



Business Intelligence 平台管理员指南

■ SAP BusinessObjects Business Intelligence platform 4.1 Support Package 1

2013-09-19

版权所有

© 2013 SAP AG 股份公司或其关联公司版权所有，保留所有权利。未经SAP股份公司明确许可，不得以任何形式或为任何目的复制或传播本文的任何内容。本文包含的信息如有更改，恕不另行事先通知。由SAP股份公司及其分销商营销的部分软件产品包含其它软件供应商的专有软件组件。各国的产品规格可能不同。上述资料由SAP股份公司及其关联公司（统称“SAP集团”）提供，仅供参考，不构成任何形式的陈述或保证，其中如若存在任何错误或疏漏，SAP集团概不负责。与SAP集团产品和服务相关的保证仅限于该等产品和服务随附的保证声明（若有）中明确提出之保证。本文中的任何信息均不构成额外保证。SAP和本文提及的其它SAP产品和服务及其各自标识均为SAP股份公司在德国和其他国家的商标或注册商标。如欲了解更多商标信息和声明，请访问：
<http://www.sap.com/china/about/company/legal/copyright/index.epx#trademark>。

2013-09-19

目录

第 1 章	文档历史记录.....	18
第 2 章	入门.....	19
2.1	关于本指南..	19
2.1.1	本指南面向的用户..	19
2.1.2	Business Intelligence 平台简介 ..	19
2.1.3	变量..	20
2.1.4	术语..	20
2.2	开始之前..	22
2.2.1	关键概念..	22
2.2.2	关键管理工具..	25
2.2.3	关键任务..	26
第 3 章	体系结构.....	29
3.1	体系结构概述..	29
3.1.1	部件图..	30
3.1.2	体系结构层..	31
3.1.3	数据库..	32
3.1.4	服务器、主机和群集..	32
3.1.5	Web 应用程序服务器..	33
3.1.6	软件开发工具包..	34
3.1.7	数据源..	36
3.1.8	身份验证和单一登录..	37
3.1.9	SAP 集成..	38
3.1.10	集成版本控制..	39
3.1.11	升级路径..	40
3.2	服务器、服务、节点和主机..	40
3.2.1	自 XI 3.1 以来所做的服务器更改..	42
3.2.2	服务 ..	43
3.2.3	服务类别..	49
3.2.4	服务器类型..	52
3.2.5	服务器..	57
3.3	客户端应用程序..	59
3.3.1	随 SAP BusinessObjects Business Intelligence 平台客户端工具一起安装..	60
3.3.2	随 SAP BusinessObjects Business Intelligence 平台一起安装..	64

3.3.3	单独提供..65
3.3.4	Web 应用程序客户端..67
3.4	流程工作流..70
3.4.1	启动和身份验证..71
3.4.2	程序对象..72
3.4.3	Crystal Reports..74
3.4.4	Web Intelligence..77
3.4.5	分析..79

第 4 章 系统配置向导.....81

4.1	系统配置向导介绍..81
4.2	指定使用的产品..81
4.3	选择部署模板..82
4.4	指定数据文件夹位置..84
4.5	复查更改..85
4.6	日志文件和响应文件..85
4.6.1	使用响应文件..86

第 5 章 管理许可.....89

5.1	管理许可密钥..89
5.1.1	查看许可信息..89
5.1.2	添加许可密钥..90
5.1.3	查看当前帐户活动..90

第 6 章 管理用户和组.....91

6.1	帐户管理概述..91
6.1.1	用户管理..91
6.1.2	组管理..92
6.1.3	可用的身份验证类型 ..93
6.2	管理 Enterprise 帐户和常规帐户..94
6.2.1	创建用户帐户..94
6.2.2	要修改用户帐户..95
6.2.3	删除用户帐户..96
6.2.4	创建新组..96
6.2.5	修改组的属性..97
6.2.6	查看组成员..97
6.2.7	添加子组..98
6.2.8	指定组成员资格..98
6.2.9	删除组..99
6.2.10	批量添加用户或用户组..99
6.2.11	启用 Guest 帐户..100
6.2.12	将用户添加到组..100
6.2.13	更改密码设置..102
6.2.14	将访问权限授予用户和组..103

6.2.15	控制对用户收件箱的访问..104
6.2.16	配置 BI 启动板选项..104
6.3	管理别名..108
6.3.1	创建用户和添加第三方别名..108
6.3.2	为现有用户创建新别名..109
6.3.3	分配来自另一用户的别名..109
6.3.4	删除别名..110
6.3.5	禁用别名..110

第 7 章 设置权限.....112

7.1	权限在 BI 平台中如何运作..112
7.1.1	访问级别..112
7.1.2	高级权限设置..113
7.1.3	继承..114
7.1.4	特定于类型的权限..118
7.1.5	确定有效权限..120
7.2	在 CMC 中管理对象的安全设置..120
7.2.1	查看主体的对象权限..121
7.2.2	将主体分配到对象的访问控制列表..122
7.2.3	修改主体的对象安全性..122
7.2.4	在 BI 平台中设置对顶层文件夹的权限..123
7.2.5	检查主体的安全设置..123
7.3	使用访问级别..126
7.3.1	在“查看”和“按需查看”访问级别之间选择..128
7.3.2	复制现有的访问级别..129
7.3.3	创建新访问级别..129
7.3.4	重命名访问级别..130
7.3.5	删除访问级别..130
7.3.6	修改访问级别中的权限..130
7.3.7	跟踪访问级别和对象之间的关系..131
7.3.8	跨站点管理访问级别..132
7.4	终止继承..133
7.4.1	禁用继承..134
7.5	使用权限来委派管理..134
7.5.1	在修改用户拥有的对象权限选项之间进行选择..136
7.5.2	所有者权限..137
7.6	权限管理的建议摘要..137

第 8 章 保护 BI 平台安全.....139

8.1	安全概述 ..139
8.2	灾难恢复计划..139
8.3	保护部署安全的一般建议..140
8.4	配置捆绑的第三方服务器的安全..141
8.5	活动信任关系..141
8.5.1	登录标记..141

8.5.2	分布式安全的票证机制..142
8.6	会话和会话跟踪..142
8.6.1	CMS 会话跟踪..143
8.7	环境保护..143
8.7.1	Web 浏览器到 Web 服务器..143
8.7.2	Web 服务器到 BI 平台..144
8.8	审核安全性配置修改 ..144
8.9	审核 Web 活动..145
8.9.1	防止恶意登录企图..145
8.9.2	密码限制..145
8.9.3	登录限制..145
8.9.4	用户限制..146
8.9.5	Guest 帐户限制..146
8.10	处理扩展..147
8.11	BI 平台数据安全概述..147
8.11.1	数据处理安全模式..147
8.12	BI 平台加密..150
8.12.1	使用群集密钥..150
8.12.2	加密人员..152
8.12.3	在 CMC 中管理加密密钥..154
8.13	针对 SSL 配置服务器..158
8.13.1	创建密钥和证书文件..158
8.13.2	当证书由证书颁发机构管理时设置 SSL..160
8.13.3	配置 SSL 协议..162
8.14	了解 BI 平台组件间的通信..167
8.14.1	BI 平台服务器和通信端口概述..167
8.14.2	BI 平台组件间的通信 ..169
8.15	为防火墙配置 BI 平台..176
8.15.1	针对防火墙配置系统..176
8.15.2	调试带防火墙的部署..179
8.16	典型的防火墙方案示例..181
8.16.1	示例 — 部署在独立网络上的应用程序层..181
8.16.2	示例 — 通过防火墙与 BI 平台服务器隔开的胖客户端和数据库层..184
8.17	集成环境的防火墙设置..186
8.17.1	SAP 集成专用防火墙指南..186
8.17.2	JD Edwards EnterpriseOne 集成的防火墙配置..188
8.17.3	Oracle EBS 的专用防火墙指南..189
8.17.4	PeopleSoft Enterprise 集成的防火墙配置 ..190
8.17.5	Siebel 集成的防火墙配置..192
8.18	BI 平台和反向代理服务器 ..193
8.18.1	受支持的反向代理服务器 ..193
8.18.2	了解如何部署 Web 应用程序 ..194
8.19	为 BI 平台 Web 应用程序配置反向代理服务器..194
8.19.1	配置反向代理服务器的详细说明..195
8.19.2	配置反向代理服务器..195
8.19.3	为 BI 平台配置 Apache 2.2 反向代理服务器 ..196

8.19.4	为 BI 平台配置 WebSEAL 6.0 反向代理服务器 ..196
8.19.5	为 BI 平台配置 Microsoft ISA 2006 ..197
8.20	反向代理部署中 BI 平台的特殊配置..199
8.20.1	为 Web 服务启用反向代理..199
8.20.2	为 ISA 2006 启用会话 cookie 的根路径..201
8.20.3	为 SAP BusinessObjects Live Office 启用反向代理..204

第 9 章 身份验证.....205

9.1	BI 平台中的身份验证选项..205
9.1.1	主要身份验证..206
9.1.2	安全插件..206
9.1.3	BI 平台的单一登录..207
9.2	Enterprise 身份验证..209
9.2.1	Enterprise 身份验证概述..209
9.2.2	Enterprise 身份验证设置..210
9.2.3	更改 Enterprise 设置..211
9.2.4	启用受信任的身份验证..212
9.2.5	为 Web 应用程序配置受信任的身份验证..214
9.3	LDAP 身份验证..222
9.3.1	使用 LDAP 身份验证..223
9.3.2	配置 LDAP 身份验证..224
9.3.3	映射 LDAP 组..234
9.4	Windows AD 身份验证..243
9.4.1	使用 Windows AD 身份验证..244
9.4.2	准备域控制器..244
9.4.3	配置 CMC 的 AD 身份验证..246
9.4.4	配置 BI 平台服务以运行 SIA..251
9.4.5	配置用于 AD 身份验证的 Web 应用程序服务器..253
9.4.6	单一登录设置..263
9.4.7	Windows AD 身份验证疑难解答..278
9.5	SAP 身份验证..280
9.5.1	配置 SAP 身份验证 ..280
9.5.2	为 BI 平台创建用户帐户..281
9.5.3	连接到 SAP 权利系统..282
9.5.4	设置 SAP 身份验证选项..284
9.5.5	导入 SAP 角色..287
9.5.6	配置安全网络通讯 (SNC) ..290
9.5.7	设置对 SAP 系统的单一登录..303
9.5.8	为 SAP Crystal Reports 和 SAP NetWeaver 配置 SS0..307
9.6	PeopleSoft 身份验证..308
9.6.1	概述..308
9.6.2	启用 PeopleSoft Enterprise 身份验证..309
9.6.3	将 PeopleSoft 角色映射到 BI 平台..309
9.6.4	计划用户更新..312
9.6.5	使用 PeopleSoft 安全桥..314

9.7	JD Edwards 身份验证..325
9.7.1	概述..325
9.7.2	启用 JD Edwards EnterpriseOne 身份验证..325
9.7.3	将 JD Edwards EnterpriseOne 角色映射到 BI 平台..326
9.7.4	计划用户更新..329
9.8	Siebel 身份验证..330
9.8.1	启用 Siebel 身份验证..330
9.8.2	将角色映射到 BI 平台..331
9.8.3	计划用户更新..334
9.9	Oracle EBS 身份验证..335
9.9.1	启用 Oracle EBS 身份验证..336
9.9.2	将 Oracle 电子商务套件角色映射到 BI 平台..337
9.9.3	取消映射角色 ..340
9.9.4	为映射的 Oracle EBS 组和用户自定义权限 ..341
9.9.5	为 SAP Crystal Reports 和 Oracle EBS 配置单一登录 (SSO) ..342

第 10 章 服务器管理..... 344

10.1	使用 CMC 中的“服务器”管理区域..344
10.2	在 Windows 上使用脚本管理服务器 ..347
10.3	在 Unix 上管理服务器 ..347
10.4	查看和更改服务器的状态..348
10.4.1	查看服务器的状态..348
10.4.2	启动、停止和重新启动服务器..349
10.4.3	停止中央管理服务器..352
10.4.4	启用和禁用服务器..352
10.5	添加、克隆或删除服务器..353
10.5.1	添加、克隆和删除服务器..354
10.6	将中央管理服务器组成群集..357
10.6.1	将中央管理服务器组成群集..357
10.7	管理服务器组..362
10.7.1	创建服务器组..362
10.7.2	使用服务器子组..363
10.7.3	修改服务器的组成员资格..364
10.7.4	用户对服务器和服务器组的访问..365
10.8	为生产系统配置自适应处理服务器..366
10.9	评估系统的性能..367
10.9.1	监控 BI 平台服务器..367
10.9.2	分析服务器量度值..367
10.9.3	查看系统量度值..368
10.9.4	记录服务器活动..368
10.10	配置服务器设置..369
10.10.1	更改服务器的属性..370
10.10.2	向多个服务器应用服务设置..370
10.10.3	使用配置模板..371
10.11	配置服务器网络设置..373

10.11.1	网络环境选项..373
10.11.2	服务器主机标识选项..374
10.11.3	配置多宿主计算机..376
10.11.4	配置端口号..378
10.12	管理节点 ..381
10.12.1	使用节点..381
10.12.2	添加新节点..384
10.12.3	重新创建节点..388
10.12.4	删除节点..392
10.12.5	重命名节点..394
10.12.6	移动节点..396
10.12.7	脚本参数..399
10.12.8	添加 Windows 服务器依赖项..404
10.12.9	更改节点的用户凭据..405
10.13	在 BI 平台部署中重命名计算机..405
10.13.1	更改群集名称..405
10.13.2	更改 IP 地址..406
10.13.3	重命名计算机..407
10.14	结合使用 32 位和 64 位第三方库和 BI 平台..411
10.15	管理服务器和节点占位符..412
10.15.1	查看服务器占位符..412
10.15.2	查看和编辑节点的占位符..412
 第 11 章	 管理中央管理服务器 (CMS) 数据库.....413
11.1	管理 CMS 系统数据库连接..413
11.1.1	选择 SQL Anywhere 作为 CMS 数据库..413
11.1.2	选择 SAP HANA 作为 CMS 数据库..414
11.2	选择新的或现有的 CMS 数据库..415
11.2.1	在 Windows 上选择新的或现有的 CMS 数据库..416
11.2.2	在 Unix 上选择新的或现有的 CMS 数据库..416
11.3	重新创建 CMS 系统数据库..417
11.3.1	在 Windows 上重新创建 CMS 系统数据库..417
11.3.2	在 Unix 上重新创建 CMS 系统数据库..418
11.4	将数据从一个 CMS 系统数据库复制到另一个系统数据库..419
11.4.1	准备复制 CMS 系统数据库..419
11.4.2	在 Windows 上复制 CMS 系统数据库..420
11.4.3	在 Unix 上复制 CMS 系统数据库中的数据..420
 第 12 章	 管理 Web 应用程序容器服务器 (WACS)421
12.1	WACS..421
12.1.1	Web 应用程序容器服务器 (WACS) ..421
12.1.2	在部署中添加或删除附加的 WACS..424
12.1.3	在 WACS 中添加或删除服务..427
12.1.4	配置 HTTPS/SSL..429
12.1.5	受支持身份验证方法..432

12.1.6	为 WACS 配置 AD Kerberos ..433
12.1.7	配置 AD Kerberos 单一登录 ..440
12.1.8	配置 RESTful Web 服务..443
12.1.9	WACS 和 IT 环境..453
12.1.10	配置 Web 应用程序属性 ..456
12.1.11	疑难解答..457
12.1.12	WACS 属性..461
第 13 章	备份和恢复系统.....462
13.1	备份和恢复概览..462
13.2	术语..462
13.3	备份和恢复的使用情况..464
13.4	备份..466
13.4.1	备份整个系统..466
13.4.2	备份服务器设置..469
13.4.3	备份 BI 内容..471
13.5	恢复系统..472
13.5.1	恢复整个系统..472
13.5.2	恢复服务器设置..477
13.5.3	恢复 BI 内容..479
13.6	BackupCluster 和 RestoreCluster 脚本..480
第 14 章	复制 BI 平台部署.....483
14.1	系统复制概述..483
14.2	术语..483
14.3	系统复制的使用情况..484
14.4	计划复制系统..485
14.5	注意事项与限制..485
14.6	系统复制过程..487
14.6.1	从源系统导出..487
14.6.2	导入一个目标系统..491
第 15 章	版本管理.....494
15.1	管理 BI 资源的不同版本 ..494
15.2	使用版本管理设置选项..495
15.2.1	在 Windows 上设置 ClearCase 版本管理系统..496
15.2.2	在 Unix 上设置 ClearCase 版本管理系统..496
15.3	比较同一作业的不同版本..496
15.4	升级 Subversion 内容..497
第 16 章	升级管理.....498
16.1	欢迎使用升级管理..498
16.1.1	概述..498

16.1.2	功能.. 498
16.1.3	应用程序访问权限.. 499
16.1.4	升级管理中的 WinAD 支持.. 500
16.2	升级管理工具入门.. 500
16.2.1	访问升级管理应用程序.. 500
16.2.2	用户界面组件.. 501
16.2.3	使用“设置”选项.. 502
16.3	使用升级管理工具.. 509
16.3.1	创建和删除文件夹.. 509
16.3.2	创建作业.. 511
16.3.3	通过复制现有作业来创建新作业 .. 513
16.3.4	搜索作业.. 513
16.3.5	编辑作业.. 514
16.3.6	将 Infoobject 添加到作业中.. 514
16.3.7	管理作业的依赖项.. 515
16.3.8	搜索依赖项 .. 516
16.3.9	资源库连接时升级作业.. 517
16.3.10	使用 BIAR 文件升级作业.. 519
16.3.11	计划作业升级.. 521
16.3.12	查看作业的历史记录.. 523
16.3.13	回滚作业.. 523
16.4	管理 Infoobject 的不同版本.. 526
16.4.1	版本管理应用程序访问权限.. 527
16.4.2	备份和恢复 Subversion 文件.. 528
16.5	使用命令行选项.. 529
16.5.1	在 Windows 上运行命令行工具.. 529
16.5.2	在 UNIX 上运行命令行工具.. 530
16.5.3	命令行工具参数.. 531
16.5.4	示例属性文件.. 537
16.6	使用增强更改和传输系统.. 537
16.6.1	先决条件.. 538
16.6.2	配置 BI 平台和 CTS+ 集成.. 538
16.6.3	使用 CTS 升级作业.. 547
第 17 章	差异可视化工具..... 550
17.1	升级管理工具中的差异可视化工具.. 550
17.1.1	使用差异可视化工具比较对象或文件.. 551
17.1.2	在版本管理系统中比较对象或文件.. 552
17.1.3	计划比较.. 553
第 18 章	管理应用程序..... 554
18.1	通过 CMC 管理应用程序.. 554
18.1.1	概述.. 554
18.1.2	应用程序的常规设置.. 555
18.1.3	应用程序特定设置.. 556

18.2	通过 BOE.war 属性管理应用程序..598
18.2.1	BOE WAR 文件..598
18.3	自定义 BI 启动板和 OpenDocument 登录入口点..606
18.3.1	BI 启动板和 OpenDocument 文件位置..607
18.3.2	定义自定义登录页..608
18.3.3	登录时添加受信任的身份验证..609
18.4	自定义 Web Intelligence 界面..609
18.4.1	“功能”选项卡..610
18.4.2	“用户界面元素”选项卡..611
18.4.3	自定义 Web Intelligence 界面外观..620
第 19 章	管理连接和 Universe.....622
19.1	管理连接..622
19.1.1	删除 Universe 连接..622
19.2	管理 Universe..623
19.2.1	删除 Universe..623
第 20 章	监控.....625
20.1	关于监控..625
20.2	监控术语..625
20.2.1	体系结构..627
20.3	配置监控的数据库支持 ..628
20.3.1	使用 Derby 数据库的配置..629
20.3.2	使用审核数据库的配置..629
20.4	配置属性..635
20.4.1	JMX 端点 URL..638
20.4.2	监控探测器的 HTTPS 身份验证..639
20.4.3	探测器的密码加密..640
20.5	与其他应用程序集成..640
20.5.1	将监控应用程序与 IBM Tivoli 集成..640
20.5.2	将监控应用程序与 SAP Solution Manager 集成 ..643
20.6	用于监控服务器的群集支持..644
20.7	疑难解答..644
20.7.1	仪表盘..644
20.7.2	警报..645
20.7.3	监测器列表..645
20.7.4	探测器..646
20.7.5	量度..647
20.7.6	图形..647
第 21 章	审核.....648
21.1	概述..648
21.2	CMC 审核页..653
21.2.1	审核状态..653

21.2.2	配置审核事件..654	
21.2.3	审核数据存储配置设置..657	
21.3	审核事件..659	
21.3.1	审核事件和详细信息..669	
第 22 章	平台搜索.....	685
22.1	了解平台搜索..685	
22.1.1	平台搜索 SDK..685	
22.1.2	群集环境..686	
22.2	设置平台搜索..686	
22.2.1	部署 OpenSearch..686	
22.2.2	配置反向代理..688	
22.2.3	在 CMC 中配置应用程序属性..688	
22.3	使用平台搜索..692	
22.3.1	为 CMS 资源库中的内容建立索引..692	
22.3.2	索引建立失败列表..693	
22.3.3	搜索结果..694	
22.4	平台搜索与 SAP NetWeaver Enterprise Search 相集成..701	
22.4.1	在 SAP NetWeaver Enterprise Search 中创建连接器 ..702	
22.4.2	将用户角色导入 BI 平台..702	
22.5	从 NetWeaver Enterprise Search 中搜索..703	
22.6	审核..703	
22.7	疑难解答..705	
22.7.1	自我康复..705	
22.7.2	问题方案..705	
第 23 章	联盟.....	707
23.1	联盟..707	
23.2	联盟术语..708	
23.3	管理安全权限..710	
23.3.1	在源站点上所需的权限..710	
23.3.2	在目标站点上所需的权限..711	
23.3.3	联盟特定的权限..712	
23.3.4	复制对象的安全性..713	
23.3.5	复制使用访问级别的安全设置..714	
23.4	复制类型和模式选项..714	
23.4.1	单向复制 ..714	
23.4.2	双向复制 ..715	
23.4.3	从源刷新或从目标刷新..715	
23.5	复制第三方用户和组..717	
23.6	复制 Universe 和 Universe 连接..717	
23.7	管理复制列表..718	
23.7.1	创建复制列表..719	
23.7.2	修改复制列表..721	
23.8	管理远程连接..722	

23.8.1	创建远程连接.. 723
23.8.2	修改远程连接.. 725
23.9	管理复制作业.. 725
23.9.1	创建复制作业.. 726
23.9.2	计划复制作业.. 728
23.9.3	修改复制作业.. 728
23.9.4	在复制作业完成后查看日志.. 729
23.10	管理对象清除.. 730
23.10.1	如何使用对象清除.. 730
23.10.2	对象清除的限制.. 730
23.10.3	对象清除频率.. 731
23.11	管理冲突检测 and 解决.. 732
23.11.1	单向复制冲突的解决方法.. 732
23.11.2	双向复制冲突的解决方法.. 734
23.12	在联盟中使用 Web 服务.. 736
23.12.1	会话变量 .. 736
23.12.2	文件高速缓存 .. 737
23.12.3	自定义部署 .. 738
23.13	远程计划和本地运行的实例.. 738
23.13.1	远程计划.. 739
23.13.2	本地运行的实例.. 740
23.13.3	实例共享.. 740
23.14	导入和升级复制的内容.. 741
23.14.1	导入复制的内容.. 741
23.14.2	导入复制的内容并继续复制 .. 742
23.14.3	从测试环境中升级内容.. 743
23.14.4	将目标站点重新指向新位置.. 743
23.15	最佳做法.. 744
23.15.1	当前版本限制.. 746
23.15.2	错误消息疑难解答.. 747

第 24 章 ERP 环境补充配置..... 751

24.1	针对 SAP NetWeaver 集成的配置.. 751
24.1.1	与 SAP NetWeaver Business Warehouse (BW) 集成.. 751
24.2	针对 JD Edwards 集成的配置.. 808
24.2.1	为 SAP Crystal Reports 配置单一登录 (SSO) .. 808
24.2.2	为 JD Edwards 集成配置安全套接字层.. 809
24.3	针对 PeopleSoft Enterprise 集成的配置.. 810
24.3.1	为 SAP Crystal Reports 和 PeopleSoft Enterprise 配置单一登录 (SSO) . 811
24.3.2	配置安全套接字层通信.. 812
24.3.3	为 PeopleSoft 系统调优性能.. 814
24.4	配置 Siebel 集成.. 815
24.4.1	配置 Siebel 以与 SAP BusinessObjects Business Intelligence 平台相集成 .. 815
24.4.2	创建 Crystal Reports 菜单项.. 816

24.4.3	上下文感知..818
24.4.4	为 SAP Crystal Reports 和 Siebel 配置单一登录 (SSO) ..820
24.4.5	配置安全套接字层通信..821
第 25 章	管理和配置日志.....823
25.1	记录组件的跟踪消息..823
25.2	跟踪日志级别..823
25.3	为服务器配置跟踪..824
25.3.1	在 CMC 中设置日志级别..824
25.3.2	为 CMC 中的多个服务器设置日志级别..825
25.3.3	使用 BO_trace.ini 文件配置服务器跟踪..826
25.4	为 Web 应用程序配置跟踪..827
25.4.1	在 CMC 中设置 Web 应用程序跟踪日志级别..828
25.4.2	使用 BO_trace.ini 文件配置跟踪设置..828
25.5	为升级管理工具配置跟踪..832
25.5.1	为升级管理工具配置跟踪..833
25.6	为 BI 平台客户端应用程序配置跟踪..833
第 26 章	集成到 SAP Solution Manager834
26.1	集成概述..834
26.2	SAP Solution Manager 集成检查列表..834
26.3	管理系统架构目录注册..835
26.3.1	在系统架构中注册 BI 平台..835
26.3.2	何时会触发 SLD 注册? ..837
26.3.3	记录 SLD 连接 ..837
26.4	管理 Solution Manager 诊断代理..838
26.4.1	Solution Manager 诊断 (SMD) 概述..838
26.4.2	使用 SMD 代理..838
26.4.3	SMAdmin 用户帐户..839
26.5	管理性能检测..839
26.5.1	BI 平台的性能检测..840
26.5.2	为 BI 平台设置性能检测..840
26.5.3	Web 层的性能检测..841
26.5.4	检测日志文件 ..842
26.6	使用 SAP Passport 进行跟踪..842
第 27 章	命令行管理.....843
27.1	Unix 脚本 ..843
27.1.1	脚本实用程序..843
27.1.2	脚本模板..848
27.1.3	BI 平台使用的脚本..849
27.2	Windows 脚本 ..850
27.2.1	ccm.exe..850
27.3	服务器命令行..853

27.3.1	命令行概述..853	
27.3.2	适用于所有服务器的标准选项..853	
27.3.3	中央管理服务器..854	
27.3.4	Crystal Reports 处理服务器和 Crystal Reports 高速缓存服务器..856	
27.3.5	Dashboards 处理服务器和 Dashboards 高速缓存服务器..857	
27.3.6	作业服务器..858	
27.3.7	自适应处理服务器..859	
27.3.8	报表应用程序服务器..859	
27.3.9	Web Intelligence 处理服务器..861	
27.3.10	输入文件资源库服务器和输出文件资源库服务器..863	
27.3.11	事件服务器..864	
第 28 章	资源库诊断工具.....	866
28.1	资源库诊断工具概述..866	
28.2	使用资源库诊断工具..866	
28.2.1	使用资源库诊断工具..867	
28.2.2	资源库诊断工具参数..868	
28.3	CMS 与 FRS 之间的不一致..873	
28.4	CMS 元数据中的不一致项..874	
第 29 章	权限附录.....	878
29.1	关于权限附录..878	
29.2	常规权限..878	
29.3	特定对象类型的权限..880	
29.3.1	文件夹权限..880	
29.3.2	类别..881	
29.3.3	Desktop Intelligence 文档..881	
29.3.4	注释..883	
29.3.5	Crystal 报表..883	
29.3.6	Web Intelligence 文档..884	
29.3.7	用户和组..885	
29.3.8	访问级别..886	
29.3.9	Universe (.unv) 权限..887	
29.3.10	Universe (.unx) 权限..889	
29.3.11	Universe 对象访问级别..890	
29.3.12	连接权限..891	
29.3.13	应用程序..893	
第 30 章	服务器属性附录.....	909
30.1	关于服务器属性附录..909	
30.1.1	公共服务器属性..909	
30.1.2	核心服务属性..912	
30.1.3	连接服务属性..923	
30.1.4	Crystal Reports 服务属性..927	

30.1.5	分析服务属性..935
30.1.6	数据联合服务属性..936
30.1.7	Web Intelligence 服务属性..937
30.1.8	Dashboard Design 服务属性..944
第 31 章	服务器量度附录.....946
31.1	关于服务器量度附录..946
31.1.1	公用服务器量度 ..947
31.1.2	中央管理服务器量度..949
31.1.3	连接服务器量度..951
31.1.4	事件服务器量度..952
31.1.5	文件资源库服务器量度..952
31.1.6	自适应处理服务器量度..953
31.1.7	Web 应用程序容器服务器量度..958
31.1.8	自适应作业服务器量度..958
31.1.9	Crystal Reports Server 量度..960
31.1.10	Web Intelligence 服务器量度..963
31.1.11	Dashboards 服务器量度..964
第 32 章	服务器和节点占位符附录.....966
32.1	服务器和节点占位符..966
第 33 章	审核数据存储模式附录.....976
33.1	概述..976
33.2	模式图..976
33.3	审核数据存储表..977
第 34 章	监控数据库模式附录.....986
34.1	趋势数据库模式..986
第 35 章	系统复制工作表附录.....989
35.1	系统复制工作表..989
附录 A	更多信息.....991
索引.....	993

第 1 章 文档历史记录

下表概述了最重要的文档更改。

版本	日期	说明
SAP BusinessObjects Business Intelligence 平台 4.1	2013 年 5 月	本文档的第一个版本。
SAP BusinessObjects Business Intelligence 平台 4.1 支持包 1	2013 年 8 月	<ul style="list-style-type: none">更新“升级管理”一章。更新“管理许可”一章。其他更正和次要更新。

第 2 章 入门

2.1 关于本指南

本指南为您提供了部署和配置 SAP BusinessObjects Business Intelligence platform (BI 平台) 的信息和步骤。提供了执行常见任务的过程，并为所有高级主题提供了概念性信息和技术详细信息。

有关安装此产品的信息，请参阅《SAP BusinessObjects Business Intelligence 平台安装指南》。

2.1.1 本指南面向的用户

本指南介绍了 BI 平台的部署和配置。如果要执行以下任一任务，建议参阅本指南：

- 计划第一次部署
- 配置第一次部署
- 对现有部署的体系结构进行重大更改
- 提高系统的性能。

本帮助适用于那些负责配置、管理和维护 BI 平台安装的系统管理员使用。熟悉操作系统和网络环境很有用，同样，大致了解 Web 应用程序服务器管理和脚本技术也大有裨益。但是，为了对各种层次的管理人员都有所帮助，本指南旨在提供足够的背景和概念性信息，以便详细阐明所有管理任务和功能。

2.1.2 Business Intelligence 平台简介

BI 平台是一款灵活且可扩展的解决方案，可通过任何 Web 应用程序（Intranet、Extranet、Internet 或企业门户）以多种形式（仪表板和交互式报表）为终端用户提供信息。作为一种用于创建报表、分析和信息传送的集成式套件，BI 平台提供了可提高最终用户生产效率和减少管理工作量的解决方案。不管是将它用于分销售周报表、为客户提供个性化的服务产品，还是将重要信息集成到公司门户，BI 平台都提供了延伸到组织内外的实际利益。

2.1.3 变量

以下变量的使用贯穿本指南。

变量	说明
INSTALLDIR	BI 平台的安装目录。 在 Windows 中，默认目录为 C:\Program Files (x86)\SAP BusinessObjects\。
PLATFORM64DIR	Unix 操作系统的名称。接受的值如下： <ul style="list-style-type: none">• aix_rs6000_64• linux_x64• solaris_sparcv9• hpux_ia64
SCRIPTDIR	管理 BI 平台的脚本所在的目录。 在 Windows 上，目录为安装目录\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts。 在 Unix 上，目录为安装目录/sap_bobj/enterprise_xi40/PLATFORM64DIR/scripts。

2.1.4 术语

整个 BI 平台文档中使用的术语如下：

BI 平台

SAP BusinessObjects Business Intelligence 平台的简写形式。

CMS

中央管理服务器。

CMS 数据库

CMS 用于存储有关 BI 平台信息的数据库。

Web 应用程序服务器

处理动态内容的 Web 应用程序服务器。例如，4.1 的捆绑的 Web 应用程序服务器是 Tomcat 7。

主要版本

软件版本，例如 4.0。

修补程序

特定支持包版本的小范围更新。

加载项产品

可以与 BI 平台一起使用，但有自己的安装程序的产品，例如 SAP BusinessObjects Explorer。

升级

使用升级管理应用程序在相同的主要版本部署之间（例如 4.0 到 4.0）传输 Business Intelligence 内容。

升级

完成迁移过程所需的全部计划、准备、迁移和后处理。

安装

由计算机上的安装程序创建的 BI 平台文件的实例。

审核数据存储 (ADS)

用于存储审核数据的数据库。

捆绑的数据库；捆绑的 Web 应用程序服务器

与 BI 平台一起交付的数据库或 Web 应用程序服务器。

支持包

次要或主要版本的更新。

服务器

BI 平台流程。托管一项或多项服务的服务器。

服务器智能代理 (SIA)

SIA 是管理一组服务器的过程。管理任务包括停止、启动和重新启动服务器。

次要版本

软件版本，例如 4.1。

群集密钥

用于解密 CMS 数据库中的密钥。您可以使用 CCM 更改群集密钥，但是您不能像重置密码一样重置此密钥。这是一个用于加密内容的加密密钥，因此切勿丢失。

群集 (动词)

群集的意思是创建一个群集。例如，要创建群集：

- 1 在计算机上安装 CMS 和 CMS 数据库。
- 2 在计算机 B 上安装 CMS。
- 3 将计算机 B 上的 CMS 指向计算机 A 上的 CMS 数据库。

群集（名词）

群集是两个或多个一起工作并使用单一 CMS 数据库的中央管理服务器（CMS）。

节点

在同一计算机上运行且由相同的服务器智能代理（SIA）管理的一组 BI 平台服务器。

计算机

BI 平台软件安装在计算机上。

迁移

使用升级管理工具传输早期主要版本（例如 XI 3.1）中的 Business Intelligence 内容的过程。部署相同的主要版本时不可使用，请参阅“升级”。

部署

安装、配置 BI 平台软件，并在一个或多个计算机上运行。

2.2 开始之前

2.2.1 关键概念

2.2.1.1 服务器智能

服务器智能是 BI 平台的核心组件。中央管理控制台（CMC）中应用的服务器进程更改将由中央管理服务器（CMS）传播至对应的服务器对象。服务器智能代理（SIA）既可在服务器遇到意外情况时自动重新启动或关闭服务器，也可由管理员在管理节点时进行访问。

CMS 可将服务器信息存储在 CMS 系统之中，以便能够轻松地恢复默认服务器设置。由于 SIA 将定期查询 CMS，请求提供其托管服务器的信息，因此 SIA 知道服务器应处于何种状态以及何时应采取操作。

注意：

BI 平台安装是计算机上的安装程序创建的 BI 平台文件的唯一实例。BI 平台安装的实例只能在单个群集内使用。不支持属于共享同一 BI 平台安装的不同群集的节点，因为此类部署无法修补或更新。只有 Unix 平台才能支持在同一计算机上进行软件的多次安装，但仅限于使用唯一用户帐户执行每次安装且安装到单独文件夹时，这样，才能避免安装之间共享任何文件。请记住，群集中的所有计算机的版本和修补程序级别都必须相同。

相关主题

- 第 32 页上的“[服务器、主机和群集](#)”

2.2.1.2 服务器、服务、节点和主机

BI 平台使用术语“服务器”和“服务”指代运行于 BI 平台计算机上的两种类型的软件。

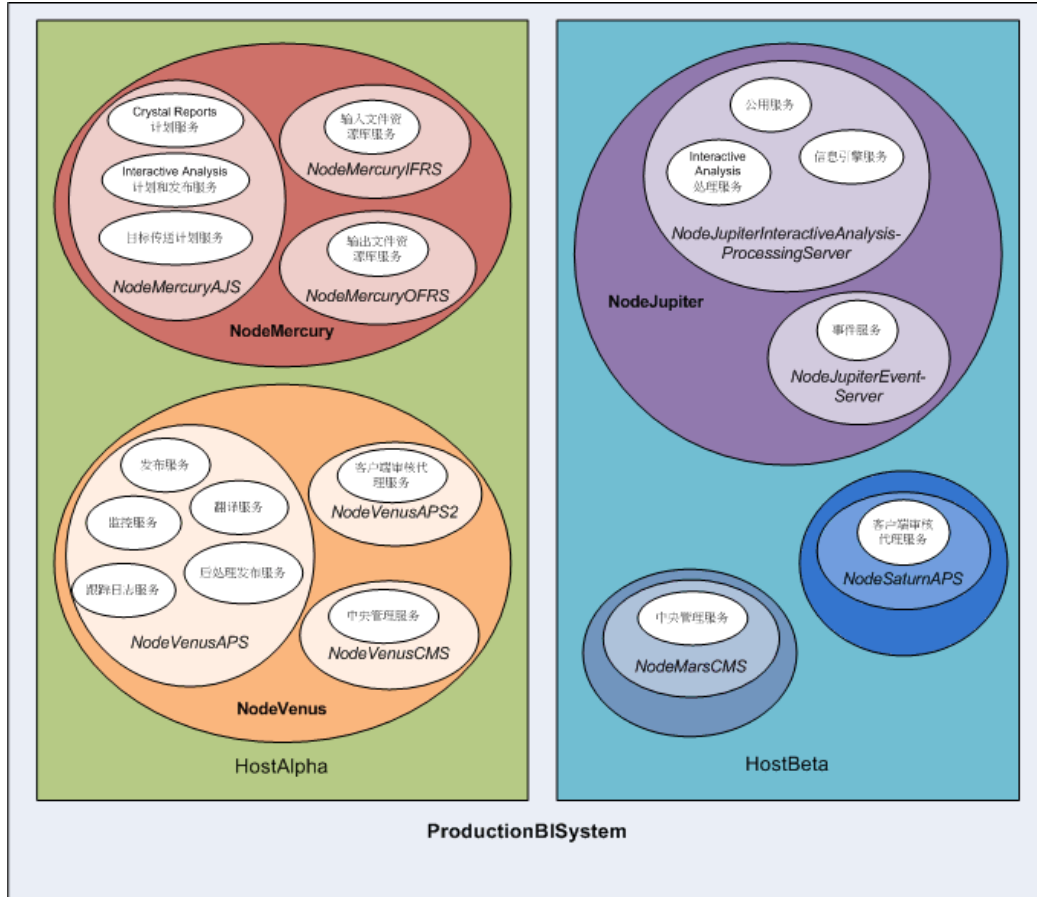
服务器一词用于描述承载一个或多个服务的操作系统级进程（在某些系统中，这称为后台驻留程序）。例如，中央管理服务器（CMS）和自适应处理服务器都是服务器。服务器采用特定操作系统帐户运行，并且有自己的进程 ID（PID）。

“服务”是执行特定功能的服务器子系统。服务采用父容器（服务器）的进程 ID 在其服务器的内存空间内运行。例如，Web Intelligence 计划服务是运行于自适应作业服务器内的一个子系统。

节点是运行于同一主机上并由相同服务器智能代理（SIA）管理的 BI 平台服务器的集合。一台主机上可以有一个或多个节点。

BI 平台可安装在一台计算机上，也可分布在 Intranet 的不同计算机上，或者分散的广域网（WAN）上。

下图所示为 BI 平台的假设安装。在实际安装中，主机、节点、服务器和服务的数量以及服务器和服务的类型都会有所不同。



两个主机组成了名为 ProductionBISystem 的群集：

- 名为 HostAlpha 的主机已安装 BI 平台并配置有两个节点：
 - NodeMercury 包含承载计划和发布报表服务的自适应作业服务器 (NodeMercury.AJS)、承载存储输入报表服务的输入文件资源库服务器 (NodeMercury.IFRS) 和承载存储报表输出服务的输出文件资源库服务器 (NodeMercury.OFRS)。
 - NodeVenus 包含承载提供发布、监控和翻译功能服务的自适应处理服务器 (NodeVenus.APS)、承载提供客户端审核服务的自适应处理服务器 (NodeVenus.APS2) 和承载提供 CMS 服务的中央管理服务器 (NodeVenus.CMS)。
- 名为 HostBeta 的主机已安装 BI 平台，并配置有三个节点：
 - NodeMars 包含提供 CMS 服务的中央管理服务器 (NodeMars.CMS)。在两台计算机上配备 CMS，可以提供负载平衡、迁移和故障转移功能。
 - NodeJupiter 包含提供 Web Intelligence 报表创建服务的 Web Intelligence 处理服务器 (NodeJupiter.Web Intelligence) 以及提供报表文件监控的事件服务器 (NodeJupiter.EventServer)。
 - NodeSaturn 包含承载提供客户端审核服务的自适应处理服务器 (NodeSaturn.APS)。

2.2.2 关键管理工具

2.2.2.1 系统配置向导

系统配置向导是一种工具，可用于简单快捷地配置 BI 平台部署。该向导通过基本配置选项进行引导，以使用以下普通设置生成有效的部署：

- 希望哪些产品的服务器随 BI 平台一起自动启动
- 是否希望为最大化性能或有限硬件资源优化部署
- 系统文件夹的位置

默认情况下，向导设置为在登录中央管理控制台（CMC）时自动运行，但用户可在向导中更改此设置。也可从 CMC 的“管理”区域随时启动向导。

2.2.2.2 中央管理控制台（CMC）

中央管理控制台（CMC）是一款基于 Web 的工具，您可用来执行管理任务（其中包括用户、内容和服务器管理）和配置安全设置。由于 CMC 是基于 Web 的应用程序，因此可以在可连接到 Web 应用程序服务器的任何计算机上的 Web 浏览器中执行所有这些管理任务。

所有用户都可以登录到 CMC 以更改其自身的首选项设置。除非明确授予用户更改管理设置的权限，否则只有 Administrators 组的成员能够更改管理设置。您可在 CMC 中分配角色，授予用户执行次要管理任务的权限，例如：管理组中的用户以及管理属于您团队的文件夹中的报告。

2.2.2.3 中央配置管理器（CCM）

中央配置管理器 (CCM) 是一个以两种形式提供的服务器故障排除和节点管理工具。在 Microsoft Windows 环境中, CCM 可用于通过其图形用户界面 (GUI) 或命令行管理本地和远程服务器。在 Unix 环境中, CCM 外壳脚本 (ccm.sh) 用于通过命令行管理服务器。

如果使用默认的捆绑式 Tomcat Web 应用程序服务器, 请使用 CCM 创建并配置节点以启动或停止 Web 应用程序服务器。在 Windows 上, 它还允许配置网络参数, 比如安全套接字层 (SSL) 加密。这些参数应用于节点内的所有服务器。

注意:

大多数服务器管理任务现在是通过 CMC (而不是 CCM) 处理的。CCM 现在仅用于故障排除和节点配置。

2.2.2.4 资源库诊断工具

资源库诊断工具 (RDT) 可以扫描、诊断和修复中央管理服务器 (CMS) 系统数据库与文件资源库服务器 (FRS) 文件存储之间可能存在的 inconsist 之处。可以为 RDT 在停止前将找到和修复的错误数设置限制。

RDT 应该在恢复 BI 平台系统之后使用。

2.2.2.5 升级管理工具

升级管理工具 (原来称为 “导入向导”) 是作为 BI 平台的一部分安装的, 用于引导管理员从 BI 平台的早期版本中导入用户、组和文件夹。此外, 还可用于导入和升级事件、服务器组、资源库对象和日历。

有关早期版本的 BI 平台升级的相关信息, 请参阅《SAP BusinessObjects Business Intelligence 平台升级指南》。

2.2.3 关键任务

视情况而定，可能需要重点阅读本帮助的特定小节，在这些特定小节中可能有其他可用资源。对于下列每种情况，都列出了建议的任务和阅读主题。

相关主题

- 第 27 页上的[“计划或执行第一次部署”](#)
- 第 27 页上的[“配置部署”](#)
- 第 28 页上的[“提高系统的性能”](#)
- 第 67 页上的[“中央管理控制台（CMC）”](#)

2.2.3.1 计划或执行第一次部署

如果计划或执行 BI 平台的首次部署，建议阅读本指南中的下列章节：

- 要熟悉 BI 平台组件，请参阅“体系结构概述”
- 了解 BI 平台组件之间的通信
- 安全概述
- 如果要使用第三方身份验证，请参阅“BI 平台中的身份验证选项”
- 安装后阅读“使用 CMC 中的“服务器”管理区域”

有关安装 BI 平台的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台安装指南》。要评估需求并设计最适合自己使用的部署体系结构，请参阅《SAP BusinessObjects Business Intelligence 平台计划指南》。

相关主题

- 第 29 页上的[“体系结构概述”](#)
- 第 169 页上的[“BI 平台组件间的通信”](#)
- 第 139 页上的[“安全概述”](#)
- 第 205 页上的[“BI 平台中的身份验证选项”](#)
- 第 344 页上的[“使用 CMC 中的“服务器”管理区域”](#)

2.2.3.2 配置部署

如果刚刚完成 BI 平台的安装并需要执行初始配置任务（如防火墙配置和用户管理），建议阅读以下小节。

相关主题

- 第 81 页上的[“系统配置向导介绍”](#)
- 第 169 页上的[“BI 平台组件间的通信 ”](#)
- 第 139 页上的[“安全概述 ”](#)
- 第 625 页上的[“关于监控”](#)

2.2.3.3 提高系统的性能

如果要评估部署的效率并对其进行微调以最大化资源，请阅读以下部分：

- 如果希望使用部署模板来配置系统，请参阅“系统配置向导介绍”。
- 如果要监控现有系统，请阅读“关于监控”。
- 有关使用 CMC 中服务器的日常维护任务和程序，请阅读“使用 CMC 中的“服务器”管理区域”。

相关主题

- 第 81 页上的[“系统配置向导介绍”](#)
- 第 625 页上的[“关于监控”](#)
- 第 344 页上的[“使用 CMC 中的“服务器”管理区域”](#)

2.2.3.4 在 CMC 中处理对象

对象是指在 BI 平台或其他软件中创建且在 BI 平台资源库中进行存储和管理的文档或文件。如果要在 CMC 中处理对象，请阅读以下小节：

- 有关在 CMC 中设置用户和组的信息，请参阅“账户管理概述”。
- 要为对象设置安全性，请参阅“BI 平台中权限的作用机制”。
- 有关处理对象的一般信息，请参阅《SAP BusinessObjects Business Intelligence 平台用户指南》。

相关主题

- 第 91 页上的[“帐户管理概述”](#)
- 第 112 页上的[“权限在 BI 平台中如何运作”](#)

第 3 章 体系结构

3.1 体系结构概述

本节概述了组成 SAP BusinessObjects Business Intelligence 平台的整体平台体系结构、系统和服务组件。此信息不仅有助于管理员了解系统要点，还有助于针对系统部署、管理和维护制定计划。

注意：

有关此版本支持的平台、数据库、Web 应用程序服务器、Web 服务器和其他系统的列表，请参阅 SAP Support Portal 中 SAP BusinessObjects 部分的产品可用性矩阵（支持的平台/PAR），网址为：
<https://service.sap.com/bosap-support>。

Business Intelligence (BI) 平台旨在提高各种用户和部署方案的性能。例如，专业化的平台服务可以根据时间和事件来处理数据的按需访问及报表生成，或报表计划。可以通过创建专用服务器来承载特定服务，以便卸载占用大量处理器资源的计划和处理任务。此体系结构旨在满足几乎任何 BI 部署的需求，而且非常灵活，可以从使用单个工具的几位用户发展到使用多个工具和接口的数万位用户。

开发人员可以使用 Web 服务、Java 或 .NET 应用程序编程接口 (API) 将 BI 平台集成到贵组织的其他技术系统。

最终用户可以使用专用的工具和应用程序访问、创建、编辑报表并与其交互，这些工具和应用程序包括：

- 由 BI 平台客户端工具安装程序安装的客户端：
 - Web Intelligence 胖客户端
 - 业务视图管理器
 - 报表转换工具
 - Universe 设计工具
 - 作为 Web 服务的查询
 - 信息设计工具（原来称为“信息设计器”）
 - 翻译管理工具（原来称为翻译管理器）
 - 微件（原来称为 BI 微件）
- 单独提供的客户端：
 - SAP Crystal Reports
 - SAP BusinessObjects Dashboards（原来称为 Xcelsius）
 - SAP BusinessObjects Analysis（原来称为 Voyager）

- BI 工作区（原来称为 Dashboard Builder）

IT 部门可以使用数据和系统管理工具，其中包括：

- 报表查看器
- 中央管理控制台（CMC）
- 中央配置管理器（CCM）
- 资源库诊断工具（RDT）
- 数据联合管理工具
- 升级管理工具（原来称为导入向导）
- Universe 设计工具（原来称为 Universe Designer）
- SAP BusinessObjects Mobile

要实现灵活性、可靠性和可伸缩性，可在一台计算机或多台计算机上安装 BI 平台组件。甚至可在同一计算机上同时安装两个不同版本的 BI 平台，不过仅建议在升级过程中或出于测试目的使用这种配置。

纵向缩放（一台计算机运行多个或全部服务器端进程）服务器进程可降低成本，横向缩放（在两台或多台联网计算机之间分配服务器进程）可改善性能。也可在多台计算机上运行数个冗余版本的相同服务器进程，以便在主要进程遇到问题时处理过程仍可继续。

注意：

虽然可以混合使用 Windows 和 Unix 或 Linux 平台，但是最好不要对中央管理服务器（CMS）进程使用混合的操作系统。

3.1.1 部件图

SAP BusinessObjects Business Intelligence 平台是商务智能（BI）平台，可提供企业级别分析和报表创建工具。可以对大量受支持数据库系统中的数据进行分析（包括文本或多维 OLAP 系统），以及将 BI 报表以各种不同格式发布到许多不同的发布系统。

SAP Community Network 上的这张体系结构图阐明了 BI 平台组件（包括服务器和客户端工具、其他分析产品、Web 应用程序组件以及可能是 BI 平台架构 <http://scn.sap.com/docs/DOC-43663> 一部分的数据库）。

BI 平台以只读连接形式向贵组织的数据库提供报表，并使用其自己的数据库存储其配置、审核和其他运营信息。系统创建的 BI 报表可以发送至各种目标（包括文件系统和电子邮件）或通过网站或门户进行访问。

BI 平台是一种独立系统，它既可安装在单一计算机上（例如，作为小型开发或预生产测试环境），也可扩展到包含运行不同组件的众多计算机的群集（例如，作为大规模生产环境）。

3.1.2 体系结构层

可以将 SAP BusinessObjects Business Intelligence 平台看作一系列概念层：

客户端层

客户端层包含所有与 BI 平台交互、旨在提供各种报表、分析和管理功能的桌面客户端应用程序。示例包括中央配置管理器（BI 平台安装程序）、信息设计工具（BI 平台客户端工具安装程序）和 SAP Crystal Reports 2011（另行提供和安装）。

Web 层

Web 层包含部署在 Java Web 应用程序服务器上的 Web 应用程序。Web 应用程序通过 Web 浏览器为最终用户提供 BI 平台功能。Web 应用程序示例包括中央管理控制台（CMC）管理 Web 界面和 BI 启动板。

Web 层还包含 Web 服务。Web 服务通过 Web 应用程序服务器为软件工具提供 BI 平台功能，例如会话身份验证、用户权限管理、计划、搜索、管理、报表创建和查询管理。例如，Live Office 这个产品使用 Web 服务将 BI 平台报表创建功能集成到 Microsoft Office 产品中。

管理层

管理层（也称为智能层）负责协调和控制 BI 平台的所有组件。它包括中央管理服务器（CMS）、事件服务器和相关服务。CMS 维护安全和配置信息、将服务请求发送至服务器、管理审核以及维护 CMS 系统数据库。事件服务器管理在存储层发生的基于文件的事件。

存储层

存储层负责处理文件，如文档和报表。

输入文件资源库服务器管理包含报表中所用信息的文件，例如下列文件类型：.rpt、.car、.exe、.bat、.js、.xls、.doc、.ppt、.rtf、.txt、.pdf、.wid、.rep、.unv。

输出文件资源库服务器管理系统创建的报表，例如下列文件类型：.rpt、.csv、.xls、.doc、.rtf、.txt、.pdf、.wid、.rep。

此外，当用户访问报表时，存储层还处理报表缓存以节省系统资源。

处理层

处理层分析数据并生成报表。只有此层访问包含报表数据的数据库。此层包含自适应作业服务器、连接服务器（32 位和 64 位）和处理服务器（如自适应处理服务器或 Crystal Reports 处理服务器）。

数据层

数据层包括承载 CMS 系统数据库和审核数据存储的数据库服务器。此外，还包括任何包含关系、OLAP 或用于报表创建和分析应用程序的其他数据类型的数据数据库服务器。

3.1.3 数据库

BI 平台使用多种不同数据库。

- 报表数据库

它表示组织的信息。这是由 SAP BusinessObjects Business Intelligence 套件产品分析和报告的源信息。通常情况下，信息存储在关系数据库中，但是也可以包含在文本文件、Microsoft Office 文档或 OLAP 系统中。

- CMS 系统数据库

CMS 系统数据库用于存储 BI 平台信息，如用户、服务器、文件夹、文档、配置和身份验证详细信息。此数据库由中央管理服务器（CMS）进行维护，有时称为系统资源库。

- 审核数据存储

审核数据存储（ADS）用于存储有关 BI 平台中发生的可跟踪事件的信息。此信息可用于监控系统组件的使用、用户活动或者日常运营的其他方面。

- 生命周期管理数据库

生命周期管理数据库跟踪与 BI 平台安装及更新相关的配置和版本信息。

- 监控数据库

监控过程使用 Java Derby 数据库存储系统配置和组件信息以提供 SAP 支持。

如果没有用于 CMS 系统和审核数据存储数据库的数据库服务器，BI 平台安装程序可为用户安装并配置一个。建议根据数据库服务器供应商提供的信息评估要求，以确定最符合贵组织要求的受支持数据库。

3.1.4 服务器、主机和群集

BI 平台由在一个或多个主机上运行的服务器集合组成。小规模安装（例如测试或开发系统）可以采用单个主机运行 Web 应用程序服务器、数据库服务器和所有 BI 平台服务器。

中等和大规模安装可以在多个主机上运行服务器。例如，可以配合使用 Web 应用程序服务器主机和 BI 平台服务器主机。这会释放 BI 平台服务器主机上的资源，从而使信息处理效率高于同时承载 Web 应用程序服务器的配置。

大规模安装可在一个群集中搭配使用多台 BI 平台服务器主机。例如，如果组织的 SAP Crystal Reports 用户众多，则可在多台 BI 平台服务器主机上创建 Crystal Reports 处理服务器，确保具备大量处理客户端请求的可用资源。

配备多个服务器的优势包括：

- 提高性能

相比单台 BI 平台服务器主机，多台 BI 平台服务器主机处理一系列报表创建信息的速度更快速。

- 负载均衡

如果某个服务器的负载比群集中的其他服务器高，CMS 会自动将新工作发送至具有更多资源的服务器。

- 提高可用性

如果服务器遇到意外情况，CMS 会自动将工作重新安排给其他服务器，直至意外情况得以解决。

3.1.5 Web 应用程序服务器

Web 应用程序服务器充当 Web 浏览器或胖应用程序与 BI 平台之间的转换层。支持运行于 Windows、Unix 和 Linux 上的 Web 应用程序服务器。

有关支持 Web 应用程序服务器的详细列表，请查询位于 <https://service.sap.com/bosap-support> 的“支持平台/PAR”。

如果没有可与 BI 平台配合使用的 Web 应用程序服务器，安装程序会为您安装和配置 Tomcat Web 应用程序服务器。建议根据 Web 应用程序服务器供应商提供的信息评估要求，以确定哪个受支持 Web 应用程序服务器最符合您的组织要求。

注意：

当配置生产环境时，建议将 Web 应用程序服务器部署在单独的系统中。在生产环境中，在同一台主机上运行 BI 平台和 Web 应用程序服务器可能会降低性能。

3.1.5.1 Web 应用程序容器服务器（WACS）

需要一个 Web 应用程序服务器承载 BI 平台 Web 应用程序。

如果您是需执行高级管理任务的高级 Java Web 应用程序服务器管理员，请使用受支持的 Java Web 应用程序服务器承载 BI 平台 Web 应用程序。如果要使用受支持的 Windows 操作系统承载 BI 平台，并希望简化 Web 应用程序服务器安装过程，或者没有用于管理 Java Web 应用程序服务器的资源，则可以在安装 BI 平台时安装 Web 应用程序容器服务（WACS）。

WACS 是一种 BI 平台服务器，允许运行诸如中央管理控制台（CMC）、BI 启动板和 Web 服务等 BI 平台 Web 应用程序，而无需提前安装 Java Web 应用程序服务器。

使用 WACS 有诸多优点：

- 安装、维护和配置 WACS 所需的工作量最少。WACS 由 BI 平台安装程序安装和配置，无需更多步骤即可开始使用。
- WACS 不要求具备 Java 应用程序服务器管理和维护技能。
- WACS 提供了一个与 BI 平台服务器一致的管理界面。
- 与其他 BI 平台服务器一样，WACS 可以安装在专用主机上。

注意：

使用 WACS 取代专用 Java Web 应用程序服务器有一些限制：

- 只有支持的 Windows 操作系统才会提供 WACS。
- 自定义 Web 应用程序不能部署到 WACS，因为它只支持随 BI 平台安装的 Web 应用程序。
- WACS 不能与 Apache 负载均衡器一起使用。

除了 WACS 以外，还可以使用一个专用 Web 应用程序服务器。这样可以由专用的 Web 应用程序服务器承载自定义 Web 应用程序，而由 WACS 承载 CMC 和其他 BI 平台 Web 应用程序。

3.1.6 软件开发工具包

软件开发工具包（SDK）可供开发人员将 SAP BusinessObjects Business Intelligence 平台的各方面合并到组织自己的应用程序和系统中。

BI 平台提供用于在 Java 和 .NET 平台上开发软件的 SDK。

注意：

默认情况下并不安装 BI 平台 .NET SDK，而必须从 SAP Service Marketplace 下载该程序。

BI 平台支持以下 SDK：

- Business Intelligence 平台 Java SDK 和 .NET SDK

BI 平台 SDK 可以使应用程序执行诸如身份验证、会话管理、资源库对象处理、报告计划和发布以及服务器管理等任务。

注意：

要完整访问安全性、服务器管理和审核功能，请使用 Java SDK。

- Business Intelligence 平台 RESTful Web 服务 SDK

BI 平台 RESTful Web 服务 SDK 允许用户使用 HTTP 协议访问 BI 平台。可以使用此 SDK 登录 BI 平台, 浏览 BI 平台资源库, 访问资源, 并执行基本资源计划。可以通过使用任何编程语言编写支持 HTTP 协议的应用程序或使用任何支持 HTTP 请求的工具访问此 SDK。

- Business Intelligence 平台 Java 使用者 SDK 和 .NET 使用者 SDK

基于 SOAP 的 Web 服务实现, 可用于处理用户身份验证和安全性、文档和报表访问、计划、发布以及服务器管理。

BI 平台 Web 服务使用诸如 XML、SOAP、AXIS 2.0 和 WSDL 等标准。此平台遵循 WS-Interoperability Basic Profile 1.0 Web 服务规范。

注意:

当前仅支持具有以下负载平衡器配置的 Web 服务应用程序:

- 1 源 IP 地址持久性。
- 2 源 IP 和目标端口持久性 (仅可用于 Cisco 内容服务交换机)。
- 3 SSL 持久性。
- 4 基于 Cookie 的会话持久性。

注意:

SSL 持久性可能导致某些 Web 浏览器出现安全性和可靠性问题。请与网络管理员联系, 以确定 SSL 持久性是否适用于贵组织。

- 数据访问驱动程序和连接 Java SDK

这些 SDK 可用于为连接服务器创建数据库驱动程序并管理数据库连接。

- 语义层 Java SDK

语义层 Java SDK 可用于开发在 Universe 和连接上执行管理和安全任务的 Java 应用程序。例如, 可以实现用于将 Universe 发布到资源库或从资源库中将安全连接检索到工作区的服务。该应用程序可嵌入到作为 OEM 与 BI 平台相集成的商务智能解决方案中。

- 报表应用程序服务器 Java SDK 和 .NET SDK

报表应用程序服务器 SDK 允许应用程序打开、创建和修改现有 Crystal 报表, 包括设置参数值、更改数据源以及导出为其他格式 (格式包括 XML、PDF、Microsoft Word 和 Microsoft Excel)。

- Java 和 .NET Crystal 报表查看器

查看器允许应用程序显示和导出 Crystal 报表。可使用以下查看器:

- DHTML 报表页面查看器: 显示数据并允许向下钻取、页面导航、缩放、提示、搜索、突出显示、导出和打印。
- 报表部件查看器: 提供了查看报表单独部件 (包括图表、文本和字段) 的功能。

- 报表引擎 Java SDK 和 .NET SDK

报表引擎 SDK 允许应用程序与使用 SAP BusinessObjects Web Intelligence 创建的报表交互。

报表引擎 SDK 包含可用于构建 Web 报表设计工具的库。使用这些 SDK 构建的应用程序可以查看、创建或修改各种不同的 Web Intelligence 文档。用户可以通过添加、删除和修改对象 (例如表、统计图、条件和过滤器) 来修改文档。

- 平台搜索 SDK: 平台搜索 SDK 是客户端应用程序和平台搜索服务之间的接口。平台搜索支持平台搜索 SDK 自带的公共 SDK。

当搜索请求参数通过客户端应用程序发送给 SDK 层时，SDK 层会将请求参数转换为 XML 编码格式，并将其传递给平台搜索服务。

可结合使用 SDK 向应用程序提供大量 BI 功能。有关这些 SDK 的更多信息，包括开发人员指南和 API 参考，请参阅<http://help.sap.com>。

3.1.7 数据源

3.1.7.1 Universe

Universe 通过使用业务语言（而不是数据语言）访问、处理和组织数据，将数据的复杂性抽象化。此业务语言作为对象存储在 Universe 文件中。Web Intelligence 和 Crystal Reports 使用 Universe 来简化简单到复杂的最终用户查询和分析所需的用户创建进程。

Universe 是 BI 平台的核心组件。所有 Universe 对象和连接均由连接服务器存储在中央资源库中并加以保护。Universe 设计工具需要登录到 BI 平台才能访问系统和创建 Universe。也可以从设计环境中在组或个体用户级别管理 Universe 访问和行级别安全性。

语义层允许 Web Intelligence 利用多个同步数据提供者（包括联机分析处理（OLAP）和公共仓库元模型（CWM）数据源）来传递文档。

3.1.7.2 业务视图

业务视图为报表开发人员将数据的复杂性抽象化，从而简化报表的创建和交互过程。业务视图有助于分隔数据连接、数据访问、业务元素和访问控制。

业务视图只能由 Crystal Reports 使用，并且旨在简化创建 Crystal 报表所需的数据访问和查看时安全性。业务视图在单个视图中支持多个数据源的组合。BI 平台充分支持业务视图。

Business Intelligence 平台包括一系列专用且预先配置的平台管理服务，用于执行诸如密码管理、服务器量度和用户访问控制等任务，以支持分散管理功能。

3.1.8 身份验证和单一登录

系统安全性由中央管理服务器（CMS）、安全插件和第三方身份验证工具（如 SiteMinder 或 Kerberos）管理。这些组件验证用户身份并授予用户对 BI 平台及其文件夹与其他对象的访问权。

可以使用以下用户身份验证单一登录安全插件：

- Enterprise（默认），包括用于 SAML、X.509、SAP NW SSO 等身份验证方法的受信任的身份验证支持，以及应用程序服务器支持的其他方法。
- LDAP
- Windows Active Directory (AD)

使用企业资源计划（ERP）系统时，可使用单一登录对访问 ERP 系统的用户进行身份验证，以便提供有关 ERP 数据的报告。系统支持以下 ERP 系统用户身份验证单一登录：

- SAP ERP 和 Business Warehouse (BW)
- Oracle 电子商务套件 (EBS)
- Siebel Enterprise
- JD Edwards Enterprise One
- PeopleSoft Enterprise

3.1.8.1 安全插件

安全插件允许将用户帐户和组从第三方系统映射到 BI 平台，以此实现帐户创建及管理过程的自动化。可以将第三方用户帐户映射到现有 Enterprise 用户帐户，也可以创建对应于外部系统中每个映射条目的新 Enterprise 用户帐户。

安全插件动态地维护第三方用户和组列表。在将轻量目录访问协议（LDAP）或 Windows Active Directory (AD) 组映射到 BI 平台之后，属于该组的所有用户均可登录到 BI 平台。随后对第三方组成员资格的更改将自动予以传播。

BI 平台支持以下安全插件：

- Enterprise 安全插件

中央管理服务器（CMS）处理诸如用户帐户、组成员资格以及定义用户和组权限的对象权限等安全信息。这称为 Enterprise 身份验证。

Enterprise 身份验证始终处于启用状态；无法将其禁用。如果要创建的独立帐户和组用于 BI 平台，或者尚未在 LDAP 或 Windows AD 服务器上设置用户和组的层次结构，请使用系统默认的 Enterprise 身份验证。

受信任的身份验证是 Enterprise 身份验证的一个组件，可与第三方单一登录解决方案相集成，例如 Java 身份验证和授权服务（JAAS）。与中央管理服务器建立了信任关系的应用程序可以使用“受信任的身份验证”，以便允许用户不提供密码便可登录。

- LDAP 安全插件
- Windows AD

注意：

虽然用户可以通过 CMC 配置为 BI 平台和自定义应用程序配置 Windows AD 身份验证，但是 CMC 和 BI 启动板并不支持使用 NTLM 的 Windows AD 身份验证。CMC 和 BI 启动板仅支持以下身份验证方法：Windows AD 及 Kerberos、LDAP、Enterprise 和受信任的身份验证。

3.1.8.2 企业资源规划（ERP）集成

企业资源规划（ERP）应用程序通过收集与日常运营相关的实时信息来支持组织进程的基本功能。BI 平台支持单一登录和来自以下 ERP 系统的报表：

- SAP ERP 和 Business Warehouse (BW)
- Siebel Enterprise
- Oracle 电子商务套件
- JD Edwards EnterpriseOne
- PeopleSoft Enterprise

注意：

- 默认安装 SAP ERP 和 BW 支持。如果希望不支持 SAP ERP 或 BW，可使用“定制/扩展”安装选项取消选择 SAP 集成支持。
- 默认情况下，不会安装 Siebel Enterprise、Oracle 电子商务套件、JD Edwards EnterpriseOne 或 PeopleSoft 的支持。可使用“定制/扩展”安装选项选择和安装非 SAP ERP 系统集成。

有关 BI 平台支持的特定版本的详细信息，请参阅位于 <https://service.sap.com/bosap-support> 的“支持的平台/PAR”。

要配置 ERP 集成，请参阅本指南的“ERP 环境补充配置”一章。

3.1.9 SAP 集成

BI 平台使用以下 SAP 工具与现有 SAP 基础架构集成：

- SAP 系统全景目录 (SLD)

SAP NetWeaver 系统全景目录是一种与软件生命周期管理相关的系统全景信息的中央源。通过提供一个包含所有可安装 SAP 软件信息和有关全景中已安装系统的自动更新数据的目录，用户便有了工具支持基础，以计划系统全景中的软件生命周期任务。

BI 平台安装程序将在 SLD 中注册供应商和产品的名称及版本，以及服务器和前端组件的名称、版本及位置。

- SAP Solution Manager

SAP Solution Manager 是一个提供集成内容、工具和方法的平台，可用于实施、支持、操作和监控企业的 SAP 解决方案和非 SAP 解决方案。

具有 SAP 认证集成的非 SAP 软件可以输入到中央资源库并自动传输到您的 SAP 系统架构目录 (SLD)。然后，SAP 客户就可以在 SAP 系统环境中轻松识别已获得 SAP 认证的第三方产品集成版本。这项服务是除我们第三方产品联机目录以外的另一种第三方产品识别途径。

SAP Solution Manager 是免费向 SAP 客户提供的，无需收取额外费用，它包含对 SAP 支持和 SAP 产品升级路径信息的直接访问。有关 SLD 的详细信息，请参阅“在系统架构中注册 BI 平台”。

- CTS 传输 (CTS+)

更改和传输系统 (CTS) 有助于组织 ABAP 工作台和自定义模式中的开发项目，然后在系统全景中的 SAP 系统之间传输更改。不仅可以传输 ABAP 对象，还可以传输全景中的 Java 对象 (J2EE、JEE) 和特定于 SAP 的非 ABAP 技术 (如 Web Dynpro Java 或 SAP NetWeaver Portal)。

- 使用 CA Wily Introscope 监控

CA Wily Introscope 是一款 Web 应用程序管理产品，用于监控和诊断生产期间在基于 Java 的 SAP 模块内可能出现的性能问题，包括自定义 Java 应用程序的可见性和后端系统的连接。它可用于隔离 NetWeaver 模块中的性能瓶颈，包括各个 Servlet、JSP、EJB、JCO、类、方法等等。它还提供实时低开销监控、端对端事务可见性、分析或容量计划的历史数据、可自定义的仪表盘、自动阈值警报以及用于将监控扩展至 NetWeaver 环境以外的开放式体系结构。

3.1.10 集成版本控制

在服务器系统上组成 BI 平台的文件现已受到版本控制。安装程序将安装和配置 Subversion 版本控制系统，用户也可以输入详细信息以使用现有 Subversion 或 ClearCase 版本控制系统。

利用版本控制系统，可以保留和恢复配置和其他文件的不同修订，这就表示始终可以将系统还原到过去任何时间内的已知状态。

3.1.11 升级路径

可以从之前版本的 SAP BusinessObjects Enterprise (例如 XI 3.x) 升级, 但必须先安装 SAP BusinessObjects Business Intelligence 平台 4.x, 然后通过升级管理工具迁移现有系统中的设置和数据。

有关如何从之前版本升级的信息, 请参阅《SAP BusinessObjects Business Intelligence 平台升级指南》。

3.2 服务器、服务、节点和主机

BI 平台使用术语“服务器”和“服务”指代运行于 BI 平台计算机上的两种类型的软件。

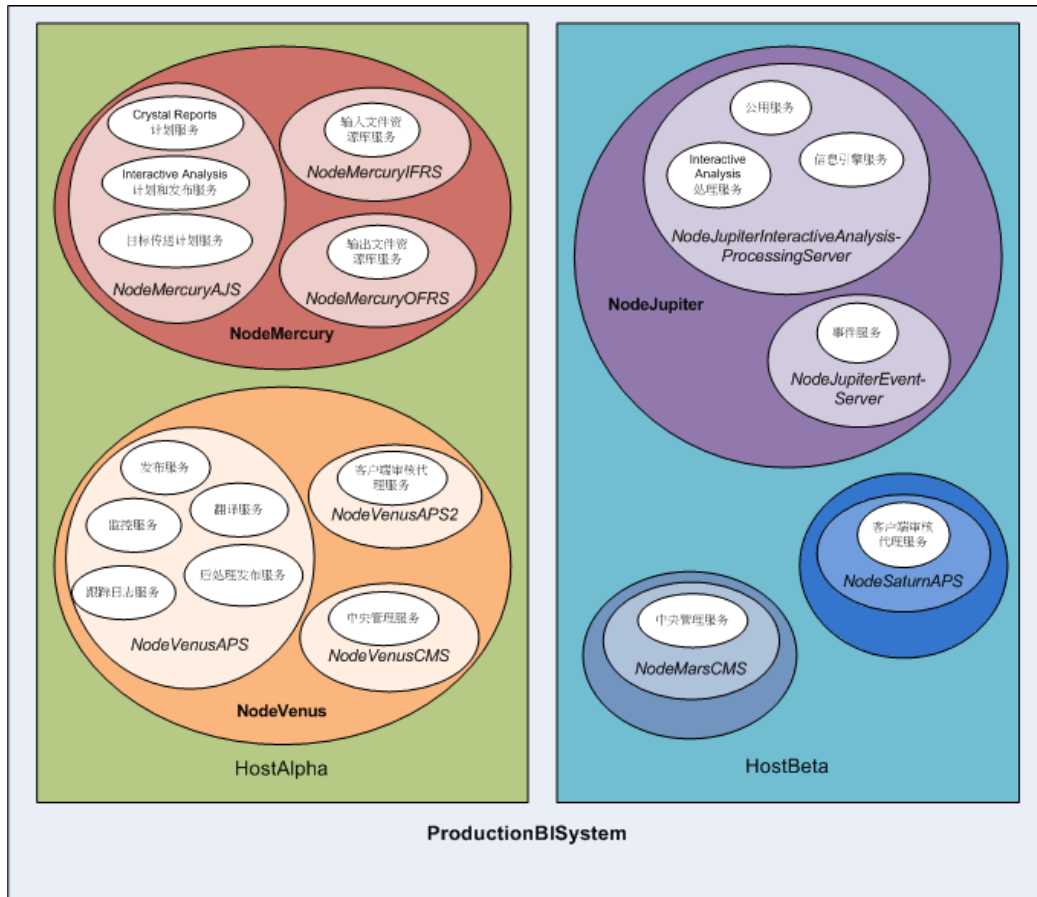
服务器一词用于描述承载一个或多个服务的操作系统级进程 (在某些系统中, 这称为后台驻留程序)。例如, 中央管理服务器 (CMS) 和自适应处理服务器都是服务器。服务器采用特定操作系统帐户运行, 并且有自己的进程 ID (PID)。

“服务”是执行特定功能的服务器子系统。服务采用父容器 (服务器) 的进程 ID 在其服务器的内存空间内运行。例如, Web Intelligence 计划服务是运行于自适应作业服务器内的一个子系统。

节点是运行于同一主机上并由相同服务器智能代理 (SIA) 管理的 BI 平台服务器的集合。一台主机上可以有一个或多个节点。

BI 平台可安装在一台计算机上, 也可分布在 Intranet 的不同计算机上, 或者分散的广域网 (WAN) 上。

下图所示为 BI 平台的假设安装。在实际安装中, 主机、节点、服务器和服务的数量以及服务器和服务的类型都会有所不同。



两个主机组成了名为 ProductionBISystem 的群集:

- 名为 HostAlpha 的主机已安装 BI 平台并配置有两个节点:
 - NodeMercury 包含承载计划和发布报表服务的自适应作业服务器 (NodeMercury.AJS)、承载存储输入报表服务的输入文件资源库服务器 (NodeMercury.IFRS) 和承载存储报表输出服务的输出文件资源库服务器 (NodeMercury.OFRS)。
 - NodeVenus 包含承载提供发布、监控和翻译功能服务的自适应处理服务器 (NodeVenus.APS)、承载提供客户端审核服务的自适应处理服务器 (NodeVenus.APS2) 和承载提供 CMS 服务的中央管理服务器 (NodeVenus.CMS)。
- 名为 HostBeta 的主机已安装 BI 平台, 并配置有三个节点:
 - NodeMars 包含提供 CMS 服务的中央管理服务器 (NodeMars.CMS)。在两台计算机上配备 CMS, 可以提供负载平衡、迁移和故障转移功能。
 - NodeJupiter 包含提供 Web Intelligence 报表创建服务的 Web Intelligence 处理服务器 (NodeJupiter.Web Intelligence) 以及提供报表文件监控的事件服务器 (NodeJupiter.EventServer)。
 - NodeSaturn 包含承载提供客户端审核服务的自适应处理服务器 (NodeSaturn.APS)。

3.2.1 自 XI 3.1 以来所做的服务器更改

下表描述了自 XI 3.1 以来所做的 BI 平台服务器的主要更改。更改类型包括：

- 版本名称已更改、但提供相同或相似功能的服务器。
- 更新版本不再提供的服务器。
- 已整合到自适应服务器中的公共服务或相关服务。

例如，XI 3.1 中由单个作业服务器提供的计划服务已移动到自适应作业服务器 4.0 中。

- 引入的新服务器。

表3-1：服务器更改

XI 3.1	4.0	4.0 Feature Pack 3	4.1
连接服务器 [1]	连接服务器 连接服务器 (32 位)	连接服务器 连接服务器 (32 位)	连接服务器 连接服务器 (32 位)
Crystal Reports 作业服务器	自适应作业服务器	自适应作业服务器	自适应作业服务器
Crystal Reports 处理服务器	Crystal Reports 2011 处理服务器 Crystal Reports 处理服务器 (适用于 SAP Crystal Reports for Enterprise 报表)	Crystal Reports 2011 处理服务器 Crystal Reports 处理服务器 (适用于 SAP Crystal Reports for Enterprise 报表)	Crystal Reports 2011 处理服务器 Crystal Reports 处理服务器 (适用于 SAP Crystal Reports for Enterprise 报表)
仪表盘服务器 (Dashboard Builder) [2]	仪表盘服务器 (BI 工作区)	自 4.0 Feature Pack 3 起不提供	在 4.1 中不可用
仪表盘分析服务器 (Dashboard Builder) [2]	仪表盘分析服务器 (BI 工作区)	自 4.0 Feature Pack 3 起不提供	在 4.1 中不可用
Desktop Intelligence 高速缓存服务器 [3]	自 4.0 起不提供	自 4.0 起不提供	在 4.1 [3] 中不可用

XI 3.1	4.0	4.0 Feature Pack 3	4.1
Desktop Intelligence 作业服务器 [3]	自 4.0 起不提供	自 4.0 起不提供	在 4.1 [3] 中不可用
Desktop Intelligence 处理服务器 [3]	自 4.0 起不提供	自 4.0 起不提供	在 4.1 [3] 中不可用
目标作业服务器	自适应作业服务器	自适应作业服务器	自适应作业服务器
值列表服务器 (LOV)	Web Intelligence 处理服务器	Web Intelligence 处理服务器	Web Intelligence 处理服务器
多维分析服务器	自适应处理服务器	自适应处理服务器	自适应处理服务器
程序作业服务器	自适应作业服务器	自适应作业服务器	自适应作业服务器
报表应用程序服务器 (RAS)	Crystal Reports 2011 报表应用程序服务器 (RAS)	Crystal Reports 2011 报表应用程序服务器 (RAS)	Crystal Reports 2011 报表应用程序服务器 (RAS)
Web Intelligence 作业服务器	自适应作业服务器	自适应作业服务器	自适应作业服务器
Xcelsius 高速缓存服务器 [4]	Dashboard Design 高速缓存服务器 (Xcelsius) [5]	Dashboards 高速缓存服务器 (Xcelsius)	Dashboards 高速缓存服务器 (Xcelsius)
Xcelsius 处理服务器 [4]	Dashboard Design 处理服务器 (Xcelsius) [5]	Dashboards 处理服务器 (Xcelsius)	Dashboards 处理服务器 (Xcelsius)

- [1] 在 4.0 中，连接服务器 32 是指专门连接到无法处理 64 位中间件的数据源的 32 位服务器。连接服务器是指连接到所有其他数据源的 64 位服务器。有关更多信息，请参阅《数据访问指南》。
- [2] 4.0 Feature Pack 3 中已删除仪表盘服务器和仪表盘分析服务器。BI 工作区功能（原来在 XI 3.1 中称为 Dashboard Builder）不再需要服务器配置。
- [3] Desktop Intelligence 在版本 4.0 和 4.0 维护包中不可用。Desktop Intelligence 客户端应用程序可用于版本 4.1，但 Desktop Intelligence 服务器不可用。使用报表转换工具可将 Desktop Intelligence 报表转换为 Web Intelligence 文档。
- [4] 自 XI 3.1 Service Pack 3 起，已引入 Xcelsius 高速缓存和处理服务，以优化 Xcelsius 提出的关系数据源的 Query as a Web Service 请求。4.0 Feature Pack 3 Dashboards 高速缓存服务器和仪表盘处理服务器均提供等效缓存和处理服务。
- [5] 4.0 中的 Dashboard Design 服务器在 4.0 Feature Pack 3 中已重命名为 Dashboards，旨在与 SAP BusinessObjects Dashboards 的产品名称变化保持一致。

3.2.2 服务

添加服务器时，必须包括自适应作业服务器上的某些服务，例如，目标交付计划服务。

注意：

新的服务或服务器类型可添加到未来的维护版本中。

服务	服务类别	服务器类型	服务说明
自适应连接服务	连接服务	自适应处理服务器	为基于 Java 的驱动程序提供连接
身份验证更新计划服务	核心服务	自适应作业服务器	为第三方安全插件提供更新同步
BEx Web 应用程序服务	Analysis 服务	自适应处理服务器	提供 SAP Business Warehouse (BW) Business Explorer (BEx) Web 应用程序与 BI 启动板的集成。
BOE Web 应用程序服务	核心服务	Web 应用程序容器服务器	为 WACS 提供 Web 应用程序：包括中央管理控制台 (CMC)、BI 启动板和 OpenDocument
Business Process BI 服务	核心服务	Web 应用程序容器服务器	为 WACS 提供 Business Process BI Web 服务，允许将 BI 技术融入 Web 应用程序中。不赞成使用 Business Process BI 服务。
中央管理服务	核心服务	中央管理服务器	提供服务器、用户、会话管理和安全（访问权限和身份验证）管理。群集中必须至少有一个中央管理服务可用于群集运行。
客户端审核代理服务	核心服务	自适应处理服务器	收集由客户端发送的审核事件并将其转发至 CMS 服务器

服务	服务类别	服务器类型	服务说明
Crystal Reports 2011 处理服务	Crystal Reports 服务	Crystal Reports 处理服务器	接受和处理 Crystal Reports 2011 报表；可以在报表之间共享数据以减少数据库访问次数
Crystal Reports 2011 计划服务	Crystal Reports 服务	自适应作业服务器	运行计划的旧 Crystal Reports 作业并将结果发布到输出位置
Crystal Reports 2011 查看和修改服务	Crystal Reports 服务	报表应用程序服务器 (RAS)	处理 Crystal Reports 2011 报表的查看和修改请求。
Crystal Reports 高速缓存服务	Crystal Reports 服务	Crystal Reports 高速缓存服务器	通过管理报表高速缓存来限制 Crystal 报表生成的数据库访问次数并加快报表生成速度
Crystal Reports 处理服务	Crystal Reports 服务	Crystal Reports 处理服务器	接受和处理 Crystal 报表；可以在报表之间共享数据以减少数据库访问次数
Crystal Reports 计划服务	Crystal Reports 服务	自适应作业服务器	运行计划的新 Crystal Reports 作业并将结果发布到输出位置
自定义数据访问服务	Web Intelligence 服务	自适应处理服务器	提供与不需要连接服务器的数据源的动态连接。此项服务允许访问和更新使用某些个人数据提供者（如 CSV 文件）创建的报表。有关根据文本文件构建查询或更新文档的更多信息，请参阅《SAP BusinessObjects Web Intelligence 胖客户端用户指南》。

服务	服务类别	服务器类型	服务说明
仪表盘高速缓存服务	Dashboards 服务	Dashboards 高速缓存服务器	通过管理报表高速缓存来限制 Dashboards 报表生成的数据库访问次数并加快报表生成速度
Dashboards 处理服务	Dashboards 服务	Dashboards 处理服务器	接受和处理 Dashboards 报表；可以在报表之间共享数据以减少数据库访问次数
数据联合服务	数据联合服务	自适应处理服务器	查询和处理多源 Universe 的基础数据源
目标传送计划服务	核心服务	自适应作业服务器	<p>运行已计划作业并将结果发布到输出位置，如文件系统、FTP 服务器、电子邮件或用户收件箱</p> <p>注意： 添加服务器时，必须包括某些自适应作业服务器服务，包括这项服务。</p>
文档恢复服务	Web Intelligence 服务	自适应处理服务器	Web Intelligence 文档自动保存和恢复。
DSL 桥服务	Web Intelligence 服务	自适应处理服务器	维语义层（DSL）会话支持
事件服务	核心服务	事件服务器	监控文件资源库服务器（FRS）上的文件事件，并在必要时触发报表运行
Excel 数据访问服务	Web Intelligence 服务	自适应处理服务器	支持将 Excel 文件上载至 BI 平台作为数据源。有关根据 Excel 文件构建查询或更新文档的更多信息，请参阅《SAP BusinessObjects Web Intelligence 胖客户端用户指南》。

服务	服务类别	服务器类型	服务说明
信息引擎服务	Web Intelligence 服务	Web Intelligence 处理服务器	Web Intelligence 文档处理所需的服务
输入文件存储服务	核心服务	输入文件资源库服务器	维护已发布报表和程序对象，这些对象可在收到输入文件时用于生成新报表
Insight to Action 服务	核心服务	自适应处理服务器	启用要调用的操作并提供 RRI 支持
生命周期管理 ClearCase 服务	生命周期管理服务	自适应处理服务器	为 LCM 提供 ClearCase 支持
生命周期管理计划服务	生命周期管理服务	自适应作业服务器	运行计划的生命周期管理作业
生命周期管理服务	生命周期管理服务	自适应处理服务器	生命周期管理核心服务
监控服务	核心服务	自适应处理服务器	提供监控功能
多维分析服务	Analysis 服务	自适应处理服务器	提供对多维联机分析处理（OLAP）数据的访问；将原始数据转换为 XML，可呈现到 Excel、PDF 或 Analysis（原来称为 Voyager）交叉表和统计图中
本机连接服务	连接服务	连接服务器	为 64 位体系结构提供本机连接
本机连接服务（32 位）	连接服务	连接服务器	为 32 位体系结构提供本机连接
输出文件存储服务	核心服务	输出文件资源库服务器	维护已完成文档的集合
平台搜索计划服务	核心服务	自适应作业服务器	运行计划的搜索，以便为中央管理服务器（CMS）资源库中的所有内容建立索引
平台搜索服务	核心服务	自适应处理服务器	为 BI 平台提供搜索功能

服务	服务类别	服务器类型	服务说明
探测器计划服务	核心服务	自适应作业服务器	提供计划的探测器作业并将结果发布到输出位置
程序计划服务	核心服务	自适应作业服务器	运行已计划于指定时间运行的程序
发布计划服务	核心服务	自适应作业服务器	运行计划的发布作业并将结果发布到输出位置
发布后处理服务	核心服务	自适应处理服务器	报表完成后执行操作，如将报表发送至输出位置
发布服务	核心服务	自适应处理服务器	协调发布后处理服务与目标作业服务，以将报表发布到输出位置，如文件系统、FTP 服务器、电子邮件或用户收件箱
Rebean 服务	Web Intelligence 服务	自适应处理服务器	Web Intelligence 和 Explorer 使用的 SDK
复制服务	核心服务	自适应作业服务器	运行计划的联合作业以在联合站点之间复制内容
RESTful Web 服务	核心服务	Web 应用程序容器服务器 (WACS)	为 RESTful Web 服务请求提供会话处理。
安全性查询计划服务	核心服务	自适应作业服务器	运行计划的安全性查询作业
安全标记服务	核心服务	自适应处理服务器	SAP 单一登录支持
翻译服务	核心服务	自适应处理服务器	通过翻译管理器客户端中的输入翻译 InfoObject
视觉差异计划服务	生命周期管理服务	自适应作业服务器	运行计划的视觉差异（生命周期管理）作业并将结果发布到输出位置

服务	服务类别	服务器类型	服务说明
视觉差异服务	生命周期管理服务	自适应处理服务器	确定文档升级与生命周期管理的文档是否视觉一致
可视化服务	Web Intelligence 服务	自适应处理服务器	Web Intelligence 所使用的公共可视化对象模型服务
Web Intelligence 公用服务	Web Intelligence 服务	Web Intelligence 处理服务器	支持 Web Intelligence 文档处理
Web Intelligence 核心服务	Web Intelligence 服务	Web Intelligence 处理服务器	支持 Web Intelligence 文档处理
Web Intelligence 处理服务	Web Intelligence 服务	Web Intelligence 处理服务器	接受和处理 Web Intelligence 文档
Web Intelligence 计划服务	Web Intelligence 服务	自适应作业服务器	允许支持计划的 Web Intelligence 作业
Web 服务 SDK 和 QaaWS	核心服务	Web 应用程序容器服务器	WACS 上的 Web 服务

3.2.3 服务类别

注意：

新的服务或服务器类型可添加到未来的维护版本中。

服务类别	服务	服务器类型
Analysis 服务	BEx Web 应用程序服务	自适应处理服务器
Analysis 服务	多维分析服务	自适应处理服务器
连接服务	自适应连接服务	自适应处理服务器
连接服务	本机连接服务	连接服务器
连接服务	本机连接服务（32 位）	连接服务器

服务类别	服务	服务器类型
核心服务	身份验证更新计划服务	自适应作业服务器
核心服务	中央管理服务	中央管理服务器
核心服务	客户端审核代理服务	自适应处理服务器
核心服务	仪表盘服务	仪表盘服务器
核心服务	目标配置服务	自适应作业服务器
核心服务	目标传送计划服务	自适应作业服务器
核心服务	事件服务	事件服务器
核心服务	Insight to Action 服务	自适应处理服务器
核心服务	输入文件存储服务	输入文件资源库服务器
核心服务	监控服务。	自适应处理服务器
核心服务	输出文件存储服务	输出文件资源库服务器
核心服务	平台搜索计划服务	自适应作业服务器
核心服务	平台搜索服务	自适应处理服务器
核心服务	探测器计划服务	自适应作业服务器
核心服务	程序计划服务	自适应作业服务器
核心服务	发布计划服务	自适应作业服务器
核心服务	发布后处理服务	自适应处理服务器
核心服务	发布服务	自适应处理服务器
核心服务	复制服务	自适应作业服务器
核心服务	RESTful Web 服务	Web 应用程序容器服务器
核心服务	安全性查询计划服务	自适应作业服务器
核心服务	安全标记服务	自适应处理服务器
核心服务	单一登录服务	中央管理服务器、连接服务器、Crystal Reports 处理服务器、RAS、Dashboards 处理服务器和 Web Intelligence 处理服务器
核心服务	跟踪日志服务	任意服务器

服务类别	服务	服务器类型
核心服务	翻译服务	自适应处理服务器
核心服务	用户和组导入计划服务	自适应作业服务器
核心服务	Web 应用程序容器服务	Web 应用程序容器服务器
Crystal Reports 服务	Crystal Reports 2011 处理服务	Crystal Reports 处理服务器
Crystal Reports 服务	Crystal Reports 2011 计划服务	自适应作业服务器
Crystal Reports 服务	Crystal Reports 2011 查看和修改服务	报表应用程序服务器 (RAS)
Crystal Reports 服务	Crystal Reports 高速缓存服务	Crystal Reports 高速缓存服务器
Crystal Reports 服务	Crystal Reports 处理服务	Crystal Reports 处理服务器
Crystal Reports 服务	Crystal Reports 计划服务	自适应作业服务器
Dashboards 服务	仪表盘高速缓存服务	Dashboards 高速缓存服务器
Dashboards 服务	Dashboards 处理服务	Dashboards 处理服务器
数据联合服务	数据联合服务	自适应处理服务器
生命周期管理服务	生命周期管理 ClearCase 服务	自适应处理服务器
生命周期管理服务	生命周期管理计划服务	自适应作业服务器
生命周期管理服务	生命周期管理服务	自适应处理服务器
生命周期管理服务	视觉差异计划服务	自适应作业服务器
生命周期管理服务	视觉差异服务	自适应处理服务器
Web Intelligence 服务	自定义数据访问服务	自适应处理服务器
Web Intelligence 服务	文档恢复服务	自适应处理服务器
Web Intelligence 服务	DSL 桥服务	自适应处理服务器
Web Intelligence 服务	Excel 数据访问服务	自适应处理服务器
Web Intelligence 服务	信息引擎服务	Web Intelligence 处理服务器
Web Intelligence 服务	Rebean 服务	自适应处理服务器

服务类别	服务	服务器类型
Web Intelligence 服务	可视化服务	自适应处理服务器
Web Intelligence 服务	Web Intelligence 公用服务	Web Intelligence 处理服务器
Web Intelligence 服务	Web Intelligence 核心服务	Web Intelligence 处理服务器
Web Intelligence 服务	Web Intelligence 监控服务	自适应处理服务器
Web Intelligence 服务	Web Intelligence 处理服务	Web Intelligence 处理服务器
Web Intelligence 服务	Web Intelligence 计划服务	自适应作业服务器

3.2.4 服务器类型

服务名称旁的星号表示该服务为次级服务。有些次级服务为自动创建，但在选择次级服务所依赖的主服务后，还必须选择包括其他次级服务。

注意：

新的服务或服务器类型可添加到未来的维护版本中。

服务器类型	服务	服务类别
任意服务器	跟踪日志服务	核心服务
自适应作业服务器	身份验证更新计划服务	核心服务
自适应作业服务器	Crystal Reports 2011 计划服务	Crystal Reports 服务
自适应作业服务器	Crystal Reports 计划服务	Crystal Reports 服务
自适应作业服务器	目标配置服务	核心服务
自适应作业服务器	目标传送计划服务	核心服务
自适应作业服务器	生命周期管理计划服务	生命周期管理服务
自适应作业服务器	平台搜索计划服务	核心服务

服务器类型	服务	服务类别
自适应作业服务器	探测器计划服务	核心服务
自适应作业服务器	程序计划服务	核心服务
自适应作业服务器	发布计划服务	核心服务
自适应作业服务器	复制服务	核心服务
自适应作业服务器	安全性查询计划服务	核心服务
自适应作业服务器	用户和组导入计划服务	核心服务
自适应作业服务器	视觉差异计划服务	生命周期管理服务
自适应作业服务器	Web Intelligence 计划服务	Web Intelligence 服务
自适应处理服务器	自适应连接服务	连接服务
自适应处理服务器	BEx Web 应用程序服务	Analysis 服务
自适应处理服务器	客户端审核代理服务	核心服务
自适应处理服务器	自定义数据访问服务	Web Intelligence 服务
自适应处理服务器	数据联合服务	数据联合服务
自适应处理服务器	文档恢复服务	Web Intelligence 服务
自适应处理服务器	DSL 桥服务	Web Intelligence 服务
自适应处理服务器	Excel 数据访问服务	Web Intelligence 服务
自适应处理服务器	Insight to Action 服务	核心服务
自适应处理服务器	生命周期管理 ClearCase 服务	生命周期管理服务
自适应处理服务器	生命周期管理服务	生命周期管理服务
自适应处理服务器	监控服务。	核心服务
自适应处理服务器	多维分析服务	Analysis 服务
自适应处理服务器	平台搜索服务	核心服务
自适应处理服务器	发布后处理服务	核心服务
自适应处理服务器	发布服务	核心服务
自适应处理服务器	Rebean 服务	Web Intelligence 服务
自适应处理服务器	安全标记服务	核心服务

服务器类型	服务	服务类别
自适应处理服务器	翻译服务	核心服务
自适应处理服务器	视觉差异服务	生命周期管理服务
自适应处理服务器	可视化服务	Web Intelligence 服务
自适应处理服务器	Web Intelligence 监控服务	Web Intelligence 服务
中央管理服务器	中央管理服务	核心服务
中央管理服务器	单一登录服务	核心服务
连接服务器	本机连接服务	连接服务
连接服务器	本机连接服务（32 位）	连接服务
连接服务器	单一登录服务	核心服务
Crystal Reports 高速缓存服务器	Crystal Reports 高速缓存服务	Crystal Reports 服务
Crystal Reports 处理服务器	Crystal Reports 2011 处理服务	Crystal Reports 服务
Crystal Reports 处理服务器	Crystal Reports 处理服务	Crystal Reports 服务
Crystal Reports 处理服务器	单一登录服务	核心服务
Dashboards 高速缓存服务器	仪表盘高速缓存服务	Dashboards 服务
Dashboards 处理服务器	Dashboards 处理服务	Dashboards 服务
Dashboards 处理服务器	单一登录服务	核心服务
仪表盘服务器	仪表盘服务	核心服务
事件服务器	事件服务	核心服务
输入文件资源库服务器	输入文件存储服务	核心服务
输出文件资源库服务器	输出文件存储服务	核心服务
报表应用程序服务器（RAS）	Crystal Reports 2011 查看和修改服务	Crystal Reports 服务
RAS	单一登录服务	核心服务
Web 应用程序容器服务器	RESTful Web 服务	核心服务
Web 应用程序容器服务器	Web 应用程序容器服务	核心服务

服务器类型	服务	服务类别
Web Intelligence 处理服务器	信息引擎服务	Web Intelligence 服务
Web Intelligence 处理服务器	单一登录服务	核心服务
Web Intelligence 处理服务器	Web Intelligence 公用服务	Web Intelligence 服务
Web Intelligence 处理服务器	Web Intelligence 核心服务	Web Intelligence 服务
Web Intelligence 处理服务器	Web Intelligence 处理服务	Web Intelligence 服务

服务器类型	服务	服务类别
自适应作业服务器	身份验证更新计划服务	核心服务
自适应作业服务器	Crystal Reports 2011 计划服务	Crystal Reports 服务
自适应作业服务器	Crystal Reports 计划服务	Crystal Reports 服务
自适应作业服务器	目标传送计划服务	核心服务
自适应作业服务器	生命周期管理计划服务	生命周期管理服务
自适应作业服务器	平台搜索计划服务	核心服务
自适应作业服务器	探测器计划服务	核心服务
自适应作业服务器	程序计划服务	核心服务
自适应作业服务器	发布计划服务	核心服务
自适应作业服务器	复制服务	核心服务
自适应作业服务器	安全性查询计划服务	核心服务
自适应作业服务器	视觉差异计划服务	生命周期管理服务
自适应作业服务器	Web Intelligence 计划服务	Web Intelligence 服务
自适应处理服务器	自适应连接服务	连接服务
自适应处理服务器	BEx Web 应用程序服务	Analysis 服务
自适应处理服务器	客户端审核代理服务	核心服务

服务器类型	服务	服务类别
自适应处理服务器	自定义数据访问服务	Web Intelligence 服务
自适应处理服务器	数据联合服务	数据联合服务
自适应处理服务器	文档恢复服务	Web Intelligence 服务
自适应处理服务器	DSL 桥服务	Web Intelligence 服务
自适应处理服务器	Excel 数据访问服务	Web Intelligence 服务
自适应处理服务器	Insight to Action 服务	核心服务
自适应处理服务器	生命周期管理 ClearCase 服务	生命周期管理服务
自适应处理服务器	生命周期管理服务	生命周期管理服务
自适应处理服务器	监控服务。	核心服务
自适应处理服务器	多维分析服务	Analysis 服务
自适应处理服务器	平台搜索服务	核心服务
自适应处理服务器	发布后处理服务	核心服务
自适应处理服务器	发布服务	核心服务
自适应处理服务器	Rebean 服务	Web Intelligence 服务
自适应处理服务器	安全标记服务	核心服务
自适应处理服务器	翻译服务	核心服务
自适应处理服务器	视觉差异服务	生命周期管理服务
自适应处理服务器	可视化服务	Web Intelligence 服务
中央管理服务器	中央管理服务	核心服务
连接服务器	本机连接服务	连接服务
连接服务器	本机连接服务（32 位）	连接服务
Crystal Reports 高速缓存服务器	Crystal Reports 高速缓存服务	Crystal Reports 服务
Crystal Reports 处理服务器	Crystal Reports 2011 处理服务	Crystal Reports 服务
Crystal Reports 处理服务器	Crystal Reports 处理服务	Crystal Reports 服务

服务器类型	服务	服务类别
Dashboards 高速缓存服务器	仪表盘高速缓存服务	Dashboards 服务
Dashboards 处理服务器	Dashboards 处理服务	Dashboards 服务
仪表盘服务器	仪表盘服务	核心服务
事件服务器	事件服务	核心服务
输入文件资源库服务器	输入文件存储服务	核心服务
输出文件资源库服务器	输出文件存储服务	核心服务
报表应用程序服务器 (RAS)	Crystal Reports 2011 查看和修改服务	Crystal Reports 服务
Web 应用程序容器服务器	RESTful Web 服务	核心服务
Web Intelligence 处理服务器	信息引擎服务	Web Intelligence 服务
Web Intelligence 处理服务器	Web Intelligence 公用服务	Web Intelligence 服务
Web Intelligence 处理服务器	Web Intelligence 核心服务	Web Intelligence 服务
Web Intelligence 处理服务器	Web Intelligence 处理服务	Web Intelligence 服务

3.2.5 服务器

这些服务器是在主机的服务器智能代理 (SIA) 下运行的一系列服务。服务器的类型由在其中运行的服务表示。可以在中央管理控制台 (CMC) 中创建服务器。下表列出了可以在 CMC 中创建的各种类型的服务器。

服务器	说明
自适应作业服务器	用于处理计划作业的通用服务器。将作业服务器添加到 BI 平台系统时，可以配置作业服务器，以处理报表、文档、程序或发布，并将结果发送至其他目标。
自适应处理服务器	<p>承载服务的通用服务器，负责处理来自不同来源的请求。</p> <p>安装程序在每个主机系统上安装一台自适应处理服务器（APS）。根据所安装的功能，此 APS 可能会承载多种服务，如监控服务、生命周期管理服务、多维分析服务（MDAS）、发布服务及其他服务。</p> <p>对于生产系统或测试系统，最佳实践旨在创建更多 APS，并对 APS 进行配置以满足用户的业务需求。有关更多信息，请参阅第 81 页上的 “系统配置向导介绍” 和第 366 页上的 “为生产系统配置自适应处理服务器”。</p>
中央管理服务器（CMS）	维护有关 BI 平台系统的信息数据库（CMS 系统数据库）和有关经审核的用户操作的信息数据库（审核数据存储）。所有平台服务都由 CMS 管理。CMS 还控制对存储文档的系统文件以及有关用户、用户组、安全级别（包括身份验证和授权）和内容等信息的访问。
连接服务器	提供对源数据的数据库访问。支持关系数据库以及 OLAP 和其他格式。连接服务器负责处理与不同数据源的连接与交互，并向客户端提供常用的功能集。
Crystal Reports 高速缓存服务器	拦截客户端发往页面服务器的报表请求。如果高速缓存服务器无法通过缓存的报表页满足请求，则会将请求传递到 Crystal Reports 处理服务器，该服务器将运行报表并返回结果。然后，高速缓存服务器将缓存报表页以供日后使用。
Crystal Reports 处理服务器	通过处理报表并生成封装页面格式（EPF）页面来响应页面请求。EPF 的主要好处在于它支持按需页面访问，从而只返回请求的页面，而不是整个报表。这样，可以提升系统性能，并减少大型报表的不必要的网络通信。
Dashboards 高速缓存服务器	拦截客户端发往仪表盘服务器的报表请求。如果高速缓存服务器无法通过缓存的报表页满足请求，则会将请求传递到仪表盘服务器，该服务器将运行报表并返回结果。然后，高速缓存服务器将缓存报表页以供日后使用。
Dashboards 处理服务器	通过处理报表并生成封装页面格式（EPF）页面来响应 Dashboards 请求。EPF 的主要好处在于它支持按需页面访问，从而只返回请求的页面，而不是整个报表。这样，可以提升系统性能，并减少大型报表的不必要的网络通信。
事件服务器	监控系统事件，这些事件可充当运行报表的触发器。设置事件触发器之后，事件服务器将对条件进行监控，并通知 CMS 已发生事件。然后，CMS 可以启动设置为在事件上运行的任何作业。事件服务器管理在存储层发生的基于文件的事件。

