. È possibile specificare un valore solo se si deselecta <b>Associa a tutti gli indirizzi IP</b> .	localhost
<b>Porta HTTP</b>	Porta su cui viene fornito il servizio HTTP in una distribuzione con proxy inverso. È possibile specificare un valore solo se si seleziona <b>Abilita HTTP su proxy</b> .	6406 L'intervallo di valori consentiti è tra 1 e 65535.
<b>Nome host proxy</b>	Indirizzo IPv4, IPv6, nome host o nome di dominio completo del server proxy. È possibile specificare un valore solo se si seleziona <b>Abilita HTTP su proxy</b> .	Vuoto
<b>Porta proxy</b>	Porta del server proxy normale o del server proxy inverso. È possibile specificare un valore solo se si seleziona <b>Abilita HTTP su proxy</b> .	0 L'intervallo di valori consentiti è tra 1 e 65535.
<b>Dimensioni massime intestazione HTTP</b>	La massima dimensione consentita, in byte, dell'intestazione HTTP di richiesta e risposta.	32768



Tabella 30 - 33: Proprietà di configurazione HTTPS

Proprietà	Descrizione	Valore predefinito
<b>Abilita HTTPS</b>	Se abilitare o meno la comunicazione HTTPS/SSL.	FALSE
<b>Associa a nome host o a indirizzo IP</b>	Specifica in quale interfaccia di rete (indirizzo IP o nome host) viene fornito il servizio HTTPS. È possibile specificare un valore solo se si seleziona <b>Abilita HTTPS</b> .	localhost
<b>Porta HTTPS</b>	Porta su cui viene fornito il servizio HTTPS. È possibile specificare un valore solo se si seleziona <b>Abilita HTTPS</b> .	443 L'intervallo di valori consentiti è tra 1 e 65535.
<b>Nome host proxy</b>	Indirizzo IPv4, IPv6, nome host o nome di dominio completo del server proxy. È possibile specificare un valore solo se si seleziona <b>Abilita HTTPS</b> .	Vuoto
<b>Porta proxy</b>	Porta del server proxy normale o del server proxy inverso. È possibile specificare un valore solo se si seleziona <b>Abilita HTTPS</b> .	0 L'intervallo di valori consentiti è tra 1 e 65535.
<b>Protocollo</b>	Protocollo di crittografia da utilizzare. È possibile specificare un valore solo se si seleziona <b>Abilita HTTPS</b> .	TLS I valori consentiti sono TLS o SSL.
<b>Tipo di archivio certificati</b>	Il tipo di archivio certificati che contiene i certificati e le chiavi private. Nella maggior parte dei casi è <b>PKCS12</b> . È possibile specificare un valore solo se si seleziona <b>Abilita HTTPS</b> .	PKCS12 I valori consentiti sono PKCS12 o JKS.
<b>Percorso file archivio certificati</b>	Il percorso completo del file di certificati. È possibile specificare un valore solo se si seleziona <b>Abilita HTTPS</b> .	Vuoto
<b>Password accesso chiave privata</b>	Gli archivi certificati PKCS12 e gli archivi di chiavi JKS presentano chiavi private protette con password per impedire accessi o appropriazioni non autorizzate. Immettere la password specificata alla generazione dell'archivio certificati, in modo da consentire al server WACS l'accesso alle chiavi private dall'archivio certificati. È possibile specificare un valore solo se si seleziona <b>Abilita HTTPS</b> .	Vuoto

Proprietà	Descrizione	Valore predefinito
<b>Alias certificato</b>	Alias del certificato all'interno dell'archivio di certificati. Se non è specificato e viene utilizzato un archivio che contiene più di un certificato, verrà utilizzato il primo certificato dell'archivio. Nella maggior parte dei casi non è necessario specificare un valore. È possibile specificare un valore solo se si seleziona <b>Abilita HTTPS</b> .	Vuoto
<b>Abilita autenticazione client</b>	Se l'autenticazione client è abilitata, solo i client con chiavi archiviate nel file di certificati attendibili possono ottenere i servizi WACS. Gli altri client sono rifiutati. È possibile abilitare l'autenticazione client solo se si seleziona <b>Abilita HTTPS</b> .	FALSE
<b>Percorso file elenco certificati attendibili</b>	Il percorso completo del file di elenco dei certificati attendibili. È possibile specificare un valore solo se si seleziona <b>Abilita HTTPS</b> e <b>Abilita autenticazione client</b> .	Vuoto
<b>Password accesso chiavi private elenco certificati attendibili</b>	La password che protegge l'accesso alle chiavi private nel file dell'elenco di certificati attendibili. È possibile specificare un valore solo se si seleziona <b>Abilita HTTPS</b> e <b>Abilita autenticazione client</b> .	Vuoto
<b>Dimensioni massime intestazione HTTP</b>	La massima dimensione consentita, in byte, dell'intestazione HTTP di richiesta e risposta.	32768

Tabella 30 - 34: Proprietà di concorrenza (per connettore)

Proprietà	Descrizione	Valore predefinito
<b>N. massimo richieste simultanee</b>	Numero di richieste HTTP o HTTPS simultanee che ogni connettore (HTTP, HTTP tramite proxy o HTTPS) è in grado di elaborare contemporaneamente.	150 L'intervallo di valori consentiti è tra 1 e 1000.

Tabella 30 - 35: Proprietà di configurazione di Active Directory

Proprietà	Descrizione	Valore predefinito
<b>Posizione file Krb5.ini</b>	Percorso completo di un file <code>krb5.ini</code> in cui sono memorizzate le proprietà di configurazione di Kerberos.	Vuoto

Proprietà	Descrizione	Valore predefinito
<b>Posizione file bscLogin.conf</b>	Percorso completo a un file <code>bscLogin.conf</code> .	Vuoto

### 30.1.3 Proprietà dei servizi di connettività

La categoria dei servizi di connettività include i servizi seguenti:

- Servizio di connettività nativo (ospitato in un server autonomo)
- Servizio di connettività nativo (a 32 bit, ospitato in un server autonomo)
- Servizio di connessione adattivo (ospitato in APS)

Tutti i servizi condividono le stesse impostazioni di configurazione.

Tabella 30 - 36: Proprietà di Servizio accesso ai dati Excel

Proprietà	Descrizione	Valore predefinito
<b>Timeout eliminazione accesso ai dati Excel (in secondi)</b>	Specifica l'intervallo di tempo, espresso in secondi, in cui il servizio attende un client inattivo prima di svuotare la sessione del client.	Il valore predefinito è 1200 secondi.
<b>Timeout scambio accesso ai dati Excel (in secondi)</b>	Specifica l'intervallo di tempo, espresso in secondi, in cui il servizio attende un client inattivo prima di eseguire lo scambio della sessione del client sul disco rigido. È consigliabile specificare un valore inferiore al valore della proprietà <b>Timeout eliminazione accesso ai dati Excel (in secondi)</b> .	Il valore predefinito è 600 secondi.

Tabella 30 - 37: Proprietà di funzionamento del servizio

Proprietà	Descrizione	Valore predefinito
<b>Promemoria:</b> Non è necessario riavviare il server dopo aver modificato le seguenti proprietà di funzionamento del servizio.		

Proprietà	Descrizione	Valore predefinito
<b>Raggruppamento delle connessioni</b>	<p>Abilita o disabilita il pool di connessioni.</p> <p>I valori possibili sono i seguenti:</p> <ul style="list-style-type: none"> <li>• Abilitato - con timeout</li> <li>• Abilitato - senza timeout</li> <li>• Disabilitato</li> </ul> <p><b>Nota:</b> Il pool di connessioni è una funzionalità di memorizzazione nella cache che mantiene le connessioni in uno stato riutilizzabile per migliorare le prestazioni del server.</p>	Abilitato - con timeout
<b>Timeout Connection Pool</b>	<p>Specifica il tempo massimo di inattività per le connessioni nel pool (in minuti).</p> <p><b>Nota:</b> Questa proprietà equivale al parametro <code>Max Pool Time</code> del file <code>cs.cfg</code>. Disabilitare il pool equivale a impostare <code>Max Pool Time</code> su 0. Abilitare il pool senza timeout equivale a impostare <code>Max Pool Time</code> su -1. Consultare il <i>Manuale dell'accesso ai dati</i> per ulteriori informazioni.</p>	60
<b>Timeout inattività oggetti transitori</b>	<p>Specifica per quanti minuti mantenere nel server gli oggetti temporanei inutilizzati. Al termine di tale periodo l'oggetto viene rimosso e le rispettive risorse vengono recuperate.</p>	60
<b>Intervallo timer oggetti transitori</b>	<p>Specifica l'intervallo di tempo tra le verifiche delle attività (in minuti). Il server verifica a intervalli regolari la presenza di oggetti da rimuovere.</p>	5
<b>Abilita raggruppamento HTTP</b>	<p>Abilita o disabilita il raggruppamento HTTP.</p> <p><b>Nota:</b> Il raggruppamento HTTP è rilevante solo per la distribuzione 3-tier e influisce sulle performance del documento in fase di apertura e aggiornamento, poiché una maggiore risposta comporta meno cicli di andata e ritorno durante il recupero di documenti di dimensioni elevate. Disabilitare il raggruppamento HTTP equivale a impostare <b>Dimensioni blocco HTTP</b> su 0.</p>	Enabled

Proprietà	Descrizione	Valore predefinito
<b>Dimensioni blocco HTML</b>	Specifica le dimensioni delle risposte HTTP emesse dal server (in kilobyte).	64

Tabella 30 - 38: Proprietà di analisi di basso livello

Proprietà	Descrizione	Valore predefinito
<b>Promemoria:</b> Non è necessario riavviare il server dopo aver modificato le seguenti proprietà di analisi di basso livello.		
<b>Abilita analisi processo</b>	Abilita l'analisi dei processi di Connection Server. <b>Nota:</b> La proprietà <b>Livello log</b> deve essere impostata su <b>Alto</b> .	Disabilitato
<b>Abilita analisi middleware</b>	Abilita l'analisi di tutto il middleware. Per analizzare un middleware specifico, è necessario configurare il file <code>cs.cfg</code> e riavviare il server. <b>Nota:</b> La proprietà <b>Livello log</b> deve essere impostata su <b>Alto</b> .	Disabilitato

Tabella 30 - 39: Proprietà delle origini dati attive

Proprietà	Descrizione	Valore predefinito
<b>Avvertenza:</b> È necessario riavviare il server dopo aver modificato le seguenti proprietà delle origini dati attive.		

Proprietà	Descrizione	Valore predefinito
<b>Attiva origine dati</b>	<p>Consente di scegliere le origini dati per le quali si desidera stabilire delle connessioni. Questa proprietà funziona come filtro per i driver. È necessario specificare le origini dati attive per caricare i driver che si desidera utilizzare.</p> <p><b>Avvertenza:</b> Per impostazione predefinita il server carica tutti i driver disponibili. Questa impostazione può essere utilizzata per differenziare il comportamento dei server ed è utile soprattutto quando si distribuiscono più server CORBA nella propria rete.</p> <p><b>Promemoria:</b> vengono caricati solo i driver per le origini dati selezionate. Tutti gli altri vengono ignorati. Se non si selezionano origini dati, il server carica tutti i driver disponibili.</p> <p><b>Nota:</b> verificare nelle metriche del server che le origini dati selezionate siano state attivate. I livelli di rete e i database vengono visualizzati in "Metriche di Servizio connessioni".</p>	Deselezionato
<b>Livello di rete</b>	<p>Specifica il livello di rete utilizzato dalla connessione.</p> <p><b>Nota:</b> Viene considerato solamente il nome non localizzato. È possibile trovare l'elenco dei livelli di rete disponibili nel file <code>driver.cfg</code> che si trova nella directory <code>dir-installaz-connectionserver\connectionServer\</code>.</p>	<ul style="list-style-type: none"> <li>• ODBC per server CORBA nativi</li> <li>• JDBC per server CORBA adattivi</li> </ul>

Proprietà	Descrizione	Valore predefinito
<b>Database</b>	<p>Specifica il database utilizzato dalla connessione.</p> <p><b>Nota:</b> Viene considerato solamente il nome non localizzato. per i nomi di database è possibile utilizzare espressioni regolari se queste sono composte unicamente da caratteri ASCII e utilizzano la sintassi GNU regexp. Utilizzare il criterio <code>.*</code> per trovare una corrispondenza per qualsiasi carattere. Ad esempio, l'espressione <code>MS SQL Server.*\$</code> significa che vengono utilizzati tutti i database MS SQL Server. Per ulteriori informazioni sulle espressioni regolari, consultare il sito Web PERL all'indirizzo <a href="http://www.perl.com/doc/manual/html/pod/perlre.html#Regular_Expressions">http://www.perl.com/doc/manual/html/pod/perlre.html#Regular_Expressions</a>.</p>	Il campo è vuoto finché non si inserisce il nome di un database.

Tabella 30 - 40: Proprietà di Servizio accesso ai dati personalizzato

Proprietà	Descrizione	Valore predefinito
<b>Timeout eliminazione accesso ai dati personalizzato (in secondi)</b>	Specifica l'intervallo di tempo, espresso in secondi, in cui il servizio attende un client inattivo prima di svuotare la sessione del client.	Il valore predefinito è 1200 secondi.
<b>Timeout scambio accesso ai dati personalizzato (in secondi)</b>	Specifica l'intervallo di tempo, espresso in secondi, in cui il servizio attende un client inattivo prima di eseguire lo scambio della sessione del client sul disco rigido. È consigliabile specificare un valore inferiore al valore della proprietà <b>Timeout eliminazione accesso ai dati personalizzato (in secondi)</b> .	Il valore predefinito è 600 secondi.

Tabella 30 - 41: Proprietà del Servizio Single Sign-On

Proprietà	Descrizione	Valore predefinito
<b>Scadenza Single Sign-On (secondi)</b>	Specifica il tempo, in secondi, di validità di una connessione SSO prima della scadenza.	Il valore predefinito è 86400 secondi.

Tabella 30 - 42: Proprietà del servizio Lifecycle Management

Proprietà	Descrizione	Valore predefinito
Nessuna proprietà di configurazione		

Tabella 30 - 43: Proprietà del servizio ClearCase di Lifecycle Management

Proprietà	Descrizione	Valore predefinito
Nessuna proprietà di configurazione		

Tabella 30 - 44: Proprietà del servizio Differenza visiva

Proprietà	Descrizione	Valore predefinito
Nessuna proprietà di configurazione		

#### Argomenti correlati

- [Proprietà comuni dei server](#)

## 30.1.4 Proprietà dei servizi Crystal Reports

La categoria del servizio Crystal Reports include i server seguenti:

- Crystal Reports Cache Server
- Crystal Reports Processing Server
- Proprietà di Report Application Server di Crystal Reports 2013
- Server di elaborazione di Crystal Reports 2013

#### Proprietà di Crystal Reports Cache Server

Le proprietà che si applicano sia a Crystal Reports Cache Server che a Crystal Reports Processing Server devono essere impostate sullo stesso valore. Ad esempio, se si imposta l'opzione **L'aggiornamento del visualizzatore produce sempre i dati correnti** su TRUE per Cache Server, è necessario impostare la stessa proprietà su TRUE per Processing Server.

#### Nota:

quando si modifica una di queste proprietà del server, è necessario riavviare il server per rendere effettive le modifiche.



Tabella 30 - 45: Proprietà del Servizio cache Crystal Reports

Proprietà	Descrizione	Valore predefinito
<b>L'aggiornamento del visualizzatore produce sempre i dati correnti</b>	<p>Specifica se, quando gli utenti aggiornano un report in modo esplicito, tutte le pagine memorizzate nella cache vengono ignorate e vengono recuperati nuovi dati direttamente dal database.</p> <p><b>Nota:</b> È possibile impostare questa proprietà su un oggetto report utilizzando valori diversi da un report a un altro. I valori specificati nell'oggetto report hanno la priorità su quelle del server. Per specificare un valore nell'oggetto report, selezionare il report nella console CMC e fare clic su <b>Impostazioni predefinite &gt; Visualizzazione gruppo di server</b>.</p>	Il valore predefinito è FALSE.
<b>Condividi dati dei report tra i client</b>	<p>Specifica se i dati di report sono condivisi tra client diversi.</p> <p><b>Nota:</b> È possibile impostare questa proprietà su un oggetto report utilizzando valori diversi da un report a un altro. I valori specificati nell'oggetto report hanno la priorità su quelle del server.</p>	Il valore predefinito è TRUE.
<b>Timeout connessione inattiva (minuti)</b>	Specifica il periodo di tempo, in minuti, di attesa di Crystal Reports Cache Server per una richiesta da una connessione inattiva. Non è in genere necessario modificare il valore predefinito.	Il valore predefinito è 20 minuti.
<b>Timeout cache di protezione (minuti)</b>	Specifica l'intervallo di tempo, in minuti, in cui il server utilizza le credenziali di accesso, i parametri del report e le informazioni sulla connessione al database memorizzate nella cache per soddisfare le richieste prima di eseguire una query sul CMS.	Il valore predefinito è 20 minuti.

Proprietà	Descrizione	Valore predefinito
<b>Dati meno recenti forniti ai client su richiesta</b>	<p>Specifica il periodo di tempo, in secondi, di utilizzo dei dati memorizzati nella cache da parte del server per soddisfare le richieste da report su richiesta.</p> <p>Se il server riceve una richiesta che può essere gestita con dati generati per una richiesta precedente e il tempo trascorso dalla generazione dei dati è inferiore al valore impostato, il server riutilizzerà tali dati per rispondere alla richiesta successiva. Il riutilizzo dei dati in questo modo migliora nettamente le prestazioni del sistema quando più utenti richiedono le stesse informazioni.</p> <p>Nell'impostazione di questo valore è opportuno considerare quanto sia importante che gli utenti ricevano dati aggiornati. Se è essenziale che tutti gli utenti ricevano dati aggiornati (poiché i dati importanti cambiano molto frequentemente), è consigliabile disattivare questo tipo di riutilizzo dei dati impostando il valore su 0.</p> <p><b>Nota:</b> È possibile impostare questa proprietà su un oggetto report utilizzando valori diversi da un report a un altro. I valori specificati nell'oggetto report hanno la priorità su quelle del server.</p>	Il valore predefinito è 0 secondi.
<b>Dimensioni cache massime (KB)</b>	Specifica la quantità di spazio su disco rigido, in KB, utilizzata per la memorizzazione dei report nella cache. Se il server deve gestire molti report o report particolarmente complessi può essere necessario disporre di una cache di grandi dimensioni.	Il valore predefinito è 256000 KB.
<b>Directory file cache</b>	Specifica il percorso della directory del file cache.	%DefaultDataDir%/CrystalReportsCachingServer/temp
<b>Argomenti Java VM</b>	Indica gli argomenti della riga di comando che è possibile specificare per la JVM.	Il valore predefinito è vuoto.
<b>Nome DLL</b>	<p>Specifica il nome del plug-in del tipo di documento attualmente caricato.</p> <p>Questa proprietà è disponibile in modalità di sola lettura.</p>	rasprocReport

### Proprietà del Server di elaborazione Crystal Reports

Le proprietà che si applicano sia a Crystal Reports Cache Server che a Crystal Reports Processing Server devono essere impostate sullo stesso valore. Ad esempio, se si imposta l'opzione **L'aggiornamento del visualizzatore produce sempre i dati correnti** su TRUE per Cache Server, è necessario impostare la stessa proprietà su TRUE per Processing Server.

**Nota:**

quando si modifica una di queste proprietà del server, è necessario riavviare il server per rendere effettive le modifiche.

Tabella 30 - 46: Proprietà del Servizio di elaborazione Crystal Reports

Proprietà	Descrizione	Valore predefinito
<b>Timeout connessione inattiva (minuti)</b>	Specifica il periodo di tempo, in minuti, di attesa di Crystal Reports Processing Server tra le richieste per un determinato processo.	Il valore predefinito è 20 minuti.
<b>Durata massima dei processi per elemento secondario</b>	Specifica il numero massimo di processi che ogni processo secondario può gestire per durata.	Il valore predefinito è 1000.
<b>L'aggiornamento del visualizzatore produce sempre i dati correnti</b>	<p>Specifica se, quando gli utenti aggiornano un report in modo esplicito, tutte le pagine memorizzate nella cache vengono ignorate e vengono recuperati nuovi dati direttamente dal database. Specifica se i dati di report sono condivisi tra client diversi.</p> <p><b>Nota:</b> È possibile impostare questa proprietà su un oggetto report utilizzando valori diversi da un report a un altro. I valori specificati nell'oggetto report hanno la priorità su quelle del server. Per specificare un valore nell'oggetto report, selezionare il report nella console CMC e fare clic su <b>Impostazioni predefinite &gt; Visualizzazione gruppo di server</b>.</p>	Il valore predefinito è FALSE.
<b>Condividi i dati dei report tra i client</b>	<p>Specifica se i dati di report sono condivisi tra client diversi. Specifica se i dati di report sono condivisi tra client diversi.</p> <p><b>Nota:</b> È possibile impostare questa proprietà su un oggetto report utilizzando valori diversi da un report a un altro. I valori specificati nell'oggetto report hanno la priorità su quelle del server.</p>	Il valore predefinito è TRUE.

Proprietà	Descrizione	Valore predefinito
<b>Timeout connessione inattiva (minuti)</b>	Specifica il periodo di tempo, in minuti, di attesa di Crystal Reports Processing Server per una richiesta da una connessione inattiva. Non è in genere necessario modificare il valore predefinito.	Il valore predefinito è 20 minuti.
<b>Numero max. processi simultanei (0 per automatico)</b>	Specifica il numero massimo di processi indipendenti che possono essere eseguiti simultaneamente su Crystal Reports Processing Server. Se il valore di questa proprietà viene impostato su "0", il server applica un valore adeguato, in base alla CPU e alla memoria del computer in cui il server è in esecuzione.	Il valore predefinito è 0.
<b>Dati meno recenti forniti ai client su richiesta (secondi)</b>	<p>Specifica il periodo di tempo, in secondi, di utilizzo dei dati memorizzati nella cache da parte del server per soddisfare le richieste da report su richiesta.</p> <p>Se il server riceve una richiesta che può essere gestita con dati generati per una richiesta precedente e il tempo trascorso dalla generazione dei dati è inferiore al valore impostato, il server riutilizzerà tali dati per rispondere alla richiesta successiva. Il riutilizzo dei dati in questo modo migliora nettamente le prestazioni del sistema quando più utenti richiedono le stesse informazioni.</p> <p>Nell'impostazione di questo valore è opportuno considerare quanto sia importante che gli utenti ricevano dati aggiornati. Se è essenziale che tutti gli utenti ricevano dati aggiornati (poiché i dati importanti cambiano molto frequentemente), è consigliabile disattivare questo tipo di riutilizzo dei dati impostando il valore su 0.</p> <p><b>Nota:</b> È possibile impostare questa proprietà su un oggetto report utilizzando valori diversi da un report a un altro. I valori specificati nell'oggetto report hanno la priorità su quelle del server.</p>	Il valore predefinito è 0.
<b>Numero massimo di elementi secondari preiavviati</b>	Specifica il numero massimo di processi secondari preiavviati consentiti dal server. Se questo valore è troppo basso, il server crea processi secondari non appena vengono effettuate le richieste e potrebbero verificarsi latenze. Se questo valore è troppo elevato, è possibile che le risorse del sistema vengano impegnate inutilmente da processi secondari inattivi.	Il valore predefinito è 1 elemento secondario.

Proprietà	Descrizione	Valore predefinito
<b>Directory temporanea</b>	Specifica la directory in cui vengono creati i file temporanei quando necessario. <b>Nota:</b> Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni.	%DefaultData Dir%/CrystalReports ProcessingServer/te mp
<b>Percorso classe Java</b>	Nome e percorso delle classi Java richieste dal server.	%CommonJavaLib Dir%/procCR.jar
<b>Argomenti VM elemento secondario Java</b>	Indica gli argomenti della riga di comando specificati per i processi secondari creati dal server.	Dbusinessobjects.co nnectivity.directo ry=%CONNECTION SER VER_DIR%,Dcom.bu sinessobje cts.mds.cs.Implemen tationID=csEX

Tabella 30 - 47: Proprietà del Servizio Single Sign-On

Proprietà	Descrizione	Valore predefinito
<b>Scadenza Single Sign-On (secondi)</b>	Specifica il tempo, in secondi, di validità di una connessione SSO prima della scadenza.	Il valore predefinito è 86400 secondi.

### Proprietà di Report Application Server di Crystal Reports 2013

**Nota:**

quando si modifica una di queste proprietà del server, è necessario riavviare il server per rendere effettive le modifiche.

Tabella 30 - 48: Proprietà del servizio di modifica e visualizzazione Crystal Reports 2013

Proprietà	Descrizione	Valore predefinito
<b>Consenti ai processi report di rimanere connessi al database fino alla chiusura del processo report</b>	Specifica se il processo report rimane connesso al database fino all'esecuzione.	Il valore predefinito è FALSE.

Proprietà	Descrizione	Valore predefinito
<b>Dimensione dati da sfogliare (record)</b>	Specifica il numero di record distinti restituiti dal database quando si sfogliano i valori di un determinato campo. I dati vengono recuperati prima dalla cache del client, se disponibile, quindi dalla cache del server. Se i dati non sono presenti in tali cache, vengono recuperati dal database.	Il valore predefinito è 100 record.
<b>Timeout connessione inattiva (minuti)</b>	<p>Specifica la quantità di tempo, in minuti, di attesa di Report Application Server (RAS) per le richieste da un cliente inattivo prima del timeout.</p> <p>Un valore troppo basso può determinare la chiusura prematura di una richiesta utente, mentre l'impostazione di un valore troppo alto può incidere sulla scalabilità del server (ad esempio, se l'oggetto <code>Report ClientDocument</code> non viene chiuso in modo esplicito, il server resterà inutilmente in attesa della chiusura di un processo inattivo).</p>	Il valore predefinito è 30 minuti.
<b>Dimensioni batch (record)</b>	<p>Specifica quante righe dell'insieme di risultati vengono restituite dal database durante ogni trasferimento di dati.</p> <p>Ad esempio, se sono richiesti 500 record e la proprietà Dimensioni batch è impostata su 100 record, i dati verranno restituiti in 5 batch separati di 100 righe. Per migliorare le prestazioni del server RAS, è necessario considerare l'ambiente di rete, il database e il tipo di richieste per impostare le dimensioni batch appropriate.</p>	Il valore predefinito è 100 record.
<b>Numero di record di database da leggere per l'anteprima o l'aggiornamento di un report (-1 per nessun limite) (</b>	<p>Specifica il numero di record di database da leggere durante la visualizzazione o l'aggiornamento di un report. Questa impostazione limita il numero di record che il server recupera dal database quando un utente esegue una query o un report. Questa impostazione è utile quando si desidera impedire agli utenti di eseguire report su richiesta che restituiscono set di record di dimensioni eccessive.</p> <p>Potrebbe essere opportuno pianificare tali report, sia per renderli più velocemente disponibili per gli utenti che per ridurre il carico sul database provocato dalle query di grandi dimensioni.</p>	Il valore predefinito è 20000 record.

Proprietà	Descrizione	Valore predefinito
<b>Numero max. report simultanei (0 per nessun limite)</b>	Specifica il numero massimo di processi indipendenti che possono essere eseguiti simultaneamente sul server RAS.	Il valore predefinito è 75 processi.
<b>Dati meno recenti forniti a un client su richiesta (in minuti)</b>	Specifica il periodo di tempo, in minuti, durante il quale un report su richiesta fornisce dati di report memorizzati nella cache.	Il valore predefinito è 20 minuti.
<b>Directory temporanea</b>	<p>Specifica la directory in cui vengono creati i file temporanei quando necessario.</p> <p><b>Nota:</b> Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni.</p>	%DefaultData Dir%/CrystalRe portsRasSer ver/temp

Tabella 30 - 49: Proprietà del Servizio Single Sign-On

Proprietà	Descrizione	Valore predefinito
<b>Scadenza Single Sign-On (secondi)</b>	Specifica il tempo, in secondi, di validità di una connessione SSO prima della scadenza.	Il valore predefinito è 86400 secondi.

### Proprietà del server di elaborazione Crystal Reports 2013

**Nota:**

quando si modifica una di queste proprietà del server, è necessario riavviare il server per rendere effettive le modifiche.

Tabella 30 - 50: Proprietà del servizio di elaborazione di Crystal Reports 2013

Proprietà	Descrizione	Valore predefinito
<b>Timeout connessione inattiva (minuti)</b>	Specifica il periodo di tempo, in minuti, di attesa di Crystal Reports Processing Server tra le richieste per un determinato processo.	Il valore predefinito è 20 minuti.
<b>Durata massima dei processi per elemento secondario</b>	Specifica il numero massimo di processi che ogni processo secondario può gestire per durata.	Il valore predefinito è 1000.

Proprietà	Descrizione	Valore predefinito
<b>L'aggiornamento del visualizzatore produce sempre i dati correnti</b>	<p>Specifica se, quando gli utenti aggiornano un report in modo esplicito, tutte le pagine memorizzate nella cache vengono ignorate e vengono recuperati nuovi dati direttamente dal database. Specifica se i dati di report sono condivisi tra client diversi.</p> <p><b>Nota:</b> È possibile impostare questa proprietà su un oggetto report utilizzando valori diversi da un report a un altro. I valori specificati nell'oggetto report hanno la priorità su quelle del server. Per specificare un valore nell'oggetto report, selezionare il report nella console CMC e fare clic su <b>Impostazioni predefinite &gt; Visualizzazione gruppo di server</b>.</p>	Il valore predefinito è FALSE.
<b>Condividi i dati dei report tra i client</b>	<p>Specifica se i dati di report sono condivisi tra client diversi. Specifica se i dati di report sono condivisi tra client diversi.</p> <p><b>Nota:</b> È possibile impostare questa proprietà su un oggetto report utilizzando valori diversi da un report a un altro. I valori specificati nell'oggetto report hanno la priorità su quelle del server.</p>	Il valore predefinito è TRUE.
<b>Timeout connessione inattiva (minuti)</b>	Specifica il periodo di tempo, in minuti, di attesa di Crystal Reports Processing Server per una richiesta da una connessione inattiva. Non è in genere necessario modificare il valore predefinito.	Il valore predefinito è 20 minuti.
<b>Numero max. processi simultanei (0 per automatico)</b>	Specifica il numero massimo di processi indipendenti che possono essere eseguiti simultaneamente su Crystal Reports Processing Server. Se il valore di questa proprietà viene impostato su "0", il server applica un valore adeguato, in base alla CPU e alla memoria del computer in cui il server è in esecuzione.	Il valore predefinito è 0.



