SAP BusinessObjects

Manuale dell'amministratore della piattaforma Business Intelligence

- SAP BusinessObjects Business Intelligence platform 4.0 Support Package 2

2011-05-06

SAP

Copyright

© 2011 SAP AG. Tutti i diritti riservati.SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign e altri prodotti e servizi SAP qui menzionati, come anche i relativi logo, sono marchi o marchi depositati di SAP AG in Germania e in altri paesi. Business Objects e il logo Business Objects, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius e altri prodotti e servizi Business Objects menzionati nel presente documento nonché i rispettivi logo sono marchi o marchi registrati di Business Objects S.A. negli Stati Uniti e in altri paesi. Business Objects è una società SAP. Tutti gli altri nomi di prodotti e servizi qui menzionati sono marchi di proprietà dei rispettivi titolari. Questo documento ha finalità prettamente informative. Le specifiche nazionali dei prodotti possono variare di caso in caso. SAP si riserva il diritto di modificare tutti i materiali senza preavviso. I materiali sono forniti da SAP AG e dalle affiliate ("Gruppo SAP") a solo scopo informativo, senza alcun fine illustrativo o di garanzia di qualsiasi natura; il Gruppo SAP si astiene da una qualsiasi responsabilità conseguente ad eventuali errori od omissioni riscontrati nei materiali. Le uniche garanzie applicabili ai prodotti e ai servizi del Gruppo SAP sono quelle espressamente menzionate nelle apposite garanzie rilasciate per i singoli prodotti o servizi. Nessuna parte della presente nota scritta è da interpretarsi quale garanzia accessoria.

2011-05-06

Sommario

Capitolo 1 **Introduzione** **17**

1.1 Informazioni sulla guida 17
1.1.1 Destinatari del Manuale 17
1.1.2 Informazioni sulla piattaforma SAP BusinessObjects Business Intelligence 17
1.1.3 Variabili 18
1.2 Prima di iniziare 18
1.2.1 Concetti fondamentali 18
1.2.2 Strumenti di amministrazione principali 21
1.2.3 Attività principali 22

Capitolo 2 **Architettura** **25**

2.1 Presentazione dell'architettura 25
2.1.1 Panoramica del sistema 26
2.1.2 Database 27
2.1.3 Server 28
2.1.4 Server di applicazioni Web 29
2.1.5 Software Development Kit 31
2.1.6 Origini dati 34
2.1.7 Supporto delle lingue 35
2.1.8 Autenticazione e Single Sign On 36
2.1.9 Integrazione SAP 38
2.1.10 Lifecycle Management (LCM) 39
2.1.11 Controllo integrato delle versioni 40
2.1.12 Dati permanenti 40
2.1.13 Percorso di aggiornamento 40
2.2 Livelli concettuali 41
2.3 Servizi e server 42
2.3.1 Servizi 44
2.3.2 Categorie di servizio 51
2.3.3 Tipi di server 54
2.3.4 Server 58
2.4 Applicazioni client 61

2.4.1 Installate con Strumenti client della piattaforma SAP BusinessObjects Business Intelligence..62
2.4.2 Installate con la piattaforma SAP BusinessObjects Business Intelligence....66
2.4.3 Disponibile separatamente....67
2.4.4 Client di applicazioni Web....69
2.5 Workflow delle informazioni....72
2.5.1 Autenticazione....73
2.5.2 Pianificazione....74
2.5.3 Visualizzazione....79
2.5.4 Su richiesta....82

Capitolo 3 Gestione delle licenze....85

3.1 Gestione delle chiavi di licenza....85
3.1.1 Per visualizzare le informazioni sulle licenze....85
3.1.2 Per aggiungere un codice di licenza....85
3.1.3 Per visualizzare l'attività dell'account corrente....86
3.2 Misurazione delle licenze....86
3.2.1 Esecuzione di un controllo della licenza 87

Capitolo 4 Gestione di utenti e gruppi....89

4.1 Panoramica della gestione dei server....89
4.1.1 Gestione utenti....89
4.1.2 Gestione gruppi....91
4.1.3 Tipi di autenticazione disponibili 92
4.2 Gestione di account Enterprise e generali....94
4.2.1 Per creare un account utente....94
4.2.2 Per modificare un account utente....96
4.2.3 Per eliminare un account utente....96
4.2.4 Per creare un nuovo gruppo....97
4.2.5 Per modificare le proprietà di un gruppo....97
4.2.6 Per visualizzare i membri del gruppo....98
4.2.7 Per aggiungere i sottogruppi....98
4.2.8 Per specificare l'appartenenza al gruppo....99
4.2.9 Per eliminare un gruppo....99
4.2.10 Per abilitare l'account Guest....100
4.2.11 Aggiunta di utenti ai gruppi....100
4.2.12 Modifica delle impostazioni password....101
4.2.13 Concessione del diritto di accesso a utenti e gruppi....103
4.2.14 Controllo dell'accesso alle caselle di posta in entrata dell'utente....104
4.2.15 Configurazione delle opzioni di BI Launch Pad....104
4.3 Gestione degli alias....108

4.3.1 Per creare un utente e aggiungere un alias di terze parti....108
4.3.2 Per creare un nuovo alias per un utente esistente....109
4.3.3 Per assegnare un alias da un altro utente....110
4.3.4 Eliminazione di un alias....110
4.3.5 Per disattivare un alias....111

Capitolo 5 Impostazione dei diritti....113

5.1 Funzionamento dei diritti nella piattaforma BI....113
5.1.1 Livelli di accesso....113
5.1.2 Impostazioni dei diritti avanzati....114
5.1.3 Ereditarietà....115
5.1.4 Diritti specifici del tipo....120
5.1.5 Determinazione dei diritti effettivi....121
5.2 Gestione delle impostazioni di protezione per gli oggetti nella CMC....122
5.2.1 Per visualizzare i diritti per un principale su un oggetto....123
5.2.2 Per assegnare principali a un elenco di controllo di accesso per un oggetto....124
5.2.3 Per modificare la protezione per un principale su un oggetto....124
5.2.4 Impostazione dei diritti su una cartella di livello superiore nella piattaforma BI....125
5.2.5 Controllo impostazioni di protezione per un principale....125
5.3 Utilizzo di livelli di accesso....128
5.3.1 Scelta tra i livelli di accesso Visualizza e Visualizza su richiesta....130
5.3.2 Per copiare un livello di accesso esistente....131
5.3.3 Per creare un nuovo livello di accesso....132
5.3.4 Per rinominare un livello di accesso....132
5.3.5 Per eliminare un livello di accesso....132
5.3.6 Per modificare i diritti in un livello di accesso....133
5.3.7 Analisi e relazione tra livelli di accesso e oggetti....134
5.3.8 Gestione dei livelli di accesso tra i siti....134
5.4 Interruzione dell'ereditarietà....135
5.4.1 Per disabilitare l'eredità....136
5.5 Utilizzo dei diritti per delegare l'amministrazione....137
5.5.1 Scelta tra le opzioni Modificare i diritti che gli utenti hanno sugli oggetti....139
5.5.2 Diritti del proprietario....140
5.6 Riepilogo delle indicazioni per l'amministrazione dei diritti....140

Capitolo 6 Protezione della piattaforma BI....143

6.1 Panoramica della protezione 143
6.2 Pianificazione del ripristino d'emergenza....143
6.3 Raccomandazioni generali per la protezione della distribuzione....144
6.4 Configurazione della protezione per server di terze parti in bundle....145

6.5 Relazione di trust attiva....145
6.5.1 Token di accesso....145
6.5.2 Meccanismo dei ticket per la distribuzione della protezione....146
6.6 Sessioni e registrazione delle sessioni....147
6.6.1 Registrazione delle sessioni CMS....147
6.7 Protezione dell'ambiente....148
6.7.1 Da browser a server Web....148
6.7.2 Comunicazione tra il server Web e la piattaforma BI....148
6.8 Controllo delle modifiche alla configurazione della protezione....149
6.9 Controllo dell'attività sul Web....149
6.9.1 Protezione contro tentativi di accesso non autorizzati....149
6.9.2 Limitazioni relative alle password....150
6.9.3 Limitazioni relative all'accesso....150
6.9.4 Limitazioni per l'utente....150
6.9.5 Limitazioni all'account Guest....151
6.10 Estensioni di elaborazione....151
6.11 Panoramica della protezione dei dati della piattaforma BI....152
6.11.1 Modalità di protezione dell'elaborazione dei dati....152
6.12 Crittografia nella piattaforma BI....154
6.12.1 Utilizzo delle chiavi cluster....155
6.12.2 Responsabili crittografia....158
6.12.3 Gestione delle chiavi di crittografia in CMC....159
6.13 Configurazione dei server per SSL....164
6.13.1 Creazione di file di chiavi e certificati....164
6.13.2 Configurazione del protocollo SSL....166
6.14 Informazioni sulla comunicazione tra componenti della piattaforma BI....171
6.14.1 Panoramica dei server della piattaforma BI e delle porte di comunicazione....171
6.14.2 Comunicazione tra componenti della piattaforma BI....174
6.15 Configurazione della piattaforma BI per i firewall....181
6.15.1 Per configurare il sistema per i firewall....182
6.15.2 Debug di una distribuzione con firewall....185
6.16 Esempi di scenari di firewall tipici....186
6.16.1 Esempio: livello applicazione distribuito su una rete separata....186
6.16.2 Esempio: livello thick client e database separato dai server della piattaforma BI mediante un firewall....189
6.17 Impostazioni firewall per gli ambienti integrati....191
6.17.1 Linee guida specifiche del firewall per Oracle EBS....192
6.17.2 Configurazione del firewall per l'integrazione con JD Edwards EnterpriseOne....194
6.17.3 Linee guida specifiche del firewall per Oracle EBS....196
6.17.4 Configurazione del firewall per l'integrazione con PeopleSoft Enterprise....197
6.17.5 Configurazione del firewall per l'integrazione con Siebel....199

6.18 Piattaforma BI e server proxy inverso 201
6.18.1 Server reverse proxy supportati 201
6.18.2 Distribuzione delle applicazioni Web 201
6.19 Configurazione di server proxy inverso per applicazioni Web della piattaforma BI....202
6.19.1 Istruzioni dettagliate per la configurazione di server reverse proxy....202
6.19.2 Per configurare il server reverse proxy....203
6.19.3 Configurazione del server proxy inverso Apache 2.2 per la piattaforma BI 203
6.19.4 Configurazione del server proxy inverso WebSEAL 6.0 per la piattaforma BI 203
6.19.5 Configurazione di Microsoft ISA 2006 per la piattaforma BI 204
6.20 Configurazione speciale per la piattaforma BI in distribuzioni di proxy inverso....206
6.20.1 Abilitazione del proxy inverso per Servizi Web....206
6.20.2 Abilitazione del percorso principale per i cookie di sessione per ISA 2006....209
6.20.3 Abilitazione di reverse proxy per SAP BusinessObjects Live Office....211

Capitolo 7 Autenticazione....213

7.1 Opzioni di autenticazione disponibili nella piattaforma BI....213
7.1.1 Autenticazione principale....214
7.1.2 Plug-in di protezione....215
7.1.3 Single Sign On alla piattaforma BI....216
7.2 autenticazione Enterprise....218
7.2.1 Presentazione dell'autenticazione Enterprise....218
7.2.2 Impostazioni di autenticazione Enterprise....218
7.2.3 Modifica delle impostazioni del database....220
7.2.4 Abilitazione dell'Autenticazione affidabile....221
7.2.5 Configurazione dell'Autenticazione affidabile per l'applicazione Web....223
7.3 Autenticazione LDAP....233
7.3.1 Utilizzo dell'autenticazione LDAP....233
7.3.2 Configurazione dell'autenticazione LDAP....235
7.3.3 Mappatura di gruppi LDAP....246
7.4 Autenticazione Windows AD....251
7.4.1 Panoramica....251
7.4.2 Preparazione per l'autenticazione AD (Kerberos)....254
7.4.3 Single Sign-On di autenticazione AD....265
7.4.4 Mappatura di gruppi AD e configurazione dell'autenticazione AD....276
7.4.5 Risoluzione dei problemi relativi all'autenticazione Windows AD....281
7.5 Autenticazione SAP....282
7.5.1 Configurazione dell'autenticazione SAP 283
7.5.2 Creazione di un account utente per la piattaforma BI....283
7.5.3 Connessione ai sistemi di autorizzazione SAP....285
7.5.4 Impostazione delle opzioni di autenticazione SAP....287
7.5.5 Importazione dei ruoli SAP 292

7.5.6 Configurazione di Secure Network Communication (SNC)....296
7.5.7 Impostazione di Single Sign On nel sistema SAP....309
7.5.8 Configurazione di SSO per SAP Crystal Reports e SAP NetWeaver....313
7.6 Autenticazione PeopleSoft....314
7.6.1 Presentazione....314
7.6.2 Abilitazione dell'autenticazione PeopleSoft Enterprise....314
7.6.3 Mappatura di ruoli PeopleSoft alla piattaforma BI....315
7.6.4 Pianificazione degli aggiornamenti utente....319
7.6.5 Utilizzo del Ponte di protezione PeopleSoft....320
7.7 Autenticazione JD Edwards....332
7.7.1 Panoramica....332
7.7.2 Abilitazione dell'autenticazione JD Edwards EnterpriseOne....332
7.7.3 Mappatura dei ruoli JD Edwards EnterpriseOne alla piattaforma BI....333
7.7.4 Pianificazione degli aggiornamenti utente....336
7.8 Autenticazione Siebel....338
7.8.1 Abilitazione dell'autenticazione Siebel....338
7.8.2 Mappatura di ruoli alla piattaforma BI....339
7.8.3 Pianificazione degli aggiornamenti utente....342
7.9 Autenticazione Oracle EBS....344
7.9.1 Abilitazione dell'autenticazione Oracle EBS....344
7.9.2 Mappatura dei ruoli Oracle E-Business Suite alla piattaforma BI....345
7.9.3 Eliminazione mappatura ruoli....349
7.9.4 Personalizzazione dei diritti per gruppi e utenti Oracle EBS mappati....350
7.9.5 Configurazione del Single Sign On (SSO) per SAP Crystal Reports e Oracle EBS....351

Capitolo 8 Amministrazione del server....353

8.1 Amministrazione del server....353
8.1.1 Utilizzo dell'area di gestione Server della console CMC....353
8.1.2 Gestione dei server mediante gli script in Windows....357
8.1.3 Gestione dei server in UNIX....357
8.1.4 Gestione delle chiavi di licenza....357
8.1.5 Misurazione delle licenze....359
8.1.6 Visualizzazione e modifica dello stato del server....360
8.1.7 Aggiunta, duplicazione o eliminazione di server....365
8.1.8 Cluster di Central Management Server....368
8.1.9 Gestione di gruppi di server....373
8.1.10 Valutazione delle prestazioni del sistema....377
8.1.11 Configurazione delle impostazioni server....382
8.1.12 Configurazione delle impostazioni di rete del server....386
8.1.13 Gestione dei nodi....394

8.1.14 Ridenominazione di un computer in una distribuzione della piattaforma SAP BusinessObjects Business Intelligence....416
8.1.15 Utilizzo di librerie di terze parti a 32 e 64 bit con la piattaforma SAP BusinessObjects Business Intelligence....417
8.1.16 Gestione dei segnaposto per server e nodi....418

Capitolo 9 Gestione dei database CMS (Central Management Server)....419

9.1 Gestione delle connessioni di database di sistema CMS....419
9.2 Selezione di un database CMS nuovo o esistente....419
9.2.1 Per selezionare un database CMS nuovo o esistente in Windows....420
9.2.2 Per selezionare un database CMS nuovo o esistente in UNIX....420
9.3 Ricreazione del database di sistema CMS....421
9.3.1 Per creare nuovamente il database di sistema CMS in Windows....421
9.3.2 Per creare nuovamente il database di sistema CMS in UNIX....422
9.4 Copia dei dati da un database di sistema CMS a un altro....423
9.4.1 Preparazione per la copia di un database di sistema CMS....423
9.4.2 Per copiare un database di sistema CMS in Windows....424
9.4.3 Copia di dati da un database di sistema CMS in Unix....424

Capitolo 10 Gestione dei server del contenitore di applicazioni Web (WACS)....427

10.1 WACS....427
10.1.1 Server contenitore applicazioni Web (WACS)....427
10.1.2 Aggiunta o rimozione di WACS aggiuntivi alla distribuzione....430
10.1.3 Aggiunta o rimozione di servizi dal server WACS....434
10.1.4 Configurazione di HTTPS/SSL....435
10.1.5 Metodi di autenticazione supportati....440
10.1.6 Configurazione di AD Kerberos per server WACS....440
10.1.7 Configurazione del Single Sign On AD Kerberos....446
10.1.8 WACS e ambiente IT....448
10.1.9 Configurazione delle proprietà delle applicazioni Web....451
10.1.10 Risoluzione dei problemi....452
10.1.11 Proprietà del server WACS....456

Capitolo 11 Backup e ripristino....457

11.1 Backup e ripristino del sistema....457
11.1.1 Esecuzione di un backup di sistema....458
11.1.2 Backup delle impostazioni server....459
11.1.3 Backup dei contenuti Business Intelligence....461
11.1.4 Ripristino del sistema....462
11.1.5 Ripristino di file perduti o danneggiati della piattaforma SAP BusinessObjects Business Intelligence se è disponibile un backup....467

11.1.6 Ripristino di un sistema della piattaforma SAP BusinessObjects Business Intelligence quando i file sono andati perduti....467
11.1.7 Parametri di BackupCluster e RestoreCluster....467

Capitolo 12 Gestione del ciclo di vita....471

12.1 Console di gestione del ciclo di vita....471
12.2 Impostazioni del sistema di gestione delle versioni per la console di gestione del ciclo di vita.471
12.2.1 Impostazioni del sistema di gestione delle versioni per la console di gestione del ciclo di vita.472
12.3 Strumento della riga di comando motore BIAR....472
12.3.1 Utilizzo di un file delle proprietà....475
12.3.2 Utilizzo dello strumento della riga di comando del motore BIAR....480

Capitolo 13 Gestione delle applicazioni....481

13.1 Gestione delle applicazioni mediante CMC....481
13.1.1 Presentazione....481
13.1.2 Impostazioni comuni per le applicazioni....482
13.1.3 Impostazioni specifiche dell'applicazione....484
13.2 Gestione delle applicazioni mediante le proprietà BOE.war....502
13.2.1 File WAR BOE....502
13.3 Personalizzazione dei punti di ingresso per l'accesso a BI Launch Pad e OpenDocument....511
13.3.1 Percorsi dei file BI Launch Pad e OpenDocument....511
13.3.2 Per definire una pagina di accesso personalizzata....512
13.3.3 Aggiunta di un'autenticazione affidabile all'accesso....513
13.4 Configurazione dell'integrazione Web BEx....514
13.4.1 Avvio di un server per le applicazioni Web BEx....515
13.4.2 Avvio di un server autonomo per le applicazioni Web BEx....516
13.4.3 Configurazione delle impostazioni server....516
13.4.4 Verifica della connessione al sistema BW....517
13.4.5 Configurazione di una connessione tra BEx Web Application Designer e la piattaforma BI....517

Capitolo 14 Gestione di connessioni e universi....521

14.1 Gestione delle connessioni....521
14.1.1 Per eliminare una connessione universo....521
14.2 Gestione degli universi....522
14.2.1 Per eliminare gli universi....522

Capitolo 15 Monitoraggio....525

15.1 Informazioni sul monitoraggio....525
15.2 Termini relativi al monitoraggio....525
15.2.1 Architettura....527

15.3 Supporto cluster per il server di monitoraggio....530
15.4 Metriche....530
15.5 Proprietà di configurazione....538
15.5.1 URL dell'endpoint JMX....541
15.6 Integrazione con altre applicazioni....543
15.6.1 Integrazione dell'applicazione di monitoraggio con IBM Tivoli....543
15.6.2 Integrazione dell'applicazione di monitoraggio con SAP Solution Manager....546
15.7 Creazione dell'universo per il database Derby....546
15.8 Risoluzione dei problemi....547
15.8.1 Cruscotto....547
15.8.2 Avvisi....548
15.8.3 Elenco di controlli....548
15.8.4 Probe....549
15.8.5 Metriche....550
15.8.6 Grafico....550

Capitolo 16 Controllo....551

16.1 Panoramica....551
16.2 Pagina di controllo CMC....557
16.2.1 Stato del controllo....557
16.2.2 Configurazione del controllo eventi....559
16.2.3 Impostazioni di configurazione dell'archivio dati di controllo (ADS)....561
16.3 Eventi di controllo....562
16.3.1 Eventi di controllo e dettagli....570

Capitolo 17 Ricerca piattaforma....587

17.1 Presentazione....587
17.2 Architettura....587
17.3 Supporto cluster per Ricerca piattaforma....589
17.4 SDK e Open Search....590
17.4.1 SDK applicazione di ricerca piattaforma....590
17.4.2 Open Search....590
17.5 Configurazione delle proprietà dell'applicazione....592
17.6 Tipi di contenuto in cui è possibile eseguire ricerche....599
17.7 Query suggerite....600
17.8 Facet....601
17.9 Supporto multilingue....602
17.10 Suggerimenti....602
17.11 Raggruppamento dei risultati della ricerca di SAP BusinessObjects Explorer....603
17.12 Integrazione in fase di ricerca con la funzionalità di ricerca di SAP NetWeaver Enterprise....603

17.12.1 Creazione di un connettore nella funzionalità di ricerca di SAP NetWeaver Enterprise 604
17.12.2 Importazione di un ruolo utente nella sezione di autenticazione di SAP BusinessObjects Enterprise.....605
17.12.3 Ricerca dalla funzionalità di ricerca di NetWeaver Enterprise.....605
17.13 Controllo.....606
17.14 Elenco errori di indicizzazione 607
17.15 Risoluzione dei problemi.....607

Capitolo 18 Federazione.....611

18.1 Federation.....611
18.2 Termini correlati a Federation.....612
18.2.1 Applicazione BI 613
18.2.2 Sito di destinazione 613
18.2.3 Local.....613
18.2.4 Istanze completate eseguite localmente 613
18.2.5 Siti di origine multipli 613
18.2.6 Replica unilaterale 614
18.2.7 Sito di origine 614
18.2.8 &Riprova.....614
18.2.9 Connessione remota.....614
18.2.10 Pianificazione remota.....614
18.2.11 Replica.....615
18.2.12 Processo di replica.....615
18.2.13 Elenco di replica.....615
18.2.14 Oggetto di replica.....615
18.2.15 Pacchetto di replica.....615
18.2.16 Aggiornamento della replica.....616
18.2.17 Replica bilaterale.....616
18.3 Gestione dei diritti di protezione.....616
18.3.1 Diritti richiesti sul sito di origine.....616
18.3.2 Diritti richiesti nel sito di destinazione.....617
18.3.3 Diritti specifici di Federation.....618
18.3.4 Replica della protezione per un oggetto.....620
18.3.5 Replica della protezione mediante i livelli di accesso.....621
18.4 Opzioni di tipi e modalità di replica.....621
18.4.1 Replica unilaterale 622
18.4.2 Replica bilaterale 622
18.4.3 Aggiornamento da origine o da destinazione.....623
18.5 Replica di utenti e gruppi di terze parti.....624
18.6 Replica di universi e connessioni agli universi.....625
18.7 Gestione degli elenchi di replica.....626

18.7.1 Creazione di elenchi di replica....627
18.7.2 Modifica degli elenchi di replica....629
18.8 Gestione delle connessioni remote....630
18.8.1 Creazione di connessioni remote....631
18.8.2 Modifica delle connessioni remote....633
18.9 Gestione dei processi di replica....633
18.9.1 Creazione di processi di replica....634
18.9.2 Pianificazione dei processi di replica....636
18.9.3 Modifica dei processi di replica....637
18.9.4 Visualizzazione di un registro dopo un processo di replica....637
18.10 Gestione dell'eliminazione di oggetti....638
18.10.1 Modalità di utilizzo dell'eliminazione di oggetti....638
18.10.2 Limiti dell'eliminazione di oggetti....639
18.10.3 Frequenza di eliminazione degli oggetti....640
18.11 Gestione del rilevamento e della risoluzione dei conflitti....641
18.11.1 Risoluzione di conflitti di replica unilaterale....641
18.11.2 Risoluzione conflitti di replica bilaterale....643
18.12 Utilizzo dei Servizi Web in Federation....646
18.12.1 Variabili di sessione....646
18.12.2 Memorizzazione di file nella cache....646
18.12.3 Distribuzione personalizzata....647
18.13 Pianificazione remota e istanze eseguite localmente....648
18.13.1 Pianificazione remota....648
18.13.2 Istanze eseguite localmente....649
18.13.3 Condivisione di istanze....650
18.14 Importazione e promozione di contenuto replicato....651
18.14.1 Importazione di contenuto replicato....651
18.14.2 Importazione del contenuto replicato e continuazione della replica....652
18.14.3 Promozione del contenuto da un ambiente di test....652
18.14.4 Puntamento a un sito di destinazione....653
18.15 Procedure consigliate....653
18.15.1 Limitazioni della release corrente....656
18.15.2 Risoluzione dei messaggi di errore....657

Capitolo 19 Configurazioni supplementari per gli ambienti ERP....661

19.1 Configurazioni per l'integrazione di SAP NetWeaver....661
19.1.1 Integrazione con SAP Netweaver Business Warehouse (BW)....661
19.2 Configurazione per l'integrazione JD Edwards....712
19.2.1 Configurazione del Single Sign On (SSO) per SAP Crystal Reports....712
19.2.2 Configurazione delle integrazioni di Secure Socket Layer per JD Edwards....713
19.3 Configurazione per l'integrazione PeopleSoft Enterprise....714

19.3.1 Configurazione di Single Sign-On (SSO) per SAP Crystal Reports e PeopleSoft Enterprise..714
19.3.2 Configurazione per le comunicazioni Secure Socket Layer....715
19.3.3 Regolazione delle prestazioni per i sistemi PeopleSoft....717
19.4 Configurazione per l'integrazione Siebel....718
19.4.1 Configurazione di Siebel per l'integrazione con la piattaforma SAP BusinessObjects Business Intelligence....719
19.4.2 Creazione della voce di menu Crystal Reports....719
19.4.3 Contextual Awareness....721
19.4.4 Configurazione di Single Sign-On (SSO) per SAP Crystal Reports e Siebel....723
19.4.5 Configurazione per le comunicazioni Secure Sockets Layer....724

Capitolo 20 Gestione e configurazione dei registri....727

20.1 Registrazione di analisi dai componenti....727
20.2 Livelli del registro di analisi....727
20.3 Configurazione dell'analisi per i server....728
20.3.1 Impostazione del livello del registro di analisi del server nella console CMC....729
20.3.2 Impostazione del livello del registro di analisi per più server gestiti nella console CMC....730
20.3.3 Per configurare l'analisi del server tramite il file BO_trace.ini....730
20.4 Configurazione dell'analisi per le applicazioni Web....733
20.4.1 Impostazione del livello del registro di analisi delle applicazioni Web nella CMC....734
20.4.2 Modifica manuale delle impostazioni di analisi mediante il file BO_trace....734
20.5 Configurazione dell'analisi per Upgrade Management Tool....740
20.5.1 Configurazione dell'analisi per Upgrade Management Tool....740

Capitolo 21 Integrazione con SAP Solution Manager....743

21.1 Panoramica sull'integrazione....743
21.2 Elenco di controllo dell'integrazione di SAP Solution Manager....743
21.3 Gestione della registrazione di System Landscape Directory....745
21.3.1 Registrazione della piattaforma BI in System Landscape....745
21.3.2 Quando viene attivata la registrazione SLD?....746
21.3.3 Registrazione della connettività SLD....747
21.4 Gestione degli agenti di Solution Manager Diagnostics....747
21.4.1 Panoramica di Solution Manager Diagnostics (SMD)....747
21.4.2 Utilizzo degli agenti SMD....748
21.4.3 Account utente SMAdmin....748
21.5 Gestione della strumentazione delle prestazioni....749
21.5.1 Strumentazione delle prestazioni per la piattaforma BI....749
21.5.2 Impostazione della strumentazione delle prestazioni per la piattaforma BI....749
21.5.3 Strumentazione delle prestazioni per il livello Web....751
21.5.4 File di registro di strumentazione....751

21.6 Analisi con SAP Passport....752

Capitolo 22 Amministrazione della riga di comando....753

22.1 Script UNIX....753
22.1.1 Utilità per gli script....753
22.1.2 Modelli di script....759
22.1.3 Script utilizzati dalla piattaforma SAP BusinessObjects Business Intelligence....760
22.2 Script Windows....761
22.2.1 ccm.exe....762
22.3 Righe di comando server....765
22.3.1 Panoramica sulle righe di comando....765
22.3.2 Opzioni standard per tutti i server....766
22.3.3 Central Management Server....767
22.3.4 Server di elaborazione Crystal Reports e Crystal Reports Cache Server....770
22.3.5 Server di elaborazione di Dashboard Design e Cache Server di Dashboard Design....771
22.3.6 Job Server....772
22.3.7 Adaptive Processing Server....773
22.3.8 Report Application Server....773
22.3.9 Web Intelligence Processing Server....776
22.3.10 Input e Output File Repository Server....777
22.3.11 Event Server....779
22.3.12 Dashboard Server e Dashboard Analytics Server....780

Capitolo 23 Appendice sui diritti....781

23.1 Appendice sui diritti....781
23.2 Diritti generali....781
23.3 Diritti per tipi di oggetti specifici....784
23.3.1 Diritti sulla cartella....784
23.3.2 Categorie....784
23.3.3 Note....785
23.3.4 Report Crystal....786
23.3.5 Documenti Web Intelligence....786
23.3.6 Utenti e gruppi....787
23.3.7 Livelli di accesso....789
23.3.8 Spazi di lavoro BI....790
23.3.9 Diritti sugli universi (.unv)....791
23.3.10 Diritti sugli universi (.unx)....792
23.3.11 Livelli di accesso agli oggetti universo....794
23.3.12 Diritti di connessione....795
23.3.13 Applicazioni....796

Capitolo 24 **Appendice sulle proprietà dei server....811**

24.1 Informazioni sull'appendice sulle proprietà dei server....811
24.1.1 Proprietà comuni dei server....811
24.1.2 Proprietà dei servizi principali....814
24.1.3 Proprietà dei servizi di connettività....825
24.1.4 Proprietà dei servizi Crystal Reports....829
24.1.5 Proprietà dei servizi Analysis....838
24.1.6 Proprietà dei servizi Data Federation....840
24.1.7 Proprietà servizi Web Intelligence....840
24.1.8 Proprietà dei servizi di Dashboard Design....850

Capitolo 25 **Appendice sulle metriche server....855**

25.1 Informazioni sull'appendice sulle metriche server....855
25.1.1 Metriche server comuni....855
25.1.2 Metriche del Central Management Server....858
25.1.3 Metriche di Connection Server....863
25.1.4 Metriche di Event Server....863
25.1.5 Metriche del File Repository Server....864
25.1.6 Metriche di Adaptive Processing Server....865
25.1.7 Metriche del server del contenitore di applicazioni Web....870
25.1.8 Metriche di Adaptive Job Server....871
25.1.9 Metriche di Crystal Reports Server....873
25.1.10 Metriche del server Web Intelligence....876
25.1.11 Metriche del server di Dashboard Design....878

Capitolo 26 **Appendice: segnaposto per server e nodi....881**

26.1 Segnaposto server e nodo....881

Capitolo 27 **Appendice: schema archivio dati di controllo....891**

27.1 Presentazione....891
27.2 Diagramma schema....891
27.3 Tabelle dell'archivio dati di controllo....892

Appendice A **Ulteriori informazioni....903**

Indice **905**

Introduzione

1.1 Informazioni sulla guida

Questa guida fornisce informazioni e procedure per la distribuzione e la configurazione della 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*.

1.1.1 Destinatari del Manuale

Questa guida illustra i task di distribuzione e configurazione. Si consiglia di consultare questo manuale se si desidera:

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

Gli argomenti di questa Guida sono destinati agli amministratori di sistema responsabili della configurazione, gestione e 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, al fine di assistere tutti i livelli di esperienza amministrativa, questa guida mira a offrire informazioni concettuali e di base sufficienti a chiarire tutte le funzioni e le attività amministrative.

1.1.2 Informazioni sulla piattaforma SAP BusinessObjects Business Intelligence

La piattaforma BI è una soluzione flessibile, scalabile e affidabile per la generazione di report interattivi e potenti tramite qualsiasi applicazione Web, Intranet, Extranet, Internet o portale aziendale. Utilizzata

per la distribuzione di report settimanali sulle vendite, per la fornitura ai clienti di offerte di servizi personalizzati o l'integrazione di informazioni cruciali nei portali aziendali, la piattaforma BI garantisce sempre vantaggi tangibili che si diffondono a tutta l'azienda e oltre. La piattaforma 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.

1.1.3 Variabili

In questo manuale vengono utilizzate le seguenti variabili.

Variabile	Descrizione
<DIRINSTALLAZ>	La directory in cui viene installata la piattaforma BI. Su un computer Windows, la directory predefinita è `C:\Programmi (x86)\SAP BusinessObjects\`.
<PLATFORM64DIR>	Il nome del sistema operativo UNIX. I valori accettabili sono: • aix_rs6000_64 • linux_x64 • solaris_sparcv9 • hpux_ia64
<DIRSCRIPT>	La directory in cui si trovano gli script di amministrazione della piattaforma BI. Su un computer Windows, la directory è *<INSTALLDIR>*`\win64_x64\scripts`. Sui computer Unix, la directory è *<INSTALLDIR>*/*<PLATFORM64DIR>*`/scripts`.

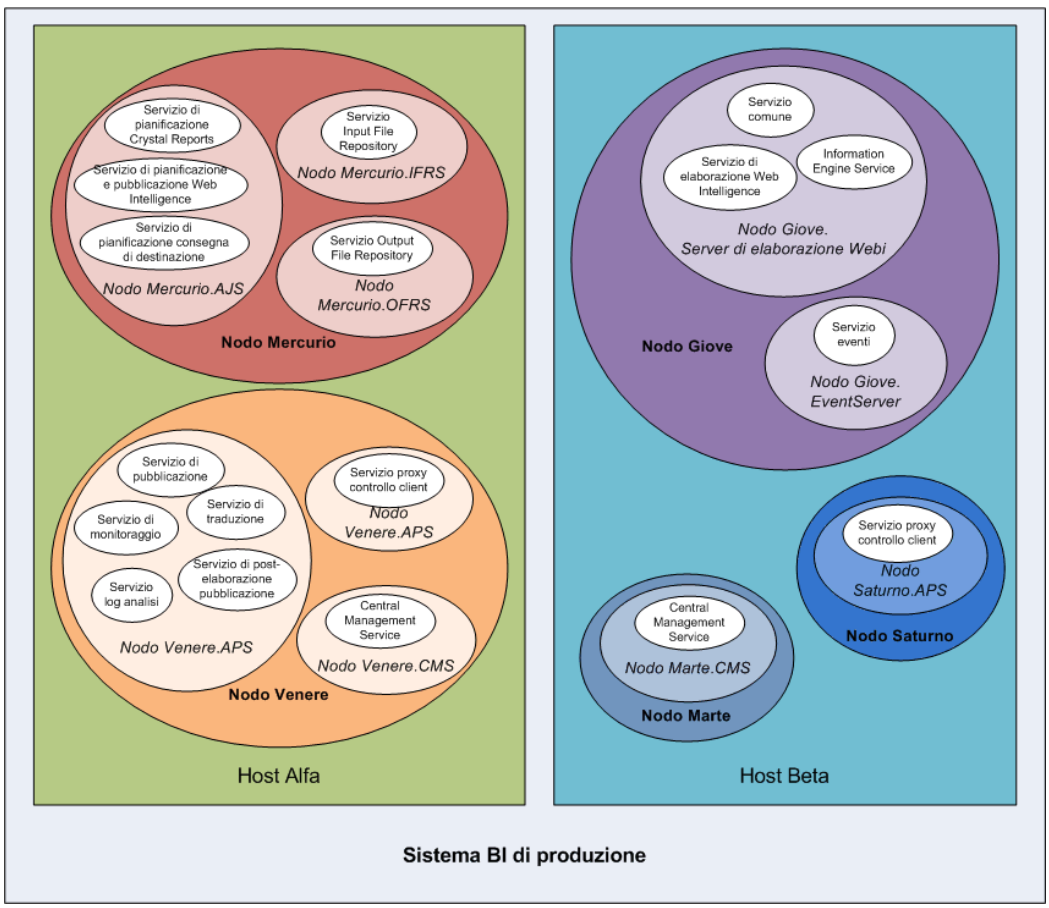
1.2 Prima di iniziare

1.2.1 Concetti fondamentali

1.2.1.1 Servizi e server

Il diagramma che segue mostra un'installazione ipotetica della piattaforma BI.

Nota:
i nodi, i server e i servizi vengono mostrati solo a scopo illustrativo. 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*, con due host:

- Sull'host denominato *HostAlpha* è installata la piattaforma BI. L'host è configurato per contenere due nodi:
  - *NodeMercuy*: contiene 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*: contiene un Adaptive Processing Server (*NodeVenus.APS*) con servizi che forniscono funzionalità per la pubblicazione, il monitoraggio e la traduzione, un Adaptive Processing Server (*NodeVenus.APS*) dotato di un servizio per fornire il controllo dei client e un Central Management Server (*NodeVenus.CMS*) con un servizio che fornisce i servizi CMS.

- Sull'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.
    - *NodeJupiter*: contiene un server di elaborazione 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 la pianificazione dei report.
    - *NodeSaturn*: contiene un Adaptive Processing Server (*NodeSaturn.APS*) dotato di un servizio che fornisce il controllo dei client.

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

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). Il servizio di pubblicazione e pianificazione di SAP BusinessObjects Web Intelligence è ad esempio un sottosistema eseguito in Adaptive Job Server.

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 PID.

Un *nodo* è un insieme di server della piattaforma BI eseguiti nello stesso host. Uno o più nodi possono trovarsi in un solo host.

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.

1.2.1.2 Server Intelligence

Server Intelligence è un componente della CMC (Central Management Console) per la gestione dei processi di una raccolta o un server, il cui insieme viene definito nodo. Le modifiche ai processi dei server applicate nella CMC vengono propagate ai server interessati da Server Intelligence Agent (SIA). SIA consente inoltre di riavviare o chiudere automaticamente un server se si verifica una condizione imprevista e viene utilizzato dal Central Management Server (CMS) per gestire i nodi.

Il server SIA archivia le informazioni dei server nel database del sistema CMS e consente quindi di ripristinare facilmente le impostazioni predefinite dei server o di creare istanze ridondanti dei processi dei server con le stesse impostazioni.

1.2.2 Strumenti di amministrazione principali

1.2.2.1 Central Management Console (CMC)

La Central Management Console (CMC) è uno strumento Web che consente di eseguire attività amministrative quotidiane, tra cui la gestione degli utenti, del contenuto e dei server. Consente inoltre di pubblicare, organizzare e 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.

Tutti gli utenti possono accedere alla console CMC per modificare le impostazioni delle preferenze utente. Solo i membri del gruppo *Amministratori* possono modificare le impostazioni di gestione, a meno che tale diritto non venga esplicitamente concesso ad altri utenti. È inoltre possibile assegnare ruoli alla CMC per concedere alcuni privilegi utente per l'esecuzione di attività amministrative minori

1.2.2.2 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 un ambiente UNIX, lo script della shell di CCM `ccm.sh` consente di gestire i server dalla riga di comando.

CCM consente di creare e configurare nodi Server Intelligence Agent (SIA) e avviare o arrestare il server di applicazioni Web. In Windows è anche possibile configurare parametri di rete, ad esempio la crittografia SSL (Secure Socket 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.

1.2.2.3 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). 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.

1.2.2.4 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 oggetti, 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 di SAP BusinessObjects Business Intelligence*.

1.2.3 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)

1.2.3.1 Pianificazione o esecuzione della prima distribuzione

Se si desidera pianificare o eseguire la prima distribuzione della piattaforma BI, si consiglia di eseguire i seguenti task e di consultare le sezioni corrispondenti:

- Per acquisire familiarità con i componenti della piattaforma BI, leggere la sezione “Panoramica dell'architettura”.

- Per valutare le esigenze e progettare un'architettura di distribuzione che funzioni in modo ottimale, consultare il *Manuale della pianificazione della distribuzione della piattaforma SAP BusinessObjects Business Intelligence*.
- “Informazioni sulla comunicazione tra componenti della piattaforma BI ”.
- “Panoramica della protezione”.
- Se si prevede di utilizzare l'autenticazione di terze parti, consultare la sezione “Autenticazione”.
- Per ulteriori informazioni sull'installazione della piattaforma BI, consultare il *Manuale di installazione della piattaforma SAP BusinessObjects Business Intelligence*.
- Dopo l'installazione, leggere la sezione “Panoramica della gestione dei server”.

Argomenti correlati

- Presentazione dell'architettura
- Informazioni sulla comunicazione tra componenti della piattaforma BI
- Panoramica della protezione
- Opzioni di autenticazione disponibili nella piattaforma BI
- Amministrazione del server

1.2.3.2 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

- Amministrazione del server
- Comunicazione tra componenti della piattaforma BI
- Panoramica della protezione
- Informazioni sul monitoraggio

1.2.3.3 Miglioramento delle prestazioni del sistema

Se si desidera valutare l'efficacia della distribuzione e ottimizzarla in modo da sfruttare al massimo le risorse, si consiglia di consultare le seguenti sezioni:

- Se si desidera monitorare il sistema esistente, consultare la sezione relativa al “monitoraggio”.

- Per le attività di manutenzione quotidiana e le procedure di utilizzo dei server nella console CMC, vedere “Manutenzione del server”.

Argomenti correlati

- Informazioni sul monitoraggio
- Amministrazione del server

1.2.3.4 Utilizzo di oggetti in CMC

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

2.1 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.

La piattaforma SAP BusinessObjects Business Intelligence 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 BI della piattaforma SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence:
  - Web Intelligence
  - Business View Manager
  - Strumento di conversione dei report
  - Universe Design Tool
  - Strumento Query del servizio Web (in precedenza Query come servizio Web)
  - Information Design Tool (in precedenza Information Designer)
  - Translation Management Tool (in precedenza Translation Manager)
  - Widget per la piattaforma SAP BusinessObjects Business Intelligence (in precedenza BI Widgets)
- Client disponibili separatamente:
  - SAP Crystal Reports
  - SAP BusinessObjects Dashboard Design (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 SAP BusinessObjects Business Intelligence su uno o più computer. È anche possibile installare contemporaneamente due versioni diverse della piattaforma SAP BusinessObjects Business Intelligence sullo stesso computer, benché questa configurazione sia consigliata solo come parte del processo di aggiornamento o di test.

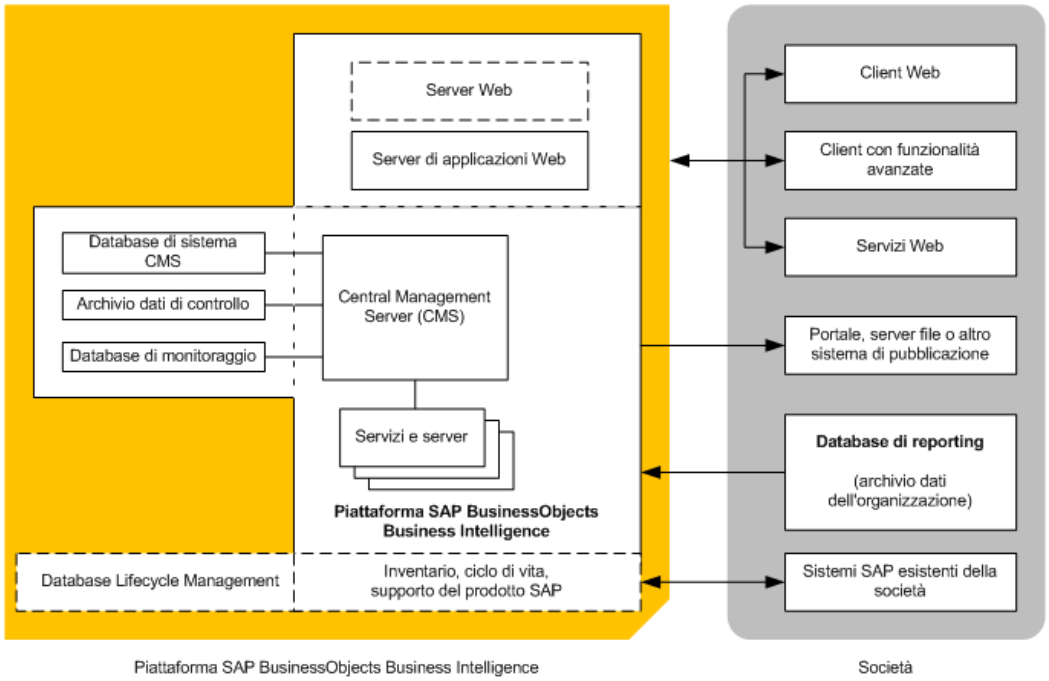
I processi server possono essere “scalati in verticale” (un computer esegue più processi server, o tutti) per ridurre i costi oppure “scalati in orizzontale” (i processi server sono distribuiti tra due o più computer connessi in rete) per migliorare le prestazioni. Inoltre, è possibile eseguire più versioni 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).

2.1.1 Panoramica del sistema

La piattaforma SAP BusinessObjects Business Intelligence fornisce strumenti di analisi e reporting aziendali. 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.

Lo schema che segue mostra in che modo la piattaforma SAP BusinessObjects Business Intelligence viene integrata nell'infrastruttura di un'organizzazione.



La piattaforma SAP BusinessObjects Business Intelligence crea report da una connessione di sola lettura ai database dell'organizzazione e utilizza i propri database per memorizzare le informazioni relative a configurazione, controllo e 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 SAP BusinessObjects Business Intelligence 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).

2.1.2 Database

La piattaforma SAP BusinessObjects Business Intelligence utilizza diversi database.

- Database di reporting

  Questo termine fa riferimento alle informazioni sull'organizzazione. Sono le informazioni di origine analizzate e restituite solo dalla piattaforma SAP BusinessObjects Business Intelligence. 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 SAP BusinessObjects Business Intelligence, 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 SAP BusinessObjects Business Intelligence. 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 SAP BusinessObjects Business Intelligence, 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 SAP BusinessObjects Business Intelligence può installarlo e configurarlo automaticamente. Per stabilire quale server di database supportato risulta più adatto ai requisiti di un'organizzazione, è consigliabile valutare i requisiti rispetto alle indicazioni del fornitore di server di database.

2.1.3 Server

La piattaforma SAP BusinessObjects Business Intelligence è costituita da gruppi di server eseguiti in uno o più host. Per le piccole installazioni, ad esempio sistemi di test o sviluppo, è possibile utilizzare un solo host per un server di applicazioni Web, un server di database e tutti i server della piattaforma SAP BusinessObjects Business Intelligence.

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 SAP BusinessObjects Business Intelligence. In questo modo vengono liberate risorse sull'host server della piattaforma SAP BusinessObjects Business Intelligence per consentire l'elaborazione di un numero maggiore di informazioni rispetto al caso in cui venga ospitato anche un server di applicazioni Web.

Per le installazioni di grandi dimensioni è possibile utilizzare diversi host server della piattaforma SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence per garantire la disponibilità di una notevole quantità di risorse per elaborare le richieste dei clienti.

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

- Miglioramento delle prestazioni

Più host server della piattaforma SAP BusinessObjects Business Intelligence sono in grado di elaborare una coda di informazioni sulla creazione dei report più veloce di un singolo host server di SAP BusinessObjects Enterprise.

- 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.

2.1.4 Server di applicazioni Web

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

I seguenti server di applicazioni Web sono pienamente supportati:

- JBoss
- Oracle Application Server
- Sun Java System Application Server (solo Unix)
- SAP NetWeaver AS Java
- Tomcat
- WebLogic
- WebSphere

Per un elenco dettagliato dei server di applicazioni Web supportati, consultare la *documentazione relativa alle piattaforme supportate* disponibile all'indirizzo http://service.sap.com/bosap-support.

Se non è disponibile un server di applicazioni Web esistente da utilizzare con la piattaforma SAP BusinessObjects Business Intelligence, il programma di installazione installa e configura automaticamente un server di applicazioni Web Tomcat 6. 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 SAP BusinessObjects Business Intelligence e di un server di applicazioni Web nello stesso host in un ambiente di produzione può determinare una riduzione delle prestazioni.

2.1.4.1 Servizio contenitore applicazioni Web (WACS)

Per l'hosting di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence è necessario un server di applicazioni Web.

Se si ricopre il ruolo di amministratore di server di applicazioni Web Java avanzate con esigenze amministrative avanzate, è necessario utilizzare un server di applicazioni Web Java supportate per l'hosting delle applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence. Se si intende utilizzare un sistema operativo Windows supportato per l'hosting della piattaforma SAP BusinessObjects Business Intelligence, 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 Servizio contenitore applicazioni Web (WACS) durante l'installazione della piattaforma SAP BusinessObjects Business Intelligence.

Il WACS è un server della piattaforma SAP BusinessObjects Business Intelligence che consente l'esecuzione di applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence, come la CMC (Central Management Console), BI Launch Pad e Servizi Web, senza che sia necessario installare in precedenza 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 SAP BusinessObjects Business Intelligence 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 a quella degli altri server della piattaforma SAP BusinessObjects Business Intelligence.
- Analogamente ad altri server della piattaforma SAP BusinessObjects Business Intelligence, 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 SAP BusinessObjects Business Intelligence.
- 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 SAP BusinessObjects Business Intelligence sono ospitate dal WACS.

2.1.5 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 SAP BusinessObjects Business Intelligence dispone di SDK per lo sviluppo di software sulle piattaforme Java e .NET.

Nota:
I kit .NET SDK per la piattaforma SAP BusinessObjects Business Intelligence non sono installati per impostazione predefinita e devono essere scaricati dal sito SAP Service Marketplace.

I seguenti SDK sono supportati per la piattaforma SAP BusinessObjects Business Intelligence:

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

  Gli SDK della Java SDK and .NET SDK consentono all'applicazione di eseguire attività quali autenticazione, gestione della sessione, utilizzo degli oggetti repository, pianificazione e pubblicazione di report e gestione dei server.

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

- 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.

- 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 SAP BusinessObjects 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.

- Crystal Reports Viewer Java SDK e .NET SDK

Gli SDK dei 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.
- Libreria tag di Viewer: consente di personalizzare il comportamento del visualizzatore nelle pagine JSP.

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

  Implementazione di Servizi Web che consente di impostare le opzioni di autenticazione e protezione utente, accesso a documenti e report, pianificazione, pubblicazione e gestione del server.

Nota:
I componenti JavaServer Faces della piattaforma SAP BusinessObjects Business Intelligencesono stati dichiarati obsoleti.

Gli SDK possono essere utilizzati in combinazione per fornire un'ampia gamma di funzionalità BI alle applicazioni in uso. Ad esempio, l'applicazione Web BI Launch Pad inclusa nella piattaforma SAP BusinessObjects Business Intelligence è stata creata utilizzando questi SDK.

Per ulteriori informazioni sugli SDK della piattaforma SAP BusinessObjects Business Intelligence, consultare il *Manuale per gli sviluppatori dell'SDK della piattaforma SAP BusinessObjects Business Intelligence*, il *Manuale per gli sviluppatori di Report Application Server Java SDK*, il manuale *Report Application Server .NET SDK Developer Guide* e il *Manuale per gli sviluppatori dell'SDK Java dei visualizzatori* disponibili all'indirizzo: http://service.sap.com/bosap-support.

2.1.5.1 SDK Servizi Web Java e .NET Consumer

Gli SDK Servizi Web Java e .NET Consumer di SAP BusinessObjects Enterprise consentono di creare applicazioni di servizi Web che sfruttano le funzionalità della piattaforma SAP BusinessObjects Business Intelligence.

I servizi Web sono costituiti da componenti software che è possibile chiamare in remoto utilizzando il protocollo SOAP (Simple Object Access Protocol). SOAP è un protocollo per lo scambio delle informazioni che non dipende da una piattaforma, da un modello a oggetti o da un linguaggio di programmazione specifico.

I servizi Web della piattaforma SAP BusinessObjects Business Intelligence includono funzionalità nelle seguenti aree:

- Sessione

  Gestione utenti e autenticazione.

- Piattaforma BI

  Espone funzionalità avanzate della piattaforma quali i servizi di pianificazione, pubblicazione, ricerca, amministrazione di utenti e gruppi, amministrazione server.

- Modulo di report

  Visualizza SAP BusinessObjects Business Intelligence Solution e Crystal Reports in formato HTML, PDF, Excel e XML.

- Query

  Crea query ad-hoc basate sul livello semantico degli universi.

Nei servizi Web della piattaforma SAP BusinessObjects Business Intelligence vengono utilizzati 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.

   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.

2.1.5.2 Web Services Query Tool

Web Service Query 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 Web Service Query non è così, in quanto il contenuto BI può essere consegnato a qualsiasi interfaccia utente in grado di elaborare i servizi Web.

L'applicazione Web Service Query 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, WSDL e XML. È composto da due componenti principali:

- Componente server

  Il componente server (incluso nella piattaforma SAP BusinessObjects Business Intelligence) memorizza il catalogo di Web Service Query 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 di Web Service Query memorizzato nel server. Lo strumento client comunica con i componenti server tramite servizi Web.

Web Service Query 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

2.1.6 Origini dati

2.1.6.1 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 SAP BusinessObjects Business Intelligence. 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 SAP BusinessObjects Business Intelligence. 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 SAP BusinessObjects Web Intelligence di recapitare i documenti, utilizzando più provider di dati sincronizzati, inclusi le origini dati OLAP (Online Analytical Processing) e CWM (Common Warehousing Metamodel).

2.1.6.2 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. Sono completamente supportate nella piattaforma SAP BusinessObjects Business Intelligence.

La piattaforma SAP BusinessObjects 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.

2.1.7 Supporto delle lingue

I prodotti della piattaforma SAP BusinessObjects Business Intelligence sono tradotti in numerose lingue e supportano la gestione dei dati in una gamma ancora più ampia di lingue.

Le interfacce dei prodotti sono disponibili nelle seguenti lingue:

- Ceco
- Cinese semplificato
- Cinese tradizionale
- Danese
- Olandese
- Inglese
- Finlandese
- Francese
- Tedesco
- Italiano
- Giapponese
- Coreano
- Norvegese Bokmal
- Polacco
- Portoghese
- Russo
- Spagnolo
- Svedese

- Tailandese

Oltre a supportare i dati in una delle lingue disponibili nell'interfaccia, sono supportati anche i seguenti set di caratteri:

- Greco
- Malese
- Ebraico
- Arabo
- Rumeno
- Vietnamese
- Ungherese
- Turco
- Hindi

2.1.8 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 ne autorizzano l'accesso per la piattaforma SAP BusinessObjects Business Intelligence, 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 di Autenticazione affidabile per l'autenticazione di terze parti.
- 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

2.1.8.1 Plug-in di protezione

I plug-in di protezione consentono di automatizzare la creazione e la gestione di account consentendo la mappatura di account utente e gruppi da sistemi di terze parti nella piattaforma SAP BusinessObjects

Business Intelligence. È possibile mappare account utente o gruppi di terze parti ad account utente o gruppi Enterprise 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. Pertanto, dopo aver mappato un gruppo LDAP (Lightweight Directory Access Protocol) o Windows Active Directory (AD) nella piattaforma SAP BusinessObjects Business Intelligence, tutti gli utenti che appartengono a quel gruppo possono accedere alla piattaforma SAP BusinessObjects Business Intelligence. Le modifiche successive alle appartenenze a gruppi di terzi vengono propagate automaticamente.

La piattaforma SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence oppure se non è stata ancora impostata una gerarchia di utenti e gruppi in un server di elenchi in linea LDAP o in un server 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 SAP BusinessObjects Business Intelligence 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 l'autenticazione affidabile.

2.1.8.2 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 SAP BusinessObjects Business Intelligence supporta il Single Sign On e la creazione di report dai sistemi ERP seguenti:

- SAP ERP e Business Warehouse (BW)

Nota:
per poter utilizzare connessioni ODA (OLAP Data Access), SAP BusinessObjects Analysis (in precedenza Voyager) o BW, è necessario che sia installata la GUI SAP.

- 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 SAP BusinessObjects Business Intelligence, consultare il *documento relativo alle piattaforme supportate*, disponibile all'indirizzo service.sap.com/bosap-support.

Per configurare l'integrazione ERP, consultare il *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

2.1.9 Integrazione SAP

La piattaforma SAP BusinessObjects Business Intelligence è integrata nell'infrastruttura SAP esistente con i seguenti strumenti SAP:

- 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 SAP BusinessObjects Business Intelligence registra il fornitore, il nome e la versione dei prodotti con SLD, nonché i nomi di componenti, le versioni e il percorso di server e front-end.

- 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 SAP BusinessObjects Business Intelligence in System Landscape” nel *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

- 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.

2.1.10 Lifecycle Management (LCM)

Lifecycle Management (LCM) è un insieme di processi che riguardano la gestione delle informazioni sul prodotto di un'installazione. Stabilisce delle procedure per l'organizzazione dell'installazione della piattaforma SAP BusinessObjects Business Intelligence negli ambienti di sviluppo, test, produzione o manutenzione.

LifeCycle Manager, nella piattaforma SAP BusinessObjects Business Intelligence, è uno strumento basato sul Web che consente di spostare oggetti BI da un sistema a un altro, senza influire sulle dipendenze di tali oggetti. Consente inoltre di gestire versioni diverse e dipendenze, nonché eseguire il rollback di un oggetto promosso per ripristinarne lo stato precedente.

Lo strumento LCM è un plug-in per la piattaforma SAP BusinessObjects Business Intelligence. È possibile promuovere un oggetto BI da un sistema a un altro solo se la stessa versione dell'applicazione è installata sia nel sistema di origine che nel sistema di destinazione.

Per ulteriori informazioni, consultare il *Manuale dell'utente di Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0*.

2.1.11 Controllo integrato delle versioni

I file che costituiscono la piattaforma SAP BusinessObjects Business Intelligence 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.

2.1.12 Dati permanenti

Il termine "dati permanenti" si riferisce a qualsiasi informazione considerata abbastanza importante per essere migrata durante l'aggiornamento di un sistema. Ad esempio, il server CMS memorizza le informazioni di configurazione nel database CMS anziché nel registro di sistema di Windows o in un file di configurazione.

Tutti i prodotti della piattaforma SAP BusinessObjects Business Intelligence memorizzano i dati permanenti nel database di sistema CMS. Ciò consente di eseguire facilmente la migrazione dei dati e delle informazioni sulla configurazione a una nuova versione durante l'aggiornamento.

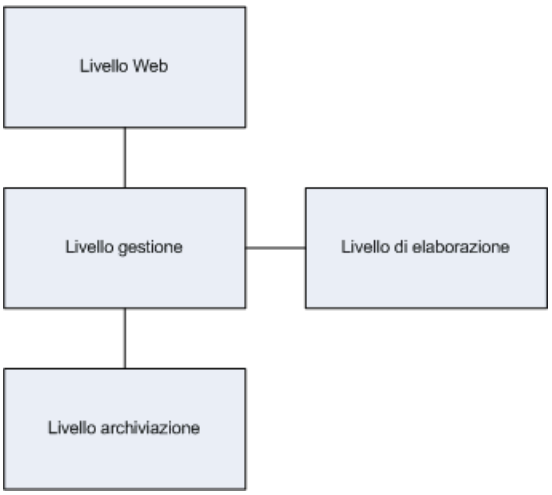
2.1.13 Percorso di aggiornamento

Per eseguire l'aggiornamento da una versione precedente della piattaforma SAP BusinessObjects Business Intelligence, è necessario innanzitutto installare la piattaforma SAP BusinessObjects Business Intelligence 4.0, quindi effettuare la migrazione dal sistema esistente utilizzando Upgrade Management Tool.

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

2.2 Livelli concettuali

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



- Livello Web

  Il livello Web contiene le applicazioni Web distribuite a un server di applicazioni Web Java. Le applicazioni Web forniscono tramite un browser le funzionalità della piattaforma SAP BusinessObjects Business Intelligence 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 che forniscono tramite il server di applicazioni Web agli strumenti software funzionalità della piattaforma SAP BusinessObjects Business Intelligence, 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. Live Office è ad esempio un prodotto che utilizza i Servizi Web per integrare la creazione di report della piattaforma SAP BusinessObjects Business Intelligence con i prodotti Microsoft Office.

- Livello gestione

  Il livello di gestione coordina e controlla tutti i componenti della piattaforma SAP BusinessObjects Business Intelligence. Comprende CMS (Central Management Server) ed Event Server. Il server CMS fornisce e 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 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.

- Livello archiviazione

Il livello di archiviazione è responsabile della gestione di file, come 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`.

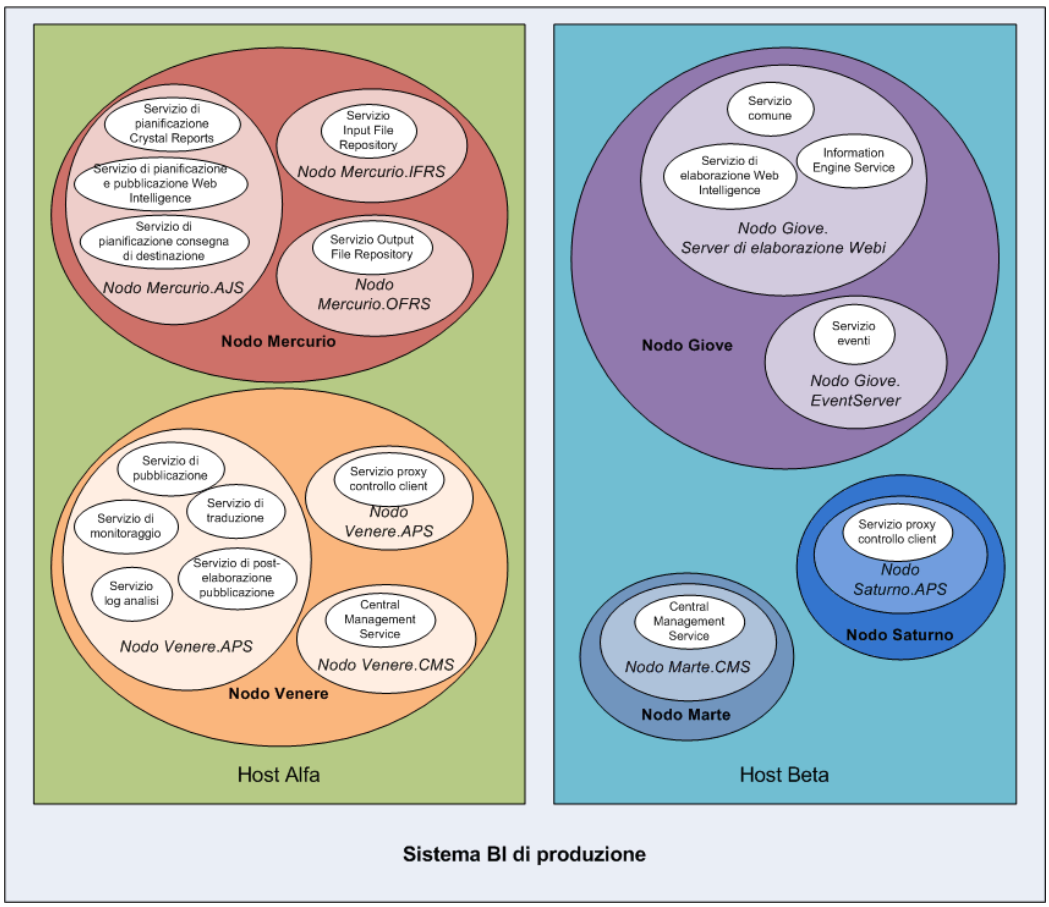
Output File Repository Server gestisce i report creati dal sistema, come i seguenti tipi di file: `.rpt`, `.csv`, `.xls`, `.doc`, `.rtf`, `.txt`, `.pdf`, `.wid`, `.rep`.

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.

2.3 Servizi e server

Il diagramma che segue mostra un'installazione ipotetica della piattaforma BI.

Nota:
i nodi, i server e i servizi vengono mostrati solo a scopo illustrativo. 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*, con due host:

- Sull'host denominato *HostAlpha* è installata la piattaforma BI. L'host è configurato per contenere due nodi:
  - *NodeMercuy*: contiene 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*: contiene un Adaptive Processing Server (*NodeVenus.APS*) con servizi che forniscono funzionalità per la pubblicazione, il monitoraggio e la traduzione, un Adaptive Processing Server (*NodeVenus.APS*) dotato di un servizio per fornire il controllo dei client e un Central Management Server (*NodeVenus.CMS*) con un servizio che fornisce i servizi CMS.
- Sull'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.
  - *NodeJupiter*: contiene un server di elaborazione 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 la pianificazione dei report.

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

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

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). Il servizio di pubblicazione e pianificazione di SAP BusinessObjects Web Intelligence è ad esempio un sottosistema eseguito in Adaptive Job Server.

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 PID.

Un *nodo* è un insieme di server della piattaforma BI eseguiti nello stesso host. Uno o più nodi possono trovarsi in un solo host.

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.

2.3.1 Servizi

Nella tabella che segue sono descritti tutti i servizi.

Tabella 2 - 1: Servizi

Servizio	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio di connessione adattivo	Servizi di connessione	Adaptive Processing Server	Fornisce servizi di connettività (sostituisce Connection Server).
Servizio di pianificazione aggiornamento autenticazione	Servizi principali	Adaptive Job Server	Fornisce la sincronizzazione di aggiornamenti per i plug-in di protezione di terze parti.
Servizio applicazione Web BEx	Servizi di connessione	Adaptive Processing Server	Fornisce l'integrazione delle applicazioni Web SAP Business Warehouse (BW) Business Explorer (BEx) con BI Launch Pad.

Servizio	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio applicazione Web BOE	Servizi principali	Server del contenitore di applicazioni Web	Fornisce applicazioni Web per WACS: include la 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: consente di incorporare la tecnologia BI nelle applicazioni Web. Il servizio BI Business Process è obsoleto.
Central Management Service	Servizi principali	Central Management Server	Fornisce funzionalità di gestione di server, utenti, gestione delle sessioni e protezione (autorizzazione 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 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	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio di modifica e visualizzazione Crystal Reports 2011	Servizi Crystal Reports	RAS	Report Application Server (RAS).
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 nuova versione di Crystal Reports e pubblica i risultati in una determinata posizione di output.
Servizio di accesso ai dati personalizzato	Servizi di connessione	Adaptive Processing Server	Fornisce connessioni dinamiche a origini dati che non richiedono un Connection Server.
Servizio Analitiche del cruscotto	Servizi principali	Dashboard Analytics Server	Fornisce spazi di lavoro BI e funzionalità di modulo per l'analisi dei dati.
Servizio cache di Dashboard Design	Servizi di Dashboard Design	Server cache di Dashboard Design	Limita il numero di accessi al database generati dai report Dashboard Design e velocizza la generazione di report mediante la gestione di una cache di report.

Servizio	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio di elaborazione di Dashboard Design	Servizi di Dashboard Design	Server di elaborazione di Dashboard Design	Accetta ed elabora i report Dashboard Design; è in grado di condividere i dati contenuti in più report per ridurre il numero di accessi al database.
Servizio cruscotto	Servizi principali	Dashboard Server	Supporto di BI Workspace
Servizio Data Federation	Servizi Data Federation	Adaptive Processing Server	Servizio Data Federation.
Servizio di pianificazione consegna di destinazione	Servizi principali	Adaptive Job Server	Esegue i processi pianificati e pubblica i risultati in una posizione di output specifica, ad esempio il file system, FTP, la posta elettronica o la posta in arrivo di un utente.
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 del doppio livello semantico.
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 di connessione	Adaptive Processing Server	Supporta i file Excel caricati nella piattaforma SAP BusinessObjects Business Intelligence come origini dati.
Servizio Information Engine	Servizi Web Intelligence	Web Intelligence Processing Server	Servizio necessario per l'elaborazione di documenti Web Intelligence.

Servizio	Categoria del servizio	Tipo server	Descrizione del servizio
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 comune di Web Intelligence	Servizi Web Intelligence	Web Intelligence Processing Server	Supporta l'elaborazione di documenti Web Intelligence.
Servizio principale di Web Intelligence	Servizi Web Intelligence	Web Intelligence Processing Server	Supporta l'elaborazione di documenti Web Intelligence.
Servizio di monitoraggio Web Intelligence	Servizi Web Intelligence	Adaptive Processing Server	Monitora i server Web Intelligence.
Servizio di elaborazione di Web Intelligence	Servizi Web Intelligence	Web Intelligence Processing Server	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.
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 per la gestione del ciclo di vita.
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	Categoria del servizio	Tipo server	Descrizione del servizio
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 di connessione nativo	Servizi di connessione	Connection Server	Fornitura di servizi di connettività nativi per architetture a 64 bit.
Servizio di connettività nativo (32 bit)	Servizi di connessione	Connection Server	Fornitura di servizi di connettività nativi per architetture 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 determinata 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	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio di pianificazione pubblicazione	Servizi principali	Adaptive Job Server	Esegue i processi di pubblicazione pianificati e pubblica i risultati in una determinata 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 specifica.
Servizio di pubblicazione	Servizi principali	Adaptive Processing Server	Coordina con il servizio di post-elaborazione pubblicazione e il servizio di destinazione per la pubblicazione dei report in una determinata posizione di output, ad esempio il file system, 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 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 Single Sign-On	Servizi principali	Central Management Server	Supporto Single Sign On di Active Directory. Servizio secondario. Viene aggiunto automaticamente al servizio Central Management.

Servizio	Categoria del servizio	Tipo server	Descrizione del servizio
Servizio log analisi	Servizi principali	QUALSIASI SERVER	Supporto per analisi, registrazione e compatibilità
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 specifica.
Servizio Differenza visiva	Servizi Lifecycle Management	Adaptive Processing Server	Determina se i documenti sono visivamente identici per la promozione e Lifecycle Management.
Servizio di visualizzazione	Servizi Web Intelligence	Adaptive Processing Server	Servizio modello di oggetto visualizzazione comune utilizzato da Web Intelligence.
SDK e QaaWS di servizi Web	Servizi principali	Server del contenitore di applicazioni Web	Servizi Web su WACS.

Nota:
È possibile che nelle versioni di manutenzione future della piattaforma SAP BusinessObjects Business Intelligence vengano aggiunti nuovi servizi o tipi di server.

2.3.2 Categorie di servizio

Nella tabella che segue sono elencati tutti i server, ordinati in base alla categoria di servizio. Per una descrizione di ciascun servizio, vedere *Servizi*.

Nota:
È possibile che nelle versioni di manutenzione future della piattaforma SAP BusinessObjects Business Intelligence vengano aggiunti nuovi servizi o tipi di server.

Tabella 2 - 2: Servizi, ordinati per categoria di servizio

Categoria del servizio	Servizio	Tipo di server
Analysis Services	Servizio applicazione Web BEx	Adaptive Processing 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 accesso ai dati personalizzato	Adaptive Processing Server
Servizi di connessione	Servizio di accesso ai dati di Excel	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 applicazione Web BOE	Server del contenitore di applicazioni Web
Servizi principali	Servizio Business Process BI	Server del contenitore di applicazioni Web
Servizi principali	Central Management Service	Central Management Server
Servizi principali	Servizio proxy controllo client	Adaptive Processing Server
Servizi principali	Servizio Analitiche del cruscotto	Dashboard Analytics Server
Servizi principali	Servizio cruscotto	Dashboard Server
Servizi principali	Servizio di pianificazione consegna di destinazione	Adaptive Job Server
Servizi principali	Servizio eventi	Event 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

Categoria del servizio	Servizio	Tipo di 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
Servizi principali	Servizio di pubblicazione	Adaptive Processing Server
Servizi principali	Servizio di replica	Adaptive Job Server
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
Servizi principali	Servizio log analisi	QUALSIASI SERVER
Servizi principali	Servizio di traduzione	Adaptive Processing Server
Servizi principali	SDK e QaaWS di servizi 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	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 di Dashboard Design	Servizio cache di Dashboard Design	Server cache di Dashboard Design

Categoria del servizio	Servizio	Tipo di server
Servizi di Dashboard Design	Servizio di elaborazione di Dashboard Design	Server di elaborazione di Dashboard Design
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 recupero documenti	Adaptive Processing Server
Servizi Web Intelligence	Servizio DSL Bridge	Adaptive Processing Server
Servizi Web Intelligence	Servizio Information Engine	Web Intelligence Processing Server
Servizi Web Intelligence	Servizio di monitoraggio Web Intelligence	Adaptive Processing Server
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	Web Intelligence Processing Server
Servizi Web Intelligence	Servizio principale di Web Intelligence	Web Intelligence Processing Server
Servizi Web Intelligence	Servizio di elaborazione di Web Intelligence	Web Intelligence Processing Server
Servizi Web Intelligence	Servizio di pianificazione di Web Intelligence	Adaptive Job Server

2.3.3 Tipi di server

Nella tabella che segue sono elencati tutti i server, ordinati in base al tipo. Per una descrizione di ciascun servizio, vedere *Servizi*.

Tabella 2 - 3: Server, ordinati in base al tipo

Tipo di 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
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

Tipo di server	Servizio	Categoria del servizio
Adaptive Processing Server	Servizio di accesso ai dati personalizzato	Servizi di connessione
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 di connessione
Adaptive Processing Server	Servizio di monitoraggio Web Intelligence	Servizi Web Intelligence
Adaptive Processing Server	Servizio ClearCase di Lifecycle Management	Servizi Lifecycle Management
Adaptive Processing Server	Servizio Lifecycle Management Console	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
Adaptive Processing Server	Servizio Differenza visiva	Servizi Lifecycle Management
Adaptive Processing Server	Servizio di visualizzazione	Servizi Web Intelligence
QUALSIASI SERVER	Servizio log analisi	Servizi principali
Central Management Server	Central Management Service	Servizi principali
Central Management Server	Servizio Single Sign-On	Servizi principali
Connection Server	Servizio di connessione nativo	Servizi di connessione

Tipo di server	Servizio	Categoria del servizio
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
Dashboard Analytics Server	Servizio Analitiche del cruscotto	Servizi principali
Server cache di Dashboard Design	Servizio cache di Dashboard Design	Servizi di Dashboard Design
Server di elaborazione di Dashboard Design	Servizio di elaborazione di Dashboard Design	Servizi di Dashboard Design
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
RAS	Servizio di modifica e visualizzazione Crystal Reports 2011	Servizi Crystal Reports
Server del contenitore di applicazioni Web	Servizio applicazione Web BOE	Servizi principali
Server del contenitore di applicazioni Web	Servizio Business Process BI	Servizi principali
Server del contenitore di applicazioni Web	SDK e QaaWS di servizi Web	Servizi principali
Web Intelligence Processing Server	Servizio Information Engine	Servizi Web Intelligence
Web Intelligence Processing Server	Servizio comune di Web Intelligence	Servizi Web Intelligence
Web Intelligence Processing Server	Servizio principale di Web Intelligence	Servizi Web Intelligence
Web Intelligence Processing Server	Servizio di elaborazione di Web Intelligence	Servizi Web Intelligence

2.3.4 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 generale che elabora processi pianificati. Quando si aggiunge un Job Server alla piattaforma SAP BusinessObjects Business Intelligence, è possibile configurarlo in modo da elaborare report, documenti, programmi o pubblicazioni e inviare i risultati a destinazioni differenti.
Adaptive Processing Server	Server generico che ospita i servizi responsabili dell'elaborazione di richieste provenienti da diverse origini. **Nota:** 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 i servizi di monitoraggio, di gestione del ciclo di vita, di analisi multidimensionale (MDAS), di pubblicazione e altri ancora. Se si installa un ambiente di produzione, non utilizzare il server APS predefinito. È fortemente consigliato invece eseguire un ridimensionamento del sistema al termine dell'installazione per determinare: • Il tipo e il numero di servizi APS. • La distribuzione di servizi tra più server APS. • Il numero ottimale di server APS. Più server APS offrono ridondanza, migliori prestazioni e un'affidabilità più elevata. • La distribuzione di server APS su più nodi. Creare nuove istanze di server APS secondo quanto stabilito dal processo di ridimensionamento. Se ad esempio il risultato del ridimensionamento sembra suggerire la creazione di un server APS per ogni categoria di servizio, è possibile che porti alla creazione di otto server APS. ovvero uno per ciascuna categoria di servizi: servizi di analisi, servizi di connettività, servizi principali, servizi Crystal Reports, servizi di Dashboard Design, servizi Data Federation, servizi Lifecycle Management e servizi Web Intelligence.
Central Management Server (CMS)	Gestisce un database di informazioni sulla piattaforma SAP BusinessObjects Business Intelligence (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 fornisce 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.
Dashboard Analytics Server	Processo server utilizzato dal componente BI Workspaces per creare e gestire il contenuto dei moduli di spazi di lavoro BI aziendali e personali.
Dashboard Server	Utilizzato dal componente spazio di lavoro BI per creare e gestire i cruscotti aziendali e personali. BI Workspaces offre funzionalità di gestione dei cruscotti per agevolare le organizzazioni nel monitoraggio e nella comprensione delle attività aziendali.
Server cache di Dashboard Design	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 Dashboard Design	Risponde alle richieste di Dashboard Design 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.

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.
Web Intelligence Processing Server	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.

2.4 Applicazioni client

È possibile interagire con la piattaforma SAP BusinessObjects Business Intelligence mediante due tipi di applicazioni desktop:

- 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 SAP BusinessObjects Business Intelligence non installa più le applicazioni desktop. Per installare le applicazioni desktop su 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 l'implementazione della piattaforma SAP BusinessObjects Business Intelligence tramite SSL CORBA o 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 SAP BusinessObjects Business Intelligence 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 Business Web Intelligence, Central Management Console (CMC) e i visualizzatori di report.

2.4.1 Installate con Strumenti client della piattaforma SAP BusinessObjects Business Intelligence

2.4.1.1 Web Intelligence Desktop

Web Intelligence Desktop è uno strumento per l'analisi ad-hoc e la creazione di report disponibile per gli utenti business con o senza accesso alla piattaforma SAP BusinessObjects Business Intelligence.

Consente agli utenti aziendali di accedere e combinare i dati provenienti da origini relazionali, OLAP (Online Analytical Processing), fogli di lavoro o file di testo, utilizzando una terminologia aziendale familiare e un'interfaccia con trascinamento della selezione. 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 Desktop 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).

2.4.1.2 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.

2.4.1.3 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.

2.4.1.4 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.

2.4.1.5 Strumento Web Service Query

Lo strumento Web Service Query (in precedenza Query come servizio Web) consente di utilizzare le query BI (Business Intelligence) in applicazioni Web personalizzate. Gli utenti business possono creare una propria query mediante la connessione a un universo e pubblicarla come servizio Web in modo tale da poterla incorporare in un'applicazione Web.

Web Service Query fornisce nuove soluzioni client per le aziende. Consente ad esempio a SAP BusinessObjects Dashboard Design (in precedenza Xcelsius) di aggregare più origini dati disparate in una vista BI attendibile.

Lo strumento Web Service Query funziona inoltre con 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
- Enterprise Services

2.4.1.6 Information Design Tool

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

2.4.1.7 Translation Management Tool

La piattaforma SAP BusinessObjects Business Intelligence 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 dei relativi prompt e documenti Web Intelligence.

Translation Management Tool:

- Traduce l'universo o i documenti SAP BusinessObjects Web Intelligence 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 SAP BusinessObjects Web Intelligence 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.

2.4.1.8 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 SAP BusinessObjects Business Intelligence, il servizio Data Federation consente universi con più origini grazie alla distribuzione di query in più origini dati e consente di eseguire 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.

2.4.1.9 Widget per la piattaforma SAP BusinessObjects Business Intelligence

I widget sono piccole applicazioni che consentono l'accesso agevole e rapido alle funzioni utilizzate con maggiore frequenza e forniscono informazioni visive dal desktop. La funzionalità dei widget per la piattaforma SAP BusinessObjects Business Intelligence (in precedenza BI Widgets) consente di fornire a tutti i dipendenti di un'azienda l'accesso ai contenuti di Business Intelligence (BI) esistenti nella piattaforma SAP BusinessObjects Business Intelligence. 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 trovato solo nei widget XBCML nelle versioni specificate.

Grazie ai widget per la piattaforma SAP BusinessObjects Business Intelligence, è possibile eseguire ricerche nel contenuto esistente, ad esempio in documenti Web Intelligence, modelli Dashboard Design e applicazioni Web Dynpro, quindi incollare le informazioni chiave sul desktop in modo da renderle velocemente 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 SAP BusinessObjects Business Intelligence (solo per le parti di report Web Intelligence e i modelli Dashboard Design)
- 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 Dashboard Design)

2.4.2 Installate con la piattaforma SAP BusinessObjects Business Intelligence

2.4.2.1 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 un ambiente UNIX, lo script della shell di CCM `ccm.sh` consente di gestire i server dalla riga di comando.

CCM consente di creare e configurare nodi Server Intelligence Agent (SIA) e avviare o arrestare il server di applicazioni Web. In Windows è anche possibile configurare parametri di rete, ad esempio la crittografia SSL (Secure Socket 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.

2.4.2.2 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 oggetti, 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 di SAP BusinessObjects Business Intelligence*.

2.4.2.3 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 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 SAP BusinessObjects Business Intelligence. L'utente può impostare un limite per il numero di errori che lo strumento RDT può trovare e ripristinare prima di interrompersi.

2.4.3 Disponibile separatamente

2.4.3.1 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.

2.4.3.2 SAP Crystal Reports

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

2.4.3.3 SAP BusinessObjects Dashboard Design

SAP BusinessObjects Dashboard Design (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 SAP BusinessObjects Business Intelligence ed esportati in svariati formati, che gli utenti dei dati possono visualizzare nei formati standard, ad esempio PowerPoint, PDF o Flash.

2.4.3.4 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 SAP BusinessObjects Business Intelligence vengono aggiunti i seguenti server:

- 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.

2.4.4 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 quando si installa la piattaforma SAP BusinessObjects Business Intelligence.

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*.

2.4.4.1 Central Management Console (CMC)

La Central Management Console (CMC) è uno strumento Web che consente di eseguire attività amministrative quotidiane, tra cui la gestione degli utenti, del contenuto e dei server. Consente inoltre di pubblicare, organizzare e 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.

Tutti gli utenti possono accedere alla console CMC per modificare le impostazioni delle preferenze utente. Solo i membri del gruppo *Amministratori* possono modificare le impostazioni di gestione, a meno che tale diritto non venga esplicitamente concesso ad altri utenti. È inoltre possibile assegnare ruoli alla CMC per concedere alcuni privilegi utente per l'esecuzione di attività amministrative minori

2.4.4.2 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, cruscotti, scorecard e mappe di strategia.

BI Launch Pad consente agli utenti di gestire:

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

2.4.4.3 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:
per utilizzare le funzionalità degli spazi di lavoro BI, è necessario acquistare una licenza della piattaforma SAP BusinessObjects Business Intelligence che includa l'utilizzo degli spazi di lavoro BI.

2.4.4.4 Visualizzatori di report

I visualizzatori di report supportano diverse piattaforme e diversi browser e rientrano in una delle seguenti categorie:

- 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 di applicazioni elabora la richiesta e recupera le pagine del report dalla piattaforma SAP BusinessObjects Business Intelligence. Il server di applicazioni Web trasferisce quindi le pagine del report al visualizzatore lato client, che le elabora e le visualizza nel browser Web.

- 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 SAP BusinessObjects Business Intelligence e crea pagine DHTML che vengono visualizzate nel browser Web.

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*.

2.4.4.5 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.

2.4.4.6 SAP BusinessObjects Analysis, versione OLAP

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

2.4.4.7 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*.

2.5 Workflow delle informazioni

Quando vengono eseguiti task nella piattaforma SAP BusinessObjects Business Intelligence, ad esempio la registrazione, la pianificazione di un report 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 del sistema della piattaforma SAP BusinessObjects Business Intelligence.

2.5.1 Autenticazione

2.5.1.1 Accesso alla piattaforma SAP BusinessObjects Business Intelligence

Questo workflow è relativo all'accesso di un utente alla piattaforma SAP BusinessObjects Business Intelligence da un browser Web.

1. Il browser invia la richiesta di accesso tramite il server Web al server di applicazioni 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. 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.
6. Il server di applicazioni Web genera una pagina HTML da inviare al client. Il server di applicazioni Web invia la risposta al computer dell'utente dove viene visualizzata nel client Web.

2.5.1.2 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.

   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.

2.5.1.3 Arresto di SIA

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

Quando si arresta il SIA vengono effettuate le seguenti operazioni:

1. Il server CMS indica al SIA di arrestarsi.
2. 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.

2.5.2 Pianificazione

2.5.2.1 Pianificazione di un report SAP Crystal

Questo flusso di lavoro descrive il processo di pianificazione da parte di un utente dell'esecuzione di un report SAP Crystal in un'ora successiva.

1. Il client Web invia una richiesta di pianificazione in un URL, in genere 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 server CMS specificato.
3. Il server CMS garantisce che l'utente disponga dei diritti necessari 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.

2.5.2.2 Pianificazione dell'esecuzione immediata di un report SAP Crystal

Questo flusso di lavoro descrive il processo di pianificazione dell'esecuzione immediata di un report SAP Crystal da parte di un utente.