服务器	说明
文件资源库服务器	负责创建文件系统对象，例如导出的报表和非原始格式的导入文件。输入 FRS 可以存储已由管理员或最终用户发布到系统的报表和程序对象。输出 FRS 存储由作业服务器生成的所有报表实例。
Web Intelligence 处理服务器	处理 SAP BusinessObjects Web Intelligence 文档。
报表应用程序服务器	提供即席报表生成功能，利用这些功能，用户可以通过 SAP Crystal Reports Server 嵌入版软件开发套件（SDK）创建和修改 Crystal 报表。

3.3 客户端应用程序

可使用两种主要的客户端应用程序与 BI 平台交互：

- 桌面应用程序

这些应用程序必须安装在受支持的 Microsoft Windows 操作系统上，并可本地处理数据和创建报表。

注意：

BI 平台安装程序不再安装桌面应用程序。要在服务器上安装桌面应用程序，请使用单机版 SAP BusinessObjects Business Intelligence 平台客户端工具安装程序。

桌面客户端可用于将一些 BI 报表处理任务卸载到各台客户端计算机上。大多数桌面应用程序通过安装在桌面上的驱动程序直接访问组织的数据，并通过 CORBA 或加密型 CORBA SSL 与 BI 平台部署进行通信。

此类应用程序的示例包括：Crystal Reports 和 Live Office。

注意：

虽然 Live Office 应用程序具有丰富的功能，但它要通过 HTTP 才能与 BI 平台 Web 服务连接。

- Web 应用程序

这些应用程序由 Web 应用程序服务器承载，并可使用 Windows、Macintosh、Unix 和 Linux 操作系统上支持的 Web 浏览器进行访问。

这可用于为大型的用户组提供商务智能（BI）访问权，而不会遇到部署桌面软件产品的挑战。通过使用或不使用 SSL 加密的 HTTP（HTTPS）进行通信。

此类应用程序的示例包括 BI 启动板、SAP BusinessObjects Web Intelligence、中央管理控制台（CMC）和报表查看器。

3.3.1 随 SAP BusinessObjects Business Intelligence 平台客户端工具一起安装

3.3.1.1 Web Intelligence 胖客户端

Web Intelligence 胖客户端是一种供企业用户使用的即席分析和报表创建工具，企业用户不论是否具有 BI 平台的访问权限都能使用此工具。

该工具支持业务用户通过 Universe (.unv 和 .unx)、BEx 查询或其他渠道访问数据，在拖放界面中使用类似的业务术语。工作流可用于分析各种广度与深度的问题，并在分析工作流期间随时提出更多问题。

Web Intelligence 胖客户端用户可继续使用 Web Intelligence 文档文件 (.wid)，即使在无法连接到中央管理服务器 (CMS) 时也能如此。

3.3.1.2 业务视图管理器

业务视图管理器用于构建可简化基础数据库复杂性的语义层对象。

业务视图管理器可创建数据连接、动态数据连接、数据基础、业务元素、业务视图及关系视图。它也允许为报表中的对象设置详细的列和行级安全。

设计人员可以构建与多个数据源的连接，联接表，为字段名称指定别名，创建计算所得字段，然后将此简化结构用作业务视图。然后，报表设计人员和用户可以使用该业务视图作为其报表的基础，而不是直接通过数据构建自己的查询。

3.3.1.3 报表转换工具

报表转换工具将报表转换为 Web Intelligence 格式，并将转换的报表发布到中央管理服务器（CMS）。

可从 CMS 文件夹“公共”、“收藏夹”或“收件箱”中获取报表。转换后，可将报表发布到原始 Web Intelligence 报表所在的文件夹或其他文件夹。该工具并不会转换所有的 Web Intelligence 功能和报表。转换程度取决于原始报表中的功能。某些功能会使得报表无法被转换。其他功能会在转换过程中被该工具修改、重新实现或删除。

通过报表转换工具还可以审核转换的报表。这有助于确定报表转换工具无法完全转换的报表以及出现这种情况的原因。

3.3.1.4 Universe 设计工具

Universe 设计工具（原来称为 Universe Designer）可供数据设计人员合并源自语义层中多个源的数据，该语义层旨在让最终用户避免数据库的复杂性。它通过使用业务语言（而非技术语言）访问、操作和组织数据，将数据的复杂性抽象化。

Universe 设计工具提供了用于选择和查看数据库表的图形界面。在模式图中，以表符号来表示数据库表。设计人员可以使用此界面操作表、创建表之间的联接、创建别名表、创建上下文和解决模式中的循环。

也可以从元数据源创建 Universe。Universe 设计工具用于在创建流程结束时生成 Universe。

3.3.1.5 作为 Web 服务的查询

Query as a Web Service 是一个基于向导的应用程序，用于将查询转化为 Web 服务并与 Web 就绪的应用程序集成在一起。可以保存查询以创建标准查询的目录，而应用程序生成器可以根据需要选择这些查询。

商务智能（BI）内容通常与 BI 工具的特定用户界面绑定。通过允许将 BI 内容传送给可处理 Web 服务的任意用户接口，Query as a Web Service 改变了这一情况。

Query as a Web Service 旨在像其他 Web 服务一样在任何 Microsoft Windows 应用程序之上运行。Query as a Web Service 以 W3C Web 服务规范 SOAP、SDL 和 XML 为基础。它有两个主要组件：

- 服务器组件

服务器组件（包括在 BI 平台中）存储 Query as a Web Service 目录，并承载已发布的 Web 服务。

- 客户端工具

业务用户利用此工具可以在服务器上创建其查询并将查询作为 Web 服务发布。可以在数台计算机上安装客户端工具，这些计算机可以访问和共享服务器上存储的同一个目录。客户端工具通过 Web 服务与服务器组件通信。

Query as a Web Service 允许将 Web 查询用作一系列客户端解决方案中的一部分，包括：

- Microsoft Office、Excel 和 InfoPath
- SAP NetWeaver
- OpenOffice
- 业务规则和流程管理应用程序
- 企业服务总线平台

3.3.1.6 信息设计工具

信息设计工具（原来称为“信息设计器”）是一种元数据设计环境，用于供设计员提取、定义以及处理关系源和 OLAP 源中的元数据，以创建和部署 SAP BusinessObjects Universe。

3.3.1.7 翻译管理工具

BI 平台提供对多语言文档和 Universe 的支持。多语言文档包含 Universe 元数据和文档提示的本地化版本。例如，用户可以使用所选的语言，依据同一个 Universe 创建报表。

翻译管理工具（原来称为翻译管理器）用于定义多语言 Universe 并管理 Universe 以及 CMS 资源库中其他报表和分析资源的译文。

翻译管理工具：

- 将 Universe 或文档译成多种语言版本，供多语言读者使用。
- 定义文档的元数据语言部分及相应的译文。它可生成外部 XLIFF 格式，并导入 XLIFF 文件以获取译文信息。
- 列出要翻译的 Universe 或文档结构。

- 支持用户通过用户界面翻译元数据，或者通过导出和导入 XLIFF 文件的方式，使用外部翻译工具来翻译元数据。
- 创建多语言文档。

3.3.1.8 数据联合管理工具

数据联合管理工具（原来称为 Data Federator）是一个胖客户端应用程序，其易于使用的功能可用于管理数据联合服务。

数据联合服务与 BI 平台紧密集成，通过跨不同数据源分发查询实现多源 Universe，并允许通过单个数据基础联合数据。

此数据联合管理工具可用于优化数据联合查询和微调数据联合查询引擎，以实现最佳性能。

数据联合管理工具可用于执行以下任务：

测试 SQL 查询。

对详细说明如何将联合的查询分发到各源的优化计划进行可视化。

计算统计信息并设置系统参数，以微调数据联合服务并获取可实现的最佳性能。

管理属性以控制查询在连接器级别的各数据源中的执行方式。

监控正在运行的 SQL 查询。

浏览已执行查询的历史记录。

3.3.1.9 BI 平台微件

微件属于小型应用程序，用于轻松快速地访问各种常用功能，并可在桌面提供可视信息。通过 BI 平台微件（原来称为“BI 微件”），公司可提供对 BI 平台上的现有商务智能（BI）内容的访问；或者，您也可以将注册为 SAP NetWeaver Application Server 上的 XBCML（可扩展商务客户端标记语言）微件的 Web Dynpro 应用程序添加为桌面微件。

要在用户桌面上呈现 XBCML 微件，可使用 SAP Web Dynpro Flex 客户端。SAP Web Dynpro Flex 客户端是基于 Adobe Flex 的渲染引擎，用于渲染微件。有关如何配置 Web Dynpro 应用程序的详细信息，请参见《SAP BusinessObjects 微件用户指南》中的“在 SAP NetWeaver Application Server 上启用微件”主题。

注意：

XBCML 微件的 SAP Web Dynpro Flex 客户端支持始于版本 7.0 EhP2 SP3。Flex 客户端排队支持仅限于在这些指定版本中发现的 Flex 客户端问题。

使用微件，可以搜索或浏览现有内容（如 Web Intelligence 文档、Dashboards 模型和 Web Dynpro 应用程序），然后将信息粘贴到桌面，以便需要时可轻松获取。

作为微件，内容从微件框架获取以下功能：

- 由用户控制的大小和定位
- 自动刷新
- 作为顶部应用程序窗口的可选设置
- 完整的 BI 平台安全性（仅限 Web Intelligence 报表部件和 Dashboards 模型）
- 保存的显示
- 保存的数据上下文状态（仅 Web Intelligence 报表部件）
- 指向详细报表的 Web Intelligence OpenDocument 链接（仅限 Web Intelligence 文档）
- 选项卡式视图（仅限 Dashboards 模型）

3.3.2 随 SAP BusinessObjects Business Intelligence 平台一起安装

3.3.2.1 中央配置管理器（CCM）

中央配置管理器（CCM）是一个以两种形式提供的服务器故障排除和节点管理工具。在 Microsoft Windows 环境中，CCM 可用于通过其图形用户界面（GUI）或命令行管理本地和远程服务器。在 Unix 环境中，CCM 外壳脚本（ccm.sh）用于通过命令行管理服务器。

如果使用默认的捆绑式 Tomcat Web 应用程序服务器，请使用 CCM 创建并配置节点以启动或停止 Web 应用程序服务器。在 Windows 上，它还允许配置网络参数，比如安全套接字层（SSL）加密。这些参数应用于节点内的所有服务器。

注意：

大多数服务器管理任务现在是通过 CMC（而不是 CCM）处理的。CCM 现在仅用于故障排除和节点配置。

3.3.2.2 升级管理工具

升级管理工具（原来称为“导入向导”）是作为 BI 平台的一部分安装的，用于引导管理员从 BI 平台的早期版本中导入用户、组和文件夹。此外，还可用于导入和升级事件、服务器组、资源库对象和日历。

有关早期版本的 BI 平台升级的相关信息，请参阅《SAP BusinessObjects Business Intelligence 平台升级指南》。

3.3.2.3 资源库诊断工具

资源库诊断工具（RDT）可以扫描、诊断和修复中央管理服务器（CMS）系统数据库与文件资源库服务器（FRS）文件存储之间可能存在的不一致之处。

它还可以报告修复状态和已完成的操作。要确定文件系统与数据库之间是否同步，应在用户首次完成热备份后使用 RDT。在还原之后和启动 BI 平台服务之前，也可使用此 RDT。用户可以设置 RDT 在停止前将找到和修复的错误数限制。

3.3.3 单独提供

3.3.3.1 SAP BusinessObjects Analysis (Microsoft Office 版)

SAP BusinessObjects Analysis (Microsoft Office 版) 是 Business Explorer (BEx) 的绝佳替代之选, 允许业务分析员发掘多维联机分析处理 (OLAP) 数据。

分析员可快速解答各种业务问题, 随后将分析结果和工作区作为分析报告与他人共享。

SAP BusinessObjects Analysis (Microsoft Office 版) 可使分析员完成下列任务:

- 无需数据库管理员协助, 即可根据财务系统中存储的详细信息发现趋势和异常值。
- 可在查看多维数据集 (无论数据集大小) 的同时, 高效地解决业务问题。
- 利用一个简洁、直观的界面, 访问组织中的各种 OLAP 数据源并共享结果。
- 在同一分析中访问多个不同的 OLAP 源, 以全面了解企业的动态以及各个趋势之间的相互影响。
- 探询、分析、比较和预测业务驱动因素。
- 使用全面的业务和时间计算。

3.3.3.2 SAP Crystal Reports

SAP Crystal Reports 软件允许用户通过某个数据源设计交互式报表。

3.3.3.3 SAP BusinessObjects Dashboards

SAP BusinessObjects Dashboards (原来称为 Xcelsius) 是一种用于数据可视化和创建动态交互式仪表盘的工具体。数据和公式可导入到或直接输入到嵌入式 Excel 电子表格。Flash 界面提供可显示各种分析和仪表盘的画布。

数据可从 BI 平台动态更新, 并导出为数据使用者可采用标准格式查看的各种不同格式, 如 PowerPoint、PDF 或 Flash。

3.3.3.4 SAP BusinessObjects Explorer

SAP BusinessObjects Explorer 是一个数据发现应用程序, 该应用程序使用强大的搜索功能, 可以快速直接从公司数据中检索到业务问题的答案。

安装 SAP BusinessObjects Explorer 时，会将以下服务器添加到 BI 平台中央配置管理器（CCM）和中央管理控制台（CMC）中：

- Explorer 主服务器：管理所有 Explorer 服务器。
- Explorer 索引服务器：提供和管理信息空间数据和元数据的索引建立工作。
- Explorer 搜索服务器：处理搜索查询并返回结果。
- Explorer 发掘服务器：提供和管理信息空间发掘和分析功能，包括搜索数据、过滤和聚合。

3.3.4 Web 应用程序客户端

Web 应用程序客户端位于 Web 应用程序服务器上，可通过客户端 Web 浏览器进行访问。安装 BI 平台时会自动部署 Web 应用程序。

用户可从 Web 浏览器中轻松访问 Web 应用程序，如果希望允许用户从组织网络外进行访问，则可使用 SSL 加密来确保通信安全。

在初始安装之后，还可通过使用捆绑的 WDeploy 命令行工具来重新配置或部署 Java Web 应用程序，此工具可用于按如下两种方式向 Web 应用程序服务器部署 Web 应用程序：

。 1 独立模式

将所有 Web 应用程序资源部署到可为动态和静态内容提供服务的 Web 应用程序服务器。这种安排适合小型安装。

。 2 分离模式

Web 应用程序的静态内容（HTML、图像、CSS）部署到专用的 Web 服务器，而动态内容（JSP）则部署到 Web 应用程序服务器。这种安排适合较大的安装，好处在于使 Web 应用程序服务器不再服务于静态 Web 内容。

有关 WDeploy 的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

3.3.4.1 中央管理控制台（CMC）

中央管理控制台（CMC）是一款基于 Web 的工具，您可用来执行管理任务（其中包括用户、内容和服务器管理）和配置安全设置。由于 CMC 是基于 Web 的应用程序，因此可以在可连接到 Web 应用程序服务器的任何计算机上的 Web 浏览器中执行所有这些管理任务。

所有用户都可以登录到 CMC 以更改其自身的首选项设置。除非明确授予用户更改管理设置的权限，否则只有 Administrators 组的成员能够更改管理设置。您可在 CMC 中分配角色，授予用户执行次要管理任务的权限，例如：管理组中的用户以及管理属于您团队的文件夹中的报告。

3.3.4.2 BI 启动板

BI 启动板（原来称为 InfoView）是一个基于 Web 的界面，最终用户可以访问该界面以查看、计划和跟踪发布的商务智能（BI）报表。BI 启动板可以访问和导出任何类型的商务智能内容（包括报表、分析和仪表盘）以及与这些内容交互。

BI 启动板可用于管理以下内容：

- 浏览和搜索 BI 内容
- BI 内容访问（创建、编辑和查看）。
- 对 BI 内容的计划和发布。

3.3.4.3 BI 工作区

BI 工作区（原来称为 Dashboard Builder）使用户可通过模块（数据模板）和商务智能（BI）工作区（查看一个或多个模块中的数据）跟踪业务活动和绩效。模块和 BI 工作区提供在情况发生变化时调整业务规则所需的信息。通过管理 BI 工作区和模块，用户可以跟踪和分析关键业务数据。此外，它还可以通过集成的协作和工作流功能支持群体决策和分析。BI 工作区具备以下功能：

- 基于选项卡进行浏览
- 页面创建：管理 BI 工作区和模块
- 点击式应用程序生成器
- 用于深入数据分析的模块间的内容链接

注意：

BI 工作区是 BI 启动板应用程序的一个组成部分。因此，要使用 BI 工作区的功能，必须购买 SAP BusinessObjects Business Intelligence 平台许可，其协议中包括 BI 工作区。

3.3.4.4 报表查看器

每个报表查看器支持不同的平台和浏览器。可在 BI 启动板和中央管理控制台（CMC）中设置首选项。查看器分为两种：

- 客户端报表查看器（Active X 查看器、Java 查看器）

客户端报表查看器是在用户的浏览器中下载和安装的。当用户请求报表时，应用程序服务器将处理请求，并从 BI 平台中检索报表页。然后，Web 应用程序服务器会将报表页传递给客户端查看器，后者将处理报表页并将它们显示在 Web 浏览器中。要选择客户端报表查看器，请选择“首选项” > “Crystal Reports” > “Web ActiveX（需要 ActiveX）”或“Web Java（需要 Java）”。

- 零客户端报表查看器（DHTML 查看器）

零客户端报表查看器位于 Web 应用程序服务器上。用户请求报表时，Web 应用程序服务器将从 BI 平台中检索报表页，并创建要在 Web 浏览器中显示的 DHTML 页。要选择零客户端报表（DHTML）查看器，请选择“首选项” > “Crystal Reports” > “Web（不需要下载）”

所有报表查看器都可处理报表请求，并呈现要在浏览器中显示的报表页。

有关每个报表查看器提供的功能或平台支持的更多信息，请参阅《BI 启动板用户指南》、《Report Application Server .NET SDK Developer Guide》（报表应用程序服务器 .NET SDK 开发人员指南）或《查看器 Java SDK 开发人员指南》。

3.3.4.5 SAP BusinessObjects Web Intelligence

SAP BusinessObjects Web Intelligence 是一种基于 Web 的工具，它可为基于 Web 的单一产品中的关系数据源提供查询、报表创建和分析功能。

它用于在一个拖放式界面中创建报表、执行即席查询、分析数据和设置报表的格式。Web Intelligence 隐藏了基础数据源的复杂性。

可以将报表发布到支持的 Web 门户，或者使用 SAP BusinessObjects Live Office 发布到 Microsoft Office 应用程序。

3.3.4.6 SAP BusinessObjects Analysis（OLAP 版）

SAP BusinessObjects Analysis (OLAP 版)，原来称为 Voyager，是 BI 启动板门户中一个用于处理多维数据的联机分析处理 (OLAP) 工具。它还可合并源自单个工作区内不同 OLAP 数据源的信息。所支持的 OLAP 提供者包括 SAP BW 和 Microsoft Analysis Services。

Analysis OLAP 功能集综合了 SAP Crystal Reports 和 SAP BusinessObjects Web Intelligence 的元素，即在前者中对 OLAP 多维数据集进行直接数据访问以创建生产用报表，在后者中利用建立在 OLAP 数据源基础上的 Universe 进行即席分析报表创建。它提供一系列业务计算和时间计算，并包含诸如时间滑块等功能，以尽可能简化对 OLAP 数据的分析。

注意：

Analysis (OLAP 版) Web 应用程序只能用作 Java Web 应用程序。没有适合 .NET 的相应应用程序。

3.3.4.7 SAP BusinessObjects Mobile

SAP BusinessObjects Mobile 可用于通过无线设备远程访问桌面客户端上的可用相同商务智能 (BI) 报表、量度和实时数据。为移动设备优化内容，以使用户即使在未接受更多培训的情况下也能轻松访问、导航和分析常见报表。

借助 SAP BusinessObjects Mobile，管理人员和信息工作者可及时了解最新信息，并据此作出明智的决策。销售人员和现场服务人员可以根据需要随时随地提供正确的客户、产品和工单信息。

SAP BusinessObjects Mobile 支持各种移动设备，包括 BlackBerry、Windows Mobile 和 Symbian 等。

有关 Mobile 安装、配置和部署的信息，请参阅《SAP BusinessObjects Mobile 安装和部署指南》。有关 SAP BusinessObjects Mobile 使用的信息，请参阅《使用 SAP BusinessObjects Mobile》指南。

3.4 流程 workflow

执行任务（比如登录、计划报表或查看报表）时，信息将在系统中流动，并且服务器将相互通信。下一节按某些过程流在 BI 平台中的出现方式描述了这些过程流。

要使用视觉辅助工具查看其他流程工作流，请参阅 SAP BusinessObjects Business Intelligence 4.x 平台官方产品教程，其网址为：<http://scn.sap.com/docs/DOC-8292>

3.4.1 启动和身份验证

3.4.1.1 登录到 BI 平台

本工作流介绍用户从 Web 浏览器登录到 BI 平台 Web 应用程序的过程。本工作流适用于 BI 启动板和中央管理控制台（CMC）等 Web 应用程序。

- 1 浏览器（Web 客户端）通过 Web 服务器将登录请求发送到 Web 应用程序运行所在的 Web 应用程序服务器。
- 2 Web 应用程序服务器确定该请求是登录请求。Web 应用程序服务器将用户名、密码和身份验证类型发送到 CMS 进行身份验证。
- 3 CMS 依据相应的数据库验证用户名和密码（在这里，采用 Enterprise 身份验证，并依据 CMS 系统数据库对用户凭据进行身份验证）。
- 4 成功验证后，CMS 将在内存中为用户创建一个会话。
- 5 CMS 将响应发送到 Web 应用程序服务器，告知其验证已成功。
- 6 Web 应用程序服务器在内存中为用户会话生成一个登录标记。对于此会话的其余部分，Web 应用程序服务器使用登录标记依据 CMS 来验证用户。Web 应用程序服务器将生成下一个 Web 页，以发送到 Web 客户端。
- 7 Web 应用程序服务器将下一个 Web 页发送到 Web 服务器。
- 8 Web 服务器将 Web 页发送到 Web 客户端，并在其中的用户浏览器中呈现该页面。

3.4.1.2 SIA 启动

服务器智能代理（SIA）可配置为自动随主机操作系统一起启动，也可以通过中央配置管理器（CCM）手动启动。

SIA 从中央管理服务器 (CMS) 中检索有关所管理服务器的信息。如果 SIA 使用本地 CMS，并且该 CMS 尚未运行，则 SIA 将启动该 CMS。如果 SIA 使用远程 CMS，它会尝试连接到该 CMS。

启动 SIA 后，会立即执行以下一系列事件。

- 1 SIA 将搜索其高速缓存以找到 CMS。
 - a 如果 SIA 配置为启动本地 CMS，而 CMS 尚未运行，SIA 将启动 CMS 并进行连接。
 - b 如果 SIA 配置为使用正在运行的 CMS（本地或远程），它将尝试连接到其高速缓存中的第一个 CMS。如果该 CMS 当前不可用，它将尝试连接到高速缓存中的下一个 CMS。如果在高速缓存中没有可用的 CMS，SIA 将等到有一个变为可用。
- 2 CMS 将确认 SIA 身份以确保它有效。
- 3 一旦 SIA 成功连接到 CMS，它将请求要托管的服务器的列表。

注意：

SIA 不存储有关所管理服务器的信息。有关 SIA 管理哪个服务器的配置信息将存储在 CMS 系统数据库中，当 SIA 启动时将通过 CMS 检索这些信息。

- 4 CMS 将查询 CMS 系统数据库以获取 SIA 托管的服务器的列表。也会获取每个服务器的配置。
- 5 CMS 会将服务器列表及其配置返回给 SIA。
- 6 对于配置为自动启动的每个服务器，SIA 将使用相应的配置启动它并监控其状态。SIA 启动的每个服务器将配置为与 SIA 使用同一个 CMS。

所有未配置为随 SIA 自动启动的服务器将不会启动。

3.4.1.3 SIA 关闭

服务器智能代理 (SIA) 在关闭主机操作系统时可自动停止，用户也可在中央配置管理器 (CCM) 中手动停止 SIA。

在关闭 SIA 时，将执行以下步骤。

- SIA 通知 CMS 它正在关闭。
 - a 如果 SIA 因主机操作系统关机而停止，则 SIA 将请求停止其服务器。在 25 秒内未停止的服务器将强制终止。
 - b 如果正在手动停止 SIA，它将等到托管服务器完成处理现有作业。托管服务器不接受任何新作业。一旦完成所有作业，服务器将停止。在所有服务器停止后，SIA 也随即停止。

注意：

在强制关闭期间，SIA 将通知所有托管服务器立即停止。

3.4.2 程序对象

3.4.2.1 设置程序对象的计划

本工作流程介绍用户如何通过中央管理控制台（CMC）或 BI 启动板等 Web 应用程序计划在未来时间运行程序对象。

- 1 用户通过 Web 服务器将计划请求从 Web 客户端发送到 Web 应用程序服务器。
- 2 Web 应用程序服务器解释请求，并确定该请求是计划请求。Web 应用程序服务器将计划时间、数据库登录值、参数值、目标和格式发送到指定的中央管理服务器（CMS）。
- 3 CMS 确保用户具有权限来计划对象。如果用户拥有足够权限，CMS 将向 CMS 系统数据库添加新的记录，并将实例添加到其待计划列表中。
- 4 CMS 向 Web 应用程序服务器发送已成功执行计划操作的响应。
- 5 Web 应用程序服务器生成下一个 HTML 页面，并通过 Web 服务器将其发送到 Web 客户端。

3.4.2.2 运行已计划的程序对象

本工作流程介绍计划程序对象在计划时间的运行过程。此外，还必须同时运行自适应作业服务器和输入文件资源库服务器。

注意：

此工作流程需要运行 CMS、自适应作业服务器和输入文件资源库服务器。

- 1 中央管理服务器（CMS）检查 CMS 系统数据库，以确定该时间是否存在要运行的计划 SAP Crystal 报表。
- 2 到达计划的作业时间时，CMS 将查找自适应作业服务器上运行的可用程序计划服务。CMS 将作业信息发送到程序计划服务。
- 3 程序计划服务将与输入文件资源库服务器（FRS）通信，以获得程序对象。

注意：

此步骤也需要与 CMS 通信，以查找所需的服务器和对象。

- 4 程序计划服务将启动该程序。
- 5 程序计划服务用作业状态定期更新 CMS。当前状态为“正在处理”。
- 6 程序计划服务将日志文件发送到输出 FRS。输出文件 FRS 通过发送对象日志文件，通知程序计划服务对象已成功计划。

注意：

此步骤也需要与 CMS 通信，以查找所需的服务器和对象。

- 7 程序计划服务用作业状态更新 CMS。当前状态为“成功”。
- 8 CMS 在其内存中更新作业状态，然后将实例信息写入 CMS 系统数据库。

3.4.3 Crystal Reports

3.4.3.1 查看缓存的 SAP Crystal 报表页面

本工作流程介绍高速缓存服务器中已存在报表页面时、用户在 SAP Crystal 报表（如通过 BI 启动板中的报表查看器）中请求页面的过程。本工作流程适用于 SAP Crystal Reports 2011 和 SAP Crystal Reports for Enterprise。

注意：

此工作流程需要运行 CMS 和 Crystal Reports 高速缓存服务器。

- 1 Web 客户端在 URL 中提交视图报表，通常通过 Web 服务器提交到 Web 应用程序服务器。
- 2 Web 应用程序服务器解释请求，并确定该请求是查看选定报表页面的请求。Web 应用程序服务器向中央管理服务器（CMS）发送请求，以确保用户具有足够的权限来查看报表。
- 3 CMS 将检查 CMS 系统数据库，验证用户是否具有足够的权限查看报表。
- 4 CMS 将响应发送到 Web 应用程序服务器，以确认用户具有足够的权限来查看报表。
- 5 Web 应用程序服务器向 Crystal Reports 高速缓存服务器发送请求，请求报表页面（.epf 文件）。
- 6 Crystal Reports 高速缓存服务器检查以查看请求的 .epf 文件是否存在于高速缓存目录中。在此示例中，已找到 .epf 文件。
- 7 Crystal Reports 高速缓存服务器将请求的页面返回到 Web 应用程序服务器。
- 8 Web 应用程序服务器通过 Web 服务器将该页面发送至 Web 客户端，之后即可在此客户端上显示该页面。

3.4.3.2 查看非缓存的 SAP Crystal Reports 2011 页面

本工作流程介绍高速缓存服务器中不存在页面时、用户在 SAP Crystal Reports 2011 报表（如通过 BI 启动板中的报表查看器）中请求页面的过程。

注意：

此工作流程需要运行 CMS、Crystal Reports 高速缓存服务器、Crystal Reports 2011 处理服务器和输出文件资源库服务器。

- 1 用户通过 Web 服务器将查看请求发送到 Web 应用程序服务器。
- 2 Web 应用程序服务器解释请求，确定该请求是查看选中报表页面的请求，并向中央管理服务器（CMS）发送请求，以确保用户拥有查看报表的足够权限。
- 3 CMS 将检查 CMS 系统数据库，验证用户是否具有足够的权限查看报表。
- 4 CMS 将响应发送到 Web 应用程序服务器，以确认用户具有足够的权限来查看报表。
- 5 Web 应用程序服务器向 Crystal Reports 高速缓存服务器发送请求，请求报表页面（.epf 文件）。
- 6 Crystal Reports 高速缓存服务器确定请求的文件是否存在于高速缓存目录中。
在此示例中，系统没有在高速缓存目录中找到请求的 .epf 文件。
- 7 Crystal Reports 高速缓存服务器将请求发送到 Crystal Reports 2011 处理服务器。
- 8 Crystal Reports 2011 处理服务器针对请求报表实例查询输出文件资源库服务器（FRS），然后输出 FRS 将请求报表实例发送到 Crystal Reports 2011 处理服务器。

注意：

此步骤也需要与 CMS 通信，以查找所需的服务器和对象。

- 9 Crystal Reports 2011 处理服务器打开报表实例，并检查报表以确定其是否包含数据。
Crystal Reports 2011 处理服务器确定报表包含数据，并为请求的报表页面创建 .epf 文件，而不必连接到生产数据库。
- 10 Crystal Reports 2011 处理服务器将 .epf 文件发送到 Crystal Reports 高速缓存服务器。
- 11 Crystal Reports 高速缓存服务器将 .epf 文件写入高速缓存目录。
- 12 Crystal Reports 高速缓存服务器将请求的页面发送到 Web 应用程序服务器。
- 13 Web 应用程序服务器通过 Web 服务器将该页面发送至 Web 客户端，之后即可在此客户端上显示该页面。

3.4.3.3 按需查看 SAP Crystal Reports 2011 报表

此工作流程介绍用户按需请求 SAP Crystal Reports 2011 报表页面以查看最新数据的过程；例如，通过 BI 启动板的报表查看器。

注意：

此工作流程需要运行 CMS、Crystal Reports 高速缓存服务器、Crystal Reports 2011 处理服务器和输入文件资源库服务器。

- 1 用户通过 Web 服务器将查看请求发送到 Web 应用程序服务器。

- 2 Web 应用程序服务器解释请求，并确定该请求是查看选定报表页面的请求。Web 应用程序服务器向中央管理服务器（CMS）发送请求，以确保用户具有足够的权限来查看报表。
- 3 CMS 将检查 CMS 系统数据库，验证用户是否具有足够的权限查看报表。
- 4 CMS 将响应发送到 Web 应用程序服务器，以确认用户具有足够的权限来查看报表。
- 5 Web 应用程序服务器向 Crystal Reports 高速缓存服务器发送请求，请求报表页面（.epf 文件）。
- 6 Crystal Reports 高速缓存服务器检查以确定该页面是否已存在。除非报表满足按需报表共享（在另一个按需请求、数据库登录、参数的规定时间内）的要求，否则 Crystal Reports 高速缓存服务器会针对 Crystal Reports 2011 处理服务器发送请求以生成页面。
- 7 Crystal Reports 2011 处理服务器从输入文件资源库服务器（FRS）中请求报表对象。输入 FRS 将对象的副本发送到 Crystal Reports 2011 处理服务器。

注意：

此步骤也需要与 CMS 通信，以查找所需的服务器和对象。

- 8 Crystal Reports 2011 处理服务器在其内存中打开报表，并检查以确定报表是否包含数据。在此示例中，由于报表对象中不存在任何数据，因此 Crystal Reports 2011 处理服务器将连接到数据源，以检索数据并生成报表。
- 9 Crystal Reports 2011 处理服务器将页面（.epf 文件）发送到 Crystal Reports 高速缓存服务器。Crystal Reports 高速缓存服务器将 .epf 文件的副本存储在其高速缓存目录中，以供新查看请求使用。
10. Crystal Reports 高速缓存服务器将页面发送到 Web 应用程序服务器。
11. Web 应用程序服务器通过 Web 服务器将该页面发送至 Web 客户端，之后即可在此客户端上显示该页面。

3.4.3.4 设置 SAP Crystal 报表计划

本工作流程介绍用户通过中央管理控制台（CMC）或 BI 启动板等 Web 应用程序计划在未来时间运行的 SAP Crystal 报表的过程。本工作流程适用于 SAP Crystal Reports 2011 和 SAP Crystal Reports for Enterprise。

- 1 Web 客户端在 URL 中提交计划请求，通常通过 Web 服务器提交到 Web 应用程序服务器。
- 2 Web 应用程序服务器解释 URL 请求，并确定该请求是计划请求。Web 应用程序服务器将计划时间、数据库登录值、参数值、目标和格式发送到指定的中央管理服务器（CMS）。
- 3 CMS 确保用户具有权限来计划对象。如果用户有足够的权限，CMS 会向 CMS 系统数据库中添加一条新记录。CMS 还会将实例添加到其待定计划列表。
- 4 CMS 将响应发送到 Web 应用程序服务器，告知其计划操作已成功。
- 5 Web 应用程序服务器生成下一个 HTML 页面，并通过 Web 服务器将其发送到 Web 客户端。

3.4.3.5 运行已计划 SAP Crystal Reports 2011 报表

本工作流程介绍计划的 SAP Crystal Reports 2011 报表在计划时间的运行过程。

1. 中央管理服务器 (CMS) 检查 CMS 系统数据库, 以确定该时间是否存在要运行的计划 SAP Crystal 报表。
2. 到达计划的作业时间时, CMS 查找在自适应作业服务器上运行的可用的 Crystal Reports 2011 计划服务 (基于为每个自适应作业服务器配置的“允许的最大作业数”值。CMS 将作业信息 (报表 ID、格式、目标、登录信息、参数和选择公式) 发送到 Crystal Reports 2011 计划服务。
3. Crystal Reports 2011 计划服务与输入文件资源库服务器 (FRS) 的通信, 以按照请求的报表 ID 获取报表模板。

注意:

此步骤也需要与 CMS 通信, 以查找所需的服务器和对象。

4. Crystal Reports 2011 计划服务启动 JobChildserver 进程。
5. 子进程 (JobChildserver) 从输入文件资源库服务器中收到模板时启动 ProcReport.dll。ProcReport.dll 包含从 CMS 传递到 Crystal Reports 2011 计划服务的所有参数。
6. ProcReport.dll 将启动 crpe32.dll, 并根据已传递的参数处理报表。
7. 当 crpe32.dll 仍在处理报表时, 系统将从报表中定义的数据源中提取记录。
8. Crystal Reports 2011 计划服务使用作业状态来更新 CMS。当前状态为“正在处理”。
9. 将报表编译到 Crystal Reports 2011 计划服务的内存中之后, 就需要将该报表导出为另一种格式, 例如可移植文档格式 (PDF)。导出为 PDF 后, 使用 crxfpdf.dll。
10. 含有保存数据的报表将提交到计划的位置 (如电子邮件), 然后发送到输出 FRS。

注意:

此步骤也需要与 CMS 通信, 以查找所需的服务器和对象。

11. Crystal Reports 2011 计划服务使用作业状态来更新 CMS。当前状态为“成功”。
12. CMS 在其内存中更新作业状态, 然后将实例信息写入 CMS 系统数据库。

3.4.4 Web Intelligence

3.4.4.1 按需查看 SAP BusinessObjects Web Intelligence 文档

此工作流程介绍用户按需查看 SAP BusinessObjects Web Intelligence 文档以查看最新数据的过程：例如，通过 BI 启动板中的 Web Intelligence 查看器。

- 1 Web 浏览器通过 Web 服务器将查看请求发送到 Web 应用程序服务器。
- 2 Web 应用程序服务器将解释请求，并确定该请求是否是查看 Web Intelligence 文档的请求。Web 应用程序服务器向中央管理服务器（CMS）发送请求，以确保用户有足够的权限来查看文档。
- 3 CMS 将检查 CMS 系统数据库，验证用户是否具有足够的权限查看文档。
- 4 CMS 将响应发送到 Web 应用程序服务器，以确认用户具有足够的权限来查看文档。
- 5 Web 应用程序服务器向 Web Intelligence 处理服务器发送请求，同时请求文档。
- 6 Web Intelligence 处理服务器从输入文件资源库服务器（FRS）中请求文档，以及构建请求的文档所依据的 Universe 文件。该 Universe 文件包含元层信息，其中包括行级别和列级别安全性。
- 7 输入 FRS 将文档的副本以及构建请求的文档所依据的 Universe 文件发送到 Web Intelligence 处理服务器。

注意：

此步骤也需要与 CMS 通信，以查找所需的服务器和对象。

- 8 Web Intelligence 报表引擎（在 Web Intelligence 处理服务器上）打开内存中的文档并在进程中启动 QT.dll 和连接服务器。
- 9 QT.dll 将生成、验证和重新生成 SQL，并连接到数据库以运行查询。连接服务器使用 SQL 从数据库中获取数据并发送到在其中处理文档的报表引擎。
- 10 Web Intelligence 处理服务器将请求的可查看文档页面发送到 Web 应用程序服务器。
- 11 Web 应用程序服务器通过 Web 服务器将文档页面发送到 Web 客户端，之后即可在此客户端上显示该页面

3.4.4.2 设置 SAP BusinessObjects Web Intelligence 文档计划

本工作流程介绍用户通过中央管理控制台（CMC）或 BI 启动板等 Web 应用程序计划在未来时间运行的 SAP BusinessObjects Web Intelligence 文档的过程。

- 1 Web 客户端在 URL 中提交计划请求，通常通过 Web 服务器提交到 Web 应用程序服务器。
- 2 Web 应用程序服务器解释 URL 请求，并确定该请求是计划请求。Web 应用程序服务器将计划时间、数据库登录值、参数值、目标和格式发送到指定的中央管理服务器（CMS）。

- 3 CMS 确保用户具有权限来计划对象。如果用户有足够的权限，CMS 会向 CMS 系统数据库中添加一条新记录。CMS 还会将实例添加到其待定计划列表。
- 4 CMS 将响应发送到 Web 应用程序服务器，告知其计划操作已成功。
- 5 Web 应用程序服务器生成下一个 HTML 页面，并通过 Web 服务器将其发送到 Web 客户端。

3.4.4.3 运行计划的 SAP BusinessObjects Web Intelligence 文档

本工作流程介绍计划的 SAP BusinessObjects Web Intelligence 文档在计划时间的运行过程。

- 1 中央管理服务器（CMS）将检查 CMS 系统数据库，确定是否已计划运行 Web Intelligence 文档。
- 2 达到计划的时间时，CMS 查找在自适应作业服务器上运行的可用 Web Intelligence 计划服务。CMS 将计划请求及其相关的所有信息发送到 Web Intelligence 计划服务。
- 3 Web Intelligence 计划服务将基于每个 Web Intelligence 处理服务器上配置的“最大连接数”值查找可用的 Web Intelligence 处理服务器。
- 4 Web Intelligence 处理服务器确定输入文件资源库服务器（FRS）的位置，后者承载文档以及文档所基于的 Universe 元层文件。然后，Web Intelligence 处理服务器从输入 FRS 中请求文档。输入 FRS 查找 Web Intelligence 文档以及文档所基于的 Universe 文件，然后将它们传递到 Web Intelligence 处理服务器。

注意：

此步骤也需要与 CMS 通信，以查找所需的服务器和对象。

- 5 Web Intelligence 文档位于 Web Intelligence 处理服务器上的一个临时目录中。Web Intelligence 处理服务器打开内存中的文档，同时 QT.dll 从文档基于的 Universe 上生成 SQL。Web Intelligence 处理服务器中附带的连接服务器库将连接到数据源。查询数据通过 QT.dll 重新传递到 Web Intelligence 处理服务器中的报表引擎，文档在该引擎中处理。创建一个新的成功实例。
- 6 Web Intelligence 处理服务器将文档实例上载到输出 FRS。

注意：

此步骤也需要与 CMS 通信，以查找所需的服务器和对象。

- 7 Web Intelligence 处理服务器通知自适应作业服务器上的 Web Intelligence 计划服务，指出文档创建已完成。如果将文档安排为转到某个目标（文件系统、FTP、SMTP 或收件箱），自适应作业服务器将从输出 FRS 中检索经过处理的文档，并将其传递到指定的目标。假定本示例中不是这种情况。
- 8 Web Intelligence 计划服务使用作业状态来更新 CMS。
- 9 CMS 在其内存中更新作业状态，然后将实例信息写入 CMS 系统数据库。

3.4.5 分析

3.4.5.1 查看 SAP BusinessObjects Analysis (OLAP 版) 工作区

本工作流程介绍用户请求通过 BI 启动板查看 SAP BusinessObjects Analysis (OLAP 版) 工作区的过程。

注意：

此工作流程需要运行 CMS、自适应处理服务器（包括多维分析服务（MDAS））和输入文件资源库服务器。

- 1 Web 客户端通过 Web 服务器将请求发送到 Web 应用程序服务器以查看新工作区。Web 客户端使用 DHTML AJAX 技术（异步 JavaScript 和 XML）与 Web 应用程序服务器通信。AJAX 技术允许更新部分页面，因此不必为每个新请求呈现一个新页面。
- 2 Web 应用程序服务器转换请求，并将其发送到中央管理服务器（CMS）以确定用户是否有权查看或创建新工作区。
- 3 CMS 从 CMS 系统数据库中检索用户的凭据。
- 4 如果允许该用户查看或创建工作区，则 CMS 会向 Web 应用程序服务器发送确认。同时，它还会发送一个或多个可用多维分析服务（MDAS）的列表。
- 5 Web 应用程序服务器从可用的选择列表中选取一个 MDAS，并将 CORBA 请求发送到该服务，以查找适当的 OLAP 服务器来创建新工作区（或刷新现有工作区）。
- 6 MDAS 需要与输入文件资源库服务器（FRS）通信以检索适当的工作区文档，该文档包含有关基础 OLAP 数据库以及与其一起保存的初始 OLAP 查询的信息。输入 FRS 从基础目录中检索适当的分析工作区，然后将该工作区返回至 MDAS。
- 7 MDAS 打开工作区，建立查询公式，并将其发送到 OLAP 数据库服务器。MDAS 必须针对 OLAP 数据源配置适当的 OLAP 数据库客户端。需要将 Web 客户端查询转换为相应的 OLAP 查询。OLAP 数据库服务器将查询结果发送回 MDAS。
- 8 MDAS（基于创建、查看、打印或导出请求）会预先呈现结果，以便 Java WAS 能够更快地完成呈现。MDAS 将预先呈现的结果的 XML 包发送回 Web 应用程序服务器。
- 9 Web 应用程序服务器呈现工作区，并通过 Web 服务器将经过格式设置的页面或部分页面发送到 Web 客户端。Web 客户端显示更新的页面或新请求的页面。这是一种零客户端解决方案，它不需要下载任何 Java 或 ActiveX 组件。

第 4 章 系统配置向导

4.1 系统配置向导介绍

安装 SAP BusinessObjects Business Intelligence 平台后，可能要执行基本的安装后配置，如：选择部署模板、选择组织要用的 SAP BusinessObjects 产品。要执行此配置，并且在尽可能短的时间内使 BI 平台投入运行，请运行“系统配置向导”。

使用向导的重要优势：

- 向导说明并引导需要执行的配置步骤。
- 使用向导可减少系统的配置错误几率。
- 使用向导进行设置配置可加速系统配置。

默认情况下，向导设置为登录中央管理控制台（CMC）时自动运行，但也可以从 CMC 中的“管理”区域启动向导。可随时重新运行向导调整设置，并可以使用 CMC 中的“服务器”管理页面调优任何设置，包括使用向导进行的设置。

注意：

- 为增强安全性，只有管理员组的成员能够访问向导。
- 为了防止该向导自动运行，管理员用户可在向导首页上选中“启动 CMC 时不再显示此向导”复选框。
- 如果计划安装任何加载项，或者将节点添加到 BI 平台部署，建议在运行系统配置向导前执行这些步骤。

4.2 指定使用的产品

可以通过指定组织使用的产品简化 BI 平台服务器的配置，并通过停止组织不使用的产品的服务器优化资源分配。为此，可在“产品”页面选择产品。指定组织使用的产品时，向导会启动运行这些产品

所需的所有服务器及依赖项，并将这些服务器和依赖项配置为在 BI 平台启动时自动启动。同时，通过取消选择不使用的产品，可以改善 BI 平台的启动时间和资源利用。

例如，如果选择 Crystal Reports 产品，则 BI 平台将自动启动所有 Crystal Reports 服务器以及相应的依赖项。

要查看为某一产品自动启动的服务器列表，请单击产品名称旁的“？”图标。

向导如下配置产品服务器：

- 选择一个产品意味着在向导完成后，将启动所有属于该产品的服务器，以及该产品运行所需的其他服务器（依赖项）。选择一个产品同时还意味着将该产品的服务器设置为随 BI 平台自动启动。如果一台服务器支持多个产品的服务，则只要选择其中一个产品，即会启动该服务器。请注意，如果所选产品的支持服务器同时支持其他产品，则即便未选择这些产品，它们的某些服务也会运行。
- 取消选择一个产品意味着，如果该产品的服务器没有同时支持其他仍选择使用的产品服务或属于“核心服务”类别的服务，则该产品使用的服务器将停止。停止的产品服务器将设置为不随 BI 平台自动启动。如果服务器同时支持选择使用和取消选择使用的产品服务，则该服务器仍保持运行。
- 取消选择一个产品同时意味着，停止不属于所取消产品但仅为该取消产品提供相关服务的服务器。由于不再需要这些依赖服务器，这样做可以释放资源。
- 当选择或取消选择一个产品时，所有承载属于 BI 平台“核心服务”类别的服务的服务器（由 WACS 承载的服务除外）将自动启动。WACS 将保留其当前状态。
- 取消选择产品并不会卸载或移除这些产品的文件。

打开“产品”页面时，页面上的产品状态代表当前系统状态。

如果一个产品的所有服务器都在运行，则该产品的复选框为选定状态。如果一个产品的所有服务器都已停止，则该产品的复选框已清除。如果一个产品只有部分服务器在运行，其他服务器处于其他状态，例如：已停止，则“产品”页面显示“保留现有配置”复选框，表示系统在向导外进行了配置。如果想要使用向导更改配置，可以清除该复选框。

注意：

- “产品”页面显示群集内安装的所有产品。例如：如果计算机 A 安装了产品 P1 和 P2，计算机 B 安装了产品 P2 和 P3，则“产品”页面显示产品 P1、P2、P3。未安装产品不会显示在“产品”页面上。
- 为简化部署，不必为每个节点重复该页面上的配置，可将其应用至整个群集。
- 如果先前在 CMC 中修改了任何设置，则向导会显示消息，告知设置已在向导外进行了更改。可以选择保留现有配置或覆盖当前设置。
- 只有在“复查”页面上单击“应用”后，才会应用向导中所作的更改。

完成更改后，单击“下一步”转到向导的下一页面。还可以使用左侧的导航面板直接跳转到已访问过的任何页面。

4.3 选择部署模板

BI 平台的默认安装会配置小型部署，这种部署适合有限系统硬件上的演示环境。为更好地与您的硬件和计划使用情况相匹配，例如：准备测试系统或生产系统，请在“容量”页面选择一个预定义部署模板。这些模板旨在帮助您快速安装并运行 BI 平台系统，缩短初始部署时间。

虽然选择合适的部署模板有助于进行初始配置，提供一个良好的起点，但并不能替代系统的大小调整和调优。系统大小调整和调优仍必须执行。为了达到最佳性能，应根据规模调整指南来调整系统的大小：<http://www.sap.com/bisizing>。

选择合适的部署模板非常重要，原因如下：

- 系统的请求处理容量受所选部署模板的影响。较大的部署可提供更大的容量，用来处理更多请求或更复杂的请求。但是，较大部署需要更多系统资源。
- 选择较大的部署并不能保证一定会有更好的性能，尤其当可用的硬件资源不充足时。
- 所选部署模板应与业务需求和可用硬件资源相匹配。如果所选部署模板相对于业务需求来讲太小，或相对于可用硬件资源来讲太大，则系统的容量和性能有可能下降。
- 较大部署模板可提供更好的分区，从而降低一个产品中的失败对其他产品产生影响的可能性。选择能够兼顾资源（RAM）利用率和性能两者之间平衡的模板。例如：如果有大量可用 RAM，则可能会选择 RAM 允许的最大部署模板，这样就能拥有更好的系统分区。

可使用滑块选择部署模板，也可以从下拉列表中选择 RAM 数量。更改设置时，请注意“自适应处理服务器的数量”标识会相应变化，显示选择某种设置时，系统会如何配置。

注意：

- 所选部署模板仅影响自适应处理服务器（APS）。其他服务器不会受到影响，例如：CMS、自适应作业服务器。
- “所需 RAM”是 BI 平台服务器需要的最低 RAM 量。例如，在一台 16 GB RAM 的计算机上，操作系统使用 1 GB RAM，数据库服务器使用 1 GB，BI 平台服务器使用 10 GB，则“所需 RAM”为 10 GB，而非 12 GB 或 16 GB。“所需 RAM”代表的只是一个常规值，在高负载情况下，系统可能需要更多 RAM。为达到最佳系统性能，应始终执行系统大小调整。
- 如果当前系统状态与预定义部署模板之一相匹配，则打开“容量”页面时，页面上显示的部署模板代表当前系统状态。例如：如果使用 CMC 手动创建了额外的自适应处理服务器，则系统的当前状态与任何一种部署模板都不相匹配，这时，“容量”页面显示“保留现有配置”复选框，指示系统在向导之外进行了配置。在多节点部署中，如果任何节点有许多与部署模板不相匹配的 APS，或各节点上的 APS 数目不同，也会显示“保留现有配置”复选框。如果想要使用向导更改配置，可以清除该复选框。
- 为简化部署，所选 APS 配置会应用到每个节点（只要这些节点安装了 APS），因此节点越多，群集的容量就越大。
- 加载项（例如，Data Services 或 Analysis Application Design Service (AADS)）不受向导管理。向导不会将加载项创建的服务移至多个 APS。

示例：

- 如果承载 AADS 的 APS 同时承载除主 BI 平台安装外的其他服务，则运行向导并将部署模板大小从 XS 更改为 M 时，该向导将创建七个新的 APS，并将所有服务移至这七个 APS。AADS 服务则将保留在初始 APS 中。
- Data Services 加载项将创建一个专用 APS。该向导不会更改此 APS 且在报告系统中的 APS 数量时不将此 APS 计算在内。

DeploymentTemplates.pdf 文件

有关向导为每个可用部署模板所做设置的详细说明，请单击“容量”页面上的“部署模板”链接打开 DeploymentTemplates.pdf 文件。

DeploymentTemplates.pdf 文件对部署模板进行了详细说明。请注意模板并不指定支持的用户数，因为支持的用户数取决于负载。应执行系统大小调整确定将需要支持的用户数、所需 RAM 数量、CPU 需求等。

4.4 指定数据文件夹位置

使用“文件夹”页面指定希望 BI 平台保存其数据和日志文件的位置。可以指定文件夹位置，或接受当前位置。

如果 BI 平台部署有多个节点，则可以选择以下两个选项来定义文件夹位置：

- 如果要为所有节点配置相同文件夹位置，请选择“所有节点具有相同的文件夹位置”选项。
- 如果群集中的服务器设置不同，那么安装路径或文件目录结构可能不同。可以选择“节点的文件夹位置不同”选项为每个节点配置特定的文件夹位置。

向导打开“文件夹”页面时，将如下显示文件夹名称。

- 如果所有节点的文件夹的值完全相同（即群集中所有服务器上的日志文件夹、群集中所有服务器上的数据文件夹等都相同），则选择“所有节点具有相同的文件夹位置”选项，显示当前文件夹名称。
- 如果每个节点内的特定类型（日志、数据、审核、输入文件存储或输出文件存储）的所有文件夹相同，但各节点间的不同，则选择“节点的文件夹位置不同”选项，显示当前文件夹名称。
- 如果每个节点内特定类型的所有文件夹不同，且各节点间的也不同，则选择“节点的文件夹位置不同”选项，文件夹名称留空。

如果正在更改文件夹位置，则向导配置系统使用新文件夹。除审核数据文件夹外，向导不会将原始文件夹中的内容复制或移动到新文件夹中。如果新文件夹中尚未包含正确内容，或原始文件夹中有想要迁移的数据，则可能会想将数据移动或复制到新文件夹中。

对于输入文件存储、输出文件存储和数据文件夹，如果新文件夹位置为空，应手动从旧文件夹位置复制文件，或通过备份还原文件。对于日志文件夹，仅当想要在新文件夹中包含旧文件夹位置中的日志文件时，才从旧文件夹中复制文件。

提示：

如果计划将文件复制或还原至新文件夹中，请在重启节点前进行操作。

示例方案：

- 如果更改文件夹位置，而原始文件夹中包含报表，只有将这些报表复制到新文件夹中并重启节点，才能在 BI 平台中使用这些报表。
- 如果原始文件夹中包含损坏或修改的报表，您想要恢复到已知的完好备份，则从备份中检索报表并将其放入新文件夹中，而非从原始文件夹中复制内容。
- 如果数据文件原来位于驱动器名称为 X 的磁盘上，而您在操作系统中将该名称更改为 Y，则无需复制或移动数据文件，而只需更改 BI 平台中的文件夹位置。

如果手动更改了部分文件夹位置，使节点上的一些服务器使用一组文件夹，同一节点上的其他服务器使用其他文件夹，则“文件夹”页面显示“保留现有配置”复选框，指示系统在向导外进行了配置。

例如：相同节点上配置了两个文件资源库服务器使用不同的日志文件夹路径。如想使用向导更改当前配置，可清除复选框。

更多有关每个文件夹中所存储文件的类型的信息，请单击“？”图标。

注意：

如果更改下列任何文件夹位置，则需要在向导完成后手动重启所有节点，更改才能生效。

- 输入文件存储
- 输出文件存储
- 日志文件夹
- 数据文件夹

4.5 复查更改

完成配置设置选择后，它们会显示在“复查”页面以供复查，然后更改才能应用于 BI 平台系统。对于每个类别的设置，可单击“详细信息”查看详细描述或即将应用的设置和更改的列表。

如果想更改任何设置，可通过向导左侧的导航菜单直接访问相关页面。

所作选择会保存到日志文件中，日志文件可从“已完成”页面下载。

同时还会生成和保存一个响应文件。响应文件可帮助自动进行系统配置。可单击“下载”按钮查看响应文件或将其下载到本地磁盘。

单击“应用”时，配置设置将应用于 BI 平台部署。向导完成时，会显示“已完成”页面，显示接下来应手动执行的步骤。

相关主题

- 第 85 页上的“[日志文件和响应文件](#)”

4.6 日志文件和响应文件

“已完成”页面显示更改状态，支持下载和查看会话的日志和响应文件。

日志和响应文件自动保存到“系统配置向导”文件夹，该文件夹可从 CMC 访问。文件名时戳格式年_月_日_时_分_秒。日志文件使用 .log 作为扩展名，响应文件的扩展名为 .ini。

还可以单击“下载”按钮查看日志和响应文件，或下载到本地磁盘。

日志文件包含下列内容：

- 在此配置会话中所作全部更改的记录。
- 响应文件保存的位置。
- 后续步骤列表。

相关主题

- 第 86 页上的“[使用响应文件](#)”

4.6.1 使用响应文件

每次完成向导后，会保存一份响应文件，其中包含在向导各页面中所作的选择或对所有问题的回答。响应文件可用于配置 BI 平台部署中的其他群集，从而可以不必为每个群集逐步执行一次向导，也可在日后您想将系统设置为相同的配置状态时使用。使用响应文件可自动进行部署，避免操作错误。

要使用响应文件，需要运行一个将响应文件作为参数的脚本。首先，找到要使用的响应文件，将其保存到磁盘。响应文件自动保存到“系统配置向导”文件夹，管理员可从 CMC 访问对其进行访问。文件名时戳格式：年_月_日_时_分_秒，扩展名 .ini。可从 CMC 中查看响应文件并将其保存到磁盘中，或使用菜单命令“组织” > “发送” > “文件位置”。

还可以从“复查”或“已完成”页面下载当前向导会话的响应文件，并将其保存到磁盘中。

如需在使用前修改响应文件中的设置，可在文本编辑器中编辑响应文件。有关详细信息，请参阅下面的示例响应文件。

运行脚本

如果有合适的响应文件，使用该文件作为执行向导的脚本命令行参数：

- 在 Windows 中，运行批文件 SCW.bat。
- 在 Unix 中，运行脚本文件 scw.sh。

批文件和脚本文件与其他服务器管理脚本一起，位于相同文件夹中。

- Windows: <安装目录>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts。
- Unix: <安装目录>/sap_bobj/enterprise_xi40/linux_x64/scripts。

批文件和脚本文件使用以下命令行参数：

- -help: 显示命令行帮助。
- -r: 指定响应文件路径和名称。
- -cms: 指定要登录的中央管理服务器 (CMS)。如果该参数缺失，CMS 将默认为本地计算机及默认端口 (6400)。示例: machine_name:6500
- -username: 指定提供 BI 平台管理权限的帐户。如果该参数缺失，将使用默认管理员帐户。
- -password: 为帐户指定密码。如果未指定，则会尝试空密码。要使用 -password 参数，还必须使用 -username 参数。

示例

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

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

示例响应文件

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

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

Products.KeepExistingConfiguration = true

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

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

# Crystal Reports
Products.crystalreports = true

# Analysis edition for OLAP
Products.olap = true

# Web Intelligence
Products.webintelligence = false

# Dashboards (Xcelsius)
Products.dashboards = false

# Data Federator
Products.datafederator = true

# Lifecycle Manager
Products.LCM = true

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

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

Capacity.KeepExistingConfiguration = true

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

Capacity.DeploymentTemplate = xs

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

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

Folders.KeepExistingConfiguration = true

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



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

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

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

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

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

必须指定响应文件中的所有设置，不能有任何设置留空，以下情况除外：

- 如果有多节点部署，可以选择删除一个或多个节点的文件夹设置，这样，这些节点的文件夹将保持不变。但是，对于在响应文件中指定的节点，必须指定所有文件夹位置。
- 如果 `KeepExistingConfiguration` 参数设置为 `true`，则可以省略该页的剩余设置。例如：如果 `Products.KeepExistingConfiguration = true`，则可以省去通过响应文件进行的剩余“产品”设置。

有时，响应文件中包含的产品与目标群集中安装的产品不同。这种情况下，适用以下行为：

- 如果响应文件中不包含目标群集中所安装产品的定义，则操作将失败。
- 如果响应文件中包含目标群集中不存在的产品的定义，则会向日志文件中添加警告消息，且剩余产品将适当配置。

注意：

- 使用响应文件配置群集后，需要手动执行日志文件“后续步骤”部分描述的附加步骤。
- 为增强安全性，需要 Enterprise 身份验证支持（非 Windows AD、LDAP 或 SAP）。
- 如果想将任何节点的重启推迟到下一次计划重启，请在计划系统停机时间前运行脚本。

第 5 章 管理许可

5.1 管理许可密钥

本节介绍如何管理 BI 平台部署的许可密钥。

相关主题

- 第 89 页上的“[查看许可信息](#)”
- 第 90 页上的“[添加许可密钥](#)”
- 第 90 页上的“[查看当前帐户活动](#)”

5.1.1 查看许可信息

CMC 的“许可密钥”管理区域标识了与每个密钥关联的并发许可、命名许可和处理器许可的数量。

- 1 转到 CMC 的“许可密钥”管理区域。
- 2 选择许可密钥。

“许可密钥信息”区域显示与密钥关联的详细信息。要购买更多许可密钥，请联系 SAP 销售代表。

相关主题

- 第 90 页上的“[添加许可密钥](#)”
- 第 90 页上的“[查看当前帐户活动](#)”

5.1.2 添加许可密钥

如果您从该产品的试用版升级，请务必在添加任何新的许可密钥或产品激活密钥号码前删除评估密钥。添加新许可密钥后，将需要重新启用所有服务器。

注意：

如果您在更改企业实施 BI 平台许可的方式之后，收到了新许可密钥，则必须从系统中删除先前的所有许可密钥，才能保持合规性。

- 1 转到 CMC 的“许可密钥”管理区域。
- 2 在“添加密钥”字段中输入密钥。
- 3 单击“添加”。

即会将密钥添加到列表。

相关主题

- 第 89 页上的“[查看许可信息](#)”
- 第 90 页上的“[查看当前帐户活动](#)”

5.1.3 查看当前帐户活动

- 1 转到 CMC 的“设置”管理区域。
- 2 单击“查看全局系统量度”。

此部分显示当前的许可使用情况以及其他作业量度。

相关主题

- 第 90 页上的“[添加许可密钥](#)”
- 第 89 页上的“[查看许可信息](#)”

第 6 章 管理用户和组

6.1 帐户管理概述

帐户管理涉及与创建、映射、更改和组织用户及组信息相关的所有任务。利用中央管理控制台（CMC）的“用户和组”管理区域，将能够集中执行这些任务。

创建了用户帐户和组之后，可以添加对象并为它们指定权限。用户登录之后即可使用 BI 启动板或自定义 Web 应用程序查看对象。

6.1.1 用户管理

在“用户和组”管理区域中，可以指定用户访问 BI 平台所需的全部信息。还可以查看由默认用户帐户表概述的两个默认用户帐户。

表6-1：默认用户帐户

帐户名称	说明
Administrator	此用户属于 Administrators 和 Everyone 组。管理员可以在所有 BI 平台应用程序（例如 CMC、CCM、发布向导和 BI 启动板）中执行所有任务。
Guest	此用户属于 Everyone 组。默认情况下启用此帐户，并且系统没有为其分配密码。如果为其分配密码，则对 BI 启动板的单一登录将被破坏。
SMAAdmin	这是 SAP Solution Manager 用来访问 BI 平台组件的只读帐户。

注意：

对象迁移最好由管理员组的成员执行，尤其是管理员用户帐户。要迁移一个对象，可能同时需要迁移很多相关对象。委派管理员帐户可能无法为所有对象获取需要的安全权限。

6.1.2 组管理

组是共享相同帐户权限的用户集；因此，可以创建基于部门、角色或位置的组。组使您可以更改在一个位置（组）中的用户的权限，而不是逐个为用户帐户修改权限。同时，您可以为组分配对象权限。

在“用户和组”区域中，可以创建使多个人员能够访问报表或文件夹的组。这样，您将能够集中进行更改，而不用单独修改每个用户帐户。还可以查看由默认组帐户表概述的几个默认组帐户。

若要在 CMC 中查看可用的组，请在树面板中单击“组列表”。或者，可以单击“组层次结构”以显示所有可用组的分层列表。

表6-2：默认组帐户

帐户名称	说明
Administrators	此组的成员可以在所有 BI 平台应用程序（CMC、CCM、发布向导和 BI 启动板）中执行所有任务。默认情况下，Administrators 组只包含 Administrator 用户。
Everyone	每个用户都是 Everyone 组的成员。
QaaWS Group Designer	此组的成员能够访问 Query as a Web Service。
Report Conversion Tool Users	此组的成员能够访问报表转换工具应用程序。
Translators	此组的成员能够访问翻译管理器应用程序。
Universe Designer Users	将为属于此组的用户授予对“Universe Designer”文件夹和“连接”文件夹的访问权限。他们可以控制谁对 Designer 应用程序具有访问权限。您必须根据需要向此组中添加用户。默认情况下，没有用户属于此组。

相关主题

- 第 112 页上的[“权限在 BI 平台中如何运作”](#)
- 第 103 页上的[“将访问权限授予用户和组”](#)

6.1.3 可用的身份验证类型

在设置 BI 平台中的用户帐户和组之前，请确定要使用的身份验证类型。身份验证类型表概述了可用的身份验证选项（它们视贵组织使用的安全工具而定）。

表6-3：身份验证类型

身份验证类型	说明
Enterprise	如果希望创建独立的帐户和组用于 BI 平台，或者尚未在 LDAP 目录服务器或 Windows AD 服务器中设置用户和组层次结构，请使用系统默认的 Enterprise 身份验证。
LDAP	如果设置了 LDAP 目录服务器，您可以在 BI 平台中使用现有的 LDAP 用户帐户和组。将 LDAP 帐户映射到 BI 平台之后，用户将能够使用他们的 LDAP 用户名和密码访问 BI 平台应用程序。这样就不需要在 BI 平台中重新创建单独的用户和组帐户。
Windows AD	可在 BI 平台中使用现有 Windows AD 用户帐户和组。将 AD 帐户映射到 BI 平台之后，用户将能够使用他们的 AD 用户名和密码登录到 BI 平台应用程序。这样就不需要在 BI 平台中重新创建单独的用户和组帐户。
SAP	可以将现有 SAP 角色映射到 BI 平台帐户。在映射 SAP 角色后，用户可使用 SAP 凭据登录到 BI 平台应用程序。这样就不需要在 BI 平台中重新创建单独的用户和组帐户。
Oracle EBS	可以将现有 Oracle EBS 角色映射到 BI 平台帐户。在映射 Oracle EBS 角色后，用户可使用 Oracle EBS 凭据登录到 BI 平台应用程序。这样就不需要在 BI 平台中重新创建单独的用户和组帐户。
Siebel	可以将现有 Siebel 角色映射到 BI 平台帐户。在映射 Siebel 角色后，用户可使用 Siebel 凭据登录到 BI 平台应用程序。这样就不需要在 BI 平台中重新创建单独的用户和组帐户。

身份验证类型	说明
PeopleSoft Enterprise	可以将现有 PeopleSoft 角色映射到 BI 平台帐户。在映射 PeopleSoft 角色后，用户可使用 PeopleSoft 凭据登录到 BI 平台应用程序。这样就不需要在 BI 平台中重新创建单独的用户和组帐户。
JD Edwards EnterpriseOne	可以将现有 JD Edwards 角色映射到 BI 平台帐户。在映射 JD Edwards 角色后，用户可使用 JD Edwards 凭据登录到 BI 平台应用程序。这样就不需要在 BI 平台中重新创建单独的用户和组帐户。

6.2 管理 Enterprise 帐户和常规帐户

由于 Enterprise 身份验证是 BI 平台的默认身份验证方法，因此在首次安装系统时会自动启用该方法。当您添加和管理用户及组时，BI 平台会在其数据库中保留用户和组信息。

注意：

当用户通过导航至非平台页面或关闭 Web 浏览器注销 BI 平台中的 Web 会话时，其 Enterprise 会话不会被注销，而且该用户仍占用许可。Enterprise 会话将在大约 24 小时后超时。要结束该用户的 Enterprise 会话并释放许可以供其他用户使用，该用户必须从 BI 平台注销。

6.2.1 创建用户帐户

在创建新用户时，您需要指定用户的属性并为用户选择组。

- 1 转到 CMC 的“用户和组”管理区域。
- 2 单击“管理” > “新建” > “新建用户”。
将出现“新建用户”对话框。
- 3 要创建 Enterprise 用户，请
 - a 在“身份验证类型”列表中，选择“Enterprise”。
 - b 输入帐户名称、全名、电子邮件和说明信息。

提示：

使用说明区域来包括有关用户或帐户的额外信息。

g 指定密码信息和设置。

- 4 要创建将使用不同身份验证类型登录的用户，请从“身份验证类型”列表中选择相应选项并键入帐户名称。
- 5 执行下列操作之一指定用户帐户（基于 BI 平台许可协议）：
 - 如果用户属于规定一次允许连接的用户数的许可协议，请选择“并发用户”。
 - 如果用户属于将特定用户与许可关联的许可协议，请选择“命名用户”。对于需要访问 BI 平台，而不管已连接了多少其他用户的用户而言，命名用户许可十分有用。
- 6 单击“创建并关闭”。

用户被添加到系统中，并且自动添加到 Everyone 组中。将自动为用户创建收件箱，同时生成一个 Enterprise 别名。

现在，您可以将用户添加到某个组中，或为用户指定权限。

相关主题

- 第 112 页上的“[权限在 BI 平台中如何运作](#)”

6.2.2 要修改用户帐户

使用此过程来修改用户的属性或组成员资格。

注意：

如果在您进行更改时用户已登录，则用户将受到影响。

- 1 转到 CMC 的“用户和组”管理区域。
 - 2 选择要更改其属性的用户。
 - 3 单击“管理” > “属性”。
- 将出现该用户的“属性”对话框。
- 4 修改该用户的属性。

除了最初创建帐户时提供的所有选项之外，现在还可以通过选中“已禁用帐户”复选框来禁用帐户。

注意：

在用户下次登录之前，对用户帐户所做的任何更改不会出现。

- 5 单击“保存并关闭”。

相关主题

- 第 109 页上的[“为现有用户创建新别名”](#)

6.2.3 删除用户帐户

使用此过程来删除用户的帐户。如果在删除帐户时用户已登录，用户可能会收到错误。删除某个用户帐户时，该用户的收藏夹文件夹、个人类别和收件箱也被删除。

如果认为该用户可能需要在将来再次访问帐户，请在选定用户的“属性”对话框中选中“已禁用帐户”复选框，而不是删除帐户。

注意：

删除用户帐户并不一定能够阻止用户再次登录到 BI 平台。如果用户帐户还存在于第三方系统中，并且该帐户属于映射到 BI 平台的第三方组，则该用户可能仍可以登录。

- 1 转到 CMC 的“用户和组”管理区域。
- 2 选择要删除的用户。
- 3 单击“管理” > “删除”。

将出现删除确认对话框。

- 4 单击“确定”。
- 该用户帐户即被删除。

相关主题

- 第 95 页上的[“要修改用户帐户”](#)
- 第 96 页上的[“删除用户帐户”](#)
- 第 110 页上的[“禁用别名”](#)

6.2.4 创建新组

- 1 转到 CMC 的“用户和组”管理区域。
 - 2 单击“管理” > “新建” > “新建组”。
- 将出现“创建新用户组”对话框。

- 3 输入组的名称和说明。
- 4 单击“确定”。

创建了新组之后，您可以添加用户、添加子组或指定组成员资格以使新组实际成为一个子组。由于子组提供了附加的组织级别，因此在设置对象权限以控制用户对 BI 平台内容的访问时，子组非常有用。

6.2.5 修改组的属性

可通过更改任何设置来修改组的属性。

注意：

属于组的用户在下次登录时，将受到所做修改的影响。

- 1 在 CMC 的“用户和组”管理区域中选择组。
- 2 单击“管理” > “属性”。
- 将出现“属性”对话框。
- 3 修改组的属性。
- 从导航列表中单击链接，以访问不同的对话框和修改不同的属性。
 - 如果要更改组的标题或说明，请单击“属性”。
 - 如果要修改主体拥有的组权限，请单击“用户安全性”。
 - 如果要修改组成员的配置文件值，请单击“配置文件值”。
 - 如果要将组以子组的形式添加到另一个组，请单击“成员”。
- 4 单击“保存”。

6.2.6 查看组成员

可以使用此过程来查看属于特定组的用户。

- 1 转到 CMC 的“用户和组”管理区域。
- 2 在树面板中展开“组层次结构”。
- 3 在树面板中选择组。

注意：

如果组中包含大量用户或已将组映射到某个第三方目录，则列表可能需要几分钟才能显示。

将显示属于该组的用户的列表。

6.2.7 添加子组

可以将组添加到另一个组。这样做时，所添加的组成为一个子组。

注意：

添加子组在过程上与指定组成员资格类似。

- 1 在 CMC 的“用户和组”管理区域中，选择要作为子组添加到另一个组的组。
- 2 单击“操作” > “加入组”。
将出现“加入组”对话框。
- 3 将要向其中添加第一个组的组从“可用组”列表中移到“目标组”列表。
- 4 单击“确定”。

相关主题

- 第 98 页上的[“指定组成员资格”](#)

6.2.8 指定组成员资格

可以使某个组成为另一个组的成员。成为成员的组称为子组。将子组添加到其中的组是父组。子组会继承父组的权限。

- 1 在 CMC 的“用户和组”管理区域中，单击要添加到另一个组的组。
- 2 单击“操作” > “成员”。
将出现“成员”对话框。
- 3 单击“加入组”。
将出现“加入组”对话框。
- 4 将要向其中添加第一个组的组从“可用组”中移到“目标组”列表。

您创建的新组将继承与父组关联的任何权限。

- 5 单击“确定”。
将返回到“成员”对话框，并且父组出现在父组列表中。

6.2.9 删除组

可以在不再需要某个组时将其删除。无法删除 Administrator 和 Everyone 这两个默认组。

注意：

- 属于被删除组的用户在下次登录时，将受到所做更改的影响。
- 属于被删除组的用户将丢失他们从该组继承的任何权限。

若要删除第三方身份验证组（如“Windows AD 用户”组），请使用 CMC 中的“身份验证”管理区域。

- 1 转到 CMC 的“用户和组”管理区域。
- 2 选择要删除的组。
- 3 单击“管理” > “删除”。
将出现删除确认对话框。
- 4 单击“确定”。
组即被删除。

6.2.10 批量添加用户或用户组

可使用 CSV（逗号分隔值）文件向 CMC 批量添加用户或用户组。CSV 文件的正确格式是使用逗号将一行中的数据分隔开来，如下所示：

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

以下情况适用于批量添加过程：

- 导入过程中将忽略 CSV 文件中任何包含错误的行。
 - 导入后用户帐户最初处于禁用状态。
 - 创建新用户时可以使用空白密码。但是，针对现有用户的任何后续更新都必须使用有效的 Enterprise 身份验证密码。
 - 将数据库凭据添加到帐户后，数据库凭据将在用户配置文件中启用。
- 1 在 CMC “用户和组”管理区域中，选择“管理” > “导入” > “用户/组/数据库凭据”。
出现“导入用户/组/数据库凭据”对话框。
 - 2 单击“浏览”，选择一个 CSV 文件并单击“验证”。

这时将处理该文件。如果文件中的数据格式正确，“导入”按钮将为活动状态。如果数据格式不正确，将显示有关错误的信息，必须先解决错误，CMC 才能导入验证文件。

3 单击“导入”。

用户或用户组导入 CMC。

要查看所添加的用户或用户组，请在“用户和组”管理区域中选择“管理” > “导入” > “历史记录”。

6.2.11 启用 Guest 帐户

默认情况下会禁用 Guest 帐户，以确保没有人能够使用此帐户登录到 BI 平台。此默认设置还会禁用 BI 平台的匿名单一登录功能，因此用户在未提供有效用户名和密码的情况下，无法访问 BI 启动板。

如果要启用 Guest 帐户，以便用户无需自己的帐户就能访问 BI 启动板，请执行此任务。

- 1 转到 CMC 的“用户和组”管理区域。
- 2 在导航面板中单击“用户列表”。
- 3 选择“Guest”。
- 4 单击“管理” > “属性”。
将出现“属性”对话框。
- 5 清除“已禁用帐户”复选框。
- 6 单击“保存并关闭”。

6.2.12 将用户添加到组

可通过以下方式向组中添加用户：

- 选择组，然后单击“操作” > “将成员添加到组”。
- 选择用户，然后单击“操作” > “成员”。
- 选择用户，然后单击“操作” > “加入组”。

以下过程描述如何使用这些方法将用户添加到组中。

相关主题

- 第 98 页上的“[指定组成员资格](#)”

6.2.12.1 将用户添加到一个或多个组中

- 1 转到 CMC 的“用户和组”管理区域。
- 2 选择要添加到组的用户。
- 3 单击“操作” > “加入组”。

注意：

系统的所有 BI 平台用户都属于 Everyone 组。

将出现“加入组”对话框。

- 4 将要向其中添加用户的组从“可用组”列表中移到“目标组”列表。

提示：

使用 Shift + 单击或 Ctrl + 单击以选择多个组。

- 5 单击“确定”。

6.2.12.2 将用户添加到组

- 1 在 CMC 的“用户和组”管理区域中选择组。
 - 2 单击“操作” > “将成员添加到组”。
- 将出现“添加”对话框。
- 3 单击“用户列表”。
- “可用用户/组”列表将刷新，并显示系统中的所有用户帐户。
- 4 将要添加到组的用户从“可用用户/组”列表中移到“选定的用户/组”列表。

提示：

- 若要选择多个用户，请使用 Shift + 单击或 Ctrl + 单击组合。
- 若要搜索特定用户，请使用搜索字段。
- 如果系统上有很多用户，请单击“上一页”或“下一页”按钮浏览用户列表。

- 5 单击“确定”。

6.2.13 更改密码设置

在 CMC 内，可以更改系统中特定用户或所有用户的密码设置。下面列出的各种限制仅适用于 Enterprise 帐户 — 也就是说，这些限制不适用于已映射到外部用户数据库（LDAP 或 Windows AD）的帐户。但是，通常情况下，您可以使用外部系统为外部帐户进行类似的限制。

6.2.13.1 更改用户密码设置

- 1 转到 CMC 的“用户和组”管理区域。
- 2 选择要更改其密码设置的用户。
- 3 单击“管理” > “属性”。
将出现“属性”对话框。
- 4 选择或清除与要更改的密码设置关联的复选框。
可用选项如下：
 - 密码从不过期
 - 用户必须在下一次登录时更改密码
 - 用户不能更改密码
- 5 单击“保存并关闭”。

6.2.13.2 更改常规密码设置

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“Enterprise”。
将出现“Enterprise”对话框。
- 3 为要使用的每个密码设置选中该复选框，并在必要时提供值。
下表标识了可以配置的每个设置的最小和最大值。

表6-4：密码设置

密码设置	最小值	建议最大值
强制大小写混合的密码	不适用	不适用
至少必须包含 N 个字符	0 个字符	64 个字符
必须每隔 N 天更改密码	1 天	100 天
不能重新使用 N 个最近的密码	1 个密码	100 个密码
必须等待 N 分钟才能更改密码	0 分钟	100 分钟
在 N 次登录尝试失败后禁用帐户	1 次失败	100 次失败
在 N 分钟后重置失败的登录次数	1 分钟	100 分钟
在 N 分钟后重新启用帐户	0 分钟	100 分钟

- 4 单击“更新”。

注意：

非活动用户帐户不会自动停用。

6.2.14 将访问权限授予用户和组

可以将用户和组管理访问权限授予其他用户和组。管理权限包括：查看、编辑和删除对象；查看和删除对象实例；以及暂停对象实例。例如，为了进行疑难排解和系统维护，您可能需要授予 IT 部门访问权限以便编辑和删除对象。

相关主题

- 第 122 页上的“[将主体分配到对象的访问控制列表](#)”

6.2.15 控制对用户收件箱的访问

在您添加用户时，系统会自动为该用户创建收件箱。收件箱的名称与用户的名称相同。默认情况下，只有用户和管理员才有权访问用户的收件箱。

相关主题

- 第 73 页上的“[设置程序对象的计划](#)”
- 第 120 页上的“[在 CMC 中管理对象的安全设置](#)”

6.2.16 配置 BI 启动板选项

管理员可以配置用户访问 BI 启动板应用程序的方式。通过配置 BOE.war 文件中的属性，可以指定显示在用户登录屏幕上的信息。也可以使用 CMC 为特定组设置 BI 启动板首选项。

6.2.16.1 配置 BI 启动板登录屏幕

默认情况下，BI 启动板登录屏幕会提示用户输入其用户名和密码。还可以提示用户输入 CMS 名称和选择身份验证类型。要更改此设置，需要编辑 BOE.war 文件的 BI 启动板属性。

6.2.16.1.1 配置 BI 启动板登录屏幕

要修改 BI 启动板默认设置，需要为 BOE.war 文件设置自定义 BI 启动板属性。此文件部署在承载 Web 应用程序服务器的计算机上。

- 1 转至 BI 平台安装的下列目录：
 <安装目录>\SAP BusinessObjects Enterprise XI
 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\
- 2 使用文本编辑器创建新文件。
- 3 使用以下名称保存该文件：
 BIlaunchpad.properties
- 4 要在 BI 启动板登录屏幕上包含身份验证选项，请添加以下行：

```
authentication.visible=true
```

- 5 要更改默认身份验证，请添加以下行：

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

将 <authentication> 替换为以下任一选项：

身份验证类型	<authentication> 值
Enterprise	secEnterprise
LDAP	secLDAP
Windows AD	secWinAD
SAP	secSAPR3

- 6 要在 BI 启动板登录屏幕上提示用户输入 CMS 名称，请添加以下行：

```
cms.visible=true
```

- 7 保存并关闭文件。
- 8 重新启动 Web 应用程序服务器。

使用 WDeploy 在 Web 应用程序服务器上重新部署 BOE.war 文件。有关使用 WDeploy 的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

6.2.16.2 为用户组设置 BI 启动板首选项

管理员可以指定适用于用户组内所有用户的 BI 启动板首选项默认值。

注意：

当用户设置自己的首选项时，管理员定义的设置不会应用到该用户的 BI 启动板视图。用户可随时从其自设首选项切换到管理员定义的首选项。

默认情况下，不为任何用户组指定 BI 启动板首选项。管理员可指定下列首选项的默认值：

- 主选项卡
- 文档存储位置
- 文件夹
- 类别
- 每页的对象数
- “文档”选项卡中显示的列
- 文档在 BI 启动板中的显示方式，通过选项卡还是新窗口。

6.2.16.2.1 设置用户组的 BI 启动板首选项

- 1 转到 CMC 的“用户和组”管理区域。
- 2 从“组列表”中选择组。
- 3 单击“操作” > “BI 启动板首选项”
将显示“BI 启动板首选项”对话框
- 4 取消选择“未定义首选项”。
- 5 设置用户的初始视图：
 - 要在用户首次登录时显示“主页”选项卡，请单击“主选项卡”并选择以下选项之一：

选项	说明
默认主选项卡	显示将使用随 BI 平台提供的默认“主页”选项卡。
选择主选项卡	<p>显示特定网站作为主选项卡。</p> <p>单击“浏览主选项卡”。在“选择自定义主选项卡”窗口中，选择一个资源库对象，然后单击“打开”。</p> <p>注意： 只能选择已经添加到资源库中的对象。</p>

- 要在用户首次登录时显示“文档”选项卡，请单击“文档”，然后指定要默认打开的抽屉和节点。可以选择以下选项

抽屉	节点选项
我的文档	选择以下选项之一将其显示在“文档”选项卡中： <ul style="list-style-type: none"> • 我的收藏夹 • 个人类别 • 我的收件箱
文件夹	选择以下选项之一： <ul style="list-style-type: none"> • 公共文件夹：这将在“文档”选项卡中显示公共文件夹 • 选择公共文件夹 单击“浏览文件夹”以选择要显示在“文档”选项卡中的特定公共文件夹。
类别	选择以下选项之一： <ul style="list-style-type: none"> • 公司类别：这将在“文档”选项卡中显示公司类别 • 选择公司类别 单击“浏览文件夹”以选择要显示在“文档”选项卡中的特定公司类别。

例如，如果想要在第一次登录时，“我的文档”抽屉打开到用户的 BI 收件箱，则单击“我的文档”，然后单击“我的收件箱”。

- 6 在“选择“文档”选项卡中显示的列”下，选择想要在“列表”面板中看到的每个对象的摘要信息：
 - 类型
 - 上次运行时间
 - 实例
 - 说明
 - 创建者
 - 创建日期
 - 位置（类别）
 - 接收日期（收件箱）
 - 发件人（收件箱）
- 7 在“设置文档查看位置”下，选择希望用户如何查看其文档。
用户可以打开文档并在 BI 启动板的新选项卡中进行查看，或者在新的 Web 浏览器窗口中查看。
- 8 在“设置每页最大项目数”字段中输入一个数字，以指定希望用户在查看对象列表时每页显示的最大对象数。
- 9 单击“保存并关闭”。

指定的首选项将作为第 2 步中所选组中的用户的默认设置。但是，如果用户具有设置首选项的权限，则可以创建自己的 BI 启动板首选项。如果不希望用户修改首选项，则不应赋予用户设置首选项的权限。

6.3 管理别名

如果用户在 BI 平台中具有多个帐户，则可以使用“分配别名”功能将这些帐户进行链接。这在用户拥有映射到 Enterprise 的第三方帐户和 Enterprise 帐户时很有用。

通过将别名分配给用户，用户可以使用第三方用户名和密码或者 Enterprise 用户名和密码进行登录。因此，别名使用户能够通过多个身份验证类型登录。

在 CMC 中，别名信息显示在用户的“属性”对话框的底部。用户可以具有 Enterprise、LDAP 或 Windows AD 别名的任意组合。

6.3.1 创建用户和添加第三方别名

创建用户并选择除 Enterprise 之外的身份验证类型时，系统将在 BI 平台中创建新用户，并为该用户创建第三方别名。

注意：

要使系统创建第三方别名，必须满足以下条件：

- 需要已在 CMC 中启用了身份验证工具。
- 帐户名的格式必须与身份验证类型所需的格式一致。
- 用户帐户必须存在于第三方身份验证工具中，并且它必须属于已映射到 BI 平台的组。

- 1 转到 CMC 的“用户和组”管理区域。
 - 2 单击“管理” > “新建” > “新建用户”。
- 将出现“新建用户”对话框。
- 3 选择用户的身份验证类型，例如 Windows AD。
 - 4 键入用户的第三方帐户名，例如 bsmith。
 - 5 选择用户的连接类型。
 - 6 单击“创建并关闭”。

即可将用户添加到 BI 平台，并为其分配具有所选身份验证类型的别名，例如 secWindowsAD:ENTERPRISE:bsmith。如果需要，可以添加别名、将别名分配和重新分配给用户。

6.3.2 为现有用户创建新别名

可以为现有 BI 平台用户创建别名。别名可以是 Enterprise 别名，也可以是第三方身份验证工具的别名。

注意：

要使系统创建第三方别名，必须满足以下条件：

- 需要已在 CMC 中启用了身份验证工具。
- 帐户名的格式必须与身份验证类型所需的格式一致。
- 用户帐户必须在第三方身份验证工具中存在，并且它必须属于已映射到该平台的组。

1 转到 CMC 的“用户和组”管理区域。

2 选择要为其添加别名的用户。

3 单击“管理” > “属性”。

将出现“属性”对话框。

4 单击“新建别名”。

5 选择身份验证类型。

6 键入用户的帐户名。

7 单击“更新”。

即为用户创建了别名。在 CMC 中查看此用户时，至少会显示两个别名：已分配给此用户的别名，以及您刚才创建的别名。

8 单击“保存并关闭”退出“属性”对话框。

6.3.3 分配来自另一用户的别名

将别名分配给用户时，将第三方别名从另一个用户移到当前正在查看的用户。无法分配或重新分配 Enterprise 别名。

注意：

如果用户只有一个别名，而您将该最后一个别名分配给另一用户，则系统将删除前者的帐户，以及该帐户的收藏夹文件夹、个人类别和收件箱。

1 转到 CMC 的“用户和组”管理区域。

- 2 选择要为其分配别名的用户。
- 3 单击“管理” > “属性”。
将出现“属性”对话框。
- 4 单击“分配别名”。
- 5 输入具有想要分配的别名的用户帐户，并单击“立即查找”。
- 6 从“可用别名”列表中将要分配的别名移到“要添加到 Username 的别名”列表。

此处 Username 表示要为其分配别名的用户名称。

提示：

若要选择多个别名，请使用 Shift + 单击或 Ctrl + 单击组合。

- 7 单击“确定”。

6.3.4 删除别名

删除别名时，会从系统中删除别名。如果用户只有一个别名，而您删除了该别名，则系统将自动删除该用户帐户，以及该帐户的收藏夹文件夹、个人类别和收件箱。

注意：

删除用户的别名并不一定能够阻止用户再次登录到 BI 平台。如果用户帐户仍然存在于第三方系统中，并且该帐户属于映射到 BI 平台的组，则 BI 平台仍会允许该用户登录。至于系统是创建新的用户还是将别名分配给现有用户，这取决于在 CMC 的“身份验证”管理区域中为身份验证工具选择了哪些更新选项。

- 1 转到 CMC 的“用户和组”管理区域。
- 2 选择要删除其别名的用户。
- 3 单击“管理” > “属性”。
将出现“属性”对话框。
- 4 单击想要删除的别名旁边的“删除别名”按钮。
- 5 如果提示确认，请单击“确定”。
别名即被删除。
- 6 单击“保存并关闭”退出“属性”对话框。

6.3.5 禁用别名

可以通过禁用用户与特定身份验证方法关联的别名，阻止用户使用该方法登录到 BI 平台。要完全禁止用户访问平台，请禁用该用户的所有别名。

注意：

从系统中删除用户并不一定能够阻止用户再次登录到 BI 平台。如果用户帐户仍然存在于第三方系统中，并且该帐户属于映射到平台的组，则系统仍会允许该用户登录。要确保用户不能再使用某个别名登录到 BI 平台，最好禁用该别名。

- 1 转到 CMC 的“用户和组”管理区域。
 - 2 选择要禁用其别名的用户。
 - 3 单击“管理” > “属性”。
- 将出现“属性”对话框。
- 4 清除想要禁用的别名的“已启用”复选框。

为您要禁用的每个别名重复此步骤。

- 5 单击“保存并关闭”。

用户不能再使用您刚才禁用的身份验证类型进行登录。

相关主题

- 第 110 页上的[“删除别名”](#)

第 7 章 设置权限

7.1 权限在 BI 平台中如何运作

权限是控制用户对 BI 平台中的对象、用户、应用程序、服务器和其他功能的访问的基本单位。通过指定用户可对对象执行的具体操作，权限在保护系统安全方面有着非常重要的作用。权限除了可以控制对 BI 平台内容的访问之外，还允许将用户和组的管理工作委派给不同的部门，以及向 IT 人员提供服务器和服务器组的管理权。

请务必记住应设置对对象（如报表和文件夹）的权限，而不是设置对访问对象的主体（用户和组）的权限。例如，要为某经理提供特定文件夹的访问权，则在“文件夹”区域中，将该经理添加到此文件夹的访问控制列表（有权访问对象的主体的列表）中。不能通过在“用户和组”区域中配置该经理的权限设置来为该经理提供访问权。“用户和组”区域中该经理的权限设置用于将其他主体（例如委派的管理员）访问权授予作为系统中的对象的该经理。这样，主体本身就可以像对象一样由具有更高权限的其他人进行管理。

对对象的每项权限可以是授予、拒绝或未指定类型。BI 平台安全模型被设计为：如果未指定某权限，则拒绝该权限。此外，如果设置导致某项权限对于某个用户或组既被授予也被拒绝，则会拒绝该权限。此基于拒绝的设计可帮助确保用户和组不会自动获得未显式授予的权限。

此规则有一个重要例外。如果在子对象上显式设置了与从父对象继承的权限互相矛盾的权限，则在子对象上设置的权限会覆盖继承的权限。此例外也适用于作为组成员的用户。如果向用户显式授予某项权限，但拒绝授予用户组该项权限，则对用户设置的权限会覆盖继承的权限。

相关主题

- 第 116 页上的“[权限覆盖](#)”

7.1.1 访问级别

访问级别是用户经常需要的权限组。通过使用访问级别，管理员可以快速和统一地设置常用的安全级别，而不需要逐一设置每个权限。

BI 平台具有几个预定义的访问级别。这些预定义的访问级别基于权限递增的模型：以查看开始并以完全控制结束，每个访问级别都建立在前一级授予的权限之上。

但是，也可以创建和自定义自己的访问级别；这可以大幅降低与安全性相关的管理成本和维护成本。考虑这种情况：管理员必须管理两个组，即销售经理和销售员工。这两个组都需要在 BI 平台系统中访问五个报表，但销售经理需要比销售员工更多的权限。预定义的访问级别不能满足任一个组的需求。管理员可以创建两个新的访问级别（销售经理和销售员工），而不是将这两个组作为主体添加到每个报表，然后在五个不同的位置修改它们的权限。然后，管理员将这两个组作为主体添加到这些报表，并向这两个组指定各自的访问级别。需要修改权限时，管理员可以修改访问级别。由于访问级别跨所有五个报表应用于这两个组，因此这两个组对报表具有的权限会迅速得以更新。

相关主题

- 第 126 页上的“[使用访问级别](#)”

7.1.2 高级权限设置



CMC 允许设置高级权限，以便能够完全控制对象安全性。在粒度级别为对象定义安全性时，这些高级权限可以提高灵活性。

举例来说，如果需要自定义主体的权限，以使其限定为特定的对象或对象集，请使用高级权限设置。最重要的是，通过使用高级权限，可显式拒绝用户或组获得您在将来更改组成员资格或文件夹安全级别时不得更改的任何权限。

下表摘要说明了在设置高级权限时可选择的选项。

表7-1：权限选项

图标	权限选项	说明
	已授予	权限已授予主体。
	已拒绝	已对主体拒绝权限。
	未指定	权限对于主体未指定。默认情况下，会拒绝设置为“未指定”的权限。

图标	权限选项	说明
	应用于对象	权限应用于对象。单击“已授予”或“已拒绝”后，此选项将变为可用。
	应用于子对象	权限应用于子对象。单击“已授予”或“已拒绝”后，此选项将变为可用。

相关主题

- 第 118 页上的[“特定于类型的权限”](#)

7.1.3 继承

为控制对对象的访问，可为主体设置对对象的权限；但是，显式地为每个主体设置对每个对象的每个可能权限的值是不切实际的。假设某个系统具有 100 种权限、1000 位用户和 10,000 个对象：若要显式设置对每个对象的权限，则需要 CMS 在其内存中存储几十亿项权限，并且最重要的是，管理员需要手动设置每一项权限。

继承模式解决了这个不切实际的问题。通过继承，用户所拥有的对系统中对象的权限来自于他们在不同组和子组中的成员资格，以及从父文件夹和子文件夹中继承了权限的对象。这些用户可以因拥有组成员资格而继承权限；子组可以从父组继承权限；用户和组都可以从父文件夹继承权限。

默认情况下，如果用户或组具有某个文件夹的权限，则对于后来发布到该文件夹的任何对象，用户或组将会继承相同的权限。因此，最佳策略是先在文件夹级别为用户和组设置适当的权限，然后将对象发布到该文件夹。

BI 平台可识别两种类型的继承：组继承和文件夹继承。

7.1.3.1 组继承

组继承使主体能够因组成员资格而继承权限。将所有用户安排到符合组织当前安全约定的组中时，组继承特别有用。

在组继承示例 1 中，可以看到组继承如何工作。红组是蓝组的子组，因此红组继承蓝组的权限。在本例中，红组将权限 1 作为已授予的权限来继承，并将其余权限作为未指定的权限来继承。红组的每个成员均继承这些权限。此外，子组的成员将继承所设置的子组的任何其他权限。在本例中，绿色用户是红组的成员，因此他将权限 1 作为已授予的权限来继承、将权限 2、3、4 和 6 作为未指定的权限来继承，将权限 5 作为已拒绝的权限来继承。



图 7-1：组继承示例 1

如果为属于多个组的用户启用组继承，系统在检查凭据时将考虑所有父组的权限。用户会被拒绝已在任何父组中显式拒绝的任何权限，并且用户会被拒绝保持为完全未指定的任何权限。因此，只会授予用户已在一个或多个组中（显式或通过访问级别）授予并且从未显式拒绝的那些权限。

在组继承示例 2 中，绿色用户是两个不相关的组的成员。从蓝组中，该用户将权限 1 和 5 作为“已授予”的权限来继承，将其余的权限作为未指定的权限来继承；但是，由于绿色用户也属于红组，并且红组已被显式拒绝权限 5，因此绿色用户从蓝组继承的权限 5 将被覆盖。

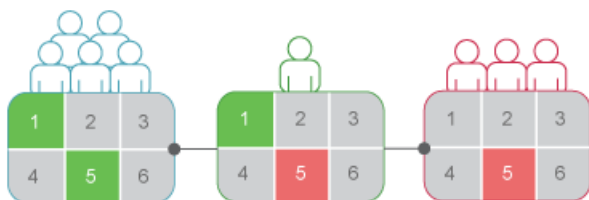


图 7-2：组继承示例 2

相关主题

- 第 116 页上的“[权限覆盖](#)”

7.1.3.2 文件夹继承

文件夹继承允许主体继承被授予的对对象父文件夹的任何权限。将 BI 平台内容安排到反映组织当前安全约定的文件夹层次结构中时，文件夹继承尤为重要。例如，假设创建了一个称为“销售报表”的文件夹，并为“销售”组提供了此文件夹的按需查看访问权限。默认情况下，对于您随后发布到“销售报表”文件夹的报表，对此文件夹具有权限的每个用户将继承相同的权限。因此，“销售”组将对所有报表具有按需查看访问权限，并且只需在文件夹级别设置一次对象权限。

在文件夹继承示例中，已为红组设置了文件夹权限。已授予权限 1 和 5，而其余的权限均处于未指定状态。启用文件夹继承后，红组成员在对象级别的权限与该组在文件夹级别的权限相同。权限 1 和 5 将作为“已授予”类型的权限被继承，而其余的权限均处于未指定状态。

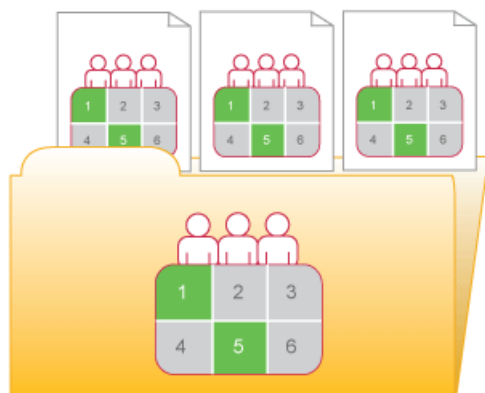


图 7-3：文件夹继承示例

相关主题

- 第 116 页上的“[权限覆盖](#)”

7.1.3.3 权限覆盖

权限覆盖是一种权限行为，也即在子对象上设置的权限将覆盖在父对象上设置的权限。在以下情况下会发生权限覆盖：

- 通常，在子对象上设置的权限会覆盖在父对象上设置的相应权限。
- 通常，在子组或组成员上设置的权限会覆盖在组上设置的相应权限。

无需禁用继承即可在对象上设置自定义权限。子对象继承父对象的权限设置，但在子对象上显式设置的权限除外。此外，对父对象的权限设置所做的任何更改均会应用到子对象。

权限覆盖示例 1描述了权限覆盖如何作用于父对象和子对象。蓝色用户被拒绝授予编辑文件夹内容的权限；权限设置由子文件夹继承。但是，管理员向蓝色用户授予对子文件夹中的文档的“编辑”权限。蓝色用户获得的文档“编辑”权限覆盖了来自文件夹和子文件夹的继承权限。

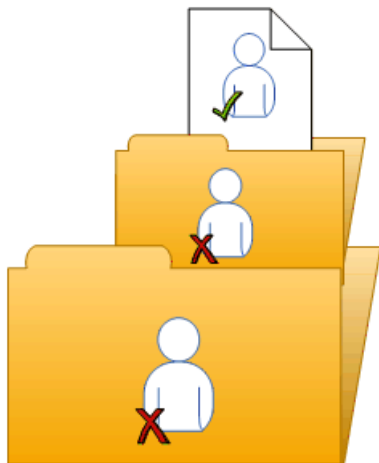


图 7-4：权限覆盖示例 1

权限覆盖示例 2描述了权限覆盖如何作用于成员和组。蓝色组被拒绝授予编辑文件夹的权限；蓝色子组继承此权限设置。但是，管理员向蓝色用户（是蓝色组和蓝色子组的成员）授予文件夹的“编辑”权限。蓝色用户获得的文件夹“编辑”权限覆盖了来自蓝色组和蓝色子组的继承权限。

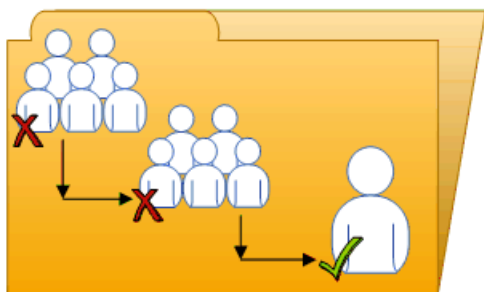


图 7-5：权限覆盖示例 2

复合权限覆盖说明了权限覆盖的影响不太明显的情况。紫色用户是子组 1A 和 2A 的成员，而这两个子组分别在组 1 和 2 中。组 1 和 2 都具有文件夹的“编辑”权限。1A 继承了组 1 的“编辑”权限，但管理员拒绝将“编辑”权限授予 2A。由于权限覆盖的缘故，2A 上的权限设置覆盖了组 2 上的权限设置。因此，紫色用户从 1A 和 2A 继承了互相矛盾的权限设置。1A 和 2A 没有父子关系，因此不会发生权限覆盖；也就是说，子组的权限设置不会互相覆盖，因为它们具有同等的状态。最终，紫色用户被拒绝授予“编辑”权限，因为 BI 平台中使用“基于拒绝”的权限模型。

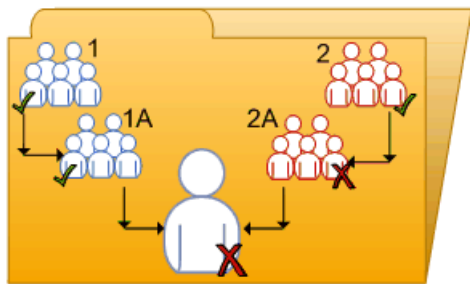


图 7-6: 复合权限覆盖

权限覆盖允许用户对子对象上的权限设置进行轻微调整，而不必丢弃所有继承的权限设置。假设有这样一种情况：销售经理需要查看“机密”文件夹中的机密报表。销售经理是“销售”组的成员，该组被拒绝访问该文件夹及其内容。管理员向该经理授予对“机密”文件夹的“查看”权限，并继续拒绝“销售”组访问。在这种情况下，授予销售经理的“查看”权限将覆盖该经理从“销售”组的成员关系中继承的拒绝访问权限。