Proprietà	Descrizione	Valore predefinito
<b>Dati meno recenti forniti ai client su richiesta (secondi)</b>	<p>Specifica il periodo di tempo, in secondi, di utilizzo dei dati memorizzati nella cache da parte del server per soddisfare le richieste da report su richiesta.</p> <p>Se il server riceve una richiesta che può essere gestita con dati generati per una richiesta precedente e il tempo trascorso dalla generazione dei dati è inferiore al valore impostato, il server riutilizzerà tali dati per rispondere alla richiesta successiva. Il riutilizzo dei dati in questo modo migliora nettamente le prestazioni del sistema quando più utenti richiedono le stesse informazioni.</p> <p>Nell'impostazione di questo valore è opportuno considerare quanto sia importante che gli utenti ricevano dati aggiornati. Se è essenziale che tutti gli utenti ricevano dati aggiornati (poiché i dati importanti cambiano molto frequentemente), è consigliabile disattivare questo tipo di riutilizzo dei dati impostando il valore su 0.</p> <p><b>Nota:</b> È possibile impostare questa proprietà su un oggetto report utilizzando valori diversi da un report a un altro. I valori specificati nell'oggetto report hanno la priorità su quelle del server.</p>	Il valore predefinito è 0.
<b>Numero massimo di elementi secondari preiavviati</b>	<p>Specifica il numero massimo di processi secondari preiavviati consentiti dal server. Se questo valore è troppo basso, il server crea processi secondari non appena vengono effettuate le richieste e potrebbero verificarsi latenze. Se questo valore è troppo elevato, è possibile che le risorse del sistema vengano impegnate inutilmente da processi secondari inattivi.</p>	Il valore predefinito è 1 elemento secondario.
<b>Directory temporanea</b>	<p>Specifica la directory in cui vengono creati i file temporanei quando necessario.</p> <p><b>Nota:</b> Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni.</p>	%DefaultDataDir%/CrystalReports2013ProcessingServer/temp

Proprietà	Descrizione	Valore predefinito
<b>Consenti ai processi report di rimanere connessi al database fino alla chiusura del processo report</b>	Specifica se il processo report rimane connesso al database fino alla chiusura.	Il valore predefinito è FALSE.
<b>Record di database letti durante l'anteprima o l'aggiornamento (0 per senza limiti)</b>	<p>Specifica il numero di record di database da leggere durante la visualizzazione o l'aggiornamento di un report. Questa impostazione limita il numero di record che il server recupera dal database quando un utente esegue una query o un report. Questa impostazione è utile quando si desidera impedire agli utenti di eseguire report su richiesta che restituiscono set di record di dimensioni eccessive.</p> <p>Potrebbe essere opportuno pianificare tali report, sia per renderli più velocemente disponibili per gli utenti che per ridurre il carico sul database provocato dalle query di grandi dimensioni.</p>	Il valore predefinito è 20000.

Tabella 30 - 51: Proprietà del Servizio Single Sign-On

Proprietà	Descrizione	Valore predefinito
<b>Scadenza Single Sign-On (secondi)</b>	Specifica il tempo, in secondi, di validità di una connessione SSO prima della scadenza.	Il valore predefinito è 86400 secondi.

### 30.1.5 Proprietà dei servizi Analysis

La categoria dei servizi Analysis include Adaptive Processing Server:

Tabella 30 - 52: Proprietà dei servizi di analisi multidimensionali

Proprietà	Descrizione	Valore predefinito
<b>Numero massimo sessioni client</b>	<p>Specifica il numero massimo di sessioni MDAS che possono essere aperte contemporaneamente sul server.</p> <p>Quando il numero di sessioni aperte raggiunge tale valore, eventuali altri tentativi di avvio di sessioni MDAS generano un messaggio di errore di tipo “server non disponibile”. È possibile cambiare questo valore per ottimizzare le prestazioni del server MDAS, in base alle specifiche necessità e all'hardware disponibile; tuttavia, aumentare il valore potrebbe causare problemi di prestazioni al server MDAS e al database. Il valore predefinito di 15 sessioni è una stima prudente. Nelle installazioni con query utente di piccole dimensioni è possibile aumentare il valore in modo significativo, mentre per le installazioni con query utente di grandi dimensioni è opportuno impostare un valore inferiore.</p>	Il valore predefinito è impostato su 15. L'intervallo valido è compreso tra 1 e 100.
<b>Numero massimo di celle restituite da una query</b>	Specifica il numero di celle restituite a un utente in una singola query. L'utente non può eseguire una query che restituisce un numero di celle estremamente elevato, che consuma un quantità eccessiva di memoria. Se la query dell'utente supera il limite di celle specificato, l'utente riceve un messaggio di errore.	Il valore predefinito è 100000 celle.
<b>Numero massimo di membri restituiti durante il filtraggio</b>	Specifica il numero di membri recuperati durante il filtraggio per membro. Un numero elevato di membri recuperati può consumare una quantità eccessiva di memoria.	Il valore predefinito è 100000 membri.

Tabella 30 - 53: Proprietà dei servizi applicazioni Web BEx

Proprietà	Descrizione	Valore predefinito
<b>Numero massimo sessioni client</b>	Numero massimo di sessioni client consentite nel servizio.	Il valore predefinito è 15 sessioni.
<b>SAP BW Master System</b>	Il nome della connessione OLAP al sistema BW creato nella piattaforma BI.	Il valore predefinito è SAP_BW.
<b>Destinazione RFC server JCo</b>	Nome della destinazione RFC server JCo specificato nel sistema BW.	Per impostazione predefinita, il valore è vuoto.

Proprietà	Descrizione	Valore predefinito
<b>Host gateway server JCo</b>	Nome dell'host gateway server JCo specificato nel sistema BW.	Per impostazione predefinita, il valore è vuoto.
<b>Servizio gateway server JCo</b>	Nome del servizio gateway server JCo specificato nel sistema BW.	Per impostazione predefinita, il valore è vuoto.
<b>Conteggio connessione server JCo</b>	Specifica il numero di programmi creati automaticamente che possono essere utilizzati per gestire le chiamate da ABAP a Java per il servizio.	Il valore predefinito è 3 connessioni.

### 30.1.6 Proprietà dei servizi Data Federation

La categoria dei servizi Data Federation include Adaptive Processing Server:

Tabella 30 - 54: Proprietà dei servizi Data Federation

Proprietà	Descrizione	Valore predefinito
<b>Connessioni max</b>	Specifica il numero massimo di connessioni consentite sul server.	Il valore predefinito è 32767.
<b>Dimensione pool di thread di esecuzione</b>	Specifica il numero massimo di query che è possibile eseguire in parallelo in un determinato momento.	Il valore predefinito è 10.
<b>Timeout inattività connessione</b>	Specifica l'intervallo di tempo, in secondi, al termine del quale una connessione inattiva viene chiusa.	Il valore predefinito è 10800 secondi.
<b>Timeout inattività istruzione</b>	Specifica l'intervallo di tempo, in secondi, al termine del quale un'istruzione di query inattiva viene chiusa.	Il valore predefinito è 600 secondi.

### 30.1.7 Proprietà dei servizi di Web Intelligence

La categoria dei servizi Web Intelligence include i server seguenti:

- Adaptive Processing Server

- Server di elaborazione Web Intelligence

### Impostazioni di Adaptive Processing Server

Tabella 30 - 55: Parametri della riga di comando

Proprietà	Descrizione	Valore predefinito
Espansione a livello	<p>Specifica il livello con cui vengono recuperati i dati da query BEx.</p> <p>Per impostazione predefinita, le gerarchie non vengono espansate a un determinato livello. Livello00 è sempre il livello predefinito. Per cambiare questo comportamento, aggiungere il parametro alla riga di comando. Se si specifica un valore troppo elevato, Web Intelligence recupera tutti i dati della gerarchia e questo potrebbe influire sulle prestazioni e sulla stabilità del sistema.</p>	<p>-Dsap.sl.bics.expandToLevel=n</p> <p>n può essere qualsiasi numero intero compreso tra 0 e 99. Se n=0 o se questo parametro non viene specificato, per le gerarchie non verrà utilizzato il parametro Espansione a livello.</p>

Tabella 30 - 56: Proprietà del servizio di monitoraggio Web Intelligence

Proprietà	Descrizione	Valore predefinito
<b>Abilita monitoraggio</b>	Specifica se il monitoraggio è abilitato per il servizio.	TRUE
<b>Ritardo del loop del thread di monitoraggio (secondi)</b>	Specifica l'intervallo di tempo, espresso in secondi, tra i tentativi di esecuzione del ping dei client effettuati dal servizio.	300
<b>Timeout svuotamento risorse monitorate predefinite (in secondi)</b>	Specifica l'intervallo di tempo, espresso in secondi, in cui il servizio attende un client inattivo prima di svuotare la sessione del client.	1500
<b>Timeout scambio risorse monitorate predefinite (in secondi)</b>	Specifica l'intervallo di tempo, espresso in secondi, in cui il servizio attende un client inattivo prima di eseguire lo scambio della sessione del client sul disco rigido. È consigliabile specificare un valore inferiore al valore della proprietà Timeout svuotamento risorse monitorate predefinite.	600
<b>Abilitare i profili di servizio</b>		TRUE
<b>Abilitare il monitoraggio delle attività di servizio</b>		TRUE

Tabella 30 - 57: Proprietà del servizio di visualizzazione

Proprietà	Descrizione	Valore predefinito
<b>Timeout svuotamento motore di visualizzazione (in secondi)</b>	Specifica l'intervallo di tempo, espresso in secondi, in cui il servizio attende un client inattivo prima di svuotare la sessione del client.	1500
<b>Timeout scambio motore di visualizzazione (in secondi)</b>	Specifica l'intervallo di tempo, espresso in secondi, in cui il servizio attende un client inattivo prima di eseguire lo scambio della sessione del client sul disco rigido. È consigliabile specificare un valore inferiore al valore della proprietà <b>Timeout svuotamento motore di visualizzazione (in secondi)</b> .	600

Tabella 30 - 58: Proprietà del servizio Rebean

Proprietà	Descrizione	Valore predefinito
Nessuna proprietà di configurazione		

Tabella 30 - 59: Proprietà del servizio recupero documenti

Proprietà	Descrizione	Valore predefinito
Nessuna proprietà di configurazione		

Tabella 30 - 60: Proprietà del servizio DSL Bridge

Proprietà	Descrizione	Valore predefinito
<b>Timeout eliminazione motore DSL Bridge (in secondi)</b>	Specifica l'intervallo di tempo, espresso in secondi, in cui il servizio attende un client inattivo prima di svuotare la sessione del client.	1500

### Proprietà di Server di elaborazione Web Intelligence

Le proprietà di Server di elaborazione Web Intelligence sono raggruppate nei servizi seguenti:

- Information Engine
- Servizio principale Web Intelligence
- Servizio di elaborazione Web Intelligence
- Servizio comune Web Intelligence

Le impostazioni di soglia vengono descritte in tabelle separate.

Tabella 30 - 61: Proprietà di Information Engine Service

Proprietà	Descrizione	Valore predefinito
<b>Abilita cache elenco dei valori</b>	Specifica se la memorizzazione nella cache è abilitata per l'elenco dei valori in Server di elaborazione Web Intelligence.	TRUE
<b>Dimensioni batch elenco dei valori (voci)</b>	Specifica il numero massimo di voci, o valori, per ogni batch di elenco dei valori.	1000
<b>Dimensioni massime ordinamento personalizzato (voci)</b>	Specifica il numero massimo di voci nell'ordinamento personalizzato.	100
<b>Dimensioni massime cache universo (Universi)</b>	Specifica il numero di universi da memorizzare nella cache in Server di elaborazione Web Intelligence.	20
<b>Dimensioni LOV massime (voci)</b>	Specifica il numero massimo di voci, o valori, per ogni elenco di valori (LOV).	50000

Tabella 30 - 62: Proprietà del servizio principale di Web Intelligence

Proprietà	Descrizione	Valore predefinito
<b>Timeout prima della reinizializzazione (secondi)</b>	Specifica il periodo di tempo, in secondi, di inattività del server prima che venga interrotto e riavviato dall'agente SIA quando il numero totale di documenti elaborati è superiore al valore specificato dalla proprietà <b>Numero max. documenti prima della reinizializzazione</b> .	1500
<b>Timeout documento inattivo (secondi)</b>	Specifica il periodo di tempo, in secondi, prima dello spostamento della sessione di Server di elaborazione Web Intelligence. Quando il client non genera richieste in questo periodo di tempo, pertanto, la sessione viene spostata su disco rigido, in modo da liberare risorse per una sessione attiva.	300 L'intervallo valido è compreso tra 100 e 10000 secondi.

Proprietà	Descrizione	Valore predefinito
<b>Intervallo di polling del server (secondi)</b>	Specifica l'intervallo di tempo, in secondi, dopo il quale il server esegue il polling per nuove richieste di thread. Durante il polling, il server esegue operazioni di pulizia, quali lo spostamento di documenti inutilizzati per evitare che la memoria del server superi la soglia di memoria superiore.	120
<b>Numero max. documenti per utente</b>	Specifica il numero massimo di sessioni attive (documenti Web Intelligence) che è possibile associare a un utente in un determinato momento. Se il valore è 5, l'utente può quindi utilizzare fino a 5 sessioni attive alla volta.	5 L'intervallo valido è compreso tra 1 e 20.
<b>Numero max. documenti prima della reinizializzazione</b>	Specifica il numero di documenti Web Intelligence che è possibile elaborare prima che venga considerata la reinizializzazione del server. Se viene raggiunto il numero di documenti elaborati e il server è inattivo, il server viene chiuso e l'agente SIA avvia una nuova istanza del server. Vi è tuttavia un ritardo prima dell'avvio di una nuova istanza del server. Il ritardo viene definito dalla proprietà <b>Timeout prima della reinizializzazione</b> .	50
<b>Consenti errori di dimensione massima mappa</b>	Specifica se la proprietà <i>Numero max. connessioni</i> è limitata. Se questa proprietà è abilitata, il valore impostato per la proprietà <i>Numero max. connessioni</i> viene riconosciuto dal server. In caso contrario, la proprietà viene ignorata.	TRUE
<b>Timeout connessione inattiva (minuti)</b>	Specifica il periodo di tempo, in minuti, di attesa del server per una richiesta da una connessione inattiva. L'impostazione di un valore troppo basso può causare la chiusura prematura di una richiesta. L'impostazione di un valore troppo alto può causare l'accodamento delle richieste mentre il server rimane in attesa della chiusura delle richieste inattive.	20



Proprietà	Descrizione	Valore predefinito
<b>Numero max. connessioni</b>	<p>Specifica il numero massimo di sessioni simultanee che è possibile aprire contemporaneamente. Si tratta di un numero approssimativo, poiché questa impostazione non tiene conto delle sessioni inattive che vengono spostate né della sessione che viene creata per analizzare il numero di sessioni. Se viene raggiunto questo limite e non sono disponibili altri server per la gestione della richiesta, l'utente riceve un messaggio di errore.</p> <p><b>Nota:</b> è necessario che la proprietà <i>Consenti errori dimensione massima mappa</i> sia abilitata affinché il server riconosca questa proprietà.</p>	<p>50</p> <p>L'intervallo valido è compreso tra 5 e 65535.</p>
<b>Abilita analisi memoria</b>	<p>Specifica se l'analisi della memoria è abilitata. Se la proprietà è abilitata, le proprietà seguenti sono attive e riconosciute dal server.</p> <ul style="list-style-type: none"> <li>• <i>Soglia massima memoria</i></li> <li>• <i>Soglia superiore memoria</i></li> <li>• <i>Soglia inferiore memoria</i></li> </ul> <p>Quando la memoria del processo del server è superiore al valore di <i>Soglia superiore memoria</i>, l'unica operazione consentita è il salvataggio dei documenti. Quando la memoria del processo è superiore al valore di <i>Soglia massima memoria</i>, tutte le operazioni vengono interrotte e hanno esito negativo.</p>	TRUE
<b>Soglia inferiore memoria (MB)</b>	Specifica la soglia inferiore per l'utilizzo della memoria.	3500
<b>Soglia superiore memoria (MB)</b>	Specifica la soglia superiore per l'utilizzo della memoria.	4500
<b>Soglia massima memoria (MB)</b>	Specifica la soglia massima per l'utilizzo della memoria.	6000
<b>Abilita monitoraggio servizio APS</b>	Consente il monitoraggio del server da parte del servizio APS, ospitato in Adaptive Processing Server.	TRUE
<b>Errore di ping nuovo tentativo di conteggio su servizio APS</b>	Specifica il numero di tentativi di raggiungere il servizio APS da parte del server prima che venga stabilito che non è possibile raggiungerlo.	3

Proprietà	Descrizione	Valore predefinito
<b>Periodo thread monitoraggio servizio APS (secondi)</b>	Specifica il ritardo tra i tentativi di accesso al servizio APS.	300
<b>Abilita registri attività corrente</b>	<p>Specifica se nei file di registro del server devono essere generate analisi complete</p> <p><b>Nota:</b> questa proprietà deve essere abilitata solo a scopo di debug durante la risoluzione di problemi. Impostare su FALSE durante le normali attività.</p>	FALSE

Tabella 30 - 63: Proprietà del servizio di elaborazione di Web Intelligence

Proprietà	Descrizione	Valore predefinito
<b>Abilita utilizzo di URL HTTP</b>	Specifica se il server è in grado di accedere ai file archiviati in remoto.	TRUE
<b>Valore proxy</b>	Specifica l'indirizzo del server proxy di rete. È necessario specificare un valore solo se la rete dispone di un server proxy e si tenta di accedere a file archiviati in remoto.	Vuoto

Tabella 30 - 64: Proprietà del servizio comune di Web Intelligence

Proprietà	Descrizione	Valore predefinito
<b>Timeout cache (minuti)</b>	Specifica il periodo di tempo, in minuti, prima della cancellazione del contenuto della cache dei documenti. Il timeout dipende dalla data di accesso più recente per documento.	4370
<b>Intervallo pulizia cache documento (secondi)</b>	Specifica l'intervallo di tempo, in minuti, necessario per la scansione e il controllo della cache del documento rispetto alle impostazioni <i>Dimensione massima cache documento</i> , <i>Spazio di riduzione massimo cache documento</i> e <i>Numero max. documenti nella cache</i> .	120

Proprietà	Descrizione	Valore predefinito
<b>Disabilita condivisione cache</b>	Specifica se la condivisione cache è disabilitata. Per impostazione predefinita la condivisione cache è abilitata, pertanto tutte le istanze di Server di elaborazione Web Intelligence condividono la stessa cache. Se tuttavia si desidera disporre di una cache per istanza di Server di elaborazione Web Intelligence, è necessario abilitare questa proprietà.	FALSE
<b>Abilita cache documento</b>	Specifica se la cache del documento è abilitata. Se la proprietà è abilitata, la cache può essere precaricata con documenti Web Intelligence pianificati.	TRUE
<b>Abilita cache in tempo reale</b>	Specifica se la cache in tempo reale è abilitata. Se la proprietà è abilitata, la cache può essere caricata in modo dinamico. Server di elaborazione Web Intelligence, pertanto, memorizza nella cache i documenti Web Intelligence quando vengono visualizzati. Il server memorizza inoltre nella cache i documenti quando vengono eseguiti come processo pianificato, a condizione che la pre-cache sia stata abilitata nel documento.	TRUE
<b>Dimensione massima cache documenti (KB)</b>	Specifica la dimensione massima della cache dei documenti. Una volta raggiunto questo limite, la cache dei documenti viene cancellata in base alla proprietà <i>Spazio di riduzione massimo cache documento</i> .	1000000
<b>Spazio di riduzione massimo cache documenti (percentuale)</b>	Specifica la percentuale di cache svuotata per consentire la memorizzazione di nuove azioni e nuovi risultati nella cache. I documenti con l'ora dell'ultimo accesso meno recente vengono eliminati.	70
<b>Dimensioni flusso caratteri massime (MB)</b>	Specifica le dimensioni massime del flusso caratteri inviate al client Web Intelligence.  <b>Nota:</b> se la proprietà <b>Dimensioni flusso caratteri massime</b> viene superata, il documento Web Intelligence non viene creato e il client riceve un messaggio di errore.	5  L'intervallo valido è compreso tra 1 e 65535 MB.
<b>Dimensione massima flusso binario (MB)</b>	Specifica le dimensioni massime in MB di un flusso binario inviato al client Web Intelligence.  <b>Nota:</b> Se la proprietà <b>Dimensione massima flusso binario</b> viene superata, il documento Web Intelligence non viene creato e il client riceve un messaggio di errore.	50  L'intervallo valido è compreso tra 1 e 65535 MB.

Proprietà	Descrizione	Valore predefinito
<b>Directory immagini</b>	Specifica il percorso della directory delle immagini.	Vuoto
<b>Directory cache di output</b>	Specifica il percorso della cache.	Vuoto

Tabella 30 - 65: Proprietà generali

Proprietà	Descrizione	Valore predefinito
<b>Scadenza Single Sign-On (secondi)</b>	Specifica il tempo, in secondi, di validità di una connessione SSO prima della scadenza.	86400

### Argomenti correlati

- [Impostazioni della soglia di memoria di Web Intelligence Server](#)

## 30.1.7.1 Impostazioni della soglia di memoria di Web Intelligence Server

Nelle sezioni seguenti vengono descritte le conseguenze per Web Intelligence Server del raggiungimento dei valori Soglia massima memoria, Soglia superiore memoria o Soglia inferiore memoria.

### Soglia massima memoria

Se viene raggiunto il limite *Soglia massima memoria*, tutte le operazioni correnti vengono interrotte.

### Soglia superiore memoria

Se viene raggiunto il limite *Soglia superiore memoria*, vengono eseguite le azioni seguenti del server per liberare risorse e proteggere il server:

- Il server impedisce l'avvio di nuove connessioni e di altri thread che utilizzano memoria. È consentita solo l'opzione **Salva** per i documenti Web Intelligence. Gli utenti che richiedono un'azione che implica l'allocazione di memoria ricevono un messaggio di tipo Server occupato e la richiesta di salvare le modifiche in sospeso.
- Il server attiva la pulizia del sistema per liberare risorse sufficienti in modo che la quantità di memoria allocata sia inferiore al limite impostato dalla proprietà *Soglia superiore memoria*.
- Il server tenta di eliminare i documenti di sola lettura.
- Se non viene liberata memoria sufficiente durante la pulizia del sistema, il server inizia a chiudere i documenti in modalità "Visualizzazione". Il server inizia a chiudere i documenti in base al protocollo LIFO, pertanto il documento attivo più recente viene eliminato per primo dalla memoria. Il server continua a chiudere i documenti finché non viene raggiunto un livello sicuro, sulla base del calcolo

seguente: *Soglia superiore memoria - (20%\*Soglia superiore memoria)*. Ad esempio, se la proprietà Soglia superiore memoria è impostata su 4500 MB, il livello sicuro è:

$4500\text{MB} - .20*4500\text{MB} = 3600\text{MB}$

- Se non viene liberata memoria sufficiente durante la chiusura dei documenti in modalità "Visualizzazione", il server inizia a chiudere i restanti documenti aperti inclusi quelli in modalità "Modifica". Il server inizia a chiudere i documenti in base al protocollo LIFO, pertanto il documento attivo più recente viene eliminato per primo dalla memoria. Il server continua a chiudere i documenti finché non viene raggiunto un livello sicuro, sulla base del calcolo seguente: *Soglia superiore memoria - (20%\*Soglia superiore memoria)*. Ad esempio, se la proprietà Soglia superiore memoria è impostata su 4500 MB, il livello sicuro è:

$4500\text{MB} - .20*4500\text{MB} = 3600\text{MB}$

### Soglia inferiore memoria

Se viene raggiunto il limite *Soglia inferiore memoria*, il server sposta i documenti inattivi sul disco rigido, allocando la memoria aggiuntiva ai documenti attivi.

## 30.1.8 Proprietà dei servizi di Dashboards

### Proprietà dei Cache Server di Dashboards

Tabella 30 - 66: Proprietà dei servizi cache di Dashboards

Proprietà	Descrizione	Valore predefinito
<b>Dimensioni cache massime (KB)</b>	Specifica la quantità di spazio su disco rigido, in KB, utilizzata per la memorizzazione delle query nella cache. Se il server deve gestire quantità ingenti di query o query molto complesse, potrebbe essere necessario disporre di una cache di grandi dimensioni.	Il valore predefinito è 256000 KB.
<b>Timeout connessione inattiva (minuti)</b>	Specifica il periodo di tempo, in minuti, di attesa del Cache Server di Dashboards per una richiesta da una connessione inattiva. Non è in genere necessario modificare il valore predefinito.	Il valore predefinito è 15 minuti.
<b>Condividi dati tra i client</b>	Specifica se i dati di report sono condivisi tra client diversi.	Il valore predefinito è "TRUE".

Proprietà	Descrizione	Valore predefinito
<b>Dati meno recenti forniti ai client su richiesta (secondi)</b>	<p>Specifica il periodo di tempo, in secondi, di utilizzo dei dati memorizzati nella cache da parte del server per soddisfare le richieste da query su richiesta.</p> <p>Se il server riceve una richiesta che può essere soddisfatta con dati generati per una richiesta precedente e il tempo trascorso dalla generazione dei dati è inferiore al valore impostato, il server riutilizzerà tali dati per rispondere alla richiesta successiva. Il riutilizzo dei dati in questo modo migliora nettamente le prestazioni del sistema quando più utenti richiedono le stesse informazioni.</p> <p>Quando si imposta questo valore è opportuno considerare quanto sia importante che gli utenti ricevano dati aggiornati. Se è essenziale che tutti gli utenti ricevano dati aggiornati (poiché i dati importanti cambiano frequentemente), potrebbe essere necessario non consentire questo tipo di riutilizzo dei dati impostando il valore su 0.</p> <p><b>Nota:</b> È possibile impostare questa proprietà in un oggetto report. I valori specificati per tale oggetto sostituiscono le impostazioni del server.</p>	Il valore predefinito è 0 secondi.
<b>Timeout cache di protezione (minuti)</b>	Specifica l'intervallo di tempo, in minuti, in cui il server utilizza le credenziali di accesso, i parametri di query e le informazioni sulla connessione al database memorizzate nella cache per soddisfare le richieste prima di eseguire una query sul CMS.	Il valore predefinito è 20 minuti.
<b>Argomenti Java VM</b>	Indica gli argomenti della riga di comando che è possibile specificare per la JVM.	Xmx858M

### Proprietà del server di elaborazione di Dashboards

Tabella 30 - 67: Proprietà dei servizi di elaborazione di Dashboards

Proprietà	Descrizione	Valore predefinito
<b>Numero max. processi simultanei</b>	Specifica il numero massimo di processi indipendenti che possono essere eseguiti contemporaneamente sul server. Se il valore di questa proprietà viene impostato su "0", il server applica un valore adeguato, in base alla CPU e alla memoria del computer in cui il server è in esecuzione.	Il valore predefinito è 0.

Proprietà	Descrizione	Valore predefinito
<b>Durata massima dei processi per elemento secondario</b>	Specifica il numero massimo di processi che ogni processo secondario può gestire per durata.	Il valore predefinito è 10000.
<b>Numero massimo di elementi secondari preavviati</b>	Specifica il numero massimo di processi secondari preriavviati consentiti dal server. Se questo valore è troppo basso, il server crea processi secondari non appena vengono effettuate le richieste e potrebbero verificarsi latenze. Se questo valore è troppo elevato, è possibile che le risorse del sistema vengano impegnate inutilmente da processi secondari inattivi.	Il valore predefinito è 1.
<b>Timeout connessione inattiva (minuti)</b>	Specifica il periodo di tempo, in minuti, di attesa del server per una richiesta da una connessione inattiva. Non è in genere necessario modificare il valore predefinito.	Il valore predefinito è 15 minuti.
<b>Timeout connessione inattiva (minuti)</b>	Specifica l'intervallo di tempo, in minuti, in cui il server attende tra le richieste per un determinato processo.	Il valore predefinito è 15 minuti.
<b>Argomenti VM elemento secondario Java</b>	Indica gli argomenti della riga di comando specificati per i processi secondari creati dal server.	Xmx858M,Dswfinjection.lang.directory=%CommonJavaLibDir%,Dbusbusinessobjects.connectivity.directory=%CONNECTIO NSERVER_DIR%

Tabella 30 - 68: Proprietà del Servizio Single Sign-On

Proprietà	Descrizione	Valore predefinito
<b>Scadenza Single Sign-On (secondi)</b>	Specifica il tempo, in secondi, di validità di una connessione SSO prima della scadenza.	Il valore predefinito è 86400 secondi.





## Appendice sulle metriche server

### 31.1 Informazioni sull'appendice sulle metriche server

In questa appendice, se non diversamente specificato, il termine server fa riferimento a un server SAP BusinessObjects e non al computer in cui è installata e in esecuzione la piattaforma SAP BusinessObjects Business Intelligence.

Le metriche server non sono disponibili su server che non sono in esecuzione.

Oltre alle metriche descritte in questa appendice, l'applicazione di monitoraggio consente anche di modificare i seguenti stati del server:

Stato del server	Descrizione
<b>Stato di integrità</b>	<p>Lo stato di integrità indica lo stato generale di un server. I valori possibili sono:</p> <ul style="list-style-type: none"> <li>• 0 = Rosso (pericolo)</li> <li>• 1 = Ambra (attenzione)</li> <li>• 2 = Verde (Integro)</li> </ul>
<b>Stato abilitato del server</b>	<p>Questo stato indica se un server è abilitato o disabilitato. I valori possibili sono:</p> <ul style="list-style-type: none"> <li>• 0 = Disabilitato</li> <li>• 1 = Abilitato</li> </ul>
<b>Stato di esecuzione server</b>	<p>Questo stato indica lo stato di esecuzione di un server. I valori possibili sono:</p> <ul style="list-style-type: none"> <li>• 0 = INTERROTTO</li> <li>• 1 = AVVIO IN CORSO</li> <li>• 2 = INIZIALIZZAZIONE IN CORSO</li> <li>• 3 = IN ESECUZIONE</li> <li>• 4 = INTERRUZIONE IN CORSO</li> <li>• 5 = NON RIUSCITO</li> <li>• 6 = IN ESECUZIONE CON ERRORI</li> <li>• 7 = IN ESECUZIONE CON AVVISI</li> </ul>

### Argomenti correlati

- [Analisi delle specifiche dei server](#)

## 31.1.1 Metriche server comuni

Le metriche seguenti descrivono la macchina su cui è in esecuzione il server specificato.