1. L'utente pianifica un report e la richiesta viene inviata al server di applicazioni Web.
2. Il server di applicazioni Web passa la richiesta al server CMS (Central Management Server).
3. Il server CMS stabilisce se l'utente dispone dei diritti appropriati per pianificare il report.
4. Se l'utente dispone dei diritti appropriati per pianificare il report, il server CMS salva la richiesta dell'oggetto pianificato nel database di sistema CMS.
5. All'ora pianificata, il server CMS individua un Crystal Reports Job Server disponibile in base al valore "Numero max. processi consentiti" configurato in ogni Crystal Reports Job Server.
6. Il server CMS invia le informazioni sul processo al Crystal Reports Job Server.
7. Il Crystal Reports Job Server determina la posizione dell'Input File Repository Server (FRS) che ospita il report. Crystal Reports Job Server richiede quindi il modello di report dal server Input FRS.
8. Il server Input FRS individua il modello di report e lo invia a Crystal Reports Job Server.
9. Il modello di report viene posizionato in una directory temporanea in Crystal Reports Job Server.
10. Crystal Reports Job Server avvia un processo secondario (JobServerChild.exe) per coordinare l'esecuzione del report.
11. Il processo JobServerChild.exe avvia il file ProcReport.dll a cui passa tutte le istanze ricevute da Crystal Reports Job Server. ProcReport.dll chiama Crpe32.dll.
12. Il report viene creato quando i task seguenti vengono completati da Crpe32.dll:
    - Aprire il report.
    - Connettersi al database di produzione.
    - Elaborare il report.

- Creare e salvare l'istanza di report.
- Passare il report a JobServerChild.exe.

13. Crystal Reports Job Server aggiorna periodicamente il server CMS con lo stato del processo. A questo punto lo stato indica che è in corso l'elaborazione del report.
14. JobServerChild.exe carica l'istanza del report nel server Output FRS.
15. Il server Output FRS segnala al processo JobServerChild.exe che il report è stato salvato correttamente.
16. JobServerChild.exe segnala a Crystal Reports Job Server il completamento della creazione del report.
17. Report Job Server aggiorna il server CMS con lo stato del processo. Il processo JobServerChild.exe viene cancellato dalla memoria.
18. Il server CMS aggiorna lo stato del processo in memoria, quindi scrive le informazioni relative all'istanza nel database di sistema CMS.

2.5.2.3 Esecuzione di un report SAP Crystal pianificato

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

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. All'ora del processo pianificato, il server CMS individua un Crystal Reports Job Server disponibile in base al valore "Numero max. processi consentiti" configurato in ogni Crystal Reports Job Server. Il server CMS invia le informazioni sul processo al Crystal Reports Job Server. Le informazioni inviate dal server CMS a Crystal Reports Job Server sono ID report, formato, destinazione, informazioni di accesso, parametri e formule di selezione.
3. Crystal Reports Job Server comunica con Input File Repository Server (FRS) per ottenere un modello di report in base all'ID report richiesto.
4. Crystal Reports Job Server avvia il processo JobChildserver.
5. Il processo secondario (JobChildserver) avvia il file ProcReport.dll alla ricezione del modello da Input File Repository Server tramite l'infrastruttura Enterprise. Il file ProcReport.dll contiene tutti i parametri passati dal server CMS a Crystal Reports Job Server.
6. Con il file ProcReport.dll viene avviato Crpe32.dll tramite cui viene elaborato il report in base a tutti i parametri passati.
7. Durante l'elaborazione, i record vengono recuperati da un server di database definito in un report.
8. Crystal Reports Job Server aggiorna periodicamente il server CMS con lo stato del processo. A questo punto lo stato indica che è in corso l'elaborazione.
9. Terminata la compilazione del report nella memoria di Crystal Reports Job Server, è necessario esportarlo in un altro formato, ad esempio PDF (Portable Document Format). Durante l'esportazione in formato PDF, viene utilizzata la dll PDF.
10. Anche il report con i dati salvati deve essere inviato alla posizione predefinita. Successivamente viene inviato al server Output FRS.

11. Al termine del processo, Crystal Reports Job Server aggiorna il server CMS con lo stato del processo. A questo punto lo stato viene segnalato come 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.

2.5.2.4 Pianificazione di un documento SAP BusinessObjects Web Intelligence

Questo workflow descrive il processo di pianificazione dell'esecuzione di un documento SAP BusinessObjects Web Intelligence a un'ora successiva.

1. L'utente imposta una pianificazione per un documento e la richiesta viene inviata al server Web. Il server Web passa la richiesta di pianificazione del documento al server di applicazioni Web.
2. Il server di applicazioni Web passa la richiesta di pianificazione del documento al server CMS.
3. Il server CMS stabilisce se l'utente dispone dei diritti appropriati per pianificare il documento.
4. Viene creata un'istanza del documento SAP BusinessObjects Web Intelligence nel server CMS che contiene tutte le informazioni di pianificazione rilevanti.
5. Se l'utente dispone dei diritti appropriati per pianificare il documento, imposta parametri di pianificazione diversi.
6. Il server CMS salva la richiesta dell'oggetto pianificato nel database di sistema.

2.5.2.5 Viene eseguito un documento SAP BusinessObjects Web Intelligence, versione OLAP

Questo workflow descrive il processo di esecuzione di un documento SAP BusinessObjects Web Intelligence a un'ora pianificata.

1. Il Central Management Server (CMS) controlla il database di sistema CMS per stabilire se è presente un processo SAP BusinessObjects Web Intelligence pianificato da eseguire.
2. All'ora pianificata, il server CMS invia la richiesta di pianificazione e tutte le informazioni sulla richiesta al server Adaptive Job Server che ospita il servizio di pianificazione e pubblicazione SAP BusinessObjects Web Intelligence.
3. Adaptive Job Server (servizio di pianificazione e pubblicazione Web Intelligence) individua un server di elaborazione Web Intelligence disponibile in base al valore Numero max. processi consentiti configurato in ogni server di elaborazione SAP BusinessObjects Web Intelligence.
4. Il server di elaborazione SAP BusinessObjects Web Intelligence determina la posizione dell'Input File Repository Server (FRS) che ospita il documento e il file di metalivello dell'universo su cui si basa il documento. Il server di elaborazione SAP BusinessObjects Web Intelligence richiede quindi il documento al server Input FRS. Il server Input FRS individua il documento SAP BusinessObjects Web Intelligence e il file dell'universo su cui si basa il documento, quindi li invia al server di elaborazione SAP BusinessObjects Business Intelligence Solution.

5. Il documento SAP BusinessObjects Web Intelligence viene posizionato in una directory temporanea nel server di elaborazione SAP BusinessObjects Web Intelligence. Il documento viene aperto in memoria dal server di elaborazione SAP BusinessObjects Web Intelligence. Il file QT.dll genera il codice SQL dall'universo su cui si basa il documento. Il Connection Server (componente del server di elaborazione SAP BusinessObjects Web Intelligence) si connette al database. I dati di query vengono passati tramite QT.dll al motore di documento in cui viene elaborato il documento. Viene creata una nuova istanza funzionante.
6. Il server di elaborazione SAP BusinessObjects Web Intelligence carica l'istanza del documento nel server Output FRS.
7. Il server di elaborazione SAP BusinessObjects Web Intelligence segnala ad Adaptive Job Server (servizio di pianificazione e pubblicazione SAP BusinessObjects Web Intelligence) che la creazione del documento è stata completata. 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. Adaptive Job Server (servizio di pianificazione e pubblicazione Web Intelligence) aggiorna il server 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.

2.5.2.6 Pianificazione di un oggetto

Questo flusso di lavoro descrive il processo di pianificazione da parte di un utente dell'esecuzione di un oggetto.

1. L'utente pianifica un oggetto e la richiesta viene inviata al server Web.
2. Il server Web passa la richiesta di pianificazione dell'oggetto al server di applicazioni Web.
3. Il server di applicazioni Web passa la richiesta al server CMS (Central Management Server).
4. Il server CMS stabilisce se l'utente dispone dei diritti appropriati per pianificare l'oggetto.
5. Se l'utente dispone dei diritti appropriati per pianificare l'oggetto, il server CMS salva la richiesta dell'oggetto pianificato nel database di sistema CMS.
6. All'ora pianificata, il server CMS individua un Program Job Server disponibile in base al valore Numero max. processi consentiti configurato in ogni Program Job Server.
7. Il server CMS invia le informazioni sul processo a Program Job Server.
8. Program Job Server comunica con Input File Repository Server e richiede l'oggetto programma.
9. Input File Repository Server restituisce l'oggetto programma a Program Job Server.
10. Program Job Server avvia l'oggetto pianificato.
11. Program Job Server aggiorna il server CMS periodicamente con lo stato del processo. A questo punto, lo stato indica che il programma è in corso di elaborazione.
12. Program Job Server invia un file di registro a Output File Repository Server.
13. Output File Repository Server segnala a Program Job Server che l'oggetto è stato pianificato correttamente mediante l'invio di un file di registro dell'oggetto.

14. Program Job Server aggiorna il server CMS con lo stato del processo.
15. Il server CMS aggiorna lo stato del processo in memoria, quindi scrive le informazioni relative all'istanza dell'oggetto nel database di sistema CMS.

2.5.2.7 Pianificazione dell'esecuzione immediata di un oggetto

Questo workflow descrive il processo di pianificazione dell'esecuzione immediata di un oggetto.

1. L'utente pianifica un oggetto e la richiesta viene inviata al server Web.
2. Il server Web passa la richiesta di pianificazione dell'oggetto al server di applicazioni Web.
3. Il server di applicazioni Web passa la richiesta al server CMS (Central Management Server).
4. Il server CMS stabilisce se l'utente dispone dei diritti appropriati per pianificare l'oggetto.
5. Se l'utente dispone dei diritti appropriati per pianificare l'oggetto, il server CMS salva la richiesta dell'oggetto pianificato nel database di sistema CMS.
6. All'ora pianificata, il server CMS individua un Program Job Server disponibile in base al valore "Numero max. processi consentiti" configurato in ogni Program Job Server.
7. Il server CMS invia le informazioni sul processo a Program Job Server.
8. Program Job Server comunica con Input File Repository Server e richiede l'oggetto programma.
9. Input File Repository Server restituisce l'oggetto programma a Program Job Server.
10. Program Job Server avvia l'oggetto pianificato.
11. Program Job Server aggiorna il server CMS periodicamente con lo stato del processo. A questo punto, lo stato indica che il programma è in corso di elaborazione.
12. Program Job Server invia un file di registro a Output File Repository Server.
13. Output File Repository Server segnala a Program Job Server che l'oggetto è stato pianificato correttamente mediante l'invio di un file di registro dell'oggetto.
14. Program Job Server aggiorna il server CMS con lo stato del processo.
15. Il server CMS aggiorna lo stato del processo in memoria, quindi scrive le informazioni relative all'istanza dell'oggetto nel database di sistema CMS.

2.5.3 Visualizzazione

2.5.3.1 Visualizzazione di un report SAP Crystal

Questo flusso di lavoro descrive il processo di richiesta da parte di un utente in una pagina in un report SAP Crystal, quando il report non esiste già in un server cache.

1. L'utente invia la richiesta di visualizzazione attraverso il server Web al server di applicazioni Web.
2. Il server di applicazioni Web riconosce che si tratta di una richiesta di visualizzazione di una pagina di report. Il server di applicazioni Web verifica nel server CMS che l'utente disponga di diritti sufficienti per visualizzare il report.
3. Il server CMS stabilisce se l'utente dispone dei diritti appropriati per 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 di report richiesta.
6. Crystal Reports Cache Server determina se il file richiesto esiste nella directory cache.
7. Il file EPF richiesto non viene trovato nella directory cache.
8. Crystal Reports Cache Server invia la richiesta a Crystal Reports Page Server.
9. Crystal Reports Page Server esegue una query nel server Output File Repository Server (FRS) per l'istanza di report richiesta.
10. Il server Output FRS invia l'istanza di report richiesta a Crystal Reports Page Server.
11. Crystal Reports Page Server apre l'istanza di report e controlla se nel report sono presenti dati.
12. Crystal Reports Page Server determina che il report contiene dati e crea il file per la pagina di report richiesta senza connettersi al database di produzione.
13. Crystal Reports Page Server invia il file EPF a Crystal Reports Cache Server.
14. Crystal Reports Cache Server scrive il file EPF nella directory cache.
15. Crystal Reports Cache Server invia la pagina richiesta al server di applicazioni Web.
16. Il server di applicazioni Web invia il file al server Web.
17. Il server Web invia la pagina richiesta al visualizzatore di report.

2.5.3.2 Visualizzazione di un report SAP Crystal di cache

Questo flusso di lavoro descrive il processo di richiesta da parte di un utente in una pagina in un report SAP Crystal, quando il report esiste già in un server cache.

1. Un client Web invia una richiesta di visualizzazione in un URL 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 prima pagina di un'istanza di report selezionata. Il server di applicazioni Web invia una richiesta al server CMS per verificare che l'utente disponga dei diritti di visualizzazione necessari per l'istanza.
3. Il server CMS esegue un controllo nel database di sistema CMS per verificare la presenza di diritti dell'utente.
4. Il server CMS invia una risposta al server di applicazioni Web per verificare che l'utente disponga dei diritti sufficienti per visualizzare l'istanza.

5. Il server di applicazioni Web invia una richiesta a Crystal Reports Cache Server per la prima pagina dell'istanza di report. Crystal Reports Cache Server verifica che la pagina esista già. Se esiste, Crystal Reports Cache Server restituisce la pagina al server di applicazioni Web.
6. Il server di applicazioni Web invia la pagina al client Web in cui viene eseguito il rendering e la visualizzazione della pagina.

2.5.3.3 Visualizzazione di uno spazio di lavoro SAP Analysis, versione OLAP

Questo workflow descrive il processo di un utente che richiede uno spazio di lavoro SAP Analysis, versione OLAP (in precedenza Voyager).

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 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 Advanced Analyzer 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.

2.5.4 Su richiesta

2.5.4.1 Visualizzazione di un report SAP Crystal su richiesta

Questo flusso di lavoro descrive il processo di un utente che richiede una pagina di un report SAP Crystal su richiesta.

1. Il client Web invia una richiesta in un URL, in genere tramite il server Web al server di applicazioni Web.
2. Il server di applicazioni Web interpreta la pagina richiesta e i valori inviati nella richiesta di URL e determina che si tratta di una richiesta di visualizzazione della prima pagina dell'oggetto report selezionato.
3. Il server di applicazioni Web invia una richiesta al server CMS per verificare che l'utente disponga dei diritti di visualizzazione necessari per l'oggetto. Il server CMS esegue un controllo nel database di sistema CMS per verificare la presenza di diritti dell'utente.
4. Il server CMS invia una risposta al server di applicazioni Web per verificare che l'utente disponga dei diritti sufficienti per visualizzare l'oggetto.
5. Il server di applicazioni Web invia una richiesta a Crystal Reports Cache Server per la prima pagina dell'oggetto report.
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, dati di accesso al database, parametri), Crystal Reports Cache Server invia una richiesta a Crystal Reports Processing Server per generare la pagina.
7. Crystal Reports Processing Server richiede l'oggetto report da Input File Repository Server. Input File Repository Server invia una copia dell'oggetto a Crystal Reports Processing Server. Crystal Reports Processing Server apre il report in memoria e verifica se il report contiene dati.
8. Supponendo che l'oggetto report non contenga dati, è necessario che Crystal Reports Processing Server si connetta al database per chiedere i dati mediante una query.
9. Crystal Reports Processing Server invia la pagina a Crystal Reports Cache Server. Crystal Reports Cache Server archivia una copia della pagina 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 la pagina EPF al server Web. Il server Web invia la pagina al computer dell'utente dove viene visualizzata nel visualizzatore del client Web.

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

Questo workflow descrive il processo di visualizzazione su richiesta di un documento SAP BusinessObjects Web Intelligence.

1. Un browser invia la richiesta di visualizzazione al server di applicazioni Web tramite il server Web.
2. Il server di applicazioni Web stabilisce che si tratta di una richiesta di documento Web Intelligence e invia una richiesta al server CMS per verificare che l'utente disponga dei diritti appropriati per visualizzare il documento.
3. Il server CMS invia una risposta al server di applicazioni Web per verificare che l'utente disponga dei diritti sufficienti per visualizzare il documento.
4. Il server di applicazioni Web invia una richiesta a Web Intelligence Processing Server che richiedere il documento.
5. Web Intelligence Processing Server 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 metalivello, inclusa la protezione a livello di riga e di colonna.
6. L'Input FRS invia una copia del documento a Web Intelligence Processing Server, nonché il file dell'universo su cui è stato generato il documento richiesto.
7. Il documento viene aperto in memoria dal modulo di report Web Intelligence.
8. Il modulo di report Web Intelligence utilizza il componente QT (inproc) e ConnectionServer (inproc). Il componente QT genera, convalida e rigenera il codice SQL e stabilisce la connessione 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.
9. Web Intelligence Processing Server invia al server di applicazioni Web la pagina del documento visualizzabile richiesta. Il server di applicazioni Web inoltra la pagina visualizzabile al server Web. Il server Web invia la pagina visualizzabile al computer dell'utente, dove viene visualizzata in un browser Web.

2.5.4.3 Visualizzazione di un report SAP Crystal su richiesta quando il formato di visualizzazione predefinito è impostato su Web Java

Questo flusso di lavoro descrive il processo di un utente che visualizza un report SAP Crystal quando il formato di visualizzazione predefinito è impostato su Web Java.

1. Il client Web invia la richiesta di visualizzazione su richiesta tramite il server Web al server di applicazioni Web.
2. Il server di applicazioni Web interpreta la pagina richiesta e i valori inviati nella richiesta di URL e determina che si tratta di una richiesta di visualizzazione della prima pagina dell'oggetto report selezionato.

3. Il server di applicazioni Web invia una richiesta al server CMS per verificare che l'utente disponga dei diritti di visualizzazione necessari per l'oggetto. Il server CMS esegue un controllo nel database di sistema CMS per verificare la presenza di diritti dell'utente.
4. Il server CMS invia una risposta al server di applicazioni Web per verificare che l'utente disponga dei diritti sufficienti per visualizzare l'oggetto.
5. Il server di applicazioni Web invia una richiesta a Crystal Reports Cache Server per la prima pagina dell'oggetto report.
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, dati di accesso al database, parametri), Crystal Reports Cache Server invia una richiesta a Crystal Reports Processing Server per generare la pagina.
7. Crystal Reports Processing Server richiede l'oggetto report da Input File Repository Server. Input File Repository Server invia una copia dell'oggetto a Crystal Reports Processing Server. Crystal Reports Processing Server apre il report in memoria e verifica se il report contiene dati.
8. Supponendo che l'oggetto report non contenga dati, è necessario che Crystal Reports Processing Server si connetta al database per chiedere i dati mediante una query.
9. Crystal Reports Processing Server invia la pagina EPF a Crystal Reports Cache Server. Crystal Reports Cache Server archivia una copia della pagina EPF nella directory cache in previsione di nuove richieste di visualizzazione. È anche possibile che una pagina ETF venga generata e inviata a Crystal Reports Cache Server in questa fase. La pagina ETF (navigazione dell'albero dei gruppi del riquadro sinistro del report) viene generata alla generazione della prima pagina del report e al raggruppamento del report. È presente una sola pagina ETF per report, ma le dimensioni di tale pagina possono essere notevoli.
10. Crystal Reports Cache Server invia la pagina EPF al server di applicazioni Web.
11. Il server di applicazioni Web invia la pagina EPF al server Web. Il server Web invia la pagina EPF al computer dell'utente dove viene visualizzata nel visualizzatore del client Web.

Gestione delle licenze

3.1 Gestione delle chiavi di licenza

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

Argomenti correlati

- Per visualizzare le informazioni sulle licenze
- Per aggiungere un codice di licenza
- Per visualizzare l'attività dell'account corrente

3.1.1 Per visualizzare le informazioni sulle licenze

L'area di gestione **Codice di licenza** della CMC identifica il numero di licenze basate su ruoli (Visualizzatore BI e Analista BI), ad accesso simultaneo, titolari e per processore 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

- Gestione delle chiavi di licenza
- Per aggiungere un codice di licenza
- Per visualizzare l'attività dell'account corrente

3.1.2 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.

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

- Per visualizzare le informazioni sulle licenze
- Per visualizzare l'attività dell'account corrente

3.1.3 Per visualizzare l'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

- Gestione delle chiavi di licenza
- Per aggiungere un codice di licenza
- Per visualizzare le informazioni sulle licenze

3.2 Misurazione delle licenze

BusinessObjects License Measurement Tool (BOLMT) è un'utilità Java della riga di comando che consente di raccogliere e archiviare i dati sulle licenze della piattaforma BI. Il documento XML di output contiene misure della distribuzione della licenza e viene inviato al servizio GLAS (Global License Auditing Services) di SAP per il consolidamento come parte di un controllo della licenza.

L'amministratore del sistema installa ed esegue BOLMT per ciascun cluster della piattaforma BI ogni volta che viene richiesto un controllo della licenza. BOLMT raccoglie le misure dell'utilizzo nelle licenze basate su ruolo, titolari e utente simultaneo.

L'amministratore può specificare una particolare directory di output per il documento XML e configurare il documento in modo tale che non contenga informazioni che possono essere utilizzate per identificare gli utenti del sistema.

3.2.1 Esecuzione di un controllo della licenza

Per eseguire un controllo della licenza, è necessario disporre dei diritti di amministratore e dell'accesso alla directory contenente il file `BOLMT.jar` nell'installazione della piattaforma BI.

1. Aprire una console della riga di comando.
2. Passare alla directory contenente gli eseguibili Java per l'installazione della piattaforma BI.

   Per impostazione predefinita, il file viene installato nella seguente directory: *[DIRINSTALLAZ]*`\SAP BusinessObjects Enterprise XI 4.0\java\lib`
3. Eseguire il file BOLMT.jar.

   Il comando di esecuzione viene immesso nel seguente formato: `-jar BOLMT.jar` [opzioni] <FileOutput>

   La tabella che segue contiene un riepilogo delle opzioni disponibili:

Opzione	Descrizione
-c --cms	Specifica l'identificatore del nome e il numero di porta per il Central Management Server (CMS). Specificato come *nomecms*:*numero porta*. Per impostazione predefinita, vengono utilizzate le impostazioni del CMS per l'host locale se questa impostazione non viene specificata.
-p --password	Specifica la password dell'account Administrator utilizzata per la connessione al server CMS.
-a--auth	Specifica il metodo di autenticazione per la connessione utente al server CMS. Il metodo predefinito è quello aziendale, specificato come `secEnterprise`.
-s--sanitize	Specifica che il documento di controllo generato deve filtrare tutte le informazioni personali che possono essere utilizzate per identificare gli utenti.

Nota:
la specificazione del file di output è sempre l'ultimo argomento della riga di comando. Questa impostazione è facoltativa. Se non viene specificato un argomento, il documento viene generato come output standard della console. È inoltre possibile inserire l'output in uno script come argomento della riga di comando.

Esempio:

```
C:\Program Files (x86)\SAP
Business Objects\SAP BusinessObjects Enterprise XI 4. 0\java\lib>"C:\Program Files
(x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin
\java.exe" -jar BOLMT.jar --cms=mycms:6400 -uAdministrator
-p=7juujg --auth=secEnterprise --sanitize audit.xml
```

Gestione di utenti e gruppi

4.1 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.

4.1.1 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 4 - 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
SMAdmin	Account di sola lettura utilizzato da SAP Solution Manager per accedere ai componenti della piattaforma BI.

4.1.1.1 Licenze basate sul ruolo

Nello schema di licenze basato su ruoli utente, sono presenti due ruoli che è possibile assegnare agli utenti della piattaforma BI:

- Analista BI
- Visualizzatore BI

Ogni ruolo include determinati livelli di accesso alle applicazioni della piattaforma BI. Non è possibile modificare o ignorare i livelli di accesso dei ruoli utente. I ruoli utente si applicano ai nuovi account utente creati nella piattaforma BI o agli utenti esistenti importati da servizi directory di terze parti come Windows AD o LDAP.

Nota:
i ruoli utente non devono essere confusi con le appartenenze a gruppi. Quando si assegna a un utente uno dei due ruoli disponibili, a tale utente vengono automaticamente assegnati i diritti predefiniti alle applicazioni. Per associare un utente ai livelli di accesso di un gruppo specifico, è necessario aggiungere l'utente al gruppo desiderato.

Fare clic su **Codice di licenza** nella CMC per ulteriori informazioni sullo schema di licenze oppure contattare il proprio account manager per SAP Business Objects per informazioni dettagliate sui diritti di accesso per ogni ruolo utente.

4.1.1.1.1 Ruolo Analista BI

Il ruolo Analista BI è destinato agli utenti che creano contenuto nel sistema della piattaforma BI. Agli utenti che modificano o creano report, progettano e gestiscono universi, o che eseguono attività amministrative nella CMC, deve essere assegnato il ruolo Analista BI.

4.1.1.1.2 Ruolo Visualizzatore BI

Il ruolo Visualizzatore BI è destinato principalmente agli utenti finali del contenuto. Tali utenti possono visualizzare i report ma non modificarne il contenuto.

Gli utenti a cui è assegnato il ruolo Visualizzatore BI non possono creare contenuto, modificare report né eseguire attività amministrative generali nel sistema. Il ruolo Visualizzatore BI non deve essere assegnato agli utenti che devono:

- Creare report
- Aggiornare o modificare report

- Eseguire attività amministrative tramite la CMC

Nota:
gli utenti Visualizzatore BI non possono accedere alla CMC.

4.1.2 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 4 - 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.
Utenti di Strumento di conversione dei report	I membri di questo gruppo hanno accesso all'applicazione Strumento di conversione dei report.

Nome account	Descrizione
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

4.1.3 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 4 - 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 nella piattaforma BI, gli utenti possono accedere alle applicazioni della piattaforma BI con il nome utente e la password di cui dispongono su LDAP. Si evita, in tal modo, di creare nuovamente degli 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 nella piattaforma BI, gli utenti possono accedere alle applicazioni della piattaforma BI con il nome utente e la password di cui dispongono su AD. Si evita, in tal modo, di creare nuovamente degli 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. Si evita, in tal modo, di creare nuovamente degli 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. Si evita, in tal modo, di creare nuovamente degli 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. Si evita, in tal modo, di creare nuovamente degli 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. Si evita, in tal modo, di creare nuovamente degli 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. Si evita, in tal modo, di creare nuovamente degli account utente e di gruppo individuali all'interno della piattaforma BI.

4.2 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 BI 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.

4.2.1 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. Selezionare **Enterprise** nell'elenco **Tipo di autenticazione**.
   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. Specificare come designare l'account utente in base alle opzioni del proprio contratto di licenza della piattaforma SAP BusinessObjects Business Intelligence.

   Se il contratto di licenza si basa sui ruoli utente, selezionare una delle opzioni seguenti:
   - **Visualizzatore BI** : l'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Visualizzatore BI è definito nel contratto di licenza. Gli utenti potranno accedere ai workflow delle applicazioni in base a quanto previsto dal ruolo Visualizzatore BI. I diritti di accesso generalmente sono limitati alla visualizzazione dei documenti business intelligence. Questo ruolo è di norma adatto agli utenti che utilizzano contenuti mediante le applicazioni della piattaforma BI.
   - **Analista BI** : l'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Analista BI è definito nel contratto di licenza. Gli utenti possono accedere a tutti i workflow delle applicazioni definiti per il ruolo Analista BI. I diritti di accesso includono la visualizzazione e la modifica dei documenti business intelligence. Questo ruolo è adatto agli utenti che creano e modificano contenuti per le applicazioni della piattaforma.

   Se il contratto di licenza non è basato sui ruoli utente, specificare un tipo di connessione per l'account utente.
   - Scegliere **Utente simultaneo** se questo utente ha sottoscritto un contratto di licenza che definisce il numero di utenti a cui è consentito l'accesso simultaneo.
   - Scegliere **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
- Licenze basate sul ruolo

4.2.2 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

4.2.3 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

4.2.4 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.

4.2.5 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**.

4.2.6 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.

4.2.7 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

4.2.8 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.

4.2.9 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.

4.2.10 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 la procedura descritta d seguito se si desidera abilitare l'account Guest in modo che gli utenti non richiedano ai propri account di accedere a BI Launch Pad.

1. Accedere all'area di gestione "Utenti e gruppi" della console 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**.

4.2.11 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

4.2.11.1 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**.

4.2.11.2 Per aggiungere uno o più 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**.

4.2.12 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.

4.2.12.1 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**.

4.2.12.2 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 4 - 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

Impostazione password	Minimo	Massimo consigliato
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**.

4.2.13 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

4.2.14 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

- Pianificazione dell'esecuzione immediata di un oggetto
- Gestione delle impostazioni di protezione per gli oggetti nella CMC

4.2.15 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.

4.2.15.1 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.

4.2.15.1.1 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 nel computer che ospita il server di applicazioni Web.

1. Nell'installazione della piattaforma BI, è necessario andare nella seguente directory:

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

Nota:
Se si utilizza la versione di Tomcat installata con la piattaforma BI, è inoltre possibile accedere alla directory seguente: `C:\Programmi (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom`

- Se si utilizza qualsiasi altro server di applicazioni Web supportato, consultare la documentazione del server per determinare il percorso appropriato.

2. Creare un nuovo file.

   Nota:
   utilizzare Blocco note o un'altra utilità per la modifica del testo.

3. Salvare il file con questo nome:

   BIlaunchpad.properties

4. Per includere le opzioni di autenticazione nella schermata di accesso di BI Launch Pad, aggiungere quanto segue:

```
authentication.visible=true
```

5. Per modificare il tipo di autenticazione predefinito, aggiungere quanto segue:

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

   Sostituire `<authentication>` con una delle seguenti opzioni

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:

```
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*

4.2.15.2 Configurazione delle preferenze di BI Launch Pad per i gruppi

Gli amministratori possono impostare le preferenze di BI Launch Pad per gruppi di utenti specifici. Tali preferenze vengono utilizzate come preferenze predefinite di BI Launch Pad per tutti gli utenti del gruppo.

Nota:
se gli utenti hanno impostato preferenze personalizzate, le impostazioni definite dall'amministratore non verranno estese alla visualizzazione di BI Launch Pad. Gli utenti possono passare dalle proprie preferenze a quelle definite dall'amministratore in qualsiasi momento e utilizzare le impostazioni aggiornate.

Per impostazione predefinita, non vengono impostate preferenze di BI Launch Pad per i gruppi di utenti. Gli amministratori possono specificare le preferenze per gli elementi seguenti:

- Scheda iniziale
- Posizione iniziale dei Documenti
- Cartelle
- Categorie
- Numero di oggetti per pagina
- Colonne visualizzate nella scheda "Documento"
- Modalità di visualizzazione dei documenti in BI Launch Pad, mediante le schede o una nuova finestra

4.2.15.2.1 Impostazione delle preferenze di BI Launch Pad per un gruppo

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	Visualizza un sito Web specifico come scheda iniziale. Fare clic su **Sfoglia scheda iniziale**. Nella finestra "Selezionare una scheda iniziale personalizzata" selezionare un oggetto repository e fare clic su **Apri**. **Nota:** è possibile selezionare solo un oggetto già aggiunto al repository.

- 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	Scegliere una delle opzioni seguenti da visualizzare nella scheda Documenti: • Preferiti • Categorie personali • Posta in arrivo
Cartelle	Scegliere una delle opzioni seguenti: • Cartelle pubbliche: visualizza le cartelle pubbliche nella scheda Documenti • Seleziona cartella pubblica Fare clic su **Sfoglia cartella** per selezionare una cartella pubblica specifica da visualizzare nella scheda Documenti.
Categorie	Scegliere una delle opzioni seguenti: • Categorie aziendali: visualizza le categorie aziendali nella scheda Documenti • Seleziona categoria aziendale Fare clic su **Sfoglia cartella** per selezionare una categoria aziendale specifica da visualizzare nella scheda Documenti.

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.

4.3 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.

4.3.1 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.

4.3.2 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".

4.3.3 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**.

4.3.4 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".

4.3.5 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

5.1 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 funzioni 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

5.1.1 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 è 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

5.1.2 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 5 - 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

5.1.3 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 sottgruppi 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.

5.1.3.1 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.

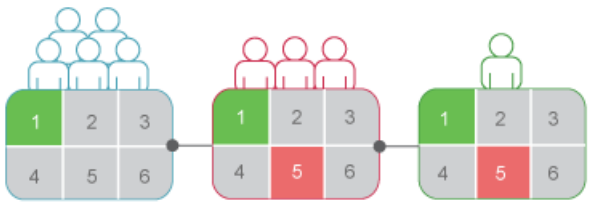


Figura 5 - 1: Ereditarietà di gruppo - Esempio 1

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.

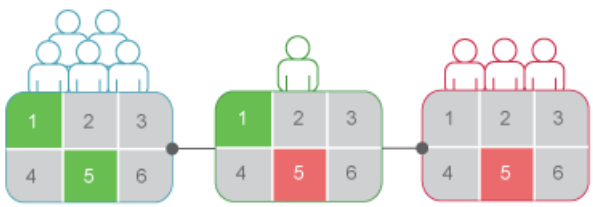


Figura 5 - 2: Ereditarietà di gruppo - Esempio 2

Argomenti correlati

- Priorità di diritti

5.1.3.2 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.

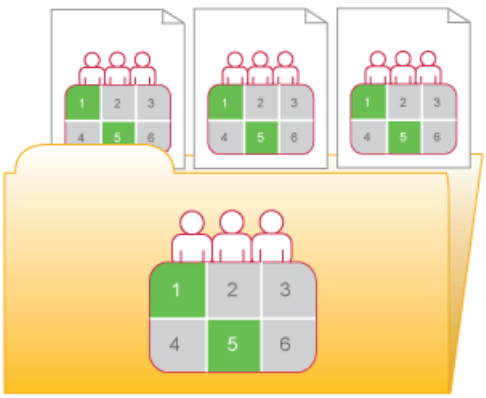


Figura 5 - 3: Esempio di ereditarietà di cartella

Argomenti correlati

- Priorità di diritti

5.1.3.3 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 dirittii 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.

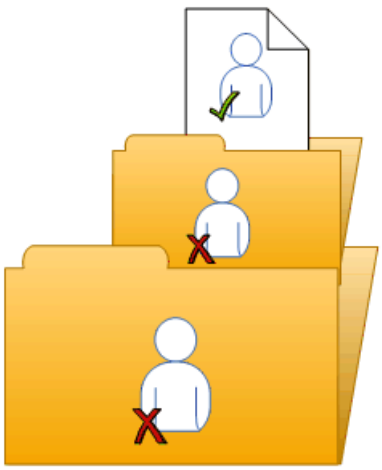


Figura 5 - 4: Esempio di override dei diritti 1

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.

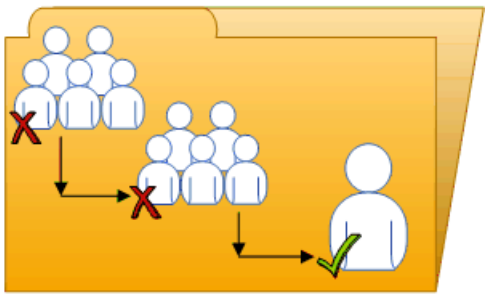


Figura 5 - 5: Esempio di override dei diritti 2

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 contradditori 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.

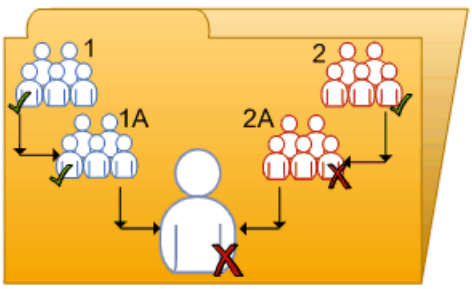


Figura 5 - 6: Priorità complessa dei diritti

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.

5.1.3.4 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 **visua lizzazione** 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 sicura** 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.

5.1.4 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.

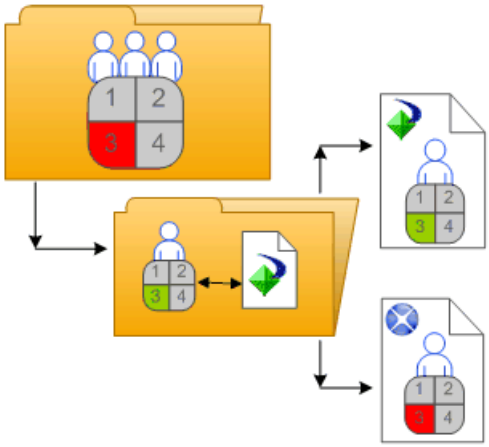


Figura 5 - 7: Esempio di diritti specifici del tipo

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.

5.1.5 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.

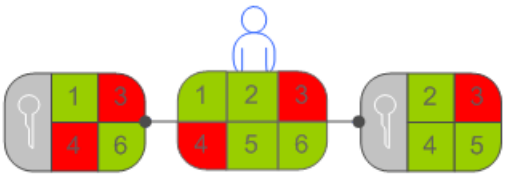


Figura 5 - 8: Livelli di accesso multipli

- 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.

5.2 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.

5.2.1 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.

5.2.2 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

5.2.3 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

5.2.4 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

5.2.5 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

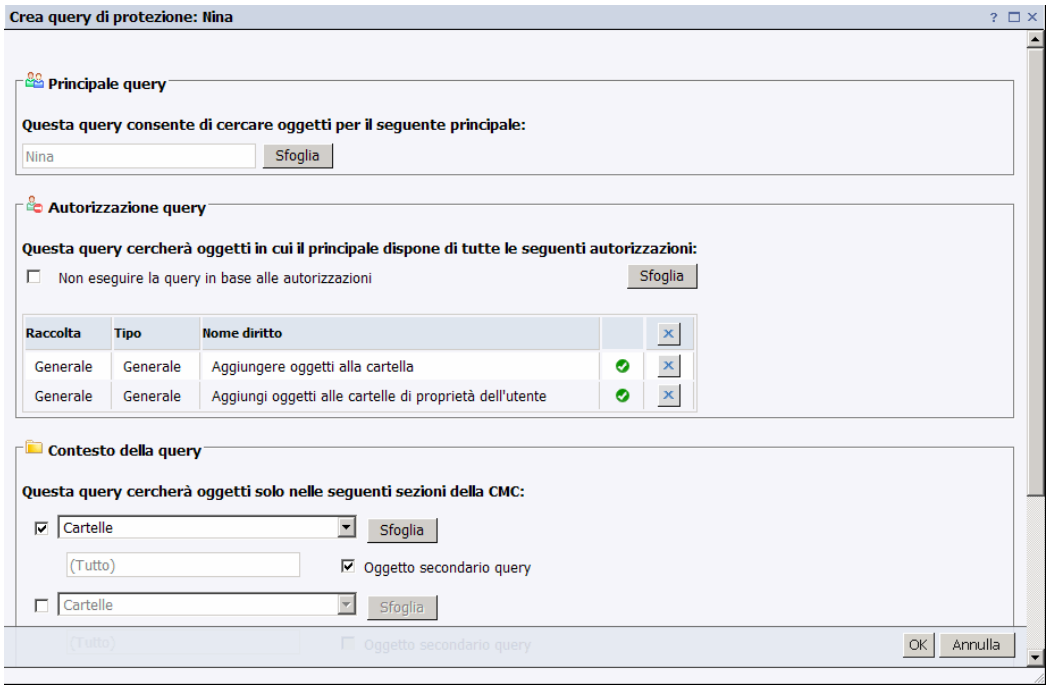
  Specificare le aree CMC in cui si desidera effettuare la ricerca tramite la query protezione. Per ogni area, è possibile scegliere se includere oggetti secondari nella query protezione. Una query protezione può avere un massimo di quattro aree.

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 pormosso 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.

5.2.5.1 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**.



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'intestazione.

   - 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.
   a. Selezionare una casella di controllo accanto a un elenco.
   b. 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.

5.3 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 riepiloga i diritti contenuti in ogni livello di accesso.

Tabella 5 - 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.	• 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: • 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: • Aggiorna i dati del report
Controllo completo	Un principale dispone del controllo amministrativo completo dell'oggetto.	Tutti i diritti disponibili, compresi: • 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	• Diritto di **aggiunta** sulla cartella principale dei **livelli di accesso**
Diritti granulari di visualizzazione in un livello di accesso	• Diritto di **visualizzazione** sul livello di accesso
Assegnazione di un livello di accesso a un principale su un oggetto	• 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** sull'oggetto e sul principale **Nota:** Gli utenti che dispongono del diritto **Modificare in modo sicuro i diritti** e desiderano assegnare un livello di accesso a un principale devono disporre dello stesso livello di accesso.
Modificare un livello di accesso	• Diritti di **visualizzazione** e **modifica** sul livello di accesso
Eliminare un livello di accesso	• Diritti di **visualizzazione** ed **eliminazione** sul livello di accesso
Duplicare un livello di accesso	• Diritto di **visualizzazione** sul livello di accesso • Diritto di **copia** sul livello di accesso • Diritto di **aggiunta** sulla cartella principale dei **livelli di accesso**

5.3.1 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 utillizzare 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.

5.3.2 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.

5.3.3 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**.

5.3.4 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".

5.3.5 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**.

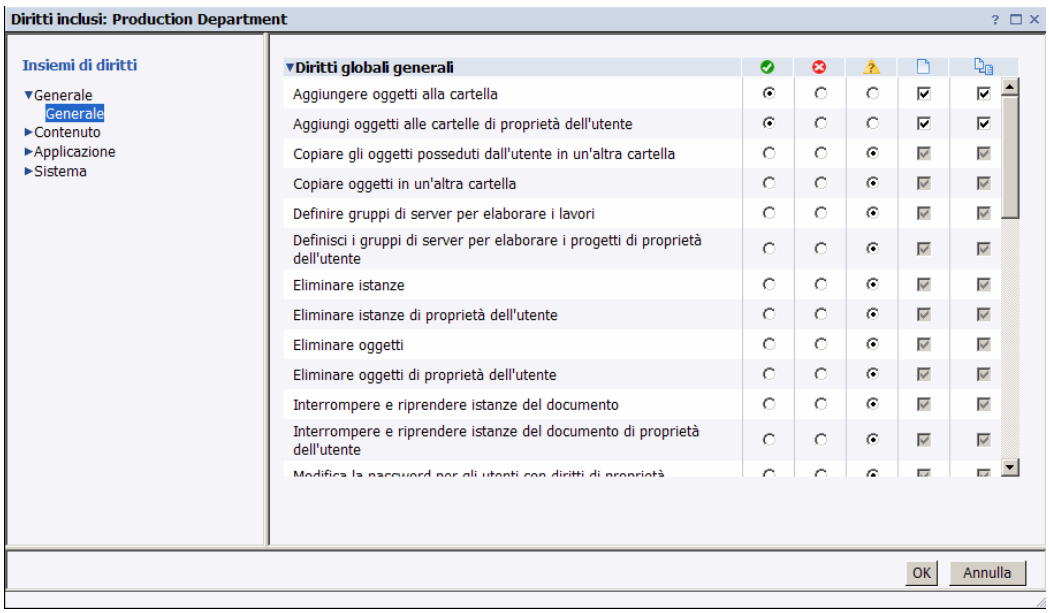
Il livello di accesso viene eliminato e si torna all'area "Livelli di accesso".

5.3.6 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

5.3.7 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 ristrutturi 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.

5.3.8 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

5.4 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.

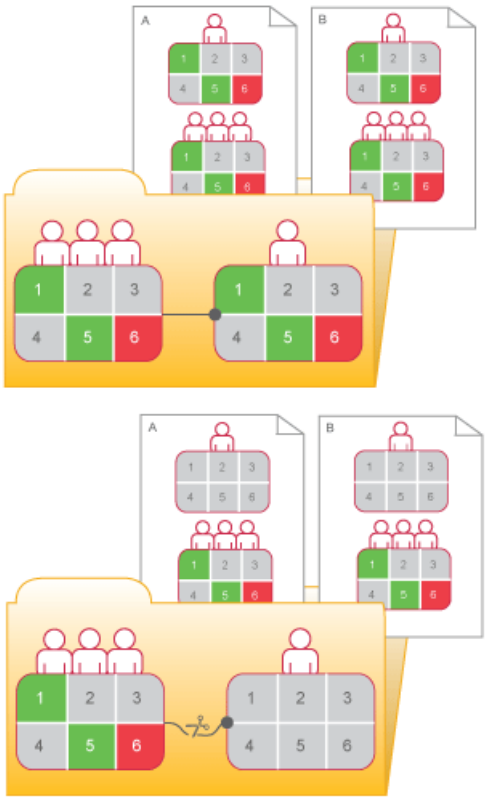


Figura 5 - 9: Interruzione dell'ereditarietà

5.4.1 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**.

5.5 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. Oppure 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 riassegni a gruppi diversi.

La tabella contenente i “diritti per amministratori delegati” contiene un riepilogo dei diritti necessari agli amministratori delegati per eseguire azioni comuni.

Tabella 5 - 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
Eliminazione di gruppi controllati nonché di singoli utenti di tali gruppi	Diritto di **eliminazione** sui relativi gruppi

Azione per amministratore autorizzato	Diritti richiesti dall'amministratore delegato
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.

5.5.1 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**. 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** 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**.

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** 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** 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 sicura** 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 **modi fica** 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. 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 garantisce questa limitazione, poiché gli amministratori delegati in genere non dispongono del diritto Modificare in modo sicuro i diritti 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.

5.5.2 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 quel 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.

5.6 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. Per ridurre la quantità di tempo necessaria per proteggere il contenuto aggiunto nella 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

6.1 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 Business Objects, 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.

6.2 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. Si consiglia vivamente di memorizzare la password per questa risorsa in un luogo sicuro e noto, dopo aver distribuito la piattaforma BI. Senza la password non sarà possibile rigenerare il file e si perderà quindi l'accesso al database di sistema.

6.3 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.
- 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.
- 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 BusinessObjectes Business Intelligence*.

Argomenti correlati

- Requisiti per la comunicazione tra i componenti della piattaforma BI
- Piattaforma BI e server proxy inverso
- Configurazione del protocollo SSL
- Limitazioni relative alle password
- Configurazione della protezione per server di terze parti in bundle

6.4 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 seguenti componenti in bundle:

- Microsoft SQL Server 2008 Express Edition: per informazioni dettagliate sulla protezione di questo database di sistema per le piattaforme Windows, vedere http://msdn.microsoft.com/en-us/library/bb283235%28v=sql.100%29.aspx.
- IBM DB2 Express: per informazioni dettagliate sulla protezione di questo database di sistema per le piattaforme UNIX, vedere http://publib.boulder.ibm.com/infocenter/db2luw/v9r7/index.jsp?nav=/2_ .
- Apache Tomcat 6.0: per informazioni dettagliate sulla protezione per questo server di applicazioni Web, vedere http://tomcat.apache.org/tomcat-6.0-doc/index.html.

6.5 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 con precisione 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.

6.5.1 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.

6.5.2 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.

6.6 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 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 della sessione.

6.6.1 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.

6.7 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. Quando si distribuisce la piattaforma BI, la protezione dell'ambiente viene divisa in due aree di comunicazione:

6.7.1 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 (Secure Sockets Layer) 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.

6.7.2 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 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.

6.8 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.

6.9 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.

6.9.1 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.

6.9.2 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.

6.9.3 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 (0,5–1,0 secondi) 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

6.9.4 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.

6.9.5 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.

6.10 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.

Suggerimento:

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.

6.11 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.

6.11.1 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 SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 4.0 non deve necessariamente utilizzare o interagire con strumenti client o applicazioni della piattaforma BI precedenti.
- 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.

6.11.1.1 Attivazione della modalità conforme a FIPS in Windows

Per impostazione predefinita, la modalità conforme a FIPS viene disattivata dopo l'installazione della piattaforma BI. Utilizzare le istruzioni riportate di seguito per attivare l'impostazione conforme a FIPS per tutti i nodi della distribuzione.

1. Per avviare CCM, accedere a **Programmi** > **SAP BusinessObjects Enterprise XI 4.0** > **SAP BusinessObjects Enterprise** > **Central Configuration Manager**.
2. In CCM, fare clic con il pulsante destro del mouse su Server Intelligence Agent (SIA) e scegliere **Arresta**.

   Avvertenza:
   non passare alla fase 3 prima che lo stato SIA venga contrassegnato come "Interrotto".

3. Fare clic con il pulsante destro del mouse su SIA e scegliere **Proprietà**.

   La finestra di dialogo "Proprietà" si apre con la scheda **Proprietà** visualizzata.
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.

6.11.1.2 Attivazione della modalità conforme a FIPS in UNIX

Tutti i nodi della distribuzione della piattaforma BI devono essere interrotti 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. Accedere alla directory in cui è installata la piattaforma BI sul computer UNIX.
2. Passare alla directory `sap_bobj`.
3. Digitare ccm.config e premere **Invio**.

   Il file `ccm.config` viene caricato.
4. Aggiungere -fips al parametro del comando di avvio del nodo.

   L'aspetto del parametro del comando di avvio del nodo è [*`nome nodo`*Launch].
5. Salvare le modifiche e **uscire**.
6. 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.

6.11.1.3 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**.

   La finestra di dialogo "Proprietà" si apre 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.

6.12 Crittografia nella piattaforma BI

Dati sensibili

Lo scopo della crittografia della piattaforma BI è proteggere i dati più importanti contenuti 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.

6.12.1 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 memorizzata in formato crittografato nel file `dbinfo`. In un'installazione Windows predefinita il file viene archiviato nella seguente directory: `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64`. Nei sistemi Unix il file viene archiviato nella directory della piattaforma in `<DIRINSTALL>/sap_bobj/enterprise_xi40/`.

Piattaforma Unix	Percorso
AIX	`<DIRINSTALL>/sap_bobj/enterprise_xi40/ aix_rs6000/`
Solaris	`<DIRINSTALL>/sap_bobj/enterprise_xi40/ solaris_sparc/`
Linux	`<DIRINSTALL>/sap_bobj/enterprise_xi40/ linux_x86/`
HP_UX	`<DIRINSTALL>/sap_bobj/enterprise_xi40/ hpux_pa-risc/`

Il nome del file è basato sulla seguente convenzione: `_boe_<nome_sia>.dbinfo`, in cui <nome_sia> corrisponde al nome del Server Intelligence Agent del cluster.

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 di otto caratteri per ogni nodo della distribuzione. Le nuove chiavi cluster vengono automaticamente utilizzate per il wrapping delle chiavi di crittografia presenti nel repository CMS.

6.12.1.1 Reimpostazione della chiave cluster in Windows

Prima di reimpostare la chiave cluster, assicurarsi che tutti i server gestiti dall'agente SIA risultino interrotti.

Utilizzare la procedura che segue per reimpostare la chiave cluster per il nodo.

1. Per avviare CCM, accedere a **Programmi** > **SAP BusinessObjects Enterprise XI 4.0** > **SAP BusinessObjects Enterprise** > **Central Configuration Manager**.
2. In CCM, fare clic con il pulsante destro del mouse su Server Intelligence Agent (SIA) e scegliere **Arresta**.

   Avvertenza:
   non passare alla fase 3 prima che lo stato SIA venga 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 database di sistema 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 nel campo "Nuova chiave cluster" e "Conferma nuova chiave cluster".

   Nota:
   Sulle piattaforme 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 correttamente reimpostata.

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.

6.12.1.2 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. Accedere alla directory in cui è installata la piattaforma BI sul computer UNIX.
2. Passare alla directory `sap bobj`.
3. Digitare cmsdbsetup.sh e premere **Invio**.

   Viene visualizzata la schermata di "configurazione del database CMS".

4. Digitare il nome del nodo e premere **Invio**.
5. Digitare 2 per modificare la chiave cluster.

   Viene visualizzato un messaggio di avviso.

6. Selezionare **Sì** per continuare.
7. 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.

8. 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.

9. Riavviare il nodo.

È necessario reimpostare tutti i nodi nella distribuzione della piattaforma BI per utilizzare la stessa chiave cluster.

6.12.2 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.

6.12.2.1 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:
È necessario essere un membro dei gruppi Amministratori e Responsabili crittografia per aggiungere un utente al 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 "Apri".
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'account utente che si desidera aggiungere al gruppo Responsabili crittografia dall'elenco **Gruppi/utenti disponibili** all'elenco **Utenti/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.

6.12.2.2 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 console CMC, selezionare **Programmi** > **SAP BusinessObjects XI 4.0** > **SAP BusinessObjects Enterprise** > **SAP BusinessObjects Enterprise Central Management Console**.

   Viene visualizzata la home page di 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

6.12.3 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	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

6.12.3.1 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.

6.12.3.2 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 aperta 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.

6.12.3.3 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 aperta la finestra di dialogo "Crea nuova chiave di crittografia" in cui è visualizzato un messaggio di avviso.

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.

6.12.3.4 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**.

   La finestra di dialogo "Contrassegna come compromessa" viene visualizzata con un messaggio di avviso.
4. Fare clic su **Continua**.
5. Selezionare una delle seguenti opzioni dalla finestra di dialogo "Contrassegna come compromessa":
   - **Sì**: 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

6.12.3.5 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 utilizzando le istruzioni seguenti.

1. Selezionare la chiave da revocare dall'elenco di chiavi dell'area di gestione "Chiavi di crittografia ".
2. Fare clic su **Azioni** > **Revoca chiave di crittografia**.

   Viene aperta la finestra di dialogo "Revoca chiave di crittografia" in cui è visualizzato un messaggio di avviso.
3. Fare clic su **OK** per revocare la chiave di crittografia.

   Viene avviato un processo per crittografare tutti gli oggetti della chiave in base alla chiave attiva corrente. Se le chiavi sono associate a più oggetti dati, verranno contrassegnate 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.

6.12.3.6 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 chiave di crittografia" con un messaggio di avviso.
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

6.13 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.

Nota:
se si utilizzano thick client, ad esempio Crystal Reports o Designer, sarà inoltre necessario configurare tali client per SSL se si prevede di utilizzarli per la connessione al CMS. 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.

6.13.1 Creazione di file di chiavi e certificati

Per impostare il protocollo SSL per la comunicazione del server, utilizzare lo strumento della 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 della riga di comando `sslconfig` per eseguire la configurazione.
- per ottenere la massima protezione, tutte le chiave 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.

6.13.1.1 Per creare file di chiavi e certificati per un computer

1. Eseguire lo strumento della riga di comando `SSLC.exe`.

   Lo strumento SSLC viene installato con il software della piattaforma BI. Ad esempio, in Windows viene installato per impostazione predefinita in `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\win64_x64`.

2. Eseguire il seguente comando:

   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, digitare il seguente comando:

   sslc rsa -in privkey.pem -out cakey.pem

   Questo comando consente la creazione della chiave decrittografata cakey.pem.

4. Per firmare il certificato CA, digitare il seguente comando:

   sslc x509 -in cacert.req -out cacert.pem -req -signkey cakey.pem -days 365

   Questo comando consente la creazione di 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`, archiviato nella stessa cartella dello strumento della riga di comando SSLC.

   Nota:
   L'utilizzo di un editor di testo è fortemente consigliato per Windows perché Windows Explorer potrebbe non riconoscere e visualizzare correttamente i file con estensione cnf.

6. Eseguire i seguenti passaggi in base alle impostazioni del file `sslc.cnf`.
   - 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

   - Creare il file con il nome specificato dall'impostazione `database` del file `sslc.cnf`.

     Nota:
     Per impostazione predefinita, il file è $dir/index.txt. Il file deve essere vuoto.

   - Creare il file con il nome specificato dall'impostazione `seriale` del file `sslc.cnf`.

     Verificare che questo file fornisca 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.

- Creare la directory specificata dall'impostazione `new_certs_dir` del file `sslc.cnf`.

7. Per creare una richiesta di certificato e una chiave privata digitare 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. Eseguire il seguente comando per decrittare la chiave nel file `privkey.pem`.

   ```
   sslc rsa -in privkey.pem -out server.key
   ```

9. Per firmare il certificato con il certificato CA, digitare 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:
    Il certificato CA (cacert.der) e la relativa chiave privata (cakey.pem) devono essere generati una sola volta nella distribuzione in rete. Tutti i computer nella stessa distribuzione devono condividere 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 chiave e certificati in una posizione sicura, nella stessa directory `(d:/ssl)`) accessibile dai computer presenti nella distribuzione della piattaforma BI:
    - il file del certificato sicuro (cacert.der)
    - il file di certificato del server generato (servercert.der)
    - il file della chiave del server (server.key)
    - il file passphrase

    Questa posizione sarà utilizzata per configurare il protocollo SSL per il CCM e il server delle applicazioni Web.

6.13.2 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.

6.13.2.1 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. Assicurarsi che l'opzione **Abilita SSL** sia selezionata
4. . Fornire il percorso di file della 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 certificati SSL richiesti con i relativi file. Ad esempio:d:\ssl
File di certificato SSL server	Nome del file utilizzato per archiviare il certificato SSL del server. Per impostazione predefinita,servercert.der
File dei certificati SSL attendibili	Nome del file con il certificato SSL attendibile. Per impostazione predefinita, cacert.der
File chiave privata SSL	Nome del file della chiave privata SSL utilizzata per accedere al certificato. Per impostazione predefinita, server.key
File della passphrase della chiave privata	Nome del file di testo contenente la password lunga per l'accesso alla chiave privata. Per impostazione predefinita, passphrase.txt

Nota:
Verificare di indicare la directory per il computer sul quale è in esecuzione il server.

6.13.2.2 Configurazione del protocollo SSL su 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 Server Intelligence Agent** e premere **Invio**.
4. Specificare il SIA di destinazione e premere **Invio**.
5. Selezionare l'opzione **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.

6.13.2.3 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
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.

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.

6.13.2.4 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 della 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 `<INSTALLDIR>\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

6.13.2.4.1 Configurazione dell'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.

6.13.2.4.2 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" -Xmx512m -Xss10m -jar "%SHAREDIR%\lib\migration.jar"
```

4. Aggiungere la sintassi seguente al parametro -Xss10m:

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir=C:/ssl
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
-Dbusinessobjects.migration
```

Nota:
verificare che tra ogni parametro sia presente uno spazio.

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

6.14 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

6.14.1 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.

6.14.1.1 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 un numero di porta specifico per i server che comunicano con altri componenti della piattaforma BI attraverso un firewall.

6.14.1.2 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.

6.14.1.3 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.

6.14.1.4 Central Management Server (CMS) fornisce una directory 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 di 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 dispone di più nomi host, viene scelto quello primario. È possibile configurare un server affinché il relativo riferimento contenga l'indirizzo IP.

Argomenti correlati

- Comunicazione tra componenti della piattaforma BI

6.14.1.5 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.

6.14.1.6 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 da cui il Job Server può eseguire la selezione aggiungendo i parametri `-requestJSChildPorts<porta più bassa>-<porta più alta>` e `-requestPort<porta>` 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

6.14.2 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.

6.14.2.1 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 sistema CMS 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 Central Management Server (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 <intervallo porta>`. 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

6.14.2.2 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.

6.14.2.2.1 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	Applicazione client	Server associati	Requisiti di porta del server
Crystal Reports	Designer di SAP Crystal Reports 2011	CMS Input FRS Output FRS Crystal Reports 2011 Report Application Server (RAS) Crystal Reports 2011 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 richiesta del Report Application Server di Crystal Reports 2011 Porta richiesta server di elaborazione Crystal Reports Porta richiesta Crystal Reports Cache Server

Prodotto	Applicazione client	Server associati	Requisiti di porta del server
Crystal Reports	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
Dashboard Design	SAP BusinessObjects Dashboard Design	CMS Input FRS Output FRS Applicazione del provider di Servizi Web (`dsws bobje.war`) che ospita i servizi Web Dashboard Design, 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 predefinita)
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 predefinita)
Piattaforma BI	SAP BusinessObjects Web Intelligence Desktop	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 Mana-ger	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)	È necessario che le seguenti porte siano aperte per consentire a CCM di gestire i server remoti della piattaforma BI: Porta server dei nomi CMS (6400 per impostazione predefinita) Porta richiesta CMS È necessario che le seguenti porte siano aperte per consentire a CCM di gestire i processi SIA remoti: Microsoft Directory Services (porta TCP 445) NetBIOS Session Service (porta TCP 139) NetBIOS Datagram Service (porta UDP 138) NetBIOS Name Service (porta UDP 137) DNS (porta TCP/UDP 53) (Si noti che alcune porte elencate in precedenza potrebbero non essere necessarie. Consultare l'amministratore di Windows).
Piattaforma BI	Server Intelli-gence Agent (SIA)	Ogni server della piattaforma BI incluso il CMS	Porta richiesta SIA (6410 per imposta-zione predefinita) Porta server dei nomi CMS (6400 per impostazione predefinita) Porta richiesta CMS

Prodotto	Applicazione 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 Servizio di elaborazione Crystal Reports 2011 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, Porta richiesta Servizio di elaborazione Crystal Reports 2011.
Piattaforma BI	Provider di Servizi Web (`dsws bobje.war`)	Tutti i server della piattaforma BI richiesti dai prodotti che accedono ai servizi Web. La comunicazione con le porte di richiesta del server di elaborazione e la cache di Dashboard Design è necessaria se SAP BusinessObjects Dashboard Design 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 Dashboard Design e Porte richiesta Server di elaborazione Dashboard Design.

Prodotto	Applicazione 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

6.14.2.2.2 Requisiti di porta per le applicazioni di terze parti

In questa tabella sono elencati i programmi software di terze parti utilizzati dai prodotti SAP Business Objects. 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 Business Objects 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 Business Objects 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 di SAP Business Objects, 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.

6.15 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.

6.15.1 Per configurare il sistema per i firewall

1. Determinare quali componenti della piattaforma BI devono comunicare attraverso un firewall.
2. Configurare 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 in 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
- Specifica delle regole del firewall
- Configurazione del file HOSTS per i firewall che utilizzano NAT

6.15.1.1 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. Può 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** del server. Tenere presente che ogni server su un computer deve utilizzare un numero di porta univoco. Alcuni server 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** della pagina di configurazione 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

6.15.1.2 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.

6.15.1.2.1 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 `\WINNT\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`.

6.15.1.2.2 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`.

6.15.2 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
```

6.15.2.1 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

6.16 Esempi di scenari di firewall tipici

In questa sezione vengono forniti esempi di scenari di distribuzione di firewall tipici

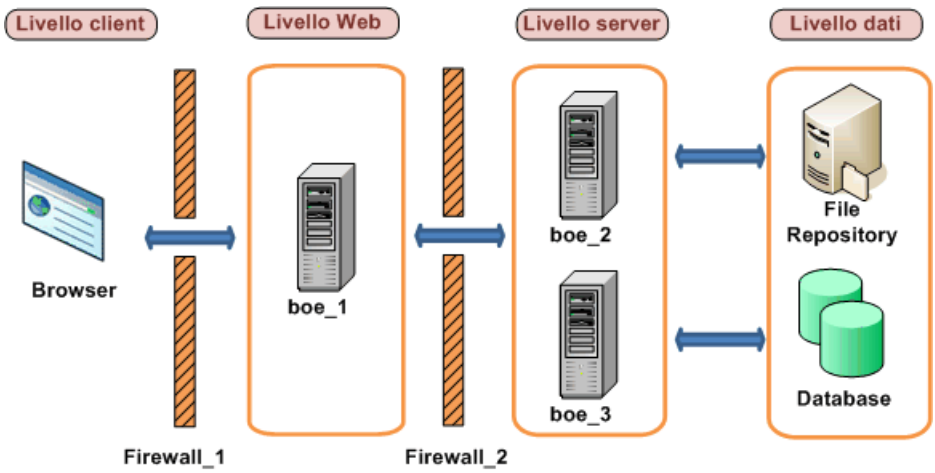
6.16.1 Esempio: livello applicazione distribuito su una rete separata

Questo esempio illustra 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 dagli 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, Web Intelligence Processing Server, Report Application Server, Crystal Reports Cache Server e Crystal Reports Processing Server.

Figura 6 - 1: Livello applicazione distribuito su una rete separata



6.16.1.1 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
Web Intelligence Processing Server	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 6 - 6: Configurazione per Firewall_1

Porta	Computer di destinazione	Porta	Azione
Qualsiasi	boe_1	8080	Consenti

   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

6.16.2 Esempio: livello thick client e database separato dai server della piattaforma BI mediante un firewall

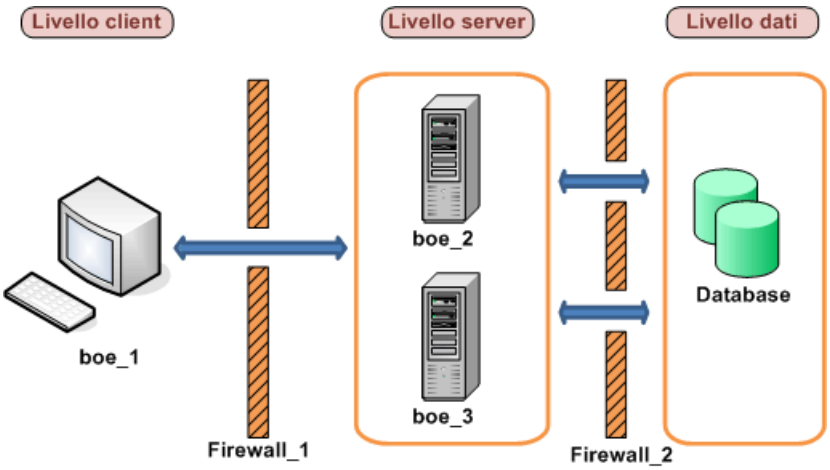
In questo esempio viene illustrato come configurare un firewall e la piattaforma BI in modo da utilizzarli insieme in una distribuzione in cui:

- 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, Web Intelligence Processing Server, 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. La porta di attesa del server di database è la 3306, ovvero la porta di attesa predefinita per il server MySQL.

Figura 6 - 2: Livello Rich Client e database distribuito su reti separate



6.16.2.1 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

6.17 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
• 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

6.17.1 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.
- Crystal Reports Job Server e il server di elaborazione Crystal Reports (insieme ai componenti di Accesso dati) devono poter 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

6.17.1.1 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

6.17.2 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.

6.17.2.1 Requisiti di porta per i server della piattaforma BI

Prodotto	Requisiti di porta del server
Piattaforma SAP BusinessObjects Business Intelligence	• Porta del server Sign On della piattaforma BI

6.17.2.2 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.

6.17.2.3 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 dagli 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 6 - 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

Computer di origine	Porta	Computer di destinazione	Porta	Azione
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

6.17.3 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 sopraccitati deve essere 1521.

6.17.3.1 Requisiti delle porte in dettaglio

Oltre alla configurazione del firewall standard per la piattaforma BI, potrebbe essere necessario aprire alcune porte supplementari per funzionare 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

Computer di origine	Porta	Computer di destinazione	Porta	Azione
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

6.17.4 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.

6.17.4.1 Requisiti di porta per i server della piattaforma BI

Prodotto	Requisiti di porta del server
Piattaforma SAP BusinessObjects Business Intelligence	• Porta del server Sign On della piattaforma BI

6.17.4.2 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

6.17.4.3 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 dagli 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 BusinessObjects Business Intelligence*.

Oltre alla configurazione firewall con la piattaforma BI, è necessario eseguire alcune operazioni di configurazione supplementari.

Tabella 6 - 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
Server della piattaforma BI con funzione Connettività dati per PeopleSoft	Qualsiasi	PeopleSoft	Porta HTTP/HTTPS servizio Web PeopleSoft	Consenti

Computer di origine	Porta	Computer di destinazione	Porta	Azione
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

6.17.5 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.

- Il server di applicazioni 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 6 - 19: Requisiti di porta per i server della piattaforma BI

Prodotto	Requisiti di porta del server
Piattaforma SAP BusinessObjects Business Intelligence	• Porta del server Sign On della piattaforma BI

Tabella 6 - 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 un 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 dagli 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	Consenti
CMS	Qualsiasi	Server Sign On della piattaforma BI per Siebel	Qualsiasi	Consenti
Server Sign On della piattaforma BI per Siebel	Qualsiasi	Siebel	Porta SCBroker	Consenti
Server della piattaforma BI con funzione Connettività dati lato server per Siebel	Qualsiasi	Siebel	Porta SCBroker	Consenti
Crystal Reports con funzione Connettività dati lato client per Siebel	Qualsiasi	Siebel	Porta SCBroker	Consenti

6.18 Piattaforma BI e server proxy inverso

È possibile distribuire la piattaforma BI in un ambiente con uno o più server proxy inverso. 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.

6.18.1 Server reverse proxy supportati

La piattaforma BI supporta i seguenti server proxy inverso:

- IBM Tivoli Access Manager WebSEAL 6
- Apache 2.2
- Microsoft ISA 2006

6.18.2 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 due file WAR specifici:

- **BOE**: include la console CMC, BI Launch Pad, Open Document,
- **dswsbobje**: contiene l'applicazione Servizio 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.

6.19 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.

6.19.1 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 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 include proprietà globali e specifiche dell'applicazione. Se è necessario modificare una delle 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`.

Non modificare le proprietà presenti nella directory config\default.

Nota:
in alcuni server di applicazioni Web, come la versione Tomcat inclusa nella piattaforma BI, è possibile accedere al file BOE.war direttamente. In scenari del genere è possibile definire le impostazioni personalizzate direttamente senza annullare la distribuzione del file WAR. Quando non è possibile accedere al file BOE.war, è necessario annullare la distribuzione, eseguire la personalizzazione e quindi ridistribuire il file.

Uso coerente del carattere '/'

Definire i percorsi di contesto nel server proxy inverso così come vengono immessi in un URL del browser. Se ad esempio la direttiva contiene '/' alla fine del percorso mirror sul server proxy inverso, immettere '/' 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.

6.19.2 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.

6.19.3 Configurazione del 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.

6.19.4 Configurazione del 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 utente **sec_master** con autorizzazione di amministrazione.
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
```

6.19.5 Configurazione di 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 reti

      ISA 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.

6.20 Configurazione speciale per la piattaforma BI in distribuzioni di proxy inverso

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.

6.20.1 Abilitazione del proxy inverso per Servizi Web

In questa sezione vengono descritte le procedure richieste per abilitare i proxy inversi per i Servizi Web.

6.20.1.1 Abilitazione del proxy inverso in Tomcat 6

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, `server.xml` si trova in `C:\Programmi (x86)\SAP BusinessObjects\Tomcat6\conf`

   In UNIX `server.xml` si trova in `<CATALINA_HOME>/conf`. Il valore predefinito di `<HOME_CATALINA>` è `<INSTALLDIR>/bobje/tomcat55`.

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.com`e `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 Business Objects 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.

6.20.1.2 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`
   - `wsresource1=BICatalog|bicatalog web service alone|http://server_proxy_inverso.dominio.com/SAP/dswsbobje/services/BICatatog`
   - `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.

6.20.2 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.

6.20.2.1 Configurazione di Apache Tomcat 6

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.

6.20.2.2 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.

6.20.2.3 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.

6.20.2.4 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.

6.20.3 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.

6.20.3.1 Per modificare l'URL del visualizzatore predefinito tramite la CMC

1. Accedere alla CMC.
2. Accedere alla pagina Applicazioni e fare clic su **CMC**.
3. Selezionare **Estensioni di elaborazione** dal menu **Azioni**.

4. Nel campo URL, impostare l'URL corretto del visualizzatore predefinito e fare clic su **Imposta URL**. Ad esempio:

   ```
   http://ReverseProxyServer:ReverseProxyServerPort/BOE/OpenDocument.jsp?sIDType=CUID&iDocID=%SI_CUID%
   ```

   Dove `ReverseProxyServer` e `ReverseProxyServerPort` rappresentano il nome del server reverse proxy corretto e la relativa porta di attesa.

Autenticazione

7.1 Opzioni di autenticazione disponibili nella piattaforma BI

L'autenticazione è il processo di verifica dell'identità di un utente che tenti di accedere al sistema, mentre l'autorizzazione è il processo di verifica che l'utente disponga 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

- Abilitazione dell'autenticazione JD Edwards EnterpriseOne
- Abilitazione dell'autenticazione Oracle EBS
- Abilitazione dell'autenticazione PeopleSoft Enterprise
- Abilitazione dell'autenticazione Siebel

7.1.1 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 metodi di autenticazione, 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.

7.1.2 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 questi 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 eseguono una selezione tra i tipi di autenticazione abilitati e impostati nell'area di gestione Autorizzazione 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.

7.1.3 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 eseguire SSO, in modo da attestare l'identità dell'utente che accede al sistema.

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.

7.1.3.1 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 utente una sola volta, in modo da semplificare l’interazione degli utenti con il sistema.

Il Single Sign On a BI Launch Pad può essere assicurato 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 su Windows o Unix, con qualsiasi server di applicazioni Web supportato per la piattaforma.

- LDAP con SiteMinder
- Autenticazione affidabile
- Windows AD con Kerberos

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. SSO a InfoView e alla console CMC richiede SiteMinder.
Enterprise	Qualsiasi piattaforma supportata	Autenticazione affidabile	L'autenticazione Enterprise a BI Launch Pad e alla console CMC è disponibile direttamente. SSO con l'autenticazione Enterprise a InfoView e alla console CMC richiede l'autenticazione affidabile.

- Single Sign On alla piattaforma BI
- Single Sign-On al database
- Single Sign-On end-to-end

7.1.3.2 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.

7.1.3.3 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.

7.2 autenticazione Enterprise

7.2.1 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 BI 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. L'impostazione di Enterprise può essere modificata solo attraverso la console CMC (Central Management Console).

7.2.2 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.
	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.
Restrizioni utente		
	La password deve essere modificata 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.
	Attendi 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		
	Disabilita 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 tentativi di accesso non riusciti dopo N minuti	Questa opzione specifica un intervallo di tempo per la reimpostazione del contatore dei tentativi di accesso.
	Riabilita account dopo N minuti	Questa opzione specifica per quanto tempo viene sospeso un account dopo N tentativi di accesso non riusciti.

Impostazioni	Opzioni	Descrizione
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		Specifica le impostazioni per la configurazione dell'Autenticazione affidabile.

Argomenti correlati

- Abilitazione dell'Autenticazione affidabile

7.2.3 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.

7.2.3.1 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 tabella seguente identifica i valori minimo e massimo per ogni impostazione correlata alla password che è possibile configurare.

Tabella 7 - 1: 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**.

7.2.4 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

7.2.4.1 Per configurare il server per l'uso dell'Autenticazione affidabile:

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.

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. Scorrere verso il basso fino a visualizzare "Autenticazione affidabile".
   a. Fare clic su **Autenticazione affidabile attivata**.
   b. Fare clic su **Nuova chiave privata condivisa**.

      Viene visualizzato il seguente messaggio:
      `Una chiave privata condivisa è stata generata ed è pronta per il download`
   c. Fare clic su **Scarica chiave privata condivisa**.

Nota:
Il segreto condiviso viene utilizzato dal client e dal server CMS per stabilire una connessione affidabile. È inoltre necessario configurare il client dopo avere completato la configurazione di Autenticazione affidabile per il server.

Viene visualizzata la finestra di dialogo "Download dei file".

d. Fare clic su "Salva" e accedere alla directory seguente per salvare il file `TrustedPrincipal.conf`:

<DIRINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\

e. Per specificare il numero di giorni di validità del segreto condiviso, specificare un valore nel campo "Periodo validità segreto condiviso".

f. Specificare un valore di timeout per le richieste di autenticazione affidabile.

Nota:
il valore di timeout è la differenza massima consentita, espressa in millesimi di secondo, tra il tempo dell'orologio del client e quello dell'orologio del CMS. Se si immette 0, la differenza tra i due valori di tempo indicati dagli orologi è illimitata. Si sconsiglia di importare questo valore su 0 per evitare di aumentare la vulnerabilità verso gli attacchi che utilizzano le risposte.

5. Fare clic su **Aggiorna** per salvare il segreto condiviso.

Nota:
tutte le modifiche apportate ai parametri dell'Autenticazione affidabile non vengono controllate dalla piattaforma BI. È consigliabile eseguire manualmente il backup di tutte le informazioni relative all'Autenticazione affidabile.

Il segreto condiviso viene utilizzato dal client e dal server CMS per stabilire una connessione affidabile. È inoltre necessario configurare il client dopo avere completato la configurazione dell'Autenticazione affidabile per il server.

7.2.5 Configurazione dell'Autenticazione affidabile per l'applicazione Web

Per configurare l'Autenticazione affidabile per il client, è necessario accedere alle proprietà globali per il file war BOE e alle proprietà specifiche delle applicazioni BI Launch Pad e OpenDocument e modificarle.

È possibile utilizzare uno dei due metodi per passare il segreto condiviso al client:

- Sessione Web
- File `TrustedPrincipal.conf`

Oltre al segreto condiviso, è necessario scegliere uno dei metodi seguenti per passare il nome utente al client:

- Sessione Web
- Biscotti
- Intestazione HTTP
- Query URL

Qualsiasi metodo si scelga, deve essere personalizzato nelle proprietà globali `Trusted.auth.user.retrieval` per il file war BOE.

7.2.5.1 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 di 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.

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:
gli utenti devono essere importati nella piattaforma BI o avere 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`.

7.2.5.2 Proprietà di Autenticazione affidabile per le applicazioni Web

Nella tabella che segue sono elencate le impostazioni di Autenticazione affidabile 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`.

Proprietà	Valore predefinito	Descrizione
`sso.enabled=true`	`sso.enabled=false`	Abilita e disabilita il Single Sign On (SSO) per la piattaforma BI. Per abilitare Autenticazione affidabile, questa proprietà deve essere impostata su `true`.
`trusted.auth.shared.secret`	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.
`trusted.auth.user.param`	Nessuno	Specifica la variabile utilizzata per recuperare il nome utente per Autenticazione affidabile.
`trusted.auth.user.retrieval`	Nessuno	Specifica il metodo utilizzato per recuperare il nome utente per Autenticazione affidabile. Può essere impostato su uno dei valori seguenti: • `"REMOTE_USER"` • `"HTTP_HEADER"` • `"COOKIE"` • `"QUERY_STRING"` • `"WEB_SESSION"` • `"USER_PRINCIPAL"` Impostare su empty per disabilitare Autenticazione affidabile.
`trusted.auth.user.namespace.enabled`	`trusted.auth.user.namespace.enabled=false`	Abilita e disabilita il collegamento dinamico degli alias ad account utente esistenti. Se la proprietà è impostata su `true`, 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 affinché fornisca il Single Sign On SAML al sistema. Se la proprietà è impostata su `false`, Autenticazione affidabile utilizza la corrispondenza dei nomi durante l'autenticazione degli utenti.

7.2.5.3 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	`<DIRINSTALL>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\`
AIX	`<DIRINSTALL>/sap_bobj/enterprise_xi40/aix_rs6000/`
Solaris	`<DIRINSTALL>/sap_bobj/enterprise_xi40/solaris_sparc/`
HP_UX	`<DIRINSTALL>/sap_bobj/enterprise_xi40/hpux_pa-risc/`
Linux	`<DIRINSTALL>/sap_bobj/enterprise_xi40/linux_x86`

esistono vari meccanismi che consentono di popolare la variabile del nome utente utilizzata per configurare Autenticazione affidabile 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 descritti in questa sede. 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 alle proprietà del file BOE.war e modificarle. Il file BOE.war include 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 per il file BOE.war nel computer che ospita le applicazioni Web.

   Se si utilizza il server di applicazioni Web Tomcat fornito con l'installazione della piattaforma BI, è possibile accedere direttamente alla directory seguente.

   ```
   C:\Programmi (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom\
   ```

   Suggerimento:
   se si utilizza un server di applicazioni Web che non consente l'accesso diretto alle applicazioni Web distribuite, è possibile utilizzare la cartella seguente nell'installazione del prodotto per modificare il file BOE.war.

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

   Sarà necessario ridistribuire successivamente il file BOE.war modificato.

2. Creare un nuovo file.

Nota:
utilizzare Blocco note o un'altra utilità per la modifica del testo.

3. Specificare le proprietà dell'autenticazione affidabile immettendo quanto segue:

```
sso.enabled=true
trusted.auth.user.retrieval=Method for user ID retrieval
trusted.auth.user.param=Variable
trusted.auth.shared.secret=WEB_SESSION
```

Le opzioni per il recupero del nome utente sono elencate nella tabella seguente:

Opzione	Metodo di recupero del nome utente
`HTTP_HEADER`	Il nome utente viene recuperato dai contenuti di un'intestazione HTTP specificata. È necessario specificare l'intestazione HTTP da utilizzare nella proprietà `trusted.auth.user.param`.
`QUERY_STRING`	Il nome utente viene recuperato dal parametro specificato dell'URL di richiesta. È necessario specificare la stringa di query da utilizzare nella proprietà `trusted.auth.user.param`.
`COOKIE`	Il nome utente viene recuperato da un cookie specificato. È necessario specificare il cookie da utilizzare nella proprietà `trusted.auth.user.param`.
`WEB_SESSION`	Il nome utente viene recuperato dai contenuti di una variabile di sessione specificata. È necessario specificare la variabile della sessione Web da utilizzare in `trusted.auth.user.param` nel file `global.properties`.
`USER_PRINCIPAL`	Il nome utente viene recuperato da una chiamata a `getUserPrincipal().getName()` sull'oggetto `HttpServletRequest` per la richiesta corrente in un servlet o JSP.

Nota:

- Alcuni server di applicazioni Web richiedono l'impostazione della variabile di ambiente REMOTE_USER su true sul server di applicazioni Web. Per ulteriori informazioni sui requisiti, consultare la documentazione specifica del server di applicazioni Web in uso. Se necessario, verificare che la variabile di ambiente sia impostata su true se si utilizza questo metodo di recupero del nome utente.

- se si utilizza `USER_PRINCIPAL` per passare il nome utente, lasciare il valore `trusted.auth.user.param` vuoto.

4. Salvare il file con questo nome:

   proprietà globali

5. Riavviare il server di applicazioni Web.

Le nuove proprietà hanno 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 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*.

7.2.5.3.1 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 *`JohnDoe`*.

Le informazioni sull'utente verranno memorizzate e passate attraverso la sessione Web, mentre il segreto condiviso verrà passato attraverso il file `TrustedPrincipal.conf`. Si presuppone che il file si trovi nella directory seguente: `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` . La versione in bundle di Tomcat 6 è il server di applicazioni Web.

1. Accedere alla directory seguente:

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

2. Creare un nuovo file.

   Nota:
   utilizzare Blocco note o un'altra utilità per la modifica del testo.

3. Specificare le proprietà dell'autenticazione affidabile immettendo quanto segue:

```
sso.enabled=truetrue
trusted.auth.user.retrieval=WEB_SESSION
trusted.auth.user.param=MyUser
trusted.auth.shared.secret=
```

4. Salvare il file con questo nome:

   proprietà globali

5. Accedere al file seguente:

   `C:\Programmi (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.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("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\Tomcat6\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. Chiudere Tomcat.
10. Eliminare la cartella di lavoro nella directory seguente:

    `C:\Programmi (x86)\ SAP BusinessObjects\Tomcat6`

11. Riavviare Tomcat.

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 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 *`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:

```
9ecb0778edcff048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc65773
841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

La versione in bundle di Tomcat 6 è il server di applicazioni Web.

1. Accedere alla directory seguente:

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

2. Creare un nuovo file.

Nota:
utilizzare Blocco note o un'altra utilità per la modifica del testo.