7.1.3.4 权限作用域

权限作用域是指控制权限继承范围的能力。若要定义权限作用域，应决定权限是应用于对象、应用于其子对象还是同时应用于两者。默认情况下，权限作用域将同时延伸到对象和子对象。

权限作用域可用于保护共享位置中的个人内容。假设有这样一种情况：财务部有一个共享的“费用索赔”文件夹，该文件夹包含每个雇员的“个人费用索赔”子文件夹。雇员希望能够查看“费用索赔”文件夹并向其中添加对象，但同时希望保护他们的“个人费用索赔”子文件夹的内容。管理员向所有雇员授予对“费用索赔”文件夹的“查看”和“添加”权限，但将这些权限的作用域限制为仅对“费用索赔”文件夹起作用。这意味着，“查看”和“添加”权限不适用于“费用索赔”文件夹中的子对象。然后，管理员向雇员授予对他们自己的“个人费用索赔”子文件夹的“查看”和“添加”权限。

权限作用域还可以限制委派的管理员所具有的有效权限。例如，委派的管理员可能具有某文件夹的安全地修改权限和编辑权限，但这些权限的作用域被限制为此文件夹，并且不应用于其子对象。委派的管理员无法向另一个用户授权，使用该用户获得对此文件夹的某个子对象的这些权限。

7.1.4 特定于类型的权限

特定于类型的权限是仅影响特定对象类型的权限，这些类型有 Crystal 报表、文件夹或访问级别等。特定于类型的权限由以下权限组成：

- 对象类型的常规权限

这些权限与常规全局权限相同（例如，添加、删除或编辑对象的权限），但在特定对象类型上设置这些权限以覆盖常规全局权限设置。

- 对象类型的特定权限

这些权限仅可用于特定对象类型。例如，会为 Crystal 报表显示导出报表数据的权限，但不会为 Word 文档显示此权限。

特定于类型的权限示例一图说明特定于类型的权限如何工作。在这里，权限 3 表示编辑对象的权限。蓝色组被拒绝授予对顶层文件夹的“编辑”权限，而被授予对文件夹和子文件夹中的 Crystal 报表的“编辑”权限。这些“编辑”权限特定于 Crystal 报表，并覆盖常规全局级别上的权限设置。因此，蓝色组的成员具有 Crystal 报表的“编辑”权限，但不具有子文件夹中 XLF 文件的“编辑”权限。

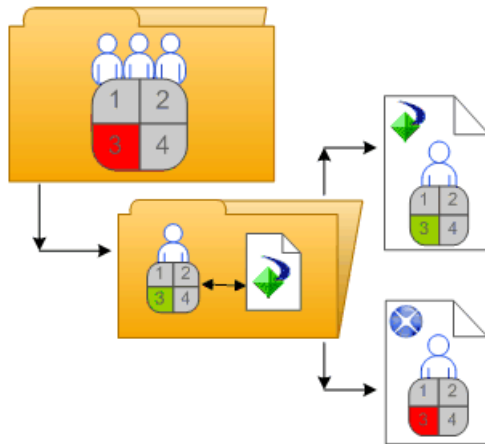


图 7-7：特定于类型的权限示例

特定于类型的权限很有用，因为利用此类权限可以根据对象类型限制主体的权限。假设有这样一种情况：管理员希望员工能够向文件夹中添加对象，但不能够创建子文件夹。管理员在文件夹的常规全局级别授予“添加”权限，然后为文件夹对象类型拒绝“添加”权限。

根据权限应用到的对象类型，权限被划分为以下集合：

- 常规

这些权限影响所有对象。

- 内容

这些权限按照特定的内容对象类型进行划分。内容对象类型的示例包括 Crystal 报表和 Adobe Acrobat PDF。

- 应用程序

这些权限按照它们影响的 BI 平台应用程序进行划分。应用程序的示例包括 CMC 和 BI 启动板。

- 系统

这些权限按照它们影响的核心系统组成部分进行划分。核心系统组成部分的示例包括：日历、事件、用户和组。

特定于类型的权限位于“内容”、“应用程序”和“系统”集合中。在各个集合中，这些权限根据对象类型进一步划分为多个类别。

7.1.5 确定有效权限

针对对象设置权限时，请考虑以下几点：

- 每个访问级别都会授予某些权限、拒绝某些权限，并保持其他权限为未指定。为用户授予了若干访问级别时，默认情况下，系统会聚合有效权限并拒绝任何未指定的权限。
- 针对某个对象将多个访问级别分配给主体时，主体将拥有每个访问级别的权限的组合。将为多个访问级别中的用户分配两个访问级别。一个访问级别向用户授予权限 3 和 4，另一个访问级别仅授予权限 3。用户的有效权限为 3 和 4。

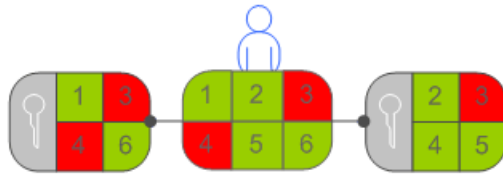


图 7-8：多个访问级别

- 可以结合高级权限与访问级别，针对某个对象自定义主体的权限设置。例如，如果针对某个对象为主体显式分配了高级权限和访问级别，并且高级权限与访问级别中的权限冲突，则高级权限将覆盖访问级别中的权限。

只有针对相同对象为相同主体设置了高级权限时，高级权限才能覆盖访问级别中与其对应的同等权限。例如，在常规全局级别设置的高级“添加”权限可以覆盖访问级别中的常规“添加”权限设置；它无法覆盖访问级别中特定于类型的“添加”权限设置。

但是，高级权限不会总是覆盖访问级别。例如，将会拒绝主体拥有父对象的编辑权限。在子对象上，为主体分配了授予其编辑权限的访问级别。最终，主体拥有子对象的编辑权限，原因是针对子对象设置的权限覆盖了针对父对象设置的权限。

- 权限覆盖使针对子对象设置的权限可能覆盖从父对象继承的权限。

7.2 在 CMC 中管理对象的安全设置

可以在 CMC 中使用“管理”菜单上的安全选项来管理大多数对象的安全设置。利用这些选项，可以将主体分配到某个对象的访问控制列表、查看主体拥有的权限，以及修改主体对某个对象拥有的权限。

依据安全需求以及为其设置权限的对象类型，安全管理的具体详细信息有所不同。不过，以下任务的工作流大体上非常类似：

- 查看主体对于某个对象的权限。
- 将主体分配给某个对象的访问控制列表，并指定这些主体具有哪些权限和访问级别。
- 在 BI 平台中设置对顶层文件夹的权限。

7.2.1 查看主体的对象权限

通常，可采用此工作流查看主体的对象权限。

- 1 选择要查看其安全设置的对象。
 - 2 单击“管理” > “用户安全性”。
- 将出现“用户安全性”对话框，并显示对象的访问控制列表。
- 3 从访问控制列表中选择主体，然后单击“查看安全性”

“权限资源管理器”将启动，并显示主体对于对象的有效权限的列表。此外，还可以利用“权限资源管理器”执行以下操作：

- 浏览到要查看其权限的另一个主体。
- 依据以下条件过滤显示的权限：
 - 分配的权限
 - 授予的权限
 - 未分配的权限
 - 来源访问级别
 - 对象类型
 - 权限的名称
- 依据以下条件按升序或降序对所显示权限的列表进行排序：
 - 集合
 - 类型
 - 权限名称
 - 权限状态（已授予、已拒绝或未指定）

此外，可以单击“源”列中的某个链接以显示继承权限的源。

7.2.2 将主体分配到对象的访问控制列表

访问控制列表指定被授予或拒绝授予对象权限的用户。通常，可采用此工作流将主体分配到访问控制列表，并指定该主体拥有的对象权限。

- 1 选择要向其中添加主体的对象。
- 2 单击“管理” > “用户安全性”。
- 将出现“用户安全性”对话框，并显示访问控制列表。
- 3 单击“添加主体”。
- 将出现“添加主体”对话框。
- 4 将要作为主体添加的用户和组从“可用用户/组”列表移到“选定的用户/组”列表中。
- 5 单击“添加和指定安全性”。
- 6 选择要授予主体的访问级别。
- 7 选择是要启用还是禁用文件夹或组继承。

如有必要，还可以在粒度级别修改权限，以改写访问级别中的某些权限。

相关主题

- 第 122 页上的[“修改主体的对象安全性”](#)

7.2.3 修改主体的对象安全性

通常，建议使用访问级别为主体分配权限。但是，有时可能需要改写访问级别中的某些粒度权限。利用高级权限可以基于主体已经拥有的访问级别自定义主体的权限。通常，可采用此工作流向主体分配对象高级权限。

- 1 将主体分配到对象的访问控制列表。
- 2 添加了主体后，转到“管理” > “用户安全性”以显示对象的访问控制列表。
- 3 从访问控制列表中选择主体，然后单击“指定安全性”。
- 将出现“指定安全性”对话框。
- 4 单击“高级”选项卡。
- 5 单击“添加/删除权限”。
- 6 修改主体的权限。

所有可用权限均在“权限附录”中进行了汇总。

相关主题

- 第 122 页上的[“将主体分配到对象的访问控制列表”](#)

7.2.4 在 BI 平台中设置对顶层文件夹的权限

通常，可采用此工作流对 BI 平台中的顶层文件夹设置权限。

注意：

对于此版本，主体需要对容器文件夹具有“查看”权限，以便能够在该文件夹中导航并查看其子对象。这意味着，主体需要对顶层文件夹具有“查看”权限才能查看文件夹中的对象。如果要限制主体的“查看”权限，可以授予主体对特定文件夹的“查看”权限，并将权限作用域设置为只应用于该文件夹。

- 1 转到包含要为其设置权限的顶层文件夹的 CMC 区域。
- 2 单击“管理” > “顶级安全性” > “所有 Objects”。

此处 Objects 表示顶层文件夹的内容。如果提示您确认，单击“确定”。

将出现“用户安全性”对话框，并显示顶层文件夹的访问控制列表。

- 3 将主体分配给顶层文件夹的访问控制列表。
- 4 如有必要，向主体分配高级权限。

相关主题

- 第 122 页上的[“将主体分配到对象的访问控制列表”](#)
- 第 122 页上的[“修改主体的对象安全性”](#)

7.2.5 检查主体的安全设置

某些情况下，可能需要知道为主体授予或拒绝访问权限的对象。为此，可以使用安全性查询。利用安全性查询可以确定主体具有哪些对象的特定权限，并可以管理用户权限。对于每个安全性查询，要提供以下信息：

- 查询主体

指定要为其运行安全性查询的用户或组。可以为每个安全性查询指定一个主体。

- 查询权限

指定要为其运行安全性查询的权限、这些权限的状态以及设置了这些权限的对象类型。例如，可以为主体可刷新所有报表运行安全性查询，或者为主体无法导出的所有报表运行安全性查询。

- 查询上下文

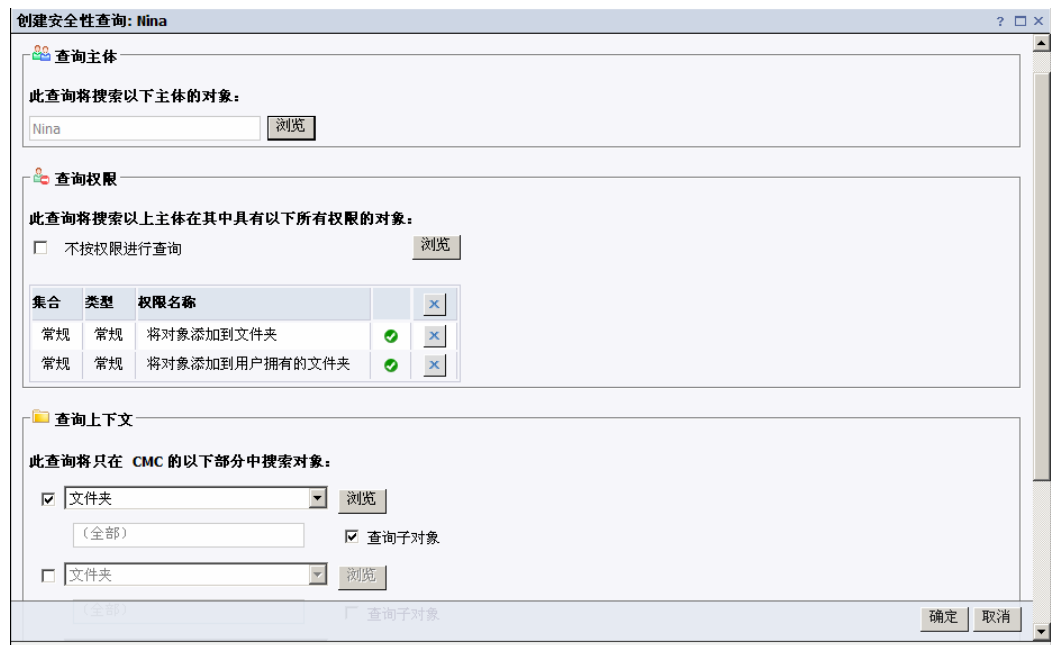
指定希望安全性查询搜索的 CMC 区域。对于每个区域，可以选择是否在安全性查询中包含子对象。安全性查询最多可以有四个区域。

运行安全性查询时，结果显示在“树”面板中“安全性查询”下的“查询结果”区域中。如果要细化安全性查询，可以在第一次查询的结果中运行第二次查询。

安全性查询很有用，因为利用此类查询可以查看主体具有特定权限的对象，而且，如果要修改这些对象，此类查询还提供了这些对象的位置。考虑这种情况：某销售员工被提升为销售经理。该销售经理需要 Crystal 报表的“计划”权限，他以前仅具有这些报表的“查看”权限，而且这些报表位于不同的文件夹中。在这种情况下，管理员运行安全性查询以了解该销售经理对所有文件夹中的 Crystal 报表的查看权限，并在查询中包含子对象。在安全性查询运行后，管理员可以在“查询结果”区域中看到该销售经理具有“查看”权限的所有 Crystal 报表。由于“详细信息”面板显示了各个 Crystal 报表的位置，因此，管理员可以浏览各个报表，并修改该销售经理对报表具有的权限。

7.2.5.1 运行安全性查询

- 1 在“用户和组”区域的“详细信息”面板中，选择要为其运行安全性查询的用户或组。
- 2 单击“管理” > “工具” > “创建安全性查询”。



将出现“创建安全性查询”对话框。

- 3 确保“查询主体”区域中的主体正确无误。
如果决定为其他主体运行安全性查询，可以单击“浏览”选择另一个主体。在“浏览查询主体”对话框中，展开“用户列表”或“组列表”以浏览主体，或按名称搜索主体。完成后，单击“确定”返回到“创建安全性查询”对话框。
- 4 在“查询权限”区域中，指定要为其运行查询的权限和每项权限的状态。
 - 如果要为主体在对象上具有的特定权限运行查询，请单击“浏览”，设置要为其运行安全性查询的每项权限的状态，然后单击“确定”。

提示：
可以通过单击权限旁边的删除按钮从查询中删除特定的权限；或者，通过单击页眉行中的删除按钮从查询中删除所有权限。

 - 如果要运行常规安全性查询，请选中“不按权限进行查询”复选框。

选中该复选框后，BI 平台会为访问控制列表中包含主体的所有对象运行常规安全性查询，而不管主体在对象上具有什么权限。
- 5 在“查询上下文”区域中，指定要查询的 CMC 区域。
 - a 选中列表旁边的复选框。
 - b 在列表上，选择要查询的 CMC 区域。
如果要查询区域内的更具体位置（例如，“文件夹”下的某个特定文件夹），请单击“浏览”打开“浏览查询上下文”对话框。在“详细信息”窗格中，选择要查询的文件夹，然后单击“确定”。返回到“安全性查询”对话框时，指定的文件夹将出现在列表下方的框中。
 - c 选择“查询子对象”。
 - d 为要查询的每个 CMC 区域重复上面的步骤。

注意：
最多可以查询四个区域。

- 6 单击“确定”。
安全性查询将运行，并且将转到“查询结果”区域。
- 7 若要查看查询结果，请在“树”面板中展开“安全性查询”，并单击一个查询结果。

提示：
查询结果按主体的名称列出。

查询结果显示在“详细信息”面板中。

“查询结果”区域保留一次用户会话中的所有安全性查询结果，直至用户注销为止。如果要再次运行查询，但要采用新的规范，请单击“操作” > “编辑查询”。也可以通过选择查询并单击“操作” > “重新运行查询”来重新运行完全相同的查询。如果要保留安全性查询结果，请单击“操作” > “导出”，将安全性查询结果导出为 CSV 文件。

7.3 使用访问级别

可以对访问级别执行以下操作：

- 复制现有的访问级别，对副本进行更改、重命名并将其保存为新的访问级别。
- 创建、重命名和删除访问级别。
- 修改访问级别中的权限。
- 跟踪访问级别与系统中其他对象之间的关系。
- 跨站点复制和管理访问级别。
- 使用 BI 平台中预定义的一种访问级别快速一致地为许多主体设置权限。

下表汇总了各种预定义的访问级别包含的权限。

表7-2：预定义的访问级别

访问级别	说明	相关权限
查看	如果在文件夹级别设置，则主体可以查看文件夹、文件夹中的对象和每个对象的生成的实例。如果在对象级别设置，则主体可以查看对象、对象的历史记录和对象的生成的实例。	<ul style="list-style-type: none">• 查看对象• 查看文档实例

访问级别	说明	相关权限
计划	通过计划对象根据指定的数据源运行一次或重复运行，主体可以生成实例。主体可以查看、删除和暂停其所拥有的实例的计划。他们还可以将对象计划为不同的格式和计划到不同的目标、设置参数和数据库登录信息、选择处理作业的服务器、向文件夹添加内容，以及复制对象或文件夹。	“查看”访问级别权限，以及： <ul style="list-style-type: none"> 计划文档运行 定义服务器组以便处理作业 将对象复制到另一文件夹 计划到目标 打印报表的数据 导出报表的数据 编辑用户拥有的对象 删除用户拥有的实例 暂停并继续用户拥有的文档实例
按需查看	主体可以依据数据源按需要刷新数据。	“计划”访问级别权限，以及： <ul style="list-style-type: none"> 刷新报表的数据
完全控制	主体具有对象的完全管理控制权限。	所有可用权限，其中包括： <ul style="list-style-type: none"> 将对象添加到文件夹 编辑对象 修改用户拥有的对象权限 删除对象 删除实例

下表汇总了为访问级别执行某些任务所需的权限。

访问级别任务	所需的权限
创建访问级别	<ul style="list-style-type: none"> “访问级别”顶层文件夹的“添加”权限
查看访问级别中的粒度权限	<ul style="list-style-type: none"> 访问级别的“查看”权限
将访问级别指定到对象上的主体	<ul style="list-style-type: none"> 访问级别的“查看”权限 访问级别的“使用访问级别进行安全性分配”权限 对象的“修改权限”权限，或者对象和主体的“安全地修改权限”权限 <p>注意： 具有“安全地修改权限”权限并且想要为主体分配访问级别的用户必须为自己分配相同的访问级别。</p>
修改访问级别	<ul style="list-style-type: none"> 访问级别的“查看”和“编辑”权限
删除访问级别	<ul style="list-style-type: none"> 访问级别的“查看”和“删除”权限
克隆访问级别	<ul style="list-style-type: none"> 访问级别的“查看”权限 访问级别的“复制”权限 “访问级别”顶层文件夹的“添加”权限

7.3.1 在“查看”和“按需查看”访问级别之间选择

当通过 Web 创建报表时，需要做出的一个最重要的决定是使用实时数据还是已保存数据。但无论作何选择，BI 平台都会尽快显示第一页，以便用户可以在其他数据尚在处理的时候看到自己的报表。本节说明两种预定义访问级别之间的区别，供用户作出此选择。

“按需查看”访问级别

按需创建报表可使用户直接从数据库服务器实时访问实时数据。使用实时数据，用户在所访问信息经常变化的情况下随时能获得最新的数据，时间可精确到秒。例如，某个大型配送中心每天货运不断，经理需要对库存进行跟踪，那么采用实时报表创建就能使他们得到所需的信息。

但是，在为所有报表提供实时数据之前，请考虑是否要让所有用户持续不断地访问数据库服务器。如果数据不是快速或经常更改，那么所有这些数据库请求除了增加网络流量和消耗服务器资源以外没有多大的意义。在这种情况下，您可能宁愿计划报表重复运行，以便用户始终能够查看最新数据（报表实例），而无需访问数据库服务器。

用户需要拥有“按需查看”权限才能依据数据库刷新报表。

“查看”访问级别

为减少网络流量以及查询数据库服务器的次数，您可以将报表计划为在指定的时间运行。当报表已运行时，用户可以根据需要查看该报表实例，而不会触发对数据库的额外查询。

报表实例可用于处理未持续更新的数据。当用户浏览报表实例并在列或统计图上执行向下钻取以查看详细资料时，他们不直接访问数据库服务器；相反，他们访问的是已保存的数据。因此，带有已保存数据的报表不仅将网络数据传输量降到最低，而且还减轻了数据库服务器的负担。

例如，如果您的销售数据库每天更新一次，则可以按类似的计划运行报表。这样，销售代表就总能使用当前的销售数据，而不必在每次打开报表时访问数据库。

用户只需拥有“查看”权限即可显示报表实例。

7.3.2 复制现有的访问级别

如果需要与现有的某个访问级别略微不同的访问级别，这是创建访问级别的最好方法。

- 1 转到“访问级别”区域。
- 2 在“详细信息”面板中，选择一个访问级别。

提示：

选择所包含权限与您的访问级别的所需权限类似的访问级别。

- 3 单击“组织” > “复制”。
- 所选访问级别的副本即会出现在“详细信息”面板中。

7.3.3 创建新访问级别

如果需要与现有的某个访问级别差别很大的访问级别，这是创建访问级别的最好方法。

- 1 转到“访问级别”区域。
 - 2 单击“管理” > “新建” > “创建访问级别”。
- 将出现“创建新访问级别”对话框。
- 3 为新访问级别输入标题和说明，然后单击“确定”。
- 将返回到“访问级别”区域，并且新访问级别将出现在“详细信息”面板中。

7.3.4 重命名访问级别

- 1 在“访问级别”区域的“详细信息”面板中，选择要重命名的访问级别。
- 2 单击“管理” > “属性”。
将出现“属性”对话框。
- 3 在“标题”字段中，为访问级别输入一个新名称，然后单击“保存并关闭”。
将返回到“访问级别”区域。

7.3.5 删除访问级别

- 1 在“访问级别”区域的“详细信息”面板中，选择想要删除的访问级别。
- 2 单击“管理” > “删除访问级别”。

注意：

不能删除预定义的访问级别。

将出现一个对话框，其中包含有关此访问级别影响的对象的信息。如果不想删除该访问级别，请单击“取消”退出对话框。

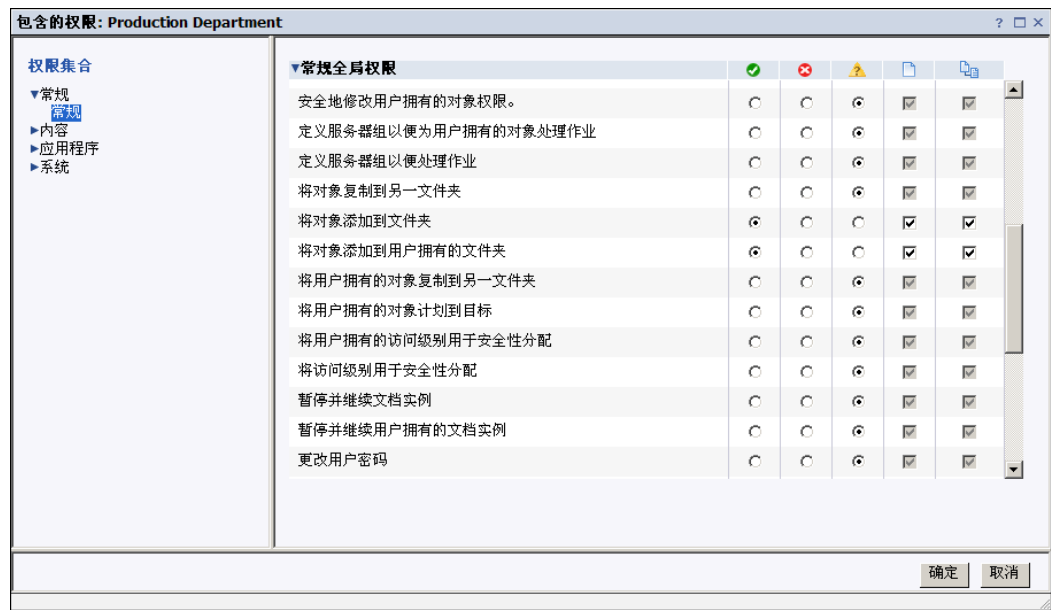
- 3 单击“删除”。
访问级别即被删除，并且将返回到“访问级别”区域。

7.3.6 修改访问级别中的权限

若要为访问级别设置权限，请首先设置适用于所有对象的常规全局权限（与类型无关），然后指定要在何时覆盖基于特定对象类型的常规设置。

- 1 在“访问级别”区域的“详细信息”面板中，选择想要为其修改权限的访问级别。
- 2 单击“操作” > “包含的权限”。
将出现“包含的权限”对话框，并显示有效权限的列表。

3 单击“添加/删除权限”。



“包含的权限”对话框在导航列表中显示访问级别的权限集合。“常规全局权限”部分默认情况下处于展开状态。

- 4 设置常规全局权限。
每个权限的状态都可能为“已授予”、“已拒绝”或“未指定”。还可以选择是将该权限仅应用于对象、仅应用于子对象还是同时应用于两者。
- 5 要为访问级别设置特定于类型的权限，请在导航列表中单击权限集合，然后单击适用于要为其设置权限的对象类型的子集合。
- 6 完成后单击“确定”。
将返回到有效权限的列表。

相关主题

- 第 120 页上的[“在 CMC 中管理对象的安全设置”](#)
- 第 118 页上的[“特定于类型的权限”](#)

7.3.7 跟踪访问级别和对象之间的关系

在修改或删除访问级别之前，务必要确认对访问级别所做的任何更改不会对 CMC 中的对象产生负面影响。为此，可以为访问级别运行关系查询。

关系查询对于权限管理很有用，因为利用此类查询可以在一个方便的位置查看某个访问级别影响的对象。考虑这种情况：某公司改组其组织结构，并将部门 A 和部门 B 这两个部门合并为部门 C。管理员决定删除部门 A 和部门 B 的访问级别，因为这两个部门不再存在。在删除这两个访问级别之前，管理员为它们运行关系查询。在“查询结果”区域中，管理员可以看到在删除这两个访问级别后将会影响的对象。如果在删除访问级别之前必须修改对象的权限，则“详细信息”面板还会向管理员显示这些对象在 CMC 中的位置。

注意：

- 若要查看受影响对象的列表，必须具有这些对象的“查看”权限。
- 访问级别的关系查询结果只会输出对其显式分配了访问级别的对象。如果对象由于继承设置的原因而使用访问级别，则该对象不会出现在查询结果中。

7.3.8 跨站点管理访问级别

访问级别是可以从源站点复制到目标站点的对象之一。如果访问级别出现在复制对象的访问控制列表中，则可以选择复制这些访问级别。例如，如果某主体被授予 Crystal 报表的访问级别 A，并且跨站点复制该 Crystal 报表，则也会复制访问级别 A。

注意：

如果目标站点中存在同名的访问级别，则访问级别复制会失败。在复制之前，用户或目标站点管理员必须重命名其中一个访问级别。

跨站点复制访问级别后，请紧记本节中的管理考虑事项。

在源站点中修改复制的访问级别

如果在源站点中修改复制的访问级别，则目标站点中的访问级别将在下次计划运行复制时更新。在双向复制的情况下，如果在目标站点中修改复制的访问级别，则源站点中的访问级别会更改。

注意：

请确保对一个站点中的访问级别所做的更改不会对其他站点中的对象产生负面影响。请与站点管理员商议，并建议他们为复制的访问级别运行关系查询，然后再进行任何更改。

在目标站点中修改复制的访问级别

注意：

这仅适用于单向复制。

在目标站点中对复制的访问级别所做的任何更改不会在源站点中反映出来。例如，目标站点管理员可以在复制的访问级别中授予计划 Crystal 报表的权限，即使此权限在源站点中被拒绝。因此，虽然访问级别的名称和复制对象的名称保持相同，但主体在对象上所具有的有效权限可能会在目标站点之间有所不同。

如果复制的访问级别在源站点和目标站点之间不同，则在下次计划运行复制作业时会检测到有效权限中的不同。可以强行使源站点的访问级别覆盖目标站点的访问级别，或者允许目标站点的访问级别保持不变。但是，如果并未强行使源站点的访问级别覆盖目标站点的访问级别，则任何挂起复制并使用该访问级别的对象将无法进行复制。

要限制用户修改目标站点中的复制访问级别，可以将目标站点用户作为主体添加到访问级别中，并仅将“查看”权限授予这些用户。这意味着目标站点用户可以查看访问级别，但无法修改其权限设置或将其分配给其他用户。

相关主题

- 第 707 页上的[“联盟”](#)
- 第 131 页上的[“跟踪访问级别和对象之间的关系”](#)

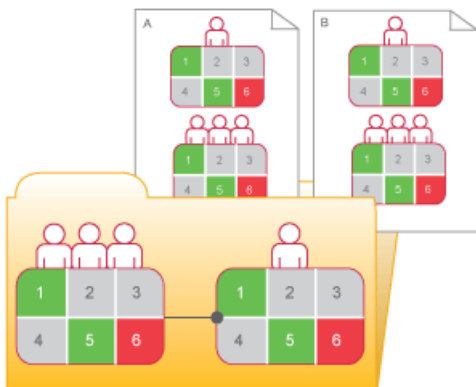
7.4 终止继承

利用继承可以在无需为每个对象设置权限的情况下管理安全设置。但是，在某些情况下，可能不希望继承权限。例如，可能想为每个对象自定义权限。可以在对象的访问控制列表中禁止某个主体的继承行为。在这样做时，可以选择是禁止组继承还是禁止文件夹继承，抑或两者都禁止。

注意：

当终止继承后，将终止继承所有权限；因此不可能对某些权限禁用继承而同时却对其他权限启用继承。

在终止继承图中，组和文件夹继承最初都有效。红组将权限 1 和 5 作为“已授予”类型的权限来继承，将权限 2、3 和 4 作为“未指定”类型的权限来继承，将权限 6 作为“显式拒绝”类型的权限来继承。在文件夹级别为组设置的这些权限表示红色用户以及组的每个其他成员对文件夹对象 A 和 B 具有这些权限。在文件夹级别终止继承后，红色用户对该文件夹中对象的权限集将被清除，直到管理员为他指定新的权限为止。



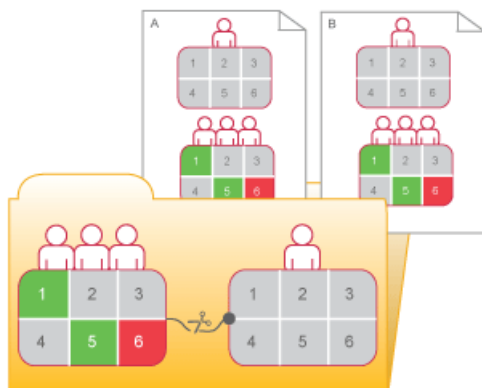


图 7-9：终止继承

7.4.1 禁用继承

此过程允许用户为对象的访问控制列表上的主体禁用组和/或文件夹继承。

- 1 选择要为其禁用继承的对象。
- 2 单击“管理” > “用户安全性”。
将出现“用户安全性”对话框。
- 3 选择要为其禁用继承的主体，然后单击“指定安全性”。
将出现“指定安全性”对话框。
- 4 配置继承设置。
 - 如果要禁用组继承（主体通过组成员资格继承的权限），请清除“从父组继承”复选框。
 - 如果要禁用文件夹继承（对象从文件夹继承的权限设置），请清除“从父文件夹继承”复选框。
- 5 单击“确定”。

7.5 使用权限来委派管理

除了控制对各个对象和设置的访问外，使用权限还可以在组织中的职能组之间分配管理任务。例如，您可能希望不同部门的员工管理各自的用户和组。或者，可能有一位负责 BI 平台高级管理的管理员，但希望所有服务器管理都交由 IT 部门的员工负责。

假设组结构和文件夹结构与委派管理安全结构相吻合，则应该向委派的管理员授予对整个用户组的权限，但是向委派的管理员授予的权限应比对其所控制的用户的完整权限少。例如，可能不希望委派的管理员编辑用户属性或将用户属性重新分配给不同的组。

注意：

对象迁移最好由管理员组的成员执行，尤其是管理员用户帐户。要迁移一个对象，可能同时需要迁移很多相关对象。委派管理员帐户可能无法为所有对象获取需要的安全权限。

“委派的管理员的权限”表概述了委派的管理员执行常用操作所需的权限。

表7-3：委派的管理员的权限

委派的管理员的操作	委派的管理员所需的权限
创建新用户	对顶层用户文件夹的“添加”权限
创建新组	对顶层用户组文件夹的“添加”权限
删除任何受控制的组以及这些组中的单独用户	对相关组的“删除”权限
只删除委派的管理员创建的用户	对顶层用户文件夹的“所有者删除”权限
只删除委派的管理员创建的用户和组	对顶层用户组文件夹的“所有者删除”“权限
只管理委派的管理员创建的用户（包括将这些用户添加到那些组中）	对顶层用户文件夹的“所有者编辑”和“所有者安全地修改权限”权限
只管理委派的管理员创建的组（包括将用户添加到那些组中）	对顶层用户组文件夹的“所有者编辑”和“所有者安全地修改权限”权限
为其控制的组中的用户修改密码	对相关组的“编辑密码”权限
只为委派的管理员创建的主体修改密码	对顶层用户文件夹或相关组的“所有者编辑密码”权限 注意： 只有在将用户添加到相关组中时，对组设置“所有者编辑密码”权限才会对该用户生效。
修改用户名、说明和其他属性，并将用户重新分配到不同的组	对相关组的“编辑”权限

委派的管理员的操作	委派的管理员所需的权限
修改用户名、说明和其他属性，并将用户重新分配到不同的组（但是只针对委派的管理员创建的用户）	<p>对顶层用户文件夹或相关组的“所有者编辑”权限</p> <p>注意： 只有在将用户添加到相关组中时，对相关组设置“所有者编辑”权限才会对该用户生效。</p>

7.5.1 在修改用户拥有的对象权限选项之间进行选择

设置委派的管理时，请向委派的管理员授予对其将控制的主体的权限。可能希望向其授予所有权限（“完全控制”）；但是，可取的做法是使用高级权限设置取消“修改权限”权限，并改为向委派的管理员授予“安全地修改权限”权限。也可以向管理员授予安全地修改权限继承设置权限，而不是修改权限继承设置权限。下面概述了这些权限之间的区别。

修改用户拥有的对象权限

此权限允许用户修改任何用户对该对象的任何权限。例如，如果用户 A 对某对象具有“查看对象”和“修改用户拥有的对象权限”的权限，则用户 A 可更改对该对象的权限，以便他或任何其他用户具有该对象的完全控制权。

安全地修改用户拥有的对象权限

此权限允许用户只授予或拒绝他自己已被授予的那些权限，或将这些权限恢复为未指定状态。例如，如果用户 A 具有“查看”和“安全地修改用户拥有的对象权限”权限，则用户 A 不可以为自己授予更多的权限，并且只可以对其他用户授予或拒绝这两种权限（“查看”和“安全地修改权限”）。此外，用户 A 只能针对那些其具有“安全地修改权限”权限的对象，更改用户对这些对象的权限。

用户 A 若要修改用户 B 对对象 O 的权限，则必须满足以下所有条件：

- 用户 A 具有对象 O 的安全地修改权限权限。
- 用户 A 为用户 B 更改的每个权限或访问级别都已授予用户 A。
- 用户 A 具有用户 B 的安全地修改权限权限。
- 如果分配访问级别，则用户 A 对为用户 B 更改的访问级别具有“分配访问级别”权限。

权限作用域可以进一步限制委派的管理员所能分配的有效权限。例如，委派的管理员可能具有某文件夹的安全地修改权限和编辑权限，但这些权限的作用域被限制为此文件夹，并且不应用于其子对象。实际上，委派的管理员只能授予对文件夹（而不是对其子对象）的“编辑”权限（该权限只具有适用于对象作用域）。另一方面，如果向委派的管理员授予对文件夹的“编辑”权限（只具有适用于子对象作

用域），则她可以向其他主体授予对文件夹子对象的“编辑”权限（具有两种作用域），但是对于文件夹本身，她只能授予具有适用于子对象作用域的“编辑”权限。

此外，对于对其他主体没有“安全地修改权限”权限的委派管理员，将限制其修改其他主体对这些组的权限。这非常有用，例如，如果有两个委派的管理员负责向不同的用户组授予对同一文件夹的权限，但是不希望一个委派的管理员能够拒绝另一个委派的管理员所控制的组访问文件夹。“安全地修改权限”权限可确保做到这一点，因为通常委派的管理员彼此不具有对对方的“安全地修改权限”权限。

安全地修改权限继承设置

此权限允许委派的管理员在其有权访问的对象上修改其他主体的继承设置。要成功地修改其他主体的继承设置，委派的管理员必须对对象和主体的用户帐户拥有此权限。

7.5.2 所有者权限

所有者权限只适用于正在检查对象权限的对象所有者。在 BI 平台中，对象的所有者是创建了对象的主体；如果从系统中永久删除该主体，则所有权将归还给管理员。

所有者权限用于管理基于所有者的安全性。例如，可能想要创建文件夹或文件夹层次结构，不同的用户可在其中创建和查看文档，但是只可以修改或删除他们自己的文档。此外，所有者权限可用于允许用户处理他们创建的报表实例，而不是处理其他人的实例。就计划访问级别而言，它只允许用户编辑、删除、暂停和重新计划他们自己的实例。

所有者权限的工作方式类似于其对应的常规权限。但是，只有在向主体授予了所有者权限，但拒绝了或未指定常规权限的情况下，所有者权限才有效。

7.6 权限管理的建议摘要

要进行权限管理，请谨记以下几点：

- 只要有可能，请使用访问级别。通过将与普通用户需求相关的权限组合在一起，这些预定义的权限集简化了管理。
- 设置对顶层文件夹的权限和访问级别。如果启用继承，可以通过系统向下传递这些权限，且人工介入的管理性操作最少。
- 尽可能避免中断继承。这样，可以减少保护已添加到 BI 平台的内容所占用的时间量。

- 先在文件夹级别为用户和组设置适当的权限，然后将对象发布到该文件夹。默认情况下，如果用户或组具有某个文件夹的权限，则对于您后来发布到该文件夹的任何对象，用户或组将会继承相同的权限。
- 将用户组织为用户组，为整个组分配访问级别和权限，并在必要时向特定成员分配访问级别和权限。
- 为系统中的每个管理员创建单独的 Administrator 帐户，并将这些帐户添加到 Administrators 组，以改善系统更改的可说明性。
- 默认情况下，对于 BI 平台中的顶层文件夹，为 Everyone 组授予的权限非常有限。安装之后，建议对 Everyone 组成员的权限进行检查，并相应指定安全性。

第 8 章 保护 BI 平台安全

8.1 安全概述

本节详细说明 BI 平台解决企业安全性问题的方式，并为管理员和系统设计者提供典型安全相关疑问的回答。

BI 平台体系结构解决了影响当今企业和组织的许多安全问题。当前版本支持分布式安全、单一登录、资源访问安全、粒度对象权限以及第三方身份验证等功能，以便防止未经授权的访问。

由于 BI 平台为 SAP Business Objects 产品的 Enterprise 系列中不断增加的组件提供了框架，所以本节将详细介绍安全特性和相关功能，以说明框架本身如何实施和维护安全。因此，本节并未提供明确的程序性详细信息；相反，它侧重于概念性信息并提供了指向主要过程的链接。

在简要介绍系统的安全概念后，将提供以下主题的详细信息：

- 如何通过加密和数据处理安全模式保护数据。
- 如何为 BI 平台部署设置安全套接字层。
- 为 BI 平台设置和维护防火墙的指导原则。
- 配置反向代理服务器。

8.2 灾难恢复计划

必须采取某些措施保护组织对 BI 平台的投资，以确保在出现灾难的情况下最大限度地维持业务的正常运行。本节提供为组织起草灾难恢复计划的指导原则。

一般指导原则

定期执行系统备份，必要时外部发送备份媒体的副本。

- 安全存储所有软件媒体。
- 安全存储所有许可文档。

具体指导原则

就灾难恢复计划而言，有三种系统资源需要特别注意：

- 文件资源库服务器中的内容：这包括诸如报表之类的专有内容。应定期备份此内容，因为只有这样，在出现灾难的情况下才能重新生成此内容。
- CMS 使用的系统数据库：此资源包含部署的所有关键元数据，如用户信息、报表和其他特定于组织的敏感信息。
- 数据库信息密钥文件（.dbinfo file）：此资源包含系统数据库的主密钥。如果此密钥因某种原因不可用，则无法访问系统数据库。强烈建议在部署 BI 平台之后，将此资源的密码存储在一个安全的已知位置。如果没有密码，将无法重新生成该文件，进而失去访问系统数据库的权限。

8.3 保护部署安全的一般建议

下面是保护 BI 平台部署安全的建议指导原则。

- 使用防火墙保护 CMS 和其他系统组件之间的通信。如果可能，应始终将 CMS 隐藏在防火墙的后面。至少要确保系统数据库在防火墙后面是安全的。
- 向文件资源库服务器添加其他加密。启动和运行系统之后，专有内容将存储在这些服务器上。通过 OS 或使用第三方工具添加其他加密。

注意：

BI 平台不支持 SFTP。如果需要 SFTP 功能，请参阅 SAP 注释 1556571 或考虑使用 SAP 合作伙伴解决方案。

- 在 Web 应用程序服务器的前面部署反向代理服务器，以便将它们隐藏在单个 IP 地址的后面。此配置路由通过反向代理服务器发送到专用 Web 应用程序服务器的所有 Internet 通信，从而隐藏专用 IP 地址。
- 严格执行公司密码政策。确保定期更改用户密码。
- 如果选择安装随 BI 平台提供的系统数据库和 Web 应用程序服务器，则应访问相关文档，确保在部署这些组件时进行充足的安全配置。
- 对部署中客户端和服务器之间的所有网络通信均采用安全套接字层（SSL）协议。
- 确保平台安装目录和子目录是安全的 — 在系统操作过程中，这些目录中可能会存储敏感的临时数据。
- 应将访问中央管理控制台（CMC）仅限为本地访问。有关 CMC 部署选项的信息，请参阅《SAP BusinessObjectes Business Intelligence 平台 Web 应用程序部署指南》。

相关主题

- 第 162 页上的[“配置 SSL 协议”](#)
- 第 145 页上的[“密码限制”](#)
- 第 141 页上的[“配置捆绑的第三方服务器的安全”](#)

8.4 配置捆绑的第三方服务器的安全

如果选择安装与 BI 平台捆绑在一起的第三方服务器组件，则建议访问和查看有关以下捆绑组件的文档：

- Sybase SQL Anywhere: 有关保护此系统数据库安全的详细信息，请参阅 <http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.help.sqlanywhere.12.0.0/dbadmin/da-part-securing.html>。
- Apache Tomcat: 有关此 Web 应用程序服务器安全的详细信息，请参阅 <http://tomcat.apache.org/>。

8.5 活动信任关系

在联网环境中，两个域之间的信任关系通常是指一种连接，该连接允许一个域识别已经过另一个域身份验证的用户。在保证安全的同时，信任关系允许用户访问多个域中的资源，而不必重复地提供凭据。

在 BI 平台环境中，活动信任关系的工作方式类似于向每个用户提供对系统中的资源的无缝访问。对用户进行身份验证并授予活动会话权限之后，所有其他 BI 平台组件将都能处理用户的请求和操作，而不会提示输入凭据。这样，活动信任关系就为 BI 平台的分布式安全提供了基础。

8.5.1 登录标记

登录标记是一个经过编码的字符串，它定义了自己的用法属性并包含了用户的会话信息。登录标记的用法属性在生成登录标记时指定。这些属性允许对登录标记设置限制，以减少恶意用户利用登录标记的机会。当前的登录标记用法属性如下：

- 分钟数

此属性限制登录标记的有效期限。

- 登录次数

此属性限制登录标记可用于登录到 BI 平台的次数。

这两种属性都能够防止恶意用户使用从合法用户处找到的登录标记，未经授权访问 BI 平台。

注意：

如果浏览器和应用程序或 Web 服务器之间的网络不安全（例如，连接是通过公共网络进行的并且未使用 SSL 或受信任的身份验证），那么将登录标记存储在 Cookie 中可能会存在安全风险。使用安全套接字层（SSL）来降低浏览器和应用程序或 Web 服务器之间的安全风险是一种好的做法。

如果已禁用了登录 Cookie，并且 Web 服务器或 Web 浏览器超时，则会向用户呈现登录屏幕。如果启用了 Cookie，并且服务器或浏览器超时，则会使用户无缝地登录回系统。但是，由于状态信息与 Web 会话关联，因此用户的状态会丢失。例如，如果用户已展开导航树并选择了特定项，则会重新设置该导航树。

对于 BI 平台，默认在 Web 客户端中启用登录标记，但可以对 BI 启动板禁用登录标记。如果在客户端禁用登录标记，则用户会话将受到 Web 服务器或 Web 浏览器超时的限制。当该会话过期时，用户将需要重新登录到 BI 平台。

8.5.2 分布式安全的票证机制

Enterprise 系统专门为通常需要某些形式的分布式安全的大量用户提供服务。企业系统可能需要分布式安全来支持诸如信任让渡（能够允许另一个组件代表用户进行操作）等功能。

BI 平台通过实现票证机制（一种类似于 Kerberos 票证机制的机制）处理分布式安全。CMS 将授予权证以准许组件代表特定用户执行操作。在 BI 平台中，该票证被称为登录标记。

此登录标记在 Web 上最常用。当用户第一次由 BI 平台验证身份时，他们会从 CMS 收到登录标记。用户的 Web 浏览器将高速缓存此登录标记。当用户发出一个新请求时，其他 BI 平台组件可以从用户的 Web 浏览器中读取登录标记。

8.6 会话和会话跟踪

通常，会话是一种能够在两台计算机之间交换信息的客户端-服务器连接。会话的状态是一组描述会话的属性、配置或内容的数据。当您在 Web 上建立客户端-服务器连接时，HTTP 的特性将每个会话的持续时间限制为一页信息；因此，Web 浏览器只会在内存中将每个会话的状态保存任何一个 Web 页面的显示时间那么久。当您从一个 Web 页面移到另一个页面时，第一个会话的状态将立即被废弃并被替换为下一个会话的状态。因此，如果 Web 站点和 Web 应用程序需要在另一个会话中重复使用某个会话的信息，则必须以某种方式存储该会话的状态。

BI 平台使用两种常用方法存储会话状态：

- **Cookie** — Cookie 是一个在客户端上存储会话状态的小文本文件：用户的 Web 浏览器将高速缓存 Cookie 以供以后使用。BI 平台登录标记就是此方法的一个示例。
- **会话变量** — 会话变量是在服务器端上存储会话状态的一部分内存。当 BI 平台授予用户活动的系统身份时，诸如用户的身份验证类型等信息将存储在会话变量中。只要保留了会话，系统既不必再次提示用户输入信息，也不必重复进行完成下一个请求所必需的任何任务。

对于 Java 部署，会话用于处理 .jsp 请求；对于 .NET 部署，会话用于处理 .aspx 请求。

注意：

当用户在系统上处于活动状态时，系统最好应保留会话变量。并且，为了确保安全和最小程度地使用资源，当用户在系统上完成工作时，系统应立即删除会话变量。但是，由于 Web 浏览器和 Web 服务器之间的交互可能没有状态，因此，可能很难知道用户何时离开系统（如果他们未明确注销）。为解决此问题，BI 平台实现了会话跟踪。

8.6.1 CMS 会话跟踪

CMS 实现一种简单的跟踪算法。用户在登录时将被授予一个 CMS 会话，CMS 将保留该会话，直至用户注销或 Web 应用程序服务器会话变量释放。

Web 应用程序服务器会话可以反复通知 CMS 自己仍处于活动状态，因此，只要 Web 应用程序服务器会话存在，就会保留 CMS 会话。如果 Web 应用程序服务器会话在 10 分钟内未能与 CMS 通信，则 CMS 将删除 CMS 会话。这样可处理客户端组件不定期关闭的情况。

8.7 环境保护

环境保护是指客户端和服务端组件通信的整体环境的安全。尽管 Internet 和基于 Web 的系统由于其灵活性和丰富的功能正在日益流行，但它们运行的环境可能难于保证安全。部署 BI 平台时，环境保护将分为两个通信区域：Web 浏览器到 Web 服务器，Web 服务器到 BI 平台。

8.7.1 Web 浏览器到 Web 服务器

在 Web 浏览器和 Web 服务器之间传输数据时，通常需要某种程度的安全。相关安全措施通常涉及到两个常规任务：

- 确保数据通信安全。
- 确保只有有效的用户才能从 Web 服务器中检索信息。

注意：

这些任务通常由 Web 服务器通过各种安全机制处理，包括安全套接字层（SSL）协议和其他此类机制。使用安全套接字层（SSL）来降低浏览器和应用程序或 Web 服务器之间的安全风险是一种好的做法。

您必须独立于 BI 平台保护 Web 浏览器和 Web 服务器之间的通信安全。有关保护客户端连接安全的详细信息，请参考 Web 服务器文档。

8.7.2 Web 服务器到 BI 平台

防火墙通常用于保护 Web 服务器和公司 Intranet 剩余部分（包括 BI 平台）之间的通信区域。该平台支持使用 IP 过滤或静态网络地址转换（NAT）的防火墙。支持的环境可以包含多个防火墙、Web 服务器或应用程序服务器。

8.8 审核安全性配置修改

BI 平台不会对以下各部分默认安全性配置的任何更改进行审核。

- Web 应用程序（BOE、Web 服务）的属性文件
- TrustedPrincipal.conf
- BI 启动板和 OpenDocument 上进行的自定义

总之，将不会审核在 CMC 外进行的任何安全性配置修改。这同时也应用于通过中央配置管理器（CCM）进行的修改。可以审核通过 CMC 提交的更改。

8.9 审核 Web 活动

BI 平台可提供系统的深层信息，即记录 Web 活动并允许您检查和监控详细信息。Web 应用程序服务器允许选择想要记录的 Web 属性，如时间、日期、IP 地址、端口号等。审核数据将被记录到磁盘并存储在逗号分隔的文本文件中，以便能够轻松地根据数据创建报表或将其导入其他应用程序。

8.9.1 防止恶意登录企图

不管系统有多安全，通常至少有一个容易受到攻击的位置：即用户连接到系统的位置。完全保护此位置几乎是不可能的，因为仅仅是猜测有效用户名和密码的过程就可以行之有效地尝试“破解”系统。

BI 平台实现了多种技术来降低恶意用户获得系统访问权限的可能性。下面列出的各种限制仅适用于 Enterprise 帐户 — 也就是说，这些限制不适用于已映射到外部用户数据库（LDAP 或 Windows AD）的帐户。但是，通常情况下，您可以使用外部系统为外部帐户进行类似的限制。

8.9.2 密码限制

密码限制确保进行默认 Enterprise 身份验证的用户创建相对复杂的密码。可以启用以下选项：

- 强制大小写混合的密码

此选项确保密码至少包含以下两类字符：大写字母、小写字母、数字或标点符号。

- 必须包含至少 N 个字符

通过强制要求密码的最低复杂程度，您可以降低恶意用户简单猜测有效用户密码的机率。

8.9.3 登录限制

登录限制主要用于防止字典攻击（恶意用户用于获取有效用户名，并企图通过尝试字典中的每个单词获悉对应密码的一种方法）。借助于现代化硬件的速度，恶意程序每分钟可以猜测上百万个密码。为了防止字典攻击，BI 平台的内部机制会在每次登录尝试之间强制要求延时（0.5 到 1.0 秒）。此外，该平台还提供了多种可自定义的选项，可利用它们降低字典攻击风险：

- 在 N 次尝试登录失败后禁用帐户
- 在 N 分钟后重置失败的登录次数
- 在 N 分钟后重新启用帐户

8.9.4 用户限制

用户限制确保进行默认 Enterprise 身份验证的用户定期创建新密码。可以启用以下选项：

- 必须每隔 N 天更改密码
- 不能重新使用 N 个最近的密码
- 必须等待 N 分钟才能更改密码

这些选项在多个方面十分有用。首先，任何尝试字典攻击的恶意用户将不得不在每次密码更改时重新开始。并且，由于密码更改基于每个用户的第一次登录时间，因此，恶意用户无法轻易地确定任何特定密码将在何时更改。此外，即使恶意用户已经猜到或以其他方式获得了另一个用户的凭据，它们也只是在有限的一段时间内有效。

8.9.5 Guest 帐户限制

BI 平台支持 Guest 帐户的匿名单一登录。因此，当用户在未指定用户名和密码的情况下连接到 BI 平台时，系统将使用 Guest 帐户使其自动登录。如果为 Guest 帐户指派了安全密码或完全禁用了 Guest 帐户，则会禁用此默认行为。

8.10 处理扩展

在 BI 平台中，通过使用自定义的处理扩展，可以进一步保证报表创建环境的安全。处理扩展是一种动态加载的代码库，在系统处理特定 BI 平台“查看”或“计划”请求之前，处理扩展会将业务逻辑应用于这些请求。

通过支持处理扩展，BI 平台管理 SDK 实质提供了一种允许开发人员拦截请求的“句柄”。然后，开发人员就能够在处理报表之前将选择公式附加到请求。

实施行级安全的报表处理扩展是一个典型的示例。这种类型的安全限制按一个或多个数据库表中的行进行数据访问。开发人员可编写一个动态加载的库，该库将拦截报表的“查看”或“计划”请求（在作业服务器、处理服务器或报表应用程序服务器处理这些请求之前）。开发人员的代码首先将确定拥有处理作业的用户；然后在第三方系统中查找用户的数据访问权限。接着，代码将生成记录选择公式并将它们附加到报表，以便限制从数据库返回的数据。在这种情况下，处理扩展提供了一种将自定义行级安全结合到 BI 平台环境中的方法。

通过启用处理扩展，您可以配置相应的 BI 平台服务器组件，以便在运行时动态加载处理扩展。SDK 中包括了一个具有详细文档描述的 API，开发人员可能使用该 API 来编写处理扩展。有关更多信息，请参阅产品分发介质上提供的开发人员文档。

8.11 BI 平台数据安全概述

BI 平台系统的管理员通过以下方式管理敏感数据的保护方式：

- 一个群集级别的安全设置，用于确定哪些应用程序和客户端可以访问 CMS。此设置通过中央配置管理器管理。
- 一种双密钥加密系统，用于控制对 CMS 资源库的访问，以及对用于加密/解密资源库中对象的密钥的访问。对 CMS 资源库的访问通过中央管理服务器设置，而中央管理控制台具有用于加密密钥的专用管理区域。

管理员可使用这些功能将 BI 平台部署设置为特定数据安全合规级别，以及管理用于加密和解密 CMS 资源库中的数据的加密密钥。

8.11.1 数据处理安全模式

BI 平台可以在两种可能的数据处理安全模式下运行：

- 默认数据处理安全模式。在某些情况中，在此模式中运行的系统将使用硬编码的加密密钥，且不遵循特定标准。默认模式支持向后兼容 BI 平台客户端工具和应用程序的早期版本。
- 旨在满足联邦信息处理标准（FIPS），特别是 FIPS 140-2 规定的准则的一种数据安全模式。在此模式中，使用 FIPS 兼容算法和加密模块保护敏感数据。当平台以 FIPS 兼容模式运行时，将自动禁用所有不满足 FIPS 准则的客户端工具和应用程序。平台客户端工具和应用程序设计为符合 FIPS 140-2 标准。当 BI 平台在 FIPS 兼容模式下运行时，更早版本的客户端和应用程序将不工作。

数据处理模式对系统用户是透明的。在这两种数据处理安全模式中，均通过内部加密引擎在后台加密和解密敏感数据。

建议用户在以下情况中使用 FIPS 兼容模式：

- BI 平台部署无需使用任何旧的 BI 平台客户端工具或应用程序，或与之交互。
- 贵组织的数据处理标准和准则禁止使用硬编码加密密钥。
- 贵组织需要根据 FIPS 140-2 规定保护敏感数据。

在 Windows 和 Unix 平台上，数据处理安全模式均通过中央配置管理器设置。群集环境中的所有节点必须均设置为相同模式。

8.11.1.1 在 Windows 上打开 FIPS 兼容模式

默认情况下，安装 BI 平台时 FIPS 兼容模式处于关闭状态。但是，仍可在部署中打开所有节点的 FIPS 兼容模式。

- 1 要启动 CCM，请单击“程序” > “SAP Business Intelligence” > “SAP BusinessObjects BI 平台 4” > “中央配置管理器”。
- 2 在 CCM 中，右击服务器智能代理（SIA）并选择“停止”。

警告：

在 SIA 状态为“已停止”之前，请勿继续到步骤 3。

- 3 右击 SIA 并选择“属性”。
将出现“属性”对话框，其中将显示“属性”选项卡。
- 4 将 -fips 添加到“命令”字段，并单击“应用”。
- 5 单击“确定”以关闭“属性”对话框。
- 6 重新启动 SIA。

SIA 现在以 FIPS 兼容模式运行。

必须在 BI 平台部署中的所有 SIA 上打开 FIPS 兼容设置。

8.11.1.2 在 Unix 上打开 FIPS 兼容模式

在尝试执行以下过程前，必须停止 BI 平台部署中的所有节点。

默认情况下，在安装 BI 平台之后 FIPS 兼容模式会处于关闭状态。使用下面的说明可为部署中的所有节点打开 FIPS 兼容设置。

- 1 从安装目录/sap_bobj 目录中，打开 ccm.config 文件进行编辑。
- 2 将 -fips 添加到节点启动命令参数。

节点启动命令参数按此格式显示：节点名LAUNCH。例如，对于名为“SAP”的节点，节点启动命令参数为 SAPLAUNCH。

- 3 保存更改并键入“Exit”以退出。
- 4 重新启动节点。

节点现在以 FIPS 兼容模式运行。

必须在 BI 平台部署中的所有节点上打开 FIPS 兼容设置。

8.11.1.3 在 Windows 上关闭 FIPS 兼容模式

在尝试执行以下过程前，必须停止 BI 平台部署中的所有服务器。

如果用户的部署以 FIPS 兼容模式运行，请使用以下说明关闭该设置。

- 1 在 CCM 中，右击服务器智能代理（SIA）并选择“停止”。

警告：

在节点状态标记为“已停止”之前，请勿继续到步骤 2。

- 2 右击 SIA 并选择“属性”。
将出现“属性”对话框，并显示“属性”选项卡。
- 3 从“命令”字段中删除 -fips，并单击“应用”。
- 4 单击“确定”以关闭“属性”对话框。
- 5 重新启动 SIA。

8.12 BI 平台加密

敏感数据

BI 平台加密旨在保护存储在 CMS 资源库中的敏感数据。敏感数据包括用户凭据、数据源连接数据以及存储有密码的任何其他 Info 对象。加密这些数据可保护隐私、确保其不受损坏，并可维护访问控制。所有必需的加密资源（包括加密引擎以及 RSA 库）均默认安装在每个 BI 平台部署中。

BI 平台系统使用双密钥加密系统。

加密密钥

通过与内部加密引擎进行交互，对敏感数据的加密和解密借助 SDK 在后台处理。系统管理员通过对称的加密密钥管理数据安全，而非直接加密或解密特定的数据块。

在 BI 平台中，对称的加密密钥也称为“加密密钥”，用于加密/解密敏感数据。中央管理控制台具有专用于加密密钥的管理区域。使用“加密密钥”可查看、生成、取消激活、撤销以及删除密钥。系统可确保解密敏感数据所需的任何密钥均无法删除。

群集密钥

群集密钥是对称密钥的包装密钥，用于保护 CMS 资源库中存储的加密密钥。通过使用对称密钥算法，群集密钥可维护对 CMS 资源库的某一级别的访问控制。在安装设置期间，会为 BI 平台中的每个节点分配一个群集密钥。系统管理员可使用 CCM 重置群集密钥。

8.12.1 使用群集密钥

在 BI 平台安装设置过程中，会为服务器智能代理创建一个由八个字符组成的群集密钥。此密钥用于加密 CMS 资源库中的所有加密密钥。如果没有正确的群集密钥，则无法访问 CMS。

群集密钥以加密的格式存储在 dbinfo 文件中。dbinfo 文件名遵守此约定：
boe<sia_name>.dbinfo，其中 <sia_name> 是群集的服务器智能代理的名称。

在 Windows 上，文件存储在以下目录中：<安装目录>\SAP BusinessObjects Enterprise XI 4.0\win64_x64。

在 Unix 系统中，文件存储在 <安装目录>/sap_bobj/enterprise_xi40/ 下的平台目录中：

Unix 平台	平台目录
AIX	<安装目录>/sap_bobj/enterprise_xi40/aix_rs6000_64 /
Solaris	<安装目录>/sap_bobj/enterprise_xi40/solaris_sparcv9/
Linux	<安装目录>/sap_bobj/enterprise_xi40/linux_x64/

注意：

不能从 Dbinfo 文件中获取给定节点的群集密钥。建议系统管理员采用谨慎小心的措施来保护群集密钥。

只有具有管理员权限的用户才能重置群集密钥。在需要时，可使用 CCM 为部署中的每个节点重置该群集密钥。新群集密钥自动用于保护 CMS 资源库中的加密密钥。

8.12.1.1 在 Windows 上重置群集密钥

在重置节点的群集密钥前，请确保服务器智能代理托管的所有服务器均已停止。

- 1 要启动 CCM，请转到“程序” > “SAP Business Intelligence” > “SAP BusinessObjects BI 平台” > “中央配置管理器”。
- 2 在 CCM 中，右击服务器智能代理（SIA）并选择“停止”。

警告：

在 SIA 状态为“已停止”之前，请勿继续到步骤 3。

- 3 右击服务器智能代理（SIA），并选择“属性”。
将出现“属性”对话框。
- 4 单击“配置”选项卡。
- 5 单击“CMS 群集密钥配置”下的“更改”。
将出现一条警告消息。
- 6 单击“是”以继续。
将显示“更改群集密钥”对话框。
- 7 在“新群集密钥”和“确认新群集密钥”字段中输入同一个八字符密钥。

注意：

在 Windows 上，群集密钥必须同时包含大写和小写字符。此外，用户还可以生成随机密钥。需要随机密钥以与 FIPS 兼容。

- 8 单击“确定”，向系统提交新的群集密钥。
将显示一条消息，确认群集密钥已成功重置。
- 9 重新启动 SIA。

在多节点的群集中，必须将 BI 平台部署中所有 SIA 的群集密钥重置为这个新密钥。

8.12.1.2 在 Unix 上重置群集密钥

在重置某个节点的群集密钥前，请确保该节点托管的所有服务器均已停止。

- 1 导航到 <安装目录>/sap_bobj 目录。
- 2 键入 ./cmsdbsetup.sh 并按 Enter 键。
将出现“CMS 数据库设置”屏幕。
- 3 键入节点的名称，并按 Enter 键。
- 4 键入 2，以更改群集密钥。
将出现一条警告消息。
- 5 选择“是”以继续。
- 6 在提供的字段中，键入新的八字符群集密钥，并按 Enter 键。

注意：

在 Unix 平台上，有效的群集密钥包含任何八个字符的组合，没有任何限制。

- 7 在提供的字段中重新输入新群集密钥，并按 Enter 键。
将显示一条消息，提示用户群集密钥已成功重置。
- 8 重新启动节点。

必须将 BI 平台部署中的所有节点重置为使用相同的群集密钥。

8.12.2 加密人员

要在 CMC 中管理加密密钥，必须是“加密人员”组的成员。为 BI 平台创建的默认管理员帐户也是“加密人员”组的成员。使用此帐户可以根据需要将用户添加到“加密人员”组。建议该组的成员资格仅限于有限数量的用户。

注意：

当用户添加到“Administrators”组后，他们不会继承对加密密钥执行管理任务所需的权限。

8.12.2.1 将用户添加到“加密人员”组

用户帐户必须已经存在于 BI 平台中，才能将其添加到“加密人员”组中。

注意：

必须同时是“Administrators”和“加密人员”组中的成员，才能将用户添加到“加密人员”组。

- 1 在 CMC 的“用户和组”管理区域中，选择“加密人员”组。
- 2 单击“操作” > “将成员添加到组”。
将出现“添加”对话框。
- 3 单击“用户列表”。
“可用用户或组”列表将刷新并显示系统中的所有用户帐户。
- 4 将要添加到“加密人员”组的用户从“可用用户或组”列表中移到“选定用户或组”列表。

提示：

若要搜索特定用户，请使用搜索字段。

- 5 单击“确定”。

作为“加密人员”组的成员，新添加的帐户将有权访问 CMC 中的“加密密钥”管理区域。

8.12.2.2 在 CMC 中查看加密密钥

CMC 应用程序中有一个管理区域专用于管理 BI 平台系统使用的加密密钥。仅“加密人员”组的成员有权访问该区域。

- 1 要启动 CMC，请单击“程序” > “SAP Business Intelligence” > “SAP BusinessObjects BI 平台 4” > “SAP BusinessObjects BI 平台中央管理控制台”。
将显示 CMC 主页。
- 2 单击“加密密钥”选项卡。
将显示“加密密钥”管理区域。
- 3 双击要查看其更多详细信息的加密密钥。

相关主题

- 第 155 页上的[“查看与加密密钥关联的对象”](#)

8.12.3 在 CMC 中管理加密密钥

加密人员可在“加密密钥”管理区域中查看、生成、取消激活、撤销和删除密钥。这些密钥用于保护 CMS 资源库中存储的敏感数据。

“加密密钥”管理区域列出了当前在系统中定义的所有加密密钥。每个密钥的基本信息按下表所述标题分类：

标题	说明
标题	加密密钥的名称标识符
状态	密钥的当前状态
上次状态更改	与加密密钥关联的上次更改的日期和时间戳
对象	与密钥关联的对象数

相关主题

- 第 154 页上的[“加密密钥状态 ”](#)
- 第 156 页上的[“创建新加密密钥”](#)
- 第 157 页上的[“从系统删除加密密钥”](#)
- 第 157 页上的[“撤销加密密钥”](#)
- 第 155 页上的[“查看与加密密钥关联的对象”](#)
- 第 156 页上的[“将加密密钥标记为已泄露 ”](#)

8.12.3.1 加密密钥状态

下表列出了 BI 平台中加密密钥的所有可能状态选项：

状态	说明
活动	该系统中只能将一个加密密钥指定为“活动”。此密钥用于加密将存储到 CMS 数据库中的最新敏感数据。此密钥还用于加密出现在其“对象列表”中的所有对象。创建新加密密钥后，当前“活动”密钥将恢复为“已取消激活”状态。不能从系统中删除活动的密钥。
已取消激活	“已取消激活”密钥不能再用于加密数据。但是，它可以用于解密其“对象列表”中包含的所有对象。一旦取消激活某个密钥，就不能将其重新激活。不能从系统中删除标记为“已取消激活”的密钥。必须先将密钥的状态更改为“已撤销”，然后才能将其删除。
已泄露	如果认为某个加密密钥不安全，可将其标记为“已泄露”。通过标记此类密钥，可以在以后继续重新加密仍然与该密钥关联的数据对象。一旦某个密钥被标记为“已泄露”后，必须先将其撤销，然后才能将其从系统中删除。
已撤销	加密密钥被撤销后，将启动以下过程：当前与该密钥关联的所有对象将使用当前的“活动”加密密钥重新加密。某个密钥被撤销后，将可以从系统中安全删除。撤销机制可确保 CMS 数据库中的数据始终可以被加密。一旦某个密钥被撤销，就不可能将其重新激活。
已取消激活：正在重新加密	表明加密密钥正在撤销。此过程完成后，该密钥将被标记为“已撤销”。
已取消激活：已暂挂重新加密	表明撤销某个加密密钥的过程已暂挂。如果该过程已被故意暂挂，或如果与该密钥关联的数据对象不可用，通常会发生此情形。
已撤销 - 已泄露	如果某个密钥被标记为“已泄露”并且先前与其关联的所有数据已使用其他密钥加密，则该密钥被标记为“已撤销 - 已泄露”。当某个“已取消激活”密钥被标记为“已泄露”时，用户可以选择采取或不采取操作或撤销该密钥。某个“已泄露”密钥被撤销后，将可以被删除。

8.12.3.2 查看与加密密钥关联的对象

- 1 选择 CMC 的“加密密钥”管理区域中的密钥。
- 2 单击“管理” > “属性”。
将显示加密密钥的“属性”对话框。
- 3 单击“属性”对话框左边导航窗格中的“对象列表”。
与加密密钥关联的所有对象的列表将显示在导航窗格的右侧。

提示：

使用搜索功能可查找特定对象。

8.12.3.3 创建新加密密钥

警告：

在创建新加密密钥时，系统会自动取消激活当前“活动”密钥。一旦取消激活某个密钥，即无法恢复为“活动”密钥。

- 1 在 CMC 的“加密密钥”管理区域中，单击“管理” > “新建” > “加密密钥”。
将显示“创建新加密密钥”对话框。

- 2 单击“继续”，以创建新加密密钥。

- 3 输入新加密密钥的名称和说明，然后单击“确定”以保存信息。

在“加密密钥”管理区域中，新密钥显示为唯一的活动密钥。现在，此前的“活动”密钥标记为“已取消激活”。

现在，所有新生成并存储在 CMS 数据库中的敏感数据将使用新的加密密钥进行加密。用户可以选择撤销此前的密钥，并用新的活动密钥对其所有数据对象进行重新加密。

8.12.3.4 将加密密钥标记为已泄露

如果某个加密密钥因特定原因而视为不再安全，可以将加密密钥标记为已泄露。此操作可用于跟踪目的。用户还可以进一步标识哪些数据对象与该密钥关联。用户必须先取消激活加密密钥，然后才能将其标记为已泄露。

注意：

在撤销某个密钥后，也可以将其标记为已泄露。

- 1 转到 CMC 的“加密密钥”管理区域。
- 2 选择要标记为已泄露的加密密钥。
- 3 单击“操作” > “标记为已泄露”。

将显示“标记为已泄露”对话框。

- 4 单击“继续”。

- 5 在“标记为已泄露”对话框中，选择以下选项之一：

- “是”：启动一个进程，对所有与已泄露密钥关联的数据对象进行重新加密。
- “否”：关闭“标记为已泄露”对话框，并且该加密密钥在“加密密钥”管理区域中标记为“已泄露”。

注意：

如果选择“否”，则敏感数据继续与已泄露的密钥关联。系统将使用已泄露的密钥对关联对象解密。

相关主题

- 第 157 页上的[“撤销加密密钥”](#)
- 第 154 页上的[“加密密钥状态”](#)
- 第 155 页上的[“查看与加密密钥关联的对象”](#)

8.12.3.5 撤销加密密钥

已取消激活的加密密钥仍可由与之相关联的数据对象使用。要打破加密对象与已取消激活的密钥之间的关联，必须撤销密钥。

- 1 在“加密密钥”管理区域列出的密钥中，选择要撤销的密钥。
- 2 单击“操作” > “撤销”。
- 3 单击“确定”。

此时，启动一个进程，用当前活动的密钥对该密钥的所有对象进行加密。如果该密钥与许多数据对象关联，在重新加密过程结束之前，该密钥将标记为“已取消激活 — 正在重新加密”。

在撤销某个加密密钥后，所有敏感数据对象都不需要该密钥进行加密，因此可以安全地从系统删除该密钥。

8.12.3.6 从系统删除加密密钥

要从 BI 平台中删除某个加密密钥，首先必须确保系统中的所有数据对象均不需要该密钥。此限制可确保 CMS 资源库中存储的所有敏感数据始终受加密保护。

在成功撤销某个加密密钥后，请按照下列说明从系统删除该密钥。

- 1 转到 CMC 的“加密密钥”管理区域。
- 2 选择想要删除的加密密钥。
- 3 单击“管理” > “删除”。

将出现“删除”对话框。

- 4 单击“删除”，从系统删除该加密密钥。

CMC 的“加密密钥”管理区域将不再显示已删除的密钥。

注意：

从系统删除某个加密密钥后，即无法恢复该密钥。

相关主题

- 第 157 页上的[“撤销加密密钥”](#)
- 第 154 页上的[“加密密钥状态”](#)

8.13 针对 SSL 配置服务器

可以为 BI 平台部署的客户端和服务端之间的所有网络通信使用安全套接字层（SSL）协议。

要为所有服务器通信设置 SSL，您需要执行以下步骤：

- 在启用 SSL 的情况下部署 BI 平台。
- 为部署中的每台计算机创建密钥和证书文件。
- 在中央配置管理器（CCM）和 Web 应用程序服务器中配置这些文件的位置。
- 或者，为证书颁发机构管理的证书配置 SSL。

注意：

如果使用的是诸如 Crystal Reports 之类的胖客户端，那么，倘若要从这些胖客户端连接到 CMS，则还需要为 SSL 配置这些客户端。否则，如果尝试从尚未采用相同方式配置的胖客户端连接到已针对 SSL 进行配置的 CMS，则会收到错误。

8.13.1 创建密钥和证书文件

要为服务器通信设置 SSL 协议，请使用 SSLC 命令行工具为部署中的每台计算机创建一个密钥文件和一个证书文件。

注意：

- 需要为部署中的所有计算机（包括运行诸如 Crystal Reports 之类的胖客户端组件的计算机）创建证书和密钥。对于这些客户端计算机，请使用 sslconfig 命令行工具进行配置。

- 为了获得最大程度的安全性，应对所有私钥加以保护，并且，不能通过不安全的通信信道传送私钥。
- 为早期版本的 BI 平台创建的证书不适用于 SAP BusinessObjects Business Intelligence 平台 4.0。将需要重新创建这些证书。

8.13.1.1 为计算机创建密钥和证书文件

- 1 运行 sslc 命令行工具。

SSLC 工具是随 BI 平台软件一起安装的。（例如，在 Windows 上，它默认安装在 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\win64_x64 中。）

- 2 输入以下命令：

```
sslc req -config sslc.cnf -new -out cacert.req
```

此命令将创建两个文件：一个证书颁发机构（CA）证书请求（cacert.req），以及一个私钥（privkey.pem）。

- 3 要对私钥进行解密，请输入以下命令：

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

此命令将创建经过解密的密钥 cakey.pem。

- 4 要对 CA 证书签名，请输入以下命令：

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

此命令将创建一个自签名证书 cacert.pem，该证书将在 365 天后过期。选择适合于您的安全需求的天数。

- 5 在文本编辑器中打开 sslc.cnf 文件，此文件存储在 SSLC 命令行工具所在的同一个文件夹中。

注意：

对于 Windows，必须使用文本编辑器，因为 Windows 资源管理器无法识别和显示扩展名为 .cnf 的文件。

- 6 根据 sslc.cnf 文件中的设置，执行以下操作：

- a 将 cakey.pem 和 cacert.pem 文件放在由 sslc.cnf 文件的 certificate 和 private_key 选项所指定的目录中。默认情况下，sslc.cnf 文件中的设置为：

```
certificate = $dir/cacert.pem
```

```
private_key = $dir/private/cakey.pem
```

- b 使用 sslc.cnf 文件的 database 设置所指定的名称创建一个文件。

注意：

默认情况下，该文件称为 \$dir/index.txt，且为空文件。

- c 使用 sslc.cnf 文件的 serial 设置所指定的名称创建一个文件。

该文件必须提供一个八进制字符串序列号（采用十六进制格式）。

注意：

为了确保能够创建和签署更多的证书，请选择一个数字位数为偶数的较大的十六进制数字，如 111111111111111111111111111111111111。

d 创建由 sslc.cnf 文件的 new_certs_dir 设置所指定的目录。

7. 要创建证书请求和私钥，请输入以下命令：

```
sslc req -config sslc.cnf -new -out servercert.req
```

生成的证书和密钥文件放在当前工作文件夹中。

8. 要解密 privkey.pem 文件中的密钥，请输入以下命令：

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

9. 要使用 CA 证书对证书签名，请输入以下命令：

```
sslc ca -config sslc.cnf -days 365 -out servercert.pem -in servercert.req
```

此命令将创建 servercert.pem 文件，该文件包含经过签名的证书。

10. 使用以下命令将证书转换为 DER 编码的证书：

```
sslc x509 -in cacert.pem -out cacert.der -outform DER
```

```
sslc x509 -in servercert.pem -out servercert.der -outform DER
```

注意：

每次部署只能生成一次 CA 证书（cacert.der）及其相应的私钥（cakey.pem）。相同部署中的所有计算机共享相同的 CA 证书。所有其他证书都必须通过任何证书颁发机构证书的私钥进行签名。

11. 创建一个文本文件（passphrase.txt），以便存储用于对生成的私钥进行解密的纯文本密码短语。
12. 将以下密钥和证书文件存储在一个可由 BI 平台部署中的计算机访问的安全位置（在相同目录下）：
 - 受信任的证书文件（cacert.der）
 - 生成的服务器证书文件（servercert.der）
 - 服务器密钥文件（server.key）
 - 密码短语文件（passphrase.txt）

此位置将用于为 CCM 和 Web 应用程序服务器配置 SSL。

8.13.2 当证书由证书颁发机构管理时设置 SSL

为服务器通信设置 SSL 时，如果证书由证书颁发机构进行管理，请遵循以下步骤。

1. 使用证书私钥将所需证书导出为 PKCS #12 (.PFX) 格式。
这将用作证书颁发机构的证书。
2. 使用 OpenSSL，运行以下命令：

- a 从 .pfx 文件导出私钥文件：


```
openssl pkcs12 -in filename.pfx -nocerts -out privkey.pem
```
- b 从 .pfx 文件导出证书文件：


```
openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cacert.pem
```
- c 从私钥删除密码短语：


```
openssl rsa -in privkey.pem -out cakey.pem
```
- 3 设置某些必要文件：
 - 将 cakey.pem 复制到 C:\SSL\private\cakey.pem。
 - 将 cacert.pem 复制到 C:\SSL\cacert.pem。
 - 在 C:\SSL 文件夹中创建名为 index.txt 的空文本文件（数据库索引文件）。
 - 创建另一个文本文件：C:\SSL\serial。
 - 在文本编辑器中打开 C:\SSL\serial 文件，键入以下值并保存文件：11111111111111111111
- 4 在文本编辑器中，打开文件 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86\ssl.cnf。

选择以下任一选项：

 - 将 policy 变量的值更改为 policy_anything。此更改可支持用户创建与证书颁发机构的证书具有不同策略的服务器证书。
 - 或者，将 policy 变量的值保持 policy_match 不变。这可强制确保服务器证书的策略与证书颁发机构具有相同的证书策略。在此情况下，可能需要相应地更改 req_distinguished_name 属性。
- 5 创建证书请求和私钥。

在命令行提示符中，运行以下命令：

```
ssl.cnf req -config ssl.cnf -new -out servercert.req
```

注意：

 - 对于 PEM 密码短语，键入任何密码（至少使用四个字符）。
 - 对于公用名称，键入运行 BI 平台服务器的计算机的全限定域名。
 - 文件 servercert.req 在 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86 中创建。
 - 已修改文件 .rnd 和 privkey.pem。
- 6 解密私钥。


```
ssl.cnf rsa -in privkey.pem -out server.key
```
- 7 为证书签名。


```
ssl.cnf ca -config ssl.cnf -days 365 -out servercert.pem -in servercert.req
```

注意：

 - 文件 servercert.pem 在 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86 中创建。
 - 文件 11111111111111111111111111111111.pem 在 C:\SSL\newcerts 中创建。
 - 已创建文件 serial 的备份，名为 serial.old。

- serial 的值从 111111111111111111 增加到 111111111111111112。

8 将证书转换为 DER 编码。

运行以下命令：

```
sslc x509 -in cacert.pem -out cacert.der -outform DER
sslc x509 -in servercert.pem -out servercert.der -outform DER
```

注意：

- 文件 servercert.der 在 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86 中创建。
 - 文件 cacert.der 在 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86 中创建。
- 9 创建名为 passphrase.txt 的文本文件。
该文件的内容应为之前使用的 PEM 密码短语。
10. 将以下文件存储到安全的位置，例如，C:\SSLCerts。
- 受信任的证书文件 cacert.der
 - 生成的服务器证书文件 servercert.der
 - 服务器密钥文件 server.key
 - 密码短语文件 passphrase.txt

8.13.3 配置 SSL 协议

为部署中的每台计算机创建了密钥和证书并将它们存储在安全的位置后，您需要向中央配置管理器 (CCM) 和 Web 应用程序服务器提供该安全位置。

还需要执行特定的步骤，才能为 Web 应用程序服务器和任何运行胖客户端应用程序的计算机配置 SSL 协议。

8.13.3.1 在 CCM 中配置 SSL 协议

- 1 在 CCM 中，右击服务器智能代理并选择“属性”。
- 2 在“属性”对话框中，单击“协议”选项卡。
- 3 确保选择了“启用 SSL”。

- 4 提供其中存储了密钥和证书文件的目录的文件路径。

字段	说明
SSL 证书文件夹	存储所有所需的 SSL 证书和文件的文件夹。例如：d:\ssl
服务器 SSL 证书文件	用于存储服务器 SSL 证书的文件名称。默认情况下为 servercert.der
SSL 信任证书文件	包含 SSL 信任证书的文件名称。默认情况下为 cacert.der
SSL 私钥文件	用于访问证书的 SSL 私钥文件的名称。默认情况下为 server.key
SSL 私钥密码短语文件	包含用于访问私钥的密码短语的文本文件名称。默认情况下为 passphrase.txt

注意：

确保为运行该服务器的计算机提供该目录。

8.13.3.2 在 Unix 上配置 SSL 协议

必须使用 serverconfig.sh 脚本为 SIA 配置 SSL 协议。此脚本提供一个基于文本的程序，可让您查看服务器信息以及在所安装的程序中添加和删除服务器。serverconfig.sh 脚本安装在安装程序的 sap_bobj 目录中。

- 1 使用 ccm.sh 脚本停止 SIA 和所有 SAP BusinessObjects 服务器。
 - 2 运行 serverconfig.sh 脚本。
 - 3 选择“3 - 移动节点”，并按 Enter 键。
 - 4 指定目标 SIA 并按 Enter 键。
 - 5 选择“1 - 修改服务器智能代理 SSL 配置”。
 - 6 选择“ssl”。
- 出现提示时，指定 SSL 证书位置。
- 7 如果 BI 平台部署是一个 SIA 群集，则针对每个 SIA 重复步骤 1-6。
 - 8 使用 ccm.sh 脚本启动 SIA，并等待服务器启动。

8.13.3.3 为 Web 应用程序服务器配置 SSL 协议

- 1 如果有 J2EE Web 应用程序服务器，请在设置了以下系统属性的情况下运行 Java SDK。例如：

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=d:\ssl -DtrustedCert=cacert.der -DsslCert=clientcert.der -DsslKey=client.key  
-Dpassphrase=passphrase.txt
```

下表显示了与这些示例相对应的说明：

示例	说明
DcertDir=d:\ssl	用于存储所有证书和密钥的目录。
DtrustedCert=cacert.der	受信任的证书文件。如果指定多个文件，请用分号加以分隔。
DsslCert=clientcert.der	SDK 使用的证书。
DsslKey=client.key	SDK 证书的私钥。
Dpassphrase=passphrase.txt	存储私钥的密码短语的文件。

- 2 如果有 IIS Web 应用程序服务器，请从命令行中运行 sslconfig 工具，并遵循配置步骤。

8.13.3.4 配置胖客户端

在执行以下步骤之前，需要在大家都知道的目录中创建并保存所有要求的 SSL 资源（例如，证书和私钥）。

下面的过程将假设您已遵照相关说明创建了以下 SSL 资源：

SSL 资源	
SSL 证书文件夹	d:\ssl
服务器 SSL 证书文件名	servercert.der
SSL 受信任的证书或根证书文件名	cacert.der
SSL 私钥文件名	server.key
包含用于访问 SSL 私钥文件的短语的文件	passphrase.txt

创建上述资源后，根据以下说明配置胖客户端，例如中央配置管理器（CCM）或升级管理工具。

- 1 确保胖客户端应用程序没有运行。

注意：
确保为运行该服务器的计算机提供该目录。

- 2 运行 sslconfig.exe 命令行工具。

SSLC 工具是随 BI 平台软件一起安装的。（例如，在 Windows 上，它默认安装在 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\win64_x64 中。）

- 3 键入以下命令：

```
sslconfig.exe -dir d:\SSL -mycert servercert.der -rootcert cacert.der -mykey server.key  
-passphrase passphrase.txt -protocol ssl
```

- 4 重新启动胖客户端应用程序。

相关主题

- 第 159 页上的“[为计算机创建密钥和证书文件](#)”

8.13.3.4.1 为翻译管理工具配置 SSL 登录

要使用户能够使用翻译管理工具进行 SSL 登录，必须将有关 SSL 资源的信息添加到工具配置（.ini）文件。

- 1 在以下目录中找到 TransMgr.ini 文件：安装目录\SAP BusinessObjects Enterprise XI 4.0\win32_x86。
- 2 使用文本编辑器打开 TransMgr.ini。
- 3 添加以下参数：

```
-Dbusinessobjects.orb.oci.protocol=ssl -DcertDir=D:\SSLCert  
-DtrustedCert=cacert.der -DsslCert=servercert.der -DsslKey=server.key  
-Dpassphrase=passphrase.txt -jar program.jar
```

- 4 保存该文件并关闭文本编辑器。
- 现在，用户可以使用 SSL 登录到翻译管理工具。

8.13.3.4.2 为报表转换工具配置 SSL

在执行以下步骤之前，需要在大家都知道的目录中创建并保存所有要求的 SSL 资源（例如，证书和私钥）。此外，必须将报表转换工具作为 BI 平台部署的一部分进行安装。

下面的过程将假设您已遵照相关说明创建了以下 SSL 资源：

SSL 资源	
SSL 证书文件夹	d:\ssl
服务器 SSL 证书文件名	servercert.der
SSL 受信任的证书或根证书文件名	cacert.der
SSL 私钥文件名	server.key
包含用于访问 SSL 私钥文件的短语的文件	passphrase.txt

创建上述资源后，利用以下说明将 SSL 配置为使用报表转换工具。

- 1 在承载报表转换工具的计算机上创建 Windows 环境变量 BOBJ_MIGRATION 。

提示：
可将该变量设置为任意值。

- 2 使用文本编辑器打开以下目录中的 migration.bat：
<安装目录>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\scripts\。
- 3 找到以下行：

```
start "" "%JRE%\bin\javaw" -cp migration.jar;* -Xmx512m -Xss10m com.bo.migration.MigrationTool
```

- 4 在 -Xss10m 参数之后添加以下内容：

```
-Dbusinessobjects.orb.ocj.protocol=ssl  
-DcertDir=d:\ssl  
-DtrustedCert=cacert.der  
-DsslCert=servercert.der  
-DsslKey=server.key  
-Dpassphrase=passphrase.txt  
-Dbusinessobjects.migration
```

注意：
请确保各个参数之间有一个空格，且行末没有空格。

- 5 保存该文件并关闭文本编辑器。

此时，用户可使用 SSL 访问报表转换工具。

相关主题

- 第 159 页上的“[为计算机创建密钥和证书文件](#)”

8.14 了解 BI 平台组件间的通信

如果 BI 平台系统完全部署在同一安全子网中，则无需对防火墙进行任何特殊配置。但是，可以选择在由一个或多个防火墙隔离的不同子网中部署某些组件。

在配置系统使用防火墙之前，请务必先了解 BI 平台服务器、胖客户端以及承载 SAP BusinessObjects SDK 的 Web 应用程序服务器之间的通信。

相关主题

- 第 176 页上的“[为防火墙配置 BI 平台](#)”
- 第 181 页上的“[典型的防火墙方案示例](#)”

8.14.1 BI 平台服务器和通信端口概述

如果系统部署中包含防火墙，则了解 BI 平台服务器及其通信端口十分重要。

8.14.1.1 每个 BI 平台服务器都绑定到一个请求端口

BI 平台服务器（例如输入文件资源库服务器）在启动时将绑定到一个请求端口上。其他 BI 平台组件（包括服务器、胖客户端以及在 Web 应用程序服务器中承载的 SDK）可以使用此请求端口与该服务器进行通信。

除非将服务器配置为使用特定的端口号，否则服务器将在启动或重新启动时动态选择其请求端口号。必须为跨防火墙与其他 BI 平台组件进行通信的服务器手动配置特定的请求端口号。

8.14.1.2 每个 BI 平台服务器都会在 CMS 中注册

BI 平台服务器在启动时会向 CMS 进行注册。当服务器进行注册时，CMS 会记录以下内容：

- 服务器主机的主机名（或 IP 地址）。
- 服务器的请求端口号。

8.14.1.3 CMS 使用两个端口

CMS 使用两个端口：请求端口和名称服务器端口。默认情况下将动态选择请求端口。默认情况下，名称服务器端口为 6400。

所有 BI 平台服务器和客户端应用程序最初会与其名称服务器端口上的 CMS 进行联系。CMS 将返回其请求端口值以响应此初始联系。这些服务器以后与 CMS 通信时将使用此请求端口。

8.14.1.4 注册服务的中央管理服务器（CMS）目录

CMS 提供已向其注册的服务的目录。其他 BI 平台组件（如 Web 服务、胖客户端和承载于 Web 应用程序服务器上的 SDK）可以与 CMS 联系，并请求对特定服务的引用。服务的引用包含服务的请求端口号和服务器主机的主机名（或 IP 地址）以及服务 ID。

BI 平台组件可能与它们所使用的服务器位于不同的子网上。服务引用中包含的主机名（或 IP 地址）必须可以从组件的计算机上进行路由。

注意：

默认情况下，对 BI 平台服务器的引用将包含服务器计算机的主机名。（如果计算机有多个主机名，则选择主要主机名）。或者，可以配置服务器，使其引用中包含 IP 地址。

相关主题

- 第 169 页上的“[BI 平台组件间的通信](#)”

8.14.1.5 服务器智能代理（SIA）与中央管理服务器（CMS）通信

如果服务器智能代理（SIA）和中央管理服务器（CMS）无法相互通信，部署将无法工作。确保将防火墙端口配置为允许群集中的所有 SIA 和 CMS 之间进行通信。

8.14.1.6 作业服务器子进程与数据层和 CMS 进行通信

大多数作业服务器将创建子进程以处理任务，如生成报表。作业服务器将创建一个或多个子进程。每个子进程都有其自己的请求端口。

默认情况下，作业服务器将为每个子进程动态选择请求端口。可以指定作业服务器能够从中进行选择的端口号范围。

所有子进程都与 CMS 进行通信。如果此通信跨防火墙，则必须：

- 通过将 `-requestJSChildPorts` 最低端口-最高端口和 `-requestPort` 端口参数添加到服务器的命令行，指定作业服务器可以从中选择的端口号范围。请注意，端口范围应该足够大，以便顾及 `-maxJobs` 所指定的子进程最大数量。
- 在防火墙上打开指定的端口范围。

许多子进程与数据层进行通信。例如，子进程可以连接到报表创建数据库、提取数据以及计算报表值。如果作业服务器子进程跨防火墙与数据层进行通信，则必须：

- 在防火墙上打开从作业服务器计算机上的任一端口到数据库服务器计算机上的数据库侦听端口间的通信路径。

相关主题

- 第 853 页上的“[命令行概述](#)”

8.14.2 BI 平台组件间的通信

BI 平台组件（如浏览器客户端、胖客户端、服务器以及 Web 应用程序服务器中承载的 SDK）在典型工作流程中通过网络相互通信。要跨越由防火墙分隔的不同子网部署 SAP BusinessObjects 产品，必须了解这些工作流程。

8.14.2.1 BI 平台组件之间的通信要求

BI 平台部署必须符合以下一般要求。

- 。 1 每个服务器必须可以在其他每个 BI 平台服务器的请求端口上与该服务器进行通信。
- 。 2 中央管理服务器使用两个端口。每个 BI 平台服务器、胖客户端以及承载 SDK 的 Web 应用程序服务器必须能够在中央管理服务器的两个端口上发起与 CMS 之间的通信。
- 。 3 每个作业服务器子进程都必须能够与 CMS 进行通信。
- 。 4 胖客户端必须能够发起与输入和输出文件资源库服务器的请求端口之间的通信。
- 。 5 如果胖客户端和 Web 应用程序启用了审核，则它们必须能够发起与承载客户端审核代理服务的自适应处理服务器的请求端口之间的通信。
- 。 6 通常，承载 SDK 的 Web 应用程序服务器必须能够与每个 BI 平台服务器的请求端口进行通信。

注意：

Web 应用程序服务器只需与部署中使用的 BI 平台服务器进行通信。例如，如果未使用 Crystal Reports，则 Web 应用程序服务器不需要与 Crystal Reports 高速缓存服务器进行通信。

- 。 7 作业服务器使用通过 `-requestJSChildPorts` 最低端口-最高端口 命令指定的端口号。如果未在命令行中指定范围，则服务器使用随机端口号。若要允许作业服务器与另一台计算机上的 CMS、FTP 或邮件服务器进行通信，请打开防火墙上由 `-requestJSChildPorts` 指定的范围中的所有端口。
- 。 8 CMS 必须能够与 CMS 数据库侦听端口进行通信。
- 。 9 连接服务器、大多数作业服务器子进程和每个系统数据库以及审核处理服务器必须能够进行与报表数据库侦听端口之间的通信。

相关主题

- 第 170 页上的“[BI 平台端口要求](#)”

8.14.2.2 BI 平台端口要求

本节列出了 BI 平台服务器、胖客户端、承载 SDK 的 Web 应用程序服务器和第三方软件应用程序所使用的通信端口。如果部署带有防火墙的 BI 平台，则可以使用此信息在这些防火墙中打开最少数量的端口。

8.14.2.2.1 BI 平台应用程序的端口要求

下表列出了 BI 平台应用程序所使用的服务器和端口号。

产品	客户端应用程序	关联的服务器	服务器端口要求
Crystal Reports	SAP Crystal Reports 2013 设计器	CMS 输入 FRS 输出 FRS Crystal Reports 2013 报表应用程序服务器 (RAS) Crystal Reports 2013 处理服务器 Crystal Reports 高速缓存服务器	CMS 名称服务器端口 (默认为 6400) CMS 请求端口 输入 FRS 请求端口 输出 FRS 请求端口 Crystal Reports 2013 报表应用程序服务器请求端口 Crystal Reports 2013 处理服务器请求端口 Crystal Reports 高速缓存服务器请求端口
Crystal Reports	SAP Crystal Reports for Enterprise 设计器	CMS 输入 FRS 输出 FRS Crystal Reports 处理服务器 Crystal Reports 高速缓存服务器	CMS 名称服务器端口 (默认为 6400) CMS 请求端口 输入 FRS 请求端口 输出 FRS 请求端口 Crystal Reports 处理服务器的请求端口 Crystal Reports 高速缓存服务器请求端口

产品	客户端应用程序	关联的服务器	服务器端口要求
Dashboards	SAP BusinessObjects Dashboards	CMS 输入 FRS 输出 FRS Web 服务提供应用程序 (dswsbobje.war)，可承载 Dashboards、Live Office 和某些数据源连接所需的 QaaWS Web 服务	CMS 名称服务器端口（默认为 6400） CMS 请求端口 输入 FRS 请求端口 输出 FRS 请求端口 HTTP 端口（默认为 80）
Live Office	Live Office 客户端	承载 Live Office Web 服务的 Web 服务提供应用程序 (dswsbobje.war)	HTTP 端口（默认为 80）
BI 平台	SAP BusinessObjects Web Intelligence 胖客户端	CMS 输入 FRS	CMS 名称服务器端口（默认为 6400） CMS 请求端口 输入 FRS 请求端口
BI 平台	Universe 设计工具	CMS 输入 FRS 连接服务器	CMS 名称服务器端口（默认为 6400） CMS 请求端口 输入 FRS 请求端口 连接服务器端口
BI 平台	业务视图管理器	CMS 输入 FRS	CMS 名称服务器端口（默认为 6400） CMS 请求端口 输入 FRS 请求端口

产品	客户端应用程序	关联的服务器	服务器端口要求
BI 平台	中央配置管理器 (CCM)	CMS 服务器智能代理 (SIA)	<p>如果要允许 CCM 管理远程 BI 平台服务器，则必须打开以下端口：</p> <p>CMS 名称服务器端口（默认为 6400）</p> <p>CMS 请求端口</p> <p>如果要允许 CCM 管理远程 SIA 进程，则必须打开以下端口：</p> <p>Microsoft 目录服务（TCP 端口 445）</p> <p>NetBIOS 会话服务（TCP 端口 139）</p> <p>NetBIOS 数据报服务（UDP 端口 138）</p> <p>NetBIOS 名称服务（UDP 端口 137）</p> <p>DNS（TCP/UDP 端口 53）</p> <p>（请注意，上面列出的某些端口可能不是必需的端口。请咨询 Windows 管理员）。</p>
BI 平台	服务器智能代理 (SIA)	包含 CMS 的每个 BI 平台服务器	<p>SIA 请求端口（默认情况下为端口 6410）</p> <p>CMS 名称服务器端口（默认为 6400）</p> <p>CMS 请求端口</p>
BI 平台	报表转换工具	CMS 输入 FRS	<p>CMS 名称服务器端口（默认为 6400）</p> <p>CMS 请求端口</p> <p>输入 FRS 请求端口</p>

产品	客户端应用程序	关联的服务器	服务器端口要求
BI 平台	资源库诊断工具	CMS 输入 FRS 输出 FRS	CMS 名称服务器端口（默认为 6400） CMS 请求端口 输入 FRS 请求端口 输出 FRS 请求端口
BI 平台	承载于 Web 应用程序服务器中的 BI 平台 SDK	所部署产品需要的所有 BI 平台服务器。 例如，如果 SDK 是从 CMS 获取 Crystal 报表并与其交互的，则需要与 Crystal Reports 2013 处理服务器请求端口的通信。	CMS 名称服务器端口（默认为 6400） CMS 请求端口 所需的每个服务器的请求端口。例如 Crystal Reports 2013 处理服务器请求端口。
BI 平台	Web 服务提供者（dswebobje.war）	访问 Web 服务的产品需要的所有 BI 平台服务器。 例如，如果 SAP BusinessObjects Dashboards 通过 Web 服务提供者访问 Enterprise 数据源连接，则需要与 Dashboards 高速缓存和处理服务器请求端口的通信。	CMS 名称服务器端口（默认为 6400） CMS 请求端口 所需的每个服务器的请求端口。例如，Dashboards 高速缓存服务器和 Dashboards 处理服务器请求端口。
BI 平台	SAP BusinessObjects Analysis (OLAP 版)	CMS 承载多维分析服务的自适应处理服务器 输入 FRS 输出 FRS	CMS 名称服务器端口（默认为 6400） CMS 请求端口 自适应处理服务器请求端口 输入 FRS 请求端口 输出 FRS 请求端口

8.14.2.2.2 第三方应用程序的端口要求

下表列出了 SAP Business Objects 产品使用的第三方软件。其中包括某些软件供应商提供的特定示例，然而不同的供应商将有不同的端口要求。

第三方应用程序	使用第三方产品的 SAP Business Objects 组件	第三方应用程序端口要求	说明
CMS 系统数据库	中央管理服务器 (CMS)	数据库服务器侦听端口	CMS 是唯一与 CMS 系统数据库通信的服务器。
CMS 审核数据库	中央管理服务器 (CMS)	数据库服务器侦听端口	CMS 是唯一与 CMS 审核数据库通信的服务器。
报表数据库	连接服务器 每个作业服务器子进程 每台处理服务器	数据库服务器侦听端口	这些服务器从报表创建数据库中获取信息。
Web 应用程序服务器	包括 BI 启动板和 CMC 在内的所有 SAP BusinessObjects Web 服务和 Web 应用程序	HTTP 端口和 HTTPS 端口。 例如，在 Tomcat 上，默认 HTTP 端口为端口 8080，默认 HTTPS 端口为端口 443。	只有在进行安全的 HTTP 通信的情况下才需要使用 HTTPS 端口。
FTP 服务器	每台作业服务器	FTP 输入 (端口 21) FTP 输出 (端口 22)	作业服务器使用 FTP 端口以允许发送到 FTP。
电子邮件服务器	每台作业服务器	SMTP (端口 25)	作业服务器使用 SMTP 端口以允许发送到电子邮件。

第三方应用程序	使用第三方产品的 SAP Business Objects 组件	第三方应用程序端口要求	说明
作业服务器能够将内容发送到的 Unix 服务器	每台作业服务器	rexec 输出（端口 512） （仅限 Unix）rsh 输出（端口 514）	（仅限 Unix）作业服务器使用这些端口以允许发送到磁盘。
身份验证服务器	CMS 承载 SDK 的 Web 应用程序服务器 每个胖客户端，例如 Live Office。	第三方身份验证的连接端口。 例如，Oracle LDAP 服务器的连接服务器由用户在 ldap.ora 文件中进行定义。	用户凭据存储在第三方身份验证服务器中。在用户登录时，CMS、SDK 和此处列出的胖客户端需要与第三方身份验证服务器进行通信。

8.15 为防火墙配置 BI 平台

本节提供配置 BI 平台系统以便在防火墙环境中工作的分步说明。

8.15.1 针对防火墙配置系统

- 1 确定哪些 BI 平台组件必须跨防火墙通信。
- 2 为必须跨防火墙进行通信的每个 BI 平台服务器手动配置请求端口。
- 3 通过将 `-requestJSChildPorts` 最低端口-最高端口 和 `-requestPort` 端口参数添加到服务器的命令行，为必须跨防火墙通信的任何作业服务器子服务器配置端口范围。
- 4 将防火墙配置为允许与上一步中配置的 BI 平台服务器上的请求端口和作业服务器端口范围进行通信。
- 5 （可选）在承载必须跨防火墙通信的 BI 平台服务器的每台计算机上配置 `hosts` 文件。

相关主题

- 第 169 页上的“[BI 平台组件间的通信](#)”
- 第 378 页上的“[配置端口号](#)”
- 第 853 页上的“[命令行概述](#)”
- 第 177 页上的“[指定防火墙规则](#)”
- 第 178 页上的“[为使用 NAT 的防火墙配置 hosts 文件](#)”

8.15.1.1 指定防火墙规则

必须将防火墙配置为允许在 BI 平台组件之间进行必需的通信。有关如何指定这些规则的详细信息，请参阅防火墙文档。

为跨防火墙的每个通信路径指定一个入站访问规则。可能不需要为防火墙背后的每个 BI 平台服务器指定访问规则。

使用在 CMC 中服务器“属性”页上的服务器“请求端口”框中指定的端口号。请记住，计算机上的每个服务器都必须使用唯一的端口号。某些 SAP BusinessObjects 服务器使用多个端口。

注意：

如果跨使用 NAT 的防火墙部署 BI 平台，则所有计算机上的每个服务器都需要唯一的请求端口号。也就是说，整个部署中任何两个服务器都不能共享相同的请求端口。

注意：

不需要指定任何出站访问规则。BI 平台服务器不会与 Web 应用程序服务器或任何客户端应用程序进行通信。BI 平台服务器可以与同一群集中的其他平台服务器通信。不支持在配置了出站防火墙的环境中用群集服务器进行部署。

示例：

此示例显示了 Web 应用程序服务器与 BI 平台服务器之间的防火墙的入站访问规则。在本例中将为 CMS 打开两个端口，一个端口用于输入文件资源库服务器（FRS），另一个端口用于输出 FRS。请求端口号是在服务器的 CMC 配置页的“请求端口”框中指定的端口号。

来源计算机	端口	目标计算机	端口	操作
Web 应用程序服务器	任意	CMS	6400	允许

来源计算机	端口	目标计算机	端口	操作
Web 应用程序服务器	任意	CMS	<请求端口号>	允许
Web 应用程序服务器	任意	输入 FRS	<请求端口号>	允许
Web 应用程序服务器	任意	输出 FRS	<请求端口号>	允许
任意	任意	CMS	任意	拒绝
任意	任意	其他平台服务器	任意	拒绝

相关主题

- 第 169 页上的“[BI 平台组件间的通信](#)”

8.15.1.2 为使用 NAT 的防火墙配置 hosts 文件

仅当 BI 平台服务器必须跨越启用了网络地址转换（NAT）的防火墙进行通信时，才需要执行此步骤。此步骤允许客户端计算机将服务器的主机名映射到可路由的 IP 地址。

注意：

可以将 BI 平台部署在使用域名系统（DNS）的计算机上。在这种情况下，可以在 DNS 服务器上将服务器计算机的主机名映射到可在外部路由的 IP 地址，而不是在每台计算机的 hosts 文件中这样做。

了解网络地址转换

部署防火墙是为了阻止未经授权者访问内部网络。使用 NAT 的防火墙会将来自内部网络的 IP 地址映射到外部网络使用的另一个地址。此地址转换通过向外部网络隐藏内部 IP 地址提高了安全性。

BI 平台组件（如服务器、胖客户端和承载 SDK 的 Web 应用程序服务器）将使用服务引用与服务器联系。服务引用包含服务器计算机的主机名。此主机名必须可通过 BI 平台组件的计算机路由。这意味

着组件的计算机上的 hosts 文件必须将服务器计算机的主机名映射到服务器计算机的外部 IP 地址。服务器计算机的外部 IP 地址可从防火墙的外侧路由，而内部 IP 地址不能这样。

对于 Windows 和 Unix，配置 hosts 文件的过程有所不同。

8.15.1.2.1 在 Windows 上配置 hosts 文件

- 1 找到符合以下条件的每台计算机：运行 BI 平台组件，而该组件必须跨越启用了网络地址转换（NAT）的防火墙进行通信。
- 2 在找到的每台计算机上，使用文本编辑器（如记事本）打开 hosts 文件。hosts 文件位于 \Windows\System32\drivers\etc\hosts 中。
- 3 按照 hosts 文件中的说明，为防火墙后面运行 BI 平台服务器的每台计算机添加一个条目。将服务器计算机的主机名或全限定的域名映射到其外部 IP 地址。
- 4 保存 hosts 文件。

8.15.1.2.2 在 Unix 上配置 hosts 文件

注意：

必须对 Unix 操作系统进行配置，以便在查询 DNS 之前首先查询 hosts 文件以解析域名。有关详细信息，请参阅 Unix 文档。

- 1 找到符合以下条件的每台计算机：运行 BI 平台组件，而该组件必须跨越启用了网络地址转换（NAT）的防火墙进行通信。
- 2 使用编辑器（如 vi）打开 hosts 文件。hosts 文件位于以下目录中：\etc
- 3 按照 hosts 文件中的说明，为防火墙后面运行 BI 平台服务器的每台计算机添加一个条目。将服务器计算机的主机名或全限定的域名映射到其外部 IP 地址。
- 4 保存 hosts 文件。

8.15.2 调试带防火墙的部署

如果启用防火墙时有一个或多个 BI 平台服务器没有工作（即使已经在防火墙上打开了预期端口），则可以使用事件日志确定哪些服务器试图侦听哪些端口或 IP 地址。然后可以在防火墙上打开这些端口，或者使用中央管理控制台（CMC）更改这些服务器尝试侦听的端口号或 IP 地址。

只要 BI 平台服务器启动，该服务器就会为其尝试绑定到的每个请求端口向事件日志中写入以下信息。

- Server（服务器）— 服务器的名称，及其是否成功启动。
- 发布的地址 — IP 地址和端口组合的列表，这些组合发布到其他服务器将用于与此服务器通信的名称服务。

如果服务器成功绑定到端口，则日志文件还将显示“侦听端口”、IP 地址和服务器正在侦听的端口。如果服务器未成功绑定到端口，则日志文件将显示“未能侦听端口”、IP 地址和服务器尝试侦听但侦听失败的端口。

当中央管理服务器启动时，它也会写入有关服务器名称服务端口的“发布的地址”、“侦听端口”和“未能侦听”信息。

注意：

如果服务器配置为使用自动分配的端口，以及配置为使用无效的主机名或 IP 地址，则事件日志将指示该服务器侦听主机名或 IP 地址以及端口 0 失败。如果指定的主机名或 IP 地址无效，则在该主机操作系统可以分配端口前，服务器就会失败。

示例：

以下示例显示了成功侦听两个请求端口和一个名称服务端口的中央管理服务器的一个条目。