Tabella 31 - 2: Metriche specifiche della macchina

Metrica	Descrizione
<b>Nome macchina</b>	Il nome host della macchina in cui viene eseguito il server.
<b>Sistema operativo</b>	Il sistema operativo della macchina in cui viene eseguito il server.
<b>Tipo CPU</b>	Il tipo di CPU della macchina in cui viene eseguito il server. Questa metrica non è disponibile negli Adaptive Processing Server o nei server del contenitore applicazioni Web (WACS).
<b>CPU</b>	Il numero di CPU disponibili per il server. In un hardware multi core, questa metrica potrebbe restituire il numero di CPU logiche e non il numero dei processori fisici. Questa metrica non è disponibile negli Adaptive Processing Server o nei server del contenitore applicazioni Web (WACS).
<b>RAM (MB)</b>	La quantità di memoria in megabyte disponibile nella macchina su cui è viene eseguito il server. Questa metrica non è disponibile negli Adaptive Processing Server o nei server del contenitore applicazioni Web (WACS).
<b>Ora locale</b>	L'ora locale.
<b>Dimensione disco (GB)</b>	La dimensione del disco su cui è installata la piattaforma BI, espressa in GB. Questa metrica non è disponibile negli Adaptive Processing Server o nei server del contenitore applicazioni Web (WACS).
<b>Spazio su disco utilizzato (GB)</b>	La quantità di spazio utilizzato nel disco su cui è installata la piattaforma BI, espressa in GB. Tale valore include lo spazio su disco utilizzato da altri programmi installati nel computer e non solo quello utilizzato dalla piattaforma BI. Questa metrica non è disponibile negli Adaptive Processing Server o nei server del contenitore applicazioni Web (WACS).

Le seguenti metriche descrivono il server SAP BusinessObjects specificato.

Tabella 31 - 3: Metriche specifiche del server

<b>Metrica</b>	<b>Descrizione</b>
<b>Server dei nomi</b>	Il nome e il numero di porta del server CMS su cui viene pubblicato l'indirizzo del server.
<b>Nome registrato</b>	Il nome interno del server. Non si tratta del nome visualizzato nella schermata "Server" della CMC.
<b>Versione</b>	La versione del server.
<b>Ora di inizio</b>	L'ora in cui il server è stato avviato per l'ultima volta.
<b>PID</b>	Il numero ID di processo univoco del server. Il sistema operativo della macchina in cui viene eseguito il server genera il PID. Il PID può essere utilizzato per identificare il server specifico.
<b>Nome host</b>	Un elenco separato da virgole di nomi di host correntemente utilizzati dal server.
<b>Indirizzo IP host</b>	Un elenco separato da virgole di indirizzi IP su cui si basano le richieste del server.
<b>Porta richiesta</b>	La porta dalla quale il server riceve le richieste da altri server. Se il server accetta richieste da più di un indirizzo IP, la porta richiesta per il server sarà sempre la stessa. Se qualsiasi altro processo utilizza la porta richiesta, il server non verrà avviato. Assicurarsi che gli altri processi non utilizzino questa porta.
<b>Thread server occupato</b>	Il numero di thread server correntemente occupati con una richiesta. Se questo numero corrisponde alla dimensione massima del pool di thread del server, il sistema non sarà in grado di elaborare ulteriori richieste in parallelo e le nuove richieste dovranno attendere finché i thread occupati diventano disponibili.

Tabella 31 - 4: Metriche di controllo

Metrica	Descrizione
<b>Numero corrente degli eventi di controllo in coda</b>	<p>Il numero di eventi di controllo registrati da un sistema di controllo, ma che non sono ancora stati recuperati dallo strumento di controllo CMS. Se questo numero aumenta senza limiti, potrebbe indicare che lo strumento di controllo non è configurato correttamente o che il sistema è in sovraccarico e che la generazione di eventi di controllo è più veloce della loro ricezione da parte dello strumento di controllo.</p> <p><b>Nota:</b> Quando si interrompe un server, prima disattivarlo e attendere che questa metrica arrivi a "0". In caso contrario, gli eventi di controllo potrebbero rimanere in coda e non riuscire a raggiungere l'archivio dati di controllo finché il server viene riavviato e il CMS esegue il relativo polling.</p>

Tabella 31 - 5: Metriche servizio di accesso

Metrica	Descrizione
<b>Directory di registrazione</b>	I file di registro per il server sono disponibili in questa posizione.

### 31.1.2 Metriche del Central Management Server

La tabella seguente descrive le metriche del server che vengono visualizzate nella schermata "Metriche" per Central Management Server (CMS).

Tabella 31 - 6: Metriche del Central Management Server

Metrica	Descrizione
<b>Connessione al database di controllo stabilita</b>	<p>Indica se il CMS è connesso in modo sicuro con il database di controllo. Un valore di "1" indica che c'è una connessione. Un valore pari a "0" indica che non c'è alcuna connessione al database di controllo. Se il CMS è un strumento di controllo, questo valore dovrebbe essere pari a "1". Se invece è pari a "0", individuare la causa della mancata connessione al database di controllo.</p>

<b>Metrica</b>	<b>Descrizione</b>
<b>Strumento di controllo CMS</b>	Indica se il CMS funge da strumento di controllo. Un valore di "1" indica che il CMS sta fungendo da strumento di controllo. Un valore di "0" indica che il CMS non sta fungendo da strumento di controllo.
<b>Nome connessione database di controllo</b>	Il nome della connessione al database di controllo. Non deve necessariamente essere il nome dello stesso database di controllo. Se questa metrica è vuota, non è possibile stabilire una connessione con il database di controllo.
<b>Nome utente database di controllo</b>	Il nome dell'account utente utilizzato per la connessione al database di controllo.
<b>Ultimo aggiornamento database di controllo</b>	La data e ora più recenti in cui il CMS ha iniziato a recuperare eventi da un sistema controllato. Se il CMS svolge la funzione di strumento di controllo, questa metrica deve indicare un orario molto vicino a quello in cui è stata caricata la schermata "Metriche". Se l'orario indicato precede di più di due ore quello in cui è stata caricata la schermata, è possibile che il controllo non funzioni correttamente.
<b>Durata ultimo ciclo di polling del thread di controllo (secondi)</b>	La durata dell'ultimo ciclo di polling in secondi. Indica il ritardo massimo con cui i dati dell'evento possono raggiungere il database di controllo durante il ciclo di polling precedente. <ul style="list-style-type: none"> <li>• Un valore inferiore a 20 minuti indica che il sistema funziona correttamente.</li> <li>• Un valore compreso tra 20 minuti e 2 ore indica che il sistema è occupato.</li> <li>• Un valore superiore a 2 ore indica che il sistema è estremamente occupato. Se questo stato persiste e il ritardo è troppo lungo, è consigliabile aggiornare la distribuzione a tutti i database di controllo per ricevere i dati a intervalli maggiori o ridurre il numero di eventi di controllo tracciati dal sistema.</li> </ul>
<b>Utilizzo thread di controllo</b>	La percentuale del ciclo di polling impiegata dallo strumento di controllo CMS per raccogliere i dati dai sistemi controllati. Viene restituito il tempo impiegato tra i due cicli di polling.  Se il valore raggiunge il 100%, lo strumento di controllo sta ancora raccogliendo dati dai sistemi controllati al momento in cui dovrebbe iniziare il prossimo ciclo di polling. Questo potrebbe causare ritardi negli eventi relativi al database dello strumento di controllo. Se l'utilizzo del thread raggiunge spesso il 100% e mantiene tale percentuale per vari giorni, è consigliabile aggiornare la distribuzione per consentire al database di controllo di ricevere dati a intervalli maggiori o ridurre il numero di eventi di controllo tracciati dal sistema.
<b>Server CMS cluster</b>	Elenco separato da punti e virgola dei nomi host e dei numeri di porta dei Central Management Server in esecuzione nel cluster.

<b>Metrica</b>	<b>Descrizione</b>
<b>Numero di sessioni stabilite da utenti simultanei</b>	Il numero totale di sessioni per utenti che utilizzano licenze simultanee.
<b>Numero di sessioni stabilite da utenti specifici</b>	Il numero totale di sessioni per utenti che utilizzano licenze specifiche.
<b>Numero massimo di sessioni utente dall'avvio</b>	Il numero massimo di sessioni simultanee di utenti che possono essere gestite dal CMS dall'avvio.
<b>Numero di sessioni stabilite dai server</b>	Il numero di sessioni simultanee create dai server della piattaforma BI con il CMS. Se questo numero è superiore a 250, creare un CMS aggiuntivo.
<b>Numero di sessioni stabilite da tutti gli utenti</b>	Il numero di sessioni utente simultanee gestite dal CMS al momento del caricamento della schermata "Metriche". Più questo numero è alto, maggiore sarà il numero di utenti che stanno utilizzando il sistema. Se questo numero è superiore a 250, creare un CMS aggiuntivo.
<b>Processi non riusciti</b>	Il numero di processi non riusciti nel sistema.
<b>Processi in sospeso</b>	Il numero di processi pianificati ma non pronti per l'esecuzione perché l'ora pianificata non è ancora giunta o l'evento pianificato non si è ancora verificato.
<b>Processi in esecuzione</b>	Il numero di processi attualmente in esecuzione.
<b>Processi completati</b>	Il numero di processi completati nel sistema.
<b>Processi in attesa</b>	Il numero di processi nel sistema pianificati e in attesa di risorse disponibili.
<b>Licenze utente simultanee</b>	Il numero di licenze utente simultaneo indicato dal codice.
<b>Licenze utenti specifici</b>	Il numero di licenze per utenti designati indicato dal codice di attivazione del prodotto.
<b>Data build</b>	La data di build del CMS.
<b>Nome connessione database di sistema</b>	Il nome della connessione al database di sistema CMS. Non deve necessariamente essere il nome dello stesso database di sistema CMS.
<b>Nome server database di sistema</b>	Il nome del server su cui il database di sistema CMS è in esecuzione. Non deve necessariamente essere il nome dello stesso database di sistema CMS.
<b>Nome utente database di sistema</b>	Il nome dell'account utente utilizzato per la connessione al database di sistema CMS.
<b>Nome origine dati</b>	Il nome della connessione al database di sistema CMS.

<b>Metrica</b>	<b>Descrizione</b>
<b>Numero build</b>	Il numero di build del CMS. Tale numero può essere utilizzato per identificare la versione della piattaforma SAP BusinessObjects Business Intelligence installata.
<b>Versione prodotto</b>	La versione prodotto del CMS.
<b>Versione risorsa</b>	La versione risorsa del CMS.
<b>Tempo medio di risposta a commit dall'avvio (msec)</b>	Il periodo di tempo medio in millisecondi impiegato dal CMS per eseguire le operazioni di commit dal momento di avvio del server. Un tempo di risposta superiore a 1000 millisecondi potrebbe indicare la necessità di regolare il CMS o il database di sistema CMS.
<b>Tempo medio di risposta alle query dall'avvio (msec)</b>	Il periodo di tempo medio in millisecondi impiegato dal CMS per eseguire le operazioni di query dal momento di avvio del server. Un tempo di risposta superiore a 1000 millisecondi potrebbe indicare la necessità di regolare il CMS o il database di sistema CMS.
<b>Tempo di risposta a commit più lungo dall'avvio (msec)</b>	Il periodo di tempo più lungo in millisecondi impiegato dal CMS per eseguire le operazioni di commit dal momento di avvio del server. Un tempo di risposta superiore a 10000 millisecondi potrebbe indicare la necessità di regolare il CMS o il database di sistema CMS.
<b>Tempo di risposta alle query più lungo dall'avvio (msec)</b>	Il periodo di tempo più lungo in millisecondi impiegato dal CMS per eseguire le operazioni di query dall'avvio del server. Un tempo di risposta superiore a 10000 millisecondi potrebbe indicare la necessità di regolare il CMS o il database di sistema CMS.
<b>Numero di commit dall'avvio</b>	Il numero di commit al database di sistema CMS dal momento di avvio del server.
<b>Numero di query dall'avvio</b>	Il numero totale di query al database dal momento di avvio del server. Un numero alto potrebbe indicare in sistema più attivo o in sovraccarico.
<b>Numero di accessi dall'avvio</b>	Il numero di accessi dal momento di avvio del server. Un numero alto potrebbe indicare in sistema più attivo o in sovraccarico.
<b>Connessioni database di sistema stabilite</b>	Il numero di connessioni al database di sistema CMS stabilite dal CMS. Se viene persa una connessione a un database, il CMS tenterà di ripristinarla. Se il numero di connessioni stabilite con il database è sensibilmente inferiore al numero di connessioni al database di sistema specificato dalla proprietà <b>Connessioni richieste al database di sistema</b> (area "Servizio Central Management" della schermata "Proprietà"), è possibile che il CMS non sia in grado di stabilire connessioni aggiuntive e che il funzionamento del sistema non sia ottimale. Una possibile soluzione è configurare il server database in modo da consentire più connessioni per il CMS.

<b>Metrica</b>	<b>Descrizione</b>
<b>Connessioni database di sistema utilizzate correntemente</b>	Il numero di connessioni al database di sistema CMS correntemente utilizzate dal CMS. Il numero di connessioni correntemente utilizzate potrebbe essere inferiore o uguale al numero di connessioni stabilite con il database di sistema. La corrispondenza per un certo periodo di tempo tra il numero di connessioni stabilite e il numero di connessioni utilizzate potrebbe indicare un collo di bottiglia. Aumentare il valore della proprietà <b>Connessioni richieste al database di sistema</b> nella schermata "Proprietà" potrebbe migliorare le prestazioni del CMS. Anche regolare il database di sistema CMS potrebbe migliorare le prestazioni.
<b>Richieste database di sistema in sospeso</b>	Il numero di richieste per le quali il database di sistema CMS è in attesa di una connessione disponibile. Se questo numero è alto, considerare di aumentare il valore per la proprietà <b>Connessioni richiesta al database di sistema</b> . Anche regolare il database di sistema CMS potrebbe migliorare le prestazioni.
<b>Numero di oggetti nella cache di sistema di CMS</b>	Il numero totale di oggetti correntemente nella cache di sistema del CMS.
<b>Numero di oggetti nel database di sistema di CMS</b>	Il numero totale di oggetti correntemente nel database di sistema del CMS.
<b>Account utente simultanei esistenti</b>	Il numero totale di utenti esistenti con licenze simultanee in cluster.
<b>Account utente specifici esistenti</b>	Il numero totale di utenti esistenti con licenze specifiche in cluster.

### 31.1.3 Metriche di Connection Server

Le seguenti metriche sono specifiche di Connection Server.



Tabella 31 - 7: Metriche del servizio di connettività

Metrica	Descrizione
<b>Origini dati</b>	<p>Vengono elencate in una tabella le origini dati attivate tramite la pagina "Proprietà". Per ogni livello di rete e coppia di database vengono visualizzate le seguenti informazioni:</p> <ul style="list-style-type: none"> <li>• "Stato"("Caricato"o "Non riuscito"): stato attuale del driver</li> <li>• "Connessioni disponibili: numero di connessioni del pool utilizzabili"</li> <li>• "Processi (CORBA): numero di processi in elaborazione (distribuzione 2-tier)"</li> <li>• "Processi (HTTP): numero di processi in elaborazione (distribuzione livello Web)"</li> </ul> <p><b>Nota:</b> Per ulteriori informazioni sui pool di connessioni, consultare il <i>Manuale dell'accesso ai dati</i>.</p>

### 31.1.4 Metriche di Event Server

La tabella seguente descrive le metriche del server che vengono visualizzate nella schermata "Metriche" per Event Server.

Tabella 31 - 8: Metriche servizio eventi

Metrica	Descrizione
<b>Elenco di file monitorati</b>	Una tabella contenente i file attualmente monitorati da Event Server. Nella colonna "Nome file" sono visualizzati il nome e il percorso del file. Nella colonna "Ora ultima notifica" è visualizzato l'indicatore di data/ora più recente relativo al momento in cui il server ha eseguito un polling e ha rilevato che il file esiste.
<b>File monitorati</b>	Il numero totale di file monitorati da Event Server.

### 31.1.5 Metriche del File Repository Server

La tabella seguente descrive le metriche del server che vengono visualizzate nella schermata "Metriche" per Input/Output File Repository Server.

Tabella 31 - 9: Metriche del servizio archivio file

<b>Metrica</b>	<b>Descrizione</b>
<b>File attivi</b>	Il numero di file nel File Repository Server a cui è stato effettuato l'accesso.
<b>Dati scritti (MB)</b>	Il numero totale di megabyte scritti su file nel server.
<b>Dati inviati (MB)</b>	Il numero complessivo di megabyte letti dai file nel server.
<b>Elenco di file attivi</b>	Una tabella in cui sono indicati i file presenti nel File Repository Server a cui è stato effettuato l'accesso.
<b>Connessioni attive</b>	Il numero totale di connessioni attive dai client e verso altri server.
<b>Spazio su disco disponibile nella directory principale (GB)</b>	Quantità totale, espressa in gigabyte, di spazio disponibile sul disco contenente il file eseguibile del server.
<b>Spazio su disco libero nella directory principale (GB)</b>	La quantità totale di spazio libero sul disco contenente il file eseguibile del server, in gigabyte.
<b>Spazio su disco totale nella directory principale (GB)</b>	Quantità totale, espressa in gigabyte, di spazio disponibile sul disco contenente il file eseguibile del server.
<b>Spazio su disco disponibile nella directory principale (%)</b>	Quantità, espressa in percentuale, di spazio disponibile su disco contenente il file eseguibile del server.

### 31.1.6 Metriche di Adaptive Processing Server

La tabella seguente descrive le metriche del server che vengono visualizzate nella schermata "Metriche" per Adaptive Processing Server.

Tabella 31 - 10: Metriche di Adaptive Processing Server

<b>Metrica</b>	<b>Descrizione</b>
<b>Thread nel livello di trasporto</b>	Il numero totale di thread in tutti i pool di thread del livello di trasporto.
<b>Dimensioni pool di thread livello di trasporto</b>	Il numero totale di thread livello di trasporto condivisi. Questi thread possono essere utilizzati da qualsiasi servizio ospitato in Adaptive Processing Server.
<b>Processori disponibili</b>	Il numero di processori disponibili per la Java Virtual Machine (JVM) in cui viene eseguito il server.
<b>Memoria massima (MB)</b>	La quantità massima di memoria, in megabyte, che Java Virtual Machine tenterà di utilizzare
<b>Memoria libera (MB)</b>	La quantità di memoria, in megabyte, disponibile per l'allocazione di nuovi oggetti da parte di JVM.
<b>Memoria totale (MB)</b>	La quantità totale di memoria, in megabyte, in Java Virtual Machine. Questo valore può variare nel tempo, in base all'ambiente di host.
<b>Percentuale utilizzo CPU (ultimi 5 minuti)</b>	La percentuale del tempo totale della CPU utilizzato dal server durante i cinque minuti precedenti. Ad esempio, se un singolo thread utilizza una CPU completa per un sistema a quattro CPU, l'utilizzo corrisponde al 25%. Vengono considerati tutti i processori allocati alla JVM. Un valore superiore all'80% può indicare un collo di bottiglia della CPU.
<b>Percentuale utilizzo CPU (ultimi 15 minuti)</b>	La percentuale del tempo totale della CPU utilizzato dal server durante i quindici minuti precedenti. Ad esempio, se un singolo thread utilizza una CPU completa per un sistema a quattro CPU, l'utilizzo corrisponde al 25%. Vengono considerati tutti i processori allocati alla JVM. Un valore superiore al 70% può indicare un collo di bottiglia.
<b>Percentuale di sistema arrestato durante GC (ultimi 5 minuti)</b>	<p>Percentuale di sistema arrestato durante l'esecuzione di Garbage Collection (GC) negli ultimi cinque minuti. In questo stato, tutti i servizi APS vengono bloccati quando la macchina virtuale esegue un'operazione critica di garbage collection che richiede accesso esclusivo.</p> <p>In genere, un valore basso da una cifra dovrebbe rappresentare il comportamento normale, anche durante una fase di caricamento. Un valore a due cifre ripetuto può indicare un problema di throughput basso che deve essere esaminato.</p>

Metrica	Descrizione
<b>Percentuale di sistema arrestato durante GC (ultimi 15 minuti)</b>	<p>Percentuale di sistema arrestato durante l'esecuzione di Garbage Collection (GC) negli ultimi quindici minuti. In questo stato, tutti i servizi APS vengono bloccati quando la macchina virtuale esegue un'operazione critica di garbage collection che richiede accesso esclusivo.</p> <p>In genere, un valore basso da una cifra dovrebbe rappresentare il comportamento normale, anche durante una fase di caricamento. Un valore a due cifre ripetuto può indicare un problema di throughput basso che deve essere esaminato.</p>
<b>Numero di errori di pagina durante GC (ultimi 5 minuti)</b>	Il numero di errori di pagina che si sono verificati durante l'esecuzione di Garbage Collection nei cinque minuti precedenti. Qualsiasi valore superiore a 0 indica un sistema in sovraccarico e condizioni di memoria scarsa.
<b>Numero di errori di pagina durante GC (ultimi 15 minuti)</b>	Il numero di errori di pagina che si sono verificati durante l'esecuzione di Garbage Collection nei quindici minuti precedenti. Qualsiasi valore superiore a 0 indica un sistema in sovraccarico e condizioni di memoria scarsa.
<b>Numero di GC completi</b>	Il numero di Garbage Collection completati dall'avvio del server. Un incremento rapido di questo valore potrebbe indicare un sistema con scarse condizioni di memoria.
<b>Conteggio conflitti blocco JVM</b>	Il numero di oggetti sincronizzati i cui thread sono in attesa di accesso. Qualsiasi valore di molto superiore a 0 potrebbe indicare thread che non possono essere più eseguiti. Avviare un dump del thread per ottenere ulteriori informazioni sulla causa del problema.
<b>Informazioni debug JVM</b>	Debug delle informazioni su SAP Java Virtual Machine, incluso lo stato, la porta e il client allegato, se disponibile.
<b>Informazioni versione JVM</b>	Informazioni di versione su SAP Java Virtual Machine.
<b>Contatore thread in stallo JVM</b>	Il numero di thread in stallo. Qualsiasi valore superiore a 0 indica thread che non possono essere più eseguiti. Avviare un dump del thread per ottenere ulteriori informazioni sulla causa del problema.
<b>Flag analisi JVM</b>	I flag di analisi correntemente attivati per JVM. Indica il livello di analisi di JVM.
<b>Servizi</b>	Un elenco separato da virgole dei servizi ospitati dal server.

Tabella 31 - 11: Metriche del servizio DSL Bridge

Metrica	Descrizione
<b>DSLServiceMetrics.queryCount</b>	Numero di richieste dati aperte tra i client e il servizio

<b>Metrica</b>	<b>Descrizione</b>
<b>DSLServiceMetrics.activeConnectionCount</b>	Numero di connessioni correntemente aperte tra i client e il servizio.
<b>DSLServiceMetrics.activeSessionCount</b>	Numero di sessioni correntemente aperte tra i client e il servizio.
<b>DSLServiceMetrics.activeOLAPConnectionCount</b>	Numero di connessioni attualmente aperte tra i client OLAP e il servizio.

Tabella 31 - 12: Metriche del servizio proxy controllo client

<b>Metrica</b>	<b>Descrizione</b>
<b>Numero di eventi di controllo ricevuti dall'avvio del server</b>	Il numero di eventi di controllo client ricevuti dal servizio dal suo avvio. Questa metrica può essere utilizzata per verificare che il controllo client sia stato configurato correttamente. I valori superiori a "0" indicano che gli eventi di controllo client vengono instradati correttamente attraverso questo servizio di controllo client.

Tabella 31 - 13: Metriche del servizio di ricerca piattaforma

<b>Metrica</b>	<b>Descrizione</b>
<b>Numero di tentativi di estrazione riusciti dall'avvio del servizio</b>	Numero di tentativi di estrazione dei documenti riusciti dall'avvio del servizio di ricerca piattaforma.
<b>Data/ora ultimo aggiornamento indice</b>	La data e l'ora dell'ultimo aggiornamento dell'indice.
<b>Data/ora ultima generazione archivio contenuti</b>	La data e l'ora in cui è stato generato l'ultimo archivio contenuti.
<b>Numero di tentativi di estrazione non riusciti dall'avvio del servizio</b>	Numero di tentativi di estrazione dei documenti non riusciti dall'avvio del servizio di ricerca piattaforma.
<b>Servizio disponibile</b>	TRUE se il servizio è disponibile. In caso contrario, FALSE.
<b>Indicizzazione in esecuzione</b>	TRUE se l'indicizzazione è in corso. In caso contrario, FALSE.
<b>Numero di documenti indicizzati</b>	Visualizza il numero di documenti indicizzati dall'avvio del servizio.

Tabella 31 - 14: Metriche dei servizi di analisi multidimensionali

<b>Metrica</b>	<b>Descrizione</b>
<b>Conteggio sessione</b>	Numero corrente di connessioni dai client MDAS al server.
<b>Conteggio cubi</b>	Numero di origini dati utilizzate per fornire i dati alle connessioni non ancora scadute.
<b>Conteggio query</b>	Numero di richieste dati aperte tra i client MDAS e il server.

Tabella 31 - 15: Metriche del servizio Data Federation

<b>Metrica</b>	<b>Descrizione</b>
<b>Numero di query in esecuzione</b>	Numero totale di query in esecuzione (che utilizzano memoria o meno).
<b>Numero di connessioni</b>	Numero totale di connessioni utente al motore delle query di Data Federation.
<b>Byte totali trasferiti dalle origini dati</b>	Quantità di dati letti dalle origini dati (in byte).
<b>Record totali trasferiti dalle origini dati</b>	Numero totale di righe lette dalle origini dati.
<b>Byte totali prodotti dall'esecuzione query</b>	Quantità di dati prodotti come output di query (in byte).
<b>Record totali prodotti dall'esecuzione query</b>	Numero totale di righe prodotte come output di query.
<b>Numero di query che utilizzano memoria</b>	Numero totale di query in esecuzione che utilizzano memoria.
<b>Byte totali di memoria utilizzati dall'esecuzione query</b>	Quantità di memoria attualmente utilizzata dalle query in esecuzione (in byte).
<b>Byte totali di disco utilizzati dall'esecuzione query</b>	Spazio sul disco attualmente utilizzato dalle query in esecuzione (in byte).
<b>Numero di query che utilizzano il disco</b>	Numero totale di query in esecuzione che utilizzano il disco.
<b>Numero di query che attendono risorse</b>	Numero totale di query in esecuzione attualmente in attesa di esecuzione.
<b>Numero di thread attivi</b>	Numero totale di thread attivi utilizzati per l'esecuzione delle richieste.

Metrica	Descrizione
<b>Byte totali di memoria utilizzati dalla cache di metadati</b>	Quantità di memoria utilizzata per la cache di configurazione di metadati, statistiche e connettori (in byte).
<b>Numero di query non riuscite</b>	Numero totale di query non riuscite (eccezione generata).
<b>Numero di query nel passaggio di analisi query</b>	Numero totale di query in esecuzione attualmente in fase di analisi.
<b>Numero di query nel passaggio di ottimizzazione query</b>	Numero totale di query in esecuzione attualmente in fase di ottimizzazione.
<b>Numero di query nel passaggio di esecuzione query</b>	Numero totale di query in esecuzione attualmente in funzione.
<b>Numero di connettori caricati</b>	Numero totale di connettori caricati nel servizio.
<b>Numero di connessioni attive per i connettori caricati</b>	Numero totale di connessioni attive per i connettori caricati nel servizio.
<b>Il servizio Data Federation è disponibile</b>	"TRUE" se il servizio è disponibile. In caso contrario, "FALSE".

Tabella 31 - 16: Metriche del servizio di connettività

Metrica	Descrizione
<b>Origini dati</b>	<p>Vengono elencate in una tabella le origini dati attivate tramite la pagina "Proprietà". Per ogni livello di rete e coppia di database vengono visualizzate le seguenti informazioni:</p> <ul style="list-style-type: none"> <li>• Stato ("Caricato" o "Non riuscito"): stato corrente del driver</li> <li>• Connessioni disponibili: numero di connessioni del pool utilizzabili</li> <li>• Processi (CORBA): numero di processi in elaborazione (distribuzione 2-tier)</li> <li>• Processi (HTTP): numero di processi in elaborazione (distribuzione livello Web)</li> </ul> <p>Per ulteriori informazioni sui pool di connessioni, consultare il <i>Manuale dell'accesso ai dati</i>.</p>

Tabella 31 - 17: Metriche del servizio di monitoraggio

Metrica	Descrizione
<b>Tempo di calcolo medio stato controllo per gli ultimi 15 cicli (msec)</b>	Tempo medio necessario per il calcolo dello stato di controllo negli ultimi 15 cicli, per questa istanza del servizio di monitoraggio.

Metrica	Descrizione
<b>Numero di metriche create dall'utente</b>	Numero totale di metriche create dall'utente nel cluster, per tutti gli utenti.
<b>Numero di controlli</b>	Numero totale di controlli nel cluster, inclusi quelli disabilitati e abilitati.
<b>serviceBean.monitoringAppPropEnabled</b>	TRUE se l'applicazione di monitoraggio è abilitata. In caso contrario, FALSE. Questa metrica corrisponde all'impostazione nella pagina Proprietà dell'applicazione di monitoraggio della CMC.
<b>Intervallo di aggiornamento metriche di monitoraggio (secondi)</b>	Intervallo di aggiornamento attualmente utilizzato da questa istanza del servizio di monitoraggio. Quando viene avviato il servizio, questa metrica viene inizializzata sull'impostazione nella pagina Proprietà dell'applicazione di monitoraggio della CMC in quel momento. La metrica può pertanto essere talvolta diversa dall'impostazione corrente nella pagina CMC.
<b>Servizio disponibile</b>	TRUE se il servizio di monitoraggio è attivo. In caso contrario, FALSE. È attivo un solo servizio di monitoraggio nel cluster.
<b>Numero di metriche con tendenza</b>	Numero totale di metriche attualmente registrate nel database di monitoraggio.