3. Specificare le proprietà dell'autenticazione affidabile immettendo quanto segue:

```
sso.enabled=truetrue
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\Tomcat6\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.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","9ecb0778edcff048edae0fcdde1a5db82112934
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\Tomcat6\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. Chiudere Tomcat.
10. Eliminare la cartella di lavoro nella directory seguente:
    `C:\Programmi (x86)\ SAP BusinessObjects\Tomcat6`
11. Riavviare Tomcat.

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 `JohnDoe`.

Le informazioni sull'utente verranno memorizzate e passate attraverso l'opzione Utente principale, mentre il segreto condiviso verrà passato attraverso il file `TrustedPrincipal.conf`. Si presuppone che il file si trovi nella directory seguente: `C:\Programmi (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86` . La versione in bundle di Tomcat 6 è il server di applicazioni Web.

1. Arrestare il server Tomcat.
2. Aprire il file server.xml per Tomcat.

   Il file è disponibile per impostazione predefinita nella directory seguente:

   `C:\Programmi (x86)\ SAP BusinessObjects\Tomcat6\conf\.`

3. Impostare il valore di Realm className= su:

   `Realm className="org.apache.catalina.realm.MemoryRealm "`

4. Aprire il file tomcat-users.xml.

   Per impostazione predefinita, il file si trova nel percorso:

   `C:\Programmi (x86)\ SAP BusinessObjects\Tomcat6\conf\.`

5. Individuare il tag `<utenti-tomcat>` e modificare quanto segue:

```
<user name="JohnDoe" password="password"
roles="onjavauser"/>
```

6. Aprire il file web.xml nella directory seguente:

   `C:\Programmi (x86)\ SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\`

7. Aggiungere quanto segue prima del tag `</web-app>`:

```
<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>
```

   Nota:
   è necessario specificare 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. Eliminare la cartella di lavoro nella directory seguente:

   `C:\Programmi (x86)\ SAP BusinessObjects\Tomcat6`

9. Riavviare Tomcat.

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`, dove *[nomecms]* è il nome del computer che ospita il server CMS. Dopo qualche minuto viene visualizzata una finestra di dialogo di accesso.

7.3 Autenticazione LDAP

7.3.1 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 ai relativi elenchi è possibile per qualsiasi client che disponga dell'autorizzazione appropriata. LDAP consente di impostare l'accesso degli utenti

alla piattaforma BI tramite l'autenticazione LDAP. Inoltre, consente agli utenti di essere autorizzati quando tentano di accedere agli 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, viene generato un certificato di protezione del server LDAP che la piattaforma BI utilizza per verificare se il server è attendibile, benché il server LDAP consenta connessioni da client anonimi. Con l'autenticazione reciproca, sono disponibili certificati di protezione sia per il server LDAP che per la piattaforma BI e il server LDAP deve anche verificare il certificato client prima che possa essere stabilita una connessione.

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, occorre conoscere a fondo le differenze tra questi tipi di LDAP. Per ulteriori dettagli, vedere la RFC2251, attualmente disponibile all'indirizzo http://www.faqs.org/rfcs/rfc2251.html.

Argomenti correlati

- Configurazione dell'autenticazione LDAP
- Mappatura di gruppi LDAP

7.3.1.1 Plug-in di protezione LDAP

Il plug-in di protezione LDAP consente di mappare account utente e di gruppo dal server di directory LDAP nella 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 impostare l'autenticazione, l'autorizzazione 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

7.3.2 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.

7.3.2.1 Per configurare l'host LDAP

È consigliabile installare ed eseguire il server LDAP prima di configurare l'host LDAP.

1. Accedere all'area di gestione **Autenticazione** della console CMC, quindi fare doppio clic su **LDAP**.

Nota:
Per accedere all'area di gestione **Autenticazione**, scegliere **Autenticazione** dall'elenco di spostamento.

2. 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 **OK**.

   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**.

3. Selezionare il tipo di server dall'elenco **Tipo di server LDAP**.

   Nota:
   Se si mappa LDAP a AD, selezionare Microsoft Active Directory Application Server per il tipo di server.

4. Se si desidera visualizzare o modificare una mappatura di attributi del server LDAP o gli attributi di ricerca predefiniti LDAP, fare clic su **Mostra mappature attributi**.

   Per impostazione predefinita, le mappature di attributi di server e gli attributi di ricerca di ciascun tipo di server supportato sono già impostate.

5. Fare clic su **Avanti**.
6. Nel campo **Nome distinto LDAP di base** digitare il nome distinto, ad esempio o=SomeBase, per il server LDAP, quindi fare clic su **Avanti**.
7. Nell'area delle credenziali del server LDAP specificare il nome e la password per un account utente che dispone dell'accesso in lettura alla directory.

   Nota:
   Le credenziali di amministratore non sono necessarie.

   Nota:
   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.

8. Se sono stati configurati riferimenti all'host LDAP, immettere le informazioni di autenticazione nell'area **Credenziali di riferimento LDAP** e immettere il numero di hop di riferimento nel campo **Numero massimo di hop di riferimento**.

   Nota:
   L'area "Credenziali di riferimento LDAP" deve essere configurata se sono valide tutte le seguenti condizioni:

   - 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.

9. Fare clic su **Avanti**.
10. Scegliere il tipo di autenticazione SSL (Secure Sockets Layer) utilizzato e fare clic su **Avanti**.

    Le opzioni disponibili sono:

    - Base (senza SSL)
    - Autenticazione server
    - Autenticazione reciproca

11. Scegliere un metodo di autenticazione Single Sign On LDAP, quindi fare clic su **Avanti**.

    Le opzioni disponibili sono:

    - Base (senza SSO)
    - SiteMinder

12. Selezionare il modo in cui alias e utenti vengono mappati agli account della piattaforma BI.
    a. In "Nuove opzioni alias" selezionare in che modo i nuovi alias vengono mappati agli account Enterprise. Selezionare una delle opzioni seguenti:
       - **Assegna ciascun alias LDAP aggiunto a un account con lo stesso nome**

         Utilizzare questa opzione quando si sa che gli utenti possiedono un account Enterprise già esistente con lo stesso nome; di conseguenza gli alias LDAP 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 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 in che modo gestire gli aggiornamenti degli alias per gli account Enterprise. Selezionare una delle opzioni seguenti:
       - **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. In "Nuove opzioni utente" specificare la modalità di creazione dei nuovi utenti.

Se la licenza della piattaforma SAP BusinessObjects Business Intelligence di cui si dispone si basa sui ruoli utente, selezionare una delle seguenti "Nuove opzioni utente":

- **Visualizzatore BI**

  I nuovi account utente vengono configurati con il ruolo Visualizzatore BI. L'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Visualizzatore BI è definito nel contratto di licenza. Gli utenti potranno accedere ai workflow delle applicazioni in base a quanto previsto dal ruolo Visualizzatore BI. I diritti di accesso generalmente sono limitati alla visualizzazione dei documenti business intelligence. Questo ruolo è di norma adatto agli utenti che utilizzano contenuti mediante le applicazioni della piattaforma BI.

- **Analista BI** I nuovi account utente vengono configurati con il ruolo Analista BI. L'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Analista BI è definito nel contratto di licenza. Gli utenti possono accedere a tutti i workflow delle applicazioni definiti per il ruolo Analista BI. I diritti di accesso includono la visualizzazione e la modifica dei documenti business intelligence. Questo ruolo è adatto agli utenti che creano e modificano contenuti per le applicazioni della piattaforma BI.

Se la licenza della piattaforma SAP BusinessObjects Business Intelligence di cui si dispone non si basa sui ruoli utente, selezionare una delle opzioni seguenti:

- **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 con accesso simultaneo specificano quanti utenti possono connettersi contemporaneamente alla piattaforma SAP BusinessObjects Business Intelligence. 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.

13. Nell'area "Opzioni di collegamento attributi" è possibile specificare la priorità di collegamento degli attributi per il plug-in LDPA:

a. Fare clic sulla casella **Importa nome completo e indirizzo di posta elettronica**.

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 è impostata su "3", avranno la priorità gli attributi di altri plug-in abilitati.

14. 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
- Licenze basate sul ruolo

7.3.2.2 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

7.3.2.3 Configurazione delle impostazioni SSL per l'autenticazione del server LDAP o reciproca

Questa sezione contiene le informazioni relative alla CMC per la configurazione di SSL con l'autenticazione server o reciproca LDAP. In questa sezione si presuppone che sia stato configurato l'host LDAP e che sia stata selezionata una delle seguenti opzioni di autenticazione SSL:

- Autenticazione server

- Autenticazione reciproca

Per informazioni aggiuntive sulla configurazione del server host LDAP, consultare la documentazione del fornitore LDAP.

Argomenti correlati

- Per configurare l'host LDAP

7.3.2.3.1 Configurazione dell'autenticazione del server LDAP o reciproca

Risorsa	Prerequisiti
Certificato CA	È necessario disporre di un'autorità di certificazione per generare un certificato CA da aggiungere al server LDAP. Per ulteriori informazioni, consultare la documentazione del fornitore LDAP. Questo prerequisito riguarda sia l'autenticazione reciproca che server con SSL.
Certificato server	È necessario richiedere e generare un certificato server. Il certificato deve essere autorizzato prima di poter essere aggiunto al server LDAP. Questo prerequisito riguarda sia l'autenticazione reciproca che server con SSL.

cert7.db key3.db	È necessario accedere all'applicazione certutil in grado di generare un file cert7.db. È possibile scaricare l'applicazione accedendo all'URL seguente: ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_6_RTM/ . Copiare il certificato CA nella stessa directory di certutil. Generare i file `cert7.dbkey3.db` e `secmod.db` utilizzando il comando seguente:
	`certutil -N -d .`
	Aggiungere il certificato CA al file `cert7.db` utilizzando il comando seguente:
	`certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer`
	Archiviare i tre file in una directory nota del computer che ospita la piattaforma SAP BusinessObjects Business Intelligence. I file sono necessari sia per l'autenticazione reciproca che server con SSL.

cacerts	Questo file è necessario solo per l'autenticazione reciproca o server con SSL per applicazioni Java quale BI Launch Pad. Accedere al file keytool nella directory bin di Java. Utilizzare il comando seguente per creare il file cacerts: `keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore` Archiviare il file cacerts nella stessa directory dei file `cert7.db` e `key3.db`.
Certificato client	

Risorsa	Prerequisiti

	È necessario creare richieste client separate per i file `cert7.db` e `.keystore`. Per configurare il plug-in LDAP, è necessario generare una richiesta di certificato client utilizzando certutil. Per generare la richiesta di certificato client, utilizzare il comando:
	`certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .`
	Nota:
	in un `<client_dn>` sono incluse informazioni quali "CN=<client_name>, OU=*org unit*, O=*Companyname*, L=*city*, ST=*province*, C=*country*. Questa richiesta di certificato deve quindi essere autenticata mediante l'autorità di certificazione. Per recuperare il certificato e inserirlo nel file `cert7.db`, utilizzare il comando seguente:
	`certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name>`
	Per agevolare l'autenticazione Java con SSL, è necessario generare una richiesta di certificato client mediante l'utilità keytool dalla directory bin di Java. Generare una coppia di chiavi con il comando seguente:
	`keytool -genkey -keystore .keystore`
	Dopo avere specificato le informazioni relative al client, generare una richiesta di certificato client utilizzando il comando seguente:
	`keytool -certreq -file <certificate_request_name> -keystore .keystore`
	Dopo che la richiesta di certificato client è stata autenticata dall'autorità di certificazione, è necessario inserire il certificato CA nel file `.keystore` utilizzando il seguente comando:
	`keytool -import -v -alias <CA_alias_name> -file <ca_certificate_name> -trustcacerts -keystore .keystore`
	Infine recuperare la richiesta di certificato client dal CA e inserirla nel file `.keystore` con il comando seguente:
	`keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore`
	Archiviare il file `.keystore` nella stessa directory di `cert7.db` e `cacerts` nel computer che ospita la piattaforma BI.

1. Scegliere il livello di protezione SSL che si desidera utilizzare tra le opzioni disponibili:

   Nota:
   Le applicazioni Java ignoreranno la prima e l'ultima impostazione e accetteranno il certificato del server solo se proviene da un'autorità di certificazione attendibile.

   - **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, la piattaforma BI deve individuare l'autorità di certificazione che lo ha rilasciato nel suo database dei certificati.

- **Accetta certificato server se proviene da un'autorità di certificazione attendibile e 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 individuare l'autorità di certificazione che lo ha rilasciato nel proprio database dei certificati. Deve inoltre essere in grado di confermare che l'attributo CN del certificato server corrisponda esattamente al nome host dell'host LDAP digitato nel campo “Aggiungi host LDAP” nel primo passaggio della procedura guidata. In altre parole, se il nome host LDAP è stato immesso nella forma ABALONE.rd.crystald.net:389, l’uso di CN =ABALONE:389 nel certificato non funzionerà.

  il nome host presente sul certificato di protezione server è il nome dell'host LDAP primario. Quindi, se si seleziona questa opzione, non è possibile utilizzare un host LDAP di failover.

2. Nella casella **Host SSL** digitare il nome host di ciascun computer, quindi fare clic su **Aggiungi**.

   Nota:
   È quindi necessario aggiungere il nome host di ogni computer della distribuzione della piattaforma BI che utilizza l'SDK della piattaforma SAP BusinessObjects Business Intelligence. 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 ciascun host SSL aggiunto all'elenco e specificare le impostazioni predefinite che verranno utilizzate per tutti gli host che non sono nell'elenco.

   Nota:
   le impostazioni predefinite verranno utilizzate per qualsiasi impostazione (per qualsiasi host) dove la casella "Usa il valore predefinito" viene lasciata selezionata o per qualsiasi computer il cui nome non viene esplicitamente aggiunto all'elenco degli host SSL.

   Per specificare le impostazioni predefinite:

   a. Selezionare i valori predefiniti dall'elenco di SSL.
   b. Deselezionare le caselle **Usa il valore predefinito**.
   c. Digitare i valori desiderati per il "Percorso dei file di database dei certificati e delle chiavi" e la "Password per il database delle chiavi".
   d. Se vengono specificate impostazioni per l'autenticazione reciproca, è inoltre possibile immettere un valore nel campo "Nome fittizio per il certificato client in cert7.db".

   Per selezionare le impostazioni di un altro host, selezionarne il nome nell'elenco a sinistra. Quindi digitare i valori appropriati nelle caselle a destra.

4. Fare clic su **Avanti**.

5. Scegliere un metodo di autenticazione Single Sign-On LDAP tra una di queste opzioni:
   - Base (senza SSO)
   - SiteMinder
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

7.3.2.4 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'autorizzazione LDAP è configurata, viene visualizzata la pagina di riepilogo della configurazione server LDAP. In questa pagina è possibile modificare qualsiasi area o campo dei parametri di connessione. È inoltre possibile modificare l'area Gruppi di membri LDAP mappati.
3. Eliminare i gruppi correntemente mappati che non saranno più accessibili con le nuove impostazioni di connessione, quindi fare clic su **Aggiorna**.
4. Modificare le impostazioni di connessione, quindi fare clic su **Aggiorna**.
5. Modificare le opzioni Alias e Nuovo utente, quindi fare clic su **Aggiorna**.
6. Mappare i nuovi gruppi dei membri LDAP, quindi fare clic su **Aggiorna**.

7.3.2.5 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

7.3.2.5.1 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.
   - 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 **Nome agente** e **Segreto condiviso**. Ripetere l'immissione del segreto condiviso.
5. Fare clic su **Avanti**.
6. Continuare con la configurazione delle opzioni LDAP.

7.3.2.5.2 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 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.

   Nota:
   utilizzare Blocco note o un'altra utilità per la modifica del testo.
3. Chiudere il file e salvarlo con il nome seguente:

   BIlaunchpad.properties
4. Immettere l'istruzione seguente:

```
siteminder.authentication=secLDAP
siteminder.enabled=true
```

5. Chiudere il file e salvarlo con il nome seguente:

   proprietà globali

   Nota:
   accertarsi che il nome file non venga salvato con un'estensione diversa da `.txt`.

6. Creare un altro file nella stessa directory.
7. Immettere l'istruzione seguente:

```
authentication.default=LDAP
cms.default=[enter your cms name]:[Enter the CMS port number]
```

   Ad esempio:

```
authentication.default=LDAP
cms.default=mycms:6400
```

8. Chiudere il file e salvarlo con il nome seguente:

   bilaunchpad.properties

Le nuove proprietà hanno 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 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*.

7.3.3 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'autorizzazione LDAP è configurata, l'area Gruppi membri LDAP mappati riporterà i gruppi LDAP mappati alla piattaforma BI.

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

7.3.3.1 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'autorizzazione LDAP è configurata, viene visualizzata la pagina di riepilogo LDAP.

3. Nell'area "Membri del gruppo LDAP mappati" specificare il gruppo LDAP (per nome comune o nome distinto) nel campo **Aggiungi un gruppo LDAP (per cn o dn)**; fare clic su **Aggiungi**.

   Ripetendo questa procedura è possibile aggiungere più di un gruppo LDAP. Per rimuovere un gruppo, evidenziare il gruppo LDAP quindi fare clic su Elimina.

4. Le nuove opzioni alias consentono di specificare come vengono mappati gli alias LDAP agli account Enterprise. Selezionare una delle due opzioni riportate di seguito:
   - **Assegna ciascun alias LDAP aggiunto a un account con lo stesso nome**

     Utilizzare questa opzione quando si sa che gli utenti possiedono un account Enterprise già esistente con lo stesso nome; di conseguenza gli alias LDAP 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 LDAP, verranno aggiunti come nuovi utenti LDAP.

     oppure

   - **Crea un nuovo account per ogni alias LDAP aggiunto**

     Utilizzare questa opzione quando si desidera creare un nuovo account per ciascun utente.

5. Le opzioni di aggiornamento consentono di specificare se gli alias LDAP vengono creati automaticamente per tutti i nuovi utenti. Selezionare una delle due opzioni riportate di seguito:
   - **Nuovi alias verranno aggiunti e nuovi utenti verranno creati**

     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" e si è fatto clic su **Aggiorna**.

     oppure

   - **Non verranno aggiunti nuovi alias e non verranno creati nuovi utenti**

     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 BI.

6. Le opzioni nuovo utente consentono di specificare le proprietà dei nuovi account Enterprise creati per essere mappati agli account LDAP.

   Se la licenza della piattaforma SAP BusinessObjects Business Intelligence di cui si dispone si basa sui ruoli utente, selezionare una delle seguenti "Nuove opzioni utente":
   - **Visualizzatore BI**

     I nuovi account utente vengono configurati con il ruolo Visualizzatore BI. L'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Visualizzatore BI è definito nel contratto di licenza. Gli utenti potranno accedere ai workflow delle applicazioni in base a quanto previsto dal ruolo Visualizzatore BI. I diritti di accesso generalmente sono limitati alla visualizzazione dei documenti business intelligence. Questo ruolo è di norma adatto agli utenti che utilizzano contenuti mediante le applicazioni della piattaforma BI.

- **Analista BI**

  I nuovi account utente vengono configurati con il ruolo Analista BI. L'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Analista BI è definito nel contratto di licenza. Gli utenti possono accedere a tutti i workflow delle applicazioni definiti per il ruolo Analista BI. I diritti di accesso includono la visualizzazione e la modifica dei documenti business intelligence. Questo ruolo è adatto agli utenti che creano e modificano contenuti per le applicazioni della piattaforma BI.

Se la licenza della piattaforma SAP BusinessObjects Business Intelligence di cui si dispone non si basa sui ruoli utente, selezionare una delle opzioni seguenti:

- **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 quanti utenti 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**.

Argomenti correlati

- Licenze basate sul ruolo

7.3.3.2 Eliminazione della mappatura dei gruppi LDAP mediante la piattaforma BI

1. Passare all'area di gestione **Autenticazione** della CMC.
2. Fare doppio clic su **LDAP**.

   Se l'autorizzazione 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**.

7.3.3.3 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	È possibile mappare in: • 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. Non è possibile mappare in: • 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. 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.
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.

7.3.3.4 Risoluzione dei problemi relativi agli account LDAP

- Se si crea un nuovo account utente LDAP che non appartiene a un account di gruppo mappato nella piattaforma BI, mappare il gruppo oppure aggiungere il nuovo account utente LDAP già mappato nel sistema.
- Se viene creato un nuovo account utente LDAP e l'account appartiene a un account di gruppo mappato nella piattaforma BI, occorre aggiornare l'elenco degli utenti.

Argomenti correlati

- Configurazione dell'autenticazione LDAP
- Mappatura di gruppi LDAP

7.4 Autenticazione Windows AD

7.4.1 Panoramica

7.4.1.1 Utilizzo dell'autenticazione Windows AD

In questa sezione viene fornita una descrizione generale del funzionamento dell'autenticazione Windows Active Directory (AD) con la piattaforma BI. Vengono descritti inoltre i workflow di amministrazione necessari per abilitare e gestire account AD nella piattaforma BI. Al termine della sezione sono presenti alcuni suggerimenti di base per la risoluzione dei problemi.

Requisiti di supporto

Per facilitare 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 le piattaforme Windows 2003 e 2008 siano entrambe supportate per l'autenticazione Kerberos e NTLM, è possibile che alcune applicazioni della piattaforma BI utilizzino solo metodi di autenticazioni particolari. Ad esempio, le applicazioni come BI Launch Pad e Central Management Console supportano solo Kerberos.

Workflow di autenticazione AD di base

Per utilizzare l'autenticazione AD con la piattaforma BI è necessario seguire il seguente workflow di base:

1. Configurare le risorse del controller di dominio necessarie.
2. Preparare l'host della piattaforma BI per l'autenticazione Windows AD.
3. Abilitare il plug-in di protezione AD e mapparlo i gruppi AD.
4. Scegliere un metodo di autenticazione:
   - Windows AD con Kerberos
   - Windows AD con NTLM

5. Impostare il Single Sign On alle applicazioni della piattaforma BI. Questo passaggio facoltativo può essere semplificato tramite i metodi seguenti:
   - Windows AD con Vintela (Kerberos)
   - Windows AD con SiteMinder (Kerberos)

7.4.1.1.1 Plug-in di protezione di Windows AD

Il plug-in di protezione Windows AD consente di mappare account utente e gruppi dal database utenti Microsoft Active Directory (AD) 2003 e 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 a fronte del 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 della piattaforma BI.

Il plug-in di protezione Windows AD consente di configurare quanto segue:

- Autenticazione Windows AD con NTLM
- Autenticazione Windows AD con Kerberos
- Autenticazione Windows AD con SiteMinder per il Single Sign-On

Il plug-in di protezione Windows AD è compatibile con domini Microsoft Active Directory 2003 e 2008 in esecuzione in modalità nativa o mista.

Dopo essere stati mappati, gli utenti e i gruppi AD potranno accedere agli strumenti client della piattaforma BI utilizzando l'autenticazione AD.

- L'autenticazione Windows AD funziona solo se il CMS viene eseguito su Windows. Per il corretto funzionamento del Single Sign On nel database, è inoltre necessario che i server per la creazione di report vengano eseguiti in Windows. Negli altri casi, tutti gli altri server e servizi possono essere eseguiti su tutte le piattaforme supportate.
- Il plug-in di Windows AD per la piattaforma BI supporta i domini in più foreste.

7.4.1.1.2 Utilizzo di utenti e gruppi Windows AD

La piattaforma BI supporta l'autenticazione Active Directory (AD) con il plug-in di protezione Windows, incluso per impostazione predefinita quando il prodotto viene installato su una piattaforma Windows. Il supporto per l'autenticazione Windows AD implica la possibilità di utilizzare account di utenti e gruppi creati in Microsoft Active Directory 2003 e 2008 per l'autenticazione con la piattaforma BI. L'amministratore di sistema può quindi mappare gli account AD esistenti anziché impostare ogni utente e gruppo nella piattaforma BI.

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 Windows 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.

Schema ricorrente	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 Active Directory (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 Windows Active Directory (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 allo stesso modo creati, eliminati o disabilitati 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 ora grafico gruppo e alias AD** nell'area "Aggiornamento AD su richiesta" della console CMC.

Nota:
Non viene memorizzata alcuna password AD nell'alias utente.

7.4.1.1.3 Single Sign On con Windows AD

Il plug-in di protezione di Windows AD supporta il Single Sign On, consentendo in questo modo agli utenti AD autenticati di accedere alla piattaforma BI senza inserire in modo esplicito le relative credenziali. I requisiti di Single Sign On dipendono dalla modalità di accesso degli utenti alla piattaforma: tramite thick client oppure dal Web. In entrambi gli scenari, il plug-in di protezione ottiene il contesto di protezione per l'utente dal provider di autenticazione e concede all'utente una sessione attiva della piattaforma BI, se l'utente è un membro di un gruppo AD mappato.

Lo scenario di utilizzo più comune implica il Single Sign-On all'applicazione Web BI Launch Pad.

Single Sign-On al database

Il plug-in Windows AD supporta il Single Sign-On al database. Se sono impostati correttamente, gli utenti AD autenticati non devono fornire le credenziali del proprio account quando accedono a report dall'applicazione BI Launch Pad.

Argomenti correlati

- Utilizzo di Windows AD con SiteMinder
- Configurazione dell'autenticazione Windows AD (Kerberos) con il Single Sign-On Vintela

7.4.2 Preparazione per l'autenticazione AD (Kerberos)

7.4.2.1 Utilizzo dell'autenticazione Windows AD con Kerberos

In questa sezione vengono illustrate le attività essenziali per l'impostazione dell'autenticazione Kerberos per la piattaforma BI. Dopo aver implementato tutte le attività essenziali, è possibile procedere a configurare opzioni di autenticazione Windows AD per Kerberos nel plug-in di protezione Windows AD.

Workflow consigliato

Per impostare correttamente l'autenticazione Windows AD è necessario implementare le seguenti attività essenziali:

- Impostazione di un account di servizio per l'esecuzione della piattaforma BI
- Preparazione dei server della piattaforma BI per l'autenticazione Windows AD con Kerberos
- Configurazione del server di applicazioni Web per l'autenticazione Windows AD con Kerberos.

7.4.2.1.1 Impostazione di un account di servizio per l'autenticazione AD con Kerberos

Per configurare la piattaforma BI per l'autenticazione Kerberos e Windows AD, è necessario un account di servizio. È possibile creare un nuovo account di dominio o utilizzare un account già esistente. L'account di servizio verrà utilizzato per eseguire i server della piattaforma BI.

Nota:
dopo aver impostato l'account di servizio, sarà necessario concedere all'account i diritti appropriati.

Se si utilizza un dominio Windows 2003 o 2008, è anche possibile scegliere di impostare una delega vincolata.

Per impostare l'account di servizio in un dominio Windows 2003 o 2008

Per abilitare correttamente l'autenticazione Windows AD con Kerberos è necessario impostare un nuovo account di servizio sul controller di dominio. Questo account di servizio verrà utilizzato appositamente per consentire agli utenti di un determinato gruppo Windows AD di accedere a BI Launch Pad. Questa attività viene eseguita sul computer controller di dominio AD.

1. Creare un nuovo account con una password sul controller di dominio o utilizzare un account già esistente.

   Per istruzioni dettagliate, consultare http://msdn.microsoft.com/

2. Eseguire il comando keytab`ktpass` per creare e posizionare un file di codice Kerberos.

   Sarà necessario specificare i parametri `ktpass` elencati nella seguente tabella:

Parametro	Descrizione
-out	Specifica il nome del file di codice Kerberos da generare.

Parametro	Descrizione
-mapuser	Specifica il nome dell'account utente a cui è stato mappato l'SPN. Si tratta dell'account con cui viene eseguito il Server Intelligence Agent.
-pass	Specifica la password utilizzata dall'account di servizio.
-kvno	Specifica il numero di versione della chiave utilizzato per creare la chiave.
-ptype	Specifica il tipo principale. Deve essere specificato come: `-ptype KRB5_NT_PRINCIPAL`
-crypto	Specifica quale tipo di crittografia utilizzare con l'account di servizio. Utilizzare quanto di seguito riportato: `-crypto RC4-HMAC-NT`

Ad esempio:

```
ktpass -out -mapuser sbo.serviceDOMAIN.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. Il comando mappa anche il nome principale all'account di servizio (locale).

3. Eseguire il comando `setspn -l` per verificare che il comando `ktpass` sia stato correttamente eseguito.

   L'output visualizzato elenco tutti i nomi principali di servizio registrati nell'account di servizio locale.
4. Fare clic con il pulsante destro del mouse sull'account di servizio creato nel passaggio 1 e scegliere **Proprietà** > **Delega**.
5. Fare clic su **Utente attendibile per la delega a qualsiasi servizio (solo Kerberos)**.
6. Fare clic su **OK** per salvare le modifiche apportate.

Dopo la creazione è necessario concedere diritti all'account di servizio e aggiungere quest'ultimo al gruppo degli amministratori locali dei server.

Concessione dei diritti per l'account di servizio

Per supportare Windows AD e Kerberos, 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).

Se si richiede il Single Sign-On al database, il SIA deve includere i seguenti server:

- Crystal Reports Processing Server
- Report Application Server
- Web Intelligence Processing Server

Nota:
Perché il Single Sign-On al database funzioni, l'account di servizio deve essere attendibile per la delega.

Per concedere i diritti per l'account di servizio

1. Fare clic su **Start > Pannello di controllo > Strumenti di amministrazione > Criteri di protezione locali**.
2. Espandere **Criteri locali**, quindi fare clic su **Assegnazione diritti utente**.
3. Fare doppio clic su **Agisci come parte del sistema operativo**.
4. Fare clic su **Aggiungi**.
5. Immettere il nome dell'account di servizio creato e fare clic su **OK**.
6. Verificare che sia selezionata la casella di controllo **Impostazioni criterio locale** e fare clic su **OK**.
7. Ripetere la procedura precedente per ogni computer in 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.

Aggiunta dell'account di servizio al gruppo Amministratori locali dei server

Per supportare Kerberos, l'account di servizio deve appartenere al gruppo Amministratori locale per ciascun server che dispone di SIA con uno dei seguenti servizi distribuiti:

- CMS
- Server di elaborazione Crystal Reports (necessario solo per SSO2DB)
- Report Application Server (necessario solo per SSO2DB)
- Web Intelligence Processing Server (necessario solo per SSO2DB)

Nota:
Se si utilizza SSO2DB, è necessario un account di servizio che sia reso attendibile per delega. È necessario inoltre disporre dei diritti di amministratore sul server.

Per aggiungere un account al gruppo Amministratori

1. Sul computer desiderato, fare clic con il pulsante destro del mouse su **Risorse del computer** e scegliere **Gestisci**.
2. Selezionare **Utilità di sistema > Utenti e gruppi locali > Gruppi**.
3. Fare clic con il pulsante destro del mouse su **Amministratori**, quindi scegliere **Aggiungi al gruppo**.
4. Fare clic su **Aggiungi** e digitare il nome di accesso dell'account di servizio.
5. Fare clic su **Verifica i nomi** per assicurare la corretta risoluzione dell'account.
6. Fare clic su **OK**, quindi di nuovo su **OK**.

7. Ripetere questa procedura per ogni server della piattaforma BI da configurare.

7.4.2.1.2 Preparazione dei server per l'autenticazione Windows AD con Kerberos

Dopo aver creato e configurato l'account di servizio per l'autenticazione Windows AD con Kerberos, è possibile eseguire con esso ogni SIA presente nella distribuzione della piattaforma BI.

Configurazione del SIA con l'account di servizio

È necessario eseguire la procedura seguente per qualsiasi SIA (Server Intelligence Agent) che esegue servizi utilizzati dall'account di servizio creato per l'autenticazione Windows AD con Kerberos.

1. Selezionare **Programmi** > **SAP BusinessObjects Enterprise XI 4.0** > **SAP BusinessObjects Enterprise** > **Central Configuration Manager** .
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**.
6. Riavviare il SIA.
7. Se necessario, ripetere i passaggi da 1 a 5 per ogni SIA che esegue un servizio da configurare.

7.4.2.1.3 Preparazione del server di applicazioni per l'autenticazione Windows AD (Kerberos)

In questa sezione sono contenute le attività relative alla configurazione di Kerberos per l'utilizzo con i seguenti server di applicazioni:

- Tomcat
- WebSphere
- WebLogic
- Oracle Application Server
- SAP NetWeaver 7.10

In questa sezione sono contenute le seguenti informazioni:

- Il workflow specifico per un particolare server di applicazioni Web. Questo workflow è necessario poiché l'implementazione di Java Authentication and Authorization Service (JAAS) varia tra server di applicazioni diversi.
- Dettagli di tipo procedurale per ciascun passaggio nel workflow.
- File Krb5.ini di esempio per server di applicazioni Java.

Panoramica

Il particolare processo di configurazione di Kerberos per un server di applicazioni Web varia leggermente a seconda del server di applicazioni. Tuttavia, il processo generale di configurazione di Kerberos include i seguenti passaggi:

- Creazione del file di configurazione di Kerberos.
- Creazione del file di configurazione per l'accesso JAAS.

  Nota:
  questo passaggio non è necessario per il server di applicazioni Java SAP NetWeaver 7.10. Sarà però necessario aggiungere LoginModule al server SAP NetWeaver.

- Modifica delle opzioni Java.
- Riavvio del server di applicazioni Java.

Creazione di un file di configurazione Kerberos per SAP NetWeaver, Tomcat, WebLogic, SAP NetWeaver o Oracle

Seguire questa procedura per creare il file di configurazione Kerberos se si utilizza SAP Netweaver 7.10, Tomcat 6, Oracle Application Server o WebLogic.

1. Creare il file `krb5.ini`, se non è già presente e archiviarlo in C:\WINNT 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 il file in un'altra posizione, ma in tal caso, sarà necessario specificarla nelle opzioni Java. Per ulteriori informazioni su `krb5.ini`, vedere http://docs.sun.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:
`DOMINIO.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. `[capath]` definisce l'attendibilità tra i domini che si trovano in un'altra foresta AD. Nell'esempio riportato sopra `DOMINIO2.COM` è un dominio di una foresta esterna con trust transitivo diretto e bidirezionale a `DOMINIO.COM`. In una configurazione con più domini, in `[libdefaults]` 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.

Argomenti correlati

- Per modificare le opzioni Java per Kerberos su Tomcat

Creazione del file di configurazione di Kerberos per WebSphere

1. Creare il file `krb5.ini`, se non è già presente e archiviarlo in C:\WINNT per Windows.

   Nota:
   è possibile memorizzare il file in un'altra posizione, ma in tal caso, sarà necessario specificarla nelle opzioni Java.

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:

   - Se si utilizza la crittografia DES, sostituire `rc4-hmac` con `des-cbc-crc`.
   - `DOMINIO.COM` è il nome DNS del dominio che deve essere immesso in lettere maiuscole nel formato FQDN.
   - `nomehost` è il nome host del controller di dominio.

3. Salvare e chiudere il file.

Argomenti correlati

- Per modificare le opzioni Java per Kerberos in WebSphere

Esempio di file Krb5.ini con più domini

Di seguito viene riportato un esempio di file con più domini.

```
[domain_realm]
  ; trust relationship: childtest4<->sboptest3<->sboptest<->sboptest2
[libdefaults]
  default_realm = SBOPTEST.COM
[realms]
SBOPTEST.COM = {
  kdc = VANPGVMBOBJ01.sboptest.com
}
SBOPTEST2.COM = {
  kdc = VANPGVMBOBJ05.sboptest2.com
}
SBOPTEST3.COM = {
  kdc = VANPGVMBOBJ07.sboptest3.com
}
CHILDTEST4.SBOPTEST3.COM = {
  kdc = vanpgvmbobj08.childtest4.sboptest3.com
}
[capaths]
; for clients in sboptest3 to login sboptest2
SBOPTEST3.COM = {
  SBOPTEST2.COM = SBOPTEST.COM
}
; for clients in childtest4 to login sboptest2
CHILDTEST4.SBOPTEST3.COM = {
  SBOPTEST2.COM = SBOPTEST.COM
  SBOPTEST2.COM = SBOPTEST3.COM
}
```

Creazione di un file di configurazione degli accessi JAAS Tomcat o WebLogic

1. Creare un file denominato `bscLogin.conf`, se non è già presente, e memorizzarlo nella posizione predefinita: C:\WINNT.

   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.

Creazione di 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 nella posizione predefinita: C:\WINNT
2. Aggiungere il codice seguente al file di configurazione `bscLogin.conf` JAAS:

```
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 7.10, 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 7.10.

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.

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.

4. Chiudere il file di configurazione Tomcat.
5. Riavviare Tomcat.

Modifica delle opzioni Java per SAP NetWeaver 7.10

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**.
8. Aggiungere le informazioni sui parametri personalizzati seguenti:

java.security.kbr5.conf	*<percorso del file krb5.ini incluso il nome file>*
javax.security.auth.useSubjectCredsOnly	False

9. Fare clic su **Save**.
10. Fare clic su **Configuration Editor**.
11. Fare clic su **Configurations > Security > Configurations > com.businessobjects.security.jgss.initiate > Security > Authentication**.

12. Fare clic su **Edit Mode**.
13. Fare clic con il pulsante destro del mouse sul nodo **Authentication** e scegliere **Create sub-node**.
14. Selezionare **Value-Entry** nell'elenco in alto.
15. Immettere quanto segue:

Name	Create_security_session
Valore	False

16. Fare clic su **Crea**.
17. Chiudere la finestra.
18. Fare clic su **Config Tool**.
19. Fare clic 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 di WebLogic in cui si eseguono 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.co
nf=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 digitare il percorso del file Krb5.ini e quello del file bscLogin.conf.

   -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.

7.4.3 Single Sign-On di autenticazione AD

7.4.3.1 Opzioni per il Single Sign-On di autenticazione Windows AD

Sono supportati due metodi per l'impostazione del Single Sign-On per l'autenticazione Windows AD con la piattaforma BI:

- Single Sign-On Vintela - questa opzione può essere utilizzata solo con Kerberos.

- Single Sign-On con SiteMinder - questa opzione può essere utilizzata solo con Kerberos.

Nota:
Lo scenario di Single Sign-On più comune implica l'accesso all'applicazione BI Launch Pad distribuibile solo su un server di applicazioni java. Il Single Sign-On per BI Launch Pad è disponibile solo tramite Kerberos.

7.4.3.2 Preparazione per il Single Sign-On di autenticazione Windows AD

7.4.3.2.1 Configurazione dell'autenticazione Windows AD (Kerberos) con il Single Sign-On Vintela

Nella seguente sezione vengono illustrate in dettaglio le attività necessarie per impostare la piattaforma BI per l'utilizzo dell'autenticazione Windows AD e del Single Sign-On Vintela.

Nota:
Le attività di impostazione essenziali per l'autenticazione Windows AD, insieme all'attività di Single Sign-On Vintela, devono essere completate prima di configurare le opzioni di autenticazione Windows AD nella CMC.

Argomenti correlati

- Impostazione di un account di servizio per l'autenticazione AD con Kerberos
- Preparazione dei server per l'autenticazione Windows AD con Kerberos
- Preparazione del server di applicazioni per l'autenticazione Windows AD (Kerberos)

7.4.3.2.2 Flusso di lavoro per la configurazione di Kerberos e Single Sign On per Java BI Launch Pad

Per impostare la piattaforma BI per l'utilizzo dell'autenticazione Windows AD e del Single Sign-On Vintela è necessario completare le seguenti attività:

1. Creare e configurare un account di servizio da utilizzare per il Single Sign-On Vintela.
2. Impostare la distribuzione della piattaforma BI in modo da eseguirla con l'account di servizio.
3. Configurare le proprietà generali di BOE e specifiche di BI Launch Pad per il Single Sign-On Vintela.
4. Alzare il limite per le dimensioni delle intestazioni del server di applicazioni Java.
5. Configurare i browser Internet per il Single Sign-On Vintela.
6. Configurare la delega vincolata per il Single Sign-On Vintela (facoltativo).

Dopo aver completato tutte queste attività, è possibile configurare le opzioni di autenticazione Windows AD nella CMC.

7.4.3.2.3 Impostazione dell'account di servizio per il Single Sign-On Vintela

Per abilitare correttamente il Single Sign-On Vintela per l'autenticazione Windows AD è necessario impostare un nuovo account di servizio sul controller di dominio. Questo account di servizio verrà utilizzato appositamente per consentire agli utenti di un determinato gruppo Windows AD di accedere a BI Launch Pad. Questa attività viene eseguita sul computer controller di dominio AD. I passaggi 1-5 seguenti sono necessari per utilizzare Windows AD con Kerberos, mentre i passaggi 6-7 servono all'impostazione del Single Sign-On Vintela.

1. Creare un nuovo account di servizio con una password sul controller di dominio principale.
2. Eseguire il comando di impostazione del codice Kerberos `ktpass` per creare e posizionare un file di codice.

   Sarà necessario specificare i parametri `ktpass` elencati nella seguente tabella:

Parametro	Descrizione
-out	Specifica il nome del file di codice Kerberos da generare.
-princ	Specifica il nome principale utilizzato per l'account di servizio. Questo parametro deve essere specificato in formato SPN. **Nota:** Per il nome dell'account di servizio occorre distinguere tra maiuscole e minuscole. Un SPN include sempre il nome del computer host su cui è in esecuzione l'istanza del servizio. **Suggerimento:** L'SPN deve essere univoco nella foresta in cui viene registrato. Per verificare è possibile utilizzare lo strumento di supporto Windows `Ldp.exe` per cercare l'SPN.
-mapuser	Specifica il nome dell'account utente a cui è stato mappato il parametro -princ prima riportato. Si tratta dell'account con cui viene eseguito il Server Intelligence Agent.
-pass	Specifica la password utilizzata dall'account di servizio.
-kvno	Specifica il numero di versione della chiave utilizzato per creare la chiave.
-ptype	Specifica il tipo principale. Deve essere specificato come: `-ptype KRB5_NT_PRINCIPAL`
-crypto	Specifica quale tipo di crittografia utilizzare con l'account di servizio. Utilizzare quanto di seguito riportato: `-crypto RC4-HMAC-NT`

Ad esempio:

```
ktpass -out keytab_filename.keytab -princ
MYSIAMYSERVER/sbo.service.DOMAIN.COM
```

```
-mapuser sbo.serviceDOMAIN.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. Il comando mappa anche il nome principale all'account di servizio (locale).

3. Eseguire il comando `setspn -l` per verificare che il comando `ktpass` sia stato correttamente eseguito.

   L'output visualizzato elenco tutti i nomi principali di servizio registrati nell'account di servizio locale.

4. Fare clic con il pulsante destro del mouse sull'account di servizio creato nel passaggio 1 e scegliere **Proprietà** > **Delega**.
5. Fare clic su **Utente attendibile per la delega a qualsiasi servizio (solo Kerberos)**.
6. Utilizzare il comando `setspn -a` per aggiungere i nomi principali di servizio HTTP all'account di servizio creato al passaggio 1. Specificare i nomi principali di servizio per il server, il server di dominio completo e l'indirizzo IP del computer su cui è distribuito BI Launch Pad.

   Ad esempio:

```
setspn -a HTTP/servername servicename
setspn -a HTTP/servernamedomain servicename
setspn -a HTTP/<ip address of server> servicename
```

   In cui *`nome server`* è il nome del server su cui è distribuito BI Launch Pad e *`dominio nome server`* è il nome di dominio completo di quest'ultimo.

7. Eseguire `setspn -l` *`nome servizio`* per verificare che i nomi principali di servizio HTTP siano stati aggiunti all'account di servizio.

   L'output del comando deve includere tutti i nomi principali di servizio registrati, come illustrato nell'esempio seguente:

```
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
```

All'account di servizio sono stati aggiunti tutti i nomi principali di servizio necessari e il file di codice richiesto è stato creato.

Affinché il Single Sign On Vintela funzioni è necessario impostare i server della piattaforma BI, modificare le proprietà di BI Launch Pad e copiare il file di codice nella directory appropriata.

7.4.3.2.4 Preparazione dei server per il Single Sign-On Vintela

È necessario assicurarsi che il computer su cui sono distribuiti i server della piattaforma BI sia stato aggiunto al dominio principale e che tutti i suffissi DNS necessari siano stati accodati.

Per eseguire la seguente attività sarà necessario il file di codice creato per l'autenticazione Windows AD con Kerberos.

1. Copiare il file di codice Kerberos in una posizione sul computer che ospita i server della piattaforma BI.
2. Aggiungere l'account di servizio Kerberos al gruppo degli amministratori del computer host.

Formattare il nome account come segue: *DOMAINNAME\nome servizio*.

3. Aggiungere l'account di servizio Kerberos ai seguenti diritti di sistema nella MMC Criteri di protezione locali:

Diritto di sistema	Impatto
Agisci come parte del sistema operativo	Consente a un processo di rappresentare qualsiasi utente senza la necessità di eseguire l'autenticazione.
Accesso come processo batch	Consente a un utente di effettuare l'accesso tramite una funzionalità che utilizza una coda batch.
Accedi come servizio	Consente a un account di servizio di registrare un processo come servizio.
Sostituzione di token a livello di processo	Consente a un account di chiamare l'API CreateProcessAsUser() consentendo così a un servizio di avviarne un altro.

È necessario eseguire i server della piattaforma BI con l'account di servizio.

4. Selezionare **Programmi > SAP BusinessObjects Enterprise XI 4.0 > SAP BusinessObjects Enterprise > Central Configuration Manager** .
5. In CCM fare clic con il pulsante destro del mouse su Server Intelligence Agent (SIA) e scegliere **Arresta**.
6. Fare clic con il pulsante destro del mouse sul SIA e scegliere **Proprietà**.
7. Deselezionare la casella di controllo **Account sistema**.
8. Immettere le credenziali dell'account Kerberos (*DOMAINNAME\nome servizio*) create al passaggio 2 e fare clic su **OK**.
9. Riavviare il SIA.

Per completare l'impostazione del Single Sign-On Vintela è necessario eseguire le seguenti attività:

- Preparare le proprietà del server di applicazioni Web e di and BI Launch Pad per il Single Sign-On Vintela.
- Configurare il plug-in di protezione Window AD per consentire l'autenticazione Windows AD e il Single Sign-On Vintela.

7.4.3.2.5 Abilitazione del Single Sign-On Vintela per BI Launch Pad e OpenDocument

Questa procedura può essere utilizzata per applicazioni Web OpenDocument e BI Launch Pad. Oltre che per il plug-in di protezione Windows AD, le impostazioni di Vintela Single Sign On devono essere specificate anche per le proprietà BOE.war.

1. Accedere alla cartella personalizzata dell'applicazione Web BOE nel computer che ospita il server di applicazioni Web.

Se si utilizza il server di applicazioni Web Tomcat fornito con l'installazione della piattaforma BI, è possibile accedere direttamente alla directory seguente.

`C:\Programmi (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\config\custom\`

Suggerimento:
se si utilizza un server di applicazioni Web che non consente l'accesso diretto alle applicazioni Web distribuite, è possibile utilizzare la cartella seguente nell'installazione del prodotto per modificare l'applicazione Web BOE.

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

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. Immettere quanto segue:

```
sso.enabled=true
siteminder.enabled=false
vintela.enabled=true
idm.realm=[YOUR_REALM]
idm.princ=[YOUR_PRINCIPAL]
idm.allowUnsecured=true
idm.allowNTLM=false
idm.logger.name=simple
idm.logger.props=error-log.properties
```

   Nota:
   è necessario specificare valori validi per i parametri idm.realm e idm.princ. Il valore di idm.realmdeve 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 il Single Sign-On Vintela.

4. Se si è scelto di utilizzare un file di codice, aggiungere il parametro keytab e specificare il percorso del file, come mostrato nell'esempio seguente:

```
idm.keytab=C:/WIN/filename.keytab
```

   Ignorare il seguente passaggio se non si desidera utilizzare la delega vincolata per l'autenticazione Windows AD e il Single Sign-On Vintela.

5. Per utilizzare la delega vincolata aggiungere:

```
idm.allowS4U=true
```

6. Chiudere il file e salvarlo con il nome seguente:

   proprietà globali

   Nota:
   accertarsi che il nome file non venga salvato con un'estensione diversa da `.txt`.

7. Creare un altro file nella stessa directory. Salvare il file come `OpenDocument.properties` o `BI launchpad.properties`, a seconda dei requisiti.

8. Immettere l'istruzione seguente:

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

   Ad esempio:

```
authentication.default=secWinAD
cms.default=mycms:6400
```

9. Salvare e chiudere il file.
10. 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.

Argomenti correlati

- Esempio di file Krb5.ini con più domini
- Preparazione del server di applicazioni per l'autenticazione Windows AD (Kerberos)

7.4.3.2.6 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 `<TomcatINSTALLDIR>/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\Tomcat6\`
   - 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.

7.4.3.2.7 Configurazione dei browser Internet

Per supportare Kerberos Single Sign On, è necessario configurare i client della piattaforma BI, nonché configurare il browser Internet Explorer (IE) nei computer client.

Per configurare Internet Explorer nei computer client

1. Nel computer client aprire la 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 la finestra 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 la finestra 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 InfoView. 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.

7.4.3.2.8 Configurazione della delega vincolata per il Single Sign-on Vintela

La delega vincolata è facoltativa per l'autenticazione AD e il Single Sign-On Vintela. È invece necessaria per gli scenari di distribuzione che implicano il Single Sign-On al database di sistema.

1. Nel computer controller di dominio AD aprire lo snap-in "Utenti e computer" di Active Directory.
2. Fare clic con il pulsante destro del mouse sull'account di servizio creato per il Single Sign-On Vintela 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. Digitare il nome dell'account di servizio (utilizzato per il Single Sign-On Vintela) e fare clic su **OK**.

   Viene visualizzato un elenco di servizi.

7. Selezionare i seguenti servizi 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 (Single Sign-On Vintela).

Per giustificare questa modifica, è necessario modificare le proprietà dell'applicazione Web. Aprire il file BOE global.properties nel server di applicazioni Web. Aggiungere quanto segue e quindi riavviare il server di applicazioni Web.

```
idm.allowS4U=true
```

7.4.3.3 Utilizzo di SiteMinder

7.4.3.3.1 Utilizzo di Windows AD con SiteMinder

In questa sezione viene illustrato come utilizzare AD e SiteMinder. SiteMinder è uno strumento di terze parti per l'autenticazione e l'accesso utente che è possibile utilizzare con il plug-in di protezione AD per creare il Single Sign On alla 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.

Modifica del file delle proprietà BOE per l'autenticazione Windows AD con SiteMinder

Oltre che per il plug-in di protezione Windows AD, le impostazioni di SiteMinder devono essere specificate anche per le proprietà war BOE.

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

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

2. Creare un nuovo file.

Nota:
utilizzare Blocco note o un'altra utilità per la modifica del testo.

3. Chiudere il file e salvarlo con il nome seguente:
   `BIlaunchpad.properties`
4. Immettere l'istruzione seguente:

```
sso.enabled=true
siteminder.authentication=secWinAD
siteminder.enabled=true
```

5. Chiudere il file e salvarlo con il nome seguente:
   proprietà globali

   Nota:
   accertarsi che il nome file non venga salvato con un'estensione diversa da `.txt`.

6. Creare un altro file nella stessa directory.
7. Immettere l'istruzione seguente:

```
authentication.default=secWinAD
cms.default=[enter your cms name]:[Enter the CMS port number]
```

   Ad esempio:

```
authentication.default=LDAP
cms.default=mycms:6400
```

8. Chiudere il file e salvarlo con il nome seguente:
   `BIlaunchpad.properties`

Le nuove proprietà verranno applicate solo dopo la ridistribuzione 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*.

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:
   `<DIRINSTALLAZ>\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 ridistribuzione 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*.

7.4.4 Mappatura di gruppi AD e configurazione dell'autenticazione AD

7.4.4.1 Per mappare utenti e gruppi AD e configurare il plug-in di protezione di Windows AD

Per configurare l'autenticazione Windows AD perché funzioni con un determinato tipo di autenticazione, è prima necessario completare tutte le attività preparatorie richieste. Per ulteriori informazioni, vedere la sezione "Argomenti correlati" riportata di seguito.

Indipendentemente dal protocollo in uso, è necessario completare i passaggi seguenti per consentire l'autenticazione degli utenti AD. Effettuare le operazioni dei passaggi da 1 a 8 della procedura seguente per importare gruppi AD nella piattaforma BI.

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. Nell'area **Riepilogo della configurazione Windows AD** fare clic sul collegamento accanto a **Nome amministrazione AD**.

   Nota:
   prima della configurazione del plug-in Windows AD, questo collegamento viene visualizzato come due virgolette doppie. Una volta salvata la configurazione, il collegamento viene completato con i nomi di amministrazione AD.

5. Immettere il nome e la password di un account utente di dominio abilitato. Questo account verrà utilizzato dalla piattaforma BI per richiedere informazioni ad AD.

   Le credenziali di amministrazione possono utilizzare uno dei formati seguenti:

   - Nome NT (`NomeDominio\NomeUtente`)

- UPN (`utente@DNS_dominio_nome`)

Il contenuto di AD non viene mai modificato, aggiunto o eliminato dalla piattaforma BI. Le informazioni vengono solo lette, pertanto sono necessari solo i diritti appropriati per tale operazione.

Nota:
L'autenticazione AD non viene mantenuta se l'account AD 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. Compilare il campo **Dominio AD predefinito**.

   Nota:
   - I gruppi dal dominio predefinito possono essere mappati senza specificare il prefisso del nome del dominio.
   - Se si digita il 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 di membri AD mappati", immettere dominio\gruppo AD nel campo **Aggiungere il gruppo AD (dominio\gruppo)**.

   È possibile mappare i gruppi utilizzando uno dei formati seguenti:

   - Nome account SAM (Security Account Manager), indicato anche come nome NT (`NomeDominio\NomeGruppo`)
   - DN (`cn=NomeGruppo, ....., dc=NomeDominio, dc=com`)

   Nota:
   Se si desidera mappare un gruppo locale, è possibile utilizzare solo il formato del nome NT (\\NomeServer\NomeGruppo). AD non supporta utenti locali. Questo significa che gli utenti locali appartenenti a un gruppo locale mappato non vengono mappati alla piattaforma BI e pertanto non possono accedere al sistema.

8. Fare clic su **Aggiungi**.

   Il gruppo verrà aggiunto all'elenco.

   È possibile ignorare i passaggi 9-18 se si desidera importare account di gruppo AD senza configurare opzioni di autenticazione AD o aggiornamenti dei gruppi AD.

9. Per configurare il Single Sign-On, selezionare **Abilita il Single Sign-On per la modalità di autenticazione selezionata**.

   Nota:
   Se si seleziona questa opzione, è necessario configurare le proprietà generali e BI Launch Pad dell'applicazione Web BOE per consentire il Single Sign-On.

10. Selezionare l'opzione nell'area "Sincronizzazione delle credenziali" per abilitare e aggiornare le credenziali dell'origine dati dell'utente AD al momento dell'accesso. L'origine dati verrà in questo modo sincronizzata con le credenziali di accesso correnti dell'utente.
11. Utilizzare l'area **Opzioni SiteMinder** della pagina per configurare SiteMinder come opzione di Single Sign-On per l'autenticazione AD mediante Kerberos.

Nota:
Come opzione di Single Sign-On è possibile configurare Vintela o SiteMinder, non entrambi. Cancellare qualsiasi voce presente nel campo **Nome principale servizio** (passaggio 9b) se si desidera configurare le opzioni SiteMinder.

a. Fare clic su **Disabilitato.**

   Viene visualizzata la pagina di configurazione di Windows AD SiteMinder.

   Nota:
   Se non è stato configurato il plug-in Windows AD, si riceverà un avviso e un messaggio chiederà 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 specificare i numeri di porta **Accounting**, **Autenticazione** e **Autorizzazione**.
e. Specificare il **Nome dell'agente** e il **Segreto condiviso**. Immettere di nuovo il **Segreto condiviso**.

   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.

f. Fare clic su **Aggiorna** per salvare le informazioni e tornare alla pagina di autenticazione AD principale.

12. Nell'area "Opzioni alias AD" specificare in che modo aggiungere e aggiornare i nuovi alias nella piattaforma BI.
    a. In "Nuove opzioni alias" selezionare in che modo i nuovi alias vengono mappati agli account Enterprise. Selezionare una delle opzioni seguenti:
       - **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 automatica di alias 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. In "Opzioni di aggiornamento alias" selezionare in che modo gestire gli aggiornamenti degli alias per gli account Enterprise. Selezionare una delle opzioni seguenti:
       - **Crea nuovi alias all'aggiornamento dell'alias**

         Utilizzare 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 senza 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**

  Utilizzare questa opzione se la directory AD che si sta mappando contiene 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 BI.

c. In "Nuove opzioni utente" specificare in che modo vengono creati i nuovi utenti selezionando una delle opzioni seguenti:

   Se la licenza della piattaforma SAP BusinessObjects Business Intelligence di cui si dispone si basa sui ruoli utente, selezionare una delle opzioni seguenti:

   - **Utente visualizzatore BI**

     I nuovi account utente vengono configurati con il ruolo Visualizzatore BI. L'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Visualizzatore BI è definito nel contratto di licenza. Gli utenti potranno accedere ai workflow delle applicazioni in base a quanto previsto dal ruolo Visualizzatore BI. I diritti di accesso generalmente sono limitati alla visualizzazione dei documenti business intelligence. Questo ruolo è di norma adatto agli utenti che utilizzano contenuti mediante le applicazioni della piattaforma BI.

   - **Utente analista BI**

     I nuovi account utente vengono configurati con il ruolo Analista BI. L'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Analista BI è definito nel contratto di licenza. Gli utenti possono accedere a tutti i workflow delle applicazioni definiti per il ruolo Analista BI. I diritti di accesso includono la visualizzazione e la modifica dei documenti business intelligence. Questo ruolo è adatto agli utenti che creano e modificano contenuti per le applicazioni della piattaforma BI.

   Se la licenza della piattaforma SAP BusinessObjects Business Intelligence di cui si dispone non si basa sui ruoli utente, selezionare una delle opzioni seguenti:

   - **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 quanti utenti 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.

13. Per configurare la modalità di pianificazione degli aggiornamenti degli alias AD, fare clic su **Pianifica aggiornamenti alias AD**.

    a. Nella finestra di dialogo "Pianificazione" selezionare una ricorrenza nell'elenco **Esegui oggetto**.

b. Impostare le altre opzioni di pianificazione e i parametri in base alle esigenze.
c. Fare clic su **Pianifica**.

   All'aggiornamento degli alias vengono aggiornate anche le informazioni sul gruppo.

14. Nell'area "Opzioni di collegamento attributi" è possibile specificare la priorità di collegamento degli attributi per il plug-in AD:
    a. Fare clic sulla casella **Importa nome completo e indirizzo di posta elettronica**.

       I nomi completi e le descrizioni utilizzati negli account AD vengono importati e memorizzati con gli oggetti utente nella piattaforma BI.
    b. Specificare un'opzione per **Imposta priorità collegamento attributi AD relativo ad altri collegamenti attributi**.

       Nota:
       se l'opzione è impostata su "1", gli attributi AD hanno la priorità in scenari in cui sono abilitati AD e altri plug-in (LDAP e SAP). Se è impostata su "3", avranno la priorità gli attributi di altri plug-in abilitati.

15. È possibile configurare gli aggiornamenti del gruppo AD nell'area "Opzioni gruppo AD".
    a. Fare clic su **Pianifica aggiornamenti gruppi AD**.

       Viene visualizzata la finestra di dialogo "Pianificazione".
    b. Selezionare una ricorrenza dall'elenco a discesa **Esegui oggetto**.
    c. Impostare le altre opzioni di pianificazione e i parametri in base alle esigenze.
    d. Fare clic su **Pianifica**.

    Il sistema pianifica l'aggiornamento e lo esegue in base alle informazioni di pianificazione specificate. È possibile visualizzare il prossimo aggiornamento pianificato per gli account di gruppo AD in "Opzioni gruppo AD".

16. Utilizzare le impostazioni dell'area "Aggiornamento AD su richiesta" per specificare gli elementi da aggiornare. È possibile selezionare una delle opzioni seguenti:
    - **Aggiorna gruppi AD ora**

      Selezionare questa opzione se si desidera aggiornare i gruppi AD. L'aggiornamento viene eseguito solo quando si fa clic su **Aggiorna**.

      Nota:
      Questa opzione ha effetto su qualsiasi aggiornamento pianificato del gruppo AD. 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 aggiornare il gruppo AD e gli alias utente. Gli aggiornamenti vengono eseguiti solo quando si fa clic su **Aggiorna**.

      Nota:
      Questa opzione ha effetto su qualsiasi aggiornamento pianificato del gruppo AD. I successivi aggiornamenti pianificati sono elencati in "Opzioni gruppo AD" e "Opzioni alias AD".

    - **Non aggiornare alias e gruppi AD ora**

      Se si fa clic su **Aggiorna**, non vengono aggiornati né gli alias utente né quelli gruppo.

Nota:
questa opzione ha effetto su qualsiasi aggiornamento di gruppo o alias pianificato. I successivi aggiornamenti pianificati sono elencati in "Opzioni gruppo AD" e "Opzioni alias AD".

17. Fare clic su **Aggiorna**.
18. Fare clic su **OK**.

Argomenti correlati

- Single Sign On con Windows AD
- Utilizzo di Windows AD con SiteMinder
- Utilizzo dell'autenticazione Windows AD con Kerberos

7.4.5 Risoluzione dei problemi relativi all'autenticazione Windows AD

7.4.5.1 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

7.4.5.1.1 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
```

7.4.5.1.2 Per verificare la configurazione di Kerberos Java

- 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.

```
<Install Directory>\SAP Business Objects 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
```

Se il problema persiste, controllare che il dominio e il nome principale di servizio immessi corrispondano esattamente a quanto impostato in Active Directory.

7.4.5.1.3 Errore di accesso dovuto a nomi AD UPN e SAM diversi

L'ID di Active Directory di un utente è stato correttamente mappato nella 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.

7.4.5.1.4 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.

7.5 Autenticazione SAP

7.5.1 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 i nomi utente e le password SAP, senza memorizzare le password nella piattaforma BI. Consente inoltre di preservare le informazioni sui ruoli dell'utente in SAP e utilizzare queste informazioni sul ruolo nella piattaforma per assegnare i diritti per l'esecuzione delle attività amministrative o accedere al contenuto.

Accesso all'applicazione di autenticazione SAP

Dopo avere installato l'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 funzione 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 nome utente e la password SAP. Inoltre, la piattaforma BI può convalidare i ticket di accesso Enterprise Portal nei sistemi SAP.
- Consente di mappare i ruoli da SAP nella piattaforma BI per facilitare la creazione di account e consente 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.

7.5.2 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 i dati di autorizzazione del nuovo ruolo impostando questi 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)	*
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)	* **Nota:** per maggiore sicurezza, si consiglia di elencare esplicitamente i gruppi di utenti i cui membri richiedono l'accesso alla piattaforma BI.

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.

7.5.3 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.

7.5.3.1 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

7.5.3.2 Per verificare l'aggiunta corretta di un sistema di autorizzazione

1. Fare clic sulla scheda **Importazione ruoli**.
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.

7.5.3.3 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 **Autorizzazione**.
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**.

7.5.4 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

7.5.4.1 Per impostare le opzioni di autenticazione SAP

1. Passare all’area di gestione "Autenticazione" della CMC.
2. Fare doppio clic sulla scheda **SAP** e quindi sulla scheda **Opzioni**.
3. Se necessario, esaminare e modificare le impostazioni:

Impostazione	Descrizione
Abilita autenticazione SAP	Deselezionare questa casella di controllo se si desidera disabilitare completamente l'autenticazione SAP. Per disabilitare l'autenticazione SAP per specifici sistemi SAP, selezionare la casella **Disattivato** del sistema nella scheda **Sistemi di autorizzazione**.
Radice cartella contenuti	Utilizzare questo campo per specificare dove si desidera che la piattaforma BI inizi a replicare la struttura delle cartelle BW nella CMC e in BI Launch Pad. Il valore predefinito è `/SAP/2.0` ma è possibile selezionare una cartella differente, se necessario. Per modificare questo valore, è necessario cambiarlo sia nella CMC che nell'area di lavoro per l'amministrazione dei contenuti.
Sistema predefinito	In questo elenco selezionare il sistema di autorizzazione SAP che la piattaforma BI utilizza per impostazione predefinita (cioè il sistema che viene contattato per autenticare gli utenti che tentano di accedere con credenziali SAP ma senza specificare un sistema SAP particolare). **Nota:** Se si specifica un sistema predefinito, gli utenti di tale sistema non devono immettere il client e 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 potrà accedere come user1 quando viene scelta l'autenticazione SAP.
Numero massimo di tentativi di accesso non riusciti al sistema di autorizzazione	

Impostazione	Descrizione
	Digitare il numero di tentativi che la piattaforma deve effettuare per tentare di contattare un sistema SAP per soddisfare le richieste di autenticazione. 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. **Nota:** utilizzare questa impostazione insieme a **Mantieni disabilitato sistema di autorizzazione [secondi]** per configurare il modo in cui la piattaforma BI gestisce i sistemi di autorizzazione SAP che temporaneamente non disponibili. Il sistema utilizza queste impostazioni per determinare quando interrompere la comunicazione con un sistema SAP che non è disponibile e quando riprendere la comunicazione con tale sistema.
Mantieni disabilitato sistema di autorizzazione [secondi]	Digitare il numero di secondi che la piattaforma BI deve attendere prima di riprovare ad autenticare gli utenti nel sistema SAP. Se ad esempio si digita 3 nel campo **Numero max. accessi al sistema di autorizzazione non riusciti**, la piattaforma BI consente al massimo tre tentativi mancati di autenticazione degli utenti in un dato sistema SAP. Al quarto tentativo non riuscito, la piattaforma smette di provare ad autenticare gli utenti in tale sistema per il periodo di tempo specificato.
Numero max connessioni simultanee per sistema	Utilizzare questo campo per specificare quante connessioni devono restare contemporaneamente aperte con il sistema SAP. Se ad esempio si digita 2 in questo campo, la piattaforma BI mantiene aperte due connessioni separate a SAP.
Numero di utenti per connessione	Utilizzare questo campo per specificare quante operazioni consentire per ogni connessione al sistema SAP. Se ad esempio si specifica 2 per **Numero max. connessioni simultanee per sistema** e 3 per **Numero di utilizzi per connessione**, una volta raggiunti i tre accessi di una connessione, la piattaforma BI chiude e riavvia la connessione.

Impostazione	Descrizione
Visualizzatore BI e **Analista BI**	Utilizzare queste opzioni per specificare se i nuovi account utente verranno configurati con i ruoli utente Visualizzatore BI o Analista BI. Il ruolo Visualizzatore BI viene generalmente assegnato agli utenti che sono consumer di contenuto. Questo ruolo ha accesso limitato ai workflow dell'applicazione, in base a quanto stipulato nell'accordo di licenza della piattaforma SAP BusinessObjects Business Intelligence. Il ruolo Analista BI è destinato agli utenti che creano e modificano il contenuto per le applicazioni della piattaforma. Questo ruolo non ha limitazioni di accesso ai workflow dell'applicazione. **Nota:** 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.

Impostazione	Descrizione
Utenti simultanei e **Utenti specifici**	Utilizzare queste opzioni per specificare se i nuovi account utente sono configurati in modo tale da utilizzare le licenze degli utenti simultanei o degli utenti designati. Le licenze di accesso simultaneo specificano quanti utenti 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. 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. **Nota:** 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.
Importa nome completo e indirizzo di posta elettronica	Selezionare questa opzione se si desidera specificare un livello di priorità per il plug-in di autenticazione SAP. I nomi completi e le descrizioni utilizzati negli account SAP vengono importati e memorizzati con gli oggetti utente nella piattaforma BI.
Imposta priorità collegamento attributi SAP relativo ad altri collegamenti attributi.	Specifica una priorità per il collegamento degli attributi utente SAP (nome completo e indirizzo di posta elettronica). Se l'opzione è impostata su "1", gli attributi SAP hanno la priorità in scenari in cui sono abilitati SAP e altri plug-in (Windows AD e LDAP). Se è impostata su "3", avranno la priorità gli attributi di altri plug-in abilitati.

I campi che seguono consentono di 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	Questo pulsante consente di caricare il file archivio chiavi generato per abilitare il servizio Single Sign-On SAP. È inoltre possibile immettere manualmente il percorso completo del file nel campo fornito.
"Password archivio chiavi"	Specificare la password richiesta per l'accesso al file dell'archivio chiavi.
"Password chiave privata"	Specificare la password richiesta per l'accesso al certificato corrispondente al file dell'archivio chiavi. Il certificato è archiviato nel sistema SAP
"Alias chiave privata"	Specificare l'alias richiesto per l'accesso al file dell'archivio chiavi.

4. Fare clic su **Aggiorna**.

Argomenti correlati

- Licenze basate sul ruolo
- Configurazione dell'autenticazione SAP

7.5.4.2 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/`.

7.5.5 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 quegli 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 **visua lizzazione**, **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

7.5.5.1 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 **Visualizzatore BI**, **Analista BI**,**Utenti simultanei** oppure **Utenti specifici** a seconda dell'accordo di licenza.

   Si noti che 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 ruoli**, 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**.

7.5.5.2 Verifica della corretta importazione di ruoli e utenti

1. Assicurarsi di conoscere il nome utente e la password di un utente SAP che appartiene a uno dei ruoli appena mappati nella piattaforma BI.
2. 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 numero del server Web, il numero di porta o l'URL esatto per accedere.
3. Nell'elenco **Tipo autenticazione** selezionare **SAP**.
4. Digitare il sistema SAP e il client di sistema a cui si desidera accedere.
5. Digitare il nome utente e la password di un utente mappato.
6. Fare clic su **Accedi**.

   È necessario essere connessi a BI Launch Pad come l'utente selezionato.

7.5.5.3 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.

7.5.5.3.1 Pianificazione degli aggiornamenti per i ruoli SAP

Una volta mappati i ruoli nella piattaforma BI, è necessario specificare il modo in cui il sistema li aggiorna.

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.

Schema ricorrente	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.

Schema ricorrente	Descrizione
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".

7.5.6 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. Si

consiglia di seguire le istruzioni contenute nella sezione relativa alla *configurazione dell'attendibilità lato server in SAP* nel capitolo *Configurazioni supplementari per gli ambienti ERP* di questo manuale.

7.5.6.1 Panoramica dell'attendibilità lato server SAP

Questa sezione include le procedure per la configurazione dell'attendibilità lato server tra SAP Web Application Server (versione 6.20 e superiori) e la piattaforma BI. 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 il 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 bursting di report utilizzando le credenziali SNC, ad esempio Crystal Reports Job Server.

Inoltre, è necessario disporre di una libreria di crittografia per configurare l'attendibilità lato server. Sul sito Web SAP è disponibile per il download una libreria di crittografia SAP. 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 dei certificati che dimostrano l'identità l'uno all'altro. 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). Questa documentazione descrive 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 in effetti configurato nella transazione `SNC0` di modo che sia possibile 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 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
	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
Web Intelligence Processing Server	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`.

7.5.6.2 Configurazione SAP per l'attendibilità lato server

La procedura seguente descrive come impostare SNC per l'utilizzo con la piattaforma BI. Per ulteriori informazioni o per assistenza per la risoluzione dei problemi, è possibile consultare la documentazione SAP fornita con il server SAP.

7.5.6.2.1 Per configurare l'attendibilità lato server SAP

1. Dal sito Web SAP, scaricare la libreria di crittografia SAP per tutte le piattaforme pertinenti.

   Nota:
   Per ulteriori informazioni sulla libreria di crittografia, consultare le note SAP 711093, 597059 e 397175 sul sito Web SAP.

2. 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.
3. Sul computer SAP, copiare la libreria di crittografia SAP e lo strumento SAPGENPSE nella directory `<UNITÀ>:\usr\sap\<SID>\SYS\exe\run\` (in Windows).
4. Individuare il file denominato "ticket" installato con la libreria di crittografia SAP e copiarlo nella directory `<UNITÀ>:\usr\sap\<SID>\<istanza>\sec\` (in Windows).
5. 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**.

6. Nella GUI SAP, passare alla transazione RZ10 modificare il profilo di istanza nella modalità di **gestione estesa**.
7. 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:
   tenere presente che 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.

8. 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

9. Riavviare l'istanza SAP.
10. 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.
11. 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.
12. Fare clic su **OK**.
13. 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.
14. Salvare le modifiche.

    Nota:
    se le modifiche on vengono salvate, il server di applicazioni non verrà avviato nuovamente quando si abilita l'SNC.
15. 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_cpic	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_in secure_cpic impostati su (1) garantiscono che i precedenti metodi per le comunicazioni (potenzialmente non sicuri) sono ancora consentiti.

16. Riavviare il sistema SAP.

È ora necessario configurare la piattaforma BI per l'attendibilità lato server.

7.5.6.3 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

7.5.6.3.1 Per impostare l'ambiente

Prima di iniziare, verificare che:

- La libreria di crittografia SAP sia stata scaricata e 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`
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.
6. Copiare il file `ticket` dalla libreria di crittografia SAP alla cartella sec.

Argomenti correlati

- Configurazione SAP per l'attendibilità lato server

7.5.6.3.2 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 SNC.
   Verrà richiesta la password assegnata.
5. Importare il file *CertBOE.crt* precedentemente creato:

   I certificati SAPGENPSE hanno la codifica Base64. Quando vengono importati, selezionare Base64:
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. Per aggiungere un certificato SAP al PSE della piattaforma BI fare doppio clic su di esso.
8. Salvare le modifiche in STRUST.
9. 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.
10. Passare alla transazione SNC0.
11. 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:
12. 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 son scambiati 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

7.5.6.3.3 Configurazione dei server della piattaforma BI

Dopo aver generato un PSE per la piattaforma BI, è necessario configurare un 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.

7.5.6.3.4 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\hareskoug\Desktop\sapcrypto.x86\ntintel>sapgenpse.exe
maintain_pk -l
 maintain_pk for PSE "C:\Documents and Settings\hareskoug\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\hareskoug\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 -O per specificare tale accesso. Ad esempio, per consentire l'accesso al PSE ad un utente specifico in un determinato dominio, digitare:

```
sapgenpse seclogin -p SBOE.pse -O <domain\user>
```

7.5.6.3.5 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)**.
6. Specificare il percorso della libreria SNC in **Percorso della libreria SNC**.

   Nota:
   Questa procedura è necessaria anche se la libreria è già definita nella variabile di ambiente *SNC_LIB*.

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. Utilizzando la libreria di crittografia SAP, il nome distinto consigliato è quello che segue le convenzioni di assegnazione dei nomi LDAP. È necessario che abbia "p:" come prefisso.

9. Verificare che il nome SNC delle credenziali sotto cui vengono eseguiti i server della piattaforma BI venga visualizzato nel campo **Nome SNC del sistema Enterprise**.

   Nota:
   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.

7.5.6.3.6 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 Interactive Analysis. Eliminare i server duplicati dal SIA di origine. Non è necessario creare gruppi di server ma meno server hanno accesso a PSE.
3. Creare un SIA esclusivamente per SAP con accesso a PSE. Aggiungerlo ai server di elaborazione Crystal Reports o Web Intelligence. In questi server deve essere eseguito solo il contenuto SAP e soprattutto il contenuto SAP deve essere 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
- Publication Server
- Destination 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 contenuito e il gruppo di server non SAP.

7.5.6.4 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.

7.5.6.5 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

7.5.6.6 Configurazione delle impostazioni SNC nella Central Management Console

Per potere configurare le impostazioni SNC, è necessario aggiungere un nuovo sistema di autorizzazione nella piattaforma BI. È inoltre necessario copiare il file della libreria SNC in una directory conosciuta e creare una variabile di ambiente `RFC_LIB` associata a questo 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)**.
4. Specificare il percorso della libreria SNC in **Percorso della libreria SNC**.

   Nota:
   Il server di applicazioni e il server CMS devono trovarsi sullo stesso tipo di sistema operativo con lo stesso percorso della libreria crypto.

5. 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.

6. Immettere il nome SNC del sistema SAP in **Impostazioni autenticazione reciproca**.

   Il formato del nome SNC dipende dalla libreria SNC. Utilizzando la libreria di crittografia SAP, il nome distinto consigliato è quello che segue le convenzioni di assegnazione dei nomi LDAP. È necessario che abbia "p:" come prefisso.

7. Verificare che il nome SNC delle credenziali sotto cui vengono eseguiti i server della piattaforma BI venga visualizzato nel campo **Nome SNC del sistema Enterprise**.

   Nota:
   in scenari in cui vengono configurati diversi nomi SNC, è necessario lasciare vuoto questo campo.

8. Fare clic su **Aggiorna**.
9. Fare clic sulla scheda **Sistemi di autorizzazione** nella pagina di autenticazione SAP.
10. È ora disponibile un altro campo sotto il campo **Lingua** denominato **nome SNC**.
11. Nel campo facoltativo **Nome SNC**, digitare 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 fosse considerata attendibile.

Argomenti correlati

- Connessione ai sistemi di autorizzazione SAP

7.5.6.7 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 4.
5. Fare clic su **Salva**.

7.5.6.8 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**.

7.5.7 Impostazione di Single Sign On nel sistema SAP

Per abilitare 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 SAP ABAP BW e alla piattaforma BI utilizzando la CMC.

Nota:
per poter impostare il Single Sign On nel database SAP, è necessario configurare il plug-in dell'autenticazione SAP.

7.5.7.1 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.

7.5.7.2 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.

7.5.7.3 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.

7.5.7.4 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`

7.5.7.5 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**.

   Viene visualizzato l'elenco dei server in "Servizi principali".

3. Fare clic con il pulsante destro del mouse su Adaptive Processing Server e scegliere **Interrompi**.
   Non continuare fino a quando lo stato del server viene contrassegnato come "Interrotto".
4. Fare clic con il pulsante destro del mouse su Adaptive Processing Server e scegliere **Seleziona servizi**.
   Viene visualizzata la finestra di dialogo "Seleziona servizi".
5. Spostare Servizio token di protezione dall'elenco dei servizi disponibili all'elenco "Servizi" a destra.
   Utilizzare il pulsante **Aggiungi alla selezione** per spostare la selezione.
6. Fare clic su **OK**.
7. Riavviare l'Adaptive Processing Server.

7.5.8 Configurazione di SSO per SAP Crystal Reports e SAP NetWeaver

Per impostazione predefinita, la piattaforma BI verrà configurata per consentire agli utenti di SAP Crystal Reports di accedere ai dati SAP mediante il Single Sign On (SSO).

7.5.8.1 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.

7.5.8.2 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.

7.6 Autenticazione PeopleSoft

7.6.1 Presentazione

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.

7.6.2 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.

7.6.2.1 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 **Sistemi**.
6. Fare clic sulla scheda **Server**.
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.

7.6.3 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.

7.6.3.1 Mappatura di un ruolo PeopleSoft alla piattaforma BI

1. Eseguire l'accesso alla Central Management Console come amministratore,
2. quindi 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. Per attivare la sincronizzazione di utenti e gruppi tra la piattaforma BI e PeopleSoft, selezionare la casella di controllo **Imponi sincronizzazione dell'utente**. Per rimuovere i gruppi PeopleSoft già importati dalla piattaforma BI, lasciare deselezionata la casella di controllo **Imponi sincronizzazione dell'utente**.
7. 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 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**, 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. 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.

   Se la licenza della piattaforma SAP BusinessObjects Business Intelligence di cui si dispone si basa sui ruoli utente, selezionare una delle opzioni seguenti:
   - **I nuovi utenti vengono creati come Visualizzatore BI**

     I nuovi account utente vengono configurati con il ruolo Visualizzatore BI. L'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Visualizzatore BI è definito nel contratto di licenza. Gli utenti potranno accedere ai workflow delle applicazioni in base a quanto previsto dal ruolo Visualizzatore BI. I diritti di accesso generalmente sono limitati alla visualizzazione dei documenti business intelligence. Questo ruolo è di norma adatto agli utenti che utilizzano contenuti mediante le applicazioni della piattaforma BI.

   - **I nuovi utenti vengono creati come Analista BI** I nuovi account utente vengono configurati con il ruolo Analista BI. L'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Analista BI è definito nel contratto di licenza. Gli utenti possono accedere a tutti i workflow delle applicazioni definiti per il ruolo Analista BI. I diritti di accesso includono la visualizzazione e la modifica dei documenti business intelligence. Questo ruolo è di norma adatto agli utenti che creano e modificano contenuti per le applicazioni della piattaforma BI.

   Se la licenza della piattaforma SAP BusinessObjects Business Intelligence di cui si dispone non si basa sui ruoli utente, selezionare una delle opzioni seguenti:
   - **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 vengono visualizzati come gruppi nella piattaforma BI.

7.6.3.2 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.

7.6.3.3 Per eliminare la mappatura di un ruolo

1. Eseguire l'accesso alla Central Management Console come amministratore,
2. quindi 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.

7.6.4 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.

7.6.4.1 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.

Schema ricorrente	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".

7.6.5 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 nella piattaforma BI.

7.6.5.1 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 avere importato le impostazioni, vedere la sezione Gestione delle impostazioni di protezione.

7.6.5.1.1 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 diritti di 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 gruppo, è possibile configurare Ponte di protezione in modo da non eseguire l'aggiornamento delle impostazioni di protezione per alcuni utenti rimuovendo semplicemente 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 ai dati mediante questi universi, il cui accesso è impossibile da PeopleSoft EPM.

7.6.5.1.2 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:

   - Solitamente, l'SDK di PeopleSoft EPM si trova nel server PeopleSoft in <PS_HOME>/class/com.peoplesoft.epm.pf.jar.
   - In genere l'SDK della piattaforma BI si torva 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 database.
Numero di porta	Il numero della porta per accedere al server.
Posizione classe	Posizione dei file di classe del driver di database.
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.

    La finestra di dialogo visualizza 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”.

7.6.5.2 Applicazione delle impostazioni di protezione

Per applicare le impostazioni di protezione, eseguire il file `crpsepmsecuritybridge.bat (in Windows) o il file crpsempsecuritybridge.sh` (in UNIX) e utilizzare il file di risposta creato come argomento. Ad esempio, digitare `crpsepmsecuritybridge.bat` (Windows) o `crpsempsecuritybridge.sh` (UNIX) `myresponsefile.properties`.

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..

7.6.5.2.1 Considerazioni sulla mappatura

In modalità di esecuzione, Ponte di protezione crea un utente nella piattaforma BI per ogni 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 nella piattaforma BI mediante il plug-in di protezione PeopleSoft, consentendo così agli utenti di accedere utilizzando le credenziali PeopleSoft.

7.6.5.3 Gestione delle impostazioni di protezione

È possibile gestire le impostazioni di protezione applicate modificando gli oggetti gestiti da Ponte di protezione.

7.6.5.3.1 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 a un 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 sia membro di un ruolo PeopleSoft gestito e del gruppo della piattaforma BI gestito.

- Ponte di protezione crea account e assegna casualmente 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 nella piattaforma BI mediante il plug-in di protezione PeopleSoft, in modo da consentire agli utenti di accedere alla piattaforma BI.
- Per i membri sia di ruoli PeopleSoft che di 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 nonaggiorna 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 efficiente per la gestione della protezione: rimuovendo gli utenti dal gruppo della piattaforma BI gestito, è possibile configurare le loro 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 nella 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.

7.6.5.3.2 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.

7.6.5.4 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 '\:').

7.6.5.4.1 Parametri del file di risposta

La seguente tabella contiene una descrizione dei parametri inclusi nel file di risposta:

Parametro	Descrizione
classpath	Il percorso della classe per il caricamento dei file .jar necessari. Più percorsi devono essere separati da un ';' sia in Windows che in UNIX. Sono necessari i percorsi di classe per i file `com.peoplesoft.epm.pf.jar` e per i file .jar del driver JDBC.
db.driver.name	Il nome del driver JDBC utilizzato per connettersi al database PeopleSoft (ad esempio, com.microsoft.jdbc.sqlserver.SQLServerDriver).
db.connect.str	La stringa di connessione JDBC utilizzata per connettersi al database PeopleSoft (ad esempio, jdbc:microsoft:sqlserver://vanrdpsft01:1433;DatabaseName=PRDMO).
db.user.name	Il nome utente utilizzato per accedere al database PeopleSoft.
db.password	La password utilizzata per accedere al database PeopleSoft.

Parametro	Descrizione
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.
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.

Parametro	Descrizione
peoplesoft.role.n	L'elenco dei ruoli PeopleSoft gestiti. Per ulteriori informazioni consultare Definizione degli oggetti gestiti. *n* è un numero intero e ciascuna voce occupa una proprietà con il prefisso peoplesoft.role. **Nota:** *n* è a base 1. È possibile utilizzare '*' per identificare tutti ruoli PeopleSoft disponibili, stabilito che n è 1 ed è l'unica proprietà con il prefisso peoplesoft.role nel file di risposta.
mapped.universe.n	L'elenco degli universi che si desidera aggiornare tramite la funzione Ponte di protezione. Per ulteriori informazioni consultare Definizione degli oggetti gestiti. *n* è un numero intero e ciascuna voce occupa una proprietà con il prefisso mapped.universe. **Nota:** *n* è a base 1. È possibile utilizzare '*' per identificare tutti gli universi disponibili, stabilito che n è 1 ed è l'unica proprietà con il prefisso mapped.universe nel file di risposta.
log4j.appender.file.File	Il file di registro scritto dalla funzione Ponte di protezione.

Parametro	Descrizione
log4j.*	Le proprietà log4j predefinite necessarie per il funzionamento corretto di log4j: log4j.rootLogger=INFO, file, stdout log4j.appender.file=org.apache.log4j.RollingFileAppender log4j.appender.file.layout=org.apache.log4j.PatternLayout log4j.appender.file.MaxFileSize=5000KB log4j.appender.file.MaxBackupIndex=100 log4j.appender.file.layout.ConversionPattern=%d [%-5] %c{1} - %m%n log4j.appender.stdout=org.apache.log4j.ConsoleAppender log4j.appender.stdout.layout=org.apache.log4j.PatternLayout log4j.appender.stdout.layout.ConversionPattern=%d [%-5] %c{1} - %m%n
peoplesoft classpath	Il percorso della classe per i file .jar API di PeopleSoft EPM. Questo parametro è facoltativo.
enterprise.classpath	Il percorso della classe per i file .jar SDK della piattaforma BI. Questo parametro è facoltativo.

Parametro	Descrizione
db.driver.type	Il tipo di database PeopleSoft. Questo parametro potrebbe assumere uno dei seguenti valori: Microsoft SQL Server 2000 Oracle Database 10.1 DB2 UDB 8.2 Fixpack 7 Personalizzato Il valore Custom può essere utilizzato per specificare i database, oltre che per distinguerne i tipi o le versioni. Questo parametro è facoltativo.
sql.db.class.location sql.db.host sql.db.port sql.db.database	La posizione dei file .jar del driver JDB, il computer host SQL Server, la porta SQL Server e il nome del database SQL Server. Questi parametri possono essere utilizzati solo se db.driver.type corrisponde a Microsoft SQL Server 2000. Questi parametri sono facoltativi.
oracle.db.class.location oracle.db.host oracle.db.port oracle.db.sid	La posizione dei file .jar del driver JDBC Oracle, il computer host Oracle, la porta e il SID del database Oracle. Questi parametri possono essere utilizzati solo se db.driver.type corrisponde a Oracle Database 10.1. Questi parametri sono facoltativi.
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.

Parametro	Descrizione
custom.db.class.location custom.db.drivername 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.

7.7 Autenticazione JD Edwards

7.7.1 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.

7.7.2 Abilitazione dell'autenticazione JD Edwards EnterpriseOne

Per fare in modo che nella piattaforma BI vengano utilizzate le informazioni di JD Edwards EnterpiseOne, è necessario configurare l'applicazione per l'autenticazione nel sistema JD Edwards EnterpriseOne.

7.7.2.1 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". Nella pagina sono presenti quattro schede: **Opzioni**, **Server**, **Ruoli** e **Aggiornamento utente**.

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. 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.
8. 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**.
9. Fare clic su **Aggiorna** per salvare le modifiche.

7.7.3 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.

7.7.3.1 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.

   Se la licenza della piattaforma SAP BusinessObjects Business Intelligence di cui si dispone si basa sui ruoli utente, selezionare una delle opzioni seguenti:
   - **I nuovi utenti vengono creati come Visualizzatore BI**

     I nuovi account utente vengono configurati con il ruolo Visualizzatore BI. L'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Visualizzatore BI è definito nel contratto di licenza. Gli utenti potranno accedere ai workflow delle applicazioni in base a quanto previsto dal ruolo Visualizzatore BI. I diritti di accesso generalmente sono limitati alla visualizzazione dei documenti business intelligence. Questo ruolo è di norma adatto agli utenti che utilizzano contenuti mediante le applicazioni della piattaforma BI.
   - **I nuovi utenti vengono creati come Analista BI**

I nuovi account utente vengono configurati con il ruolo Analista BI. L'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Analista BI è definito nel contratto di licenza. Gli utenti possono accedere a tutti i workflow delle applicazioni definiti per il ruolo Analista BI. I diritti di accesso includono la visualizzazione e la modifica dei documenti business intelligence. Questo ruolo è adatto agli utenti che creano e modificano contenuti per le applicazioni della piattaforma BI.

Se la licenza della piattaforma SAP BusinessObjects Business Intelligence di cui si dispone non si basa sui ruoli utente, selezionare una delle opzioni seguenti:

- **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 quanti utenti 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 BI, 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 **Ruoli**.
8. In **Selezionare un server**, selezionare il server JD Edwards che contiene i ruoli da mappare.
9. In "Ruoli importati" selezionare i ruoli da mappare alla piattaforma BI e fare clic su **<**.
10. Fare clic su **Aggiorna**.

    I ruoli verranno mappati alla piattaforma BI.

7.7.3.2 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.

7.7.3.3 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.

7.7.4 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.

7.7.4.1 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.

Schema ricorrente	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.

Schema ricorrente	Descrizione
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".

7.8 Autenticazione Siebel

7.8.1 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.

7.8.1.1 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.

7.8.2 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.

7.8.2.1 Mappatura di un ruolo Siebel eBusiness alla piattaforma BI

1. Eseguire l'accesso alla Central Management Console come amministratore,
2. quindi fare clic su **Autenticazione**.
3. Fare doppio clic su **Siebel eBusiness**.
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 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.
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 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.
6. 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:
   - **I nuovi utenti vengono creati come Visualizzatore BI**

     I nuovi account utente vengono configurati con il ruolo Visualizzatore BI. L'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Visualizzatore BI è definito nel contratto di licenza. Gli utenti potranno accedere ai workflow delle applicazioni in base a quanto previsto dal ruolo Visualizzatore BI. I diritti di accesso generalmente sono limitati alla visualizzazione dei documenti business intelligence. Questo ruolo è di norma adatto agli utenti che utilizzano contenuti mediante le applicazioni della piattaforma BI.
   - **I nuovi utenti vengono creati come Analista BI**

I nuovi account utente vengono configurati con il ruolo Analista BI. L'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Analista BI è definito nel contratto di licenza. Gli utenti possono accedere a tutti i workflow delle applicazioni definiti per il ruolo Analista BI. I diritti di accesso includono la visualizzazione e la modifica dei documenti business intelligence. Questo ruolo è di norma adatto agli utenti che creano e modificano contenuti per le applicazioni della piattaforma BI.

Se la licenza della piattaforma BI di cui si dispone non si basa sui ruoli utente, selezionare una delle opzioni seguenti:

- **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.

7. Fare clic sulla scheda **Ruoli**.
8. Selezionare il dominio che corrisponde al server Siebel per il quale si desidera mappare i ruoli.
9. 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**.

10. Fare clic su **Aggiorna**.

    I ruoli verranno mappati nella piattaforma BI.

7.8.2.2 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 esclusivamente 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.

7.8.2.3 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.

7.8.3 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.

7.8.3.1 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.

Schema ricorrente	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.

Schema ricorrente	Descrizione
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".

7.9 Autenticazione Oracle EBS

7.9.1 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.

7.9.1.1 Abilitazione dell'autenticazione 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**.

   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

7.9.2 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 vengono utilizzati 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 l'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.

7.9.2.1 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:
   - **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 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.
   - **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 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**.

   Se la licenza della piattaforma SAP BusinessObjects Business Intelligence di cui si dispone si basa sui ruoli utente, selezionare una delle opzioni seguenti:
   - **I nuovi utenti vengono creati come Visualizzatore BI**

     I nuovi account utente vengono configurati con il ruolo Visualizzatore BI. L'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Visualizzatore BI è definito nel contratto di licenza. Gli utenti potranno accedere ai workflow delle applicazioni in base a quanto previsto dal

ruolo Visualizzatore BI. I diritti di accesso generalmente sono limitati alla visualizzazione dei documenti business intelligence. Questo ruolo è di norma adatto agli utenti che utilizzano contenuti mediante le applicazioni della piattaforma BI.

- **I nuovi utenti vengono creati come Analista BI**

  I nuovi account utente vengono configurati con il ruolo Analista BI. L'accesso alle applicazioni della piattaforma BI per tutti gli account con ruolo Analista BI è definito nel contratto di licenza. Gli utenti possono accedere a tutti i workflow delle applicazioni definiti per il ruolo Analista BI. I diritti di accesso includono la visualizzazione e la modifica dei documenti business intelligence. Questo ruolo è adatto agli utenti che creano e modificano contenuti per le applicazioni della piattaforma BI.

Se la licenza della piattaforma SAP BusinessObjects Business Intelligence di cui si dispone non si basa sui ruoli utente, selezionare una delle opzioni seguenti:

- **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 quanti utenti 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. Selezionare **Imponi sincronizzazione utente** per sincronizzare le informazioni dell'account utente Oracle EBS quando si fa clic su **Aggiorna** nella scheda **Responsabilità**.
9. In **Servizi Oracle EBS correnti**, selezionare il servizio Oracle EBS che contiene i ruoli da mappare.
10. 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.
11. Fare clic su **Aggiorna**.

    I ruoli verranno mappati alla piattaforma BI.

Una volta mappati i ruoli nella piattaforma BI, è necessario specificare in che modo vengono aggiornati dal sistema.

Argomenti correlati

- Licenze basate sul ruolo

7.9.2.1.1 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.

7.9.2.1.2 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.

Schema ricorrente	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".

7.9.3 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.

7.9.3.1 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** o **Ruoli**.
5. Selezionare il ruolo di destinazione dall'area **Ruoli importati** e fare clic su **<** o **Elimina** per rimuoverli.
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.

7.9.4 Personalizzazione dei diritti per gruppi e utenti Oracle EBS mappati

Quando si mappano ruoli nella piattaforma BI, è possibile impostare i diritti o concedere autorizzazioni per i gruppi e gli utenti creati.

7.9.4.1 Per assegnare i diritti di amministrazione

Per consentire agli utenti di gestire la piattaforma BI, è necessario renderli membri del gruppo predefinito dell'amministratore. 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 console CMC (Central Management Console) come amministratore.
2. Dall'area "Organizza", fare clic su **Utenti**.
3. Nella colonna **Nome**, fare clic su **Amministratori**.
4. Fare clic su **Elenco gruppi**, quindi nell'elenco Azioni, fare clic su **Aggiungi**.

Viene visualizzata la pagina Utenti/gruppi disponibili.

5. Dall'area **Elenco utenti** o **Elenco gruppi**, selezionare il ruolo mappato al quale si desidera concedere diritti amministrativi.
6. Fare clic su **>** per rendere il ruolo un sottogruppo del gruppo Administrators, quindi fare clic su **OK**.

Ora i membri del ruolo dispongono di diritti di amministrazione nella piattaforma BI.

Nota:
È anche possibile creare un ruolo in Oracle EBS, aggiungere gli utenti appropriati al ruolo, mappare il ruolo nella piattaforma BI e rendere il ruolo mappato un sottogruppo del gruppo predefinito dell'amministratore, concedendo così i diritti amministrativi ai membri del ruolo.

7.9.4.2 Per assegnare i diritti di pubblicazione

Se il sistema utilizzato dispone di utenti nominati come creatori di contenuti all'interno dell'organizzazione, è possibile concedere loro delle 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/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, fare clic su **Rimuovi accesso**.

7.9.5 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).

7.9.5.1 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. Riavviare SAP Crystal Reports.

7.9.5.2 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" digitare **crdb_oraapps**.
5. Fare clic su **Aggiungi**.
6. Fare clic su **Salva e chiudi**.
7. Riavviare SAP Crystal Reports.

Amministrazione del server

8.1 Amministrazione del server

8.1.1 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.

Opzione dell'albero di spostamento	Descrizione
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.
Categorie di servizio	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: • **Servizi di connessione** • **Servizi principali** • **Servizi Crystal Reports** • **Servizi Data Federation** • **Servizi Lifecycle Management** • **Servizi Analysis** • **Servizi Web Intelligence** • **Servizi Dashboard Design** Selezionare una categoria di servizio nell'elenco di navigazione per visualizzare o gestire i relativi server. **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.

Opzione dell'albero di spostamento	Descrizione
Stato server	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: • **Interrotto** • **Avvio in corso** • **Inizializzazione in corso** • **In esecuzione** • **Interruzione** • **Avviato con errori** • **Terminato in errore** • **In attesa delle risorse**

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.

Colonna del riquadro Dettagli	Descrizione
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: • **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.
Stato	Indica lo stato generale del server.
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

8.1.2 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

8.1.3 Gestione dei server in UNIX

Il file eseguibile `ccm.sh` consente di avviare, arrestare, riavviare, abilitare e disabilitare i server nella distribuzione Windows mediante la riga di comando.

Argomenti correlati

- ccm.sh

8.1.4 Gestione delle chiavi di licenza

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

Argomenti correlati

- Per visualizzare le informazioni sulle licenze
- Per aggiungere un codice di licenza
- Per visualizzare l'attività dell'account corrente

8.1.4.1 Per visualizzare le informazioni sulle licenze

L'area di gestione **Codice di licenza** della CMC identifica il numero di licenze basate su ruoli (Visualizzatore BI e Analista BI), ad accesso simultaneo, titolari e per processore 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

- Gestione delle chiavi di licenza
- Per aggiungere un codice di licenza
- Per visualizzare l'attività dell'account corrente

8.1.4.2 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.

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

- Per visualizzare le informazioni sulle licenze
- Per visualizzare l'attività dell'account corrente

8.1.4.3 Per visualizzare l'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

- Gestione delle chiavi di licenza
- Per aggiungere un codice di licenza
- Per visualizzare le informazioni sulle licenze

8.1.5 Misurazione delle licenze

BusinessObjects License Measurement Tool (BOLMT) è un'utilità Java della riga di comando che consente di raccogliere e archiviare i dati sulle licenze della piattaforma BI. Il documento XML di output contiene misure della distribuzione della licenza e viene inviato al servizio GLAS (Global License Auditing Services) di SAP per il consolidamento come parte di un controllo della licenza.

L'amministratore del sistema installa ed esegue BOLMT per ciascun cluster della piattaforma BI ogni volta che viene richiesto un controllo della licenza. BOLMT raccoglie le misure dell'utilizzo nelle licenze basate su ruolo, titolari e utente simultaneo.

L'amministratore può specificare una particolare directory di output per il documento XML e configurare il documento in modo tale che non contenga informazioni che possono essere utilizzate per identificare gli utenti del sistema.

8.1.5.1 Esecuzione di un controllo della licenza

Per eseguire un controllo della licenza, è necessario disporre dei diritti di amministratore e dell'accesso alla directory contenente il file `BOLMT.jar` nell'installazione della piattaforma BI.

1. Aprire una console della riga di comando.
2. Passare alla directory contenente gli eseguibili Java per l'installazione della piattaforma BI.

   Per impostazione predefinita, il file viene installato nella seguente directory: *[DIRINSTALLAZ]*`\SAP BusinessObjects Enterprise XI 4.0\java\lib`
3. Eseguire il file BOLMT.jar.

   Il comando di esecuzione viene immesso nel seguente formato: `-jar BOLMT.jar` [opzioni] <FileOutput>

   La tabella che segue contiene un riepilogo delle opzioni disponibili:

Opzione	Descrizione
-c --cms	Specifica l'identificatore del nome e il numero di porta per il Central Management Server (CMS). Specificato come *nomecms*:*numero porta*. Per impostazione predefinita, vengono utilizzate le impostazioni del CMS per l'host locale se questa impostazione non viene specificata.
-p --password	Specifica la password dell'account Administrator utilizzata per la connessione al server CMS.
-a--auth	Specifica il metodo di autenticazione per la connessione utente al server CMS. Il metodo predefinito è quello aziendale, specificato come `secEnterprise`.
-s--sanitize	Specifica che il documento di controllo generato deve filtrare tutte le informazioni personali che possono essere utilizzate per identificare gli utenti.

Nota:
la specificazione del file di output è sempre l'ultimo argomento della riga di comando. Questa impostazione è facoltativa. Se non viene specificato un argomento, il documento viene generato come output standard della console. È inoltre possibile inserire l'output in uno script come argomento della riga di comando.

Esempio:

```
C:\Program Files (x86)\SAP
Business Objects\SAP BusinessObjects Enterprise XI 4. 0\java\lib>"C:\Program Files
(x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin
\java.exe" -jar BOLMT.jar --cms=mycms:6400 -uAdministrator
-p=7juujg --auth=secEnterprise --sanitize audit.xml
```

8.1.6 Visualizzazione e modifica dello stato del server

8.1.6.1 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 SAP BusinessObjects Business Intelligence, 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 SAP BusinessObjects Business Intelligence. 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
- Avvio, arresto e riavvio dei server
- Abilitazione e disabilitazione dei server
- Arresto di Central Management Server
- Per avviare un server automaticamente

8.1.6.1.1 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** fornisce indicazioni sullo 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.

8.1.6.2 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 SAP BusinessObjects Business Intelligence prima di apportare modifiche a determinate proprietà e impostazioni.
Avvio di un server	Se si è eseguito l'arresto di un server per configurarlo, sarà necessario riavviarlo affinché le modifiche risultino effettive e per consentire al server di riprendere 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.
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

8.1.6.2.1 Per avviare, arrestare o riavviare i server con 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

8.1.6.2.2 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.

8.1.6.2.3 Per avviare un server automaticamente

Per impostazione predefinita, i server della distribuzione vengono avviati automaticamente all'avvio di Server Intelligence Agent. In questa procedura viene illustrato dove impostare questa opzione.

1. Passare all’area di gestione degli **Server** della CMC.
2. Fare doppio clic sul server che si desidera 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**, quindi fare clic su **Salva** oppure su **Salva e chiudi**.

   Nota:
   Se si deseleziona l'avvio automatico per tutti i server CMS nel cluster, è necessario utilizzare CCM per riavviare il sistema. 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, impostare Avvio automatico su Sì, quindi fare clic su Salva. Riavviare il SIA.

8.1.6.3 Arresto di Central Management Server

Se l'installazione della piattaforma SAP BusinessObjects Business Intelligence prevede più di un server CMS (Central Management Server) attivo, è possibile spegnere un singolo CMS senza perdere dati o influenzare la funzionalità del sistema. Un altro server CMS nel nodo acquisirà il carico di lavoro del server arrestato. Il clustering di più server CMS consente di eseguire la manutenzione sui singoli server CMS in sequenza senza interrompere la piattaforma SAP BusinessObjects Business Intelligence.

Tuttavia, se la distribuzione della piattaforma SAP BusinessObjects Business Intelligence prevede un solo server CMS, l'arresto di tale server impedirà agli utenti di utilizzare la piattaforma SAP BusinessObjects Business Intelligence e interromperà l'elaborazione di report e programmi. 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 SIA, ma prima di arrestare il 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 SAP BusinessObjects Business Intelligence, perché verranno arrestati anche tutti gli altri server nel nodo.

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 server CMS di un nodo e tutti i CMS non sono impostati per l'avvio automatico all'avvio del SIA, è necessario utilizzare CCM per riavviare il sistema. In CCM, fare clic con il pulsante destro del mouse sul SIA e scegliere Proprietà. Nella scheda Avvio, impostare Avvio automatico su Sì, quindi fare clic su Salva. Riavviare il SIA.

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

8.1.6.4 Abilitazione e disabilitazione dei server

Disabilitando un server della piattaforma SAP BusinessObjects Business Intelligence si evita che il server riceva e risponda a nuove richieste della piattaforma SAP BusinessObjects Business Intelligence, senza tuttavia arrestare 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.

8.1.6.4.1 Per abilitare e disabilitare i server con 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**.

8.1.6.4.2 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.

8.1.7 Aggiunta, duplicazione o eliminazione di server

8.1.7.1 Aggiunta, duplicazione ed eliminazione di server

Se si desidera aggiungere nuovi elementi hardware alla piattaforma SAP BusinessObjects Business Intelligence installando componenti server su nuovi computer supplementari, eseguire il programma di installazione della piattaforma SAP BusinessObjects Business Intelligence dalla distribuzione del prodotto. 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*.

8.1.7.1.1 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

- Servizi e server
- Configurazione delle impostazioni server
- Configurazione dei numeri di porta
- Visualizzazione dello stato dei server

8.1.7.1.2 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.

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, SAP BusinessObjects Enterprise è installato 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\`.

Nel computer B è presente una sola unità disco (non esiste l'unità D) e SAP BusinessObjects Enterprise è installato 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.

Per duplicare 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.

8.1.7.1.3 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**.

8.1.8 Cluster di Central Management Server

8.1.8.1 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 su cui è in esecuzione un CMS, un computer con un altro CMS continuerà a rispondere alle richieste della piattaforma SAP BusinessObjects Business Intelligence. Il supporto per l'alta disponibilità garantisce che gli utenti della piattaforma SAP BusinessObjects Business Intelligence possano comunque accedere alle informazioni in caso di problemi alle apparecchiature.

In questa sezione viene illustrato come aggiungere un nuovo membro del cluster CMS a un sistema di produzione già in funzione. Quando si aggiunge un nuovo CMS 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 gli altri computer CMS in uso. Per informazioni sul CMS corrente, accedere all'area di gestione Server della console 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 nel file `platforms.txt` incluso nella distribuzione del prodotto.

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 del database non è in grado di elaborare tali richieste in modo tempestivo, le prestazioni della piattaforma SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence (patch incluse, 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.
  - Verificare che ogni CMS utilizzi lo stesso client di database per la connessione 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.
  - Assicurarsi 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 impostate correttamente in ogni computer CMS (incluse le impostazioni dell'ora legale).
  - Assicurarsi che in tutti i server di applicazioni Web del cluster siano installati gli stessi file WAR. Per ulteriori informazioni sulla distribuzione dei file WAR, consultare il *Manuale di installazione della piattaforma SAP BusinessObjects Business Intelligence*.
- Accertarsi che ogni CMS in un cluster sia presente nella stessa rete LAN.
- Se il 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>` rappresenta il numero di server CMS 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 Righe di comando 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 specifico del primo CMS installato.

Argomenti correlati

- Modifica del nome di un cluster CMS

8.1.8.1.1 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:
Creare un backup del database di sistema CMS corrente e dei contenuti di Input e Output File Repository prima di apportare delle modifiche. Se necessario, contattare l’amministratore del database.

Argomenti correlati

- Aggiunta di un nuovo nodo a un cluster
- Aggiunta di un server
- Duplicazione di server
- Backup e ripristino del sistema

8.1.8.1.2 Aggiunta di un nuovo nodo a un cluster

Quando si aggiunge un nodo, viene richiesto di creare un nuovo CMS o di aggregare il nodo a 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 SAP BusinessObjects Business Intelligence nel 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, è possibile specificare il CMS esistente di cui si desidera espandere il sistema e selezionare i componenti da installare nel computer locale. In tal caso, specificare il nome del CMS in esecuzione nel sistema esistente, quindi scegliere di installare un nuovo CMS nel computer locale. Fornire le informazioni necessarie affinché il programma di installazione stabilisca la connessione al database CMS esistente. Quando il nuovo CMS viene installato nel computer locale, viene automaticamente aggiunto il server al cluster esistente.

Argomenti correlati

- Utilizzo dei nodi

8.1.8.1.3 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.

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.

   Se si utilizza il server di applicazioni Web Tomcat fornito con l'installazione della piattaforma SAP BusinessObjects Business Intelligence, è necessario accedere direttamente alla cartella seguente:

   ```
   C:\Programmi (x86)\SAP BusinessObjects\Tomcat6\webapps\BOE\WEB-INF\co
   nfig\custom\
   ```

   Suggerimento:
   se si utilizza un server di applicazioni Web che non consente l'accesso diretto alle applicazioni Web distribuite, è possibile utilizzare la cartella seguente nell'installazione del prodotto per modificare il file BOE.war.

`<DIRINSTALL>\Piattaforma SAP BusinessObjects Business Intelligence 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\`.

Successivamente sarà necessario ridistribuire il file BOE.war modificato.

2. Creare un nuovo file.

   Nota:
   utilizzare Blocco note o un'altra utilità per la modifica del testo.

3. Specificare le proprietà del cluster CMC.

   La proprietà `cms.clusters` consente di specificare tutti i cluster della distribuzione. Ciascun nome di cluster deve essere preceduto dal carattere `@` e i nomi devono essere separati tra loro da una virgola. 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:
   separare i nomi di CMS con una virgola. Il numero della porta è separato dal nome del CMS con i due punti e si suppone sia 6400 se non specificato. Ripetere la procedura per ogni cluster disponibile.

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*.

8.1.8.1.4 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 SAP BusinessObjects Business Intelligence, 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.

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.

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*.

8.1.9 Gestione di gruppi di server

I gruppi di server rappresentano un modo di organizzare i server della piattaforma SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence 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.

8.1.9.1 Creazione di un gruppo di server

Per creare un gruppo di server, è necessario specificare il nome e la descrizione del gruppo e aggiungervi, quindi, i server.

8.1.9.1.1 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

8.1.9.2 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.

8.1.9.2.1 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.

8.1.9.2.2 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**.

8.1.9.3 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.

8.1.9.3.1 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**.

8.1.9.4 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 al solo amministratore della piattaforma SAP BusinessObjects Business Intelligence. 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 del server della piattaforma SAP BusinessObjects Business Intelligence ad altre persone, oppure consentire a gruppi diversi dell'organizzazione di controllare la propria gestione server.

8.1.9.4.1 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**.

   Per informazioni sull'assegnazione di diritti, consultare il capitolo relativo all'impostazione dei diritti.

8.1.9.4.2 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

L'utente deve inoltre disporre dell'autorizzazione ad aggiungere oggetti ad almeno una cartella prima di poter salvare i nuovi report nella piattaforma SAP BusinessObjects Business Intelligence.

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.

8.1.10 Valutazione delle prestazioni del sistema

8.1.10.1 Monitoraggio dei server della piattaforma SAP BusinessObjects Business Intelligence

L'applicazione di monitoraggio fornisce la possibilità di acquisire le metriche cronologiche e di runtime dei server della piattaforma SAP BusinessObjects Business Intelligence per la creazione di report e la notifica. 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

8.1.10.2 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.

8.1.10.2.1 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

8.1.10.3 Visualizzazione delle specifiche del sistema

L'area di gestione "Impostazioni" della console CMC visualizza le metriche del sistema che forniscono informazioni generali sull'installazione della piattaforma SAP BusinessObjects Business Intelligence. 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.

8.1.10.3.1 Per visualizzare le specifiche del sistema

1. Passare all'area di gestione "Impostazioni" di CMC.
2. Fare clic sulle frecce per espandere e visualizzare le impostazioni nelle sezioni "Proprietà", "Visualizza le metriche di sistema globali" e "Cluster".

8.1.10.4 Registrazione dell'attività dei server

La piattaforma SAP BusinessObjects Business Intelligence consente di registrare informazioni specifiche sull'attività Web della piattaforma SAP BusinessObjects Business Intelligence.

- Inoltre, ciascuno dei server della piattaforma SAP BusinessObjects Business Intelligence è progettato per registrare messaggi nel registro di sistema standard del sistema operativo.
  - In Windows la piattaforma SAP BusinessObjects Business Intelligence esegue la registrazione nel servizio Registro eventi. È possibile visualizzare i risultati con il Visualizzatore eventi (nel Registro applicazione).
  - In UNIX la piattaforma SAP BusinessObjects Business Intelligence esegue la registrazione nel daemon syslog come applicazione utente. Ogni server aggiunte 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, a scopo di debug avanzato. Il percorso dei file di registro dipende dal sistema operativo:

- In Windows la directory di registrazione predefinita è `<DIRINSTALLAZ>\SAP BusinessObjects Enterprise XI 4.0\Logging`.
- In UNIX la directory di registrazione predefinita è `<DIRINSTALLAZ>/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 SAP BusinessObjects Business Intelligence, è necessario impostare e configurare la registrazione di sistema

in modo da registrare tutti i messaggi registrati nella funzionalità “user” a livello “info” o superiore. 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.

8.1.10.5 Configurazione di server nella console CMC per ottimizzare le prestazioni di pubblicazione

In genere, è possibile effettuare le operazioni seguenti per ottimizzare le prestazioni del server per la pubblicazione.

- Nell'area "Server" della CMC, disabilitare i server non necessari. Ad esempio, se si eseguono pubblicazioni solo di report Crystal, è possibile disabilitare i server Desktop Intelligence e Web Intelligence. Tuttavia, prima di effettuare tale operazione, verificare che i server da disabilitare non siano utilizzati da altri utenti nel sistema.
- Per i Job Server utilizzati nella pubblicazione, assicurarsi che **Numero max. processi simultanei** sia impostato su cinque per CPU. A tale scopo, nell'area "Server" selezionare il Job Server e fare clic su **Gestisci** > **Proprietà**.

Si consideri di modificare il livello di dettagli registrati da Adaptive Processing Server.

Nota:
L'aumento del livello di dettagli nei file di registro può avere effetti negativi sulle prestazioni del server.

L'impostazione predefinita e consigliata per il livello di dettagli nel file di registro è **ERRORE**. Può essere tuttavia preferibile aumentare il livello di dettagli nei file di registro di Adaptive Processing Server per tenere più agevolmente traccia dello stato dei processi di pubblicazione. A tale scopo, nell'area "Server" selezionare Adaptive Processing Server e fare clic su **Gestisci** > **Proprietà**. Nell'elenco "Livello di registrazione" selezionare **INFO**. L'opzione **INFO** offre più dettagli, ad esempio:

- La pubblicazione è stata consegnata a un destinatario.
- Un batch di destinatari è stato elaborato.
- Le estensioni di pubblicazione di post-elaborazione sono state inizializzate.

Configurare Adaptive Processing Server affinché gestisca più processi.

Per migliorare le prestazioni di Adaptive Processing Server adottare i seguenti suggerimenti:

- Se vengono eseguite più pubblicazioni contemporaneamente, creare più istanze di Adaptive Processing Server. In genere, è consigliabile disporre di un'istanza di Adaptive Processing Server ogni tre pubblicazioni simultanee.
- Aumentare le dimensioni di heap per Adaptive Processing server A tale scopo, fare clic su **Gestisci** > **Proprietà**, quindi aggiungere quanto segue al parametro della riga di comando: `-Xmx1024M`.
- Eseguire il servizio di pubblicazione e il servizio di post-elaborazione di pubblicazione su diverse istanze di Adaptive Processing Server.

Se l'autore della pubblicazione desidera attivare il controllo e l'eliminazione, configurare il controllo per il server CMS in modo che registri tutti i dettagli.

Per le pubblicazioni di grandi dimensioni, è consigliabile attivare l'eliminazione in modo da eliminare i file non necessari generati dal processo di pubblicazione e per conservare spazio sul server. A tale scopo, durante il processo di progettazione della pubblicazione, deselezionare il percorso predefinito di Enterprise come destinazione.

Se si attiva il controllo per la pubblicazione, è necessario configurare il server CMS affinché supporti questo scenario in modo che i dettagli dei file eliminati vengano comunque registrati. Nell'area "Server" selezionare il server CMS e fare clic su **Gestisci** > **Proprietà**. Nella finestra di dialogo che viene visualizzata, fare clic su **Eventi di controllo** nell'elenco di spostamento. Assicurarsi che le opzioni **Controllo abilitato** e **Oggetto eliminato** siano selezionate.

Assicurarsi che le impostazioni di posta elettronica siano state configurate correttamente in Destination Job Server.

Le pubblicazioni rivolte a destinazioni di posta elettronica potrebbero generare errori se la posta elettronica non viene configurata correttamente come destinazione per Destination Job Server. Nell'area "Server" della CMC, fare doppio clic su Destination Job Server. Nella finestra di dialogo "Proprietà", fare clic su **Destinazione** nell'elenco di spostamento per verificare quanto segue:

- Che **Posta elettronica** sia stata aggiunta come destinazione.
- Che i valori nei campi **Nome dominio**, **Host** e **Porta** siano corretti.
- Che il campo **A** contenga %SI_EMAIL_ADDRESS%.

Aumentare il numero di processi simultanei che è possibile elaborare in Destination Job Server.

Se le pubblicazioni sono destinate al percorso della piattaforma BI predefinito o a una destinazione di disco non gestito e si utilizzano dischi con striping per l'Output FRS, è consigliabile impostare il numero massimo di processi simultanei come il numero dei dischi moltiplicato per cinque.

Se l'autore della pubblicazione utilizza origini dei destinatari dinamici del report Crystal, verificare che Report Application Server (RAS) sia configurato correttamente.

Il RAS deve essere configurato in modo che possa leggere un numero di record di database che sia almeno uguale al numero di destinatari dell'origine del destinatario dinamico. Ad esempio, per elaborare un'origine del destinatario dinamico con dati relativi a 100.000 destinatari, il RAS deve essere impostato per leggere più di 100.000 record di database.

Per verificare questa impostazione, nell'area "Server" della CMC, selezionare il RAS e accedere a **Gestisci** > **Proprietà**. Nel campo **Numero di record di database da leggere per l'anteprima o l'aggiornamento di un report**, verificare che il numero sia corretto oppure immettere un nuovo valore.

Risoluzione dei problemi relativi agli errori di “memoria esaurita”

Se viene visualizzato un messaggio di errore simile al seguente, `java.lang.OutOfMemoryError: impossibile creare un nuovo thread nativo` durante l'esecuzione di una pubblicazione di grandi dimensioni, quando la memoria stack di Adaptive Processing Server e del servizio di pubblicazione non è sufficiente per la gestione dei thread di pubblicazione generati. Questo errore può verificarsi se la memoria stack è designata come spazio dell'heap Java.

È possibile impostare un limite di thread per Adaptive Processing Server. Nell'area "Server" della CMC, selezionare Adaptive Processing Server, quindi accedere a **Gestisci > Proprietà**. Nel campo **Parametri riga di comando**, immettere il seguente parametro:

-Dcom.businessobjects.publisher.threadpool.size=*threadlimitnumber*

Sostituire *threadlimitnumber* con il numero limite di thread desiderato.

Viene visualizzato un messaggio di errore simile al seguente, `java.lang.OutOfMemoryError: spazio heap Java` durante l'esecuzione di una pubblicazione di grandi dimensioni, quando lo spazio dell'heap di Adaptive Processing Server non è sufficiente. Nell'area "Server" della CMC, selezionare Adaptive Processing Server, quindi accedere a **Gestisci > Proprietà**. Nel campo **Parametri della riga di comando**, cambiare il numero del parametro -Xmx256m con un numero maggiore (ad esempio -Xmx1024m).

Nota:
In alcuni casi può essere necessario creare più istanze di Adaptive Processing Server per risolvere gli errori “Memoria insufficiente”.

8.1.11 Configurazione delle impostazioni server

Questa sezione include informazioni tecniche e procedure che illustrano come modificare le impostazioni per i server della piattaforma SAP BusinessObjects Business Intelligence.

La maggior parte delle impostazioni descritte in questa sezione consentono di integrare più efficacemente la piattaforma SAP BusinessObjects Business Intelligence 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 delle applicazioni Web per distribuire le applicazioni della piattaforma SAP BusinessObjects Business Intelligence. 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

8.1.11.1 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.

8.1.11.2 Applicazione delle impostazioni dei servizi a più server

Per applicare la stessa impostazione ai servizi ospitati in più server,

1. Passare all'area di gestione "Server" della CMC.
2. Fare clic con il pulsante destro del mouse sui servizi di cui si desidera modificare le impostazioni e selezionare **Modifica servizi comuni**.

   Nella finestra di dialogo "Modifica servizi comuni" sono visualizzati i servizi ospitati in tutti i server selezionati e che utilizzano impostazioni che possono essere modificate.
3. Se nella finestra di dialogo "Modifica servizi comuni" sono presenti più servizi, selezionare quello che si desidera modificare e fare clic su **Continua**.
4. Apportare le modifiche desiderate e fare clic su **OK**.

Nota:
Viene visualizzata l'area di gestione dei "server" della console CMC. Se i server richiedono un riavvio, vengono contrassegnati con Non aggiornato. Dopo il riavvio, i server utilizzano le impostazioni desiderate e il contrassegno Non aggiornato viene rimosso.

8.1.11.3 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 SAP BusinessObjects Business Intelligence utilizza 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

8.1.11.3.1 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

8.1.11.3.2 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

8.1.11.3.3 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.

8.1.12 Configurazione delle impostazioni di rete del server

Le impostazioni di rete per i server della piattaforma SAP BusinessObjects Business Intelligence vengono gestite mediante la console 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 SAP BusinessObjects Business Intelligence vengono associati in modo dinamico alle porte disponibili. I numeri di porta vengono gestiti automaticamente dalla piattaforma SAP BusinessObjects Business Intelligence, tuttavia è possibile utilizzare la CMC per specificare i numeri di porta.

8.1.12.1 Opzioni dell'ambiente di rete

La piattaforma SAP BusinessObjects Business Intelligence supporta il traffico di rete basato su Internet Protocol 6 (IPv6) e su 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 SAP BusinessObjects Business Intelligence non prevede un meccanismo per la definizione di un ambiente di rete. È possibile utilizzare la console CMC per creare un'associazione a un indirizzo IPv6 o IPv4 specifico per qualsiasi server della piattaforma SAP BusinessObjects Business Intelligence.

8.1.12.1.1 Ambiente IPv6/IPv4 misto

L'ambiente di rete IPv6/IPv4 consente:

- I server della piattaforma SAP BusinessObjects Business Intelligence possono gestire richieste sia 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.

Nota:
I nomi DNS non vengono risolti correttamente se il nodo solo IPv6 viene utilizzato con Windows 2003. È consigliabile che la distribuzione venga eseguita come IPv6/IPv4 se lo stack IPv4 è disabilitato in Windows 2003.

8.1.12.2 Opzioni di identificazione host del server

È possibile specificare le opzioni di identificazione host nella console CMC per ogni server della piattaforma SAP BusinessObjects Business Intelligence. Nella seguente tabella sono riepilogate le opzioni disponibili nell'area Impostazioni comuni:

Opzione	Descrizione
Assegna automaticamente	Impostazione predefinita per tutti i server Quando si seleziona **Assegna automaticamente**, il server associa automaticamente la porta di richiesta del server alla prima scheda NIC nel computer. **Nota:** È consigliabile selezionare la casella di controllo Assegna automaticamente per l'impostazione Nome host. In alcuni casi, tuttavia, 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. Per ulteriori informazioni, consultare “Configurazione di un computer multi-home” e il capitolo “Utilizzo dei firewall” nel *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.
Nome host	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 di richiesta e la porta del server dei nomi.
Indirizzo IP	Specifica l'indirizzo IP dell'interfaccia di rete su cui il server resta in ascolto delle richieste. Per il server CMS, questa impostazione specifica l'indirizzo dell'interfaccia di rete cui il server CMS associa la porta di richiesta e la porta del server dei nomi. Per ogni server, vengono forniti campi separati per specificare gli indirizzi IP IPv4 e/o IPv6.

Avvertenza:
importante: se si specifica **Assegna automaticamente** su computer multi-home, è possibile che il CMS associ automaticamente l'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 inoltre necessario specificare l'impostazione Nome host per il server CMS nella console CMC.

Nota:
Se si utilizzano computer multi-home o alcune configurazioni firewall NAT, può essere necessario specificare il nome host tramite nomi di dominio completi anziché nomi host.

Argomenti correlati

- Configurazione di un computer multi-home
- Per risolvere i problemi relativi a più interfacce di rete

8.1.12.2.1 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 automa-ticamente	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	Immettere nei campi forniti un indirizzo IP IPv4 o IPv6 per l'interfaccia di rete su cui il server rimane in attesa di richieste. **Nota:** Per fare in modo che il server possa funzionare come nodo IPv4/IPv6 doppio, immettere un indirizzo IP valido in entrambi i campi.

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.

8.1.12.3 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 utilizzano più interfacce di rete, ciascuna con un solo indirizzo IP, modificare l'ordine di associazione in modo che l'interfaccia di rete in cima a tale ordine sia quella a cui si desidera siano associati i server della piattaforma SAP BusinessObjects Business Intelligence. Se l'interfaccia ha più indirizzi IP, utilizzare l'opzione Nome host nella console CMC per specificare una scheda di interfaccia di rete per il server della piattaforma SAP BusinessObjects Business Intelligence. È possibile specificarla con nome host o indirizzo IP. Per ulteriori informazioni sulla configurazione dell'impostazione Nome host, consultare “Per eseguire la risoluzione dei problemi di più schede NIC ”.

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 SAP BusinessObjects Business Intelligence. In questo esempio, il DNS deve instradare le comunicazioni dagli altri server della piattaforma SAP BusinessObjects Business Intelligence all'indirizzo privato dei File Repository Server.

Argomenti correlati

- Per risolvere i problemi relativi a più interfacce di rete

8.1.12.3.1 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.

8.1.12.3.2 Configurazioni degli altri server da associare a un indirizzo di rete

Gli altri server della piattaforma SAP BusinessObjects Business Intelligence selezionano dinamicamente le porte 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

8.1.12.3.3 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 questa procedura immediatamente dopo l'installazione della piattaforma BI sul computer locale, prima di installare la piattaforma su 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 l'agente SIA a un'interfaccia di rete specifica, digitare nel campo **Porta** uno degli elementi seguenti:
   - nome host dell'interfaccia di rete di destinazione e numero della porta (utilizzare il formato nomehost:numero porta)
   - indirizzo IP dell'interfaccia di rete di destinazione e numero della porta (utilizzare il formato indirizzo IP:numero 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 server CMS a un'interfaccia di rete specifica, digitare nel campo **Porta** uno degli elementi seguenti:
   - nome host dell'interfaccia di rete di destinazione e numero della porta (utilizzare il formato nomehost:numero porta)
   - indirizzo IP dell'interfaccia di rete di destinazione e numero della porta (utilizzare il formato indirizzo IP:numero 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.

8.1.12.4 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 SAP BusinessObjects Business Intelligence viene dinamicamente associato a una porta disponibile (con un numero superiore a 1024), viene registrato con questa porta nel CMS e attende le richieste della piattaforma SAP BusinessObjects Business Intelligence. Se necessario, è possibile indicare a ciascun componente server di restare in attesa su una porta specifica (piuttosto che selezionare dinamicamente qualsiasi porta disponibile).

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 SAP BusinessObjects Business Intelligence su cui il CMS resta in ascolto delle richieste del servizio dei nomi. Il numero di porta predefinito è 6400.	Non applicabile.

8.1.12.4.1 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".

8.1.12.4.2 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 CMS a una porta specifica, digitare nel campo **Porta** uno dei seguenti:
   - numero della porta
   - nome host e numero della porta (utilizzare il formato nomehost:numero porta)
   - indirizzo IP e numero della porta (utilizzare il formato indirizzo IP:numero porta)
6. Fare clic su **OK** per applicare le nuove impostazioni.
7. Avviare SIA e attendere l'avvio dei server.

8.1.12.4.3 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, sarà necessario 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, lo script si trova nella directory *<DirInstallaz>*/sap_bobj.
3. Selezionare 3: Modifica Server Intelligence Agent e premere **Invio**.
4. Selezionare il SIA che ospita il CMS che si desidera modificare e premere **Invio**.
5. Selezionare 4: Modifica nodo e premere **Invio**.

   Viene visualizzato un elenco di CMS attualmente ospitati nel SIA.
6. Selezionare il CMS che si desidera modificare e premere **Invio**.
7. Digitare il nuovo numero di porta per il CMS e premere **Invio**.
8. Specificare se si desidera che il CMS si avvii automaticamente all'avvio del SIA e premere **Invio**.
9. Digitare gli argomenti della riga di comando per il CMS o accettare gli argomenti correnti, quindi premere **Invio**.
10. Avviare il SIA con lo script `ccm.sh` e attendere l'avvio dei server.

8.1.12.4.4 Per modificare la porta utilizzata da un server 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 CMS e inizia l'ascolto delle richieste della piattaforma SAP BusinessObjects Business Intelligence sulla nuova porta.

8.1.13 Gestione dei nodi

8.1.13.1 Utilizzo dei nodi

Un nodo è un gruppo di server della piattaforma BI in esecuzione sullo stesso host. Tutti i server di un nodo vengono eseguiti con lo stesso account utente.

In una macchina possono essere presenti molti nodi, pertanto è possibile eseguire i processi con account utente diversi.

Un solo SIA (Server Intelligence Agent) gestisce e controlla tutti i server di un nodo, garantendone il corretto funzionamento.

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 procedura di gestione dei nodi. Per ulteriori informazioni, vedere la sezione “Configurazione dei server per SSL”.

8.1.13.1.1 Variabili

In questo capitolo vengono utilizzate le variabili seguenti.

Variabile	Descrizione
<DIRINSTALLAZ>	La directory in cui viene installata la piattaforma BI. In un computer Windows è la directory `C:\Programmi (x86)\SAP BusinessObjects`
<DIRSCRIPT>	La directory in cui si trovano gli script di gestione dei nodi. In un computer Windows è *<DIRINSTALLAZ>*`\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\scripts` Nei computer Unix è *<DIRINSTALLAZ>*`/sap_bobj/enterprise_xi40/`*<PIATTAFORMA>*`/scripts`
<PIATTAFORMA>	Nome del sistema operativo Unix. I valori accettabili sono: • `aix_rs6000_64` • `linux_x64` • `solaris_sparcv9` • `hpux_ia64`

8.1.13.2 Aggiunta di un nuovo nodo

Il programma di installazione crea nodi alla prima installazione della piattaforma BI.

Potrebbero essere necessari ulteriori nodi se si desidera aggiungere un nuovo computer a un cluster esistente per migliorare le prestazioni del cluster oppure se si intende eseguire i server con account utente diversi con una distribuzione esistente.

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.

Promemoria:
è possibile aggiungere un nodo solo sul computer in cui risiede.

8.1.13.2.1 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 nodi aggiuntivi, utilizzare Central Configuration Manager oppure lo script.

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

8.1.13.2.2 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 viene richiesto, immettere il nome host e la 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 viene richiesto, immettere il nome host e la 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. Verrà avviato un CMS temporaneo, che verrà interrotto quando termina il processo.

     Avvertenza:
     evitare di utilizzare la distribuzione durante l'esecuzione del CMS temporaneo. Assicurarsi che il CMS esistente e quello temporaneo 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.

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, vedere la sezione “Parametri di 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 ignorare gli spazi, il simbolo di uguaglianza (=) e il punto e virgola (;) nella stringa `-connect`.

```
<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
```

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

8.1.13.2.3 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 `<DIRINSTALLAZ>/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 viene richiesto, immettere il nome host e la 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 viene richiesto, immettere il nome host e la 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. Verrà avviato un CMS temporaneo, che verrà interrotto quando termina il processo.

     Avvertenza:
     evitare di utilizzare la distribuzione durante l'esecuzione del CMS temporaneo. Assicurarsi che il CMS esistente e quello temporaneo 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 `<DIRINSTALLAZ>/sap_bobj/ccm.sh -start <NomeNodo>` per avviare il nuovo nodo.

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
```

Argomenti correlati

- Variabili
- Parametri script per l'aggiunta, la ricreazione e l'eliminazione di nodi

8.1.13.3 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

8.1.13.3.1 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 la porta del CMS esistente, le credenziali dell'amministratore, il nome dell'origine dati, le credenziali del database di sistema di origine 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 e la porta 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. Verificare che il CMS esistente e quello temporaneo utilizzino porte diverse.

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.

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 di 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 ignorare gli spazi, il simbolo di uguaglianza (=) e il punto e virgola (;) nella stringa `-connect`.

```
<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

8.1.13.3.2 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 la porta del CMS esistente, le credenziali dell'amministratore, le informazioni sulla connessione al database, le credenziali del database di sistema e la chiave cluster.

   - Se la distribuzione è stata interrotta, selezionare **temporary** e premere **Invio**.

     Se richiesto, immettere il nome host e la porta 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. Verificare che il CMS esistente e quello temporaneo utilizzino porte diverse.

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.

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
  -siaport 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

8.1.13.4 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

8.1.13.4.1 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, le credenziali dell'amministratore per il CMS e la chiave cluster.

Vengono eliminati il nodo e tutti i server in esso contenuti.

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

8.1.13.4.2 Eliminazione di un nodo in Unix

Avvertenza:
eseguire il backup della configurazione server per l'intero cluster prima e dopo l'eliminazione di un nodo.

1. Eseguire `<DIRINSTALL>/sap_bobj/ccm.sh -stop <Nomenodo>` per interrompere 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, la porta, le credenziali dell'amministratore per il CMS e la chiave cluster.

Vengono eliminati il nodo e tutti i server in esso contenuti.

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

8.1.13.5 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

8.1.13.5.1 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

8.1.13.5.2 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. Digitare il numero di porta del nuovo SIA, quindi 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

8.1.13.6 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 produzione.
- 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.

Promemoria:
è possibile spostare un nodo solo sul computer in cui risiede.

8.1.13.6.1 Spostamento di un nodo esistente in Windows

In questo esempio il nodo da spostare viene installato nel sistema di origine. Il computer non faceva inizialmente parte di un cluster, ma deve essere 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 la porta del CMS esistente 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.

   - 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 la 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. Verificare che il CMS esistente e quello temporaneo utilizzino porte diverse.

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.

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 ignorare gli spazi, il simbolo di uguaglianza (=) e il punto e virgola (;) nella stringa `-connect`.

```
<SCRIPTDIR>\MoveNode.bat -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
```

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

8.1.13.6.2 Spostamento di un nodo esistente in Unix

In questo esempio il nodo da spostare viene installato nel sistema di origine. Il computer faceva inizialmente parte di un cluster stand-alone, ma deve essere 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 interrompere 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 la porta del CMS esistente 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.
   - 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.

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

8.1.13.7 Parametri script

8.1.13.7.1 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`	Il nome e la porta del server CMS (Central Management Server). **Avvertenza:** non utilizzare questo parametro se si utilizza `-usetempcms` **Nota:** è necessario specificare un numero di porta se il server CMS non viene eseguito sulla porta predefinita 6400.	-cms mycms:6409

Parametro	Descrizione	Esempio
`-cmsport`	• La porta del server CMS quando si avvia un CMS temporaneo. **Limitazione:** inoltre, è necessario utilizzare i parametri `-usetempcms`, `-dbdriver`, `-connect` e `-dbkey`. • La porta del server CMS quando si crea un nuovo CMS. **Limitazione:** inoltre, è necessario utilizzare i parametri `-dbdriver`, `-connect` e `-dbkey`.	-cmsport 6401
`-connect`	La stringa di connessione del server CMS o del database di sistema CMS temporaneo. **Nota:** omettere gli attributi `HOSTNAME` e `PORT` per eseguire la connessione ai database DB2, Oracle, SQL Server o Sybase.	-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=password;HOSTNAME=database;PORT=3306"
`-dbdriver`	Il driver di database del server CMS. Valori accettati: • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem	-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 `-createcms` 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 `-cms` 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

8.1.13.7.2 Parametri script per lo spostamento di nodi

Parametro	Descrizione	Esempio
`-cms`	Il nome del server CMS (Central Management Server) di origine. **Avvertenza:** non utilizzare questo parametro se si utilizza `-usetempcms` **Nota:** è necessario specificare un numero di porta se il server CMS non viene eseguito sulla porta predefinita 6400.	-cms sourceMachine:6409
`-cmsport`	• La porta del server CMS quando si avvia un CMS temporaneo. **Limitazione:** inoltre, è necessario utilizzare i parametri `-usetempcms`, `-dbdriver`, `-connect` e `-dbkey`. • La porta del server CMS quando si crea un nuovo CMS. **Limitazione:** inoltre, è necessario utilizzare i parametri `-dbdriver`, `-connect` e `-dbkey`.	-cmsport 6401
`-connect`	La stringa di connessione del server CMS di origine o del database di sistema CMS temporaneo. **Nota:** omettere gli attributi `HOSTNAME` e `PORT` per eseguire la connessione ai database DB2, Oracle, SQL Server o Sybase.	-connect "DSN=Source BOEXI40;UID=username;PWD=password;HOSTNAME=database;PORT=3306"

Parametro	Descrizione	Esempio
-dbdriver	Il driver di database del server CMS di origine. Valori accettati: • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem	-dbdriver mysqldatabasesubsystem
-dbkey	La chiave cluster di origine.	-dbkey abc1234
-destcms	Il nome del server CMS di destinazione. **Nota:** è necessario specificare un numero di porta se il server CMS non viene eseguito sulla porta predefinita 6400.	-destcms destinationMachine:6401
-destconnect	La stringa di connessione del database di sistema CMS di destinazione. **Nota:** omettere gli attributi HOSTNAME e PORT per eseguire la connessione ai database DB2, Oracle, SQL Server o Sybase.	-destconnect "DSN=Destin BOEXI40;UID=username;PWD=pass word;HOSTNAME=data base;PORT=3306"
-destdbdriver	Il driver di database del server CMS di destinazione. Valori accettati: • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem **Nota:** sqlserverdatabase non è supportato in Unix.	-destdbdriver sybasedatabasesubsystem

Parametro	Descrizione	Esempio
`-destdbkey`	La chiave cluster di destinazione.	-destdbkey def5678
`-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`	**Avvertenza:** non utilizzare questo parametro se si utilizza `-cms` Avvia e utilizza il server CMS temporaneo. **Nota:** utilizzare un server CMS temporaneo quando la distribuzione non è in esecuzione.	-usetempcms

Argomenti correlati

- Spostamento di un nodo in Windows mediante uno script
- Spostamento di un nodo in Unix mediante uno script

8.1.13.8 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.

8.1.13.8.1 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.

8.1.13.9 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.

8.1.13.9.1 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.

8.1.14 Ridenominazione di un computer in una distribuzione della piattaforma SAP BusinessObjects Business Intelligence

In qualsiasi momento è possibile modificare il nome di un computer in una distribuzione della piattaforma SAP BusinessObjects Business Intelligence assegnandogli un nome diverso dopo avere arrestato tutti i server della piattaforma SAP BusinessObjects Business Intelligence. Se il computer fa parte di un cluster, non è necessario arrestare tutti i computer e i server del cluster. È possibile assegnare un nome

diverso ai server nella Central Management Console (CMC) anche se gli altri computer sono in esecuzione.

Se il database di sistema CMS o il database di controllo si trova nel computer che si intende ridenominare, dopo l'operazione di ridenominazione sarà è necessario aggiornare la informazioni di connessione del database. Se si utilizzano connessioni ODBC a uno di questi database, è necessario aggiornare la connessione con il nuovo nome del computer. Per tutte le altre connessioni del database, è necessario selezionare il database esistente in Central Configuration Manager (CCM).

Se si intende ridenominare un computer che fa parte di una distribuzione, non è necessario ridenominare i nodi nel computer.

Argomenti correlati

- Selezione di un database CMS nuovo o esistente

8.1.15 Utilizzo di librerie di terze parti a 32 e 64 bit con la piattaforma SAP BusinessObjects Business Intelligence

I server della piattaforma SAP BusinessObjects Business Intelligence 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 o 64 bit) con i processi della piattaforma SAP BusinessObjects Business Intelligence, è necessario impostare variabili di ambiente separate per ogni versione del computer che ospita la piattaforma SAP BusinessObjects Business Intelligence. 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 SAP BusinessObjects Business Intelligence, 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 SAP BusinessObjects Business Intelligence 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_AMB32>*=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 SAP BusinessObjects Business Intelligence è stata installata in un computer AIX, oltre che in 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

8.1.16 Gestione dei segnaposto per server e nodi

8.1.16.1 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

8.1.16.2 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 **OK** per continuare.

Argomenti correlati

- Segnaposto server e nodo

Gestione dei database CMS (Central Management Server)

9.1 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 SAP BusinessObjects Business Intelligence utilizza più server CMS, le richieste successive vengono inoltrate a qualsiasi server CMS del cluster con 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

9.2 Selezione di un database CMS nuovo o esistente

È possibile utilizzare CCM 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 SAP BusinessObjects Business Intelligence, 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.

9.2.1 Per selezionare un database CMS nuovo o esistente in Windows

1. Utilizzare CCM per arrestare Server Intelligence Agent (SIA).
2. Selezionare SIA e fare clic su **Specifica origine dati database di sistema CMS** sulla barra degli strumenti.
3. Nella scheda **Configurazione** della finestra di dialogo "Proprietà" in **Origine dati CMS**, fare clic su **Specifica**.
4. Le fasi successive dipendono dal tipo di connessione selezionato:
   - Se viene selezionato ODBC, viene visualizzata la finestra di dialogo Windows “Selezione 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.

   L'utente verrà notificato al termine dell'installazione del database CMS.
5. Nella finestra di dialogo "Proprietà" fare clic su **OK**.
6. Riavviare Server Intelligence Agent.

9.2.2 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 `<directory_installazione>/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 e password).

   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 attraverso il quale il server CMS deve comunicare.

Nota:
Queste informazioni vengono richieste solo se si fa riferimento a un database CMS vuoto.

9.3 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. La procedura è utile, ad esempio, se la piattaforma SAP BusinessObjects Business Intelligence è installata in un ambiente di sviluppo per progettare e sottoporre a verifica le 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

9.3.1 Per creare nuovamente il 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.

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.

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**.

   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.

9.3.2 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 si trova in `<directory_installazione>/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 `<DIRINSTALL>/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.

9.4 Copia dei dati da un database di sistema CMS a un altro

È possibile utilizzare CCM (Central Configuration Manager) per copiare i dati di sistema da un server di database in 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 precedente della piattaforma BI nella versione corrente, utilizzare Upgrade Management Tool. Per ulteriori informazioni, consultare il *Manuale di aggiornamento della piattaforma SAP BusinessObjects Business Intelligence*.

9.4.1 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 dati da un database all'altro, il database di destinazione viene inizializzato prima che i nuovi dati vi siano copiati. Ovvero, se il database di destinazione non contiene le tabelle di sistema della piattaforma SAP BusinessObjects Business Intelligence, tali tabelle vengono create. Se il database di destinazione contiene le tabelle di sistema della piattaforma SAP BusinessObjects Business Intelligence, 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 MaxDB sia stato aggiunto alla variabile di ambiente *PATH*. Ad esempio, `;C:\Programmi\sdb\MAXDB1\pgm`.

9.4.2 Per copiare 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**.

9.4.3 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 si trova in `<directory_installazione>/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)

10.1 WACS

10.1.1 Server contenitore applicazioni Web (WACS)

I server WACS forniscono una piattaforma per l'hosting delle applicazioni Web della piattaforma BI. 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.

10.1.1.1 Necessità dei server WACS

Se non si desidera utilizzare un server di applicazioni Java per ospitare le applicazioni Web SAP Business Objects, è possibile ospitarle sul WACS.

Se si intende utilizzare un server di applicazioni Java supportato per distribuire le applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence o se si installa la piattaforma SAP BusinessObjects Business Intelligence in un sistema UNIX, non è necessario installare né utilizzare i server WACS.

10.1.1.2 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 analoga ad altri server della piattaforma SAP BusinessObjects Business Intelligence.

10.1.1.3 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.	• 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.	• Configurazione di HTTPS/SSL • Utilizzo dei WACS con i firewall

Attività	Descrizione	Argomento
Come migliorare la protezione della comunicazione tra WACS e altri server Business Objects nella distribuzione?	Configurare la comunicazione SSL tra il WACS e altri server della piattaforma SAP BusinessObjects Business Intelligence nella distribuzione.	• Configurazione dei server per SSL • Utilizzo dei WACS con i firewall
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.	• 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 firewall
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.	• 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	Numerose possono essere le ragioni dell'impossibilità di connettersi a un server WACS. Verificare se: • 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.	• 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

10.1.2 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.

10.1.2.1 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 applicazione Web Java" di un'installazione completa scegliere **Installare il server del contenitore applicazioni Web e distribuire automaticamente le applicazioni e i servizi Web sul server**.

  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.

10.1.2.2 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 e QaaWS di servizi Web**.
   - Se si desidera che il server WACS ospiti i servizi Web Business Process BI, selezionare **Servizio Web Business Process BI**.
   - Se si desidera che il server WACS supporti l'analisi del server, selezionare **Servizio log analisi**.
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 "Crea nuovo server" successiva, fare clic su **Avanti**.
7. 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**.
8. Nella schermata "Server", fare doppio clic sul WACS appena creato.

Viene visualizzata la schermata "Proprietà".

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

Viene creato un nuovo WACS. Le impostazioni predefinite e le proprietà vengono applicate al server.

10.1.2.3 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

10.1.2.4 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**.

10.1.3 Aggiunta o rimozione di servizi dal server WACS

10.1.3.1 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.

10.1.3.2 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.

10.1.4 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 SAP BusinessObjects Business Intelligence. SSL/HTTPS crittografa il traffico di rete e fornisce una protezione migliorata.

Esistono due tipi di SSL:

- SSL utilizzato fra i server della piattaforma SAP BusinessObjects Business Intelligence, fra cui WACS e altri server della piattaforma SAP BusinessObjects Business Intelligence nella propria distribuzione. Questo protocollo è noto come CorbaSSL. Per ulteriori informazioni sull'utilizzo di SSL tra i server della piattaforma SAP BusinessObjects Business Intelligence della distribuzione, consultare la sezione relativa alle “comunicazioni tra i componenti della piattaforma SAP BusinessObjects Business Intelligence” del capitolo relativo all'“utilizzo di firewall” del *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 della 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

10.1.4.1 Per generare un archivio di file di certificati PKCS12

Sono disponibili molti modi per generare un archivio di chiavi Java o di file di certificati PKCS12. 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).

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 Aggiungi certificati a MMC:
   a. Dal menu **File** scegliere **Aggiungi/Rimuovi snap-in**.
   b. Fare clic su **Aggiungi**.
   c. Nella finestra di dialogo "Aggiungi snap-in autonomo" selezionare **Certificati** e fare clic su **Aggiungi**.
   d. Selezionare **Account computer** e fare clic su **Avanti**.
   e. Selezionare **Computer locale** e fare clic su **Fine**.
   f. Fare clic su **Chiudi** 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.

10.1.4.2 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** e fare clic su **Aggiungi**.
   b. Nella finestra di dialogo "Aggiungi snap-in autonomo" selezionare **Gestione Internet Information Services (IIS)** e fare clic su **Aggiungi**.
   c. Fare clic su **Chiudi** e fare clic su **OK**.

   Lo snap-in IIS viene aggiunto a MMC.
4. Nel riquadro sinistro di MMC, trovare il sito Web per il quale creare l'elenco di certificati attendibili.
5. Fare clic con il pulsante destro del mouse sul sito Web e selezionare **Proprietà**.
6. Fare clic sulla scheda **Protezione directory** e in "Comunicazioni protette" fare clic su **Modifica**.
7. Fare clic su **Abilita elenco certificati attendibili** e fare clic su **Nuovo**.

Viene avviata la "Gestione guidata dell'elenco di certificati attendibili".

8. Fare clic su **Avanti**.
9. Fare clic su **Aggiungi da archivio** o **Aggiungi da file**, selezionare il certificato da aggiungere all'elenco di certificati attendibili, fare clic su **OK** e quindi su **Avanti**.
10. Digitare un nome e una descrizione per l'elenco di certificati attendibili e fare clic su **Avanti**.
11. Fare clic su **Fine** e quindi su **OK**.

    L'elenco di certificati attendibili viene visualizzato nel campo **CTL corrente**.
12. Selezionare l'elenco di certificati attendibili e fare clic su Modifica.

    Viene avviata la "Gestione guidata dell'elenco di certificati attendibili".
13. Fare clic su **Avanti**.
14. Nell'elenco **Certificati attualmente presenti nell'elenco di certificati attendibili** selezionare l'elenco di certificati attendibili e fare clic su **Visualizza certificati**.
15. Fare clic sulla scheda **Dettagli** e fare clic su **Copia su file**.

    Viene avviata l'"Esportazione guidata certificati".
16. Fare clic su **Avanti**.
17. Selezionare **Esporta la chiave privata** e fare clic su **Avanti**.
18. Selezionare **Personal Information Exchange - PKCS #12 (.PFX)** e fare clic su **Avanti**.
19. Immettere la password utilizzata per la creazione del certificato e fare clic su **Avanti**. È necessario specificare questa password nel campo **Password di accesso alle chiavi private dell'elenco degli scopo consentiti ai certificati** quando si configura HTTPS per il server WACS.

10.1.4.3 Per configurare HTTPS/SSL

Prima di configurare HTTPS/SSL sul WACS, assicurarsi di avere già creato un file PCKS12 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 l'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 PCKS12 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.

10.1.5 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

10.1.6 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.

Argomenti correlati

- Utilizzo di utenti e gruppi Windows AD
- Plug-in di protezione di Windows AD
- Impostazione di un account di servizio per l'autenticazione AD con Kerberos
- Preparazione dei server per l'autenticazione Windows AD con Kerberos
- 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

10.1.6.1 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.

-
- Immissione del nome principale di servizio (SPN) per l'account di servizio

10.1.6.1.1 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
- Per concedere i diritti per l'account di servizio
- Preparazione dei server per l'autenticazione Windows AD con Kerberos
- "Mapping Windows AD accounts"

10.1.6.1.2 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. Accertarsi che la casella di controllo **Autenticazione Windows Active Directory abilitata** sia selezionata.
4. In **Opzioni di autenticazione**, selezionare **Usa autenticazione Kerberos**.
5. 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.
- Deve essere lo stesso account utilizzato per eseguire i server della piattaforma SAP BusinessObjects Business Intelligence o l'SPN mappato a questo account.

Argomenti correlati

- Configurazione del Single Sign On AD Kerberos

10.1.6.2 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.

10.1.6.2.1 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 archiviarlo in C:\WINNT 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.

10.1.6.2.2 Per creare il file di configurazione degli accessi JAAS

1. Creare un file denominato `bscLogin.conf`, se non è già presente, e memorizzarlo nella posizione predefinita: C:\WINNT.

   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.

10.1.6.2.3 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
  }
```

10.1.6.3 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).

10.1.6.3.1 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.

10.1.6.4 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

10.1.6.4.1 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.

10.1.6.4.2 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.

```
<Install Directory>\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.

10.1.6.4.3 Un utente AD mappato non è in grado di accedere a BusinessObjects Enterprise su WACS

Anche se gli utenti sono stati mappati a SAP BusinessObjects Enterprise, 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 a SAP BusinessObjects Enterprise. 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.

10.1.7 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 ulteriori informazioni, consultare Configurazione di AD Kerberos per server WACS .

Nota:
Se si prevede di utilizzare il Single Sign On in un ambiente proxy inverso, leggere il capitolo relativo alla “protezione della piattaforma SAP BusinessObjects Business Intelligence ” del *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence* prima di continuare.

10.1.7.1 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:

- Configurazione della delega vincolata per il Single Sign-on Vintela
- "To create an SPN for your web application server"
- "To reset the service account password"
- "To create and place a keytab file"
- 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.

10.1.7.1.1 Impostazione di più SPN

L'utilizzo di più SPN non è supportato.

10.1.7.1.2 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.

10.1.7.2 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.

10.1.7.3 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 SAP BusinessObjects Business Intelligence avviene 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 dettagli, vedere Configurazione del Single Sign On AD Kerberos .

10.1.7.3.1 Per abilitare Single Sign-On nel database

1. Aprire il file `krb5.ini` che viene utilizzato per la distribuzione della piattaforma SAP BusinessObjects Business Intelligence.

   La posizione predefinita di questo file è la directory WINNT 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.

10.1.8 WACS e ambiente IT

In questa sezione viene descritto come configurare un WACS in un ambiente complesso.

10.1.8.1 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.

10.1.8.2 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

10.1.8.3 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.

10.1.8.3.1 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**.

10.1.8.3.2 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.

10.1.8.4 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 SAP BusinessObjects Business Intelligence 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

10.1.8.5 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 di applicazioni Web", deselezionare **Associa a tutti gli indirizzi IP** e digitare un indirizzo IP per il WACS a cui effettuare l'associazione.
4. Nella sezione "Configurazione HTTPS" deselezionare **Associa a tutti gli indirizzi IP** e digitare un indirizzo IP o un nome host per il WACS a cui effettuare l'associazione.
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.

10.1.9 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 proprietà esposte 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

10.1.10 Risoluzione dei problemi

10.1.10.1 Configurazione dell'analisi sul server WACS

Per configurare l'analisi per il server WACS, consultare Registrazione di analisi dai componenti

10.1.10.2 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

10.1.10.3 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 dispongono di un nuovo stato definito “Avviato con errori”. Un WACS che si trova in questo stato è in esecuzione, ma presenta almeno un connettore HTTP, HTTP su proxy o HTTPS configurato in modo errato.

Se lo stato di un server WACS è “Avviato con errori”, accedere alla pagina "Metriche" e visualizzare la metrica "Elenco di connettori WACS in esecuzione". Se un connettore abilitato non compare nell'elenco, il connettere non è stato configurato correttamente.

10.1.10.4 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 al servizio CMC e controllare i connettori WACS in esecuzione e gli errori di avvio del WACS. Se i connettori HTTP, HTTP su proxy o HTTP non figurano nell'elenco dei connettori WACS in esecuzione, non sarà possibile avviare tali connettori 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.

10.1.10.4.1 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.

10.1.10.4.2 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**.

10.1.10.5 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.

10.1.10.6 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**.

10.1.10.7 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.

10.1.10.8 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, quindi fare clic su **OK**.
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.

10.1.11 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

11.1 Backup e ripristino del sistema

In questo capitolo vengono descritte le procedure suggerite per l'esecuzione dei backup del sistema della piattaforma SAP BusinessObjects Business Intelligence e dei file di dati, nonché le procedure di ripristino in caso di perdita dei dati o malfunzionamenti dell'hardware. L'esecuzione del piano richiede un tecnico esperto di BusinessObjects, un amministratore di sistema e un amministratore di database.

Il processo di backup e ripristino è simile per tutti gli ambienti: sviluppo, test e produzione. Di conseguenza, questo capitolo non fa riferimento a un ambiente specifico. Si consiglia di eseguire il backup di tutti gli ambienti.

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. Lo scopo del piano è ridurre al minimo gli effetti del disastro sulle attività quotidiane, in modo da poter continuare a utilizzare o riprendere rapidamente le funzioni più importanti.

Si consiglia di eseguire regolarmente il backup del database di sistema CMS (Central Management Server), dei contenuti dei server Input e Output File Repository e del file system dei computer in cui è installata la piattaforma SAP BusinessObjects Business Intelligence per proteggere il sistema da problemi di hardware, errori del software o impostazioni non corrette del server.

Si consiglia inoltre di eseguire regolarmente il backup dei contenuti Business Intelligence, inclusi report, utenti e diritti, utilizzando Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0 ed esportando i contenuti nei file Business Intelligence Archive Resource (LCMBIAR). Nel caso in cui i contenuti siano danneggiati o mancanti, è possibile ripristinarli in un secondo tempo senza dover ripristinare l'intero database CMS o i file repository. Per ulteriori informazioni sull'utilizzo di Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0, consultare il *Manuale dell'utente di Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0*. Se si sta utilizzando Subversion con Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0, consultare il capitolo relativo al “backup dei file Subversion” nel *Manuale dell'utente di Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0* per informazioni sul backup del repository di Subversion.

Nella parte restante di questo capitolo viene descritta la procedura di backup e ripristino del sistema nel caso in cui un database di sistema CMS, un file repository o il file system vada perduto o risulti danneggiato. Viene descritto inoltre come eseguire il ripristino nel caso in cui un server CMS sia configurato in modo non corretto e non sia quindi possibile utilizzare Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0 per ripristinare le impostazioni del server o i contenuti Business Intelligence.

Nota:
è possibile eseguire il backup di una piattaforma SAP BusinessObjects Business Intelligence e quindi ripristinare un sistema per crearne una copia.

11.1.1 Esecuzione di un backup di sistema

Si consiglia di eseguire regolarmente il backup dei seguenti elementi:

- Database di sistema CMS (Central Management Server)

  È essenziale eseguire spesso il backup del database di sistema CMS. L'ambiente non può essere ripristinato senza un database di sistema CMS di cui è stato eseguito correttamente il backup. Il sistema deve essere arrestato prima di eseguire il backup del database di sistema CMS. Il backup del database di sistema CMS deve essere eseguito utilizzando gli strumenti di backup del database del fornitore del database.

  Il backup del database CMS deve essere la prima operazione eseguita nel processo di backup. Una volta avviato il processo, è possibile iniziare a eseguire il backup dei File Repository Server.

- Input e Output File Repository Server

  Per mantenere integro il backup, si consiglia di eseguire il backup dei contenuti dei server FRS (File Repository Server) quando si esegue quello del database di sistema CMS. Il backup dei file repository include il backup di tutti i file presenti nelle cartelle specificate dalle proprietà “Directory archivio file” degli Input e Output File Repository Server. Il sistema deve essere arrestato prima di eseguire il backup dei file repository. Il backup deve essere eseguito utilizzando uno degli strumenti di backup del file system.

La frequenza con cui esegue il backup del database di sistema CMS, dei file repository e del file system dipende dalle esigenze aziendali dell'organizzazione.

È possibile scegliere di arrestare il sistema della piattaforma BI ed eseguire un backup non in linea, per assicurarsi che le istanze di database siano statiche e per ridurre al minimo la possibilità di modificare i dati, evitando di danneggiare la qualità del backup.

Può anche essere opportuno eseguire il backup degli elementi indicati di seguito.

- Database di controllo
- File temporanei di controllo
- Applicazioni personalizzate

  Creare un backup di eventuali applicazioni o personalizzazioni ogni volta che vengono modificate.

- Connessioni di database

11.1.2 Backup delle impostazioni server

Per proteggere il sistema dall'errata configurazione delle impostazioni server, è consigliabile 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 Business Intelligence.

È essenziale eseguire il backup delle impostazioni server ogni volta che si apportano modifiche alla topologia del sistema, quali 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 eseguire il backup delle impostazioni del server della piattaforma BI in un file BIAR, quindi archiviare il file in un computer separato. È consigliabile eseguire il backup delle impostazioni server ogni volta che queste vengono modificate.

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 `<DIRINSTALL>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\scripts`.

In UNIX lo script `backupcluster.sh` si trova nella directory `/<DIRINSTALL>/sap_bobj/enterprise_xi40/<platform64>/scripts`.

Argomenti correlati

- Configurazione del protocollo SSL

11.1.2.1 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 avviare CCM in un computer che presenti un 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 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 backup o il ripristino, specificare un numero di porta diverso da quelli utilizzati per i CMS esistenti.
5. 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**.
6. 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 schermata "Conferma" vengono visualizzate le informazioni fornite.
7. Verificare che le informazioni fornite nella schermata "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.
8. Se l'operazione di backup non riesce, verificare il file di registro per identificare il motivo.
9. Fare clic su **OK** per chiudere la procedura guidata.

11.1.2.2 Backup delle impostazioni del server in UNIX

Sui computer 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 al minimo il rischio che gli utenti possano accedere al sistema mentre si esegue il backup o si ripristina il sistema, specificare un numero di porta diverso dai numeri di porta utilizzati dal CMS esistente.

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 schermata di riepilogo.
6. Verificare che le informazioni visualizzate sullo schermo siano corrette, quindi 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. Il nome e il percorso del file di registro vengono visualizzati sullo schermo.
7. Se l'operazione di backup non riesce, verificare il file di registro per identificare il motivo.

11.1.2.3 Backup delle impostazioni del server mediante script

Per creare un backup delle impostazioni del server della distribuzione, è possibile eseguire lo script `backupcluster.bat` in Windows o lo script `BackupCluster.sh` in UNIX.

In Windows lo script `BackupCluster.bat` si trova nella directory `<DIRINSTALL>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\scripts`.

In UNIX, il file `backupcluster.sh` si trova nella directory `/<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform64>/scripts`.

Per informazioni sui parametri utilizzati dallo script, consultare Parametri di BackupCluster e RestoreCluster.

11.1.3 Backup dei contenuti Business Intelligence

Si consiglia di utilizzare Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0 per eseguire regolarmente il backup dei contenuti Business Intelligence, quali report, utenti, 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 di Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0, consultare il *Manuale dell'utente di Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0*.

Se si sta utilizzando Subversion con Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0, consultare il capitolo relativo al “backup dei file Subversion” nel *Manuale dell'utente di Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0* per informazioni sul backup del repository di Subversion.

11.1.4 Ripristino del sistema

Le operazioni da eseguire per ripristinare il sistema variano a seconda se il database di sistema CMS (Central Management Server), gli Input e Output File Repository o il file system del computer in cui è installata la piattaforma SAP BusinessObjects Business Intelligence risultano perduti o danneggiati e se sono disponibili copie di backup di questi componenti.

- Se il database di sistema CMS è danneggiato o mancante e sono disponibili copie di backup del database di sistema e dei File Repository, vedere Ripristino di un sistema della piattaforma SAP BusinessObjects Business Intelligence quando sono disponibili backup.
- Se il database di sistema CMS è danneggiato o è andato perduto e non sono disponibili copie di backup sia del database che dei File Repository, ma è stato eseguito il backup del contenuto Business Intelligence in un file BIAR, vedere Ripristino di un sistema della piattaforma SAP BusinessObjects Business Intelligence quando non sono disponibili backup.
- Se i File Repository risultano danneggiati o perduti e si dispone di copie di backup sia del database di sistema CMS che dei File Repository, vedere Ripristino di un sistema della piattaforma SAP BusinessObjects Business Intelligence quando sono disponibili backup.
- Se i File Repository sono danneggiati o sono andati perduti e non sono disponibili copie di backup sia del database di sistema CMS che dei File Repository, ma è stato eseguito il backup del contenuto in un file BIAR, vedere Ripristino di un sistema della piattaforma SAP BusinessObjects Business Intelligence quando non sono disponibili backup.
- Se la configurazione dei server non è corretta, si desidera riportare l'intero sistema a uno stato precedente e sono disponibili copie di backup sia del database di sistema CMS che dei File Repository, vedere Ripristino di un sistema della piattaforma SAP BusinessObjects Business Intelligence quando sono disponibili backup.

Prima di ripristinare il database di sistema CMS o i File Repository, è necessario:

1. Arrestare la piattaforma SAP BusinessObjects Business Intelligence.
2. Eseguire un backup del database di sistema CMS e dei File Repository correnti.

Nota:
Se non si dispone di copie di backup sia del database di sistema CMS che dei File Repository e non è stato eseguito un backup delle impostazioni di configurazione del server in un file BIAR né dei File Repository in un file LCMBIAR, non è possibile ripristinare il sistema.

Argomenti correlati

- Strumento Repository Diagnostic Tool

11.1.4.1 Ripristino di un sistema della piattaforma SAP BusinessObjects Business Intelligence quando sono disponibili backup

In questo workflow si presume quanto segue:

- È disponibile un backup del database di sistema CMS
- È disponibile un backup dei File Repository

Se il database di sistema CMS o uno dei File Repository Server risulta mancante o danneggiato, ripristinare il database di sistema CMS e i File Repository dai backup correnti.

Nota:

Quando si ripristina il database di sistema CMS o i File Repository da un backup, è necessario ripristinare sia il database che i File Repository dai backup eseguiti per entrambi alla stessa ora. Per assicurarsi che non vi siano incoerenze tra CMS e File Repository, non ripristinare l'uno senza ripristinare anche gli altri. Per ripristinare il database di sistema CMS, utilizzare gli strumenti per il backup e il ripristino messi a disposizione dal fornitore del database. Il ripristino dei File Repository consiste nel ripristino da un backup dei file disponibili nelle cartelle specificate dalle proprietà “Directory archivio file” degli Input e Output File Repository Server. Il ripristino deve essere eseguito utilizzando gli strumenti per il backup e il ripristino del file system.

Non è necessario ripristinare il file system del computer in cui è installata la piattaforma BI quando si ripristina il database di sistema CMS o i File Repository.

1. Ripristinare il database di sistema CMS da un backup disponibile.
2. Ripristinare i File Repository da un backup disponibile.

   Nota:
   è possibile ripristinare entrambi i componenti in parallelo per ridurre i tempi di inattività.

Il sistema della piattaforma BI viene riportato allo stesso stato in cui si trovava prima del backup, inclusi il contenuto del sistema, gli utenti e le impostazioni del server.

Al termine del ripristino:

1. Eseguire Repository Diagnostic Tool (RDT) per assicurarsi che non vi siano incoerenze tra il database di sistema CMS e i File Repository. Per ulteriori informazioni sull'utilizzo di Repository Diagnostic Tool, consultare il *Manuale dell'utente di Repository Diagnostic Tool della piattaforma SAP BusinessObjects Business Intelligence*.
2. Avviare la piattaforma BI e verificare che il sistema funzioni correttamente.

La decisione di avviare prima la piattaforma BI e successivamente eseguire lo strumento RDT o di eseguire prima lo strumento RDT e poi avviare la piattaforma BI dipenderà da quanto è importante riportare in linea il sistema il più presto possibile. Eventuali incoerenze rilevate dallo strumento RDT non vengono risolte finché RDT non viene completato.

11.1.4.2 Ripristino di un sistema della piattaforma SAP BusinessObjects Business Intelligence quando non sono disponibili backup

Se il database di sistema CMS o uno dei File Repository risulta perduto o danneggiato e non sono disponibili backup, è possibile ricreare il sistema se è stato eseguito un backup delle impostazioni del server di sistema in un file BIAR ed è stato eseguito il backup del contenuto Business Intelligence in un file LCMBIAR.

1. Ricreare il database di sistema CMS in Central Configuration Manager (CCM).

   Il database di sistema CMS viene riportato allo stato predefinito e vengono cancellati tutti i contenuti.

2. Ripristinare le impostazioni del server dal file BIAR, utilizzando Central Configuration Manager (CCM) o lo script `RestoreCluster`.
3. Utilizzare Lifecycle Management Console per ripristinare il contenuto Business Intelligence dal file LCMBIAR.

   Per ulteriori informazioni sulla gestione del ciclo di vita, consultare il *Manuale dell'utente di Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0*.

Argomenti correlati

- Ricreazione del database di sistema CMS
- Ripristino delle impostazioni server

11.1.4.3 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 del protocollo SSL

11.1.4.3.1 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 del sistema.

1. Arrestare tutti i nodi su tutti i computer inclusi nel cluster per i quali è in corso il ripristino delle impostazioni di configurazione server arrestando il 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. Quando viene richiesto, accedere al CMS immettendo il nome del CMS e il nome utente e la password di un account con privilegi amministrativi, quindi fare clic su **Avanti** per continuare.
7. Specificare la posizione e il nome del file BIAR che contiene le impostazioni di configurazione del server da ripristinare, quindi fare clic su **Avanti** per continuare.

   Viene visualizzata una schermata di riepilogo in cui sono contenute le informazioni fornite.
8. Fare clic su **Fine** per continuare.

   Viene visualizzato un messaggio di avviso in cui si è informati che le impostazioni server esistenti verranno sovrascritte dai valori specificati nel file BIAR. Se si continua a eseguire questa procedura, le impostazioni server correnti verranno perse.
9. 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 alla procedura di ripristino vengono scritti in un file di registro. Il nome e il percorso del file di registro vengono visualizzati in una finestra di dialogo.
10. Se l'operazione di ripristino non riesce, verificare il file di registro per identificare il motivo.
11. 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 e non nel sistema prima del ripristino. Vengono eliminati i nodi e i server esistenti nel sistema ma non nel file BIAR.

Dopo aver ripristinato le impostazioni server del cluster, è necessario creare nuovamente i nodi del sistema in ogni computer del cluster.

Argomenti correlati

- Ricreazione di un nodo

11.1.4.3.2 Ripristino delle impostazioni del server con CCM in UNIX

Sui computer UNIX utilizzare lo script `serverconfig.sh` per ripristinare le impostazioni del server della distribuzione da un file BIAR.

1. Selezionare 6 - Ripristina configurazione server e premere Invio.
2. Immettere un numero di porta per il server CMS (Central Management Server) temporaneo da utilizzare e premere Invio.
3. Nelle schermate successive specificare le informazioni di connessione al database di sistema CMS.
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 da cui eseguire il ripristino delle impostazioni di configurazione e premere Invio.

   Le informazioni fornite vengono visualizzate in una schermata di riepilogo.
6. Verificare che le informazioni visualizzate sullo schermo 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.

11.1.4.3.3 Ripristino delle impostazioni del server con uno script

Se si preferisce, è possibile ripristinare le impostazioni del 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 Business Intelligence platform 4.0\win64_x64\scripts`.

In UNIX, `restorecluster.sh` si trova in `/<INSTALLDIR>/sap_bobj/enterprise_xi40/<platform64>/scripts`.

Per informazioni sui parametri utilizzati dallo script, consultare Parametri di BackupCluster e RestoreCluster.

11.1.4.4 Ripristino del contenuto Business Intelligence

Se è stato eseguito il backup del contenuto Business Intelligence nei file LCMBIAR, è possibile ripristinare il contenuto senza dover ripristinare l'intero sistema utilizzando Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0. Per ulteriori informazioni, consultare il *Manuale dell'utente di Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0*.

11.1.5 Ripristino di file perduti o danneggiati della piattaforma SAP BusinessObjects Business Intelligence se è disponibile un backup

Se il database di sistema CMS e i repository dei file funzionano correttamente, ma i file di configurazione della piattaforma SAP BusinessObjects Business Intelligence mancano o sono danneggiati e sono disponibili backup dei file, ripristinare il file system dalla copia di backup. Per ripristinare un file system, è necessario ripristinare il database di sistema CMS e i repository dei file del sistema.

11.1.6 Ripristino di un sistema della piattaforma SAP BusinessObjects Business Intelligence quando i file sono andati perduti

In questa procedura si presume che siano disponibili:

- Un backup del database di sistema CMS
- Un backup dei contenuti dei File Repository Server

Se il file system del computer in cui è installata la piattaforma SAP BusinessObjects Business Intelligence va perduto o viene danneggiato e non si ha a disposizione un backup del file system, si può tentare di recuperarlo reinstallando la piattaforma SAP BusinessObjects Business Intelligence nello stesso computer o in un computer diverso.

1. Eseguire una nuova installazione della piattaforma SAP BusinessObjects Business Intelligence con le stesse opzioni dell'installazione originale. La nuova installazione deve avere lo stesso numero di nodi dell'installazione originale. I nomi dei nodi devono essere gli stessi dell'installazione originale. La piattaforma SAP BusinessObjects Business Intelligence deve essere installata nella stessa cartella dell'installazione originale. Quando si installa la piattaforma SAP BusinessObjects Business Intelligence, specificare il database di sistema CMS già esistente come database.

   Nota:
   quando si seleziona il database di sistema CMS esistente durante l'installazione, nella schermata "Configura database repository CMS" è fondamentale verificare che la casella di controllo **Reimposta database esistente** sia deselezionata. In caso contrario, verrà eliminato tutto il contenuto del database esistente.

2. Ripristinare i File Repository da un backup disponibile.

11.1.7 Parametri di `BackupCluster` e `RestoreCluster`

Nella tabella che segue sono riportati i parametri della riga di comando utilizzati con lo script `Backup Cluster`.

Tabella 11 - 1: 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 `Restore Cluster`.

Tabella 11 - 2: 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:
si consiglia di eseguire lo script `RestoreCluster` con il parametro `-displaycontents` per visualizzare i contenuti del file BIAR prima di ripristinare le impostazioni del server.

I seguenti parametri sono necessari se si esegue il backup delle impostazioni del server da un sistema non in esecuzione oppure se si stanno ripristinando le impostazioni del server.

Tabella 11 - 3: 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 6400
`-dbdriver`	Il driver di database del data base di sistema CMS. I valori accettati sono: • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem	-dbdriver sqlserverdatabasesubsystem
`-connect`	La stringa di connessione al database di sistema CMS. **Nota:** A causa delle limitazioni del prompt dei comandi, è necessario utilizzare l'accento circonflesso (^) per ignorare gli spazi, il simbolo di uguaglianza (=) e il punto e virgola (;) nella stringa `-connect`. 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.	-connect "DSN^=BusinessObjects^ CMS^ 140^;UID^=username^;PWD^=Password1^;HOSTNAME^=database^;PORT^=3306"

Nome	Descrizione	Esempio
-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
```

Gestione del ciclo di vita

12.1 Console di gestione del ciclo di vita

Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0 è uno strumento basato sul Web che consente di spostare le risorse di BI da un sistema all'altro, senza influire sulle dipendenze di tali risorse. Consente inoltre di gestire versioni diverse di risorse BI, gestire dipendenze delle risorse BI e di eseguire il rollback di una risorsa promossa per ripristinare il sistema di destinazione allo stato precedente.