```
Server mynode.cms1 successfully started.
Request Port :
  Published Address(es): mymachine.corp.com:11032, mymachine.corp.com:8765
  Listening on port(s): [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:11032, 10.90.172.216:8765
Name Service Port :
  Published Address(es): mymachine.corp.com:6400
  Listening on port(s): [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:6400, 10.90.172.216:6400
```

8.15.2.1 调试带防火墙的部署

1. 请阅读事件日志，以确定服务器是否成功绑定到用户指定的端口。

如果服务器无法成功绑定到端口，则服务器和在同一台计算机上运行的其他进程之间可能存在端口冲突。“Failed to List On”（侦听失败对象）条目指示了服务器尝试侦听的端口。运行 netstat 之类的实用工具确定哪个进程占用了该端口，然后将另一个进程或服务器配置为侦听其他端口。

- 2 如果服务器可以成功绑定到端口，“Listening On”（侦听对象）将指示服务器正在侦听的端口。如果服务器虽然正在侦听某个端口，但是仍未正常工作，请确保该端口在防火墙上已打开，或者配置服务器以便其侦听已打开的端口。

注意：

如果部署中的所有中央管理服务器均尝试侦听不可用的端口或 IP 地址，则这些 CMS 将不会启动，而您将无法登录到 CMC。如果要更改 CMS 尝试侦听的端口号或 IP 地址，必须使用中央配置管理器（CCM）指定有效的端口号或 IP 地址。

相关主题

- 第 378 页上的[“配置端口号”](#)

8.16 典型的防火墙方案示例

本节举例说明了典型的防火墙部署方案。

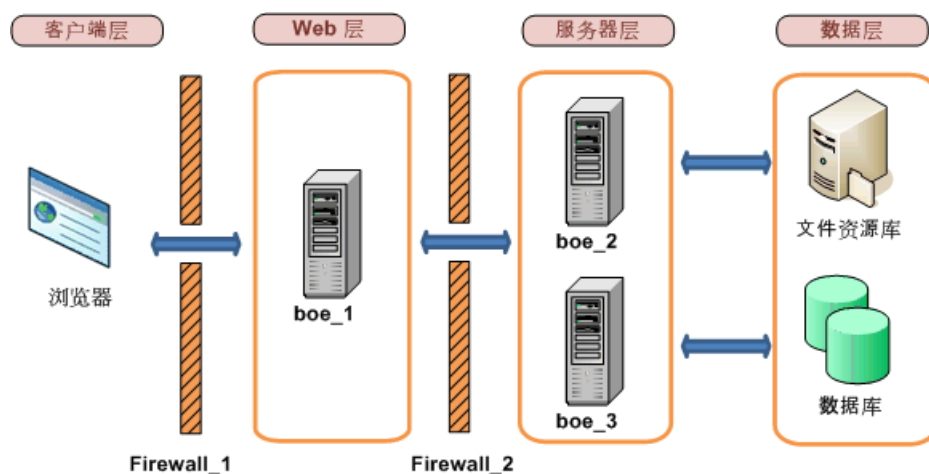
8.16.1 示例 — 部署在独立网络上的应用程序层

此示例说明如何配置防火墙和 BI 平台，以便它们在使用防火墙将 Web 应用程序服务器和其他 BI 平台服务器隔开的部署中协同工作。

在此示例中，BI 平台组件部署跨越以下计算机：

- 计算机 boe_1，该计算机承载 Web 应用程序服务器和 SDK。
- 计算机 boe_2，该计算机承载智能层服务器，其中包括中央管理服务器、输入文件资源库服务器、输出文件资源库服务器和事件服务器。
- 计算机 boe_3，该计算机承载处理层服务器，其中包括自适应作业服务器、Web Intelligence 处理服务器、报表应用程序服务器、Crystal Reports 高速缓存服务器和 Crystal Reports 处理服务器。

图 8-1：部署在独立网络上的应用程序层



8.16.1.1 配置部署在独立网络上的应用程序层

以下步骤说明如何配置此示例。

1. 将以下通信要求应用于此示例：

- 承载 SDK 的 Web 应用程序服务器必须能够在 CMS 的两个端口上与 CMS 进行通信。
- 承载 SDK 的 Web 应用程序服务器必须能够与每个 BI 平台服务器进行通信。
- 浏览器必须能够访问 Web 应用程序服务器上的 http 或 https 请求端口。

2. Web 应用程序服务器必须与计算机 boe_2 和 boe_3 上的所有 BI 平台服务器进行通信。为这些计算机上的每个服务器配置端口号。请注意，可以使用 1,025 与 65,535 之间的任何空闲端口。

下表中列出了为此示例选择的端口号：

服务器	端口号
中央管理服务器	6400
中央管理服务器	6411
输入文件资源库服务器	6415
输出文件资源库服务器	6420
事件服务器	6425
自适应作业服务器	6435
Crystal Reports 高速缓存服务器	6440
Web Intelligence 处理服务器	6460

服务器	端口号
报表应用程序服务器	6465
Crystal Reports 处理服务器	6470

- 3 将防火墙 Firewall_1 和 Firewall_2 配置为允许与上一个步骤中配置的服务器和 Web 应用程序服务器上的固定端口进行通信。

在此示例中将为 Tomcat 应用程序服务器打开 HTTP 端口。

表8-6: Firewall_1 的配置

端口	目标计算机	端口	操作
任意	boe_1	8080	允许

表8-7: firewall_2 的配置

来源计算机	端口	目标计算机	端口	操作
boe_1	任意	boe_2	6400	允许
boe_1	任意	boe_2	6411	允许
boe_1	任意	boe_2	6415	允许
boe_1	任意	boe_2	6420	允许
boe_1	任意	boe_2	6425	允许
boe_1	任意	boe_3	6435	允许
boe_1	任意	boe_3	6440	允许
boe_1	任意	boe_3	6460	允许
boe_1	任意	boe_3	6465	允许
boe_1	任意	boe_3	6470	允许

- 4 此防火墙不启用 NAT，因此我们不必配置 hosts 文件。

相关主题

- 第 378 页上的[“配置端口号”](#)
- 第 167 页上的[“了解 BI 平台组件间的通信”](#)

8.16.2 示例 — 通过防火墙与 BI 平台服务器隔开的胖客户端和数据库层

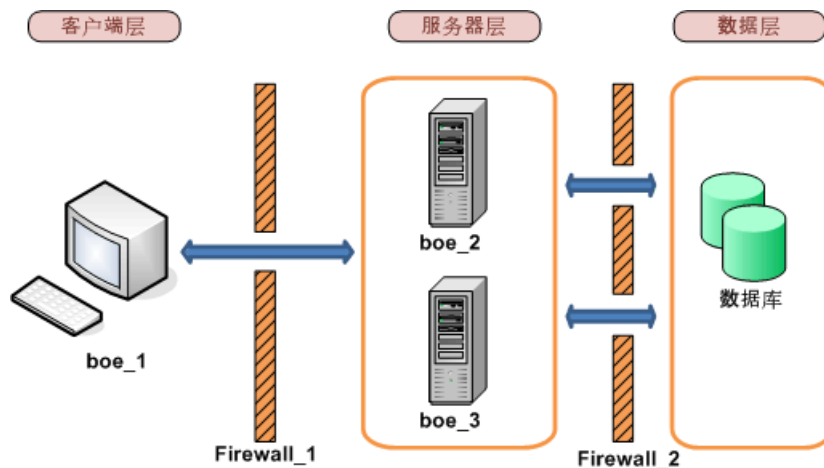
此示例显示如何将防火墙和 BI 平台配置为在以下部署方案中协同工作：

- 一个防火墙将胖客户端与 BI 平台服务器隔开。
- 一个防火墙将 BI 平台服务器与数据库层隔开。

在此示例中，BI 平台组件部署跨越以下计算机：

- 计算机 boe_1，该计算机承载发布向导。发布向导是一个 BI 平台胖客户端。
- 计算机 boe_2，该计算机承载智能层服务器，其中包括中央管理服务器（CMS）、输入文件资源库服务器、输出文件资源库服务器和事件服务器。
- 计算机 boe_3，该计算机承载处理层服务器，其中包括自适应作业服务器、Web Intelligence 处理服务器、报表应用程序服务器、Crystal Reports 处理服务器和 Crystal Reports 高速缓存服务器。
- 计算机 Databases 承载 CMS 系统、审核数据库和报表数据库。请注意，可以将这两个数据库部署在相同的数据库服务器上，也可以将每个数据库部署在各自的数据库服务器上。在此示例中，所有 CMS 数据库和报表数据库均部署在同一个数据库服务器上。

图 8-2：部署在独立网络上的胖客户端和数据库层



8.16.2.1 配置通过防火墙与 BI 平台服务器隔开的层

以下步骤说明如何配置此示例。

- 1 将以下通信要求应用于此示例：
 - 发布向导必须能够在 CMS 的两个端口上与 CMS 进行通信。
 - 发布向导必须能够与输入文件资源库服务器和输出文件资源库服务器进行通信。
 - 连接服务器、每个作业服务器子进程以及每个处理服务器必须能够访问报表数据库服务器上的侦听端口。
 - CMS 必须能够访问 CMS 数据库服务器上的数据库侦听端口。
- 2 为 CMS、输入 FRS 和输出 FRS 配置特定端口。请注意，可以使用 1,025 与 65,535 之间的任何空闲端口。

下表中列出了为此示例选择的端口号：

服务器	端口号
中央管理服务器	6411
输入文件资源库服务器	6415
输出文件资源库服务器	6416

- 3 不需要为作业服务器子进程配置端口范围，因为作业服务器与数据库服务器之间的防火墙将被配置为允许任何端口进行通信。
- 4 将 Firewall_1 配置为允许与上一个步骤中配置的平台服务器上的固定端口进行通信。请注意，端口 6400 是 CMS 名称服务器端口的默认端口号，不需要在上一个步骤中对其进行显式配置。

端口	目标计算机	端口	操作
任意	boe_2	6400	允许
任意	boe_2	6411	允许
任意	boe_2	6415	允许
任意	boe_2	6416	允许

将 Firewall_2 配置为允许与数据库服务器侦听端口进行通信。CMS（在 boe_2 上）必须有权访问 CMS 系统和审核数据库，而且作业服务器（在 boe_3 上）必须有权访问系统和审核数据库。请注意，没有为作业服务器子进程配置端口范围，因为这些进程与 CMS 之间的通信未跨越防火墙。

来源计算机	端口	目标计算机	端口	操作
boe_2	任意	数据库	3306	允许
boe_3	任意	数据库	3306	允许

- 5 此防火墙不启用 NAT，因此我们不必配置 hosts 文件。

相关主题

- 第 167 页上的[“了解 BI 平台组件间的通信”](#)
- 第 176 页上的[“为防火墙配置 BI 平台”](#)

8.17 集成环境的防火墙设置

本部分详细介绍有关与以下 ERP 环境集成的 BI 平台部署的具体注意事项和端口设置。

- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

BI 平台组件包括浏览器客户端、胖客户端、服务器以及承载在 Web 应用程序服务器上的 SDK。系统组件可以安装在多台计算机上。将系统配置为使用防火墙之前，了解 BI 平台和 ERP 组件之间通信的基本知识将大有用处。

BI 平台服务器的端口要求

BI 平台中的相应服务器需要以下端口：

服务器端口要求
<ul style="list-style-type: none">• 中央管理服务器的名称服务器端口• 中央管理服务器的请求端口• 输入 FRS 的请求端口• 输出 FRS 的请求端口• 报表应用程序服务器的请求端口• Crystal Reports 高速缓存服务器的请求端口• Crystal Reports 页面服务器请求端口• Crystal Reports 处理服务器请求端口

8.17.1 SAP 集成专用防火墙指南

BI 平台部署必须遵循以下通信规则：

- CMS 必须能够在 SAP 系统网关端口上发起与 SAP 系统的通信。
- 自适应作业服务器和 Crystal Reports 处理服务器（及数据访问组件）必须能够在 SAP 系统网关端口上启动与 SAP 系统的通信。
- BW 发布器组件必须能够在 SAP 系统网关端口上启动与 SAP 系统的通信。
- SAP Enterprise Portal 端上部署的 BI 平台组件（如 iViews 和 KMC）必须能够在 HTTP/HTTPS 端口上发起与 BI 平台 Web 应用程序的通信。
- Web 应用程序服务器必须能够在 SAP 系统网关服务上启动通信。
- Crystal Reports 必须能够在 SAP 系统网关端口和 SAP 系统调度程序端口上启动与 SAP 主机的通信。

SAP 网关服务正在侦听的端口与安装中指定的端口相同。

注意：

如果某组件需要 SAP 路由器才能连接到 SAP 系统，则可以使用 SAP 路由器字符串配置该组件。例如，在配置 SAP 权利系统以导入角色和用户时，SAP 路由器字符串可以替代应用程序服务器的名称。这可确保 CMS 将通过 SAP 路由器与 SAP 系统进行通信。

相关主题

- 第 756 页上的“[安装本地 SAP 网关](#)”

8.17.1.1 详细的端口要求

SAP 的端口要求

BI 平台使用 SAP Java 连接器（SAP JCO）与 SAP NetWeaver（ABAP）进行通信。需要配置并确保以下端口的可用性：

- SAP 网关服务侦听端口（如 3300）。
- SAP 调度程序服务侦听端口（如 3200）。

下表汇总了所需的特定端口配置。

源计算机	端口	目标计算机	端口	操作
SAP	任意	BI 平台 Web 应用程序服务器	Web 服务 HTTP/HTTPS 端口	允许
SAP	任意	CMS	CMS 名称服务器端口	允许
SAP	任意	CMS	CMS 请求端口	允许
Web 应用程序服务器	任意	SAP	SAP 系统网关服务端口	允许
中央管理服务器 (CMS)	任意	SAP	SAP 系统网关服务端口	允许
Crystal Reports	任意	SAP	SAP 系统网关服务端口和 SAP 系统调度程序端口	允许

8.17.2 JD Edwards EnterpriseOne 集成的防火墙配置

部署将与 JD Edwards 软件进行通信的 BI 平台时，必须遵循下面这些通信规则：

- 中央管理控制台 Web 应用程序必须能够通过 JDENET 端口和随机选择的端口发起与 JD Edwards EnterpriseOne 的通信。
- 使用数据连接客户端组件的 Crystal Reports 必须能够通过 JDENET 端口发起与 JD Edwards EnterpriseOne 的通信。为检索数据，JD Edwards EnterpriseOne 端必须能够通过不受控的随机端口与驱动程序通信。
- 中央管理服务器必须能够通过 JDENET 端口和随机选择的端口发起与 JD Edwards EnterpriseOne 的通信。
- JDENET 端口号可以在 JDENET 部分中的 JD Edwards EnterpriseOne 应用程序服务器配置文件 (JDE.INI) 中找到。

BI 平台服务器的端口要求

产品	服务器端口要求
SAP BusinessObjects Business Intelligence 平台	<ul style="list-style-type: none"> • BI 平台登录服务器端口

JD Edwards EnterpriseOne 的端口要求

产品	端口要求	说明
JD Edwards EnterpriseOne	JDENET 端口和随机选择的端口	用于 BI 平台和 JD Edwards EnterpriseOne 应用程序服务器之间的通信。

配置 Web 应用程序服务器以与 JD Edwards 通信

本节介绍如何配置防火墙和 BI 平台，以便它们在防火墙将 Web 应用程序服务器和其他平台服务器隔开的部署中协同工作。

有关 BI 平台服务器和客户端的防火墙配置，请参阅本指南中的“BI 平台端口要求”部分。除标准防火墙配置外，与 JD Edwards 服务器的通信还需要打开一些额外端口。

表8-14: 对于 JD Edwards EnterpriseOne Enterprise

来源计算机	端口	目标计算机	端口	操作
用于 JD Edwards EnterpriseOne 的具有安全连通性功能的 CMS	任意	JD Edwards EnterpriseOne	任意	允许
用于 JD Edwards EnterpriseOne 的具有数据连通性功能的 BI 平台服务器	任意	JD Edwards EnterpriseOne	任意	允许
用于 JD Edwards EnterpriseOne 的具有客户端数据连接功能的 Crystal Reports	任意	JD Edwards EnterpriseOne	任意	允许
Web 应用程序服务器	任意	JD Edwards EnterpriseOne	任意	允许

8.17.3 Oracle EBS 的专用防火墙指南

BI 平台的部署必须允许以下组件发起与 Oracle 数据库侦听器端口之间的通信。

BI 平台 Web 组件

- CMS（具体指 Oracle EBS 安全插件）
- BI 平台后端服务器（具体而言，即 EBS 数据访问组件）
- Crystal Reports（具体指 EBS 数据访问组件）

注意：

上述所有 Oracle 数据库侦听器端口的默认值为 1521。

8.17.3.1 详细的端口要求

除 BI 平台的标准防火墙配置外，还需要打开一些要在集成 Oracle EBS 环境中使用的额外端口。

来源计算机	端口	目标计算机	端口	操作
Web 应用程序服务器	任意	Oracle EBS	Oracle 数据库端口	允许
具有 Oracle EBS 安全连通性的 CMS	任意	Oracle EBS	Oracle 数据库端口	允许
具有服务器端 Oracle EBS 数据连通性的 BI 平台服务器	任意	Oracle EBS	Oracle 数据库端口	允许
具有客户端 Oracle EBS 数据连通性的 Crystal Reports	任意	Oracle EBS	Oracle 数据库端口	允许

8.17.4 PeopleSoft Enterprise 集成的防火墙配置

要与 PeopleSoft Enterprise 通信的 BI 平台部署必须遵循以下一般通信规则：

- 使用安全连通性组件的中央管理服务器（CMS）必须能够发起与 PeopleSoft 查询访问（QAS）Web 服务的通信。
- 使用数据连通性组件的 BI 平台服务器必须能够发起与 PeopleSoft QAS Web 服务的通信。
- 使用数据连通性客户端组件的 Crystal Reports 必须能够发起与 PeopleSoft QAS Web 服务的通信。
- Enterprise 管理（EPM）桥必须能够与 CMS 和输入文件资源库服务器通信。
- EPM 桥必须能够通过 ODBC 连接与 PeopleSoft 数据库通信。

Web 服务端口号与 PeopleSoft Enterprise 域名中指定的端口号相同。

BI 平台服务器的端口要求

产品	服务器端口要求
SAP BusinessObjects Business Intelligence 平台	<ul style="list-style-type: none"> BI 平台登录服务器端口

PeopleSoft 的端口要求

产品	端口要求	说明
PeopleSoft Enterprise (People Tools 8.46 或更新版本)	Web 服务 HTTP/HTTPS 端口	当对 PeopleSoft Enterprise for People Tools 8.46 和更新解决方案使用 SOAP 连接时，需要此端口

为防火墙配置 BI 平台和 PeopleSoft

本节介绍如何配置 BI 平台和 PeopleSoft Enterprise，以便它们在防火墙将 Web 应用程序服务器和其他 BI 平台服务器隔开的部署中协同工作。

有关 BI 平台服务器和客户端的防火墙配置，请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》。

除了 BI 平台的防火墙配置外，还需要进行某些额外配置。

表8-18: 对于 PeopleSoft Enterprise (PeopleTools 8.46 或更新版本)

来源计算机	端口	目标计算机	端口	操作
用于 PeopleSoft 的具有安全连通性功能的 CMS	任意	PeopleSoft	PeopleSoft Web 服务 HTTP/HTTPS 端口	允许
用于 PeopleSoft 的具有数据连通性功能的 BI 平台服务器	任意	PeopleSoft	PeopleSoft Web 服务 HTTP/HTTPS 端口	允许
用于 PeopleSoft 的具有客户端数据连通性功能的 Crystal Reports	任意	PeopleSoft	PeopleSoft Web 服务 HTTP/HTTPS 端口	允许
EPM 桥	任意	CMS	CMS 名称服务器端口	允许
EPM 桥	任意	CMS	CMS 请求端口	允许
EPM 桥	任意	输入文件资源库服务器	输入 FRS 的端口	允许

来源计算机	端口	目标计算机	端口	操作
EPM 桥	任意	PeopleSoft	PeopleSoft 数据库端口	允许

8.17.5 Siebel 集成的防火墙配置

本节介绍当 BI 平台和 Siebel eBusiness Application 系统由防火墙隔离开时用于两者间通信的特定端口。

- Web 应用程序必须能够发起与“用于 Siebel 的 BI 平台登录服务器”的通信。用于 Siebel 的 Enterprise 登录服务器需要三个端口：
 - 1 Echo (TCP) 端口 7，用于检查对登录服务器的访问。
 - 2 “用于 Siebel 的 BI 平台登录服务器”端口（默认为 8448），用作 CORBA IOR 侦听端口。
 - 3 用于 CORBA 通信的随机 POA 端口；由于无法对其进行控制，因此需要打开所有端口。
- CMS 必须能够发起与“用于 Siebel 的 BI 平台登录服务器”的通信。为每个登录服务器配置的 CORBA IOR 侦听端口（如 8448）。还需要打开在安装 BI 平台之前无法获知的随机 POA 端口号。
- 用于 Siebel 的 BI 平台登录服务器必须能够发起与 SCBroker（Siebel 连接代理）端口（例如 2321）的通信。
- BI 平台后端服务器（Siebel 数据访问组件）必须能够发起与 SCBroker（Siebel 连接代理）端口（例如 2321）的通信。
- Crystal Reports（Siebel 数据访问组件）必须能够发起与 SCBroker（Siebel 连接代理）端口（例如 2321）的通信。

端口的详细说明

本节列出了 BI 平台使用的端口。如果部署使用防火墙的 BI 平台，则可以使用此信息在特定于 Siebel 集成的防火墙中打开最低数量的端口。

表8-19: BI 平台服务器的端口要求

产品	服务器端口要求
SAP BusinessObjects Business Intelligence 平台	<ul style="list-style-type: none"> • BI 平台登录服务器端口

表8-20: Siebel 的端口要求

产品	端口要求	说明
Siebel eBusiness Applications	2321	默认 SCBroker (Siebel 连接代理) 端口

为 Siebel 集成配置 BI 平台防火墙

本节介绍如何为 Siebel 和 BI 平台配置防火墙，以便它们在防火墙将 Web 应用程序服务器和其他平台服务器隔开的部署中协同工作。

来源计算机	端口	目标计算机	端口	操作
Web 应用程序服务器	任意	用于 Siebel 的 BI 平台登录服务器	任意	允许
CMS	任意	用于 Siebel 的 BI 平台登录服务器	任意	允许
用于 Siebel 的 BI 平台登录服务器	任意	Siebel	SCBroker 端口	允许
用于 Siebel 的具有服务器端数据连通性的 BI 平台服务器	任意	Siebel	SCBroker 端口	允许
用于 Siebel 的具有客户端数据连通性的 Crystal Reports	任意	Siebel	SCBroker 端口	允许

8.18 BI 平台和反向代理服务器

BI 平台可以部署在具有一个或多个反向代理服务器的环境中。通常，反向代理服务器部署在 Web 应用程序服务器之前，目的是隐藏单一 IP 地址后面的 Web 应用程序服务器。此配置路由通过反向代理服务器发送到私有 Web 应用程序服务器的所有 Internet 通信，并隐藏私人 IP 地址。

由于反向代理服务器将公共 URL 转换为内部 URL，因此必须使用在内部网络上部署的 BI 平台 Web 应用程序的 URL 对其进行配置。

8.18.1 受支持的反向代理服务器

BI 平台支持以下反向代理服务器：

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

8.18.2 了解如何部署 Web 应用程序

BI 平台 Web 应用程序部署在 Web 应用程序服务器上。这些应用程序在安装期间通过 WDeploy 工具自动部署。也可以在部署 BI 平台之后使用该工具手动部署应用程序。在默认的 Windows 安装中，Web 应用程序位于以下目录：

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI  
4.0\warfiles\webapps
```

WDeploy 用于部署 WAR 文件，如：

- BOE：包括中央管理控制台（CMC）、BI 启动板、OpenDocument
- dswsbobje：包含 Web 服务应用程序

如果 Web 应用程序服务器位于反向代理服务器的后面，则应该以 WAR 文件的正确上下文路径配置该反向代理服务器。要公开所有 BI 平台功能，需要为部署的每个 BI 平台 WAR 文件配置一个上下文路径。

8.19 为 BI 平台 Web 应用程序配置反向代理服务器

反向代理服务器必须配置为将传入的 URL 请求映射到部署（其中 BI 平台 Web 应用程序部署在反向代理服务器后面）中正确的 Web 应用程序。

本节包含某些受支持反向代理服务器的具体配置示例。有关更多信息，请参阅反向代理服务器供应商文档。

8.19.1 配置反向代理服务器的详细说明

配置 WAR 文件

BI 平台 Web 应用程序作为 WAR 文件部署在 Web 应用程序服务器上。确保在反向代理服务器上为部署所需的 WAR 文件配置一个指令。可以使用 WDeploy 部署 BOE 或 dswsbobje WAR 文件。有关 WDeploy 的更多信息，请参阅《BI 平台 Web 应用程序部署指南》。

在自定义配置目录中指定 BOE 属性

BOE.war 文件包括全局和应用程序特定属性。如果需要修改属性，请使用自定义配置目录。默认情况下，目录位于：C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom。

警告：

要避免覆盖默认目录中的文件，请勿修改 config/default 目录中的属性。用户应使用 custom 目录。

注意：

在某些 Web 应用程序服务器（如与 BI 平台捆绑在一起的 Tomcat 版本）上，可以直接访问 BOE.war 文件。在此情况下，可以直接设置自定义设置而无需取消部署 WAR 文件。当无法访问 BOE.war 文件时，必须取消部署该文件，然后自定义和重新部署文件。

一致使用正斜线 (/)

在反向代理服务器中定义上下文路径，方式与在浏览器 URL 中输入上下文路径相同。例如，如果指令在反向代理服务器上镜像路径末尾包含正斜线 (/)，则在浏览器 URL 末尾键入正斜线。

确保在反向代理服务器指令的源 URL 和目标 URL 中统一使用 “/” 字符。如果在源 URL 末尾添加了 “/” 字符，则也必须向目标 URL 末尾添加该字符。

8.19.2 配置反向代理服务器

要使 BI 平台 Web 应用程序在受支持的反向代理服务器后工作，需要执行以下步骤。

- 1 确保根据供应商的说明和部署的网络拓扑正确设置反向代理服务器。
- 2 确定需要哪个 BI 平台 WAR 文件。
- 3 为每个 BI 平台 WAR 文件配置反向代理服务器。请注意，针对每种反向代理服务器类型指定的规则不同。

- 4 执行所需的任一特殊配置。在某些 Web 应用程序服务器上部署一些 Web 应用程序时，需要对这些应用程序进行特殊配置。

8.19.3 为 BI 平台配置 Apache 2.2 反向代理服务器

本节介绍如何配置 BI 平台和 Apache 2.2 以使其协同工作的工作流。

- 1 确保将 BI 平台和 Apache 2.2 安装在不同的计算机上。
- 2 确保按照供应商文档中的说明安装 Apache 2.2 并将其配置为反向代理服务器。
- 3 为部署在反向代理服务器后面的每个 WAR 文件配置 ProxyPass。
- 4 为部署在反向代理服务器后面的每个 Web 应用程序配置 ProxyPassReverseCookiePath。例如：

```
ProxyPass /C1/BOE/ http://appservername:80/BOE/
ProxyPassReverseCookiePath / /C1/BOE
ProxyPassReverse /C1/BOE/ http://appservername:80/BOE/
ProxyPass /C1/explorer/ http://appservername:80/explorer/
ProxyPassReverseCookiePath / /C1/explorer
ProxyPassReverse /C1/explorer/ http://appservername:80/explorer/
```

8.19.4 为 BI 平台配置 WebSEAL 6.0 反向代理服务器

本节阐释如何配置 BI 平台和 WebSEAL 6.0 以使其协同工作。

推荐的配置方法是创建单个标准连接，该连接将内部 Web 应用程序服务器或 Web 服务器上承载的所有 BI 平台 Web 应用程序映射到单个安装点。

- 1 确保将 BI 平台和 WebSEAL 6.0 安装在不同的计算机上。
可以在同一台计算机上部署 BI 平台和 WebSEAL 6.0，但不推荐此做法。有关配置此部署方案的说明，请参阅 WebSEAL 6.0 供应商文档。
- 2 确保按供应商文档中的说明安装和配置了 WebSEAL 6.0。
- 3 启动 WebSEAL pdadmin 命令行实用程序。以具有管理特权的用户身份登录到安全域，如 sec_master。
- 4 在“pdadmin sec_master”提示处输入以下命令：

```
server task <instance_name-webseald-host_name> create -t
<type> -h <host_name> -p <port> <junction_point>
```

其中：

- <instance_name-webseald-host_name> 指定已安装 WebSEAL 实例的完整服务器名称。请按照服务器列表命令输出中显示的格式使用此完整服务器名称。

- <type> 指定联接类型。如果联接映射到内部 HTTP 端口，则使用 tcp。如果联接映射到内部 HTTPS 端口，则使用 ssl。
- <host_name> 指定将接收请求的内部服务器的 DNS 主机名或 IP 地址。
- <port> 指定将接收请求的内部服务器的 TCP 端口。
- <junction_point> 指定受 WebSEAL 保护的受保护空间中的目录，其中设置了内部服务器的文档空间。

示例：

```
server task default-webseald-webseal.rp.sap.com
create -t tcp -h 10.50.130.123 -p 8080/hr
```

8.19.5 为 BI 平台配置 Microsoft ISA 2006

本节阐释如何配置 BI 平台和 ISA 2006 以使其协同工作。

推荐的配置方法是创建单个标准连接，该连接将内部 Web 应用程序服务器或 Web 服务器上承载的所有 BI 平台 WAR 文件映射到单个安装点。需要对应用程序服务器进行其他配置才能使其与 ISA 2006 协同工作，具体取决于 Web 应用程序服务器。

- 1 确保将 BI 平台和 ISA 2006 安装在不同的计算机上。

可以在同一台计算机上部署 BI 平台和 ISA 2006，但不推荐此做法。有关配置此部署方案的说明，请参阅 ISA 2006 文档。

- 2 确保按照供应商文档中的描述安装和配置 ISA 2006。

- 3 启动 ISA 服务器管理实用程序。

- 4 使用导航面板启动新分布规则

- a 转到

“阵列” > <计算机名称> > “防火墙策略” > “新建” > “网站发布规则”

记忆：

使用安装有 ISA 2006 的计算机的名称替代 <计算机名称>。

- b 在“Web 发布规则名称”中键入规则名称并单击“下一步”

- c 选择“允许”作为规则操作并单击“下一步”。

- d 选择“发布单个网站或负载均衡器”作为发布类型并单击“下一步”。

- e 选择 ISA 服务器和所发布网站间的连接类型，并单击“下一步”。

例如，选择“使用不安全的连接连接发布的 Web 服务器或服务场”。

- f 在“内部站点名称”中键入正在发布的网站（例如承载 BI 平台的计算机名称）的内部名称，并单击“下一步”。

注意：

如果承载 ISA 2006 的计算机不能连接至目标服务器，请选择“使用计算机名称或 IP 地址连接到发布的服务器”，并在所提供的字段中键入名称或 IP 地址。

- g 在“公共名称明细”中，选择域名（例如“任何域名”，并指定任意内部发布明细（例如 /*）。单击“下一步”。

现在需要创建新的 Web 侦听器以监视传入 Web 请求。

- 5 单击“新建”以启动“新建 Web 侦听器定义向导”。

- a 在“Web 侦听器名称”中键入名称，然后单击“下一步”。

- b 选择 ISA 服务器和所发布网站间的连接类型，并单击“下一步”。

例如，选择“不需要与客户端建立 SSL 安全连接”。

- c 在“Web 侦听器 IP 地址”部分中，选择以下内容并单击“下一步”。

- 内部
- 外部
- 本地主机
- 所有网络

ISA 服务器现已配置为仅通过 HTTP 进行发布。

- d 选择“身份验证设置”选项，单击“下一步”，再单击“完成”。

现在为 Web 发布规则配置了新的侦听器。

- 6 在“用户集”中单击“下一步”，然后单击“完成”。

- 7 单击“应用”，以保存 Web 发布规则的所有设置，并更新 ISA 2006 配置。

现在必须更新 Web 发布规则的属性，才能映射 Web 应用程序的路径。

- 8 在导航面板中，右击所配置的防火墙策略，并选择“属性”。

- 9 在“路径”选项卡上，单击“添加”，将路线映射到 SAP BusinessObjects Web 应用程序中。

- 10 在“公共名称”选项卡上，选择“Request for the following Web sites”（请求下列网站），然后单击“添加”。

- 11 在“公共名称”对话框中，键入 ISA 2006 服务器名称并单击“确定”。

- 12 单击“应用”，以保存 Web 发布规则的所有设置，并更新 ISA 2006 配置。

- 13 通过访问下列 URL 验证连接：

http://ISA 服务器主机名:Web 侦听器端口号/应用程序的外部路径

例如：http://myISAServer:80/Product/BOE/CMC

注意：

可能必须多次刷新浏览器。

需要为刚配置的规则修改 HTTP 策略以确保可以登录到 CMC。右击在 ISA 服务器管理实用程序中创建的规则并选择“配置 HTTP”。现在必须在“URL 保护”区域中取消选择“验证正则化”。

要远程访问 BI 平台，需要创建一个访问规则。

8.20 反向代理部署中 BI 平台的特殊配置

某些 BI 平台产品需要其他配置才能在反向代理部署中正常运行。本节阐释如何执行其他配置。

8.20.1 为 Web 服务启用反向代理

本节介绍为 Web 服务启用反向代理所必须完成的过程。

8.20.1.1 在 Tomcat 上启用反向代理

要在 Tomcat Web 应用程序服务器上启用反向代理，必须修改 `server.xml` 文件。必须进行的修改步骤包括：将 `proxyPort` 设置为反向代理服务器侦听端口，以及添加新的 `proxyName`。本节介绍该过程。

- 1 停止 Tomcat。
- 2 打开 Tomcat 的 `server.xml`。

在 Windows 上，`server.xml` 位于：C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf

在 Unix 上，`server.xml` 位于 <CATALINA 主目录>/conf 中。<CATALINA 主目录> 的默认值为 <安装目录>/sap_bobj/tomcat。

- 3 在 `server.xml` 文件中找到此节：

```
<!-- 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 通过删除 `<!--` 和 `-->` 取消注释 `Connector` 元素。
- 5 将 `proxyPort` 的值修改为反向代理服务器侦听端口。

- 6 将一个新的 proxyName 属性添加到 Connector 的属性列表。proxyName 的值必须是代理服务器名称，Tomcat 应可将该名称解析为正确的 IP 地址。

示例：

```
<!--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" />
```

其中的 my_reverse_proxy_server.domain.com 和 ReverseProxyServerPort 应被替换为正确的反向代理服务器名称及其侦听端口。

- 7 保存并关闭 server.xml 文件。
- 8 重新启动 Tomcat。
- 9 确保反向代理服务器将其虚拟路径映射到正确的 Tomcat 连接器端口。在上面的示例中，该端口为 8082。

以下示例显示了一个配置为反向代理 SAP BusinessObjects Web 服务（部署在 Tomcat 上）的 Apache HTTP Server 2.2 示例配置：

```
ProxyPass /XI3.0/dswsbobje http://internalServer:8082/dswsbobje
ProxyPassReverseCookiePath /dswsbobje /XI3.0/dswsbobje
```

要启用 Web 服务，必须为连接器确定代理名称和端口号。

8.20.1.2 在除 Tomcat 外的其他 Web 应用程序服务器上为 Web 服务启用反向代理

以下过程要求依据所选的 Web 应用程序服务器成功配置 BI 平台 Web 应用程序。请注意，wsresources 区分大小写。

- 1 停止 Web 应用程序服务器。
- 2 在 dsws.properties 文件中指定 Web 服务的外部 URL。

此文件位于 dswsbobje Web 应用程序中。例如，如果外部 URL 是 http://my_reverse_proxy_server.domain.com/dswsbobje/，请在 dsws.properties 文件中更新以下属性：

- wsresource1=ReportEngine|reportengine web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/ReportEngine
- wsresource2=BICatalog|bicatalog web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BICatalog

- wsresource3=Publish|publish web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/Publish
 - wsresource4=QueryService|query web service alone|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/QueryService
 - wsresource5=BIPlatform|BIPlatform web service|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/BIPlatform
 - wsresource6=LiveOffice|Live Office web service|http://my_reverse_proxy_server.domain.com/SAP/dswsbobje/services/LiveOffice
- 3 保存并关闭 dsws.properties 文件。
 - 4 重新启动 web 应用程序服务器。
 - 5 确保反向代理服务器将其虚拟路径映射到正确的 Web 应用程序服务器连接器端口。以下示例显示了一个配置为反向代理 BI 平台 Web 服务（部署在所选 Web 应用程序服务器上）的 Apache HTTP Server 2.2 示例配置：

```
ProxyPass /SAP/dswsbobje http://internalServer:<侦听端口> /dswsbobje
```

```
ProxyPassReverseCookiePath /dswsbobje /SAP/dswsbobje
```

其中 <侦听端口> 是 Web 应用程序服务器的侦听端口。

8.20.2 为 ISA 2006 启用会话 cookie 的根路径

本节说明如何配置特定的 Web 应用程序服务器以启用会话 cookie 的根路径，从而将 ISA 2006 用作反向代理服务器。

8.20.2.1 配置 Apache Tomcat

要配置会话 cookie 的根路径以将 ISA 2006 用作反向代理服务器，请将以下内容添加到 server.xml 中的 <Connector> 元素：

```
emptySessionPath="true"
```

- 1 停止 Tomcat
- 2 打开以下位置中的 server.xml：
 - <CATALINA 主目录>\conf

- 3 在 server.xml 文件中找到以下部分：

```
<!-- 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 通过删除 `<!--` 和 `-->` 取消注释 Connector 元素。
- 5 要配置会话 cookie 的根路径以将 ISA 2006 用作反向代理服务器，请将以下内容添加到 server.xml 中的 `<Connector>` 元素：

```
emptySessionPath="true"
```

- 6 将 proxyPort 的值修改为反向代理服务器侦听端口。
- 7 将一个新的 proxyName 属性添加到 Connector 的属性列表。值必须是代理服务器名称，Tomcat 可将该名称解析为正确的 IP 地址。

例如：

```
<!--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 保存并关闭 server.xml 文件。
- 9 重新启动 Tomcat。

确保反向代理服务器将其虚拟路径映射到正确的 Tomcat 连接器端口。在上面的示例中，该端口为 8082。

8.20.2.2 配置 Sun Java 8.2

需要为每个 BI 平台 Web 应用程序修改 sun-web.xml。

- 1 转到 `<SUN_WEBAPP_DOMAIN>\generated\xml\j2ee-modules\webapps\BOE\WEB-INF`
- 2 打开 sun-web.xml
- 3 在 `<context-root>` 容器后添加以下内容：

```
<session-config>
  <cookie-properties>
    <property name="cookiePath" value="/" />
  </cookie-properties>
```

```
</session-config>
<property name="reuseSessionID" value="true"/>
```

- 4 保存并关闭 sun-web.xml。
- 5 为每个 Web 应用程序重复步骤 1-4。

8.20.2.3 配置 Oracle Application Server 10gR3

需要为每个 BI 平台 Web 应用程序的部署目录修改 global-web-application.xml 或 orion-web.xml。

- 1 转到 <ORACLE_HOME>\j2ee\home\config\
- 2 打开 global-web-application.xml 或 orion-web.xml。
- 3 将下行添加到 <orion-web-app> 容器：

```
<session-tracking cookie-path="/" />
```

- 4 保存并关闭此配置文件。
- 5 登录到 Oracle 管理控制台：
 - a 转到“OC4J:home (OC4J: 主页)” > “Administration (管理)” > “Server Properties (服务器属性)”。
 - b 在“Command Line Options” (命令行选项) 下，选择“Options” (选项)。
 - c 单击“Add another Row” (添加另一行)，然后键入以下内容：

```
Doracle.useSessionIDFromCookie=true
```

- 6 重新启动 Oracle 服务器。

8.20.2.4 配置 WebSphere Community Edition 2.0

- 1 打开 WebSphere Community Edition 2.0 管理控制台。
- 2 在左侧导航面板中，找到“Server” (服务器) 并选择“Web Server” (Web 服务器)。
- 3 选择连接器并单击“编辑”。
- 4 选中“emptySessionPath”复选框，并单击“Save” (保存)。
- 5 在“ProxyName”中键入 ISA 服务器名称。
- 6 在“ProxyPort”中键入 ISA 侦听器端口号。
- 7 先停止然后再重新启动该连接器。

8.20.3 为 SAP BusinessObjects Live Office 启用反向代理

要针对反向代理启用 SAP BusinessObjects Live Office 的“在 Web 浏览器中查看对象”功能，请调整默认查看器 URL。可在中央管理控制台（CMC）中或通过 Live Office 选项完成此操作。

注意：

本节假设已成功为 BI 启动板和 BI 平台 Web 服务启用了反向代理。

8.20.3.1 在 CMC 中调整默认查看器 URL

- 1 登录到 CMC。
- 2 在“应用程序”页面中，单击“中央管理控制台”。
- 3 选择“操作” > “处理设置”。
- 4 在“URL”字段中，选择正确的默认查看器 URL，然后单击“保存并关闭”。

例如：

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

ReverseProxyServer 和 ReverseProxyServerPort 表示正确的反向代理服务器名称及其侦听端口。

第 9 章 身份验证

9.1 BI 平台中的身份验证选项

身份验证是验证尝试访问系统的用户身份的过程，而权限管理是验证是否已授予用户足够权限对指定对象执行所请求操作的过程。

安全插件可以扩展和自定义 BI 平台对用户进行身份验证的方法。安全插件允许将用户帐户和组从第三方系统映射到平台，从而简化了帐户的创建和管理。可以将第三方用户帐户或组映射到现有 BI 平台用户帐户或组，也可以创建对应于外部系统中每个映射条目的新 Enterprise 用户帐户或组。

当前版本支持以下身份验证方法：

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

由于 BI 平台可全面自定义，因此身份验证和过程可能因系统而异。

相关主题

- 第 209 页上的“[Enterprise 身份验证概述](#)”
- 第 280 页上的“[配置 SAP 身份验证](#)”
- 第 223 页上的“[使用 LDAP 身份验证](#)”
- 第 244 页上的“[Windows AD 支持要求和初始设置](#)”
- 第 325 页上的“[启用 JD Edwards EnterpriseOne 身份验证](#)”
- 第 336 页上的“[启用 Oracle EBS 身份验证](#)”
- 第 309 页上的“[启用 PeopleSoft Enterprise 身份验证](#)”
- 第 330 页上的“[启用 Siebel 身份验证](#)”

9.1.1 主要身份验证

当用户第一次尝试访问系统时，将进行主要身份验证。在主要身份验证过程中，可能会发生以下两种情况之一：

- 如果未配置单一登录，则用户提供他们的凭据，如用户名、密码和身份验证类型。

用户在登录屏幕上输入这些详细信息。

- 如果配置了单一登录的方法，则会以静默方式传播用户的凭据。

这些详细信息是使用其他方法（比如 Kerberos 或 SiteMinder）提取的。

身份验证类型可能是 Enterprise、LDAP、Windows AD、SAP、Oracle EBS、Siebel、JD Edwards EnterpriseOne、PeopleSoft Enterprise，具体取决于在中央管理控制（CMC）的“身份验证”管理区域中所启用和设置的类型。用户的 Web 浏览器通过 HTTP 将信息发送到 Web 服务器，后者将信息路由到 CMS 或相应的平台服务器。

Web 应用程序服务器通过服务器端脚本传递用户信息。脚本将以内部方式与 SDK 通信并最终与相应的安全插件通信，以便依据用户数据库对用户进行身份验证。

例如，如果用户登录到 BI 启动板，并且指定 Enterprise 身份验证，则 SDK 将确保 BI 平台安全插件执行身份验证。中央管理服务器（CMS）使用安全插件，依据系统数据库对用户名和密码进行验证。或者，如果用户指定不同的身份验证方法，SDK 将使用相应的安全插件对用户进行身份验证。

如果安全插件报告凭据成功匹配，则 CMS 将授予用户一个活动系统标识，并执行以下操作：

- CMS 为用户创建一个 Enterprise 会话。处于活动状态时，此会话将消耗系统上的一个用户许可。
- CMS 生成并编码登录标记，并将其发送到 Web 应用程序服务器。
- Web 应用程序服务器将用户的信息存储在内存中的一个会话变量中。如果有效，此会话将存储允许 BI 平台响应用户请求的信息。

注意：

会话变量不包含用户的密码。

- Web 应用程序服务器将登录标记保留在客户端浏览器上的 Cookie 中。这仅用于故障转移，如具有群集 CMS 时，或者针对会话亲缘性将 BI 启动板组成群集时。

注意：

可以禁用登录标记，但是，如果禁用登录标记，将会同时禁用故障转移。

9.1.2 安全插件

安全插件可以扩展和自定义 BI 平台对用户进行身份验证的方法。BI 平台当前附带有以下插件：

- Enterprise
- LDAP
- Windows AD
- SAP
- Oracle EBS
- Siebel
- JD Edwards
- PeopleSoft

安全插件允许将用户帐户和组从第三方系统映射到 BI 平台，以此简化帐户的创建和管理。可以将第三方用户帐户或组映射到现有 BI 平台用户帐户或组，也可以创建对应于外部系统中每个映射条目的新 Enterprise 用户帐户或组。

安全插件动态地维护第三方用户和组列表。将外部组映射到 BI 平台后，属于该组的所有用户都可以成功登录 BI 平台。如果随后更改了第三方组成员资格，将不需要更新或刷新 BI 平台中的列表。例如，如果将 LDAP 组映射到 BI 平台，然后向该组添加新用户，则当该新用户首次利用有效的 LDAP 凭据登录到 BI 平台时，安全插件会为其动态创建别名。

此外，安全插件还使您能够以一致的方式将权限分配给用户和组，因为映射的用户和组将被视为好像 Enterprise 帐户一样。例如，可能从 Windows AD 中映射某些用户帐户或组，并从 LDAP 目录服务器中映射某些帐户或组。然后，当您需要在 BI 平台中分配权限或创建新的自定义组时，可以在 CMC 中进行所有设置。

每个安全插件都充当一个依据相应用户数据库对用户凭据进行验证的身份验证提供程序。当用户登录到 BI 平台时，他们会从您在 CMC 的“身份验证”管理区域中启用和设置的可用身份验证类型中进行选择。

注意：

如果 BI 平台服务器组件在 Unix 上运行，则 Windows AD 安全插件将无法对用户进行身份验证。

9.1.3 BI 平台的单一登录

BI 平台的单一登录意味着用户一旦登录到操作系统，即可访问支持 SSO 的应用程序，而无需再次提供凭据。当用户登录时，将为用户创建一个安全上下文。该上下文可传播至 BI 平台以执行 SSO。

术语匿名单一登录也指 BI 平台的单一登录，但它特指 Guest 用户帐户的单一登录功能。如果启用了 Guest 用户帐户（默认情况下已启用），任何人都能够以 Guest 身份登录到 BI 平台，并将对该系统具有访问权限。

9.1.3.1 单一登录支持

术语“单一登录”用于描述不同的方案。就其最基本的层面来说，单一登录是指用户只需提供一次登录凭据便可访问两个或多个应用程序或系统的情形，这就使得用户能够更轻松地与系统交互。

BI 平台或不同身份验证工具可以提供对 BI 启动板的单一登录，具体取决于应用程序服务器类型和操作系统。

如果在 Windows 上使用 Java 应用程序服务器，则可以使用以下单一登录方法：

- Windows AD 及 Kerberos
- Windows AD 及 SiteMinder

如果在 Windows 上使用 IIS，则可以使用以下单一登录方法：

- Windows AD 及 Kerberos
- Windows AD 及 NTLM
- Windows AD 及 SiteMinder

对于 Windows 或 Unix 上任何平台支持的 Web 应用程序服务器，均可提供单一登录支持方法。

- LDAP 及 SiteMinder
- 受信任的身份验证
- Windows AD 及 Kerberos
- 通过 SUSE 11 中 Kerberos 的 LDAP
- 通过受信任的身份验证进行 SAP NetWeaver 单一登录

注意：

如果 Java 应用程序位于 Unix 上，则支持 Windows AD 及 Kerberos。但是，BI 平台服务需要在 Windows 服务器上运行。

下表介绍了 BI 启动板的单一登录支持的方法。

身份验证模式	CMS 服务器	选项	注释
Windows AD	仅限 Windows	仅限 Windows AD 及 Kerberos	对 BI 启动板和 CMC 的 Windows AD 身份验证可以即装即用。
LDAP	任何支持的平台	仅限支持的 LDAP 目录服务器及 SiteMinder	对 BI 启动板和 CMC 的 LDAP 身份验证可以即装即用。BI 启动板和 CMC 的 SSO 需要 SiteMinder。
Enterprise	任何支持的平台	受信任的身份验证	对 BI 启动板和 CMC 的 Enterprise 身份验证可以即装即用。BI 启动板和 CMC 的 SSO 及 Enterprise 身份验证需要受信任的身份验证。

- 第 207 页上的 [“BI 平台的单一登录”](#)

- 第 209 页上的 [“到数据库的单一登录”](#)
- 第 209 页上的 [“端到端单一登录”](#)

9.1.3.2 到数据库的单一登录

用户登录到 BI 平台后，数据库的单一登录功能将使他们能够执行需要数据库访问权限的操作（特别是，查看和刷新报表），而不必再次提供他们的登录凭据。数据库的单一登录可与 BI 平台的单一登录组合使用，以使用户能够更轻松地了解访问所需资源。

9.1.3.3 端到端单一登录

端到端单一登录是指这样一种配置，在该配置中，用户既有前端到 BI 平台的单一登录，也有后端到数据库的单一登录。因此，用户只需在登录到操作系统时提供一次他们的登录凭据，即可访问 BI 平台，并能够执行需要数据库访问权限的操作（如查看报表）。

在 BI 平台中，端到端单一登录是通过 Windows AD 和 Kerberos 支持的。

9.2 Enterprise 身份验证

9.2.1 Enterprise 身份验证概述

Enterprise 身份验证是 BI 平台的默认身份验证方法；首次安装系统时会自动启用该方法，并且无法禁用。当您添加和管理用户及组时，BI 平台会在其数据库中保留用户和组信息。

提示：

如果希望创建独立的帐户和组用于 BI 平台，或者尚未在第三方目录服务器中设置用户和组层次结构，请使用系统默认的 Enterprise 身份验证。

无需配置或启用 Enterprise 身份验证。但是，可以修改 Enterprise 身份验证设置以满足组织的特定安全要求。仅可通过中央管理控制台（CMC）修改 Enterprise 身份验证设置。

9.2.2 Enterprise 身份验证设置

设置	选项	说明
密码限制	强制大小写混合的密码	此选项确保密码至少包含以下两类字符：大写字母、小写字母、数字或标点符号。
	必须至少包含 N 个字符	通过强制要求密码的最低复杂程度，您可以降低恶意用户简单猜测有效用户密码的机率。
用户限制	必须每隔 N 天更改密码	此选项确保密码不会成为薄弱环节并会定期刷新。
	不能重新使用 N 个最近的密码	此选项确保不会机械地重复密码。
	必须等待 N 分钟才能更改密码	此选项确保将新密码输入系统后无法立即进行更改。
登录限制	在 N 次登录尝试失败后禁用帐户	此安全选项指定在禁用其帐户之前，允许用户进行多少次系统登录尝试。
	在 N 分钟后重置失败的登录次数	此选项指定重置登录尝试计数器的时间间隔。
	在 N 分钟后重新启用帐户	此选项指定在 N 次登录尝试失败后要将该帐户暂挂多长时间。
将数据源凭据与登录同步	登录时启用并更新用户的数据源凭据	此选项将在用户登录后启用数据源凭据。
受信任的身份验证	已启用受信任的身份验证	提供用于设置“受信任的身份验证”的设置。

相关主题

- 第 212 页上的[“启用受信任的身份验证”](#)

9.2.3 更改 Enterprise 设置

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“Enterprise”。
- 将出现“Enterprise”对话框。
- 3 更改设置。
- 提示：**
要将所有设置恢复为默认值，请单击“重置”。
- 4 单击“更新”以保存所做的修改。

9.2.3.1 更改常规密码设置

- 注意：**
长期不用的帐户不会自动取消激活。管理员必须手动删除非活动帐户。
- 1 转到 CMC 的“身份验证”管理区域。
 - 2 双击“Enterprise”。
 - 将出现“Enterprise”对话框。
 - 3 为要使用的每个密码设置选中该复选框，并在必要时提供值。
- 下表标识了可以配置的每个密码相关设置的最小和最大值。

密码设置	最小值	建议最大值
强制大小写混合的密码	不适用	不适用
至少必须包含 N 个字符	0 个字符	64 个字符
必须每隔 N 天更改密码	1 天	100 天

密码设置	最小值	建议最大值
不能重新使用 N 个最近的密码	1 个密码	100 个密码
必须等待 N 分钟才能更改密码	0 分钟	100 分钟
在 N 次登录尝试失败后禁用帐户	1 次失败	100 次失败
在 N 分钟后重置失败的登录次数	1 分钟	100 分钟
在 N 分钟后重新启用帐户	0 分钟	100 分钟

4 单击“更新”。

注意：

空闲 Enterprise 帐户不会自动禁用。系统管理员必须手动删除不再活动的帐户。

9.2.4 启用受信任的身份验证

通过借助 Web 应用程序服务器验证用户的身份，Enterprise 受信任的身份验证可用于执行单一登录。此身份验证法包括在中央管理服务器（CMS）和承载 BI 平台 Web 应用程序的 Web 应用程序服务器之间建立信任。建立信任之后，系统会延迟对访问 Web 应用程序服务器的用户进行身份验证。受信任的身份验证可用于支持 SAML、x.509 以及其他没有专用身份验证插件的身份验证方法。

用户更喜欢只登录系统一次，而不用在一次会话过程中多次提供密码。“受信任的身份验证”提供了一个 Java 单一登录解决方案，可用于将 BI 平台身份验证解决方案与第三方身份验证解决方案相集成。与中央管理服务器（CMC）建立了信任关系的应用程序可以使用“受信任的身份验证”，以便允许用户不提供密码便可登录。

要启用“受信任的身份验证”，则必须通过 Enterprise 身份验证设置在服务器上配置一个共享秘密，并通过为 BOE WAR 文件指定的属性配置客户端。

注意：

- 必须已创建了 Enterprise 用户或映射了需要登录到 BI 平台的第三方用户，然后才能使用受信任的身份验证。

BI 启动板的单一登录 URL 为：<http://server:port/BOE/BI>。

相关主题

- 第 213 页上的[“将服务器配置为使用“受信任的身份验证””](#)
- 第 216 页上的[“为 Web 应用程序配置受信任的身份验证”](#)

9.2.4.1 将服务器配置为使用“受信任的身份验证”

在可以配置“受信任的身份验证”之前，必须已创建 Enterprise 用户或已映射需要登录到 BI 平台的第三方用户。

1 登录到 CMC。

2 转到“身份验证”管理区域。

3 单击“Enterprise”选项。

随后将显示“Enterprise”对话框。

4 在“受信任的身份验证”下：

a 单击“已启用受信任的身份验证”。

b 单击“新建共享秘密”。

将显示消息“共享秘密密钥已生成，可供下载”。

c 单击“下载共享秘密”。

客户端和 CMS 使用共享秘密来建立信任。必须首先配置服务器，然后为“受信任的身份验证”配置客户端。

将出现“文件下载”对话框。

d 单击“保存”，并将 TrustedPrincipal.conf 文件保存到以下目录之一：

- 安装目录\SAP BusinessObjects Enterprise XI 4.0\win64_x64\
- 安装目录\SAP BusinessObjects Enterprise XI 4.0\win32_x86\

警告：

不要将超时设置为 0（零）。0 值意味着两个时钟时间差异的时间量是无限的，这将增加重放攻击的脆弱性。

e 在“共享秘密有效性期间”字段中，输入共享秘密的有效天数。

f 对于“受信任的身份验证”请求，请指定客户端上的时钟与 CMS 中的时钟允许的最大时间差异值（以毫秒为单位）。

5 单击“更新”以提交共享秘密。

BI 平台不对“受信任的身份验证”参数所做的一切修改进行审核。用户必须手动备份受信任的身份验证信息。

客户端和 CMS 使用共享秘密来建立信任。下一步是为“受信任的身份验证”配置客户端。

9.2.5 为 Web 应用程序配置受信任的身份验证

要为客户端配置受信任的身份验证，必须修改 BOE.war 文件的全局属性以及 BI 启动板和 OpenDocument 应用程序的特定属性。

使用以下方法之一将共享秘密传递至客户端：

- WEB_SESSION 选项
- TrustedPrincipal.conf 文件

使用以下方法之一将用户名传递至客户端：

- REMOTE_USER
- HTTP_HEADER
- COOKIE
- QUERY_STRING
- WEB_SESSION
- USER_PRINCIPAL

不管如何传递共享秘密，都必须在 BOE.war 文件的 Trusted.auth.user.retrieval 全局属性中对要使用的方法进行自定义。

9.2.5.1 对 SAML 单一登录使用受信任的身份验证

安全性断言标记语言（SAML）是一种基于 XML 的标准，用于传输身份信息。SAML 提供了一种传输身份和信任的安全连接，从而启用单一登录机制，排除寻求访问 BI 平台的受信任用户的其他登录。

启用 SAML 身份验证

如果应用程序服务器可充当 SAML 服务提供商，则可以使用受信任的身份验证提供对 BI 平台的 SAML SSO。

为此，必须首先配置 Web 应用程序服务器，以启用 SAML 身份验证。

另外，还必须使用下列方法之一将用户名传输到客户端：

- REMOTE_USER
- USER_PRINCIPAL

以下示例包含了为 SAML 身份验证配置的示例 Web.xml:

```
<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>
```

请参阅您的应用程序服务器文档，了解有关如何完成此操作的更多信息，因为不同应用程序服务器的配置方法不同。

使用受信任的身份验证

将 Web 应用程序服务器配置为充当 SAML 服务提供商之后，即可使用受信任的身份验证提供 SAML SSO。

注意：

用户必须导入到 BI 平台或拥有 Enterprise 帐户。

动态别名用于启用 SSO。当用户首次通过 SAML 访问登录页时，将会被要求使用其现有的 BI 平台帐户凭据手动登录。验证用户凭据之后，系统将为用户的 BI 平台帐户设置 SAML 标识的别名。用户的后续登录尝试将使用 SSO 执行，因为系统会将用户的标识别名与现有帐户进行动态匹配。

注意：

必须启用 BOE.war 文件的特定属性 `trusted.auth.user.namespace.enabled`，这种机制才能发挥作用。

9.2.5.2 Web 应用程序的受信任身份验证属性

下表列出了 BOE.war 文件默认 global.properties 中受信任的身份验证设置。要覆盖该设置，请在以下路径中新建一个文件：C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom。

属性	默认值	说明
sso.enabled=true	sso.enabled=false	为 BI 平台启用和禁用单一登录（SSO）。设置为 true 可启用“受信任的身份验证”。
trusted.auth.shared.secret	无	用于检索受信任的身份验证秘密的会话变量名。仅在使用 Web 会话传递共享秘密时适用。
trusted.auth.user.param	无	指定用于为受信任的身份验证检索用户名的变量。
trusted.auth.user.retrieval	无	指定用于为受信任的身份验证检索用户名的方法： <ul style="list-style-type: none"> • REMOTE_USER • HTTP_HEADER • COOKIE • QUERY_STRING • WEB_SESSION • USER_PRINCIPAL 设置为空白，可禁用“受信任的身份验证”。
trusted.auth.user.namespace.enabled	无	<p>启用和禁用对现有用户帐户的动态别名绑定。如果设置为 true，则受信任的身份验证会使用别名绑定，对登录到 BI 平台的用户进行身份验证。通过别名绑定，应用程序服务器可充当 SAML 服务提供商，从而启用受信任的身份验证，以提供对系统的 SAML 单一登录。</p> <p>如果该属性为空白，则“受信任的身份验证”将在对用户进行身份验证时使用名称匹配。</p>

9.2.5.3 为 Web 应用程序配置受信任的身份验证

如果打算在 TrustedPrincipal.conf 文件中存储共享秘密，请确保文件存储在相应的平台目录中：

平台	TrustedPrincipal.conf 的位置
Windows (默认安装)	<ul style="list-style-type: none"> • <安装目录>\SAP BusinessObjects Enterprise XI 4.0\win32_x86\ • <安装目录>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\
AIX	<安装目录>/sap_bobj/enterprise_xi40/ aix_rs6000/
Solaris	<安装目录>/sap_bobj/enterprise_xi40/ solaris_sparc/
Linux	<安装目录>/sap_bobj/enterprise_xi40/linux_x86

有多种机制可以填充用户名变量，该变量用于为承载 Web 应用程序的客户端配置受信任的身份验证。配置或设置 Web 应用程序服务器，以便在使用这些用户名检索方法之前，用户名会显示出来。有关进一步信息，请参阅<http://java.sun.com/j2ee/1.4/docs/api/javax/servlet/http/HttpServletRequestQuest.html>。

要为客户端配置受信任的身份验证，必须访问并修改 BOE.war 文件的属性，其中包括 BI 启动板和 OpenDocument 应用程序的常规及特定属性。

注意：

可能还需要其他一些步骤，这取决于计划检索用户名或共享秘密的方式。

- 1 在承载 Web 应用程序的计算机上访问 BOE.war 文件的自定义文件夹：

<安装目录>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\。

之后，必须重新部署修改后的 BOE.war 文件。

- 2 使用“记事本”或其他文本编辑实用程序创建一个新文件。
- 3 输入以下受信任的身份验证属性：

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

对于 trusted.auth.shared.secret 属性，为用户名检索选择以下选项之一：

选项	如何检索用户名
HTTP_HEADER	从 HTTP 标头的内容中检索用户名。指定要在 trusted.auth.user.param 属性中使用的 HTTP 标头。

选项	如何检索用户名
QUERY_STRING	从请求 URL 的参数中检索用户名。指定要在 <code>trusted.auth.user.param</code> 属性中使用的查询字符串。
COOKIE	从指定的 Cookie 中检索用户名。指定要在 <code>trusted.auth.user.param</code> 属性中使用的 Cookie。
WEB_SESSION	从指定会话变量的内容中检索用户名。指定要在 <code>global.properties</code> 的 <code>trusted.auth.user.param</code> 属性中使用的 Web 会话变量。
REMOTE_USER	从对 <code>HttpServletRequest.getRemoteUser()</code> 的调用中检索用户名。
USER_PRINCIPAL	通过为 Servlet 或 JSP 中的当前请求在 <code>HttpServletRequest</code> 对象上调用 <code>getUserPrincipal().getName()</code> 来检索用户名。

注意：

- 某些 Web 应用程序服务器要求将服务器上的环境变量 `REMOTE_USER` 设置为 “true”。要了解是否有此要求，请参阅 Web 应用程序服务器文档。如果要求，请确认该环境变量设置为 “true”。
- 如果使用 `USER_PRINCIPAL` 或 `REMOTE_USER` 传递用户名，请保留 `trusted.auth.user.param` 为空白。

4 使用名称 `global.properties` 保存文件。

5 重新启动 Web 应用程序服务器。

仅在运行 Web 应用程序服务器的计算机上重新部署修改的 BOE Web 应用程序后，新属性才会生效。使用 WDeploy 在 Web 应用程序服务器上重新部署 WAR 文件。有关使用 WDeploy 的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

9.2.5.3.1 示例配置

9.2.5.3.1.1 通过 TrustedPrincipal.conf 文件传递共享秘密

下面的示例配置假设已在 BI 平台中创建了用户 JohnDoe。

用户信息通过 Web 会话进行存储和传递，共享秘密通过 TrustedPrincipal.conf 文件进行传递，该文件默认位于 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86 目录中。Tomcat 的绑定版是 Web 应用程序服务器。

- 1 在安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\ 目录中，使用“记事本”或任何其他文本编辑实用程序创建一个新文件。
- 2 要指定“受信任的身份验证”属性，请输入以下值：

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

- 3 使用名称 global.properties 保存文件。
- 4 访问 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp 文件。
- 5 修改文件的内容，以包括下列值：

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<%@ page language="java" contentType="text/html; charset=utf-8" %>
<%
//custom Java code
request.getSession().setAttribute("MyUser", "JohnDoe");
%>
<html>
<head>
<title>Custom Entry Point</title>
</head>
<body>
<script type="text/javascript" src="noCacheCustomResources/myScript.js"></script>
<a href="javascript:goToLogonPage()">Click this to go to the logon page of BI launch pad</a>
</body>
</html>
```

- 6 在 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources 目录中创建 myScript.js 文件。
- 7 将下列值添加到 myScript.js 中：

```
function goToLogonPage() {
    window.location = "logon.jsp"; }
```

- 8 重新启动 Web 应用程序服务器。
- 9 使用 WDeploy 在 Web 应用程序服务器上重新部署 WAR 文件。

有关使用 WDeploy 的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

要验证是否已经正确配置“受信任的身份验证”，请使用以下 URL 访问 BI 启动板：[http://\[cmsname\]:8080/BOE/BI/custom.jsp](http://[cmsname]:8080/BOE/BI/custom.jsp)，其中 [cmsname] 是承载 CMS 的计算机的名称。此时应显示以下链接：单击此链接以转到 BI 启动板的登录页。

9.2.5.3.1.2 通过 Web 会话变量传递共享秘密

下面的示例配置假设已在 BI 平台中创建了用户 JohnDoe。

将通过 Web 会话存储和传递用户信息，同时通过 Web 会话变量传递共享秘密。假设此文件位于以下目录：`C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86`。需要打开文件并记录文件的内容。在此示例配置中，假设共享秘密如下：

```
9ecb0778edcff048edae0fcdde1a5db8211293486774a127ec949c1bdb98dae8e0ea388979edc65773
841c8ae5d1f675a6bf5d7c66038b6a3f1345285b55a0a7
```

Tomcat 的绑定版是 Web 应用程序服务器。

- 1 访问以下目录：
 <安装目录>\SAP BusinessObjects Enterprise XI
 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\
- 2 使用文本编辑器创建新文件。
- 3 通过输入以下内容，指定受信任的身份验证属性：

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

- 4 使用以下名称保存该文件：
 global.properties
- 5 访问以下文件：
 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
 4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp
- 6 修改文件的内容，以包括以下信息：

```
<!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 在以下目录中创建 myScript.js 文件：

C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomRe
sources

- 8 将以下信息添加到 myScript.js 中：

```
function goToLogonPage() {
    window.location = "logon.jsp";
}
```

- 9 重新启动 Web 应用程序服务器。

- 10 使用 WDeploy 在 Web 应用程序服务器上重新部署 WAR 文件。

有关使用 WDeploy 的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

要验证是否正确配置了受信任的身份验证，请使用以下 URL 访问 BI 启动板应用程序：

http://[cmsname]:8080/BOE/BI/custom.jsp，其中 [cmsname] 是承载 CMS 的计算机的名称。应显示以下链接：

单击此链接以转到 BI 启动板的登录页。

9.2.5.3.1.3 通过用户主体传递用户名

下面的示例配置假设已在 BI 平台中创建了用户 JohnDoe。

用户信息通过“用户主体”选项进行存储和传递，共享秘密通过 TrustedPrincipal.conf 文件传递，该文件默认位于 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win32_x86 目录中。Tomcat 的绑定版是 Web 应用程序服务器。

- 1 停止 Tomcat 服务器。
- 2 打开位于默认目录 C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\ 中的 Tomcat 的 server.xml 文件。
- 3 找到 <Realm className="org.apache.catalina.realm.UserDatabaseRealm"..../>，并将其更改为以下值：

```
Realm className="orgapachecatalinarealmMemoryRealm".../
```

- 4 打开位于默认目录 C:\Program Files (x86)\SAP BusinessObjects\Tomcat\conf\ 中的 tomcat-users.xml 文件。

- 5 找到 <tomcat-users> 标记，并修改以下值：

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

- 6 打开 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\ 目录中的 web.xml 文件。

- 7 在 </web-app> 标记前面，添加以下值：

```
<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>
```

为 <url-pattern></url-pattern> 参数输入一个特定页。通常，此页不是 BI 启动板或任何其他 Web 应用程序的默认 URL。

- 8 在自定义 global.properties 文件中，输入以下值：

```
trusted.auth.user.retrieval=USER_PRINCIPAL
trusted.auth.user.namespace.enabled=true
```

注意：

可以选择设置 trusted.auth.user.namespace.enabled=true。如果要将外部用户名映射到其他 BI 平台用户名，可添加该参数。

- 9 重新启动 Web 应用程序服务器。
10. 使用 WDeploy 在 Web 应用程序服务器上重新部署 WAR 文件。
有关使用 WDeploy 的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

注意：

如果使用“远程用户”方法，则 Web 应用程序服务器上的配置相同。

要验证是否正确配置了“受信任的身份验证”，请使用以下 URL 访问 BI 启动板：http://[cmsname]:8080/BOE/BI，其中 [cmsname] 是承载 CMS 的计算机的名称。片刻后将出现登录对话框。

9.3 LDAP 身份验证

9.3.1 使用 LDAP 身份验证

本节提供 LDAP 身份验证如何与 BI 平台配合工作的一般说明。之后，它介绍允许为 BI 平台管理和配置 LDAP 帐户的管理工具。

安装 BI 平台时将自动安装 LDAP 身份验证插件，但不会默认启用。要使用 LDAP 身份验证，用户需要首先确保已设置了相应的 LDAP 目录。有关 LDAP 的更多信息，请参阅 LDAP 文档。

轻量级目录访问协议（LDAP）（一种常用的独立于应用程序的目录）使用户能够在多个应用程序间共享信息。LDAP 基于开放式标准，提供在目录中访问和更新信息的方法。

LDAP 基于 X.500 标准，该标准使用目录访问协议（DAP）在目录客户端和目录服务器之间通信。LDAP 替代了 DAP，因为它使用更少的资源，并简化和省略了某些 X.500 操作和功能。

LDAP 内目录结构中的条目是按特定架构编排的。每个条目都由其对应的可分辨名称（DN）或通用名称（CN）标识。其他常用属性包括组织单位名称（OU）和组织名称（O）。例如，成员组可能按如下方式处于目录树中：cn=BI 平台用户，ou=Enterprise 用户 A，o=研发部门。有关更多信息，请参考 LDAP 文档。

由于 LDAP 独立于应用程序，因此具有适当权限的任何客户端都能访问其目录。LDAP 使您能够设置用户通过 LDAP 身份验证登录到 BI 平台。这可为用户提供对系统中相关对象的访问权限。只要运行了 LDAP 服务器并在现有联网计算机系统中使用 LDAP，就可以（随 Enterprise 和 Windows AD 身份验证一起）使用 LDAP 身份验证。

如果需要，BI 平台附带的 LDAP 安全插件能够使用 SSL 连接（使用服务器身份验证或相互身份验证建立）与 LDAP 服务器通信。通过服务器身份验证，LDAP 服务器将拥有 BI 平台用于验证它是否信任服务器的安全证书，同时 LDAP 服务器允许来自匿名客户端的连接。通过相互身份验证，LDAP 服务器和 BI 平台都拥有安全证书，并且 LDAP 服务器还必须验证客户端证书，然后才能建立连接。

可将 BI 平台附带的 LDAP 安全插件配置为通过 SSL 与 LDAP 服务器通信，但在验证用户的凭据时始终执行基本身份验证。在部署 LDAP 身份验证与 BI 平台之前，请确保已熟悉这些 LDAP 类型之间的差异。有关更多信息，请参阅 RFC2251（当前位于 <http://www.faqs.org/rfcs/rfc2251.html> 上）。

相关主题

- 第 224 页上的“[配置 LDAP 身份验证](#)”
- 第 234 页上的“[映射 LDAP 组](#)”

9.3.1.1 LDAP 安全插件

LDAP 安全插件允许将 LDAP 目录服务器中的用户帐户和组映射到 BI 平台；它还使系统能够验证所有指定了 LDAP 身份验证的登录请求。将依据 LDAP 目录服务器对用户进行身份验证，并在 CMS 授予这些用户活动的 BI 平台会话之前，对他们在所映射 LDAP 组中的成员资格进行验证。用户列表和组成员资格由系统动态维护。可以指定该平台使用安全套接字层（SSL）连接与 LDAP 目录服务器通信，以便更加安全。

BI 平台的 LDAP 身份验证与 Windows AD 身份验证的相似之处在于：可以映射组，设置身份验证、访问权限和创建别名。同时，与 NT 或 AD 身份验证一样，可为现有 LDAP 用户创建新的 Enterprise 帐户，并且，如果现有用户的用户名与 Enterprise 用户名匹配，还可为其分配 LDAP 别名。此外，可以执行以下操作：

- 映射 LDAP 目录服务中的用户和组。
- 依据 AD 映射 LDAP。如果依据 AD 配置 LDAP，则有许多限制。
- 指定多个主机名及其端口。
- 配置 LDAP 及 SiteMinder。

映射了 LDAP 用户和组之后，所有 BI 平台客户端工具都将支持 LDAP 身份验证。还可以创建自己的支持 LDAP 身份验证的应用程序。

相关主题

- 第 228 页上的“[为 LDAP 服务器或相互身份验证配置 SSL](#)”
- 第 236 页上的“[依据 Windows AD 映射 LDAP](#)”
- 第 232 页上的“[为 SiteMinder 配置 LDAP 插件](#)”

9.3.2 配置 LDAP 身份验证

为简化管理，BI 平台支持用户和组帐户的 LDAP 身份验证。先必须将用户的 LDAP 帐户映射到 BI 平台中，然后才可以使用其 LDAP 用户名和密码登录系统。映射 LDAP 帐户时，可以选择创建新帐户或链接到现有 BI 平台帐户。

在设置和启用 LDAP 身份验证之前，请确保已设置了 LDAP 目录。有关更多信息，请参阅 LDAP 文档。

LDAP 身份验证的配置包括以下任务：

- 配置 LDAP 主机
- 为 SSL 准备 LDAP 服务器（若需要）

- 为 SiteMinder 配置 LDAP 插件（若需要）

注意：

如果依据 AD 配置 LDAP，将能够映射用户，但是，将无法配置 AD 单一登录或到数据库的单一登录。但是，LDAP 单一登录方法（如 SiteMinder 和受信任的身份验证）仍将可用。

9.3.2.1 配置 LDAP 主机

建议在配置 LDAP 主机之前安装并运行 LDAP 服务器。

- 1 在导航列表中选择“身份验证”转到 CMC 的“身份验证”管理区域。
- 2 双击“LDAP”。
- 3 如果首次设置 LDAP 身份验证，则单击“启动 LDAP 配置向导”。
- 4 在“添加 LDAP 主机（主机名:端口）”字段中输入 LDAP 主机的名称和端口号（例如，“myserver:123”），单击“添加”，然后单击“下一步”。

提示：

如果要添加可充当故障转移服务器的主机，请重复此步骤，以便添加相同服务器类型的多个 LDAP 主机。如果要删除主机，请突出显示主机名称并单击“删除”。

- 5 从“LDAP 服务器类型”列表中选择服务器类型。

注意：

如果将 LDAP 映射到 AD，请选择“Microsoft Active Directory Application Server”作为服务器类型。

- 6 如果要查看或更改任何 LDAP 服务器属性映射或 LDAP 默认搜索属性，请单击“显示属性映射”。

默认情况下，已经设置了每个支持的服务器类型的服务器属性映射和搜索属性。

- 7 单击“下一步”。
- 8 在“LDAP 基本可分辨名称”字段中，键入 LDAP 服务器的可分辨名称（例如，o=SomeBase），然后单击“下一步”。
- 9 在“LDAP 服务器管理凭据”区域中，为具有目录读权限的用户帐户指定可分辨的名称和密码。不需要管理员凭据。

如果 LDAP 服务器允许匿名绑定，请将此区域留空。BI 平台服务器和客户端将通过匿名登录绑定到主要主机。

- 10 如果在 LDAP 主机上配置了引用，请在“LDAP 引用凭据”区域中输入身份验证信息，然后在“最大引用跃距”字段中输入引用跃距的数量。

如果满足所有以下条件，则必须配置“LDAP 引用凭据”：

- 已将主要主机配置为引用另一台目录服务器，该服务器依据指定基础对条目查询进行处理。
- 已被引用的主机配置为不允许匿名绑定。

- 所引用主机中的组将映射到 BI 平台。

注意：

- 尽管组可以从多台主机中进行映射，但只能设置一个引用凭据集。因此，如果有多台引用主机，则必须在每台主机上创建一个使用相同可分辨名称和密码的用户帐户。
- 如果“最大引用跃距”设置为零，则不会采用引用。

11. 单击“下一步”，
12. 然后选择所用安全套接字层（SSL）身份验证的类型：

- 基本（无 SSL）
- 服务器身份验证
- 相互身份验证

服务器和相互身份验证的细节和前提条件将在后续部分中讨论。要使用其中一种 SSL 类型成功设置 LDAP，请在进行本过程下一步之前查看本文档中的“为 LDAP 服务器或相互身份验证配置 SSL”。

13. 单击“下一步”，并选择 LDAP 单一登录身份验证的方法：

- 基本（无 SSO）
- SiteMinder

14. 单击“下一步”，然后选择将别名和用户映射到 BI 平台帐户的方式。

- a 在“新别名选项”区域中，选择如何将新别名映射到 Enterprise 帐户：

- 将每个添加的 LDAP 别名分配给具有相同名称的帐户

如果您知道用户具有名称相同的 Enterprise 帐户，请使用此选项；也就是说，会将 LDAP 别名分配给现有用户（启用了自动别名创建）。如果用户没有现有 Enterprise 帐户或 Enterprise 和 LDAP 帐户中没有相同的名称，则会将他们作为新用户添加。

- 为每个添加的 LDAP 别名创建一个新帐户

如果要为每个用户创建一个新帐户，请使用此选项。

- b 在“别名更新选项”区域中，选择如何管理 Enterprise 帐户的别名更新。

- 在发生别名更新时创建新的别名

使用此选项可自动为映射到 BI 平台的每个 LDAP 用户创建新别名。系统将为没有 BI 平台帐户的用户，或者为所有用户（如果选择了“为每个添加的 LDAP 别名创建一个新帐户”选项）添加新的 LDAP 帐户。

- 仅当用户登录时才创建新的别名

如果所映射的 LDAP 目录包含许多用户，但其中只有少数用户将使用 BI 平台，请使用此选项。系统不会自动为所有用户创建别名和 Enterprise 帐户。而只会为登录到 BI 平台的用户创建别名（如有必要，也会创建帐户）。

- c 在“新用户选项”区域中指定如何创建新用户：

- 将新用户创建为命名用户

新用户帐户被配置为使用命名用户许可。命名用户许可与特定用户关联，并允许用户基于他们的用户名和密码访问系统。这样，不管连接了多少其他用户，命名用户都能够访问系统。必须为使用此选项创建的每个用户帐户提供一个命名用户许可。

- 将新用户创建为并发用户

新用户帐户被配置为使用并发用户许可。并发许可指定可同时连接到 BI 平台的用户数。这种类型的许可模式非常灵活，因为少量的并发许可就可以支持大量用户。例如，根据用户访问平台的频率和时长，一份 100 个用户的并发许可可能支持 250、500 或 700 个用户。

15. 如果正在设置用户属性映射或计划从 LDAP 服务器中导入电子邮件地址，请执行该步骤。在“属性绑定选项”区域中，为 LDAP 插件指定属性绑定优先级：

- a 单击“导入全名、电子邮件地址和其他属性”框。

这将导入 LDAP 帐户中使用的全名和说明，并将其与用户对象一起存储在系统中。

- b 为“设置 LDAP 属性绑定相对于其他属性绑定的优先级”指定一个选项。

注意：

如果将选项设置为“1”，则在启用了 LDAP 和其他插件（Windows AD 和 SAP）的情况下，LDAP 属性具有优先级。如果该选项设置为“3”，则已启用的其他插件的属性将具有优先级。

16. 单击“完成”。。

相关主题

- 第 228 页上的“[为 LDAP 服务器或相互身份验证配置 SSL](#)”
- 第 232 页上的“[为 SiteMinder 配置 LDAP 插件](#)”

9.3.2.2 管理多台 LDAP 主机

使用 LDAP 和 BI 平台时，可以通过添加多台 LDAP 主机来提高系统的容错能力。系统使用所添加的第一台主机作为主 LDAP 主机。后面的主机被视为故障转移主机。

必须按完全相同的方式配置主要 LDAP 主机和所有故障转移主机，而且每台 LDAP 主机都必须引用要映射的所有其他主机。有关 LDAP 主机和引用的更多信息，请参阅 LDAP 文档。

要添加多台 LDAP 主机，请在使用 LDAP 配置向导配置 LDAP 时输入所有主机（有关详细信息，请参阅）。或者，如果已经配置了 LDAP，请转到中央管理控制台的“身份验证”管理区域，并单击“LDAP”选项卡。在“LDAP 服务器配置摘要”区域中，单击 LDAP 主机的名称，以打开使您能够添加或删除主机的页面。

注意：

- 确保先添加主要主机，然后再添加其余的故障转移主机。

- 如果使用故障转移 LDAP 主机，则无法使用最高级别的 SSL 安全（也就是说，您无法选择“如果服务器证书来自受信任的证书颁发机构，并且该证书的 CN 属性与服务器的 DNS 主机名匹配，则接受服务器证书”。）

相关主题

- 第 224 页上的“[配置 LDAP 身份验证](#)”

9.3.2.3 为 LDAP 服务器或相互身份验证配置 SSL

本部分包含 LDAP 的基于 SSL 的服务器和相互身份验证的详细信息。设置基于 SSL 的身份验证需要执行预备步骤。本部分还介绍了在 CMC 中使用 LDAP 服务器和相互身份验证配置 SSL 的特定信息。假设已经配置了 LDAP 主机，并且选择了以下任一 SSL 身份验证选项：

有关其他信息或有关配置 LDAP 主机服务器的信息，请参考 LDAP 提供商文档。

相关主题

- 第 225 页上的“[配置 LDAP 主机](#)”

9.3.2.3.1 配置 LDAP 服务器或相互身份验证

资源	请在启动此任务之前执行此操作
CA 证书	<p>此操作对于使用 SSL 的服务器身份验证和相互身份验证都是必需的。</p> <ol style="list-style-type: none"> 1 获取一个证书颁发机构 (CA) 以生成 CA 证书。 2 将该证书添加到 LDAP 服务器。 <p>有关更多信息, 请参阅 LDAP 供应商文档。</p>
服务器证书	<p>此操作对于使用 SSL 的服务器身份验证和相互身份验证都是必需的。</p> <ol style="list-style-type: none"> 1 请求并生成一个服务器证书。 2 为该证书授权, 然后将其添加到 LDAP 服务器。
cert7.db 或 cert8.db、key3.db	<p>这些文件是使用 SSL 的服务器身份验证和相互身份验证所必需的。</p> <ol style="list-style-type: none"> 1 从 ftp://ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_6_RTm/ 下载用于生成 cert7.db 或 cert8.db 文件 (取决于具体要求) 的 Certutil 应用程序。 2 将 CA 证书复制到 Certutil 应用程序所在的相同目录。 3 使用以下命令生成 cert7.db 或 cert8.db、key3.db 以及 secmod.db 文件: <pre>certutil -N -d .</pre> 4 使用以下命令将 CA 证书添加到 cert7.db 或 cert8.db 文件: <pre>certutil -A -n <CA_alias_name> -t CT -d . -I cacert.cer</pre> 5 将这三个文件存储在承载 BI 平台的计算机上的一个目录中。
cacerts	<p>具有使用 SSL 的服务器身份验证或相互身份验证的 Java 应用程序 (如 BI 启动板) 需要此文件。</p> <ol style="list-style-type: none"> 1 找到 Java bin 目录中的 keytool 文件。 2 使用以下命令创建 cacerts 文件: <pre>keytool -import -v -alias <CA_alias_name> -file <CA_certificate_name> -trustcacerts -keystore</pre> 3 将 cacerts 文件存储在 cert7.db 或 cert8.db 以及 key3.db 文件所在的相同目录中。
客户端证书	

资源	请在启动此任务之前执行此操作
	<ol style="list-style-type: none"> 为 cert7.db 或 cert8.db 以及 .keystore 文件创建单独的客户端请求： <ul style="list-style-type: none"> 要配置 LDAP 插件，请使用 Certutil 应用程序生成客户端证书请求。 使用以下命令生成客户端证书请求： <pre>certutil -R -s "<client_dn>" -a -o <certificate_request_name> -d .</pre> <client_dn> 包含诸如 CN= 客户端名称、OU=组织单位、O=公司名称、L=城市、ST=省份和 C=国家等信息。 使用 CA 对证书请求进行身份验证。使用以下命令检索证书并将其插入到 cert7.db 或 cert8.db 文件： <pre>certutil -A -n <client_name> -t Pu -d . -I <client_certificate_name></pre> 要实现使用 SSL 的 Java 身份验证： <ul style="list-style-type: none"> 使用 Java bin 目录中的 keytool 实用程序生成客户端证书请求。 使用以下命令生成密钥对： <pre>keytool -genkey -keystore .keystore</pre> 在指定有关客户端的信息后，使用以下命令生成客户端证书请求： <pre>keytool -certreq -file <certificate_request_name> -keystore .keystore</pre> 在证书颁发机构对客户端证书请求进行身份验证后，使用以下命令将该 CA 证书添加到 .keystore 文件： <pre>keytool -import -v -alias <CA_alias_name> -file <ca_certificate_name> -trustcacerts -keystore .keystore</pre> 从证书颁发机构中检索客户端证书请求，然后使用以下命令将其添加到 .keystore 文件： <pre>keytool -import -v -file <client_certificate_name> -trustcacerts -keystore .keystore</pre> 将 .keystore 文件存储在承载 BI 平台的计算机上 cert7.db 或 cert8.db 以及 cacerts 文件所在的相同目录中。

1. 选择要使用的 SSL 安全级别：

如果是首次使用 LDAP 配置向导配置 LDAP 身份验证，则应从“SSL 身份验证的类型”列表中选择“相互身份验证”，然后单击“下一步”。或者，如果正在重新配置 LDAP 身份验证配置，请转到 CMC “身份验证”区域，然后双击“LDAP”。随后将显示“LDAP 服务器配置摘要”页面。单击“SSL 类型”值，然后从“SSL 身份验证的类型”列表中选择“相互身份验证”。

- 始终接受服务器证书

这是最低级别的安全选项。在 BI 平台能够与 LDAP 主机建立 SSL 连接（以便对 LDAP 用户和组进行身份验证）之前，它必须接收来自 LDAP 主机的安全证书。BI 平台不会验证其所接收的证书。

- 如果服务器证书来自受信任的证书颁发机构，则接受服务器证书

这是中等级别的安全选项。在 BI 平台能够与 LDAP 主机建立 SSL 连接（以便对 LDAP 用户和组进行身份验证）之前，它必须接收并验证 LDAP 主机发送的安全证书。要验证证书，系统必须在其证书数据库中找到颁发该证书的证书颁发机构。

- 如果服务器证书来自受信任的证书颁发机构，并且证书的 CN 属性与服务器的 DNS 主机名相匹配，则接受服务器证书

这是最高级别的安全选项。在 BI 平台能够与 LDAP 主机建立 SSL 连接（以便对 LDAP 用户和组进行身份验证）之前，它必须接收并验证 LDAP 主机发送的安全证书。要验证证书，BI 平台必须在其证书数据库中找到颁发该证书的证书颁发机构，且如果已输入 LDAP 主机名作为 ABALONE.rd.crystald.net:389，则必须能够确认服务器证书上的 CN 属性与在向导第一步中的“添加 LDAP 主机”框中输入的 LDAP 主机名完全匹配。（在证书中使用 CN =ABALONE:389 不起作用。）

服务器安全证书上的主机名是主 LDAP 主机的名称。如果选择此选项，则无法使用故障转移 LDAP 主机。

注意：

Java 应用程序将忽略第一个和最后一个设置，并且只有在服务器证书来自受信任的证书颁发机构时，才接受服务器证书。

- 2 在“SSL 主机”框中，键入每台计算机的主机名，然后单击“添加”。

接下来，必须添加使用 BI 平台 SDK 的 BI 平台部署中的每台计算机的主机名。（其中包括运行中央管理服务器的计算机和运行 Web 应用程序服务器的计算机。）

- 3 为添加到列表中的每台 SSL 主机指定 SSL 设置：

- a 从 SSL 列表中选择“默认”。
- b 清除“使用默认值”复选框。
- c 在“证书和密钥数据库文件的路径”框和“密钥数据库的密码”框中键入值。
- d 如果为相互身份验证指定设置，请在“证书数据库中客户端证书的昵称”框中键入一个值。

注意：

默认设置将用于选中了“使用默认值”复选框的任何主机（的任何设置），或用于未将其名称添加至 SSL 主机列表中的任何计算机。

- 4 为不在列表中的每台主机指定默认设置，然后单击“下一步”。

要指定另一台主机的设置，请在左边的列表中选择主机名称，然后在右边的框中键入值。

注意：

默认设置将用于选中了“使用默认值”复选框的（任何主机的）任何设置，或用于未将其名称添加至 SSL 主机列表中的任何计算机。

- 5 选择“基本（无 SSL）”或“SiteMinder”作为 LDAP 单一登录身份验证的方法。
- 6 选择创建新 LDAP 用户和别名的方式。
- 7 单击“完成”。

相关主题

- 第 232 页上的[“为 SiteMinder 配置 LDAP 插件”](#)

9.3.2.4 修改 LDAP 配置设置

使用 LDAP 配置向导配置 LDAP 身份验证之后，用户可以在“LDAP 服务器配置摘要”页面上更改 LDAP 连接参数和成员组。

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“LDAP”。

如果已配置 LDAP 身份验证，则会显示“LDAP 服务器配置摘要”页面。在该页面中，用户可以更改任何连接参数区域或字段，以及在“映射的 LDAP 成员组”区域修改选项。

- 3 删除依据新连接设置不再可访问的当前已映射的组，然后单击“更新”。
用户可以删除已映射的组，操作如下：选择用户组，然后在“映射的 LDAP 成员组”区域单击“删除”按钮。
- 4 更改连接设置，然后单击“更新”。
- 5 如有必要，可更改“新别名选项”、“别名更新选项”和“新用户选项”，然后单击“更新”。
- 6 映射新的 LDAP 成员组，然后单击“更新”。

9.3.2.5 为 SiteMinder 配置 LDAP 插件

本节说明如何配置 CMC 以便将 LDAP 与 SiteMinder 一起使用。SiteMinder 是第三方用户访问和身份验证工具，可以与 LDAP 安全插件一起使用，创建到 BI 平台的单一登录。

若要将 SiteMinder 和 LDAP 用于 BI 平台，需要在以下两处进行配置更改：

- 通过 CMC 更改 LDAP 插件
- BOE.war 文件属性

注意：

确保 SiteMinder 管理员已启用了 4.x 代理的支持。无论使用哪种受支持的 SiteMinder 版本，都必须完成此操作。有关 SiteMinder 和如何安装它的更多信息，请参阅 SiteMinder 文档。

相关主题

- 第 225 页上的[“配置 LDAP 主机”](#)

9.3.2.5.1 用 SiteMinder 配置 LDAP 单一登录

- 1 使用以下一种方法打开“请配置 SiteMinder 设置”屏幕：
 - 在 LDAP 配置向导中“请选择一种 LDAP 单一登录身份验证方法”屏幕上选择“SiteMinder”。
 - 如果已配置 LDAP 并且正添加 SSO，请在可用的 LDAP 身份验证屏幕上选择“单一登录类型”。
- 2 在“策略服务器主机”框中，键入每个策略服务器的名称，然后单击“添加”。
- 3 对于每个策略服务器主机，指定“结算”、“身份验证”和“授权”端口号。
- 4 输入“代理名”的名称和“共享秘密”。在“确认共享秘密”框中重新输入共享秘密。
- 5 单击“下一步”。
- 6 继续配置 LDAP 选项。

9.3.2.5.2 在 BOE.war 文件中启用 LDAP 和 SiteMinder

除了为 LDAP 安全插件指定 SiteMinder 设置外，还必须为 BOE.war 属性指定 SiteMinder 设置。

- 1 转到 BI 平台安装中的安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\ 目录。
- 2 使用“记事本”或任何其他文本编辑实用程序创建一个新文件。
- 3 输入以下语句：

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

- 4 关闭该文件并使用名称 global.properties 保存，不含文件扩展名。
- 5 在同一目录下创建另一个文件。
- 6 输入以下语句：