Tabella 31 - 18: Metriche dei servizi applicazioni Web BEx

Metrica	Descrizione
<b>Conteggio sessione</b>	Conteggio del numero totale di sessioni attive all'interno di un servizio applicazioni Web BEx.

### 31.1.7 Metriche del server del contenitore di applicazioni Web

La tabella seguente descrive le metriche del server che vengono visualizzate nella schermata "Metriche" per i server del contenitore di applicazioni Web.

**Nota:**

i server del contenitore di applicazioni Web dispongono inoltre di tutte le metriche descritte nella sezione Metriche di Adaptive Processing Server.



Tabella 31 - 19: Metriche del server del contenitore di applicazioni Web

Metrica	Descrizione
<b>Elenco di connettori WACS in esecuzione</b>	Un elenco di tutti i connettori in esecuzione sul server. Se non si visualizzano tutti i connettori (HTTP, HTTPS e HTTP tramite proxy), indica che il connettore non è abilitato o che si è verificato un errore durante l'avvio.
<b>Errore connettori WACS all'avvio</b>	Eventuali connettori su cui si è verificato un errore. Se true, almeno un connettore non si è avviato. Se false, tutti i connettori sono in esecuzione. Non eseguire un server quando non è stato possibile avviare uno o più connettori. È necessario risolvere i problemi del server per assicurarsi che tutti i connettori vengano avviati correttamente.

#### Argomenti correlati

- [Metriche di Adaptive Processing Server](#)

## 31.1.8 Metriche di Adaptive Job Server

Tabella 31 - 20: Metriche di Job Server

Metrica	Descrizione
<b>Richieste processi ricevute</b>	Il numero di processi che dovrebbero essere stati eseguiti sul server.
<b>Processi simultanei</b>	Il numero di processi che sono correntemente in esecuzione sul server. Se questo numero è alto, il server è occupato.
<b>Processi di picco</b>	Il numero massimo di processi simultanei che sono stati eseguiti contemporaneamente sul server. Questo numero non scende fino al riavvio del server.
<b>Creazioni processi non riuscite</b>	Il numero di processi non riusciti nel server.
<b>Directory temporanea</b>	La directory in cui vengono creati i file temporanei. Questo può essere specificato nella schermata "Proprietà" per il server.  Se questa directory non dispone di spazio su disco sufficiente possono verificarsi dei problemi.

<b>Metrica</b>	<b>Descrizione</b>
<b>Impostazioni predefinite destinazione file system valide</b>	"TRUE" se il server è in grado di inviare documenti alla destinazione file system specificata nella schermata "Destinazione" per il server. In caso contrario, "FALSE".
<b>Impostazioni predefinite destinazione FTP valide</b>	"TRUE" se il server è in grado di inviare documenti alla destinazione FTP specificata nella schermata "Destinazione" del server. In caso contrario, "FALSE".
<b>Impostazioni predefinite destinazione Posta in arrivo valide</b>	"TRUE" se il server è in grado di inviare oggetti alla destinazione Posta in arrivo specificata nella schermata "Destinazione" del server. In caso contrario, "FALSE".
<b>Impostazioni predefinite destinazione posta elettronica valide</b>	"TRUE" se il server è in grado di inviare oggetti alla destinazione posta elettronica specificata nella schermata "Destinazione" del server. In caso contrario, "FALSE".
<b>Servizi di pianificazione</b>	Una tabella che visualizza i servizi in esecuzione sul server.
<b>Elementi secondari</b>	Una tabella che visualizza i processi secondari in esecuzione sul server.
<b>Impostazioni predefinite di destinazione SAP StreamWork valide</b>	"TRUE" se il server è in grado di inviare oggetti alla destinazione SAP StreamWork specificata nella schermata "Destinazione" del server. In caso contrario, "FALSE".

Nella tabella che segue sono indicate le metriche per ogni servizio di pianificazione in esecuzione sul server.

Tabella 31 - 21: Metriche del servizio di pianificazione

<b>Metrica</b>	<b>Descrizione</b>
<b>Servizio di pianificazione</b>	Il nome del servizio.
<b>Richieste processi ricevute</b>	Il numero di processi che dovrebbero essere stati eseguiti nel servizio.
<b>Processi simultanei</b>	Il numero di processi che sono correntemente in esecuzione nel servizio. Se questo numero è alto, il servizio è occupato.
<b>Processi di picco</b>	Il numero massimo di processi simultanei che sono stati eseguiti contemporaneamente nel servizio.
<b>N. massimo consentito processi simultanei</b>	Il numero di processi indipendenti simultanei (processi secondari) consentiti dal server.  Questo può essere specificato nella schermata "Proprietà" per il server.

<b>Metrica</b>	<b>Descrizione</b>
<b>Creazioni processi non riuscite</b>	Il numero di processi non riusciti nel servizio.

Nella tabella che segue sono indicate le metriche per ogni processo secondario in esecuzione sul server.

*Tabella 31 - 22: Metriche secondarie*

<b>Metrica</b>	<b>Descrizione</b>
<b>Servizio di pianificazione</b>	Il nome dell'elemento secondario.
<b>PID</b>	L'identificatore del processo secondario.
<b>Richieste processi ricevute</b>	Il numero di processi che dovrebbero essere stati eseguiti nel processo secondario.
<b>Processi simultanei</b>	Il numero di processi che sono correntemente in esecuzione nel processo secondario. Generalmente, questo numero deve essere "1".
<b>Processi di picco</b>	Il numero massimo di processi simultanei che sono stati eseguiti contemporaneamente nel processo secondario.
<b>Numero max. processi consentiti</b>	Il numero di processi simultanei consentiti dal processo secondario.
<b>Errori di comunicazione</b>	Il numero di errori di comunicazione che si sono verificati con l'Adaptive Job Server principale. Se questo numero è alto, il processo secondario verrà riavviato.
<b>Inizializzazione in corso</b>	"TRUE" se il processo secondario è in fase di inizializzazione. In caso contrario, "FALSE".
<b>Arresto in corso</b>	"TRUE" se il processo secondario è in fase di arresto. In caso contrario, "FALSE".

### 31.1.9 Metriche di Crystal Reports Server

La tabella seguente descrive le metriche del server che vengono visualizzate nella schermata "Metriche" per i server di elaborazione Crystal Reports e Crystal Reports 2013.

Tabella 31 - 23: Metriche di Crystal Reports Processing Server

<b>Metrica</b>	<b>Descrizione</b>
<b>Processi aperti</b>	Tabella che elenca i processi attualmente eseguiti sul server. La tabella indica l'ID e il nome del documento, il nome dell'utente che esegue il processo, la data dell'ultimo accesso al documento e per quanto tempo il processo è stato in esecuzione.
<b>Numero di richieste servite</b>	Numero totale delle richieste servite dal server dopo l'avvio.
<b>Numero di processi aperti</b>	Il numero di processi attualmente elaborati dal server e dai suoi processi secondari.
<b>Tipo di oggetto</b>	Il tipo di InfoObject gestito generalmente dal server. Il valore di questa metrica non cambia.
<b>Tempo di elaborazione medio (ms)</b>	Il tempo medio, in millisecondi, impiegato dal server per elaborare le ultime 500 richieste ricevute. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.
<b>Tempo di elaborazione massimo (ms)</b>	Il tempo massimo, in millisecondi, impiegato dal server per elaborare una delle ultime 500 richieste. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.
<b>Tempo di elaborazione minimo (msec)</b>	Il tempo minimo, in millisecondi, impiegato dal server per elaborare una delle ultime 500 richieste. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.
<b>Numero di richieste in coda</b>	Il numero di richieste in attesa di essere elaborate o in fase di elaborazione. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.
<b>Nome DLL oggetto</b>	Il nome del plug-in di elaborazione per il server. Il valore di questa metrica non cambia.
<b>Numero di connessioni aperte</b>	Numero di connessioni attualmente aperte tra il server e i client.
<b>Frequenza errori di richieste</b>	La percentuale delle ultime 500 richieste ricevute che il server non è riuscito a elaborare.
<b>Dati trasferiti (KB)</b>	Quantità totale di dati, in kilobyte, trasferiti ai client dopo l'avvio del server.
<b>Numero di richieste non riuscite</b>	Numero di richieste che il server non è stato in grado di completare dopo l'avvio.
<b>Numero massimo di processi secondari</b>	Il numero massimo di processi secondari simultanei consentiti sul server.

La tabella seguente descrive le metriche del server che vengono visualizzate nella schermata "Metriche" per i Crystal Reports Cache Server.

Tabella 31 - 24: Metriche di Crystal Reports Cache Server

<b>Metrica</b>	<b>Descrizione</b>
<b>Riscontri cache (%)</b>	La percentuale delle ultime 500 richieste servite con dati cache.
<b>Server di elaborazione connessi</b>	Tabella che elenca i server di elaborazione Crystal Reports nella propria distribuzione. La tabella include il nome del server e il numero di connessioni con il server attualmente aperte.
<b>Numero di richieste servite</b>	Numero totale delle richieste servite dal server dopo l'avvio.
<b>Tipo di oggetto</b>	Il tipo di InfoObject gestito generalmente dal server. Il valore di questa metrica non cambia.
<b>Tempo di elaborazione medio (msec)</b>	Il tempo medio, in millisecondi, impiegato dal server per elaborare le ultime 500 richieste ricevute. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.
<b>Tempo di elaborazione massimo (msec)</b>	Il tempo massimo, in millisecondi, impiegato dal server per elaborare una delle ultime 500 richieste. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.
<b>Tempo di elaborazione minimo (msec)</b>	Il tempo minimo, in millisecondi, impiegato dal server per elaborare una delle ultime 500 richieste. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.
<b>Numero di richieste in coda</b>	Il numero di richieste in attesa di essere elaborate o in fase di elaborazione. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.
<b>Nome DLL oggetto</b>	Il nome del plug-in di elaborazione per il server. Il valore di questa metrica non cambia.
<b>Dimensione della cache</b>	La quantità di dati, in kilobyte, attualmente memorizzati nella cache del server sul disco.
<b>Numero di connessioni aperte</b>	Numero di connessioni attualmente aperte tra il server e i client.
<b>Dati trasferiti (KB)</b>	Quantità totale di dati, in kilobyte, trasferiti ai client dopo l'avvio del server.

La tabella seguente descrive le metriche del server che vengono visualizzate nella schermata "Metriche" per i Report Application Server di Crystal Reports 2013.

Tabella 31 - 25: Metriche del Report Application Server di Crystal Reports 2013

<b>Metrica</b>	<b>Descrizione</b>
<b>metric_currentdoccount</b> <b>Nota:</b> Questa metrica viene visualizzata come “document_s_” nella pagina Monitoraggio della CMC.	Numero di documenti attualmente elaborati dal server.
<b>metric_totaldoccount</b> <b>Nota:</b> Questa metrica viene visualizzata come “document_s_” nella pagina Monitoraggio della CMC.	Numero di documenti elaborati dal server dal momento dell'avvio.
<b>metric_currentagentthreadcount</b> <b>Nota:</b> Questa metrica viene visualizzata come “agent thread_s_” nella pagina Monitoraggio della CMC.	Numero di thread attualmente elaborati dal server.
<b>metric_totalagentthreadcount</b> <b>Nota:</b> Questa metrica viene visualizzata come “agent thread_s_” nella pagina Monitoraggio della CMC.	Numero di thread elaborati dal server dal momento dell'avvio.

### 31.1.10 Metriche del server Web Intelligence

Tabella 31 - 26: Metriche del servizio di elaborazione di Web Intelligence

<b>Metrica</b>	<b>Descrizione</b>
<b>Dimensione cache (Kb)</b>	La quantità totale di dati, in kilobyte, memorizzati nella cache.
<b>Numero di documenti non aggiornati nella cache</b>	Il numero di documenti eliminati dalla cache poiché troppo vecchi dall'avvio del server.

<b>Metrica</b>	<b>Descrizione</b>
<b>Conteggio contrassegno superiore della cache</b>	Il numero massimo di volte in cui la cache ha raggiunto le dimensioni massime consentite sul server dall'avvio.
<b>Utilizzo CPU (%)</b>	La percentuale del tempo totale della CPU impiegata dal server dall'avvio.
<b>Tempo totale CPU (secondi)</b>	Il tempo totale della CPU in secondi impiegato dal server dall'avvio.
<b>Conteggio soglia superiore di memoria</b>	Il numero di volte in cui la soglia elevata di memoria è stata raggiunta sul server dall'avvio.
<b>Conteggio soglia massima di memoria</b>	Il numero di volte in cui la soglia massima di memoria è stata raggiunta sul server dall'avvio.
<b>Dimensioni della memory virtuale (Mb)</b>	La quantità totale di memoria, in megabyte, assegnata al server.
<b>Numero corrente di chiamate client</b>	Il numero corrente di chiamate CORBA in elaborazione da parte del server.
<b>Numero di errori estensione remota Web</b>	Il numero di tentativi non riusciti da parte del server per la connessione a un servizio di estensione remota ospitata da un Adaptive Processing Server.
<b>Numero corrente di task</b>	Il numero corrente di attività in esecuzione sul server.
<b>Numero totale di chiamate client</b>	Il numero totale di chiamate CORBA ricevute dal server dall'avvio.
<b>Numero totale di task</b>	Il numero totale di attività eseguite sul server dall'avvio.
<b>Tempo di inattività (secondi)</b>	La quantità di tempo, in secondi, trascorsa dall'ultima richiesta ricevuta dal server da parte di un client.
<b>Numero corrente di sessioni attive</b>	Il numero corrente di sessioni in grado di accettare richieste dai client.
<b>Numero di documenti aperti dalla cache</b>	Il numero di documenti per i quali il risultato dell'ultima richiesta è stato letto direttamente dalla cache.
<b>Numero di documenti</b>	Il numero di documenti attualmente aperti sul server.
<b>Current number of sessions</b>	Il numero corrente di sessioni create sul server.
<b>Numero di scambi di documenti</b>	Il numero di documenti per i quali un thread di pulizia ha pianificato richieste di scambio.
<b>Numero di documenti scambiati</b>	Il numero di documenti scambiati in seguito a richieste di scambio.

<b>Metrica</b>	<b>Descrizione</b>
<b>Numero di timeout di sessioni</b>	Il numero di sessioni scadute a causa del mancato avvio del server.
<b>Numero totale di sessioni</b>	Il numero di sessioni create sul server dall'avvio.
<b>Numero di utenti</b>	Il numero totale di utenti collegati al server.
<b>Numero di thread attivi</b>	Il numero di thread che soddisfano le richieste ricevute dal server (pool di thread di asincronia).
<b>Numero totale di thread</b>	Il numero totale di thread creati dall'avvio del server (pool di thread di asincronia).

### 31.1.11 Metriche server di Dashboards

Tabella 31 - 27: Metriche dei server di elaborazione di Dashboards

<b>Metrica</b>	<b>Descrizione</b>
<b>Processi aperti</b>	Tabella che elenca i processi attualmente eseguiti sul server. La tabella indica l'ID e il nome del documento, il nome dell'utente che esegue il processo, la data dell'ultimo accesso al documento e per quanto tempo il processo è stato in esecuzione.
<b>Numero di richieste servite</b>	Numero totale delle richieste servite dal server dopo l'avvio.
<b>Numero di processi aperti</b>	Il numero di processi attualmente elaborati dal server e dai suoi processi secondari.
<b>Tipo di oggetto</b>	Il tipo di InfoObject gestito generalmente dal server. Il valore di questa metrica non cambia.
<b>Tempo di elaborazione medio (msec)</b>	Il tempo medio, in millisecondi, impiegato dal server per elaborare le ultime 500 richieste ricevute. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.
<b>Tempo di elaborazione massimo (msec)</b>	Il tempo massimo, in millisecondi, impiegato dal server per elaborare una delle ultime 500 richieste. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.



<b>Metrica</b>	<b>Descrizione</b>
<b>Tempo di elaborazione minimo (msec)</b>	Il tempo minimo, in millisecondi, impiegato dal server per elaborare una delle ultime 500 richieste. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.
<b>Numero di richieste in coda</b>	Il numero di richieste in attesa di essere elaborate o in fase di elaborazione. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.
<b>Nome DLL oggetto</b>	Il nome del plug-in di elaborazione per il server. Il valore di questa metrica non cambia.
<b>Numero di connessioni aperte</b>	Numero di connessioni attualmente aperte tra il server e i client.
<b>Frequenza errori di richieste</b>	La percentuale delle ultime 500 richieste ricevute che il server non è riuscito a elaborare.
<b>Dati trasferiti (KB)</b>	Quantità totale di dati, in kilobyte, trasferiti ai client dopo l'avvio del server.
<b>Numero di richieste non riuscite</b>	Numero di richieste che il server non è stato in grado di completare dopo l'avvio.
<b>Numero massimo di processi secondari</b>	Il numero massimo di processi secondari simultanei consentiti sul server.

Tabella 31 - 28: Metriche del Cache Server

<b>Metrica</b>	<b>Descrizione</b>
<b>Riscontri cache (%)</b>	La percentuale delle ultime 500 richieste servite con dati cache.
<b>Server di elaborazione connessi</b>	Una tabella che elenca i server di elaborazione di Dashboards nella distribuzione. La tabella include il nome del server e il numero di connessioni con il server attualmente aperte.
<b>Numero di richieste servite</b>	Numero totale delle richieste servite dal server dopo l'avvio.
<b>Tipo di oggetto</b>	Il tipo di InfoObject gestito generalmente dal server. Il valore di questa metrica non cambia.
<b>Tempo di elaborazione medio (msec)</b>	Il tempo medio, in millisecondi, impiegato dal server per elaborare le ultime 500 richieste ricevute. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.

<b>Metrica</b>	<b>Descrizione</b>
<b>Tempo di elaborazione massimo (msec)</b>	Il tempo massimo, in millisecondi, impiegato dal server per elaborare una delle ultime 500 richieste. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.
<b>Tempo di elaborazione minimo (msec)</b>	Il tempo minimo, in millisecondi, impiegato dal server per elaborare una delle ultime 500 richieste. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.
<b>Numero di richieste in coda</b>	Il numero di richieste in attesa di essere elaborate o in fase di elaborazione. Se questo numero è costantemente alto e in aumento, potrebbe essere necessario creare ulteriori server su altre macchine.
<b>Nome DLL oggetto</b>	Il nome del plug-in di elaborazione per il server. Il valore di questa metrica non cambia.
<b>Dimensioni cache (KB)</b>	La quantità di dati, in kilobyte, attualmente memorizzati nella cache del server sul disco.
<b>Numero di connessioni aperte</b>	Numero di connessioni ai client attualmente aperte.
<b>Dati trasferiti (KB)</b>	Quantità totale di dati, in kilobyte, trasferiti ai client dopo l'avvio del server.

## Appendice: segnaposto per server e nodi

### 32.1 Segnaposto server e nodo

Ad eccezione di "%SERVER\_FRIENDLY\_NAME%" e "%SERVER\_NAME%", questi segnaposto si applicano a tutti i server dello stesso nodo.

Tabella 32 - 1: Segnaposto

Segnaposto	Descrizione	Valori predefiniti
<b>%AuditingDatabaseConnection%</b>	La connessione al database di controllo utilizzata dal CMS.	Questo valore viene specificato durante l'installazione.
<b>%AuditingDatabaseDriver%</b>	Il tipo di driver di database utilizzato per connettersi al database di controllo.	In Windows il valore predefinito è sqlserverauditdbss.
<b>%BINDIR%</b>	La cartella nella quale si trovano i file binari a 64 bit della piattaforma SAP BusinessObjects Business Intelligence.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64. In UNIX, <DIRINSTALLAZ>/sap_bobj/enterprise_xi40/<piattaforma>/
<b>%BINDIR32%</b>	La cartella nella quale si trovano i file binari a 32 bit della piattaforma SAP BusinessObjects Business Intelligence.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\win32_x86. In UNIX, <DIRINSTALLAZ>/sap_bobj/enterprise_xi40/<piattaforma>/
<b>%CACHESERVER_EXE%</b>	Il nome dell'eseguibile per il Crystal Reports Cache Server.	In Windows, crcache.exe. In UNIX, boe_crcached.bin.
<b>%CMS_EXE%</b>	Il nome dell'eseguibile per il Central Management Server.	In Windows, cms.exe. In UNIX, boe_cmsd.
<b>%CONNECTIONSERVER32_EXE%</b>	Il nome dell'eseguibile per il Connection Server a 32 bit.	In Windows, ConnectionServer32.exe. In UNIX, ConnectionServer32.

Segnaposto	Descrizione	Valori predefiniti
<b>%CONNECTIONSERVER_DIR%</b>	La cartella principale del Connection Server.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer. In UNIX, <DIRINSTAL LAZ>/sap_bobj/enterprise_xi40/dataAccess/connectionServer
<b>%CONNECTIONSERVER_EXE%</b>	Il nome dell'eseguibile per il Connection Server a 64 bit.	In Windows, ConnectionServer.exe. In UNIX, ConnectionServer.
<b>%CR2011_BINDIR%</b>	La directory in cui risiedono i file binari del server Crystal Reports 2011 server.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjectsEnterprise XI 4.0\win32_x86. In UNIX, la directory sarà simile alla seguente: <DIRINSTALLAZ>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9.
<b>%CR2011_DefaultWorkingDir%</b>	La directory operativa predefinita per i server Crystal Reports 2011.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjectsEnterprise XI 4.0\win32_x86. In UNIX, la directory sarà simile alla seguente: <DIRINSTALLAZ>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9.
<b>%CRYSTALRAS_EXE%</b>	Il nome dell'eseguibile per il Report Application Server.	In Windows, crystalras.exe. In UNIX, boe_crystalrasd.
<b>%CR_ODBCINI%</b>	Il nome e il percorso del file .odbc.ini.	In UNIX, <DIRINSTAL LAZ>/bobje/odbc.ini. In Windows si tratta di una stringa vuota.

Segnaposto	Descrizione	Valori predefiniti
<b>%CommonJavaBundlesDir%</b>	La cartella in cui risiedono i raggruppamenti di OSGI condivisi.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bundles. In UNIX, <DIRINSTAL LAZ>/sap_bobj/enterprise_xi40/java/lib/bundles.
<b>%CommonJavaLibDir%</b>	La cartella in cui risiedono le librerie Java comuni.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\java\lib. In UNIX, <DIRINSTAL LAZ>/sap_bobj/enterprise_xi40/java/lib.
<b>%DLLEXT%</b>	Estensione predefinita di un file .dll o .so.	In Windows, .dll. In UNIX, .so.
<b>%DLLPATH%</b>	Il nome della variabile di ambiente nel computer in cui è installata la piattaforma SAP BusinessObjects Business Intelligence, che specifica le directory nelle quali l'interprete cercherà i file eseguibili.	In Windows, "Path". In UNIX, "LD_LIBRARY_PATH".
<b>%DLLPATH32%</b>	Nei sistemi Solaris a 32 bit è il nome della variabile di ambiente nel computer in cui è installata la piattaforma SAP BusinessObjects Business Intelligence, che specifica le directory nelle quali l'interprete cercherà i file eseguibili.	Nel computer Solaris "LD_LIBRARY_PATH_32". Questo segnaposto corrisponde a una stringa vuota in altri sistemi operativi.
<b>%DLLPATH64%</b>	Nei sistemi Solaris a 64 bit è il nome della variabile di ambiente nel computer in cui è installata la piattaforma SAP BusinessObjects Business Intelligence, che specifica le directory nelle quali l'interprete cercherà i file eseguibili.	Nei computer Solaris "LD_LIBRARY_PATH_64". Questo segnaposto corrisponde a una stringa vuota in altri sistemi operativi.
<b>%DLLPREFIX%</b>	Prefisso predefinito di un file .dll o .so.	In UNIX "lib". Questo segnaposto corrisponde a una stringa vuota nei computer Windows.

Segnaposto	Descrizione	Valori predefiniti
<b>%DLLPRELOAD%</b>	Nome della variabile d'ambiente LD_PRELOAD per la piattaforma.	In UNIX, LD_PRELOAD. Questo segnaposto corrisponde a una stringa vuota nei computer Windows.
<b>%DLLPRELOAD32%</b>	Nome della variabile di ambiente LD_PRELOAD sui sistemi AIX a 32 bit.	In AIX, "LDR_PRELOAD". Questo segnaposto corrisponde a una stringa vuota in altri computer.
<b>%DLLPRELOAD64%</b>	Nome della variabile di ambiente LD_PRELOAD sui sistemi AIX a 64 bit.	In AIX, "LDR_PRELOAD64". Questo segnaposto corrisponde a una stringa vuota in altri computer.
<b>%DP%</b>	Il delimitatore di percorso.	In Windows, “;”. In UNIX, “:”.
<b>%DefaultAuditingDir%</b>	La directory in cui vengono scritti i file temporanei di controllo. Per ottenere prestazioni ottimali, questa posizione deve trovarsi nell'unità locale del server.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\Auditing. In UNIX, <DIRINSTAL LAZ>/sap_bobj/data/Auditing/.
<b>%DefaultDataDir%</b>	La directory temporanea utilizzata da Job Server.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\Data. In UNIX, <DIRINSTAL LAZ>/sap_bobj/data/.
<b>%DefaultInputFRSDir%</b>	La cartella principale dell'Input File Repository Server.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Input. In UNIX, <DIRINSTALLAZ>/sap_bobj/data/frsinput.
<b>%DefaultLoggingDir%</b>	La posizione di archiviazione dei file di registro.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\logging. In UNIX, <DIRINSTAL LAZ>/sap_bobj/logging.
<b>%DefaultOutputFRSDir%</b>	La cartella principale dell'Output File Repository Server.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Output. In UNIX, <DIRINSTAL LAZ>/sap_bobj/data/frsoutput.

Segnaposto	Descrizione	Valori predefiniti
<b>%DefaultWorkingDir%</b>	La directory operativa per i server a 64 bit	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64. In UNIX, <DIRINSTALLAZ>/sap_bobj/enterprise_xi40/<piattaforma>.
<b>%DefaultWorkingDir32%</b>	La directory operativa per i server a 32 bit.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\win32_x86. In UNIX, <DIRINSTALLAZ>/sap_bobj/enterprise_xi40/<piattaforma>.
<b>%EPM_LD_PRELOAD_ONCE%</b>	Nome della variabile d'ambiente LD_PRELOAD_ONCE per la piattaforma.	\$LD_PRELOAD_ONCE\$
<b>%EVENTSERVER_EXE%</b>	Il nome dell'eseguibile per l'Event Server.	In Windows, EventServer.exe. In UNIX, boe_eventsd.
<b>%EXEEXT%</b>	Estensione predefinita dei file eseguibili.	In Windows, .exe. Questo segnaposto non è disponibile in UNIX.
<b>%EXEPATH%</b>	Il nome della variabile di ambiente nel computer in cui è installata la piattaforma SAP BusinessObjects Business Intelligence, che specifica le directory nelle quali l'interprete cercherà i file eseguibili.	In Windows, "Path". In UNIX, "PATH".
<b>%EnterpriseDir%</b>	La posizione in cui viene installata la piattaforma SAP BusinessObjects Business Intelligence a 64 bit.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\.. In UNIX, <DIRINSTALLAZ>/sap_bobj/enterprise_xi40/.
<b>%EnterpriseDir32%</b>	La posizione in cui viene installata la piattaforma SAP BusinessObjects Business Intelligence a 32 bit.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\.. In UNIX, <DIRINSTALLAZ>/sap_bobj/enterprise_xi40/.