Lo strumento Lifecycle Management Console è un plug-in dell'applicazione della piattaforma SAP BusinessObjects Business Intelligence. È possibile promuovere una risorsa BI da un sistema all'altro solo se nel sistema di origine e nel sistema di destinazione è installata la stessa versione dell'applicazione della piattaforma SAP BusinessObjects Business Intelligence.

In SAP BusinessObjects sono disponibili gli strumenti seguenti, che consentono di importare oggetti tra due distribuzioni della piattaforma SAP BusinessObjects Business Intelligence appartenenti allo stesso numero di versione.

- Console di gestione del ciclo di vita

  Per ulteriori informazioni sull'utilizzo di Lifecycle Management Console, consultare il *Manuale dell'utente di Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0*.

- Strumento della riga di comando BIAR

  Per ulteriori informazioni sull'utilizzo dello strumento da riga di comando BIAR, consultare il *Manuale dell'utente di Lifecycle Management Console per la piattaforma SAP BusinessObjects Business Intelligence 4.0*.

12.2 Impostazioni del sistema di gestione delle versioni per la console di gestione del ciclo di vita

12.2.1 Impostazioni del sistema di gestione delle versioni per la console di gestione del ciclo di vita

- Quando si installa il sistema Subversion di Lifecycle Management Console insieme alla piattaforma SAP BusinessObjects Business Intelligence, le impostazioni di configurazione vengono eseguite automaticamente.
- Se tuttavia si desidera configurare il sistema Subversion di Lifecycle Management Console già installato, immettere i valori appropriati nella pagina "Impostazioni sistema gestione versioni" delle **Opzioni di amministrazione** dello strumento Lifecycle Management Console.

  La seguente figura mostra i valori appropriati da specificare nella pagina "Impostazioni VMS":

- Se il sistema Subversion per la gestione del ciclo di vita viene installato dopo l'installazione della piattaforma SAP BusinessObjects Business Intelligence,

  Nota:
  verificare che il servizio Subversion sia in esecuzione e che sia stato creato il repository;

  1. immettere i valori appropriati nella pagina "Impostazioni sistema gestione versioni" delle **Opzioni di amministrazione** dello strumento Lifecycle Management Console;
  2. riavviare il SIA.

12.3 Strumento della riga di comando motore BIAR

Lo strumento della riga di comando del motore BIAR consente agli amministratori e agli amministratori delegati di promuovere il contenuto tra ambienti di sviluppo, controllo qualità e produzione della piattaforma SAP BusinessObjects Business Intelligence. Lo strumento utilizza script per automatizzare le operazioni di importazione ed esportazione degli oggetti.

Lo strumento della riga di comando del motore BIAR supporta solo la migrazione di oggetti da un sistema della piattaforma SAP BusinessObjects Business Intelligence 4.0 a un altro. Non è possibile utilizzare lo strumento per importare gli oggetti da BusinessObjects , Crystal Enterprise o versioni precedenti della piattaforma SAP BusinessObjects Business Intelligence. Per importare il contenuto delle versioni precedenti, è necessario utilizzare Upgrade Management Tool della piattaforma SAP BusinessObjects Business Intelligence.

Lo strumento della riga di comando del motore BIAR è denominato `biarengine.jar`. In un ambiente Windows questo file si trova in `<DirInstallaz>\SAP BusinessObjects Enterprise XI 4.0\java\lib`. In UNIX, il file si trova in `<DirInstallaz>/sap_bobj/java/lib/`.

Nota:

- È necessario avere installato Java Runtime Environment. Per un elenco di JRE supportati, consultare la guida in linea delle piattaforme supportate per la piattaforma SAP BusinessObjects Business Intelligence nel sito Web del Supporto tecnico.
- Per utilizzare lo strumento della riga di comando del motore BIAR, è necessario disporre delle credenziali dell'account Administrator per l'ambiente in cui o da cui si importa il contenuto. È anche possibile utilizzare un account amministratore autorizzato.
- L'utilizzo dello strumento della riga di comando del motore BIAR per importare i file BIAR generati da Upgrade Management Tool della piattaforma SAP BusinessObjects Business Intelligence non è supportato.

Lo strumento della riga di comando del motore BIAR importa i seguenti tipi di oggetti:

Connessioni di analisi	Documenti Web Intelligence
Spazi di lavoro di analisi	Utenti LDAP
Documenti generali	LOV (List Of Values)
Oggetti analitici	Pacchetti di oggetti
Oggetti BI Modeler	Sovraccarichi
Spazi di lavoro BI	PDF
Viste aziendali	Presentazioni PowerPoint
Calendari	Profili
Categorie	Oggetti programma
Azioni client	Gruppi prompt
Ruoli personalizzati	Pubblicazioni
Documenti di Dashboard Design	Query come servizio Web
Discussions	Report
Enciclopedie	Istanze di report
Gruppi di utenti Enterprise	Documenti RTF (Rich Text Format)
Utenti aziendali	Gruppi di server
Eventi	Tasti di scelta rapida
Fogli di calcolo Excel	File di testo
File Flash	Universi
Cartelle	Utenti WinAD
Componenti aggiuntivi Full Client	Documenti di Word
Modelli Full Client	Modelli Xcelsius DMT
Collegamenti ipertestuali	

Importazione di relazioni

Lo strumento della riga di comando del motore BIAR mantiene intatte le relazioni tra gli oggetti importati solo se gli oggetti vengono importati insieme o se uno degli oggetti è già presente nel sistema di destinazione. Ad esempio, se si importa un report Web Intelligence che utilizza un universo senza importare l'universo, la relazione tra i due oggetti viene persa. Il report non potrà essere eseguito nel sistema di destinazione.

Importazione di utenti e gruppi

Se si importano gruppi e utenti in un sistema della piattaforma SAP BusinessObjects Business Intelligence e uno dei gruppi è già presente nel sistema di destinazione, l'appartenenza al gruppo nella destinazione viene sovrascritta con l'appartenenza al gruppo esportata dal file BIAR. Ciò significa che se nel gruppo nel sistema di destinazione sono presenti utenti aggiuntivi che non sono contenuti nel gruppo nel file BIAR, tali utenti non faranno parte del gruppo dopo l'importazione.

Importazione dei diritti

Lo strumento della riga di comando del motore BIAR importa i diritti su un oggetto solo se l'utente o il gruppo viene esportato con l'oggetto o esiste già nella destinazione.

Se l'oggetto e l'utente o gruppo esistono già nel sistema di destinazione, i diritti importati per tale oggetto e tale utente sovrascriveranno i diritti esistenti nel sistema di destinazione.

Se tuttavia un oggetto esiste già nella destinazione e un utente o gruppo ha diritti specifici su tale oggetto nella destinazione, ma non viene specificato nessun diritto per questo utente o gruppo sull'oggetto nel file BIAR, i diritti esistenti per l'utente o gruppo non vengono rimossi dallo strumento.

Ciò significa che i diritti esistenti su un oggetto di destinazione possono essere sovrascritti, ma non rimossi.

Utilizzo di più file BIAR

Quando si utilizza lo strumento della riga di comando del motore BIAR per esportare contenuto, il contenuto viene inserito in un file BIAR. Il percorso e il nome del file BIAR sono determinati dal parametro *`exportBiarLocation`*. Quando si esporta contenuto che supera la quantità di informazioni che è possibile archiviare in un solo file BIAR, le informazioni vengono suddivise dallo strumento e archiviate in più file BIAR. Per i file viene utilizzato il nome specificato alla fine del quale viene aggiunto un numero.

Ad esempio, se si imposta `exportBiarLocation = C:\Archive.biar` e si esporta più contenuto di quanto possa essere inserito in un unico file BIAR, lo strumento crea i file `Archive.biar`, `Archive1.biar`, `Archive2.biar` e così via. I file vengono creati dallo strumento nella directory `C:`.

Nota:
Per importare contenuto archiviato in più file BIAR, è necessario assicurarsi che tutti i file BIAR si trovino nella stessa directory.

12.3.1 Utilizzo di un file delle proprietà

Lo strumento della riga di comando del motore BIAR richiede un file delle proprietà contenente i parametri che indicano al motore BIAR quali azioni eseguire, il sistema della piattaforma SAP BusinessObjects Business Intelligence a cui connettersi e così via.

Il file deve avere estensione `.properties`. Ad esempio `proprietà.properties`

Il file delle proprietà può includere i parametri seguenti.

Parametro	Valori consentiti	Descrizione	Esempio
Azione	exportXML, importXML	Specifica se lo strumento importa contenuto da un file BIAR in un sistema della piattaforma SAP BusinessObjects Business Intelligence o esporta contenuto da una distribuzione in un file BIAR. Obbligatorio	Action=exportXML
exportBiarLocation	Testo libero. Deve includere l'estensione `.biar`.	Specifica il percorso in cui lo strumento salva il file BIAR esportato. Obbligatorio se action=exportXML.	exportBiarLocation=C:/BiarExportFile.biar
importBiarLocation	Testo libero. Deve includere l'estensione `.biar`.	Specifica il percorso in cui si trova il file BIAR da importare. I file BIAR vengono suddivisi se il contenuto è troppo grande per essere inserito in un solo file BIAR. È possibile immettere qualsiasi partizione di file BIAR, ma è necessario assicurarsi che tutte le partizioni si trovino nella stessa directory. Obbligatorio se action=importXML.	importBiarLocation=C:/BiarImportFile.biar

Parametro	Valori consentiti	Descrizione	Esempio
userName	Testo libero.	Il nome utente dell'account amministratore che lo strumento dovrà utilizzare per connettersi al Central Management Server (CMS). Può essere il nome utente di un account amministratore autorizzato. Obbligatorio	userName=Amministratore
password	Testo libero.	La password per l'account amministratore. Obbligatorio	password=password
autenticazione	secEnterprise, secWinAd, secLdap	Il tipo di autenticazione utilizzato dallo strumento. Facoltativo. Se non si specifica un tipo di autenticazione, il valore predefinito è secEnterprise.	authentication=secEnterprise
CMS	Testo libero.	Il nome del CMS a cui connettersi. Obbligatorio	CMS=cms:6400

Parametro	Valori consentiti	Descrizione	Esempio
exportDependencies	True, False	Specifica se importare tutte le dipendenze di un oggetto. È opportuno utilizzare con attenzione questa opzione poiché importa tutti gli oggetti associati con qualsiasi oggetto selezionato. In questo modo le dimensioni di un file BIAR potrebbero essere aumentate notevolmente. Facoltativo. Se non si specifica un valore, l'impostazione predefinita è False. Utilizzato solo se ac tion=exportXML.	exportDependen cies=false
includeSecurity	True, False	Specifica se tramite l'esecuzione dello strumenti viene esportata o importata la protezione associata agli oggetti e agli utenti selezionati Per mantenere la protezione è importante impostare *in cludeSecurity* su true quando si esporta e si importa il contenuto. **Nota:** Se si utilizzano i livelli di accesso, è necessario esportare esplicitamente questi oggetti. Facoltativo. Se non si specifica un valore, l'impostazione predefinita è True.	includeSecurity=false

Parametro	Valori consentiti	Descrizione	Esempio
exportQuery	Testo libero. Deve utilizzare il formato del linguaggio di query CMS.	Specifica le query che lo strumento deve eseguire per raccogliere gli oggetti da esportare. È possibile utilizzare il numero di query desiderato in un solo file di proprietà, ma le query devono essere denominate “exportQuery1”, “exportQuery2” e così via. Obbligatorio se action=exportXML.	exportQuery=select * from ci_Infoobjects dove si_name = 'Xtreme Employees' e si_kind = 'Webi'
exportQueriesTotal	Numeri interi positivi.	Specifica quante query di esportazione vengono eseguite dallo strumento. Se sono presenti “x” query di esportazione e si desidera eseguirle tutte, impostare questo parametro su “x”. Facoltativo. Se non si specifica un valore per questo parametro, l'impostazione predefinita è 1. Utilizzato solo se action=exportXML.	exportQueriesTotal=5

Nota:
Per contrassegnare le righe come commento, utilizzare il carattere #. Ad esempio:

```
action=importXML
#exportLocation=C:/mybiar.biar
importLocation=C:/mybiar.biar
```

Di seguito viene fornito un esempio di file di proprietà che importa contenuto da un file BIAR:

```
#This file imports a biar, note this line is a comment
importBiarLocation=C:/CR.biar
action=importXML
userName=Administrator
password=
CMS=mycms:6400
authentication=secEnterprise
```

Si tratta di un esempio di file di proprietà che esporta un report Web Intelligence denominato “Dipendenti Xtreme” in un file BIAR:

```
#This file exports a single report
# Remember to include indexed properties with your query!
# The more indexed properties, the better!
exportBiarLocation=C:/CR.biar
action=importXML
userName=Administrator
password=
CMS=mycms:6400
authentication=secEnterprise
exportDependencies=false
exportQuery= select * from ci_Infoobjects where si_name = 'Xtreme Employees' and si_kind = 'Webi'
```

12.3.2 Utilizzo dello strumento della riga di comando del motore BIAR

1. Aprire una finestra della riga di comando e passare alla directory in cui si trova il file `biarengine.jar`.

   Ad esempio, *<DirInstallaz>*`\SAP BusinessObjects Enterprise XI4.0\java\lib`.

2. Eseguire il file `biarengine.jar`.

   Ad esempio, `java -jar biarengine.jar` *<file di proprietà>*

   Lo strumento della riga di comando del motore BIAR consente di esportare il contenuto dalla distribuzione della piattaforma SAP BusinessObjects Business Intelligence in un file BIAR oppure di importare il contenuto da un file BIAR in una distribuzione della piattaforma SAP BusinessObjects Business Intelligence, a seconda del parametro di azione nel file di proprietà.

Gestione delle applicazioni

13.1 Gestione delle applicazioni mediante CMC

13.1.1 Presentazione

L'area "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:

- Analysis, versione per OLAP
- Avvisi
- BI Launch Pad
- Spazi di lavoro BI
- Central Management Console
- Crystal Reports
- Dashboard Design
- Discussions
- Information Designer
- Web Intelligence
- LifeCycle Manager
- Monitoraggio
- OpenDocument
- Ricerca piattaforma
- Strumento di conversione dei report
- SAP BusinessObjects Mobile
- Translation Management Tool
- Universe Design Tool
- Upgrade Management Tool

- Applicazione Differenza visiva
- Servizio Web
- Widget per la piattaforma SAP BusinessObjects Business Intelligence

13.1.2 Impostazioni comuni per le applicazioni

13.1.2.1 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* .

13.1.2.2 Impostazione del livello del registro di analisi delle applicazioni Web nella CMC

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

Per analizzare tutte le altre applicazioni Web, utilizzare il metodo manuale per configurare il file `BO_Trace` corrispondente.

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

   Viene visualizzata la finestra di dialogo "Applicazioni".

2. Fare clic con il pulsante destro del mouse sull'applicazione e scegliere **Impostazioni registro di analisi**.

   Viene visualizzata la finestra di dialogo "Impostazioni registro di analisi".

3. Selezionare l'impostazione desiderata nell'elenco **Livello di registrazione**.
4. Fare clic su **Salva e chiudi** per inviare il livello del registro di analisi.

Il nuovo livello del registro di analisi sarà effettivo al successivo accesso all'applicazione Web.

Argomenti correlati

- Livelli del registro di analisi

13.1.2.2.1 Livelli del registro di analisi

Nella tabella seguente sono descritti i livelli del registro di analisi disponibili per i componenti della piattaforma BI:

Livello	Descrizione
Non specificato	Il livello del registro di analisi viene specificato mediante un altro meccanismo, in genere un file con estensione `ini`.
Nessuno	Quando il livello del registro di analisi è impostato su "Nessuno", il filtro che consente di sopprimere le analisi al di sotto di un livello di importanza specificato è disattivato. **Nota:** il livello del registro di analisi "Nessuno" non indica che la funzione di analisi è disattivata. Le risorse di sistema continuano a essere monitorate e le analisi vengono registrate per eventi critici rari quali asserzioni non riuscite.
Basso	Il filtro del registro di analisi è impostato in modo da consentire la registrazione dei messaggi di errore ignorando i messaggi di avviso e la maggior parte dei messaggi di stato. Verranno comunque registrati i messaggi di stato più importanti, ad esempio quelli per l'avvio e la chiusura dei componenti o i messaggi di richiesta di avvio e chiusura. **Nota:** 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 nell'output del registro i messaggi di errore, avviso e la maggior parte dei messaggi di stato. I messaggi di stato meno importanti o con un livello di dettaglio elevato verranno esclusi dal filtro. Questo livello non è sufficientemente dettagliato per le finalità di debug.
Alto	Il filtro non escluderà alcun messaggio. L'impostazione di questo livello è consigliata per le finalità di debug. **Nota:** un livello di registro di analisi "Alto" potrebbe avere un impatto negativo sulle risorse di sistema. Potrebbe comportare un utilizzo maggiore della CPU nonché richiedere una quantità di spazio di archiviazione maggiore nel file system.

13.1.3 Impostazioni specifiche dell'applicazione

13.1.3.1 Gestione delle impostazioni dell'applicazione CMC

13.1.3.1.1 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 console 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". Nel menu **Azioni** fare clic su **Diritti oggetto programma**. Fare clic su **Pianifica con le seguenti credenziali del sistema operativo** e fornire 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 i Program Job Server in esecuzione sullo stesso computer.
- Per impostazione predefinita, il file dei criteri Java è installato nella directory dell'SDK Java nella directory principale di installazione della piattaforma BI. Una posizione tipica di Windows è ad

esempio: `C:\Programmi\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\conf\crystal-program.policy`

Per abilitare o disabilitare 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 BI.
4. Fare clic su **Salva e chiudi**.

13.1.3.1.2 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. Il programma di 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.

Argomenti correlati

- Condivisione delle estensioni di elaborazione tra più server

Per registrare un'estensione di elaborazione nel sistema

1. Passare all'area di gestione "Applicazioni" della CMC.
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 è valida per i documenti o i report Web Intelligence creati nella piattaforma BI.

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 sono 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 eseguire questa operazione, aggiungere `-report_ProcessExt Path`*`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.

13.1.3.2 Gestione delle impostazioni di Discussions

Nell'area "Applicazioni" della CMC della piattaforma BI è possibile specificare le impostazioni del livello di sistema per i thread di discussione.

L'applicazione "Discussions" 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 Discussions. È tuttavia possibile impostare diritti sui singoli report.

13.1.3.2.1 Per ricercare un thread di discussione

Per impostazione predefinita, nella pagina "Discussions" 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** > **Proprietà**.
   Verrà 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**.

13.1.3.2.2 Per ordinare i 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** > **Proprietà**.

   Verrà 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**.

13.1.3.2.3 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** > **Proprietà**.

   Verrà 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**.

13.1.3.3 Gestione delle impostazioni di BI Launch Pad

Nell'area "Applicazioni" della console CMC nella piattaforma BI è possibile modificare le opzioni di visualizzazione di BI Launch Pad scegliendo **Gestisci** > **Proprietà**.

Per BI Launch Pad è possibile concedere a utenti o gruppi la capacità di:

- Modificare le preferenze
- Organizzare le cartelle
- Cerca
- Filtrare gli elenchi di oggetti per tipo di oggetto
- Visualizzare la cartella Preferiti

Ad esempio, se sono già state create cartelle degli utenti utilizzando una convenzione di denominazione standard, può essere opportuno negare agli utenti la possibilità di organizzare le proprie cartelle.

Nota:
per impostazione predefinita, tutti gli utenti hanno accesso a queste funzioni.

13.1.3.3.1 Modifica delle impostazioni di visualizzazione di BI Launch Pad

1. Passare all'area "Applicazioni" della CMC e selezionare **BI Launch Pad**.
2. Fare clic su **Gestisci** > **Proprietà**.

   Viene visualizzata la finestra di dialogo "Proprietà di BI Launch Pad".
3. Per abilitare Discussions per gli utenti di BI Launch Pad, selezionare **Abilita discussioni**.
4. Per abilitare la funzionalità dei filtri per la pianificazione, selezionare la scheda **Mostra filtri nella pagina Pianificazione**.

   Questa impostazione controlla se gli utenti possono immettere formule di selezione di record o gruppi quando pianificano un report Crystal.
5. Fare clic su **Salva e chiudi**.

13.1.3.4 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.

13.1.3.4.1 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**.

Verrà visualizzata la finestra di dialogo "Proprietà" con le opzioni di visualizzazione.

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.

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

Nota:
Per riselezionare le variabili di visualizzazione predefinite, scegliere **Reimposta**.

13.1.3.5 Gestione delle impostazioni di avviso

Nell'area "Applicazioni" della CMC della 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
- Gestione delle impostazioni di avviso

13.1.3.5.1 Modifica delle proprietà della destinazione di avviso

1. Passare all'area "Applicazioni" della CMC e selezionare **Applicazione di gestione degli avvisi**.
2. Fare clic su **Gestisci** > **Proprietà**.

   Si aprirà la finestra di dialogo "Avvisi" che visualizzerà le proprietà predefinite di destinazione.
3. Impostare le opzioni appropriate.

Opzione	Descrizione
"Abilita avvisi personali"	Selezionare questa opzione per consentire ai sottoscrittori di avvisi di ricevere notifiche nella sezione "Avvisi personali" di BI Launch Pad.
"Abilita posta elettronica"	Selezionare questa opzione per consentire ai sottoscrittori di avvisi di ricevere notifiche via posta elettronica. Quando si seleziona questa opzione, vengono visualizzate le impostazioni globali di posta elettronica per gli avvisi.

Nota:
è necessario specificare una o entrambe le opzioni di destinazione soprastanti.

Se è stata selezionata l'opzione "Abilita posta elettronica", sarà possibile modificare le seguenti impostazioni globali:

Opzione	Descrizione
"Da"	Specifica l'indirizzo di posta elettronica da cui vengono inviate le notifiche di avviso. I sottoscrittori riceveranno messaggi di posta elettronica di avviso dal mittente specificato. È consigliabile utilizzare un indirizzo di posta elettronica valido riconosciuto dal sistema.
"A"	Specifica l'indirizzo di posta elettronica del sottoscrittore a un avviso. **Suggerimento:** è consigliabile mantenere il segnalibro `%SI_EMAIL_ADDRESS%` per questa impostazione. Se si indica un indirizzo di posta elettronica o un destinatario specifico, per impostazione predefinita tutti gli avvisi di sistema verranno inviati a uno specifico indirizzo di posta elettronica.
"Cc"	Specifica quale destinatario o destinatari debbano ricevere gli avvisi in copia conoscenza tramite posta elettronica.
"Oggetto"	Specifica l'oggetto predefinito utilizzato nei messaggi di posta elettronica contenenti gli avvisi di sistema.

Opzione	Descrizione
"Messaggio"	Specifica il messaggio predefinito da includere nei messaggi di posta elettronica contenenti gli avvisi di sistema.
"Aggiungi allegato"	Selezionare questa opzione per abilitare l'inclusione predefinita di allegati nei messaggi di posta elettronica contenenti gli avvisi di sistema. Questa opzione è generalmente utilizzata per includere per impostazione predefinita i Crystal Reports associati agli avvisi attivati.
"Nome file"	Se è stata selezionata l'opzione **Aggiungi allegato**, specificare come vengono nominati gli allegati nei messaggi di posta elettronica selezionando **Generato automaticamente** o **Nome specifico**.

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

Argomenti correlati

- Impostazione dei diritti sulle applicazioni
- Gestione delle impostazioni di avviso

13.1.3.5.2 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 protezione per gli oggetti nella CMC
- Gestione delle impostazioni di avviso

13.1.3.6 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.

Argomenti correlati

- Gestione delle impostazioni di protezione per gli oggetti nella CMC

13.1.3.7 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.

Argomenti correlati

- Gestione delle impostazioni di protezione per gli oggetti nella CMC

13.1.3.7.1 Modifica delle proprietà delle applicazioni SAP BusinessObjects Explorer

1. Accedere all'area "Applicazioni" della console CMC.
2. Scegliere **Gestisci** > **Proprietà**.
   Viene visualizzata la finestra di dialogo "Proprietà" di SAP BusinessObjects Explorer.
3. Definire tutte le impostazioni SAP BusinessObjects Explorer seguenti desiderate:
   - Posizione predefinita della cartella di indice
   - Numero di thread
   - Validità dei segnalibri
4. Fare clic su **Salva e chiudi**.

13.1.3.8 Gestione delle impostazioni di Ricerca piattaforma

Nell'area "Applicazioni" della 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

13.1.3.8.1 Configurazione delle proprietà dell'applicazione

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 desiderate.

   Le proprietà configurabili vengono descritte nella seguente tabella:

Opzione	Descrizione
Statistiche della ricerca	L'applicazione di ricerca piattaforma fornisce le seguenti statistiche della ricerca: • 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	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. Per interrompere l'indicizzazione, fare clic su **Interrompi indicizzazione**, quindi su **OK** nella finestra di dialogo di conferma.

Opzione	Descrizione
Impostazioni internazionali indice	Quando si cambiano le impostazioni locali dell'indice in quelle di un'altra lingua, Ricerca piattaforma reindicizza i documenti nella lingua selezionata. Specificare le impostazioni locali di indicizzazione in una delle lingue seguenti: brasiliano, cinese, ceco, danese, olandese, inglese, finlandese, francese, tedesco, italiano, giapponese, coreano, norvegese (Bokmål), polacco, portoghese, russo, spagnolo, svedese e tailandese. **Nota:** la scelta predefinita per questa opzione è l'Inglese.
Frequenza di ricerca per indicizzazione	È possibile indicizzare l'intero repository della piattaforma BI utilizzando le seguenti opzioni: • Ricerca per indicizzazione continua: questa opzione implica un'indicizzazione continua, ovvero il repository viene indicizzato ogni volta che si aggiunge, modifica o elimina un oggetto. Tale ricerca consente di visualizzare o utilizzare i contenuti più aggiornati della piattaforma SAP BusinessObjects Business Intelligence. La ricerca per indicizzazione continua costituisce l'impostazione predefinita e aggiorna in modo continuativo il repository della piattaforma BI 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. Per ulteriori informazioni sulla pianificazione di un oggetto, consultare la sezione *Pianificazione di un oggetto* di Ricerca piattaforma nella *Guida in linea della CMC della piattaforma BI*. **Nota:** • 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
	Quando i documenti vengono indicizzati, vengono archiviati in cartelle condivise nelle seguenti posizioni: • Posizione indice principale (indici, correttori ortografici): gli indici principale e correttore ortografico archiviati in questa posizione. Durante un flusso di lavoro di ricerca, i riscontri iniziali vengono recuperati mediante l'indice principale, mentre per recuperare i suggerimenti vengono utilizzati gli indici correttore ortografico. In una distribuzione BOE 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. La posizione dei dati persistenti è l'unica posizione di indice interessata dall'ambiente cluster, poiché contiene le cartelle degli archivi contenuto. Se un computer utilizza un solo servizio di ricerca, esisterà solo una posizione dell'archivio contenuti. Ad esempio, {bobj.enterprise.home}\data\PlatformSearchData\workspace\Server\ContentStores. 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: a. {bobj.enterprise.home}\data\PlatformSearchData\workspace\Server\ContentStores. b. {bobj.enterprise.home}\data\PlatformSearchData\workspace\Server1\ContentStores. • 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, i documenti indicizzati 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. **Nota:** • tutte le posizioni degli indici devono essere percorsi condivisi. • È necessario fare clic su **Interrompi indicizzazione** per modificare la posizione dell'indice.

Opzione	Descrizione
	• Se si modifica la posizione di un indice, è necessario copiare il contenuto in una nuova posizione. In caso contrario, le informazioni relative all'indice esistente verranno perdute.

Livello di indicizzazione	È possibile regolare il contenuto della ricerca impostando il livello di indicizzazione nei seguenti modi:
	• 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:
	  • il contenuto effettivo del documento
	  • il contenuto dei prompt e degli elenchi di valori
	  • grafici ed etichette
	Nota:
	quando si modifica il livello di indicizzazione, l'indicizzazione viene reinizializzata per l'intero repository della piattaforma BI.

Tipi contenuto	È possibile selezionare i seguenti tipi di contenuto per l'indicizzazione: • Microsoft Word • Microsoft Excel • Microsoft PowerPoint • Testo • Adobe Acrobat • Rich Text • Crystal Reports • Universo • Web Intelligence

Opzione	Descrizione
Rigenera indice	Questa opzione consente di eliminare tutti i contenuti indicizzati esistenti e di ripetere l'indicizzazione dell'intero documento dall'inizio. È possibile selezionare l'opzione **Rigenera indice** indipendentemente dallo stato di indicizzazione. Tale opzione tuttavia non funziona se l'indicizzazione viene interrotta e si seleziona **Rigenera indice**, quindi si salva e si chiude l'applicazione Ricerca piattaforma. Quando l'indicizzazione viene interrotta e si seleziona **Rigenera indice**, si salva e si chiude l'applicazione Ricerca piattaforma, quindi si riapre la pagina di configurazione e si fa clic su **Avvia indicizzazione**, l'indice rigenerato archiviato eseguirà di nuovo automaticamente l'indicizzazione dell'intero documento. Se non si desidera che Ricerca piattaforma indicizzi nuovamente i documenti, è necessario deselezionare **Rigenera indice** prima di fare clic su **Avvia indicizzazione**.
Documenti esclusi dall'indicizzazione	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. 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. Per impostazione predefinita, solo l'account Administrator ha il controllo completo dei **Documenti esclusi dall'indicizzazione**. Gli altri utenti con i diritti seguenti possono solo aggiungere documenti al gruppo **Documenti esclusi dall'indicizzazione**: • 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 deseleziona gli estrattori, l'indice viene aggiornato in modo incrementale dall'inizio senza che venga eliminato l'indice esistente.

13.2 Gestione delle applicazioni mediante le proprietà BOE.war

13.2.1 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 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*.

13.2.1.1 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
`persistentcookies.enabled`	`persistentcookies.enabled=true`	Abilita o disabilita i cookie permanenti nella pagina di accesso all'applicazione Web.
`siteminder.authentication`	`siteminder.authentication=secLDAP`	Specifica il metodo di autenticazione da utilizzare con SiteMinder. Le uniche opzioni sono secLDAP e secwinAD.
`siteminder.enabled`	`siteminder.enabled=false`	Abilita e disabilita l'autenticazione con SiteMinder.
`sso.enabled`	`sso.enabled=false`	Abilita e disabilita il Single Sign On (SSO) nella piattaforma BI.
`sso.sap.primary`	`sso.sap.primary=false`	Impostare su `true` 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.
`tree.pagesize`	`tree.pagesize=100`	Specifica il numero massimo di voci che è possibile visualizzare nel riquadro di spostamento dell'applicazione Web.
`trusted.auth.shared.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.
`trusted.auth.user.param`	Nessuno	Specifica la variabile utilizzata per recuperare il nome utente per Autenticazione affidabile. Può essere impostato su uno dei valori seguenti: • `Header` • `URL Parameter` • `Cookie` • `Session`

Impostazione	Valori predefiniti	Descrizione
`trusted.auth.user.retrieval`	Nessuno	Specifica il metodo utilizzato per recuperare il nome utente per Autenticazione affidabile. Può essere impostato su uno dei valori seguenti: • `"REMOTE_USER"` • `"HTTP_HEADER"` • `"COOKIE"` • `"QUERY_STRING"` • `"WEB_SESSION"` • `"USER_PRINCIPAL"` Impostare su empty per disabilitare Autenticazione affidabile.
`trusted.auth.user.namespace.enabled`	`trusted.auth.user.namespace.enabled=false`	Abilita e disabilita il collegamento dinamico degli alias ad account utente esistenti. Se la proprietà è impostata su `true`, 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 `false`, Autenticazione affidabile utilizza la corrispondenza dei nomi per autenticare gli utenti.

`vintela.enabled`	`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`
		Utilizzato per abilitare o disabilitare le impostazioni Vintela per l'autenticazione Windows AD.

`pinger.showWarningDialog.cmc`	`pinger.showWarningDialog.cmc=true`	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.bilaunchpad`	`pinger.showWarningDialog.bilaunchpad=true`	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.

Impostazione	Valori predefiniti	Descrizione
pinger.warningPeriod.pingIncrementsInSeconds	pinger.warningPeriod.pingIncrementsInSeconds=15	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	pinger.warningPeriod.lengthInMinutes=5	Specifica con quanto anticipo visualizzare l'avviso prima della scadenza della sessione.
logoff.on.websession.expiry	logoff.on.websession.expiry=true	Specifica se tutte le sessioni dell'applicazione vengono scollegate allo scadere della sessione Web.
pinger.enabled	pinger.enabled=true	Abilita o disabilita il meccanismo di invio di messaggi di avviso relativi alla scadenza della sessione.
system.com.sap.bip.jcomanager.destinations.maxsize	system.com.sap.bip.jcomanager.destinations.maxsize=1000	Specifica il numero massimo di connessioni Java nella cache.

13.2.1.2 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`.

<table>
<tr><th>Impostazione</th><th>Descrizione</th></tr>
<tr><td>app.name</td><td>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</td></tr>
<tr><td>app.name.greeting</td><td>Impostazione predefinita: app.name.greeting=BusinessObjects</td></tr>
<tr><td>app.name.short</td><td>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</td></tr>
<tr><td>app.url.name</td><td>Specifica il nome dell'URL dell'applicazione, preceduto dal carattere “/”". Impostazione predefinita: app.url.name=/BI</td></tr>
<tr><td>authentication.default</td><td>Specifica il metodo di autenticazione predefinito utilizzato per autenticare gli utenti nell'applicazione. È possibile utilizzare uno dei valori seguenti per questa impostazione:
<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>
Impostazione predefinita: authentication.default=secEnterprise</td></tr>
<tr><td>authentication.visible</td><td>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</td></tr>
<tr><td>cms.default</td><td>Specifica il nome CMS predefinito. Impostazione predefinita: cms.default=[name of host machine]</td></tr>
<tr><td>cms.visible</td><td>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</td></tr>
<tr><td>dialogue.prompt.enabled</td><td>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</td></tr>
</table>

Impostazione	Descrizione
`logontoken.enabled`	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: `logontoken.enabled=false`
`SMTPFrom`	Abilita o disabilita il campo "From" durante la pianificazione di un oggetto in una destinazione. Impostazione predefinita: `SMTPFrom=true`
`url.exit`	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.
`disable.locale.preference`	Abilita o disabilita la visualizzazione e la conseguente modifica delle preferenze di visualizzazione locali dell'utente relative a BI Launch Pad. Impostazione predefinita: `disable.locale.preference=false`
`extlogon.allow.logoff`	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: `extlogon.allow.logoff=true`

13.2.1.3 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`	Specifica il metodo di autenticazione predefinito utilizzato per autenticare gli utenti nell'applicazione. È possibile utilizzare uno dei valori seguenti per questa impostazione: **Autenticazione** — **Valore di impostazione** Enterprise — `SecEnterprise` LDAP — `secLDAP` Windows AD — `secWinAD` SAP — `secSAPR3` PeopleSoft — `secpsenterprise` JD Edwards — `secPSE1` Siebel — `secSiebel7` Oracles EBS — `secOraApps` Impostazione predefinita: `authentication.default=secEnterprise`
`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]`

Impostazione	Descrizione
`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`

13.2.1.4 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`.

<table>
<tr><th>Impostazione</th><th>Descrizione</th></tr>
<tr><td>app.url.name</td><td>Specifica il nome dell'URL dell'applicazione, preceduto dal carattere “/”". Impostazione predefinita: app.url.name=/CMC</td></tr>
<tr><td>authentication.default</td><td>Specifica il metodo di autenticazione predefinito utilizzato per autenticare gli utenti nell'applicazione. È possibile utilizzare uno dei valori seguenti per questa impostazione:
<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>
Impostazione predefinita: authentication.default=secEnterprise</td></tr>
<tr><td>authentication.visible</td><td>Specifica se gli utenti che accedono alla CMC hanno la possibilità di visualizzare e modificare il metodo di autenticazione. Impostazione predefinita: authentication.visible=false</td></tr>
<tr><td>cms.default</td><td>Specifica il nome CMS predefinito. Impostazione predefinita: cms.default=[name of host machine]</td></tr>
</table>

Impostazione	Descrizione
`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`
`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`
`logontoken.enabled`	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: `logontoken.enabled=false`

13.3 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*.

13.3.1 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 13 - 2: 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 13 - 3: 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

13.3.2 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.

13.3.3 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` file 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="..."
```

5. Ridistribuire l'applicazione Web e riavviare il server Web.

Argomenti correlati

- Abilitazione dell'Autenticazione affidabile

13.4 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 con autorizzazione per l'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 accedono ai dati dal portale SAP NetWeaver o da BI Launch Pad. 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:
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.
- L'elemento Web **Report** non è supportato. 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 BusinessObjects Business Intelligence.
- 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.

Per ulteriori informazioni sulle funzionalità delle applicazioni Web BEx, vedere il SAP Help Portal all'indirizzohttp://help.sap.com: **SAP NetWeaver 7.0 (2004s)** > **SAP NetWeaver Library** > **SAP NetWeaver By Key Capability** > **Information Integration by Key Capability** > **Business Intelligence** > **BI Suite: 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

13.4.1 Avvio di un server 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 **Seleziona servizi** nel menu di scelta rapida.
5. Selezionare **BExWebApplicationsService** nell'elenco **Servizi disponibili** e spostarlo nell'elenco **AdaptiveProcessingServerServices**.
6. Attivare e avviare le applicazioni BEx Web utilizzando il menu di scelta rapida.

13.4.2 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 server richiesto nella casella **Duplica su nodo**.
6. Selezionare il server duplicato e scegliere **Seleziona servizi** nel menu di scelta rapida.
7. Selezionare **BExWebApplicationsService** nell'elenco **Servizi disponibili** e spostarlo nell'elenco **AdaptiveProcessingServerServices**.
8. Attivare e avviare le applicazioni BEx Web utilizzando il menu di scelta rapida.

13.4.3 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 servizio 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 seguenti impostazioni.
   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 servizio applicazioni Web BEx e scegliere **Riavvia il 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

13.4.4 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. In caso negativo, configurarne 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.

13.4.5 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

13.4.5.1 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 la 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

Gestione di connessioni e universi

14.1 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

14.1.1 Per eliminare 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**.

14.2 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)

14.2.1 Per eliminare gli 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

15.1 Informazioni sul monitoraggio

L'applicazione di monitoraggio è una novità della piattaforma SAP BusinessObjects Business Intelligence 4.0. Questa applicazione fornisce la possibilità di acquisire le metriche cronologiche e di runtime dei server della piattaforma SAP BusinessObjects Business Intelligence 4.0 per la creazione di report e la notifica. L'applicazione di monitoraggio consente agli amministratori del sistema di stabilire se un'applicazione funziona normalmente e se i tempi di risposta sono quelli previsti. Utilizzando metriche chiave di gestione, l'applicazione di monitoraggio fornisce un'analisi più approfondita della piattaforma SAP BusinessObjects Business Intelligence 4.0.

Il monitoraggio consente inoltre di:

- 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.
- 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 Enterprise funzionano come previsto. Analizzando l'ora di andata e ritorno di queste 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.
- Integrarsi con altre applicazioni aziendali: l'applicazione di monitoraggio della piattaforma SAP BusinessObjects Business Intelligence 4.0 può essere integrata con altre applicazioni aziendali, ad esempio SAP Solution Manager e IBM Tivoli Monitoring.

15.2 Termini relativi al monitoraggio

Nel seguente elenco vengono forniti i termini correlati all'applicazione di monitoraggio:

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 SAP BusinessObjects Business Intelligence. Gli utenti possono associare soglie e avvisi a un controllo. È possibile creare un controllo utilizzando i dati di probe, server, SAPOSCOL o metriche derivate.

Metriche derivate

Le metriche derivate offrono la flessibilità necessaria per creare le metriche in base alle esigenze dell'utente e di creare un controllo partendo da tali metriche. Per creare una metrica derivata è possibile combinare due o più metriche esistenti in un'equazione matematica.

KPI

I KPI (key performance indicators) sono metriche standard nella distribuzione della piattaforma SAP BusinessObjects Business Intelligence. 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 controllano servizi diversi e simulano le diverse funzionalità dei componenti della piattaforma SAP BusinessObjects Business Intelligence. Pianificando l'esecuzione delle probe a intervalli specificati, l'amministratore di sistema può tenere traccia della disponibilità e delle prestazioni dei servizi chiave forniti dalla piattaforma SAP BusinessObjects Business Intelligence 4.0. Questi dati possono essere utilizzati anche per la pianificazione della capacità.

Semafori

I semafori rappresentano lo stato del controllo in un dato momento. Lo stato di un controllo viene indicato dai colori Verde, Ambra, e Rosso. Gli utenti possono impostare due o tre stati per un controllo.

Grafico di tendenza

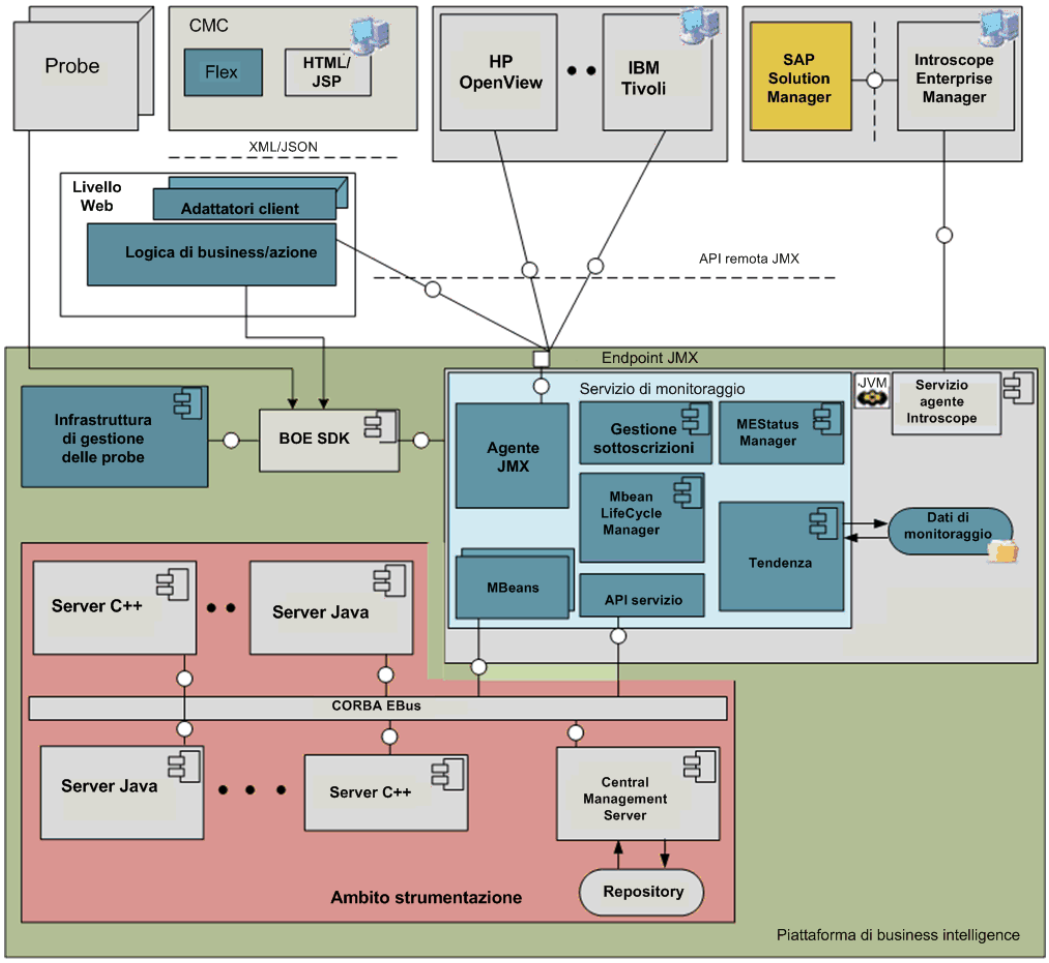
Il grafico di tendenza è una rappresentazione grafica dei dati metrici cronologici generati da probe e server. Consente all'amministratore di sistema di monitorare il sistema a intervalli di tempo diversi e di valutare i criteri di utilizzo del sistema.

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 visualizzarli nella pagina "Cruscotto".

15.2.1 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:

- Platform Java Server (PJS)
- Agente/server Java Management Extensions (JMX)
- MBeans
- Client JMX
- Console di gestione
- Database di tendenza

Il servizio di monitoraggio viene ospitato su Platform Java Server. L'applicazione è basata sulla tecnologia JMX.

Il servizio di monitoraggio Platform Java Service 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.
- Fornisce una funzione di tendenza mediante l'archiviazione di 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, quali SAP Solution Manager e IBM Tivoli Monitoring, possono connettersi all'applicazione di monitoraggio e accedere alle metriche di SAP BusinessObjects 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 database di tendenza.

15.2.1.1 Schema database di tendenza

Il diagramma 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.

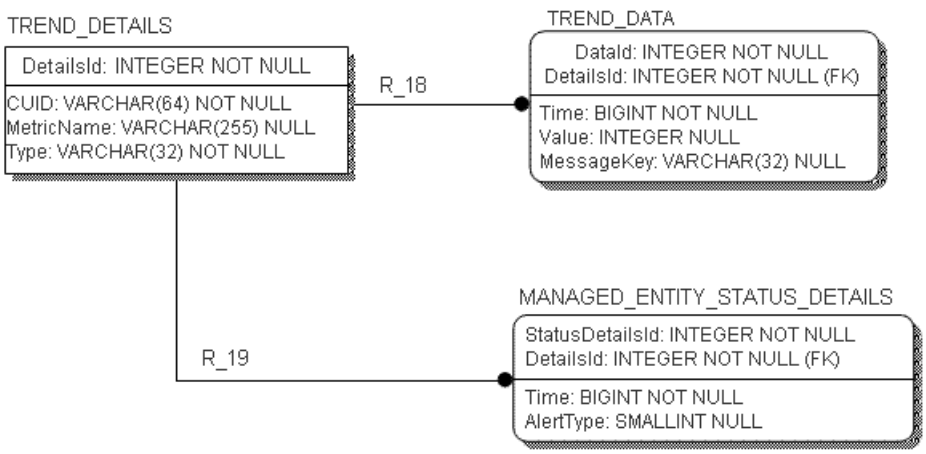


Tabella 15 - 1: TREND_DETAILS

Questa tabella registra le informazioni sulle entità gestite, le probe e i controlli. Ad esempio, i nomi di metrica e CUID.

Nome colonna	Descrizione	Chiave primaria
DetailsId		Generata automaticamente
CUID (64)	CUID dell'InfoObject (o) l'ID univoco di un non-InfoObject	NOT NULL
MetricName	Nome della metrica	NOT NULL
Type (32)	Tipi sottoscrizione o metrica	NOT NULL

Tabella 15 - 2: 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	Descrizione	Chiave primaria
DataId		Generata automaticamente
DetailsId		Chiave esterna
Time	Ora di raccolta dei dati	NOT NULL
Value	Valore della metrica/sottoscrizione	No

Tabella 15 - 3: MANAGED_ENTITY_STATUS_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	Descrizione	Chiave primaria
StatusDetailsId		Generata automaticamente
DetailsId		Chiave esterna
Time	Ora di raccolta dei dati	NOT NULL
AlertType	Tipo di consegna della notifica di sottoscrizione (ad esempio, posta elettronica)	No

15.3 Supporto cluster per il server di monitoraggio

L'applicazione di monitoraggio fornisce il supporto cluster. Il supporto cluster è facile da implementare e fornisce supporto di failover.

Con il supporto cluster, solo un servizio sarà attivo in un dato momento e tutti gli altri servizi saranno passivi. Si supponga di avere due servizi di monitoraggio, s1 e s2, in un ambiente cluster. Solo uno di essi deve essere disponibile. Sia s1 che s2 tentano di passare allo stato attivo. Solo uno di essi riuscirà a diventare attivo, mentre l'altro passerà a uno stato non attivo o passivo.

I servizi passivi verificano a intervalli regolari (ogni minuto) la disponibilità del servizio attivo. 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 l'arresto anomalo, il riavvio o la riduzione delle prestazioni del server APS.

15.4 Metriche

Sono disponibili numerose metriche che possono essere utilizzate per la creazione di controlli. I tipi di metrica sono:

- Metriche probe
- Specifiche dei server
- Metriche host
- Metriche derivate

Quando si esegue una probe predefinita, vengono generate le metriche `tempo di esecuzione` e `riuscito`. Queste metriche vengono chiamate metriche virtuali.

Le metriche del server della piattaforma SAP BusinessObjects Business Intelligence sono riportate nella tabella che segue:

Server	Metriche
Adaptive Processing Server	• Auditing Events Received • AuditingMetrics.number of Events in the Queue • Available Processors • Busy Server Threads • CPU Usage Percentage • Cube Count • CvomServerImpl.debugClassID • DataFederatorService.activeConnectorsConnectionsCount • DataFederatorService.activeConnectorsCount • DataFederatorService.activeQueriesCount • DataFederatorService.activeThreadsCount • DataFederatorService.analyzingQueriesCount • DataFederatorService.connectionsCount • DataFederatorService.diskUsedSize • DataFederatorService.executingQueriesCount • DataFederatorService.failedQueriesCount • DataFederatorService.memoryUsedSize • DataFederatorService.metadataCacheSize • DataFederatorService.optimizingQueriesCount • DataFederatorService.outputDataTransfer • DataFederatorService.outputRowsCount • DataFederatorService.queriesConsumingMemoryCount • DataFederatorService.queries UsingDiskCount • DataFederatorService.sourceInputDataTransfer • DataFederatorService.sourceInputRowsCount • DataFederatorService.waitingQueriesCount • Failed extraction attempts since the service start • Free Memory • JVM Deadlocked Threads Counter • JVM Lock Contention Count • Maximum Memory • Number of Full GCs • Number of Page Faults during GC • Percentage of stopped system during GC • Query Count • Server Enabled State • Server Running State • Session Count • Successful extraction attempts since the service start • Threads in Transport Layer • Total Memory • Transport Layer Thread Pool Size

Server	Metriche
Central Management Server	• Auditing Thread Utilization • Average Commit Response Time Since Startup (msec) • Average Query Response Time Since Startup (msec) • Busy Server Threads • CPUs • Completed Jobs • Currently Used System Database Connections • Disk Size (GB) • Established System Database Connections • Existing Concurrent User Accounts • Existing Named User Accounts • Failed Jobs • Tempo di risposta a commit più lungo dall'avvio (msec) • Longest Query Response Time Since Startup (msec) • Numero di commit dall'avvio • Number of Objects in CMS System Cache • Number of Objects in CMS System DB • Numero di query dall'avvio • Number of Sessions Established by All Users • Number of Sessions Established by Concurrent Users • Number of Sessions Established by Named Users • Number of Sessions Established by Servers • Number of User Logons Since Startup • PID • Peak Number of User Sessions Since Startup • Pending Jobs • Pending System Database Request • RAM (MB) • Running Jobs • Server Enabled State • Server Pending State • Used Disk Space (GB) • Waiting Jobs • Auditing Database Last Updated On • Auditing Thread Last Polling Cycle Duration (sec) • CMS Auditor • Concurrent User Licenses • Connection to Auditing Database is Established • Current Number of Auditing Events in Queue • Licenze utenti designati
Connection Server	

Server	Metriche
	• Busy Server Threads • CPUs • Disk Size • PID • RAM • Server Enabled State • Server Running State • Used Disk Space
Connection Server 32	• Busy Server Threads • CPUs • Disk Size • PID • RAM • Server Enabled State • Server Running State • Used Disk Space
Crystal Reports 2010 Processing Server	• Busy Server Threads • CPUs • CrystalReports service through Page and Cache Servers • Disk Size (GB) • PID • RAM (MB) • Server Enabled State • Server Running State • Used Disk Space
Crystal Reports 2010 Report Application Server	• Busy Server Threads • CPUs • CrystalReports service through Report Application Servers • Disk Size (GB) • PID • RAM (MB) • Server Enabled State • Server Running State • Used Disk Space • Current Number of Auditing Events in the Queue • Current Agent Thread Count • Current Doc Count • Total Agent Thread Count • Total Doc Count

Server	Metriche
Crystal Reports Cache Server	• Busy Server Threads • CPUs • Disk Size (GB) • PID • RAM (MB) • Server Enabled State • Server Running State • Used Disk Space
Crystal Reports Processing Server	• Busy Server Threads • CPUs • CrystalReportsservicethroughPageandCacheServer execution-time • Disk Size (GB) • PID • RAM (MB) • Server Enabled State • Server Running State • Used Disk Space (GB)
Dashboard Analytics Server	• Busy Server Threads • CPUs • Disk Size • PID • RAM • Server Enabled State • Server Running State • Used Disk Space
Dashboard Server	• Busy Server Threads • CPUs • Disk Size • PID • RAM • Server Enabled State • Server Running State • Used Disk Space • Current Number of Auditing Events in the Queue N Pseudoloc

Server	Metriche
Event Server	• Busy Server Threads • CPUs • Disk Size (GB) • Monitored Files • PID • RAM (MB) • Server Enabled State • Server Running State • Used Disk Space (GB) • Current Number of Auditing Events in the Queue N Pseudoloc
Input File Repository	• Active Connections • Active Files • Available Disk Space in Root Directory (%) • Available Disk Space in Root Directory (GB) • Busy Server Threads • CPUs • Data Sent (MB) • Data Written (MB) • Disk Size (GB) • Free Disk Space in Root Directory (GB) • PID • RAM (MB) • Server Enabled State • Server Running State • Total Disk Space in Root Directory (GB) • Used Disk Space (GB)

Server	Metriche
Output File Repository	• Active Connections • Active Files • Available Disk Space in Root Directory (%) • Available Disk Space in Root Directory (GB) • Busy Server Threads • CPUs • Data Sent (MB) • Data Written (MB) • Disk Size (GB) • Free Disk Space in Root Directory (GB) • PID • RAM (MB) • Server Enabled State • Server Running State • Total Disk Space in Root Directory (GB) • Used Disk Space (GB)
PM Repository Server	• Busy Server Threads • CPUs • Disk Size • PID • RAM • Server Enabled State • Server Running State • Used Disk Space
Web Application Container Server	• Server Enabled State • Server Running State

Server	Metriche
Web Intelligence Processing Server	• Busy Server Threads • CPU Usage (%) • CPUs • Cache high mark count • Cache Size (KB) • Current number of active sessions • Current number of client calls • Current number of sessions • Current number of tasks • Disk Size (GB) • Memory high threshold count • Memory level • Memory max threshold count • Number of document swap • Number of document timeout • Number of documents • Number of swapped documents • Number of users • PID • RAM (MB) • Server Enabled State • Server Running State • Total CPU time (seconds) • Total number of client calls • Total number of sessions • Total number of tasks • Used Disk Space (GB) • Virtual memory size (MB) • WebI memory (MB) • WebI server (Timeout) • Current Number of Auditing Events in the Queue N Pseudoloc
Xcelsius Data Cache Server	• Busy Server Threads • CPUs • Disk Size • PID • RAM • Server Enabled State • Server Running State • Used Disk Space
Xcelsius Data Processing Server	

Server	Metriche
	• Busy Server Threads • CPUs • Disk Size • PID • RAM • Server Enabled State • Server Running State • Used Disk Space

Nota:
quando si aggiunge un nuovo server o si avvia un server esistente le cui metriche non sono visualizzate nella pagina Metrica, attendere per circa 10 minuti che le metriche vengano visualizzate nella pagina Metriche.

15.5 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 all'area **Applicazioni** della console CMC.
2. Fare clic con il pulsante destro del mouse su **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 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.

Sezione	Campo	Descrizione
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.
Metriche host	**Abilita metriche host**	Per impostazione predefinita, questa opzione è disabilitata. Se si abilita questa opzione, è necessario fornire il percorso dell'installazione dei file binari SAPOSCOL. Per abilitare le metriche host, è necessario installare SAPOSCOL. Per ulteriori informazioni su come installare SAPOSCOL, consultare Installazione di SAPOSCOL

Sezione	Campo	Descrizione
Altre impostazioni	**Intervallo di aggiornamento metrica (secondi)**	L'intervallo minimo che è possibile specificare è di 15 secondi. Tale intervallo si applica a quanto segue: • Calcolo delle sottoscrizioni per i controlli: le regole di attenzione e di pericolo vengono calcolate costantemente con l'intervallo di tempo specificato qui. • Calcolo dello stato del controllo: lo stato del controllo viene calcolato costantemente con l'intervallo di tempo specificato nel periodo di aggiornamento della metrica 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 tendenza della modalità Cronologia per i grafici viene eseguita sempre e in modo costante con l'intervallo di tempo specificato qui.
	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 il limite impostato è 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.
	Intervallo di aggiornamento automatico UI di monitoraggio (secondi)	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.
	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	Per impostazione predefinita, questa opzione è disabilitata. Se si abilita questa opzione, l'attività di backup del database di tendenza viene avviata nell'orario specificato.
	Directory di backup del database di tendenza	

Sezione	Campo	Descrizione
		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.
	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.
	Posizione database di tendenza	Per impostazione predefinita, la posizione del database di tendenza è `BOE_Install_Dir\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0/Data/TrendingDB`. 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.

3. Fare clic su **Salva**.

Nota:
quando si modifica una qualsiasi di queste proprietà, tranne l'abilitazione e la disabilitazione dell'applicazione di monitoraggio, è necessario riavviare il servizio di monitoraggio ospitato in Adaptive Processing Server.

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`.

15.5.1 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
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.

15.6 Integrazione con altre applicazioni

Soluzioni Enterprise, come SAP Solution Manager e 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.

15.6.1 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**, quindi scegliere 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	Il nome utente utilizzato per accedere a SAP BusinessObjects Enterprise
Password	La password utilizzata per accedere a SAP BusinessObjects Enterprise
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 crea un agente per la piattaforma SAP BusinessObjects Business Intelligence mediante Generatore agente, la piattaforma SAP BusinessObjects Business Intelligence 4.0 deve essere installata nello stesso sistema. Tuttavia, se si esegue l'installazione di un agente già esistente utilizzando il relativo file di installazione, non è necessario che il monitoraggio BOE 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 `%InstallDir%\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib` a una cartella sul proprio 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 cegliere **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

15.6.2 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 la procedura seguente durante l'installazione della piattaforma SAP BusinessObjects Business Intelligence 4.0:

1. Nel passaggio Configure Connectivity to Introscope Enterprise Manager, fornire il nome host e i dettagli della porta. Introscope Agent sarà installato in `C:\Programmi (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\Wiley` durante l'installazione della piattaforma SAP BusinessObjects Business Intelligence 4.0.
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 relativo alla *gestione dei server* nella *Guida in linea di CMC di SAP BOE*.

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.

15.7 Creazione dell'universo per il database Derby

La creazione di un universo per i database Derby consente di eseguire query nel database Derby al fine di creare report ed eseguire analisi dei dati. Per ulteriori informazioni sulla creazione di universi, consultare il manuale di *SAP BOE Universe Designer*.

Nota:
è possibile creare un universo per il database Derby solo dopo aver eseguito le attività di backup del database. Per ulteriori informazioni sulle attività di backup del database, vedere *Proprietà di configurazione* negli argomenti correlati.

1. Creare un universo per il database Derby eseguendo la procedura guidata Universe Design Tool.

Per ulteriori informazioni sulla creazione dell'universo mediante la procedura guidata, consultare *Uso corretto dell'assistente Creazione rapida degli universi* nel manuale di *SAP BOE Universe Designer*.

È possibile creare l'universo utilizzando due connessioni di database, ovvero al database Apache e a un database generico.

2. Se si seleziona la connessione al database Apache, procedere come segue:
   a. Fare clic su **Driver JDBC**
   b. Selezionare il file `derby.sbo` dalla posizione `DIR_INSTALL\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\jdbc`.
   c. Aggiungere il percorso di classe `<Percorsoclasse> <Percorso>\...\...\derby.jar</Percorso></Percorsoclasse>`.

      Scaricare l'ultima versione del file `derby.jar` (versione 10.5.x) dal sito Web Apache prima di aggiungere il percorso di classe.
   d. Per creare una nuova connessione al database Apache, immettere la posizione della cartella del database Derby nel campo **Server**.

      Se il database si trova in `C:\Derby`, immettere `C:\Derby;create=false`
3. Se si seleziona la connessione al database generico, procedere come segue:
   a. Selezionare **JDBC generico**.
   b. Selezionare il file `jdbc.sbo` dalla posizione `DIR_ INSTALL\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer\jdbc`.
   c. Aggiungere il percorso di classe `<Percorsoclasse> <Percorso>\...\...\derby.jar</Percorso></Percorsoclasse>` e i dettagli della classe JDBC `<Nome parametro="Classe JDBC">org.apache.derby.jdbc.EmbeddedDriver</Parametro>`
   d. Se si crea un nuovo database generico, immettere `jdbc:derby:C:\Derby;create=false` nel campo **URL**.

Argomenti correlati

- Proprietà di configurazione

15.8 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.

15.8.1 Cruscotto

Il collegamento del cruscotto di monitoraggio non è visualizzato sulla pagina CMC

- Verificare se l'utente dispone di diritti di accesso adeguati.
- Assicurarsi 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 (10.5.x).

15.8.2 Avvisi

Impossibile ricevere avvisi nella pagina Avvisi

- Verificare se l'opzione **Attiva messaggio di notifica di avviso** nelle impostazioni **Notifica** è selezionata.
- Assicurarsi di disporre di diritti di accesso adeguati per ricevere avvisi.
- Verificare se gli avvisi recenti sono visibili sul cruscotto di monitoraggio.
- Verificare se il server SMTP funziona.
- Verificare se l'ID di posta elettronica impostato per ricevere avvisi tramite posta elettronica è appropriato.
- Assicurarsi che l'istanza AdaptiveJobServer sia abilitata.
- Verificare le impostazioni SMTP nella destinazione dell'istanza AdaptiveJobServer.

Nota:

per verificare se il SMTP funziona nel modo previsto, è possibile inviare un documento CR all'ID di posta elettronica impostato.

15.8.3 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.

- Assicurarsi 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 se l'istanza di AdaptiveProcessingServer è in esecuzione.

La scheda Elenco di controlli è disabilitata

- Verificare se il server a cui è assegnata la metrica è in esecuzione.
- Verificare se nella metrica corrispondente nella pagina di elenco metriche sono visualizzate le informazioni in modalità live e cronologica.
- Verificare la presenza di messaggi di errore nei registri del servizio di monitoraggio.
- Verificare se la metrica è visibile nella jconsole.

Argomenti correlati

- Proprietà di configurazione

15.8.4 Probe

Impossibile pianificare i probe

- Verificare se l'istanza di AdaptiveJobServer è in esecuzione.
- Assicurarsi che il CUID del report, utilizzato per 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 del probe è "in sospeso"

- Verificare se l'istanza di ProbeSchedulingService è installata.
- Verificare se l'istanza di AdaptiveJobServer è 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.

15.8.5 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

15.8.6 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

16.1 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 in SAP Developer Network.

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.

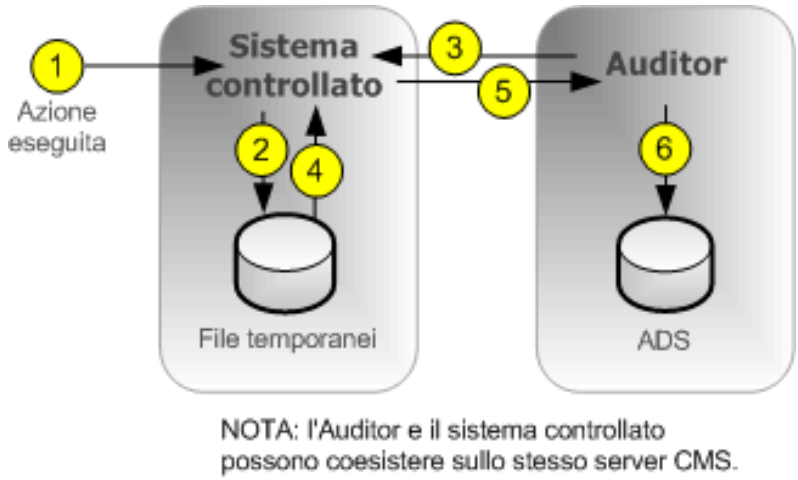
Funzionamento delle attività di controllo

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.

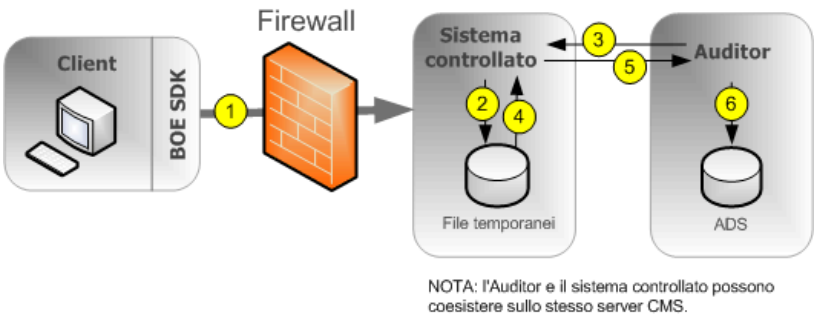
Controllo dei server



1. Un evento controllabile è eseguito dal server.
2. Il sistema controllato scrive gli eventi in un file temporaneo.
3. 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.



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.

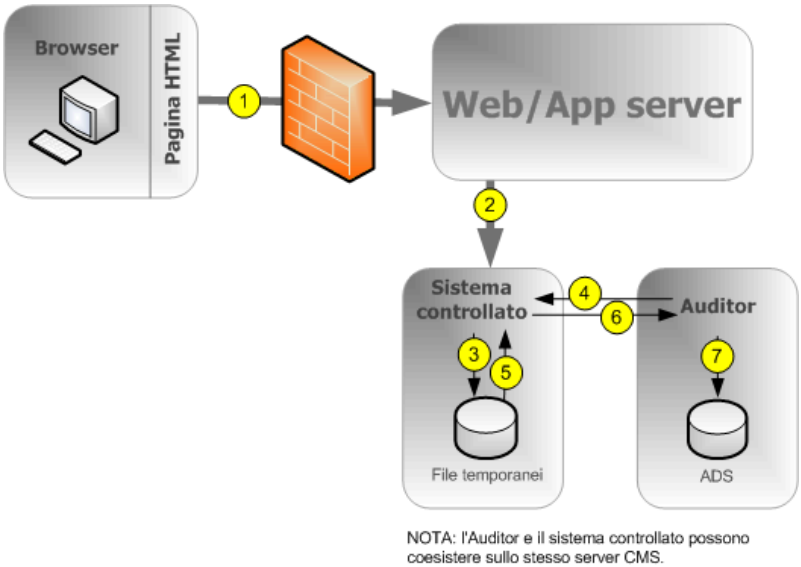
   Nota:
   è necessario aprire una porta nel firewall tra il client e CMS. Per ulteriori informazioni sui firewall, consultare il capitolo relativo alla protezione del *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

2. Il sistema controllato scrive gli eventi in un file temporaneo.
3. 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

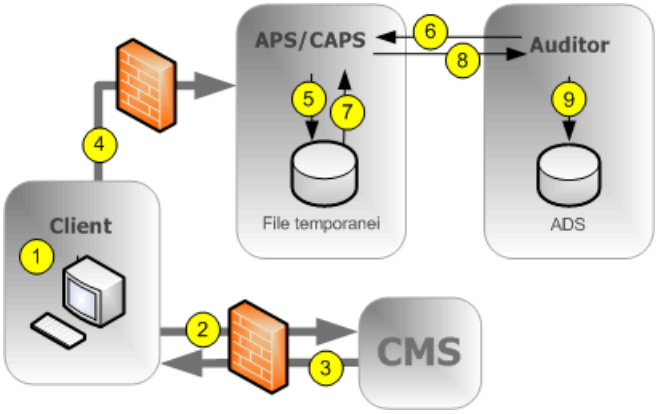
Riguarda applicazioni online come BI Launch Pad, Central Management Console, SAP BusinessObjects Web Intelligence e così via.



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.
4. 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.



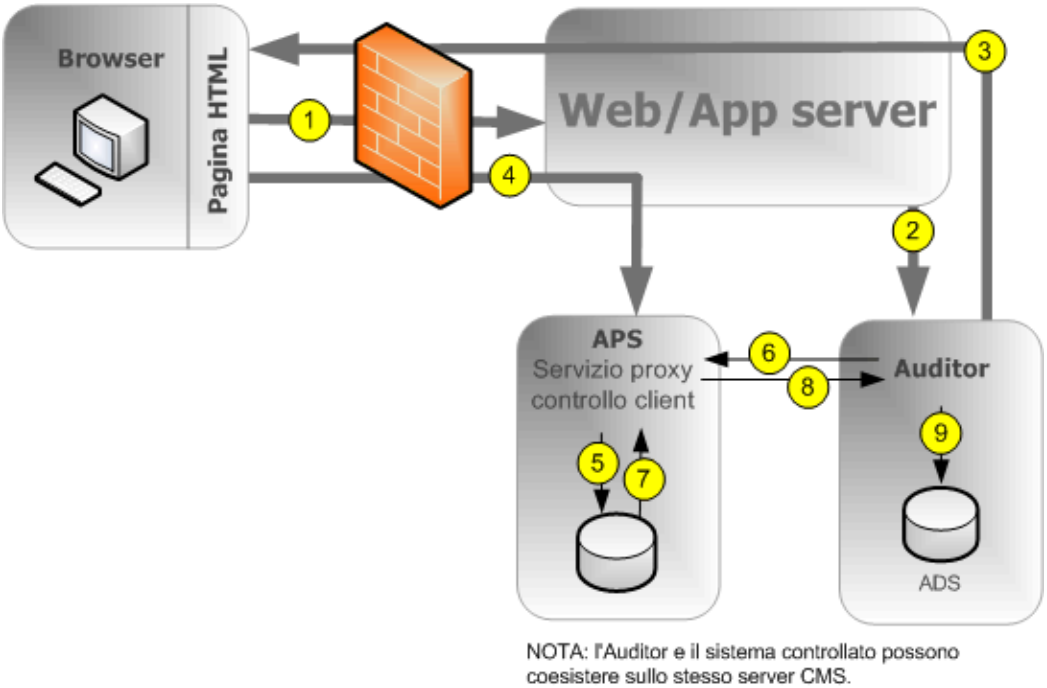
1. L'utente esegue un'operazione che può essere controllata.
2. Il client contatta CMS per verificare se l'operazione è configurata per il controllo.
3. Se l'azione è impostata per il controllo, CMS comunica l'informazioni al client.
4. Il client invia le informazioni sugli eventi al servizio proxy di 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.
6. 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.



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.
6. 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 Desktop

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.

Si verifica sempre un ritardo tra l'ora in cui si verifica un evento e il suo trasferimento finale nel database del sistema di controllo. 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. Non fanno eccezione gli eventi generati dal cache server di BI Workspace, poiché questo server è esterno all'area attendibile.
- 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** 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

16.2 Pagina di controllo CMC

La pagina "Controllo" della console CMC è costituita dalle seguenti aree:

- "Riepilogo stato"
- "Imposta eventi"
- " Dettagli imposta eventi"
- "Configurazione"

16.2.1 Stato del controllo

Nello "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.

Metriche dello stato del controllo

Metrica	Dettagli
ADS Last Updated on	Data e ora dell'ultima volta in cui il CMS di controllo ha iniziato a richiedere gli eventi ai sistemi controllati.
Auditing Thread Utilization	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. 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. 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.
Last Polling Cycle Duration	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. • 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. 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.
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 i server SQL sarà il nome della connessione ODBC. Per gli altri tipi di database sarà il nome del database, seguito dal nome del server e dalla porta di connessione.
ADS Database User Name	Nome utente utilizzato dal CMS di controllo per accedere al database ADS.

16.2.2 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. Vedere *Impostazioni di configurazione ADS*.

16.2.2.1 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 quattro diverse impostazioni dell'indicatore e gli eventi acquisiti a ciascun livello.

Livello di controllo	Eventi acquisiti
Disattivato	Nessuna
Minimo	• Accesso • Logout • Modifica dei diritti • Livello di accesso personalizzato modificato • Modifica controllo
Predefinito	Eventi contrassegnati con **Minimo** più: • Visualizza • Aggiorna • Prompt • Crea • Elimina • Modifica • Salva • Cerca • Modifica • Esegui • Fornitura
Completa	Eventi contrassegnati con **Minimo** e **Predefinito** più: • Recupera • 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 • Connessione cubo • Sessione MDAS
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. • " 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. • "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. • "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.

16.2.3 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 della piattaforma BI ed è stata installata la versione 3.x di Business Objects Metadata Manager (BOMM), è consigliabile 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.

16.2.3.1 Configurazione delle impostazioni del database ADS

1. Selezionare la scheda **Controllo** nella console CMC.

   Viene visualizzata la pagina **Controllo**.
2. Sotto l'intestazione "Configurazione", fare clic su **Tipo di database ADS**.

   Viene visualizzato un elenco di tipi di database supportati.
3. Selezionare il tipo di database impostato per i dati di controllo.
4. Sotto **Nome connessione**, immettere il nome della connessione configurata per il database di controllo. Per i database SQL può trattarsi del nome ODBC. Per gli altri database può avere il formato `<nomehostserver>,<porta>,<nomedatabase>`.
   a. Se si utilizza un database Microsoft SQL con autenticazione Windows, attivare l'opzione **Autenticazione Windows**.
5. 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.
6. 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.
7. 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.
8. Fare clic su **Salva**.
9. Riavviare CMS.

16.3 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 controllo	Le impostazioni di controllo del sistema vengono modificate. • Servizio Central Management
Crea	Un nuovo oggetto viene aggiunto al sistema. • Servizio di elaborazione di Web Intelligence • Servizio di modifica e visualizzazione Crystal Reports • Servizio Central Management • Web Intelligence • Lifecycle Management
Connessione cubo	Viene eseguita un'operazione di connessione al cubo OLAP. • Servizio di analisi multidimensionale
Livello di accesso personalizzato modificato	Le informazioni relative ai privilegi vengono modificate. • Servizio Central Management
Elimina	Un oggetto viene rimosso dal sistema. • Servizio Central Management • Servizio Lifecycle Management
Fornitura	Un oggetto viene inviato/consegnato a una destinazione. • Servizio di pianificazione consegna di destinazione • Servizio di pianificazione di Crystal Reports • Servizio di pianificazione di Crystal Reports for Enterprise • Servizio di pubblicazione e pianificazione di Web Intelligence • Servizio Central Management • Servizio di pianificazione programma
Drill fuori dal livello	Un utente di un documento Web Intelligence ha eseguito il drill down fino a un livello di dettaglio esterno ai dati precaricati del report. • Web Intelligence • Servizio di elaborazione di Web Intelligence
Modifica	Il contenuto di un oggetto è stato modificato. • Servizio di elaborazione di Web Intelligence • Servizio cruscotto • Web Intelligence
Configurazione LCM	I dettagli di configurazione della console LCM (Lifecycle Management Console) sono cambiati. • Lifecycle Management

Evento	Descrizione, server e client che generano il tipo di evento
Accesso	Un utente ha eseguito l'accesso al sistema. • Servizio Central Management
Logout	Un utente ha eseguito la disconnessione dal sistema. • Servizio Central Management
Modifica	Le proprietà di file di un oggetto sono state modificate. • Web Intelligence • Lifecycle Management • Servizio Central Management
Sessione MDAS	Viene eseguita un'operazione da parte dei servizi di analisi multidimensionali • Servizio di analisi multidimensionale
Pagina recuperata	Un client SAP BusinessObjects Web Intelligence recupera informazioni aggiuntive dal repository. • Servizio di elaborazione di Web Intelligence
Prompt	Vengono immesse informazioni per un prompt di oggetto. • Servizio cache di Dashboard Design • Live Office • Servizio di pianificazione di Crystal Reports • Crystal Reports for Enterprise • Servizio cache di Crystal Reports • Servizio di elaborazione di Web Intelligence • Web Intelligence
Aggiorna	I dati di un oggetto vengono aggiornati dal database su richiesta di un utente. • Servizio cache di Dashboard Design • Live Office • Servizio di pianificazione di Crystal Reports for Enterprise • Servizio cache di Crystal Reports • Servizio di pianificazione di Crystal Reports • Servizio di elaborazione di Web Intelligence • Web Intelligence
Recupera	Viene recuperato un oggetto dal repository. • Servizio Central Management
Modifica dei diritti	Vengono modificate le informazioni sulla protezione per un utente, un gruppo o un oggetto. • Servizio Central Management

Evento	Descrizione, server e client che generano il tipo di evento
Rollback	Viene utilizzato Lifecycle Manager per riportare un oggetto a una versione precedente. • Lifecycle Management
Esegui	Viene eseguito un processo. • Servizio di pianificazione di Lifecycle Management • Servizio di pianificazione consegna di destinazione • Servizio di replica • Servizio di pianificazione di Crystal Reports • Servizio di pianificazione di Crystal Reports for Enterprise • Servizio di pubblicazione e pianificazione di Web Intelligence • Servizio di pianificazione pubblicazione • Servizio di pianificazione programma • Lifecycle Management
Salva	Un oggetto viene salvato dopo essere stato aggiornato o modificato. • Servizio di pianificazione di Crystal Reports for Enterprise • Servizio cache di Crystal Reports • Servizio di analisi multidimensionale • Servizio Lifecycle Management • Servizio di elaborazione di Web Intelligence • Servizio di modifica e visualizzazione Crystal Reports • Servizio di pianificazione di Crystal Reports
Cerca	Viene eseguita una ricerca. • Servizio di ricerca
Attiva	Viene attivato un evento di file. • Servizio eventi • Servizio Central Management
Visualizza	Viene visualizzato un oggetto. • Web Intelligence • Servizio di elaborazione di Web Intelligence • Central Management Console • BI Launch Pad • Servizio cache di Dashboard Design • Servizio cache di Crystal Reports • Servizio di modifica e visualizzazione Crystal Reports • Servizio cruscotto • Apertura documento

Evento	Descrizione, server e client che generano il tipo di evento
Aggiungi VMS	Un oggetto viene aggiunto al sistema di gestione delle versioni di LCM. • Lifecycle Management
Archiviazione in VMS	Un oggetto viene archiviato nel sistema di gestione delle versioni di LCM. • Lifecycle Management
Estrazione da VMS	Un oggetto viene estratto dal sistema di gestione delle versioni di LCM. • Lifecycle Management
Esporta VMS	Una risorsa viene esportata dal sistema VMS. • Lifecycle Management

Evento	Descrizione, server e client che generano il tipo di evento
Blocca VMS	Una risorsa in VMS è bloccata. • Lifecycle Management
Sblocca VMS	Una risorsa in VMS viene sbloccata. • Lifecycle Management
Recupera VMS	Un oggetto viene recuperato dal sistema di gestione delle versioni di LCM. • Lifecycle Management

Eventi per tipo di servizio

Tipo di servizio	Tipi di evento generati
BI Launch Pad	Visualizza
Central Management Service	• Modifica controllo • Crea • Livello di accesso personalizzato modificato • Elimina • Fornitura • Accesso • Logout • Modifica • Recupera • Modifica dei diritti • Attiva
Central Management Console	Visualizza
Servizio cache Crystal Reports	• Prompt • Aggiorna • Salva • Visualizza
Servizio di pianificazione di Crystal Reports for Enterprise	• Fornitura • Prompt • Aggiorna • Esegui • Salva

Tipo di servizio	Tipi di evento generati
Servizio di pianificazione Crystal Reports	• Fornitura • Prompt • Aggiorna • Esegui • Salva
Servizio di modifica e visualizzazione Crystal Reports	• Crea • Salva • Visualizza
Servizio cache di Dashboard Design	• Prompt • Aggiorna • Visualizza
Servizio cruscotto	• Modifica • Visualizza
Servizio di pianificazione consegna di destinazione	• Fornitura • Esegui
Servizio eventi	Attiva
Servizio di pianificazione LCM	Esegui
Servizio LCM	• Crea • Elimina • Configurazione console LCM • Modifica • Rollback • Esegui • Salva • Versione • Aggiungi VMS • Archivia nel sistema di gestione delle versioni • Estrai VMS • Blocca VMS • Sblocca VMS
Live Office	• Prompt • Aggiorna
Servizio di analisi multidimensionale	• Connessione cubo MDAS • Sessione MDAS • Salva

Tipo di servizio	Tipi di evento generati
OpenDocument	Visualizza
Servizio di pianificazione programma	• Fornitura • Esegui
Servizio di pianificazione pubblicazione	Esegui
Servizio di replica	Esegui
Servizio di ricerca	Cerca
Web Intelligence	• Crea • Drill fuori dal livello • Modifica • Modifica • Prompt • Aggiorna • Salva • Visualizza
Servizio di elaborazione di Web Intelligence	• Crea • Drill fuori dal livello • Modifica • Pagina recuperata • Prompt • Aggiorna • Salva • Visualizza
Servizio di pubblicazione e pianificazione di Web Intelligence	• 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.

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.

16.3.1 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.

16.3.1.1 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.

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.

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.

Dettagli dell'evento	ID	Descrizione
ID documento principale	12	• 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.

16.3.1.2 Eventi comuni

I seguenti tipi di eventi sono comuni a tutti i componenti di SAP BusinessObjects XI.

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).

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.
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 Xcelsius al momento della progettazione. Viene generato solo per aggiornamenti di Xcelsius o per un documento Xcelsius o 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).

Esegui

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.

Fornitura

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'implememtazione di Business Objects.

Dettagli dell'evento	ID	Descrizione
Account Name	45	Restituisce uno dei seguenti elementi: • 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.
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	35	Indica in che modo la consegna è stata avviata: • "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

Recupera

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 segnalato dal client	51	Nome host del client restituito dal client.
Nome host 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 segnalato dal client	53	Indirizzo IP del client restituito dal client.
Indirizzo IP 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.

Logout

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.

Attiva

Viene attivato un evento di file.

- ID tipo di evento: 10016

Dettagli dell'evento	ID	Descrizione
Nome file	17	Nome del file che ha monitorato e attivato l'evento.

16.3.1.3 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 modificato	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`.

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 modificato	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`.

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	70	Se la connessione all'archivio dati di controllo viene modificata, registra le nuove impostazioni di connessione utilizzando il formato seguente: `DBType=Oracle,DB Name=MyADS,Username=USR1,Pass word="*****",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.

16.3.1.4 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

16.3.1.5 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.

16.3.1.6 Eventi di SAP BusinessObjects Lifecycle Management Console

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=abilitate, 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	10901	Il nome dell'utente che ha eseguito l'azione.

Ricerca piattaforma

17.1 Presentazione

Ricerca piattaforma consente agli utenti di eseguire ricerche sul contenuto del repository della piattaforma SAP BusinessObjects Business Intelligence. Affina i risultati della ricerca raggruppandoli in categorie e classificandoli in ordine di rilevanza. Supporta inoltre un SDK pubblico che funziona come interfaccia tra l'applicazione client e il servizio Ricerca piattaforma.

In questa versione di SAP BusinessObjects Business Intelligence, Ricerca piattaforma è stata potenziata con le funzionalità seguenti:

- Ricerca di contenuto della piattaforma SAP BusinessObjects Business Intelligence e di 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.

17.2 Architettura

In questa sezione viene offerta una panoramica dell'architettura di Ricerca piattaforma e viene spiegato brevemente il ruolo dei singoli componenti. Il servizio Ricerca piattaforma viene ospitato in Adaptive Processing Server che ospita al suo interno diversi componenti responsabili delle funzionalità di indicizzazione e ricerca. Il servizio Ricerca piattaforma esegue l'indicizzazione sulla base del tipo di indice, ovvero in base a pianificazione o continua.

Ricerca piattaforma comprende due processi principali: indicizzazione e ricerca. Dispone inoltre di un proprio meccanismo di riparazione automatica.

Indicizzazione

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 dimensione e al tipo dei documenti.

   L'indice della ricerca viene memorizzato in una posizione designata nel file e contiene tutte le informazioni ricercabili dei documenti indicizzati.

   Per eseguire correttamente l'indicizzazione, i server seguenti devono essere in esecuzione e abilitati:
   - InputFileRepositoryServer (IFRS)
   - OutputFileRepositoryServer (OFRS)
   - CentralManagementServer (CMS)
   - AdaptiveProcessingServer (APS)

   Se il tipo di oggetto viene selezionato come report di Web Intelligence o Crystal Reports, è necessario eseguire e abilitare Web Intelligence Processing Server e Crystal Report Application Server corrispondenti 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.

Ricerca

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.

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.

Argomenti correlati

- Configurazione delle proprietà dell'applicazione
- Tipi di contenuto in cui è possibile eseguire ricerche

17.3 Supporto cluster per Ricerca piattaforma

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

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. Il meccanismo di failover garantisce la continuità delle operazioni di ricerca e di indicizzazione degli utenti.

17.4 SDK e Open Search

L'applicazione di ricerca piattaforma supporta sia SDK che Open Search.

17.4.1 SDK applicazione di ricerca piattaforma

L'SDK di Ricerca piattaforma è l'interfaccia tra l'applicazione client e il servizio 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, vedere il manuale *SAP BusinessObjects Business Intelligence platform Java API Reference*.

17.4.2 Open Search

Ricerca piattaforma supporta lo standard OpenSearch, consentendo la comunicazione con le applicazioni client mediante tale standard o il rispettivo formato. OpenSearch non viene installato per impostazione predefinita con la suite della piattaforma SAP BusinessObjects Business Intelligence, pertanto gli utenti devono distribuirlo manualmente come file WAR separato (opensearch.war) in un server di applicazioni come Tomcat utilizzato per la piattaforma SAP BusinessObjects Business Intelligence oppure mediante lo strumento WDeploy. Tale file viene copiato nella directory {DIR_INSTALL_BOE}\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 SAP BusinessObjects Business Intelligence, il server di applicazioni Tomcat viene installato per impostazione predefinita.

17.4.2.1 Distribuzione di OpenSearch

Per distribuire OpenSearch in un ambiente della piattaforma SAP BusinessObjects Business Intelligence, effettuare le operazioni seguenti:

1. Passare alla seguente posizione: {dirinstall}/SAP BusinessObjects Enterprise 4.0\warfiles\
2. Copiare la cartella OpenSearch in {DIRINSTALL}\Tomcat6\webapps.
3. Modificare i parametri di configurazione nel file OpenSearch\WEB-INF\config.properties come indicato sotto:
   - CMS: nome del CMS con il numero di porta, ad esempio <Nome CMS>:<Numero porta>
   - OpenDocURL: URL dell'applicazione OpenDocument, ad esempio http://<hosttomcat>:<portaconnettore>/BOE/OpenDocument/opendoc/openDocument.jsp
   - Proxy.rpurl: 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.

17.4.2.2 Distribuzione di OpenSearch mediante WDeploy

Per distribuire OpenSearch utilizzando WDeploy, effettuare le operazioni seguenti:

Nota:
i comandi per Windows e UNIX vengono indicati rispettivamente come `wdeploy.bat <parametri>` e `wdeploy.sh <parametri>`.

1. Aggiornare il file config.<server server app> che si trova in `<Dir_Install_BOE>\<DIR_Enterprise>\wdeploy\conf` con i parametri di applicazione 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 `OpenSearch\WEB-INF\config.properties`, come indicato di seguito:
   - CMS: nome del CMS con il numero di porta, ad esempio <Nome CMS>:<Numero porta>
   - OpenDocURL: URL dell'applicazione OpenDocument, ad esempio `http://<Host server applicazione Web>:<portaconnettore>/BOE/OpenDocument/opendoc/openDocument.jsp`
   - Proxy.rpurl: 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 il proxy inverso.
3. Eseguire il comando `wdeploy.bat <SERVER_APPLICAZIONE_WEB> -Dapp_source_dir=<POSIZIONE_DI_Webapp OpenSearch> -DAPP=OpenSearch deploy` dal percorso `<Dir_Install_BOE>\<DIR_Enterprise\wdeploy`

   Ad esempio, il comando seguente distribuisce OpenSearch in un server di applicazioni Web WebSphere 7:

```
wdeploy.bat websphere7 -Dapp_source_tree=<BOE_Install_Dir>\<Enterprise_DIR>\warfiles" -DAPP=OpenSearch
deploy
```

4. Riavviare il server delle applicazioni.

17.4.2.3 Configurazione del proxy inverso per OpenSearch

Per distribuire le applicazioni Web della piattaforma SAP BusinessObjects Business Intelligence 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.

Nota:
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 reverse proxy e apportare le modifiche nel file WEB-INF\config.properties di OpenSearch.
2. Abilitare i seguenti parametri di contesto e modificare i relativi 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 seguenti impostazioni:
   - 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.

17.5 Configurazione delle proprietà dell'applicazione

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 desiderate.

   Le proprietà configurabili vengono descritte nella seguente tabella:

Opzione	Descrizione
Statistiche della ricerca	L'applicazione di ricerca piattaforma fornisce le seguenti statistiche della ricerca: • 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	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. Per interrompere l'indicizzazione, fare clic su **Interrompi indicizzazione**, quindi su **OK** nella finestra di dialogo di conferma.
Impostazioni internazionali indice	Quando si cambiano le impostazioni locali dell'indice in quelle di un'altra lingua, Ricerca piattaforma reindicizza i documenti nella lingua selezionata. Specificare le impostazioni locali di indicizzazione in una delle lingue seguenti: brasiliano, cinese, ceco, danese, olandese, inglese, finlandese, francese, tedesco, italiano, giapponese, coreano, norvegese (Bokmål), polacco, portoghese, russo, spagnolo, svedese e tailandese. **Nota:** la scelta predefinita per questa opzione è l'Inglese.

Opzione	Descrizione
Frequenza di ricerca per indicizzazione	È possibile indicizzare l'intero repository della piattaforma BI utilizzando le seguenti opzioni: • Ricerca per indicizzazione continua: questa opzione implica un'indicizzazione continua, ovvero il repository viene indicizzato ogni volta che si aggiunge, modifica o elimina un oggetto. Tale ricerca consente di visualizzare o utilizzare i contenuti più aggiornati della piattaforma SAP BusinessObjects Business Intelligence. La ricerca per indicizzazione continua costituisce l'impostazione predefinita e aggiorna in modo continuativo il repository della piattaforma BI 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. Per ulteriori informazioni sulla pianificazione di un oggetto, consultare la sezione *Pianificazione di un oggetto* di Ricerca piattaforma nella *Guida in linea della CMC della piattaforma BI*. **Nota:** • 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
	Quando i documenti vengono indicizzati, vengono archiviati in cartelle condivise nelle seguenti posizioni: • Posizione indice principale (indici, correttori ortografici): gli indici principale e correttore ortografico archiviati in questa posizione. Durante un flusso di lavoro di ricerca, i riscontri iniziali vengono recuperati mediante l'indice principale, mentre per recuperare i suggerimenti vengono utilizzati gli indici correttore ortografico. In una distribuzione BOE 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. La posizione dei dati persistenti è l'unica posizione di indice interessata dall'ambiente cluster, poiché contiene le cartelle degli archivi contenuto. Se un computer utilizza un solo servizio di ricerca, esisterà solo una posizione dell'archivio contenuti. Ad esempio, {bobj.enterprise.home}\data\PlatformSearchData\workspace\Server\ContentStores. 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: a. {bobj.enterprise.home}\data\PlatformSearchData\workspace\Server\ContentStores. b. {bobj.enterprise.home}\data\PlatformSearchData\workspace\Server1\ContentStores. • 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, i documenti indicizzati 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. **Nota:** • 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, è necessario copiare il conte

Opzione	Descrizione
	nuto in una nuova posizione. In caso contrario, le informazioni relative all'indice esistente verranno perdute.

Livello di indicizzazione	È possibile regolare il contenuto della ricerca impostando il livello di indicizzazione nei seguenti modi:
	• 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:
	  • il contenuto effettivo del documento
	  • il contenuto dei prompt e degli elenchi di valori
	  • grafici ed etichette
	Nota:
	quando si modifica il livello di indicizzazione, l'indicizzazione viene reinizializzata per l'intero repository della piattaforma BI.

Tipi contenuto	È possibile selezionare i seguenti tipi di contenuto per l'indicizzazione: • Microsoft Word • Microsoft Excel • Microsoft PowerPoint • Testo • Adobe Acrobat • Rich Text • Crystal Reports • Universo • Web Intelligence

Opzione	Descrizione
Rigenera indice	Questa opzione consente di eliminare tutti i contenuti indicizzati esistenti e di ripetere l'indicizzazione dell'intero documento dall'inizio. È possibile selezionare l'opzione **Rigenera indice** indipendentemente dallo stato di indicizzazione. Tale opzione tuttavia non funziona se l'indicizzazione viene interrotta e si seleziona **Rigenera indice**, quindi si salva e si chiude l'applicazione Ricerca piattaforma. Quando l'indicizzazione viene interrotta e si seleziona **Rigenera indice**, si salva e si chiude l'applicazione Ricerca piattaforma, quindi si riapre la pagina di configurazione e si fa clic su **Avvia indicizzazione**, l'indice rigenerato archiviato eseguirà di nuovo automaticamente l'indicizzazione dell'intero documento. Se non si desidera che Ricerca piattaforma indicizzi nuovamente i documenti, è necessario deselezionare **Rigenera indice** prima di fare clic su **Avvia indicizzazione**.
Documenti esclusi dall'indicizzazione	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. 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. Per impostazione predefinita, solo l'account Administrator ha il controllo completo dei **Documenti esclusi dall'indicizzazione**. Gli altri utenti con i diritti seguenti possono solo aggiungere documenti al gruppo **Documenti esclusi dall'indicizzazione**: • 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 deseleziona gli estrattori, l'indice viene aggiornato in modo incrementale dall'inizio senza che venga eliminato l'indice esistente.

17.6 Tipi di contenuto in cui è possibile eseguire ricerche

Per i contenuti pubblicati nella piattaforma SAP BusinessObjects Business Intelligence è possibile utilizzare 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)	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. 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.
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.

Tipo di oggetto	Contenuto indicizzato
LCMJob, Universe, AFDashboard Page, Dashboard Design, ObjectPackage, query del servizio Web (QaaWS), Profile, Discussions, InformationDesigner, widget per la piattaforma SAP BusinessObjects Business Intelligence, MDAnalysis, Publications, Flash, Analytic e Hyperlink	Nel contenuto dei metadati è possibile eseguire ricerche.
Eventi	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. **Nota:** Ricerca piattaforma supporta eventi per Crystal Reports for Enterprise.

Nota:
la dimensione massima supportata per i documenti generali (documenti MS Office 2003 e 2007 e PDF) è 15 MB.

17.7 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 SAP BusinessObjects Business Intelligence.

Ricerca piattaforma analizza la struttura degli universi e dei report esistenti nel repository della piattaforma SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects 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 di SAP BusinessObjects 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 SAP BusinessObjects 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.

17.8 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 della piattaforma SAP Business Objects Business Intelligence vengono raggruppati nelle categorie o nei facet generici elencati di seguito:

- Personale o pubblico (ad esempio HR, Aziendale e Finanziario): basato sulle categorie di documenti della piattaforma BI.
- Tipo di documento: basato sul tipo di documento, ad esempio Web Intelligence, Crystal Report, Microsoft Word (2003 e 2007), Microsoft Excel (2003 e 2007) e Xcelsius.
- 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.

17.9 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. Recupera i risultati in base alla lingua impostata nelle **Impostazioni internazionali indice** nell'applicazione CMC, indipendentemente dalle impostazioni locali del client. Ricerca piattaforma indicizza i metadati, le proprietà dei documenti e il contenuto dei report.

Il processo di indicizzazione utilizza l'Analyzer per le impostazioni locali specificate nella pagina di configurazione. In qualsiasi momento viene utilizzata solo una lingua per l'indicizzazione.

Per ottenere risultati migliori dalla ricerca, è necessario utilizzare le stesse impostazioni locali sia per l'indicizzazione che per la ricerca. Per impostazione predefinita, la lingua specificata in Impostazioni internazionali indice è l'inglese, pertanto viene utilizzata la lingua inglese sia per l'indicizzazione che per la ricerca. Se si modificano le impostazioni locali, l'indice viene nuovamente inizializzato o creato in base all'opzione selezionata quando si salva la nuova configurazione. L'impostazione della nuova lingua verrà utilizzata per l'indicizzazione dei documenti successivi.

Se si modificano le impostazioni locali e si sceglie un'altra lingua, ad esempio si passa dall'inglese al tedesco nell'applicazione CMC, l'intero indice viene gradualmente aggiornato utilizzando l'Analyzer per il tedesco per tutti i documenti esistenti.

Se le impostazioni locali vengono reimpostate su un'altra lingua, ad esempio si passa dall'inglese al tedesco, e quindi si seleziona **Rigenera indice**, l'indice corrente viene eliminato e viene creato un nuovo indice in tedesco.

17.10 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 algoritmicamente 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** nell'applicazione CMC.

Nota:
Ricerca piattaforma non genera suggerimenti:

- 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

17.11 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 SAP BusinessObjects Business Intelligence.

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.

17.12 Integrazione in fase di ricerca con la funzionalità di ricerca di SAP NetWeaver Enterprise

La funzionalità di ricerca di SAP NetWeaver Enterprise 7.20 e le versioni successive possono utilizzare il 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. Importare un ruolo utente nella sezione di autenticazione della piattaforma SAP BusinessObjects Business Intelligence.

17.12.1 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.

17.12.2 Importazione di un ruolo utente nella sezione di autenticazione di SAP BusinessObjects Enterprise

Per importare un ruolo utente nella sezione di autenticazione della piattaforma SAP BusinessObjects Business Intelligence, attenersi alla procedura riportata di seguito:

Nota:
è necessario che l'amministratore disponga dei dettagli relativi all'utente, delle informazioni di sistema e di credenziali utente e informazioni relativi 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. Fare clic sulla scheda "Importazione ruolo" e importare i ruoli utente.
6. Scegliere **Aggiorna**.
7. Scegliere **Gestisci** > **funzioni di protezione dell'utente** nella CMC per assegnare i diritti utente appropriati.

17.12.3 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.

17.13 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.

Esistono un ID evento 1009 per Ricerca piattaforma e quattro dettagli evento specifici per 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 evento 1009
- ID dei dettagli evento 19 con valore vendite
- ID dei dettagli evento 63 con valore 5
- Cuid sessione
- Cuid utente
- Stato con valore 0, che rappresenta lo stato riuscito
- Ora di inizio
- Durata
- Oggetto
- ID 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 evento 1009
- ID dei dettagli evento 19 con valore vendite
- ID dei dettagli evento 63 con valore 5
- ID dei 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 evento 1009
- ID dei dettagli evento 19 con valore vendite
- ID dei dettagli evento 63 con valore 0
- ID dei 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

17.14 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. Fare clic su **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.

17.15 Risoluzione dei 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 SAP BusinessObjects Business Intelligence e viene avviata la reindicizzazione del documento.

  Per ulteriori informazioni sul documento di cui non è riuscita 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. Nel file system passare alla directory {Dir install BOE}\logging\ contenente il registro di analisi di APS con estensione .gif.
  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.

Impossibilità di recuperare i documenti Crystal Report come risultati della ricerca

Ricerca piattaforma indicizza il contenuto Crystal Report 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 del documento, quali il titolo, la descrizione e la parola chiave, che fanno parte delle 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.*

Impossibilità di recuperare i risultati della ricerca nella lingua definita nelle impostazioni locali del prodotto in BI Launch Pad

Ricerca piattaforma consente agli utenti di eseguire ricerche sul contenuto del repository della piattaforma SAP BusinessObjects Business Intelligence e di indicizzarlo in base alle impostazioni locali dell'indice della CMC. Se le impostazioni locali del prodotto definite in BI Launch Pad sono diverse da quelle definite nella CMC, Ricerca piattaforma non recupera i risultati.

Per ulteriori informazioni sulla configurazione delle impostazioni locali dell'indice, fare riferimento all'argomento *Configurazione delle proprietà delle applicazioni* negli argomenti correlati elencati di seguito.

Impossibilità di recuperare gli infospace SAP BusinessObjects Explorer come risultati della ricerca

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 risultati dal repository della piattaforma SAP BusinessObjects Business Intelligence

- 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 SAP BusinessObjects Enterprise 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 SAP BusinessObjects Business Intelligence 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
- Tipi di contenuto in cui è possibile eseguire ricerche

Federazione

18.1 Federation

Federation è uno strumento di replica tra siti per l'utilizzo di più distribuzioni della piattaforma SAP BusinessObjects Business Intelligence 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 livello individuale.
Report	Crystal Reports, 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.

18.2 Termini correlati a Federation

Nel seguente elenco di termini vengono introdotte parole e frasi correlate a Federation con istruzioni per l'utilizzo:

18.2.1 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.

18.2.2 Sito di destinazione

Un sistema della piattaforma BI che estrae il contenuto replicato della piattaforma da un sito di origine.

18.2.3 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.

18.2.4 Istanze completate eseguite localmente

Istanze elaborate nel sito di destinazione e inviate nuovamente al sito di origine.

18.2.5 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.

18.2.6 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.

18.2.7 Sito di origine

Il sistema della piattaforma BI in cui ha origine il contenuto.

18.2.8 &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.

18.2.9 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.

18.2.10 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.

18.2.11 Replica

Processo di copia del contenuto da un sistema della piattaforma BI a un altro.

18.2.12 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.

18.2.13 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.

18.2.14 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.

18.2.15 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).

18.2.16 Aggiornamento della replica

Tutti gli oggetti inclusi in un elenco di replica vengono aggiornati a prescindere dall'ultima versione modificata.

18.2.17 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.

18.3 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.

18.3.1 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. **Nota:** I diritti “Visualizzazione” e “Replica” sono necessari su tutti gli oggetti da replicare, inclusi quelli replicati automaticamente dai calcoli di dipendenza.	• “Visualizza” e “Replica” su tutti gli oggetti che si desidera replicare. • Diritto di “Visualizzazione” nell'elenco di replica.
Replica bilaterale	Esegue la replica dal sito di origine al sito di destinazione e viceversa.	• “Visualizza” e “Replica” su tutti gli oggetti che si desidera replicare. • Diritto di “Visualizzazione” nell'elenco di replica. • “Modifica i diritti” sugli oggetti dell'utente per replicare qualsiasi modifica di password.
Pianificazione	Consente l'esecuzione della pianificazione remota nel sito di origine dal sito di destinazione.	• Diritto “Pianifica” per tutti gli oggetti che si desidera pianificare in modo remoto

Argomenti correlati

• Diritti richiesti nel sito di destinazione

18.3.2 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.	• “Visualizza,”“Aggiungi,”“Modifica” e “Modifica i diritti” su tutti gli oggetti • Diritto “Modifica password utente”, per gli oggetti utente
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.	• Diritti “Visualizza”, “Aggiungi”,“Modifica” e “Modifica diritti” in tutte le cartelle di livello superiore e in tutti gli oggetti predefiniti

Argomenti correlati

- Diritti richiesti sul sito di origine

18.3.3 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.	• L'account in cui è in esecuzione il processo di replica richiede i diritti “Elimina” su tutti gli oggetti che potrebbero essere potenzialmente eliminati.
Disabilitare l'eliminazione per determinati oggetti	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. 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.	• Negare i diritti “Elimina” dell'account utente con cui è in esecuzione il processo di replica per gli oggetti che si desidera mantenere.
Replica bilaterale, senza modifiche nel sito di origine		• Negare i diritti “Modifica”dell'account utente utilizzato per la connessione nell'oggetto connessione remota.

Azione	Descrizione	Diritti richiesti
	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. **Nota:** per la pianificazione remota, è possibile creare un processo che gestisca solo gli oggetti per la pianificazione remota. Tuttavia, in questo caso gli oggetti antenati 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.	

18.3.4 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.

18.3.5 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 acceso 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.

18.4 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

18.4.1 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

18.4.2 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

18.4.3 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 di 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.

18.5 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.

18.6 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”.

18.7 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. **Nota:** Tutti gli oggetti sono supportati anche se non al singolo livello.
Report	Report Crystal, documenti Web Intelligence e oggetti Xcelsius. **Nota:** 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

18.7.1 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.

18.7.1.1 Per creare 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.

18.7.1.2 Per creare 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: 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**.

18.7.2 Modifica degli elenchi di replica

Dopo avere creato un elenco di replica, è possibile modificarne le proprietà o gli oggetti.

18.7.2.1 Per modificare le 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

18.7.2.2 Per modificare 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

18.8 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.

18.8.1 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.

18.8.1.1 Per creare 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.

18.8.1.2 Per creare 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	URL di Servizi Web di Federation, distribuiti automaticamente sul server delle applicazioni Java. È possibile utilizzare qualsiasi servizio Web di Federation nella piattaforma BI sia sul sito di origine sia su quello di destinazione o un'altra distribuzione. Utilizzare questo formato: http://*nome_server_applicazioni*:*porta*/dswsbobje Esempio: http://*computer.dominio.com*:*8080*/dswsbobje
CMS sistema remoto	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. Si tratta del formato: Nome_CMS:porta Esempio: mymachine:6400 **Nota:** se si utilizza la porta predefinita 6400, la specifica della porta è facoltativa.
Nome utente	Nome utente che verrà utilizzato per connettersi al sito di origine. **Nota:** assicurarsi che il nome utente utilizzato disponga dei diritti di visualizzazione per l'elenco di replica nella distribuzione del sito di origine.
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. Fare clic su **OK**.

Argomenti correlati

- Gestione dell'eliminazione di oggetti

18.8.2 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**.

18.9 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.

18.9.1 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.

18.9.1.1 Per creare 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
Attiva eliminazione oggetto sulla destinazione	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. **Nota:** con l'eliminazione di oggetti non verranno eliminati oggetti replicati utilizzando dipendenze o oggetti selezionati nell'elenco di replica.
Replica unilaterale	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.
Replica bilaterale	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.
Precedenza del sito di origine	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.
Nessuna risoluzione conflitti automatica	Specifica che non venga eseguita alcuna azione per risolvere eventuali conflitti rilevati.
Precedenza del sito di destinazione (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.
Replica normale	Specifica che il processo di replica venga eseguito normalmente.
Aggiorna da origine	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.
Aggiorna da destinazione (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
Replica tutti gli oggetti (disponibile unicamente con la replica bilaterale)	Replica l'intero elenco di replica. **Nota:** Si tratta dell'opzione più completa, ma anche più lunga.
Replica pianificazioni remote (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.
Replica modelli documento	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.
Replica istanze completate eseguite localmente	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

18.9.2 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.

18.9.2.1 Per pianificare 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.

18.9.3 Modifica dei processi di replica

Dopo avere creato un processo di replica in Federation, è possibile modificarne le proprietà.

18.9.3.1 Per modificare 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.

18.9.4 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 nel percorso:

   - Windows:`<DirInstall>\SAP BusinessObjects XI 4.0\logging`
   - Unix:`<DirInstall>/sap_bobj/logging`

18.10 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.

18.10.1 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.

18.10.2 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.

18.10.3 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

18.11 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.

18.11.1 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.

18.11.2 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 reinviate 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.

18.12 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.

18.12.1 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>`\dswsbobje\Web-INF\classes`

Ad esempio:

`C:\Programmi\SAP BusinessObjects\Tomcat6\webapps\dswsbobje\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.

18.12.2 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\Tomcat6\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.

18.12.3 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\Tomcat6\webapps\dswsbobje\WEB-INF\services

Per disattivare 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\Business Objects\Tomcat55\webapps\dswsbobje\WEB-INF\services\federator\META-INF

Modificare il nome come segue:

<service name="Federator">

A:

<service name="Federator" activate="false">

18.13 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.

18.13.1 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 riuscita sarà 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

18.13.2 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.

18.13.3 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

18.14 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.

18.14.1 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.

18.14.2 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:

- Assicurarsi che il CUID degli oggetti venga mantenuto quando si utilizza LifeCycle Manager.
- Assicurarsi 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 LyfeCicle 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.

18.14.3 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.

18.14.4 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.

18.15 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 alto numero 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. I processi di replica più grandi potrebbero impegnare più a lungo il provider di servizi Web e rallentarne la risposta alle richieste di altri servizi Web e delle applicazioni che gestisce.

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 "$BOBJEDIR"/tomcat ]; then
 # set the JAVA_OPTS for Tomcat
 JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"

 if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" =
"SunOS" -o "$SOFTWARE" = "Linux" -o "$SOFTWARE" = "HP-UX" ];
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:

```
Dbobj.biar.suggestSplit
and
Dbobj.biar.forceSplit
```

`bobj.biar.suggestSplit` suggerisce una dimensione appropriata per il file BIAR, che cercherà di raggiungere e mantenere. Il nuovo valore suggerito è 90 MB.

`bobj.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
      -Dbobj.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 "$SOFTWARE" = "Linux" -o "$SOFTWARE" = "HP-UX" ]; 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

18.15.1 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

18.15.2 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` o `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 altro percorso per la directory temporanea nel sito di origine, aggiungere la riga seguente nei file di configurazione del server di applicazioni Java: `-Dbobj.tmp.dir=<TempDir>`.

Per specificare un altro percorso per la directory temporanea nel sito di destinazione, aggiungere la riga seguente negli 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

19.1 Configurazioni per l'integrazione di SAP NetWeaver

19.1.1 Integrazione con SAP Netweaver Business Warehouse (BW)

19.1.1.1 Presentazione

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

19.1.1.1.1 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 a seguito della definizione di un sistema di autorizzazione durante a 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

19.1.1.1.2 Comprensione dei modelli di protezione predefiniti delle cartelle

Quando si esegue la pubblicazione del contenuto nella piattaforma BI da SAP, il sistema crea automaticamente la gerarchia rimanente dei ruoli, delle cartelle e dei report. In altre parole, la piattaforma BI organizza i report Crystal in cartelle i cui nomi si basano sull'ID di sistema e sul numero client, in base al nome del ruolo.

Nel diagramma che segue viene illustrato come la piattaforma BI organizza il contenuto quando si pubblicano due ruoli da un sistema BW:

- La piattaforma BI crea le cartelle di livello principale, ossia 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. A tale scopo, è necessario assegnare i seguenti diritti nel workbench per l'amministrazione dei contenuti.

Cartelle dei contenuti

La piattaforma BI importa un gruppo per ogni ruolo che viene aggiunto al sistema di autorizzazione come definito nella CMC.

Per assicurarsi 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.

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 predefiniti per i report** su **Visualizza**.
5. Impostare **Criteri di protezione predefiniti per le cartelle di ruoli** su **Visualizza 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.

19.1.1.2 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 con 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 nell'area di lavoro per l'amministrazione dei contenuti.

19.1.1.3 Configurazione di Publisher BW come servizio

In questa sezione viene illustrato come abilitare la pubblicazione dei report da BW alla piattaforma BI, utilizzando Publisher BW come un servizio.

19.1.1.3.1 Distribuzione dell'installazione di Publisher BW

In questa sezione viene illustrata la distribuzione del servizio Publisher BW e some 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 nella stessa distribuzione 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 che si è creata una destinazione RFC che utilizza questo ID programma, BW esegue il bilanciamento del carico della pubblicazione tra i computer della 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 su 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 (Software Development Kit) della piattaforma BI e al motore di stampa di Crystal Reports. Quindi, se si installa Publisher BW e il gateway SAP locale su un computer dedicato, è necessario installare anche il server SIA.

19.1.1.3.2 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.

19.1.1.3.3 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.

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.

19.1.1.3.4 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 ciascun sistema della piattaforma BI. È necessario utilizzare ID di programma univoci per ciascuna destinazione, ma gli stessi host e servizio gateway.

19.1.1.3.5 Configurazione di Publisher BW con un gateway SAP locale

Nota:
Non utilizzare questa configurazione se la piattaforma BI è installata su UNIX. L'utilizzo di questo metodo in UNIX potrebbe restituire un comportamento di sistema imprevedibile.

Per abilitare la pubblicazione dei report da BW alla piattaforma BI utilizzando un gateway SAP locale, attenersi alla procedura seguente:

- Installazione di un gateway SAP locale.
- Configurazione di una destinazione per Publisher BW.

19.1.1.3.6 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 per la piattaforma BI, 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, ecc.

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`.

19.1.1.4 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.

19.1.1.5 Configurazione della pubblicazione nel workbench per l'amministrazione dei contenuti

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 distribuzione della piattaforma BI in cui è pubblicato il contenuto.
- Definire i ruoli che possono eseguire la pubblicazione in ciascuna distribuzione della piattaforma BI.
- Pubblicare il contenuto da BW alla piattaforma BI.

19.1.1.6 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.

19.1.1.7 Creazione dei ruoli in BW per i publisher dei contenuti designati

Quando è necessario configurare 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.

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:
nella piattaforma BI 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 necessario dapprima impostare l'autenticazione SAP e importare i ruoli. È quindi possibile modificare i diritti di ciascun ruolo importato tramite la Central Management Console.

19.1.1.8 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 19 - 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

Oggetto autorizzazione	Campo	Valori
S_TABU_CLI	CLIIDMAINT	X
S_TABU_DIS	ACTVT	Modifica, Visualizza (02, 03)
	DICBERCLS	&NC&
	JOBACTION	DELE, RELE
	JOBGROUP	' '
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 19 - 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	JOBACTION	DELE, RELE
	JOBGROUP	' '
	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 presente, però, 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 BI, 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)

19.1.1.9 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.

19.1.1.9.1 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. Nella scheda **Sistema** immettere i seguenti valori:
   - 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 della piattaforma BI. 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 al sistema della piattaforma BI. 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 la ridondanza del sistema.

7. A questo punto provare la destinazione. Selezionare la destinazione appena aggiunta facendo clic sulla casella grigia a sinistra del nome.
8. Fare clic su **Verifica la definizione CE**.

   In questa prova viene verificato se BW può contattare il Publisher BW specificato e può accedere a questo sistema della piattaforma BI mediante l'account utente di autorizzazione Crystal.

9. Nella scheda **HTTP** immettere i seguenti valori:
   - **Protocollo**

     Digitare http (a meno che il server Web connesso alla piattaforma BI non sia configurato in modo da utilizzare https).

   - **Porta e host del server Web**

     Digitare il nome di dominio completo o l'indirizzo IP 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:

     ```
     boserver01.businessobjects.com:8080
     ```

   - **Percorso**

     Tipo:

     ```
     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 si sono personalizzati l'ambiente Web e il percorso dei file del contenuto Web della piattaforma BI.

     Non includere una barra rovesciata all'inizio o alla fine della voce.

   - **Applicazione visualizzatore**

     Digitare il nome dell'applicazione visualizzatore. Digitare reportview.do per utilizzare il visualizzatore predefinito per le installazioni della piattaforma BI che utilizzano la versione Java di InfoView. Se la piattaforma BI è stata installata in Windows mediante la configurazione ASP.NET predefinita, digitare report/report_view.aspx per utilizzare il browser predefinito.

10. Nella scheda **Lingue** selezionare le lingue dei report che verranno pubblicati in questo sistema della piattaforma BI.
11. Utilizzare la scheda **Ruoli** per aggiungere i ruoli di generazione dei contenuti che si desidera associare a questo sistema della piattaforma BI.
12. Fare clic sul pulsante **Inserisci riga**.

    Viene visualizzato un elenco dei ruoli disponibili da aggiungere a questo sistema della piattaforma BI.

Nota:
ciascun ruolo può eseguire la pubblicazione solo in un sistema della piattaforma BI. Se i ruoli che si desidera aggiungere a questa piattaforma BI non appaiono nell'elenco, fare clic su **Annulla** per tornare alla scheda **Ruoli**. Quindi, fare clic su **Riassegna i ruoli**.

13. Selezionare i ruoli che si desidera pubblicare nel sistema della piattaforma BI e fare clic sul pulsante **OK**.
14. Quindi definire le impostazioni di protezione predefinite per i contenuti pubblicati in questo sistema della piattaforma BI. Fare clic sulla scheda **Layout**, quindi selezionare le impostazioni di protezione utilizzate per impostazione predefinita per i report e le cartelle dei ruoli.

    Nota:

    - Per ciascun ruolo pubblicato nel sistema viene automaticamente creata una cartella nella piattaforma BI. Questa 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 BI, eliminare le cartelle dei ruoli e i collegamenti nella piattaforma BI. Si tenga presente che non vengono eliminati i report effettivi. Modificare quindi le impostazioni di protezione e pubblicare di nuovo i ruoli e i report.
15. Fare clic sul pulsante **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.

19.1.1.10 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 può utilizzare il workbench per l'amministrazione dei contenuti per pubblicare e gestire i report.

Argomenti correlati

- Creazione e applicazione delle autorizzazioni

19.1.1.11 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 **Sistema** selezionare il sistema o i sistemi della piattaforma BI in cui è disponibile il contenuto che si desidera visualizzare.

   Nota:
   l'elenco **Sistema** contiene tutti i sistemi disponibili definiti in questo 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 > 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

19.1.1.12 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 il sistema 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.

19.1.1.13 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.

19.1.1.14 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 BI (Post-migrazione).

19.1.1.14.1 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 Manutenzione report.

19.1.1.14.2 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.

19.1.1.15 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.

19.1.1.16 Configurazioni per l'elaborazione di dati SAP

19.1.1.16.1 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_OPENSQL_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 su 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 (cioè i report eseguiti dal Report Job Server), evitare di impostare le variabili di ambiente di sistema sui computer su cui sono in esecuzione combinazioni di server della piattaforma BI. Eseguire invece queste operazioni per personalizzare le variabili di ambiente per ciascun Report 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

19.1.1.16.2 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_OPENSQL_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 Report Job Server.
3. Avviare il Central Configuration Manager (CCM) dal gruppo di programmi della piattaforma BI.
4. Fare clic con il pulsante destro del mouse su **Crystal Report Job Server**, quindi selezionare **Arresta** dal menu di scelta rapida.
5. Fare clic con il pulsante destro del mouse su **Crystal Report Job Server**, quindi selezionare **Proprietà** dal menu di scelta rapida.
6. Nella scheda **Proprietà** individuare il campo **Comando**.

   Si tratta del comando di avvio per il Report Job Server. Ad esempio, il comando può assumere l'aspetto seguente (una sola linea):

```
"\\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
```

7. Fare precedere al comando predefinito il percorso completo del file `jobserver_batchmode.bat` salvato sul computer su cui è in esecuzione il Report 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 il Report Job Server è:

```
"\\SERVER01\C$\Crystal Scripts\jobserver_batchmode.bat" "\\SERVER01\C$\Program Files\SAP Business Obje
cts\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 il Report Job Server. In questo modo le variabili di ambiente disponibili per il Report 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).

8. Dopo avere modificato il campo **Comando** nel CCM, fare clic su **OK**.
9. Fare clic con il pulsante destro del mouse su **Crystal Report Job Server**, quindi selezionare **Avvia** dal menu di scelta rapida.

Nota:
se il Report Job Server non viene avviato, verificare il nuovo comando di avvio.

10. Sulla barra degli strumenti del CCM fare clic su **Abilita/Disabilita server**, accedere con le credenziali di amministratore della piattaforma BI, quindi assicurarsi che il Report Job Server sia abilitato.

19.1.1.17 Configurazioni per trasporti SAP

19.1.1.17.1 Panoramica

La piattaforma BI include otto trasporti: Open SQL Connectivity, connettività InfoSet, the Row-level Security Definition, Cluster Definition, Content Administration Workbench, il trasporto per la personalizzazione dei parametri BW Query, il trasporto MDX e il 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.

19.1.1.17.2 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.

Ogni tipo di trasporto è descritto di seguito.

- 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.

Verifica dei conflitti

Il contenuto dei file di trasporto viene registrato automaticamente nello spazio dei nomi SAP Business Objects quando si importano i file. Lo spazio dei nomi SAP Business Objects 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 della piattaforma BI. Fare riferimento alla documentazione di SAP per le procedure appropriate alla versione di SAP.

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

Oggetto	Tipo	Descrizione
/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_PA RAM	Tabella	Metadati funzione
/CRYSTAL/OSQL_FCN_PA RAM_FIELD	Tabella	Metadati funzione
/CRYSTAL/OSQL_FIELD_EN TRY	Tabella	Metadati tabella
/CRYSTAL/OSQL_OBJECT_EN TRY	Tabella	Metadati tabella
/CRYSTAL/OS QL_RLS_CHK_ENTRY	Tabella	Metadati RLS

Oggetto	Tipo	Descrizione
/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
/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/QUE RY_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

Oggetto	Tipo	Descrizione
/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

Oggetto	Tipo	Descrizione
ZCDD	Transazione	Transazione programma principale

Workbench per amministrazione 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
/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

Oggetto	Tipo	Descrizione
/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
/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

Oggetto	Tipo	Descrizione
/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
/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

Oggetto	Tipo	Descrizione
/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

Oggetto	Tipo	Descrizione
/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
/CRYS TAL/MDX_STREAM_LAYOUT	Definizione tabella	Struttura di insieme di dati
/CRYSTAL/CX_BAPI_ERROR	Classe	Eccezione
/CRYSTAL/CX_METADATA_ER ROR	Classe	Eccezione
/CRYSTAL/CX_MISSI NG_STREAMINFO	Classe	Eccezione
/CRYS TAL/CX_NO_MORE_CELLS	Classe	Eccezione
/CRYSTAL/CX_NO_MORE_ME MBERS	Classe	Eccezione

Oggetto	Tipo	Descrizione
/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
/CRYSTAL/MDX_STREAM_LAYOUT_TAB	Tipo di tabella	Struttura di metadati

19.1.1.18 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 appendice 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 di BusinessObjects XI Integration for SAP necessari per il supporto delle query Open SQL.

19.1.1.18.1 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

19.1.1.19 Azioni in BW

In queste sezione vengono illustrate una serie di azioni eseguibili in BW.

19.1.1.19.1 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***
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, /CRYS-TAL/PERS, RSOB
	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

* *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	*USER_ROLE**
	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	*USER_ROLE**
	ACTVT	01
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 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.

19.1.1.19.2 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	STOR, STOM

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	*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.

Pianificazione di un report

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

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

19.1.1.19.3 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 SWL.

Connessione a un server SAP

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	ACTVT	16

Creazione di un nuovo report

Oggetto autorizzazione	Campo	Valori
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST, /CRYSTAL/OPENSQL
	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/OPENSQL
	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	STOR, STOM
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

Impostazione del percorso dell'origine dati

Oggetto autorizzazione	Campo	Valori
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQL
	ACTVT	16

19.1.1.19.4 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	STOR, STOM

Impostazione del percorso dell'origine dati

Oggetto autorizzazione	Campo	Valori
P_ABAP	REPID	AQTGSYSTGENERATESY, SAPDBPNP
	COARS	2

19.1.1.19.5 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	STOR, STOM
S_TABU_DIS	ACTVT	03
	GROUP	Nome del gruppo di tabelle

Verifica del database

Oggetto autorizzazione	Campo	Valori
S_ADMI_FCD	S_ADMI_FCD	STOR, STOM
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	STOR, STOM
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16
S_TABU_DIS	ACTVT	03
	GROUP	Nome del gruppo di tabelle

19.1.1.19.6 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)	* **Nota:** per maggiore sicurezza, si consiglia di elencare esplicitamente i gruppi di utenti i cui membri richiedono l'accesso alla piattaforma BI.

19.2 Configurazione per l'integrazione JD Edwards

19.2.1 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).

19.2.1.1 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. Riavviare SAP Crystal Reports.

19.2.1.2 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. "In Utilizza il contesto SSO per accedere al database..." digitare **crdb_pseone**.
5. Fare clic su **Aggiungi**.
6. Fare clic su **Salva e chiudi**.
7. Riavviare i server Crystal Reports.

19.2.2 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).

19.2.2.1 Per abilitare la connettività dati JD Edwards EnterpriseOne con SSL

Nota:
Tutti i valori descritti nella procedura seguente fanno distinzione tra maiuscole e minuscole.

- Configurare i due valori del registro sotto la chiave del registro seguente:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Business
Objects\Suite 12.0\Integration Kit for
PeopleSoft EnterpriseOne\QRY\Instances\noname]
 "CommunicationProtocol"="ssl"
 "SSL Configuration File"="C:\Program
Files\Business Objects\BusinessObjects XI 13.0\sslconf.properties"
```

Riavviare i servizi di reporting della piattaforma BI, ad esempio Crystal Reports Job Server, per applicare le modifiche.

19.2.2.2 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, ovvero `C:\Programmi\Business Objects\BusinessObjects 13.0` per impostazione predefinita.

19.3 Configurazione per l'integrazione PeopleSoft Enterprise

19.3.1 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).

19.3.1.1 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. Riavviare SAP Crystal Reports.

19.3.1.2 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. "In Utilizza il contesto SSO per accedere al database..." digitare **crdb_psenterprise**.
5. Fare clic su **Aggiungi**.
6. Fare clic su **Salva e chiudi**.
7. Riavviare SAP Crystal Reports.

19.3.2 Configurazione per le comunicazioni Secure Socket 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).

19.3.2.1 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 SAP. 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 in cui è installata la piattaforma BI. Per impostazione predefinita, la cartella è `C:\Programmi\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\`.

19.3.2.2 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 reporting di BusinessObjects, ad esempio Crystal Reports Job Server, per rendere effettive le modifiche.

19.3.2.3 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.

19.3.3 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.

19.3.3.1 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.

19.3.3.2 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.

19.4 Configurazione per l'integrazione Siebel

19.4.1 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 BusinessObjects Business Intelligence in un'applicazione Siebel. Dopo l'installazione e la configurazione, la nuova voce di menu consente agli utenti di avviare InfoView 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.

19.4.1.1 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: *<directory installazione>*`\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 **Merge the object definition form the archive file with the definition in the 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. Fare clic sul progetto **SAP BusinessObjects Integration**.

19.4.2 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
   - Caption: 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.

19.4.2.1 Ricompilazione dell'applicazione Siebel

Una volta installata la piattaforma BI e messo il relativo comando a disposizione degli utenti mediante una voce di menu Siebel, è necessario ricompilare l'applicazione Siebel attenendosi alle consuete procedure. Per informazioni dettagliate, 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.cfg`. Per impostazione predefinita il file si trova in `C:\sea77\siebsrvr\bin\ENU\uagent.cfg` 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.

19.4.3 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.

19.4.3.1 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) per la piattaforma BI.
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.

19.4.3.2 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 incollare il file BusinessObjectsEnterpriseServer.html nella sottocartella della lingua appropriata.

   Se ad esempio i file JavaScript dell'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.

19.4.3.3 Verifica della funzionalità Contextual Awareness

1. Accedere a un'applicazione Siebel che utilizza il menu Generic Web modificato.
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 viene aperta la finestra BI Launch Pad, che richiede l'immissione di nome utente e password per la connessione (solo quando si accede per la prima volta prima del timeout della 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 nella piattaforma BI.

19.4.3.4 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: `Directory principale\Siebel\Nome dominio`. Solo i report memorizzati nella sottocartella `Nome dominio` e configurati nel sistema Siebel per l'associazione allo specifico componente business di 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.

19.4.4 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).

19.4.4.1 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.

19.4.4.2 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.

19.4.5 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 BusinessObjects XI Integration for Siebel. Ad esempio:

```
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 in cui è installata la piattaforma BI, ovvero `C:\Programmi\Business Objects\SAP BusinessObjects Enterprise XI\` per impostazione predefinita.

Gestione e configurazione dei registri

20.1 Registrazione di analisi dai componenti

L'analisi consente agli amministratori di sistema e al personale di supporto di creare report sulle prestazioni dei componenti della piattaforma BI (server e applicazioni Web) e sull'attività svolta all'interno dei componenti monitorati.

I messaggi a livello di sistema generati dai server della piattaforma BI vengono analizzati e scritti nei file di registro. I file di registro vengono utilizzati dagli amministratori di sistema per il monitoraggio delle prestazioni o per il debug. Le analisi sono registrazioni di eventi che si verificano durante il funzionamento di un componente monitorato. Gli eventi analizzati vanno dai gravi errori di eccezione ai semplici messaggi di stato.

Registro di analisi

I messaggi di analisi vengono raccolti in file di registro salvati con la generica estensione `glf`. Quando si imposta il livello del registro di analisi per un componente, si determina il tipo e il dettaglio delle informazioni inviate al file di registro. Il livello del registro di analisi è in effetti un filtro che sopprime le analisi che si trovano al di sotto di un livello di importanza specificato. Le analisi soppresse non vengono scritte nel file di registro di output. Monitorando il registro di analisi per un componente, è possibile determinare se è necessario modificare l'istanza corrente del componente o la configurazione per gestire l'aumento del carico di lavoro o se l'aumento del carico non influisce in modo significativo sulle prestazioni.

20.2 Livelli del registro di analisi

Nella tabella seguente sono descritti i livelli del registro di analisi disponibili per i componenti della piattaforma BI:

Livello	Descrizione
Non specificato	Il livello del registro di analisi viene specificato mediante un altro meccanismo, in genere un file con estensione `ini`.
Nessuno	Quando il livello del registro di analisi è impostato su "Nessuno", il filtro che consente di sopprimere le analisi al di sotto di un livello di importanza specificato è disattivato. **Nota:** il livello del registro di analisi "Nessuno" non indica che la funzione di analisi è disattivata. Le risorse di sistema continuano a essere monitorate e le analisi vengono registrate per eventi critici rari quali asserzioni non riuscite.
Basso	Il filtro del registro di analisi è impostato in modo da consentire la registrazione dei messaggi di errore ignorando i messaggi di avviso e la maggior parte dei messaggi di stato. Verranno comunque registrati i messaggi di stato più importanti, ad esempio quelli per l'avvio e la chiusura dei componenti o i messaggi di richiesta di avvio e chiusura. **Nota:** 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 nell'output del registro i messaggi di errore, avviso e la maggior parte dei messaggi di stato. I messaggi di stato meno importanti o con un livello di dettaglio elevato verranno esclusi dal filtro. Questo livello non è sufficientemente dettagliato per le finalità di debug.
Alto	Il filtro non escluderà alcun messaggio. L'impostazione di questo livello è consigliata per le finalità di debug. **Nota:** un livello di registro di analisi "Alto" potrebbe avere un impatto negativo sulle risorse di sistema. Potrebbe comportare un utilizzo maggiore della CPU nonché richiedere una quantità di spazio di archiviazione maggiore nel file system.

20.3 Configurazione dell'analisi per i server

Le analisi relative a un server della piattaforma BI monitorato vengono scritte in un file di registro specifico (`.glf`) e archiviate nella cartella o directory di registrazione. Nelle piattaforme Windows la directory di `registrazione` si trova per impostazione predefinita in `Programmi <DIRINSTALLAZ>\SAP BusinessObjects Enterprise XI 4.0\logging`. In Unix si trova in `<DIRINSTALLAZ>/sap_bobj/logging`.

Nota:
il nome del file .glf viene formattato come una combinazione di identificatore abbreviato, nome del server e numero di riferimento, ad esempio `aps_mysia.AdaptiveProcessingSer`

`ver_trace.000012.glf`. Viene creato un nuovo file di registro di analisi per il server monitorato quando la dimensione del file di registro si avvicina alla soglia di 1 megabyte.

Gli amministratori possono 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. È possibile modificare il livello del registro di analisi utilizzando i seguenti metodi consigliati:

- Utilizzando il "Servizio log analisi" per un server specifico o un gruppo di server nella console CMC
- Modificando manualmente il livello del registro di analisi e altre impostazioni nel file `BO_trace.ini`.

Se si desidera modificare il livello del registro di analisi solo per server specifici, si consiglia di utilizzare il "Servizio log analisi" nella console CMC. Per modificare altri parametri di analisi, è necessario riconfigurare il file `BO_trace.ini`.

20.3.1 Impostazione del livello del registro di analisi del server nella console CMC

Il livello del registro di analisi per un server può essere modificato senza influire su altre impostazioni dell'analisi. Per modificare il livello del registro di analisi, attenersi alle indicazioni che seguono.

1. Passare all’area di gestione "Server" della CMC.
2. Accedere ai server di cui si desidera modificare il livello del registro di analisi.
   a. Fare clic sulla categoria del server per accedere a un server o ai server di una “categoria” specifica.
   b. Fare clic su **Elenco server** nel riquadro di spostamento per accedere all'elenco completo di server.
3. Fare clic con il pulsante destro del mouse sul server e scegliere **Proprietà**.

   Viene visualizzata la finestra di dialogo "Proprietà".
4. Nell'area del "servizio Registro di analisi" selezionare l'impostazione desiderata nell'elenco "Livello log".
5. Fare clic su **Salva e chiudi** per inviare il livello del registro di analisi modificato.

Il nuovo livello del registro di analisi diventa effettivo entro un minuto.

Per specificare un'altra directory per i file di registro, utilizzare il parametro `-loggingPath` insieme a un percorso alla directory di destinazione nell'area "Parametri riga di comando". Questa modifica viene applicata solo dopo il riavvio del server.

Argomenti correlati

- Livelli del registro di analisi

20.3.2 Impostazione del livello del registro di analisi per più server gestiti nella console CMC

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

   Le categorie di servizio disponibili sono visualizzate nella pagina "Server".
2. Accedere ai server per cui si desidera reimpostare il livello del registro di analisi.
   a. Fare clic sulla categoria del server per accedere a un server o ai server di una categoria specifica.
   b. Fare clic su **Elenco server** nel pannello di spostamento per accedere all'elenco completo dei server.
3. Selezionare i server.

   Per selezionare più server, tenere premuto il tasto **Ctrl** mentre si effettua la selezione.
4. Fare clic con il pulsante destro e selezionare **Modifica servizi comuni**.

   Viene visualizzata la schermata "Modifica servizi comuni".
5. Nell'area del "servizio Registro di analisi" selezionare l'impostazione desiderata nell'elenco "Livello log".
6. Fare clic su **OK** per inviare il livello del registro di analisi modificato.

Il nuovo livello del registro di analisi diventa effettivo entro un minuto.

Per specificare un'altra directory per i file di registro, utilizzare il parametro `-loggingPath` insieme a un percorso alla directory di destinazione nell'area "Parametri riga di comando". Questa modifica viene applicata solo dopo il riavvio dei server.

Argomenti correlati

- Livelli del registro di analisi

20.3.3 Per configurare l'analisi del server tramite il file BO_trace.ini.

Il file BO_trace.ini viene letto ogni minuto e, per impostazione predefinita, è configurato per disabilitare l'analisi. Per attivare e configurare l'analisi tramite il file `BO_trace.ini`, procedere come segue:

1. Aprire il file `BO_trace.ini`.
   - Il percorso predefinito in Windows è: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
   - Il percorso predefinito in UNIX è: `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`.
2. Rimuovere il commento alle righe richieste nella sezione "Trace Syntax and Setting".
3. Modificare i parametri di analisi del server secondo le esigenze.

Nella tabella seguente sono elencati i parametri generali utilizzati per la configurazione dell'analisi del server.

Parametro	Valori possibili	Descrizione
active	false, true	Se impostato su `true`, verranno analizzati i messaggi che soddisfano la soglia impostata dal parametro `importance`. Se impostato su `false`, i messaggi non verranno analizzati in base al rispettivo livello di "importance". Il valore predefinito è false.
importance	'<<', '<=', '==', '>=', '>>', xs, s, m, l, xl **Nota:** `importance = xs` o `importance = <<` sono le opzioni più dettagliate possibile disponibili, mentre `importance = xl` o `importance = >>` sono le meno dettagliate.	Specifica la soglia per i messaggi di analisi. Viene tenuta traccia di tutti i messaggi oltre la soglia. Il valore predefinito è m (medio).
alert	false, true	Se impostato su `true`, verranno analizzati i messaggi che soddisfano la soglia impostata dal parametro `severity`. Se impostato su `false`, i messaggi non verranno analizzati in base al rispettivo livello di "severity". Il valore predefinito è true.
severity	' ', 'W', 'E', 'A', success, warning, error, assert	Specifica la gravità di soglia oltre la quale viene tenuta traccia dei messaggi. Il valore predefinito è 'E'.
size	I valori possibili sono numeri interi >= 1000.	Specifica il numero di messaggi in un file di registro di analisi prima che ne venga creato uno nuovo. Il valore predefinito è 100000.
keep_num	I valori possibili sono numeri interi >= 1000.	Specifica il numero di registri da mantenere.

Parametro	Valori possibili	Descrizione
administrator	Stringhe o numeri interi	Specifica un'annotazione da utilizzare nel file di registro di output. Ad esempio, se `administrator = "hello"` questa stringa verrà inserita nel file di registro.
log_dir		Specifica la directory del file di registro di output. Per impostazione predefinita, i file di registro sono memorizzati nella cartella `Logging`.
always_close	on, off	Specifica se il file di registro deve essere chiuso dopo la scrittura di una traccia nel file. Il valore predefinito è off.

4. Salvare e chiudere il file `BO_trace.ini`.

Le nuove impostazioni verranno applicate solo dopo il riavvio di tutti i server.

Esempio:

```
active=false;
severity='E';
importance='==';
size=1000000;
keep_num=437;
```

20.3.3.1 Configurazione dell'analisi per server

Il file `BO_trace.ini` viene utilizzato per specificare 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.

1. Aprire il file `BO_trace.ini`.
   - Il percorso predefinito in Windows è: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf/`.
   - Il percorso predefinito in UNIX è: `<INSTALLDIR>/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 per un server specifico, utilizzare un'istruzione IF come indicato nell'esempio che segue:

```
if (process == "aps_MySIA.ProcessingServer")
{
            active = true;
            importance = '<<' ;
            alert = true;
            severity = ' ';
            keep_num = 487;
            size = 100 * 1000;
}
```

4. Salvare e chiudere il file `BO_trace.ini`.

Le impostazioni modificate vengono implementate entro un minuto. Le nuove impostazioni sovrascrivono l'eventuale livello del registro di analisi specificato nella console CMC per un determinato server.

20.4 Configurazione dell'analisi per le applicazioni Web

Le analisi per un'applicazione Web della piattaforma BI monitorata vengono scritte in un file di registro specifico (`.glf`) e archiviate in una cartella nel computer che ospita la cartella delle applicazioni Web. I file di registro di analisi si trovano per impostazione predefinita nella directory seguente: `$userHome/SBOPWebapp_$application_$IPaddress_$port/`

Gli amministratori possono valutare la gravità e l'importanza delle analisi raccolte nel file di registro impostando il livello del registro di analisi per un'applicazione Web specifica o un gruppo di applicazioni. È possibile modificare il livello del registro di analisi utilizzando i seguenti metodi consigliati:

- Utilizzando le impostazioni dell'applicazione "Registro di analisi" nella console CMC
- Riconfigurando manualmente il livello del registro di analisi e tutte le altre impostazioni di analisi nel file `BO_trace.ini`. Questo file viene distribuito insieme ai file WAR `BOE` e `dswsbobje` nel server di applicazioni Web.

Per modificare solo il livello del registro di analisi di un'applicazione Web BOE, si consiglia vivamente di utilizzare l'opzione CMC. Per modificare tutti i parametri di analisi, è necessario riconfigurare il file `BO_trace.ini`.

Nota:
prima di riconfigurare il file `BO_trace.ini`, è necessario utilizzare lo strumento Wdeploy per annullare la distribuzione delle applicazioni Web già esistenti dal server di applicazioni Web. Dopo avere riconfigurato il file `BO_trace.ini`, è necessario ridistribuirlo insieme alle applicazioni Web nel 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*.

20.4.1 Impostazione del livello del registro di analisi delle applicazioni Web nella CMC

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

Per analizzare tutte le altre applicazioni Web, utilizzare il metodo manuale per configurare il file `BO_Trace` corrispondente.

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

   Viene visualizzata la finestra di dialogo "Applicazioni".

2. Fare clic con il pulsante destro del mouse sull'applicazione e scegliere **Impostazioni registro di analisi**.

   Viene visualizzata la finestra di dialogo "Impostazioni registro di analisi".

3. Selezionare l'impostazione desiderata nell'elenco **Livello di registrazione**.
4. Fare clic su **Salva e chiudi** per inviare il livello del registro di analisi.

Il nuovo livello del registro di analisi sarà effettivo al successivo accesso all'applicazione Web.

Argomenti correlati

- Livelli del registro di analisi

20.4.2 Modifica manuale delle impostazioni di analisi mediante il file BO_trace

Il file `BO_trace.ini` viene distribuito insieme ai file WAR `BOE` e `dswsbobje` nel server di applicazioni Web. Questo file non è sempre accessibile nel server di applicazioni Web e devono quindi essere eseguite alcune operazioni preliminari. 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*.

Nota:
se si utilizza il server di applicazioni Web Tomcat fornito con l'installazione della piattaforma BI, è possibile accedere al file `BO_trace.ini` nella directory seguente. Non è necessario annullare la distribuzione delle applicazioni web e modificare direttamente il file.

- Il file di configurazione dell'analisi per il file `BOE.war` è disponibile in: `<INSTALLDIR>\Tomcat6\webapps\BOE\WEB-INF\TraceLog`.
- Il file di configurazione dell'analisi per il file `dswsbobje.war` è disponibile in:`<INSTALLDIR>\Tomcat6\webapps\dswsbobje\WEB-INF\conf`.

Se si utilizza il server di applicazioni Web Tomcat in bundle, passare al punto 3.

2. Accedere a una versione precedente alla distribuzione del file `BO_trace.ini` per i file WAR `BOE` o `dswsbobje`.
   - Una versione precedente alla distribuzione del file di configurazione per il file `BOE.war` è disponibile per impostazione predefinita nella directory seguente: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog`.
   - Una versione precedente alla distribuzione del file di configurazione per il file `dswsbobje.war` è disponibile per impostazione predefinita nella directory seguente: `<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf`.
3. Aprire il file `BO_trace.ini`.
   - Il percorso predefinito in Windows è `<INSTALLDIR>\SAP BusinessObjects Enterprise 12.0\logging\logConfig`.
   - Il percorso predefinito in UNIX è: `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`.
4. Rimuovere il commento alle righe richieste nella sezione "Trace Syntax and Setting".
5. Modificare i parametri di analisi del server secondo le esigenze.

   Nella tabella seguente sono elencati tutti i parametri disponibili per la configurazione dell'analisi del server.

Parametro	Valori possibili	Descrizione
active	false, true	Abilita l'analisi per il processo o il server corrente se impostato su true. Il valore predefinito è false.
importance	'<<', '<=', '==', '>=', '>>', xs, s, m, l, xl **Nota:** `importance = xs` è l'opzione più dettagliata disponibile mentre `importance = xl` è la meno dettagliata.	Specifica la soglia per i messaggi di analisi. Viene tenuta traccia di tutti i messaggi oltre la soglia. Il valore predefinito è m (medio).
alert	false, true	Specifica se abilitare automaticamente l'analisi per gravi eventi di sistema. Il valore predefinito è true.
severity	' ', 'W', 'E', 'A', success, warning, error, assert	Specifica la gravità di soglia oltre la quale viene tenuta traccia dei messaggi. Il valore predefinito è 'E'.
size	I valori possibili sono numeri interi >= 1000.	Specifica il numero di messaggi in un file di registro di analisi prima che ne venga creato uno nuovo. Il valore predefinito è 100000.
keep	false, true	Specifica se il file di registro precedente viene conservato o meno dopo la creazione di un nuovo file. Il valore predefinito è false.

Parametro	Valori possibili	Descrizione
amministratore	Stringhe o numeri interi	Specifica un'annotazione da utilizzare nel file di registro di output. Ad esempio, se `administrator = "hello"` questa stringa verrà inserita nel file di registro.
log_dir		Specifica la directory del file di registro di output. Per impostazione predefinita, i file di registro sono memorizzati nella cartella `Logging`.
always_close	on, off	Specifica se il file di registro deve essere chiuso dopo la scrittura di una traccia nel file. Il valore predefinito è off.

```
active=false;
severity='E';
importance='==';
size=1000000;
keep=false;
```

6. Salvare e chiudere il file `BO_trace.ini`.
7. Utilizzare Wdeploy per distribuire il file WAR sul computer che ospita il server di applicazioni Web.

Le impostazioni di analisi modificate avranno effetto dopo il primo accesso all'applicazione Web.

20.4.2.1 Configurazione dell'analisi per un'applicazione Web specifica

Il file `BO_trace.ini` viene utilizzato per specificare i parametri di analisi per le applicazioni Web della piattaforma BI. Le impostazioni interessano tutte le applicazioni associate al file WAR distribuito. Gli amministratori possono inoltre utilizzare il file `BO_trace.ini` per impostare determinati parametri di analisi per un'applicazione Web specifica.

Nella versione corrente della piattaforma BI, la tabella che segue contiene le applicazioni Web e i file WAR associati alle stesse.

Applicazione Web	File WAR	Posizione predistribuita
Central Management Console	BOE.war	<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
BI Launch Pad	BOE.war	<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
OpenDocument	BOE.war	<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
Servizio Web	dsws bobje.war	<INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf

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*.

   Nota:
   se si utilizza il server di applicazioni Web Tomcat fornito con l'installazione della piattaforma BI, è possibile accedere al file BO_trace.ini nella directory seguente. 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: <INSTALLDIR>\Tomcat6\webapps\BOE\WEB-INF\TraceLog.
   - Il file di configurazione dell'analisi per il file dswsbobje.war è disponibile in:<INSTALLDIR>\Tomcat6\webapps\dswsbobje\WEB-INF\conf.

   Se si utilizza il server di applicazioni Web Tomcat in bundle, passare al punto 3.

2. Accedere a una versione precedente alla distribuzione del file BO_trace.ini per i file WAR BOE o dswsbobje.
   - Una versione precedente alla distribuzione del file di configurazione per il file BOE.war è disponibile per impostazione predefinita nella directory seguente: <INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog.
   - Una versione precedente alla distribuzione del file di configurazione per il file dswsbobje.war è disponibile per impostazione predefinita nella directory seguente: <INSTALLDIR>\ SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf.
3. Aprire il file BO_trace.ini.
4. Rimuovere il commento alle righe richieste nella sezione "Trace Syntax and Setting".
5. Per specificare le impostazioni di analisi per un'applicazione Web specifica, utilizzare un'istruzione IF come indicato nell'esempio che segue:

```
if (device_name == "Webapp_opendocument_trace")
{
active = true;
importance = '<<' ;
alert = true;
severity = ' ';
keep_num = 332;
```

```
size = 100 * 1000;
}
```

Nella tabella seguente sono elencati tutti i parametri disponibili per la configurazione dell'analisi delle applicazioni Web.

Parametro	Valori possibili	Descrizione
active	false, true	Abilita l'analisi per il processo o il server corrente se impostato su true. Il valore predefinito è false.
importance	'<<', '<=', '==', '>=', '>>', xs, s, m, l, xl **Nota:** `importance = xs` è l'opzione più dettagliata disponibile mentre `importance = xl` è la meno dettagliata.	Specifica la soglia per i messaggi di analisi. Viene tenuta traccia di tutti i messaggi oltre la soglia. Il valore predefinito è m (medio).
alert	false, true	Specifica se abilitare automaticamente l'analisi per gravi eventi di sistema. Il valore predefinito è true.
severity	' ', 'W', 'E', 'A', success, warning, error, assert	Specifica la gravità di soglia oltre la quale viene tenuta traccia dei messaggi. Il valore predefinito è 'E'.
size	I valori possibili sono numeri interi >= 1000.	Specifica il numero di messaggi in un file di registro di analisi prima che ne venga creato uno nuovo. Il valore predefinito è 100000.
keep	false, true	Specifica se il file di registro precedente viene conservato o meno dopo la creazione di un nuovo file. Il valore predefinito è false.

Parametro	Valori possibili	Descrizione
amministratore	Stringhe o numeri interi	Specifica un'annotazione da utilizzare nel file di registro di output. Ad esempio, se `administrator = "hello"` questa stringa verrà inserita nel file di registro.
log_dir		Specifica la directory del file di registro di output. Per impostazione predefinita, i file di registro sono memorizzati nella cartella `Logging`.
always_close	on, off	Specifica se il file di registro deve essere chiuso dopo la scrittura di una traccia nel file. Il valore predefinito è off.

6. Salvare e chiudere il file `BO_trace.ini`.
7. Utilizzare Wdeploy per distribuire il file WAR sul computer che ospita il server di applicazioni Web.

20.5 Configurazione dell'analisi per Upgrade Management Tool

L'analisi per Upgrade Management Tool viene eseguita tramite il file di configurazione `BO_trace.ini`.

Il percorso predefinito in Windows è: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`.

Il percorso predefinito in Unix è: `<INSTALLDIR>/sap_bobj/enterprise_xi40/conf/`.

Nota:
A differenza di altri componenti della piattaforma BI, la configurazione dell'analisi per Upgrade Management Tool non può essere eseguita nella console CMC.

20.5.1 Configurazione dell'analisi per Upgrade Management Tool

1. Aprire il file `BO_trace.ini`.

- Il percorso predefinito in Windows è: `<INSTALLDIR>\SAP BusinessObjects Enterprise XI 4.0\conf\`.
- Il percorso predefinito in UNIX è: `<INSTALLDIR>/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 per un server specifico, utilizzare un'istruzione IF come indicato nell'esempio che segue:

```
if (process == "upgrademanagementtool")
{
active = true;
importance = '<<' ;
alert = true;
severity = ' ';
keep = false;
size = 100 * 1000;
}
```

Suggerimento:
il processo deve essere specificato come `upgrademanagementtool` per l'impostazione di analisi da applicare a Upgrade Management Tool.

4. Salvare e chiudere il file `BO_trace.ini`.

Le impostazioni modificate vengono implementate entro un minuto.

Integrazione con SAP Solution Manager

21.1 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

21.2 Elenco di controllo dell'integrazione di SAP Solution Manager

Nella tabella seguente vengono riepilogati i componenti richiesti per abilitare SAP Solution Manager a fornire supporto per la piattaforma BI.

Supporto SAP Solution Manager	Necessario per la piattaforma BI
Registrazione SLD	• È necessario installare SAPHOSTAGENT per abilitare la registrazione dei server della piattaforma BI. **Nota:** il programma di installazione della piattaforma BI registrerà automaticamente i server, se SAPHOSTAGENT è già installato. • È necessario creare un file connect.key per il fornitore di dati che crea report sui server di back-end. • (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. • (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.
Integrazione SMD	• È necessario scaricare e installare l'agente SMD (DIAGNOSTICS.AGENT) su tutti gli host dei server della piattaforma BI. • È necessario abilitare l'account utente SMAdmin nella piattaforma BI.
Strumentazione delle prestazioni	• 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. • È necessario installare l'agente SMD. • 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.
SAP Passport	• È necessario scaricare e installare lo strumento client SAP Passport.

21.3 Gestione della registrazione di System Landscape Directory

21.3.1 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 SLS. 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.

21.3.1.1 Creazione di un file connect.key per il fornitore di dati SLD

Piattaforma BI

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.

21.3.2 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.

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.

21.3.3 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: `<DIRINSTALLAZ>/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: `<DIRINSTALLAZ>/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: `<DIRINSTALLAZ>/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: `sldrg_<Indicazione data e ora>.log`.

Viene creato un nuovo file di registro ogni volta che il fornitore di dati chiama sldreg.

21.4 Gestione degli agenti di Solution Manager Diagnostics

21.4.1 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.

21.4.2 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 SMAdmin per abilitare l'accesso del server SMD al server CMS.

21.4.3 Account utente SMAdmin

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 SMAdmin è disattivato per impostazione predefinita.

21.4.3.1 Attivazione dell'account SMAdmin

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 "SMAdmin".
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**.

21.5 Gestione della strumentazione delle prestazioni

21.5.1 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.

21.5.2 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

21.5.2.1 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**.

   Viene 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 `true` 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.

Segnaposto	Descrizione
%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 (`DIAGNOSTICS.AGENT`).
%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 sopecificati verranno propagati in tutti i server gestiti.

21.5.3 Strumentazione delle prestazioni per il livello Web

I dati di strumentazione per i componenti del livello Web non sono inclusi nella piattaforma BI.

21.5.4 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: `<DIRINSTALLAZ>/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 `AutoProbe.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: `<DIRINSTALLAZ>/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: `<DIRINSTALLAZ>/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`.

21.6 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, `SAPIEPlugin.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

22.1 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 SAP BusinessObjects Business Intelligence 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 SAP BusinessObjects Business Intelligence. Ogni script viene descritto di seguito e vengono fornite, laddove possibile, le opzioni della riga di comando.

22.1.1 Utilità per gli script

In questa sezione vengono descritti gli script amministrativi che assistono l'utente nell'utilizzo della piattaforma SAP BusinessObjects Business Intelligence 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.

22.1.1.1 ccm.sh

Lo script `ccm.sh` è installato nella directory *<SCRIPTDIR>* dell'installazione. Questo script fornisce una versione della riga di comando di CCM. 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 SAP BusinessObjects Business Intelligence.
- 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.
`-start`	`all` o *`sianame`*	Avviare ogni Server Intelligence Agent come processo. L'opzione `all` avvia tutti i nodi presenti nel computer, inclusi quelli appartenenti a cluster diversi.
`-stop`	`all` o *`sianame`*	Arrestare ogni Server Intelligence Agent terminando il relativo ID di processo. L'opzione `all` avvia tutti i nodi presenti nel computer, inclusi quelli appartenenti a cluster diversi.
`-restart`	`all` o *`sianame`*	Arrestare ogni Server Intelligence Agent terminando il relativo ID processo, dopodiché viene avviato ogni SIA. L'opzione `all` avvia tutti i nodi presenti nel computer, inclusi quelli appartenenti a cluster diversi.
`-managedstart`	*`<nome server completo>[altre informazioni di autenticazione]`*	Avvia un server.
`-managedstop`	*`<nome server completo>[altre informazioni di autenticazione]`*	Arresta un server.

Opzione CCM	Argomenti validi	Descrizione
-managedrestart	*<nome server completo>[altre informazioni di autenticazione]*	Arresta un server, quindi avvia il server.
-managedforceterminate	*<nome server completo>[altre informazioni di autenticazione]*	Arresta il server immediatamente senza completare le richieste di elaborazione correnti.
-enable	*<nome server completo>[altre informazioni di autenticazione]*	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	*<nome server completo>[altre informazioni di autenticazione]*	Disabilitare un server in modo che non risponda più alle richieste della piattaforma BusinessObjects Business Intelligence ma rimanga avviato come processo. Utilizzare la forma completa del nome server.
-display	*[altre informazioni di autenticazione]*	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`	*`cmsname:port#`*	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`	*`username`*	Specificare un account che fornisca diritti amministrativi per la piattaforma BusinessObjects Business Intelligence. Se non specificato, si tenta con l'account Administrator predefinito.
`-password`	*`password`*	Consente di specificare la password corrispondente. Se non specificata, si tenta con una password vuota. **Nota:** 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

22.1.1.1.1 Esempi

Questi due comandi consentono di avviare e attivare tutti i server della piattaforma SAP BusinessObjects Business Intelligence. 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 attivare tutti i server della piattaforma SAP BusinessObjects Business Intelligence. Il CMS viene avviato sulla porta 6701 anziché sulla porta predefinita:

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701
```

Questi due comandi avviano e abilitano tutti i server della piattaforma SAP BusinessObjects Business Intelligence per i quali è stato specificato l'account amministrativo `SysAdmin`:

```
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
```

22.1.1.1.2 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 da altre utilità per gli script della piattaforma SAP BusinessObjects Business Intelligence. Questo file viene in genere modificato solo quando è necessario modificare la riga di comando di Server Intelligence Agent.

Argomenti correlati

- Panoramica sulle righe di comando

22.1.1.2 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 di comando del SIA. Il nome corrente del SIA viene visualizzato dopo l'opzione `-name`.

Argomenti correlati

- Cluster di Central Management Server
- Backup e ripristino del sistema

22.1.1.3 configpatch.sh

Lo script `configpatch.sh` è installato nella directory `sap_bobj/enterprise/generic` dell'installazione. Utilizzare lo script `configpatch.sh` durante l'installazione di patch che richiedono aggiornamenti ai valori di configurazione del sistema. Dopo l'installazione della patch, eseguire `configpatch.sh` con il nome utente `.cf` appropriato come argomento. Il file `readme.txt` che accompagna le patch della piattaforma BusinessObjects Business Intelligence indica quando eseguire `configpatch.sh` e il nome del file `.cf` da utilizzare.

22.1.1.4 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
- Elencare i nodi

22.1.1.4.1 Aggiunta/eliminazione/modifica/elenco di nodi in UNIX

1. Passare alla directory *`<SCRIPTDIR>`* dell'installazione.
2. Eseguire il seguente comando:

   ```
   ./serverconfig.sh
   ```

   Lo script richiede all'utente un elenco di opzioni:

   - 1 - Aggiungere un Server Intelligence Agent
   - 2 - Eliminare un Server Intelligence Agent
   - 3 - Modificare un Server Intelligence Agent
   - 4 - Elencare tutti i Server Intelligence Agent nel file config

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.

   Suggerimento:
   lo script richiederà all'utente il nome del CMS. Per impostazione predefinita, il nome del server CMS è hostname.cms. In altre parole, il nome predefinito di un CMS installato su un computer denominato MACHINE01 è MACHINE01.cms. Tuttavia, in questo script è possibile immettere il nome host per controllare il nome del CMS (o di qualsiasi altro server), visualizzare il contenuto di ccm.config e cercare la stringa di avvio del server. Il nome corrente del server viene visualizzato dopo l'opzione -name.

22.1.2 Modelli di script

Questi script vengono forniti principalmente come modelli sui quali è possibile basare i propri script di automazione.

22.1.2.1 startservers

Lo script `startservers` è installato nella directory *<SCRIPTDIR>* 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 SAP BusinessObjects Business Intelligence eseguendo una serie di comandi CCM. Per informazioni dettagliate sulla scrittura di comandi CCM per i server, consultare ccm.sh.

22.1.2.2 stopservers

Lo script `stopservers` è installato nella directory *<SCRIPTDIR>* 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 SAP BusinessObjects Business Intelligence eseguendo una serie di comandi CCM. Per informazioni dettagliate sulla scrittura di comandi CCM per i server, consultare ccm.sh.

22.1.3 Script utilizzati dalla piattaforma SAP BusinessObjects Business Intelligence

Questi script secondari spesso vengono eseguiti in background quando si eseguono le principali utilità per gli script della piattaforma SAP BusinessObjects Business Intelligence. È necessario non eseguire tali script manualmente.

22.1.3.1 bobjrestart.sh

Questo script viene eseguito internamente da CCM quando quest'ultimo avvia i componenti dei server della piattaforma SAP BusinessObjects Business Intelligence. Se un processo server termina bruscamente senza restituire il normale codice di uscita, questo script riavvierà automaticamente un nuovo processo server in sostituzione. Non eseguire questo script manualmente.

22.1.3.2 env.sh

Lo script `env.sh` viene installato nella directory *`sap_bobj/setup`* dell'installazione. Questo script imposta le variabili di ambiente della piattaforma SAP BusinessObjects Business Intelligence richieste da alcuni degli altri script. Gli script della piattaforma SAP BusinessObjects Business Intelligence eseguono env.sh come richiesto. Quando si installa la piattaforma SAP BusinessObjects Business Intelligence su UNIX, è necessario configurare il server di applicazioni Java in modo che generi questo script all'avvio. Per ulteriori informazioni, consultare il *Manuale di installazione della piattaforma SAP BusinessObjects Business Intelligence*.

22.1.3.3 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.

22.1.3.4 initlaunch.sh

Lo script `initlaunch.sh` esegue `env.sh` per impostare le variabili di ambiente della piattaforma SAP BusinessObjects Business Intelligence, 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 Business Objects.

22.1.3.5 setup.sh

Lo script `setup.sh` è installato nella directory principale dell'installazione. Questo script fornisce un programma basato su testo che consente di impostare l'installazione della piattaforma SAP BusinessObjects Business Intelligence. Questo script viene eseguito automaticamente quando si installa la piattaforma SAP BusinessObjects Business Intelligence. Richiede all'utente le informazioni necessarie per impostare la piattaforma SAP BusinessObjects Business Intelligence per la prima volta.

Per informazioni complete sulla risposta allo script di impostazione quando si installa la piattaforma SAP BusinessObjects Business Intelligence, consultare il *Manuale di installazione della piattaforma SAP BusinessObjects Business Intelligence*.

22.1.3.6 setupinit.sh

Lo script `setupinit.sh` viene installato nella directory *`/sap_bobj/init`* dell'installazione quando si esegue un'installazione di sistema. Questo script copia gli script di controllo dell'esecuzione nelle directory `rc#` per un avvio automatico. Quando esegue un'installazione di sistema, l'utente viene istruito per eseguire questo script dopo il completamento dello script `setup.sh`.

Nota:
per eseguire questo script, è necessario disporre di privilegi principali.

22.2 Script Windows

In questa sezione sono descritti in dettaglio tutti gli strumenti e gli script amministrativi inclusi nella distribuzione Windows 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 Windows della piattaforma SAP BusinessObjects Business Intelligence 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.

22.2.1 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 il file eseguibile di CCM 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`	`all` oppure *`<nome server completo>[altre informazioni di autenticazione]`*	Avvia un server.
`-managedstop`	`all` oppure *`<nome server completo>[altre informazioni di autenticazione]`*	Arresta un server.

Opzione CCM	Argomenti validi	Descrizione
-managedrestart	all oppure *<nome server completo>[altre informazioni di autenticazione]*	Arresta un server, quindi avvia il server.
-managedforceterminate	all oppure*<nome server completo>[altre informazioni di autenticazione]*	Arresta il server immediatamente senza completare le richieste di elaborazione correnti.
-enable	all oppure *<nome server completo>[altre informazioni di autenticazione]*	Consente di abilitare un server avviato in modo che si registri con il sistema e inizi ad attendere in corrispondenza della porta appropriata.
-disable	all oppure *<nome server completo>[altre informazioni di autenticazione]*	Consente di disabilitare un server in modo che non risponda più alle richieste della piattaforma BusinessObject Business Intelligence ma rimanga avviato come processo.
-display	*[altre informazioni di autenticazione]*	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`	*`cmsname:port#`*	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`	*`username`*	Consente di specificare un account che fornisce diritti amministrativi per la piattaforma SAP BusinessObjects Business Intelligence. Se non specificato, si tenta con l'account Administrator predefinito.
`-password`	*`password`*	Consente di specificare la password corrispondente. Se non specificata, si tenta con una password vuota. **Nota:** Per specificare l'argomento `-password`, è necessario specificare anche l'argomento `-username`.
`-authentication`	*`tipo autenticazione`*	Specificare il tipo di autenticazione. È supportato solamente secEnterprise.

CCM legge le stringhe di avvio e altri valori di configurazione dal file `ccm.config`.

Argomenti correlati

- ccm.config

22.2.1.1 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 (MACHINE01)"
```

È possibile anche arrestare il servizio SIA mediante `net stop "Server Intelligence Agent (MACHINE01)"`.