```
authentication.default=secLDAP  
cms.default=[your cms name]:[the CMS port number]
```

例如：

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

- 7 关闭该文件并使用名称 bilaunchpad.properties 保存。

只有在运行 Web 应用程序服务器的计算机上重新部署修改的 BOE Web 应用程序后，新属性才会生效。使用 WDeploy 在 Web 应用程序服务器上重新部署 WAR 文件。有关使用 WDeploy 的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

9.3.3 映射 LDAP 组

使用 LDAP 配置向导配置了 LDAP 主机之后，便可以将 LDAP 组映射到 Enterprise 组。

映射 LDAP 组之后，可通过在“身份验证”管理区域中单击“LDAP”选项查看这些组。如果配置了 LDAP 身份验证，则“映射的 LDAP 成员组”区域将显示已映射到 BI 平台的 LDAP 组。

注意：

还可以通过 LDAP 安全插件映射要在 BI 平台中进行身份验证的 Windows AD 组。

注意：

如果已依据 AD 配置了 LDAP，此过程将映射 AD 组。

相关主题

- 第 236 页上的“[依据 Windows AD 映射 LDAP](#)”

9.3.3.1 使用 BI 平台映射 LDAP 组

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“LDAP”。

如果配置了 LDAP 身份验证，则会显示 LDAP 摘要页面。

- 3 在“映射的 LDAP 成员组”区域的“添加 LDAP 组（按 cn 或 dn）”字段中，指定 LDAP 组（按通用名称或可分辨名称）；然后单击“添加”。

要添加多个 LDAP 组，请重复此步骤。要删除某个组，请突出显示该 LDAP 组并单击“删除”。

- 4 在“新别名选项”区域中，选择下列选项之一指定将 LDAP 别名映射到 Enterprise 帐户的方式：
 - 将每个添加的 LDAP 别名分配给具有相同名称的帐户

如果您知道用户具有名称相同的现有 Enterprise 帐户，请使用此选项（也就是说，会将 LDAP 别名分配给现有用户，即启用了自动别名创建）。如果用户没有现有 Enterprise 帐户或 Enterprise 和 LDAP 帐户中没有相同的名称，则会将他们作为新 LDAP 用户添加。

- 为每个添加的 LDAP 别名创建一个新帐户

如果要为每个用户创建一个新帐户，请使用此选项。

- 5 在“别名更新选项”区域中，选择下列选项之一来指定是否为所有新用户自动创建 LDAP 别名：

- 在发生别名更新时创建新的别名

使用此选项可自动为映射到 BI 平台的每个 LDAP 用户创建新别名。系统将为没有 BI 平台帐户的用户，或者为所有用户（如果选择了“为每个添加的 LDAP 别名创建一个新帐户”并且单击了“更新”）添加新的 LDAP 帐户。

- 仅当用户登录时才创建新的别名

如果所映射的 LDAP 目录包含许多用户，但其中只有少数用户将使用 BI 平台，请使用此选项。系统不会自动为所有用户创建别名和 Enterprise 帐户。而只会为登录到 BI 平台的用户创建别名（如有必要，也会创建帐户）。

- 6 在“新用户选项”区域中，如果 BI 平台许可基于用户角色，请在以下选项中选择为映射 LDAP 帐户创建的新 Enterprise 帐户指定属性的选项。

- 将新用户创建为命名用户

新用户帐户被配置为使用命名用户许可。命名用户许可与特定用户关联，并允许用户基于他们的用户名和密码访问系统。这样，不管连接了多少其他用户，命名用户都能够访问系统。必须为使用此选项创建的每个用户帐户提供一个命名用户许可。

- 将新用户创建为并发用户

新用户帐户被配置为使用并发用户许可。并发许可指定可同时连接到 BI 平台的用户数。这种类型的许可模式非常灵活，因为少量的并发许可就可以支持大量用户。例如，根据用户访问系统的频率和时长，一份 100 个用户的并发许可可能支持 250、500 或 700 个用户。

- 7 单击“更新”。

9.3.3.2 使用 BI 平台取消映射 LDAP 组

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“LDAP”。

如果配置了 LDAP 身份验证，则会显示 LDAP 摘要页面。

- 3 在“映射的 LDAP 成员组”区域中，选择要删除的 LDAP 组。
- 4 单击“删除”，然后单击“更新”。

该组中的用户将无法访问 BI 平台。

注意：

这只有在用户具有某个 Enterprise 帐户的别名时才会出现例外。要限制访问，请禁用或删除用户的 Enterprise 帐户。

要为所有组拒绝 LDAP 身份验证，请清除“已启用 LDAP 身份验证”复选框，然后单击“更新”。

9.3.3.3 依据 Windows AD 映射 LDAP

如果依据 Windows AD (AD) 配置 LDAP，请注意以下限制：

如果依据 AD 配置 LDAP，将能够映射用户，但是，将无法配置 AD 单一登录或到数据库的单一登录。但是，LDAP 单一登录方法（如 SiteMinder 和受信任的身份验证）仍将可用。

只是 AD 中的默认组成员的用户将无法成功登录。用户必须同时是 AD 中另一个明确创建的组的成员，而且，必须已映射了该组。“域用户”组就是这样一个组的示例。

如果映射的域本地组包含来自目录林中其他域的用户，则来自目录林中其他域的用户将无法成功登录。

来自与指定为 LDAP 主机的 DC 不同的域的通用组中的用户将无法成功登录。

- 无法使用 LDAP 插件在安装了 BI 平台的目录林外部映射来自 AD 目录林的用户和组。
- 无法在 AD 中的“域用户”组中进行映射。
- 无法映射计算机本地组。

如果使用的是全局目录域控制器，在依据 AD 映射 LDAP 时还需要另外考虑以下因素：

情况	考虑因素
指向全局目录域控制器时使用多个域	<p>可在以下项目中映射：</p> <p>子域上的通用组，</p> <p>包含来自子域的通用组的同一域上的组，以及</p> <ul style="list-style-type: none"> 交叉域上的通用组。 <p>无法在以下项目中映射：</p> <ul style="list-style-type: none"> 子域上的全局组， 子域上的本地组， 包含来自子域的全局组的同一域上的组，以及 交叉域全局组。 <p>通常，如果组是通用组，它将支持来自交叉域或子域的用户。如果其他组包含来自交叉域或子域的用户，将不会映射这些组。在所指向的域内，可以映射域的本地组、全局组和通用组。</p>
在通用组中映射	<p>要在通用组中映射，必须指向全局目录域控制器。还应使用端口号 3268，而不是默认的 389。</p>

- 如果要使用多个域但未指向全局目录域控制器，则无法在来自交叉域或子域的任何类型的组中映射。只能在来自所指向特定域的所有类型的组中映射。

9.3.3.4 使用 LDAP 插件为 SAP HANA 数据库配置 SSO

本节为管理员提供在运行于 SUSE Linux 11 之上的 BI 平台与 SAP HANA 数据库之间设置和配置单一登录（SSO）所需的步骤。使用 Kerberos 的 LDAP 身份验证允许在运行于 Linux（具体而言，就是 SUSE）之上的 BI 平台上对 AD 用户进行身份验证。该方案还支持作为报表数据库的 SAP HANA 的单一登录。

注意：

有关如何设置 SAP HANA 数据库的信息，请参阅 SAP HANA 数据库 – 服务器安装和更新指南。有关如何为 SAP HANA 设置数据访问组件的信息，请参阅《数据访问指南》。

实施概览

为使 Kerberos SSO 能够正常工作，以下组件必须就位。

组件	要求
域控制器	承载于运行 Active Directory 安装的计算机上，以使用 Kerberos 身份验证。
中央管理服务器	在运行 SUSE Linux Enterprise 11 (SUSE) 的计算机上安装并运行。
Kerberos V5 客户端	连同所需的实用程序和库一起安装在 SUSE 主机上。 注意： 请使用最新版本的 Kerberos V5 客户端。将 bin 和 lib 文件夹添加到 PATH 和 LD_LIBRARY_PATH 环境变量中。
LDAP 身份验证插件	已在 SUSE 主机上启用。
Kerberos 登录配置文件	已在承载 Web 应用程序服务器的计算机上创建。

实施 workflow

必须执行以下任务，以支持 BI 平台用户通过 JDBC 使用 Kerberos 身份验证单一登录 SAP HANA。

- 。 1 设置 AD 主机。
- 。 2 为 SUSE 主机以及 AD 主机上的 BI 平台创建帐户和 keytab 文件。
- 。 3 在 SUSE 主机上安装 Kerberos 资源。
- 。 4 为 Kerberos 身份验证配置 SUSE 主机。
- 。 5 在 LDAP 身份验证插件中配置 Kerberos 身份验证选项。
- 。 6 为 Web 应用程序主机创建 Kerberos 登录配置文件。

9.3.3.4.1 设置域控制器

可能需要在 SUSE 主机与域控制器之间设置信任关系。如果 SUSE 主机位于 Windows 域控制器中，则不必设置信任关系。但是，如果 BI 平台部署与域控制器位于不同域中，则可能需要在 SUSE Linux 计算机与域控制器之间设置信任关系。这需要执行以下操作：

- 1 为运行 BI 平台的 SUSE 计算机创建用户帐户。
- 2 创建主机服务主体名称 (SPN)。

注意：

SPN 的格式应遵照 Windows AD 的约定：host/hostname@DNS_REALM_NAME。/hostname 应使用小写的全限定域名。DNS_REALM_NAME 应以大写字母指定。

3 运行 Kerberos keytab 设置命令 ktpass 将 SPN 与用户帐户相关联:

```
c:\> ktpass -princ host/hostname@DNS_REALM_NAME-mapuser username -pass Password1 -crypto RC4-HMAC-NT -out usernamebase.keytab
```

必须在承载域控制器的计算机上执行以下步骤。

- 1 为运行 BI 平台的服务创建用户帐户。
- 2 在“用户帐户”页面上，右击该新服务帐户并选择“属性” > “委派”。
- 3 选择“信任此用户作为任何服务的委派(仅 Kerberos)”。
- 4 运行 Kerberos keytab 设置命令 ktpass 为该新服务帐户创建一个 SPN 帐户:

```
c:\>ktpass -princ sianame/service_name@DNS_REALM_NAME -mapuser service_name -pass password -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT -out sianame.keytab
```

注意:

SPN 的格式应遵照 Windows AD 的约定: sianame/service_name@DNS_REALM_NAME。以小写字母指定 service name, 否则 SUSE 平台可能无法解析它。DNS_REALM_NAME 应以大写字母指定。

参数	说明
-princ	为 Kerberos 身份验证指定主体名称。
-out	指定要生成的 Kerberos keytab 文件的名称。这应与 -princ 中使用的 sianame 相匹配。
-mapuser	指定 SPN 映射到的用户帐户的名称。服务器智能代理在此帐户上运行。
-pass	指定服务帐户使用的密码。
-ptype	指定主体类型。 -ptype KRB5_NT_PRINCIPAL
-crypto	指定服务帐户使用的加密类型: -crypto RC4-HMAC-NT

这样就生成了 SUSE 计算机与域控制器之间的信任关系所需的 keytab 文件。

必须将 keytab 文件传输至 SUSE 计算机并将其存储在 /etc 目录中。

9.3.3.4.2 设置 SUSE Linux Enterprise 11 计算机

在运行 BI 平台的 SUSE Linux 计算机上设置 Kerberos 需要以下资源:

- 在域控制器上创建 keytab 文件。必须为 BI 平台服务创建 keytab 文件。建议为 SUSE 主机创建 keytab，尤其是对于 BI 平台主机和域控制器位于不同域中的情况。
- 必须在 SUSE 主机上安装最新版本的 Kerberos V5 库（包括 Kerberos 客户端）。必须将这些二进制文件的位置添加到 PATH 和 LD_LIBRARY_PATH 环境变量中。要验证是否正确安装和配置了 Kerberos 客户端，请确保 SUSE 主机上存在以下实用程序和库：

- kinit
- ktutil
- kdestroy
- klist
- /lib64/libgssapi_krb5.so.2.2
- /lib64/libkrb5.so.3.3
- /lib/libkrb5support.so.0.1
- /lib64/libk5crypto.so.3
- /lib64/libcom_err.so.2

提示：

运行 `rpm -qa | grep krb` 以检查这些库的版本。有关最新的 Kerberos 客户端、库以及 Unix 主机配置的信息，请参阅 <http://web.mit.edu/Kerberos/krb5-1.9/krb5-1.9.2/doc/krb5-in-stall.html#Installing%20Kerberos%20V5>。

当在 SUSE 主机上获得所有必需资源后，请按照以下说明设置 Kerberos 身份验证。

注意：

要执行这些步骤，必须具有 root 权限。

- 1 要合并 keytab 文件，请运行以下命令：

```
> ktutil
ktutil: rkt <susemachine>.keytab
ktutil: rkt <BI platform service>.keytab
ktutil: wkt /etc/krb5.keytab
ktutil:q
```

- 2 编辑 /etc/krb5.conf 文件以引用域控制器（在 Windows 平台上）作为 Kerberos 域控制器（KDC）。请参考以下示例：

```
[domain_realm]
.name.mycompany.corp = DOMAINNAME.COM
.name.mycompany.corp = DOMAINNAME.COM

[libdefaults]
forwardable = true
default_realm = DOMAINNAME.COM
default_tkt_encypes = rc4-hmac
default_tgs_encypes = rc4-hmac

[realms]
DOMAINNAME.COM = {
    kdc = machinename.domainname.com
}
```

注意：

krb5.conf 文件包含 Kerberos 配置信息，其中包括相关 Kerberos 系列的 KDC 和服务器的位置、Kerberos 应用程序以及主机名到 Kerberos 系列的映射。通常，krb5.conf 文件安装在 /etc 目录下。

- 3 将域控制器添加到 `/etc/hosts`，以便 SUSE 主机能够找到 KDC。
- 4 运行 `/usr/local/bin` 目录中的 `kinit` 程序以验证是否已正确设置 Kerberos。验证 AD 帐户用户帐户是否能够登录 SUSE 计算机。

提示：

KDC 应发出一个权证授予权证（TGT），后者可在缓存中查看。可以使用 `klist` 程序查看 TGT。

示例：

```
> kinit <AD user>
Password for <AD user>@<domain>: <AD user password>

> klist
Ticket cache: FILE:/tmp/krb5cc_0Default principal: <AD user>@<domain>
Valid starting Expires Service principal08/10/11 17:33:43 08/11/11 03:33:46 krbtgt/<domain>@<domain>renew until 08/11/11 17:33:43
Kerberos 4 ticket cache: /tmp/tkt0klist: You have no tickets cached

>klist -k
Keytab name: FILE:/etc/krb5.keytabKVNO Principal-3hdb/<FQDN>@<Domain>
```

此外，还应使用 `kinit` 测试 SPN。

9.3.3.4.3 为 LDAP 配置 Kerberos 身份验证选项

在为 LDAP 配置 Kerberos 身份验证之前，必须先启用并配置 BI 平台 LDAP 身份验证插件以连接到 AD 目录。要使用 LDAP 身份验证，需要首先确保已设置了相应的 LDAP 目录。

注意：

运行 LDAP 配置向导时，必须指定 Microsoft Active Directory Application Server 并提供所需配置详细信息。

启用并将 LDAP 身份验证连接到 Microsoft Active Directory Application Server 后，“LDAP 服务器配置摘要”页面上将显示“启用 Kerberos 身份验证”区域。使用此区域配置 Kerberos 身份验证，这是从部署在 SUSE 上的 BI 平台单一登录 SAP HANA 数据库所必需的操作。

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“LDAP”。

将显示“LDAP 服务器配置摘要”页面，从中可以修改任何连接参数或字段。

- 3 要配置 Kerberos 身份验证，请在“启用 Kerberos 身份验证”区域中执行以下步骤：
 - a 单击“启用 Kerberos 身份验证”。
 - b 单击“高速缓存安全上下文（对于数据库的 SSO 为必需）”。

注意：

SAP HANA 单一登录尤其需要启用缓存安全上下文。

- g 在“服务主体名称”中为 BI 平台帐户指定服务主体名称（SPN）。
指定 SPN 时的格式为 `sianame/service@DNS_REALM_NAME`，其中

sianame	服务器智能代理名称
service	用于运行 BI 平台的服务帐户的名称
DNS_REALM_NAME	大写的域控制器的域名

提示：

指定 SPN 时，请注意 `sianame/service` 区分大小写。

- d 在“默认 Kerberos 域”中指定域控制器的域。
e 在“用户主体名称”中指定 `userPrincipalName`。
LDAP 身份验证应用程序使用该值提供 Kerberos 所需的用户 ID 值。指定的值应与创建 keytab 文件时提供的值相匹配。

- 4 单击“更新”以提交并保存所做更改。

这样就配置了 Kerberos 身份验证选项以引用 AD 目录中的用户帐户。

需要创建 Kerberos 登录配置文件 - `bscLogin.conf` - 以启用 Kerberos 登录和单一登录。

相关主题

- 第 224 页上的“[配置 LDAP 身份验证](#)”

9.3.3.4.4 创建 Kerberos 登录配置文件

要启用 Kerberos 登录和单一登录，需要在承载 BI 平台 Web 应用程序服务器的计算机上添加一个登录配置文件。

- 1 创建一个名为 `bscLogin.conf` 文件并将其存储在 `/etc` 目录中。

注意：

可以将此文件存储在其他位置，然而，如果这样做，则需要在 `java` 选项中指定其位置。建议 `bscLogin.conf` 和 Kerberos keytab 文件驻留在相同目录下。在分布式部署中，必须为承载 Web 应用程序服务器的每台计算机添加一个 `bscLogin.conf` 文件。

- 2 将以下代码添加到登录 bscLogin.conf 配置文件中：

```
com.businessobjects.security.jgss.initiate {
com.sun.security.auth.module.Krb5LoginModule required;
};
com.businessobjects.security.jgss.accept {
com.sun.security.auth.module.Krb5LoginModule required
storeKey=true
useKeyTab=true
keyTab="/etc/krb5.keytab"
principal="principal name";
};
```

注意：

以下部分尤其是单一登录所需的：

```
com.businessobjects.security.jgss.accept {
com.sun.security.auth.module.Krb5LoginModule required
storeKey=true
useKeyTab=true
keyTab="/etc/krb5.keytab"
principal="principal name";
};
```

- 3 保存并关闭文件。

9.3.3.5 新 LDAP 帐户疑难解答

- 如果创建新的 LDAP 用户帐户，并且此帐户不属于映射到 BI 平台的某个组帐户，请将该组映射到 BI 平台，或将新的 LDAP 用户帐户添加到一个已映射到该系统的组。
- 如果创建新的 LDAP 用户帐户，并且该帐户属于映射到 BI 平台的组帐户，请刷新用户列表。

相关主题

- 第 224 页上的[“配置 LDAP 身份验证”](#)
- 第 234 页上的[“映射 LDAP 组”](#)

9.4 Windows AD 身份验证

9.4.1 使用 Windows AD 身份验证

9.4.1.1 Windows AD 支持要求和初始设置

本节可指导您配置 Windows Active Directory (AD) 身份验证，以便在 BI 平台上使用。所有需要执行的端到端 workflows 均伴有验证测试和前提检查。

支持要求

要简化 BI 平台的 Windows AD 身份验证，应记住以下支持要求。

- CMS 必须始终安装在受支持的 Windows 平台上。
- 对于 Kerberos 和 NTLM 身份验证，尽管 Windows 2008 都是支持的平台，但特定的 BI 平台应用程序仅可使用特定的身份验证方法。例如，BI 启动板和中央管理控制台等应用程序仅支持 Kerberos。

建议 AD 设置 workflow

要手动初始设置 AD 身份验证和 BI 平台，请使用下列 workflow：

- 1 设置域控制器。
- 2 配置 CMC 的 AD 身份验证
- 3 配置服务器智能代理 (SIA) 的 AD 用户帐户
- 4 为 Windows AD 身份验证及 Kerberos 配置 Web 应用程序服务器。

注意：

无论是否要求单一登录 (SSO) 均请使用此 workflow。以下部分描述的 workflow 使您能够手动（使用 AD 用户名和密码）登录 BI 平台。成功配置手动 AD 身份验证后，将向您提供一个详细的部分引导您完成 AD 验证设置 SSO 的整个过程。

9.4.2 准备域控制器

9.4.2.1 为使用 Kerberos 的 AD 身份验证设置服务帐户

若要配置 BI 平台使其同 Windows AD (Kerberos) 身份验证一起工作，则需要一个服务帐户。可以创建新的域帐户或使用现有的域帐户。该服务帐户将用于运行 BI 平台服务器。该帐户设置完成后，您需要为该帐户设置一个 SPN。该 SPN 用于将 AD 用户组导入 BI 平台。

注意：

如果 AD 要使用 SSO，您需要在稍后再次访问服务帐户设置，为该帐户授予合适的权限，并将其配置用于约束委派。

9.4.2.1.1 在 Windows 2008 域上设置服务帐户

若要使用 Kerberos 协议成功启用 Windows AD 身份验证，您需要设置一个新的服务帐户。该服务帐户将主要用于允许给定 AD 组中的用户登录 BI 启动板。下列任务在 AD 域控制器计算机上执行。

- 1 在主域控制器上创建带有密码的新服务帐户。
- 2 使用 `setspn -a` 命令将服务主体名称 (SPN) 添加到在步骤 1 中创建的服务帐户中。为服务帐户指定服务主体名称 (SPN)，并为部署了 BI 启动板的计算机指定服务器、全限定域服务器和 IP 地址。

例如：

```
setspn -a BICMS/service_account_name.domain.com serviceaccountname
setspn -a HTTP/servername servicename
setspn -a HTTP/servername.domain.com servicename
setspn -a HTTP/<ip address of server> servicename
```

BICMS 是运行 SIA 的计算机名称，servername 是部署了 BI 启动板的服务器名称，其全限定域名为 servernamedomain。

- 3 运行 `setspn -l servicename` 验证服务主体名称已添加到服务帐户中。
命令输出应包含所有已注册的 SPN，如下所示：

```
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
```

输出样本如下：

```
C:\Users\Admin>setspn -L bossosvcacct  
Registered ServicePrincipalNames for  
CN=bossosvcacct,OU=svcaccts,DC=domain,DC=com:  
    BICMS/bossosvcacct.domain.com  
    HTTP/Tomcat HTTP/Tomcat.domain.com  
    HTTP/Load_Balancer.domain.com
```

创建后，需要为该服务帐户授权并将其添加到服务器的本地 Administrators 组。在下一部分中，SPN 将用于导入 AD 组。

9.4.3 配置 CMC 的 AD 身份验证

9.4.3.1 Windows AD 安全插件

利用 Windows AD 安全插件，可以将用户帐户和组从 AD 2008 用户数据库映射到 BI 平台。该插件还使系统能够验证指定 AD 身份验证的所有登录请求。系统将依据 AD 用户数据库对用户进行身份验证，并在中央管理服务器（CMS）授予这些用户进行活动会话的权限之前，对他们在所映射的 AD 组中的成员资格进行验证。您可使用插件对导入的 AD 组进行更新配置。

Windows AD 安全插件允许进行以下配置：

- Windows AD 身份验证及 Kerberos
- Windows AD 身份验证及 NTLM
- Windows AD 身份验证及 SiteMinder（针对单一登录）

AD 安全插件与运行于本机模式或混合模式下的 AD 2008 域兼容。

在映射 AD 用户和组后，它们将能够使用“Windows AD”身份验证选项访问 BI 平台客户端工具。

- 只有当 CMS 在 Windows 上运行时，Windows AD 身份验证才会工作。要使数据库单一登录工作，报表生成服务器也必须在 Windows 上运行。否则，所有其他服务器和服务可在 BI 平台支持的所有平台上运行。
- BI 平台的 Windows AD 插件支持多个目录林中的域。

9.4.3.2 映射 AD 用户和组

在将 AD 用户组导入 BI 平台之前必须完成下列前提操作：

- 已在 BI 平台的域控制器上创建服务帐户。该帐户将用于运行 BI 平台服务器。

注意：

要使用 Vintela 单一登录 (SSO) AD 身份验证，必须提供一个为该用途而配置的 SPN。下列步骤用于为 BI 平台配置手动 AD 身份验证。完成 AD 身份验证手动配置后，请参照本章节中的“单一登录设置”部分了解如何为 AD 身份验证配置添加 SSO 的详细信息。

- 已验证包含运行 SIA 的计算机名称的 SPN 已被添加至服务帐户。

下面的步骤 1 到 11 是将 AD 组导入 BI 平台的必需步骤。

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“Windows AD”。
- 3 选中“启用 Windows Active Directory (AD)”复选框。
- 4 在“AD 配置摘要”区域中，单击“AD 管理名称”旁边的链接。

注意：

在配置 Windows AD 插件之前，该链接显示为引号。保存配置后，该链接将用 AD 管理名称进行填充。

- 5 输入已启用域用户帐户的名称和密码。

管理凭据可使用以下格式之一：

- NT 名称 (域名\用户名)
- UPN (用户@DNS_域_名称)

BI 平台使用此帐户查询 AD 中的信息。平台不会修改、添加或删除来自 AD 的内容。由于仅读取信息，因此只需具有相应的权限。

注意：

如果用于读取 AD 目录的帐户成为无效帐户，例如：如果帐户密码更改或过期，或者帐户被禁用，则 AD 身份验证将会中断。

- 6 在“默认 AD 域”字段中输入 AD 域。

域必须以大写字母表示的完整域名指定，或是大多数用户将由其登录 BI 平台的子域名。该域应该与在用来配置应用程序服务器的 Kerberos 配置文件中指定的默认域相同。可以映射默认域中的组，而不必指定域名前缀。如果输入默认 AD 域名，默认域中的用户在通过 AD 身份验证登录到 BI 平台时不必指定 AD 域名。

- 7 在“映射的 AD 成员组”区域中，使用以下格式之一在“添加 AD 组 (域\组)”框中输入 AD 域\组以映射组：
 - 安全帐户管理器帐户名称 (SAM)，也称为 NT 名称 (域名\组名)

- DN (cn=组名,, dc=域名, dc=com)

注意:

如果要映射本地组, 只能使用 NT 名称格式: \\服务器名称\组名。AD 不支持本地用户; 属于某个映射的本地组的本地用户不会映射到 BI 平台。因此他们不能访问系统。

提示:

手动登录 BI 启动板时, 来自其他域的用户必须在用户名后以大写字母附加域名。例如: 在下面的示例中, CHILD.PARENTDOMAIN.COM 便是域:

```
user@CHILD.PARENTDOMAIN.COM
```

- 8 单击“添加”。

组随即添加到“映射的 AD 成员组”下的列表中。

- 9 在“身份验证选项”下, 选择“使用 Kerberos 身份验证”。

10. 在“服务主体名称”框中, 输入为运行 BI 平台服务器所创建的映射至服务帐户的 SPN。

注意:

必须为运行 SIA 的服务帐户指定 SPN。例如: BICMS/bossosvcacct.domain.com。

11. 单击“更新”。

警告:

若用户和/或组未正确映射, 请勿继续操作! 要解决特定的 AD 组映射问题, 请参见 SAP 注释 1631734。

注意:

若已成功映射 AD 组帐户, 且不希望配置 AD 身份验证选项或 AD 组更新, 请跳过步骤 12 至 19。在成功设置手动 AD Kerberos 身份验证后, 可以配置这些可选设置。

12. 若数据库需要 SSO 配置, 请选择“高速缓存安全上下文”。

注意:

如果这是您初次进行 AD 身份验证, 建议先完成手动 AD 身份验证设置, 再考虑 SSO 所需的额外配置。

13. 若 AD 身份验证配置需要 SSO, 请选择“为选定身份验证模式启用单一登录”。

14. 在“凭据的同步”区域中, 选择一个选项启用并更新 AD 用户的数据源登录凭据。

该选项将实现用户当前的登录凭据与数据源之间的同步, 从而使用户能够在未登录 BI 平台且 Kerberos SSO 不可用时运行计划报表。

15. 在“AD 别名选项”区域中, 指定如何向 BI 平台添加和更新新别名。

- a 在“新别名选项”区域中, 选择下列选项之一将新别名映射到 Enterprise 帐户:

- 将每个新的 AD 别名分配给同名的现有用户帐户

如果您知道用户具有名称相同的现有 Enterprise 帐户, 请选择此选项; 也就是说, 会将 AD 别名分配给现有用户 (启用了自动别名创建)。如果用户没有现有 Enterprise 帐户或 Enterprise 和 AD 帐户中没有相同的名称, 则会将他们作为新用户添加。

- 为每个新的 AD 别名创建新的用户帐户

如果要为每个用户创建一个新帐户, 请选择此选项。

- b 在“别名更新选项”区域中，选择下列选项之一来管理 Enterprise 帐户的别名更新：
- 在发生别名更新时创建新的别名
使用此选项可自动为映射到 BI 平台的每个 AD 用户创建新别名。系统会为没有 BI 平台帐户的用户，或为所有用户（如果选择了“为每个新的 AD 别名创建新的用户帐户”并单击了“更新”）添加新 AD 帐户。
 - 仅当用户登录时才创建新的别名
如果所映射的 AD 目录包含许多用户，但其中只有少数用户将使用 BI 平台，请使用此选项。平台不会自动为所有用户创建别名和 Enterprise 帐户。而只会为登录到 BI 平台的用户创建别名（如有必要，也会创建帐户）。
- c 在“新用户选项”区域中，选择创建新用户的选项：
- 将新用户创建为命名用户
新用户帐户被配置为使用命名用户许可。命名用户许可与特定用户关联，并允许用户基于用户名和密码访问 BI 平台。这样，不管连接了多少用户，命名用户都能够访问系统。必须为使用此选项创建的每个用户帐户提供一个命名用户许可。
 - 将新用户创建为并发用户
新用户帐户被配置为使用并发用户许可。并发许可指定可同时连接到 BI 平台的用户数。这种类型的许可模式非常灵活，因为少量的并发许可就可以支持大量用户。例如，根据用户访问系统的频率和时长，一份 100 个用户的并发许可可能支持 250、500 或 700 个用户。
16. 配置如何计划 AD 别名更新：单击“计划”。
- 在“计划”对话框中，从“运行对象”列表中选择重复发生。
 - 根据需要设置其他计划选项和参数。
 - 单击“计划”。
发生别名更新时，组信息也将更新。
17. 在“属性绑定选项”区域中，为 AD 插件指定属性绑定优先级：
- 选择“导入全名、电子邮件地址和其他属性”复选框。
这将导入 AD 帐户中使用的全名和说明，并将其与用户对象一起存储在 BI 平台中。
 - 为“Set priority of AD attribute binding relative to other attributes binding”（设置与其他属性绑定相关的 AD 属性绑定的优先级）指定一个选项。
如果该选项设置为“1”，则 AD 属性在启用 AD 和其他插件（LDAP 和 SAP）时具有优先权。如果选项设置为“3”，则已启用的其他插件的属性具有优先级。
18. 在“AD 组选项”区域中，配置 AD 组更新：
- 单击“计划”。
将出现“计划”对话框。
 - 从“运行对象”列表中选择重复发生。
 - 根据需要设置其他计划选项和参数。
 - 单击“计划”。
系统将计划更新并根据指定的计划运行更新。AD 组帐户的下一计划更新显示在“AD 组选项”中。
19. 在“按需 AD 更新”区域中，选择以下其中一个选项：

- 立即更新 AD 组

如果在单击“更新”时要开始更新所有已计划的 AD 组，请选择该选项。下一个计划的 AD 组更新将在“AD 组选项”下列出。

- 立即更新 AD 组和别名

如果在单击“更新”时要开始更新所有已计划的 AD 组 and 用户别名，请选择该选项。接下来的已计划更新将在“AD 组选项”和“AD 别名选项”下列出。

- 不立即更新 AD 组和别名

在单击“更新”时不会更新 AD 组或用户别名。

20. 单击“更新”，然后单击“确定”。

要验证是否已导入 AD 用户帐户，请转到“CMC” > “用户和组” > “组层次结构”，然后选择已映射的 AD 组来查看该组用户。随即显示 AD 组中当前和嵌套的用户。

相关主题

- 第 254 页上的[“创建 Kerberos 配置文件”](#)

9.4.3.3 计划 Windows AD 组的更新

BI 平台允许管理员为 AD 组 and 用户别名计划更新。此功能可用于通过 Kerberos 或 NTLM 进行 AD 身份验证。CMC 还允许查看执行上次更新的时间和日期。

注意：

要在 BI 平台上使用 AD 身份验证，必须配置如何为 AD 组和别名计划更新。

在计划更新时，可以从下表中概述的重复发生模式中进行选择：

重复发生模式	说明
每小时	更新将每小时运行一次。可以指定将在何时开始，以及开始和结束日期。
每天	更新将每天或每隔指定天数运行一次。可以指定对象将在何时运行，以及开始和结束日期。
每周	更新将每周运行一次。它可以一周运行一次或多次。可以指定对象运行的具体日期和时间，以及开始和结束日期。
每月	更新将每月或每隔几个月运行一次。可以指定将在何时运行，以及开始和结束日期。

重复发生模式	说明
每月的第 N 天	更新将在每月的特定一天运行。可以指定将在月中的哪一天以及在何时运行，也可以指定开始和结束日期。
每月的第一个星期一	更新将在每月的第一个星期一运行。可以指定将在何时运行，以及开始和结束日期。
每月的最后一天	更新将在每月的最后一天运行。可以指定将在何时运行，以及开始和结束日期。
每月第 N 周的第 X 天	更新将在月中某指定周的指定一天运行。可以指定将在何时运行，以及开始和结束日期。
日历	更新将在以前已创建的日历中指定的日期运行。

计划 AD 组的更新

BI 平台依赖 AD 获取用户和组信息。为了最大程度地减小发送到 AD 的查询量，AD 插件将高速缓存有关组、组之间的相互关系以及组与其用户成员资格之间的关系的信息。当未定义特定计划时，不会运行更新。

必须使用 CMC 配置组更新刷新的重复发生。此计划应反映组成员资格信息的修改频率。

计划 AD 用户别名更新

可为用户对象创建 AD 帐户别名，以允许该用户使用 AD 凭据登录至 BI 平台。AD 帐户的更新会通过 AD 插件传播给 BI 平台。在 AD 中创建、删除或禁用的帐户在 BI 平台中会相应地被创建、删除或禁用。

如果不计划 AD 别名更新，则只有在以下情况下才会发生更新：

- 用户登录；AD 别名将更新。
- 管理员在 CMC 的“按需 AD 更新”区域中选择“立即更新 AD 组和别名”选项。

注意：

不会在用户别名中存储 AD 密码。

9.4.4 配置 BI 平台服务以运行 SIA

9.4.4.1 在 BI 平台服务账号下运行 SIA

为支持用于 BI 平台的 AD Kerberos 身份验证，您必须授予服务帐户充当操作系统一部分的权限。必须在运行包含中央管理服务器（CMS）的服务器智能代理（SIA）的每台计算机上完成此操作。

若要使服务帐户运行/ SIA，您必须配置本部分所描述的特定操作系统设置。

注意：

如果需要对数据库进行单一登录，SIA 必须包含以下服务器：

Crystal Reports 处理服务器

报表应用程序服务器

Web Intelligence 处理服务器

9.4.4.2 配置 SIA 以在服务帐户下运行

在配置 SIA 帐户以在 BI 平台服务帐户下运行之前，必须完成下列操作：

- 已在域控制器上创建用于 BI 平台的服务帐户。
- 已验证所需服务主体名称（SPN）已添加至服务帐户。
- 已成功将 AD 用户组映射至 BI 平台。

为任何运行服务帐户所用服务的服务器智能代理（SIA）执行此任务。

- 1 要启动 CCM，请选择“程序” > “SAP Business Intelligence” > “SAP BusinessObjects BI 平台” > “中央配置管理器”。

将出现 CCM 主页。

- 2 在 CCM 中，右击服务器智能代理（SIA）并选择“停止”。

注意：

如果停止 SIA，则将停止 SIA 托管的所有服务。

- 3 右击 SIA 并选择“属性”。
- 4 清除“系统帐户”复选框。
- 5 键入服务帐户凭据（域名\服务名）并单击“确定”。

服务帐户必须在运行 SIA 的计算机上获得下列权限：

- 帐户必须明确具有“以操作系统方式执行”的权限。
- 帐户必须明确具有“作为服务登录”的权限。
- 针对 BI 平台安装文件夹的完全控制权限。
- 针对系统注册表中的 HKEY_LOCAL_MACHINE\SOFTWARE\SAP BusinessObjects 的完全控制权限。

- 6 单击“开始” > “控制面板” > “管理工具” > “本地安全策略”。
- 7 展开“本地策略”，然后单击“用户权利指派”。
- 8 双击“作为操作系统的一部分”。

9. 单击“添加”，输入创建的服务帐户的名称，然后单击“确定”。
10. 在运行 BI 平台服务器的每台计算机上重复上面的步骤。

注意：

选择了“以操作系统方式操作”后，务必要检查最终有效权限。通常，您将需要重新启动服务器以进行此操作。如果重新启动服务器后此选项仍然未启用，则本地策略设置已被域策略设置覆盖。

11. 重新启动 SIA。
12. 如有必要，对运行有必须配置的服务的每个 SIA 重复步骤 1 到 5。

现在应该可以使用 AD 凭据登录 CCM 了。

9.4.4.3 在 CCM 上测试 AD 凭据

在执行该任务之前，您需将 AD 用户组成功映射至 BI 平台。

1. 打开 CCM 并单击“管理服务器”图标。
 2. 确保“系统”字段的信息显示正确。
 3. 在身份验证选项列表中选择“Windows AD”。
- 登录对话框将随即打开。
4. 使用已映射至 BI 平台的 AD 组中现有的 AD 帐户登录。

注意：

如果您正使用一个未驻留在默认域中的 AD 帐户，请使用域\用户名 登录。

此时，不得出现任何错误消息。在继续下一部分之前，您必须能够使用已映射的 AD 帐户通过 CCM 登录。

提示：

如果收到错误消息，请转到“CMC” > “身份验证” > “Windows AD”。在“身份验证选项”下，将“使用 Kerberos 身份验证”更改为“使用 NTLM 身份验证”，然后单击“更新”。重复上述步骤 1-4。如果有效果，则表示 Kerberos 配置有问题。

9.4.5 配置用于 AD 身份验证的 Web 应用程序服务器

9.4.5.1 为 Windows AD 身份验证 (Kerberos) 准备应用程序服务器

对于具体应用程序服务器，为 Web 应用程序服务器配置 Kerberos 的流程会略有不同。不过，Kerberos 的配置流程一般都涉及以下步骤：

- 创建 Kerberos (krb5.ini) 配置文件。
- 创建 JAAS 登录 bscLogin.conf 配置文件。

注意：

SAP NetWeaver 7.3 Java 应用程序服务器无需此步骤。但是，需要向 SAP NetWeaver 服务器中添加 LoginModule。

- 修改应用程序服务器的 Java 选项。
- 覆盖用于 Windows AD 身份验证的 BOE.war 文件属性。
- 重新启动 Java 应用程序服务器。

本部分包含用于下列应用程序服务器的 Kerberos 配置详细信息：

- Tomcat
- WebSphere
- WebLogic
- Oracle Application Server
- SAP NetWeaver 7.3

9.4.5.1.1 创建 Kerberos 配置文件

9.4.5.1.1.1 创建 Kerberos 配置文件

继续处理前，请确保已执行下列前提任务：

- 已在域控制器上创建用于 BI 平台的服务帐户。
- 已验证服务主体名称 (SPN) 已添加至服务帐户。
- 已成功将 AD 用户组映射至 BI 平台。
- 已在 CCM 上测试 AD 凭据。

如果使用 SAP NetWeaver 7.3、Tomcat、Oracle Application Server、WebSphere 或 WebLogic 作为部署 BI 平台的 Web 应用程序服务器，请按下列步骤创建 Kerberos 配置文件。

- 1 创建文件 krb5.ini（如果该文件不存在），并将其存储在 Windows 的 C:\Windows 下。

注意：

- 如果应用程序服务器安装在 Unix 上，则应使用以下目录：

Solaris: /etc/krb5/krb5.conf

Linux: /etc/krb5.conf

- 可以将此文件存储在其他位置中，但是如果这样做，将需要在 java 选项中指定其位置。有关 krb5.ini 的更多信息，请转到 <http://docs.sun.com/app/docs/doc/816-0219/6m6njqb94?a=view>。

- 2 在 Kerberos 配置文件中添加以下所需信息：

```
[libdefaults]
default_realm = DOMAIN.COM
dns_lookup_kdc = true
dns_lookup_realm = true
default_tkt_encypes = rc4-hmac
default_tgs_encypes = 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 =
```

注意：

下表对关键参数进行了说明。

DOMAIN.COM	域的 DNS 名称，必须采用 FQDN 格式以大写形式输入。
kdc	域控制器的主机名。
[capath]	定义位于其他 AD 目录林中的域间的信任。在上面的示例中，DOMAIN2.COM 是外部目录林中的域，它具有可传递给 DOMAIN.COM 的直接双向信任。

default_realm	在多域配置中，[libdefaults] 下的 default_realm 值可以是任何源域。最好使用将用 AD 帐户进行身份验证的用户数量最多的域。如果在登录期间未提供 UPN 后缀，则默认值为 default_realm。此值应该与 CMC 中的“默认域”设置一致。所有域必须按如上示例指定为大写字母。
---------------	---

9.4.5.1.2 创建 JAAS 登录配置文件

9.4.5.1.2.1 创建 Tomcat 或 WebLogic JAAS 登录配置文件

bscLogin.conf 文件用于载入 Java 登录模块和 Java Web 应用程序服务器上的 AD Kerberos 身份验证。

该文件的默认位置为：C:\Windows。

- 1 创建一个名为 bscLogin.conf 的文件（如果该文件不存在），并将其存储在：C:\Windows。

注意：

可以将此文件存储在其他位置。但是，如果这样做，将需要在 Java 选项中指定其位置。

- 2 将以下代码添加到 JAAS bscLogin.conf 配置文件中：

```
com.businessobjects.security.jgss.initiate {  
  com.sun.security.auth.module.Krb5LoginModule required;  
};
```

- 3 保存并关闭文件。

9.4.5.1.2.2 创建 Oracle JAAS 登录配置文件

- 1 找到 jazn-data.xml 文件。

注意：

此文件的默认位置为 C:\OraHome_1\j2ee\home\config。如果在不同位置中安装了 Oracle Application Server，请查找特定于安装的文件。

- 2 将以下内容添加到文件中的 <jazn-loginconfig> 标记之间：

```
<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 保存并关闭 jazn-data.xml 文件。

9.4.5.1.2.3 创建 WebSphere JAAS 登录配置文件

- 1 创建一个名为 bscLogin.conf 的文件（如果该文件不存在），并将其存储在默认位置：C:\Windows 中
- 2 将以下代码添加到您的 bscLogin.conf 配置文件中：

```
com.businessobjects.security.jgss.initiate {
com.ibm.security.auth.module.Krb5LoginModule required;
};
```

- 3 保存并关闭文件。

9.4.5.1.2.4 向 SAP NetWeaver 添加 LoginModule

若要使用 Kerberos 和 SAP NetWeaver 7.3，可按照使用 Tomcat Web 应用程序服务器时的情况配置系统。无需创建 bscLogin.conf 文件。

完成此操作后，需要在 SAP NetWeaver 7.3 上添加一个 LoginModule，并更新某些 Java 设置。

要将 `com.sun.security.auth.module.Krb5LoginModule` 映射至 `com.businessobjects.security.jgss.initiate`，您需手动向 NetWeaver 添加一个 LoginModule。

- 1 通过在 Web 浏览器中键入以下地址打开 NetWeaver Administrator: `http://<计算机名>:<端口>/nwa`。
- 2 单击“Configuration Management”（配置管理）>“Security”（安全）>“Authentication”（身份验证）>“Login Modules”（登录模块）>“Edit”（编辑）。
- 3 通过以下信息添加新的登录模块：

显示名称	Krb5LoginModule
类名	com.sun.security.auth.module.Krb5LoginModule

- 4 单击“保存”。
- NetWeaver 将创建该新模块。
- 5 单击“Components”（组件）>“Edit”（编辑）。
- 6 添加一个名为 `com.businessobjects.security.jgss.initiate` 的新策略。
- 7 在“Authentication Stack”（身份验证堆栈）中，添加在步骤 3 中创建的登录模块，将其设置为“Required”（必需）。
- 8 确认“Options for Selected Login Module”（所选登录模块的选项）中没有其他条目。如果有，请将其删除。
- 9 单击“保存”。
- 10 注销 NetWeaver Administrator。

9.4.5.1.3 修改应用程序服务器 Java 设置以载入配置文件

9.4.5.1.3.1 在 Tomcat 上针对 Kerberos 修改 Java 选项

- 1 从“开始”菜单中，选择“程序”>“Tomcat”>“Tomcat Configuration”（Tomcat 配置）。
- 2 单击“Java”选项卡。

3 添加以下选项:

```
-Djava.security.auth.login.config=C:\XXXX\bscLogin.conf  
-Djava.security.krb5.conf=C:\XXXX\krb5.ini
```

将 XXXX 替换为存储 bscLogin.conf 文件的位置。

4 关闭 Tomcat 配置文件。

5 重新启动 Tomcat。

9.4.5.1.3.2 修改 SAP NetWeaver 7.3 的 Java 选项

1 浏览到 Java 配置工具（默认情况下位于 C:\usr\sap\<NetWeaver ID>\<实例>\j2ee\configtool\）并双击 configtool.bat。

这将打开该配置工具。

2 单击“View”（查看）>“Expert Mode”（专家模式）。

3 展开“Cluster-Data”（群集数据）>“Template”（模板）。

4 选择对应于 NetWeaver 服务器的实例（例如“Instance - <系统 ID><计算机名>”（实例 - <系统 ID><计算机名>））。

5 单击“VM Parameters”（VM 参数）。

6 从“Vendor”（供应商）列表中选择“SAP”，并从“Platform”（平台）列表中选择“GLOBAL”（全局）。

7 单击“System”（系统），添加下列自定义参数信息：

java.security.krb5.conf	<krb5.ini 文件的路径，包括文件名>
javax.security.auth.useSubjectCredsOnly	false

8 单击“Save”（保存），然后单击“Configuration Editor”（配置编辑器）。

9 单击“Configurations”（配置）>“Security”（安全）>“Configurations”（配置）>“com.businessobjects.security.jgss.initiate”>“Security”（安全）>“Authentication”（身份验证）。

10 单击“Edit Mode”（编辑模式）。

11 右击“Authentication”（身份验证）节点，并选择“Create sub-node”（创建子节点）。

12 从顶端列表中选择“Value-Entry”（值输入）。

13 输入以下内容：

名称	create_security_session
值	false

14. 单击“Create”（创建），然后关闭窗口。
15. 单击“Config Tool”（配置工具），然后单击“Save”（保存）。
更新配置后，需要重新启动 NetWeaver 服务器。

9.4.5.1.3.3 在 WebLogic 上针对 Kerberos 修改 Java 选项

如果要将 Kerberos 与 WebLogic 结合使用，则需要修改 Java 选项以指定 Kerberos 配置文件的位置和 Kerberos 登录模。

- 1 停止运行 BI 平台应用程序的 WebLogic 域。
- 2 打开用于启动运行 BI 平台应用程序的 WebLogic 域的脚本（对于 Windows 为 startWeblogic.cmd，对于 Unix 为 startWebLogic.sh）。
- 3 将以下信息添加到文件的 Java_Options 部分中：

```
set JAVA_OPTIONS=-Djava.security.auth.login.config=C:/XXXX/bscLogin.conf  
-Djava.security.krb5.conf=C:/XXX/krb5.ini
```

将 XXXX 替换成存储文件的位置。

- 4 重新启动运行 BI 平台应用程序的 WebLogic 的域。

9.4.5.1.3.4 在 Oracle Application Server 上针对 Kerberos 修改 Java 选项

如果要将 Kerberos 与 Oracle Application Server 结合使用，则需要修改 Java 选项以指定 Kerberos 配置文件的位置。

- 1 登录到 Oracle Application Server 的管理控制台。
- 2 单击运行 BI 平台应用程序的 OC4J 实例的名称。
- 3 选择“Server Properties”（服务器属性）。
- 4 向下滚动到“Multiple VM Configuration”（多 VM 配置）部分。

- 5 在“Command Line Options”（命令行选项）部分中，将以下内容附加到“Java Options”（Java 选项）文本字段的末尾：-Djava.security.krb5.conf=C:/XXXX/krb5.ini，XXXX 替换为文件的存储位置。
- 6 重新启动 OC4J 实例。

9.4.5.1.3.5 在 WebSphere 上针对 Kerberos 修改 Java 选项

- 1 登录到 WebSphere 管理控制台。
对于 IBM WebSphere 5.1，键入 `http://servername:9090/admin/`。对于 IBM WebSphere 6.0，键入 `http://servername:9060/ibm/console`
- 2 展开“Server”（服务器），单击“Application Servers”（应用程序服务器），然后单击所创建的要用于 BI 平台的应用程序服务器的名称。
- 3 转到“JVM”页面。

如果使用 WebSphere 5.1，请执行以下步骤转到“JVM”页面。

- a 在服务器页面上，向下滚动，直到在“Additional Properties”（附加属性）列中看到“Process Definition”（进程定义）。
- b 单击“Process Definition”（进程定义）。
- c 向下滚动并单击“Java Virtual Machine”（Java 虚拟机）。

如果使用 WebSphere 6.0，请执行以下步骤转到“JVM”页面。

- a 在服务器页面上，选择“Java 和进程管理”（Java and Process Management）。
- b 选择“进程定义”（Process Definition）。
- c 选择“Java Virtual Machine”（Java 虚拟机）。

- 4 单击“Generic JVM arguments”（普通 JVM 参数），然后如下指定 Krb5.ini 文件和 bscLogin.conf 文件的位置。

-Djava.security.auth.login.config=C:\XXXX\bscLogin.conf

-Djava.security.krb5.conf=C:\XXXX\krb5.ini

将 XXXX 替换成存储文件的位置。

- 5 单击“Apply”（应用），然后单击“Save”（保存）。
- 6 停止并重新启动服务器。

9.4.5.1.4 验证 Java 是否可接收 Kerberos 权证

在测试 Java 是否已接收 Kerberos 权证前，必须完成下列前提操作：

- 为应用程序服务器创建 bscLogin.conf 文件。
 - 创建 krb5.ini 文件。
- 1 转至命令提示符并导航至 BI 平台安装中的 jdk\bin 目录。
其默认位置为：C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\jdk\bin。
 - 2 运行 kinit <用户名>。
 - 3 按 Enter 键。
 - 4 键入密码。

如果 krb5.ini 文件配置恰当，且已载入 Java 登录模块，您应可看到下面的消息：
新的权证保存在高速缓存文件 C:\Users\Administrator\krb5cc_Administrator 中。

在成功接收到 Kerberos 权证前请勿继续 AD 设置。

若您无法接收权证，请考虑下列选项：

- 查阅本章末尾的疑难解答部分。
- 有关 Kerberos 数据库中 KDC、Kerberos 配置文件和用户凭据不可用的问题，请参阅 SAP 知识库文章 KBA 1476374 和 KBA 1245178。

9.4.5.1.5 为手动 AD 登录配置 BI 启动板

在为手动 AD 登录配置 BI 平台应用程序前，必须首先完成以下前提操作：

- 已在域控制器上为 BI 平台创建服务帐户。
- 确认 HTTP 服务主体名称 (SPN) 已添加至服务帐户。
- 已成功将 AD 用户组映射至 BI 平台。
- 已在 CCM 上测试 AD 凭据。
- 已为 Web 应用程序服务器创建、配置并测试了所需配置文件。
- 已修改应用程序服务器的 Java 设置以载入配置文件。

要为 BI 启动板启用 Windows AD 身份验证选项，请按下列步骤操作：

- 1 在承载 Web 应用程序服务器的计算机上访问 BOE Web 应用程序的自定义文件夹：

<安装目录>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\。

在 config\custom 中，而非在 config\default 目录中进行更改。否则当未来修补程序应用至部署时，您的更改将被覆盖。

之后必须重新部署修改后的 BOE Web 应用程序。

- 2 创建一个新文件。

注意：

使用记事本或任何其他文本编辑实用程序。

- 3 请按该格式保存文件：BIlaunchpad.properties。

- 4 键入以下内容：

```
authentication.visible=true  
authentication.default=secWinAD
```

- 5 保存并关闭文件。

- 6 重新启动 Web 应用程序服务器。

现在可以手动登录 BI 启动板了。访问两个应用程序中的其中一个，并在身份验证选项列表中选择 Windows AD。

注意：

在能够使用现有 AD 帐户手动登录 BI 启动板前，请不要继续 Windows AD 的设置操作。

只有在运行 Web 应用程序服务器的计算机上重新部署 BOE Web 应用程序后，新属性才会生效。使用 WDeploy 在 Web 应用程序服务器上重新部署 BOE。有关使用 WDeploy 取消部署 Web 应用程序的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

注意：

如果部署使用了防火墙，请务必打开所有必要端口，否则 Web 应用程序将无法连接 BI 平台服务器。

9.4.6 单一登录设置

9.4.6.1 BI 平台 AD 身份验证 SSO

使用 Windows AD 的 SSO 选项

为 Windows AD 身份验证及 BI 平台设置单一登录（SSO）有两种支持的方法：

- Vintela — 该选项仅可同 Kerberos 一起使用。
- SiteMinder — 该选项仅可同 Kerberos 一起使用。

数据库 SSO

数据库 SSO 使已登录用户能够执行需要访问数据库的操作，尤其是无需再次提供登录凭据，即可查看和刷新报表。由于约束委派是 AD 身份验证和 Vintela SSO 的可选项，因此系统数据库的单一登录部署方案需要约束委派。

端到端 SSO

在 BI 平台中，端到端 SSO 是通过 Windows AD 和 Kerberos 支持的。在这一方案中，用户同时拥有前端的 BI 平台单一登录访问，也有后端的数据库 SSO 访问。因此，用户只需在登录到操作系统时提供一次他们的登录凭据，即可访问 BI 平台，并能够执行需要数据库访问权限的操作（如查看报表）。

手动和 SSO AD 身份验证配置

成功配置部署以启用 AD 帐户手动登录 BI 启动板后，您需要重新访问 AD 身份验证设置以启用特定 SSO 需求。需求取决于您所选的 SSO 方法。

9.4.6.2 使用 Vintela SSO

9.4.6.2.1 Vintela SSO 设置检查清单

要在 BI 平台上使用 Vintela SSO，需要完成下列任务：

- 1 针对 Vintela SSO 为服务帐户进行特别配置。
- 2 配置约束委派（可选）。
- 3 在 CMC 中配置 Windows AD SSO 身份验证选项。
- 4 为 Vintela SSO 配置常规属性和 BI 启动板特定属性。
- 5 如果使用 Tomcat 作为部署时的 Web 应用程序服务器，则需要增加标头大小限制。
- 6 配置 Vintela 的 Internet 浏览器。

9.4.6.2.2 为 Vintela SSO 设置服务帐户

Ktpass 命令行工具为 Active Directory 中的主机或服务配置服务主体名称，并生成一个包含了服务帐户共享秘密密钥的 Kerberos “keytab” 文件。该工具一般位于域控制器上，或可从 Microsoft 支持站点：<http://support.microsoft.com/kb/892777> 下载。

您需要对服务帐户进行特别配置，以允许某一给定 Windows AD 组中的用户能够在登录 BI 启动板时自动使用其 AD 凭据进行身份验证。您可对在域控制器上创建的用于 AD Kerberos 身份验证的服务帐户进行重新配置。

当某客户端尝试登录 BI 启动板时，启动发送至 Kerberos 权证生成服务器的申请。为完成这一请求，为 BI 平台创建的服务帐户必须拥有与应用程序服务器 URL 相匹配的 SPN。在承载域控制器的计算机上执行下列步骤。

1. 运行 Kerberos keytab 设置命令 ktpass 以创建并放置一个 keytab 文件。

指定在下表中列出的 ktpass 参数：

参数	说明
-out	指定要生成的 Kerberos keytab 文件的名称。
-princ	<p>指定用于服务帐户的主体名称，并以 SPN 格式表示：MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.COM，其中 MYSIAMYSERVER 为中央配置管理器（CCM）中指定的服务智能代理名称。</p> <p>注意： 服务帐户的名称区分大小写。SPN 包含运行服务实例的主机计算机的名称。</p> <p>提示： SPN 在它所注册的目录林中必须唯一。在检查时，可使用 Windows 支持工具 Ldp.exe 搜索 SPN。</p>
-pass	指定服务帐户使用的密码。
-ptype	<p>指定主体类型。</p> <p>-ptype KRB5_NT_PRINCIPAL</p>
-crypto	<p>指定服务帐户使用的加密类型：</p> <p>-crypto RC4-HMAC-NT</p>

例如：

```
ktpass -out keytab_filename.keytab -princ MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.COM  
-pass password -kvno 255 -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT
```

ktpass 命令的输出应确认目标域控制器以及已经创建了一个包含共享秘密的 Kerberos keytab 文件。该命令还会将主体名称映射到（本地）服务帐户。

- 2 右键单击服务帐户，选择“属性” > “委派”。
- 3 单击“信任此用户作为任何服务的委派（仅 Kerberos）”。
- 4 单击“确定”保存设置。

服务帐户现在拥有所有所需的用于 Vintela SSO 的服务主体名称，且已生成包含服务帐户加密密码的 keytab 文件。

9.4.6.2.2.1 为 Vintela SSO 配置约束委派

约束委派是设置 Vintela SSO 的可选项。对于系统数据库需要 SSO 的部署，则必须使用约束委派。

- 1 在 AD 域控制器计算机中打开 Active Directory “用户和计算机”管理单元。
- 2 右键单击在上一部分创建的服务帐户，然后单击“属性” > “委派”。
- 3 选择“仅信任此用户作为指定服务的委派”。
- 4 选择“仅使用 Kerberos”。
- 5 单击“添加” > “用户或计算机”。
- 6 键入服务帐户名称，然后单击“确定”。
- 7 选择以下服务并单击“确定”。

- HTTP 服务
- 该服务用于在承载 BI 平台的计算机上运行服务智能代理（SIA）。

服务将添加到可委派给服务帐户的服务列表中。

需要修改 Web 应用程序属性以说明此项修改。

9.4.6.2.3 在 CMC 中配置 SSO 设置

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“Windows AD”。
- 3 确保已选中“启用 Windows Active Directory (AD)”复选框。
- 4 请确保“身份验证选项”中的“使用 Kerberos 身份验证”选项已选中。
- 5 若数据库需要配置 SSO，请选择“高速缓存安全上下文”。
- 6 选择“为选定身份验证模式启用单一登录”。
- 7 单击“更新”。

9.4.6.2.4 为 BI 启动板和 OpenDocument 启用 Vintela 单一登录

该过程适用于 BI 启动板或 OpenDocument。要为 BI 平台 Web 应用程序启用 SSO，需要在 BOE.war 文件中指定 Vintela 和 SSO 特定的属性。为设置 SSO，建议在处理其他应用程序之前，为 BI 启动板启用 AD 帐户的 SSO。

- 1 在承载 Web 应用程序服务器的计算机上访问 BOE Web 应用程序的自定义文件夹：

<安装目录>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\。

在 config\custom 目录中，而非在 config\default 目录中进行更改。否则当未来修补程序应用至部署时，您的更改将被覆盖。

之后必须重新部署修改后的 BOE Web 应用程序。

- 2 使用文本编辑器创建新文件。
- 3 输入以下内容：

```
sso.enabled=true
siteminder.enabled=false
vintela.enabled=true
idm.realm=DOMAIN.COM
idm.princ=MYSIAMYSERVER/sbo.service.domain.com@DOMAIN.COM
idm.allowUnsecured=true
idm.allowNTLM=false
idm.logger.name=simple
idm.keytab=C:/WIN/filename.keytab
idm.logger.props=error-log.properties
```

注意：

- idm.realm 和 idm.princ 参数要求存在有效值。idm.realm 应与在 krb5.ini 文件中配置 default_realm 时所设置的值相同。值必须采用大写形式。idm.princ 参数是用于为 Vintela SSO 创建的服务帐户的 SPN。
- 指定 keytab 文件位置时请使用正斜线。

如果不想为 Windows AD 身份验证和 Vintela SSO 使用约束委派，可跳过以下步骤。

- 4 要使用约束委派，请添加：

```
idm.allowS4U=true
```

- 5 关闭该文件并使用名称 `global.properties` 保存。

注意：

确保所保存的文件名不含任何扩展名，如 `.txt`。

- 6 在同一目录下创建另一个文件。根据需要将文件另存为 `OpenDocument.properties` 或 `BIlaunchpad.properties`。
- 7 键入以下内容：

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

例如：

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

- 8 保存并关闭文件。
- 9 重新启动 Web 应用程序服务器。

只有在运行 Web 应用程序服务器的计算机上重新部署 BOE Web 应用程序后，新属性才会生效。使用 WDeploy 在 Web 应用程序服务器上重新部署 BOE。有关使用 WDeploy 取消部署 Web 应用程序的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

注意：

如果部署使用了防火墙，请记住打开所有必要端口，否则 Web 应用程序将无法连接 BI 平台服务器。

9.4.6.2.5 为 Web 服务启用 Vintela 单一登录

某些客户端工具要求通过 Web 服务进行身份验证。按照这些步骤，为 Web 服务启用单一登录 (SSO)。

- 1 备份该文件：安装目录\ SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\web.xml，然后将其打开进行编辑。
- 2 取消注释 Kerberos 代理过滤器和 Kerberos 过滤器部分，以便为 Windows Active Directory (参阅 WinAD) 身份验证启用 Kerberos SSO。
必须指定以下选项（其余为可选项）：
 - `idm.realm`（与 `Krb5.ini` 文件中指定的 `default_realm` 相同）。
 - `idm.princ`（与位于安装目录\ SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom的 `global.properties` 文件中为 `idm.princ` 指定的相同）。

- `idm.keytab`（与位于安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom的 `global.properties` 文件中的 `idm.keytab` 指定的相同）。

注意：

如果使用在 Tomcat 的 Java 选项中设置的硬编码密码，则请勿在 `web.xml` 文件中对 `keytab` 行做任何更改。

- 3 如果 SSL 未与 Java 应用程序服务器一起使用，则将 `idm.allowUnsecured` 参数设置为 `true`。
有关 Tomcat SSL 的更多信息，请参阅 ID 为 1484802 的知识库文章。
- 4 备份该文件：安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswebobje\WEB-INF\classes\dsweb.properties，然后将其打开进行编辑。
- 5 将 `kerberos.sso` 设置为 `true`，然后保存该文件。
- 6 使用 WDeploy 在 Web 应用程序服务器上重新部署 WAR 文件。
有关使用 WDeploy 的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。
- 7 重新启动 Tomcat。
- 8 要测试设置，请在已安装客户端工具的客户端计算机上，启动 Query as a Web Service 设计器。
- 9 添加一个新的托管主机。
- 10 输入应用程序服务器名称。
- 11 按如下格式输入 Web 服务 URL：`http://<Web 应用程序服务器>:<端口号>/dswebobje/services/Session`。
示例：`http://BI4:8080/dswebobje/services/Session`。
- 12 输入 CMS 主机名称。
- 13 将身份验证类型更改为 Windows AD。
- 14 选择“启用 Windows Active Directory 单一登录”。
- 15 在登录提示时，将“用户”和“密码”字段留空并单击“确定”。

9.4.6.2.6 增加 Tomcat 的标头大小限制

Active Directory 会创建将在身份验证过程中使用的 Kerberos 标记。此标记存储在 HTTP 标头中。Java 应用程序服务器将具有一个默认 HTTP 标头大小。为了避免故障，请确保该服务器的最小默认大小为 16384 字节。（某些部署可能需要较大的大小。有关更多信息，请参阅 Microsoft 支持站点 (<http://support.microsoft.com/kb/327825>) 上有关规模调整的指引。）

- 1 在安装有 Tomcat 的服务器上，打开 `server.xml` 文件。
在 Windows 上，此文件位于 <Tomcat 安装目录>/conf 中
 - 如果在 Windows 上使用随 BI 平台一起安装的 Tomcat 版本，并且未修改默认

安装位置，请使用 C:\Program Files (x86)\SAP BusinessObjects\Tomcat\ 替换 <TomcatINSTALLDIR>。

- 如果使用支持的任何其他 Web 应用程序服务器，请查阅 Web 应用程序服务器的文档以确定相应的路径。

2 查找所配置端口号的对应 <Connector ...> 标记。

如果使用默认端口 8080，请查找其中包含 port=8080 的 <Connector ...> 标记。

例如：

```
<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 在 <Connector ...> 标记内添加以下值：

maxHttpHeaderSize="16384"

例如：

```
<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 保存并关闭 server.xml 文件。

5 重新启动 Tomcat。

注意：

对于其他 Java 应用程序服务器，请查阅 Java 应用程序服务器的文档。

9.4.6.2.7 配置 Internet 浏览器

要使 AD Kerberos 身份验证支持 Vintela SSO，必须对 BI 平台客户端进行配置。这涉及到在客户端计算机上配置 Web 浏览器。

9.4.6.2.7.1 在客户端计算机上配置 Internet Explorer

- 1 在客户端计算机上，打开 IE 浏览器。
- 2 启用集成 Windows 身份验证。
 - a 在“工具”菜单上，单击“Internet 选项”。
 - b 单击“高级”选项卡。
 - c 滚动到“安全”，选择“启用集成 Windows 身份验证”，然后单击“应用”。
- 3 将 Java 应用程序计算机或 URL 添加到受信任的站点。可以输入站点的完整域名。
 - a 在“工具”菜单上，单击“Internet 选项”。
 - b 单击“安全”选项卡。
 - c 单击“站点”，然后单击“高级”。
 - d 选择或输入站点并单击“添加”。
 - e 单击“确定”直至“Internet 选项”对话框关闭。
- 4 关闭并重新打开 Internet Explorer 浏览器窗口以使这些更改生效。
- 5 在每台 BI 平台客户端计算机上重复所有这些步骤。

9.4.6.2.7.2 在客户端计算机上配置 Firefox

- 1 修改 network.negotiate-auth.delegation-uris
 - a 在客户端计算机上，打开 Firefox 浏览器。
 - b 在 URL 地址字段中键入 about:config。
将出现可配置的属性的列表。
 - c 双击“network.negotiate-auth.delegation-uris”以编辑属性。
 - d 输入将用于访问 BI 启动板的 URL。

例如，如果您的 BI 启动板 URL 是 http://machine.domain.com:8080/BOE/BI，则需要输入 http://machine.domain.com。

注意：
要添加多个 URL，请以逗号分隔。例如：http://machine.domain.com,machine2.domain.com。
 - e 单击“确定”。
- 2 修改 network.negotiate-auth.trusted-uris
 - a 在客户端计算机上，打开 Firefox 浏览器。
 - b 在 URL 地址字段中键入 about:config。
将出现可配置的属性的列表。
 - c 双击“network.negotiate-auth.trusted-uris”以编辑属性。
 - d 输入将用于访问 BI 启动板的 URL。

例如，如果 BI 启动板 URL 是 `http://machine.domain.com:8080/BOE/BI`，则需要输入 `http://machine.domain.com`。

注意：

要添加多个 URL，请以逗号分隔。例如：`http://machine.domain.com,machine2.domain.com`。

- a 单击“确定”。
- 3 关闭并重新打开 Firefox 浏览器窗口以使这些更改生效。
- 4 在每台 BI 平台客户端计算机上重复所有这些步骤。

9.4.6.2.8 测试 AD Kerberos 身份验证的 Vintela SSO

您应在客户端工作站上测试您的 SSO 设置。请确保客户端与您的 BI 平台部署处于同一域中，且您已作为映射的 AD 用户登录工作站。该用户帐户必须能够手动登录 BI 启动板。

要测试 SSO，请打开浏览器并输入 BI 启动板的 URL。若 SSO 配置得当，您应不会收到要求输入登录凭据的提示。

提示：

建议在部署中测试多个 AD 用户方案。例如，若环境中来自不同操作系统的多个用户，您应为每种操作系统的用户都进行 SSO 测试。还应对您的组织所支持的所有浏览器进行 SSO 测试。若您的环境中来自多个目录林或域的用户，则应为来自每个目录林和域中的用户帐户测试 SSO。

9.4.6.2.9 为应用程序服务器配置 Kerberos 和数据库单一登录

满足所有以下要求的部署支持数据库单一登录：

- 在 Web 应用程序服务器上部署 BI 平台。
- Web 应用程序服务器已配置 Vintela SSO 以用于 AD 身份验证。
- 要求 SSO 的数据库是 SQL Server 或 Oracle 的支持版本。
- 必须已在 SQL Server 或 Oracle 内为需要访问该数据库的组或用户授予权限。

最后一步是修改 `krb5.ini` 文件以支持 Web 应用程序的数据库 SSO。

9.4.6.2.9.1 为 Java 应用程序服务器启用数据库单一登录

- 1 打开用于部署 BI 平台的 krb5.ini 文件。
此文件的默认位置为 Web 应用程序服务器上的 WIN 目录。

注意：

如果无法在 WIN 目录中找到该文件，请检查文件位置的 Java 参数：

```
-Djava.security.auth.login.config
```

此变量是在 Web 应用程序服务器上配置 AD 和 Kerberos 时指定的。

- 2 转到该文件的 [libdefaults] 部分。
- 3 在文件的 [realms] 部分的开头位置前输入以下字符串：

```
forwardable=true
```

- 4 保存并关闭文件。
- 5 重新启动 Web 应用程序服务器。

仅当在 CMC 的 Windows AD 身份验证页面中选中“高速缓存安全上下文（对于数据库的 SSO 为必需）”框后，才会启用数据库的单一登录。

9.4.6.3 使用 SiteMinder

9.4.6.3.1 使用 Windows AD 及 SiteMinder

本节说明如何使用 AD 和 SiteMinder。SiteMinder 是第三方用户访问和身份验证工具，可以与 AD 安全插件一起使用，共同创建 BI 平台的单一登录。可以将 SiteMinder 与 Kerberos 一起使用。

请确保在配置 Windows AD 身份验证以配合使用 SiteMinder 之前，已安装并配置了 SiteMinder 标识管理资源。有关 SiteMinder 和如何安装它的更多信息，请参阅 SiteMinder 文档。

必须执行以下两项任务才能启用 SiteMinder AD 单一登录：

- 为 SiteMinder 单一登录配置 AD 插件
- 为 BOE Web 应用程序配置 SiteMinder 属性

注意：

确保 SiteMinder 管理员已启用了 4.x 代理的支持。无论使用哪种受支持的 SiteMinder 版本，都必须完成此操作。有关配置 SiteMinder 的更多信息，请参阅 SiteMinder 文档。

9.4.6.3.1.1 启用 BI 启动板的 SiteMinder 属性

除了为 Windows AD 安全插件指定 SiteMinder 设置外，还必须为 BOE war 属性指定 SiteMinder 设置。

- 1 在 BI 平台安装中找到安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom\ 目录。
- 2 使用“记事本”或其他文本编辑实用程序在该目录中创建一个新文件。
- 3 在新文件中，输入以下值：

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

- 4 使用名称 global.properties 保存文件。

注意：

确保所保存的文件名不含扩展名，如 .txt。

- 5 在同一目录下创建另一个文件。
- 6 在新文件中，输入以下值：

```
authentication.default=secWinAD  
cms.default=[cms name]:[CMS port number]
```

例如：

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

- 7 使用名称 BIlaunchpad.properties 保存并关闭该文件。

新属性将在运行 Web 应用程序服务器的计算机上重新部署 BOE.war 后生效。使用 WDeploy 在 Web 应用程序服务器上重新部署 WAR 文件。有关使用 WDeploy 取消部署 Web 应用程序的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

9.4.6.3.1.2 在 CMC 中配置 SiteMinder 设置

在为 SiteMinder 配置 CMC 前，必须完成下列前提操作：

- 已成功将 AD 用户组映射至 BI 平台。
- 已在 CCM 上测试 AD 凭据。

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“Windows AD”。
- 3 选中“启用 Windows Active Directory (AD)”复选框。
- 4 在“身份验证选项”下，选择“使用 NTLM 身份验证”或“使用 Kerberos 身份验证”。

要为 Kerberos 和使用 Kerberos 的 AD 身份验证配置 BI 平台，必须要有服务帐户。可以创建新的域帐户或使用现有的域帐户。服务帐户将用于运行 BI 平台服务器。

提示：

手动登录到 BI 启动板时，来自其他域的用户必须在其用户名后以大写字母附加域名。例如，在 user@CHILD.PARENTDOMAIN.COM 中，CHILD.PARENTDOMAIN.COM 是域。

- 5 如果选择“使用 Kerberos 身份验证”：
 - a 如果希望配置数据库的单一登录，请选择“高速缓存安全上下文”。
 - b 删除“服务主体名称”框中的所有信息。
- 6 如果要配置单一登录，请选中“为选定身份验证模式启用单一登录”。
若要启用单一登录，您还必须配置 BOE Web 应用程序常规属性和 BI 启动板属性。
- 7 在“凭据的同步”区域中，选择一个选项并在登录时启用并更新 AD 用户的数据源凭据。
该选项将数据源与用户的当前登录凭据同步。
- 8 在“SiteMinder 选项”区域中，将 SiteMinder 配置为使用 Kerberos 的 AD 身份验证的单一登录选项：
 - a 单击“已禁用”。

“Windows Active Directory”页面随即弹出。

若未配置 Windows AD 插件，则将弹出警告，询问是否要继续。单击“确定”。

- b 单击“使用 SiteMinder 单一登录”。
- c 在“策略服务器主机”框中，键入每个策略服务器的名称，然后单击“添加”。
- d 在“结算”、“身份验证”和“授权”框中为每个策略服务主机输入端口号。
- e 在“代理名”框中输入代理名。
- f 在“共享秘密”框中输入共享秘密。

确保 SiteMinder 管理员已启用 4.x 代理支持，无论您使用的是哪个 SiteMinder 支持版本。有关 SiteMinder 及其安装方式的信息，请参阅 SiteMinder 文档。

- g 单击“更新”保存并返回到 AD 身份验证主页面。
- 9 在“AD 别名选项”区域中，指定如何向 BI 平台添加和更新新别名。
- a 在“新别名选项”区域中，选择下列选项之一将新别名映射到 Enterprise 帐户：
- 将每个新的 AD 别名分配给同名的现有用户帐户
- 如果您知道用户具有名称相同的现有 Enterprise 帐户，请选择此选项；也就是说，会将 AD 别名分配给现有用户（启用了自动别名创建）。如果用户没有现有 Enterprise 帐户或 Enterprise 和 AD 帐户中没有相同的名称，则会将他们作为新用户添加。
- 为每个新的 AD 别名创建新的用户帐户
- 如果要为每个用户创建一个新帐户，请选择此选项。
- b 在“别名更新选项”区域中，选择下列选项之一来管理 Enterprise 帐户的别名更新：
- 在发生别名更新时创建新的别名
- 使用此选项可自动为映射到 BI 平台的每个 AD 用户创建新别名。系统会为没有 BI 平台帐户的用户，或为所有用户（如果选择了“为每个新的 AD 别名创建新的用户帐户”并单击了“更新”）添加新 AD 帐户。
- 仅当用户登录时才创建新的别名
- 如果所映射的 AD 目录包含许多用户，但其中只有少数用户将使用 BI 平台，请使用此选项。平台不会自动为所有用户创建别名和 Enterprise 帐户。而只会为登录到 BI 平台的用户创建别名（如有必要，也会创建帐户）。
- c 在“新用户选项”区域中，选择创建新用户的选项：
- 将新用户创建为命名用户
- 新用户帐户被配置为使用命名用户许可。命名用户许可与特定用户关联，并允许用户基于用户名和密码访问系统。这样，不管连接了多少用户，命名用户都能够访问系统。必须为使用此项创建的每个用户帐户提供一个命名用户许可。
- 将新用户创建为并发用户
- 新用户帐户被配置为使用并发用户许可。并发许可指定可同时连接到 BI 平台的用户数。这种类型的许可模式非常灵活，因为少量的并发许可就可以支持大量用户。例如，根据用户访问系统的频率和时长，一份 100 个用户的并发许可可能支持 250、500 或 700 个用户。
10. 配置如何计划 AD 别名更新：单击“计划”。
- a 在“计划”对话框中，从“运行对象”列表中选择重复发生。
- b 根据需要设置其他计划选项和参数。
- c 单击“计划”。
- 发生别名更新时，组信息也将更新。
11. 在“属性绑定选项”区域中，为 AD 插件指定属性绑定优先级：
- a 选择“导入全名、电子邮件地址和其他属性”复选框。
- 这将导入 AD 帐户中使用的全名和说明，并将其与用户对象一起存储在 BI 平台中。
- b 为“Set priority of AD attribute binding relative to other attributes binding”（设置与其他属性绑定相关的 AD 属性绑定的优先级）指定一个选项。

如果该选项设置为“1”，则 AD 属性在启用 AD 和其他插件（LDAP 和 SAP）时具有优先权。如果选项设置为“3”，则已启用的其他插件的属性具有优先级。

12. 在“AD 组选项”区域中，配置 AD 组更新：

a. 单击“计划”。

将出现“计划”对话框。

b. 从“运行对象”列表中选择重复发生。

c. 根据需要设置其他计划选项和参数。

d. 单击“计划”。

系统将计划更新并根据指定的计划运行更新。AD 组帐户的下一计划更新显示在“AD 组选项”中。

13. 在“按需 AD 更新”区域中选择一个选项，指示在单击“更新”时是更新 AD 组还是用户（或均不更新）：

- 立即更新 AD 组

如果在单击“更新”时要开始更新所有已计划的 AD 组，请选择该选项。下一个计划的 AD 组更新将在“AD 组选项”下列出。

- 立即更新 AD 组和别名

如果在单击“更新”时要开始更新所有已计划的 AD 组 and 用户别名，请选择该选项。接下来的已计划更新将在“AD 组选项”和“AD 别名选项”下列出。

- 不立即更新 AD 组和别名

在单击“更新”时不会更新 AD 组或用户别名。

14. 单击“更新”，然后单击“确定”。

9.4.6.3.1.3 禁用 SiteMinder

如果要阻止配置 SiteMinder，或者在 CMC 中配置后禁用 SiteMinder，请修改 BI 启动板的 Web 配置文件。

9.4.6.3.1.3.1 为 Java 客户端禁用 SiteMinder

除了为 Windows AD 安全插件禁用 SiteMinder 设置外，还必须为 Web 应用程序服务器上的 BOE war 文件禁用 SiteMinder 设置。

- 1 转至 BI 平台安装的下列目录：

<安装目录>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\

- 2 打开 global.properties 文件。
- 3 将 siteminder.enabled 更改为 False

```
siteminder.enabled=false
```

- 4 保存所做的更改，然后关闭文件。

只有在运行 Web 应用程序服务器的计算机上重新部署 BOE.war 后，更改才能生效。使用 WDeploy 在 Web 应用程序服务器上重新部署 WAR 文件。有关使用 WDeploy 取消部署 Web 应用程序的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

9.4.7 Windows AD 身份验证疑难解答

9.4.7.1 配置疑难解答

如果在配置 Kerberos 时遇到问题，以下步骤可能有用：

- 启用日志记录
- 测试 Java SDK Kerberos 配置

9.4.7.1.1 启用日志记录

- 1 从“开始”菜单中，选择“程序”>“Tomcat”>“Tomcat Configuration”（Tomcat 配置）

- 2 单击“Java”选项卡。
- 3 添加以下选项：

```
-Dcrystal.enterprise.trace.configuration=verbose  
-sun.security.krb5.debug=true
```

这将在以下位置中创建日志文件：

```
C:\Documents and Settings\<user name>\.businessobjects\jce_verbose.log
```

9.4.7.1.2 测试 Kerberos 配置

- 运行以下命令测试 Kerberos 配置，其中 servant 是服务帐户和在其中运行 CMS 的域，password 是与服务帐户关联的密码。

```
<InstallDirectory>\SAP BusinessObjects Enterprise XI 4.0\win64_64\jdk\bin\servact@TESTM03.COM Password
```

例如：

```
C:\Program Files\SAP BusinessObjects\  
SAP Business Objects Enterprise XI 4.0\win64_64\jdk\bin\  
servact@TESTM03.COM Password
```

域和服务主体名称必须与 Active Directory 中的域和服务主体名称完全匹配。如果问题仍然存在，请检查输入的名称是否相同；请注意名称区分大小写。

9.4.7.1.3 由于 AD UPN 和 SAM 名称不同而导致的登录失败

用户的 Active Directory ID 已成功映射到 BI 平台。尽管如此，但用户仍无法使用以下格式的 Windows AD 身份验证和 Kerbero 成功登录到 CMC 或 BI 启动板：DOMAIN\ABC123

当使用不完全相同的 UPN 和 SAM 名称在 Active Directory 中设置用户时，就会出现此问题。以下示例可能导致出现问题：

- UPN 为 abc123@company.com，但 SAM 名称为 DOMAIN\ABC123。
- UPN 为 jsmith@company，但 SAM 名称为 DOMAIN\johnsmith。

可通过两种方式解决此问题：

- 让用户使用 UPN 名称（而不是 SAM 名称）登录。

- 确保 SAM 帐户名和 UPN 名称相同。

9.4.7.1.4 预身份验证错误

以前能够登录的用户无法再成功登录。该用户将收到以下错误消息：无法识别帐户信息。Tomcat 错误日志将显示以下错误消息：“Pre-authentication information was invalid (24)”（预身份验证信息无效（24））

由于 Kerberos 用户数据库未对 AD 中的 UPN 进行更改，因此可能出现此问题。这可能表示 Kerberos 用户数据库和 AD 信息不同步。

要解决此问题，请重置 AD 中的用户密码。这样将确保正确地传播更改的信息。

注意：

J2SE 5.0 不存在此问题。

9.5 SAP 身份验证

9.5.1 配置 SAP 身份验证

本节介绍如何为 SAP 环境配置 BI 平台身份验证。

SAP 身份验证让 SAP 用户能够使用其 SAP 用户名和密码登录 BI 平台，而不必在 BI 平台中存储密码。SAP 身份验证还允许保留有关 SAP 中用户角色的信息，并在平台中使用此角色信息分配权限，以执行管理任务或访问内容。

访问 SAP 身份验证应用程序

必须为 BI 平台提供有关 SAP 系统的信息。该专用 Web 应用程序可通过主要 BI 平台管理工具“中央管理控制台”（CMC）进行访问。要从 CMC 主页访问该应用程序，请单击“身份验证”。

对 SAP 用户进行身份验证

安全插件可以扩展和自定义 BI 平台对用户进行身份验证的方法。SAP 身份验证功能包括一个用于 BI 平台的中央管理服务器 (CMS) 组件的 SAP 安全插件 (secSAPR3.d11)。该 SAP 安全插件有若干重要优点：

- 它可充当身份验证提供程序，代表 CMS 依据您的 SAP 系统验证用户凭据。当用户直接登录 BI 平台时，可以选择 SAP 身份验证，并提供其常用的 SAP 用户名和密码。BI 平台也可以依据 SAP 系统验证 Enterprise Portal 登录权证。
- 它允许将角色从 SAP 映射到 BI 平台用户组，从而简化帐户创建操作；同时还允许在 BI 平台中以统一方式向用户和组分配权限，从而简化帐户管理工作。
- 它会动态地维护 SAP 角色列表。因此，一旦将 SAP 角色映射到平台，属于该角色的所有用户就都能够登录该系统。如果随后更改了 SAP 角色成员资格，则无需更新或刷新 BI 平台中的列表。
- SAP 身份验证组件包括一个用于配置该插件的 Web 应用程序。用户可以在中央管理控制台 (CMC) 的“身份验证”区域访问此应用程序。

9.5.2 为 BI 平台创建用户帐户

BI 平台系统需要一个已获授权可访问 SAP 角色成员资格列表并对 SAP 用户进行身份验证的 SAP 用户帐户。需要使用帐户凭据将 BI 平台连接到 SAP 系统。有关创建 SAP 用户帐户和通过角色分配权限的一般说明，请参阅 SAP BW 文档。

使用事务 SU01 创建名为 CRYSTAL 的新 SAP 用户帐户。使用事务 PFCG 创建名为 CRYSTAL_ENTITLEMENT 的新角色。（这些是建议的名称，可不必使用。）通过设置下列授权对象的值更改新角色的授权：

授权对象	字段	值
文件访问授权 (S_DATASET)	活动 (ACTVT)	Read、Write (33、34)
	物理文件名 (FILENAME)	* (代表所有值)
	ABAP 程序名 (PROGRAM)	*

授权对象	字段	值
RFC 访问的授权检查 (S_RFC)	活动 (ACTVT)	16
	要保护的 RFC 名称 (RFC_NAME)	BDCH、STPA、SUS0、BDL5、 SUUS、SU_USER、SYST、SUNI、 RFC1、SDIFRUNTIME、 PRGN_J2EE、/CRYSTAL/SECURITY
	要保护的 RFC 对象类型 (RFC_TYPE)	函数组 (FUGR)
用户主维护：用户组 (S_US ER_GRP)	活动 (ACTVT)	Create 或 Generate 和 Display (03)
	用户主维护中的用户组 (CLASS)	* 注意： 为获得更高的安全性，可以 明确列出其成员需要访问 BI 平 台的用户组。

最后，将 CRYSTAL 用户添加到 CRYSTAL_ENTITLEMENT 角色。

提示：

如果系统策略要求用户在首次登录系统后更改密码，现在请使用 CRYSTAL 用户帐户登录并重置密码。

9.5.3 连接到 SAP 权利系统

将角色导入 BI 平台或向其发布 BW 内容之前，必须提供有关要与之集成的 SAP 权利系统的信息。BI 平台在确定角色成员资格和对 SAP 用户进行身份验证时，会使用此信息连接至目标 SAP 系统。

9.5.3.1 添加 SAP 权利系统

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“SAP”链接。

将显示权利系统设置。

提示：

如果权利系统已经显示在“逻辑系统名”列表中，则单击“新建”。

- 3 在“系统”字段中，键入由三个字符组成的 SAP 系统的系统 ID (SID)。
- 4 在“客户端”字段中，键入 BI 平台在登录到 SAP 系统时必须使用的客户端编号。
BI 平台会将系统与客户端信息合并到一起，并在“逻辑系统名称”列表中添加一个条目。
- 5 确保清除了“禁用”复选框。

注意：

使用“禁用”复选框可以向 BI 平台指示特定 SAP 系统暂时不可用。

- 6 如果设置了负载平衡，以使 BI 平台必须通过消息服务器登录，请相应填写“消息服务器”和“登录组”字段。

注意：

必须在 BI 平台计算机上的 Services 文件中输入相应条目才能启用负载平衡，尤其是部署不在一台计算机上时。特别地，应考虑到承载 CMS 的计算机、Web 应用程序服务器以及所有管理身份验证帐户和设置的计算机。

- 7 如果未设置负载平衡（或者希望 BI 平台直接登录到 SAP 系统），请相应填写“应用程序服务器”和“系统编号”字段。
- 8 在“用户名”、“密码”和“语言”字段中，键入希望 BI 平台在登录到 SAP 时使用的 SAP 帐户的用户名、密码和语言代码。

注意：

这些凭据必须与为 BI 平台创建的用户帐户相对应。

- 9 单击“更新”。

如果添加多个权利系统，请单击“选项”选项卡，以指定 BI 平台用作默认系统的系统（即，为对尝试使用 SAP 凭据登录但未指定特定 SAP 系统的用户进行身份验证而联系的系统）。

相关主题

- 第 281 页上的“[为 BI 平台创建用户帐户](#)”

9.5.3.2 验证是否正确添加了权利系统

- 1 单击“角色导入”选项卡。
- 2 从“逻辑系统名称”列表中选择权利系统名称。

如果正确添加了权利系统，“可用角色”列表将包含一系列用户可以选择导入的角色。

提示：

如果“逻辑系统名称”列表中未显示任何角色，请查找页面上的错误消息。这些错误消息会为您提供修正错误所需的信息。

9.5.3.3 临时禁用与 SAP 权利系统的连接

在 CMC 中，可以临时禁用 BI 平台和 SAP 权利系统之间的连接。在 SAP 权利系统计划停机等情形下，这样做有助于保持 BI 平台的响应性。

- 1 在 CMC 中，转到“身份验证”管理区域。
- 2 双击“SAP”链接。
- 3 在“逻辑系统名”列表中，选择要禁用的系统。
- 4 选择“禁用”复选框。
- 5 单击“更新”。

9.5.4 设置 SAP 身份验证选项

SAP 身份验证包含许多选项，您可以在集成 BI 平台与 SAP 系统时指定这些选项。这些选项包括：

- 启用或禁用 SAP 身份验证
- 指定连接设置
- 将导入的用户链接到 BI 平台许可模型。
- 配置对 SAP 系统的单一登录

9.5.4.1 设置 SAP 身份验证选项

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“SAP”链接，然后单击“选项”选项卡。

3 按需要检查并修改以下设置：

设置	说明
启用 SAP 身份验证	<p>取消选中此复选框以禁用 SAP 身份验证。</p> <p>注意： 要针对特定 SAP 系统禁用 SAP 身份验证，请在“权利系统”选项卡上选中该系统的“禁用”复选框。</p>
内容文件夹根目录	<p>指定 BI 平台在 CMC 和 BI 启动板中开始复制 BW 文件夹结构的文件夹。</p> <p>默认值为 /SAP/2.0，但可以将其更改为其他文件夹。如果需要更改该值，必须在 CMC 与内容管理工作台中同时进行更改。</p>
默认系统	<p>选择 SAP 权力系统，以便 BI 平台与之联系，对尝试以 SAP 凭据登录但未指定特定 SAP 系统的用户进行身份验证。</p> <p>注意： 如果选择一个默认系统，当该系统的用户使用 SAP 身份验证从客户端工具（如 Live Office 或 Universe Designer）进行连接时，无需输入自己的系统 ID 或客户端。例如，如果将 SYS~100 设置为默认系统，当选择 SAP 身份验证时，SYS~100/user1 可以以 user1 身份登录。</p>
访问权利系统的最大失败尝试次数	<p>键入 BI 平台尝试联系 SAP 系统以满足身份验证请求的次数。</p> <p>如果将该值设为 -1，BI 平台可以无限次地尝试联系权利系统。如果将该值设为 0，则会限定 BI 平台仅进行一次联系权利系统的尝试。</p> <p>注意： 将此设置与“使权利系统保持禁用状态 [秒]”选项一起使用，可配置 BI 平台处理暂时不可用的 SAP 权利系统的方式。系统使用这两个选项确定何时停止与不可用 SAP 系统的通信，以及何时恢复与该系统的通信。</p>
使权利系统保持禁用状态 [秒]	<p>键入 BI 平台在继续尝试根据 SAP 系统验证用户身份之前等待的秒数。</p> <p>例如，如果将“权利系统访问最高失败次数”设置为 3，则 BI 平台允许根据任意 SAP 系统对用户进行身份验证时最多可以失败三次。第四次失败的尝试将禁止系统在指定的时间长度内尝试对用户进行身份验证。</p>
每个系统的最大并发连接数	<p>指定为 SAP 系统同时打开多少个连接。</p> <p>例如，如果键入 2，则 BI 平台保持为 SAP 打开两个连接。</p>
每个连接的使用次数	<p>指定允许每个连接登录到 SAP 系统多少次。</p> <p>例如，如果将“每个系统的最大并发连接数”设置为 2，且将“每个连接的使用次数”设置为 3，则当一个连接上有 3 个登录时，BI 平台将关闭并重启该连接。</p>

设置	说明
“并发用户数”和“命名用户数”	<p>指定新用户将使用并发用户许可还是命名用户许可。</p> <p>并发许可指定可同时连接到 BI 平台的用户数。这种类型的许可模式非常灵活，因为少量的并发许可就可以支持大量用户。例如，根据用户访问系统的频率和时长，一份 100 个用户的并发许可可能支持 250、500 或 700 个用户。</p> <p>命名用户许可与用户关联，并允许用户基于他们的用户名和密码访问系统。这样，不管连接了多少其他用户，命名用户都能够访问系统。</p> <p>注意： 所选的选项不会更改 BI 平台中已安装的用户许可的数目或类型。系统必须具有相应的许可。</p>
导入全名、电子邮件地址和其他属性	<p>为 SAP 身份验证插件指定优先级。</p> <p>这将导入 SAP 帐户中使用的全名和说明，并将其与用户对象一起存储在 BI 平台中。</p>
设置 SAP 属性绑定相对于其他属性绑定的优先级	<p>指定绑定 SAP 用户属性（全名和电子邮件地址）的优先级。</p> <p>如果将该选项设置为“1”，则在启用了 SAP 和其他插件（Windows AD 和 LDAP）的情况下，SAP 属性具有优先级。如果选项设置为“3”，则已启用的其他插件的属性具有优先级。</p>

设置下列选项配置 SAP 单一登录服务：

设置	说明
系统 ID	在执行 SAP 单一登录服务时，BI 平台提供给 SAP 系统的系统标识符。
浏览	单击以上生成的密钥存储文件从而启用 SAP 单一登录。也可以手动输入文件的完整路径。
密钥存储密码	提供访问密钥存储文件所需的密码。
私钥密码	提供访问与密钥存储文件相对应的证书所需的密码。该证书存储在 SAP 系统上
私钥别名	提供访问密钥存储文件所需的别名。

4 单击“更新”。

相关主题

- 第 280 页上的[“配置 SAP 身份验证”](#)

9.5.4.2 更改内容文件夹根目录

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“SAP”链接。
- 3 在“内容文件夹根目录”字段中单击“选项”并键入文件夹名称。
在此处键入的文件夹名称是您希望 BI 平台开始从中复制 BW 文件夹结构的文件夹。
- 4 单击“更新”。
- 5 在 BW 内容管理工作台中，展开“Enterprise 系统”。
- 6 展开“可用系统”，并双击 BI 平台所连接的系统。
- 7 单击“布局”选项卡，并在“内容基准文件夹”中键入要在 BI 平台中用作 SAP 根文件夹的文件夹（例如 /SAP/2.0/）。

9.5.5 导入 SAP 角色

通过将 SAP 角色导入到 BI 平台，可以允许角色成员使用其常用 SAP 凭据登录系统。此外，还可以启用单一登录，以使 SAP 用户在 SAP GUI 或 SAP Enterprise Portal 中访问报表时能够自动登录到 BI 平台。

注意：

启用 SSO 通常有许多要求。其中可能包括使用具有 SSO 功能的驱动程序和应用程序，以及确保您的服务器和 Web 服务器位于同一域中。

对于导入的每个角色，BI 平台都会生成一个组。每个组都使用以下规则进行命名：系统 ID~客户端编号@角色名称。可以在 CMC 的“用户和组”管理区域中查看这些新组。还可以使用这些组在 BI 平台中定义对象安全性。

当为进行发布而配置 BI 平台以及将角色导入到系统时，请考虑下面三个主要类别的用户：

- BI 平台管理员

Enterprise 管理员配置系统，以发布来自 SAP 的内容。他们在 BI 平台中导入适当的角色、创建所需文件夹并将权限分配给这些角色和文件夹。

- 内容发布者

内容发布者是指那些有权将内容发布到角色的用户。此用户类别的作用是将常规角色成员与有权发布报表的用户区别开来。

- 角色成员

角色成员是属于内容承载角色的用户。也就是说，这些用户属于报表被发布到的角色。对于发布到角色成员所属角色的任何报表，他们拥有“查看”、“按需查看”以及“计划”权限。但是，常规角色成员不能发布新内容，也不能发布内容的已更新版本。

在第一次发布之前，必须将所有内容发布角色和所有内容承载角色导入到 BI 平台中。

注意：

强烈建议您保持角色活动的区别。例如，虽然可以从管理员角色进行发布，但更好的做法是只从内容发布者角色进行发布。此外，内容发布角色的功能只是定义哪些用户可以发布内容。因此，内容发布角色不应包含任何内容；内容发布者应发布到正常的角色成员可以访问的内容承载角色。

相关主题

- 第 112 页上的[“权限在 BI 平台中如何运作”](#)
- 第 120 页上的[“在 CMC 中管理对象的安全设置”](#)

9.5.5.1 导入 SAP 角色

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“SAP”链接。
- 3 在“选项”选项卡上，根据许可协议而定，选择“并行用户数”或“命名用户数”。
该选项不会更改 BI 平台中已安装的用户许可的数目或类型。您的系统必须有适当的许可可用。
- 4 单击“更新”。
- 5 在“角色导入”选项卡上，从“逻辑系统名”列表中选择合适的权利系统。
- 6 在“可用角色”区域中，选择要导入的角色，然后单击“添加”。
- 7 单击“更新”。

9.5.5.2 验证是否正确导入了角色和用户

开始该任务前，请记下属于映射至 BI 平台的某个角色的 SAP 用户的用户名和密码。

- 1 对于 Java BI 启动板，请转到 <http://webserver:portnumber/BOE/BI>。
将 webserver 替换为 Web 服务器的名称，并将 portnumber 替换为 BI 平台的端口号。可能需要咨询管理员，以了解 Web 服务器的名称、端口号或要输入的 URL。

- 2 在“身份验证类型”列表中，选择“SAP”。

注意：

默认情况下，“身份验证类型”列表在 BI 启动板中是隐藏的。如果列表不可见，请让系统管理员启用 `BIlaunchpad.properties` 文件中的“身份验证类型”列表。

- 3 输入要登录的 SAP 系统和系统客户端。
- 4 输入映射的用户的用户名和密码。
- 5 单击“登录”。

以选定用户的身份登录到 BI 启动板。

9.5.5.3 更新 SAP 角色和用户

启用 SAP 身份验证后，必须对已导入到 BI 平台的映射角色计划和运行定期更新。这将确保 SAP 角色信息准确地反映在平台中。

有两个选项可用于为 SAP 角色运行和计划更新：

- 仅更新角色：使用此选项，将仅更新当前映射的角色之间的链接，这些角色已导入到 BI 平台中。如果希望经常运行更新，并且考虑系统资源的使用，则建议使用该选项。如果仅更新 SAP 角色，则不会创建新用户帐户。
- 更新角色和别名：此选项不仅更新角色之间的链接，还会在 BI 平台中为添加到 SAP 系统中的角色的用户别名创建新的用户帐户。

注意：

如果未指定在启用 SAP 身份验证时自动为更新创建用户别名，则不会为新别名创建帐户。

9.5.5.3.1 为 SAP 角色计划更新

在 BI 平台中映射角色之后，必须指定系统更新角色的方式。

- 1 单击“用户更新”选项卡。
- 2 单击“仅更新角色”部分或“更新角色和别名”区域内的“计划”。

提示：

要立即运行更新，请单击“立即更新”。

提示：

如果希望经常运行更新并且考虑系统资源的使用，则使用“仅更新角色”选项。对角色和别名都进行更新占用系统的时间会比较长。

“重复发生”对话框随即出现。

- 3 从“运行对象”列表中选择一项，并在所提供的字段中填写所有所需的计划信息。

在计划更新时，可以从下表中概述的重复发生模式中进行选择：

重复发生模式	说明
每小时	更新将每小时运行一次。 指定其开始时间以及开始和结束日期。
每天	更新将每天或每 n 天（n 为指定的天数）运行。可指定其开始时间以及开始和结束日期。
每周	更新将每周运行一次或每周运行数次。可指定运行日期、运行开始时间，以及开始和结束日期。
每月	更新将每月或每隔几个月运行一次。 可指定其开始时间以及开始和结束日期。
每月的第 N 天	更新将在每月的特定一天运行。可以指定将在月中的哪一天以及在何时运行，也可以指定开始和结束日期。
每月的第一个星期一	更新将在每月的第一个星期一运行。可以指定更新将在何时运行，以及开始和结束日期。
每月的最后一天	更新将在每月的最后一天运行。可以指定更新将在何时运行，以及开始和结束日期。
每月第 N 周的第 X 天	更新将在月中某指定周的指定一天运行。可以指定更新将在何时运行，以及开始和结束日期。
日历	更新将在之前所创建的日历中指定的日期运行。

- 4 单击“计划”。

计划的下一次角色更新的日期显示在“用户更新”选项卡中。

提示：

要取消计划的下一次更新，请单击“仅更新角色”区域或“更新角色和别名”区域内的“取消计划的更新”。

9.5.6 配置安全网络通讯（SNC）

本节介绍如何配置 SNC，这是设置 SAP 对 BI 平台身份验证过程的一个步骤

在设置 SAP 和 BI 平台系统之间的信任前，必须确保将 SIA 配置为在已为 SNC 设置的帐户下启动和运行。同时还必须将 SAP 系统配置为信任 BI 平台。

相关主题

- 第 291 页上的“[SAP 服务器端信任概述](#)”

9.5.6.1 SAP 服务器端信任概述

本节提供在 SAP Web 应用程序服务器（6.20 版及更高版本）和 SAP BusinessObjects Business Intelligence 平台之间配置服务器端信任的过程。如果正在使用多处理环节报表群发（对于报表查询依赖于用户上下文的发布），则需要设置服务器端信任。

服务器端信任涉及无密码模拟。要在不提供密码的情况下模拟 SAP 用户，必须使用比常规用户名和密码更安全的方法，通过 SAP 识别用户。（拥有 SAP_ALL 授权配置文件的 SAP 用户无法在不知道另一个 SAP 用户密码的情况下模拟该 SAP 用户。）

使用 SAP 密码库启用服务器端信任

要使用 SAP Cryptographic Library 为 BI 平台启用服务器端信任，必须在通过经注册的安全网络通信（SNC）提供程序进行身份验证的凭据下运行相关服务器。这些凭据在 SAP 内配置，可以在不提供密码的情况下进行模拟。对于 BI 平台，需要在这些 SNC 凭据下运行报表群发所涉及的服务器，如自适应作业服务器。

需要 32 位 SNC 二进制用于 32 位进程；64 位 SNC 二进制用于 64 位进程。SAP Cryptographic Library 和 BI 平台一起安装。请注意，SAP Cryptographic Library 只能用于设置服务器端信任。SAP Cryptographic Library 可用于 Windows 和 Unix。

有关 SAP Cryptographic Library 的更多信息，请参阅 SAP 网站上的 SAP 注释 711093、597059 和 397175。

需要为 SAP 服务器和 BI 平台分配提供彼此身份的证书。每个服务器都将拥有自己的证书和一个可信方证书的列表。要在 SAP 与 BI 平台之间配置服务器端信任，需要创建一组受密码保护的证书，称之为“个人安全环境（PSE）”。本节介绍如何设置和维护 PSE，以及如何利用 BI 平台处理服务器安全地关联它们。

客户端与服务器 SNC

在客户端 SNC 中，SNC 名称标识符被映射到 SU01 中的一个（或多个）SAP 用户名。在发送登录请求时，SNC 名称将与 SAP 名称一起传递给 SAP 系统，但不会发送密码。如果将 SNC 名称映射到指定的 SAP 名称，则允许登录。用于直接应用程序主机登录的客户端登录字符串如下所示：

```
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"
```

要使此登录成功，必须将 SAP 用户 USER123 映射到 SU01 中的 p:CN=TheUser, O=TheCompany, C=US。另一方面，在服务器 SNC 中，不要求在 SNC 名称标识符和 SAP 用户名之间进行显式映射。相反，系统将在事务 SNC0 中对 SNC 名称进行配置，以允许它为任何用户执行模拟形式的登录，而无需提供此用户的密码。例如：

```
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
```

与客户端登录相比，服务器 SNC 模拟登录（或通过外部 ID 进行的登录）的功能更强大。通过使用这种登录，可以访问系统中的任何 SAP 用户帐户。其他外部 ID 登录选项包括登录权证和 X.509 客户端证书。

SAP BusinessObjects BI 平台服务器的职责

就单一登录（SSO）而言，特定 BI 平台服务器与 SAP 集成相关联。下表列出了这些服务器及其特定职责范围所需的 SNC 类型。

服务器	SNC 类型	职责范围
Web 应用程序服务器	客户端	SAP 身份验证角色列表
BW 发布器服务	服务器	Crystal 报表动态参数选取列表和个性化
CMS	客户端	密码、权证、检查角色成员资格和用户列表
页面服务器	服务器	按需查看 Crystal 报表
作业服务器	服务器	计划 Crystal 报表
Web Intelligence 处理服务器	服务器	查看和计划 Web Intelligence 报表和值列表（LOV）提示
多维分析服务	服务器	分析

注意：

Web 应用程序服务器和 CMS 使用客户端 SNC，因此需要将 SNC 名称显式映射到 SAP 用户名。将在事务 SU01 或 SM30 中为表 USRACL 指定此操作。

9.5.6.2 为服务器端信任配置 SAP

服务器端信任仅适用于 Crystal 报表和基于 Universes (.unv) 的 Web Intelligence 报表。必须将 SNC 设置为与 BI 平台结合使用。有关疑难解答协助的更多信息，请参阅 SAP 服务器随附提供的 SAP 文档。

9.5.6.2.1 为客户端信任配置 SAP

- 1 对于 SAP 和运行 SAP 的计算机，确保拥有 SAP 管理员凭据，同样，对于 BI 平台以及运行它的一台或多台计算机，确保也拥有管理员凭据。
- 2 在 SAP 计算机上，确保 SAP Cryptographic Library 和 SAPGENPSE 工具位于 <驱动器>:\usr\sap\SID\SYS\exe\run\ 目录（在 Windows 上）。
- 3 创建名为“SECUDIR”的环境变量，该变量指向“ticket”文件所在的目录。

注意：

运行 SAP 的“disp+work”进程的用户必须能够访问该变量。

- 4 在 SAP GUI 中，转到事务 RZ10，然后在“扩展维护”模式下更改实例配置文件。
- 5 在“配置文件编辑”模式下，将 SAP 配置文件变量指向 Cryptographic Library，并为 SAP 系统提供一个可分辨名称（DN）。这些变量应遵循以下 LDAP 命名约定：

标记	含义	说明
CN	公用名称	证书所有者的日常名称。
OU	组织单位	例如，PG 代表产品组。
O	组织	颁发证书的组织的名称。
C	国家/地区	组织所在的国家/地区。

例如，对于 R21：p:CN=R21, OU=PG, O=BOBJ, C=CA

注意：

前缀“p:”代表 SAP Cryptographic Library。在引用 SAP 内部的可分辨名称时，必须使用此前缀，但在 STRUST 中或使用 SAPGENPSE 检查证书时，此前缀不可见。

- 6 输入以下配置文件值，以在必要时对 SAP 系统进行替换：

配置文件变量	值
ssf/name	SAPSECULIB
ssf/ssfapi_lib	sapcrypto lib 的完整路径
sec/libsapsecu	sapcrypto lib 的完整路径
snc/gssapi_lib	sapcrypto lib 的完整路径
snc/identity/as	SAP 系统的可分辨名称

7. 重新启动 SAP 实例。
8. 当系统再次运行时，请登录并转到事务 STRUST，此事务现在应具有 SNC 和 SSL 的附加条目。
9. 右击 SNC 节点，然后单击“创建”。
此时将出现在 RZ10 中指定的标识。
10. 单击“确定”。
11. 要为 SNC PSE 分配密码，请单击锁图标。