Segnaposto	Descrizione	Valori predefiniti
<b>%ExternalJavaLibDir%</b>	La cartella in cui risiedono le librerie Java esterne e di terze parti.	In Windows, <DIRINSTALLAZ>\SAP BusinessObjects Enterprise XI 4.0\java\lib\external. In UNIX, <DIRINSTALLAZ>/sap_bobj/enterprise_xi40/java/lib/external.
<b>%FILESERVER_EXE%</b>	Il nome dell'eseguibile per il File Server.	In Windows, fileserver.exe. In UNIX, boe_filesd.
<b>%HOARD_PATH%</b>	La posizione del gestore della memoria.	Per impostazione predefinita il segnaposto è vuoto.
<b>%HOARD_PRELOAD%</b>	Specifica se precaricare il gestore della memoria.	Per impostazione predefinita il segnaposto è vuoto.
<b>%INSTALLROOTDIR%</b>	La cartella in cui viene installata la piattaforma SAP BusinessObjects Business Intelligence a 64 bit.	Questo valore viene specificato durante l'installazione.
<b>%INSTALLROOTDIR32%</b>	La cartella in cui viene installata la piattaforma SAP BusinessObjects Business Intelligence a 32 bit.	Questo valore viene specificato durante l'installazione.
<b>%IntroscopeAgentEnableInstrumentation%</b>	Indica se la strumentazione per i server Java che utilizzano Introscope Agent Enterprise Manager è attivata.	I valori possibili sono TRUE o FALSE, a seconda che Introscope Agent Enterprise Manager sia stato o meno abilitato durante l'installazione della piattaforma SAP BusinessObjects Business Intelligence.
<b>%IntroscopeAgentEnterpriseManagerHost%</b>	Il nome host dell'Introscope Agent Enterprise Manager al quale vengono inviati i dati di strumentazione.	Questo valore viene specificato durante l'installazione.
<b>%IntroscopeAgentEnterpriseManagerPort%</b>	La porta dell'Introscope Agent Enterprise Manager alla quale vengono inviati i dati di strumentazione.	Questo valore viene specificato durante l'installazione.
<b>%IntroscopeAgentEnterpriseManagerTransport%</b>	Il trasporto utilizzato per l'invio dei dati di strumentazione all'Introscope Agent Enterprise Manager. I valori consentiti sono: <ul style="list-style-type: none"> <li>TCP</li> <li>HTTP</li> <li>HTTPS</li> <li>SSL</li> </ul>	TCP



Segnaposto	Descrizione	Valori predefiniti
<b>%IntroscopeAgentEnterpriseManagerTransportHTTP%</b>	La classe utilizzata per l'invio dei dati di strumentazione all'Intro-scope Agent Enterprise Manager mediante HTTP.	com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory
<b>%IntroscopeAgentEnterpriseManagerTransportHTTPS%</b>	La classe utilizzata per l'invio dei dati di strumentazione all'Intro-scope Agent Enterprise Manager mediante HTTPS.	com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory
<b>%IntroscopeAgentEnterpriseManagerTransportSSL%</b>	La classe utilizzata per l'invio dei dati di strumentazione all'Intro-scope Agent Enterprise Manager mediante SSL.	com.wily.isengard.postofficehub.link.net.SSLSocketFactory
<b>%IntroscopeAgentEnterpriseManagerTransportTCP%</b>	La classe utilizzata per l'invio dei dati di strumentazione all'Intro-scope Agent Enterprise Manager mediante TCP.	com.wily.isengard.postofficehub.link.net.DefaultSocketFactory
<b>%IntroscopeDir%</b>	La cartella in cui è installato Intro-scope Agent Enterprise Manager.	In Windows, <DIRINSTALLAZ>\SAP BusinessObjects Enterprise XI 4.0\java\wily. In UNIX, <DIRINSTALLAZ>/sap_bobj/enterprise_xi40/java/wily.
<b>%JAVAW_EXE%</b>	Il nome del file eseguibile per Java Virtual Machine che non dispone di finestra della console.	In Windows, javaw.exe. In UNIX, java.
<b>%JAVA_EXE%</b>	Il nome dell'eseguibile di Java Virtual Machine.	In Windows, java.exe. In UNIX, java.
<b>%JOBSEVERCHILD_EXE%</b>	Il nome dell'eseguibile per l'Adaptive Job Server secondario.	In Windows, JobServerChild.exe. In UNIX, boe_jobcd.
<b>%JOBSEVER_EXE%</b>	Il nome dell'eseguibile per l'Adaptive Job Server.	In Windows, JobServer.exe. In UNIX, boe_jobcd.
<b>%JdkBinDir%</b>	La cartella in cui risiedono i file binari JDK.	In Windows, <DIRINSTALLAZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin. In UNIX, <DIRINSTALLAZ>/sap_bobj/<PIATTAFORMA>/sapjvm/bin.

Segnaposto	Descrizione	Valori predefiniti
<b>%JreBinDir%</b>	La cartella in cui risiedono i file binari JRE.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin. In UNIX, <DIRINSTAL LAZ>/sap_bobj/<PIATTAFORMA>/sapjvm/jre/bin.
<b>%JVM_ARCH_ENVIRONMENT%</b>	Indica se il computer è in esecuzione su una JVM a 32 o 64 bit.	Per i computer UNIX a 32 bit il valore predefinito è “-d32”. Per i computer a 64 bit il valore predefinito è “-d64”. Nei computer Windows si tratta di una stringa vuota.
<b>%JVM_HEADLESS_MODE%</b>	L'argomento della riga di comando che specifica se la JVM funziona in modalità Headless.	In Windows, -Djava.awt.headless=false. In UNIX, -Djava.awt.headless=true
<b>%JVM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%</b>	I parametri della riga di comando che specificano le operazioni eseguite dalla JVM quando rileva errori di memoria insufficiente.	"-XX:+HeapDumpOnOutOfMemoryError"-XX:HeapDumpPath=%DefaultLoggingDir%" "-XX:+ExitVMOnOutOfMemoryError"
<b>%JVM_SHARED_MEMORY_SEGMENT%</b>	I parametri della riga di comando che abilitano le estensioni JVM e impostano il numero di istanza della JVM.	Per impostazione predefinita, il segnaposto è vuoto.
<b>%LANGUAGEPACKSDIR%</b>	La cartella in cui sono installate le lingue di distribuzione.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\Languages. In UNIX, <DIRINSTALLAZ>/sap_bobj/enterprise_xi40/Languages/.
<b>%LANGUAGEPACKSDIR32%</b>	La cartella in cui sono installate le lingue di distribuzione sui sistemi a 32 bit.	. In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\Languages. In UNIX, <DIRINSTALLAZ>/sap_bobj/enterprise_xi40/Languages/.
<b>%LSTDir%</b>	La cartella in cui sono archiviati i file di configurazione LST.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\conf\lst. In UNIX, <DIRINSTAL LAZ>/sap_bobj/enterprise_xi40/conf/lst.

Segnaposto	Descrizione	Valori predefiniti
<b>%MDAS_JVM_OS_STACK_SIZE%</b>	Specifica le dimensioni dello stack della JVM per il servizio di analisi multidimensionale.	Per impostazione predefinita, il segnaposto è vuoto.
<b>%NCSInstrumentLevelThreshold%</b>	Il livello di soglia della registrazione di analisi per la libreria NCS.	Per impostazione predefinita, il valore è 0.
<b>%PAGESERVER_EXE%</b>	Il nome dell'eseguibile per il server di elaborazione Crystal Reports 2011.	In Windows, <code>crproc.exe</code> . In UNIX, <code>boe_crprocd.bin</code> .
<b>%PJSContainerDir%</b>	La cartella in cui risiedono i file JARS del contenitore APS.	In Windows, <code>&lt;DIRINSTALLAZ&gt;\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container</code> . In UNIX, <code>&lt;DIRINSTALLAZ&gt;/sap_bobj/enterprise_xi40/java/pjs/container</code> .
<b>%PJSServicesDir%</b>	La cartella in cui risiedono i file JARS del servizio APS.	In Windows, <code>&lt;DIRINSTALLAZ&gt;\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services</code> . In UNIX, <code>&lt;DIRINSTALLAZ&gt;/sap_bobj/enterprise_xi40/java/pjs/services</code> .
<b>%Platform%</b>	Il sistema operativo del computer in cui è in esecuzione la piattaforma SAP BusinessObjects Business Intelligence.	Il sistema operativo del computer in cui è in esecuzione la piattaforma SAP BusinessObjects Business Intelligence.
<b>%Platform32%</b>	Il sistema operativo del computer in cui è in esecuzione la piattaforma SAP BusinessObjects Business Intelligence a 32 bit.	Il sistema operativo del computer in cui è in esecuzione la piattaforma SAP BusinessObjects Business Intelligence.
<b>%RasBinDir%</b>	La cartella principale del Report Application Server.	In Windows, <code>&lt;DIRINSTALLAZ&gt;\SAP BusinessObjects Enterprise XI 4.0\win32_x86</code> . In UNIX, <code>&lt;DIRINSTALLAZ&gt;/sap_bobj/enterprise_xi40/&lt;PLATFORM&gt;/ras</code> .
<b>%SERVER_FRIENDLY_NAME%</b>	Nome completo del server.	Nome completo del server.

Segnaposto	Descrizione	Valori predefiniti
<b>%SERVER_NAME%</b>	Nome completo del server.	Nome completo del server.
<b>%SMDAgentHost%</b>	Il nome host di SDM Agent al quale vengono inviati i dati di strumentazione.	Questo valore viene specificato durante l'installazione.
<b>%SMDAgentPort%</b>	La porta di SDM Agent alla quale vengono inviati i dati di strumentazione.	Questo valore viene specificato durante l'installazione.
<b>%TRACE_CONFIGFILE_INI%</b>	Il nome e il percorso del file BO_Trace.ini.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\conf\BO_trace.ini. In UNIX, <DIRINSTAL LAZ>/sap_bobj/enterprise_xi40/conf/BO-trace.ini.
<b>%WarFilesDir%</b>	La posizione dei file delle applicazioni Web.	In Windows, <DIRINSTAL LAZ>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps. In UNIX, <DIRINSTAL LAZ>/sap_bobj/enterprise_xi40/warfiles/webapps.
<b>%WEBI_LD_PRELOAD%</b>	Nome della variabile d'ambiente LD_PRELOAD per la piattaforma.	\$LD_PRELOAD\$
<b>%WEBISERVER_EXE%</b>	Il nome dell'eseguibile per Web Intelligence Processing Server.	In Windows, wireportserver.exe. In UNIX, WIReportServer.
<b>%WEBI_LD_PRELOAD_ONCE%</b>	Nome della variabile d'ambiente LD_PRELOAD_ONCE per la piattaforma.	\$LD_PRELOAD_ONCE\$
<b>%XCCACHE_EXE%</b>	Il nome dell'eseguibile per Dashboards Cache Server.	In Windows, xccache.exe. In UNIX, boe_xccached.
<b>%XCPROC_EXE%</b>	Il nome dell'eseguibile per il server di elaborazione di Dashboards.	In Windows, xcproc.exe. In UNIX, boe_xcprocd.

**Nota:**

i segnaposto riportati di seguito possono essere modificati a livello di nodo. Nella tabella precedente sono contenute le descrizioni e i valori predefiniti. I segnaposto non inclusi nell'elenco sono di sola lettura.

- %DefaultAuditingDir%
- %DefaultDataDir%
- %DefaultLoggingDir%
- %IntroscopeAgentEnableInstrumentation%
- %IntroscopeAgentEnterpriseManagerHost%
- %IntroscopeAgentEnterpriseManagerPort%
- %IntroscopeAgentEnterpriseManagerTransport%
- %NCSInstrumentLevelThreshold%
- %SMDAgentHost%
- %SMDAgentPort%

**Argomenti correlati**

- [Visualizzazione e modifica dei segnaposto per un nodo](#)

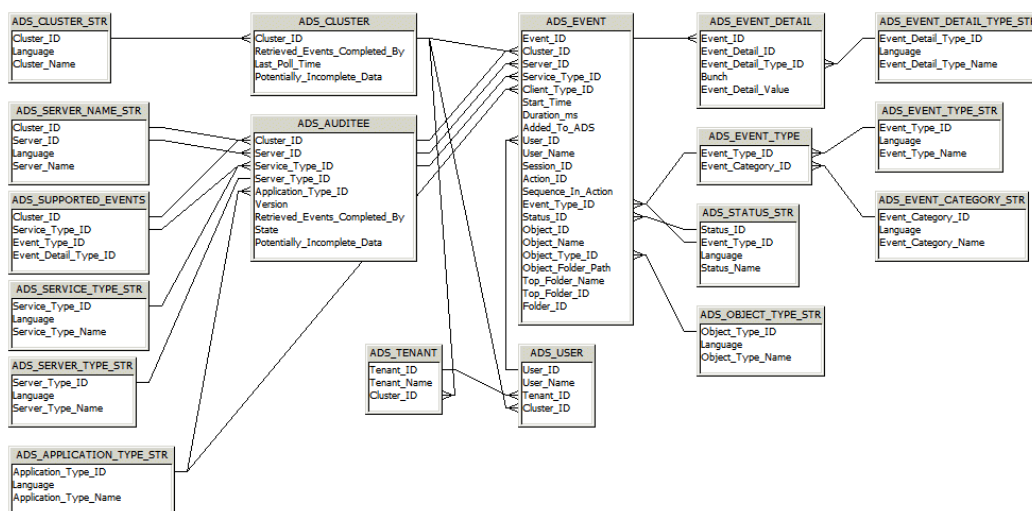


## Appendice: schema archivio dati di controllo

### 33.1 Panoramica

Questa appendice costituisce un riferimento per i progettisti di report che creano report dai dati delle tabelle dell'archivio dati di controllo. Il diagramma e le spiegazioni sulla tabella riportati di seguito mostrano le tabelle in cui verranno registrati i dati di controllo, nonché le relazioni tra le tabelle.

### 33.2 Diagramma schema



### 33.3 Tabelle dell'archivio dati di controllo

## Tabella ADS\_APPLICATION\_TYPE\_STR

Questa tabella fornisce un dizionario multilingua dei nomi di tipo di applicazione client.

Nome colonna	Tipo	Chiave	Descrizione
Application_Type_ID	Carattere (64)	Chiave primaria	CUID del tipo di applicazione per l'applicazione.
Lingua	Carattere (10)	Chiave primaria	Codice per la lingua in cui viene registrato il tipo di applicazione, ad esempio <i>EN</i> o <i>DE</i> .
Application_Type_Name	Carattere (255)	N/D	Nome di testo del tipo di applicazione, ad esempio Crystal Reports o Web Intelligence.

### Tabella ADS\_AUDITEE

Questa tabella contiene informazioni sulle proprietà per tutti i server di controllo che fanno parte della distribuzione.

Nome colonna	Tipo	Chiave	Descrizione
Cluster_ID	Carattere (64)	Chiave primaria	GUID per il cluster a cui appartiene il sistema controllato.
Server_ID	Carattere (64)	<ul style="list-style-type: none"> <li>Chiave primaria</li> <li>Chiave esterna (da ADS_SERVER_NAME_SIR)</li> </ul>	CUID del server che ha attivato l'evento. Se l'evento è attivato dal client, verrà restituito il CUID dell'Adaptive Processing Server che ha elaborato l'evento.
Service_Type_ID	Carattere (64)	<ul style="list-style-type: none"> <li>Chiave primaria</li> <li>Chiave esterna (da ADS_SERVICE_TYPE_SIR)</li> </ul>	CUID del tipo di servizio per il servizio che ha attivato l'evento. Gli eventi attivati da client restituiscono un CUID del tipo di applicazione.
Server_Type_ID	Carattere (64)	<ul style="list-style-type: none"> <li>Chiave primaria</li> <li>Chiave esterna (da ADS_SERVER_TYPE_SIR)</li> </ul>	CUID del tipo di server per il server che ha attivato l'evento.



Nome colonna	Tipo	Chiave	Descrizione
Application_Type_ID	Carattere (64)	<ul style="list-style-type: none"> <li>Chiave primaria</li> <li>Chiave esterna (da ADS_APPLICATION_TYPE_STR)</li> </ul>	CUID del tipo di applicazione per il client che ha attivato l'evento. Per gli eventi di server viene restituito l'ID del tipo di servizio.
Versione	Carattere (64)	N/D	La versione del server o del client che ha attivato l'evento nel momento in cui è stato registrato.
Retrieved_Events_Completed_By	Datetime	N/D	L'ultima volta in cui il server CMS di controllo ha eseguito il polling del sistema controllato per verificare i file temporanei. Indica che tutti gli eventi del sistema controllato che sono stati completati prima di questa data/ora si trovano nell'archivio dati di controllo.
Stato	INTEGER	N/D	Lo stato (In esecuzione, Non in esecuzione, Eliminato) in cui si trovava il sistema controllato.
Potentially_Incomplete_Data	INTEGER	N/D	Indica se il sistema controllato può contenere eventi che non sono stati trasferiti all'archivio dati di controllo.

### Tabella ADS\_CLUSTER

Questa tabella contiene informazioni su tutti i cluster che contengono sistemi controllati.

Nome colonna	Tipo	Chiave	Descrizione
Cluster_ID	Carattere (64)	<ul style="list-style-type: none"> <li>Chiave primaria</li> <li>Chiave esterna (da ADS_CLUSTER_STR)</li> </ul>	GUID del cluster.
Retrieved_Events_Completed_By	Datetime	N/D	Indica in che misura sono aggiornate le informazioni di controllo nel database per il cluster. Restituisce l'indicazione di data e ora più vecchia recuperata per tutti i server controllati attualmente in esecuzione in un dato momento. Indica che tutti gli eventi completati prima di questa data si trovano nell'archivio dati di controllo.

Nome colonna	Tipo	Chiave	Descrizione
Last_Poll_Time	Datetime	N/D	L'ultima volta che il server CMS di controllo ha eseguito il polling sui sistemi controllati in questo cluster.
Potentially_Incomplete_Data	INTEGER	N/D	Indica informazioni di controllo potenzialmente incomplete nel cluster: "0" = tutti i server hanno trasferito i dati normalmente; "1" = per almeno un server in esecuzione o non in esecuzione del cluster è impostato il flag <b>Dati potenzialmente incompleti</b> , per indicare che un sistema controllato contiene eventi che non sono ancora stati trasferiti all'archivio dati di controllo.

### Tabella ADS\_CLUSTER\_STR

Questa tabella fornisce un record di riferimento dei diversi cluster della distribuzione.

Nome colonna	Tipo	Chiave	Descrizione
Cluster_ID	Carattere (64)	Chiave primaria	ID univoco del cluster.
Lingua	Carattere (10)	Chiave primaria	Codice per l'impostazione della lingua per il cluster, ad esempi <i>EN</i> o <i>DE</i> .
Cluster_Name	Carattere (255)	N/D	Indica il nome del cluster.

### Tabella ADS\_EVENT

Questa tabella contiene le proprietà di base per ciascun evento e rappresenta il punto di collegamento centrale per le altre tabelle dello schema.

Nome colonna	Tipo di campo	Chiave	Descrizione
Event_ID	Carattere (64)	Chiave primaria	ID univoco generato per l'evento.
Cluster_ID	Carattere (64)	Chiave esterna (da ADS_CLUSTER)	GUID del cluster di controllo. Viene restituito perché più cluster potrebbero utilizzare lo stesso archivio dati di controllo.
Server_ID	Carattere (64)	Chiave esterna (da ADS_SERVER_NAME)	CUID del server che ha attivato l'evento.

Nome colonna	Tipo di campo	Chiave	Descrizione
Service_Type_ID	Carattere (64)	Chiave esterna (da ADS_SERVICE_TYPE_STR)	<ul style="list-style-type: none"> <li>CUID del tipo di servizio che ha attivato l'evento. I servizi presenti su un server utilizzano il proprio CUID del tipo di servizio.</li> <li>Le applicazioni client (ad esempio BI Launch Pad o Web Intelligence) registreranno il proprio CUID del tipo di applicazione.</li> </ul>
Client_Type_ID	Carattere (64)	Chiave esterna (da ADS_APPLICATION_TYPE)	Indica l'ID del tipo di client per il client che ha stabilito la sessione.
Start_Time	Datetime	N/D	Data e ora (UTC) in cui l'operazione di evento è iniziata (inclusi i millesimi di secondo).
Duration_ms	INTEGER	N/D	Durata dell'operazione in millesimi di secondo.
Added_to_ADS	Datetime	N/D	Data e ora (UTC) in cui l'evento è stato registrato nell'archivio dati di controllo.
User_ID	Carattere (64)	N/D	CUID dell'utente che ha eseguito l'azione.
User_Name	Carattere (255)	N/D	Il nome associato all'ID dell'utente che ha eseguito l'azione. Viene restituito nella lingua predefinita del CMS dello strumento di controllo.
Session_ID	Carattere (64)	N/D	GUID della sessione durante la quale l'evento è stato attivato. Se non è associata una sessione, il campo dati sarà null.
Action_ID	Carattere (64)	N/D	ID dell'azione utente che ha attivato l'evento. Viene utilizzato per raggruppare eventi che risultano da un'unica azione utente.
Sequence_In_Action	INTEGER	N/D	Per gli eventi multiserver (o client e multiserver), l'applicazione server o client della sequenza che ha attivato l'evento. In tutti i workflow di pianificazione l'ID della sequenza sarà sempre 0.
Event_Type_ID	INTEGER	Chiave esterna (da ADS_EVENT_TYPE)	Tipo di evento (ad esempio Visualizza o Salva)
Status_ID	INTEGER	Chiave esterna (da ADS_STATUS_STR)	Stato dell'operazione (ad esempio, "0" = riuscita, "1" = non riuscita).

Nome colonna	Tipo di campo	Chiave	Descrizione
Object_ID	Carattere (64)	N/D	CUID dell'oggetto su cui è stata eseguita l'operazione.
Object_Name	Carattere (255)	N/D	Il nome dell'oggetto su cui è stata eseguita l'operazione. Viene restituito nella lingua predefinita del CMS dello strumento di controllo.
Object_Type_ID	Carattere (64)	Chiave esterna (da ADS_OBJECT_TYPE_STR)	CUID del tipo di oggetto su cui è stata eseguita l'operazione.
Object_Folder_Path	Carattere (255)	N/D	Il percorso completo della cartella (ad esempio Paese/Regione/Città) per l'oggetto su cui è stata eseguita l'operazione. Viene restituito nella lingua predefinita del CMS dello strumento di controllo. Se non è possibile determinare il percorso della cartella, il valore verrà impostato su null.
Folder_ID	Carattere (64)	N/D	CUID della cartella per l'oggetto su cui è stata eseguita l'operazione.
Top_Folder_Name	Carattere (255)	N/D	Nome della cartella di livello superiore per l'oggetto. Ad esempio, se l'oggetto è situato in Paese/Regione/Città verrà restituito Paese.
Top_Folder_ID	Carattere (64)	N/D	CUID della cartella di livello superiore in cui risiede l'oggetto. Ad esempio, se l'oggetto è situato in Paese/Regione/Città verrà restituito il CUID della cartella Paese.

### Tabella ADS\_EVENT\_CATEGORY\_STR

Questa tabella fornisce un dizionario multilingua dei nomi di categoria di evento.

Nome colonna	Tipo	Chiave	Descrizione
Event_Type_ID	INTEGER	Chiave primaria	ID della categoria di evento.
Lingua	Carattere (10)	Chiave primaria	Codice per la lingua in cui è registrato il nome della categoria dell'evento, ad esempio <i>EN</i> o <i>DE</i> .
Event_Category_Name	Carattere (255)	N/D	Nome della categoria dell'evento.

### ADS\_EVENT\_DELETES

Non utilizzare o creare report al di fuori di questa tabella. È destinato a un uso di sistema interno e potrebbe essere rimosso nelle versioni future.

### Tabella ADS\_EVENT\_DETAIL

Questa tabella contiene le proprietà dei dettagli di evento.

Nome colonna	Tipo	Chiave	Descrizione
Event_Detail_ID	INTEGER	Chiave primaria	GUID per il dettaglio di evento.
Event_ID	Carattere (64)	<ul style="list-style-type: none"> <li>Chiave primaria</li> <li>Chiave esterna (da ADS_EVENT)</li> </ul>	GUID dell'evento superiore.
Event_Detail_Type_ID	INTEGER	Chiave esterna (da ADS_EVENT_DETAIL_STR)	Tipo di dettaglio di evento.
Gruppo	INTEGER	N/D	<p>Se il dettaglio fa parte di una serie, viene utilizzato per raggruppare i dettagli.</p> <p>Ad esempio, se un report contiene prompt per Stato e Paese, un utente può immettere "USA" per il prompt Paese e "California" e "Nevada" per il prompt Stato. In questo modo vengono generati dettagli di evento con due gruppi. Il gruppo 1 è costituito da:</p> <ul style="list-style-type: none"> <li>Nome prompt: Paese</li> <li>Valore prompt: USA</li> </ul> <p>Il gruppo 2 è costituito da:</p> <ul style="list-style-type: none"> <li>Nome prompt: Stato</li> <li>Valore prompt: California</li> <li>Valore prompt: Nevada</li> </ul>
Event_Detail_Value	Carattere (testo lungo)	N/D	Il valore del dettaglio di evento.

### Tabella ADS\_EVENT\_DETAIL\_TYPE\_STR

Questa tabella fornisce un dizionario multilingua dei nomi di tipo di dettaglio evento.

Nome colonna	Tipo	Chiave	Descrizione
Event_Detail_ID	INTEGER	Chiave primaria	ID del tipo di dettaglio evento per il dettaglio dell'evento.
Lingua	Carattere (10)	Chiave primaria	Codice per la lingua in cui è registrato il nome del dettaglio dell'evento, ad esempio <i>EN</i> o <i>DE</i> .
Event_Detail_Type_Name	Carattere (255)	N/D	Nome di testo del tipo di dettaglio evento.

### Tabella ADS\_EVENT\_TYPE

Questa tabella fornisce un record di riferimento per le diverse categorie di eventi.

Nome colonna	Tipo	Chiave	Descrizione
Event_Type_ID	INTEGER	<ul style="list-style-type: none"> <li>Chiave primaria</li> <li>Chiave esterna (da ADS_EVENT_TYPE_STR)</li> </ul>	Identificatore univoco per il tipo di evento.
Event_Category_ID	INTEGER	<ul style="list-style-type: none"> <li>Chiave primaria</li> <li>Chiave esterna (da ADS_EVENT_CATEGORY_STR)</li> </ul>	Categoria di evento. Ad esempio, comune, Web Intelligence o Lifecycle Management.

### Tabella ADS\_EVENT\_TYPE\_STR

Questa tabella fornisce un dizionario multilingua dei nomi di tipo di evento.

Nome colonna	Tipo	Chiave	Descrizione
Event_Category_ID	INTEGER	Chiave primaria	ID del tipo di evento per l'evento.
Lingua	Carattere (10)	Chiave primaria	Codice per la lingua in cui è registrato il nome della categoria dell'evento, ad esempio <i>EN</i> o <i>DE</i> .
Event_Type_Name	Carattere (255)	N/D	Nome di testo del tipo di evento, ad esempio Visualizza o Accesso.

### Tabella ADS\_OBJECT\_TYPE\_STR

Questa tabella fornisce un dizionario multilingua dei nomi di oggetto evento.

Nome colonna	Tipo	Chiave	Descrizione
Object_Type_ID	Carattere (64)	Chiave primaria	CUID del tipo di oggetto per l'oggetto.
Lingua	Carattere (10)	Chiave primaria	Codice per la lingua in cui è registrato il nome del tipo di oggetto, ad esempio <i>EN</i> o <i>DE</i> .
Object_Type_Name	Carattere (255)	N/D	Nome del tipo di oggetto.

### Tabella ADS\_SERVER\_NAME\_STR

Questa tabella fornisce un dizionario multilingua dei nomi di server. I valori verranno aggiornati quando i server vengono rinominati.

Nome colonna	Tipo	Chiave	Descrizione
Cluster_ID	Carattere (64)	Chiave primaria	GUID del cluster a cui appartiene il server.
Server_ID	Carattere (64)	Chiave primaria	CUID del server.
Lingua	Carattere (10)	Chiave primaria	Codice per la lingua del nome del server, ad esempio <i>EN</i> o <i>DE</i> .
Server_Name	Carattere (255)	N/D	Il nome del server.

### Tabella ADS\_SERVICE\_TYPE\_STR

Questa tabella fornisce un dizionario multilingua dei nomi di tipo di servizio.

Nome colonna	Tipo	Chiave	Descrizione
Service_Type_ID	Carattere (64)	Chiave primaria	CUID del tipo di servizio o della categoria di servizio per il servizio.
Lingua	Carattere (10)	Chiave primaria	Codice per la lingua in cui è registrato il nome del tipo di servizio, ad esempio <i>EN</i> o <i>DE</i> .
Service_Type_Name	Carattere (255)	N/D	Nome del tipo di servizio.

### Tabella ADS\_STATUS\_STR

Questa tabella fornisce un dizionario multilingua dei nomi di stato dell'evento.

Nome colonna	Tipo	Chiave	Descrizione
Status_ID	INTEGER	Chiave primaria	Rappresentazione numerica dello stato dell'operazione.
Event_Type_ID	INTEGER	Chiave primaria	ID del tipo di evento. Ad esempio, 1002 per Visualizza.
Lingua	Carattere (10)	Chiave primaria	Codice per la lingua in cui è registrato lo stato dell'evento, ad esempio <i>EN</i> o <i>DE</i> .
Status_Name	Carattere (255)	N/D	Descrizione di testo dello stato dell'evento, ad esempio Riuscito o Non riuscito.

#### Tabella ADS\_SUPPORTED\_EVENTS

Questa tabella contiene un elenco di eventi supportati con i dettagli di evento associati per ogni tipo di servizio o applicazione client.

Nome colonna	Tipo	Chiave	Descrizione
Cluster_ID	Carattere (64)	Chiave primaria	GUID del cluster a cui appartiene il servizio.
Service_Type_ID	Carattere (64)	Chiave primaria	CUID del tipo di servizio per il servizio che ha attivato l'evento. Se l'evento viene attivato da un'applicazione client, viene restituito un CUID del tipo di applicazione.
Event_Type_ID	INTEGER	Chiave esterna (da ADS_EVENT_TYPE)	ID per il tipo di evento restituito, ad esempio l'ID di Salva.
Event_Detail_Type_ID	INTEGER	Chiave esterna (da ADS_EVENT_DETAIL_TYPE_STR)	CUID che identifica il tipo di dettaglio di evento acquisito per quell'evento (ad esempio, Percorso file).

#### Tabella ADS\_TENANT

Questa tabella contiene la relazione tra i nomi e gli ID di database.

Nome colonna	Tipo	Chiave	Descrizione
Cluster_ID	Carattere (64)	Chiave primaria	GUID del cluster.
Tenant_ID	Carattere (64)	Chiave primaria	CUID del database.



Nome colonna	Tipo	Chiave	Descrizione
Tenant_Name	Carattere (255)	N/D	Nome del database.

### **Tabella ADS\_USER**

Questa tabella contiene la relazione tra utenti e database.

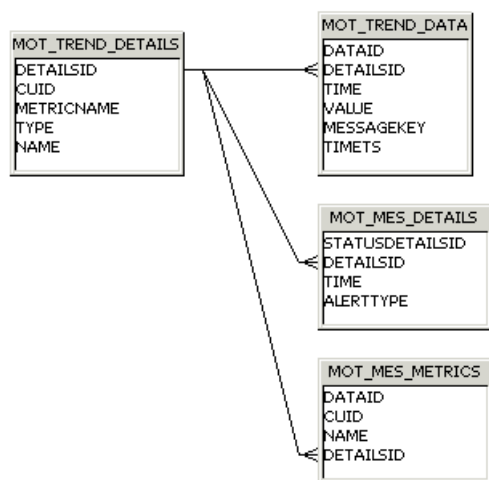
Nome colonna	Tipo	Chiave	Descrizione
Cluster_ID	Carattere (64)	Chiave primaria	GUID del cluster.
User_ID	Carattere (64)	Chiave primaria	CUID dell'utente.
User_Name	Carattere (255)	N/D	Nome dell'utente.
Tenant_ID	Carattere (64)	Chiave primaria	CUID del database.