Questo comando lancia tutti i server della piattaforma SAP BusinessObjects Business Intelligence:

```
ccm.exe -managedstart all
```

Questo comando avvia un Adaptive Job Server. Il CMS viene 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
```

22.3 Righe di comando server

22.3.1 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 SAP BusinessObjects Business Intelligence.

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. Inoltre, è possibile manipolare la maggior parte delle impostazioni comuni tramite diverse schermate di configurazione server di CCM. 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 SAP BusinessObjects Business Intelligence.

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 SAP BusinessObjects Business Intelligence utilizzano una serie di opzioni interne non elencate in queste tabelle. Tali opzioni non devono essere modificate.

22.3.1.1 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.

22.3.2 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
`-requestPort`	*port*	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. **Nota:** 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 *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence.*

Opzione	Argomenti validi	Comportamento
`-loggingPath`	*percorso assoluto*	Specificare il percorso in cui vengono creati i file di registro.

22.3.2.1 Gestione dei segnali UNIX

In UNIX, i daemon della piattaforma SAP BusinessObjects Business Intelligence gestiscono i seguenti segnali:

- `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).

22.3.3 Central Management Server

Questa sezione riporta le opzioni della riga di comando specifiche del CMS. Il percorso predefinito del server in Windows è *<INSTALLDIR>*`\BusinessObjects Enterprise XI 4.0\win64_x64\CMS.exe`.

Il percorso predefinito del server in UNIX è *<DIRINSTALLAZ>*`/bobje/enterprise40/`*<piattaforma>*`/boe_cmsd`.

Opzione	Argomenti validi	Comportamento
`-threads`	*number*	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.

Opzione	Argomenti validi	Comportamento
`-reinitializedb`		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.
`-quit`		Imporre la chiusura del CMS dopo l'elaborazione dell'opzione `-reinitializedb` .
`-receiverPool`	*number*	Specificare il numero di thread che il CMS crea per ricevere le richieste client. Un client può essere un altro server Business Objects, 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.
`-maxobjectsincache`	*number*	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.

Opzione	Argomenti validi	Comportamento
`-ndbqthreads`	*number*	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.
`-oobthreads`	*number*	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.
`-AuditeeTimeSyncInterval`	*minutes*	Specificare l'intervallo tra gli eventi di sincronizzazione temporale. Il CMS trasmette l'ora di sistema ai server controllati all'intervallo specificato da `-AuditeeTimeSyncInterval`. I server controllati confrontano i rispettivi orologi interni con l'ora del CMS e regolano quindi le datazioni assegnate a tutti i successivi record di controllo, in modo che l'ora di tali record sia sincronizzata con quella del CMS. L'intervallo predefinito è di 5 minuti. Il valore massimo è pari a un giorno o 1440 minuti. Il valore minimo è 15 minuti. Se si imposta un intervallo pari a 0 si disattiva la sincronizzazione dell'ora.

Argomenti correlati

- Opzioni standard per tutti i server

22.3.4 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:

- `<DIRINSTALLAZ>\Piattaforma SAP BusinessObjects Business Intelligence 4.0\win64_x64\cacheserver.exe`.
- `<DIRINSTALLAZ>\Piattaforma BusinessObjects Business Intelligence XI 4.0\win64_x64\pageserver.exe`.

I percorsi predefiniti dei server in UNIX sono:

- `<DIRINSTALLAZ>/sap_bobj/enterprise_xi40/<PIATTAFORMA>/boe_cachesd`.
- `<DIRINSTALLAZ>/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`	*absolutepath*	Specificare la directory predefinita per le estensioni di elaborazione. Per ulteriori informazioni consultare il *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

Argomenti correlati

- Opzioni standard per tutti i server

22.3.5 Server di elaborazione di Dashboard Design e Cache Server di Dashboard Design

Il server di elaborazione di Dashboard Design e il Cache Server di Dashboard Design 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:

- `<DIRINSTALLAZ>\SAP BusinessObjects\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\xccache.exe`.
- `<DIRINSTALLAZ>\SAP BusinessObjects\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\xcproc.exe`.

I percorsi predefiniti dei server in UNIX sono:

- `<DIRINSTALLAZ>/sap_bobj/enterprise_xi40/<piattaforma>_64/boe_xccached`.
- `<DIRINSTALLAZ>/sap_bobj/enterprise_xi40/<piattaforma>_64/xcprocd`.

Opzione	Argomenti validi	Comportamento
`-cache`		Abilitare la funzionalità Cache Server.
`-dir`	*absolutepath*	Specificare la directory di cache per Cache Server e la directory temporanea per il server di elaborazione. Le directory create sono `absolutepath/cache` e `absolutepath/temp`
`-deleteCache`		Eliminare la directory cache ogni volta che il server viene avviato e interrotto.
`-psdir`	*absolutepath*	Specificare la directory temporanea per il server di elaborazione. Questa opzione sostituisce `-dir`.

Opzione	Argomenti validi	Comportamento
-refresh	*minutes*	Condividere le pagine memorizzate nella cache per il numero specificato di minuti.
-auditMaxEventsPerFile	*number*	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

22.3.6 Job Server

Questa sezione riporta le opzioni della riga di comando specifiche per i Job Server adattivi.

Il percorso predefinito del server su Windows è *<DIRINSTALLAZ>*\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\JobServer.exe.

Il percorso predefinito del server in UNIX è *<DIRINSTALLAZ>*/sap_bobj/enterprise_xi40/*<PIATTAFORMA>*/boe_reportjobsd.

Opzione	Argomenti validi	Comportamento
-dir	*absolutepath*	Specificare la directory dei dati del Job Server.
-maxJobs	*number*	Impostare il numero massimo di processo simultanei che il server gestirà. Il valore predefinito è 5.

Opzione	Argomenti validi	Comportamento
`-requestJSChildPorts`	*lowerbound-upperbound*	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. **Nota:** Affinché questa opzione diventi operativa, è inoltre necessario specificare l'impostazione `-requestPort`.
`-report_ProcessExtPath`	*absolutepath*	Specificare la directory predefinita per le estensioni di elaborazione. Per ulteriori informazioni consultare il *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

Argomenti correlati

- Opzioni standard per tutti i server

22.3.7 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.

22.3.8 Report Application Server

Questa sezione riporta le opzioni della riga di comando specifiche Report Application Server.

Il percorso predefinito del server su Windows è `<DIRINSTALLAZ>\Piattaforma SAP BusinessObjects Business Intelligence 4.0\win32_x86\crystalras.exe`.

Il percorso predefinito del server in UNIX è `<DIRINSTALLAZ>/sap_bobj/enterprise_xi40/<PIATTAFORMA>/ras/boe_crystalrasd`.

Opzione	Argomenti validi	Comportamento
`-ipport`	*port*	Specificare il numero di porta per la ricezione delle richieste TCP/IP durante l'esecuzione in modalità autonoma (all'esterno della piattaforma SAP BusinessObjects Business Intelligence).
`-report_ProcessExtPath`	*absolutepath*	Specificare la directory predefinita per le estensioni di elaborazione. Per ulteriori informazioni consultare il *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.

Opzione	Argomenti validi	Comportamento
`-ProcessAffinityMask`	*mask*	Utilizzare una maschera per specificare esattamente quali CPU utilizzerà il RAS quando viene eseguito in un computer multiprocessore. La maschera presenta il formato `0xffffffff`, dove ogni `f` rappresenta un processore e l'elenco dei processori viene letto da destra a sinistra (in altre parole, l'ultima `f` rappresenta il primo processore). Per ogni `f`, sostituire 0 (utilizzo della CPU non consentito) o `1` (l'utilizzo della CPU consentito). Ad esempio, se si esegue il RAS su un computer a 4 processori e si desidera utilizzare il terzo e il quarto processore, adoperare la maschera `0x1100`. Per utilizzare il secondo e il terzo processore, utilizzare `0x0110`. **Nota:** • RAS utilizza il primi processori consentiti nella stringa, fino al numero massimo specificato dalla licenza. Se si dispone di una licenza per due processori, `0x1110` ha lo stesso effetto di `0x0110`. • Il valore predefinito della maschera è `-1`, che ha lo stesso significato di `0x1111`.

Argomenti correlati

- Opzioni standard per tutti i server

22.3.9 Web Intelligence Processing Server

In questa sezione sono elencate le opzioni della riga di comando specifiche di Web Intelligence Processing Server.

Il percorso predefinito del server su Windows è `<DIRINSTALLAZ>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\WIReportServer.exe`.

Il percorso predefinito del server in UNIX è `<DIRINSTALLAZ>/sap_bobj/enterprise_xi40/<PIATTAFORMA>/WIReportServer`.

Opzione	Argomenti validi	Comportamento
-ConnectionTimeout Minutes	*minutes*	Specifica il numero di minuti prima del timeout del server.
-MaxConnections	*number*	Specifica il numero massimo di connessioni simultanee che il server consente in una volta.
-DocExpressEnable		Abilita la memorizzazione dei documenti Web Intelligence durante la visualizzazione dei documenti stessi.
-DocExpressRealTime CachingEnable		Abilita la cache in tempo reale dei documenti Web Intelligence.
-DocExpressCache DurationMinutes	*minutes*	Specifica il tempo (in minuti) per il quale il contenuto è memorizzato nella cache.
-DocExpressMaxCache SizeKB	*kilobytes*	Specifica la dimensione della cache dei documenti.
-EnableListOfValues Cache		Abilita la cache per sessioni utente degli elenchi di valori

Opzione	Argomenti validi	Comportamento
-ListOfValuesBatchSize	*number*	Il numero massimo di valori che possono essere restituiti per ogni batch di elenco dei valori.
-UniverseMaxCacheSize	*number*	Specifica il numero di universi da memorizzare.
-WIDMaxCacheSize	*number*	Specifica il numero di documenti Web Intelligence che possono essere memorizzati nella cache.

Argomenti correlati

- Opzioni standard per tutti i server

22.3.10 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 su Windows è `<DIRINSTALLAZ>\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\fileserver.exe`

I percorsi predefiniti del programma che fornisce entrambi i server in UNIX sono:

- `<DIRINSTALLAZ>/sap_bobj/enterprise_xi40/<piattaforma>/boe_inputfilesd`.
- `<DIRINSTALLAZ>/sap_bobj/enterprise_xi40/<piattaforma>/boe_outputfilesd`.

Opzione	Argomenti validi	Comportamento
`-rootDir`	*absolutepath*	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. **Nota:** 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.
`-tempDir`	*absolutepath*	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. **Nota:** 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.

Opzione	Argomenti validi	Comportamento
-maxidle	*minutes*	Specificare il numero di minuti trascorsi i quali una sessione inattiva viene eliminata.

Argomenti correlati

- Opzioni standard per tutti i server

22.3.11 Event Server

Questa sezione riporta le opzioni della riga di comando specifiche dell'Event Server.

Il percorso predefinito del server su Windows è *<DIRINSTALLAZ>*\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\EventServer.exe

Il percorso predefinito del server in UNIX è *<DIRINSTALLAZ>*/sap_bobj/enterprise_xi40/*<piattaforma>*/boe_eventsd

Opzione	Argomenti validi	Comportamento
-poll	*seconds*	Specificare la frequenza (in secondi) con cui il server controlla gli eventi file.
-cleanup	*minutes*	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 eliminati ogni 5 minuti.

Argomenti correlati

- Opzioni standard per tutti i server

22.3.12 Dashboard Server e Dashboard Analytics Server

Dashboard Server e Dashboard Analytics Server non presentano parametri specifici della riga di comando per l'amministrazione della riga di comando.

Appendice sui diritti

23.1 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*.

23.2 Diritti generali

I diritti descritti in questa sezione sono applicabili a più tipi di oggetto.

Nota:

- 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 Preferiti o i pacchetti 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 *Manuale dell'amministratore della piattaforma SAP BusinessObjects Business Intelligence*.
"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. **Nota:** 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"	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. Per pianificare un oggetto per altri utenti o gruppi, è anche necessario disporre dei diritti seguenti: • Questo diritto sull'utente o il gruppo. • Diritto "Pianificare il documento da eseguire" sull'oggetto.
"Pianificare in destinazioni"	Consente di eseguire le operazioni seguenti: • Pianificare gli oggetti in destinazioni diversa dal percorso Enterprise predefinito. • Modificare le destinazioni predefinite specificate per la pianificazione. Per pianificare l'oggetto in destinazioni, è anche necessario disporre dei diritti seguenti: • Diritto "Pianificare il documento da eseguire" sull'oggetto da pianificare. • Diritto "Aggiungere oggetti alla cartella" nella Posta in arrivo del destinatario, per pianificare in una destinazione Posta in arrivo. • Diritto "Copia oggetti in un'altra cartella" sull'oggetto da pianificare, per inviare una copia in una destinazione Posta in arrivo anziché un collegamento.
"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

23.3 Diritti per tipi di oggetti specifici

23.3.1 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

23.3.2 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"	Consente di eseguire le seguenti operazioni: • Modificare le proprietà delle categorie. • Spostare la categoria in un'altra categoria come categoria secondaria. • Aggiungere oggetti alla categoria. • Rimuovere oggetti dalla categoria. Per spostare una categoria in un'altra categoria come categoria secondaria, sono necessari i seguenti diritti: • Il diritto "Eliminare oggetti" nella categoria originale. • Il diritto "Aggiungere oggetti alla cartella" nella categoria di destinazione.
"Eliminare oggetti"	Consente di eliminare la categoria.

23.3.3 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	Questo diritto consente di eseguire le seguenti operazioni: • Avviare e rispondere ai thread di discussione. • Visualizzare le note in un thread di discussione. • Modificare o eliminare le note pubblicate.

23.3.4 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"	Consente di esportare dati del report in qualsiasi formato quando si visualizza il report in linea nel visualizzatore Crystal Reports. Per esportare dati del report nel formato RPT, è necessario disporre anche del diritto "Scarica file associati all'oggetto".
"Scarica file associati all'oggetto"	Questo diritto consente di eseguire le seguenti operazioni: • Esportare il report nel formato RPT. • Aprire il report in Crystal Reports Designer. • Pianificare il report nel formato RPT in destinazioni esterne.

23.3.5 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 Desktop di inviare documenti come allegati di messaggi di posta elettronica.

23.3.6 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"	Consente di eseguire le seguenti operazioni: • Modificare le proprietà per l'utente o il gruppo. • Gestire l'appartenenza al gruppo. 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.

"Modifica password utente"	Consente di eseguire le seguenti operazioni:
	• Modificare la password per l'account utente. A tale scopo, è necessario disporre del diritto "Modificare oggetti" per l'account utente.
	• 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.
	Nota:
	• Questo diritto non influisce sulle seguenti impostazioni della password utente:
	  • "Nessuna scadenza password"
	  • "Modifica obbligatoria password all'accesso successivo"
	  • "Modifica password non consentita"
	• Questo diritto non è applicabile alle credenziali delle origini dati per gli universi di Business Objects.

"Sottoscrivi a pubblicazioni"	Consente di aggiungere l'utente alle pubblicazioni come destinatario.
"Pianifica per conto degli utenti"	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.

23.3.7 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"	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.

Argomenti correlati

- Scelta tra le opzioni Modificare i diritti che gli utenti hanno sugli oggetti

23.3.8 Spazi di lavoro BI

I diritti in questa sezione sono diritti generali che controllano azioni utente specifiche nel contesto degli spazi di lavoro BI.

Diritto	Descrizione
"Aggiungere oggetti alla cartella"	Consente di aggiungere menu allo spazio di lavoro BI. Questo diritto, tuttavia, non consente di aggiungere moduli o altri oggetti allo spazio di lavoro BI. Per aggiungere un menu allo spazio di lavoro BI, è inoltre necessario il diritto "Modifica spazi di lavoro BI".
"Modificare oggetti"	Questo diritto consente di eseguire le seguenti operazioni: • Modificare il contenuto e le proprietà degli spazi di lavoro BI. • Modificare i menu degli spazi di lavoro BI. • Eliminare uno spazio di lavoro BI.

Diritti di moduli e spazi di lavoro BI

I moduli sono modelli in cui vengono inseriti i dati che si desidera visualizzare nello spazio di lavoro BI. Uno spazio di lavoro BI è costituito da uno o più moduli.

Il modo in cui i moduli vengono aggiunti al repository influisce sulle relative impostazioni di protezione. Se si aggiungono moduli al repository come oggetti autonomi, è possibile impostare diritti generali sui moduli stessi; tali diritti vengono applicati quando i moduli vengono utilizzati negli spazi di lavoro.

23.3.9 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: • Modificare l'universo nella console CMC o in Universe Design Tool. • Bloccare o sbloccare l'universo. 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. **Nota:** 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: • Associare nuovi elenchi di valori. agli oggetti. • Modificare gli elenchi di valori esistenti. **Nota:** Questo diritto non impedisce la creazione di elenchi sovrapposti di valori.

Diritto	Descrizione
"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.
"Sblocca universo"	Consente di: • Sbloccare l'universo se è bloccato da un altro utente. • Esportare l'universo dal server CMS. Per sbloccare un universo, è anche necessario il diritto "Modificare oggetti".
"Accesso ai dati"	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.
"Crea e modifica query in base all'universo"	Consente di creare documenti e modificare query basate sull'universo.

23.3.10 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"	Consente di accedere all'universo e di visualizzarlo.
"Modificare oggetti"	Consente di ripubblicare l'universo.
"Eliminare oggetti"	Consente di eliminare l'universo.
"Recuperare universi"	Consente di recuperare un universo pubblicato e di modificare le risorse sottostanti (livello aziendale e base dati) in Information Design Tool. **Nota:** il diritto Recuperare universi è necessario anche per l'applicazione "Information Design Tool".
"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. **Nota:** 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.

Diritto	Descrizione
"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. **Nota:** il diritto Salva per tutti gli utenti è anche necessario per l'applicazione "Information Design Tool".

23.3.11 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 minino 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

23.3.11.1 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**.

23.3.12 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.
"Eliminare oggetti"	Consente di eliminare la connessione.
"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. **Nota:** 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.

23.3.13 Applicazioni

23.3.13.1 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.

23.3.13.2 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: • Spostare e copiare oggetti. • Aggiungere oggetti alla cartella Preferiti. • Creare collegamenti agli oggetti.
"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.

23.3.13.3 Spazi di lavoro BI

I diritti elencati in questa sezione sono applicabili unicamente agli spazi di lavoro BI.

Diritto	Descrizione
" Creare spazi di lavoro BI"	Consente all'utente di creare nuovi spazi di lavoro BI e di modificare quelli esistenti.
"Modificare oggetti"	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.

23.3.13.4 Web Intelligence

I diritti in questa sezione sono applicabili unicamente a SAP BusinessObjects Web Intelligence (inclusa l'interfaccia desktop) 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 desktop: abilita Web Intelligence Desktop"	Consente l'utilizzo dell'interfaccia desktop.
"Interfaccia desktop: abilita fornitori di dati locali"	Consente l'utilizzo di fornitori di dati personali nell'interfaccia desktop.
"Interfaccia desktop: esportazione di un documento"	Consente l'esportazione dei documenti nel CMS nell'interfaccia desktop.
"Interfaccia desktop: importazione di un documento"	Consente l'importazione dei documenti dal CMS nell'interfaccia desktop.
"Interfaccia desktop: installazione da BI Launch Pad"	Consente il download dell'interfaccia desktop da BI Launch Pad.
"Interfaccia desktop: stampa di un documento"	Consente la stampa dei documenti dall'interfaccia desktop.
"Interfaccia desktop: rimozione della protezione del documento"	Consente la rimozione della protezione dei documenti dall'interfaccia desktop.
"Interfaccia desktop: salvataggio di un documento per tutti gli utenti"	Consente il salvataggio dei documenti per tutti gli utenti dall'interfaccia desktop.
"Interfaccia desktop: salva documento in locale"	Consente il salvataggio dei documenti sul disco locale nell'interfaccia desktop.
"Interfaccia desktop: invio tramite posta elettronica"	Consente l'invio dei documenti tramite posta elettronica nell'interfaccia desktop.
"Interfaccia desktop: abilita fornitori di dati locali"	Consente l'utilizzo di fornitori di dati personali nell'interfaccia desktop.
"Documenti: disabilita l'aggiornamento automatico all'apertura"	Interrompe l'aggiornamento automatico dei documenti all'apertura.

Diritto	Descrizione
"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.
"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.

Diritto	Descrizione
"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.
"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).

23.3.13.5 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.
"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.

23.3.13.6 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.

23.3.13.7 Diritti di Information Design Tool

I diritti in questa sezione sono validi per l'applicazione Information Design Tool.

Diritto	Descrizione
"Amministra profili di protezione"	Consente di aprire l'editor di protezione. **Nota:** Per utilizzare i profili di protezione, è necessario che siano stati concessi diritti per l'universo.
"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"	Consente di eseguire le seguenti operazioni: • creare ed eliminare le connessioni protette dalla vista Risorse pubblicate • modificare le connessioni nell'editor delle connessioni • pubblicare le connessioni in un repository
"Pubblica universo"	Consente di pubblicare universi in un repository.

Diritto	Descrizione
"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.

23.3.13.8 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.

23.3.13.9 Avvisi

I diritti in questa sezione sono applicabili unicamente all'applicazione Avvisi.

Diritto	Descrizione
""Attiva avvisi""	Consente di attivare gli eventi di avviso. Per attivare un avviso per un documento, è necessario disporre dei seguenti diritti: • Diritti di visualizzazione e di pianificazione sul documento • Diritti visualizzazione e attivazione sull'evento corrispondente
""Sottoscrivi oggetti""	Consente di sottoscrivere un evento di avviso. Per sottoscrivere un evento, è necessario disporre dei seguenti diritti: • Diritto di visualizzazione sull'evento corrispondente • Diritto di sottoscrizione sull'account utente Per sottoscrivere un avviso per un documento, è necessario disporre dei seguenti diritti: • Diritto di visualizzazione sul documento • Diritto di visualizzazione istanza sul documento • Diritto di visualizzazione sull'evento corrispondente • Diritto di sottoscrizione sull'account utente

23.3.13.10 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"	Consente di esplorare uno spazio informazioni. Per eseguire questa attività, è necessario disporre anche del diritto "Accedere a Explorer e visualizzare questo oggetto nella CMC".
"Esplora spazi informazioni: Esporta in segnalibro/posta elettronica"	Consente di utilizzare segnalibri e segnalibri di posta elettronica. Per eseguire questa attività, è necessario disporre anche dei seguenti diritti: • "Accedere a Explorer e visualizzare questo oggetto nella CMC" • "Esplora spazi informazioni"
"Esplora spazi informazioni: Esporta in CSV"	Consente di esportare i risultati di un'esplorazione in un file CSV o Excel. Per eseguire questa attività, è necessario disporre anche dei seguenti diritti: • "Accedere a Explorer e visualizzare questo oggetto nella CMC" • "Esplora spazi informazioni"
"Esplora spazi informazioni: Esporta in immagine"	Consente di esportare i risultati di un'esplorazione come immagine. Per eseguire questa attività, è necessario disporre anche dei seguenti diritti: • "Accedere a Explorer e visualizzare questo oggetto nella CMC" • "Esplora spazi informazioni"
"Esplora spazi informazioni: Esporta in Web Intelligence"	Consente di esportare i risultati di un'esplorazione come query. Per eseguire questa attività, è necessario disporre anche dei seguenti diritti: • "Accedere a Explorer e visualizzare questo oggetto nella CMC" • "Esplora spazi informazioni"

Diritto	Descrizione
"Gestione spazi informazioni"	Consente di accedere al menu Gestione spazi e ad eseguire le attività associate. Per eseguire questa attività, è necessario disporre anche del diritto "Accedere a Explorer e visualizzare questo oggetto nella CMC".
"Gestione spazi informazioni: Crea nuovo spazio"	Consente di creare un nuovo spazio informazioni Per eseguire questa attività, è necessario disporre anche dei seguenti diritti: • "Accedere a Explorer e visualizzare questo oggetto nella CMC" • "Gestione spazi informazioni"

Diritto	Descrizione
"Gestione spazi informazioni: Modifica spazio"	Consente di modificare o eliminare uno spazio informazioni. Per eseguire questa attività, è necessario disporre anche dei seguenti diritti: • "Accedere a Explorer e visualizzare questo oggetto nella CMC" • "Gestione spazi informazioni"
"Gestione spazi informazioni: Pianifica indicizzazione"	Consente di pianificare l'indicizzazione per i dati degli spazi informazioni. Per eseguire questa attività, è necessario disporre anche dei seguenti diritti: • "Accedere a Explorer e visualizzare questo oggetto nella CMC" • "Gestione spazi informazioni"
"Gestione spazi informazioni: Avvia indicizzazione"	Consente di eseguire l'indicizzazione per i dati degli spazi informazioni. Per eseguire questa attività, è necessario disporre anche dei seguenti diritti: • "Accedere a Explorer e visualizzare questo oggetto nella CMC" • "Gestione spazi informazioni"

23.3.13.11 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 per accedere alla piattaforma BI tramite l'applicazione Mobile e visualizzare i documenti.
"Sottoscrivere gli avvisi del documento"	Concede l'accesso per la sottoscrizione di avvisi su documenti/ricorrenza. **Nota:** • 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. • Per sottoscrivere gli 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" in Central Management Console (CMC).
"Salvare i documenti nella memoria locale di un dispositivo"	Concede l'accesso per il salvataggio di documenti sul dispositivo Mobile. **Nota:** 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.
"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

24.1 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.

24.1.1 Proprietà comuni dei server

Le proprietà dei server descritte in questa sezione si applicano a tutti i tipi di server.

Tabella 24 - 1: Proprietà della porta richiesta

Proprietà	Descrizione	Valore predefinito
Nome server	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.
ID, CUID	L'ID abbreviato e l'ID univoco del cluster del server. Valori in sola lettura.	Questi valori vengono generati automaticamente.
Nodo	Nome del nodo in cui si trova il server.	Questo valore viene specificato durante l'installazione.
Descrizione	Descrizione del server	Il valore predefinito è il nome del server.
Parametri della riga di comando	Parametri della riga di comando relativi al server.	Il valore predefinito dipende dal tipo di server.

Proprietà	Descrizione	Valore predefinito
Porta richiesta	Specifica la porta dalla quale il server riceve richieste. In un ambiente con firewall può essere opportuno imporre al server di 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. **Nota:** se si seleziona **Assegna automaticamente**, 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.	Per impostazione predefinita, l'opzione **Assegna automaticamente** è impostata su TRUE e l'opzione **Porta richiesta** è vuota.
Assegna automaticamente	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 **Assegna automaticamente** su FALSE e specificare una **Porta richiesta** valida.	Il valore predefinito è TRUE.

Tabella 24 - 2: Proprietà di avvio automatico

Proprietà	Descrizione	Valore predefinito
Avvia automaticamente questo server all'avvio di Server Intelligence Agent	Specifica se il server viene avviato automaticamente all'avvio o al riavvio di Server Intelligence Agent (SIA). Se il valore viene impostato su FALSE e l'agente SIA viene avviato o riavviato, il server non viene avviato.	Il valore predefinito è TRUE.

Tabella 24 - 3: Proprietà degli identificatori host

Proprietà	Descrizione	Valore predefinito
Assegna automaticamente	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.	Il valore predefinito è TRUE.

Proprietà	Descrizione	Valore predefinito
Nome host	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 **Assegna automaticamente** è impostata su TRUE e l'opzione **Nome host** è vuota.
Indirizzo IP	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 **Assegna automaticamente** è impostata su TRUE e l'opzione **Indirizzo IP** è vuota.

Tabella 24 - 4: Proprietà dei modelli di configurazione

Proprietà	Descrizione	Valore predefinito
Usa modello configurazione	Specifica se utilizzare un modello di configurazione.	Il valore predefinito è FALSE.
Ripristina valori predefiniti di sistema	Specifica se ripristinare le impostazioni predefinite originali per questo server.	Il valore predefinito è FALSE.
Imposta modello configurazione	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 **Usa modello configurazione** vengono immediatamente riconfigurati per l'utilizzo delle impostazioni del servizio corrente.	Il valore predefinito è FALSE.

Tabella 24 - 5: Proprietà del Servizio log analisi

Proprietà	Descrizione	Valore predefinito
Livello di registrazione	Specifica il livello di gravità minimo di messaggi che si desidera registrare e determina quante informazioni vengono registrate nel file di registro del server. I livelli della soglia di registrazione possibili sono: • **Non specificato** • **Nessuno** • **Bassa** • **Media** • **Alta**	Il valore predefinito è Non specificato.

Argomenti correlati

- Utilizzo di modelli di configurazione
- Livelli del registro di analisi

24.1.2 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 24 - 6: Proprietà generali

Proprietà	Descrizione	Valore predefinito
Directory temporanea	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. **Nota:** È necessario riavviare il server per rendere effettive le modifiche.	%DefaultDataDir%

Adaptive Job Server può ospitare alcuni servizi differenti. Ogni servizio ha le proprietà seguenti:

Tabella 24 - 7: Proprietà servizio

Proprietà	Descrizione	Valore predefinito
Numero max. processi simultanei	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. 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.	Il valore predefinito è 5.
Numero max. richieste secondarie	Specifica il numero di processi che l'elemento secondario elaborerà prima di essere riavviato.	Il valore predefinito è 100.

Proprietà Adaptive Processing Server

Tabella 24 - 8: Proprietà generali

Proprietà	Descrizione	Valore predefinito
Timeout di avvio servizio (secondi)	Specifica, in secondi, per quanto tempo il server rimane in attesa dell'avvio dei servizi. Se un servizio non viene avviato nel periodo di tempo specificato, i motivi possibili sono due: • 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. • Il servizio non è stato attivato nel periodo di tempo specificato, ad esempio, perché il sistema è troppo lento. 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.	Il valore predefinito è 1200 secondi.

Proprietà del Central Management Server

Nota:
quando si modifica una di queste proprietà del server, è necessario riavviare il server per rendere effettive le modifiche.

Tabella 24 - 9: Proprietà del servizio Central Management

Proprietà	Descrizione	Valore predefinito
Porta server dei nomi	Specifica la porta di attesa del server CMS per le richieste iniziali del servizio dei nomi.	Il valore predefinito è 6400.
Connessioni richieste al database di sistema	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 **Connessioni database di sistema stabilite** del CMS mostra il numero corrente di connessioni stabilite.	Il valore predefinito è 14.

Proprietà	Descrizione	Valore predefinito
Riconnessione automatica al database di sistema	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.	Il valore predefinito è TRUE.

Tabella 24 - 10: Proprietà del servizio Single Sign On

Proprietà	Descrizione	Valore predefinito
Scadenza Single Sign-On (secondi)	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.	Il valore predefinito è 86400 secondi.

Proprietà di Event Server

Tabella 24 - 11: Proprietà del servizio eventi

Proprietà	Descrizione	Valore predefinito
Intervallo di svuotamento (minuti)	Specifica la frequenza con cui viene eseguita l'utilità di pulizia, in minuti.	Il valore predefinito è 20 minuti.
Intervallo di polling eventi (minuti)	Specifica la frequenza con cui il server esegue il polling di un file che attiva un evento, in secondi.	Il valore predefinito è 10 secondi. L'intervallo di valori consentiti è tra 1 e 1200 secondi.

Proprietà dell'Input File Repository Server

Tabella 24 - 12: Proprietà del servizio archivio file di input

Proprietà	Descrizione	Valore predefinito
Numero max. tentativi per l'accesso file	Specifica il numero di tentativi effettuati dal server per accedere a un file.	Il valore predefinito è 1.

Proprietà	Descrizione	Valore predefinito
Tempo massimo di inattività (in minuti)	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.	Il valore predefinito è 10 minuti.
Directory temporanea	Specifica la directory in cui vengono creati i file temporanei quando necessario. **Nota:** Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni. Per garantire prestazioni migliori, è preferibile che la **Directory temporanea** si trovi nello atesso file system della **Directory archivio file**.	%DefaultInputFRS Dir/temp%
Directory archivio file	Specifica la directory in cui vengono archiviati gli oggetti repository dei file. **Nota:** Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni.	%DefaultInputFRS Dir/%

Proprietà dell'Output File Repository Server

Tabella 24 - 13: Proprietà del servizio archivio file di output

Proprietà	Descrizione	Valore predefinito
Numero max. tentativi per l'accesso file	Specifica il numero di tentativi effettuati dal server per accedere a un file.	Il valore predefinito è 1.
Tempo massimo di inattività (in minuti)	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.	Il valore predefinito è 10 minuti.

Proprietà	Descrizione	Valore predefinito
Directory temporanea	Specifica la directory in cui vengono creati i file temporanei quando necessario. **Nota:** Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni.	%DefaultOutputFRSDir/temp%
Directory archivio file	Specifica la directory in cui vengono archiviati gli oggetti repository dei file. **Nota:** Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni.	%DefaultOutputFRSDir/%

Proprietà del server del contenitore di applicazioni Web

Tabella 24 - 14: Proprietà generali

Proprietà	Descrizione	Valore predefinito
Timeout di avvio servizio (secondi)	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. 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).	Il valore predefinito è 600 secondi.

Tabella 24 - 15: Proprietà del servizio applicazione Web BOE

Tipo di proprietà	Descrizione	Valore predefinito
Tipo di autenticazione	Il tipo di autenticazione utilizzato per autenticare gli utenti per l'accesso a BI Launch Pad. I valori accettati sono: • **AD Kerberos** • **AD Kerberos SSO** • **Enterprise** • **LDAP**	Il valore predefinito è **Enterprise**.
Dominio AD predefinito	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”.	Per impostazione predefinita, il valore è vuoto.
Nome principale servizio	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.	Per impostazione predefinita, il valore è vuoto.
File di codice	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.	Per impostazione predefinita, il valore è vuoto.

Tabella 24 - 16: Proprietà di SDK e QaaWS di servizi Web

Proprietà	Descrizione	Valore predefinito
Abilita Single Sign On per Kerberos Active Directory	Se abilitare Single Sign On di Kerberos AD per SDK e QaaWS di servizi Web.	Il valore predefinito è FALSE.

Proprietà	Descrizione	Valore predefinito
Dominio AD predefinito	Il dominio Active Directory predefinito viene utilizzato in modo che gli utenti non debbano fornire un dominio al momento dell'accesso.	Per impostazione predefinita, il valore è vuoto.
Nome principale servizio	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.	Per impostazione predefinita, il valore è vuoto.
File di codice	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.	Per impostazione predefinita, il valore è vuoto.

Tabella 24 - 17: Proprietà di configurazione HTTP

Proprietà	Descrizione	Valore predefinito
Associa a tutti gli indirizzi IP	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.	Il valore predefinito è TRUE.
Associa a nome host o a indirizzo IP	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 **Associa a tutti gli indirizzi IP**.	Il valore predefinito è localhost.
Porta HTTP	Porta su cui viene fornito il servizio HTTP.	Il valore predefinito è 6405. L'intervallo di valori consentiti è tra 1 e 65535.
Dimensioni massime intestazione HTTP	La massima dimensione consentita, in byte, dell'intestazione HTTP di richiesta e risposta.	Il valore predefinito è 32768.

Tabella 24 - 18: Proprietà della configurazione di HTTP tramite proxy

Proprietà	Descrizione	Valore predefinito
Abilita HTTP su proxy	Se abilitare il connettore HTTP tramite proxy sul server WACS. Questa opzione è in genere selezionata nelle distribuzioni con proxy inverso.	Il valore predefinito è FALSE.
Associa a tutti gli indirizzi IP	Se associare o meno la porta HTTP su proxy a tutte le interfacce di rete.	Il valore predefinito è TRUE.
Associa a nome host o a indirizzo IP	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 deseleziona **Associa a tutti gli indirizzi IP**.	Il valore predefinito è localhost.
Porta HTTP	Porta su cui viene fornito il servizio HTTP in una distribuzione con proxy inverso. È possibile specificare un valore solo se si seleziona **Abilita HTTP su proxy**.	Il valore predefinito è 6406. L'intervallo di valori consentiti è tra 1 e 65535.
Nome host proxy	Indirizzo IPv4, IPv6, nome host o nome di dominio completo del server proxy. È possibile specificare un valore solo se si seleziona **Abilita HTTP su proxy**.	Per impostazione predefinita, il valore è vuoto.
Porta proxy	Porta del server proxy normale o del server proxy inverso. È possibile specificare un valore solo se si seleziona **Abilita HTTP su proxy**.	Per impostazione predefinita, il valore è 0. L'intervallo di valori consentiti è tra 1 e 65535.
Dimensioni massime intestazione HTTP	La massima dimensione consentita, in byte, dell'intestazione HTTP di richiesta e risposta.	Il valore predefinito è 32768.

Tabella 24 - 19: Proprietà di configurazione HTTPS

Proprietà	Descrizione	Valore predefinito
Abilita HTTPS	Se abilitare o meno la comunicazione HTTPS/SSL.	Il valore predefinito è FALSE.
Associa a nome host o a indirizzo IP	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 **Abilita HTTPS**.	Il valore predefinito è localhost.
Porta HTTPS	Porta su cui viene fornito il servizio HTTPS. È possibile specificare un valore solo se si seleziona **Abilita HTTPS**.	Il valore predefinito è 443. L'intervallo di valori consentiti è tra 1 e 65535.
Nome host proxy	Indirizzo IPv4, IPv6, nome host o nome di dominio completo del server proxy. È possibile specificare un valore solo se si seleziona **Abilita HTTPS**.	Per impostazione predefinita, il valore è vuoto.
Porta proxy	Porta del server proxy normale o del server proxy inverso. È possibile specificare un valore solo se si seleziona **Abilita HTTPS**.	Per impostazione predefinita, il valore è 0. L'intervallo di valori consentiti è tra 1 e 65535.
Protocollo	Protocollo di crittografia da utilizzare. È possibile specificare un valore solo se si seleziona **Abilita HTTPS**.	Il valore predefinito è TLS. I valori consentiti sono TLS o SSL.
Tipo di archivio certificati	Il tipo di archivio certificati che contiene i certificati e le chiavi private. Nella maggior parte dei casi è **PCKS12**. È possibile specificare un valore solo se si seleziona **Abilita HTTPS**.	Il valore predefinito è PKCS12. I valori consentiti sono PKCS12 o JKS.
Percorso file archivio certificati	Il percorso completo del file di certificati. È possibile specificare un valore solo se si seleziona **Abilita HTTPS**.	Per impostazione predefinita, il valore è vuoto.

Proprietà	Descrizione	Valore predefinito
Password accesso chiave privata	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 **Abilita HTTPS**.	Per impostazione predefinita, il valore è vuoto.
Alias certificato	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 **Abilita HTTPS**.	Per impostazione predefinita, il valore è vuoto.
Abilita autenticazione client	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 **Abilita HTTPS**.	Il valore predefinito è FALSE.
Percorso file elenco certificati attendibili	Il percorso completo del file di elenco dei certificati attendibili. È possibile specificare un valore solo se si seleziona **Abilita HTTPS** e **Abilita autenticazione client**.	Per impostazione predefinita, il valore è vuoto.

Proprietà	Descrizione	Valore predefinito
Password accesso chiavi private elenco certificati attendibili	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 **Abilita HTTPS** e **Abilita autenticazione client**.	Per impostazione predefinita, il valore è vuoto.
Dimensioni massime intestazione HTTP	La massima dimensione consentita, in byte, dell'intestazione HTTP di richiesta e risposta.	Il valore predefinito è 32768.

Tabella 24 - 20: Impostazioni valuta (per connettore)

Proprietà	Descrizione	Valore predefinito
N. massimo richieste simultanee	Numero di richieste HTTP o HTTPS simultanee che ogni connettore (HTTP, HTTP tramite proxy o HTTPS) è in grado di elaborare contemporaneamente.	Il valore predefinito è 150. L'intervallo di valori consentiti è tra 1 e 1000.

Tabella 24 - 21: Impostazioni di configurazione di Active Directory

Proprietà	Descrizione	Valore predefinito
Posizione file Krb5.ini	Percorso completo di un file `krb5.ini` in cui sono memorizzate le proprietà di configurazione di Kerberos.	Per impostazione predefinita, il valore è vuoto.
Posizione file bscLogin.conf	Percorso completo a un file `bscLogin.conf`.	Per impostazione predefinita, il valore è vuoto.

24.1.3 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 24 - 22: Proprietà di funzionamento del servizio

Proprietà	Descrizione	Valore predefinito
Promemoria: Non è necessario riavviare il server dopo aver modificato le seguenti proprietà di funzionamento del servizio.		
Raggruppamento delle connessioni	Abilita o disabilita il pool di connessioni. I valori possibili sono i seguenti: • Abilitato - con timeout • Abilitato - senza timeout • Disabilitato **Nota:** 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.	Abilitato - con timeout
Timeout Connection Pool	Specifica il tempo massimo di inattività per le connessioni nel pool (in minuti). **Nota:** Questa proprietà equivale al parametro `Max Pool Time` del file `cs.cfg`. Disabilitare il pool equivale a impostare `Max Pool Time` su `0`. Abilitare il pool senza timeout equivale a impostare `Max Pool Time` su `-1`. Consultare il *Manuale dell'accesso ai dati* per ulteriori informazioni.	60
Timeout inattività oggetti transitori	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.	60
Intervallo timer oggetti transitori	Specifica l'intervallo di tempo tra le verifiche delle attività (in minuti). Il server verifica a intervalli regolari la presenza di oggetti da rimuovere.	5

Proprietà	Descrizione	Valore predefinito
Abilita raggruppamento HTTP	Abilita o disabilita il raggruppamento HTTP. **Nota:** Il raggruppamento HTTP è rilevante solo per la distribuzione 3-tier e influisce sulle perfomance 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 **Dimensioni blocco HTTP** su 0.	Enabled
Dimensioni blocco HTML	Specifica le dimensioni delle risposte HTTP emesse dal server (in kilobyte).	64

Tabella 24 - 23: Proprietà di analisi di basso livello

Proprietà	Descrizione	Valore predefinito
Promemoria: Non è necessario riavviare il server dopo aver modificato le seguenti proprietà di analisi di basso livello.		
Abilita analisi processo	Abilita l'analisi dei processi di Connection Server. **Nota:** La proprietà **Livello log** deve essere impostata su **Alto**.	Disabilitato
Abilita analisi middleware	Abilita l'analisi di tutto il middleware. Per analizzare un middleware specifico, è necessario configurare il file `cs.cfg` e riavviare il server. **Nota:** La proprietà **Livello log** deve essere impostata su **Alto**.	Disabilitato

Tabella 24 - 24: Proprietà delle origini dati attive

Proprietà	Descrizione	Valore predefinito
Avvertenza: È necessario riavviare il server dopo aver modificato le seguenti proprietà delle origini dati attive.		
Attiva origine dati	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. **Avvertenza:** 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. **Promemoria:** 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. **Nota:** 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".	Deselezionato
Livello di rete	Specifica il livello di rete utilizzato dalla connessione. **Nota:** Viene considerato solamente il nome non localizzato. è possibile trovare l'elenco dei livelli di rete disponibili nel file `driver.cfg` che si trova nella directory *`dir-installaz-connectionserver`*`\connectionServer\`.	• `ODBC` per server CORBA nativi • `JDBC` per server CORBA adattivi

Proprietà	Descrizione	Valore predefinito
Database	Specifica il database utilizzato dalla connessione. **Nota:** 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 `.*` per trovare una corrispondenza per qualsiasi carattere. Ad esempio, l'espressione `MS SQL Server.*$` significa che vengono utilizzati tutti i database MS SQL Server. Per ulteriori informazioni sulle espressioni regolari, consultare il sito Web PERL all'indirizzo http://www.perl.com/doc/manual/html/pod/perlre.html#Regular_Expressions.	Il campo è vuoto finché non si inserisce il nome di un database.

Argomenti correlati

- Proprietà comuni dei server

24.1.4 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 Crystal Reports 2011 Report Application Server
- Servizio di elaborazione Crystal Reports 2011

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 24 - 25: Proprietà del Servizio cache Crystal Reports

Proprietà	Descrizione	Valore predefinito
L'aggiornamento del visualizzatore produce sempre i dati correnti	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. **Nota:** 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 **Impostazioni predefinite** > **Visualizzazione gruppo di server**.	Il valore predefinito è TRUE.
Condividi dati dei report tra i client	Specifica se i dati di report sono condivisi tra client diversi. **Nota:** 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.	Il valore predefinito è TRUE.
Timeout connessione inattiva (minuti)	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.
Timeout cache di protezione (minuti)	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
Dati meno recenti forniti ai client su richiesta	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. 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. 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. **Nota:** 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.	Il valore predefinito è 0 secondi.
Dimensioni cache massime (KB)	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.
Directory file cache	Specifica il percorso della directory del file cache.	`%DefaultDataDir%/CrystalReportsCachingServer/temp`
Argomenti Java VM	Indica gli argomenti della riga di comando che è possibile specificare per la JVM.	Il valore predefinito è vuoto.

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 24 - 26: Proprietà del Servizio di elaborazione Crystal Reports

Proprietà	Descrizione	Valore predefinito
Timeout connessione inattiva (minuti)	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 60 minuti.
Durata massima dei processi per elemento secondario	Specifica il numero massimo di processi che ogni processo secondario può gestire per durata.	Il valore predefinito è 1000.
L'aggiornamento del visualizzatore produce sempre i dati correnti	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. **Nota:** 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 **Impostazioni predefinite** > **Visualizzazione gruppo di server**.	Il valore predefinito è TRUE.
Condividi i dati dei report tra i client	Specifica se i dati di report sono condivisi tra client diversi. Specifica se i dati di report sono condivisi tra client diversi. **Nota:** 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.	Il valore predefinito è TRUE.
Timeout connessione inattiva (minuti)	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.

Proprietà	Descrizione	Valore predefinito
Numero max. processi simultanei (0 per automatico)	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.
Dati meno recenti forniti ai client su richiesta (secondi)	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. 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. 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. **Nota:** 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.	Il valore predefinito è 0.
Numero massimo di elementi secondari preriavviati	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 elemento secondario.
Directory temporanea	Specifica la directory in cui vengono creati i file temporanei quando necessario. **Nota:** Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni.	%DefaultDataDir%/CrystalReportsProcessingServer/temp

Proprietà	Descrizione	Valore predefinito
Percorso classe Java	Nome e percorso delle classi Java richieste dal server.	%CommonJavaLibDir%/procCR.jar
Argomenti VM elemento secondario Java	Indica gli argomenti della riga di comando specificati per i processi secondari creati dal server.	Dbusinessobjects.connectivity.directory=%EnterpriseDir%/dataAccess/connectionServer,Xmx512m,XX:MaxPermSize=128m

Tabella 24 - 27: Proprietà del Servizio Single Sign-On

Proprietà	Descrizione	Valore predefinito
Scadenza Single Sign-On (secondi)	Specifica il tempo, in secondi, di validità di una connessione SSO prima della scadenza.	Il valore predefinito è 86400 secondi.

Proprietà di Crystal Reports 2011 Report Application Server

Nota:
quando si modifica una di queste proprietà del server, è necessario riavviare il server per rendere effettive le modifiche.

Tabella 24 - 28: Proprietà del servizio di modifica e visualizzazione Crystal Reports 2011

Proprietà	Descrizione	Valore predefinito
Consenti ai processi report di rimanere connessi al database fino alla chiusura del processo report	Specifica se il processo report rimane connesso al database fino all'esecuzione.	Il valore predefinito è FALSE.
Dimensione dati da sfogliare (record)	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.

Proprietà	Descrizione	Valore predefinito
Timeout connessione inattiva (minuti)	Specifica la quantità di tempo, in minuti, di attesa di Report Application Server (RAS) per le richieste da un cliente inattivo prima del timeout. 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 `ReportClientDocument` non viene chiuso in modo esplicito, il server resterà inutilmente in attesa della chiusura di un processo inattivo).	Il valore predefinito è 30 minuti.
Dimensioni batch (record)	Specifica quante righe dell'insieme di risultati vengono restituite dal database durante ogni trasferimento di dati. 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.	Il valore predefinito è 100 record.
Numero di record di database da leggere per l'anteprima o l'aggiornamento di un report (-1 per nessun limite) (	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. 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.	Il valore predefinito è 20000 record.
Numero max. report simultanei (0 per nessun limite)	Specifica il numero massimo di processi indipendenti che possono essere eseguiti simultaneamente sul server RAS.	Il valore predefinito è 75 processi.
Dati meno recenti forniti a un client su richiesta (in minuti)	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.
Directory temporanea	Specifica la directory in cui vengono creati i file temporanei quando necessario. **Nota:** Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni.	`%DefaultDataDir%/CrystalReportsRasServer/temp`

Tabella 24 - 29: Proprietà del Servizio Single Sign-On

Proprietà	Descrizione	Valore predefinito
Scadenza Single Sign-On (secondi)	Specifica il tempo, in secondi, di validità di una connessione SSO prima della scadenza.	Il valore predefinito è 86400 secondi.

Proprietà del Servizio di elaborazione Crystal Reports 2011

Nota:
quando si modifica una di queste proprietà del server, è necessario riavviare il server per rendere effettive le modifiche.

Tabella 24 - 30: Proprietà del Servizio di elaborazione Crystal Reports 2011

Proprietà	Descrizione	Valore predefinito
Timeout connessione inattiva (minuti)	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 60 minuti.
Durata massima dei processi per elemento secondario	Specifica il numero massimo di processi che ogni processo secondario può gestire per durata.	Il valore predefinito è 1000.
L'aggiornamento del visualizzatore produce sempre i dati correnti	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. **Nota:** 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 **Impostazioni predefinite > Visualizzazione gruppo di server**.	Il valore predefinito è TRUE.
Condividi i dati dei report tra i client	Specifica se i dati di report sono condivisi tra client diversi. Specifica se i dati di report sono condivisi tra client diversi. **Nota:** 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.	Il valore predefinito è TRUE.

Proprietà	Descrizione	Valore predefinito
Timeout connessione inattiva (minuti)	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.
Numero max. processi simultanei (0 per automatico)	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.
Dati meno recenti forniti ai client su richiesta (secondi)	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. 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. 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. **Nota:** 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.	Il valore predefinito è 0.
Numero massimo di elementi secondari preriavviati	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 elemento secondario.

Proprietà	Descrizione	Valore predefinito
Directory temporanea	Specifica la directory in cui vengono creati i file temporanei quando necessario. **Nota:** Se questa directory non dispone di spazio su disco sufficiente possono verificarsi problemi di prestazioni.	%DefaultData Dir%/CrystalReports ProcessingServer/temp
Consenti ai processi report di rimanere connessi al database fino alla chiusura del processo report	Specifica se il processo report rimane connesso al database fino alla chiusura.	Il valore predefinito è FALSE.
Record di database letti durante l'anteprima o l'aggiornamento	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. 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.	Il valore predefinito è 20000.

Tabella 24 - 31: Proprietà del Servizio Single Sign-On

Proprietà	Descrizione	Valore predefinito
Scadenza Single Sign-On (secondi)	Specifica il tempo, in secondi, di validità di una connessione SSO prima della scadenza.	Il valore predefinito è 86400 secondi.

24.1.5 Proprietà dei servizi Analysis

La categoria dei servizi Analysis include Adaptive Processing Server:

Tabella 24 - 32: Proprietà dei servizi di analisi multidimensionali

Proprietà	Descrizione	Valore predefinito
Numero massimo sessioni client	Specifica il numero massimo di sessioni MDAS che possono essere aperte contemporaneamente sul server. 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.	Il valore predefinito è impostato su 15. L'intervallo valido è compreso tra 1 e 100.
Numero massimo di celle restituite da una query	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.
Numero massimo di membri restituiti durante il filtraggio	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 3000 membri.

Tabella 24 - 33: Proprietà dei servizi applicazioni Web BEx

Proprietà	Descrizione	Valore predefinito
Numero massimo sessioni client	Numero massimo di sessioni client consentite nel servizio.	Il valore predefinito è 15 sessioni.
SAP BW Master System	Il nome della connessione OLAP al sistema BW creato nella piattaforma BI.	Il valore predefinito è SAP_BW.
Destinazione RFC server JCo	Nome della destinazione RFC server JCo specificato nel sistema BW.	Per impostazione predefinita, il valore è vuoto.

Proprietà	Descrizione	Valore predefinito
Host gateway server JCo	Nome dell'host gateway server JCo specificato nel sistema BW.	Per impostazione predefinita, il valore è vuoto.
Servizio gateway server JCo	Nome del servizio gateway server JCo specificato nel sistema BW.	Per impostazione predefinita, il valore è vuoto.
Conteggio connessione server JCo	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.

24.1.6 Proprietà dei servizi Data Federation

La categoria dei servizi Data Federation include Adaptive Processing Server:

Tabella 24 - 34: Proprietà dei servizi Data Federation

Proprietà	Descrizione	Valore predefinito
Connessioni max	Specifica il numero massimo di connessioni consentite sul server.	Il valore predefinito è 32767.
Dimensione pool di thread di esecuzione	Specifica il numero massimo di query che è possibile eseguire in parallelo in un determinato momento.	Il valore predefinito è 10.
Timeout inattività connessione	Specifica l'intervallo di tempo, in secondi, al termine del quale una connessione inattiva viene chiusa.	Il valore predefinito è 1080 secondi.
Timeout inattività istruzione	Specifica l'intervallo di tempo, in secondi, al termine del quale un'istruzione di query inattiva viene chiusa.	Il valore predefinito è 60 secondi.

24.1.7 Proprietà servizi Web Intelligence

La categoria dei servizi Web Intelligence include i server seguenti:

- Adaptive Processing Server
- Web Intelligence Processing Server

Impostazioni di Adaptive Processing Server

Tabella 24 - 35: Servizio di monitoraggio Web Intelligence APS

Proprietà	Descrizione	Valore predefinito
Abilita monitoraggio	Specifica se il monitoraggio è abilitato per il servizio.	Il valore predefinito è "TRUE".
Ritardo del loop del thread di monitoraggio (secondi)	Specifica l'intervallo di tempo, espresso in secondi, tra i tentativi di esecuzione del ping dei client effettuati dal servizio.	Il valore predefinito è 300 secondi.
Timeout svuotamento risorse monitorate predefinite (in secondi)	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.
Timeout scambio risorse monitorate predefinite (in secondi)	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.	Il valore predefinito è 600 secondi.

Tabella 24 - 36: Proprietà del servizio di visualizzazione

Proprietà	Descrizione	Valore predefinito
Timeout svuotamento motore di visualizzazione (in secondi)	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.
Timeout scambio motore di visualizzazione (in secondi)	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 motore di visualizzazione (in secondi)**.	Il valore predefinito è 600 secondi.

Proprietà di Web Intelligence Processing Server

Le proprietà di Web Intelligence Processing Server 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 24 - 37: Impostazioni del servizio Information Engine

Proprietà	Descrizione	Valore predefinito
Abilita cache elenco dei valori	Specifica se la memorizzazione nella cache è abilitata per l'elenco dei valori in Web Intelligence Processing Server.	Il valore predefinito è TRUE.
Dimensioni batch elenco dei valori (voci)	Specifica il numero massimo di voci, o valori, per ogni batch di elenco dei valori.	Il valore predefinito è di 1000 voci per batch.
Dimensioni massime ordinamento personalizzato (voci)	Specifica il numero massimo di voci nell'ordinamento personalizzato.	Il valore predefinito è di 100 voci per ordinamento personalizzato.
Dimensioni massime cache universo (Universi)	Specifica il numero di universi da memorizzare nella cache in Web Intelligence Processing Server.	Il valore predefinito è 20 minuti.
Dimensioni LOV massime (voci)	Specifica il numero massimo di voci, o valori, per ogni elenco di valori (LOV).	Il valore predefinito è 50000 voci per elenco di valori.

Tabella 24 - 38: Impostazioni del servizio principale Web Intelligence

Proprietà	Descrizione	Valore predefinito
Timeout prima della reinizializzazione (secondi)	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 **Numero max. documenti prima della reinizializzazione**.	Il valore predefinito è 1200 secondi.

Proprietà	Descrizione	Valore predefinito
Timeout documento inattivo (secondi)	Specifica il periodo di tempo, in secondi, prima dello spostamento della sessione di Web Intelligence Processing Server. 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.	Il valore predefinito è 300 secondi. L'intervallo valido è compreso tra 100 e 1000 secondi.
Intervallo di polling del server (secondi)	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.	Il valore predefinito è 120 secondi.
Numero max. documenti per utente	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.	Il valore predefinito è 5. L'intervallo valido è compreso tra 1 e 20.
Numero max. documenti prima della reinizializzazione	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 **Timeout prima della reinizializzazione**.	Il valore predefinito è 50 documenti.

Proprietà	Descrizione	Valore predefinito
Consenti errori dimensione massima mappa	Specifica se la proprietà *Numero max. connessioni* è limitata. Se questa proprietà è abilitata, il valore impostato per la proprietà *Numero max. connessioni* viene riconosciuto dal server. In caso contrario, la proprietà viene ignorata.	Il valore predefinito è TRUE.
Timeout connessione inattiva (minuti)	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.	Il valore predefinito è 20 minuti.
Numero max. connessioni	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. **Nota:** È necessario che la proprietà *Consenti errori dimensione massima mappa* sia abilitata affinché il server riconosca questa proprietà.	Il valore predefinito è 50 sessioni. L'intervallo valido è compreso tra 5 e 65535.

Proprietà	Descrizione	Valore predefinito
Abilita analisi memoria	Specifica se l'analisi della memoria è abilitata. Se la proprietà è abilitata, le proprietà seguenti sono attive e riconosciute dal server. • *Soglia massima memoria* • *Soglia superiore memoria* • *Soglia inferiore memoria* Quando la memoria del processo del server è superiore al valore di *Soglia superiore memoria*, l'unica operazione consentita è il salvataggio dei documenti. Quando la memoria del processo è superiore al valore di *Soglia massima memoria*, tutte le operazioni vengono interrotte e hanno esito negativo.	Il valore predefinito è TRUE.
Soglia massima memoria (MB)	Specifica la soglia massima per l'utilizzo della memoria.	Il valore predefinito è 6000 MB.
Soglia superiore memoria (MB)	Specifica la soglia superiore per l'utilizzo della memoria.	Il valore predefinito è 4500 MB.
Soglia inferiore memoria (MB)	Specifica la soglia inferiore per l'utilizzo della memoria.	Il valore predefinito è 3500 MB.
Abilita monitoraggio servizio PJS	Consente il monitoraggio del server da parte del servizio PJS, ospitato nel server di elaborazione adattivo.	Il valore predefinito è TRUE.
Conteggio tentativi errori ping servizio PJS	Specifica il numero di volte in cui il server tenterà di raggiungere il servizio PJS prima di decidere di non essere in grado di raggiungerlo.	Il valore predefinito è 3 tentativi.
Periodo thread monitoraggio servizio PJS	Specifica il ritardo tra i tentativi di accesso al servizio PJS.	Il valore predefinito è 300 secondi.

Tabella 24 - 39: Impostazioni del servizio di elaborazione Web Intelligence

Proprietà	Descrizione	Valore predefinito
Abilita utilizzo di URL HTTP	Specifica se il server è in grado di accedere ai file archiviati in remoto.	Il valore predefinito è TRUE.
Valore proxy	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.	Il valore predefinito è vuoto.

Tabella 24 - 40: Impostazioni del servizio comune Web Intelligence

Proprietà	Descrizione	Valore predefinito
Timeout cache (minuti)	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.	Il valore predefinito è 4370 minuti.
Intervallo pulizia cache documento (secondi)	Specifica l'intervallo di tempo, in minuti, necessario per la scansione e il controllo della cache del documento rispetto alle impostazioni `Dimensione massima cache documento`, `Spazio di riduzione massimo cache documento` e `Numero max. documenti nella cache`.	Il valore predefinito è 120 minuti.
Disabilita condivisione cache	Specifica se la condivisione cache è disabilitata. Per impostazione predefinita la condivisione cache è abilitata, pertanto tutte le istanze di Web Intelligence Processing Server condividono la stessa cache. Se tuttavia si desidera disporre di una cache per istanza di Web Intelligence Processing Server, è necessario abilitare questa proprietà.	Il valore predefinito è FALSE.

Proprietà	Descrizione	Valore predefinito
Abilita cache documento	Specifica se la cache del documento è abilitata. Se la proprietà è abilitata, la cache può essere precaricata con documenti Web Intelligence pianificati.	Il valore predefinito è TRUE.
Abilita cache in tempo reale	Specifica se la cache in tempo reale è abilitata. Se la proprietà è abilitata, la cache può essere caricata in modo dinamico. Web Intelligence Processing Server, 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.	Il valore predefinito è TRUE.
Dimensione massima cache documenti (KB)	Specifica la dimensione massima della cache dei documenti. Una volta raggiunto questo limite, la cache dei documenti viene cancellata in base alla proprietà *`Spazio di riduzione massimo cache documento`*.	Il valore predefinito è 1000000 KB.
Spazio di riduzione massimo cache documenti	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.	Il valore predefinito è 70%.

Proprietà	Descrizione	Valore predefinito
Dimensioni flusso caratteri massime (MB)	Specifica le dimensioni massime del flusso caratteri inviate al client Web Intelligence. **Nota:** Se la proprietà **Dimensioni flusso caratteri massime** viene superata, il documento Web Intelligence non viene creato e il client riceve un messaggio di errore.	Il valore predefinito è 5 MB. L'intervallo valido è compreso tra 1 e 65535 MB.
Dimensione massima flusso binario (MB)	Specifica le dimensioni massime in MB di un flusso binario inviato al client Web Intelligence. **Nota:** Se la proprietà **Dimensione massima flusso binario** viene superata, il documento Web Intelligence non viene creato e il client riceve un messaggio di errore.	Il valore predefinito è 50 MB. L'intervallo valido è compreso tra 1 e 65535 MB.
Numero max. documenti nella cache	Numero massimo di documenti Web Intelligence che possono essere memorizzati nella cache. Nella cache non è mai presente un numero di documenti superiore a questo valore e le dimensioni totali della cache non sono mai superiori al valore specificato dall'impostazione **Spazio di riduzione massimo cache documento (MB)**. **Nota:** Per migliorare le prestazioni del sistema, impostare questo valore su 0 quando si seleziona `Abilita cache in tempo reale`, ma immettere un valore quando l'opzione `Abilita cache in tempo reale` è deselezionata.	Il valore predefinito è 0. L'intervallo valido è compreso tra 0 e 65535 documenti.

Proprietà	Descrizione	Valore predefinito
Directory immagini	Specifica il percorso della directory delle immagini.	Il valore predefinito è vuoto.
Directory cache di output	Specifica il percorso della cache.	Il valore predefinito è vuoto.

Tabella 24 - 41: Proprietà generali

Proprietà	Descrizione	Valore predefinito
Scadenza Single Sign-On (secondi)	Specifica il tempo, in secondi, di validità di una connessione SSO prima della scadenza.	Il valore predefinito è 86400 secondi.

Argomenti correlati

- Impostazioni della soglia di memoria di Web Intelligence Server

24.1.7.1 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 corrente 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 sufficiente 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:

```
4500MB - .20*4500MB = 3600MB
```

- 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:

```
4500MB - .20*4500MB = 3600MB
```

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.

24.1.8 Proprietà dei servizi di Dashboard Design

Proprietà server cache di Dashboard Design

Tabella 24 - 42: Proprietà servizio cache di Dashboard Design

Proprietà	Descrizione	Valore predefinito
Dimensioni cache massime (KB)	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.
Timeout connessione inattiva (minuti)	Specifica l'intervallo di tempo, in minuti, in cui la server cache di Dashboard Design attende una richiesta da una connessione inattiva. Non è in genere necessario modificare il valore predefinito.	Il valore predefinito è 15 minuti.

Proprietà	Descrizione	Valore predefinito
Condividi dati tra i client	Specifica se i dati di report sono condivisi tra client diversi.	Il valore predefinito è "TRUE".
Dati meno recenti forniti ai client su richiesta (secondi)	Specifica l'intervallo di tempo, in secondi, in cui il server utilizza i dati memorizzati nella cache per soddisfare le richieste da query su richiesta. 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. 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. **Nota:** È possibile impostare questa proprietà in un oggetto report. I valori specificati per tale oggetto sostituiscono le impostazioni del server.	Il valore predefinito è 0 secondi.

Proprietà	Descrizione	Valore predefinito
Timeout cache di protezione (minuti)	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.
Argomenti Java VM	Indica gli argomenti della riga di comando che è possibile specificare per la JVM.	

Proprietà del server di elaborazione di Dashboard Design

Tabella 24 - 43: Proprietà del servizio di elaborazione di Dashboard Design

Proprietà	Descrizione	Valore predefinito
Numero max. processi simultanei	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.
Durata massima dei processi per elemento secondario	Specifica il numero massimo di processi che ogni processo secondario può gestire per durata.	Il valore predefinito è 1000.
Numero massimo di elementi secondari preavviati	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.

Proprietà	Descrizione	Valore predefinito
Timeout connessione inattiva (minuti)	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 20 minuti.
Timeout connessione inattiva (minuti)	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.
Argomenti VM elemento secondario Java	Indica gli argomenti della riga di comando specificati per i processi secondari creati dal server.	

Tabella 24 - 44: Proprietà del Servizio Single Sign-On

Proprietà	Descrizione	Valore predefinito
Scadenza Single Sign-On (secondi)	Specifica il tempo, in secondi, di validità di una connessione SSO prima della scadenza.	Il valore predefinito è 86400 secondi.

Appendice sulle metriche server

25.1 Informazioni sull'appendice sulle metriche server

In questa appendice, se non diversamente specificato, il termine "server" fa riferimento a un server della piattaforma BI e non al computer in cui la piattaforma è installata o in esecuzione.

Le metriche server non sono disponibili su server che non sono in esecuzione.

Argomenti correlati

- Analisi delle specifiche dei server

25.1.1 Metriche server comuni

Le metriche seguenti descrivono la macchina su cui è in esecuzione il server specificato.

Tabella 25 - 1: Metriche specifiche della macchina

Metrica	Descrizione
Nome macchina	Il nome host della macchina in cui viene eseguito il server.
Sistema operativo	Il sistema operativo della macchina in cui viene eseguito il server.
Tipo CPU	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).

Metrica	Descrizione
CPU	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).
RAM (MB)	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).
Ora locale	L'ora locale.
Dimensione disco (GB)	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).
Spazio su disco utilizzato (GB)	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 25 - 2: Metriche specifiche del server

Metrica	Descrizione
Server dei nomi	Il nome e il numero di porta del server CMS su cui viene pubblicato l'indirizzo del server.
Nome registrato	Il nome interno del server. Non si tratta del nome visualizzato nella schermata "Server" della CMC.
Versione	La versione del server.
Ora di inizio	L'ora in cui il server è stato avviato per l'ultima volta.

Metrica	Descrizione
PID	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.
Nome host	Un elenco separato da virgole di nomi di host correntemente utilizzati dal server.
Indirizzo IP host	Un elenco separato da virgole di indirizzi IP su cui si basano le richieste del server.
Porta richiesta	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.
Thread server occupato	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 25 - 3: Metriche di controllo

Metrica	Descrizione
Numero corrente degli eventi di controllo in coda	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. **Nota:** 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.

Tabella 25 - 4: Metriche servizio di accesso

Metrica	Descrizione
Directory di registrazione	I file di registro per il server sono disponibili in questa posizione.

25.1.2 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 25 - 5: Metriche del Central Management Service

Metrica	Descrizione
Connessione al database di controllo stabilita	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.
Strumento di controllo CMS	Indica se Central Management Server (CMS) funziona 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.
Nome connessione database di controllo	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.
Nome utente database di controllo	Il nome dell'account utente utilizzato per la connessione al database di controllo.

Metrica	Descrizione
Ultimo aggiornamento database di controllo	La data e ora più recenti in cui il CMS ha iniziato a recuperare eventi da un sistema controllato. Se il CMS funge da strumento di controllo, questa metrica deve indicare un orario molto vicino a quello in cui è stata caricata la pagina “Metriche”. Se l'orario indicato precede di più di due ore quello in cui è stata caricata la pagina, è possibile che il controllo non stia funzionando correttamente.
Durata ultimo ciclo di polling del thread di controllo (secondi)	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. • Un valore inferiore a 20 minuti indica che il sistema funziona correttamente. • Un valore compreso tra 20 minuti e 2 ore indica che il sistema è occupato. • 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.
Utilizzo thread di controllo	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.
Server CMS cluster	Elenco separato da punti e virgola dei nomi host e dei numeri di porta dei Central Management Server in esecuzione nel cluster.
Numero di sessioni stabilite da utenti simultanei	Il numero totale di sessioni per utenti che utilizzano licenze simultanee.

Metrica	Descrizione
Numero di sessioni stabilite da utenti specifici	Il numero totale di sessioni per utenti che utilizzano licenze specifiche.
Numero massimo di sessioni utente dall'avvio	Il numero massimo di sessioni simultanee di utenti che possono essere gestite dal CMS dall'avvio.
Numero di sessioni stabilite dai server	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.
Numero di sessioni stabilite da tutti gli utenti	Il numero di sessioni simultanee di utenti 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.
Processi non riusciti	Il numero totale di processi non riusciti nel CMS dall'avvio del server.
Processi in sospeso	Il numero attuale di processi in sospeso.
Processi in esecuzione	Il numero attuale di processi in esecuzione. Questo valore comprende i processi pianificati ma non pronti per l'esecuzione poiché il relativo orario pianificato non è ancora arrivato.
Processi completati	Il numero totale di processi completati nel CMS dall'avvio del server.
Processi in attesa	Il numero di processi in attesa simultaneamente nel CMS. Sono inclusi i processi pianificati e in attesa di risorse libere.
Licenze utente simultanee	Il numero di licenze utente simultaneo indicato dal codice.
Licenze utenti specifici	Il numero di licenze per utenti designati indicato dal codice di attivazione del prodotto.
Data build	La data di build del CMS.
Nome connessione database di sistema	Il nome della connessione al database di sistema CMS. Non deve necessariamente essere il nome dello stesso database di sistema CMS.
Nome server database di sistema	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.

Metrica	Descrizione
Nome utente database di sistema	Il nome dell'account utente utilizzato per la connessione al database di sistema CMS.
Nome origine dati	Il nome della connessione al database di sistema CMS.
Numero build	Il numero di build del CMS. Tale numero può essere utilizzato per identificare la versione della piattaforma BI installata.
Versione prodotto	La versione prodotto del CMS.
Versione risorsa	La versione risorsa del CMS.
Tempo medio di risposta a commit dall'avvio (msec)	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.
Tempo medio di risposta alle query dall'avvio (msec)	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.
Tempo di risposta a commit più lungo dall'avvio (msec)	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.
Tempo di risposta alle query più lungo dall'avvio (msec)	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.
Numero di commit dall'avvio	Il numero di commit al database di sistema CMS dal momento di avvio del server.
Numero di query dall'avvio	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.
Numero di accessi dall'avvio	Il numero di accessi dal momento di avvio del server. Un numero alto potrebbe indicare in sistema più attivo o in sovraccarico.

Metrica	Descrizione
Connessioni database di sistema stabilite	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 **Connessioni richieste al database di sistema** nella schermata "Proprietà", potrebbe indicare che il CMS non può stabilire connessioni aggiuntive e che il funzionamento del sistema non è ottimale. Una possibile soluzione è configurare il server database in modo da consentire più connessioni per il CMS.
Connessioni database di sistema utilizzate correntemente	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 **Connessioni richieste al database di sistema** nella schermata "Proprietà" potrebbe migliorare le prestazioni del CMS. Anche regolare il database di sistema CMS potrebbe migliorare le prestazioni.
Richieste database di sistema in sospeso	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 **Connessioni richiesta al database si sistema**. Anche regolare il database di sistema CMS potrebbe migliorare le prestazioni.
Numero di oggetti nella cache di sistema di CMS	Il numero totale di oggetti correntemente nella cache di sistema del CMS.
Numero di oggetti nel database di sistema di CMS	Il numero totale di oggetti correntemente nel database di sistema del CMS.
Account utente simultanei esistenti	Il numero totale di utenti esistenti con licenze simultanee in cluster.
Account utente specifici esistenti	Il numero totale di utenti esistenti con licenze specifiche in cluster.

25.1.3 Metriche di Connection Server

Le seguenti metriche sono specifiche di Connection Server.

Tabella 25 - 6: Metriche del servizio di connettività

Metrica	Descrizione
Origini dati	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: • "Stato"("Caricato"o "Non riuscito"): stato attuale del driver • "Connessioni disponibili: numero di connessioni del pool utilizzabili" • "Processi (CORBA): numero di processi in elaborazione (distribuzione 2-tier)" • "Processi (HTTP): numero di processi in elaborazione (distribuzione livello Web)" **Nota:** Per ulteriori informazioni sui pool di connessioni, consultare il *Manuale dell'accesso ai dati*.

25.1.4 Metriche di Event Server

La tabella seguente descrive le metriche del server che vengono visualizzate nella schermata "Metriche" per Event Server.

Tabella 25 - 7: Metriche servizio eventi

Metrica	Descrizione
Elenco di file monitorati	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.
File monitorati	Il numero totale di file monitorati da Event Server.

25.1.5 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 25 - 8: Metriche del servizio archivio file

Metrica	Descrizione
File attivi	Il numero di file nel File Repository Server a cui è stato effettuato l'accesso.
Dati scritti (MB)	Il numero totale di megabyte scritti su file nel server.
Dati inviati (MB)	Il numero complessivo di megabyte letti dai file nel server.
Elenco di file attivi	Una tabella in cui sono indicati i file presenti nel File Repository Server a cui è stato effettuato l'accesso.
Connessioni attive	Il numero totale di connessioni attive dai client e verso altri server.
Spazio su disco disponibile nella directory principale (GB)	Quantità totale, espressa in gigabyte, di spazio disponibile sul disco contenente il file eseguibile del server.
Spazio su disco libero nella directory principale (GB)	La quantità totale di spazio libero sul disco contenente il file eseguibile del server, in gigabyte.
Spazio su disco totale nella directory principale (GB)	Quantità totale, espressa in gigabyte, di spazio disponibile sul disco contenente il file eseguibile del server.

Metrica	Descrizione
Spazio su disco disponibile nella directory principale (%)	Quantità, espressa in percetuale, di spazio disponibile su disco contenente il file eseguibile del server.

25.1.6 Metriche di Adaptive Processing Server

La tabella seguente descrive le metriche del server che vengono visualizzate nella schermata "Metriche" per Adaptive Processing Server.

Tabella 25 - 9: Metriche di Adaptive Processing Server

Metrica	Descrizione
Thread nel livello di trasporto	Il numero totale di thread in tutti i pool di thread del livello di trasporto.
Dimensioni pool di thread livello di trasporto	Il numero totale di thread livello di trasporto condivisi. Questi thread possono essere utilizzati da qualsiasi servizio ospitato in Adaptive Processing Server.
Processori disponibili	Il numero di processori disponibili per la Java Virtual Machine (JVM) in cui viene eseguito il server.
Memoria massima (MB)	La quantità massima di memoria, in megabye, che Java Virtual Machine tenterà di utilizzare
Memoria libera (MB)	La quantità di memoria, in megabyte, disponibile per l'allocazione di nuovi oggetti da parte di JVM.
Memoria totale (MB)	La quantità totale di memoria, in megabyte, in Java Virtual Machine. Questo valore può variare nel tempo, in base all'ambiente di host.
Percentuale utilizzo CPU (ultimi 5 minuti)	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.

Metrica	Descrizione
Percentuale utilizzo CPU (ultimi 15 minuti)	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.
Percentuale di sistema arrestato durante GC (ultimi 5 minuti)	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. 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.
Percentuale di sistema arrestato durante GC (ultimi 15 minuti)	Percentuale di sistema arrestato durante l'esecuzione di Garbage Collection (GC) negli ultimi quindici minuti. In questo stato, il codice dell'applicazione in esecuzione su Java Virtual Machine viene bloccato durante un'operazione critica di Garbage Collection che richiede accesso esclusivo. 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.
Numero di errori di pagina durante GC (ultimi 5 minuti)	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.
Numero di errori di pagina durante GC (ultimi 15 minuti)	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.

Metrica	Descrizione
Numero di GC completi	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.
Conteggio conflitti blocco JVM	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.
Informazioni debug JVM	Debug delle informazioni su SAP Java Virtual Machine, incluso lo stato, la porta e il client allegato, se disponibile.
Informazioni versione JVM	Informazioni di versione su SAP Java Virtual Machine.
Contatore thread in stallo JVM	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.
Flag analisi JVM	I flag di analisi correntemente attivati per JVM. Indica il livello di analisi di JVM.
Servizi	Un elenco separato da virgole dei servizi ospitati dal server.

Tabella 25 - 10: Metriche del servizio DSL Bridge

Metrica	Descrizione
DSLServiceMetrics.queryCount	Numero di richieste dati aperte tra i client e il servizio
DSLServiceMetrics.activeConnectionCount	Numero di connessioni correntemente aperte tra i client e il servizio.
DSLServiceMetrics.activeSessionCount	Numero di sessioni correntemente aperte tra i client e il servizio.
DSLServiceMetrics.activeOLAPConnection Count	Numero di connessioni correntemente aperte tra i client OLAP e il servizio.

Tabella 25 - 11: Metriche del servizio proxy controllo client

Metrica	Descrizione
Eventi di controllo ricevuti	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 25 - 12: Metriche del servizio di ricerca piattaforma

Metrica	Descrizione
Numero di tentativi di estrazione riusciti dall'avvio del servizio	Numero di tentativi di estrazione dei documenti riusciti dall'avvio del servizio di ricerca piattaforma.
Numero di tentativi di estrazione riusciti dall'avvio del servizio	Numero di tentativi di estrazione dei documenti riusciti dall'avvio del servizio di ricerca piattaforma.
Data/ora ultima generazione archivio contenuti	La data e l'ora in cui è stato generato l'ultimo archivio contenuti.
Numero di tentativi di estrazione non riusciti dall'avvio del servizio	Numero di tentativi di estrazione dei documenti non riusciti dall'avvio del servizio di ricerca piattaforma.
Servizio disponibile	TRUE se il servizio è disponibile. In caso contrario, FALSE.
Indicizzazione in esecuzione	TRUE se l'indicizzazione è in corso. In caso contrario, FALSE.
Numero di documenti indicizzati	Visualizza il numero di documenti indicizzati dall'avvio del servizio.

Tabella 25 - 13: Metriche del servizio di analisi multidimensionale

Metrica	Descrizione
Conteggio sessione	Numero corrente di connessioni dai client MDAS al server.
Conteggio cubi	Numero di origini dati utilizzate per fornire i dati alle connessioni non ancora scadute.

Metrica	Descrizione
Conteggio query	Numero di richieste dati aperte tra i client MDAS e il server.

Tabella 25 - 14: Metriche del servizio Data Federation

Metrica	Descrizione
Numero di query in esecuzione	Numero totale di query in esecuzione (che utilizzano memoria o meno).
Numero di connessioni	Numero totale di connessioni utente al motore delle query di Data Federation.
Byte totali trasferiti dalle origini dati	Quantità di dati letti dalle origini dati (in byte).
Record totali trasferiti dalle origini dati	Numero totale di righe lette dalle origini dati.
Byte totali prodotti dall'esecuzione query	Quantità di dati prodotti come output di query (in byte).
Record totali prodotti dall'esecuzione query	Numero totale di righe prodotte come output di query.
Numero di query che utilizzano memoria	Numero totale di query in esecuzione che utilizzano memoria.
Byte totali di memoria utilizzati dall'esecuzione query	Quantità di memoria attualmente utilizzata dalle query in esecuzione (in byte).
Byte totali di disco utilizzati dall'esecuzione query	Spazio sul disco attualmente utilizzato dalle query in esecuzione (in byte).
Numero di query che utilizzano il disco	Numero totale di query in esecuzione che utilizzano il disco.
Numero di query che attendono risorse	Numero totale di query in esecuzione attualmente in attesa di esecuzione.
Numero di thread attivi	Numero totale di thread attivi utilizzati per l'esecuzione delle richieste.
Byte totali di memoria utilizzati dalla cache di metadati	Quantità di memoria utilizzata per la cache di configurazione di metadati, statistiche e connettori (in byte).
Numero di query non riuscite	Numero totale di query non riuscite (eccezione generata).

Metrica	Descrizione
Numero di query nel passaggio di analisi query	Numero totale di query in esecuzione attualmente in fase di analisi.
Numero di query nel passaggio di ottimizzazione query	Numero totale di query in esecuzione attualmente in fase di ottimizzazione.
Numero di query nel passaggio di esecuzione query	Numero totale di query in esecuzione attualmente in funzione.
Numero di connettori caricati	Numero totale di connettori caricati nel servizio.
Numero di connessioni attive per i connettori caricati	Numero totale di connessioni attive per i connettori caricati nel servizio.
Il servizio Data Federation è disponibile	"TRUE" se il servizio è disponibile. In caso contrario, "FALSE".

25.1.7 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 25 - 15: Metriche del server del contenitore di applicazioni Web

Metrica	Descrizione
Elenco di connettori WACS in esecuzione	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.
Errore connettori WACS all'avvio	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

25.1.8 Metriche di Adaptive Job Server

Tabella 25 - 16: Metriche di Job Server

Metrica	Descrizione
Richieste processi ricevute	Il numero di processi che dovrebbero essere stati eseguiti sul server.
Processi simultanei	Il numero di processi che sono correntemente in esecuzione sul server. Se questo numero è alto, il server è occupato.
Processi di picco	Il numero massimo di processi simultanei che sono stati eseguiti contemporaneamente sul server. Questo numero non scende fino al riavvio del server.
Creazioni processi non riuscite	Il numero di processi non riusciti nel server.
Directory temporanea	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.
Impostazioni predefinite destinazione file system valide	"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".
Impostazioni predefinite destinazione FTP valide	"TRUE" se il server è in grado di inviare documenti alla destinazione FTP specificata nella schermata "Destinazione" del server. In caso contrario, "FALSE".
Impostazioni predefinite destinazione Posta in arrivo valide	"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".

Metrica	Descrizione
Impostazioni predefinite destinazione posta elettronica valide	"TRUE" se il server è in grado di inviare oggetti alla destinazione posta elettronica specificata nella schermata "Destinazione" del server. In caso contrario, "FALSE".
Servizi di pianificazione	Una tabella che visualizza i servizi in esecuzione sul server.
Elementi secondari	Una tabella che visualizza i processi secondari in esecuzione sul server.

Nella tabella che segue sono indicate le metriche per ogni servizio di pianificazione in esecuzione sul server.

Tabella 25 - 17: Metriche del servizio di pianificazione

Metrica	Descrizione
Servizio di pianificazione	Il nome del servizio.
Richieste processi ricevute	Il numero di processi che dovrebbero essere stati eseguiti nel servizio.
Processi simultanei	Il numero di processi che sono correntemente in esecuzione nel servizio. Se questo numero è alto, il servizio è occupato.
Processi di picco	Il numero massimo di processi simultanei che sono stati eseguiti contemporaneamente nel servizio.
N. massimo consentito processi simultanei	Il numero di processi indipendenti simultanei (processi secondari) consentiti dal server. Questo può essere specificato nella schermata "Proprietà" per il server.
Creazioni processi non riuscite	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 25 - 18: Metriche secondarie

Metrica	Descrizione
Servizio di pianificazione	Il nome dell'elemento secondario.
PID	L'identificatore del processo secondario.
Richieste processi ricevute	Il numero di processi che dovrebbero essere stati eseguiti nel processo secondario.
Processi simultanei	Il numero di processi che sono correntemente in esecuzione nel processo secondario. Generalmente, questo numero deve essere “1”.
Processi di picco	Il numero massimo di processi simultanei che sono stati eseguiti contemporaneamente nel processo secondario.
Numero max. processi consentiti	Il numero di processi simultanei consentiti dal processo secondario.
Errori di comunicazione	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.
Inizializzazione in corso	"TRUE" se il processo secondario è in fase di inizializzazione. In caso contrario, "FALSE".
Arresto in corso	"TRUE" se il processo secondario è in fase di arresto. In caso contrario, "FALSE".

25.1.9 Metriche di Crystal Reports Server

La tabella seguente descrive le metriche del server che vengono visualizzate nella schermata "Metriche" per i servizi di elaborazione Crystal Reports e i server di elaborazione Crystal Reports 2011.

Tabella 25 - 19: Metriche di Crystal Reports Processing Server

Metrica	Descrizione
Processi aperti	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.
Numero di richieste servite	Numero totale delle richieste servite dal server dopo l'avvio.
Numero di processi aperti	Il numero di processi attualmente elaborati dal server e dai suoi processi secondari.
Tipo oggetto	Il tipo di InfoObject gestito generalmente dal server. Il valore di questa metrica non cambia.
Tempo di elaborazione medio (ms)	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.
Tempo di elaborazione massimo (ms)	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.
Tempo di elaborazione minimo (msec)	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.
Numero di richieste in coda	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.
ObjectDllName	Il nome del plug-in di elaborazione per il server. Il valore di questa metrica non cambia.
Numero di connessioni aperte	Numero di connessioni attualmente aperte tra il server e i client.
Frequenza errori di richieste	La percentuale delle ultime 500 richieste ricevute che il server non è riuscito a elaborare.

Metrica	Descrizione
Dati trasferiti (KB)	Quantità totale di dati, in kilobyte, trasferiti ai client dopo l'avvio del server.
Numero di richieste non riuscite	Numero di richieste che il server non è stato in grado di completare dopo l'avvio.
MaxChildProcesses	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 25 - 20: Metriche di Crystal Reports Cache Server

Metrica	Descrizione
Riscontri cache (%)	La percentuale delle ultime 500 richieste servite con dati cache.
Server di elaborazione connessi	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.
Numero di richieste servite	Numero totale delle richieste servite dal server dopo l'avvio.
Tipo oggetto	Il tipo di InfoObject gestito generalmente dal server. Il valore di questa metrica non cambia.
Tempo di elaborazione medio (msec)	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.
Tempo di elaborazione massimo (msec)	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.
Tempo di elaborazione minimo (msec)	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.

Metrica	Descrizione
Numero di richieste in coda	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.
ObjectDllName	Il nome del plug-in di elaborazione per il server. Il valore di questa metrica non cambia.
Dimensione della cache	La quantità di dati, in kilobyte, attualmente memorizzati nella cache del server sul disco.
Numero di connessioni aperte	Numero di connessioni attualmente aperte tra il server e i client.
Dati trasferiti (KB)	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 2011.

Tabella 25 - 21: Metriche del Report Application Server di Crystal Reports 2011

Metrica	Descrizione
metric_currentdoccount	Numero di documenti attualmente elaborati dal server.
metric_totaldoccount	Numero di documenti elaborati dal server dal momento dell'avvio.
metric_currentagentthreadcount	Numero di thread attualmente elaborati dal server.
metric_totalagentthreadcount	Numero di thread elaborati dal server dal momento dell'avvio.

25.1.10 Metriche del server Web Intelligence

Tabella 25 - 22: Metriche del servizio di elaborazione di Web Intelligence

Metrica	Descrizione
Cache size (Kb)	La quantità totale di dati, in kilobyte, memorizzati nella cache.

Metrica	Descrizione
Number of out-of-date documents in cache	Il numero di documenti eliminati dalla cache poiché troppo vecchi dall'avvio del server.
Cache high mark count	Il numero massimo di volte in cui la cache ha raggiunto le dimensioni massime consentite sul server dall'avvio.
CPU usage (%)	La percentuale del tempo totale della CPU impiegata dal server dall'avvio.
Total CPU time (seconds)	Il tempo totale della CPU in secondi impiegato dal server dall'avvio.
Memory high threshold count	Il numero di volte in cui la soglia elevata di memoria è stata raggiunta sul server dall'avvio.
Memory max threshold count	Il numero di volte in cui la soglia massima di memoria è stata raggiunta sul server dall'avvio.
Virtual memory size (Mb)	La quantità totale di memoria, in megabyte, assegnata al server.
Current number of client calls	Il numero corrente di chiamate CORBA in elaborazione da parte del server.
Current number of tasks	Il numero corrente di attività in esecuzione sul server.
Total number of client calls	Il numero totale di chiamate CORBA ricevute dal server dall'avvio.
Total number of tasks	Il numero totale di attività eseguite sul server dall'avvio.
Idle time (seconds)	La quantità di tempo, in secondi, trascorsa dall'ultima richiesta ricevuta dal server da parte di un client.
Current number of active sessions	Il numero corrente di sessioni in grado di accettare richieste dai client.
Number of documents	Il numero di documenti attualmente aperti sul server.
Current number of sessions	Il numero corrente di sessioni create sul server.
Number of document swap	Il numero di documenti per i quali un thread di pulitura ha pianificato richieste di scambio.
Number of swapped documents	Il numero di documenti scambiati in seguito a richieste di scambio.

Metrica	Descrizione
Number of sessions timeout	Il numero di sessioni scadute a causa del mancato avvio del server.
Total number of sessions	Il numero di sessioni create sul server dall'avvio.
Number of users	Il numero totale di utenti collegati al server.

25.1.11 Metriche del server di Dashboard Design

Tabella 25 - 23: Metriche del server di elaborazione di Dashboard Design

Metrica	Descrizione
Processi aperti	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.
Numero di richieste servite	Numero totale delle richieste servite dal server dopo l'avvio.
Numero di processi aperti	Il numero di processi attualmente elaborati dal server e dai suoi processi secondari.
Tipo oggetto	Il tipo di InfoObject gestito generalmente dal server. Il valore di questa metrica non cambia.
Tempo di elaborazione medio (msec)	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.
Tempo di elaborazione massimo (msec)	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.

Metrica	Descrizione
Tempo di elaborazione minimo (msec)	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.
Numero di richieste in coda	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.
ObjectDllName	Il nome del plug-in di elaborazione per il server. Il valore di questa metrica non cambia.
Numero di connessioni aperte	Numero di connessioni attualmente aperte tra il server e i client.
Frequenza errori di richieste	La percentuale delle ultime 500 richieste ricevute che il server non è riuscito a elaborare.
Dati trasferiti (KB)	Quantità totale di dati, in kilobyte, trasferiti ai client dopo l'avvio del server.
Numero di richieste non riuscite	Numero di richieste che il server non è stato in grado di completare dopo l'avvio.
MaxChildProcesses	Il numero massimo di processi secondari simultanei consentiti sul server.

Tabella 25 - 24: Metriche del Cache Server

Metrica	Descrizione
Riscontri cache (%)	La percentuale delle ultime 500 richieste servite con dati cache.
Server di elaborazione connessi	Tabella che elenca i server di elaborazione di Dashboard Design nella propria distribuzione. La tabella include il nome del server e il numero di connessioni con il server attualmente aperte.
Numero di richieste servite	Numero totale delle richieste servite dal server dopo l'avvio.
Tipo oggetto	Il tipo di InfoObject gestito generalmente dal server. Il valore di questa metrica non cambia.

Metrica	Descrizione
Tempo di elaborazione medio (msec)	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.
Tempo di elaborazione massimo (msec)	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.
Tempo di elaborazione minimo (msec)	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.
Numero di richieste in coda	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.
ObjectDllName	Il nome del plug-in di elaborazione per il server. Il valore di questa metrica non cambia.
Dimensioni cache (KB)	La quantità di dati, in kilobyte, attualmente memorizzati nella cache del server sul disco.
Numero di connessioni aperte	Numero di connessioni ai client attualmente aperte.
Dati trasferiti (KB)	Quantità totale di dati, in kilobyte, trasferiti ai client dopo l'avvio del server.

Appendice: segnaposto per server e nodi

26.1 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 26 - 1: Segnaposto

Segnaposto	Descrizione	Valori predefiniti
%AAANALYTICS_EXE%	Il nome dell'eseguibile per il Dashboard Analytics Server.	In Windows, `AAAnalytics.exe`. In UNIX, `AAAnalytics`.
%AADASHBOARD_EXE%	Il nome dell'eseguibile per il Dashboard Server.	In Windows, `AADashboard.exe`. In UNIX, `AADashboard`.
%AuditingDatabaseConnection%	La connessione al database di controllo utilizzata dal CMS.	Questo valore viene specificato durante l'installazione.
%AuditingDatabaseDriver%	Il tipo di driver di database utilizzato per connettersi al database di controllo.	In Windows il valore predefinito è sqlserverauditdbss.
%BINDIR%	La cartella in cui risiedono i file binari della piattaforma BI per i sistemi a 64 bit.	In Windows, *<DIRINSTALLAZ>*`/Piattaforma SAP BusinessObjects Business Intelligence 4.0/win64_x64`. In UNIX, *<DIRINSTALLAZ>*/sap_bobj/enterprise_xi40/*<piattaforma>*/
%BINDIR32%	La cartella in cui risiedono i file binari della piattaforma BI per i sistemi a 32 bit.	In Windows, *<DIRINSTALLAZ>*`/Piattaforma SAP BusinessObjects Business Intelligence 4.0/win32_x86`. In UNIX, *<DIRINSTALLAZ>*/sap_bobj/enterprise_xi40/*<piattaforma>*/

Segnaposto	Descrizione	Valori predefiniti
%CACHESERVER_EXE%	Il nome dell'eseguibile per il Crystal Reports Cache Server.	In Windows, `crcache.exe`. In UNIX, `boe_crcached`.
%CMS_EXE%	Il nome dell'eseguibile per il Central Management Server.	In Windows, `cms.exe`. In UNIX, `boe_cmsd`.
%CONNECTIONSERVER32_EXE%	Il nome dell'eseguibile per il Connection Server a 32 bit.	In Windows, `ConnectionServer32.exe`. In UNIX, `ConnectionServer32`.
%CONNECTIONSERVER_DIR%	La cartella principale del Connection Server.	In Windows, *<DIRINSTALLAZ>*/Piattaforma SAP BusinessObjects Business Intelligence 4.0/dataAccess/connectionServer. In UNIX, *<DIRINSTALLAZ>*/sap_bobj/enterprise_xi40/*<piattaforma>*.
%CONNECTIONSERVER_EXE%	Il nome dell'eseguibile per il Connection Server a 64 bit.	In Windows, `ConnectionServer.exe`. In UNIX, `ConnectionServer`.
%CR2011_BINDIR%	La directory in cui risiedono i file binari del server Crystal Reports 2011 server.	In Windows *<DIRINSTALLAZ>*/SAP BusinessObjectsEnterprise XI 4.0/win32_x86.
%CR2011_DefaultWorkingDir%	La directory operativa predefinita per i server Crystal Reports 2011.	In Windows *<DIRINSTALLAZ>*/SAP BusinessObjectsEnterprise XI 4.0/win32_x86.
%CRYSTALRAS_EXE%	Il nome dell'eseguibile per il Report Application Server.	In Windows, `crystalras.exe`. In UNIX, `boe_crystalrasd`.
%CR_ODBCINI%	Il nome e il percorso del file `.odbc.ini`.	In UNIX, *<DIRINSTALLAZ>*/bobje/odbc.ini . In Windows si tratta di una stringa vuota.
%CommonJavaBundlesDir%	La cartella in cui risiedono i raggruppamenti di OSGI condivisi.	In Windows, *<DIRINSTALLAZ>*/Piattaforma SAP BusinessObjects Business Intelligence 4.0/java/bundles. In UNIX, *<DIRINSTALLAZ>*/sap_bobj/enterprise_xi40/java/bundles.

Segnaposto	Descrizione	Valori predefiniti
%CommonJavaLibDir%	La cartella in cui risiedono le librerie Java comuni.	In Windows, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/java/lib`. In UNIX, `<DIRINSTALLAZ>/sap_bobje/enterprise_xi40/java/lib`.
%DLLEXT%	Estensione predefinita di un file `.dll` o `.so`.	In Windows, `.dll`. In UNIX, `.so`.
%DLLPATH%	Il nome della variabile di ambiente nel computer in cui è installata la piattaforma BI che specifica le directory in cui l'interprete cercherà i file eseguibili.	In Windows, “Path”. In UNIX, “LD_LIBRARY_PATH”.
%DLLPATH32%	Nei sistemi Solaris a 32 bit, il nome della variabile di ambiente nel computer in cui è installata la piattaforma BI che specifica le directory in cui l'interprete cercherà i file eseguibili.	Nel computer Solaris “LD_LIBRARY_PATH_32”. Questo segnaposto corrisponde a una stringa vuota in altri sistemi operativi.
%DLLPATH64%	Nei sistemi Solaris a 32 bit, il nome della variabile di ambiente nel computer in cui è installata la piattaforma BI che specifica le directory in cui l'interprete cercherà i file eseguibili.	Nei computer Solaris “LD_LIBRARY_PATH_64”. Questo segnaposto corrisponde a una stringa vuota in altri sistemi operativi.
%DLLPREFIX%	Prefisso predefinito di un file `.dll` o `.so`.	In UNIX “lib”. Questo segnaposto corrisponde a una stringa vuota nei computer Windows.
%DLLPRELOAD%	Nome della variabile d'ambiente LD_PRELOAD per la piattaforma.	In UNIX, LD_PRELOAD. Questo segnaposto corrisponde a una stringa vuota nei computer Windows.
%DLLPRELOAD32%	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.
%DLLPRELOAD64%	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.
%DP%	Il delimitatore di percorso.	In Windows, “;”. In UNIX, “:”.

Segnaposto	Descrizione	Valori predefiniti
%DefaultAuditingDir%	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, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/Auditing`. In UNIX, `<DIRINSTALLAZ>/sap_bobj/data/Auditing/`.
%DefaultDataDir%	La directory temporanea utilizzata da Job Server.	In Windows, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/Data`. In UNIX, `<DIRINSTALLAZ>/sap_bobj/data/`.
%DefaultInputFRSDir%	La cartella principale dell'Input File Repository Server.	In Windows, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/FileStore/Input`. In UNIX, `<DIRINSTALLAZ>/sap_bobj/data/frsinput`.
%DefaultLoggingDir%	La posizione di archiviazione dei file di registro.	In Windows, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/logging`. In UNIX, `<DIRINSTALLAZ>/sap_bobj/logging`.
%DefaultOutputFRSDir%	La cartella principale dell'Output File Repository Server.	In Windows, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/FileStore/Output`. In UNIX, `<DIRINSTALLAZ>/sap_bobj/data/frsoutput`.
%DefaultWorkingDir%	La directory operativa per i server a 64 bit	In Windows `<DIRINSTALLAZ>/SAP BusinessObjectsEnterprise XI 4.0/win64_x64`. In UNIX, `<DIRINSTALLAZ>/sap_bobj/enterprise_xi40/<piattaforma>`.

Segnaposto	Descrizione	Valori predefiniti
%DefaultWorkingDir32%	La directory operativa per i server a 32 bit.	In Windows, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/win32_x86`. In UNIX, `<DIRINSTALLAZ>/sap_bobj/enterprise_xi40/<piattaforma>`.
%EPM_LD_PRELOAD_ONCE%	Nome della variabile d'ambiente LD_PRELOAD_ONCE per la piattaforma.	$LD_PRELOAD_ONCE$
%EVENTSERVER_EXE%	Il nome dell'eseguibile per l'Event Server.	In Windows, `EventServer.exe`. In UNIX, `boe_eventsd`.
%EXEEXT%	Estensione predefinita dei file eseguibili.	In Windows, `.exe`. Questo segnaposto non è disponibile in UNIX.
%EXEPATH%	Il nome della variabile di ambiente nel computer in cui è installata la piattaforma BI che specifica le directory in cui l'interprete cercherà i file eseguibili.	In Windows, “Path”. In UNIX, “PATH”.
%EnterpriseDir%	La posizione in cui è installata la piattaforma BI a 64 bit.	In Windows, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/`. In UNIX, `<DIRINSTALLAZ>/sap_bobj/enterprise_xi40/`.
%EnterpriseDir32%	La posizione in cui è installata la piattaforma BI a 32 bit.	In Windows, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/`. In UNIX, `<DIRINSTALLAZ>/sap_bobj/enterprise_xi40/`.
%ExternalJavaLibDir%	La cartella in cui risiedono le librerie Java esterne e di terze parti.	In Windows, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/java/lib/external`. In UNIX, `<DIRINSTALLAZ>/sap_bobje/enterprise_xi40/java/lib/external`.

Segnaposto	Descrizione	Valori predefiniti
%FILESERVER_EXE%	Il nome dell'eseguibile per il File Server.	In Windows, `fileserver.exe`. In UNIX, `boe_filesd`.
%HOARD_PATH%	La posizione del gestore della memoria.	Per impostazione predefinita il segnaposto è vuoto.
%HOARD_PRELOAD%	Specifica se precaricare il gestore della memoria.	Per impostazione predefinita il segnaposto è vuoto.
%INSTALLROOTDIR%	La cartella in cui è installata la piattaforma BI a 64 bit.	Questo valore viene specificato durante l'installazione.
%INSTALLROOTDIR32%	La cartella in cui è installata la piattaforma BI a 32 bit.	Questo valore viene specificato durante l'installazione.
%IntroscopeAgentEnableInstrumentation%	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 BI.
%IntroscopeAgentEnterpriseManagerHost%	Il nome host dell'Introscope Agent Enterprise Manager al quale vengono inviati i dati di strumentazione.	Questo valore viene specificato durante l'installazione.
%IntroscopeAgentEnterpriseManagerPort%	La porta dell'Introscope Agent Enterprise Manager alla quale vengono inviati i dati di strumentazione.	Questo valore viene specificato durante l'installazione.
%IntroscopeAgentEnterpriseManagerTransport%	Il trasporto utilizzato per l'invio dei dati di strumentazione all'Introscope Agent Enterprise Manager. I valori consentiti sono: • TCP • HTTP • HTTPS • SSL	TCP
%IntroscopeAgentEnterpriseManagerTransportHTTP%	La classe utilizzata per l'invio dei dati di strumentazione all'Introscope Agent Enterprise Manager mediante HTTP.	com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportHTTPS%	La classe utilizzata per l'invio dei dati di strumentazione all'Introscope Agent Enterprise Manager mediante HTTPS.	com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory

Segnaposto	Descrizione	Valori predefiniti
%IntroscopeAgentEnterpriseManagerTransportSSL%	La classe utilizzata per l'invio dei dati di strumentazione all'Introscope Agent Enterprise Manager mediante SSL.	com.wily.isengard.postofficehub.link.net.SSLSocketFactory
%IntroscopeAgentEnterpriseManagerTransportTCP%	La classe utilizzata per l'invio dei dati di strumentazione all'Introscope Agent Enterprise Manager mediante TCP.	com.wily.isengard.postofficehub.link.net.DefaultSocketFactory
%IntroscopeDir%	La cartella in cui è installato Introscope Agent Enterprise Manager.	In Windows, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/java/wily`. In UNIX, `<DIRINSTALLAZ>/sap_bobje/enterprise_xi40/java/wily`.
%JAVAW_EXE%	Il nome del file eseguibile per Java Virtual Machine che non dispone di finestra della console.	In Windows, `javaw.exe`. In UNIX, `java`.
%JAVA_EXE%	Il nome dell'eseguibile di Java Virtual Machine.	In Windows, `java.exe`. In UNIX, `java`.
%JOBSERVERCHILD_EXE%	Il nome dell'eseguibile per l'Adaptive Job Server secondario.	In Windows, `JobServerChild.exe`. In UNIX, `boe_jobcd`.
%JOBSERVER_EXE%	Il nome dell'eseguibile per l'Adaptive Job Server.	In Windows, `JobServer.exe`. In UNIX, `boe_jobsd`.
%JdkBinDir%	La cartella in cui risiedono i file binari JDK.	In Windows, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/sapjvm/bin`. In UNIX `<DIRINSTALLAZ>/sap_bobje/<PIATTAFORMA>/sapjvm/bin`.
%JreBinDir%	La cartella in cui risiedono i file binari JRE.	In Windows, `<DIRINSTALLAZ>/javasdk/bin`. In UNIX `<DIRINSTALLAZ>/sap_bobje/<PIATTAFORMA>/sapjvm/jre/bin`.

Segnaposto	Descrizione	Valori predefiniti
%JVM_ARCH_ENVIRONMENT%	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.
%JVM_HEADLESS_MODE%	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
%JVM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%	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"
%JVM_SHARED_MEMORY_SEGMENT%	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.
%LANGUAGEPACKSDIR%	La cartella in cui sono installate le lingue di distribuzione.	In Windows e UNIX, *<DIRINSTALLAZ>*.
%LANGUAGEPACKSDIR32%	La cartella in cui sono installate le lingue di distribuzione sui sistemi a 32 bit.	In Windows e UNIX, *<DIRINSTALLAZ>*.
%LSTDir%	La cartella in cui sono archiviati i file di configurazione LST.	In Windows, *<DIRINSTALLAZ>*`/Piattaforma SAP BusinessObjects Business Intelligence 4.0/conf/lst`. In UNIX, *<DIRINSTALLAZ>*`/sap_bobj/enterprise_xi40/conf/lst`.
%MDAS_JVM_OS_STACK_SIZE%	Specifica le dimensioni dello stack della JVM per il servizio di analisi multidimensionale.	Per impostazione predefinita, il segnaposto è vuoto.
%NCSInstrumentLevelThreshold%	Il livello di soglia della registrazione di analisi per la libreria NCS.	Il valore viene determinato durante l'installazione.
%PAGESERVER_EXE%	Il nome dell'eseguibile per il server di elaborazione Crystal Reports 2011.	In Windows, `crproc.exe`. In UNIX, `boe_crprocd.bin`.

Segnaposto	Descrizione	Valori predefiniti
%PJSContainerDir%	La cartella in cui risiedono i file JARS del contenitore APS.	In Windows, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/java/pjs/container`. In UNIX `<DIRINSTALLAZ>/sap_bobj/enterprise_xi140/java/pjs/container`.
%PJSServicesDir%	La cartella in cui risiedono i file JARS del servizio APS.	In Windows, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/java/pjs/services`. In UNIX `<DIRINSTALLAZ>/sap_bobj/enterprise_xi140/java/pjs/services`.
%Platform%	Il sistema operativo del computer in cui è in esecuzione la piattaforma BI.	Il sistema operativo del computer in cui è in esecuzione la piattaforma BI.
%Platform32%	Il sistema operativo del computer in cui è in esecuzione la piattaforma BI a 32 bit.	Il sistema operativo del computer in cui è in esecuzione la piattaforma BI.
%RasBinDir%	La cartella principale del Report Application Server.	In Windows, `<DIRINSTALLAZ>/Piattaforma SAP BusinessObjects Business Intelligence 4.0/win32_x86`. In UNIX, `<DIRINSTALLAZ>/sap_bobj/enterprise_xi40/<PLATFORM>/ras`.
%SERVER_FRIENDLY_NAME%	Nome completo del server.	Nome completo del server.
%SERVER_NAME%	Nome completo del server.	Nome completo del server.
%SMDAgentHost%	Il nome host di SDM Agent al quale vengono inviati i dati di strumentazione.	Questo valore viene specificato durante l'installazione.
%SMDAgentPort%	La porta di SDM Agent alla quale vengono inviati i dati di strumentazione.	Questo valore viene specificato durante l'installazione.

Segnaposto	Descrizione	Valori predefiniti
%TRACE_CONFIGFILE_INI%	Il nome e il percorso del file `BO_Trace.ini`.	In Windows *<DIRINSTALLAZ>*`/Piattaforma SAP BusinessObjects Enterprise 4.0/logging/logConfig/BO_Trace.ini`. In UNIX *<DIRINSTALLAZ>*`/sap_bobj/enterprise_xi140/conf/BO-trace.ini`.
%WEBI_LD_PRELOAD%	Nome della variabile d'ambiente LD_PRELOAD per la piattaforma.	$LD_PRELOAD$
%WEBISERVER_EXE%	Il nome dell'eseguibile per Web Intelligence Processing Server.	In Windows, `wireportserver.exe`. In UNIX, `WIReportServer`.
%WEBI_LD_PRELOAD_ONCE%	Nome della variabile d'ambiente LD_PRELOAD_ONCE per la piattaforma.	$LD_PRELOAD_ONCE$
%XCCACHE_EXE%	Il nome dell'eseguibile per la server cache di Dashboard Design.	In Windows, `xccache.exe`. In UNIX, `boe_xccached`.
%XCPROC_EXE%	Il nome dell'eseguibile del server di elaborazione di Dashboard Design.	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

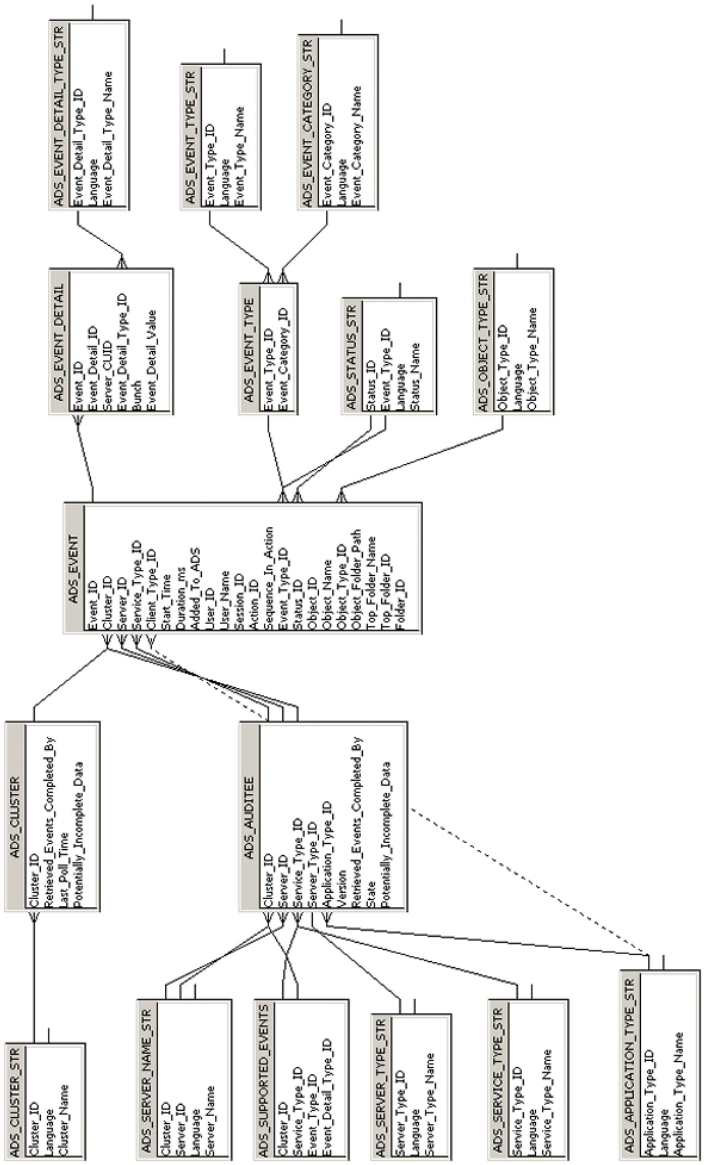
- Visualizzazione e modifica dei segnaposto per un nodo

Appendice: schema archivio dati di controllo

27.1 Presentazione

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.

27.2 Diagramma schema



27.3 Tabelle dell'archivio dati di controllo

Tabella ADS_EVENT

Questa tabella contiene le proprietà di base per ciascun evento, 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 nella tabella ADS_Auditee	GUID del cluster di controllo. Viene restituito perché più cluster potrebbero utilizzare lo stesso archivio dati di controllo.
Server_ID	Carattere (64)	Chiave esterna nella tabella ADS_Auditee	CUID del server che ha attivato l'evento.
Service_Type_ID	Carattere (64)	Chiave esterna nella tabella ADS_Auditee	• CUID del tipo di servizio che ha attivato l'evento. I servizi presenti su un server utilizzano il proprio CUID del tipo di servizio. • Le applicazioni client (ad esempio BI Launch Pad o Web Intelligence) registreranno il proprio CUID del tipo di applicazione.
Client_Type_ID	Carattere (64)	Chiave esterna nella tabella 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 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 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.

Nome colonna	Tipo di campo	Chiave	Descrizione
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 nella tabella ADS_Event_type	Tipo di evento (ad esempio Visualizza o Salva)
Status_ID	INTEGER	Chiave esterna nella tabella ADS_Status_Str	Stato dell'operazione (ad esempio, "0" = riuscita, "1" = non riuscita).
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 nella tabella 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_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)	Chiave esterna in ADS_Event	GUID dell'evento superiore.
Event_Detail_Type_ID	INTEGER	Chiave esterna in ADS_Event_Detail_Str	Tipo di dettaglio di evento.
Gruppo	INTEGER	N/D	Se il dettaglio fa parte di una serie, viene utilizzato per raggruppare i dettagli. 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: • Nome prompt: Paese • Valore prompt: USA Il gruppo 2 è costituito da: • Nome prompt: Stato • Valore prompt: California • Valore prompt: Nevada
Event_Detail_Value	Carattere (testo lungo)	N/D	Il valore del dettaglio di evento.

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.

Nome colonna	Tipo	Chiave	Descrizione
Server_ID	Carattere (64)	• Chiave primaria • ADS_Server_Name_STR	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)	• Chiave primaria • ADS_Service_Type_Str • ADS_Supported_Events	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)	ADS_Server_Type_Str	CUID del tipo di server per il server che ha attivato l'evento.
Application_Type_ID	Carattere (64)	ADS_Application_Type_Str	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_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 *EN* o *DE*.
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 *EN* o *DE*.
Service_Type_Name	Carattere (255)	N/D	Nome del tipo di servizio.

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 *EN* o *DE*.
Application_Type_Name	Carattere (255)	N/D	Nome di testo del tipo di applicazione, ad esempio Crystal Reports o Web Intelligence.

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 in ADS_Event_Type	ID per il tipo di evento restituito, ad esempio l'ID di Salva.
Event_Detail_Type_ID	INTEGER	ADS_EVENT_DETAIL_TYPE_STR	CUID che identifica il tipo di dettaglio di evento acquisito per quell'evento (ad esempio, Percorso file).

Tabella ADS_CLUSTER

Questa tabella contiene informazioni su tutti i cluster che contengono sistemi controllati.

Nome colonna	Tipo	Chiave	Descrizione
Cluster_ID	Carattere (64)	• Chiave primaria • ADS_Cluster_Str	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.
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.

Nome colonna	Tipo	Chiave	Descrizione
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 **Dati potenzialmente incompleti**, 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)	N/D	Codice per l'impostazione della lingua per il cluster, ad esempi `EN` o `DE`.
Cluster_Name	Carattere (255)	N/D	Indica il nome del cluster.

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	Composita • Chiave primaria • ADS_Event_Type_Str	Identificatore univoco per il tipo di evento.
Event_Catagory_ID	INTEGER	Tabella ADS_Event_Category_Str	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 *EN* o *DE*.
Event_Type_Name	Carattere (255)	N/D	Nome di testo del tipo di evento, ad esempio Visualizza o Accesso.

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 *EN* o *DE*.
Event_Category_Name	Carattere (255)	N/D	Nome della categoria dell'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 *EN* o *DE*.
Event_Detail_Type_Name	Carattere (255)	N/D	Nome di testo del tipo di dettaglio evento.

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 *EN* o *DE*.
Object_Type_Name	Carattere (255)	N/D	Nome del tipo di oggetto.

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 *EN* o *DE*.
Status_Name	Carattere (255)	N/D	Descrizione di testo dello stato dell'evento, ad esempio Riuscito o Non riuscito.

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.

Ulteriori informazioni

Informazioni	Posizione
Informazioni sul prodotto SAP BusinessObjects	http://www.sap.com
SAP Help Portal	Passare a http://help.sap.com/businessobjects/ e nel pannello laterale "SAP BusinessObjects Overview" fare clic su **All Products**. 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. 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.
SAP Service Marketplace	http://service.sap.com/bosap-support > Documentazione • Guide all'installazione: https://service.sap.com/bosap-instguides • Note sulla versione: http://service.sap.com/releasenotes 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.
Docupedia	https://cw.sdn.sap.com/cw/community/docupedia Docupedia fornisce ulteriori risorse di documentazione, un ambiente di creazione collaborativo e un canale di feedback interattivo.

Informazioni	Posizione
Risorse per lo sviluppatore	https://boc.sdn.sap.com/ https://www.sdn.sap.com/irj/sdn/businessobjects-sdklibrary
Articoli su SAP BusinessObjects relativi a SAP Community Network	https://www.sdn.sap.com/irj/boc/businessobjects-articles Questi articoli erano conosciuti in precedenza come schede tecniche.
Note	https://service.sap.com/notes Queste note erano conosciute in precedenza come articoli di knowledge base.
Forum su SAP Community Network	https://www.sdn.sap.com/irj/scn/forums
Formazione	http://www.sap.com/services/education 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	http://service.sap.com/bosap-support 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	http://www.sap.com/services/bysubject/businessobjectsconsulting I consulenti sono a disposizione dei clienti dalla fase di analisi iniziale fino alla consegna del progetto di distribuzione. Possono essere fornite co nsulenze su argomenti quali i database relazionali e multidimensionali, la connettività, gli strumenti di progettazione del database e la tecnologia di incorporamento personalizzata.

Indice

Caratteri speciali

.NET Software Development Kit (SDK) 31

A

abilitazione
  server 364, 365
accesso 113
  applicazioni 482
  BI Launch Pad 104, 482
  CMC 482
  connessioni universo 521
  gruppi 103
  gruppi server 376
  pannello HTML query 491
  personalizzazione 511
  Posta in arrivo 104
  protezione contro tentativi di accesso non autorizzati 149
  server 376
  utenti 103
  workflow 73
account di servizio
  configurazione dei server 258
  delega 255
  impostazione 255
account di servizio, diritti 256
  concessione 257
account Guest
  disabilitazione 100
account sistema 283
account SMAdmin 748
account utente
  creazione 94
  eliminazione 96
  gestione 89, 94
  modifica 96
  predefinita 89
Adaptive Job Server 19, 42, 814, 871
  opzioni della riga di comando 772
  Timeout del socket 653
Adaptive Processing Server 19, 42, 530, 814
affinità, e SSL 146
Agente di monitoraggio 543
aggiornamenti 40
aggiunta 369
  CMS 370
  membri del cluster 369
aggiunta *(segue)*
  server 366
  sottogruppi 98
  utenti ai gruppi 100
albero di spostamento
  server 353
alias
  assegnazione a utenti 110
  creazione 109
    per nuovi utenti 108
    per utenti esistenti 109
  disabilitazione 111
  eliminazione 110
  gestione 108
alias utente 110
  assegnazione 110
  creazione 109
    per nuovi utenti 108
    per utenti esistenti 109
  disabilitazione 111
  eliminazione 110
ambienti di rete
  IPv4
    nodi IPv4/IPv6 doppi 387
  IPv6 387
ambito dei diritti 119
amministrazione
  applicazioni 482
  assegnazione dei diritti di 350
  BI Launch Pad 482
  CMC 482
  delega 137
  diritti 137
  gruppi 103
  Posta in arrivo 104
  server e gruppi server 376
  utenti 103
amministrazione delegata 137
analisi 67
analisi end-to-end 752
Analysis, versione OLAP 71
API remota JMX 541
applicazioni 481
  proprietà 496, 592
  Ricerca piattaforma 496, 592
applicazioni Web BEx 514
architettura 25, 527
  Ricerca piattaforma 587
architettura, diagramma 26
attendibilità, relazione di trust attiva 145
attributi, token di accesso 146
autenticazione 36
  Autenticazione affidabile 221
  azienda 218
  LDAP 233, 234
  plug-in di protezione 215
  primario 214
  server del contenitore di applicazioni Web (WACS) 440
  tipi 92
  Windows AD 251
autenticazione affidabile 513
  configurazione di esempio 229
  proprietà 225
Autenticazione affidabile 221
  SAML 224
  utente principale 232
autenticazione principale 214
autenticazione SAP 283
  opzioni CMC 287
autorizzazione, sistemi 285
autorizzazioni
  applicazione 691
  diritti in piattaforma BI 661
  per i servizi Information Platform 283
  per l'accesso ai dati SAP 691
  workbench per l'amministrazione dei contenuti 667
avvio automatico di server 363
Avvisi 492
  diritti 804
  gestione 492
  gestione delle impostazioni 492
  proprietà di destinazione 493
  proprietà predefinite 494

B

backup della piattaforma BI
  impostazioni server 459
backup di SAP BusinessObjects Enterprise
  impostazioni server 461
BackupCluster.bat 461
backupcluster.sh 461
BI Launch Pad
  accesso 104
  configurazione 104
  controllo accesso a 482
  diritti 797

BI Launch Pad *(segue)*
gestione 491
personalizzazione dell'accesso 511
preferenze per i gruppi 105, 106
bilanciamento del carico 146
aggiunta di un server CMS 370
clustering 369
e protezione distribuita 146
server del contenitore di applicazioni Web (WACS) 449
BOLMT 86, 359
Business view manager 62
BW
attivazione della visualizzazione 676
integrazione con piattaforma BI 661

C

CA Wily Introscope 38
cacert.der 164, 165
Cache Server 770, 771
cakey.pem 164, 165
cartelle
diritti 784
diritti relativi agli oggetti ereditarietà 117
categorie 106
diritti 784
Categorie di dati di monitoraggio 543
categorie di servizio 51, 353
CCM
abilitazione e disabilitazione dei server 364, 365
aggiunta di un server 366
avvio, interruzione e riavvio dei server 361, 363
eliminazione di un server 368
nodi 395
aggiunta 397
credenziali utente, modifica 416
eliminazione 403
ricreazione 400
ridenominazione 405
spostamento 407
per UNIX 753, 756
per Windows 762, 764
ccm.config 757
ccm.exe 762, 764
ccm.sh 753, 756
ripristino impostazioni server 466
Central Configuration Manager (CCM) 21, 66
Central Management Console (CMC) 21, 69
Central Management Server 19, 42
Central Management Server.Vedere CMS. 283
chiavi cluster 154
file dbinfo 155
panoramica 155
reimpostazione in UNIX 157
reimpostazione in Windows 156
chiavi del registro 245
chiavi di crittografia 154
CMC 159
contrassegno come compromesse 162
creazione di una nuova 161
elenco degli oggetti 161
revoca 163
stato 160
ClearCase 40
client
Business view manager 62
Data Federator:vedere Strumento di amministrazione di Data Federation 65
desktop 61
Information Design Tool 64
Information Designer:vedere Information Design Tool 64
SAP BusinessObjects Analysis, versione per Microsoft Office 67
SAP BusinessObjects Dashboard Design 68
SAP Crystal Reports 68
Strumento di amministrazione di Data Federation 65
Strumento di conversione dei report 63
strumento Web Service Query 63
Translation Management Tool 64
Universe Design Tool 63
Web 61
Web Intelligence Desktop 62
widget per piattaforma SAP BusinessObjects Business Intelligence 65
client basati su browser 61
client desktop 61
client Web 61
client, basati su browser 69
Analysis, versione OLAP 71
BI Launch Pad 70
Central Management Console (CMC) 21, 69
report, visualizzatori 71
SAP BusinessObjects Mobile 72
SAP BusinessObjects Web Intelligence 71
client, basati su browser *(segue)*
spazi di lavoro BI 70
client, desktop
Central Configuration Manager (CCM) 21, 66
Repository Diagnostic Tool 22, 67
Upgrade Management Tool 22, 67
clonazione
server 367, 368
server del contenitore di applicazioni Web (WACS) 433
cluster 369, 371
aggiunta di un server CMS 370
modifica di nomi 372
nodi 369
visualizzazione dettagli 379
Cluster Definition, strumento 679, 684
CMC
abilitazione e disabilitazione dei server 364, 365
avvio, interruzione e riavvio dei server 361, 362
chiavi di crittografia 159
clonazione dei server 367, 368
controllo accesso a 482
dipendenze dei server Windows, aggiunta 415
diritti 797
eliminazione di un server 368
gestione dei server 353
CMS 283, 314, 530
abilitazione e disabilitazione di altri server 364, 365
aggiunta a un cluster 370
autenticazione 214
avvio 364
clustering 369, 371
installazione di un membro cluster 371
requisiti 369
come server dei nomi 392, 393
configurazione 392, 393, 419, 420, 421, 422
interruzione 364
metriche 379
modifica del nome di un cluster 372
opzioni della riga di comando 767
porta predefinita 392, 393
proprietà 814
protezione distribuita 146
risoluzione dei problemi 364
risoluzione dei problemi dei computer multi-home 392
variabili di sessione 147
autenticazione 214
registrazione 147

CMS, database di sistema 419, 420, 464
backup 458
copia 423, 424
eliminazione 421, 422
modifica della password 419
ricreazione 421, 422
ripristino 462, 463, 464
selezione 419, 420
cmsdbsetup.sh 757
codice di licenza 86, 358
acquisti 85, 358
aggiunta 86, 358
panoramica 85, 357
utilizzo misurazione 86, 359
visualizzazione 85, 358
codici di licenza
migrazione di database CMS 423
codifica, token di accesso 146
componenti 679, 684
Cluster Definition, strumento 679, 684
computer multi-home 389
server del contenitore di applicazioni Web (WACS) 451
comunicazione 214
tra browser e server di applicazioni Web 214
tra server della piattaforma BI 171
condivisione di istanze 648, 650
configurazione 538
Apache 2.2 203
Autenticazione affidabile 222
cluster 369
cluster CMS 372
CMS, database 419, 420
database di sistema CMS 421, 422
firewall 181, 182
ISA 2006 204
livello applicazione 382
livello di elaborazione 382
livello intelligence 382
modelli configurazione 384
nodi 369
più server 384
Secure Sockets Layer 724
server reverse proxy 202, 203
WebSEAL 6.0 203
configurazione controllo, vedere controllo 557
configurazione di Kerberos 258
configurazione OpenSearch 591
configurazione reverse proxy 592
conflitti tra oggetti
replica bilaterale 641, 643
replica unilaterale 641
Connection Server 530
Connection Server 32 530
connessioni origini dati 521
connessioni remote
creazione 631
creazione di cartelle 631
modifica 633
protezione 633
visualizzazione 630
connessioni universo
diritti 795
eliminazione 521
gestione 521
replica 625
Connettività 546
Connettività InfoSet, trasporto 679
Connettività Open SQL 679
Connettività Open SQL, trasporto 679
console di gestione del ciclo di vita
strumento della riga di comando BIAR 471
Contextual Awareness 721
configurazione 721, 723
conti
gestione 89, 94
Servizi Information Platform 283
controllo
architettura 551
attività Web 149
configurazione 557
controllo archivio dati
diagramma schema 891
tabelle schema 892
dettagli eventi 570, 579, 582, 583, 584
eventi
configurazione 559
elenco di 563
proprietà e dettagli 563
retention del database 561
eventi comuni 570
eventi di Analyzer 583
eventi di Lifecycle Management Console 584
eventi piattaforma 579
eventi Web Intelligence 582
flusso di informazioni 551
ID dettaglio evento 570, 579, 582, 583, 584
ID tipo di evento 570, 579, 582, 583, 584
impostazioni di connessione al database 561
metriche 557
pagina CMC 557
proprietà eventi 570, 582, 583, 584
controllo *(segue)*
riepilogo stato 557
tipi di evento
accesso 570
Aggiungi VMS 584
Archivia VMS 584
attivazione 570
Blocca VMS 584
connessione cubo MDAS 583
consegna 570
creazione 570
disconnessione 570
drill fuori dal livello 582
eliminazione 570
esecuzione 570
Esporta VMS 584
Estrai VMS 584
livello di accesso personalizzato modificato 579
modifica 570
modifica controllo 579
modifica dei diritti 579
pagina recuperata 582
prompt 570
Recupera VMS 584
recupero 570
ricerca 570
rollback 584
salvare 570
Sblocca VMS 584
sessione MDAS 583
visualizzazione 570
Controllo 525
controllo delle versioni 40
controllo licenza 86, 359
procedura 87, 359
cookie 147
registrazione delle sessioni 147
token di accesso 146
copia
livelli di accesso 131
creazione
account utente 94
gruppi 97
livelli di accesso 132
sottogruppi di server 375
credenziali utente, modifica per i nodi 416
cruscotto 525
Crystal Reports
diritti 786
vedere SAP Crystal Reports 68
Crystal Reports 2010 Report Application Server 530
Crystal Reports Cache Server 530

Crystal Reports Viewer SDK 31
CTS Transport (CTS+) 38
custom.jsp 512

D

daemon, gestione dei segnali 767
Dashboard Analytics Server 530, 814
    opzioni della riga di comando 780
Dashboard Builder 70
Dashboard Server 530, 814
    opzioni della riga di comando 780
database 27
    accesso con Single Sign-On 217
    inizializzazione del CMS 421, 422
    selezione per il CMS 419, 420
    universo 34
    visualizzazioni 35
database di controllo 458
Database di tendenza 527
dati
    dinamici 130
    permanente 40
    salvati 130
dati permanenti 40
dati, accesso
    panoramica sull'installazione 678
Definizione cluster, trasporto 679, 684
destinazione RFC 665
    per il gateway SAP locale 666
    per il servizio Publisher BW 665
diagramma, architettura 26
dinamici, dati 130
dipendenze dei server
    aggiunta 415
    Registro eventi 415
    Remote Procedure Call 415
diritti 113, 350, 781
    ambito dei diritti 119
    amministrazione 137, 140
    applicazioni 482
    assegnazione ai principali 124
    Avvisi 804
    BI Launch Pad 482, 797
    cartelle 784
    cartelle di livello superiore 125
    categorie 784
    CMC 482, 797
    connessioni universo 795
    Crystal Reports 786
    diritti
        replica 616, 617, 618, 620, 621
    diritti avanzati 114, 124
    diritti del proprietario 140
    diritti di amministrazione 350
    diritti di pubblicazione 351
diritti *(segue)*
    diritti effettivi 122
    documenti Web Intelligence 786
    ereditarietà 115
        cartella 117
        gruppo 116
        interruzione 135
    Explorer 805
    generale 781
    gestione 122
    gestione della protezione 616, 617, 618, 620, 621
    gruppi 103, 788
    gruppi server 376
    Information Design Tool 803
    limitazione dell'ambito 119
    livelli di accesso 114, 789
        attività 128
        gestione tra siti 134
        modifica dei diritti inclusi 133
        query di relazione 134
        replicati 134
    Mobile 808
    note 785
    override dei diritti 118
    Posta in arrivo 104
    query protezione 125, 126
    Report Application Server 377
    server 376
    spazi di lavoro BI 790, 798
    specifici del tipo 120
    Strategy Builder 801
    Universe Design Tool 802
    universi (.unv) 791
    universi (.unx) 792
    utenti 103, 788
    Visualizza e Visualizza su richiesta 130
    visualizzazione 123
    Web Intelligence 798
    widget 804
diritti avanzati 114, 122, 124
diritti del proprietario 140
diritti effettivi 122
diritti specifici
    spazi di lavoro BI 790, 798
disabilitazione
    account Guest 100
    alias 111
    server 364, 365
Discussions
    gestione delle impostazioni 488
distribuzione
    Publisher BW, componenti 664

E

Editor definizione Protezione trasporto 679, 683
elaborazione, livello 382
elenchi di controllo di accesso
    aggiunta di principali 124
    visualizzazione 123
elenchi di replica
    creazione 627, 628
    gestione 629
    modifica 629, 630
    oggetti supportati 626
    opzioni di dipendenza 627, 628
elenchi scopi consentiti ai certificati 437
elenco degli errori di indicizzazione 607
eliminazione 421, 422
    account utente 96
    alias 110
    connessioni universo 521
    database di sistema CMS 421, 422
    gruppi 99
    livelli di accesso 132
    server 368
    server del contenitore di applicazioni Web (WACS) 434
    universi 522
eliminazione mappatura ruoli 318, 350
Enterprise Resource Planning (ERP) 37
env.sh 760
ereditarietà 115
    cartella 117
    gruppo 116
    interruzione 135
    limitazioni 119
    override dei diritti 118
ereditarietà cartelle 117
    override dei diritti 118
estensioni di elaborazione 151
    condivisione 487
    registrazione 486
estensioni, elaborazione 151
Event Server 530, 814
    opzioni della riga di comando 779
Explorer 603
    diritti 805
    vedere SAP BusinessObjects Explorer 68
Explorer autorizzazioni 123

F

facet 601

federazione 611
aggiornamento dall'origine 621, 622, 623
aggiornamento dalla destinazione 621, 622, 623
connessioni remote 630
creazione 631
modifica 633
elenchi di replica 626
cartelle 627
creazione 627, 628
gestione 629
eliminazione oggetti 638, 639, 640
gestione della protezione 616, 617, 618, 620, 621
gestione di conflitti 641, 643
importazione e promozione di contenuto replicato 651, 652
istanze eseguite localmente 648, 649
livelli di accesso 134
miglioramento delle prestazioni 656
modalità di replica 621, 622, 623
pianificazione remota 648, 649, 650
procedure consigliate 653
processi di replica 633
creazione 634
modifica 637
pianificazione 636, 637
reindirizzamento di siti di destinazione 651, 653
replica bilaterale 621, 622, 623
replica di oggetti di grandi dimensioni 653
replica unilaterale 621, 622, 623
risoluzione dei problemi 657
servizi Web 646, 647
termini 612
utenti e gruppi di terze parti, replica 624
vantaggi 611
visualizzazione di registri 637
file di certificati 164, 165, 436
file di chiavi 164, 165
file di registro di controllo 458
file di risposta 322
applicazione 324
creazione 322
file di risposta PeopleSoft 327
parametri 327
file host, configurazione per il firewall NAT 184
File Repository Server 19, 42, 814
backup 458
opzioni della riga di comando 777
File Repository Server *(segue)*
ripristino 462, 463
file system
backup 458
ripristino 467
file WAR BOE 104
firewall 148
comunicazione server 171
configurazione 181, 182
integrazione JD Edwards EnterpriseOne 194
integrazione per Oracle E-Business 196
integrazione SAP 192
integrazione Siebel 199
integrazioni PeopleSoft Enterprise 197
debug 185, 186
imposizione della registrazione dei server tramite nome 394
scenari di configurazione 186
server del contenitore di applicazioni Web (WACS) 450

G

gateway SAP 307
distribuzione dei componenti 664
e SNC 307
installazione 665
pubblicazione mediante un gateway locale 665
Generatore agente 543
gestione del ciclo di vita
strumento della riga di comando motore BIAR 475
gestione delle applicazioni 481
file war BOE 502
thread di discussione, eliminazione 490
Grafico di tendenza 525
gruppi 293
aggiunta di sottogruppi 98
aggiunta di utenti 100
assegnazione dei diritti a 124
concessione dell'accesso 103
controllo dei diritti 125, 126
creazione 97
diritti 788
ereditarietà 116
interruzione dell'ereditarietà 135
override dei diritti 118
per cartelle di livello superiore 125
eliminazione 99
gruppi *(segue)*
gestione 91
mappatura 315, 333, 339, 345
modifica 97
predefinita 91
preferenze di BI Launch Pad 105
responsabili crittografia 158
specifica dell'appartenenza ai gruppi 99
visualizzazione
diritti 123
membri 98
gruppi di terze parti, replica 624
gruppi server
accesso 376
creazione 374
nodi 353
sottogruppi 375
sottogruppi di server 373, 375
GWSETUP 665

H

host
configurazione di LDAP 235, 241
HTTP 147, 214
HTTPS
configurazione di server del contenitore di applicazioni Web (WACS) 435, 438, 450

I

Importazione guidata
vedere Upgrade Management Tool 22, 67
impostazioni
Avvisi 492
BI Launch Pad 491
cartelle di livello superiore, diritti 125
Discussions 488
impostazioni di memoria
modifica in un server del contenitore di applicazioni Web (WACS) 454
impostazioni predefinite
porte 392, 393
server 386
impostazioni server
backup 459, 460, 461
ccm.sh
backup impostazioni server 460
ripristino 464, 465, 466
indicizzazione 587
Information Design Tool 64

Information Design Tool, diritti 803
InfoView 70
initlaunch.sh 761
inizializzazione di un database di sistema CMS 421, 422
Input File Repository 19, 42, 530, 814
installazione
gateway SAP in Windows 665
livelli di protezione predefiniti 662
INSTALLDIR 18
integrazione
SAP 38
SNC 307
integrazione in fase di ricerca con NWES 603
intelligence, livello 382
interfaccia di rete
risoluzione dei problemi 391
interfaccia di rete non primaria 391
interfaccia di rete primaria 391
internazionalizzazione 35
Introscope 546
invio della notifica 528
IPv6
CMC 386
impostazione di indirizzi in CMC 388
opzioni 386
ISA 2006
configurazione per Oracle 10gR3 209
configurazione per Sun Java 8.2 209
configurazione per Tomcat 5.5 209
configurazione per WebSphere CE 2.0 209
iView
attivazione della visualizzazione 676

J

JAAS, file di configurazione 261, 262, 443
Java Application Server, Kerberos 259
Java Management Extensions (JMX) 527
Java Software Development Kit (SDK) 31
Java, Kerberos 264, 265
JD Edwards EnterpriseOne 37
JD Edwards EnterpriseOne, integrazione
configurazione firewall 194

K

Kerberos 259, 442
e NetWeaver SSO 262
file di configurazione 259, 260, 442
Krb5.ini 261, 443
risoluzione dei problemi 281, 445
Single Sign On per Java 448
Single Sign On per Java InfoView 266
KPI (Key Performance Indicator) 525
Krb5.ini 261, 443

L

launch pad BI 70
LDAP
account 233
risoluzione dei problemi 250
autenticazione 233
configurazione 235
configurazione Single Sign On 244
gruppi
mappatura 246
host
configurazione 235, 241
gestione multipla 239
mapping a Windows AD 249
plug-in di autenticazione 234
plug-in di protezione 234
Secure Sockets Layer (SSL) 233
librerie condivise, come estensioni di elaborazione 151
librerie di collegamento dinamico, estensioni di elaborazione 151
Lifecycle Management (LCM) 39
Lifecycle Management Console
strumento della riga di comando
motore BIAR 473, 480
Lightweight Directory Access ProtocolVedere LDAP 233
limitazione
ambito dei diritti 119
limitazioni 151
accesso 150
account guest 151
password 150
utente 150
lingue 35
Live Office
configurazione per server reverse proxy 206
livelli 41
livelli di accesso 114, 122, 137
amministrazione 137
assegnazione ai principali 124
livelli di accesso *(segue)*
attività, diritti richiesti 128
copia 131
creazione 132
diritti 789
eliminazione 132
gestione tra siti 134
modifica dei diritti in 133
predefiniti 128
RAS 377
relazioni con gli oggetti 134
ridenominazione 132
Visualizza e Visualizza su richiesta 130
visualizzazione 123
livello applicazione 382
livello più elevato
cartelle, diritti 125
livello registro di analisi
impostazione server CMC 729, 730
localizzazione 35
logon.csp 214

M

macchine multi-homed 390
mappatura dei ruoli 293, 315, 333, 339, 345
MBean JMX 543
MBeans 527
metrica 528
metriche
visualizzazione 378
metriche globali del sistema 379
metriche server 855
Metriche del Central Management Service
Account utente simultanei esistenti 858
Account utente specifici esistenti 858
Connessione al database di controllo stabilita 858
Connessioni database di sistema stabilite 858
Connessioni database di sistema utilizzate correntemente 858
Data build 858
Durata ultimo ciclo di polling del thread di controllo (secondi) 858
Licenze utente simultanee 858
Licenze utenti specifici 858
Nome connessione database di controllo 858
Nome connessione database di sistema 858
Nome origine dati 858
Nome server database di sistema 858
Nome utente database di controllo 858

metriche server *(segue)*
Metriche del Central Management Service *(segue)*
Nome utente database di sistema 858
Numero build 858
Numero di accessi utente dall'avvio 858
Numero di commit dall'avvio 858
Numero di oggetti nel database di sistema di CMS 858
Numero di oggetti nella cache di sistema di CMS 858
Numero di query dall'avvio 858
Numero di sessioni stabilite da tutti gli utenti 858
Numero di sessioni stabilite da utenti simultanei 858
Numero di sessioni stabilite da utenti specifici 858
Numero di sessioni stabilite dai server 858
Numero massimo di sessioni utente dall'avvio 858
Processi completati 858
Processi in attesa 858
Processi in esecuzione 858
Processi in sospeso 858
Processi non riusciti 858
Richieste database di sistema in sospeso 858
Server CMS cluster 858
Strumento di controllo CMS 858
Tempo di risposta a commit più lungo dall'avvio (msec) 858
Tempo di risposta alle query più lungo dall'avvio (msec) 858
Tempo medio di risposta a commit dall'avvio (msec) 858
Tempo medio di risposta alle query dall'avvio (msec) 858
Ultimo aggiornamento database di controllo 858
Utilizzo thread di controllo 858
Versione prodotto 858
Versione risorsa 858
metriche del File Repository Server
Connessioni attive 864
Dati inviati (MB) 864
Dati scritti (MB) 864
Elenco di file attivi 864
File attivi 864
Spazio su disco disponibile nella directory principale (%) 864
Spazio su disco disponibile nella directory principale (GB) 864
Spazio su disco libero nella directory principale (GB) 864

metriche server *(segue)*
metriche del File Repository Server *(segue)*
Spazio su disco totale nella directory principale (GB) 864
metriche del Server del contenitore di applicazioni Web
Elenco di connettori WACS in esecuzione 870
Errore connettori WACS all'avvio 870
Metriche del server di Dashboard Design
Dati trasferiti (KB) 878
Dimensioni cache (KB) 878
Frequenza errori di richieste 878
MaxChildProcesses 878
Numero di connessioni aperte 878
Numero di processi aperti 878
Numero di richieste in coda 878
Numero di richieste non riuscite 878
Numero di richieste servite 878
ObjectDllName 878
Processi aperti 878
Riscontri cache (%) 878
Tempo di elaborazione massimo (msec) 878
Tempo di elaborazione medio (msec) 878
Tempo di elaborazione minimo (msec) 878
Tipo oggetto 878
Metriche del server Web Intelligence
Cache high mark count 876
Cache size (Kb) 876
CPU usage (%) 876
Current number of active sessions 876
Current number of client calls 876
Current number of sessions 876
Current number of tasks 876
Idle time (seconds) 876
Memory high threshold count 876
Memory max threshold count 876
Number of document swap 876
Number of documents 876
Number of out-of-date documents in cache 876
Number of sessions timeout 876
Number of swapped documents 876
Number of users 876
Total CPU time (seconds) 876
Total number of client calls 876
Total number of sessions 876
Total number of tasks 876
Virtual memory size (Mb) 876
metriche di Adaptive Job Server
Arresto in corso 871
Creazioni processi non riuscite 871
Directory temporanea 871
Elementi secondari 871

metriche server *(segue)*
metriche di Adaptive Job Server *(segue)*
Errori dicomunicazione 871
Impostazioni predefinite destinazione file system valide 871
Impostazioni predefinite destinazione FTP valide 871
Impostazioni predefinite destinazione posta elettronica valide 871
Impostazioni predefinite destinazione Posta in arrivo valide 871
Inizializzazione 871
N. massimo consentito processi 871
N. massimo consentito processi simultanei 871
PID 871
Processi di picco 871
Processi simultanei 871
Richieste processi ricevute 871
Servizi di pianificazione 871
Servizio di pianificazione 871
Metriche di Adaptive Processing Server
Byte totali di disco utilizzati dall'esecuzione query 865
Byte totali di memoria utilizzati dall'esecuzione query 865
Byte totali di memoria utilizzati dalla cache di metadati 865
Byte totali prodotti dall'esecuzione query 865
Byte totali trasferiti dalle origini dati 865
Contatore thread in stallo JVM 865
Conteggio conflitti blocco JVM 865
Conteggio cubi 865
Conteggio query 865
Conteggio sessione 865
Data/ora ultima generazione archivio contenuti 865
Data/ora ultimo aggiornamento indice 865
Dimensioni pool di thread livello di trasporto 865
DSLServiceMetrics.activeConnectionCount 865
DSLServiceMetrics.activeOLAPConnectionCount 865
DSLServiceMetrics.activeSessionCount 865
DSLServiceMetrics.queryCount 865
Eventi di controllo ricevuti 865
Flag analisi JVM 865
Il servizio Data Federation è disponibile 865
Indicizzazione in esecuzione 865
Informazioni debug JVM 865
Informazioni versione JVM 865
Memoria libera (MB) 865
Memoria massima (MB) 865
Memoria totale (MB) 865
Numero di connessioni 865

metriche server *(segue)*
Metriche di Adaptive Processing Server *(segue)*
Numero di connessioni attive per i connettori caricati 865
Numero di connettori caricati 865
Numero di documenti indicizzati 865
Numero di errori di pagina durante GC (ultimi 15 minuti) 865
Numero di errori di pagina durante GC (ultimi 5 minuti) 865
Numero di GC completi 865
Numero di query che attendono risorse 865
Numero di query che utilizzano il disco virtuale 865
Numero di query che utilizzano memoria 865
Numero di query in esecuzione 865
Numero di query nel passaggio di analisi query 865
Numero di query nel passaggio di esecuzione query 865
Numero di query nel passaggio di ottimizzazione query 865
Numero di query non riuscite 865
Numero di tentativi di estrazione non riusciti dall'avvio del servizio 865
Numero di tentativi di estrazione riusciti dall'avvio del servizio 865
Numero di thread attivi 865
Percentuale di sistema arrestato durante GC (ultimi 15 minuti) 865
Percentuale di sistema arrestato durante GC (ultimi 5 minuti) 865
Percentuale utilizzo CPU (ultimi 15 minuti) 865
Percentuale utilizzo CPU (ultimi 5 minuti) 865
Processori disponibili 865
Record totali prodotti dall'esecuzione query 865
Record totali trasferiti dalle origini dati 865
servizi 865
Servizio disponibile 865
Thread nel livello di trasporto 865
metriche di Connection Server
Origini dati 863
Metriche di Crystal Reports Server
Connessioni attualmente aperte 873
Dati trasferiti (KB) 873
Dimensione della cache 873
Frequenza errori di richieste 873
MaxChildProcesses 873
Numero di connessioni aperte 873
Numero di richieste in coda 873
Numero di richieste non riuscite 873
ObjectDllName 873
Processi aperti 873
Processi report attualmente aperti 873
Richieste servite 873
metriche server *(segue)*
Metriche di Crystal Reports Server *(segue)*
Riscontri cache (%) 873
Tempo di elaborazione massimo (msec) 873
Tempo di elaborazione medio (msec) 873
Tempo di elaborazione minimo (msec) 873
Tipo oggetto 873
metriche di Event Server
Elenco di file monitorati 863
File monitorati 863
visualizzazione 378
metriche server, informazioni
metriche comuni
CPU 855
Dimensione disco (GB) 855
Directory di registrazione 855
Indirizzo IP host 855
Nome host 855
Nome macchina 855
Nome registrato 855
Ora locale 855
PID 855
Porta richiesta 855
RAM (MB) 855
Server dei nomi 855
Sistema operativo 855
Spazio su disco utilizzato (GB) 855
Thread server occupato 855
Tipo CPU 855
Versione 855
metriche di controllo
Numero corrente degli eventi di controllo in coda 855
metriche virtuali 530
MIME
diritti 808
modalità conforme a FIPS
attivazione in UNIX 153
attivazione in Windows 153
disattivazione in Windows 154
Federal Information Processing Standard 152
impostazione protezione 152
modalità di configurazione 321
modalità di esecuzione 321
modelli configurazione 384
applicazione 385
impostazione 384
procedure consigliate 384
ripristino dei valori predefiniti di sistema 386
modelli di protezione predefiniti 662
monitoraggio 525

N

Network Address Translation
configurazione, file host server 184
nodi 19, 42, 395
aggiunta 396, 410
a un cluster 371
AddNode.bat 397
addnode.sh 399
CCM 397
CMS 370
nuovo computer 396
serverconfig.sh 398
clustering 369
CMC 353
eliminazione 403, 410
CCM 403
serverconfig.sh 404
ricreazione 410
AddNode.bat 401
addnode.sh 402
CCM 400
RemoveNode.bat 404
removenode.sh 404
scenari 400
serverconfig.sh 402
ridenominazione 405
CCM 405
serverconfig.sh 406
spostamento 407, 413
CCM 407
MoveNode.bat 408
movenode.sh 409
serverconfig.sh 408
note, diritti 785
notifica 527
numeri porta
conflitti 453, 454
modifica 392, 393
server del contenitore di applicazioni Web (WACS) 453
numero di accessi, token di accesso 146
numero di minuti, token di accesso 146

O

ODBC
CMS, database connettività 423
oggetti
diritti 661, 781
impostazione 124
visualizzazione 123

oggetti gestiti 321
gruppi BusinessObjects Enterprise 321, 325
ruoli PeopleSoft 321, 325
universi 321, 326
oggetti programma
abilitazione, disabilitazione 485, 486
autenticazione 485
oggetti report
diritti 786
diritti per la creazione/modifica 377
OpenDocument
personalizzazione dell'accesso 511
OpenSearch 590
OpenSearch mediante WDeploy 591
opzioni della riga di comando 765, 766, 780
Adaptive Job Server 772
Cache Server 770, 771
CMS 767
Dashboard Analytics Server 780
Dashboard Server 780
Event Server 779
Input e Output File Repository Server 777
SSL 164
opzioni delle modalità di aggiornamento, per Federation 621, 623
ora violazione 528
Oracle
JAAS 261
Kerberos 259
opzioni Java 264
Oracle E-Business Suite 37
mappatura dei ruoli a Servizi Information Platform 345
Oracle E-Business Suite, integrazione
configurazione firewall 196
Oracle EBS
aggiornamento degli alias 348
aggiornamento dei ruoli 348
Output File Repository 19, 42, 530, 814

P

pannello HTML query, diritti di accesso 491
panoramica 587
parametri script, nodi
aggiunta 410
eliminazione 410
ricreazione 410
spostamento 413
password 419, 420
limitazioni 150
modifica 101
opzioni 102, 220
per il database CMS 419
PeopleSoft Analytic Server 718
PeopleSoft Enterprise 37
PeopleSoft Enterprise, integrazione
configurazione firewall 197
percorso directory di installazione 395
Personal Security Environment
vedere PSE . 297
personalizzazione dell'accesso
BI Launch Pad 511
OpenDocument 511
pianificazione remota 648, 650
piattaforma BI
cartelle di livello superiore, diritti 125
comunicazione tra i server 171
consigli relativi alla sicurezza 144
distribuzione con server proxy inverso 201
importazione dei ruoli 293
mappatura dei ruoli 339
pianificazione ripristino d'emergenza 143
processo di autenticazione principale 214
server del contenitore applicazioni Web (WACS) 427
piattaforma BI, server
configurazione dei file host per il firewall 184
configurazione di Kerberos e browser 259
piattaforma SAP BusinessObjects Business Intelligence
backup e ripristino 458
diagramma dell'architettura 26
piattaforma SAP BusinessObjects Business Intelligence, backup 457, 458
impostazioni server 460
piattaforma SAP BusinessObjects Business Intelligence, ripristino 457
piattaforma SAP BusinessObjects Business Intelligence, SDK 31
piattaforma SAP BusinessObjects Business Intelligence, SDK Consumer 31
piattaforma SAP BusinessObjects Business Intelligence, widget 65
Platform Java Server 527
PLATFORM64DIR 18
PlatformServices.properties 371
plug-in
protezione 36
plug-in, protezione 215
PM Repository Server 530
Ponte di protezione per PeopleSoft EPM
file di risposta 322
Posta in arrivo
controllo accesso a 104
prestazioni 525
bilanciamento del carico 146
cluster 369
principali
assegnazione dei diritti a 124
assegnazione di diritti avanzati 124
controllo dei diritti 125, 126
diritti, per cartelle di livello superiore 125
visualizzazione di diritti 123
probe 528
Probe 525
processi di replica
creazione 634
modifica 637
opzioni di configurazione 634
pianificazione 636, 637
visualizzazione 633
processo PSANALYTIC 718
processo PSAPPSRV 718
profilo, parametri 307
protezione 36, 321, 350, 662
applicazione 324
cartella 661
cartelle di livello superiore 125
controllo dell'attività Web 149
da browser a server Web 148
distribuita 146
estensioni di elaborazione 151
firewall 148
gestione 122
gestione delle impostazioni 325
impostazioni di importazione 321
in piattaforma BI 661
limitazioni 150
limitazioni all'account Guest 151
limitazioni per l'utente 150
limitazioni relative all'accesso 150
limitazioni relative alle password 150
modelli predefiniti 662
oggetti dell'universo 794
personalizzazione dei diritti 350
plug-in 36, 215
protezione contro tentativi di accesso non autorizzati 149
protezione dell'ambiente 148

protezione *(segue)*
query 125, 126
registrazione delle sessioni 147
relazione di trust attiva 145
server Web 148
protezione a livello di riga, estensioni di elaborazione 151
protezione dati
chiavi cluster 154
chiavi di crittografia 154
compatibilità con le versioni precedenti 152
crittografia 154
crittografia a due chiavi 152
crittografia, chiavi 154
modalità conforme a FIPS 152
modalità di elaborazione dati predefinita 152
panoramica 152
protezione di oggetti universo 794
protezione, plug-in 215, 283
autenticazione LDAP 234
autenticazione Windows AD 252
Protocollo RMI 538
PSE
attendibilità lato server 297
configurazione dell'accesso 304
pubblicazione
definizione dei ruoli per, in BW 667
impostazione 666
in background 675
in più sistemi della piattaforma BI 670
pianificazione in background 675
più report mediante i ruoli 672
report in modalità batch 676
report in un ruolo o un sistema 672
suggerimenti di amministrazione 380
pubblicazione, assegnazione dei diritti di 351
Publisher BW
configurazione come servizio 664
configurazione su UNIX 664
distribuzione dei componenti 664
Publisher BW, servizio 664
avvio 664
configurazione 664
creazione di una destinazione RFC 665

Q

query
protezione 125, 126
Query come servizio Web
vedere Strumento Query servizio Web 63
query di relazione
per livelli di accesso 134

R

registrazione 379, 751
attività server 379
attività Web 149
registrazione, sessioni 147
registro di analisi
livelli 483, 727
Registro eventi 379, 415
relazione di trust attiva 145
Remote Method Invocation (RMI) 527
Remote Procedure Call 415
replica
oggetti 611
utenti e gruppi di terze parti 624
replica bilaterale 621, 622
replica unilaterale 621, 622
report
aggiornamento di origini dati 675
eliminazione 675
pubblicazione 672
in modalità batch 676
Report Application Server
diritti richiesti per gli oggetti 377
opzioni della riga di comando 773
Report Engine SDK 31
report, manutenzione 675
report, visualizzatori 71
Repository Diagnostic Tool 22, 67
requisiti
clustering 369
responsabili crittografia 158
aggiunta di membri 158
restart.sh 760
RestoreCluster.bat 466
restorecluster.sh 466
reverse proxy, server
configurazione con la piattaforma BI 203
configurazione di Apache 2.2 203
configurazione di ISA 2006 204
configurazione di WebSEAL 6.0 203
configurazione speciale 206
cookie di sessione 209
distribuzione con la piattaforma BI 201
distribuzione con un server del contenitore di applicazioni Web 450
reverse proxy, server *(segue)*
Live Office 211
servizi Web 206, 207, 208
supportate 201
Tomcat 206, 207
URL visualizzatore 211
utilizzo con server del contenitore di applicazioni Web (WACS) 450
riavvio dei server 361, 362, 363
ricerca 488, 587
thread di discussione 488
Ricerca dalla funzionalità di ricerca di NetWeaver Enterprise 605
Ricerca piattaforma 496, 592
ridenominazione, livelli di accesso 132
riga di comando, opzioni 776, 779
Report Application Server 773
Server di elaborazione 770, 771
tutti i server 766
ripristino 464
valori predefiniti di sistema 386, 455
ripristino d'emergenza,pianificazione 143
ripristino della piattaforma BI
impostazioni server 465
ripristino della piattaforma SAP BusinessObjects Business Intelligence
database di sistema CMS 462
file system 462, 467
impostazioni server 464, 466
ripristino di SAP BusinessObjects Enterprise
database di sistema CMS 463
risoluzione dei problemi 607
account LDAP 250
Impostazione di Kerberos 281
Kerberos 445
messaggi di errore 657
server del contenitore di applicazioni Web (WACS) 452
Single Sign On 245
risoluzione dei problemi delle interfacce di rete 392
ruoli 315, 333, 339, 345, 667
assegnazione dei diritti a 350
creazione per l'amministrazione 667
eliminazione mappatura 318, 350
importazione 293
mappatura 293, 315, 318, 333, 335, 339, 345
rimappatura 341

S

salvati, dati 130
SAML
  SSO 224
SAP
  aggiornamento degli alias 294
  aggiornamento dei ruoli 294
  configurazione firewall 192
  integrazione 38
SAP Business Explorer 514
SAP BusinessObjects Analysis, versione per Microsoft Office 67
SAP BusinessObjects Dashboard Design 68
SAP BusinessObjects Enterprise
  analisi 727
  diritti 113
SAP BusinessObjects Explorer 68, 495
  gestione delle impostazioni 495
  proprietà dell'applicazione 495
SAP BusinessObjects Mobile 72
SAP BusinessObjects SDK 151
SAP BusinessObjects Web Intelligence 71
SAP Crystal Reports 68
SAP ERP 37
SAP Passport 752
SAP Solution Manager 38
  panoramica 743
  SLD 745
  SMD 747
SAPGENPSE 304
script di gestione dei nodi, percorso 395
script UNIX, panoramica 753
Script Windows, panoramica 761
script, Windows 761
SCRIPTDIR 18
scripts, UNIX 753
SDK
  Ricerca piattaforma 590
  SDK Servizi Web 32
  vedere Software Development Kit 31
SDK RAS 31
Secure Network Communication
  client e server 297
  configurazione dei server 304
  configurazione SAP 298
  generazione PSE 302
  gruppi server 305
  impostazione dell'ambiente 302
  impostazioni CMC 305
  libreria di crittografia SAP 297
  pubblicazioni multi-pass 306
Secure Network Communication *(segue)*
  server BusinessObjects Enterprise 297
  workflow 301
Secure Network Communication (SNC), integrazione con
  configurazione per SNC 307
Secure Sockets Layer (SSL) 148, 164, 166, 167, 168, 233
  e bilanciamento del carico 146
  e LDAP 233
Secure Sockets Layer, configurazione 724
segnali, gestione 767
segnaposto 881
  strumentazione 750
segnaposto nodi 881
segnaposto server 881
segno di spunta verde, per il sistema predefinito 670
Semafori 525
server 28
  Abilita autenticazione del client 814
  Abilita HTTP tramite proxy 814
  Abilita HTTPS 814
  abilitazione 364, 365
  accesso 376
  aggiunta 366
  albero di spostamento 353
  Alias certificato 814
  Associa a nome host o indirizzo IP 814
  Associa a tutti gli indirizzi IP 814
  avvio 361, 362, 363
    automatico 361, 362
  clonazione 367, 368
  comunicazione 171
  concessione diritti account utente 256, 257
  configurazione 382
  configurazione dei server per l'uso di account di servizio 258
  Connessioni richieste al database di sistema 814
  contrasto con i servizi 19, 42
  Dimensioni massime intestazione HTTP 814
  Directory archivio file 814
  Directory temporanea 814
  disabilitazione 364, 365
  elenco 353
  eliminazione 368
  gestione dei segnali UNIX 767
  impostare indirizzo IP 388
server *(segue)*
  impostazione account di servizio 255
  impostazioni del server Web Intelligence
    Soglia inferiore memoria 849
    Soglia massima memoria 849
    Soglia superiore memoria 849
  impostazioni predefinite 386
  impostazioni relative alle prestazioni 383
  indirizzo IPv6 388
  interruzione 361, 362, 363
  Intervallo di polling eventi 814
  Intervallo di svuotamento 814
  Livello di registrazione 814
  modelli configurazione 384
    applicazione 385
    impostazione 384
  modifica 360
    stato 360, 361
  modifica dell'appartenenza di gruppo 376
  N. massimo richieste simultanee 814
  nodi 19, 42
  nome host 388
  Nome host proxy 814
  Numero max. processi simultanei 814
  Numero max. richieste secondarie 814
  Numero max. tentativi per l'accesso file 814
  Offset porta 814
  opzioni della riga di comando standard 766
  opzioni di identificazione host 387
  Password di accesso alle chiavi private 814
  Password di accesso alle chiavi private dell'elenco degli scopi consentiti ai certificati 814
  Percorso file elenco scopi consentiti ai certificati 814
  Porta 814
  Porta HTTP 814
  Porta HTTPS 814
  Porta proxy 814
  Porta server dei nomi 814
  Posizione file bscLogin.conf 814
  Posizione file elenco scopi consentiti ai certificati 814
  Posizione file Krb5.ini 814
  proprietà 383

server *(segue)*
proprietà comuni del server
Assegna automaticamente 811
Avvia automaticamente questo server all'avvio di Server Intelligence Agent 811
Identificatori host 811
Imposta modello configurazione 811
Livello di registrazione 811
Porta richiesta 811
Ripristina valori predefiniti di sistema 811
Usa modello configurazione 811
proprietà dei servizi applicazioni Web BEx
conteggio connessione server JCo 838
destinazione RFC server JCo 838
host gateway server JCo 838
Numero massimo sessioni client 838
SAP BW Master System 838
servizio gateway server JCo 838
proprietà dei servizi Data Federation
Connessioni max 840
dimensione pool di esecuzione 840
Timeout inattività connessione 840
Timeout inattività istruzione 840
proprietà dei servizi di analisi multidimensionali
Numero massimo di celle restituite da una query 838
Numero massimo di membri restituiti durante il filtraggio 838
Numero massimo sessioni client 838
proprietà dei servizi di Dashboard Design
Argomenti Java VM 850
Argomenti VM elemento secondario Java 850
Condividi dati tra i client 850
Consenti ai processi report di rimanere connessi al database fino alla chiusura del processo report 850

server *(segue)*
proprietà dei servizi di Dashboard Design *(segue)*
Dati meno recenti forniti ai client su richiesta (secondi) 850
Dimensioni cache massime (KB) 850
Durata massima dei processi per elemento secondario 850
Numero massimo di elementi secondari preavviati 850
Numero max. processi simultanei 850
Record di database letti durante l'anteprima o l'aggiornamento 850
Timeout cache di protezione (minuti) 850
Timeout connessione inattiva 850
Timeout connessione inattiva (minuti) 850
Timeout processo inattivo 850
proprietà dei servizi principali
Abilita autenticazione del client 814
Abilita HTTP tramite proxy 814
Abilita HTTPS 814
Alias certificato 814
Associa a nome host o indirizzo IP 814
Associa a tutti gli indirizzi IP 814
Connessioni richieste al database di sistema 814
Dimensioni massime intestazione HTTP 814
Directory archivio file 814
Directory temporanea 814
Intervallo di polling eventi 814
Intervallo di svuotamento 814
Livello di registrazione 814
N. massimo richieste simultanee 814
Nome host proxy 814
Numero max. processi simultanei 814
Numero max. richieste secondarie 814
Numero max. tentativi per l'accesso file 814
Offset porta 814
Password di accesso alle chiavi private 814

server *(segue)*
proprietà dei servizi principali *(segue)*
Password di accesso alle chiavi private dell'elenco degli scopi consentiti ai certificati 814
Percorso file elenco scopi consentiti ai certificati 814
Porta 814
Porta HTTP 814
Porta HTTPS 814
Porta proxy 814
Porta server dei nomi 814
Posizione file bscLogin.conf 814
Posizione file elenco scopi consentiti ai certificati 814
Posizione file Krb5.ini 814
Protocollo 814
Riconnessione automatica al database di sistema 814
Scadenza Single Sign-On 814
Tempo massimo di inattività 814
Tentativo massimo 814
Timeout connessione inattiva 814
Timeout di avvio servizio 814
Timeout inattività oggetti transitori 814
Timeout scambio motore di visualizzazione (in secondi) 814
Timeout svuotamento motore di visualizzazione (in secondi) 814
Tipo archivio certificati 814
URL endpoint dell'agente JMX predefinito (IIOP) 814
Proprietà di Connection Server
Abilita analisi middleware 825
Abilita analisi processo 825
Abilita raggruppamento HTTP 825
Attiva origine dati 825
Database 825
Dimensioni blocco HTTP 825
Intervallo timer oggetti transitori 825
Livello rete 825
Raggruppamento delle connessioni 825
Timeout Connection Pool 825
Timeout inattività oggetti transitori 825

server *(segue)*
proprietà di Crystal Reports Server
Argomenti Java VM 829
Argomenti VM elemento secondario Java 829
Condividi dati dei report tra i client 829
Consenti ai processi report di rimanere connessi al database fino alla chiusura del processo report 829
Dati meno recenti forniti ai client su richiesta 829
Dimensione dati da sfogliare 829
Dimensioni batch 829
Dimensioni cache massime 829
Directory file cache 829
Directory temporanea 829
Durata massima dei processi per elemento secondario 829
L'aggiornamento del visualizzatore produce sempre i dati correnti 829
Numero di record di database da leggere durante l'anteprima o l'aggiornamento di un report 829
Numero massimo di elementi secondari preavviati 829
Numero max. processi simultanei 829
Percorso classe Java 829
Record di database letti durante l'anteprima o l'aggiornamento 829
Scadenza Single Sign-On 829
Timeout cache di protezione 829
Timeout connessione inattiva 829
Timeout processo inattivo 829
Proprietà servizi Web Intelligence
Abilita analisi memoria 840
Abilita cache documento 840
Abilita cache elenco dei valori 840
Abilita cache in tempo reale 840
Abilita monitoraggio 840
Abilita monitoraggio servizio PJS 840
Abilita utilizzo di URL HTTP 840

server *(segue)*
Proprietà servizi Web Intelligence *(segue)*
Consenti errori dimensione massima mappa 840
Conteggio tentativi errori ping servizio PJS 840
Dimensione massima cache documenti 840
Dimensione massima flusso binario 840
Dimensioni batch elenco dei valori 840
Dimensioni batch elenco dei valori (voci) 840
Dimensioni flusso caratteri massime 840
Dimensioni LOV massime 840
Dimensioni massime cache universo 840
Dimensioni massime ordinamento personalizzato 840
Directory cache di output 840
Directory immagini 840
Disabilita condivisione cache 840
Intervallo di polling del server 840
Intervallo pulizia cache documento 840
Numero max. connessioni 840
Numero max. documenti nella cache 840
Numero max. documenti per utente 840
Numero max. documenti prima della reinizializzazione 840
Periodo thread monitoraggio servizio PJS 840
Ritardo del loop del thread di monitoraggio (secondi) 840
Scadenza Single Sign-On 840
Soglia inferiore memoria 840
Soglia massima memoria 840
Soglia superiore memoria 840
Spazio di riduzione massimo cache documenti 840
Timeout cache 840
Timeout connessione inattiva 840
Timeout documento inattivo 840
Timeout prima della reinizializzazione 840

server *(segue)*
Proprietà servizi Web Intelligence *(segue)*
Timeout scambio motore di visualizzazione (in secondi) 840
Timeout scambio risorse monitorate predefinite (in secondi) 840
Timeout svuotamento motore di visualizzazione (in secondi) 840
Timeout svuotamento risorse monitorate predefinite (in secondi) 840
Valore proxy 840
Protocollo 814
raggruppamento 373
registrazione dell’attività 379
registrazione tramite nome 394
riavvio 361, 362, 363
Riconnessione automatica al database di sistema 814
righe di comando 765, 766
Scadenza Single Sign-On 814
segnaposto 367
stato 353, 360
Tempo massimo di inattività 814
Tentativo massimo 814
Timeout connessione inattiva 814
Timeout di avvio servizio 814
Timeout inattività oggetti transitori 814
Timeout scambio motore di visualizzazione (in secondi) 814
Timeout svuotamento motore di visualizzazione (in secondi) 814
Tipo archivio certificati 814
URL endpoint dell'agente JMX predefinito (IIOP) 814
visualizzazione dello stato di un server 361
server del contenitore applicazioni Web (WACS) 30, 530, 814
aggiunta di servizi Web 434
connettori 427
panoramica 427
rimozione di servizi Web 435
servizio CMC 427
server del contenitore di applicazioni Web (WACS)
AD Kerberos 444
aggiunta 430
attività comuni 428
bilanciamento del carico 449
clonazione 433

server del contenitore di applicazioni Web (WACS) *(segue)*
computer multi-home 451
creazione di nuovi server 432
eliminazione 434
errori server 452
file di configurazione di Kerberos 442
file JAAS 443
firewall 450
HTTPS 435, 438, 450
installazione 431
metriche 870
metriche del sistema 452
modifica delle impostazioni di memoria 454
proprietà 456
rimozione 430
ripristino dei valori predefiniti di sistema 455
risoluzione dei conflitti tra porte 453, 454
risoluzione dei problemi 452
SSL 435, 438
utilizzo con altri server Web 449
utilizzo con server proxy 449, 450
server della piattaforma SAP BusinessObjects Business Intelligence
configurazione di Kerberos e browser 442
server di applicazioni Web 29
autenticazione 214
Software Development Kit (SDK) 31
Server di elaborazione
opzioni della riga di comando 770, 771
Web Intelligence 776
Server di elaborazione Crystal Reports 530, 770
opzioni della riga di comando 770
Server di elaborazione Crystal Reports 2010 530
Server di elaborazione di Dashboard Design 771
opzioni della riga di comando 771
server di elenchi in linea 234
informazioni su LDAP 233
plug-in di protezione 234
server di monitoraggio 530
Server Intelligence Agent 20
avvio automatico di server 363
dipendenze dei server Windows, aggiunta 415
Server Intelligence Agent *(segue)*
nodi 395, 396, 400, 403, 405
aggiunta 397, 398, 399, 410
credenziali utente, modifica 416
eliminazione 403, 404, 410
nuovo computer, aggiunta 396
ricreazione 400, 401, 402, 404, 410
ridenominazione 405, 406
spostamento 407, 408, 409, 413
Server Intelligence Agent (SIA)
workflow di arresto 74
workflow di avvio 73
server proxy inverso
configurazione con la piattaforma BI 202
distribuzione con la piattaforma BI 201
Server SAP BusinessObjects Enterprise 543
server Web
protezione 148
server, proprietà 811
serverconfig.sh 758
nodi
aggiunta 398
eliminazione 404
ricreazione 402
ridenominazione 406
spostamento 408
servizi 44
contrasto con i server 19, 42
modelli configurazione 384
Servizi Information Platform
creazione di account per 283
diritti di amministrazione 350
diritti di pubblicazione 351
mappatura dei ruoli 315, 333, 345
servizi Web
aggiunta a un Server del contenitore di applicazioni Web 434
configurazione per server reverse proxy 206, 207, 208
distribuzione personalizzata 646, 647
memorizzazione di file nella cache 646
rimozione da un Server del contenitore di applicazioni Web 435
variabile di sessione 646
Servizio applicazioni Web BEx 515
servizio Business Process BI
aggiunta a un Server del contenitore di applicazioni Web 434
rimozione da un Server del contenitore di applicazioni Web 435
servizio di monitoraggio 538
sessione, variabili 147
autenticazione 214
sessioni 147
registrazione 147
setup.sh 761
SI_AVAILABILITY_PROPERTY 530
Siebel Enterprise 37
Siebel, integrazione
configurazione firewall 199
Crystal Reports, creazione voce di menu 720
progetto di integrazione 719
ricompilazione applicazione Siebel 720
sincronizzazione delle informazioni sui report 675
Single Sign On 36, 216, 274, 283
account di servizio 267
al database 217
anonimo 216
autenticazione Windows AD 254
end-to-end 218
importazione dei ruoli 293
impostazione
LDAP 244
SiteMinder 244, 274
Windows AD 254
Kerberos 266, 448
piattaforma BI 216
risoluzione dei problemi 245
Single Sign On, configurazione per JD Edwards 712
Single Sign On, configurazione per Oracle EBS 352
Single Sign On, configurazione per PeopleSoft 714
Single Sign On, configurazione per Siebel 723
Single Sign-On anonimo 216
Single Sign-On end-to-end 218
Single Sign-On, configurazione per SAP Netweaver 313
SiteMinder
configurazione di Single Sign-On con LDAP 244, 274
configurazione plug-in LDAP 244
configurazione war BOE 245

SiteMinder *(segue)*
errore 245
risoluzione dei problemi 245
Windows AD 274
siti
gestione dei diritti 616, 617, 618, 620, 621
livelli di accesso 134
siti di destinazione
livelli di accesso 134
siti di origine
livelli di accesso 134
SMD 747
agente SMD 748
SNC
vedere Secure Network Communication 297
Software Development Kit (SDK)
Crystal Reports Viewer SDK 31
piattaforma SAP BusinessObjects Business Intelligence, SDK Consumer 31
Report Application Server SDK 31
Report Engine SDK 31
SDK piattaforma SAP BusinessObjects Business Intelligence 31
Solution Manager 525
account SMAdmin 748
sottogruppi, aggiunta 98
spazi di lavoro BI 70
spazi di lavoro BI, diritti 790, 798
specifiche del sistema, visualizzazione 379
server del contenitore di applicazioni Web (WACS) 452
specifici del tipo, diritti 120
Avvisi 804
BI Launch Pad 797
cartelle 784
categorie 784
CMC 797
connessioni universo 795
Crystal Reports 786
documenti Web Intelligence 786
gruppi 788
Information Design Tool 803
livelli di accesso 789
note 785
Strategy Builder 801
Universe Design Tool 802
universi (.unv) 791
universi (.unx) 792
utenti 788
Web Intelligence 798
widget 804
SSL 164, 166, 167, 168
certificati 164, 165
chiavi 164, 165
configurazione dei server 164, 166, 167, 168
configurazione di server del contenitore di applicazioni Web (WACS) 435, 438
sslconfig.exe 168
Strumento di conversione dei report 170
thick client 168
Translation Management Tool 169
SSL (Secure Socket Layer)
configurazione 713, 715
SSL.Vedere Secure Sockets Layer (SSL) 233
sslc.cnf 164
sslc.exe 164
startservers 759
stati del server 353
statistiche, controllo dell'attività Web 149
stato, visualizzazione e modifica per i server 360, 361
stopservers 759
Strategy Builder, diritti 801
strumentazione 751
livello Web 751
panoramica 749
registrazione 751
segnaposto 750
server non Java 749
verifica 751
strumento della riga di comando BIAR 471
strumento della riga di comando motore BIAR 473, 475, 480
Strumento di amministrazione di Data Federation 65
Strumento di conversione dei report 63
SSL 170
Subversion 40
suggerimenti 602
suggerimenti sulle prestazioni 717
supporto cluster 530, 589
Supporto multilingua 602
syslog 379
System Landscape Directory (SLD) 38
file connect.key 746
registrazione 745
trigger 746
verifica della registrazione 747

T

tempo di risposta 525
terze parti, plug-in di protezione 215
thread di discussione 488
annullamento della ricerca 488
ordinamento dei risultati della ricerca 490
ricerca 488
ticket 146
per la protezione distribuita 146
token di accesso 146
Timeout del socket 653
tipi di contenuto in cui è possibile eseguire ricerche 599
tipi di server 55, 58
token di accesso 146
autenticazione 214
protezione distribuita 146
registrazione delle sessioni 147
Tomcat
JAAS 261
Kerberos 259
traccia 727
end-to-end 752
server 728
file configuring .ini 730
Translation Management Tool 64
Translation Management Tool: SSL 169
trasferimento di attendibilità 146
trasporti 679, 680
Connettività InfoSet 679, 683
Connettività Open SQL 680
definizione cluster 679, 684
definizione protezione a livello di riga 683
Editor definizione Protezione 679
gruppi di funzioni 678
importazione 680
oggetti 678
panoramica 678
personalizzazione dei parametri 679, 688
programmi 678
tabelle 678
verifica dei conflitti 680
workbench per l'amministrazione dei contenuti 685

U

Universe Design Tool 63
Universe Design Tool, diritti 802
Universe Designer
vedere Universe Design Tool 63

universi
diritti (.unv) 791
diritti (.unx) 792
gestione 522
replica 625
universo 34
UNIX
syslog 379
Upgrade Management Tool 22, 67
utenti
assegnazione dei diritti a 124
assegnazione di diritti avanzati 124
concessione dell'accesso 103
controllo dei diritti 125, 126
diritti 788
diritti, per cartelle di livello superiore 125
mappatura 315, 333, 339, 345
visualizzazione di diritti 123
utenti di terze parti, replica 624
utenti mappati, gestione degli alias 108
utilità SPN 255

V

variabili
directory di installazione 18, 395
directory script 18
script di gestione dei nodi 395
sistema operativo UNIX 18
Vintela 266
considerazioni su WebLogic 269
visualizzazione
dettagli cluster CMS 379
diritti per principali 123
metriche correnti 378
metriche del server del contenitore di applicazioni Web (WACS) 452
metriche del sistema 379
visualizzazione dell'account corrente 86, 358
visualizzazioni 35
Voyager 71
vedere SAP BusinessObjects Analysis 67

W

WAR, file
applicazioni Web della piattaforma BI 201
BOE 201, 502, 505, 507
dswsbobje 201
WAR, file *(segue)*
file war BOE
proprietà CMC 509
proprietà di BI Launch Pad 505
proprietà globali 502
proprietà OpenDocument 507
OpenDocument 266
WDeploy 69
Web Intelligence 491, 772
diritti 798
diritti applicazione 491
diritti di accesso HTML query 491
Server di elaborazione 776
Web Intelligence Desktop 62
Web Intelligence Processing Server 19, 42, 530
Web Intelligence, documenti
diritti 786
Web Service Query, strumento 33, 63
Web, servizi 32
strumento Web Service Query 33
WebLogic
JAAS, file di configurazione 261
Kerberos 259
opzioni Java 264
WebSphere
JAAS 262
Kerberos 260
opzioni Java 265
widget
diritti 804
gestione delle impostazioni 495
Widget BI
vedere Widget per la piattaforma SAP BusinessObjects Business Intelligence 65
Windows
dipendenze dei server, aggiunta 415
Registro eventi 379
Windows AD
account di servizio 267
account e gruppi 252
pianificazione di aggiornamenti 252
attivazione di Kerberos 441
autenticazione 251
configurazione di Kerberos server delle applicazioni 258
mappatura account 252
mapping di gruppi 252
mapping di LDAP 249
plug-in di protezione 252
Single Sign On 267, 269
Vintela 269
workbench per l'amministrazione dei contenuti 670
aggiornamento dell'origine dati dei report 675
aggiunta di sistemi della piattaforma BI 670
applicazione delle autorizzazioni 667
definizione dei livelli di accesso dell'utente 667
eliminazione dei report 675
panoramica sulla pubblicazione dei report 666
pubblicazione dei report in background 675
pubblicazione di report 672
sincronizzazione delle informazioni sui report 675
workflow 72
accesso utente 73
arresto SIA 74
avvio SIA 73
diritti avanzati, assegnazione 124
documento Web Intelligence pianificato 77
elenchi di controllo degli accessi, assegnazione di principali 124
esecuzione di un report Crystal 76
impostazione di diritti per cartelle di livello superiore 125
invio di un'istanza alla destinazione 79
oggetto pianificato 78
pianificazione di un report Crystal 75
visualizzazione di diritti 123
visualizzazione di un report Crystal con Web Java 83
visualizzazione di un report Crystal di cache 80
visualizzazione di un report Crystal non di cache 79
visualizzazione di un report Crystal su richiesta 82
visualizzazione di uno spazio di lavoro Analysis 81
visualizzazione su richiesta di un report Web Intelligence 83

X

Xcelsius Data Cache Server 530
Xcelsius Data Processing Server 530
Xcelsius vedere SAP BusinessObjects Dashboard Design 68