注意：

请勿丢失此密码。用户每次查看或编辑 SNC PSE 时，STRUST 都会提示输入此密码。

12. 保存更改。

注意：

如果不保存所做的更改，当启用 SNC 时，应用程序服务器不会再次启动。

13. 返回事务 RZ10，然后添加其余的 SNC 配置文件参数：

配置文件变量	参数
snc/accept_insecure_rfc	1
snc/accept_insecure_r3int_rfc	1
snc/accept_insecure_gui	1
snc/accept_insecure_cplic	1
snc/permit_insecure_start	1
snc/data_protection/min	1
snc/data_protection/max	3
snc/enable	1

最低保护级别设置为“仅身份验证”(1)，最高保护级别为“隐私”(3)。snc/data_protection/use 值定义在此情况下使用“仅身份验证”，但也可能为(2)(完整性)、(3)(隐私)以及(9)(可能的最高保护级别)。snc/accept_insecure_rfc、snc/accept_insecure_r3int_rfc、snc/accept_insecure_gui 和 snc/accept_insecure_cplic 值设置为(1)，确保以前(和潜在不安全)的通信方法仍然可用。

14. 重新启动 SAP 系统。

现在必须为服务器端信任配置 BI 平台。

9.5.6.3 为服务器端信任配置 BI 平台

要为服务器端信任配置 BI 平台，需要执行以下步骤。请注意，这些步骤是基于 Windows 的，不过因为 SAP 工具是一个命令行工具，因此在 Unix 上执行的步骤也与此非常相似。

- 。 1 设置环境
- 。 2 生成个人安全环境（PSE）
- 。 3 配置 BI 平台服务器
- 。 4 配置 PSE 访问
- 。 5 配置 SAP 身份验证 SNC 设置
- 。 6 设置 SAP 专用服务器组

相关主题

- 第 295 页上的[“设置环境”](#)
- 第 296 页上的[“生成 PSE”](#)
- 第 297 页上的[“配置 BI 平台服务器”](#)
- 第 298 页上的[“配置 PSE 访问”](#)
- 第 298 页上的[“配置 SAP 身份验证 SNC 设置”](#)
- 第 299 页上的[“使用服务器组”](#)

9.5.6.3.1 设置环境

BI 平台包括一个默认 SAP Cryptographic Library。如果使用默认库，只需要执行稍后两个步骤：创建子文件夹，并添加环境变量。否则，要配置 SAP Cryptographic Library 的自定义副本，请执行所有步骤。

可在此位置找到默认的 SAP Cryptographic Library。

- Windows: 安装目录\sap\sapcrypto.dll
- Unix: 安装目录/sap/libsapcrypto.so

开始之前，请确保：

- 已在运行 BI 平台处理服务器的主机上展开 SAP Cryptographic Library。
 - 已配置相应的 SAP 系统，以便使用 SAP Cryptographic Library 作为 SNC 提供商。
- 必须先设置库、工具以及存储 PSE 的环境，然后才能开始 PSE 维护。
- 1 将 SAP Cryptographic Library（包括 PSE 维护工具）复制到运行 BI 平台的计算机的文件夹上。
例如：C:\Program Files\SAP\Crypto
 - 2 将文件夹添加到 PATH 环境变量。
 - 3 添加系统范围内的环境变量 SNC_LIB，该变量指向 Cryptographic Library。
例如：C:\Program Files\SAP\Crypto\sapcrypto.dll

注意：

最大路径长度为 100 个字符。

- 4 创建名为“sec”的子文件夹。
例如：C:\Program Files\SAP\Crypto\sec
- 5 添加系统范围内的环境变量 SECUDIR，该变量指向 sec 文件夹。

相关主题

- 第 292 页上的“[为服务器端信任配置 SAP](#)”

9.5.6.3.2 生成 PSE

当相关的 BI 平台服务器具有 PSE 而且该 PSE 与 SAP 关联时，SAP 接受 BI 平台服务器作为受信任的实体。SAP 与 BI 平台组件之间的信任关系通过共享各自证书的公共版本建立。第一步是为 BI 平台生成 PSE，以自动生成自己的证书。

- 1 打开命令提示符，然后从 Cryptographic Library 文件夹内运行 `sapgenpse.exe gen_pse -v -p BOE.pse`。
- 2 选择要用于 BI 平台系统的个人识别号（PIN）和识别名称（DN）。
例如 CN=MyBOE01, OU=PG, O=BOBJ, C=CA。
现在用户拥有一个默认 PSE 和它自己的证书。
- 3 使用以下命令导出 PSE 中的证书：

```
sapgenpse.exe export_own_cert -v -p BOE.pse -o MyBOECert.crt
```

- 4 在 SAP GUI 中，转到事务 STRUST，并打开与 SAP 系统相关联的系统 PSE。
系统可能会提示用户输入已分配给此系统 PSE 的密码。
- 5 通过单击 STRUST 事务屏幕底部左侧的“Import Certificate”（导入证书）按钮，导入之前创建的 MyBOECert.crt 文件。

通过 SAPGENPSE 导出的证书采用 Base64 编码。请确保在导入这些文件时选择 Base64。

- 6 要将 BI 平台证书添加到 SAP 服务器的 PSE 证书列表，请单击“Add to certificate list”（添加到证书列表）按钮。
- 7 保存在 STRUST 中所做的更改。
- 8 单击“Export certificate”（导出证书）按钮，然后为该证书提供一个文件名。
例如，MySAPCert.crt。

注意：

格式应当仍保留 Base64。

- 9 转到事务 SNC0。
10. 添加新条目，其中：
 - 系统 ID 可为任意值，但要反映用户的 BI 平台系统。
 - SNC 名称应为在创建 BI 平台 PSE 时（步骤 2 中）提供的识别名称（前缀为“p:”）。
 - 同时选中“RFC 的条目已激活”和“外部标识的条目已激活”复选框：
11. 要将导出的证书添加到 BI 平台 PSE，请在命令提示符位置运行以下命令：

```
sapgenpse.exe maintain_pk -v -a MySAPCert.crt -p BOE.pse
```

SAP Cryptographic Library 安装在 BI 平台计算机上。用户已创建一个 PSE，BI 平台服务器将使用它向 SAP 服务器标识自身。SAP 和 BI 平台 PSE 已交换证书。SAP 允许有权访问 BI 平台 PSE 的实体执行 RFC 调用和无密码模拟。

相关主题

- 第 297 页上的[“配置 BI 平台服务器”](#)

9.5.6.3.3 配置 BI 平台服务器

为 BI 平台生成 PSE 之后，必须为 SAP 处理配置相应的服务器结构。以下过程将为 SAP 处理服务器创建一个节点，以便可以在节点级别设置操作系统凭据。

注意：

在此版本的 BI 平台中，不必再在中央配置管理器（CCM）中配置服务器。而是改为必须创建一个新的服务器智能代理（SIA）。

- 1 在 CCM 中，为 SAP 处理服务器创建一个新节点。
为该节点指定相应的名称（如 SAPProcessor）。
- 2 在 CMC 中，将所需的服务器添加至新节点，然后启动新服务器。

9.5.6.3.4 配置 PSE 访问

配置 BI 平台节点和服务端之后，需要使用 SAPGENPSE 工具配置 PSE 访问。

- 1 在命令提示符位置运行以下命令：

```
sapgenpse.exe seclogin -p SBOE.pse
```

注意：

系统将提示输入 PSE PIN。如果在 BI 平台 SAP 处理服务器使用的相同凭据下运行工具，则不需要指定用户名。

- 2 要验证是否已建立单一登录（SSO）链接，请使用以下命令列出 PSE 的内容：

```
sapgenpse.exe maintain_pk -l
```

结果应类似于：

```
C:\Documents and Settings\username\Desktop\sapcrypto.x86\ntintel>sapgenpse.exe
maintain_pk -l
maintain_pk for PSE "C:\Documents and Settings\username\My Documents\snc\sec\bobjsapproc.pse"
*** Object <PKList> is of the type <PKList_OID> ***

1. -----
Version:                0 (X.509v1-1988)
SubjectName:            CN=R21Again, OU=PG, O=BOBJ, C=CA
IssuerName:             CN=R21Again, OU=PG, O=BOBJ, C=CA
SerialNumber:           00
Validity - NotBefore:   Wed Nov 28 16:23:53 2007 (071129002353Z)
                   NotAfter: Thu Dec 31 16:00:01 2037 (380101000001Z)
Public Key Fingerprint: 851C 225D 1789 8974 21DB 9E9B 2AE8 9E9E
SubjectKey:             Algorithm RSA (OID 1.2.840.113549.1.1.1), NULL
```

```
C:\Documents and Settings\username\Desktop\sapcrypto.x86\ntintel>
```

在成功运行 seclogin 命令之后，将不会再提示输入 PSE PIN。

注意：

如果遇到 PSE 访问问题，请使用 -O 自变量指定 PSE 访问权限。例如，要将 PSE 访问权限授予特定域中的特定用户，请在 Windows 上键入此命令：

```
sapgenpse seclogin -p SBOE.pse -O SYSTEM
```

9.5.6.3.5 配置 SAP 身份验证 SNC 设置

配置 PSE 访问之后，必须在 CMC 中配置 SAP 身份验证设置。

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“SAP”链接。

将显示权利系统设置。

- 3 在“SAP 身份验证”页面上单击“SNC 设置”选项卡。
- 4 从“逻辑系统名称”列表中选择权利系统。
- 5 在“基本设置”下选择“启用安全网络通信（SNC）”。
- 6 选择“使用默认值”选项接受库的默认路径，或选择“定义自定义路径”选项，选择其他位置。
- 7 在“保护质量”下，选择一个保护级别。
例如，选择“身份验证”。

注意：

不要超出在 SAP 系统上配置的保护级别。该保护级别是可自定义的保护级别，并由组织需求及其 SNC 库的功能所决定。

- 8 在“相互身份验证设置”下，输入 SAP 系统的 SNC 名称。

SNC 名称格式取决于 SNC 库。使用 SAP 加密库，可分辨名称建议遵循 LDAP 命名约定，且前缀为 p:。

- 9 请确保在运行 BI 平台服务器时使用的凭据的 SNC 名称显示在“Enterprise 系统的 SNC 名称”框中。

在配置了若干 SNC 名称的情况下，应将此字段留空。

- 10 提供 SAP 系统和 BI 平台 PSE 的 DN。

9.5.6.3.6 使用服务器组

除非运行处理（Crystal Reports 或 Web Intelligence）服务器时使用的凭据具有 PSE 访问权限，否则，必须创建一个特定的服务器组，其中仅包含这些服务器以及所需的支持服务器。有关更多信息以及各种 BI 平台服务器的说明，请参阅“体系结构”一章。

在为 SAP 内容配置内容处理服务器时，有三个选项可供选择：

- 1 保持单一 SIA，其中包括使用具有 PSE 访问权限的凭据运行的所有 BI 平台服务器。这是最简单的选项，不需要创建服务器组。这种方法最不安全，因为有些多余的服务器也具有 PSE 访问权限。

- 。 2 创建第二个具有 PSE 访问权限的 SIA，并在其中添加 Crystal Reports 或 Web Intelligence 处理服务器。从原始 SIA 中删除重复的服务器。不需要创建服务器组，但只有较少的服务器具有 PSE 访问权限。
- 。 3 创建一个专用于具有 PSE 访问权限的 SAP 的 SIA。在其中添加 Crystal Reports 或 Web Intelligence 处理服务器。在这种选项中，这些服务器上应只运行 SAP 内容，更重要的是，SAP 内容应只在这些服务器上运行。由于此方案需要将内容传送到某些服务器，因此，必须为 SIA 创建服务器组。

使用服务器组的准则

服务器组需要引用专用于处理 SAP 内容的 SIA。此外，服务器组还需要引用以下服务器：

- 自适应服务器
- 自适应作业服务器

需要使用最严格的关联，将所有 SAP 内容、Web Intelligence 文档和 Crystal 报表与服务器组相关联，即它们必须在该组的服务器上运行。在对象级别完成这种关联后，服务器组设置应被传播到用于直接计划和发布的设置中。

为防止在 SAP 特定处理服务器上处理其他（非 SAP）内容，应创建另一个服务器组，其中包含原始 SIA 中的所有服务器。建议用户在此内容与非 SAP 服务器组之间建立严格的关联。

9.5.6.4 配置多处理环节发布

多处理环节发布疑难解答

如果遇到多处理环节发布问题，请对用于 SAP 的 Crystal Reports (CR) 或多维数据访问 (MDA) 驱动程序启用跟踪，并查看用于每个作业或收件人的登录字符串。这些登录字符串应类似于：

```
SAP: Successfully logged on to SAP server.  
Logon handle: 1. Logon string: CLIENT=800 LANG=en  
ASHOST="vanrdw2k107.sap.crystal.d.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
```

登录字符串必须具有相应的 EXTIDTYPE=UN（用于用户名），EXTIDDATA 应是收件人的 SAP 用户名。在本例中，登录尝试成功。

9.5.6.5 与安全网络通信集成的工作流

BI 平台支持为 SAP 组件之间的身份验证和数据加密实现安全网络通信（SNC）的环境。如果已部署 SAP Cryptographic Library（或其他使用 SNC 接口的外部安全产品），则必须设置一些其他值，才能在安全环境中有效集成 BI 平台。

要将平台配置为使用安全网络通信，必须完成以下任务：

- 1 将 BI 平台服务器配置为在适当用户帐户下启动和运行。
- 2 将 SAP 系统配置为信任 BI 平台系统。
- 3 在中央管理控制台中的 SNC 链接上配置 SNC 设置。
- 4 将 SAP 角色和用户导入到 BI 平台。

相关主题

- 第 287 页上的[“导入 SAP 角色”](#)
- 第 292 页上的[“为服务器端信任配置 SAP”](#)
- 第 295 页上的[“为服务器端信任配置 BI 平台”](#)

9.5.6.6 在中央管理控制台中配置 SNC 设置

在配置 SNC 设置前，必须为 BI 平台添加新的权利系统，确保 SNC 库文件位于已知目录中，并创建环境变量 RFC_LIB 指向此文件。

- 1 在“SAP 身份验证”页面上单击“SNC 设置”选项卡。
- 2 从“逻辑系统名称”列表中选择权利系统。
- 3 在“基本设置”下选择“启用安全网络通信（SNC）”。
- 4 如果要为使用 .unx Universe 或 OLAP BICS 连接配置 SAP 身份验证并计划使用 STS，请选中“阻止不安全的传入 RFC 连接”复选框。
- 5 选择“使用默认值”选项接受库的默认路径，或选择“定义自定义路径”选项，选择其他位置。应用程序服务器和 CMS 必须位于相同类型的操作系统上，而且具有相同的加密库路径。
- 6 在“保护质量”下，选择一个保护级别。
例如，选择“身份验证”。

注意：

该保护级别是可自定义的保护级别，并由组织需求及其 SNC 库的功能所决定。

- 7 在“相互身份验证设置”下，输入 SAP 系统的 SNC 名称。

SNC 名称格式取决于 SNC 库。使用 SAP 加密库，可分辨名称建议遵循 LDAP 命名约定，且前缀为 p:。

- 8 请确保在运行 BI 平台服务器时使用的凭据的 SNC 名称显示在“Enterprise 系统的 SNC 名称”框中。
在已配置多个 SNC 名称的情况下，请将此框留空。
- 9 单击“更新”。
- 10 在“SAP 身份验证”页上，单击“权利系统”选项卡。
语言选项下将出现 SNC 名称选项。
- 11 在“SNC 名称”框中，输入在 SAP BW 服务器上配置的 SNC 名称。
此名称应该与用于将 SAP 系统配置为信任 BI 平台的名称相同。
如果是使用 Insight to Action 框架启用报表到报表接口，则启用 SNC 或对 SNC 设置的更改生效可能需要花费 10 分钟。要触发即刻更新，请重新启动运行 Insight to Action 服务的自适应处理服务器。

相关主题

- 第 282 页上的[“连接到 SAP 权利系统”](#)

9.5.6.7 将权利用户与 SNC 名称相关联

- 1 登录到 SAP BW 系统，然后执行事务 SU01。
“用户维护：初始屏幕”将打开。
- 2 在“用户”字段中，键入指定为权利用户的 SAP 帐户的名称，然后在工具栏上单击“更改”。
“维护用户”屏幕将打开。
- 3 单击“SNC”选项卡。
- 4 在“SNC 名称”字段中，键入在上面步骤 2 中输入的 SNC USER ACCOUNT。
- 5 单击“保存”。

9.5.6.8 向 SNC 访问控制列表添加一个系统 ID

- 1 登录到 SAP BW 系统，然后执行事务 SNC0。

将打开屏幕：修改视图“SNC：系统的存取控制列表（ACL）：总览”。

- 2 在工具栏上单击“New Entries”（新条目）。

“新条目：所添加条目的细节”屏幕将会打开。

- 3 在“系统标识”字段中键入 BI 平台计算机的名称。
- 4 在“SNC 用户名”字段中输入 p:<SNC USER NAME>，其中 SNC USER NAME 表示在配置 BI 平台服务器时使用的帐户。

注意：

如果 SNC 提供者是 gssapi32.dll，请在指示 SNC USER NAME 时使用大写字母。在指定用户帐户时必须包含域名。例如：domain\username。

- 5 选择“RFC 条目已激活”和“外部标识的条目已激活”。
- 6 清除所有其他选项，然后单击“保存”。

9.5.7 设置对 SAP 系统的单一登录

在集成环境中，不同 BI 平台客户端和后端服务要与 NetWeaver ABAP 后端系统交互。设置从 BI 平台到这些（通常是 BW）后端系统的单一登录会很有帮助。将 ABAP 系统配置为外部身份验证系统后，将使用专有的 SAP 标记提供一种机制，以支持连接到 NetWeaver ABAP 系统的所有 BI 平台客户端和服务的单一登录。

要启用对 SAP 数据库的单一登录，需要创建一个 keystore 文件和对应的证书。可以使用 keytool 命令行程序生成该文件和证书。默认情况下，keytool 程序安装在每个平台的 sdk/bin 目录下。

需要使用 CMC 将证书添加到 SAP ABAP BW 系统和 BI 平台中。

注意：

必须先配置 SAP 身份验证插件，然后才能设置对 SAP BW 使用的数据库的单一登录。

9.5.7.1 生成密钥存储文件

PKCS12Tool 程序用于生成为 SAP 数据库设置单一登录所必需的密钥存储文件和凭据。下表列出了每个受支持平台上 PKCS12Tool.jar 的默认位置：

平台	默认位置
Windows	<安装目录>\SAP BusinessObjects Enterprise XI 4.0\java\lib
Unix	sap_bobj/enterprise_xi40/java/lib

- 1 启动命令提示，并导航到 PKCS12Tool 程序所在的目录。
- 2 若要以默认设置生成密钥存储文件，请运行以下命令：

```
java -jar PKCS12Tool.jar
```

文件 cert.der 和 keystore.p12 在相同目录下生成。文件包含以下默认值：

参数	默认值
-keystore	keystore.p12
-alias	myalias
-storepass	123456
-dname	CN=CA
-validity	365
-cert	cert.der

提示：

若要覆盖默认值，请与 -? 参数一起运行工具。此时将显示以下消息：

```
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>
```

可使用这些参数覆盖默认值。

9.5.7.2 导出公钥证书

需要为密钥存储文件创建并导出证书。

- 1 启动一个命令提示符并导航到 keytool 程序所在的目录
- 2 要使用以下命令为密钥存储文件导出密钥证书：

```
keytool -exportcert -keystore <keystore> -storetype pkcs12 -file <filename>
-alias <alias>
```


将 <keystore> 替换为密钥存储文件的名称。
将 <filename> 替换为证书的名称。
将 <alias> 替换为用于创建密钥存储文件的别名。

- 看到提示后，输入为密钥存储文件提供的密码。
现在 keytool 程序所在的目录中已经有了一个密钥存储文件和一个证书。

9.5.7.3 将证书文件导入目标 ABAP SAP 系统

要执行以下任务，需要 BI 平台部署的密钥存储文件和关联的证书：

注意：

此操作仅可在 SAP ABAP 系统上执行。

- 使用 SAP GUI 连接到 SAP ABAP BW 系统。
注意：
应作为具有管理权限的用户进行连接。
- 在 SAP GUI 中执行 STRUSTSS02。
系统已准备导入证书文件。
- 转到“证书”选项卡。
- 确保选中“Use Binary option”（使用二进制选项）复选框。
- 单击文件路径按钮以指向证书文件所在的位置。
- 单击绿色选中标记。
上载证书文件。
- 单击“Add to Certificate List”（添加到证书列表）。
证书将显示在证书列表中。
- 单击“Add to ACL”（添加到 ACL），并指定一个系统 ID 和客户端。
该系统 ID 必须与用于向 SAP BW 标识 BI 平台系统的系统 ID 相同。
证书已添加到访问控制列表（ACL）。客户端应指定为 000。
- 保存设置并退出。
更改将保存在 SAP 系统中。

9.5.7.4 在 CMC 中设置对 SAP 数据库的单一登录

要执行以下过程，需要使用管理员帐户访问 SAP 安全插件。

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“SAP”链接，然后单击“选项”选项卡。
如果尚未导入任何证书，则“SAP SSO 服务”部分中会显示以下消息：
未上载任何密钥存储文件
- 3 在所提供的字段中指定 BI 平台系统的系统 ID。
该 ID 应该与在目标 SAP ABAP 系统中导入证书时使用的值相同。
- 4 单击“浏览”按钮以指向密钥存储文件。
- 5 提供以下必需的详细信息：

字段	必需信息
密钥存储密码	提供访问密钥存储文件所需的密码。此密码是在创建密钥存储文件时指定的。
私钥密码	提供访问与密钥存储文件相对应的证书所需的密码。此密码是在为密钥存储文件创建证书时指定的。
私钥别名	提供访问密钥存储文件所需的别名。别名是在创建密钥存储文件时指定的。

- 6 单击“更新”以提交设置。
成功提交设置后，“系统 ID”字段下会显示以下消息：
已上载密钥存储文件

9.5.7.5 向自适应处理服务器添加安全标记服务

在群集环境中，安全标记服务将单独添加到每台自适应处理服务器。

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击“核心服务”。
“核心服务”下将显示服务器列表。

- 3 右击“自适应处理服务器”并选择“停止服务器”。
在服务器状态变为“已停止”之前，请勿继续操作。
- 4 右击“自适应处理服务器”并选择“选择服务”。
将显示“选择服务”对话框。
- 5 使用“添加”按钮，将“安全标记服务”从“可用服务”列表移到“服务”列表中。
- 6 单击“确定”。
- 7 重新启动自适应处理服务器。

9.5.8 为 SAP Crystal Reports 和 SAP NetWeaver 配置 SSO

默认情况下，BI 平台将配置为允许 SAP Crystal Reports 用户使用单一登录（SSO）访问 SAP 数据。

9.5.8.1 为 SAP NetWeaver 和 SAP Crystal Reports 取消激活 SSO

- 1 在中央管理控制台（CMC）中，单击“应用程序”。
- 2 双击“Crystal Reports 配置”。
- 3 单击“单一登录选项”。
- 4 选择下列驱动程序之一：

驱动程序	显示名称
操作数据存储驱动程序	crdb_ods
Open SQL 驱动程序	crdb_opensql
InfoSet 驱动程序	crdb_infoSet
BW MDX 查询驱动程序	crdb_bwmdx

- 5 单击“删除”。
- 6 单击“保存并关闭”。
- 7 重新启动 SAP Crystal Reports。

9.5.8.2 为 SAP NetWeaver 和 SAP Crystal Reports 重新激活 SSO

按照以下步骤为 SAP NetWeaver (ABAP) 和 SAP Crystal Reports 重新激活 SSO。

- 1 在中央管理控制台 (CMC) 中，单击“应用程序”。
- 2 双击“Crystal Reports 配置”。
- 3 单击“单一登录选项”。
- 4 在“使用 SSO 上下文进行数据库登录”下，键入：

crdb_ods	激活 ODS 驱动程序
crdb_opensql	激活 Open SQL 驱动程序
crdb_bwmdx	激活 SAP BW MDX 查询驱动程序
crdb_infoset	激活 InfoSet 驱动程序

- 5 单击“添加”。
- 6 单击“保存并关闭”。
- 7 重新启动 SAP Crystal Reports。

9.6 PeopleSoft 身份验证

9.6.1 概述

要将 PeopleSoft Enterprise 数据用于 BI 平台，必须为该程序提供有关部署的信息。通过此信息，BI 平台便可以验证用户身份，使其能够使用 PeopleSoft 凭据登录程序。

9.6.2 启用 PeopleSoft Enterprise 身份验证

要允许 BI 平台使用 PeopleSoft Enterprise 信息，BI 平台需要有关如何进行身份验证以登录 PeopleSoft Enterprise 系统的信息。

9.6.2.1 在 BI 平台中启用 PeopleSoft Enterprise 身份验证

- 1 以管理员身份登录到中央管理控制台。
- 2 从“管理”区域中，单击“身份验证”。
- 3 双击“PeopleSoft Enterprise”。
- 将出现“PeopleSoft Enterprise”页面。它包含四个选项卡：“选项”、“域”、“角色”和“用户更新”。
- 4 在“选项”选项卡中，选中“启用 PeopleSoft Enterprise 身份验证”复选框。
- 5 根据 BI 平台部署，在“新建别名”、“更新选项”和“新用户选项”下进行相应更改。
单击“更新”以保存更改，然后进入“域”选项卡。
- 6 单击“域”选项卡。
- 7 在“PeopleSoft Enterprise 系统用户”区域中，键入数据库用户名和密码，以便 BI 平台使用它们登录到 PeopleSoft Enterprise 数据库。
- 8 在“PeopleSoft Enterprise 域”区域中，输入用于连接 PeopleSoft Enterprise 环境的域名和 QAS 地址，然后单击“添加”。

注意：

如果拥有多个 PeopleSoft 域，请为想要访问的任何其他域重复此步骤。输入的第一个域将成为默认域。

- 9 单击“更新”以保存更改。

9.6.3 将 PeopleSoft 角色映射到 BI 平台

BI 平台会自动为映射的每个 PeopleSoft 角色创建一个组。此外，该程序还会创建别名来表示所映射的 PeopleSoft 角色的成员。

可以为创建的每个别名创建一个用户帐户。

但是，如果运行多个系统，且用户在多个系统中具有帐户，则在 BI 平台中创建帐户之前，可以为每个用户分配一个同名的别名。

这样可以减少为 BI 平台中的相同用户创建的帐户数量。

例如，如果运行 PeopleSoft HR 8.3 和 PeopleSoft Financials 8.4，且 30 个用户可以访问这两个系统，那么只为这些用户创建 30 个帐户。如果选择不为每个用户分配同名的别名，则会为 BI 平台中的这 30 个用户创建 60 个帐户。

但是，如果运行多个系统，且用户名相同，则必须为创建的每个别名创建一个新的成员帐户。

例如，如果使用 Russell Aquino（用户名为“raquino”）的用户帐户运行 PeopleSoft HR 8.3，且使用 Raoul Aquino（用户名为“raquino”）的用户帐户运行 PeopleSoft Financials 8.4，则需要为每个用户的别名创建单独的帐户。否则，这两个用户将添加到相同的 BI 平台帐户；他们将能够使用各自的 PeopleSoft 凭据登录到 BI 平台，并且可以访问这两个 PeopleSoft 系统中的数据。

9.6.3.1 将 PeopleSoft 角色映射到 BI 平台

如果 BI 平台 JVM（Java 虚拟机）不具备 PeopleSoft 服务器证书，则需要在以下主要步骤之前执行这些附加步骤：

- 。 1 从 PeopleSoft 服务器中获取 .cer 文件。
- 。 2 将 .cer 文件复制到 安装目录\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security。
- 。 3 从安全目录“安装目录\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin\keytool.exe”中执行以下命令：-import -file peoplesoft 服务器.cer -keystore cacerts -alias peoplesoft 服务器。
- 。 4 重新启动 Web 应用程序服务器。

主要步骤：

- 1 以管理员身份登录到中央管理控制台。
- 2 单击“身份验证”。
- 3 双击“PeopleSoft Enterprise”。
- 4 在“角色”选项卡的“PeopleSoft Enterprise 域”区域中，选择与要映射到 BI 平台的角色相关联的域。

5 使用下列其中一个选项选择希望映射的角色：

- 在“PeopleSoft Enterprise 角色”区域的“搜索角色”框中，输入要查找的角色，并将其映射到 BI 平台，然后单击“>”。
- 从“可用角色”列表中，选择要映射到 BI 平台的角色并单击“>”。

注意：

- 搜索特定用户或角色时，可以使用 % 通配符。例如，要搜索所有以“A”开头的角色，请键入 A%。搜索也区分大小写。
- 如果想从另一个域中映射角色，则必须从可用域列表中选择新的域，以与不同域中的角色匹配。

6 转到“用户更新”选项卡，单击“更新”按钮或计划更新。

7 在“选项”选项卡中，转到“新用户选项”区域，然后选择以下其中一个选项：

- 将每个添加的别名分配给具有相同名称的帐户

如果运行多个 PeopleSoft Enterprise 系统，这些系统中有些用户或多个系统中拥有帐户（且对于不同的系统，不会有用户具有相同的用户名），请选择此选项。

- 为每个添加的别名创建一个新帐户

如果只运行一个 PeopleSoft Enterprise，大部分用户只在一个系统中拥有帐户，或者两个或多个系统中的不同用户的用户名相同，请选择此选项。

8 在“别名更新选项”区域中，选择以下其中一个选项：

- 在发生别名更新时创建新的别名

选择此选项可以为映射到 BI 平台的每个用户创建一个新别名。系统将为没有 BI 平台帐户的用户，或者为所有用户（如果选择了“为每个添加的别名创建一个新帐户”选项）添加新帐户。

- 仅当用户登录时才创建新的别名

如果想要映射的角色包含许多用户，但只有其中部分用户将使用 BI 平台，请选择此选项。平台不会自动为用户创建别名和帐户。而只会在用户第一次登录到 BI 平台时为用户创建别名（如有必要，也会创建帐户）。这是默认选项。

9 可以在“新用户选项”区域中指定如何创建新用户。

选择以下选项之一：

- 将新用户创建为命名用户。

将新用户帐户配置为使用命名用户许可。命名用户许可与特定用户关联，并允许用户基于他们的用户名和密码访问系统。这样，不管连接了多少其他用户，命名用户都能够访问系统。必须为使用此选项创建的每个用户帐户提供一个命名用户许可。

- 将新用户创建为并发用户。

新用户帐户被配置为使用并发用户许可。并发许可指定可同时连接到 BI 平台的用户数。这种类型的许可模式非常灵活，因为少量的并发许可就可以支持大量用户。例如，根据用户访问 BI 平台的频率和时长，一份 100 个用户的并发许可可能支持 250、500 或 700 个用户。

所选角色现在作为组显示在 BI 平台中。

9.6.3.2 重新映射注意事项

如果将用户添加到已映射到 BI 平台的角色，则需要重新映射该角色，以将用户添加到 BI 平台中。重新映射角色时，用于将用户映射成命名用户或并发用户的选项只影响已添加到角色中的新用户。

例如，首先选择“将新用户创建为命名用户”选项并将某个角色映射到 BI 平台。然后，向同一角色中添加用户，选择“将新用户创建为并发用户”选项并重新映射该角色。

在此情况下，只有该角色中的新用户会作为并发用户映射到 BI 平台，已映射的用户仍然为命名用户。如果首先将用户映射为并发用户，然后更改设置以将新用户重新映射为命名用户，则会出现相同的情况。

9.6.3.3 取消映射角色

- 1 以管理员身份登录到中央管理控制台。
- 2 单击“身份验证”。
- 3 单击“PeopleSoft Enterprise”。
- 4 单击“角色”。
- 5 选择要删除的角色，并单击“<”。
- 6 单击“更新”。

该角色的成员将无法再访问 BI 平台，除非他们拥有其他帐户或别名。

注意：

也可以删除个别帐户，或在将角色映射到 BI 平台之前删除角色中的用户，以禁止特定用户登录。

9.6.4 计划用户更新

为确保 ERP 系统的用户数据更改反映在 BI 平台用户数据中，可以计划进行定期用户更新。这些更新将根据在中央管理控制台（CMC）中配置的映射设置，自动同步 ERP 和 BI 平台用户。

有两个选项可用于运行和计划已导入角色的更新：

- 仅更新角色：使用此选项，将仅更新当前映射的角色之间的链接，这些角色已导入到 BI 平台中。如果希望经常运行更新，而又在意系统资源使用情况的话，可以使用此选项。如果仅更新角色，则不会创建新的用户帐户。
- 更新角色和别名：此选项不仅更新角色之间的链接，还会在 BI 平台中为添加到 ERP 系统的新用户别名创建新的用户帐户。

注意：

如果未指定在启用身份验证时自动为更新创建用户别名，则不会为新别名创建帐户。

9.6.4.1 计划用户更新

将角色映射到 BI 平台后，需要指定系统更新这些角色的方式。

- 1 单击“用户更新”选项卡。
- 2 在“仅更新角色”或“更新角色和别名”区域中单击“计划”。

提示：

如果要立即运行更新，请单击“立即更新”。

提示：

如果希望经常运行更新，而又在意系统资源的使用情况，则可以使用“仅更新角色”选项。对角色和别名都进行更新占用系统的时间会比较长。

“重复发生”对话框随即出现。

- 3 从“运行对象”列表选择一个选项，并提供需要的所有计划信息。

在计划更新时，可以从下表中概述的重复发生模式中进行选择：

重复发生模式	说明
每小时	更新将每小时运行一次。 可以指定将在何时开始，以及开始和结束日期。
每天	更新将每天或每隔指定天数运行一次。可以指定对象将在何时运行，以及开始和结束日期。
每周	更新将每周运行一次。 它可以一周运行一次或多次。可以指定对象运行的具体日期和时间，以及开始和结束日期。
每月	更新将每月或每隔几个月运行一次。 可以指定更新将在何时运行，以及开始和结束日期。

重复发生模式	说明
每月的第 N 天	更新将在每月的特定一天运行。可以指定将在月中的哪一天以及在何时运行，也可以指定开始和结束日期。
每月的第一个星期一	更新将在每月的第一个星期一运行。可以指定将在何时运行，以及开始和结束日期。
每月的最后一天	更新将在每月的最后一天运行。可以指定将在何时运行，以及开始和结束日期。
每月第 N 周的第 X 天	更新将在月中某指定周的指定一天运行。可以指定将在何时运行，以及开始和结束日期。
日历	更新将在之前所创建的日历中指定的日期运行。

- 4 完成填写计划信息后，单击“计划”。

在“用户更新”选项卡中显示计划的下一次角色更新的日期。

注意：

可以通过单击“仅更新角色”或“更新角色和别名”部分的“取消计划的更新”取消计划的下一次更新。

9.6.5 使用 PeopleSoft 安全桥

通过 BI 平台的安全桥功能，用户可以向 BI 平台导入 PeopleSoft EPM 安全设置。

安全桥在两种模式下工作：

- 配置模式

在配置模式中，安全桥提供了可让用户创建响应文件的接口。此响应文件的作用是在执行模式中控制安全桥的行为。

- 执行模式

根据响应文件中定义的参数，安全桥将 PeopleSoft EPM 中的维表的安全设置导入到 BI 平台中的 Universe。

9.6.5.1 导入安全设置

要导入安全设置，必须执行以下任务，以便：

- 定义安全桥将托管的对象。
- 创建响应文件。
- 运行安全桥应用程序。

有关在导入设置后管理安全性的信息，请参阅第 318 页上的 [“管理安全设置”](#)。

9.6.5.1.1 定义托管的对象

在运行安全桥之前，确定此应用程序托管的对象很重要。安全桥管理一个或多个 PeopleSoft 角色、一个 BI 平台组以及一个或多个 Universe。

- 托管的 PeopleSoft 角色

这些是 PeopleSoft 系统中的角色。这些角色的成员通过 PeopleSoft EPM 处理 PeopleSoft 数据。必须选择包含特定成员（要为这些成员提供/更新对 BI 平台中托管的 Universe 的访问权限）的角色。

为这些角色的成员定义的访问权限基于其在 PeopleSoft EPM 中的权限；安全桥会将这些安全设置导入到 BI 平台中。

- 托管的 BI 平台组

运行安全桥时，该程序会在 BI 平台中为托管的 PeopleSoft 角色的每个成员都创建一个用户。

在其中创建用户的组为托管的 BI 平台组。此组的成员是一些用户，这些用户对托管的 Universe 的访问权限由安全桥维护。由于用户是在一个组中创建的，因此只需将某些用户从托管的 BI 平台组中删除就可以将安全桥配置为不更新这些用户的安全设置。

在运行安全桥之前，必须选择 BI 平台中的一个组，作为创建用户的位置。如果指定的组不存在，则安全桥将在 BI 平台中创建该组。

- 托管的 Universe

托管的 Universe 是安全桥将 PeopleSoft EPM 中的安全设置导入到其中的那些 Universe。必须从 BI 平台系统内存储的 Universe 中选择将由安全桥托管的那些 Universe。如果托管的 PeopleSoft 角色的成员也是托管的 BI 平台组的成员，则这些成员无法通过不能从 PeopleSoft EPM 访问的那些 Universe 访问任何数据。

9.6.5.1.2 创建响应文件

- 1 转到在安装安全桥的过程中指定的文件夹，然后运行 `crpsepmsecuritybridge.bat`（在 Windows 中）或 `crpsepmsecuritybridge.sh`（在 Unix 中）文件。

注意：

在 Windows 中，此位置默认为 `C:\Program Files\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\epm`。

“PeopleSoft EPM 的安全桥”对话框将会出现。

- 2 选择“新建”以创建响应文件，或选择“打开”，然后单击“浏览”以指定要修改的响应文件。选择要用于文件的语言。
- 3 单击“下一步”。
- 4 提供“PeopleSoft EPM SDK”和“BI 平台 SDK”的位置。

注意：

- PeopleSoft EPM SDK 通常位于 PeopleSoft 服务器上的 `<PS_HOME>/class/com.people soft.epm.pf.jar`。
- BI 平台 SDK 通常位于 `C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib` 中。

- 5 单击“下一步”。

对话框提示输入 PeopleSoft 数据库的连接和驱动程序信息。

- 6 从“数据库”列表中选择适当的数据库类型，然后为以下字段提供信息：

字段	说明
数据库	PeopleSoft 数据库的名称。
主机	作为数据库主机的服务器的名称。
端口号	用于访问服务器的端口号。
类位置	数据库驱动程序的类文件的位置。
用户名	用户名。
密码	密码。

- 7 单击“下一步”。

对话框将显示安全桥在运行时使用的所有类的列表。如有必要，可以在列表中添加或删除类。

8. 单击“下一步”。

该对话框向用户提示 BI 平台的连接信息。

9. 为以下字段提供适当的信息：

字段	说明
服务器	中央管理服务器（CMS）所在服务器的名称。
用户名	用户名。
密码	密码。
身份验证	身份验证类型。

10. 单击“下一步”。

11. 选择一个 BI 平台组，然后单击“下一步”。

注意：

- 安全桥将在此字段中指定的组中为托管的 PeopleSoft 角色的成员创建用户。
- 如果指定一个不存在的组，则安全桥将创建此组。

对话框显示 PeopleSoft 系统中的角色的列表。

12. 为希望管理其安全桥的角色选择“已导入”选项，然后单击“下一步”。

注意：

安全桥会在托管的 BI 平台组（在前一步中指定）中为所选角色的每个成员都创建一个用户。

对话框会显示 BI 平台中的 Universe 列表。

13. 选择希望安全桥向其导入安全设置的 Universe，然后单击“下一步”。

14. 为安全桥日志文件指定文件名和保存位置。可以使用此日志文件来确定安全桥是否成功从 PeopleSoft EPM 中导入安全设置。

15. 单击“下一步”。

对话框显示安全桥将在执行模式中使用的响应文件的预览。

16. 单击“保存”，然后选择响应文件的保存位置。

17. 单击“下一步”。

此时已成功为安全桥创建了响应文件。

18. 单击“退出”。

注意：

响应文件是一个也可以手动创建和/或修改的 Java 属性文件。有关更多信息，请参阅“PeopleSoft 响应文件”一节。

9.6.5.2 应用安全设置

要应用安全设置，请运行 `crpsepmsecuritybridge.bat` 批处理文件（在 Windows 上）或 `crpsempsecuritybridge.sh` 文件（在 Unix 上），并将创建的响应文件用作参数。例如，在 Windows 上键入 `crpsepmsecuritybridge.bat myresponsefile.properties` 或在 Unix 上键入 `crpsempsecuritybridge.sh myresponsefile.properties`。

安全桥应用程序将运行。它在 BI 平台中为在响应文件中指定的 PeopleSoft 角色的成员创建用户，并将安全设置从 PeopleSoft EPM 导入到适当的 Universe 中。

9.6.5.2.1 进行映射应考虑的事项

在执行模式中，安全桥会在 BI 平台中为托管的 PeopleSoft 角色的每个成员都创建一个用户。

所创建的用户只具有 Enterprise 身份验证别名，而且 BI 平台会向其分配随机密码。因此，在管理员手动重新分配新密码，或通过 PeopleSoft 安全插件将角色映射到 BI 平台以允许用户使用其 PeopleSoft 凭据进行登录之前，用户无法登录到 BI 平台。

9.6.5.3 管理安全设置

可以通过修改安全桥托管的对象来管理所应用的安全设置。

9.6.5.3.1 托管的用户

安全桥根据以下条件管理用户：

- 用户是否为托管的 PeopleSoft 角色的成员。
- 用户是否为托管的 BI 平台组的成员。

如果要允许某个用户通过 BI 平台中的 Universe 访问 PeopleSoft 数据，请确保该用户同时是托管的 PeopleSoft 角色的成员和托管的 BI 平台组的成员。

- 如果托管的 PeopleSoft 角色的成员在 BI 平台中没有帐户，则安全桥会创建帐户并向其分配随机密码。管理员必须决定是手动重新分配新的密码，还是通过 PeopleSoft 安全插件将角色映射到 BI 平台以允许用户登录到 BI 平台。
- 如果托管的 PeopleSoft 角色的成员也属于托管的 BI 平台组的成员，则安全桥会更新应用于用户的安全设置，以使用户能够通过托管的 Universe 访问适当的数据。

如果托管的 PeopleSoft 角色的成员已经在 BI 平台中拥有帐户，但该成员不是托管的 BI 平台组的成员，则安全桥不会更新应用于该用户的安全设置。通常，这种情况只会在管理员从托管的 BI 平台组中手动删除由安全桥创建的用户帐户时发生。

注意：

这是一种有效的安全管理方法：通过从托管的 BI 平台组中删除用户，可以将这些用户的安全设置配置为不同于其在 PeopleSoft 中的安全设置。

反之，如果托管的 BI 平台组的成员不是托管的 PeopleSoft 角色的成员，则安全桥不会向其提供对托管的 Universe 的访问权限。通常，这种情况只会在 PeopleSoft 管理员从托管的 PeopleSoft 角色中删除之前由安全桥映射到 BI 平台的用户时发生。

注意：

这是另一种安全管理方法：通过从托管的 PeopleSoft 角色中删除用户，可以确保用户无法访问 PeopleSoft 中的数据。

9.6.5.3.2 托管的 Universe

安全桥通过限制集管理 Universe（限制集限制了托管的用户可以通过托管的 Universe 访问的数据）。

限制集是限制的分组（例如，对查询控制、SQL 生成等的限制）。安全桥应用/更新托管的 Universe 的行访问和对象访问限制：

- 它将行访问限制应用于在 PeopleSoft EPM 中定义的维表。这些限制特定于用户，并可配置为以下其中一个设置：

- 用户具有所有数据的访问权。
- 用户没有所有数据的访问权。
- 用户具有数据访问权，具体取决于他们在 PeopleSoft 中的行级权限（可通过在 PeopleSoft EPM 中定义的安全联接表（SJT）看到这些权限）。
- 它根据度量对象访问的字段向度量对象应用对象访问限制。

如果度量对象访问在 PeopleSoft 中定义为指标（Metric）的字段，则视用户是否能访问 PeopleSoft 中被引用的指标（Metric）而定，将允许/不允许对度量对象进行访问。如果某用户无法访问任何指标（Metric），则将拒绝该用户对度量对象进行访问。如果某用户可以访问所有指标（Metric），则允许该用户对度量对象进行访问。

作为管理员，也可以通过限制安全桥托管的 Universe 的数量，限制用户可通过 PeopleSoft 系统访问的数据。

9.6.5.4 PeopleSoft 响应文件

BI 平台的安全桥功能根据在响应文件中指定的设置工作。

通常，通过在配置模式中使用由安全桥提供的接口来生成响应文件。但是，由于此文件是 Java 属性文件，因此，也可以手动创建或修改它。

本附录提供相关信息，说明在选择了手动生成响应文件后需包含在此文件中的参数。

注意：

创建此文件时，必须遵守 Java 属性文件的换码要求（例如，“:”被换码为“\:”）。

9.6.5.4.1 响应文件参数

下表说明了包含在响应文件中的参数：

参数	说明
classpath	<p>用于加载必需的 .jar 文件的类路径。Windows 和 Unix 上的多个类路径均必须以 “;” 分隔。</p> <p>所需的类路径针对的是 com.peoplesoft.epm.pf.jar 和 JDBC 驱动程序 .jar 文件。</p>
db.driver.name	用于连接到 PeopleSoft 数据库的 JDBC 驱动器名称（例如 com.microsoft.jdbc.sqlserver.SQLServerDriver）。
db.connect.str	用于连接到 PeopleSoft 数据库的 JDBC 连接字符串（例如 jdbc:microsoft:sqlserver://vanrdpsft01:1433;DatabaseName=PRDM0）
db.user.name	用于登录到 PeopleSoft 数据库的用户名。
db.password	用于登录到 PeopleSoft 数据库的密码。
db.password.encrypted	此参数的值确定了是否加密响应文件中的密码参数。此值可设置为 True 或 False。（如果未指定值，则值默认为 False。）
enterprise.cms.name	Universe 所在的 CMS。
enterprise.user.name	用于登录到 CMS 的用户名。
enterprise.password	用于登录到 CMS 的密码。
enterprise.password.encrypted	此参数的值确定了是否加密响应文件中的密码参数。此值可设置为 True 或 False。（如果未指定值，则值默认为 False。）
enterprise.authMethod	用于登录到 CMS 的身份验证方法。
enterprise.role	托管的 BI 平台组。有关更多信息，请参阅第 315 页上的 “定义托管的对象” 。

参数	说明
enterprise.license	从 PeopleSoft 导入用户时控制许可类型。 “0”表示设置为命名用户许可，“1”表示设置为并发用户许可。
peoplesoft.role.n	<p>托管的 PeopleSoft 角色的列表。有关更多信息，请参阅第 315 页上的“定义托管的对象”。</p> <p>n 是一个整数，而且每个条目均拥有一个带有 peoplesoft.role 前缀的属性。</p> <p>注意： n 从 1 开始。</p> <p>如果 n 为 1，而且它是响应文件中唯一带有 peoplesoft.role 前缀的属性，则可以使用 “*” 来表示所有可用的 PeopleSoft 角色。</p>
mapped.universe.n	<p>希望安全桥更新的 Universe 的列表。有关更多信息，请参阅第 315 页上的“定义托管的对象”。</p> <p>n 是一个整数，而且每个条目均拥有一个带有 mapped.universe 前缀的属性。</p> <p>注意： n 从 1 开始。</p> <p>如果 n 为 1，而且它是响应文件中唯一带有 mapped.universe 前缀的属性，则可以使用 “*” 来表示所有可用的 Universe。</p>
log4j.appender.file.File	由安全桥写入的日志文件。

参数	说明
log4j.*	<p>为使 log4j 正常工作而需要的默认 log4j 属性:</p> <pre>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 [%-5s] %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 [%-5s] %c{1} - %m%n</pre>
peoplesoft classpath	<p>PeopleSoft EPM API .jar 文件的类路径。 此参数是可选的。</p>
enterprise.classpath	<p>BI 平台 SDK .jar 文件的类路径 此参数是可选的。</p>

参数	说明
db.driver.type	<p>PeopleSoft 数据库类型。此参数可以具有以下其中一个值：</p> <p>Microsoft SQL Server 2000</p> <p>Oracle Database 10.1</p> <p>DB2 UDB 8.2 Fixpack 7</p> <p>Custom</p> <p>“Custom” 可用于指定不同于已指出的类型或版本的数据库。</p> <p>此参数是可选的。</p>
sql.db.class.location sql.db.host sql.db.port sql.db.database	<p>SQL Server JDB 驱动程序 .jar 文件的位置、SQL Server 主机、SQL Server 端口和 SQL Server 数据库名称。</p> <p>只有在 db.driver.type 为 Microsoft SQL Server 2000 时才能使用这些参数。</p> <p>这些参数是可选的。</p>
oracle.db.class.location oracle.db.host oracle.db.port oracle.db.sid	<p>Oracle JDBC 驱动程序 .jar 文件的位置、Oracle 数据库主机、Oracle 数据库端口和 Oracle 数据库 SID。</p> <p>只有在 db.driver.type 为 Oracle Database 10.1 时才能使用这些参数。</p> <p>这些参数是可选的。</p>
db2.db.class.location db2.db.host db2.db.port db2.db.sid	<p>DB2 JDBC 驱动程序 .jar 文件的位置、DB2 数据库主机、DB2 数据库端口和 DB2 数据库 SID。</p> <p>只有在 db.driver.type 为 DB2 UDB 8.2 Fixpack 7 时才能使用这些参数。</p> <p>这些参数是可选的。</p>

参数	说明
<code>custom.db.class.location</code> <code>custom.db.drivertype</code> <code>custom.db.connectStr</code>	自定义的 JDBC 驱动程序的位置、名称和连接字符串。 只有在 <code>db.driver.type</code> 为 “Custom” 时才能使用这些参数。 这些参数是可选的。

9.7 JD Edwards 身份验证

9.7.1 概述

若要将 JD Edwards 数据用于 BI 平台，则必须为系统提供有关 JD Edwards 部署的信息。BI 平台可使用此信息来验证用户身份，以便用户能够使用其 JD Edwards EnterpriseOne 凭据登录到 BI 平台。

9.7.2 启用 JD Edwards EnterpriseOne 身份验证

若要允许 BI 平台使用 JD Edwards EnterpriseOne 信息，该平台需要有关如何进行身份验证以登录到 JD Edwards EnterpriseOne 系统的信息。

9.7.2.1 在 BI 平台中启用 JD Edwards 身份验证

- 1 以管理员身份登录到中央管理控制台。
- 2 从“管理”区域中，单击“身份验证”。
- 3 双击“JD Edwards EnterpriseOne”。
- 将显示“JD Edwards EnterpriseOne” 页面。
- 4 在“选项”选项卡中，选择“启用 JD Edwards EnterpriseOne 身份验证”复选框。
- 5 根据 BI 平台部署，在“新建别名”、“更新选项”和“新用户选项”下进行相应更改。单击“更新”以保存更改，然后进入“系统”选项卡。
- 6 单击“服务器”选项卡。
- 7 将 jdeutil.jar、kernel.jar 和 log4j.jar 从 JD Edwards 安装复制到以下位置（在 Windows 上）：<安装目录>\SAP BusinessObjects Enterprise XI 4.0\java\lib\jdedwards\default\jdedwards\ 和 <安装目录>\Tomcat\lib\。
- 8 重新启动 Tomcat 和服务器智能代理。
- 9 在“JD Edwards EnterpriseOne 系统用户”区域中，键入数据库用户名和密码，以便 BI 平台使用它们登录到 JD Edwards EnterpriseOne 数据库。
10. 在“JD Edwards EnterpriseOne 域”区域中，输入用于连接到 JD Edwards EnterpriseOne 环境的名称、主机和端口，输入环境的名称并单击“添加”。
11. 单击“更新”以保存更改。

9.7.3 将 JD Edwards EnterpriseOne 角色映射到 BI 平台

BI 平台会自动为映射的每个 JD Edwards EnterpriseOne 角色创建一个组。另外，系统还会创建别名以表示所映射的 JD Edwards EnterpriseOne 角色的成员。

可以为创建的每个别名创建一个用户帐户。

但是，如果运行多个系统，且用户在多个系统中具有帐户，则在 BI 平台中创建帐户之前，可以为每个用户分配一个同名的别名。

这样可以减少为 BI 平台中的相同用户创建的帐户数量。

例如，如果运行 JD Edwards EnterpriseOne 测试环境和生产环境，并且有 30 个用户具有两个系统的访问权限，则仅为这些用户创建 30 个帐户。如果选择不为每个用户分配同名的别名，则会为 BI 平台中的这 30 个用户创建 60 个帐户。

但是，如果运行多个系统，且用户名相同，则必须为创建的每个别名创建一个新的成员帐户。

例如，如果使用 Russell Aquino（用户名为“raqino”）的用户帐户运行测试环境，且使用 Raoul Aquino（用户名为“raqino”）的用户帐户运行生产环境，则需要为每个用户的别名创建单独的帐户。否则，这两个用户将添加到相同的 BI 平台帐户，并且他们无法使用各自的 JD Edwards EnterpriseOne 凭据登录到 BI 平台。

9.7.3.1 映射 JD Edwards EnterpriseOne 角色

- 1 以管理员身份登录到中央管理控制台。
- 2 从“管理”区域中，单击“身份验证”。
- 3 双击“JD Edwards EnterpriseOne”。
- 4 在“新别名选项”区域中，选择以下其中一个选项：

- 将每个添加的别名分配给具有相同名称的帐户

如果运行多个 JD Edwards EnterpriseOne Enterprise 系统，并且有些用户在多个系统中拥有帐户（对于不同的系统，不会有两个用户具有相同的用户名），请选择此选项。

- 为每个添加的别名创建一个新帐户

如果只运行一个 JD Edwards EnterpriseOne，大部分用户只在一个系统中拥有帐户，或者两个或多个系统中的不同用户的用户名相同，请选择此选项。

- 5 在“更新选项”区域中，选择以下其中一个选项：

- 将添加新的别名并创建新用户

选择此选项可以为映射到 BI 平台的每个用户创建一个新别名。系统将为没有 BI 平台帐户的用户，或者为所有用户（如果选择了“为每个添加的别名创建一个新帐户”选项）添加新帐户。

- 不会添加新的别名，并且不会创建新用户

如果想要映射的角色包含许多用户，但只有其中部分用户将使用 BI 平台，请选择此选项。系统不会自动为用户创建别名和帐户。而只会在用户第一次登录到 BI 平台时为用户创建别名（如有必要，也会创建帐户）。这是默认选项。

- 6 可以在“新用户选项”区域中指定如何创建新用户。

选择以下选项之一：

- 将新用户创建为命名用户。

将新用户帐户配置为使用命名用户许可。命名用户许可与特定用户关联，并允许用户基于他们的用户名和密码访问系统。这样，不管连接了多少其他用户，命名用户都能够访问系统。必须为使用此选项创建的每个用户帐户提供一个命名用户许可。

- 将新用户创建为并发用户。

新用户帐户被配置为使用并发用户许可。并发许可指定可同时连接到 BI 平台的用户数。这种类型的许可模式非常灵活，因为少量的并发许可就可以支持大量用户。例如，根据用户访问 BI 平台的频率和时长，一份 100 个用户的并发许可可能支持 250、500 或 700 个用户。

所选角色现在作为组显示在 BI 平台中。

- 7 单击“角色”选项卡。
- 8 在“域列表”下，选择包含要映射的角色的 JD Edwards 服务器。
- 9 在“可用角色”下，选择要映射到 BI 平台的角色，然后单击“<”。
- 10 单击“更新”。
角色将映射到 BI 平台。

9.7.3.2 重新映射注意事项

如果将用户添加到已映射到 BI 平台的角色，则需要重新映射该角色，以将用户添加到 BI 平台中。重新映射角色时，用于将用户映射成命名用户或并发用户的选项只影响已添加到角色中的新用户。

例如，首先选择“将新用户创建为命名用户”选项并将某个角色映射到 BI 平台。然后，向同一角色中添加用户，选择“将新用户创建为并发用户”选项并重新映射该角色。

在此情况下，只有该角色中的新用户会作为并发用户映射到 BI 平台，已映射的用户仍然为命名用户。如果首先将用户映射为并发用户，然后更改设置以将新用户重新映射为命名用户，则会出现相同的情况。

9.7.3.3 取消映射角色

- 1 以管理员身份登录到中央管理控制台。
- 2 从“管理”区域中，单击“身份验证”。
- 3 单击 JD Edwards EnterpriseOne 的选项卡。
- 4 在“角色”区域中，选择想要删除的角色，然后单击“<”。
- 5 单击“更新”。

该角色的成员将无法再访问 BI 平台，除非他们拥有其他帐户或别名。

注意：

也可以删除个别帐户，或在将角色映射到 BI 平台之前删除角色中的用户，以禁止特定用户登录。

9.7.4 计划用户更新

为确保 ERP 系统的用户数据更改反映在 BI 平台用户数据中，可以计划进行定期用户更新。这些更新将根据在中央管理控制台（CMC）中配置的映射设置，自动同步 ERP 和 BI 平台用户。

有两个选项可用于运行和计划已导入角色的更新：

- 仅更新角色：使用此选项，将仅更新当前映射的角色之间的链接，这些角色已导入到 BI 平台中。如果希望经常运行更新，而又在意系统资源使用情况的话，可以使用此选项。如果仅更新角色，则不会创建新的用户帐户。
- 更新角色和别名：此选项不仅更新角色之间的链接，还会在 BI 平台中为添加到 ERP 系统的新用户别名创建新的用户帐户。

注意：

如果未指定在启用身份验证时自动为更新创建用户别名，则不会为新别名创建帐户。

9.7.4.1 计划用户更新

将角色映射到 BI 平台后，需要指定系统更新这些角色的方式。

- 1 单击“用户更新”选项卡。
- 2 在“仅更新角色”或“更新角色和别名”区域中单击“计划”。

提示：

如果要立即运行更新，请单击“立即更新”。

提示：

如果希望经常运行更新，而又在意系统资源的使用情况，则可以使用“仅更新角色”选项。对角色和别名都进行更新占用系统的时间会比较长。

“重复发生”对话框随即出现。

- 3 从“运行对象”列表中选择一项，并提供需要的所有计划信息。

在计划更新时，可以从下表中概述的重复发生模式中进行选择：

重复发生模式	说明
每小时	更新将每小时运行一次。可以指定将在何时开始，以及开始和结束日期。
每天	更新将每天或每隔指定天数运行一次。可以指定对象将在何时运行，以及开始和结束日期。
每周	更新将每周运行一次。它可以一周运行一次或多次。可以指定对象运行的具体日期和时间，以及开始和结束日期。
每月	更新将每月或每隔几个月运行一次。可以指定更新将在何时运行，以及开始和结束日期。
每月的第 N 天	更新将在每月的特定一天运行。可以指定将在月中的哪一天以及在何时运行，也可以指定开始和结束日期。
每月的第一个星期一	更新将在每月的第一个星期一运行。可以指定将在何时运行，以及开始和结束日期。
每月的最后一天	更新将在每月的最后一天运行。可以指定将在何时运行，以及开始和结束日期。
每月第 N 周的第 X 天	更新将在月中某指定周的指定一天运行。可以指定将在何时运行，以及开始和结束日期。
日历	更新将在之前所创建的日历中指定的日期运行。

- 4 完成填写计划信息后，单击“计划”。

在“用户更新”选项卡中显示计划的下一次角色更新的日期。

注意：

可以通过单击“仅更新角色”或“更新角色和别名”部分的“取消计划的更新”取消计划的下一次更新。

9.8 Siebel 身份验证

9.8.1 启用 Siebel 身份验证

要允许 BI 平台 使用 Siebel 信息，它需要有关如何进行身份验证以登录 Siebel 系统的信息。

9.8.1.1 在 BI 平台中启用 Siebel 身份验证

- 1 以管理员身份登录到中央管理控制台。
- 2 从“管理”区域中，单击“身份验证”。
- 3 双击“Siebel”。
- 将出现“Siebel”页面。它包含四个选项卡：“选项”、“系统”、“职责”和“用户更新”。
- 4 在“选项”选项卡中，选中“启用 Siebel 身份验证”复选框。
- 5 根据 BI 平台部署，在“新建别名”、“更新选项”和“新用户选项”下进行相应更改。单击“更新”以保存更改，然后进入“系统”选项卡。
- 6 单击“域”选项卡。
- 7 在“域名”字段中，输入希望连接的 Siebel 系统的域名。
- 8 在“连接”下输入该域的连接字符串。
- 9 在“用户名”区域中，键入数据库用户名和密码，以便 BI 平台使用它们登录到 Siebel 数据库。
- 10 在“密码”区域中，输入所选用户的密码。
- 11 单击“添加”以将系统信息添加到“当前域”列表中。
- 12 单击“更新”以保存更改。

9.8.2 将角色映射到 BI 平台

BI 平台会自动为映射的每个 Siebel 角色创建一个组。此外，该程序还会创建别名来表示所映射的 Siebel 角色的成员。

可以为创建的每个别名创建一个用户帐户。

但是，如果运行多个系统，且用户在多个系统中具有帐户，则在 BI 平台中创建帐户之前，可以为每个用户分配一个同名的别名。

这样可以减少为程序中的相同用户创建的帐户数量。

例如，如果运行 Siebel eBusiness 测试环境和生产环境，并且有 30 个用户具有两个系统的访问权限，则仅为这些用户创建 30 个帐户。如果选择不为每个用户分配同名的别名，则会为 BI 平台中的这 30 个用户创建 60 个帐户。

但是，如果运行多个系统，且用户名相同，则必须为创建的每个别名创建一个新的成员帐户。

例如，如果使用 Russell Aquino（用户名为“raqino”）的用户帐户运行测试环境，且使用 Raoul Aquino（用户名为“raqino”）的用户帐户运行生产环境，则需要为每个用户的别名创建单独的帐户。否则，这两个用户将添加到相同的帐户中，并且无法使用各自的 Siebel eBusiness 凭据登录到 BI 平台。

9.8.2.1 将 Siebel eBusiness 角色映射到 BI 平台

- 1 以管理员身份登录到中央管理控制台。
- 2 单击“身份验证”。
- 3 双击“Siebel”。
- 4 选择复选框“启用 Siebel 身份验证”。
- 5 在“新别名选项”区域中，选择以下其中一个选项：

- 将每个添加的别名分配给具有相同名称的帐户

如果运行多个 Siebel eBusiness 系统，这些系统中有些用户在多个系统中拥有帐户（且对于不同的系统，不会有用户具有相同的用户名），请选择此选项。

- 为每个添加的别名创建一个新帐户

如果只运行一个 Siebel eBusiness 系统，且大部分用户只在一个系统中拥有帐户，或者两个或多个系统中的不同用户的用户名相同，请选择此选项。

- 6 在“别名更新选项”区域中，选择以下其中一个选项：

- 在发生别名更新时创建新的别名

选择此选项可以为映射到 BI 平台的每个用户创建一个新别名。系统将为没有 BI 平台帐户的用户，或者为所有用户（如果选择了“为每个添加的别名创建一个新帐户”选项）添加新帐户。

- 仅当用户登录时才创建新的别名

如果想要映射的角色包含许多用户，但只有其中部分用户将使用 BI 平台，请选择此选项。该程序不会自动为用户创建别名和帐户。而只会在用户第一次登录到 BI 平台时为用户创建别名（如有必要，也会创建帐户）。这是默认选项。

- 7 可以在“新用户选项”区域中指定如何创建新用户。

如果 BI 平台许可是基于用户角色的，请选择以下选项之一：

选择以下选项之一：

- 将新用户创建为命名用户

新用户帐户被配置为使用命名用户许可。命名用户许可与特定用户关联，并允许用户基于他们的用户名和密码访问系统。这样，不管连接了多少其他用户，命名用户都能够访问系统。必须为使用此选项创建的每个用户帐户提供一个命名用户许可。

- 将新用户创建为并发用户
新用户帐户被配置为使用并发用户许可。并发许可指定可同时连接到 BI 平台的用户数。这种类型的许可模式非常灵活，因为少量的并发许可就可以支持大量用户。例如，根据用户访问 BI 平台的频率和时长，一份 100 个用户的并发许可可能支持 250、500 或 700 个用户。
- 8 单击“角色”选项卡。
 - 9 选择与要映射角色的 Siebel 服务器相对应的域。
 - 10 在“可用角色”下，选择要映射的角色并单击 >。
注意：
 - 如果有大量角色，可以使用“搜索角色始于：”字段来缩小搜索范围。输入角色的起始字符后跟通配符（%）字符，然后单击“搜索”。
 - 为使搜索功能生效，需要将一个 Siebel 插件 jar 文件部署到 Tomcat lib 目录：安装目录 \tomcat\webapps\BOE\WEB-INF\lib 和 安装目录\SAP BusinessObjects Enterprise XI 4.0\java\lib\siebel\default\siebel。然后，重新启动 Tomcat 服务器和服务器智能代理。
 - 11 单击“更新”。
角色将映射到 BI 平台。

9.8.2.2 重新映射注意事项

要强制组和用户在 BI 平台与 Siebel 之间保持同步，请设置“强制用户同步”。

注意：

要选择“强制用户同步”，首先必须选择“将添加新的别名并创建新用户”。

重新映射角色时，用于将用户映射成命名用户或并发用户的选项只影响已添加到角色中的新用户。

例如，首先选择“将新用户创建为命名用户”选项并将某个角色映射到 BI 平台。然后，向同一角色中添加用户，选择“将新用户创建为并发用户”选项并重新映射该角色。

在此情况下，只有该角色中的新用户会作为并发用户映射到 BI 平台，已映射的用户仍然为命名用户。如果首先将用户映射为并发用户，然后更改设置以将新用户重新映射为命名用户，则会出现相同的情况。

9.8.2.3 取消映射角色

- 1 以管理员身份登录到中央管理控制台。
- 2 从“管理”区域中，单击“身份验证”。
- 3 双击“Siebel”。
- 4 在“域”选项卡中，选择与要取消映射的角色相对应的 Siebel 域。
- 5 在“角色”选项卡中，选择想要删除的角色，然后单击“<”。
- 6 单击“更新”。

该角色的成员将无法再访问 BI 平台，除非他们拥有其他帐户或别名。

注意：

也可以删除个别帐户，或在将角色映射到 BI 平台之前删除角色中的用户，以禁止特定用户登录。

9.8.3 计划用户更新

为确保 ERP 系统的用户数据更改反映在 BI 平台用户数据中，可以计划进行定期用户更新。这些更新将根据在中央管理控制台（CMC）中配置的映射设置，自动同步 ERP 和 BI 平台用户。

有两个选项可用于运行和计划已导入角色的更新：

- 仅更新角色：使用此选项，将仅更新当前映射的角色之间的链接，这些角色已导入到 BI 平台中。如果希望经常运行更新，而又在意系统资源使用情况的话，可以使用此选项。如果仅更新角色，则不会创建新的用户帐户。
- 更新角色和别名：此选项不仅更新角色之间的链接，还会在 BI 平台中为添加到 ERP 系统的新用户别名创建新的用户帐户。

注意：

如果未指定在启用身份验证时自动为更新创建用户别名，则不会为新别名创建帐户。

9.8.3.1 计划用户更新

将角色映射到 BI 平台后，需要指定系统更新这些角色的方式。

- 1 单击“用户更新”选项卡。
- 2 在“仅更新角色”或“更新角色和别名”区域中单击“计划”。

提示：

如果要立即运行更新，请单击“立即更新”。

提示：

如果希望经常运行更新，而又在意系统资源的使用情况，则可以使用“仅更新角色”选项。对角色和别名都进行更新占用系统的时间会比较长。

“重复发生”对话框随即出现。

- 3 从“运行对象”列表选择一个选项，并提供需要的所有计划信息。

在计划更新时，可以从下表中概述的重复发生模式中进行选择：

重复发生模式	说明
每小时	更新将每小时运行一次。可以指定将在何时开始，以及开始和结束日期。
每天	更新将每天或每隔指定天数运行一次。可以指定对象将在何时运行，以及开始和结束日期。
每周	更新将每周运行一次。它可以一周运行一次或多次。可以指定对象运行的具体日期和时间，以及开始和结束日期。
每月	更新将每月或每隔几个月运行一次。可以指定更新将在何时运行，以及开始和结束日期。
每月的第 N 天	更新将在每月的特定一天运行。可以指定将在月中的哪一天以及在何时运行，也可以指定开始和结束日期。
每月的第一个星期一	更新将在每月的第一个星期一运行。可以指定将在何时运行，以及开始和结束日期。
每月的最后一天	更新将在每月的最后一天运行。可以指定将在何时运行，以及开始和结束日期。
每月第 N 周的第 X 天	更新将在月中某指定周的指定一天运行。可以指定将在何时运行，以及开始和结束日期。
日历	更新将在之前所创建的日历中指定的日期运行。

- 4 完成填写计划信息后，单击“计划”。

在“用户更新”选项卡中显示计划的下一次角色更新的日期。

注意：

可以通过单击“仅更新角色”或“更新角色和别名”部分的“取消计划的更新”取消计划的下一次更新。

9.9 Oracle EBS 身份验证

9.9.1 启用 Oracle EBS 身份验证

若要允许 BI 平台使用 Oracle EBS 信息，系统需要有关如何进行身份验证以登录到 Oracle EBS 系统的信息。

9.9.1.1 启用 Oracle 电子商务套件身份验证

在执行该过程之前，需要将 Oracle DLL 和 JAR 文件部署在 BI 平台上：

- 1 从 Oracle 数据库客户端应用程序中下载 ojdbc11.dll。
 - 2 将文件复制此位置：
 - 在 Windows 上，为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\win64_x64
 - 在 Unix 上，为 <安装目录>/sap_bobj/enterprise_xi40/platform
 - 3 从 Oracle 数据库客户端应用程序中下载 ojdbc5.jar。
 - 4 将文件复制此位置：
 - 在 Windows 上，为 <安装目录>\Tomcat\lib
 - 在 Unix 上，为 <安装目录>/sap_bobj/tomcat/lib
 - 1 以管理员身份登录到中央管理控制台。
 - 2 从“管理”区域中，单击“身份验证”。
 - 3 单击“Oracle EBS”。
- 将显示“Oracle EBS”页。它包含四个选项卡：“选项”、“系统”、“职责”和“用户更新”。
- 4 在“选项”选项卡中，选中“Oracle EBS 身份验证已启用”复选框。
 - 5 根据 BI 平台部署，在“新建别名”、“更新选项”和“新用户选项”下进行相应更改。单击“更新”以保存更改，然后进入“系统”选项卡。
 - 6 单击“系统”选项卡。
 - 7 在“Oracle EBS 系统用户”区域中，键入 BI 平台要用于登录到 Oracle 电子商务套件数据库的数据库用户名和密码。
 - 8 在“Oracle EBS 服务”区域中，输入 Oracle EBS 环境使用的服务名称，然后单击“添加”。
 - 9 单击“更新”以保存更改。

现在需要将 Oracle EBS 角色映射到系统。

相关主题

- 第 337 页上的[“映射 Oracle 电子商务套件角色”](#)

9.9.2 将 Oracle 电子商务套件角色映射到 BI 平台

BI 平台会自动为映射的每个 Oracle 电子商务套件 (EBS) 角色创建一个组。系统还会创建别名，以表示所映射 Oracle 电子商务套件角色的成员。

可以为创建的每个别名创建一个用户帐户。但是，如果运行多个系统，且用户在多个系统中具有帐户，则在 BI 平台中创建帐户之前，可以为每个用户分配一个同名的别名。

这样可以减少为系统中的相同用户创建的帐户数量。

例如，如果运行 EBS 测试环境和生产环境，并且有 30 个用户具有两个系统的访问权限，则仅为这些用户创建 30 个帐户。如果选择不为每个用户分配同名的别名，则会为 BI 平台中的这 30 个用户创建 60 个帐户。

但是，如果运行多个系统，且用户名相同，则必须为创建的每个别名创建一个新的成员帐户。

例如，如果使用 Russell Aquino（用户名为“raquno”）的用户帐户运行测试环境，且使用 Raoul Aquino（用户名为“raquno”）的用户帐户运行生产环境，则需要为每个用户的别名创建单独的帐户。否则，这两个用户将添加到相同的 BI 平台帐户，他们将能够使用各自的 Oracle EBS 凭据登录到系统，并且可以访问这两个 EBS 环境中的数据。

9.9.2.1 映射 Oracle 电子商务套件角色

- 1 以管理员身份登录到中央管理控制台。
- 2 从“管理”区域中，单击“身份验证”。
- 3 单击“Oracle EBS”。
- “Oracle EBS”页显示有“选项”选项卡。
- 4 在“新别名选项”区域中，选择以下其中一个选项：
 - 将每个添加的 Oracle EBS 别名分配给具有相同名称的帐户

如果运行多个 Oracle 电子商务套件系统，这些系统中有些用户在多个系统中拥有帐户（且对于不同的系统，不会有两个用户具有相同的用户名），请选择此选项。

- 为每个添加的 Oracle EBS 别名创建一个新帐户

如果只运行一个 Oracle 电子商务套件，且大部分用户只在一个系统中拥有帐户，或者两个或更多系统中的不同用户的用户名相同，请选择此选项。

5 在“更新选项”区域中，选择以下其中一个选项：

- 在发生别名更新时创建新的别名

选择此选项可以为映射到 BI 平台的每个用户创建一个新别名。系统将为没有 BI 平台帐户的用户，或者为所有用户（如果选择了“为每个添加的 Oracle EBS 别名创建一个新帐户”选项）添加新帐户。

- 仅当用户登录时才创建新的别名

如果想要映射的角色包含许多用户，但只有其中部分用户将使用 BI 平台，请选择此选项。平台不会自动为用户创建别名和帐户。而只会在用户第一次登录到 BI 平台时为用户创建别名（如有必要，也会创建帐户）。这是默认选项。

6 可以在“新用户选项”中指定新用户的创建方式，然后单击“更新”。

选择以下选项之一：

- 将新用户创建为命名用户。

将新用户帐户配置为使用命名用户许可。命名用户许可与特定用户关联，并允许用户基于他们的用户名和密码访问系统。这样，不管连接了多少其他用户，命名用户都能够访问系统。必须为使用此选项创建的每个用户帐户提供一个命名用户许可。

- 将新用户创建为并发用户。

新用户帐户被配置为使用并发用户许可。并发许可指定可同时连接到 BI 平台的用户数。这种类型的许可模式非常灵活，因为少量的并发许可就可以支持大量用户。例如，根据用户访问平台的频率和时长，一份 100 个用户的并发许可可能支持 250、500 或 700 个用户。

所选角色现在作为组显示在 BI 平台中。

7 单击“职责”选项卡。

8 在“当前 Oracle EBS 服务”下，选择包含要映射的角色的 Oracle EBS 服务。

9 在“映射的 Oracle EBS 角色”下，可以为 Oracle EBS 用户指定过滤器。

- a 从“应用程序”列表中，选择用户可用于新角色的应用程序。
- b 在“职责”列表中，选择用户可以运行的 Oracle 应用程序、函数、报表和并发程序。
- c 在“安全组”中，选择将新角色分配到其中的安全组。
- d 使用“当前角色”下的“添加”和“删除”按钮修改角色的安全组分配。

10. 单击“更新”。

角色将映射到 BI 平台。

将角色映射到 BI 平台后，需要指定系统更新这些角色的方式。

9.9.2.1.1 更新 Oracle EBS 角色和用户

启用 Oracle EBS 身份验证后，必须对已导入到 BI 平台中的映射角色计划和运行定期更新。这样可以确保更新的 Oracle EBS 角色信息正确反映在 BI 平台中。

有两个选项可用于运行和计划 Oracle EBS 角色更新：

- **仅更新角色：**使用此选项，将仅更新当前映射的角色之间的链接，这些角色已导入到 BI 平台中。如果希望经常运行更新，并且考虑系统资源的使用，则建议使用该选项。如果仅更新 Oracle EBS 角色，则不会创建新的用户帐户。
- **更新角色和别名：**此选项不仅更新角色之间的链接，还会在 BI 平台中为添加到 Oracle EBS 系统中的角色的用户别名创建新的用户帐户。

注意：

如果未指定在启用 Oracle EBS 身份验证时为更新自动创建用户别名，则不会为新别名创建帐户。

9.9.2.1.2 为 Oracle EBS 角色计划更新

将角色映射到 BI 平台后，需要指定系统更新这些角色的方式。

1. 单击“用户更新”选项卡。
2. 单击“仅更新角色”或“更新角色和别名”部分的“计划”。

提示：

如果希望立即运行更新，则点击“立即更新”。

提示：

如果希望经常运行更新并且考虑系统资源的使用，则使用“仅更新角色”选项。对角色和别名都进行更新占用系统的时间会比较长。

“重复发生”对话框随即出现。

3. 从“运行对象”下拉列表选择一个选项，并在所提供的字段中填写所有所需的计划信息。

在计划更新时，可以从下表中概述的重复发生模式中进行选择：

重复发生模式	说明
每小时	更新将每小时运行一次。 可以指定将在何时开始，以及开始和结束日期。
每天	更新将每天或每隔指定天数运行一次。可以指定对象将在何时运行，以及开始和结束日期。
每周	更新将每周运行一次。它可以每周运行一次，也可以一周运行多次。可以指定对象运行的具体日期和时间，以及开始和结束日期。
每月	更新将每月或每隔几个月运行一次。 可以指定更新将在何时运行，以及开始和结束日期。
每月的第 N 天	更新将在每月的特定一天运行。可以指定将在月中的哪一天以及在何时运行，也可以指定开始和结束日期。
每月的第一个星期一	更新将在每月的第一个星期一运行。可以指定将在何时运行，以及开始和结束日期。
每月的最后一天	更新将在每月的最后一天运行。可以指定将在何时运行，以及开始和结束日期。
每月第 N 周的第 X 天	更新将在月中某指定周的指定一天运行。可以指定将在何时运行，以及开始和结束日期。
日历	更新将在之前所创建的日历中指定的日期运行。

- 4 完成填写计划信息后，单击“计划”。
- 在“用户更新”选项卡中显示计划的下一次角色更新的日期。
- 注意：**
- 可以通过单击“仅更新角色”或“更新角色和别名”部分的“取消计划的更新”取消计划的下一次更新。

9.9.3 取消映射角色

若要禁止特定用户组登录到 BI 平台，可以取消映射其所属的角色。

9.9.3.1 取消映射角色

- 1 以管理员身份登录到中央管理控制台。
- 2 从“管理”区域中，单击“身份验证”。
- 3 双击要为其取消映射角色的 ERP 系统的名称。
ERP 系统页将显示“选项”选项卡。
- 4 单击“职责”选项卡。
- 5 选择“当前 Oracle EBS 服务”。
- 6 在“当前角色”下，选择一个角色并单击“删除”按钮。
- 7 单击“更新”。

该角色的成员将无法再访问 BI 平台，除非他们拥有其他帐户或别名。

注意：

也可以删除个别帐户，或在将角色映射到 BI 平台之前删除角色中的用户，以禁止特定用户登录。

9.9.4 为映射的 Oracle EBS 组和用户自定义权限

将角色映射至 BI 平台时，可以为创建的组 and 用户设置权限或授予权限。

9.9.4.1 分配管理权限

要允许用户维护 BI 平台，必须使用户成为默认管理员组的成员。此组的成员可获得该系统各个方面的完全控制权，其中包括帐户、服务器、文件夹、对象和设置等等。

- 1 以管理员身份登录到中央管理控制台。
- 2 从“组织”区域中，单击“用户和组”。

- 3 在“名称”列中，右击“管理员”并单击“将成员添加到组”。
随后将显示“可用用户或组”页面。
- 4 从“用户列表”或“组列表”区域中，选择要向其分配管理权限的映射角色。
- 5 单击“>”使角色成为管理员组的子组，然后单击“确定”。
现在角色成员在 BI 平台中拥有管理权限。

注意：

也可以在 Oracle EBS 中创建一个角色，将适当的用户添加到此角色，再将角色映射到 BI 平台，然后使映射的角色成为默认管理员组的一个子组，以向角色成员授予管理权限。

9.9.4.2 分配发布权限

如果系统中有用户被指定为组织内的内容创建者，则可以授权让他们将对象发布到 BI 平台。

- 1 以管理员身份登录到中央管理控制台。
- 2 从“组织”区域中，单击“文件夹”。
- 3 转到想要允许用户在其中添加对象的文件夹。
- 4 依次单击“管理”、“顶级安全性”和“所有文件夹”。
- 5 单击“添加主体”。

将出现“添加主体”页面。

- 6 在“可用用户或组”列表中，选择包含发布权限所要授予的成员的组。
- 7 单击“>”以使该组能够访问文件夹，然后单击“添加和指定安全性”。

将出现“指定安全性”页面。

- 8 在“可用访问级别”列表中，选择所需的访问级别并单击“>”以显式指定访问级别。
- 9 如果已选择“从父文件夹继承”和“从父组继承”选项，请取消选择这两个选项，并单击“应用”。
- 10 单击“确定”。

现在角色成员有权将对象添加到该文件夹及其所有子文件夹。要删除指定的权限，请选择一个组并单击“删除”。

9.9.5 为 SAP Crystal Reports 和 Oracle EBS 配置单一登录 (SSO)

默认情况下，BI 平台将配置为允许 SAP Crystal Reports 用户使用单一登录（SSO）访问 Oracle EBS 数据。

9.9.5.1 为 Oracle EBS 和 SAP Crystal Reports 取消激活 SSO

- 1 在中央管理控制台（CMC）中，单击“应用程序”。
- 2 双击“Crystal Reports 配置”。
- 3 单击“单一登录选项”。
- 4 选择 `crdb_oraapps`。
- 5 单击“删除”。
- 6 单击“保存并关闭”。
- 7 转到 CMC 的“服务器”页面，然后选择“Crystal Reports 服务”。
- 8 单击“重新启动服务器”按钮。

9.9.5.2 为 Oracle EBS 和 SAP Crystal Reports 重新激活 SSO

按照下面的步骤为 Oracle EBS 和 SAP Crystal Reports 重新激活 SSO。

- 1 在中央管理控制台（CMC）中，单击“应用程序”。
- 2 双击“Crystal Reports 配置”。
- 3 单击“单一登录选项”。
- 4 在“使用以下驱动程序时，使用单一登录上下文进行数据库登录”下面，键入 `crdb_oraapps`。
- 5 单击“添加”。
- 6 单击“保存并关闭”。
- 7 转到 CMC 的“服务器”页面，然后选择“Crystal Reports 服务”。
- 8 单击“重新启动服务器”按钮。

第 10 章 服务器管理

10.1 使用 CMC 中的“服务器”管理区域

CMC 的“服务器”管理区域是用于服务器管理任务的主要工具。它提供了部署中所有服务器的列表。对于大多数管理和配置任务，将需要在列表中选择服务器，并从“管理”或“操作”菜单中选择一个命令。

关于导航树

利用“服务器”管理区域左侧的导航树，可通过多种方式查看“服务器”列表。在导航树中选择项目以在“详细信息”窗格中更改显示的信息。

导航树选项	说明
服务器列表	显示部署中所有服务器的完整列表。
服务器组列表	显示“详细信息”窗格中所有可用服务器组的简单列表。如果要配置服务器组的设置或安全性，请选择此选项。
服务器组	列出服务器组和每个服务器组内的服务器。选择某个服务器组时，该组的服务器和服务器组将以分层视图形式显示在“详细信息”窗格中。
节点	显示部署中节点的列表。节点在 CCM 中配置。可以通过单击选择一个节点查看或管理该节点上的服务器。

导航树选项	说明
服务类别	<p>提供部署中可能存在的服务类型的列表。服务类别分为核心 BI 平台服务和与特定 SAP Business Objects 组件相关联的服务。服务类别包括：</p> <ul style="list-style-type: none"> • 连接服务 • 核心服务 • Crystal Reports 服务 • 数据联合服务 • 生命周期管理服务 • 分析服务 • Web Intelligence 服务 • Dashboard Design 服务 <p>在导航列表中选择一个服务类别以查看或管理该类别中的服务器。</p> <p>注意： 一个服务器可以承载属于多个服务类别的服务。因此，一个服务器可以出现在多个服务类别中。</p>
服务器状态	<p>依据服务器的当前状态显示服务器。这是一个有用的工具，用于检查以确定哪些服务器正在运行或已停止。举例来说，如果遇到系统性能低下的情况，可以使用“服务器状态”列表来快速确定是否有任何服务器处于异常状态。可能的服务器状态包括以下状态：</p> <ul style="list-style-type: none"> • 已停止 • 启动中 • 初始化中 • 运行中 • 停止中 • 已启动但出现错误 • 失败 • 等待资源（有关详细信息，请参阅 第 413 页上的 “管理 CMS 系统数据库连接”。）

关于“详细信息”窗格

视在导航树中选择的选项而定，“服务器”管理区域右侧的“详细信息”窗格将显示服务器、服务器组、状态、类别或节点的列表。下表描述了“详细信息”窗格中列出的服务器的信息。

注意：

对于节点、服务器组、类别和状态，“详细信息”窗格通常将显示名称和说明。

“详细信息”窗格的列	说明
服务器名称或名称	显示服务器的名称。
状态	<p>显示服务器的当前状态。可以使用导航树中的“服务器状态”列表按服务器状态进行排序。可能的服务器状态包括以下状态：</p> <ul style="list-style-type: none">• 已停止• 启动中• 初始化中• 运行中• 停止中• 已启动但出现错误• 失败• 等待资源
已启用	显示服务器处于已启用还是已禁用状态。
陈旧	如果服务器标记为“陈旧”，则服务器需要重新启动。例如，如果在服务器的“属性”屏幕中更改某些服务器设置，则可能需要重新启动服务器，更改才会生效。
类型	显示服务器的类型。
主机名	显示服务器的主机名。
健康	<p>表明服务器的一般健康状况。</p> <p>可能的服务器状态包括以下状态：</p> <ul style="list-style-type: none">• 绿色（正常）• 黄色（警告）• 红色（危险） <p>服务器的健康状态直接取决于服务器监测器的状态。例如：中央管理服务器的健康状态取决于 <NODENAME>.CentralManagementServer Watch 的状态。</p> <p>可在 CMC “监控” 页面上的“监测器列表”选项卡上选择监测器，并单击“编辑”访问监测器的详细信息。将会看到监测器的“警告规则”和“危险规则”，分别对应黄色和红色健康状态。</p>
进程 ID	显示服务器的唯一进程 ID 号。

“详细信息”窗格的列	说明
说明	显示服务器的说明。可以在服务器的“属性”页面中更改此说明。
修改的日期	显示上次修改服务器的日期或更改服务器状态的时间。如果要检查最近更改的服务器的状态，此列非常有用。

相关主题

- 第 362 页上的[“管理服务器组”](#)
- 第 381 页上的[“使用节点”](#)
- 第 348 页上的[“查看服务器的状态”](#)
- 第 349 页上的[“启动、停止和重新启动服务器”](#)
- 第 370 页上的[“更改服务器的属性”](#)

10.2 在 Windows 上使用脚本管理服务器

ccm.exe 可执行文件允许您通过命令行在 Windows 部署中启动、停止、重新启动、启用和禁用服务器。

相关主题

- 第 850 页上的[“ccm.exe”](#)

10.3 在 Unix 上管理服务器

ccm.sh 可执行文件允许您通过命令行在 Unix 部署中启动、停止、重新启动、启用和禁用服务器。

相关主题

- 第 843 页上的[“ccm.sh”](#)

10.4 查看和更改服务器的状态

10.4.1 查看服务器的状态

服务器的状态为其当前的运行状态：可以是运行中、启动中、停止中、停止、失败、初始化中、已启动但出现错误，或者等待资源。要响应 BI 平台请求，必须运行并启用服务器。已禁用的服务器但仍作为进程运行；但它不会接受 BI 平台其余部分的请求。已经停止的服务器不再作为进程运行。

此节显示如何使用 CMC 修改服务器的状态。

相关主题

- 第 348 页上的[“查看服务器的状态”](#)
- 第 349 页上的[“查看服务的状态”](#)
- 第 349 页上的[“启动、停止和重新启动服务器”](#)
- 第 352 页上的[“启用和禁用服务器”](#)
- 第 352 页上的[“停止中央管理服务器”](#)
- 第 351 页上的[“自动启动服务器”](#)

10.4.1.1 查看服务器的状态

1. 转到 CMC 的“服务器”管理区域。
“详细信息”窗格显示部署中的服务类别。
2. 要查看给定服务器组、节点或服务类别中的服务器列表，请在导航树中单击该服务器组、节点或类别。
“详细信息”窗格将显示部署中的服务器列表。“状态”列提供列表中每个服务器的状态。

- 3 如果要查看当前具有特定状态的所有服务器的列表，请在导航树中展开“服务器状态”选项，并选择所需的状态。

具有选定状态的服务器的列表将出现在“详细信息”窗格中。

注意：

如果需要快速查看未正常启动或意外停止的服务器的列表，这可能特别有用。

相关主题

- 第 349 页上的[“查看服务的状态”](#)

10.4.1.2 查看服务的状态

如果任何服务失败，则会将主机服务器的状态设置为“已启动但出现错误”（表示至少有一个服务已成功启动）或“失败”（表示没有服务成功启动）。可以在 CMC 和 CCM 中查看服务器状态。但是，在 CMC 中服务器的“属性”页上，还可以查看单个服务的状态。

- 1 转到 CMC 的“服务器”管理区域。

“详细信息”窗格显示部署中的服务类别。

- 2 要查看给定服务器组、节点或服务类别中的服务器列表，请在导航树中单击该服务器组、节点或类别。

“详细信息”窗格将显示部署中的服务器列表。

- 3 双击服务器以打开其“属性”页。

“属性”页显示服务器及其承载的服务的属性。对于失败的服务，还会显示错误消息。

相关主题

- 第 348 页上的[“查看服务器的状态”](#)

10.4.2 启动、停止和重新启动服务器

配置服务器或使服务器脱机时，启动、停止和重新启动服务器是经常要执行的操作。例如，如果要更改服务器的名称，则必须首先停止服务器。做出更改后，重新启动服务器以使更改生效。如果更改了服务器的配置设置，CMC 将提示是否需要重新启动服务器。

本节其余部分介绍哪些情况下特定的配置更改需要首先停止或重新启动服务器。但是，由于这些任务经常出现，因此，首先向您解释概念和不同之处，并提供常规步骤以供参考。

操作	说明
停止服务器	可能需要停止 BI 平台服务器才能修改某些属性和设置。
启动服务器	如果已停止服务器并对其进行配置，则必须先重新启动服务器，所做更改才会生效，且服务器才会恢复处理请求。
重新启动服务器	重新启动服务器是完全停止后再次启动服务器的快捷方式。如果需要在更改服务器设置后重新启动服务器，CMC 将进行提示。
自动启动服务器	可以将服务器设置为在服务器智能代理启动时自动启动。
强行终止	立即停止服务器（尽管在停止服务器时，服务器将在完成其当前处理活动后才停止）。仅当停止服务器失败并且需要立即停止服务器时，才强制终止服务器。

提示：

停止（或重新启动）服务器将终止服务器进程，从而完全停止服务器。在停止服务器之前，建议：

- 禁用服务器，以便它能够完成进行中的任何作业的处理，
- 确保队列中没有余下任何审核事件。要查看队列中余下的审核事件数，请导航到服务器的“量度”屏幕并查看“队列中的当前审核事件数”量度。

相关主题

- 第 352 页上的“[启用和禁用服务器](#)”

10.4.2.1 使用 CMC 启动、停止或重新启动服务器

1. 转到 CMC 的“服务器”管理区域。

“详细信息”窗格显示部署中的服务类别。

- 2 要查看特定服务器组、节点或服务类别中的服务器列表，请在导航窗格中选择组、节点或类别。
“详细信息”窗格将显示服务器列表。
- 3 如果要查看当前具有特定状态的所有服务器的列表，请在导航树中展开“服务器状态”选项，并选择所需的状态。

具有选定状态的服务器的列表将出现在“详细信息”窗格中。

注意：

如果需要快速查看未正常启动或意外停止的服务器的列表，这可能特别有用。

- 4 右击要更改状态的服务器，然后根据需要执行的操作，选择“启动服务器”、“重新启动服务器”、“停止服务器”或“强行终止”。

相关主题

- 第 348 页上的[“查看服务器的状态”](#)

10.4.2.2 用 CCM 启动、停止或重新启动 Windows 服务器

- 1 在 CCM 中，单击工具栏上的“管理服务器”按钮。
- 2 出现提示时，使用管理帐户登录到 CMS。
- 3 在“管理服务器”对话框中，选择要启动、停止或重新启动的服务器。
- 4 单击“启动”、“停止”、“重新启动”或“强行终止”。
- 5 单击“关闭”以返回到 CCM。

10.4.2.3 自动启动服务器

默认情况下，部署中的服务器会在服务器智能代理启动时自动启动。本任务显示在哪里设置自动启动选项。

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击要设置自动启动的服务器。
将显示“属性”屏幕。

- 3 在“公共设置”下，选中“在服务器智能代理启动时自动启动此服务器”复选框，并单击“保存”或“保存并关闭”。

注意：

如果已清除群集中每个 CMS 的“在服务器智能代理启动时自动启动此服务器”复选框，则必须使用 CCM 重新启动该系统。使用 CCM 停止 SIA 后，右击 SIA，选择“属性”。在“启动”选项卡上，单击“属性”以打开 CMS 的“服务器属性”页面。选择“自动启动”，再单击“确定”以关闭“服务器属性”页面，然后再次单击“确定”。重新启动 SIA。仅当已清除群集中每个 CMS 的“在服务器智能代理启动时自动启动此服务器”复选框时，“自动启动”选项才可用。

10.4.3 停止中央管理服务器

如果 BI 平台服务安装有多个活动的中央管理服务器（CMS），将能够在不丢失数据或影响系统功能的情况下关闭一个 CMS。节点上的另一个 CMS 将承担已停止服务器的工作负荷。通过建立多个 CMS 的群集，可以依次执行每个中央管理服务器的维护，而不会使 BI 平台服务中断。

但是，如果 BI 平台部署只有一个 CMS，则将其关闭将使用户无法使用该 BI 平台，并将中断报表和程序的处理。为了避免此问题，每个节点的服务器智能代理将确保至少有一个 CMS 在一直运行。仍然能够通过停止其 SIA 来停止 CMS，但在停止 SIA 之前，应通过 CMC 禁用处理服务器，以使这些服务器能够在 BI 平台关闭之前完成正在进行的任何作业，原因是节点上的所有其他服务器也将关闭。

注意：

可能会遇到 CMS 已停止并且需要从 CCM 中重新启动系统的情况。例如，如果您已关闭节点中的每个 CMS，且在 SIA 启动时已清除群集中每个 CMS 的“在服务器智能代理启动时自动启动此服务器”复选框，则必须使用 CCM 来重新启动系统。在 CCM 中，右击 SIA 并选择“属性”。在“启动”选项卡上，单击“属性”以打开 CMS 的“服务器属性”页面。选择“自动启动”，再单击“确定”以关闭“服务器属性”页面，然后再次单击“确定”。重新启动 SIA。仅当已清除群集中每个 CMS 的“在服务器智能代理启动时自动启动此服务器”复选框时，“自动启动”选项才可用。

如果希望在配置系统后能够在群集中启动和停止中央管理服务器，而不必启动和停止其他服务器，请将 CMS 放在单独的节点上。创建一个新节点，并将 CMS 克隆到该节点。如果 CMS 在其自己的节点上，将可以轻松地关闭节点，而不会影响其他服务器。

相关主题

- 第 381 页上的[“使用节点”](#)
- 第 355 页上的[“克隆服务器”](#)
- 第 357 页上的[“将中央管理服务器组成群集”](#)

10.4.4 启用和禁用服务器

如果禁用 BI 平台服务器，则会阻止服务器接收和响应新的 BI 平台请求，但实际上并未停止服务器进程。在要让服务器处理完所有当前请求之后才完全停止它时，这特别有用。

例如，您可能希望停止作业服务器之后才重新启动运行它的计算机。然而，您希望服务器能履行其队列中任何未履行的报表请求。首先，禁用作业服务器，这样它就不能接受任何其他请求了。接着，转到中央管理控制台，监视服务器何时完成其正在进行的作业。（在“服务器”管理区域中，右击服务器，然后选择“量度”。）然后，在服务器处理完当前请求后，可以安全停止服务器。

注意：

- CMS 必须处于运行状态以便启用和/或禁用其他服务器。
- 无法启用或禁用 CMS。

10.4.4.1 使用 CMC 启用和禁用服务器

- 1 转到 CMC 的“服务器”管理区域。
- 2 右击要更改状态的服务器，然后根据需要执行的操作，单击“启用服务器”或“禁用服务器”。

10.4.4.2 用 CCM 启用或禁用 Windows 服务器

- 1 在 CCM 中，单击“管理服务器”。
- 2 出现提示时，使用授予您 BI 平台管理权限的凭据登录到 CMS。
- 3 在“管理服务器”对话框中，选择要启用或禁用的服务器。
- 4 单击“启用”或“禁用”。
- 5 单击“关闭”以返回到 CCM。

10.5 添加、克隆或删除服务器

10.5.1 添加、克隆和删除服务器

如要在更多新计算机上安装服务器组件，为 BI 平台添加新硬件，则请在这些计算机上运行 BI 平台安装程序。设置程序允许执行“自定义”安装。在“自定义”安装过程中，指定现有部署中的 CMS，并选择要安装在本地计算机上的组件。有关自定义安装选项的详细信息，请参阅《SAP BusinessObjects Business Intelligence 平台安装指南》。

10.5.1.1 添加服务器

可以在同一台计算机上运行同一个 BI 平台服务器的多个实例。添加服务器：

- 1 转到 CMC 的“服务器”管理区域。
- 2 在“管理”菜单上，单击“新建” > “新建服务器”。
将出现“创建新服务器”对话框。
- 3 选择“服务类别”。
- 4 从“选择服务”列表中选择所需的服务类型，然后单击“下一步”。
- 5 若要将附加服务添加到服务器，请在“可用附加服务”列表中选择服务，然后单击“>”。

注意：

附加服务并非对所有服务器类型都可用。

- 6 添加了所需的附加服务后，单击“下一步”。
- 7 如果 BI 平台架构由多个节点组成，请从“节点”列表中选择要在其中添加新服务器的节点。
- 8 在“服务器名称”框中键入服务器的名称。

系统中每个服务器必须具有唯一的名称。默认命名约定是 <节点名称>.<服务器类型>（如果同一台主机上有多个同一类型的服务器，则追加一个数字）。

- 9 若要为服务器包括说明，请在“说明”框中键入说明。
- 10 如果要添加新的中央管理服务器，请在“名称服务器端口”字段中指定端口号。
11. 单击“创建”。

在 CMC 的“服务器”区域的服务器列表中出现新服务器，但没有启动或启用此服务器。

12. 如果希望新服务器开始响应 BI 平台请求，请使用 CMC 启动并启用该服务器。

相关主题

- 第 40 页上的[“服务器、服务、节点和主机”](#)
- 第 369 页上的[“配置服务器设置”](#)
- 第 378 页上的[“配置端口号”](#)
- 第 348 页上的[“查看服务器的状态”](#)

10.5.1.2 克隆服务器

如果要在部署中添加新的服务器实例，可以克隆现有服务器。克隆的服务器会保留原始服务器的配置设置。这在以下情况下可能特别有用：如果要扩展部署，并要创建新的服务器实例，而这些实例使用与现有服务器几乎全部相同的服务器配置设置。

克隆还简化了在节点之间移动服务器的过程。如果将现有 CMS 移到另一个节点，可以将其克隆到新节点。克隆的 CMS 将出现在新节点上，并保留原始 CMS 的所有配置设置。

在克隆服务器时，要牢记一些考虑事项。可能并不想克隆所有设置，因此，可取的做法是检查所克隆的服务器，以确保它满足需求。例如，如果要在同一台计算机上克隆一个 CMS，请确保更改从原始 CMS 复制到克隆的 CMS 的端口号设置。

注意：

- 在克隆服务器之前，确保部署中的所有计算机都具有相同的 SAP BusinessObjects Business Intelligence 平台版本（以及任何更新，如果适用）。
- 可以从任何计算机克隆服务器。不过，只能将服务器克隆到已安装了服务器所需的二进制文件的计算机中。
- 克隆服务器时，未必意味着新服务器将使用相同的操作系统凭据。用户帐户由在其下运行服务器的服务器智能代理进行控制。

10.5.1.2.1 为服务器设置使用占位符

占位符是运行于节点的服务器使用的节点级变量。占位符列在中央管理控制台（CMC）一个专门的页面上。双击 CMC 中的“服务器”下列出的任何服务器时，占位符左边的导航窗格上将出现一个链接。“占位符”页面列出了选定服务器的所有可用占位符名称及其关联的值。占位符包含只读值，并且占位符名称以百分比字符 % 开头和结尾。

注意：

可以始终用 CMC 服务器的“属性”页面中的特定字符串覆盖占位符设置。

示例：

在克隆服务器时，占位符特别有用。例如，多驱动器计算机 A 在 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0 中安装了 BI 平台。因此 %DefaultAuditingDir% 占位符将是 D:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\。

在另一台计算机（计算机 B）上，只有一个磁盘驱动器（没有驱动器 D），并且 BI 平台安装在 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0 中。在此情况下，%DefaultAuditingDir% 占位符将是 C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Auditing\。

要将事件服务器从计算机 A 克隆到计算机 B，如果为“审核临时目录”使用占位符，则占位符将会解析自身，并且事件服务器将正常工作。如果未使用占位符，除非手动覆盖“审核临时目录”设置，否则事件服务器将出现故障。

10.5.1.2.2 克隆服务器

- 1 在要添加克隆服务器的计算机上，转到 CMC 的“服务器”管理区域。
- 2 右击要克隆的服务器，然后选择“克隆服务器”。
将出现“克隆服务器”对话框。
- 3 在“新服务器名称”字段中，输入服务器名称（或使用默认名称）。
- 4 如果要克隆中央管理服务器，请在“名称服务器端口”字段中指定端口号。
- 5 在“克隆到节点”列表上，选择要在其中添加克隆服务器的节点，然后单击“确定”。
此时，CMC 的“服务器”管理区域出现新的服务器。