## Appendice sullo schema dei database di monitoraggio

### 34.1 Schema del database di tendenza

Il diagramma del database di tendenza e le spiegazioni sulla tabella riportati di seguito mostrano le tabelle in cui vengono registrati i dati su metrica, probe e controllo, nonché le relazioni tra le tabelle.



#### MOT\_TREND\_DETAILS

Questa tabella registra le informazioni sulle entità gestite, le probe e i controlli. Ad esempio, i nomi di metrica e CUID.

Nome colonna	Tipo	Chiave	Descrizione
DetailsId	INTEGER	Chiave primaria Generata automaticamente	
CUID	VARCHAR(64)	N/D	CUID dell'InfoObject che espone la metrica o che è correlato a essa
MetricName	VARCHAR(255)	N/D	Nome della metrica

Nome colonna	Tipo	Chiave	Descrizione
Tipo	VARCHAR(32)	N/D	Può essere "Subscription", "ManagedEntityStatus" o "Probe"
Nome	VARCHAR(255)	N/D	Nome del controllo quando il tipo è "ManagedEntityStatus". In caso contrario, per impostazione predefinita viene utilizzata la stessa stringa del tipo, ma contenente solo lettere maiuscole, ad esempio "PROBE" o "SUBSCRIPTION".

### MOT\_TREND\_DATA

Questa tabella registra i dati di tendenza da metriche, controlli e probe. Ad esempio, il valore e l'ora della metrica.

Nome colonna	Tipo	Chiave	Descrizione
DataId	INTEGER	Chiave primaria Generata automaticamente	
DetailsId	INTEGER	Chiave esterna (da MOT_TREND_DETAILS)	
Time o TimeT	BIGINT o NUMBER o FIXED Data epoca Unix	N/D	Ora di raccolta dei dati
Valore	FLOAT o DOUBLE o NUMBER	N/D	Valore della metrica/sottoscrizione
MessageKey	VARCHAR(32)	N/D	Chiave del messaggio di errore o null se riesce. Per il controllo, può anche essere "watchEnabled" o "watchDisabled". È una "chiave" in quanto viene in definitiva utilizzato per caricare i messaggi localizzati prima di visualizzare l'interfaccia utente.
Ts	DATETIME o TIMESTAMP	N/D	Data e ora in cui i dati vengono scritti nel database

### MOT\_MES\_DETAILS

Questa tabella registra le informazioni relative alle violazioni di sottoscrizione e alla consegna dell'avviso. Ad esempio, l'ora della violazione e l'ora della consegna dell'avviso.

Nome colonna	Tipo	Chiave	Descrizione
StatusDetailsId	INTEGER	Chiave primaria Generata automaticamente	
DetailsId	INTEGER	Chiave esterna (da MOT_TREND_DETAILS)	
Ora	BIGINT o NUMBER Data epoca Unix	N/D	Ora di raccolta dei dati
AlertType	SMALLINT o NUMBER	N/D	Tipo di consegna della notifica di sottoscrizione (ad esempio, posta elettronica)

### **MOT\_MES\_METRICS**

In questa tabella vengono registrate le informazioni relative ai controlli e alla metrica delle equazioni di controllo. Ad ogni metrica appartenente al controllo corrisponderà una voce in questa tabella.

Nome colonna	Tipo	Chiave	Descrizione
DataId	INTEGER	Chiave primaria Generata automaticamente	
DetailsId	INTEGER	Chiave esterna (da MOT_TREND_DETAILS)	
CUID	VARCHAR(64)	N/D	CUID del controllo
Nome	VARCHAR(255)	N/D	Nome del controllo



## Appendice sul foglio di lavoro della copia di sistema

### 35.1 Foglio di lavoro della copia del sistema

Proprietà	Valore
Chiave cluster.	
Nomi dei nodi.	
Nome computer e cartella di installazione della piattaforma BI di ogni computer della distribuzione.	
La password dell'amministratore della piattaforma BI.	
Connessioni al database CMS, nomi utente e password associate a tali connessioni per ogni computer della distribuzione.	
Connessioni al database di controllo, nomi utente e password associate a tali connessioni per ogni computer della distribuzione.	
Per ogni computer della distribuzione, dettagli su eventuali connessioni client ad altri database per ciascun computer del sistema di origine utilizzato da universi e report.	
Per ogni computer della distribuzione, tipi e versioni dei client di database.	

Proprietà	Valore
Versione, pacchetto di supporto e livello patch.	
I percorsi degli archivi file per ogni FRS di input e di output nella distribuzione.	
Se si intende copiare LCM (Lifecycle Management), il percorso della cartella del database LCM e le cartelle di Subversion di LCM.	
Se si intende copiare il database di monitoraggio, la cartella di quest'ultimo.	
Percorso della cartella di livello semantico.	



## Ulteriori informazioni

Informazioni	Posizione
Informazioni sul prodotto SAP BusinessObjects	<a href="http://www.sap.com">http://www.sap.com</a>
SAP Help Portal	<p>Passare a <a href="http://help.sap.com/businessobjects/">http://help.sap.com/businessobjects/</a> e nel pannello laterale "SAP BusinessObjects Overview" fare clic su <b>All Products</b>.</p> <p>Nel portale della Guida in linea SAP è possibile accedere alla documentazione più aggiornata riguardante tutti i prodotti SAP BusinessObjects e la relativa distribuzione. È possibile scaricare le versioni PDF o le librerie HTML installabili.</p> <p>Alcuni manuali sono memorizzati nel SAP Service Marketplace e non sono disponibili nel SAP Help Portal. Questi manuali sono elencati nell'Help Portal accompagnati da un collegamento al SAP Service Marketplace. I clienti con contratto di manutenzione dispongono di un ID utente autorizzato per l'accesso a questo sito. Per ottenere un ID, contattare il rappresentante del supporto tecnico.</p>
SAP Service Marketplace	<p><a href="http://service.sap.com/bosap-support">http://service.sap.com/bosap-support</a> &gt; Documentazione</p> <ul style="list-style-type: none"> <li>• Guide all'installazione: <a href="https://service.sap.com/bosap-instguides">https://service.sap.com/bosap-instguides</a></li> <li>• Note sulla versione: <a href="http://service.sap.com/releasenotes">http://service.sap.com/releasenotes</a></li> </ul> <p>Nel SAP Service Marketplace sono memorizzati alcuni documenti dei seguenti tipi: guide all'installazione, manuali di aggiornamento e migrazione, manuali della distribuzione in rete, note sulla versione e documenti relativi alle piattaforme supportate. I clienti con contratto di manutenzione dispongono di un ID utente autorizzato per l'accesso a questo sito. Per ottenere un ID, contattare il rappresentante del supporto tecnico. Se si viene reindirizzati al SAP Service Marketplace dal SAP Help Portal, utilizzare il menu nel riquadro di spostamento sulla sinistra per individuare la categoria contenente la documentazione a cui si desidera accedere.</p>
Docupedia	<p><a href="https://cw.sdn.sap.com/cw/community/docupedia">https://cw.sdn.sap.com/cw/community/docupedia</a></p> <p>Docupedia fornisce ulteriori risorse di documentazione, un ambiente di creazione collaborativo e un canale di feedback interattivo.</p>

Informazioni	Posizione
Risorse per lo sviluppatore	<a href="https://boc.sdn.sap.com/">https://boc.sdn.sap.com/</a> <a href="https://www.sdn.sap.com/irj/sdn/businessobjects-sdklibrary">https://www.sdn.sap.com/irj/sdn/businessobjects-sdklibrary</a>
Articoli su SAP BusinessObjects relativi a SAP Community Network	<a href="https://www.sdn.sap.com/irj/boc/businessobjects-articles">https://www.sdn.sap.com/irj/boc/businessobjects-articles</a> Questi articoli erano conosciuti in precedenza come schede tecniche.
Note	<a href="https://service.sap.com/notes">https://service.sap.com/notes</a> Queste note erano conosciute in precedenza come articoli di knowledge base.
Forum su SAP Community Network	<a href="https://www.sdn.sap.com/irj/scn/forums">https://www.sdn.sap.com/irj/scn/forums</a>
Formazione	<a href="http://www.sap.com/services/education">http://www.sap.com/services/education</a> I pacchetti di formazione disponibili variano dal tradizionale apprendimento in classe ai seminari di e-learning mirati e sono in grado di soddisfare qualsiasi esigenza e stile di apprendimento.
Supporto tecnico in linea	<a href="http://service.sap.com/bosap-support">http://service.sap.com/bosap-support</a> SAP Support Portal contiene informazioni sui programmi e i servizi del supporto tecnico. Inoltre, contiene collegamenti a una vasta gamma di informazioni tecniche e download. I clienti con contratto di manutenzione dispongono di un ID utente autorizzato per l'accesso a questo sito. Per ottenere un ID, contattare il rappresentante del supporto tecnico.
Consulenza	<a href="http://www.sap.com/services/bysubject/businessobjectsconsulting">http://www.sap.com/services/bysubject/businessobjectsconsulting</a> I consulenti sono a disposizione dei clienti dalla fase di analisi iniziale fino alla consegna del progetto di distribuzione. Possono essere fornite consulenze su argomenti quali i database relazionali e multidimensionali, la connettività, gli strumenti di progettazione del database e la tecnologia di incorporamento personalizzata.

# Indice

## A

- abilitazione
  - server 386, 387
- accesso 129
  - applicazioni 608
  - BI Launch Pad 122, 608
  - CMC 608
  - connessioni universo 681
  - gruppi 121
  - gruppi server 399
  - pannello HTML query 623
  - personalizzazione 663
  - Posta in arrivo 121
  - protezione contro tentativi di accesso non autorizzati 165
  - server 399
  - utenti 121
  - workflow 83
- accesso alla scheda, CMC
  - restrizione 618
  - risoluzione dei problemi 619
- accesso alle schede, CMC
  - autorizzazioni, ereditarietà 615
  - gestione dell'autorizzazione per la configurazione per altri utenti 616
  - gestione per altri utenti 613, 614
  - panoramica 613
  - Personalizzazione 617
- account di servizio
  - configurazione dei server 282
  - delega 274
  - impostazione 274
- account Guest
  - disabilitazione 117
- account sistema 309
- account SAdmin 914
- account utente
  - creazione 111
  - eliminazione 113
  - gestione 107, 111
  - modifica 112
  - predefinita 107
- Adaptive Job Server 27, 47, 996, 1057
  - opzioni della riga di comando 936
  - Timeout del socket 820
- Adaptive Processing Server 27, 47, 687, 996
- affinità, e SSL 162
- Agente di monitoraggio 703
- aggiornamenti 47
- aggiornamento 542, 562
  - ricorrenti e in sospeso
  - istanze processo 571
  - stato
    - promozione processo pianificata 571
- aggiornare il contenuto di Subversion 542
- Aggiungi oggetti 568
- aggiunta 391
  - CMS 393
  - membri del cluster 391
  - server 388
  - sistemi host 550
  - sottogruppi 115
  - utenti ai gruppi 118
- aggiunta del servizio Web 556
- aggiunta di infoobject 562
- aggiunta in blocco
  - gruppi 116
  - utenti 116
- albero di spostamento
  - server 377
- alias
  - assegnazione a utenti 127
  - creazione 126
    - per nuovi utenti 125
    - per utenti esistenti 126
  - disabilitazione 128
  - eliminazione 127
  - gestione 125
- alias utente 127
  - assegnazione 127
  - creazione 126
    - per nuovi utenti 125
    - per utenti esistenti 126
  - disabilitazione 128
  - eliminazione 127
- ambienti di rete
  - IPv4
    - nodi IPv4/IPv6 doppi 408
  - IPv6 408
- ambito dei diritti 135
- amministrazione
  - applicazioni 608
  - assegnazione dei diritti di 373
  - BI Launch Pad 608
  - CMC 608
  - delega 153
  - diritti 153
- amministrazione (*segue*)
  - gruppi 121
  - Posta in arrivo 121
  - server e gruppi server 399
  - utenti 121
- amministrazione dei servizi Web RESTful
  - abilitazione dello stack dei messaggi di errore 484
  - configurazione dell'URL di base 483
  - dimensioni del pool sessioni 485
  - impostazione del valore di timeout del token di sessione 485
  - impostazione delle dimensioni predefinite della pagina 485
  - opzioni della riga di comando 483
  - opzioni della riga di comando per l'autenticazione affidabile 491
  - pool sessioni 485
  - timeout del pool sessioni 485
  - TrustedPrincipal.conf 489
  - web.xml 488
- amministrazione delegata 153
  - gruppi di utenti 616
  - panoramica 613
- analisi 78
- analisi end-to-end 917
- Analysis, versione per OLAP 82
- API remota JMX 701
- applicazioni 607
  - proprietà 639, 757
  - Ricerca piattaforma 638, 639, 757
- applicazioni di collaborazione, integrazione
  - introduzione 630
  - prerequisiti 630
- applicazioni Web BEx 645
- architettura 35, 687
  - Ricerca piattaforma 763
- archivio file di input 98
- archivio file di output 98
- assistente 29
- attendibilità, relazione di trust attiva 161
- attributi, token di accesso 162
- autenticazione 44
  - Autenticazione affidabile 239
  - azienda 236
  - Enterprise 547
  - LDAP 251, 252, 547

autenticazione (*segue*)  
 plug-in di protezione 233  
 primario 232  
 server del contenitore di  
 applicazioni Web (WACS) 474  
 tipi 109  
 Windows AD 273, 547  
 autenticazione affidabile 665  
 configurazione di esempio 247  
 proprietà 243  
 Autenticazione affidabile 239  
 SAML 241  
 utente principale 249  
 autenticazione di base HTTP 486  
 autenticazione principale 232  
 autenticazione SAP 308  
 opzioni CMC 312  
 autorizzazione, sistemi 310  
 autorizzazioni  
 applicazione 857  
 diritti in piattaforma BI 827  
 per l'accesso ai dati SAP 857  
 per Servizi della piattaforma  
 informazioni 309  
 workbench per l'amministrazione  
 dei contenuti 833  
 avvio automatico di server 95, 385  
 avvisi 686  
 Avvisi 626  
 diritti 988  
 gestione 626  
 gestione delle impostazioni 626  
 proprietà di destinazione 626  
 proprietà predefinite 627

## B

backup a caldo 501, 505, 506  
 backup a freddo 501, 505  
 backup bare metal 501, 505  
 backup della piattaforma BI 501, 506  
 backup a caldo 501, 505  
 backup a caldo:abilitare 507  
 backup a freddo 505  
 impostazioni server 509, 510, 511  
 prerequisiti del backup a caldo 506  
 backup di applicazione 501  
 backup di sistema 501, 505  
 BackupCluster.bat 511  
 backupcluster.sh 511  
 BI Launch Pad 80  
 accesso 122  
 configurazione 121  
 controllo accesso a 608  
 diritti 977  
 gestione 622

BI Launch Pad (*segue*)  
 personalizzazione dell'accesso 663  
 preferenze per i gruppi 123  
 bilanciamento del carico 162  
 aggiunta di un server CMS 393  
 clustering 391  
 e protezione distribuita 162  
 server del contenitore di  
 applicazioni Web (WACS) 492  
 BO\_trace.ini  
 configurazione 898  
 Business view manager 72  
 BW  
 attivazione della visualizzazione  
 842  
 Integrazione con la piattaforma BI  
 827

## C

CA Wily Introscope 46  
 cacert.der 180  
 Cache Server 934  
 cakey.pem 180  
 capacità, Configurazione guidata del  
 sistema 97  
 cartella  
 creazione 557  
 cartella Promotion Management 547  
 cartelle  
 diritti 962  
 diritti relativi agli oggetti  
 ereditarietà 133  
 cartelle, Configurazione guidata del  
 sistema 98  
 categorie 123  
 diritti 962  
 Categorie di dati di monitoraggio 703  
 categorie di servizio 59, 377  
 CCM  
 abilitazione e disabilitazione dei  
 server 386, 387  
 aggiunta di un server 388  
 avvio, interruzione e riavvio dei  
 server 383, 385  
 eliminazione di un server 390  
 nodi 416  
 aggiunta 420  
 credenziali utente, modifica 440  
 eliminazione 427  
 ricreazione 424  
 ridenominazione 429  
 spostamento 431  
 per UNIX 919, 922  
 per Windows 927, 929  
 ccm.config 923

ccm.exe 927, 929  
 ccm.sh 919, 922  
 ripristino impostazioni server 520  
 Central Configuration Manager (CCM)  
 30, 76  
 Central Management Console (CMC)  
 29, 80  
 Central Management Server 27, 47,  
 547  
 Central Management Server.Vedere  
 CMS. 308  
 chiavi cluster 170  
 file dbinfo 171  
 panoramica 171  
 reimpostazione in UNIX 173  
 reimpostazione in Windows 172  
 chiavi del registro 262  
 chiavi di crittografia 170  
 CMC 175  
 contrassegno come compromesse  
 178  
 creazione di una nuova 177  
 elenco degli oggetti 177  
 revoca 179  
 stato 176  
 visualizzazione 175  
 ClearCase 47  
 client  
 Business view manager 72  
 Data Federator:vedere Strumento  
 di amministrazione di Data  
 Federation 75  
 desktop 71  
 Information Design Tool 74  
 Information Designer:vedere  
 Information Design Tool 74  
 Query come servizio Web 73  
 SAP BusinessObjects Analysis,  
 versione per Microsoft Office  
 78  
 SAP BusinessObjects Dashboards  
 78  
 SAP Crystal Reports 78  
 Strumento di amministrazione di  
 Data Federation 75  
 Strumento di conversione dei  
 report 73  
 Translation Management Tool 74  
 Universe Design Tool 73  
 Web 71  
 Web Intelligence Rich Client 72  
 widget per piattaforma SAP  
 BusinessObjects Business  
 Intelligence 75  
 client basati su browser 71  
 client desktop 71

- client Web 71
- client, basati su browser 79
  - Analysis, versione per OLAP 82
  - BI Launch Pad 80
  - Central Management Console (CMC) 29, 80
  - report, visualizzatori 81
  - SAP BusinessObjects Mobile 82
  - SAP BusinessObjects Web Intelligence 81
  - spazi di lavoro BI 80
- client, desktop
  - Central Configuration Manager (CCM) 30, 76
  - Repository Diagnostic Tool 30, 77
  - Upgrade Management Tool 30, 77
- clonazione
  - server 389, 390
  - server del contenitore di applicazioni Web (WACS) 467
- cluster 391, 393
  - aggiunta di un server CMS 393
  - modifica di nomi 395
  - nodi 391
  - visualizzazione dettagli 402
- Cluster Definition, strumento 845, 851
- CMC
  - abilitazione e disabilitazione dei server 386, 387
  - accesso alla scheda restrizione 618
  - risoluzione dei problemi 619
  - accesso alle schede
    - autorizzazioni, ereditarietà 615
    - gestione dell'autorizzazione per la configurazione per altri utenti 616
    - gestione per altri utenti 613, 614
    - panoramica 613
  - aggiunta della scheda Personalizzazione 617
  - amministrazione delegata
    - gruppi di utenti 616
    - panoramica 613
  - avvio, interruzione e riavvio dei server 383, 384
  - chiavi di crittografia 175
  - clonazione dei server 389, 390
  - controllo accesso a 608
  - dipendenze dei server Windows, aggiunta 439, 440
  - diritti 976
  - eliminazione di un server 390
  - gestione dei server 377
- CMS 308, 339
  - abilitazione e disabilitazione di altri server 386, 387
  - accesso 560
  - aggiunta a un cluster 393
  - autenticazione 232
  - avvio 385
  - clustering 391, 394
    - installazione di un membro cluster 393
    - requisiti 391
  - come server dei nomi 413, 414, 415
  - configurazione 413, 414, 415, 453, 454, 455, 456, 457
  - database SQL Anywhere, selezione 451
  - interruzione 385
  - metriche 402
  - modifica del nome di un cluster 395
  - opzioni della riga di comando 932
  - porta predefinita 413, 414, 415
  - proprietà 996
  - protezione distribuita 162
  - risoluzione dei problemi 385
  - risoluzione dei problemi dei computer multi-home 413
  - SAP HANA database, selezione 452
  - variabili di sessione 163
    - autenticazione 232
    - registrazione 163
- CMS, database di sistema 451, 452, 453, 454, 455
  - backup 506
  - copia 457, 458, 459
  - database SQL Anywhere, selezione 451
  - eliminazione 455, 456, 457
  - modifica della password 453
  - ricreazione 455, 456, 457
  - SAP HANA database, selezione 452
    - selezione 453, 454, 455
- cmsdbsetup.sh 923
- codice di licenza 106
  - acquisti 105
  - aggiunta 105
  - panoramica 105
  - visualizzazione 105
- codici di licenza
  - migrazione di database CMS 458
- codifica, token di accesso 162
- collaborazione
  - diritti 977
- completamento, Configurazione guidata del sistema 101
- componenti 845, 851
  - Cluster Definition, strumento 845, 851
- componenti, diagramma 36
- computer multi-home 410
  - server del contenitore di applicazioni Web (WACS) 493
- comunicazione 232
  - tra browser e server di applicazioni Web 232
  - tra server della piattaforma BI 189
- condivisione di istanze 814, 816
- configurazione 696
  - Apache 2.2 220
  - Autenticazione affidabile 240
  - cluster 391
  - cluster CMS 395
  - CMS, database 453, 454, 455
  - database di sistema CMS 455, 456, 457
  - firewall 199, 200
  - ISA 2006 221
  - livello applicazione 403
  - livello di elaborazione 403
  - livello intelligence 403
  - modelli configurazione 406
  - nodi 391
  - più server 405
  - Secure Sockets Layer 892
  - server reverse proxy 219, 220
  - WebSEAL 6.0 220
- configurazione controllo, vedere controllo 717
- configurazione della condivisione di risorse con diverse origini 487
- configurazione guidata del sistema 29
- Configurazione guidata del sistema 95
- configurazione guidata.consultare Configurazione guidata del sistema 29
- configurazione guidata.Vedere Configurazione guidata del sistema 95
- configurazione OpenSearch 755
- configurazione proxy inverso 756
- conflitti tra oggetti
  - replica bilaterale 807, 809
  - replica unilaterale 807
- confronto tra versioni diverse 542
- Confronto tra versioni diverse di un LCM 542
- connessione
  - nuovo CMS 560
- connessioni origini dati 681

- connessioni remote
  - creazione 797
  - creazione di cartelle 797
  - modifica 799
  - protezione 799
  - visualizzazione 796
- connessioni universo
  - diritti 974
  - eliminazione 681
  - gestione 681
  - replica 791
- Connettività 706
- Connettività InfoSet, trasporto 845
- Connettività Open SQL 845
- Connettività Open SQL, trasporto 845
- Contextual Awareness 889
  - configurazione 889, 891
- conti
  - gestione 107, 111
  - Servizi della piattaforma
    - informazioni 309
- controllo 545, 686
  - architettura 711
  - Archivio dati di controllo
    - diagramma schema 1079
    - tabelle schema 1079
  - attività Web 165
  - configurazione 717
  - dettagli eventi 734, 744, 747, 748, 749
- eventi
  - configurazione 719
  - elenco di 723
  - proprietà e dettagli 723
  - retention del database 721
- eventi comuni 734
- eventi di Analyzer 748
- eventi di Lifecycle Management
  - Console 749
- eventi piattaforma 744
- eventi Web Intelligence 747
- flusso di informazioni 711
- ID dettaglio evento 734, 744, 747, 748, 749
- ID tipo di evento 734, 744, 747, 748, 749
- impostazioni di connessione al database 721
- metriche 717
- pagina CMC 717
- proprietà eventi 734, 747, 748, 749
- riepilogo stato 717
- tipi di evento 734
  - Aggiungi VMS 749
  - Archivia VMS 749
  - Blocca VMS 749

- controllo (*segue*)
  - tipi di evento (*segue*)
    - connessione cubo MDAS 748
    - drill fuori dal livello 747
    - Esporta VMS 749
    - Estrai VMS 749
    - livello di accesso
      - personalizzato modificato 744
    - modifica dei diritti 744
    - modifica di controllo 744
    - pagina recuperata 747
    - Recupera VMS 749
    - rollback 749
    - Sblocca VMS 749
    - sessione MDAS 748
  - tipi di evento:accesso 734
  - tipi di evento:attivazione 734
  - tipi di evento:consegna 734
  - tipi di evento:creazione 734
  - tipi di evento:disconnessione 734
  - tipi di evento:eliminazione 734
  - tipi di evento:esecuzione 734
  - tipi di evento:modifica 734
  - tipi di evento:prompt 734
  - tipi di evento:recupero 734
  - tipi di evento:ricerca 734
  - tipi di evento:salvataggio 734
  - tipi di evento:visualizzazione 734
- controllo delle versioni 47
- controllo versioni 501
- cookie 163
  - registrazione delle sessioni 163
- token di accesso 162
- copia
  - livelli di accesso 147
  - processo esistente 560
- creazione
  - account utente 111
  - cartella 557
  - gruppi 114
  - livelli di accesso 148
  - nuovo processo 560
  - processo 558
  - sottogruppi di server 397
- credenziali utente, modifica per i nodi 440
- Cronologia 556
- cronologia di un processo
  - visualizzazione 572
- cruscotto 686
- Crystal Reports
  - diritti 966
  - vedere SAP Crystal Reports 78
- CTS 556
- CTS Transport (CTS+) 46

- CTS, opzioni 556
- custom.jsp 665

## D

- daemon, gestione dei segnali 931
- Dashboard Analytics Server 996
- Dashboard Builder 80
- Dashboard Server 996
- database 38
  - accesso con Single Sign-On 235
  - database SQL Anywhere 451
  - inizializzazione del CMS 455, 456, 457
  - SAP HANA, database 452
  - selezione per il CMS 453, 454, 455
  - universo 43
  - visualizzazioni 43
- database Derby, migrazione 691
- database di controllo 506
- database di controllo, migrazione del database Derby al 691
- Database di tendenza 687
- database di tendenza, migrazione 691
- database SQL Anywhere
  - selezione per il CMS 451
- database, migrazione di Derby 691
- dati
  - dinamici 146
  - salvati 146
- dati, accesso
  - panoramica sull'installazione 844
- definizione
  - schema ricorrente 570
- Definizione cluster, trasporto 845, 851
- Desktop Intelligence, documenti
  - diritti 963
- destinazione RFC 830
  - per il gateway SAP locale 831
  - per il servizio Publisher BW 830
- diagramma componenti 36
- diagramma dello schema del database di tendenza 1091
- diagramma dello schema, database di tendenza 1091
- dinamici, dati 146
- dipendenze 545
- dipendenze dei server
  - aggiunta 440
  - Registro eventi 439, 440
  - Remote Procedure Call 439, 440
- DIRINSTALL 24
- diritti 129, 373, 959
  - ambito dei diritti 135
  - amministrazione 153, 156
  - applicazioni 608



diritti (*segue*)  
 assegnazione ai principali 140  
 Avvisi 988  
 BI Launch Pad 608, 977  
 cartelle 962  
 cartelle di livello superiore 141  
 categorie 962  
 CMC 608, 976  
 connessioni universo 974  
 Crystal Reports 966  
 diritti  
   replica 782, 783, 784, 786, 787  
 diritti avanzati 130, 140  
 diritti del proprietario 156  
 diritti di amministrazione 373  
 diritti di pubblicazione 374  
 diritti effettivi 138  
 documenti Web Intelligence 963, 966  
 ereditarietà 131  
   cartella 133  
   gruppo 132  
   interruzione 151  
 Explorer 989  
 generale 959  
 gestione 138  
 gestione della protezione 782, 783, 784, 786, 787  
 gruppi 121, 968  
 gruppi server 399  
 Information Design Tool 986  
 limitazione dell'ambito 135  
 livelli di accesso 130, 970  
   attività 144  
   gestione tra siti 150  
   modifica dei diritti inclusi 149  
   query di relazione 150  
   replicati 150  
 Mobile 991  
 note 965  
 override dei diritti 134  
 Posta in arrivo 121  
 query protezione 141, 142  
 Report Application Server 399  
 server 399  
 spazi di lavoro BI 978  
 specifici del tipo 136  
 Strategy Builder 985  
 Universe Design Tool 986  
 universi (.unv) 970  
 universi (.unx) 972  
 utenti 121, 968  
 Visualizza e Visualizza su richiesta 146  
 visualizzazione 139  
 Web Intelligence 982

diritti (*segue*)  
 widget 987  
 diritti avanzati 130, 138, 140  
 diritti del proprietario 156  
 diritti di accesso per l'applicazione 546  
 diritti effettivi 138  
 diritti specifici  
   spazi di lavoro BI 978  
 disabilitazione  
   account Guest 117  
   alias 128  
   server 386, 387  
 discussioni  
   gestione delle impostazioni 619  
 dispositivo di origine 569  
 distribuzione  
   Publisher BW, componenti 830  
 dumrepo 542

## E

Editor definizione Protezione  
 trasporto 845, 849  
 elaborazione, livello 403  
 elenchi di controllo di accesso  
   aggiunta di principali 140  
   visualizzazione 139  
 elenchi di replica  
   creazione 793, 794  
   gestione 795  
   modifica 795, 796  
   oggetti supportati 792  
   opzioni di dipendenza 793, 794  
 elenchi scopi consentiti ai certificati 471  
 eliminazione 455, 456, 457, 550  
   account utente 113  
   alias 127  
   cartella 558  
   connessioni universo 681  
   database di sistema CMS 455, 456, 457  
   gruppi 116  
   istanze processo 551  
   livelli di accesso 148  
   server 390  
   server del contenitore di  
     applicazioni Web (WACS) 468  
   universi 682  
 eliminazione mappatura ruoli 343, 373  
 Enterprise Resource Planning (ERP) 45  
 env-locale.sh 925  
 env.sh 925  
 ereditarietà 131  
   cartella 133

ereditarietà (*segue*)  
 delle autorizzazioni di accesso alle  
   schede CMC 615  
 gruppo 132  
 interruzione 151  
 limitazioni 135  
 override dei diritti 134  
 ereditarietà cartelle 133  
   override dei diritti 134  
 esportazione di un processo  
   file BIAR 568  
 estensioni di elaborazione 167  
   condivisione 612  
   registrazione 611  
 estensioni, elaborazione 167  
 Event Server 996  
   opzioni della riga di comando 943  
 Explorer 771  
   diritti 989  
   vedere SAP BusinessObjects  
     Explorer 79  
 Explorer autorizzazioni 139