注意：

端口号设置也会被克隆。许多情况下（比如克隆 CMS），将需要更改端口号，以避免原始服务器和其克隆服务器之间出现端口冲突。

10.5.1.3 删除服务器

- 1 转到 CMC 的“服务器”管理区域。
- 2 停止要删除的服务器。
- 3 右击该服务器并选择“删除”。
- 4 如果提示确认，请单击“确定”。

10.6 将中央管理服务器组成群集

10.6.1 将中央管理服务器组成群集

如果实现规模较大或任务关键型的 SAP BusinessObjects Business Intelligence 平台，则可能希望在一个群集中一起运行几台 CMS 计算机。一个群集由两个或多个依据公用 CMS 系统数据库共同工作的 CMS 服务器组成。如果运行一个 CMS 的计算机出现故障，装有另一个 CMS 的计算机将继续处理 BI 平台请求。这种“高可用性”支持有助于确保 BI 平台用户在设备出现故障时仍然可以访问信息。

本节介绍如何将新的 CMS 群集成员添加到已经启动并正在运行的生产系统。向现有群集添加新的 CMS 时，指示新的 CMS 连接到现有 CMS 系统数据库，并与任何现有 CMS 计算机共同承担处理工作负载。要了解有关当前 CMS 的信息，请转到 CMC 的“服务器”管理区域。

在将 CMS 计算机组成群集前，必须确保各个 CMS 安装在满足产品可用性矩阵中概述的操作系统、数据库服务器、数据库访问方法、数据库驱动程序和数据库客户端的详细要求（包括版本和修补程序级别）的系统中。

此外，必须满足以下群集要求：

- 为了获得最好的性能，选择用来承载系统数据库的数据库服务器必须能够以极快的速度处理小查询。CMS 频繁与系统数据库通信并向该数据库发送很多小查询。如果数据库服务器不能及时处理这些请求，将极大地影响 BI 平台的性能。
- 为了获得最好的性能，在具有相同内存容量和相同类型 CPU 的计算机上运行各个 CMS 群集成员。
- 同等配置各台计算机：
 - 安装相同的操作系统，包括相同版本的操作系统 Service Pack 和修补程序。

- 安装相同版本的 BI 平台（包括修补程序，如果适用）。
 - 确保每个 CMS 都采用相同的方式连接到 CMS 系统数据库：不管是使用本机驱动程序还是 ODBC 驱动程序。确保驱动程序在每台计算机上都相同，并且都是受支持的版本。
 - 确保每个 CMS 都使用相同的数据库客户端连接到其系统数据库，并且是受支持的版本。
 - 检查每个 CMS 都使用相同的数据库用户帐户和密码连接到 CMS 系统数据库。此帐户必须具有在系统数据库中进行创建、删除和更新的权限。
 - 确保每个 CMS 所在的节点在相同的操作系统帐户下运行。（在 Windows 上，默认为“LocalSystem”帐户。）
 - 验证是否正确设置了每台 CMS 计算机上的当前日期和时间（包括夏令时设置）。
 - 确保群集中的所有计算机（包括承载 CMS 的计算机）均设置为相同的系统时间。为获得最佳结果，请将计算机与某个时间服务器（如 time.nist.gov）进行同步，或使用某个中央监控解决方案。
 - 确保在群集的所有 Web 应用程序服务器上安装相同的 WAR 文件。有关 WAR 文件部署的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台安装指南》。
 - 确保群集中的每个 CMS 都在相同的局域网中。
 - 带外线程（-oobthread）是通过群集 ping 和群集通知来使用的。由于两种操作均属于快速操作（通知属于异步操作），BI 平台不再需要多个 oobthread，且系统仅创建一个 oobthread。
- 如果群集具有超过八个 CMS 群集成员，请确保每个 CMS 的命令行都包含 -oobthreads numCMS 选项，其中 numCMS 是群集中 CMS 服务器的数量。此选项确保群集可以处理沉重的负载。有关配置服务器命令行的信息，请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》中的附录“服务器命令行”。
- 如果希望启用审核，必须将每个 CMS 配置为使用相同的审核数据库并以相同的方式连接到该数据库。在数据库服务器、客户端、访问方法、驱动程序和用户 ID 方面，审核数据库的要求与系统数据库的要求是相同的。

提示：

默认情况下，群集名称反映了安装的第一个 CMS 的计算机主机名。

相关主题

- 第 360 页上的[“更改 CMS 群集的名称”](#)

10.6.1.1 将 CMS 添加到群集中

可以采用多种方法来添加新的 CMS 群集成员。下面是相应的过程：

- 可以在新的计算机上安装包含 CMS 的新节点。

- 如果已经有包含 CMS 二进制文件的节点，则可以通过 CMC 添加新的 CMS 服务器。
- 如果已经有包含 CMS 二进制文件的节点，也可以通过克隆现有 CMS 服务器来添加新的 CMS 服务器。

注意：

在进行任何更改之前，备份当前的 CMS 系统数据库、服务器配置以及输入和输出文件资源库的内容。如有必要，请联系数据库管理员。

相关主题

- 第 359 页上的[“将新节点添加到群集中”](#)
- 第 354 页上的[“添加服务器”](#)
- 第 355 页上的[“克隆服务器”](#)
- 第 462 页上的[“备份和恢复概览”](#)

10.6.1.2 将新节点添加到群集中

添加节点（节点指由一个服务器智能代理托管的 BI 平台服务器集合）时，提示您新建 CMS 或将节点添加到一个现有 CMS 的群集。

如果要节点添加到现有 CMS 的群集，也可以使用安装设置程序。在要安装新 CMS 群集成员的计算机上运行 BI 安装和设置程序。设置程序允许执行“定制”安装。在定制安装过程中，指定要为其扩展系统的现有 CMS，并选择要在本地计算机上安装的组件。在此情况下，请指定正在现有系统上运行的 CMS 的名称，选择在本地计算机中安装新 CMS，向设置程序提供连接到现有 CMS 系统数据库所需的信息。设置程序在本地计算机上安装新的 CMS 时，它自动将服务器添加到现有群集。

注意：

在现有 CMS 中添加新节点时，如果新节点是全新服务器，那么在添加前，请确保该服务器上的 BI 平台安装与现有 BI 平台环境的修补程序级别相同。

相关主题

- 第 381 页上的[“使用节点”](#)

10.6.1.3 将群集添加到 Web 应用程序属性文件

如果已将其他 CMS 添加到部署中，并且使用 Java 应用程序服务器，则必须在 Web 应用程序部署的 \webapps\BOE\WEB-INF\config\custom 目录中修改 PlatformServices.properties 文件。

10.6.1.3.1 定义 BOE Web 应用程序的群集属性

- 1 在承载 Web 应用程序的计算机上访问 BOE.war 文件的自定义文件夹：

<安装目录>\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\BOE\WEB-INF\config\custom\。

之后，还需要重新部署已修改的 BOE.war 文件。

- 2 使用文本编辑器创建新文件。
- 3 指定 CMC 群集属性。

使用 cms.clusters 属性可指定部署中的所有群集。群集名称必须以 @ 字符开头，并用逗号分隔。例如，cms.clusters=@samplecluster、@samplecluster2、@samplecluster3。使用 cms.clusters.[群集名称] 属性指定群集中所含的每个 CMS。例如：

```
cms.clusters=@samplecluster,@samplecluster2, @samplecluster3
cms.clusters.samplecluster=cmsone:6400, cmstwo
cms.clusters.samplecluster2=cms3, cms4, cms5
cms.clusters.samplecluster3=aps05
```

注意：

用冒号将端口号与 CMS 名称分隔；除非指定端口号，否则假定端口号为 6400。

- 4 使用以下名称保存该文件：

PlatformServices.properties

- 5 重新启动应用程序服务器。

仅在在运行 Web 应用程序服务器的计算机上重新部署 BOE Web 应用程序后，新属性才生效。使用 WDeploy 在 Web 应用程序服务器上重新部署 WAR 文件。有关使用 WDeploy 的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

10.6.1.4 更改 CMS 群集的名称

通过执行以下过程，可以更改已安装的群集的名称。更改 CMS 群集的名称后，服务器智能代理会自动重新配置每个 SAP Business Objects 服务器，以便它向 CMS 群集注册，而不是向单个 CMS 注册。

注意：

提醒 BI 平台的老管理员们，请注意您可能无法再使用服务器命令行上的 `-ns` 选项配置服务器应向哪个 CMS 进行注册。此功能现在由 SIA 自动处理。

10.6.1.4.1 在 Windows 上更改群集名称

- 1 使用 CCM 为包含中央管理服务器（作为要更改其名称的群集的成员）的节点停止服务器智能代理。
- 2 右击服务器智能代理，并选择“属性”。
- 3 在“属性”对话框中，单击“配置”选项卡。
- 4 选中“将群集名称更改为”复选框。
- 5 输入群集的新名称。
- 6 单击“确定”，然后重新启动服务器智能代理。

现在 CMS 群集名称已更改。所有其他 CMS 群集成员将收到动态的新群集名称通知（尽管可能需要几分钟才能将更改通告各个群集成员）。

- 7 转到 CMC 的“服务器”管理区域，检查以确保所有服务器仍处于启用状态。如有必要，启用任何因更改而被禁用的服务器。

10.6.1.4.2 在 Unix 上更改群集名称

使用 `cmsdbsetup.sh` 脚本。有关参考，请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》中的“Unix 工具”一章。

10.7 管理服务器组

服务器组提供了一种对 BI 平台服务器进行组织以便它们更易于管理的方式。也就是说，当您管理服务器组时，您只需要查看系统上所有服务器的子集。更重要的是，使用服务器组的强大功能，您可以自定义 BI 平台以针对不同位置的用户或不同类型的对象优化系统。

如果按区域将服务器分组，您可以轻松地设置默认处理设置、重复发生计划和计划目标（适用于在特定区域办事处工作的用户）。可以将对象与单一服务器组关联，以使对象始终由同一服务器处理。并且，可以将被计划对象与特定服务器组关联，以确保将被计划对象发送到正确的打印机、文件服务器等。因此，在维护跨多个地点和多个时区的系统时，服务器组特别有用。

如果按类型对服务器进行分组，您可以将对象配置为由已针对这些对象加以优化的服务器处理。例如，处理服务器需要频繁地与包含已发布报表数据的数据库通信。如果将处理服务器放在靠近它们需要访问的数据库服务器的位置，则能够提高系统性能和最大程度地减小网络流量。因此，如果有大量依据 DB2 数据库运行的报表，可能需要创建仅依据 DB2 数据库服务器处理报表的处理服务器组。如果随后配置了相应的报表以始终使用该处理服务器组进行查看，则需要提升系统性能以便查看这些报表。

创建了服务器组之后，请配置对象以使用特定服务器组进行计划，或者查看和修改报表。使用 CMC 的“服务器”管理区域中的导航树来查看服务器组。利用“服务器组列表”选项可在“详细信息”窗格中显示服务器组的列表，而利用“服务器组”选项则可以查看组中的服务器。

10.7.1 创建服务器组

要创建某个服务器组，您需要指定该组的名称和说明，然后将服务器添加到该组。

10.7.1.1 创建服务器组

- 1 转到 CMC 的“服务器”管理区域。
- 2 选择“管理” > “新建” > “创建服务器组”。

将出现“创建服务器组”对话框。

- 3 在“名称”字段中，键入新服务器组的名称。
- 4 如果想要加上该服务器组的附加信息，请在“说明”字段中键入。
- 5 单击“确定”。
- 6 在“服务器”管理区域中，单击导航树中的“服务器组”，然后选择新的服务器组。
- 7 从“操作”菜单中选择“添加成员”。
- 8 选择要添加到该组的服务器，然后单击“>”。

提示：

使用 Ctrl + 单击操作组合来选择多个服务器。

- 9 单击“确定”。

将返回到“服务器”管理区域，该区域现在将列出已添加到组中的所有服务器。现在，您可以更改状态、查看服务器量度以及更改组中的服务器的属性。

相关主题

- 第 348 页上的“[查看服务器的状态](#)”

10.7.2 使用服务器子组

服务器的子组使您能够进一步组织您的服务器。子组只是作为另一个服务器组成员的服务器组。

例如，如果按区域和国家/地区对服务器分组，则每个区域组都将成为国家/地区组的子组。要按这种方式组织服务器，请首先为每个区域创建一个组，并将相应的服务器添加到每个区域组。然后，为每个国家/地区创建一个组，并将每个区域组添加到对应的国家/地区组。

可使用以下两种方式设置子组：您可以修改服务器组的子组，也可以使一个服务器组成为另一个服务器组的成员。这两种方法的效果相同，因此请使用最方便的方法。

10.7.2.1 将子组添加到服务器组

- 1 转到 CMC 的“服务器”管理区域。
- 2 单击导航树中的“服务器组”，然后选择要向其添加子组的服务器组。

该组是父组。

- 3 从“操作”菜单中选择“添加成员”。
- 4 单击导航树中的“服务器组”，选择要添加到该组的服务器组，然后单击“>”。

提示：

使用 Ctrl + 单击操作组合来选择多个服务器组。

- 5 单击“确定”。

将返回到“服务器”管理区域，该区域现在列出已添加到父组中的服务器组。

10.7.2.2 使一个服务器组成为另一个服务器组的成员

- 1 转到 CMC 的“服务器”管理区域。
- 2 单击要添加到另一个组的组。
- 3 从“操作”菜单中选择“添加到服务器组”。
- 4 在“可用服务器组”列表中，选择要将此组添加到的其他组，然后单击“>”。

提示：

使用 Ctrl + 单击操作组合来选择多个服务器组。

- 5 单击“确定”。

10.7.3 修改服务器的组成员资格

您可以修改服务器的组成员资格，以便快速将服务器添加到系统上已创建的任何组或子组（或从中删除服务器）。

例如，假设您为多个区域创建了服务器组。您可能要为多个区域使用一个中央管理服务器（CMS）。可以单击服务器的“成员”链接以同时将 CMS 添加到所有三个区域，而不必将 CMS 逐一添加到每个区域服务器组。

10.7.3.1 修改服务器的组成员资格

- 1 转到 CMC 的“服务器”管理区域。
- 2 右击要更改成员信息的服务器，然后选择“现有服务器组”。
在详细信息面板中，“可用服务器组”列表显示了可以将服务器添加到的组。“服务器组的成员”列表显示了服务器当前所属的任何服务器组。
- 3 要更改服务器作为其成员的组，请使用箭头在列表之间移动服务器组，然后单击“确定”。

10.7.4 用户对服务器和服务器组的访问

可以使用权限准许员工访问服务器和服务器组，以使用户可以执行如启动和停止服务器的任务。

取决于您的系统配置和安全问题，您可能想限制只有 BI 平台管理员才能管理服务器。但是，可能需要向使用这些服务器的用户提供访问权限。许多组织均设立了专职管理服务器的 IT 专业人员小组。如果服务器小组需要执行要求他们关闭和启动服务器的常规性服务器维护任务，则您需要向他们授予服务器访问权限。您可能也希望将 BI 平台服务器管理任务委派给其他人员。或者，您可能想让组织中的其他小组控制各自的服务器管理工作。

10.7.4.1 授予对服务器或服务器组的访问权限

- 1 转到 CMC 的“服务器”管理区域。
- 2 右击要授予访问权限的服务器或服务器组，然后选择“用户安全性”。
- 3 单击“添加主体”，添加要授予选定服务器或服务器组的访问权限的用户或组。
将出现“添加主体”对话框。
- 4 选择要授予指定服务器或服务器组的访问权限的用户或组，然后单击“>”。
- 5 单击“添加和指定安全性”。
- 6 在“指定安全性”屏幕上，为用户或用户组选择想要使用的安全设置，然后单击“确定”。

相关主题

- 第 112 页上的[“权限在 BI 平台中如何运作”](#)

10.7.4.2 Report Application Server的对象权限

要允许用户通过报表应用程序服务器（RAS）在 Web 上创建或修改报表，您必须拥有可在系统上使用的“RAS 报表修改”许可。同时，您必须授予用户最小的对象权限集。当您为用户授予了这些报表对象权限之后，用户将能够选择报表作为新报表的数据源，或直接修改报表：

- 查看对象（或查看文档实例，如果适用）
- 编辑对象
- 刷新报表的数据
- 导出报表的数据

用户还必须具有将对象添加到至少一个文件夹的权限，然后才能将新报表重新保存到 BI 平台中。

为了确保用户一直能够执行其他报表创建任务（如复制、计划、打印等），建议您首先分配相应的访问级别并更新您所做的更改。然后，将访问级别更改为“高级”，并添加尚未授予的任何必需权限。例如，如果用户已具有报表对象的“按需查看”权限，您可以允许用户修改报表，方法是将访问级别更改为“高级”，并显式地授予附加“编辑对象”权限。

当用户通过高级 DHTML 查看器和 RAS 查看报表时，“查看”访问级别已足以显示报表，但必须使用“按需查看”才能实际使用高级搜索功能。额外的“编辑对象”权限不是必需的。

10.8 为生产系统配置自适应处理服务器

安装程序在每个主机系统上安装一台自适应处理服务器（APS）。根据所安装的功能，此 APS 可能会承载多种服务，如监控服务、生命周期管理服务、多维分析服务（MDAS）、发布服务及其他服务。

对于生产系统或测试系统，最佳实践旨在创建更多 APS，并对 APS 进行配置以满足用户的业务需求。

可通过以下两种方式创建更多 APS：

- 运行系统配置向导。

该向导可帮助用户对 BI 平台系统进行基本配置，其中包括根据预定义部署模板配置 APS。尽管向导提供的 APS 配置是良好的起始点，但仍须执行系统大小调整。

也可从中央管理控制台（CMC）启动向导。有关向导的更多信息，请参阅第 81 页上的[“系统配置向导介绍”](#)。有关默认部署模板的更多信息，请参阅《SAP BusinessObjects BI platform Deployment

Templates》（SAP BusinessObjects BI 平台部署模板）文档，该文档可在向导中获取，也可访问 <http://help.sap.com/bobip41>。

- 使用 CMC 手动创建和配置更多 APS。有关详细信息，请参阅第 354 页上的 [“添加、克隆和删除服务器”](#)。

记忆：

在向导中选择部署模板或手动创建更多 APS 并不能取代系统大小调整。确保执行系统大小调整：
<http://www.sap.com/bisizing>。

10.9 评估系统的性能

10.9.1 监控 BI 平台服务器

通过监控应用程序，您可针对报表和通知捕获 BI 平台服务器的运行时和历史量度。该应用程序有助于系统管理员识别服务器是否工作正常，以及响应时间是否和预期一样。

相关主题

- 第 625 页上的 [“关于监控”](#)

10.9.2 分析服务器量度值

通过中央管理控制台（CMC）可以查看系统中的服务器的量度。这些量度值包括有关每台计算机的常规信息以及特定于服务器类型的详细信息。CMC 还使您可以查看系统量度值，包括有关产品版本、CMS 和当前系统活动的信息。

注意：

只能查看当前正在运行的服务器的量度。

10.9.2.1 查看服务器量度值

- 1 转到 CMC 的“服务器”管理区域。
- 2 右击要查看其量度的服务器，然后选择“量度”。
“量度”选项卡将显示服务器量度列表。

相关主题

- 第 370 页上的[“更改服务器的属性”](#)
- 第 946 页上的[“关于服务器量度附录”](#)

10.9.3 查看系统量度值

CMC 的“设置”管理区域显示系统量度值，提供有关 BI 平台服务安装的常规信息。“属性”区域包含有关产品版本和编译版本的信息。它还列出 CMS 数据库的数据源、数据库名称以及数据库用户名。“查看全局系统量度”区域列出当前帐户活动以及有关当前作业和已处理作业的统计数据。“群集”区域列出连接到的 CMS 的名称、CMS 群集的名称以及其他群集成员的名称。

10.9.3.1 查看系统量度值

- 1 转到 CMC 的“设置”管理区域。
- 2 单击箭头，扩展并查看“属性”、“查看全局系统量度”、“群集”或“热备份”区域的设置。

10.9.4 记录服务器活动

可通过 BI 平台记录关于 BI 平台 Web 活动的特定信息。

- 此外，每台 BI 平台服务器均设计为将消息记录到操作系统的标准系统日志中。
 - 在 Windows 上，BI 平台记录到事件日志服务中。可以用事件查看器查看结果（在应用程序日志中）。
 - 在 Unix 上，BI 平台将消息记录到作为用户应用程序的 syslog 后台程序中。每个服务器会在其记录的任何消息前加上它的名称和 PID。

各个服务器还将断言消息记录到产品安装的记录目录。记录到这些文件中的程序信息通常只对 SAP BusinessObjects 支持工作人员有用，他们可以用来进行高级调试。这些日志文件的位置视操作系统而定：

- 在 Windows 上，默认日志目录为安装目录\SAP BusinessObjects Enterprise XI 4.0\logging。
- 在 UNIX 上，默认日志目录为安装的安装目录/sap_bobj/logging 目录。

要注意的重要一点是，这些日志文件会被自动清除，因此为每个服务器记录的数据决不会超过大约 1 MB。

注意：

要对承载 BI 平台服务器的 Unix 计算机上的功能启用日志记录，必须设置和配置系统日志记录，以便记录已记录到信息级别或更高级别的用户设施中的所有消息。还必须将 SYSLOGD 配置为接受远程记录。

设置过程因系统而异。有关具体说明，请查阅操作系统文档。

10.10 配置服务器设置

本节包括说明如何修改 BI 平台服务器设置的技术信息和过程。

利用本节中讨论的大多数设置，可以将 BI 平台更有效地与当前的硬件、软件和网络配置集成在一起。因此，您选择的设置将在很大程度上取决于您自己的要求。

用户可通过两种方法在中央管理控制台（CMC）上更改服务器设置。

- 在服务器的“属性”屏幕上。
- 在服务器的“编辑公用服务”屏幕上。

请务必注意并非所有更改都将立即发生。如果无法立即更改设置，则“属性”和“编辑公用服务”屏幕将显示当前设置（红色文本）和所需设置。返回到“服务器管理”区域时，服务器将标记为“陈旧”。如果重启服务器，则服务器将使用所需设置，并且服务器的“陈旧”标记将被删除。

注意：

本节并不说明如何配置 Web 应用程序服务器以部署 BI 平台应用程序。此任务通常是在安装该产品时进行的。有关详细信息，请参阅《SAP BusinessObjects Business Intelligence 平台安装指南》。

相关主题

- 第 378 页上的[“配置端口号”](#)
- 第 370 页上的[“更改服务器的属性”](#)
- 第 417 页上的[“重新创建 CMS 系统数据库”](#)
- 第 415 页上的[“选择新的或现有的 CMS 数据库”](#)

10.10.1 更改服务器的属性

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击要更改设置的服务器。
将显示“属性”屏幕。
- 3 进行所需的更改，然后单击“保存”或“保存并关闭”。

注意：

并非所有更改都将立即发生。如果无法立即更改设置，则“属性”对话框将显示当前设置（红色文本）和所需设置。返回到“服务器管理”区域时，服务器将标记为“陈旧”。如果重启服务器，则服务器将使用“属性”对话框中的所需设置，并且服务器的“陈旧”标记将被删除。

10.10.2 向多个服务器应用服务设置

您可以将相同的设置应用于承载于多个服务器上的服务中。

- 1 转到 CMC 的“服务器”管理区域。
- 2 按 Ctrl 键，单击每台要更改其设置的、承载服务的服务器，然后右击并选择“编辑公用服务”。
随即显示“编辑公用服务”对话框，其中将显示您所选服务器中承载的、您已更改其设置的服务列表。
- 3 如果“编辑公用服务”对话框列出多个服务，请选择要编辑的服务并单击“继续”。
- 4 进行所需修改，然后单击“确定”。

注意：

将重新回到 CMC 的“服务器”管理区域。如果服务器需要重新启动，则该服务器将标记为“停滞”。重新启动服务器之后，它将使用新设置，且“停滞”标志将删除。

10. 10. 3 使用配置模板

利用配置模板可以轻松地配置服务器的多个实例。配置模板存储每种服务类型的设置列表，可以使用它来配置其他服务器实例。例如，如果有 12 台要以相同方式配置的 Web Intelligence 处理服务器，则只需为其中的一台服务器配置设置。然后，可以使用配置的服务来定义 Web Intelligence 处理服务器的配置模板，接着将该模板应用于其他 11 个服务实例。

每种类型的 BI 平台服务都有自己的配置模板。例如，Web Intelligence 处理服务类型有一个配置模板，发布服务类型有一个配置模板，诸如此类。配置模板是在中央管理控制台（CMC）的服务器属性中定义的。

将服务器设置为使用配置模板时，该服务器的现有设置将被模板中的值覆盖。如果稍后决定停止使用模板，将不会还原原始设置。随后对配置模板进行的更改不再会影响服务器。

最好按如下方式使用配置模板：

- 1 在一台服务器上设置配置模板。
- 2 假设要为同一类型的所有服务器使用相同的配置，请为同一类型的所有服务器（包括在其中设置配置模板的服务器）选中“使用配置模板”。
- 3 稍后，如果要更改此类型的所有服务的配置，请查看其中任意一个服务的属性，取消选中“使用配置模板”复选框。更改所需的设置，然后为此服务器选中“设置配置模板”并单击“保存”。该类型的所有服务即会更新。如果没有始终设置为配置模板的服务器，将可确保不会意外更改该类型的所有服务器的配置设置。

相关主题

- 第 371 页上的“[设置配置模板](#)”
- 第 372 页上的“[将配置模板应用于服务器](#)”

10. 10. 3. 1 设置配置模板

可以为每种类型的服务设置一个配置模板。不能为一种服务设置多个配置模板。可以使用任何服务器的“属性”页面来配置配置模板将为服务器上承载的服务类型使用的设置。

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击要设置配置模板的服务的承载服务器。
将显示“属性”屏幕。
- 3 配置了要在模板中使用的服务设置后，请选中“设置配置模板”复选框，并单击“保存”或“保存并关闭”。

所选服务类型的配置模板是根据当前服务器的设置定义的。将会自动立即重新配置承载相同服务的同一类型的其他服务器，以与配置模板相匹配（如果这些服务器已在其属性中启用了“使用配置模板”选项）。

注意：

如果未显式定义配置模板的设置，将会使用服务的默认设置。

相关主题

- 第 372 页上的[“将配置模板应用于服务器”](#)

10.10.3.2 将配置模板应用于服务器

在应用配置模板之前，请确保已为要应用模板的服务器的类型定义了配置模板设置。如果未显式定义配置模板设置，则会使用服务的默认设置。

注意：

修改配置模板的设置时，未启用“使用配置模板”设置的服务器将不会更新。

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击要应用配置模板的服务的承载服务器。
将显示“属性”屏幕。
- 3 选中“使用配置模板”复选框，并单击“保存”或“保存并关闭”。

注意：

如果服务器需要重新启动以使新设置生效，该服务器在服务器列表中将显示为“陈旧”。

即将将相应的配置模板应用于当前服务器。随后对该配置模板进行的任何更改都会改变使用该配置模板的所有服务器的配置。

取消选中“使用配置模板”不会将服务器配置还原为应用配置模板时的值。随后对配置模板进行的更改不会影响正在使用配置模板的服务器的配置。

相关主题

- 第 371 页上的[“设置配置模板”](#)

10.10.3.3 还原系统默认值

可能需要将服务的配置还原为最初安装服务所使用的设置（例如，在服务器配置不正确或遇到性能问题的情况下）。

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击要还原为系统默认设置的服务的承载服务器。
将显示“属性”屏幕。
- 3 选中“还原系统默认值”复选框，并单击“保存”或“保存并关闭”。
特定服务类型的默认设置即被还原。

10.11 配置服务器网络设置

通过 CMC 可以管理 BI 平台服务器的网络设置。这些设置分为以下两类：端口设置和主机标识。

默认设置

在安装过程中，服务器主机标识符会设置为“自动分配”。但是，可以为每台服务器分配一个特定的 IP 地址或主机名。默认 CMS 端口号为 6400。其他 BI 平台服务器会动态绑定到可用端口。端口号由 BI 平台自动管理，但可以使用 CMC 指定。

10.11.1 网络环境选项

BI 平台同时支持 Internet 协议版本 6 (IPv6) 和 Internet 协议版本 4 (IPv4) 网络通信。可以在以下任意环境中使用服务器和客户端组件：

- IPv4 网络：所有服务器和客户端组件仅使用 IPv4 协议运行。
- IPv6 网络：所有服务器和客户端组件仅使用 IPv6 协议运行。
- 混合的 IPv6/IPv4 网络：服务器和客户端组件可使用 IPv6 和 IPv4 协议运行。

注意：

网络配置应该由系统和网络管理员来执行。BI 平台并不提供用于指定网络环境的机制。可以使用 CMC 绑定到任何 BI 平台服务器的特定 IPv6 或 IPv4 地址。

10.11.1.1 混合的 IPv6/IPv4 环境

在 IPv6/IPv4 网络环境中：

- BI 平台服务器在 IPv6/IPv4 混合模式下运行时，可以为 IPv6 和 IPv4 请求提供服务。
- 客户端组件可以作为纯 IPv6 节点、纯 IPv4 节点或 IPv6/IPv4 节点与服务器进行交互操作。

在以下方案中，混合模式特别有用：

- 从纯 IPv4 节点环境向纯 IPv6 节点环境转换。所有客户端和服务组件将继续无缝地进行交互操作，直到转换完成为止。然后可以对所有服务器取消激活 IPv4 设置。
- 与 IPv6 不兼容的第三方软件在 IPv6/IPv4 节点环境中将可以继续运行。

10.11.2 服务器主机标识选项

可以在 CMC 中为所有 BI 平台服务器指定主机识别选项。下表中总结了“公共设置”区域中的可用选项：

选项	说明
自动分配	<p>这是所有服务器的默认设置。如果选中该复选框，则服务器会自动将服务器的请求端口绑定到计算机上的第一个网络接口。</p> <p>注意： 最好选中“主机名”的“自动分配”复选框。但是，在某些情况下，例如当服务器在多宿主计算机上运行，或服务器需要与某一防火墙配置进行交互操作时，应该考虑使用特定的主机名或 IP 地址。有关“配置多宿主计算机”和“使用防火墙”的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》。</p>
主机名	指定服务器侦听请求时所用的网络接口的主机名。对于 CMS，此设置将指定 CMS 将名称服务器端口和请求端口绑定到的网络接口的主机名。
IP 地址	指定服务器侦听请求时所用的网络接口的 IP 地址。对于 CMS，此设置将指定 CMS 将名称服务器端口绑定到请求端口的网络接口的地址。对于所有服务器，将提供单独的字段以指定 IPv4 和/或 IPv6 IP 地址。

警告：

如果在多宿主计算机上选中“自动分配”复选框，则 CMS 可能会自动绑定至错误的网络接口。要防止发生此类错误，请确保（使用计算机的操作系统工具）按正确顺序列出主机计算机上的网络接口。此外，还必须在 CMC 中指定 CMS 的“主机名”。

注意：

如果使用多宿主计算机或采用某些 NAT 防火墙配置，则可能需要使用全限定域名（而不是主机名）来指定主机名。

相关主题

- 第 176 页上的[“针对防火墙配置系统”](#)
- 第 376 页上的[“配置多宿主计算机”](#)
- 第 378 页上的[“多网络接口疑难解答”](#)

10.11.2.1 修改服务器的主机标识

- 1 转到 CMC 的“服务器”管理区域。
- 2 选择服务器，然后从“操作”菜单中选择“停止服务器”。
- 3 从“管理”菜单中选择“属性”。

- 4 在“公共设置”下，选择以下选项之一：

选项	说明
自动分配	服务器将绑定至可用的网络接口之一。
主机名	输入服务器侦听请求时所使用网络接口的主机名。
IP 地址	在提供的字段中为服务器侦听请求时所用的网络接口输入 IPv4 或 IPv6 IP 地址。 注意： 要使服务器能够作为 IPv4/IPv6 双重节点运行，请在两个字段中均输入有效的 IP 地址。

- 5 单击“保存”或“保存并关闭”。
更改反映在“属性”选项卡上显示的命令行中。
- 6 启动并启用服务器。

10.11.3 配置多宿主计算机

多宿主计算机是指具有多个网络地址的计算机。可以用每个接口具有一个或多个 IP 地址的多个网络接口实现多址计算机，也可以用指定了多个 IP 地址的单个网络接口实现多址计算机。

如果有多个网络接口且每个接口有一个 IP 地址，请更改绑定顺序，使位于绑定顺序最前面的网络接口成为您希望信息平台服务服务器绑定到的接口。如果接口有多个 IP 地址，请使用 CMC 中的“主机标识符”选项为 BI 平台服务器指定网络接口卡。可以按主机名或 IP 地址指定该接口卡。有关配置“主机标识符”设置的更多信息，请参阅“多网络接口疑难解答”。

提示：

本节说明如何将所有服务器限制到相同的网络地址，但您也可以将单个服务器绑定到不同的地址。例如，您可能希望将文件资源库服务器绑定到一个不能从用户的计算机访问的私有地址。此类高级配置要求 DNS 配置在所有 BI 平台服务器组件之间有效地发送通信。在此示例中，DNS 必须从其他 BI 平台服务器将通信发送到文件资源库服务器的私有地址。

相关主题

- 第 378 页上的[“多网络接口疑难解答”](#)

10.11.3.1 将 CMS 配置为绑定到一个网络地址

注意：

在多宿主计算机上，可以将“主机标识符”设置为希望服务器绑定到的接口的完全限定域名或 IP 地址。

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击 CMS。
- 3 在“公共设置”下，选择以下选项之一：
 - 主机名
 - 输入服务器要绑定到的网络接口的主机名。
 - IP 地址
 - 在提供的字段中为服务器将绑定到的网络接口输入 IPv4 或 IPv6 IP 地址。

注意：

要使服务器能够作为 IPv4/IPv6 双重节点运行，请在两个字段中均输入有效的 IP 地址。

警告：

不要选择“自动分配”。

- 4 对于“请求端口”，可执行以下操作之一：
 - 选择“自动分配”选项。
 - 在“请求端口”字段中输入有效的端口号。
- 5 确保在“名称服务器端口”对话框中指定端口号。

注意：

默认端口号为 6400。

10.11.3.2 将余下的服务器配置为绑定到一个网络地址

默认情况下，其余 BI 平台服务器将动态选择端口。有关禁用动态传播此信息的“自动分配”设置的信息，请参阅“更改服务器用于接受请求的端口”。

相关主题

- 第 381 页上的[“更改服务器用于接受请求的端口”](#)

10.11.3.3 多网络接口疑难解答

在多宿主计算机上，CMS 可能会自动绑定至错误的网络接口。要防止此类错误发生，可以确保（使用计算机的操作系统工具）按正确顺序列出主机上的网络接口，或确保在 CMC 中指定 CMS 的主机名设置。如果主网络接口不可路由，则可以使用以下过程将 BI 平台配置为绑定到可路由的非主网络接口。在本地计算机上安装 BI 平台之后，且在其他计算机上安装 BI 平台之前，请立即执行以下步骤。

1. 在具有多个网络接口的计算机上，打开 CCM 并停止节点的 SIA。
2. 右击 SIA 并选择“属性”。
3. 在“属性”对话框中，单击“配置”选项卡。
4. 要将 SIA 绑定到特定的网络接口，请在“端口”字段中键入目标网络接口的端口号。
5. 单击“确定”并选择“启动”选项卡。
6. 从“本地 CMS 服务器”列表中选择 CMS，并单击“属性”。
7. 要将 CMS 绑定到特定的网络接口，请在“端口”字段中键入目标网络接口的端口号。
8. 单击“确定”以应用新设置。
9. 启动 SIA 并等待服务器启动。
10. 启动中央管理控制台（CMC），并转到“服务器”管理区域。对每台服务器重复步骤 11-14。
11. 选择服务器，然后从“操作”菜单中选择“停止服务器”。
12. 从“管理”菜单中选择“属性”。
13. 在“公共设置”下，选择以下选项之一：
 - 主机名：输入服务器将绑定到的网络接口的主机名。
 - IP 地址：在提供的字段中为服务器将绑定到的网络接口输入 IPv4 或 IPv6 IP 地址。

注意：

要使服务器能够作为 IPv4/IPv6 双重节点运行，请在两个字段中均输入有效的 IP 地址。

警告：

不要选择“自动分配”。

14. 单击“保存”或“保存并关闭”。
15. 返回到 CCM 并重新启动 SIA。

SIA 将重新启动节点上的所有服务器。计算机上的所有服务器现在已绑定到正确的网络接口。

10.11.4 配置端口号

在安装过程中，CMS 被设置为使用默认端口号。默认 CMS 端口号为 6400。此端口位于 SAP BusinessObjects 保留的端口范围内（6400 至 6410）。这些端口上的通信应该不会与第三方应用程序冲突。

其他每个 BI 平台服务器在启动并启用后均动态绑定到可用端口（大于 1024），并通过此端口在 CMS 上注册，然后侦听 BI 平台请求。如有必要，可指示各个服务器组件侦听特定端口（而不是动态选择任何可用端口）。例如，对于必须跨防火墙进行通信的每台 BI 平台服务器，需要手动为其配置请求端口。

可以在 CMC 中每个服务器的“属性”选项卡上指定端口号。下表汇总了“公共设置”区域下与具体服务器类型的端口使用有关的选项：

设置	CMS	其他服务器
请求端口	指定 CMS 用于从其他服务器接受所有请求（除名称服务器请求外）的端口。使用相同的网络接口作为名称服务器端口。如果选中了“自动分配”，服务器将自动使用操作系统分配的端口号。	指定服务器侦听所有请求时所用的端口。如果选择了“自动分配”，服务器将自动使用 OS 分配的端口号。
名称服务器端口	指定 CMS 侦听名称服务请求时所使用的 BI 平台端口。默认值为 6400。	不适用。

10.11.4.1 在 CMC 中更改默认 CMS 端口

如果群集上有 CMS 已在运行，可以使用 CMC 来更改默认的 CMS 端口号。如果群集上没有 CMS 正在运行，则必须使用 CCM（在 Windows 上）或 serverconfig.sh 脚本（在 Unix 上）来更改端口号。

注意：

CMS 为请求端口和名称服务器端口使用相同的网络接口卡。

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击服务器列表中的 CMS。
- 3 将“名称服务器端口”号替换为想要 CMS 进行侦听所使用的端口。（默认端口为 6400。）
- 4 单击“保存并关闭”。
- 5 重新启动 CMS。

CMS 将开始使用指定的端口号侦听。如果节点上的其他服务器为请求端口选择了“自动分配”选项，服务器智能代理会将新设置动态传播到这些服务器。（所做更改需要几分钟才会出现在所有节点成员的“属性”设置中。）

在“属性”页面上选择的设置会反映在服务器命令行中，该命令行也出现在“属性”页面上。

10.11.4.2 在 Windows 上更改 CCM 中的默认 CMS 端口

如果群集中没有可访问的 CMS，而用户想要修改部署中一个或多个 CMS 的默认 CMS 端口，则必须使用 CCM 更改 CMS 端口号。

- 1 打开 CCM 并停止节点的 SIA。
- 2 右击 SIA 并选择“属性”。
- 3 在“属性”对话框中，单击“启动”选项卡。
- 4 从“本地 CMS 服务器”列表中选择要更改其端口号的 CMS，并单击“属性”。
- 5 要将 CMS 绑定到特定端口，请在“端口”字段中键入端口号。
- 6 单击“确定”以应用新设置。
- 7 启动 SIA 并等待服务器启动。

10.11.4.3 在 Unix 上更改 CCM 中的默认 CMS 端口

如果群集中没有可访问的 CMS，而用户想要修改部署中一个或多个 CMS 的默认 CMS 端口，则可使用 `serverconfig.sh` 脚本更改 CMS 端口号。

- 1 使用 `ccm.sh` 脚本来停止承载想要更改其端口号的 CMS 的服务器智能代理（SIA）。
- 2 运行 `serverconfig.sh` 脚本。
默认情况下，此脚本位于 <安装目录>/sap_bobj 目录中。
- 3 选择“3 - Modify node”，并按 Enter 键。
- 4 选择承载要修改的 CMS 的节点，并按 Enter 键。
- 5 选择“3 - 修改本地 CMS”，并按 Enter 键。
将显示该节点上承载的 CMS 列表。
- 6 选择 CMS 进行修改，并按 Enter 键。
- 7 键入 CMS 的新端口号，并按 Enter 键。
- 8 指定是否希望在 SIA 启动时 CMS 自动启动，并按 Enter 键。

9. 键入 CMS 的命令行参数，或接受当前参数，并按 Enter 键。
10. 键入 “quit” 可退出脚本。
11. 使用 ccm.sh 脚本启动 SIA，并等待服务器启动。

10.11.4.4 更改服务器用于接受请求的端口

注意：

这些步骤不能用于更改中央管理服务器（CMS）的请求端口。请参阅“更改 CMS 用于接受请求的端口”。

1. 转到 CMC 的“服务器”管理区域。
2. 选择服务器，然后从“操作”菜单中选择“停止服务器”。
3. 双击服务器。
将显示“属”屏幕。
4. 在“公共设置”下，取消选择“请求端口”的“自动分配”复选框，然后键入希望服务器侦听的端口号。
5. 单击“保存”或“保存并关闭”。
6. 启动并启用服务器。

服务器将绑定到新端口，向 CMS 注册，并开始使用新端口侦听 BI 平台请求。

10.12 管理节点

10.12.1 使用节点

节点是指在同一主机上运行且由同一服务器智能代理（SIA）管理的一组 BI 平台服务器。节点上的所有服务器都使用相同的用户帐户运行。一台计算机可以包含许多节点，因此可以在不同用户帐户下运行进程。一个 SIA 负责管理和监控某个节点上的所有服务器，确保它们正常工作。

注意：

必须使用带 Enterprise 身份验证的管理员帐户安全地执行所有节点管理过程。然而，如果已启用服务器间的 SSL 通信，则必须禁用 SSL 才能执行任何节点管理任务。

注意：

请确保使任一 BI 平台服务器连接到其数据源（例如，使 CMS 连接到 CMS 数据库）所需的所有数据库驱动程序均已安装，并且已设置了正确的环境（例如，已设置相应环境变量）。

相关主题

- 第 158 页上的[“针对 SSL 配置服务器”](#)
- 第 383 页上的[“为 SQL Anywhere 准备 Unix 计算机”](#)

10.12.1.1 变量

变量	说明
<INSTALLDIR>	安装 SAP BusinessObjects Business Intelligence 平台的目录。 在 Windows 上, 为 C:\Program Files (x86)\SAP BusinessObjects
<SCRIPTDIR>	节点管理脚本所在的目录。 <ul style="list-style-type: none"> 在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts 在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/<平台 64>/scripts
<平台 32>	Unix 操作系统的名称。接受的值包括: <ul style="list-style-type: none"> aix_rs6000 linux_x86 solaris_sparc win32_x86
<PLATFORM64>	Unix 操作系统的名称。接受的值包括: <ul style="list-style-type: none"> aix_rs6000_64 linux_x64 solaris_sparcv9 win64_x64

10.12.1.2 为 SQL Anywhere 准备 Unix 计算机

必须创建一个 odbc.ini 文件并以其为源, 然后才能使用 SQL Anywhere 作为 Unix 计算机上的 ODBC 数据源。

注意:

如果使用随 BI 平台一起安装的绑定 SQL Anywhere, 则无需执行此过程。

- 1 在安装目录/sap_bobj/enterprise_xi40/PLATFORM64中创建 odbc.ini。
- 2 输入数据库源名称 (DSN)、SQL Anywhere 的数据库名称和服务器名称以及承载 SQL Anywhere 数据库服务器的计算机的 IP 地址和端口号。
- 3 保存 odbc.ini。
- 4 将 SQL Anywhere 环境部署到当前环境中。

例如, 如果使用 Bash 作为命令行 shell, 则以 sa_config.sh 的 64 位版本为源。

- 5 定义名为 ODBCINI 的环境变量，该变量指向 odbc.ini 文件的创建位置。
对该环境变量进行设置，从而使子进程可以检测到 ODBCINI 环境变量。

示例：

示例 odbc.ini 文件：

```
[ODBC Data Sources]
SampleDatabase=SQLAnywhere 12.0

[SampleDatabase]
UID=Administrator
PWD=password
DatabaseName=SampleDatabase
ServerName=SampleDatabase
CommLinks=tcpip(host=192.0.2.0;port=2638)
Driver=/build/bo/sqlanywhere12/lib64/libdbodbc12.so
```

示例 source 命令：

```
source /build/bo/sqlanywhere12/bin64/sa_config.sh
ODBCINI=/build/bo/sap_bobj/enterprise_xi40/linux_x64/odbc.ini;export ODBCINI
```

相关主题

- 第 382 页上的[“变量”](#)

10.12.2 添加新节点

首次安装 BI 平台时，安装程序会创建单个节点。

如果希望在不同用户帐户下运行服务器，可能需要附加节点。

可以使用中央配置管理器（CCM）或节点管理脚本添加新节点。如果使用防火墙，请确保打开服务器智能代理（SIA）和中央管理服务器（CMS）的端口。

注意：

在希望添加节点的计算机上使用 CCM 或节点管理脚本。无法在远程计算机上添加节点。

BI 平台安装是计算机上的安装程序创建的 BI 平台文件的唯一实例。BI 平台安装的实例只能在单个群集内使用。不支持属于共享同一 BI 平台安装的不同群集的节点，因为此类部署无法修补或更新。只有 Unix 平台才能支持在同一计算机上进行软件的多次安装，但仅限于使用唯一用户帐户执行每次安装且安装到单独文件夹时，这样，才能避免安装之间共享任何文件。

请记住，群集中的所有计算机的版本和修补程序级别都必须相同。

10.12.2.1 向现有部署中的新计算机添加节点

使用安装程序向现有部署中添加新计算机时，可以自动在计算机上创建第一个节点。

提示：

在安装过程中，单击“展开”，并指定现有中央管理服务器。

如果要创建其他节点，可使用中央配置管理器或 `serverconfig.sh` 脚本。

有关安装的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台安装指南》。

10.12.2.2 在 Windows 上添加节点

警告：

在添加节点前后，备份整个群集的服务器配置。

- 1 在中央配置管理器（CCM）的工具栏上，单击“添加节点”。
- 2 在“添加节点向导”中，输入新服务器智能代理（SIA）的节点名称和端口号。
- 3 选择是否希望在新节点上创建服务器。

- 添加不包含服务器的节点
- 添加包含 CMS 的节点
- 添加包含默认服务器的节点

此选项只创建安装在此计算机上的服务器。其中并不包含所有可能的服务器。

- 4 选择一个 CMS。
 - 如果部署正在运行，请选择“使用正在运行的现有 CMS”并单击“下一步”。
出现提示后，输入现有 CMS 的主机名和端口号、管理员凭据、数据源名称、系统数据库的凭据以及群集密钥。
 - 如果部署已停止，请选择“启动新的临时 CMS”并单击“下一步”。
出现提示后，输入临时 CMS 的主机名和端口号、管理员凭据、数据源名称、系统数据库的数据库凭据以及群集密钥。此时，临时 CMS 将启动。（它将在此进程结束后停止。）

警告：

当临时 CMS 正在运行时，请避免使用部署。请确保现有 CMS 与新 CMS 使用不同的端口。

- 5 检查确认页面并单击“完成”。

CCM 将创建一个节点如果发生任何错误，请查看日志文件。

现在可以使用 CCM 启动新节点。

10.12.2.2.1 使用脚本在 Windows 上添加节点

警告：

在添加节点前后，备份整个群集的服务器配置。

可以使用 AddNode.bat 在 Windows 计算机上添加节点。有关更多信息，请参阅“用于添加、重新创建和删除节点的脚本参数”一节。

示例：

由于命令提示符的限制，必需使用插入符号（^）转义这些参数中的空格、等号（=）和分号（;），除非将文本包括在引号中。

```
<SCRIPTDIR>\AddNode.bat -name mynode2
-siaport 6415
-cms mycms:6400
-username Administrator
-password My Password
-cmsport 7400
-dbdriver mysqlbasesubsystem
-connect "DSN=BusinessObjects CMS 140;UID=username;PWD>Password1;HOSTNAME=database;PORT=3306"
-dbkey abc1234
-noservers
-createcms
```

注意：

要避免在长字符串中使用插入符号，可以将脚本的名称及其所有参数写入一个临时 response.bat 文件，然后在不使用任何参数的情况下运行 response.bat。

相关主题

- 第 382 页上的[“变量”](#)
- 第 399 页上的[“用于添加、重新创建和删除节点的脚本参数”](#)

10.12.2.3 在 Unix 上添加节点

警告：

在添加节点前后，备份整个群集的服务器配置。

- 1 运行安装目录/sap_bobj/serverconfig.sh
 - 2 选择“1 - 添加节点”，并按 Enter 键。
 - 3 键入新节点的名称，并按 Enter 键。
 - 4 键入新 SIA 的端口号，并按 Enter 键。
 - 5 选择是否希望在新节点上创建服务器。
 - no servers
创建不包含任何服务器的节点。
 - cms
在节点上创建一个 CMS，但不创建其他服务器。
 - 默认服务器
只创建安装在此计算机上的服务器。其中并不包含所有可能的服务器。
 - 6 选择一个 CMS。
 - 如果部署正在运行，请选择“现有”并按 Enter 键。
出现提示后，输入现有 CMS 的主机名和端口号、管理员凭据、系统数据库的数据库连接信息和凭据以及群集密钥。
 - 如果部署已停止，请选择“临时”并按 Enter 键。
出现提示后，输入临时 CMS 的主机名和端口号、管理员凭据、系统数据库的数据库连接信息和凭据以及群集密钥。此时，临时 CMS 将启动。（它将在此进程结束后停止。）
- 警告：**
当临时 CMS 正在运行时，请避免使用部署。请确保现有 CMS 与新 CMS 使用不同的端口。
- 7 检查确认页面并按 Enter 键。
CCM 将创建一个节点。如果发生任何错误，请查看日志文件。
现在可以运行安装目录/sap_bobj/ccm.sh -start nodeName 以启动新节点。

10.12.2.3.1 使用脚本在 Unix 上添加节点

警告：

在添加节点前后，备份整个群集的服务器配置。

可以使用 `addnode.sh` 在 Unix 计算机上添加节点。有关更多信息，请参阅“用于添加、重新创建和删除节点的脚本参数”一节。

示例：

```
<SCRIPTDIR>/addnode.sh -name mynode2
-siaport 6415
-cms mycms:6400
-username Administrator
-password Password1
-cmsport 7400
-dbdriver mysqldatabasesubsystem
-connect "DSN=BusinessObjects CMS 140;UID=Administrator;PWD=Password1;HOSTNAME=myDatabase;PORT=3306"
-dbkey abc1234
-noservers
-createcms
```

相关主题

- 第 382 页上的[“变量”](#)
- 第 399 页上的[“用于添加、重新创建和删除节点的脚本参数”](#)

10.12.3 重新创建节点

在恢复整个群集的服务器配置之后，或者如果承载部署的计算机出现故障、损坏或文件系统崩溃，则可以使用中央配置管理器（CCM）或节点管理脚本重新创建节点。使用以下指导原则：

- 如果使用相同的安装选项和节点名称在替代计算机上重新安装部署，则无需重新创建节点。安装程序会自动重新创建节点。
- 只能在具有相同安装选项和修补程序级别的现有部署所在的计算机上重新创建节点。
- 只能重新创建在部署中的任何计算机上都不存在的节点。请确保没有其他计算机承载同一节点。
- 虽然部署允许节点运行在不同操作系统上，但只能在使用相同操作系统的计算机上重新创建节点。
- 如果使用防火墙，请确保打开服务器智能代理（SIA）和中央管理服务器（CMS）的端口。

记忆：

只能在节点所在的计算机上重新创建节点。

相关主题

- 第 472 页上的[“恢复系统”](#)

10.12.3.1 在 Windows 上重新创建节点

- 1 在中央配置管理器（CCM）的工具栏上，单击“添加节点”。
- 2 在“添加节点向导”中，输入重新创建的服务器智能代理（SIA）的节点名称和端口号。

注意：

原始节点和重新创建的节点的名称必须相同。

- 3 选择“重新创建节点”并单击“下一步”。
 - 如果该节点存在于中央管理服务器（CMS）的系统数据库中，则会在本地主机上重新创建它。

警告：

仅当该节点不存在于群集中的任何主机上时才使用此选项。

- 如果该节点不存在于 CMS 的系统数据库中，则会添加一个包含默认服务器的新节点。默认服务器包括主机上安装的所有服务器。
- 4 选择一个 CMS。
 - 如果 CMS 正在运行，请选择“使用正在运行的现有 CMS”并单击“下一步”。

出现提示后，输入现有 CMS 的主机名和端口号、管理员凭据、数据源名称、系统数据库的凭据以及群集密钥。
 - 如果 CMS 已停止，请选择“启动新的临时 CMS”并单击“下一步”。

出现提示后，输入临时 CMS 的主机名、管理员凭据、数据源名称、系统数据库的凭据以及群集密钥。此时，临时 CMS 将启动。（它将在此进程结束后停止。）

警告：

当临时 CMS 正在运行时，请避免使用部署。

- 5 检查确认页面并单击“完成”。

CCM 重新创建该节点，并将有关该节点的信息添加到本地计算机中。如果发生任何错误，请查看日志文件。

现在可以使用 CCM 启动重新创建的节点。

10.12.3.1.1 使用脚本在 Windows 上重新创建节点

可以使用 AddNode.bat 在 Windows 计算机上重新创建节点。有关更多信息，请参阅“用于添加、重新创建和删除节点的脚本参数”一节。

示例：

由于命令提示符的限制，必需使用插入符号（^）转义这些参数中的空格、等号（=）和分号（;），除非将文本包括在引号中。

```
<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
```

注意：

要避免在长字符串中使用插入符号，可以将脚本的名称及其所有参数写入一个临时 response.bat 文件，然后在不使用任何参数的情况下运行 response.bat。

相关主题

- 第 382 页上的[“变量”](#)
- 第 399 页上的[“用于添加、重新创建和删除节点的脚本参数”](#)

10.12.3.2 在 Unix 上重新创建节点

- 1 运行安装目录/sap_bobj/serverconfig.sh
- 2 选择“1 - 添加节点”，并按 Enter 键。
- 3 键入新节点的名称，并按 Enter 键。

注意：

原始节点和重新创建的节点的名称必须相同。

- 4 键入新 SIA 的端口号，并按 Enter 键。
- 5 选择“重新创建节点”，并按 Enter 键。
 - 如果该节点存在于中央管理服务器（CMS）的系统数据库中，则会在本地主机上重新创建它。

警告：

仅当该节点不存在于群集中的任何主机上时才使用此选项。

- 如果该节点不存在于 CMS 的系统数据库中，则会添加一个包含默认服务器的新节点。默认服务器包括主机上安装的所有服务器。

6 选择一个 CMS。

- 如果部署正在运行，请选择“现有”并按 Enter 键。

出现提示后，输入现有 CMS 的主机名和端口号、管理员凭据、系统数据库的数据库连接信息和凭据以及群集密钥。

- 如果部署已停止，请选择“临时”并按 Enter 键。

出现提示后，输入临时 CMS 的主机名、管理员凭据、系统数据库的数据库连接信息和凭据以及群集密钥。此时，临时 CMS 将启动。（它将在此进程结束后停止。）

警告：

当临时 CMS 正在运行时，请避免使用部署。

7 检查确认页面并按 Enter 键。

CCM 重新创建该节点，并将有关该节点的信息添加到本地计算机中。如果发生任何错误，请查看日志文件。

现在可以运行安装目录/sap_bobj/ccm.sh -start nodeName 以启动重新创建的节点。

10.12.3.2.1 使用脚本在 Unix 上重新创建节点

可以使用 addnode.sh 在 Unix 计算机上重新创建节点。有关更多信息，请参阅“用于添加、重新创建和删除节点的脚本参数”一节。

示例：

```
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
```

相关主题

- 第 382 页上的[“变量”](#)
- 第 399 页上的[“用于添加、重新创建和删除节点的脚本参数”](#)

10.12.4 删除节点

可以使用正在运行的中央配置管理器（CCM）或节点管理脚本删除停止工作的节点。使用以下指导原则：

- 删除节点会同时永久删除该节点上的服务器。
- 如果群集中有多台计算机，请先删除节点，然后再从群集中删除计算机并卸载其上的软件。如果在删除节点之前从群集中删除计算机，或者如果计算机上的文件系统出现故障，则必须在同一群集中的另一台计算机上使用相同的服务器重新创建该节点，然后再删除该节点。

记忆：

只能在节点所在的计算机上删除节点。

相关主题

- 第 388 页上的“[重新创建节点](#)”

10.12.4.1 删除 Windows 上的节点

警告：

在删除节点前后，备份整个群集的服务器配置。

- 1 运行中央配置管理器（CCM）。
- 2 在 CCM 中，停止要删除的节点。
- 3 选择该节点并单击工具栏上的“删除节点”。
- 4 出现提示后，输入 CMS 的主机名、端口号和管理员凭据。

CCM 将删除该节点以及节点上的所有服务器。

10.12.4.1.1 使用脚本在 Windows 上删除节点

警告：

在删除节点前后，备份整个群集的服务器配置。

可以使用 RemoveNode.bat 删除 Windows 计算机上的节点。有关更多信息，请参阅“用于添加、重新创建和删除节点的脚本参数”一节。

示例：

```
SCRIPTDIR\RemoveNode.bat -name mynode2
-cms mycms:6400
-username Administrator
-password Password1
```

相关主题

- 第 382 页上的[“变量”](#)
- 第 399 页上的[“用于添加、重新创建和删除节点的脚本参数”](#)

10.12.4.2 删除 Unix 上的节点

在删除节点前后，分别备份整个群集的服务器配置。

- 1 运行安装目录/sap_bobj/ccm.sh -stop nodeName 以停止要删除的节点。
- 2 运行安装目录/sap_bobj/serverconfig.sh
- 3 选择“2 - Delete node”，并按 Enter 键。
- 4 选择要删除的节点并按 Enter 键。
- 5 出现提示后，输入 CMS 的主机名、端口号和管理员凭据。

这将删除该节点以及节点上的所有服务器。

10.12.4.2.1 使用脚本在 Unix 上删除节点

警告：

在删除节点前后，备份整个群集的服务器配置。

可以使用 `removenode.sh` 删除 Unix 计算机上的节点。有关更多信息，请参阅“用于添加、重新创建和删除节点的脚本参数”一节。

示例：

```
SCRIPTDIR\removenode.sh -name mynode2
-cms mycms:6400
-username Administrator
-password Password1
```

相关主题

- 第 382 页上的[“变量”](#)
- 第 399 页上的[“用于添加、重新创建和删除节点的脚本参数”](#)

10.12.5 重命名节点

可以使用中央配置管理器（CCM）重命名节点。要重命名节点，必须使用新名称创建一个新节点，将服务器从原始节点克隆到新节点，然后删除原始节点。使用以下指导原则：

- 如果重命名含有节点的计算机，则无需重命名该节点。可以继续使用现有节点名称。
- 如果使用防火墙，请确保打开服务器智能代理（SIA）和中央管理服务器（CMS）的端口。

记忆：

只能在节点所在的计算机上重命名节点。

相关主题

- 第 384 页上的[“添加新节点”](#)
- 第 355 页上的[“克隆服务器”](#)
- 第 392 页上的[“删除节点”](#)

10.12.5.1 重命名 Windows 上的节点

警告：

在重命名节点前后，备份整个群集的服务器配置。

- 1 启动中央配置管理器（CCM）。
- 2 在中央配置管理器（CCM）的工具栏上，单击“添加节点”。
- 3 在“添加节点向导”中，输入新服务器智能代理（SIA）的节点名称和端口号、管理员凭据、系统数据库的数据库连接信息和凭据以及群集密钥。
- 4 选择“添加不包含服务器的节点”。
- 5 创建节点后，使用中央管理控制台的服务器管理页面将原始节点上的所有服务器克隆到新节点上。

注意：

确保克隆的服务器与旧节点上的服务器不存在端口冲突。

- 6 在 CCM 中，启动新节点。
- 7 在新节点运行五分钟后，使用 CCM 删除原始节点。

相关主题

- 第 384 页上的[“添加新节点”](#)
- 第 355 页上的[“克隆服务器”](#)
- 第 392 页上的[“删除节点”](#)

10.12.5.2 重命名 Unix 上的节点

警告：

在重命名节点前后，备份整个群集的服务器配置。

- 1 运行安装目录/sap_bobj/serverconfig.sh。
- 2 选择“1 - 添加节点”，并按 Enter 键。
- 3 键入新节点的名称，并按 Enter 键。
- 4 键入新 SIA 的端口号，并按 Enter 键。
- 5 出现提示后，输入管理员凭据、系统数据库的数据库连接信息和凭据以及群集密钥。
- 6 选择“no servers”并按 Enter 键。
- 7 创建节点后，使用中央管理控制台的“服务器管理”页面将原始节点上的所有服务器克隆到新节点上。

注意：

确保克隆的服务器与旧节点上的服务器不存在端口冲突。

- 8 运行安装目录/sap_bobj/ccm.sh -start nodeName 以启动新节点。
- 9 在新节点运行五分钟后，使用 serverconfig.sh 删除原始节点。

相关主题

- 第 384 页上的[“添加新节点”](#)
- 第 355 页上的[“克隆服务器”](#)
- 第 392 页上的[“删除节点”](#)

10.12.6 移动节点

可以使用中央配置管理器（CCM）或节点管理脚本将停止工作的节点从一个群集移到另一个群集。使用以下指导原则：

- 确保目标群集中不存在同名的节点。
- 确保源节点所在计算机上安装的所有服务器类型同时安装在目标群集中。
- 如果要向生产群集添加一台新计算机，但在完成测试之前不希望使用该计算机，则可以将 BI 平台安装在一台独立的计算机上并测试该计算机，然后再将该节点移到生产群集。
- 该计算机的 BI 平台版本和服务包级别必须与群集中的其他计算机保持一致。

记忆：

只能在节点所在的计算机上移动节点。

10.12.6.1 移动 Windows 上的现有节点

在此示例中，要移动的节点安装在源系统上。源系统计算机最初为独立安装，但现在它将添加到目标群集中。

警告：

在移动节点前后，备份整个群集的服务器配置。

- 1 在中央配置管理器（CCM）中停止该节点。
 - 2 右击该节点并选择“移动”。
 - 3 出现提示后，选择数据源名称并输入目标 CMS 的主机名、端口、数据库连接信息、管理员凭据以及群集密钥。
 - 4 选择一个 CMS。
 - 如果源部署正在运行，请选择“使用正在运行的现有 CMS”并单击“下一步”。
- 出现提示后，输入源系统的现有 CMS 和管理员凭据的主机名和端口号。

- 如果源部署已停止，请选择“启动新的临时 CMS”并单击“下一步”。

出现提示后，输入源系统的临时 CMS 的主机名和端口号、管理员凭据、数据源名称、源系统数据库的数据库凭据以及群集密钥。此时，临时 CMS 将启动。（它将在此进程结束后停止。）

警告：

当临时 CMS 正在运行时，请避免使用部署。

- 5 检查确认页面并单击“完成”。

CCM 将在目标群集上创建一个新节点，并使用源群集中的相同节点名称且包含相同的服务器。该节点的副本仍保留在源群集中。节点中服务器的配置模板不会移动。如果发生任何错误，请查看日志文件。

警告：

移动节点后，请不要使用源群集。

- 6 在 CCM 中，启动移动后的节点。

10.12.6.1.1 使用脚本在 Windows 上移动节点

警告：

在移动节点前后，备份整个群集的服务器配置。

可以使用 MoveNode.bat 移动 Windows 计算机上的节点。有关更多信息，请参阅“用于移动节点脚本参数”一节。

示例：

由于命令提示符的限制，必需使用插入符号（^）转义这些参数中的空格、等号（=）和分号（;），除非将文本包括在引号中。

```
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
```

注意：

要避免在长字符串中使用插入符号，可以将脚本的名称及其所有参数写入一个临时 response.bat 文件，然后在不使用任何参数的情况下运行 response.bat。

相关主题

- 第 382 页上的[“变量”](#)
- 第 402 页上的[“用于移动节点的脚本参数”](#)

10.12.6.2 移动 Unix 上的现有节点

在此示例中，要移动的节点安装在源系统上。源系统计算机最初为独立安装，但现在它将添加到目标群集中。

警告：

在移动节点前后，备份整个群集的服务器配置。

- 1 运行安装目录/sap_bobj/ccm.sh -stop nodeName 以停止该节点。
- 2 运行安装目录/sap_bobj/serverconfig.sh
- 3 选择“4 - Move node”，并按 Enter 键。
- 4 选择要移动的节点并按 Enter 键。
- 5 出现提示后，选择系统数据库连接信息并输入目标 CMS 的主机名、端口、管理员凭据以及群集密钥。
- 6 选择一个 CMS。
 - 如果源部署正在运行，请选择“现有”并按 Enter 键。
出现提示后，输入源系统的现有 CMS 和管理员凭据的主机名和端口号。
 - 如果源部署已停止，请选择“临时”并按 Enter 键。
出现提示后，输入源系统的临时 CMS 的主机名和端口、管理员凭据、源系统数据库的数据库连接信息和凭据以及群集密钥。此时，临时 CMS 将启动。（它将在此进程结束后停止。）

警告：

当临时 CMS 正在运行时，请避免使用部署。请确保现有 CMS 与临时 CMS 使用不同的端口。

- 7 检查确认页面并按 Enter 键。
CCM 将在目标群集上创建一个新节点，并使用源群集中的相同节点名称且包含相同的服务器。该节点的副本仍保留在源群集中。节点中服务器的配置模板不会移动。如果发生任何错误，请查看日志文件。

警告：

移动节点后，请不要使用源群集。

- 8 运行安装目录/sap_bobj/ccm.sh -start nodeName 以启动移动后的节点。

10.12.6.2.1 使用脚本在 Unix 上移动节点

警告：

在移动节点前后，备份整个群集的服务器配置。

可以使用 `movenode.sh` 移动 Unix 计算机上的节点。有关更多信息，请参阅“用于移动节点的脚本参数”一节。

示例：

```
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
```

相关主题

- 第 382 页上的“[变量](#)”
- 第 402 页上的“[用于移动节点的脚本参数](#)”

10.12.7 脚本参数

10.12.7.1 用于添加、重新创建和删除节点的脚本参数

参数	说明	示例
-adopt	如果节点在 CMS 中已存在，则重新创建该节点。	-adopt
-cms	<p>中央管理服务器（CMS）的名称和端口号。</p> <p>警告： 如果使用 -usetempcms，则不要使用此参数</p> <p>注意： 如果 CMS 不在默认的 6400 端口上运行，则必须指定端口号。</p>	-cms mycms:6409
-cmsport	<ul style="list-style-type: none"> 启动临时 CMS 时的 CMS 端口号。 <p>限制： 还必须使用 -usetempcms、-dbdriver、-connect 和 -dbkey 参数。</p> <ul style="list-style-type: none"> 创建新 CMS 时的 CMS 端口号。 <p>限制： 还必须使用 -dbdriver、-connect 和 -dbkey 参数。</p>	-cmsport
-connect	<p>CMS（或临时 CMS）系统数据库的连接字符串。</p> <p>注意： 在连接到 DB2、Oracle、SQL Anywhere、SQL Server 或 Sybase 数据库时可省略 HOSTNAME 和 PORT 属性。</p>	-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=password;HOSTNAME=database;PORT=3306"

参数	说明	示例
-dbdriver	<p>CMS 的数据库驱动程序。</p> <p>接受的值包括：</p> <ul style="list-style-type: none"> • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqldatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem • newdbdatabasesubsystem 	-dbdriver mysqldatabasesubsystem
-dbkey	群集密钥。	-dbkey abc1234
-name	节点的名称。	-name mynode2
-noservers	<p>创建不带有服务器的节点。</p> <p>注意： -createcms 附加参数将创建一个带有 CMS 但不含其他服务器的节点。省略这些参数将创建一个带有所有默认服务器的节点。</p>	-noservers
-password	管理员帐户的密码。	-password Password1
-siaport	节点的服务器智能代理的端口号。	-siaport 6409
-username	管理员帐户的用户名。	-username Administrator
-usetempcms	<p>警告： 如果使用 -cms，则不要使用此参数启动并使用临时 CMS。</p> <p>注意： 部署未运行时请使用临时 CMS。</p>	-usetempcms

相关主题

- 第 386 页上的“[使用脚本在 Windows 上添加节点](#)”
- 第 387 页上的“[使用脚本在 Unix 上添加节点](#)”
- 第 389 页上的“[使用脚本在 Windows 上重新创建节点](#)”
- 第 391 页上的“[使用脚本在 Unix 上重新创建节点](#)”
- 第 392 页上的“[使用脚本在 Windows 上删除节点](#)”
- 第 393 页上的“[使用脚本在 Unix 上删除节点](#)”

10.12.7.2 用于移动节点的脚本参数

参数	说明	示例
-cms	<p>源中央管理服务器（CMS）的名称。</p> <p>警告： 如果使用 -usetempcms，则不要使用此参数</p> <p>注意： 如果 CMS 不在默认的 6400 端口上运行，则必须指定端口号。</p>	-cms sourceMachine:6409
-cmsport	<ul style="list-style-type: none">启动临时 CMS 时的 CMS 端口号。 <p>限制： 还必须使用 -usetempcms、-dbdriver、-connect 和 -dbkey 参数。</p> <ul style="list-style-type: none">创建新 CMS 时的 CMS 端口号。 <p>限制： 还必须使用 -dbdriver、-connect 和 -dbkey 参数。</p>	-cmsport
-connect	<p>源 CMS（或临时 CMS）系统数据库的连接字符串。</p> <p>注意： 在连接到 DB2、Oracle、SQL Anywhere、SQL Server 或 Sybase 数据库时可省略 HOSTNAME 和 PORT 属性。</p>	-connect "DSN=Source BOEXI40;UID=username;PWD=password;HOSTNAME=database;PORT=3306"

参数	说明	示例
-dbdriver	源 CMS 的数据库驱动程序。 接受的值包括： <ul style="list-style-type: none"> • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqldatabasesubsystem • sqlserverdatabasesubsystem • sybasedatabasesubsystem • newdbdatabasesubsystem 	-dbdriver mysqldatabasesubsystem
-dbkey	源群集密钥。	-dbkey abc1234
-destcms	目标 CMS 的名称。 注意： 如果 CMS 不在默认的 6400 端口上运行，则必须指定端口号。	-destcms destinationMachine:6401
-destconnect	目标 CMS 系统数据库的连接字符串。 注意： 在连接到 DB2、Oracle、SQL Anywhere、SQL Server 或 Sybase 数据库时可省略 HOSTNAME 和 PORT 属性。	-destconnect "DSN=Destin BOEXI40;UID=username;PWD=password;HOSTNAME=database;PORT=3306"
-destdbdriver	目标 CMS 的数据库驱动程序。 接受的值包括： <ul style="list-style-type: none"> • db2databasesubsystem • maxdbdatabasesubsystem • mysqldatabasesubsystem • oracledatabasesubsystem • sqldatabasesubsystem • sybasedatabasesubsystem • newdbdatabasesubsystem 	-destdbdriver sybasedatabasesubsystem
-destdbkey	目标群集密钥。	-destdbkey def5678
-destpassword	目标 CMS 上管理员帐户的密码。	-destpassword Password2
-destusername	目标 CMS 上管理员帐户的用户名。	-destusername Administrator
-password	源 CMS 上管理员帐户的密码。	-password Password1

参数	说明	示例
-username	源 CMS 上管理员帐户的用户名。	-username Administrator
-usetempcms	<p>警告： 如果使用 -cms，则不要使用此参数启动并使用临时 CMS。</p> <p>注意： 部署未运行时请使用临时 CMS。</p>	-usetempcms

相关主题

- 第 397 页上的[“使用脚本在 Windows 上移动节点”](#)
- 第 399 页上的[“使用脚本在 Unix 上移动节点”](#)

10.12.8 添加 Windows 服务器依赖项

在 Windows 环境中，每个服务器智能代理（SIA）实例都依赖于事件日志和远程过程调用（RPC）服务。

如果 SIA 未能正确运行，请确保这两项服务均出现在 SIA 的“依赖项”选项卡上。

10.12.8.1 添加 Windows 服务器依赖项

- 1 使用中央配置管理器（CCM）停止服务器智能代理（SIA）。
- 2 右击 SIA 并选择“属性”。
- 3 单击“依赖项”选项卡。
- 4 单击“添加”。
将显示“添加依赖项”对话框，其中显示所有可用依赖项的列表。
- 5 选择一个依赖项并单击“添加”。
- 6 单击“确定”。
- 7 使用 CCM 重新启动 SIA。

10.12.9 更改节点的用户凭据

如果操作系统密码发生更改，或者如果希望使用不同用户帐户运行某个节点上的所有服务器，则可以使用中央配置管理器（CCM）指定或更新服务器智能代理（SIA）的用户凭据。

由 SIA 托管的所有服务器将在相同的帐户下运行。要使用非系统帐户运行服务器，请确保该帐户是服务器计算机上本地管理员组的成员，并具有“替换进程级标记”权限。

限制：

在 Unix 计算机上，必须使用安装时所使用的帐户运行 BI 平台。要使用其他帐户，必须使用其他帐户重新安装部署。

10.12.9.1 在 Windows 上更改节点的用户凭据

- 1 使用中央配置管理器（CCM）停止服务器智能代理（SIA）。
- 2 右击 SIA 并选择“属性”。
- 3 清除“系统帐户”复选框。
- 4 输入用户名和密码，然后单击“确定”。
- 5 使用 CCM 重新启动 SIA。

SIA 和服务器进程将使用新用户帐户登录本地计算机。

10.13 在 BI 平台部署中重命名计算机

10.13.1 更改群集名称

以下是重命名群集的最佳做法：

警告：

请勿使用相同的名称部署多个群集。

条件	操作
群集的名称已更改。	将新群集名称通知给用户，并要求他们使用该名称（在使用主机名:端口语法首次连接到 CMS 之后）。在 Web 层中，更新所有 Web 应用程序服务器的属性文件中的群集名称。
您在以前运行 CMS 的计算机上安装了另一不同的 BI 平台版本，或者您已将该计算机添加到另一不同的群集。	<ul style="list-style-type: none"> 请确保新 CMS 运行于不同的端口。 请针对不同的群集使用不同的密码，防止用户登录到错误的群集。

10.13.2 更改 IP 地址

为避免由于计算机 IP 地址更改导致配置更改，请在 CMC 的“服务器”选项卡中选择“服务器属性”，然后确保所有服务器均已绑定到主机名，或者使用“自动分配”选项。此外，还应遵循以下最佳做法：

条件	操作
您将 ODBC 与 CMS 数据库或审核数据库结合使用。	请确保 DSN 使用 CMS 数据库的服务器主机名。
您将另一数据库连接类型与 CMS 数据库或审核数据库结合使用。	使用 CCM 更新数据库，以使用该数据库的服务器主机名。
CMS 数据库或审核数据库位于 CMS 的同一主机中。	针对计算机名称使用 localhost。
您使用允许用户使用 Web 浏览器（如 CMC）的 BI 平台 Web 应用程序的 URL。	<p>请使用默认 URL 的主机名，而不是 IP 地址。要为默认查看器更新 URL，请为所选应用程序选择“处理设置”。</p> <p>例如，对于 OpenDocument，请在 CMC 中单击“应用程序”选项卡，右键单击“OpenDocument”，然后选择“处理设置”。</p>
您使用基于 Web 服务（例如：Crystal Reports for Java 或 LiveOffice）的 BI 平台客户端的 URL。	
您使用 OpenDocument。	

备选准则

注意：

仅当无法遵循上述最佳做法时才遵循以下准则。

表10-9：对于承载服务器的计算机

条件	操作
主机包含 BI 平台服务器，且该服务器绑定到特定的 IP 地址。	在 CMC 的“服务器”选项卡上更改 IP 地址，但是在计算机上的所有设置得到更新之前，请勿重新启动服务器。然后重新启动计算机；而非单个 BI 平台服务器。
数据库连接必须使用 IP 地址。	更改 IP 地址。
静态 IP 网络中需要更改 IP 地址。	更改 BI 平台计算机的 IP 地址。 提示： 登录到 CMC，验证 BI 平台是否正常运行。

记忆：

执行任一操作之后，重新启动计算机。

表10-10：对于承载 Web 应用程序服务器的计算机

条件	操作
OpenDocument 默认查看器的 URL 必须使用 IP 地址。	在 CMC “应用程序”选项卡的“处理设置”部分中，更新“设置默认查看器 URL”字段中的 IP 地址。
用户通过在浏览器中提供带 IP 地址的 URL 访问 BI 平台 Web 应用程序（如 CMC）。	将新 IP 地址通知给用户。
基于 Web 服务（例如：Crystal Reports for Java 或 LiveOffice）的 BI 平台客户端必须使用 IP 地址。	对所有客户端进行配置，使其使用新的 IP 地址。

相关主题

- 第 415 页上的[“选择新的或现有的 CMS 数据库”](#)

10.13.3 重命名计算机

通过停止计算机上的所有 BI 平台服务器并稍后重命名计算机，您可以随时重命名 BI 平台部署中的计算机。以下是重命名计算机的最佳做法：

条件	操作
第一次登录。	请使用 CMS 计算机名称（而不是群集名称）。
已部署多个计算机。	请确保所有其他计算机中的所有 CMS 服务器均在重命名期间运行。

10.13.3.1 服务器层

注意：

在重命名 CMS 计算机之前，请在 CMC 的“服务器管理”选项卡中检查位于要重命名的计算机中的所有服务器。如果“主机名”属性使用旧的 CMS 主机名，请将它更新为新的 CMS 主机名。

记忆：

在完成计算机的所有重命名过程之前，请勿重新启动服务器。

重命名服务器层的计算机时，请遵循以下说明：

条件	操作
重命名后的计算机将承载 CMS，且用户以前已通过提供旧计算机名称的方式登录过。	将 CMS 计算机的名称通知给用户，并要求他们使用该名称。
重命名后的计算机将承载 CMS，且 BI 平台的 Web 应用程序默认属性文件包含 cms.default 属性中的 CMS 旧主机名。	<p>在所有 Web 层计算机的所有自定义属性文件中，更新 cms.default 属性中的 CMS 计算机名称。在 Tomcat 中，创建的属性文件默认位于安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom 中。</p> <p>注意： 如果不存在自定义属性文件，请创建新的自定义属性文件。将默认的属性文件复制到自定义文件夹，并从自定义属性文件中删除 cms.default 行以外的所有内容。</p>

条件	操作
重命名后的计算机将承载 CMS，且群集的任何计算机均将安装 SAP BusinessObjects Explorer。	<p>使用承载 Web 应用程序服务器的所有计算机内 default.settings.properties 文件 default.cms.name 属性中的新主机名取代 CMS 旧主机名。在 Tomcat 中，default.settings.properties 文件默认位于安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\explorer\WEB-INF\classes\ 中</p> <p>记忆： 执行该操作之后，请重新启动资源管理器的 Web 应用程序或应用程序服务器。</p>
结合使用 SSO 和资源管理器	更新 jsp-sso-provider.jsp 中的 cms 值，并将 sso.properties 中的 sso.global.cms 和 sso.trusted.auth.x509.cms 值更新为 CMS 的新主机名。
您使用门户集成套件或自定义应用程序。	请将门户集成套件或自定义应用程序配置为使用 CMS 的新主机名。
<p>您的部署符合以下所有条件：</p> <ul style="list-style-type: none"> • 一个群集具有多个节点。 • 所有 CMS 服务器仅在已重命名的计算机上运行。 • 至少有一个节点未承载 CMS。 • 您至少已重命名一个节点中的一台计算机。 • IP 地址在重命名过程中已更改。 	请使用 CCM 在所有节点中（承载 CMS 的节点除外）执行“重新创建节点”工作流，稍后启动部署中的所有 BI 平台节点。有关更多信息，请参阅“管理节点”一章。

记忆：

执行操作之后，请重新启动 Web 应用程序或应用程序服务器。

相关主题

- 第 388 页上的[“重新创建节点”](#)

10.13.3.2 Web 层

如果重命名承载 BI 平台 Web 应用程序服务器的计算机，请遵循以下说明：

条件	操作
您已更改承载 BI 平台 Web 应用程序服务器的计算机名称，且默认 OpenDocument 查看器的 URL 使用 Web 应用程序服务器主机名。	登录到 CMC，并通过“应用程序” > “CMC” > “处理设置”更新默认查看器的 URL。
您已更改承载 BI 平台 Web 应用程序服务器的计算机名称，且您的用户通过可使用一个包含 Web 应用程序服务器主机名的 URL 访问 BI 平台 Web 应用程序。	要求用户使用一个包含新 Web 应用程序服务器主机名的 URL 访问 BI 平台 Web 应用程序。
您已更改承载 BI 平台 Web 应用程序服务器的计算机名称，且基于 Web 服务的 BI 平台客户端已在 URL 中使用 Web 应用程序服务器主机名。	重新配置所有基于 Web 服务的 BI 平台客户端，以使用新 Web 应用程序服务器主机名。

10.13.3.3 数据库

如果重命名承载 CMS 系统数据库或审核数据库的计算机，请遵循以下最佳做法：

条件	操作
您必须避免更新 IP 地址。	使用 CMS 数据库或数据源名称（DSN）中审核数据库的计算机名称。
CMS 数据库或审核数据库位于 CMS 的同一主机中。	在 DSN 中使用 localhost，避免在主机名出现更改时更新它。

CMS 系统数据库

条件	操作
您重命名承载 CMS 系统数据库的计算机，且您使用 ODBC。	将 CMS 数据库的 DSN 更新为新数据库的服务器主机名。
重命名承载 CMS 系统数据库的计算机，且使用非 ODBC 连接类型。	使用 CCM 在群集中的每个节点中将 CMS 数据库更新为新数据库的服务器主机名。

审核数据库

条件	操作
您重命名承载审核数据库的计算机，且您使用 ODBC。	将审核数据库的 DSN 更新为新数据库的服务器主机名。
重命名承载审核数据库的计算机，且使用非 ODBC 连接类型。	在 CMC 的“审核”选项卡中，将数据库的服务器计算机名称更新为新数据库的服务器主机名。

10.13.3.4 文件资源库服务器

如果重命名承载 FRS 文件存储的计算机，则必须在 CMC 的“服务器管理”页面中更新“输入文件资源库”和“输出文件资源库”服务器，并确保“文件存储目录”和“临时目录”属性使用新的文件存储路径，并稍后重新启动服务器。

10.14 结合使用 32 位和 64 位第三方库和 BI 平台

BI 平台服务器为 32 位和 64 位进程的组合。某些服务器会额外启动 32 位和 64 位进程。要结合使用第三方库（32 位，而不是 64 位）的正确版本和 BI 平台进程，则必须在承载 BI 平台的计算机中为每个版本设置单独的环境变量。然后必须设置附加的环境变量，该变量包含具有 32 位和 64 位版本的环境变量列表，其中以逗号为分隔符。由 BI 平台启动进程时，将选择相应的变量，具体取决于进程是 32 位还是 64 位。

- FIRST_ENV_VAR是指 64 位 BI 平台进程将使用的值。
- FIRST_ENV_VAR32是指 32 位进程将使用的值。
- SECOND_ENV_VAR是指 64 位进程将使用的值。
- SECOND_ENV_VAR32是指 32 位进程将使用的值。
- BOE_USE_32BIT_ENV_FOR=FIRST_ENV_VAR, SECOND_ENV_VAR

例如，如果已在 AIX 计算机上安装 BI 平台以及 32 位和 64 位 Oracle 客户端，并需要设置 LIBPATH 变量，则需设置以下变量：

- ORACLE_HOME=Oracle 客户端的 64 位版本
- ORACLE_HOME32=32 位版本
- LIBPATH=64 位版本

- LIBPATH32=32 位版本
- BOE_USE_32BIT_ENV_FOR=ORACLE_HOME, LIBPATH

注意：

在 Linux 和 Solaris 中，请勿使用 BOE_USE_32BIT_ENV_FOR=LD_LIBRARY_PATH 来分隔 32 位和 64 位路径。相反，应将 32 位和 64 位路径添加到 LD_LIBRARY_PATH。

10.15 管理服务器和节点占位符

10.15.1 查看服务器占位符

- 在 CMC 的“服务器”管理区域中，右击某个服务器并选择“占位符”。
“占位符”对话框将显示所选服务器所在的相同群集中的所有服务器的占位符。如果要更改某个占位符的值，请修改该节点的占位符。

相关主题

- 第 966 页上的“[服务器和节点占位符](#)”

10.15.2 查看和编辑节点的占位符

- 1 在中央管理控制台的“服务器”管理区域中，右击要更改其占位符的节点并选择“占位符”。
- 2 如果要编辑占位符的任何设置，请进行相应更改并单击“保存”以继续。

相关主题

- 第 966 页上的“[服务器和节点占位符](#)”

第 11 章 管理中央管理服务器（CMS）数据库

11.1 管理 CMS 系统数据库连接

举例来说，如果 CMS 系统数据库由于硬件或软件故障或者网络问题而不可用，CMS 将转入等待资源状态。如果 BI 平台部署具有多个 CMS，则来自其他服务器的后续请求将转发至群集中正常连接到系统数据库的任意 CMS。当 CMS 处于等待资源状态时，将会继续处理不需要访问数据库的任何当前请求，但需要访问 CMS 数据库的请求将失败。

默认情况下，处于等待资源状态的 CMS 将定期尝试按请求的系统数据库连接数属性中指定的数目重新建立连接。至少建立一个数据库连接后，CMS 会立即同步所有必要数据并进入运行中状态，然后恢复正常操作。

某些情况下，可能需要防止 CMS 自动重新建立与数据库的连接。例如，可能需要在重新建立数据库连接前验证数据库的完整性。为此，请在 CMS 服务器的“属性”页面上取消选中“自动重新连接到系统数据库”。

相关主题

- 第 370 页上的[“更改服务器的属性”](#)

11.1.1 选择 SQL Anywhere 作为 CMS 数据库

要将 SQL Anywhere 用作 CMS 数据库，必须执行以下步骤：

- 1 停止系统中的所有节点。
- 2 运行相应的应用程序：
 - 在 Unix 上，运行 `./cmsdbsetup.sh`。
 - 在 Windows 上，启动中央配置管理器（CCM）。

- 3 选择 SQL Anywhere 作为目标数据库，从默认 CMS 数据库中复制数据。有关更多信息，请参阅“将数据从一个 CMS 系统数据库复制到另一个系统数据库”的相关链接。
- 4 在多节点部署中，将每个节点（除复制数据库所在的节点以外）中的 CMS 数据源更新到新 SQL Anywhere 数据库。有关更多信息，请参阅“选择新的或现有的 CMS 数据库”的相关链接。
- 5 请确保该部署能够正常运行（例如，登录到 CMC 并查看报表）。

相关主题

- 第 419 页上的[“将数据从一个 CMS 系统数据库复制到另一个系统数据库”](#)
- 第 415 页上的[“选择新的或现有的 CMS 数据库”](#)

11.1.2 选择 SAP HANA 作为 CMS 数据库

要将 SAP HANA 用作 CMS 数据库，必须执行以下步骤。

- 1 使用默认的 CMS 数据库安装 BI 平台。
- 2 安装 SAP HANA 客户端。
- 3 创建 SAP HANA 连接。
 - 在 Unix 上，检查环境变量 ODBCINI。如果该变量存在并指向现有的 odbc.ini 文件，则将以下几行内容串添加到该文件：

```
[ODBC Data Sources]
NewDB=<New_DB_version>
```

```
[NewDB]
SERVERNODE=<HANA Server IP address>:<HANA server port #>
```

<New_DB_version> 表示 SAP HANA 版本，例如 NewDB 1.0；<HANA Server IP address> 表示 SAP HANA 服务器 IP 地址；<HANA server port #> 表示 SAP HANA 服务器端口号。

如果 ODBCINI 环境变量不存在，则在安装目录/sap_bobj/enterprise_xi40/ 目录中创建一个 odbc.ini 文件，将上述内容添加到此文件中，然后按如下步骤设置 ODBCINI 环境变量：

```
ODBCINI=INSTALLDIR/sap_bobj/enterprise_xi40/odbc.ini
```

- 在 Windows 上，创建 SAP HANA 的 ODBC 连接。

注意：

对于 ODBC 连接更改，确保运行 64 位的 ODBC 数据源管理器：“开始” > “控制面板” > “管理工具” > “数据源（ODBC）”。

- 4 请确保可以与 SAP HANA 服务器连接起来。
 - 在 Unix 上，可通过运行以下命令测试与 SAP HANA 服务器的连接。以下示例中的变量将引用 SAP HANA 安装：

```
INSTALLDIR/odbcereg SERVER:HDBINDEXSERVERPORT SYSTEMID NONADMINUSER NONADMINPASSWORD
```

- 在 Windows 上，可使用 ODBC 数据源管理器来测试 SAP HANA ODBC 连接。

- 5 在 Unix 上，请将 libodbcHDB.so 从 SAP HANA 安装目录复制到安装目录/sap_bobj/enterprise_xi40/平台
- 6 停止系统中的所有节点。
- 7 运行相应的应用程序：
 - 在 Unix 上，运行 `./cmsdbsetup.sh`。
 - 在 Windows 上，启动中央配置管理器（CCM）。
- 8 通过选择 SAP HANA 作为目标数据库，从默认 CMS 数据库中复制数据。有关更多信息，请参阅“将数据从一个 CMS 系统数据库复制到另一个系统数据库”的相关链接。
- 9 在多节点部署中，将每个节点（除复制数据库所在的节点以外）中的 CMS 数据源更新为新的 SAP HANA 数据库。有关更多信息，请参阅“选择新的或现有的 CMS 数据库”的相关链接。
- 10 请确保该部署能够正常运行（例如，登录到 CMC 并查看报表）。

相关主题

- 第 419 页上的[“将数据从一个 CMS 系统数据库复制到另一个系统数据库”](#)
- 第 415 页上的[“选择新的或现有的 CMS 数据库”](#)

11.2 选择新的或现有的 CMS 数据库

可以使用 CCM 或 `cmsdbsetup.sh` 为节点指定新的或现有的 CMS 系统数据库。通常，只有少数情况下才需要完成以下步骤：

- 如果已经更改了当前 CMS 系统数据库的密码，可以利用以下步骤来断开与当前数据库的连接，然后重新连接到该数据库。出现提示时，可以向 CMS 提供新密码。
- 如果想为 BI 平台选择并初始化一个空的数据库，可按照这些步骤选择新的数据源。
- 如果（使用标准的数据库管理工具和过程）从备份中恢复了 CMS 系统数据库，而恢复方法导致原来的数据库连接无效，则需要将 CMS 重新连接到恢复的数据库。（例如，如果将原来的 CMS 数据库恢复到新安装的数据库服务器，则可能会出现这种情况。）

注意：

- 如果使用 IBM DB2 作为 CMS 数据库，并将其从低于 9.5 Fix Pack 5 的版本升级到 9.5 Fix Pack 5 版或更新版本（9.5 系列），或者从低于 9.7 Fix Pack 1 的版本升级到 9.7 Fix Pack 1 版或更新版本（9.7 系列），则在下次重启 BI 平台节点或 CMS 时，CMS 会自动将 CMS 数据库模式更新为支持 HADR 兼容模式。

这一过程可能会耗时很长，其间 BI 平台系统将无法使用。为避免 CMS 数据库崩溃，请不要中断更新流程。强烈建议在执行此操作前备份 CMS 数据库。另外，请不要尝试与低于 9.5 Fix Pack 5（9.5 系列）或 9.7 Fix Pack 1（9.7 系列）的 IBM DB2 CMS 数据库一起使用 IBM HADR。

- 请勿配置 BI 平台安装以使用属于不同群集的 CMS 系统数据库，除非正在执行系统复制工作流。

如果 BI 平台安装和 CMS 数据库的版本和修补程序级别不同，或者安装路径或安装组件不同等等，系统都可能发生损坏。

为了防止系统损坏，请勿尝试通过将 BI 平台部署指向另一个 BI 平台系统的 CMS 数据库（特别是版本和修补程序级别不同的 CMS 数据库）的方式，将 BI 内容从一个系统迁移到另一个系统。

11.2.1 在 Windows 上选择新的或现有的 CMS 数据库

- 1 使用 CCM 来停止服务器智能代理（SIA）。
- 2 选择 SIA，然后单击“指定 CMS 数据源”按钮。
- 3 选择“更新数据源设置”，然后单击“确定”。
- 4 选择数据库驱动程序，然后单击“确定”。
- 5 下述步骤视选择的连接类型而定：
 - 如果选择了 ODBC，将出现 Windows 的“选择数据源”对话框。选择要用作 CMS 数据库的 ODBC 数据源，单击“确定”。（单击“新建”可配置新 DSN。）出现提示时，提供数据库凭据并单击“确定”。
 - 如果选择了本机驱动程序，将提示您输入数据库服务器名称、登录 ID 和密码。提供这些信息，然后单击“确定”。
- 6 指定群集密钥。
- 7 重新启动“服务器智能代理”。

11.2.2 在 Unix 上选择新的或现有的 CMS 数据库

使用 cmsdbsetup.sh 脚本。有关参考，请参阅“Unix 工具”一章。

- 1 运行 cmsdbsetup.sh 脚本（默认位于安装目录/sap_bobj/）。
- 2 选择“update”操作（第 6 个选项）。
- 3 出现提示时，提供新 CMS 数据库的数据库类型。
- 4 提供数据库信息（例如：主机名、用户名、密码和群集密钥）。
当 CMS 数据库已指向新位置后，将出现一条通知消息。
- 5 如果提示重新生成服务器智能代理（SIA），请提供管理员密码，以及所需的 CMS 通信端口号。

注意：

只有在指向空的 CMS 数据库时，才会提示输入此信息。

11.3 重新创建 CMS 系统数据库

此过程说明如何重新创建（重新初始化）当前 CMS 系统数据库。执行此任务会破坏数据库中已有的所有数据。此过程非常有用，例如，在一个用于设计和测试您自己的自定义 Web 应用程序的开发环境中安装了 BI 平台时。在每次需要清除系统的所有数据时，可以在开发环境中重新初始化 CMS 系统数据库。

警告：

通过执行此工作流程中概述的步骤，删除 CMS 数据库中的所有数据以及诸如报表和用户等对象。不要对生产部署执行这些步骤。

非常重要的一点是，要在重新初始化 CMS 系统数据库之前备份所有服务器配置设置。重新创建数据库时，将会清除服务器配置设置，因此必须要有备份以便恢复此信息。

重新创建系统数据库时，现有的许可密钥应会保留在数据库中。但是，如果需要重新输入许可密钥，请使用默认的管理员帐户登录 CMC。转到“授权”管理区域并在“许可密钥”选项卡上输入信息。

注意：

如果重新初始化 CMS 系统数据库，当前 CMS 系统数据库中的所有数据将损坏。请考虑在开始之前备份当前的数据库。如有必要，请联系数据库管理员。

相关主题

- 第 469 页上的“[备份服务器设置](#)”

11.3.1 在 Windows 上重新创建 CMS 系统数据库

- 1 使用 CCM 来停止服务器智能代理（SIA）。

注意：

对于此过程，无法在远程计算机上运行 CCM；它必须运行于至少带有一个有效节点的计算机上。此外，必须在该计算机上安装 CMS 二进制文件。

- 2 右击 SIA 并选择“属性”。
- 3 在“属性”对话框中，转到“配置”选项卡并单击“指定”。
- 4 在“CMS 数据库设置”对话框中，单击“重新创建当前数据源”。

注意：

在步骤 1 中运行 CCM 的计算机中的服务器和对象也将被重新创建。不过，并不是所有对象都会被重新创建，而只会创建关键的默认对象。例如，不会重新创建示例报表。

- 5 单击“确定”，在提示确认时，单击“是”。
- 6 为 CMS 系统数据库指定密码并单击“确定”。

注意：

确保设置新的管理员密码。默认情况下，管理员帐户没有密码。

CMS 系统数据库设置完成后，CCM 将发出通知。

- 7 单击“确定”。

将返回到 CCM。

- 8 重新启动服务器智能代理并启用服务。

在“服务器智能代理”启动时，它会启动 CMS。CMS 会将必需的系统数据写入新清空的数据源中。

- 9 如果部署中有多台计算机，将需要在其他计算机上重新创建节点。

11.3.2 在 Unix 上重新创建 CMS 系统数据库

使用 cmsdbsetup.sh 脚本。有关参考，请参阅《SAP BusinessObjects Business Intelligence 平台 管理员指南》中的“Unix 工具”一章。

- 1 运行 cmsdbsetup.sh（默认位于 安装目录/sap_bobj/）。
- 2 选择“reinitialize”选项（第 5 个选项），然后确认选择。
cmsdbsetup.sh 脚本将开始重新创建 CMS 系统数据库。
- 3 提供 CMS 系统数据库密码。
- 4 数据库创建过程完成后，退出 cmsdbsetup.sh 脚本。
- 5 提供数据库信息（例如：主机名、用户名和密码）。
当 CMS 数据库已指向新位置后，将出现一条通知消息。
- 6 如果提示重新生成服务器智能代理（SIA），请提供管理员密码，以及所需的 CMS 通信端口号。

注意：

只有在指向空的 CMS 数据库时，才会提示输入此信息。

- 7 在安装目录/sap_bobj/ 目录中，使用以下命令启动节点。

```
ccm.sh -start nodename
```

- 8 要启用服务，请使用以下命令：

```
ccm.sh -enable all -cms CMSNAME:PORT -username administrator -password password
```

注意：

由于刚刚重新创建 CMS 数据库，因此管理员密码为空白。

11.4 将数据从一个 CMS 系统数据库复制到另一个系统数据库

可以使用中央配置管理器（CCM）或 `cmsdbsetup.sh` 将系统数据从一个数据库服务器复制到另一个数据库服务器。例如，如果由于正在升级数据库或从一个数据库类型移动到另一个类型而希望用其他数据库替换该数据库，则可以在取消现有数据库之前将其内容复制到新的数据库中。

将新数据复制到目标数据库之前，将会初始化该数据库，因此将永久删除其中的任何现有内容（将永久破坏并重建所有 BI 平台表）。复制数据后，目标数据库作为 CMS 的当前数据库建立。

注意：

如果希望将用户、组、文件夹和报表从 BI 平台的先前主版本导入到当前主版本，请使用 SAP BusinessObjects Business Intelligence 平台升级管理工具。有关更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台升级指南》。

11.4.1 准备复制 CMS 系统数据库

在复制 CMS 系统数据库之前，通过禁用并进而停止所有服务器使源环境和目标环境处于脱机状态。备份源和目标 CMS 数据库，并备份所有输入文件资源库服务器和输出文件资源库服务器使用的根目录。如有必要，请联系数据库或网络管理员。

确保您有一个有权读取源数据库中所有数据的数据库用户帐户，以及一个有权在目标数据库中进行创建、删除和更新的数据库用户帐户。同时确保可以从要替换其数据库的 CMS 计算机连接到这两个数据库 — 通过数据库客户端软件或通过 ODBC，视配置而定。

如果将 CMS 数据库从其当前位置复制到不同的数据库服务器，则当前 CMS 数据库是源环境。其内容被复制到目标数据库，然后目标数据库作为当前 CMS 的活动数据库建立。如果要将默认的 CMS 数据库从现有的默认数据库移动到专用数据库服务器（如 Microsoft SQL Server、Informix、Oracle、DB2 或 Sybase），可按此过程操作。用管理帐户登录正在运行要移动其数据库的 CMS 的计算机。

注意：

- 当将数据从一个数据库复制到另一个数据库中时，目标数据库将在复制进新数据前进行初始化。也就是说，如果目标数据库不包含 BI 平台系统表，则创建这些表。如果目标数据库包含 BI 平台系统表，则会永久删除这些系统表并创建新的系统表，而源数据库中的数据将复制到新表中。数据库中的其他表不受影响。

- 如果在 Windows 上将 CMS 系统数据库复制到 MaxDB 目标数据库，则必须确保已将 MaxDB 客户端的路径添加到 PATH 环境变量中。例如 ;C:\Program Files\sdb\MAXDB1\pgm。

11.4.2 在 Windows 上复制 CMS 系统数据库

在复制 CMS 数据库的内容之前，请确保可以使用具有以下权限的帐户登录到目标数据库：添加或删除表，以及添加、删除或修改这些表中的数据。

- 1 打开中央配置管理器 (CCM)，并停止服务器智能代理 (SIA)。
- 2 右击 SIA 并选择“属性”。
- 3 单击“配置”选项卡，然后单击“指定”。
- 4 选择“复制”，然后单击“确定”。
- 5 选择源 CMS 数据库的数据库类型，然后指定其数据库信息（包括主机名、用户名和密码）。
- 6 选择目标 CMS 数据库的数据库类型，然后指定其数据库信息（包括主机名、用户名和密码）。
- 7 当 CMS 数据库完成复制时，单击“确定”。

11.4.3 在 Unix 上复制 CMS 系统数据库中的数据

在复制 CMS 数据库的内容之前，请确保可以使用具有以下权限的帐户登录到目标数据库：添加或删除表，以及添加、删除或修改这些表中的数据。

注意：

在 Unix 上，不能直接从使用 ODBC 连接到 CMS 数据库的源环境进行迁移。如果源 CMS 数据库使用 ODBC，必须首先将系统升级到一个受支持的本机驱动程序。

- 1 通过键入以下命令停止 CMS：
 - 。 /ccm.sh -stop 节点名称
- 2 运行 cmsdbsetup.sh（默认位于 安装目录/sap_bobj/）。
- 3 选择复制选项（第 4 个选项），然后确认选择。
- 4 选择源 CMS 数据库的数据库类型，然后指定其数据库信息（包括主机名、用户名和密码）。
- 5 选择目标 CMS 数据库的数据库类型，然后指定其数据库信息（包括主机名、用户名和密码）。
CMS 数据库将复制到目标数据库中。复制完成时将显示一则消息。

第 12 章 管理 Web 应用程序容器服务器 (WACS)

12.1 WACS

12.1.1 Web 应用程序容器服务器 (WACS)

Web 应用程序容器服务器 (WACS) 为承载多个 SAP BusinessObjects Business Intelligence 平台 Web 应用程序提供了一个平台。例如，可以在 WACS 上承载中央管理控制台 (CMC)。

WACS 通过以下方式简化系统管理：删除一些以前在配置应用程序服务器和部署 Web 应用程序时必须执行的工作流，以及提供一个简化一致的管理界面。

Web 应用程序将自动部署到 WACS。WACS 不支持 BI 平台或外部 Web 应用程序的手动部署或 WDeploy 部署。

12.1.1.1 是否需要 WACS

如果不希望使用 Java 应用程序服务器承载 SAP BusinessObjects Web 应用程序，则可以将其承载于 WACS 上。

如果计划使用受支持的 Java 应用程序服务器来部署 BI 平台 Web 应用程序，或者要在 UNIX 系统上安装 BI 平台，则不需要安装和使用 WACS。

12.1.1.2 使用 WACS 有哪些优点

使用 WACS 承载 CMC 具有许多优点：

- 安装、维护和配置 WACS 所需要做的工作最少。
- 所有承载的应用程序均预先部署在 WACS 上，因此不需要手动执行一些附加步骤。
- SAP 支持 WACS。
- WACS 不要求具备 Java 应用程序服务器管理和维护技能。
- WACS 提供了一个与 BI 平台服务器一致的管理界面。