## F

facet 769  
 failover 706  
 federazione 779  
   aggiornamento dall'origine 787, 788, 789  
   aggiornamento dalla destinazione 787, 788, 789  
   connessioni remote 796  
     creazione 797  
     modifica 799  
   elenchi di replica 792  
     cartelle 793  
     creazione 793, 794  
     gestione 795  
   eliminazione oggetti 804, 805, 806  
   gestione della protezione 782, 783, 784, 786, 787  
   gestione di conflitti 807, 809  
   importazione e promozione di  
     contenuto replicato 817, 818, 819  
   istanze eseguite localmente 814, 816  
   livelli di accesso 150  
   miglioramento delle prestazioni 823  
   modalità di replica 787, 788, 789  
   pianificazione remota 814, 816  
   procedure consigliate 820  
   processi di replica 799  
     creazione 800  
     modifica 803

federazione (*segue*)  
 processi di replica (*segue*)  
 pianificazione 802, 803  
 reindirizzamento di siti di  
 destinazione 817, 819  
 replica bilaterale 787, 788, 789  
 replica di oggetti di grandi  
 dimensioni 820  
 replica unilaterale 787, 788, 789  
 risoluzione dei problemi 824  
 servizi Web 812, 813  
 termini 780  
 utenti e gruppi di terze parti, replica  
 790  
 vantaggi 779  
 visualizzazione di registri 803  
 file BIAR 567  
 importazione di un processo 569  
 processo di esportazione 568  
 file di certificati 180, 470  
 file di chiavi 180  
 file di controllo 98  
 file di dati 98  
 file di registro 98, 100, 101  
 file di registro di controllo 506  
 file di risposta 100, 101, 347  
 applicazione 349  
 creazione 347  
 file di risposta PeopleSoft 351  
 parametri 352  
 file host, configurazione per il firewall  
 NAT 202  
 file Kerberos 272  
 File Repository Server 27, 47, 996  
 backup 506  
 opzioni della riga di comando 941  
 file system  
 backup 506  
 file temporanei 98  
 file WAR BOE 122  
 firewall 164  
 comunicazione server 189  
 configurazione 199, 200  
 integrazione per Oracle  
 E-Business 213  
 integrazione SAP 210  
 configurazione per JD Edwards  
 EnterpriseOne 212  
 configurazione per l'integrazione  
 Siebel 216  
 configurazione per PeopleSoft  
 Enterprise 214  
 debug 203, 204  
 imposizione della registrazione dei  
 server tramite nome 416  
 scenari di configurazione 204

firewall (*segue*)  
 server del contenitore di  
 applicazioni Web (WACS) 493

## G

gateway SAP 331  
 distribuzione dei componenti 830  
 e SNC 331  
 installazione 831  
 pubblicazione mediante un  
 gateway locale 831  
 Generatore agente 703  
 gestione delle applicazioni 607  
 file war BOE 652  
 thread di discussione, eliminazione  
 622  
 gestione delle dipendenze 545, 562,  
 563  
 gestione delle versioni 540  
 Gestione delle versioni 545  
 Gestisci sistemi 550  
 grafico di tendenza 686  
 gruppi 318  
 aggiunta di sottogruppi 115  
 aggiunta di utenti 118  
 aggiunta, in blocco 116  
 assegnazione dei diritti a 140  
 concessione dell'accesso 121  
 controllo dei diritti 141, 142  
 creazione 114  
 diritti 968  
 ereditarietà 132  
 interruzione dell'ereditarietà  
 151  
 override dei diritti 134  
 per cartelle di livello superiore  
 141  
 eliminazione 116  
 gestione 108  
 mappatura 340, 357, 363, 369  
 modifica 114  
 predefinita 108  
 preferenze di BI Launch Pad 123  
 responsabili crittografia 174  
 specifica dell'appartenenza ai  
 gruppi 115  
 visualizzazione  
 diritti 139  
 membri 114  
 gruppi di terze parti, replica 790  
 gruppi di utenti  
 amministrazione delegata 616  
 gruppi server  
 accesso 399  
 creazione 396

gruppi server (*segue*)  
 nodi 377  
 sottogruppi 397  
 sottogruppi di server 395, 398  
 GWSETUP 831

## H

host 27, 47  
 configurazione di LDAP 253, 258  
 HTTP 163, 232  
 HTTPS  
 configurazione di server del  
 contenitore di applicazioni Web  
 (WACS) 469, 472, 493

## I

ID gestione modifiche 565  
 idm.keytab 488  
 idm.princ 488  
 idm.realm 488  
 importazione di un processo  
 file BIAR 569  
 Importazione guidata  
 vedere Upgrade Management Tool  
 30, 77  
 impostazione  
 istanze processo 551  
 processo di rollback 551  
 Impostazioni CTS, opzione 556  
 impostazioni di gestione delle versioni  
 540  
 impostazioni di memoria  
 modifica in un server del  
 contenitore di applicazioni Web  
 (WACS) 497  
 impostazioni predefinite  
 porte 413, 414, 415  
 server 407  
 Impostazioni processo 551  
 Impostazioni rollback 551  
 impostazioni server  
 backup 509, 510, 511  
 ccm.sh  
 backup impostazioni server 511  
 ripristino 518, 519, 520  
 indicizzazione 763  
 individuazione delle dipendenze di un  
 oggetto 564  
 infoobject  
 gestione di versioni differenti 539  
 infoobject filtrati 563  
 infoobject supportati 565  
 Information Design Tool 74  
 Information Design Tool, diritti 986



InfoView 80  
 initlaunch.sh 925  
 inizializzazione di un database di  
   sistema CMS 455, 456, 457  
 Input File Repository 27, 47, 996  
 installazione  
   gateway SAP in Windows 831  
   livelli di protezione predefiniti 828  
 integrazione  
   SAP 46  
   SNC 331  
 integrazione con le applicazioni di  
   collaborazione  
   chiave utente OAuth 633, 634, 637  
   console di amministrazione per le  
     applicazioni di collaborazione  
     633, 634, 637  
   introduzione 630  
   prerequisiti 630  
   spazi di lavoro BI 637  
 integrazione con SAP Jam  
   chiave utente OAuth 633, 634  
   console di amministrazione di SAP  
     Jam 633, 634  
   introduzione 630  
   prerequisiti 630  
 integrazione con SAP StreamWork  
   chiave utente OAuth 637  
   console di amministrazione di SAP  
     StreamWork 637  
   introduzione 630  
   prerequisiti 630  
   spazi di lavoro BI 637  
 integrazione in fase di ricerca con  
   NWES 771  
 intelligence, livello 403  
 interfaccia di rete  
   risoluzione dei problemi 412  
 interfaccia di rete non primaria 412  
 interfaccia di rete primaria 412  
 Introscope 706  
 invio della notifica 1091  
 IPv6  
   CMC 408  
   impostazione di indirizzi in CMC  
     410  
   opzioni 408  
 ISA 2006  
   configurazione per Oracle 10gR3  
     226  
   configurazione per Sun Java 8.2  
     226  
   configurazione per Tomcat 5.5 226  
   configurazione per WebSphere CE  
     2.0 226

istanze processo  
   eliminazione 551  
   impostazione 551  
 iView  
   attivazione della visualizzazione  
     842

## J

JAAS, file di configurazione 286, 287,  
   477  
 Java Application Server, Kerberos 284  
 Java Management Extensions (JMX)  
   687  
 Java, Kerberos 289, 290  
 JD Edwards EnterpriseOne 45  
 JD Edwards EnterpriseOne,  
   integrazione  
   configurazione firewall 212

## K

Kerberos 284, 476  
   e NetWeaver SSO 287  
   file di configurazione 285, 476  
   Krb5.ini 477  
   LDAP 271  
   risoluzione dei problemi 306, 478  
   Single Sign On per Java 300, 481,  
     482  
 KPI (Key Performance Indicator) 686  
 Krb5.ini 477

## L

LDAP  
   account 251  
   risoluzione dei problemi 273  
   autenticazione 251  
   configurazione 253  
   autenticazione Kerberos 271  
   configurazione Single Sign On 262  
   file di configurazione degli accessi  
     272  
   gruppi  
     mappatura 263  
   host  
     configurazione 253, 258  
     gestione multipla 256  
   mapping a Windows AD 265  
   plug-in di autenticazione 252  
   plug-in di protezione 252  
   Secure Sockets Layer (SSL) 251  
 librerie condivise, come estensioni di  
   elaborazione 167

librerie di collegamento dinamico,  
   estensioni di elaborazione 167  
 Lightweight Directory Access  
   ProtocolVedere LDAP 251  
 limitazione  
   ambito dei diritti 135  
 limitazioni 167  
   accesso 166  
   account guest 167  
   password 166  
   utente 166  
 Live Office  
   configurazione per server reverse  
     proxy 223  
 livelli architettura 37  
 livelli di accesso 130, 138, 153  
   amministrazione 153  
   assegnazione ai principali 140  
   attività, diritti richiesti 144  
   copia 147  
   creazione 148  
   diritti 970  
   eliminazione 148  
   gestione tra siti 150  
   modifica dei diritti in 149  
   predefiniti 144  
   RAS 399  
   relazioni con gli oggetti 150  
   ridenominazione 148  
   Visualizza e Visualizza su richiesta  
     146  
   visualizzazione 139  
 livello applicazione 403  
 livello più elevato  
   cartelle, diritti 141  
 livello registro di analisi  
   server CMC, impostazione 897  
 logon.csp 232

## M

macchine multi-homed 411  
 mappatura 545  
 mappatura dei ruoli 318, 340, 357,  
   363, 369  
 MBean JMX 703  
 MBeans 687  
 metrica 686, 1091  
 metrica derivata 686  
 metrica topologica 686  
 metriche  
   visualizzazione 401  
 metriche globali del sistema 402  
 metriche server 1041  
   metriche del File Repository Server  
     Connessioni attive 1050

metriche server ( <i>segue</i> )	metriche server ( <i>segue</i> )	metriche server ( <i>segue</i> )
metriche del File Repository Server ( <i>segue</i> )	metriche di Adaptive Job Server ( <i>segue</i> )	Metriche di Adaptive Processing Server ( <i>segue</i> )
Dati inviati (MB) 1050	Impostazioni predefinite destinazione file system valide 1057	Numero di connessioni 1050
Dati scritti (MB) 1050	Impostazioni predefinite destinazione FTP valide 1057	Numero di connessioni attive per i connettori caricati 1050
Elenco di file attivi 1050	Impostazioni predefinite destinazione posta elettronica valide 1057	Numero di connettori caricati 1050
File attivi 1050	Impostazioni predefinite destinazione Posta in arrivo valide 1057	Numero di controlli 1050
Spazio su disco disponibile nella directory principale (%) 1050	Inizializzazione 1057	Numero di documenti indicizzati 1050
Spazio su disco disponibile nella directory principale (GB) 1050	N. massimo consentito processi 1057	Numero di errori di pagina durante GC (ultimi 15 minuti) 1050
Spazio su disco libero nella directory principale (GB) 1050	N. massimo consentito processi simultanei 1057	Numero di errori di pagina durante GC (ultimi 5 minuti) 1050
Spazio su disco totale nella directory principale (GB) 1050	PID 1057	Numero di GC completi 1050
metriche del Server del contenitore di applicazioni Web	Processi di picco 1057	Numero di metriche con tendenza 1050
Elenco di connettori WACS in esecuzione 1056	Processi simultanei 1057	Numero di metriche create dall'utente 1050
Errore connettori WACS all'avvio 1056	Richieste processi ricevute 1057	Numero di query che attendono risorse 1050
Metriche del server Web Intelligence	Servizi di pianificazione 1057	Numero di query che utilizzano il disco 1050
Conteggio contrassegno superiore della cache 1062	Servizio di pianificazione 1057	Numero di query che utilizzano memoria 1050
Conteggio soglia massima di memoria 1062	metriche di Adaptive Processing Server	Numero di query in esecuzione 1050
Conteggio soglia superiore di memoria 1062	Byte totali di disco utilizzati dall'esecuzione query 1050	Numero di query nel passaggio di analisi query 1050
Dimensione cache (Kb) 1062	Byte totali di memoria utilizzati dall'esecuzione query 1050	Numero di query nel passaggio di ottimizzazione query 1050
Dimensioni della memory virtuale (Mb) 1062	Byte totali di memoria utilizzati dalla cache metadati 1050	Numero di query non riuscite 1050
Numero corrente di chiamate client 1062	Byte totali prodotti dall'esecuzione query 1050	Numero di tentativi di estrazione non riusciti dall'avvio del servizio 1050
Numero corrente di sessioni 1062	Byte totali trasferiti dalle origini dati 1050	Numero di tentativi di estrazione riusciti dall'avvio del servizio 1050
Numero corrente di sessioni attive 1062	Contatore thread in stallo JVM 1050	Numero di thread attivi 1050
Numero corrente di task 1062	Conteggio conflitti blocco JVM 1050	Percentuale di sistema arrestato durante GC (ultimi 15 minuti) 1050
Numero di documenti 1062	Conteggio cubi 1050	Percentuale di sistema arrestato durante GC (ultimi 5 minuti) 1050
Numero di documenti non aggiornati nella cache 1062	Conteggio query 1050	Percentuale utilizzo CPU (ultimi 15 minuti) 1050
Numero di documenti scambiati 1062	Conteggio sessione 1050	Percentuale utilizzo CPU (ultimi 5 minuti) 1050
Numero di errori estensione remota Web 1062	Data/ora ultima generazione archivio contenuti 1050	Processori disponibili 1050
Numero di scambi di documenti 1062	Data/ora ultimo aggiornamento indice 1050	Record totali prodotti dall'esecuzione query 1050
Numero di thread attivi 1062	Dimensioni pool di thread livello di trasporto 1050	Record totali trasferiti dalle origini dati 1050
Numero di timeout di sessioni 1062	DSLServiceMetrics.activeConnectionCount 1050	RecordBean.monitoringAppPropEnabled 1050
Numero di utenti 1062	DSLServiceMetrics.activeOLAPConnectionCount 1050	Servizi 1050
Numero totale di chiamate client 1062	DSLServiceMetrics.activeSessionCount 1050	Servizio disponibile 1050
Numero totale di sessioni 1062	DSLServiceMetrics.queryCount 1050	Tempo di calcolo medio stato controllo per gli ultimi 15 cicli (msec) 1050
Numero totale di task 1062	Eventi di controllo ricevuti 1050	Tempo di calcolo medio stato controllo per gli ultimi 15 cicli (msec) 1050
Numero totale di thread 1062	Flag analisi JVM 1050	Tempo di calcolo medio stato controllo per gli ultimi 15 cicli (msec) 1050
Tempo di inattività (secondi) 1062	Il servizio Data Federation è disponibile 1050	Tempo di calcolo medio stato controllo per gli ultimi 15 cicli (msec) 1050
Tempo totale CPU (secondi) 1062	Indicizzazione in esecuzione 1050	Tempo di calcolo medio stato controllo per gli ultimi 15 cicli (msec) 1050
Utilizzo CPU (%) 1062	Informazioni debug JVM 1050	Tempo di calcolo medio stato controllo per gli ultimi 15 cicli (msec) 1050
metriche di Adaptive Job Server	Informazioni versione JVM 1050	Tempo di calcolo medio stato controllo per gli ultimi 15 cicli (msec) 1050
Arresto in corso 1057	Intervallo di aggiornamento metriche di monitoraggio (secondi) 1050	Tempo di calcolo medio stato controllo per gli ultimi 15 cicli (msec) 1050
Creazioni processi non riuscite 1057	Memoria libera (MB) 1050	Tempo di calcolo medio stato controllo per gli ultimi 15 cicli (msec) 1050
Directory temporanea 1057	Memoria massima (MB) 1050	Tempo di calcolo medio stato controllo per gli ultimi 15 cicli (msec) 1050
Elementi secondari 1057	Memoria totale (MB) 1050	Tempo di calcolo medio stato controllo per gli ultimi 15 cicli (msec) 1050
Errori comunicazione 1057		Tempo di calcolo medio stato controllo per gli ultimi 15 cicli (msec) 1050

metriche server ( <i>segue</i> )	metriche server ( <i>segue</i> )	metriche server, informazioni ( <i>segue</i> )
Metriche di Crystal Reports Server ( <i>segue</i> ) Numero di connessioni aperte 1059 Numero di richieste in coda 1059 Numero di richieste non riuscite 1059 ObjectDllName 1059 Processi aperti 1059 Processi report attualmente aperti 1059 Richieste servite 1059 Riscontri cache (%) 1059 Tempo di elaborazione massimo (msec) 1059 Tempo di elaborazione medio (msec) 1059 Tempo di elaborazione minimo (msec) 1059 Tipo oggetto 1059	Servizio Central Management, metriche ( <i>segue</i> ) Nome connessione database di sistema 1044 Nome origine dati 1044 Nome server database di sistema 1044 Nome utente database di controllo 1044 Nome utente database di sistema 1044 Numero build 1044 Numero di accessi utente dall'avvio 1044 Numero di commit dall'avvio 1044 Numero di oggetti nel database di sistema di CMS 1044 Numero di oggetti nella cache di sistema di CMS 1044 Numero di query dall'avvio 1044 Numero di sessioni stabilite da tutti gli utenti 1044 Numero di sessioni stabilite da utenti simultanei 1044 Numero di sessioni stabilite da utenti specifici 1044 Numero di sessioni stabilite dai server 1044 Numero massimo di sessioni utente dall'avvio 1044 Processi completati 1044 Processi in attesa 1044 Processi in esecuzione 1044 Processi in sospeso 1044 Processi non riusciti 1044 Richieste database di sistema in sospeso 1044 Server CMS cluster 1044 Strumento di controllo CMS 1044 Tempo di risposta a commit più lungo dall'avvio (msec) 1044 Tempo di risposta alle query più lungo dall'avvio (msec) 1044 Tempo medio di risposta a commit dall'avvio (msec) 1044 Tempo medio di risposta alle query dall'avvio (msec) 1044 Ultimo aggiornamento database di controllo 1044 Utilizzo thread di controllo 1044 Versione prodotto 1044 Versione risorsa 1044 visualizzazione 402	metriche comuni ( <i>segue</i> ) Nome host 1042 Nome macchina 1042 Nome registrato 1042 Ora locale 1042 PID 1042 Porta richiesta 1042 RAM (MB) 1042 Server dei nomi 1042 Sistema operativo 1042 Spazio su disco utilizzato (GB) 1042 Thread server occupato 1042 Tipo CPU 1042 Versione 1042 Metriche di controllo Numero corrente degli eventi di controllo in coda 1042 migrazione del database Derby al database di controllo 691 Mobile diritti 991 modalità conforme a FIPS attivazione in UNIX 169 attivazione in Windows 169 disattivazione in Windows 170 Federal Information Processing Standard 168 impostazione protezione 168 modalità di configurazione 346 modalità di esecuzione 346 speciali configurazione 405 applicazione 406 impostazione 406 procedure consigliate 405 ripristino dei valori predefiniti di sistema 407 modelli di protezione predefiniti 828 modello di distribuzione 97 modello, distribuzione 97 modifica di un processo 562 monitoraggio 685 monitoraggio, diagramma dello schema 1091
metriche di Event Server Elenco di file monitorati 1049 File monitorati 1049		
metriche server di Dashboards Dati trasferiti (KB) 1064 Dimensioni cache (KB) 1064 Frequenza errori di richieste 1064 MaxChildProcesses 1064 Numero di connessioni aperte 1064 Numero di processi aperti 1064 Numero di richieste in coda 1064 Numero di richieste non riuscite 1064 Numero di richieste servite 1064 ObjectDllName 1064 Processi aperti 1064 Riscontri cache (%) 1064 Tempo di elaborazione massimo (msec) 1064 Tempo di elaborazione medio (msec) 1064 Tempo di elaborazione minimo (msec) 1064 Tipo oggetto 1064	Servizio Central Management, metriche Account utente simultanei esistenti 1044 Account utente specifici esistenti 1044 Connessione al database di controllo stabilita 1044 Connessioni database di sistema stabilite 1044 Connessioni database di sistema utilizzate correntemente 1044 Data build 1044 Durata ultimo ciclo di polling del thread di controllo (secondi) 1044 Licenze utente simultanee 1044 Licenze utenti specifici 1044 Nome connessione database di controllo 1044	
	metriche server, informazioni metriche comuni CPU 1042 Dimensione disco (GB) 1042 Directory di registrazione 1042 Indirizzo IP host 1042	
		<b>N</b> Network Address Translation configurazione, file host server 202 nodi 27, 47, 416 aggiunta 419, 434 a un cluster 393 AddNode.bat 421 addnode.sh 423 CCM 420

- nodi (*segue*)
    - aggiunta (*segue*)
      - CMS 393
      - nuovo computer 420
      - serverconfig.sh 422
    - clustering 391
    - CMC 377
    - eliminazione 427, 434
      - CCM 427
      - serverconfig.sh 428
    - ricreazione 434
      - AddNode.bat 425
      - addnode.sh 426
      - CCM 424
      - RemoveNode.bat 427
      - removenode.sh 428
      - scenari 423
      - serverconfig.sh 425
    - ridenominazione 429
      - CCM 429
      - serverconfig.sh 430
    - spostamento 430, 436
      - CCM 431
      - MoveNode.bat 432
      - movenode.sh 433
      - serverconfig.sh 432
  - Normalizzazione della classificazione dei risultati della ricerca 769
  - note, diritti 965
  - notifica 687
  - numeri porta
    - conflitti 496, 497
    - modifica 413, 414, 415
    - server del contenitore di applicazioni Web (WACS) 496
  - numero di accessi, token di accesso 162
  - numero di minuti, token di accesso 162
- O**
- ODBC
    - CMS, database
    - connettività 458
  - odbc.ini
    - creazione per SQL Anywhere 418
  - oggetti
    - diritti 827, 959
    - impostazione 140
    - visualizzazione 139
  - oggetti di terze parti 565
  - oggetti gestiti 346
    - gruppo piattaforma BI 346, 350
    - ruoli PeopleSoft 346, 350
    - universi 346, 351
  - oggetti programma
    - abilitazione, disabilitazione 609, 610
    - autenticazione 609
  - oggetti report
    - diritti 966
    - diritti per la creazione/modifica 399
  - OpenDocument
    - personalizzazione dell'accesso 663
  - OpenSearch 754
  - OpenSearch mediante WDeploy 755
  - opzioni della riga di comando 580, 930
    - Adaptive Job Server 936
    - Cache Server 934
    - CMS 932
    - Event Server 943
    - Input e Output File Repository Server 941
    - SSL 180
  - opzioni della riga di comando per le promozioni 580
  - opzioni della riga di comando per Promotion Management 580
  - opzioni delle modalità di aggiornamento, per Federation 787, 789
  - opzioni di amministrazione
    - Gestisci sistemi 550
    - impostazioni di sostituzione 550
    - Impostazioni processo 550
    - Impostazioni rollback 550
  - Opzioni di amministrazione 545
  - opzioni di promozione 565
  - opzioni di ricerca 561
  - ora violazione 1091
  - Oracle
    - JAAS 287
    - Kerberos 285
    - opzioni Java 290
  - Oracle E-Business Suite 45
    - mappatura ruoli a piattaforma BI 369
  - Oracle E-Business Suite, integrazione configurazione firewall 213
  - Oracle EBS
    - aggiornamento degli alias 371
    - aggiornamento dei ruoli 371
  - ottimizzazione e ridimensionamento 97
  - Output File Repository 27, 47, 996
- P**
- pagina iniziale
    - Administrator, pannello 548
    - carrello degli acquisti 548
  - pagina iniziale (*segue*)
    - Spazio di lavoro, pannello 548
    - Struttura, pannello 548
    - Visualizzatore processi, pannello 548
  - pannello HTML query, diritti di accesso 623
  - panoramica 753
  - parametri di ricerca 561
  - parametri script, nodi
    - aggiunta 434
    - eliminazione 434
    - ricreazione 434
    - spostamento 436
  - parole chiave 558
  - password 453, 454, 455
    - limitazioni 166
    - modifica 119
    - opzioni 119, 238
    - per il database CMS 453
  - PeopleSoft Analytic Server 886
  - PeopleSoft Enterprise 45
  - PeopleSoft Enterprise, integrazione
    - configurazione firewall 214
  - percorso directory di installazione 417
  - Personal Security Environment
    - vedere PSE . 322
  - Personalizzazione del peso per la classificazione dei risultati della ricerca 770
  - personalizzazione dell'accesso
    - BI Launch Pad 663
    - OpenDocument 663
  - pianificazione 545
    - promozione di processo 570
  - pianificazione remota 814, 816
  - piattaforma BI
    - analisi, registrazione 895
    - backup e ripristino 506
    - cartelle di livello superiore, diritti 141
    - comunicazione tra i server 189
    - consigli relativi alla sicurezza 160
    - diritti 129
    - distribuzione con server proxy inverso 218
    - importazione dei ruoli 318
    - livelli del registro di analisi 609, 895
    - pianificazione ripristino d'emergenza 159
    - processo di autenticazione principale 232
  - piattaforma BI, server 703
    - configurazione dei file host per il firewall 202

- piattaforma BI, server (*segue*)
    - configurazione di Kerberos e browser 284
  - piattaforma SAP BusinessObjects
    - Business Intelligence
    - documentazione 24
    - server del contenitore applicazioni Web (WACS) 461
  - piattaforma SAP BusinessObjects Business Intelligence, widget 75
  - PLATFORM64DIR 24
  - PlatformServices.properties 394
  - plug-in
    - protezione 44
  - plug-in, protezione 233
  - Ponte di protezione per PeopleSoft EPM
    - file di risposta 347
  - Posta in arrivo
    - controllo accesso a 121
  - postinstall.sh 925
  - prestazioni 97, 685
    - bilanciamento del carico 162
    - cluster 391
  - principali
    - assegnazione dei diritti a 140
    - assegnazione di diritti avanzati 140
    - controllo dei diritti 141, 142
    - diritti, per cartelle di livello superiore 141
    - visualizzazione di diritti 139
  - probe 886, 1091
  - procedura guidata, configurazione del sistema 95
  - processi correlati al processo 556
  - Processi di promozione, pagina 556
  - processi di replica
    - creazione 800
    - modifica 803
    - opzioni di configurazione 800
    - pianificazione 802, 803
    - visualizzazione 799
  - processo
    - modifica 562
    - ricerca 561
  - processo di rollback 573
  - processo PSANALYTIC 886
  - processo PSAPPSRV 886
  - processo supportato
    - stato 572
  - prodotti, Configurazione guidata del sistema 95
  - profilo, parametri 331
  - Promotion Management 548
  - Promotion Management, diritti di accesso per l'applicazione 546
  - promozione 545
  - promozione di un processo 570
    - quando i repository sono connessi 565
    - utilizzo di un file BIAR 567
  - promozione di un processo quando i repository non sono connessi 567
  - protezione 44, 346, 373, 545, 828
    - applicazione 349
    - cartella 827
    - cartelle di livello superiore 141
    - controllo dell'attività Web 165
    - da browser a server Web 164
    - distribuita 162
    - estensioni di elaborazione 167
    - firewall 164
    - gestione 138
    - gestione delle impostazioni 350
    - impostazioni di importazione 346
    - in piattaforma BI 827
    - limitazioni 166
    - limitazioni all'account Guest 167
    - limitazioni per l'utente 166
    - limitazioni relative all'accesso 166
    - limitazioni relative alle password 166
    - modelli predefiniti 828
    - oggetti dell'universo 973
    - personalizzazione dei diritti 373
    - plug-in 44, 233
    - protezione contro tentativi di accesso non autorizzati 165
    - protezione dell'ambiente 164
    - query 141, 142
    - registrazione delle sessioni 163
    - relazione di trust attiva 161
    - server Web 164
  - protezione a livello di riga, estensioni di elaborazione 167
  - protezione dati
    - chiavi cluster 170
    - chiavi di crittografia 170
    - compatibilità con le versioni precedenti 168
    - crittografia 170
    - crittografia a due chiavi 168
    - crittografia, chiavi 170
    - modalità conforme a FIPS 168
    - modalità di elaborazione dati predefinita 168
    - panoramica 168
  - protezione di oggetti universo 973
  - protezione, plug-in 233, 308
    - autenticazione LDAP 252
    - autenticazione Windows AD 275
  - protocollo RMI 696
  - Prova promozione 545
  - PSE
    - configurazione dell'accesso 329
    - panoramica attendibilità lato server 322
  - pubblicazione
    - definizione dei ruoli per, in BW 832
    - impostazione 832
    - in background 840
    - in più sistemi della piattaforma BI 836
    - pianificazione in background 840
    - più report mediante i ruoli 838
    - report in modalità batch 842
    - report in un ruolo o un sistema 838
  - pubblicazione, assegnazione dei diritti di 374
  - Publisher BW
    - configurazione come servizio 829
    - configurazione su UNIX 829
    - distribuzione dei componenti 830
  - Publisher BW, servizio 829
    - avvio 830
    - configurazione 829
    - creazione di una destinazione RFC 830
- Q**
- QaaWS 545
  - query
    - protezione 141, 142
  - Query come servizio Web 73
  - query di relazione
    - per livelli di accesso 150
- R**
- RAM 97
  - registrazione 402, 917
    - analisi 895
    - attività server 402
    - attività Web 165
    - livelli, registro di analisi 609, 895
  - registrazione, sessioni 163
  - registro di analisi
    - livelli di registrazione 609, 895
  - Registro eventi 402, 439, 440
  - relazione di trust attiva 161
  - Remote Method Invocation (RMI) 687
  - Remote Procedure Call 439, 440
  - replica 501
    - oggetti 779
    - utenti e gruppi di terze parti 790
  - replica bilaterale 787, 788
  - replica unilaterale 787, 788



- report
    - aggiornamento di origini dati 841
    - eliminazione 841
    - pubblicazione 838
      - in modalità batch 842
  - Report Application Server
    - diritti richiesti per gli oggetti 399
    - opzioni della riga di comando 937
  - report, manutenzione 841
  - report, visualizzatori 81
  - Repository Diagnostic Tool 30, 77
    - tabella delle incoerenze
    - suggerimenti 954, 955
  - requisiti
    - clustering 391
  - responsabili crittografia 174
    - aggiunta di membri 174
  - restart.sh 925
  - RestoreCluster.bat 520
  - restorecluster.sh 520
  - reverse proxy, server
    - configurazione di Apache 2.2 220
    - configurazione di ISA 2006 221
    - configurazione di WebSEAL 6.0 220
    - configurazione speciale 223
    - cookie di sessione 226
    - distribuzione con un server del contenitore di applicazioni Web 492
    - Live Office 228
    - servizi Web 223, 224, 225
    - supportate 218
    - Tomcat 223, 224
    - URL visualizzatore 228
    - utilizzo con server del contenitore di applicazioni Web (WACS) 493
  - riavvio dei server 383, 384, 385
  - ricerca 620, 763
    - thread di discussione 620
  - Ricerca dalla funzionalità di ricerca di NetWeaver Enterprise 773
  - ricerca degli oggetti dipendenti 563
  - ricerca di oggetti dipendenti 564
  - Ricerca piattaforma 639, 757
  - ridenominazione, livelli di accesso 148
  - ridimensionamento e ottimizzazione 97
  - riga di comando, opzioni 940, 943
    - Report Application Server 937
    - Server di elaborazione 934
    - tutti i server 931
  - Riparazione automatica 775
  - ripristino
    - infoobject 573
  - ripristino (*segue*)
    - processo 572
    - valori predefiniti di sistema 407, 498
  - ripristino d'emergenza, pianificazione 159
  - ripristino della piattaforma BI 501
    - impostazioni server 518, 520
  - ripristino della piattaforma SAP BI
    - impostazioni server 519
  - risoluzione dei problemi 775
    - account LDAP 273
    - Impostazione di Kerberos 306
    - Kerberos 478
    - messaggi di errore 824
    - server del contenitore di applicazioni Web (WACS) 495
    - Single Sign On 262
  - risoluzione dei problemi delle interfacce di rete 413
  - risorse BI 545
  - rollback 545
    - processo in Promotion Management 572
  - Rollback completo 572
  - rollback di infoobject
    - dopo la scadenza della password 574
  - rollback di un processo
    - dopo la scadenza della password 573
  - Rollback parziale 573
  - ruoli 832
    - assegnazione dei diritti a 373
    - creazione per l'amministrazione 832
    - eliminazione mappatura 343, 373
    - importazione 318
    - mappatura 318, 340, 343, 357, 359, 363, 369
    - rimappatura 365
- S**
- salvataggio
    - nuovo processo 558
    - processo 560
  - salvati, dati 146
  - SAML
    - SSO 241
  - SAP
    - aggiornamento degli alias 320
    - aggiornamento dei ruoli 320
    - configurazione firewall 210
    - integrazione 46
    - SAP Business Explorer 645
    - SAP BusinessObjects Analysis, versione per Microsoft Office 78
    - SAP BusinessObjects Dashboards 78
    - SAP BusinessObjects Explorer 79, 628
      - gestione delle impostazioni 628
      - proprietà dell'applicazione 628
    - SAP BusinessObjects Mobile 82
    - SAP BusinessObjects SDK 167
    - SAP BusinessObjects Web Intelligence 81
    - SAP Crystal Reports 78
    - SAP ERP 45
    - SAP HANA
      - configurazione SSO 267, 649
    - SAP HANA, database
      - selezione per il CMS 452
    - SAP Jam
      - diritti 977
    - SAP Jam, integrazione
      - introduzione 630
      - prerequisiti 630
    - SAP Passport 917
    - SAP Solution Manager 46
      - panoramica 909
      - SLD 911
      - SMD 913
    - SAP StreamWork
      - diritti 977
    - SAPGENPSE 329
    - script di gestione dei nodi, percorso 417
    - script UNIX, panoramica 919
    - Script Windows, panoramica 926
    - script, Windows 926
    - SCRIPTDIR 24
    - scripts, UNIX 919
    - SDK
      - Ricerca piattaforma 753
    - Secure Network Communication
      - client e server 322
      - configurazione dei server 328
      - configurazione SAP 324
      - generazione PSE 327
      - gruppi server 330
      - impostazione dell'ambiente 326
      - impostazioni CMC 329
      - libreria di crittografia SAP 322
      - pubblicazioni multi-pass 331
      - server della piattaforma BI 322
      - workflow 326
    - Secure Network Communication (SNC), integrazione con configurazione per SNC 331
    - Secure Sockets Layer (SSL) 164, 180, 184, 185, 251
      - e bilanciamento del carico 162

Secure Sockets Layer (SSL) (*segue*)  
e LDAP 251

Secure Sockets Layer, configurazione  
892

segnali, gestione 931

segnaposto 1067  
strumentazione 916

segnaposto nodi 1067

segnaposto server 1067

segno di spunta verde, per il sistema  
predefinito 836

selezione degli oggetti dipendenti di  
un oggetto 563

selezione dei prodotti 95

semaforo 686

server 39

- Abilita autenticazione del client 996
- Abilita HTTP tramite proxy 996
- Abilita HTTPS 996
- abilitazione 386, 387
- accesso 399
- aggiunta 388
- albero di spostamento 377
- Alias certificato 996
- Associa a nome host o indirizzo IP  
996
- Associa a tutti gli indirizzi IP 996
- avvio 383, 384, 385
  - automatico 383, 384
- clonazione 389, 390
- comunicazione 189
- configurazione 403
- configurazione dei server per l'uso  
di account di servizio 282
- Connessioni richieste al database  
di sistema 996
- contrasto con i servizi 27, 47
- Dimensioni massime intestazione  
HTTP 996
- Directory archivio file 996
- Directory temporanea 996
- disabilitazione 386, 387
- elenco 377
- eliminazione 390
- errori 382
- gestione dei segnali UNIX 931
- impostare indirizzo IP 410
- impostazione account di servizio  
274
- impostazioni del server Web  
Intelligence
  - Soglia inferiore memoria 1036
  - Soglia massima memoria 1036
  - Soglia superiore memoria 1036
- impostazioni predefinite 407

server (*segue*)

- impostazioni relative alle  
prestazioni 404
- indirizzo IPv6 410
- interruzione 383, 384, 385
- Intervallo di polling eventi 996
- Intervallo di svuotamento 996
- Livello di registrazione 996
- modelli configurazione 405
  - applicazione 406
  - impostazione 406
- modifica 381
  - stato 381, 382
- modifica dell'appartenenza di  
gruppo 398
- N. massimo richieste simultanee  
996
- nodi 27, 47
- nome host 410
- Nome host proxy 996
- Numero massimo di connessioni  
attive per sessione utente 996
- Numero massimo di connessioni  
inattive per sessione utente 996
- Numero max. processi simultanei  
996
- Numero max. richieste secondarie  
996
- Numero max. tentativi per  
l'accesso file 996
- Offset porta 996
- opzioni della riga di comando  
standard 931
- opzioni di identificazione host 408
- Password di accesso alle chiavi  
private 996
- Password di accesso alle chiavi  
private dell'elenco degli scopi  
consentiti ai certificati 996
- Percorso file elenco scopi  
consentiti ai certificati 996
- Porta 996
- Porta HTTP 996
- Porta HTTPS 996
- Porta proxy 996
- Porta server dei nomi 996
- Posizione file bscLogin.conf 996
- Posizione file elenco scopi  
consentiti ai certificati 996
- Posizione file Krb5.ini 996
- proprietà 404
- proprietà comuni del server
  - Assegna automaticamente 993
  - Avvia automaticamente questo  
server all'avvio di Server  
Intelligence Agent 993

server (*segue*)

- proprietà comuni del server (*segue*)
  - Identificatori host 993
  - Imposta modello configurazione  
993
  - Livello di registrazione 993
  - Porta richiesta 993
  - Ripristina valori predefiniti di  
sistema 993
  - Usa modello configurazione  
993
- proprietà dei server di Dashboards
  - Argomenti Java VM 1037
  - Argomenti VM elemento  
secondario Java 1037
  - Condividi dati tra i client 1037
  - Consenti ai processi report di  
rimanere connessi al  
database fino alla chiusura  
del processo report 1037
  - Dati meno recenti forniti ai  
client su richiesta (secondi)  
1037
  - Dimensioni cache massime  
(KB) 1037
  - Durata massima dei processi  
per elemento secondario  
1037
  - Numero massimo di elementi  
secondari preavviati 1037
  - Numero max. processi  
simultanei 1037
  - Record di database letti  
durante l'anteprima o  
l'aggiornamento 1037
  - Timeout cache di protezione  
(minuti) 1037
  - Timeout connessione inattiva  
1037
  - Timeout connessione inattiva  
(minuti) 1037
  - Timeout processo inattivo 1037
- proprietà dei servizi applicazioni
  - Web BEx
    - conteggio connessione server  
JCo 1026
  - destinazione RFC server JCo  
1026
  - host gateway server JCo 1026
  - Numero massimo sessioni  
client 1026
  - SAP BW Master System 1026
  - servizio gateway server JCo  
1026

*server (segue)*

- proprietà dei servizi Data Federation
  - Connessioni max 1028
  - dimensione pool di esecuzione 1028
  - Timeout inattività connessione 1028
  - Timeout inattività istruzione 1028
- proprietà dei servizi di analisi multidimensionali
  - Numero massimo di celle restituite da una query 1026
  - Numero massimo di membri restituiti durante il filtraggio 1026
  - Numero massimo sessioni client 1026
- proprietà dei servizi principali
  - Abilita autenticazione del client 996
  - Abilita HTTP tramite proxy 996
  - Abilita HTTPS 996
  - accesso a più domini, Javascript 996
  - Alias certificato 996
  - Associa a nome host o indirizzo IP 996
  - Associa a tutti gli indirizzi IP 996
  - autenticazione di base HTTP, abilitazione 996
  - Configurazione della condivisione di risorse con diverse origini 996
  - Connessioni richieste al database di sistema 996
  - Dimensione pool di thread 996
  - Dimensioni massime intestazione HTTP 996
  - Dimensioni pool sessioni 996
  - Directory archivio file 996
  - Directory temporanea 996
  - Durata max 996
  - Intervallo di polling eventi 996
  - Intervallo di svuotamento 996
  - Livello di registrazione 996
  - Mostra stack errori 996
  - N. massimo richieste simultanee 996
  - Nome host proxy 996
  - Numero massimo di connessioni attive per sessione utente 996

*server (segue)*

- proprietà dei servizi principali (*segue*)
  - Numero massimo di connessioni inattive per sessione utente 996
  - Numero max. processi simultanei 996
  - Numero max. richieste secondarie 996
  - Numero max. tentativi per l'accesso file 996
  - Numero predefinito di oggetti in una pagina 996
  - Offset porta 996
  - pageSize 996
  - Password di accesso alle chiavi private 996
  - Password di accesso alle chiavi private dell'elenco degli scopi consentiti ai certificati 996
  - Percorso file elenco scopi consentiti ai certificati 996
  - Porta 996
  - Porta HTTP 996
  - Porta HTTPS 996
  - Porta proxy 996
  - Porta server dei nomi 996
  - Posizione file bscLogin.conf 996
  - Posizione file elenco scopi consentiti ai certificati 996
  - Posizione file Krb5.ini 996
  - Protocollo 996
  - Riconnessione automatica al database di sistema 996
  - SAPR3 996
  - Scadenza Single Sign-On 996
  - secDAP 996
  - secEnterprise 996
  - secWinAD 996
  - Servizio log analisi 996
  - Tempo massimo di attesa per connessione (in secondi) 996
  - Tempo massimo di inattività 996
  - Tentativo massimo 996
  - Timeout connessione inattiva 996
  - Timeout di avvio servizio 996
  - Timeout inattività oggetti transitori 996
  - Timeout pool sessioni 996

*server (segue)*

- proprietà dei servizi principali (*segue*)
  - Timeout scambio motore di visualizzazione (in secondi) 996
  - Timeout svuotamento motore di visualizzazione (in secondi) 996
  - Timeout token sessione Enterprise 996
  - Tipo archivio certificati 996
  - URL endpoint dell'agente JMX predefinito (IIOP) 996
- Proprietà di Connection Server
  - Abilita analisi middleware 1011
  - Abilita analisi processo 1011
  - Abilita raggruppamento HTTP 1011
  - Attiva origine dati 1011
  - Database 1011
  - Dimensioni blocco HTTP 1011
  - Intervallo timer oggetti transitori 1011
  - Livello rete 1011
  - Raggruppamento delle connessioni 1011
  - Timeout Connection Pool 1011
  - Timeout inattività oggetti transitori 1011
- proprietà di Crystal Reports Server
  - Argomenti Java VM 1016
  - Argomenti VM elemento secondario Java 1016
  - Condividi dati dei report tra i client 1016
  - Consenti ai processi report di rimanere connessi al database fino alla chiusura del processo report 1016
  - Dati meno recenti forniti ai client su richiesta 1016
  - Dimensione dati da sfogliare 1016
  - Dimensioni batch 1016
  - Dimensioni cache massime 1016
  - Directory file cache 1016
  - Directory temporanea 1016
  - Durata massima dei processi per elemento secondario 1016
  - L'aggiornamento del visualizzatore produce sempre i dati correnti 1016



- server (*segue*)
- proprietà di Crystal Reports Server (*segue*)
    - Numero di record di database da leggere durante l'anteprima o l'aggiornamento di un report 1016
    - Numero massimo di elementi secondari preavviati 1016
    - Numero max. processi simultanei 1016
    - Percorso classe Java 1016
    - Record di database letti durante l'anteprima o l'aggiornamento 1016
    - Scadenza Single Sign-On 1016
    - Timeout cache di protezione 1016
    - Timeout connessione inattiva 1016
    - Timeout processo inattivo 1016
  - Proprietà servizi Web Intelligence
    - Abilita analisi memoria 1028
    - Abilita cache documento 1028
    - Abilita cache elenco dei valori 1028
    - Abilita cache in tempo reale 1028
    - Abilita monitoraggio 1028
    - Abilita monitoraggio servizio APS 1028
    - Abilita registri attività corrente 1028
    - Abilita utilizzo di URL HTTP 1028
    - Consenti errori dimensione massima mappa 1028
    - Dimensione massima cache documenti 1028
    - Dimensione massima flusso binario 1028
    - Dimensioni batch elenco dei valori 1028
    - Dimensioni batch elenco dei valori (voci) 1028
    - Dimensioni flusso caratteri massime 1028
    - Dimensioni LOV massime 1028
    - Dimensioni massime cache universo 1028
    - Dimensioni massime ordinamento personalizzato 1028
    - Directory cache di output 1028
    - Directory immagini 1028
- server (*segue*)
- Proprietà servizi Web Intelligence (*segue*)
    - Disabilita condivisione cache 1028
    - Errore di ping nuovo tentativo di conteggio su servizio APS 1028
    - Intervallo di polling del server 1028
    - Intervallo pulizia cache documento 1028
    - Numero max. connessioni 1028
    - Numero max. documenti nella cache 1028
    - Numero max. documenti per utente 1028
    - Numero max. documenti prima della reinizializzazione 1028
    - Periodo thread monitoraggio servizio APS 1028
    - Ritardo del loop del thread di monitoraggio (secondi) 1028
    - Scadenza Single Sign-On 1028
    - Soglia inferiore memoria 1028
    - Soglia massima memoria 1028
    - Soglia superiore memoria 1028
    - Spazio di riduzione massimo cache documenti 1028
    - Timeout cache 1028
    - Timeout connessione inattiva 1028
    - Timeout documento inattivo 1028
    - Timeout prima della reinizializzazione 1028
    - Timeout scambio motore di visualizzazione (in secondi) 1028
    - Timeout scambio risorse monitorate predefinite (in secondi) 1028
    - Timeout svuotamento motore di visualizzazione (in secondi) 1028
    - Timeout svuotamento risorse monitorate predefinite (in secondi) 1028
    - Valore proxy 1028
  - Protocollo 996
  - raggruppamento 395
  - registrazione dell'attività 402
  - registrazione tramite nome 416
  - riavvio 383, 384, 385
- server (*segue*)
- Riconnessione automatica al database di sistema 996
  - righe di comando 930
  - Scadenza Single Sign-On 996
  - segnaposto 389
  - stato 377, 381
  - Tempo massimo di attesa per connessione (in secondi) 996
  - Tempo massimo di inattività 996
  - Tentativo massimo 996
  - Timeout connessione inattiva 996
  - Timeout di avvio servizio 996
  - Timeout inattività oggetti transitori 996
  - Timeout scambio motore di visualizzazione (in secondi) 996
  - Timeout svuotamento motore di visualizzazione (in secondi) 996
  - Tipo archivio certificati 996
  - URL endpoint dell'agente JMX predefinito (IIOP) 996
  - visualizzazione dello stato di un server 382
- server del contenitore applicazioni Web (WACS) 40, 996
- aggiunta di servizi Web 468
  - connettori 461
  - panoramica 461
  - rimozione di servizi Web 469
  - servizio CMC 461
- server del contenitore di applicazioni Web (WACS)
- AD Kerberos 478
  - aggiunta 464
  - attività comuni 462
  - bilanciamento del carico 492
  - clonazione 467
  - computer multi-home 493
  - creazione di nuovi server 466
  - eliminazione 468
  - errori server 495
  - file di configurazione di Kerberos 476
  - file JAAS 477
  - firewall 493
  - HTTPS 469, 472, 493
  - installazione 465
  - metriche 1056
  - metriche del sistema 495
  - modifica delle impostazioni di memoria 497
  - proprietà 499
  - rimozione 464
  - ripristino dei valori predefiniti di sistema 498

- server del contenitore di applicazioni Web (WACS) (*segue*)
  - risoluzione dei conflitti tra porte 496, 497
  - risoluzione dei problemi 495
  - SSL 469, 472
  - utilizzo con altri server Web 491
  - utilizzo con server proxy 492, 493
- server della piattaforma SAP
  - BusinessObjects Business Intelligence
    - configurazione di Kerberos e browser 476
- server di applicazioni Web 39
  - autenticazione 232
- Server di elaborazione
  - opzioni della riga di comando 934
- Web Intelligence 940
- Server di elaborazione Crystal Reports 934
  - opzioni della riga di comando 934
- Server di elaborazione di Dashboards 934
  - opzioni della riga di comando 934
- Server di elaborazione Web
  - Intelligence 27, 47
- server di elenchi in linea 252
  - informazioni su LDAP 251
  - plug-in di protezione 252
- server di monitoraggio 706
- Server Intelligence Agent 26
  - avvio automatico di server 385
  - dipendenze dei server Windows,
    - aggiunta 439, 440
  - nodi 416, 419, 423, 427, 429
    - aggiunta 420, 421, 422, 423, 434
  - credenziali utente, modifica 440
  - eliminazione 427, 428, 434
  - nuovo computer, aggiunta 420
  - ricreazione 424, 425, 426, 427, 428, 434
  - ridenominazione 429, 430
  - spostamento 430, 431, 432, 433, 436
- Server Intelligence Agent (SIA)
  - workflow di arresto 85
  - workflow di avvio 84
- server proxy inverso
  - configurazione con la piattaforma BI 219, 220
  - distribuzione con la piattaforma BI 218
- server Web
  - protezione 164
- server, proprietà 993
- serverconfig.sh 924
  - nodi
    - aggiunta 422
    - eliminazione 428
    - ricreazione 425
    - ridenominazione 430
    - spostamento 432
- servizi 51
  - contrasto con i server 27, 47
  - errori 382
  - modelli configurazione 405
- Servizi della piattaforma informazioni
  - creazione di account per 309
  - diritti di amministrazione 373
  - diritti di pubblicazione 374
- servizi Web
  - aggiunta a un Server del contenitore di applicazioni Web 468
  - configurazione per server reverse proxy 223, 224, 225
  - distribuzione personalizzata 812, 813
  - memorizzazione di file nella cache 812, 813
  - rimozione da un Server del contenitore di applicazioni Web 469
  - variabile di sessione 812
- servizi Web RESTful 482
- Servizio applicazioni Web BEx 646
- servizio Business Process BI
  - aggiunta a un Server del contenitore di applicazioni Web 468
  - rimozione da un Server del contenitore di applicazioni Web 469
- servizio di monitoraggio 696
- servizio Web 556
- sessione, variabili 163
  - autenticazione 232
- sessioni 163
  - registrazione 163
- setup.sh 925
- setupinit.sh 925
- Siebel Enterprise 45
- Siebel, integrazione
  - configurazione firewall 216
  - Crystal Reports, creazione voce di menu 887
  - progetto di integrazione 886
  - ricompilazione applicazione Siebel 888
- sincronizzazione delle informazioni sui report 840, 841
- Single Sign On 44, 234, 301, 308
  - account di servizio 293
  - al database 235
  - anonimo 234
  - end-to-end 235
  - importazione dei ruoli 318
  - impostazione
    - LDAP 262
    - SiteMinder 262, 301
  - Kerberos 300, 481, 482
  - piattaforma BI 234
  - risoluzione dei problemi 262
- Single Sign On, configurazione per JD Edwards 879
- Single Sign On, configurazione per Oracle EBS 375
- Single Sign On, configurazione per PeopleSoft 882
- Single Sign On, configurazione per Siebel 891
- Single Sign-On anonimo 234
- Single Sign-On end-to-end 235
- Single Sign-On, configurazione per SAP NetWeaver 338
- Sistema di gestione delle versioni 539
- sistemi host
  - aggiungere 550
- SiteMinder
  - configurazione di Single Sign-On con LDAP 262, 301
  - configurazione plug-in LDAP 262
  - configurazione war BOE 262
  - errore 262
  - risoluzione dei problemi 262
  - Windows AD 301
- siti
  - gestione dei diritti 782, 783, 784, 786, 787
  - livelli di accesso 150
- siti di destinazione
  - livelli di accesso 150
- siti di origine
  - livelli di accesso 150
- SMD 913
  - agente SMD 914
- SNC
  - vedere Secure Network Communication 322
- Software Development Kit (SDK) 41
- Solution Manager 685
  - account SAdmin 914
- sottogruppi, aggiunta 115
- spazi di lavoro BI 80
- spazi di lavoro BI, diritti 978

- specifiche del sistema, visualizzazione 402
  - server del contenitore di applicazioni Web (WACS) 495
- specifici del tipo, diritti 136
  - Avvisi 988
  - BI Launch Pad 977
  - cartelle 962
  - categorie 962
  - CMC 976
  - connessioni universo 974
  - Crystal Reports 966
  - documenti Web Intelligence 963, 966
  - gruppi 968
  - Information Design Tool 986
  - livelli di accesso 970
  - note 965
  - Strategy Builder 985
  - Universe Design Tool 986
  - universi (.unv) 970
  - universi (.unx) 972
  - utenti 968
  - Web Intelligence 982
  - widget 987
- SQL Anywhere
  - creazione di odbc.ini 418
- SSL 180, 184, 185
  - certificati 180
  - chiavi 180
  - configurazione dei server 180, 184, 185
  - configurazione di server del contenitore di applicazioni Web (WACS) 469, 472
  - sslconfig.exe 186
  - Strumento di conversione dei report 188
  - thick client 186
  - Translation Management Tool 187
- SSL (Secure Socket Layer)
  - configurazione 880, 883
- SSL.Vedere Secure Sockets Layer (SSL) 251
- sslc.cnf 180
- sslc.exe 180
- startservers 925
- stati del server 377
- statistiche, controllo dell'attività Web 165
- stato di integrità 686
- stato, visualizzazione e modifica per i server 381, 382
- stopservers 925
- Strategy Builder, diritti 985

- strumentazione 917
  - livello Web 917
  - panoramica 915
  - registrazione 917
  - segnaposto 916
  - server non Java 915
  - verifica 917
- Strumento di amministrazione di Data Federation 75
- Strumento di conversione dei report 73
  - SSL 188
- Strumento di diagnostica del repository
  - errori
    - da oggetto a file 945
    - diagnosi e riparazione 945
    - scenari 945
  - panoramica 945
  - parametri 946
  - utilizzo
    - Windows e Unix 946
- Subversion 47
- SubVersion 539
- Subversion, aggiornamento 542
- Subversion, contenuto 542
- SubVersion, impostazioni 540
- suggerimenti 770
- suggerimenti sulle prestazioni 885
- supporto cluster 706, 754
- Supporto multilingua 770
- syslog 402
- System Landscape Directory (SLD) 46
  - file connect.key 911
  - registrazione 911
  - trigger 912
  - verifica della registrazione 913

## T

- tempo di risposta 685
- tendenza, definizione 686
- terze parti, plug-in di protezione 233
- thread di discussione 620
  - annullamento della ricerca 620
  - ordinamento dei risultati della ricerca 621
  - ricerca 620
- ticket 162
  - per la protezione distribuita 162
  - token di accesso 162
- Timeout del socket 820
- tipi di contenuto in cui è possibile eseguire ricerche 765
- tipi di server 63, 69
- token di accesso 162
  - autenticazione 232

- token di accesso (*segue*)
  - protezione distribuita 162
  - registrazione delle sessioni 163
- Tomcat
  - JAAS 286
  - Kerberos 285
- traccia
  - end-to-end 917
  - server 896
    - BO\_trace.ini, configurazione 898
- Translation Management Tool 74
- Translation Management Tool:
  - SSL 187
- trasferimento di attendibilità 162
- trasporti 845, 846
  - Connettività InfoSet 845, 849
  - Connettività Open SQL 847
  - definizione cluster 845, 851
  - definizione protezione a livello di riga 849
  - Editor definizione Protezione 845
  - gruppi di funzioni 844
  - importazione 846
  - oggetti 844
  - panoramica 844
  - personalizzazione dei parametri 845, 855
  - programmi 844
  - tabelle 844
  - verifica dei conflitti 846
  - workbench per l'amministrazione dei contenuti 851

## U

- Universe Design Tool 73
- Universe Design Tool, diritti 986
- Universe Designer
  - vedere Universe Design Tool 73
- universi 563
  - diritti (.unv) 970
  - diritti (.unx) 972
  - gestione 682
  - replica 791
- universo 43
- UNIX
  - syslog 402
- Upgrade Management Tool 30, 77
- utenti
  - aggiunta, in blocco 116
  - assegnazione dei diritti a 140
  - assegnazione di diritti avanzati 140
  - concessione dell'accesso 121
  - controllo dei diritti 141, 142
  - diritti 968

utenti (*segue*)  
 diritti, per cartelle di livello superiore 141  
 mappatura 340, 357, 363, 369  
 visualizzazione di diritti 139  
 utenti di terze parti, replica 790  
 utenti mappati, gestione degli alias 125  
 utilità SPN 274

## V

variabili  
 AIX 24  
 directory di installazione 24, 417  
 directory script 24  
 HP-UX 24  
 Linux 24  
 script di gestione dei nodi 417  
 sistema operativo UNIX 24  
 Solaris 24  
 verifica, Configurazione guidata del sistema 100  
 versioni 545  
 visualizzazione  
 cronologia di un processo 572  
 dettagli cluster CMS 402  
 diritti per principali 139  
 metriche correnti 401  
 metriche del server del contenitore di applicazioni Web (WACS) 495  
 metriche del sistema 402  
 visualizzazione dell'account corrente 106  
 visualizzazioni 43  
 Voyager 82  
 vedere SAP BusinessObjects Analysis 78

## W

WAR, file  
 applicazioni Web della piattaforma BI 218  
 BOE 218, 652, 653, 656, 659  
 dswsbobje 218  
 file war BOE  
 proprietà CMC 661  
 proprietà di BI Launch Pad 656  
 proprietà globali 653  
 proprietà OpenDocument 659

WDeploy 79  
 Web Intelligence 623, 936  
 diritti 982  
 diritti applicazione 623  
 diritti di accesso HTML query 623  
 personalizzazione dell'interfaccia 666  
 Server di elaborazione 940  
 Web Intelligence Rich Client 72  
 Web Intelligence, documenti  
 diritti 966  
 WebLogic  
 JAAS, file di configurazione 286  
 Kerberos 285  
 opzioni Java 289  
 WebSphere  
 JAAS 287  
 opzioni Java 290  
 widget  
 diritti 987  
 gestione delle impostazioni 628  
 Widget BI  
 vedere Widget per la piattaforma SAP BusinessObjects Business Intelligence 75  
 WinAD 547  
 Windows  
 dipendenze dei server, aggiunta 440  
 Registro eventi 402  
 Windows AD  
 account di servizio 293  
 account e gruppi 280  
 pianificazione di aggiornamenti 280  
 attivazione di Kerberos 474, 475  
 autenticazione 273  
 mapping di LDAP 265  
 plug-in di protezione 275  
 Single Sign On 293, 296, 297  
 Vintela 296, 297  
 workbench per l'amministrazione dei contenuti 836  
 aggiornamento dell'origine dati dei report 841  
 aggiunta di sistemi della piattaforma BI 836  
 applicazione delle autorizzazioni 833  
 definizione dei livelli di accesso dell'utente 833

workbench per l'amministrazione dei contenuti (*segue*)  
 eliminazione dei report 841  
 panoramica sulla pubblicazione dei report 832  
 pubblicazione dei report in background 840  
 pubblicazione di report 838  
 sincronizzazione delle informazioni sui report 840, 841  
 workflow 83  
 accesso utente 83  
 arresto SIA 85  
 avvio SIA 84  
 diritti avanzati, assegnazione 140  
 documento Web Intelligence pianificato 92  
 elenchi di controllo degli accessi, assegnazione di principali 140  
 esecuzione di un oggetto programma pianificato 86  
 esecuzione di un report SAP Crystal Reports 2011 pianificato 90  
 impostazione di diritti per cartelle di livello superiore 141  
 impostazione di una pianificazione per un documento Web Intelligence 92  
 impostazione di una pianificazione per un oggetto programma 85  
 impostazione di una pianificazione per un report Crystal 89  
 visualizzazione di diritti 139  
 visualizzazione di un documento Web Intelligence su richiesta 91  
 visualizzazione di un report Crystal Reports 2011 su richiesta 88  
 visualizzazione di una pagina Crystal Reports 2011 non memorizzata nella cache 87  
 visualizzazione di una pagina del report Crystal di cache 87  
 visualizzazione di uno spazio di lavoro Analysis 93

## X

Xcelsius.vedere SAP BusinessObjects Dashboards 78