12.1.1.3 常见任务

任务	说明	主题
如何才能提高承载于 WACS 上的 Web 应用程序或 Web 服务的性能。	可以通过将 WACS 安装在多台计算机上来提高 Web 应用程序或 Web 服务的性能。	<ul style="list-style-type: none"> • 第 424 页上的 “在部署中添加或删除附加的 WACS” • 第 426 页上的 “克隆 Web 应用程序容器服务器”
如何才能提高 Web 层的可用性？	在部署中创建附加的 WACS，这样，如果一台服务器上出现硬件或软件故障，则另一台服务器可以继续为请求提供服务。	第 424 页上的 “在部署中添加或删除附加的 WACS”
如何才能创建一个可以在其中轻松地配置错误的 CMC 进行恢复的环境？	创建另一个已停止的 WACS，使用此 WACS 定义配置模板。如果主 WACS 配置错误，则可以使用第二台 WACS，直到配置好第一台服务器，也可以将配置模板应用于第一台服务器。	第 424 页上的 “在部署中添加或删除附加的 WACS”
如何才能提高客户端与 WACS 之间的通信的安全性？	在 WACS 上配置 HTTPS。	<ul style="list-style-type: none"> • 第 429 页上的 “配置 HTTPS/SSL” • 第 455 页上的 “将 WACS 与防火墙结合使用”

任务	说明	主题
如何才能提高部署中 WACS 和其他 BI 平台服务器之间通信的安全性？	配置部署中的 WACS 与其他 BI 平台服务器之间的 SSL 通信。	<ul style="list-style-type: none"> 第 158 页上的 “针对 SSL 配置服务器” 第 455 页上的 “将 WACS 与防火墙结合使用”
是否可以将 WACS 与 HTTPS 以及反向代理结合使用？	如果创建了两台 WACS 并将这两台服务器配置为使用 HTTPS，则可以将 WACS 与 HTTPS 以及反向代理结合使用。使用第一台 WACS 在内部网络中进行通信，使用另一台 WACS 通过反向代理与外部网络进行通信。	第 455 页上的 “将 WACS 配置为支持 HTTPS 和反向代理”
如何使 WACS 适应我的 IT 环境？	可以在具有现有 Web 服务器、硬件负载均衡器、反向代理以及防火墙的 IT 环境中部署 WACS。	<ul style="list-style-type: none"> 第 453 页上的 “将 WACS 与其他 Web 服务器结合使用” 第 454 页上的 “将 WACS 与负载均衡器结合使用” 第 454 页上的 “将 WACS 与反向代理结合使用” 第 455 页上的 “将 WACS 与防火墙结合使用”
是否可以在包含负载均衡器的部署中使用 WACS？	可以在使用硬件负载均衡器的部署中使用 WACS。WACS 本身无法用作负载均衡器。	第 454 页上的 “将 WACS 与负载均衡器结合使用”
是否可以在包含反向代理的部署中使用 WACS？	可以在使用反向代理的部署中使用 WACS。WACS 本身无法用作反向代理。	第 454 页上的 “将 WACS 与反向代理结合使用”
如何对 WACS 服务器进行疑难解答？	如果需要确定 WACS 性能差的原因，可以查看日志文件和系统量度。	<ul style="list-style-type: none"> 第 457 页上的 “在 WACS 上配置跟踪” 第 457 页上的 “查看服务器量度值”

任务	说明	主题
使用某个特定端口时无法显示任何页面。问题出在哪里？	可能有很多原因会导致无法连接到 WACS。请检查： <ul style="list-style-type: none"> 为 WACS 指定的 HTTP、HTTP 代理以及 HTTPS 端口是否被其他应用程序占用。 是否为 WACS 分配了足够的内存。 WACS 是否能够处理足够的并发请求。 如有必要，请还原 WACS 的系统默认值。 	<ul style="list-style-type: none"> 第 458 页上的 “解决 HTTP 端口冲突” 第 459 页上的 “更改内存设置” 第 460 页上的 “更改并发请求数” 第 460 页上的 “还原系统默认值”
如何配置 WACS 上所承载的 Web 应用程序的属性？	为 Web 应用程序配置属性的过程具体取决于特定的属性和 Web 应用程序。有关更多信息，请参阅本章的“配置 Web 应用程序属性”部分。	第 456 页上的 “配置 Web 应用程序属性”
在哪里可以找到 WACS 属性列表？	本指南的服务器属性附录包含 WACS 属性列表。	第 912 页上的 “核心服务属性”

12.1.2 在部署中添加或删除附加的 WACS

通过向部署中添加附加的 WACS，可以获得许多优势：

- 从配置错误的服务器中恢复的速度更快。
- 服务器可用性更高。
- 负载平衡更佳。
- 总体性能更佳。

可以采用以下三种方式向部署中添加附加的 WACS：

- 在计算机上安装 WACS。
- 创建新的 WACS。
- 克隆 WACS。

注意：

建议在同一计算机上只同时运行一台 WACS，因为 WACS 会占用大量资源。但是，可以在同一计算机上部署多台 WACS 并只运行其中的一台，以便在某 WACS 配置错误的情况下帮助恢复。

12.1.2.1 安装 WACS

如果在单独的计算机上安装 WACS，则可以为部署提供更出色的性能、更佳的负载平衡以及更高的服务器可用性。如果所做的部署在单独的计算机上包含两台或更多台 WACS，则特定计算机上的硬件或软件故障将不会影响 Web 应用程序和 Web 服务的可用性，因为其他 WACS 将继续提供这些服务。

可以使用 BI 平台安装程序安装 Web 应用程序容器服务器。可采用以下两种方法安装 WACS：

在完整安装中，在“选择 Java Web 应用程序”屏幕上选择“安装 Web 应用程序容器服务器并自动部署 Web 应用程序和服务”。

如果在新安装中选择 Java 应用程序服务器，则不会安装 WACS。

在“自定义/扩展”安装中，可以在“选择功能”屏幕上通过展开“服务器” > “平台服务”并选择“Web 应用程序容器服务器”选择安装 WACS。

如果安装 WACS，则安装程序将自动创建一个名为 `NODE.WebApplicationContainerServer` 的服務器，其中 `NODE` 为节点的名称。然后在该服务器上部署 BI 平台 Web 应用程序和 Web 服务。部署或配置 CMC 时无需手动执行步骤。此时，系统将准备就绪，可供使用。

安装 WACS 时，安装程序将提示您为 WACS 提供一个 HTTP 端口号。请确保所指定的端口号未被使用。默认端口号为 6405。如果计划允许用户从防火墙外部连接到 WACS，则必须确保在防火墙上打开服务器的 HTTP 端口。

只有 Windows 操作系统支持 WACS。

注意：

安装 WACS 时，或者将更新或修复程序应用于 WACS 或 WACS 承载的 Web 应用程序时，将自动部署 WACS 承载的 Web 应用程序。部署 Web 应用程序需要花几分钟时间。在 Web 应用程序部署完成之前，WACS 将一直处于初始化中状态。在完全部署 Web 应用程序之前，用户将无法访问 WACS 上承载的 Web 应用程序。在初始部署完成之前，请不要停止服务器。可以通过中央配置管理器 (CCM) 查看 WACS 的服务器状态。

仅在安装 WACS 或对其应用更新后首次启动 WACS 时，才会发生此延迟。以后重新启动 WACS 时不会出现此延迟现象。

无法将 Web 应用程序手动部署到 WACS 服务器。不能使用 WDeploy 将 Web 应用程序部署到 WACS。

12.1.2.2 添加新的 Web 应用程序容器服务器

注意：

建议在同一计算机上只同时运行一台 WACS，因为 WACS 会占用大量资源。但是，可以在同一计算机上部署多台 WACS 并只运行其中的一台，以便在某 WACS 配置错误的情况下帮助恢复。

- 1 转到 CMC 的“服务器”管理区域。
- 2 选择“管理” > “新建” > “新建服务器”。
将显示“创建新服务器”屏幕。
- 3 从“服务类别”列表中，选择“核心服务”。
- 4 从“选择服务”列表中，选择希望 WACS 承载的服务并单击“下一步”。
 - 如果希望 WACS 承载 Web 应用程序（如 CMC、BI 启动板或 OpenDocument），请选择“BOE Web 应用程序服务”。
 - 如果希望 WACS 承载 Web 服务（如 Live Office 或作为 Web 服务的查询（QaaWS）），请选择“Web 服务 SDK 和 QaaWS 服务”。
 - 如果希望 WACS 承载 Business Process BI Web 服务，请选择“Business Process BI Web 服务”。
- 5 在接下来的“创建新服务器”屏幕上，选择希望 WACS 承载的任何其他服务，然后单击“下一步”。
- 6 在接下来的“创建服务器”屏幕上，选择要向其中添加服务器的节点，键入服务器名称和服务器说明，然后单击“创建”。

注意：

“节点”列表中只显示那些安装了 WACS 的节点。

- 7 在“服务器”屏幕上，双击新 WACS。
将显示“属性”屏幕。
 - 8 如果不想在重新启动系统时自动启动 WACS，则在“公共设置”面板中，确保取消选中“在服务器智能代理启动时自动启动此服务器”复选框。
 - 9 单击“保存并关闭”。
- 将创建新 WACS。将对服务器应用默认设置和属性。

12.1.2.3 克隆 Web 应用程序容器服务器

作为向部署中添加新 WACS 的一种替代方法，也可以向同一台计算机或另一台计算机克隆 WACS。虽然添加新 WACS 可采用默认设置创建服务器，但克隆 WACS 会将源 WACS 的设置应用于新 WACS。

服务器只能克隆到已安装了 WACS 的计算机上。

注意：

建议在同一计算机上只同时运行一台 WACS，因为 WACS 会占用大量资源。但是，可以在同一计算机上部署多台 WACS 并只运行其中的一台，以便在某 WACS 配置错误的情况下帮助恢复。

- 1 转到 CMC 的“服务器”管理区域。
- 2 选择想要克隆的 WACS，单击鼠标右键并选择“克隆服务器”。
“克隆服务器”屏幕将显示可向其克隆 WACS 的部署中节点的列表。克隆到节点列表中只显示那些安装了 WACS 的节点。
- 3 在“克隆服务器”屏幕上，键入新服务器名称，选择想要向其克隆服务器的节点，并单击“确定”。

将创建新 WACS。新服务器所包含的服务与从中克隆新服务器的服务器所包含的服务相同。新服务器及其承载的服务与从中克隆新服务器的服务器具有相同的设置，只有服务器名称例外。

注意：

如果向同一计算机克隆了 WACS，则可能会与用于克隆的 WACS 发生端口冲突。如果发生端口冲突，则必须更改新克隆的 WACS 实例上的端口号。

相关主题

- 第 458 页上的[“解决 HTTP 端口冲突”](#)

12.1.2.4 从部署中删除 WACS

只有当服务器目前没有为用户提供 CMC 服务时，才可以删除 WACS。如果要从部署中删除 WACS，则必须通过另一 WACS 或 Java 应用程序服务器登录至 CMC。无法删除当前正为用户提供 CMC 服务的 WACS。

- 1 转到 CMC 的“服务器”管理区域。
- 2 通过右击服务器并单击“停止服务器”，停止要删除的服务器。
- 3 右击该服务器并选择“删除”。
- 4 如果提示确认，请单击“确定”。

12.1.3 在 WACS 中添加或删除服务

12.1.3.1 向 WACS 添加 Web 应用程序或 Web 服务

向 WACS 添加其他 BI 平台 Web 应用程序或 Web 服务时，需要停止 WACS。因此，在停止 WACS 并向其他 WACS 添加服务时，至少还要有一个 CMC 承载于部署中的某台 WACS 上，以便提供 BOE Web 应用程序服务。

向 WACS 添加服务时，服务会在服务器重新启动时自动部署到 WACS。

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击要向其中添加服务的 WACS，并查看该服务器的属性，以确保要添加的服务尚未存在。
- 3 单击“取消”返回至“服务器”屏幕。
- 4 通过右击服务器并单击“停止服务器”来停止服务器。

如果尝试停止当前正为用户提供 CMC 服务的 WACS，则将出现一条警告消息。除非部署中的另一台 WACS 上至少还有一个 BOE Web 应用程序服务正在运行，否则请勿继续操作。如果存在，请单击“确定”，登录到另一台 WACS，并从头开始进行此过程。

- 5 右击服务器并选择“选择服务”。

将显示“选择服务”屏幕。

- 6 选择要向服务器添加的服务，通过单击“>”将该服务添加到服务器，然后单击“确定”。
- 7 通过右击服务器并单击“启动服务器”来启动 WACS。

服务即被添加到 WACS 中。将应用服务的默认设置及属性。

12.1.3.2 从 WACS 中删除 Web 应用程序或 Web 服务

要从 WACS 中删除 Web 应用程序或 Web 服务，必须登录到另一 WACS 或 Java 应用程序服务器上的 CMC。不能停止当前正为用户提供 CMC 服务的 WACS。

无法从 WACS 中删除最后一个服务。因此，如果要从 WACS 中删除 Web 服务，则必须确保该服务器正在承载另一服务。

如果要从 WACS 中删除最后一项服务，请删除 WACS 本身。

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击要从中删除 Web 服务的 WACS，并查看该服务器的属性，以确保要删除的 Web 服务已经存在。
- 3 单击“取消”返回至“服务器”屏幕。
- 4 通过右击服务器并单击“停止服务器”来停止 WACS。

如果尝试停止当前正为用户提供 CMC 服务的 WACS，则将出现一条警告消息。除非部署中的另一台 WACS 上至少还有一个 BOE Web 应用程序服务正在运行，否则请勿继续操作。如果存在，请单击“确定”，登录到另一台 WACS，并从头开始进行此过程。

- 5 右击 WACS 并选择“选择服务”。
将显示“选择服务”屏幕。
- 6 选择要删除的服务，单击“<”，然后单击“确定”。
- 7 通过右击服务器并单击“启动服务器”来启动 WACS。
服务即从 WACS 中删除。

12.1.4 配置 HTTPS/SSL

在 BI 平台部署中，可以为客户端与 WACS 之间的网络通信使用安全套接字层 (SSL) 协议和 HTTP。SSL/HTTPS 将对网络通信进行加密并具有更高的安全性。

有两种类型的 SSL：

- 在 BI 平台服务器之间使用的 SSL，其中包括部署中的 WACS 和其他 BI 平台服务器。这称为 CORBA SSL。有关在部署中的 BI 平台服务器之间使用 SSL 的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》中“使用防火墙”一章的“了解 SAP BusinessObjects Business Intelligence 平台组件之间的通信”一节。
- 安全 HTTP 协议 (HTTP over SSL)，存在于 WACS 与同其通信的客户端（例如浏览器）之间。

注意：

如果想在具有代理或反向代理的部署中部署 WACS，并且想要使用 SSL 来保护部署中的网络通信，则必须创建两个 WACS。有关更多信息，请参阅“将 WACS 与反向代理结合使用”。

要在 WACS 上配置 HTTPS/SSL，必须完成以下步骤：

生成或获得一个包含证书和私钥的 PKCS12 证书存储或 JKS 密钥存储。可以使用 Microsoft 的 Internet 信息服务 (IIS) 和 Microsoft 管理控制台 (MMC) 生成一个 PKCS12 文件，或者使用 openssl 或 Java Keytool 命令行工具生成一个密钥存储文件。

如果只想让某些客户端连接至 WACS，则必须生成一个证书信任列表文件。

如果具有证书存储和证书信任列表文件（如果需要），请将文件复制到 WACS 计算机上。

在 WACS 上配置 HTTPS。

相关主题

- 第 167 页上的[“了解 BI 平台组件间的通信”](#)
- 第 454 页上的[“将 WACS 与反向代理结合使用”](#)

12.1.4.1 生成 PKCS12 证书文件存储

生成 PKCS12 证书文件存储或 Java 密钥存储的方法以及可以使用的工具有很多。所使用的方法取决于用户可以获得并熟悉的工具。

此示例演示对于 Windows Server 2008，如何使用 Microsoft 的 Internet 信息服务 (IIS) 以及 Microsoft 管理控制台 (MMC) 生成 PKCS2008 文件。

- 1 以管理员身份登录到承载 WACS 的计算机。
 - 2 在 IIS 中，请求证书颁发机构颁发证书。有关请求颁发证书的信息，请参阅 IIS 帮助文档。
 - 3 通过以下方式启动 MMC：依次单击“开始” > “运行”，键入 mmc.exe，然后单击“确定”。
 - 4 将证书管理单元添加到 MMC：
 - a 从“文件”菜单中单击“添加/删除管理单元”。将出现“添加或删除管理单元”屏幕。
 - b 从“可用管理单元”列表中，选择“证书”，然后单击“添加”。
 - c 选择“计算机帐户”，然后单击“下一步”。
 - d 选择“本地计算机”，然后单击“完成”。
 - e 单击“确定”。证书管理单元将添加到 MMC 中。
 - 5 在 MMC 中，展开“证书”，选择想要使用的证书。
 - 6 在“操作”菜单上，依次选择“所有任务” > “导出”。将启动“证书导出向导”。
 - 7 单击“下一步”。
 - 8 选择“是，导出私钥”，然后单击“下一步”。
 - 9 选择“个人信息交换 - PKCS #12(.PFX)”，然后单击“下一步”。
 - 10 输入创建证书时使用的密码，然后单击“下一步”。为 WACS 配置 HTTPS 时必须在“私钥访问密码”字段中指定此密码。
- 将创建 PKCS12 证书文件存储。

12.1.4.2 生成证书信任列表

- 1 以管理员身份登录到承载 WACS 的计算机。

- 2 启动 Microsoft 管理控制台 (MMC)。
- 3 添加 Internet 信息服务管理单元：
 - a 从“文件”菜单中选择“添加/删除管理单元”。
 - b 在“可用管理单元”列表中，选择“Internet 信息服务 (IIS) 管理器”，然后单击“添加”。
 - c 单击“确定”。
 IIS 管理单元将添加到 MMC 中。
- 4 按照下述步骤创建证书信任列表：<http://www.iis.net/learn/install/installing-iis-7/compatibility-and-feature-requirements-for-windows-vista#NoWizard>。

12.1.4.3 配置 HTTPS/SSL

在 WACS 上配置 HTTPS/SSL 之前，请确保已经创建了一个 PKCS12 文件或 JKS 密钥存储，并且已经将该文件复制或移动到承载 WACS 的计算机中。

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击要为其启用 HTTPS 的 WACS 服务器。
将显示“属性”屏幕。
- 3 在“HTTPS 配置”部分中，选中“启用 HTTPS”复选框。
- 4 在“绑定到主机名或 IP 地址”字段中，指定已为其发放证书并且要向其绑定 WACS 的 IP 地址。
HTTPS 服务将通过指定的 IP 地址予以提供。
- 5 在“HTTPS 端口”字段中，指定端口号以便让 WACS 提供 HTTPS 服务。必须确保此端口为空闲端口。如果计划让用户从防火墙外部连接到 WACS，则还必须确保在防火墙上打开此端口。
- 6 如果要配置 SSL 及反向代理，请在“代理主机名”和“代理端口”字段中指定代理服务器的主机名和端口。
- 7 在“协议”列表上选择协议。可用选项如下：
 - SSL
SSL 是安全套接字层协议，用于对网络通信进行加密。
 - TLS
TLS 是传输层安全性协议，这是一种较新的增强型协议。SSL 与 TLS 之间的差异较小，但 TLS 中的加密算法的功能更强大。
- 8 在“证书存储类型”字段中，指定证书的文件类型。可用选项如下：
 - PKCS12
如果觉得 Microsoft 工具用起来更加轻松，请选择 PKCS12。
 - JKS

如果觉得 Java 工具用起来更加轻松，请选择 JKS。

9. 在“证书存储文件位置”字段中，指定从中复制或移动证书文件存储或 Java 密钥存储文件的路径。
 10. 在“私钥访问密码”字段中，指定密码。
PKCS12 证书存储和 JKS 密钥存储具有受密码保护的私钥，用于防止未经授权的访问。必须指定用于访问私钥的密码，以便 WACS 能够访问私钥。
 11. 建议使用符合以下任一条件的证书文件存储或密钥存储：包含一个证书，或者想要使用的证书列在首位。但是，如果要使用包含多个证书的证书文件存储或密钥存储，并且该证书不是文件存储中的第一个证书，则必须在“证书别名”字段中指定证书的别名。
 12. 如果想让 WACS 只接受某些客户端的 HTTPS 请求，请启用客户端身份验证。
客户端身份验证不会对用户进行身份验证。客户端身份验证可以确保 WACS 只向某些客户端的 HTTPS 请求提供服务。
 - a. 选中“启用客户端身份验证”。
 - b. 在“证书信任列表文件位置”中，指定包含信任列表文件的 PKCS12 文件或 JKS 密钥存储的位置。

注意：
证书信任列表类型必须与证书存储类型相同。

 - c. 在“证书信任列表私钥访问密码”字段中，键入用于保护对证书信任列表文件中私钥的访问的密码。
- 注意：**
如果启用客户端身份验证，并且浏览器或 Web 服务使用者未通过身份验证，则将拒绝 HTTPS 连接。
13. 单击“保存并关闭”。
14. 转到“量度”屏幕，确保 HTTPS 连接器出现在“运行中的 WACS 连接器”列表中。如果未出现 HTTPS，则确保 HTTPS 连接器配置正确。

12.1.5 受支持身份验证方法

WACS 支持以下身份验证方法：

- Enterprise
- LDAP
- AD Kerberos

WACS 不支持以下身份验证方法：

- NT
- AD NTLM
- LDAP 单一登录

12.1.6 为 WACS 配置 AD Kerberos

要为 WACS 配置 AD Kerberos 身份验证，首先必须将计算机配置为支持 AD。必须执行以下步骤。

- 启用 Windows AD 安全插件。
- 映射用户和组。
- 建立服务帐户。
- 设置约束委派。
- 在 Windows AD 插件中对 WACS 启用 Kerberos 身份验证。
- 创建配置文件。

将承载 WACS 的计算机设置为使用 AD Kerberos 身份验证后，必须通过中央管理控制台 (CMC) 执行附加配置步骤。

如果要为 Web 服务 SDK 和 QaaWS 配置 AD Kerberos 单一登录，则还必须配置 WACS 以及承载 WACS 的计算机。

相关主题

- 第 246 页上的[“Windows AD 安全插件”](#)
- 第 247 页上的[“映射 AD 用户和组 ”](#)
- 第 245 页上的[“为使用 Kerberos 的 AD 身份验证设置服务帐户”](#)
- 第 251 页上的[“在 BI 平台服务账号下运行 SIA”](#)
- 第 433 页上的[“在 Windows AD 插件中对 WACS 启用 Kerberos 身份验证”](#)
- 第 435 页上的[“创建配置文件”](#)
- 第 437 页上的[“针对 AD Kerberos 配置 WACS”](#)
- 第 440 页上的[“配置 AD Kerberos 单一登录 ”](#)

12.1.6.1 在 Windows AD 插件中对 WACS 启用 Kerberos 身份验证

为了支持 Kerberos，必须在 CMC 中配置 Windows AD 安全插件才能使用 Kerberos 身份验证。这包括：

- 确保启用了 Windows AD 身份验证。
- 输入 AD 管理员帐户。

注意：

此帐户只需要对 Active Directory 的读权限；不需要任何其他权限。

- 启用 Kerberos 身份验证和单一登录（如果需要单一登录）。
- 输入服务帐户的服务主体名称（SPN）。

12.1.6.1.1 先决条件

在为 Kerberos 配置 Windows AD 安全插件之前，必须已完成了以下任务：

- 第 245 页上的 [“为使用 Kerberos 的 AD 身份验证设置服务帐户”](#)
- 第 251 页上的 [“在 BI 平台服务账号下运行 SIA”](#)
- 第 247 页上的 [“映射 AD 用户和组”](#)

12.1.6.1.2 为 Kerberos 配置 Windows AD 安全插件

- 1 转到 CMC 的“身份验证”管理区域。
- 2 双击“Windows AD”。
- 3 确保已选中“启用 Windows Active Directory (AD)”复选框。
- 4 在“身份验证选项”下，选择“使用 Kerberos 身份验证”。
- 5 如果要配置对数据库的单一登录，请选中“高速缓存安全上下文（对于数据库的 SS0 为必需）”复选框。
- 6 在“服务主体名称”字段中，输入服务帐户的帐户和域，或到服务帐户的 SPN 映射。

使用以下格式，其中 svcacct 是之前创建的服务帐户的名称或 SPN，DNS.COM 是采用大写形式的完全限定的域。例如，服务帐户将为 svcacct@DNS.COM，SPN 将为 BOBJCentralMS/some_name@DOMAIN.COM。

注意：

如果计划允许其他域（而非默认域）中的用户登录，则必须提供之前映射的 SPN。

服务帐户区分大小写。在此输入的帐户的大小写必须与在 Active Directory 域中设置的内容的大小写匹配。

它必须与用于运行 BI 平台服务器的帐户或映射到此帐户的 SPN 相同。

- 7 如果要配置单一登录，请选中“为选定身份验证模式启用单一登录”。

注意：

如果选择了启用单一登录，将需要配置 WACS。

相关主题

- 第 440 页上的[“配置 AD Kerberos 单一登录”](#)

12.1.6.2 创建配置文件

在应用程序服务器上配置 Kerberos 的常规过程包括以下步骤：

- 创建 Kerberos 配置文件。
- 创建 JAAS 登录配置文件。

注意：

- 默认的 Active Directory 域必须采用大写 DNS 格式。
- 不需要下载和安装适用于 Windows 的 MIT Kerberos。也不再需要服务帐户密钥表。

12.1.6.2.1 创建 Kerberos 配置文件

要创建 Kerberos 配置文件，请执行以下步骤。

- 1 创建文件 krb5.ini（如果该文件不存在），并将其存储在 Windows 的 C:\Windows 下。

注意：

可以将此文件存储在其他位置。但是，如果这样做，则需要要在 CMC 中 WACS 服务器“属性”页面上的“Krb5.ini 文件位置”字段中指定此文件的位置。

- 2 在 Kerberos 配置文件中添加以下所需信息：

```
[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 =
}
```

注意：

- DNS.COM 是域的 DNS 名称，必须采用 FQDN 格式以大写形式输入。
- kdc 是域控制器的主机名。
- 如果用户从多个域中登录，则可以将多个域条目添加到 [realms] 部分中。要查看具有多个域条目的此文件的示例，请参阅 第 436 页上的 [“Krb5.ini 文件示例”](#)。
- 在多域配置中，[libdefaults] 下的 default_realm 值可以是任何所需的域。最好使用将用 AD 帐户进行身份验证的用户数量最多的域。

12.1.6.2.2 创建 JAAS 登录配置文件

- 1 创建一个名为 bscLogin.conf 的文件（如果该文件不存在），并将其存储在默认位置：C:\Windows。

注意：

可以将此文件存储在其他位置。但是，如果这样做，则需要在 CMC 中 WACS 服务器“属性”页面上的“bscLogin.conf 文件位置”字段中指定此文件的位置。

- 2 将以下代码添加到 JAAS bscLogin.conf 配置文件中：

```
com.businessobjects.security.jgss.initiate {
    com.sun.security.auth.module.Krb5LoginModule required;
};
```

- 3 保存并关闭文件。

12.1.6.2.3 Krb5.ini 文件示例

多域 Krb5.ini 文件示例

以下是具有多个域的示例文件：

```
[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
}
```

单域 Krb5.ini 文件示例

以下是具有单个域的 krb5.ini 文件示例。

```
[libdefaults]
default_realm = ABCD.MFROOT.ORG
dns_lookup_kdc = true
dns_lookup_realm = true
[realms]
ABCD.MFROOT.ORG = {
    kdc = ABCDIR20.ABCD.MFROOT.ORG
    kdc = ABCDIR21.ABCD.MFROOT.ORG
    kdc = ABCDIR22.ABCD.MFROOT.ORG
    kdc = ABCDIR23.ABCD.MFROOT.ORG
    default_domain = ABCD.MFROOT.ORG
}
```

12.1.6.3 针对 AD Kerberos 配置 WACS

在针对 AD Kerberos 身份验证而配置了承载 WACS 的计算机后，必须通过中央管理控制台 (CMC) 配置 WACS 本身。

12.1.6.3.1 为 AD Kerberos 配置 WACS

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击要为其配置 AD 的 WACS。
将显示“属性”屏幕。
- 3 在“Krb5.ini 文件位置”字段中，指定 krb5.ini 配置文件的路径。
- 4 在“bscLogin.conf 文件位置”字段中，指定 bscLogin.conf 配置文件的路径。
- 5 单击“保存并关闭”。
- 6 重新启动 WACS。

12.1.6.4 Kerberos 疑难解答

如果在配置 Kerberos 时遇到问题，以下步骤可能有用：

- 启用日志记录
- 测试 Kerberos 配置

12.1.6.4.1 启用 Kerberos 日志记录

- 1 启动中央配置管理器 (CCM)，然后单击“管理服务器”。

- 2 指定登录凭据。
- 3 在“管理服务器”屏幕上，停止 WACS。
- 4 单击“Web 层配置”。

注意：

“Web 层配置”图标仅在选择停止的 WACS 时才处于启用状态。

将显示“Web 层配置”屏幕。

- 5 在“命令行参数”下，将以下文本复制到参数末尾：

```
-Dcrystal.enterprise.trace.configuration=verbose  
-Djcsi.Kerberos.debug=true
```

- 6 单击“确定”。
- 7 在“管理服务器”屏幕上，启动 WACS。

12.1.6.4.2 测试 Kerberos 配置

- 运行以下命令测试 Kerberos 配置，其中 servact 是服务帐户和在其中运行 CMS 的域，password 是与服务帐户关联的密码。

```
INSTALLDIR\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM Password
```

例如：

```
C:\Program Files\Business Objects\javasdk\bin\kinit.exe servact@TESTM03.COM Password
```

如果仍有问题，请确保为域和服务主体名称输入的内容的大小写与 Active Directory 中设置的内容的大小完全匹配。

12.1.6.4.3 映射的 AD 用户无法登录到 WACS 上的 BI 平台

尽管事实上已将用户已映射到 BI 平台，但是仍可能会出现以下两个问题。

12.1.6.4.3.1 由于 AD UPN 和 SAM 名称不同而导致的登录失败

用户的 Active Directory ID 已成功映射到 BI 平台。尽管如此，用户仍然无法使用 AD 身份验证和以下格式的 Kerberos 成功登录到 CMC: DOMAIN\ABC123

如果在 Active Directory 中设置的用户的 UPN 和 SAM 名称在大小写或其他方面不相同，则可能会发生此问题。下面是两个可能会导致问题的示例：

- UPN 为 abc123@company.com，但 SAM 名称为 DOMAIN\ABC123。
- UPN 为 jsmith@company，但 SAM 名称为 DOMAIN\johnsmith。

可通过两种方式解决此问题：

- 让用户使用 UPN 名称（而不是 SAM 名称）登录。
- 确保 SAM 帐户名和 UPN 名称相同。

12.1.6.4.3.2 预身份验证错误

以前能够登录的用户无法再成功登录。该用户将收到以下错误消息：无法识别帐户信息。WACS 日志将显示以下错误：“Pre-authentication information was invalid (24)”（预身份验证信息无效 (24)）

由于 Kerberos 用户数据库未对 AD 中的 UPN 进行更改，因此可能出现此问题。这可能表示 Kerberos 用户数据库和 AD 信息不同步。

要解决此问题，请重置 AD 中的用户密码。这样将确保正确地传播更改的信息。

12.1.7 配置 AD Kerberos 单一登录

如果要为 BI 启动板或 Web 服务 SDK 和 QaaWS 配置 AD Kerberos 单一登录，必须确保已经为 WACS 和承载 WACS 的计算机配置了 AD Kerberos 身份验证。

要配置 WACS 的 AD Kerberos 单一登录，必须首先配置承载 WACS 的计算机，然后才能配置 WACS。

注意：

如果计划在反向代理环境中使用单一登录，请阅读本指南中的安全信息。

相关主题

- 第 139 页上的[“安全概述 ”](#)
- 第 433 页上的[“为 WACS 配置 AD Kerberos ”](#)
- 第 441 页上的[“为计算机配置 AD Kerberos 单一登录 ”](#)
- 第 442 页上的[“为 AD Kerberos 单一登录配置 WACS”](#)

12.1.7.1 为计算机配置 AD Kerberos 单一登录

要配置对 Web 服务 SDK 和 QaaWS 的 AD Kerberos 单一登录，必须首先配置承载 WACS 的计算机：

- 第 266 页上的[“为 Vintela SSO 配置约束委派”](#)
- 第 265 页上的[“为 Vintela SSO 设置服务帐户”](#)
- 第 441 页上的[“设置多个 SPN”](#)
- 第 441 页上的[“增加 WACS 的标头大小限制”](#)

以下各节描述如何完成以上每个步骤。

12.1.7.1.1 设置多个 SPN

不支持使用多个 SPN。

12.1.7.1.2 增加 WACS 的标头大小限制

Active Directory 会创建将在身份验证过程中使用的 Kerberos 标记。此标记存储在 HTTP 标头中。WACS 将有一个默认的 HTTP 标头大小，它对于大多数用户而言已足够。可以配置此标头大小。

- 1 转到 CMC 的服务器管理区域。
- 2 双击要更改其 HTTP 标头大小的 WACS。
将显示属性屏幕。
- 3 在HTTP 配置、通过代理的 HTTP 的配置或HTTPS 配置区域的“最大 HTTP 标头大小（字节）”字段中指定一个值。
- 4 单击“保存并关闭”。
- 5 重新启动服务器。

12.1.7.2 为 AD Kerberos 单一登录配置 WACS

可以将 Web 应用程序容器服务器配置为使用 AD Kerberos 单一登录。支持 AD Kerberos 单一登录。不支持 AD NTLM。

在配置 WACS 之前，必须将承载 WACS 的计算机配置为 AD Kerberos 单一登录。

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击要配置的 WACS。
将显示“属性”屏幕。
- 3 选中“启用 Kerberos Active Directory 单一登录”。
- 4 指定“默认 AD 域”、“服务主要名称”的值和“Keytab 文件”选项的属性，然后单击“保存并关闭”。
- 5 重新启动 WACS。
活动目录单一登录准备就绪。

12.1.7.3 配置 Kerberos 和对数据库的单一登录

满足所有以下要求的部署支持数据库单一登录：

- 在 WACS 上部署 BI 平台。
- 已将 WACS 配置为与 AD 和 Kerberos 一起使用。
- 要求单一登录的数据库是 SQL Server 或 Oracle 的支持版本。

- 必须已在 SQL Server 或 Oracle 内为需要访问该数据库的组或用户授予权限。
- CMC 的“AD 身份验证”页中的“高速缓存安全上下文”（单一登录到数据库所必需的上下文）复选框处于选中状态。

最后一步是修改 krb5.ini 文件以支持数据库的单一登录。

注意：

这些说明介绍如何配置数据库单一登录。如果要配置端到端数据库单一登录，则还必须进行 Vintela 单一登录所需的配置步骤。有关详细信息，请参阅第 440 页上的 [“配置 AD Kerberos 单一登录”](#)。

12.1.7.3.1 启用对数据库的单一登录

- 1 打开用于部署 BI 平台的 krb5.ini 文件。
此文件的默认位置为 Web 应用程序服务器中的 C:\Windows 目录。
- 2 转到该文件的 [libdefaults] 部分。
- 3 在文件的 [realms] 部分的开头位置前输入以下字符串：

```
forwardable = true
```

- 4 保存并关闭文件。
- 5 重新启动 WACS。

12.1.8 配置 RESTful Web 服务

Business Intelligence 平台 RESTful Web 服务 SDK 允许用户使用 HTTP 协议访问 BI 平台。这样，用户便可以使用支持 HTTP 请求的任何编程语言导航 BI 平台资源库和计划对象。RESTful Web 服务是作为 WACS 的一部分安装的。

本节将说明如何管理 RESTful Web 服务。有关 RESTful Web 服务的更多信息，请参阅《Business Intelligence Platform RESTful Web Service Developer Guide》（Business Intelligence 平台 RESTful Web 服务开发人员指南）。

12.1.8.1 应用程序

12.1.8.1.1 配置 RESTful Web 服务的基本 URL

如果 BI 平台部署使用代理服务器或包含了多个 Web 应用程序容器服务器 (WACS) 的实例，则可能需要配置 RESTful Web 服务使用的基本 URL。配置基本 URL 前，必须先了解侦听 RESTful Web 服务请求的服务器的名称和端口号。

基本 URL 会作为每个 RESTful Web 服务请求的一部分使用。开发人员可以通过编程方式发现基本 URL，并借此将 RESTful Web 服务请求定向到正确的服务器和端口。RESTful Web 服务响应中也会使用基本 URL 来定义指向其他 RESTful 资源的超级链接。

注意：

在 BI 平台的默认安装中，基本 URL 为 `http://<servername>:6405/biprws`。请将 `<servername>` 替换为承载 RESTful Web 服务的服务器的名称。

- 1 以管理员身份登录到中央管理控制台 (CMC)。
- 2 在 CMC 中，单击“应用程序”。
此时将显示应用程序列表。
- 3 右键单击“RESTful Web 服务” > “属性”。
此时将出现“属性”对话框。
- 4 在“访问 URL”文本框中，输入 RESTful Web 服务基本 URL 的名称。
例如，输入 `http://<servername>:<portnumber>/biprws`。请将 `<servername>` 和 `<portnumber>` 替换为侦听 RESTful Web 服务请求的服务器名称和端口号。
- 5 单击“保存并关闭”。

12.1.8.2 WACS 属性

12.1.8.2.1 配置方法和表头命令行参数

作为管理员，用户可以限制 RESTful Web 服务使用哪些方法和表头，方法是将合适的选项添加到 Web 应用程序容器服务 (WACS) 的“命令行参数”中。更改参数后需要重新启动 WACS 服务。

- 1 以管理员用户身份登录到中央管理控制台。
 - 2 单击“服务器”，然后单击“服务器列表”。
 - 3 在 Web 应用程序容器服务器 (WACS) 上单击鼠标右键（例如 MySIA.WebApplicationContainerServer），然后单击“属性”。
- 此时，将出现 WACS 服务器的“属性”选项卡。
- 4 在“命令行参数”区域，输入允许的方法和表头。
- 每个选项组均由双引号引起。使用的方法不包括 GET、HEAD 和 POST。使用逗号将选项值隔开，如在以下示例中显示的 PUT 和 DELETE。

```
"-Dcom.sap.bip.rs.cors.extra.methods= PUT, DELETE"  
"-Dcom.sap.bip.rs.cors.extra.headers= X-SAP-LogonToken, X-SAP-PVL, WWW-Authenticate"
```

注意：

允许所有方法和表头的默认值是 *（星号）。完全忽略命令行参数可产生相同效果。

- 5 单击“保存并关闭”。
- 6 右键单击 WACS 服务器名称（例如 MySIA.WebApplicationContainerServer），然后单击“重新启动服务器”将服务重新启动。

12.1.8.2.2 系统属性配置

12.1.8.2.2.1 启用错误消息堆栈

管理员可以将 RESTful Web 服务返回的错误消息配置为包含错误堆栈。错误堆栈可以提供额外的调试信息，这些信息可以用来发现错误出现的位置。

注意：

在生产方案中启用错误堆栈可能并不是一个明智的做法，因为错误堆栈可能会透露出不想让最终用户看到的 BI 平台相关信息。在生产方案中，建议仅当需要调试时才启用错误堆栈，在不需要时应禁用错误堆栈。

- 1 以管理员用户身份登录到中央管理控制台。
- 2 单击“服务器”，然后单击“服务器列表”。
- 3 在 Web 应用程序容器服务器 (WACS) 上单击鼠标右键（例如右键单击 MySIA.WebApplicationContainerServer），然后单击“属性”。

此时，将出现 WACS 服务器的“属性”选项卡。

- 4 在“RESTful Web 服务”区域中，选择“显示错误堆栈”。
- 5 单击“保存并关闭”。

此时，RESTful Web 服务的错误消息中会包含错误堆栈信息。

12.1.8.2.2.2 设置每页上默认显示的条目数

如果 RESTful Web 服务响应包含具有大量条目的源，可以将响应的条目分页显示。可以配置每页显示的默认条目数。开发人员向 RESTful Web 服务提交请求时可以指定每页显示的条目数。不过，如果未指定此值，则使用默认的页面大小。

- 1 以管理员身份登录到中央管理控制台。
- 2 单击“服务器”，然后单击“服务器列表”。
- 3 在 Web 应用程序容器服务器 (WACS) 上单击鼠标右键（例如右键单击 MySIA.WebApplicationContainerServer），然后单击“属性”。

此时，将出现 WACS 服务器的“属性”选项卡。

- 4 在“RESTful Web 服务”区域的“一页的默认对象数”文本区域内，输入默认页面大小。
- 5 单击“保存并关闭”。

12.1.8.2.2.3 设置登录标记的超时值

登录标记在一段时间不使用后会过期。可以设置未使用的登录标记保持有效的时间量。

注意：

默认情况下，登录标记超时值为一小时。

- 1 以管理员身份登录到中央管理控制台。
 - 2 单击“服务器”，然后单击“服务器列表”。
 - 3 在 Web 应用程序容器服务器 (WACS) 上单击鼠标右键（例如右键单击 `MySIA.WebApplicationContainerServer`），然后单击“属性”。
- 此时，将出现 WACS 服务器的“属性”选项卡。
- 4 在“RESTful Web 服务”区域的“Enterprise 会话标记超时（分钟）”文本区域中，输入登录标记有效的分钟数。
 - 5 单击“保存并关闭”。

12.1.8.2.2.4 配置会话池设置

使用会话池可以提高服务器的性能。会话池可以缓存活动的 RESTful Web 服务会话，因此当用户在 HTTP 请求标头中使用与之前相同的登录标记发送请求时，就可以重新使用之前的会话。会话池大小定义了同时存储的缓存会话数，会话超时值控制会话缓存的时间量。

可以设置会话池的大小和会话的超时值：

- 1 以管理员身份登录到中央管理控制台 (CMC)。
 - 2 单击“服务器”，然后单击“服务器列表”。
 - 3 在 Web 应用程序容器服务器 (WACS) 上单击鼠标右键（例如右键单击 `MySIA.WebApplicationContainerServer`），然后单击“属性”。
- 此时，将出现 WACS 服务器的“属性”选项卡。
- 4 在“RESTful Web 服务”区域的“会话池大小”文本框中输入要缓存的最大会话数。
 - 5 在“RESTful Web 服务”区域的“会话池超时（分钟）”文本框中输入会话池超时值。
 - 6 单击“保存并关闭”。
 - 7 右键单击 WACS 服务器（例如 `MySIA.WebApplicationContainerServer`），然后单击“重新启动服务器”。

12.1.8.2.2.5 启用 HTTP 基本身份验证

使用 HTTP 基本身份验证，用户无需提供登录标记即可提交 RESTful Web 服务请求。启用 HTTP 基本身份验证后，会在用户第一次提交 RESTful Web 服务请求时提示输入用户名和密码。

注意：

除非与 HTTPS 结合使用，否则使用 HTTP 基本身份验证的过程中用户名和密码并不以安全的方式传输。

启用 HTTP 基本身份验证时，可以将默认的 HTTP 基本身份验证类型设置为 SAP、Enterprise、LDAP 或 WinAD。用户可以在登录时覆盖默认的 HTTP 基本身份验证类型。

使用 HTTP 基本身份验证登录 BI 平台需要占用许可。如果使用了会话池缓存，登录请求会使用与其缓存的会话关联的许可。如果没有使用会话池缓存，那么请求正在处理时会占用许可，请求完成后便会释放许可。

- 1 以管理员身份登录到中央管理控制台 (CMC)。
 - 2 单击“服务器” > “服务器列表”。
 - 3 在 Web 应用程序容器服务器 (WACS) 上单击鼠标右键（例如右键单击 MySIA.WebApplicationContainerServer），然后单击“属性”。
- 此时，将出现 WACS 服务器的“属性”选项卡。
- 4 在“RESTful Web 服务”区域中，选择“启用 HTTP 基本身份验证”。
 - 5 （可选）在“HTTP 基本身份验证作为默认基本身份验证方案”列表中，选择默认的 HTTP 基本身份验证类型。
 - 6 单击“保存并关闭”。

注意：

当最终用户使用 HTTP 基本身份验证登录时，可以指定要使用的身份验证类型。在 Web 浏览器的用户名提示中输入 <authtype>\<username>，在密码提示中输入 <password>。

如果要以编程方式使用 HTTP 基本身份验证登录，用户需要在 HTTP 请求标头中加入 Authorization 属性，并将其值设置为 Basic <authtype>\<username>:<password>。

请将 <authtype> 替换为身份验证类型，<username> 替换为用户名，<password> 替换为密码。按照 RFC 2617 的定义，身份验证类型、用户名和密码必须使用 Base64 进行编码。在 HTTP 基本身份验证中不能使用包含“:”字符的用户名。

相关主题

- 第 447 页上的[“配置会话池设置”](#)

12.1.8.2.3 跨源资源共享

12.1.8.2.3.1 配置跨源资源共享 (CORS)

使用“跨源资源共享配置”(CORS)设置可添加域名列表以使用户在基于 JavaScript 的 Web 页面上从多个源中检索数据。这是为了应对 JavaScript 和 Ajax 语言采用的阻止跨域访问安全策略所进行的必要操作。为避免损害安全性,只有可能会访问到的网站才会添加到 CMC 的“允许源”WACS 服务器属性中。

也可以使用“最长寿命(分钟)”设置调整高速缓存的有效期,该选项设置了浏览器最多可以保留 HTTP 请求的分钟数。

注意:

默认情况下,* (星号)表示可以对任一域及所有域进行访问。

- 1 以管理员身份登录到中央管理控制台。
 - 2 单击“服务器”>“服务器列表”。
 - 3 在 Web 应用程序容器服务器(WACS)上单击鼠标右键(例如右键单击 MySIA.WebApplicationContainerServer),然后单击“属性”。
- 此时,将出现 WACS 服务器的“属性”选项卡。
- 4 在“RESTful Web 服务”区域,转到“允许源:”旁边的“跨源资源共享配置”文本框,然后用域名称列表替换*(星号),各名称之间用逗号分隔。例如: `http://origin1.server:8080`, `http://origin2.server:8080`
 - 5 在“最长寿命(分钟):”文本框中,键入希望浏览器缓存 HTTP 请求的最多分钟数。
 - 6 单击“保存并关闭”。

12.1.8.2.4 身份验证

12.1.8.2.4.1 配置 web.xml 以启用 WinAD SSO

配置 RESTful Web 服务以识别 Windows Active Directory 单一登录 (WinAD SSO) 要求对位于 BI 平台服务器上的 web.xml 配置文件进行编辑。有关更多信息, 请参阅《Business Intelligence Platform RESTful Web Service Developer Guide》(Business Intelligence Platform RESTful Web 服务开发人员指南) 中的 “Using the SDK” > “Authentication” > “To get a logon token using an Active Directory Single Sign-On (AD SSO) account” (“使用 SDK” > “身份验证” > “使用 Active Director 单一登录 (AD SSO) 帐户获取登录标记”)。

要使客户端计算机 WinAD SSO 登录凭据被 BI 平台服务器识别, 用户必须取消注释 web.xml 的 Kerberos Proxy filter 部分, 并为可反映所使用的 Active Directory 环境的 idm.realm、idm.princ 和 idm.keytab 更新值。

- 1 将 web.xml 配置放置于 <boe 根目录>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\RestWebService\biprws\WEB-INF\。以下是示例文件路径。

```
C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services\RestWebService\biprws\WEB-INF\web.xml
```

- 2 在 web.xml 文件中, 取消注释 Kerberos Proxy Filter 部分, 方法是在 <filter> 标签前添加注释结束标签 -->, 然后将原有的注释结束标签 --> 删除

```
<!-- Kerberos Proxy Filter
- Uncomment this filter and the corresponding filter-mapping to enable Kerberos SSO
- for Windows AD (secWinAD) authentication.
- The following options must be specified (the rest are optional):
-   idm.realm
-   idm.princ
-   idm.keytab (unless using password, see below)
-->

<filter>
  <filter-name>WrappedResponseAuthFilter</filter-name>
  .
  .
  .
</filter>

<filter-mapping>
  <filter-name>WrappedResponseAuthFilter</filter-name>
  <url-pattern>/logon/adso</url-pattern>
</filter-mapping>

</web-app>
```

- 3 将 idm.realm、idm.princ 和 idm.keytab 中每个设置的 <param-value> 更新为在 Active Directory 环境中使用的值。

```
<init-param>
  <param-name>idm.realm</param-name>
  <param-value>ADDOM.COM</param-value>
  <description>
    Required: Set this value to the Kerberos realm to use.
  </description>
</init-param>

<init-param>
  <param-name>idm.princ</param-name>
  <param-value>BOE120SIAVMB0ESRVR/bo.service.addom.com</param-value>

  <description>
    Set this value to the Kerberos service principal to use.
    This will be a name of the form HTTP/fully-qualified-host.
    For example, HTTP/example.vintela.com
    If not set, defaults to the server's hostname and the
```

```

        idm.realm property above.
      </description>
    </init-param>

    <init-param>
      <param-name>idm.kdc</param-name>
      <param-value></param-value>
      <description>
        The KDC against which secondary credentials must be validated
        This can be used for BASIC fallback or credential delegation.
        By default the KDC will be discovered automatically and this
        parameter must only be used if automatic discovery fails, or
        if a different KDC to the one discovered must automatically be used.
      </description>
    </init-param>

    <init-param>
      <param-name>idm.keytab</param-name>
      <param-value>C:/winnt/BOE120SIAMBOESRVR.keytab</param-value>
      <description>
        The file containing the keytab that Kerberos will use for
        user-to-service authentication. If unspecified, SSO will default
        to using an in-memory keytab with a password specified in the
        com.wedgetail.idm.sso.password environment variable.
      </description>
    </init-param>

```

注意：

idm.keytab 的值为 BI 平台服务器上的文件路径。可以从中央管理控制台查看 idm.realm 和 idm.prince 的值。在 CMC 的“身份验证”选项卡中，双击“Windows AD”。idm.realm 的值使用“AD 配置摘要”下的“默认 AD 域”参数进行设置。idm.prince 的值使用“身份验证选项”下的“服务主体名称”参数进行设置。

- 4 重新启动 WACS 服务以识别对 web.xml 的更改。
- 5 使用客户端计算机验证使用 RESTful Web 服务 API 可以获取 AD SSO 登录标记（例如，<http://<boe主机>:6405/biprws/logon/adsso>）。
- 6 通过使用头部中包括 X-SAP-LogonToken 的 GET 查询并使用 /infostore API 对该标记进行测试。

12.1.8.2.4.2 启用和配置受信任的身份验证

受信任的身份验证通过以下区域中的中央管理控制台（CMC）激活和配置：在“身份验证”>“Enterprise”中启用受信任的身份验证并生成共享秘密密钥文件；在“用户和组”>“用户列表”中为受信任的用户创建帐户；在“服务器”>“服务器列表”>“WACS”>“属性”中为 /logon/trusted API 登录标记请求选择“获取方法”选项。

- 1 以管理员身份登录到中央管理控制台。
- 2 转到“身份验证”>“Enterprise”，然后单击“已启用受信任的身份验证”。
- 3 单击“新建共享秘密”，然后单击“下载共享秘密”。
- 4 单击“保存”，然后将 TrustedPrincipal.conf 文件放置在默认位置 <Enterprise 安装目录>\<平台> 下。

示例位置显示如下：

```
"C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjectsEnterprise XI 4.0\win64_x64\"
```

注意：

- 通过在“服务器”>“服务器列表”>“WACS”>“属性”>“命令行参数”的 CMC 中添加命令行条目，然后重新启动 WACS 服务，用户可更改 TrustedPrincipal.conf 共享秘密文件的默认位置。例如，如果命令行条目使用 -Dbobj.trustedauth.home= 和 BI 平台服务器 C:\ 驱动器根目录的 SharedSecrets 文件夹，则该命令行条目如下所示：

```
"-Dbobj.trustedauth.home=C:\SharedSecrets"
```

- 可以将选项“共享秘密有效期(天)”保留为默认值零(0)，如此便不会过期。“受信任的登录请求在 N 毫秒后超时(0 表示无限制)”选项可以保留为默认值零(0)，这样受信任的登录请求便无时间限制。

5 单击“更新”以保存更改。

6 使用“管理”>“新建”>“新建用户”在“用户和组”>“用户列表”中添加新的用户名和密码，例如 bob 和 Passw0rd。取消选中“用户必须在下一次登录时更改密码”，然后单击“创建并关闭”。

注意：

还可通过单击“创建新用户”图标，或者通过在列出用户名的窗口的开放区域右键单击，然后选择“新建”>“新建用户”来创建新用户。

7 转到“服务器”>“核心服务”>“WACS”>“属性”，向下滚动到“受信任的身份验证配置”部分，然后使用“获取方法”菜单选择“HTTP_HEADER”、“QUERY_STRING”或“COOKIE”。

注意：

用户可以选择将“用户名参数”从默认标签 X-SAP-TRUSTED-USER 更改为其他任何方便的标签（例如 Username、bankteller 或 nurse），RESTful Web 服务开发人员必须使用这些标签。

8 右键单击 WACS 服务器名称（例如 MySIA.WebApplicationContainerServer），然后单击“重新启动服务器”将该服务重新启动。

注意：

以后更改“获取方法”下的此选项（如步骤 7 所示）便不必重新启动 WACS。

9 验证用户可以获取登录标记，方法是使用 .../biprsw/logon/trusted/ API 并使用在步骤 5 中创建的用户名发送带有默认表头标签 X-SAP-TRUSTED-USER 的 GET 请求。

12.1.8.2.4.3 配置重新定位 TrustedPrincipal.conf 共享秘密配置文件的命令行参数

RESTful Web 服务包括为受信任的身份验证 TrustedPrincipal.conf 文件选择其他位置的命令行参数。

TrustedPrincipal.conf 文件包含通过 CMC：“身份验证”>“Enterprise”生成的共享秘密密钥，生成方法是单击“新建共享秘密”按钮，然后通过单击“下载共享秘密”将此文件保存到默认位置。

使用 TrustedPrincipal.conf 的自定义路径更新 Web 应用程序容器服务器 (WACS) 命令行，步骤如下：

- 1 以管理员用户身份登录到中央管理控制台。
- 2 单击“服务器”，然后单击“服务器列表”。
- 3 右键单击 WACS 服务（例如 MySIA.WebApplicationContainerServer），然后单击“属性”。此时，将出现 WACS 服务器的“属性”选项卡。
- 4 在“命令行参数”区域，输入指向将包含 TrustedPrincipal.conf 文件的目录的路径。该字符串由双引号引起，如下例所示。

```
"-Dbobj.trustedauth.home=C:\SharedSecrets"
```

注意：

TrustedPrincipal.conf 文件的默认位置为 <Enterprise 安装目录>\<平台>。示例位置如下：

```
"C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\win64_x64"
```

- 5 单击“保存并关闭”。
- 6 右键单击 WACS 服务器名称（例如 MySIA.WebApplicationContainerServer），然后单击“重新启动服务器”将服务重新启动。

12.1.9 WACS 和 IT 环境

本节描述如何在复杂的环境中配置 WACS。

12.1.9.1 将 WACS 与其他 Web 服务器结合使用

安装了 Web 应用程序容器服务器 (WACS) 后，该服务器将用作应用程序服务器和 Web 服务器，而不需要进行任何额外配置。可以将类似 Internet 信息服务 (IIS) 和 Apache 这样的受支持的 Web 服务器配置为执行转发至 WACS 服务器的 URL。

注意：

不支持使用 ISAPI 过滤器将请求从 IIS 转发到 WACS。

WACS 不支持符合以下条件的部署方案：Web 服务器承载静态内容，WACS 承载动态内容。静态和动态内容必须始终位于 WACS 上。

12.1.9.2 将 WACS 与负载均衡器结合使用

要在包含硬件负载均衡器的部署中使用 WACS，必须配置负载均衡器，使其使用 IP 路由或主动 cookie。这样，一旦在一台 WACS 上建立了某用户的会话，则该用户的所有后续请求都将发送到相同的 WACS。

使用被动 cookie 的硬件负载均衡器不支持 WACS。

如果硬件负载均衡器将 SSL 加密的 HTTPS 请求转发到 WACS，则必须在 WACS 上配置 HTTPS，并在每台 WACS 上安装 SSL 证书。

如果硬件负载均衡器对 HTTPS 通信进行解密并将解密的 HTTP 请求转发到 WACS，则不需要额外配置 WACS。

相关主题

- 第 429 页上的“[配置 HTTPS/SSL](#)”

12.1.9.3 将 WACS 与反向代理结合使用

可以在包含正向或反向代理服务器的部署中使用 WACS。无法将 WACS 本身用作代理服务器。

12.1.9.3.1 将 WACS 配置为支持 HTTP 和反向代理

要在包含反向代理的部署中使用 WACS，请配置 WACS，使 HTTP 端口用于防火墙内部（例如，安全网络上）的通信，HTTP 代理端口用于防火墙外部（例如，Internet）的通信。

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击要配置的 WACS。

将显示“属性”屏幕。

- 3 在“HTTP 代理配置”部分中：
 - a 选中“启用 HTTP 代理”。
 - b 指定 WACS 的 HTTP 端口，该端口将用于通过代理进行通信。
 - c 指定代理服务器的代理主机名和代理端口。
- 4 单击“保存并关闭”。

12.1.9.3.2 将 WACS 配置为支持 HTTPS 和反向代理

可以将某些负载均衡器和反向代理服务器配置为对 HTTPS 通信进行解密，然后将解密的通信转发到应用程序服务器。在这种情况下，可以将 WACS 配置为使用 HTTP 或 HTTP 代理。

如果负载均衡器或反向代理转发 HTTPS 通信，并且您想要配置 HTTPS 和反向代理，请创建两台 WACS。针对 HTTPS 将一台 WACS 配置为通过反向代理进行外部通信；将另一台 WACS 配置为通过 HTTPS 与内部网络上的客户端进行通信。

12.1.9.4 将 WACS 与防火墙结合使用

支持在具有防火墙的 IT 环境中部署 WACS。

默认情况下，WACS 将绑定到其安装所在的计算机上的所有 IP 地址。如果计划在客户端与 WACS 之间使用防火墙，则必须针对 HTTP 或 HTTP 代理使 WACS 绑定到特定的 IP 地址。为此，请取消选中“绑定到所有 IP 地址”，然后指定要绑定到的主机名或 IP 地址。

如果计划在部署中的 WACS 服务器与其他 BI 平台服务器之间使用防火墙，请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》的“了解 SAP BusinessObjects Business Intelligence 平台组件之间的通信”一节。

相关主题

- 第 167 页上的[“了解 BI 平台组件间的通信”](#)

12.1.9.5 在多宿主计算机上配置 WACS

多宿主计算机是指具有多个网络地址的计算机。默认情况下，Web 应用程序容器服务器实例会将其 HTTP 端口绑定到所有 IP 地址。如果想将 WACS 绑定到特定的网络接口卡 (NIC)，例如，想将 WACS 的 HTTP 端口绑定到一个 NIC，而将请求端口绑定到另一个 NIC：

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击要配置的 WACS。
将显示“属性”屏幕。
- 3 在“Web 应用程序容器服务”窗格的“通过代理的 HTTP 的配置”部分中，取消选中“绑定到所有 IP 地址”，并键入要将 WACS 绑定到的 IP 地址。
- 4 在“HTTPS 配置”部分中，取消选中“绑定到所有 IP 地址”，并键入要将 WACS 绑定到的 IP 地址或主机名。
- 5 在“公共设置”下，取消选择“自动分配”，然后指定 NIC 的主机名或 IP 地址，以用于 WACS 和部署中其他 BI 平台服务器之间的通信。
- 6 单击“保存并关闭”。
- 7 重新启动 WACS。

12.1.10 配置 Web 应用程序属性

可以按照以下方法配置 WACS 上所承载的 Web 应用程序的属性：

- 会为 WACS 提供经常变更的属性，作为可配置的服务属性。要编辑这些属性，打开中央管理控制台 (CMC) 中 WACS 的“属性”页面，修改相应的属性值，然后单击“保存”。
- 要修改 WACS 上所承载的 Web 应用程序的会话超时，首先确定 Web 应用程序是否具有可在 CMC 中进行配置的任何属性。

如果 Web 应用程序具有可在 CMC 中进行修改的属性，则修改 Web 应用程序的 web_xml.ino 文件。该文件为 WebAppName_web_xml.ino，其中 WebAppName 是 Web 应用程序的名称，可以在 Enterprise 目录/java/pjs/services/Web 应用程序名称 目录中找到该文件。

如果 Web 应用程序没有可在 CMC 中进行修改的属性，则修改 Web 应用程序的 web.xml 文件。在 Enterprise 目录/warfile/webapps/WebAppName 中可以找到此文件，其中 WebAppName 是 Web 应用程序的名称。

- 要修改不是会话超时或 CMC 中 WACS 的“属性”屏幕上所提供属性的属性，请修改 Web 应用程序的 .properties 文件。有关更多信息，请参阅《SAP BusinessObjects Business Intelligence platform 管理员指南》的“通过 BOE.war 属性管理应用程序”一节。

注意：

- 请勿修改 Enterprise 目录/java/pjs/container/work/ServerFriendlyName 目录中的 web.xml、web_xml.ino 或 .properties 文件，因为每次 WACS 启动或重新启动时都将覆盖您所做的更改。
- 修改 WACS 的属性后，必须重新启动 WACS。

相关主题

- 第 370 页上的[“更改服务器的属性”](#)
- 第 598 页上的[“BOE WAR 文件”](#)

12.1.11 疑难解答

12.1.11.1 在 WACS 上配置跟踪

要为 WACS 配置跟踪，请参阅第 823 页上的[“记录组件的跟踪消息”](#)

12.1.11.2 查看服务器量度值

可以从中央管理控制台 (CMC) 中查看 WACS 的系统量度。

- 1 转到 CMC 的“服务器”管理区域。
- 2 右击 WACS，然后单击“量度”。

相关主题

- 第 958 页上的[“Web 应用程序容器服务器量度”](#)

12.1.11.3 查看 WACS 的状态

要查看 WACS 的状态，请转到 CMC 的“服务器”区域。“服务器列表”包括一个“状态”列，该列提供列表中每个服务器的状态。

WACS 有一种服务器状态叫作“已启动但出现错误”。该状态表示 WACS 正在运行，但存在一个或多个以下错误状况：

- HTTP、通过代理的 HTTP 或 HTTPS 连接器配置错误。
- WACS 上运行的服务，如：跟踪日志服务，未正常运行。
- WACS 中存在部署失败的 Web 应用程序。

请参阅 WACS “属性”页面查看失败的服务。

12.1.11.4 解决端口冲突

如果在尝试通过特定端口访问 CMC 时无法获取任何页面，请确保另一应用程序尚未接管为 WACS 指定的 HTTP、HTTP 代理或 HTTPS 端口。

以下两种方法可确定是否存在 WACS 端口冲突。如果部署中存在多台 WACS，请登录至 CMC，并检查正在运行的 WACS 连接器列表和 WACS 启动失败量度。如果 HTTP、HTTP 代理或 HTTP 连接器未显示在“正在运行的 WACS 连接器”列表中，则表示这些连接器因端口冲突而无法启动。

如果部署中仅存在一台 WACS，或如果不能通过任何 WACS 访问 CMC，请使用诸如 `netstat` 之类的实用程序确定另一应用程序是否已占用 WACS 端口。

12.1.11.4.1 解决 HTTP 端口冲突

- 1 启动中央配置管理器 (CCM)，然后单击“管理服务器”图标。
- 2 指定登录凭据。

- 3 在“管理服务器”屏幕上，停止 WACS。
- 4 单击“Web 层配置”图标。

注意：

“Web 层配置”图标仅在选择停止的 WACS 时才处于启用状态。

将显示“Web 层配置”屏幕。

- 5 在“HTTP 端口”字段中，指定 Web 应用程序容器服务器将使用的空闲 HTTP 端口，然后单击“确定”。
- 6 在“管理服务器”屏幕上，启动 WACS。

12.1.11.4.2 解决 HTTP 代理或 HTTPS 端口冲突

如果无法通过 HTTP 代理或 HTTPS 端口访问 WACS，但仍然可以通过 HTTP 端口连接到中央管理控制台 (CMC)，请通过 CMC 更改端口号。

- 1 转到 CMC 的“服务器”管理区域。
- 2 要停止想要配置的 WACS，请右击该服务器并单击“停止服务器”。
- 3 双击要配置的 WACS。
将显示“属性”屏幕。
- 4 在“HTTP 代理配置”部分中，指定一个新的 HTTP 端口。
- 5 要更改 HTTPS 端口，请在“HTTPS 配置”部分内的“HTTPS 端口”字段中键入一个新值。
- 6 单击“保存并关闭”。
- 7 要启动 WACS，请右击该服务器并单击“启动服务器”。

12.1.11.5 更改内存设置

要提高 WACS 的服务器性能，可以通过中央配置管理器 (CCM) 更改分配给服务器的内存量。

- 1 启动 CCM 并单击“管理服务器”图标。
- 2 指定 CMC 的登录凭据。
- 3 在“管理服务器”屏幕上，停止 WACS。
- 4 单击“Web 层配置”图标。

注意：

“Web 层配置”图标仅在选择停止的 WACS 时才处于启用状态。

将显示“Web 层配置”屏幕。

- 5 在“命令行参数”下面，通过编辑命令行指定新内存值：
 - a 查找 `-Xmx` 选项。通常已经指定了此选项的值。
例如 `-Xmx1g`。此设置分配 1 千兆字节的内存给服务器。
 - b 为该参数指定一个新值。
 - 若要以兆字节指定一个值，请使用 `m`。例如，`-Xmx640m` 分配 640 兆字节的内存给 WACS。
 - 若要以千兆字节指定一个值，请使用 `g`。例如，`-Xmx2g` 分配两千兆字节的内存给 WACS。
 - c 单击“确定”。
- 6 在“管理服务器”屏幕上，启动 WACS。

12.1.11.6 更改并发请求数

并发 HTTP 请求（将 WACS 配置为处理这些并发请求）的默认数为 150。对于大多数部署方案，应该可以接受此数值。要提高 WACS 的性能，可增加并发 HTTP 请求的最大数量。尽管增加并发请求数可以提高性能，但将此值设置得太高可能有损性能。理想的设置取决于硬件、软件和 IT 要求。

- 1 转到 CMC 的“服务器”管理区域。
- 2 要停止想要配置的 WACS，请右击该服务器并单击“停止服务器”。
- 3 双击要配置的 WACS。
将显示“属性”屏幕。
- 4 在“并发设置（按连接器）”下的“最大并发请求数”字段中，输入所需的并发请求数，然后单击“保存并关闭”。
- 5 要启动 WACS，请右击该服务器并单击“启动服务器”。

12.1.11.7 还原系统默认值

如果错误配置了 WACS，则可以通过中央配置管理器 (CCM) 恢复系统默认值。

- 1 启动 CCM 并单击“管理服务器”图标。
- 2 指定登录凭据。

- 3 在“管理服务器”屏幕上，停止 WACS。
- 4 单击“Web 层配置”图标。

注意：

仅在选择已停止的 WACS 时，才启用“Web 层配置”图标。

将显示“Web 层配置”屏幕。

- 5 单击“还原系统默认值”。
- 6 如有必要，请指定一个空闲的 HTTP 端口，然后单击“确定”。
- 7 在“管理服务器”屏幕上，启动 WACS。

12.1.11.8 防止用户通过 HTTP 连接到 WACS

在某些情况下，可能希望只允许本地计算机上的用户通过 HTTP 或 HTTPS 连接到 WACS。例如，虽然不能关闭 HTTP 端口，但可能希望配置 WACS，以便它只接受来自与 WACS 位于相同计算机上的客户端的 HTTP 请求。这样，便可以通过与 WACS 位于同一台计算机上的浏览器对 WACS 执行维护或配置任务，同时防止其他用户访问服务器。

- 1 转到 CMC 的“服务器”管理区域。
- 2 双击要修改的 WACS。
将显示“属性”屏幕。
- 3 在“Web 应用程序容器服务”部分中，清除“绑定到所有 IP 地址”复选框。
- 4 在“绑定到主机名或 IP 地址”字段中，键入“127.0.0.1”，然后单击“保存并关闭”。
- 5 要启动 WACS，请右击该服务器并单击“启动服务器”。
以这种方式配置的 WACS 仅接受来自本地计算机的连接。

12.1.12 WACS 属性

有关可为 WACS 配置的常规、HTTP、HTTP 代理和 HTTPS 配置属性的完整列表，请参阅服务器属性附录的核心服务器设置一节。

相关主题

- 第 912 页上的“[核心服务属性](#)”

第 13 章 备份和恢复系统

13.1 备份和恢复概览

本章介绍了如何备份 BI 平台，以及如何从硬件故障、软件故障及数据丢失中恢复系统。要执行备份与恢复计划，需要具有丰富经验的 SAP BusinessObjects 专家、系统管理员和数据库管理员。

相关主题

- 第 466 页上的[“备份整个系统”](#)
- 第 471 页上的[“备份 BI 内容”](#)
- 第 470 页上的[“在 Windows 上的 CCM 中备份服务器设置”](#)
- 第 470 页上的[“备份 Unix 上的服务器设置”](#)
- 第 483 页上的[“系统复制概述”](#)

13.2 术语

术语	定义
数据复制	数据复制是创建一个或多个数据副本的流程。实时更新副本；例如，在使用镜像驱动器时。它可提供针对物理数据损坏的实时数据保护，但由于驱动器会不断更新，因此如果数据发生崩溃或被意外删除，系统将无法恢复到早期状态。

术语	定义
版本管理	<p>版本功能可在系统上创建特定文件的多个版本。这时便可以将系统恢复为早期状态。</p> <p>所有数据版本通常都存储在相同主机系统上。如果此系统性能下降或受损，就会面临丢失当前版本和旧版本的风险。类似地，取消删除功能会保留“已删除”文件的副本以供将来恢复，但这些副本通常也存储在与原始数据相同的主机系统上。它并未提供针对物理数据损坏（例如磁盘故障）的保护。</p>
裸机系统备份	<p>裸机系统备份是整个文件系统的备份，包括操作系统。裸机系统备份旨在将一个备份系统恢复到不包含软件或操作系统的硬件。</p> <p>对于裸机系统备份，如果出现故障，整个文件系统（包括操作系统）均会恢复为相同的硬件，或如果恢复工具支持独立于硬件的恢复，则可恢复到任何硬件。</p>
裸机系统备份对比应用程序备份	<p>裸机系统备份创建整个系统的副本，包括操作系统。裸机系统备份可以将整个系统恢复为早期版本。</p> <p>应用程序备份备份有关个别应用程序的文件。</p> <p>BI 平台支持裸机系统备份，而非应用程序备份。</p> <p>对于裸机系统备份，如果出现故障，整个文件系统（包括操作系统）均会恢复为相同的硬件，或如果恢复工具支持独立于硬件的恢复，则可恢复到任何硬件。</p> <p>完整的 BI 平台系统备份被称作一个备份集。</p>
备份集	<p>备份集包括同时创建的这些个别备份：</p> <ul style="list-style-type: none"> • CMS 系统数据库的备份 • BI 平台部署中所有计算机的整个文件系统的裸机备份，包括操作系统 • 输入 FRS 和输出 FRS 文件存储的备份（如果未包含在 BI 平台文件系统中） • Web 层组件的备份（如果未作为 BI 平台文件系统的一部分包含在内） • 审核数据库的备份
冷热备份对比	<p>冷备份是在系统已停止、无法供用户使用时执行的备份。热备份在系统运行并对用户可用时执行，并且在执行备份时数据会发生变化。此外，在执行热备份时，必须按顺序执行备份步骤，而冷备份则不需要。</p> <p>BI 平台同时支持冷热备份。</p> <p>热备份有时被称作在线备份。</p>

13.3 备份和恢复的使用情况

下表介绍用户通过拥有的资源可能希望实现的目标，并指导用户使用最恰当的备份解决方案。

目标	所需资源	解决方法
<p>目标：恢复系统</p> <p>1 我的 BI 平台系统崩溃。因此，我需要将它恢复到上次备份时的工作状态。</p> <p>2 一台承载 BI 平台的计算机损坏。我需要用新计算机替换它。</p>	<ul style="list-style-type: none"> 与源系统具有相同硬件的目标系统 和 源系统的备份 	<p>使用本指南中所详细说明的系统备份和恢复工作流，请参阅第 466 页上的 “备份整个系统” 过程。从源系统的备份重新创建目标系统。</p>
<p>目标：恢复对象</p> <p>我想恢复意外删除的文档或其他对象。</p>	<ul style="list-style-type: none"> 源系统数据库和文件的备份 和 第 487 页上的 “从源系统导出” 中详细介绍的系统信息。 	<p>使用备份，在另一台计算机上建立系统的副本，使用“复制 Business Intelligence 平台部署”一章中的系统复制工作流。然后使用升级管理工具，从新系统升级意外删除的对象。请参阅系统复制工作流，从第 485 页上的 “计划复制系统” 开始，并遵循本章其余部分的说明。</p> <p>注意： 可以在具有相同版本、支持包和修补程序级别的现有 BI 平台部署的计算机上创建目标系统，或在未安装 BI 平台的“干净”计算机上创建目标系统。</p>
<p>目标：恢复对象 2</p> <p>我想恢复意外删除的文档或其他对象。</p>	使用升级管理版本管理的系统	使用升级管理应用程序恢复文档的早期版本。有关详细信息，请参阅升级管理方面的相关主题。
<p>目标：备份对象</p> <p>我想备份少量对象（例如：文档、文件夹、用户）。</p>	使用升级管理版本管理的系统	<p>使用升级管理应用程序备份 BI 内容，然后将内容导出到商务智能存档（LCMBIAR）文件。如果内容崩溃或缺失，可以稍后恢复它，而不必恢复整个系统。</p> <p>有关详细信息，请参阅升级管理方面的相关主题。</p>

相关主题

- 第 466 页上的 [“备份”](#)
- 第 485 页上的 [“计划复制系统”](#)
- 第 498 页上的 [“概述”](#)

13.4 备份

备份和恢复计划包括在系统因自然灾害或意外故障而出故障的情况下要采取的措施。计划旨在尽量减少灾难对日常操作的影响，以便能够维护或快速恢复关键功能。

备份 BI 平台部署时，有三种选择：

- 备份整个系统，这将允许恢复整个系统。在这种情况下，不能只恢复一部分系统。如果要重建 BI 平台而并非从备份恢复，请参阅介绍系统复制的相关主题。
- 备份服务器设置，将能够只恢复服务器设置而不恢复其他对象，从而保留系统 BI 内容的当前状态。
- 备份 BI 内容（例如文档），将允许选择性地恢复部分 BI 内容，而无需恢复所有对象。

请参阅相关主题，了解有关全部三种备份类型的详细信息。

提示：

- 要避免丢失数据，请定期执行备份。
- 可以备份 BI 平台系统，然后恢复到同一台或另一台主机计算机以创建系统的副本。

相关主题

- 第 466 页上的[“备份整个系统”](#)
- 第 469 页上的[“备份服务器设置”](#)
- 第 471 页上的[“备份 BI 内容”](#)
- 第 483 页上的[“系统复制概述”](#)

13.4.1 备份整个系统

通过执行可创建备份集的冷备份或热备份，备份整个 BI 平台系统。保留多个时刻的多个备份集可在恢复系统时提供更多选择。根据组织的业务需要，尽可能频繁地备份系统。

可以选择停止 BI 平台系统并执行冷备份，也可以选择执行热备份。热备份意味着在备份过程中系统仍保持运行状态并可供用户使用。其优点是系统没有停机时间。

注意：

- 建议将事务日志写入到主数据库服务器系统以外的某个文件系统中，定期备份此事务日志，并将其与其他文件一起放在备份集中。

- 如果备份审核数据库，请确保在备份文件集中包含审核数据库的数据库事务日志。不需要在备份中包含审核临时文件。

13.4.1.1 热备份

热备份功能允许用户在备份 BI 平台系统的同时，继续正常使用系统。如果业务要求在系统备份时持续运营，请在中央管理控制台中启用并配置热备份。

“热备份最长持续时间”设置指定预期进行备份的最长时间（从 CMS 备份开始起至 FRS 备份结束止）。如果指定的持续时间过短，在备份过程复制文件之前文件可能已被删除。为避免此问题，将所需时间高估一些会更保险。该问题需要与系统资源权衡考虑，因为较高的值会略微增加 FRS 文件存储的大小。

注意：

只要选中 CMC 中的“启用热备份”复选框，则将一直启用热备份；“热备份最长持续时间”设置不会影响热备份是否启用。

将系统恢复到特定备份时间非常简单。例如，如果每天凌晨 3:00 执行系统备份，则可以轻松将系统恢复至启动 CMS 系统备份时的状态（所选日期的凌晨 3:00）。在 CMS 数据库或审核数据库出现故障后，如果在 CMS 数据库或审核数据库上启用了事务日志，则可以将系统恢复至出现故障前一刻的状态。

为确保最大的安全性，请将事务日志记录保存在不同于主数据库备份记录的位置。此举确保在数据库故障时可将数据库恢复到故障前的状态。

注意：

- 由于旧版本的 IBM DB2 存在事务日志大小限制，因此仅当 CMS 系统数据库承载于 DB2 数据库版本 9.5 FixPack 5 或更高版本（对于 9.5 系列）和 9.7 FixPack 1 或更高版本（对于 9.7 系列）上时才支持热备份和事务日志相关的任务。
- 建议将事务日志写入到主数据库服务器系统以外的某个文件系统中，定期备份此事务日志，并将其与其他文件一起放在备份集中。

Crystal Reports 2011 设计器客户端、Web Intelligence 胖客户端、4.0 FP3 之前的 Universe 设计工具客户端以及针对 4.0 FP3 之前的 SDK 编译的自定义开发胖客户端应用程序可能不支持在热备份过程中修改文件。如果这些客户端应用程序在备份过程中修改 BI 内容，可能会有损在备份过程中修改的数据的质量。可以禁止客户端应用程序修改文档以确保备份数据的一致性。尽可能将客户端应用程序更新为 4.0 FP3。如果不能，则需要另寻解决办法。例如，可以建议这些客户端应用程序的用户删除现有对象并保存新版本，而不是修改这些对象。

13.4.1.1.1 启用热备份

1. 打开中央管理控制台（CMC）。
2. 在“管理”区域中，打开“设置”页面。
3. 在“热备份”部分，选择“启用热备份”。
4. 在“热备份最长持续时间（分钟）”下输入备份的预期最大分钟数。
确保包括备份 CMS 数据库和 BI 平台主机文件系统所需的时间。

注意：

如果备份的实际持续时间超出这里输入的限值，可能会导致所备份数据的不一致。为避免此问题，将所需时间高估一些会更保险。

5. 要允许早期版本（4.0 FP3 之前）的 Web Intelligence 胖客户端、Crystal Reports 设计器或自定义 SDK 胖客户端应用程序修改系统上的文档，请选中“启用旧应用程序支持（备份限制）”复选框。
允许旧客户端应用程序在备份操作过程中修改文档可能会导致在备份过程中修改的文档出现不一致。有关备份限制的信息，请参阅有关热备份的相关链接。
6. 单击“更新”。
将启用热备份。

启用热备份支持后，便可以使用数据库和文件系统供应商的备份工具执行备份。

相关主题

- 第 467 页上的[“热备份”](#)
- 第 468 页上的[“要执行热或冷系统备份”](#)

13.4.1.2 要执行热或冷系统备份

如果要执行热备份，首先请查阅有关热备份先决条件的主题或更多信息。如果要执行冷备份，请停止 BI 平台部署中的所有节点。

警告：

如果在没有启用热备份和停止所有节点的情况下执行备份，CMS 数据库和 FRS 文件存储之间可能产生数据不一致。

注意：

对于热备份，重要的是按说明的顺序开始程序。对于冷备份，可按任意顺序执行程序。在任一情况下，开始下一步前都无需等待每个备份步骤完成。

1. 使用数据库供应商的工具备份中央管理服务器（CMS）系统数据库。

注意：

对于热备份，请以在线原子模式使用数据库供应商的备份工具。

- 2 使用数据库供应商的工具以在线原子模式备份 BI 平台审核数据库。
- 3 在 BI 平台部署中备份所有计算机的整个文件系统，包括操作系统。
 - a 如果输入和输出 FRS 文件存储未包含在 BI 平台备份中（单独的主机计算机），请使用文件备份工具创建这两者的备份副本。
 - b 如果 Web 层组件未包含在 BI 平台备份中（单独的主机计算机），请使用文件备份工具创建其备份副本。

对于热备份，如果可能，请使用原子文件备份工具。

如果执行冷备份，请等待所有备份完成，然后启动 BI 平台节点。

相关主题

- 第 467 页上的“[热备份](#)”

13.4.2 备份服务器设置

为防止系统错误配置服务器设置，可定期将服务器设置备份至 BIAR 文件。拥有服务器的可用备份就可以恢复设置，且无需恢复中央管理服务器（CMS）系统数据库、文件资源库或 Business Intelligence 内容。

每次更改系统部署时都有必要备份服务器设置。包括创建、重命名、移动、删除节点以及创建或删除服务器。建议在更改设置之前先备份服务器设置，并在对所做更改满意后再次备份。

使用中央配置管理器（CCM）或者脚本，将 BI 平台服务器设置备份至 BIAR 文件，然后将该文件存储在其他计算机或存储介质中。

注意：

如果在启用 SSL 的部署中备份或恢复服务器设置，则必须先通过 CCM 禁用 SSL，然后在备份或恢复完成后重新启用它。

在 Windows 计算机上，BackupCluster.bat 脚本位于 安装目录\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts 目录中。

在 Unix 计算机上，backupcluster.sh 脚本位于 /安装目录/sap_bobj/enterprise_xi40/平台64/scripts 目录中。

相关主题

- 第 162 页上的“[配置 SSL 协议](#)”

13.4.2.1 在 Windows 上的 CCM 中备份服务器设置

此操作过程为整个群集备份服务器设置。无法为单个服务器备份设置。

注意：

如果正在使用临时 CMS，则必须在安装了本地 CMS 二进制文件的计算机上使用 CCM。

- 1 启动 CCM，并单击工具栏中的“备份服务器配置”。
此时将出现“服务器配置备份向导”。
- 2 单击“下一步”启动向导。
- 3 指定是使用现有 CMS 备份服务器配置设置，还是创建一个临时 CMS。
 - 要从正在运行的系统备份服务器设置，请选择“使用正在运行的现有 CMS”，并单击“下一步”。
 - 若要从未运行的系统中备份服务器设置，请选择“启动新的临时 CMS”，并单击“下一步”。
- 4 如果正在使用临时 CMS，请选择一个在上面运行 CMS 的端口号，并指定数据库连接信息。
为在恢复系统时使用户访问系统的风险最小化，请指定一个与现有 CMS 使用的端口号不同的端口号。
- 5 输入群集密钥，并单击“下一步”继续。
- 6 收到提示时，通过指定系统和具有管理权限的帐户的用户名和密码登录到 CMS，然后单击“下一步”继续。
- 7 指定要将服务器配置设置备份到其中的 BIAR 文件的位置和名称，然后单击“下一步”继续。
“确认”页面将显示已提供的信息。
- 8 验证“确认”页面中显示的信息是否正确，然后单击“完成”继续。
CCM 将整个群集的服务器配置设置备份至已指定的 BIAR 文件。备份过程的详细信息将写入日志文件。日志文件的名称和路径显示在对话框中。
- 9 如果备份操作失败，请检查日志文件确定原因。
- 10 单击“确定”关闭向导。

13.4.2.2 备份 Unix 上的服务器设置

在 Unix 计算机上，使用 `serverconfig.sh` 脚本将部署的服务器设置备份到一个 BIAR 文件中。

- 1 选择“5 - 备份服务器配置”，并按 Enter 键。

- 2 指定是使用现有 CMS 备份服务器配置设置，还是创建一个临时 CMS。
 - 若要备份正在运行系统中的服务器设置，请选择“现有”并按 Enter 键。
 - 若要备份未运行系统中的服务器设置，或者恢复服务器设置，请选择“临时”并按 Enter 键。
- 3 如果使用临时 CMS 备份服务器设置，请在随后显示的屏幕中选择该临时 CMS 的运行端口号，以及与 CMS 系统数据库的连接信息。

为在恢复系统时使用户访问系统的风险最小化，请指定一个与现有 CMS 使用的端口号不同的端口号。
- 4 出现提示时，通过指定系统和具有管理权限的帐户的用户名和密码，登录到 CMS 并按 Enter 键。
- 5 出现提示时，指定备份服务器配置设置的 BIAR 文件的位置和名称，并按 Enter 键。

摘要屏幕将显示所提供的信息。
- 6 确保显示的信息正确无误，然后按 Enter 键继续。

serverconfig.sh 脚本将整个群集的服务器配置设置备份到指定的 BIAR 文件。详细的备份过程将写入日志文件。屏幕上将显示日志文件的名称和路径。
- 7 如果备份操作失败，请检查日志文件确定原因。

13.4.2.3 使用脚本备份服务器设置

通过在 Windows 上运行 BackupCluster.bat 脚本或在 Unix 上运行 backupcluster.sh 脚本，可以备份部署中的服务器设置。

在 Windows 上，BackupCluster.bat 文件位于 安装目录\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts 目录中。

在 UNIX 上，backupcluster.sh 位于 /安装目录/sap_bobj/enterprise_xi40/platform64/scripts 目录中。

相关主题

- 第 480 页上的“[BackupCluster 和 RestoreCluster 脚本](#)”

13.4.3 备份 BI 内容

建议使用升级管理应用程序定期备份 Business Intelligence 内容，例如报表、用户和组以及 Universe。如果具备内容的当前备份，就可以在不恢复整个系统或服务器设置的情况下恢复商务智能。

有关使用升级管理应用程序的更多信息，请参阅“升级管理”一章。

如果正在使用 Subversion 和升级管理应用程序，请参阅“版本管理”一章。

13.5 恢复系统

如果系统受损或崩溃，可以恢复整个系统，这将恢复 BI 平台。根据系统的具体情况，可能不需要执行完整恢复。如果系统工作正常，但有内容丢失或损坏，可以选择仅恢复 Business Intelligence (BI) 内容。如果 BI 内容有效，但平台服务器出现配置错误，可以选择仅恢复服务器设置。

从热备份中恢复与从冷备份中恢复的过程相同。

相关主题

- 第 472 页上的[“恢复整个系统”](#)
- 第 477 页上的[“恢复服务器设置”](#)
- 第 479 页上的[“恢复 BI 内容”](#)

13.5.1 恢复整个系统

恢复整个系统时，会同时恢复 BI 平台群集。根据系统中具体的故障对象，可以选择只进行部分恢复。

如果任何以下组件出现故障或丢失，则必须恢复整个系统：

- CMS 数据库

注意：

如果 BI 平台的其余部分运行正常，但 CMS 数据库崩溃，可以恢复 CMS 数据库，而不必恢复整个系统。

- FRS 文件存储
- 计算机的文件系统

注意：

对于完整的系统恢复，目标系统无需提前安装 BI 平台。

如果只有审核数据库出现崩溃或丢失，可以恢复审核数据库，而不必恢复整个系统。

如果 Web 层出现崩溃或丢失，可以恢复 Web 层内容，而不必恢复整个系统。

相关主题

- 第 473 页上的[“恢复整个系统”](#)
- 第 474 页上的[“仅恢复审核数据库”](#)
- 第 474 页上的[“恢复 Web 层内容”](#)
- 第 475 页上的[“仅恢复 CMS 数据库”](#)

13.5.1.1 恢复整个系统

在恢复系统之前，必须使用中央配置管理器（CCM）停止 BI 平台部署中的所有节点，并且必须选择要将系统恢复到的时间点。

注意：

如果有可能要将系统恢复到当前状态，请在恢复之前先备份系统。

1 找到以下备份文件：

- CMS 数据库备份
- 输入 FRS 和输出 FRS 文件存储备份
- BI 平台群集中每台主机计算机的文件系统的备份

注意：

确保验证备份，并确保以上所列全部文件均来自相同的备份集。如果以热备份的形式获得备份集，则应确保该 CMS 数据库备份的开始时间戳早于匹配的 FRS 文件存储、Web 层和主机计算机文件系统时间戳。所有这些文件都是必需的，即使只有一个组件出现故障。

- 2 使用文件恢复工具恢复 BI 平台群集中所有主机计算机的文件系统。
- 3 使用文件恢复工具恢复输入和输出 FRS 文件存储。
- 4 使用数据库工具恢复 CMS 数据库。
- 5 如果在创建备份之后更改了 CMS 数据库密码，请使用 CCM 在所有节点和 BI 平台主机计算机上更新 CMS 数据库密码。
- 6 如果使用审核功能：
 - a 找到审核数据库的最新备份和事务日志。
 - b 使用数据库工具恢复审核数据库。
 - c 对审核数据库执行前滚，重放事务日志。
- 7 选择以下选项之一恢复搜索索引：
 - 如果要运行搜索索引恢复脚本，请参阅第 476 页上的[“运行搜索索引恢复脚本”](#)并按照其中的说明操作。这样将可以更快提供完整的索引。
 - 如果希望重新建立搜索索引而不使用恢复脚本，请使用 CCM 重新启动 BI 平台节点。这个过程很简单，但在索引重新建立的过程中，只能对平台数据进行部分搜索访问。
- 8 启动系统，并注意后续必要步骤内的使用时间。
- 9 验证系统是否按预期运行，并执行健全性测试。

验证系统后，执行以下操作：

- 运行资源库诊断工具，删除任何不用的临时文件并检查资源库的一致性。请参阅本指南的“数据库诊断工具”一节。
- 如果未使用索引恢复脚本，请重新建立平台搜索索引。
- 备份系统时，处理中的任何发布作业均将显示为失败。请不要重新运行这些实例，而应启动新的发布作业。
- 如果审核数据库已恢复，则必须运行 SQL 查询，删除任何在数据库故障与重新启动时间（步骤 8 中记录的时间）之间发生的事件。例如：`delete from [DB_NAME].ADS_EVENT where Start_Time > '[time of DB failure]' and Start_Time < '[time of DB restoration]'`

相关主题

- 第 692 页上的“[为 CMS 资源库中的内容建立索引](#)”

13.5.1.2 仅恢复审核数据库

在恢复审核数据库之前，请使用中央配置管理器（CCM）停止 BI 平台部署中的所有节点。还必须选择要将数据库恢复到哪个时间点。

注意：

仅当确定审核数据库是唯一受损的 BI 平台组件时才执行此任务。如果还有其他组件受到影响，则必须执行整个系统恢复。

- 1 找到审核数据库的最新备份和事务日志。
- 2 使用数据库工具恢复审核数据库。
- 3 对审核数据库执行前滚，重放事务日志。

相关主题

- 第 473 页上的“[恢复整个系统](#)”

13.5.1.3 恢复 Web 层内容

在恢复 Web 层的内容之前，必须使用中央配置管理器（CCM）停止 BI 平台部署中的所有节点。还需要确定要将 Web 层内容恢复到哪个时间点。

如果希望能够选择返回到系统的当前状态，必须在恢复之前执行系统备份。

如果 Web 层崩溃，可单独进行恢复。

- 1 使用文件恢复工具恢复 Web 层主机计算机上的 Web 层文件夹。
- 2 使用 CCM 重新启动 BI 平台部署的所有节点。

13.5.1.4 仅恢复 CMS 数据库

注意：

仅当 CMS 数据库损坏时执行此过程。如果数据库已崩溃或有其他组件受损，必须执行完整的系统恢复。

修复或替换 CMS 数据库主机计算机。如果要替换，请确保其系统名称、端口设置以及数据库凭据与原主机计算机相同。

注意：

如果无法使用相同的名称和凭据恢复计算机，则需要使用 CCM 为群集中的每个节点更新此数据库连接信息，并重新启动这些节点。

- 1 使用 CCM 停止所有 BI 平台节点。
- 2 找到最新的 CMS 数据库备份集。
- 3 使用数据库工具恢复 CMS 数据库。
- 4 找到最近的 CMS 数据库事务日志，即，包含上一次备份后所执行事务的日志。
- 5 重放 CMS 数据库的整个事务日志。
- 6 使用 CCM 启动 BI 平台节点。

验证系统正常工作后，执行以下操作：

- 运行资源库诊断工具，删除任何不用的临时文件并检查资源库的一致性。请参阅本指南的“数据库诊断工具”一节。
- 备份系统时，处理中的任何发布作业均将显示为失败。请不要重新运行这些实例，而应启动新的发布作业。

相关主题

- 第 692 页上的“[为 CMS 资源库中的内容建立索引](#)”

13.5.1.5 搜索索引恢复

平台搜索功能将维护系统中一系列的索引和信息文件，从而帮助进行更高效的搜索。如果需要恢复系统，这些信息文件可能会出现不一致。可以通过使用索引恢复脚本或重新建立索引修复这些不一致问题。

重建索引是一个简单的过程，但是完成这个过程需要花费大量资源和时间；在重建过程中执行的搜索将仅针对数据库的索引部分返回结果。恢复脚本涉及的过程较为复杂，但是可以更快地提供完整、有效的索引。

如果要恢复具有多台计算机的部署，可在任一承载搜索服务的计算机上运行脚本。对于群集中的第一台计算机，应使用 `-Both` 选项，然后在该群集的所有后续计算机中使用 `-ContentStore` 选项。

相关主题

- 第 692 页上的“[为 CMS 资源库中的内容建立索引](#)”

13.5.1.5.1 运行搜索索引恢复脚本

- 确认 CMS 正在运行，停止所有已安装搜索服务的自适应处理服务器（APS）。

注意：

在启动节点之后必须尽快停止这些 APS。

- 将 `JAVA_HOME` 设置为 BI 平台安装目录中的 `sapjvm/bin` 位置。
 - 可通过运行脚本的计算机访问平台搜索数据目录。
- 1 在 CMS 或 APS 主机计算机上，打开命令行窗口（如果使用 Windows 操作系统）。
 - 2 切换到以下目录安装目录 `\SAP BuinessObjects Enterprise XI 4.0\java\lib\`。
Unix 计算机使用相应的 Unix 文件路径。
 - 3 键入 `java -jar platformSearchOnlineHotbackupRestore.jar` 并按 Enter 键。
 - 4 收到提示后，输入以下信息并按 Enter 键：
 - BI 平台安装位置（例如，安装目录 `/SAP businessObjects Enterprise XI 4.0`）
 - CMS 登录凭据，包括 CMS 名称、用户 ID 和密码以及身份验证类型。身份验证类型具有以下选项：
 - `secEnterprise`
 - `secLDAP`
 - `secWinAD`
 - `secSAPR3`
 - 5 当系统提示提供索引恢复类型时，键入以下选项之一并按 Enter 键。

值	说明
-Both	应当用于单个服务器部署，或者在多计算机部署中，用于搜索服务的第一台 APS 主机计算机。 在有多个搜索 APS 的系统上，脚本首次运行时，请使用 -Both 值（更新数据库和内容存储）。为全部其他搜索 APS 运行脚本时，请使用 -ContentStore 值（只更新内容存储）。
-ContentStore	应在安装搜索服务的 APS 主机计算机上运行脚本时使用（除非它是运行脚本的群集中的第一台计算机）。
-Exit	退出脚本而不执行任何索引恢复。

- 6 脚本完成运行后，关闭命令行窗口（对于 Windows 计算机）。

启动所有已停止的 APS。

13.5.2 恢复服务器设置

如果需要从 BIAR 文件恢复系统的服务器设置，可以使用中央配置管理器（CCM）或者 RestoreCluster 脚本来恢复服务器设置。从 BIAR 文件恢复服务器内容不会影响商务智能内容，如报表、用户和组或安全设置。

注意：

- 恢复服务器设置时，仅支持恢复整个群集的设置。无法只恢复群集中一部分服务器的设置。
- 如果在启用 SSL 的部署中备份或恢复服务器设置，则必须先通过 CCM 禁用 SSL，然后在备份或恢复完成后重新启用它。

相关主题

- 第 158 页上的“[针对 SSL 配置服务器](#)”

13.5.2.1 在 Windows 上通过 CCM 恢复服务器设置

可以使用中央配置管理器（CCM）恢复服务器设置。恢复服务器设置后，必须在系统群集中的每台计算机上重新创建系统节点。

- 1 通过停止每个节点的服务器智能代理，停止群集中正在为之恢复服务器配置设置的所有计算机上的所有节点。
- 2 在具有 CMS 的计算机上启动 CCM。
- 3 从工具栏中，单击“恢复服务器配置”。
此时将出现“恢复服务器配置向导”。
- 4 单击“下一步”启动向导。
- 5 出现提示时，请提供用于临时中央管理服务器（CMS）的端口号以及连接至 CMS 系统数据库的信息，然后单击“下一步”继续。
- 6 输入群集密钥，并单击“下一步”继续。
- 7 出现提示时，通过输入 CMS 名称和具有管理权限的帐户的用户名和密码登录到 CMS，然后单击“下一步”继续。
- 8 指定包含要恢复的服务器配置设置的 BIAR 文件位置和名称，然后单击“下一步”继续。
摘要页面将显示该 BIAR 文件的内容。
- 9 单击“下一步”以继续。
摘要页面将显示所输入的信息。
- 10 单击“完成”继续。
一条警告消息提示现有服务器设置将被 BIAR 文件中的值覆盖，如果继续，当前服务器设置将丢失。
- 11 单击“是”恢复服务器配置设置。

CCM 将从 BIAR 文件中恢复整个群集的服务器配置设置。恢复过程的详细信息将写入日志文件。日志文件的名称和路径显示在对话框中。

- 12 如果恢复操作失败，请检查日志文件以确定原因。
- 13 单击“确定”关闭向导。

在用户系统中，从 BIAR 文件恢复服务器设置。还将创建在恢复之前系统中不存在而在 BIAR 文件中存在的所有节点和服务器。

注意：

存在于系统中但不在 BIAR 文件中的节点和服务器将从资源库中删除。节点和服务器仍显示在 CCM 中，但可以手动删除某个节点的 dbinfo 和 bootstrap 文件。

必须在群集中每台计算机的系统中重新创建节点。

相关主题

- 第 381 页上的[“使用节点”](#)

13.5.2.2 在 Unix 上使用 CCM 恢复服务器设置

在 Unix 计算机上，使用 `serverconfig.sh` 脚本从 BIAR 文件中恢复部署的服务器设置。

- 1 选择 “6 - Restore server configuration” 并按 Enter 键。
- 2 输入临时中央管理服务器 (CMS) 要使用的端口号，并按 Enter 键。
- 3 在后续屏幕中，指定与 CMS 系统数据库的连接信息。
- 4 出现提示时，通过指定系统和具有管理权限的帐户的用户名和密码，登录到 CMS 并按 Enter 键。
- 5 出现提示时，指定要从中恢复服务器配置设置的 BIAR 文件的位置和名称，并按 Enter 键。
摘要屏幕将显示所提供的信息。
- 6 确保屏幕上显示的信息正确无误，然后按 Enter 键继续。
`serverconfig.sh` 脚本从指定的 BIAR 文件中恢复整个群集的服务器配置设置。详细的恢复过程将写入日志文件。屏幕上将显示该日志文件的名称和路径。
- 7 如果恢复操作失败，请检查该日志文件以确定原因。

13.5.2.3 用脚本恢复服务器设置

如果愿意，可以通过在 Windows 上运行 `RestoreCluster.bat` 脚本或在 Unix 上运行 `restorecluster.sh` 脚本恢复部署的服务器设置。

在 Windows 上，`RestoreCluster.bat` 位于安装目录 `\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts` 目录中。

在 Unix 上，`restorecluster.sh` 位于 `/安装目录/sap_bobj/enterprise_xi40/PLATFORM64/scripts` 目录中。

相关主题

- 第 480 页上的“[BackupCluster 和 RestoreCluster 脚本](#)”

13.5.3 恢复 BI 内容

如果已将 Business Intelligence (BI) 内容备份到 LCMBIAR 文件，可以使用生命周期管理控制台恢复 BI 内容，而不必恢复整个系统。有关更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台生命周期管理控制台用户指南》。

13.6 BackupCluster 和 RestoreCluster 脚本

下表介绍了 BackupCluster 脚本使用的命令行参数。

注意：

该脚本只备份群集的服务器设置。其他数据必须另行备份。

表13-2: BackupCluster 参数

名称	说明	示例
-backup	用于备份要恢复的系统服务器设置的 BIAR 文件的名称和路径。	-backup "C:\Users\Administrator\Desktop\my.biar"
-cms	系统的中央管理服务器所在计算机的主机名。如果 CMS 在默认端口 6400 以外的其他端口上运行，还必须指定端口号。	-cms mycms:6400
-username	管理员帐户的用户名。	-username Administrator
-password	管理员帐户的密码。	-password Password1

下表介绍了 RestoreCluster 脚本使用的命令行参数。

表13-3: RestoreCluster 参数

名称	说明	示例
-restore	包含要恢复的服务器配置设置的 BIAR 文件的名称和路径。	-restore "C:\Users\Administrator\Desktop\my.biar"
-username	管理员帐户的用户名。	-username Administrator
-password	管理员帐户的密码。	-password Password1
-displaycontents	显示 BIAR 文件所含节点和服务器的列表。	-displaycontents "C:\Users\Administrator\Desktop\my.biar"

注意：

请使用 `-displaycontents` 参数运行 `RestoreCluster` 脚本，以便在恢复服务器设置前显示 BIAR 文件的内容。

如果备份未运行系统的服务器设置，或者恢复服务器设置，则以下参数是必需的。

表13-4：在采用临时 CMS 时使用的参数

名称	说明	示例
<code>-usetempcms</code>	为指定操作创建临时 CMS。操作完成后，将停止该临时 CMS。	<code>-usetempcms</code>
<code>-cmsport</code>	临时 CMS 的端口号。	<code>-cmsport 6700</code>
<code>-dbdriver</code>	<p>CMS 系统数据库的数据库驱动程序。接受的值包括：</p> <ul style="list-style-type: none"> • <code>db2databasesubsystem</code> • <code>maxdbdatabasesubsystem</code> • <code>mysqldatabasesubsystem</code> • <code>oracledatabasesubsystem</code> • <code>sqlserverdatabasesubsystem</code> • <code>sybasedatabasesubsystem</code> • <code>sqlanywheredatabasesubsystem</code> • <code>newdbdatabasesubsystem</code> <p>注意： <code>newdbdatabasesubsystem</code> 参数可用于 SAP HANA 数据库。</p>	<code>-dbdriver sqlserverdatabasesubsystem</code>
<code>-connect</code>	CMS 系统数据库连接字符串。	<code>-connect "DSN=BusinessObjects CMS 140;UID=username;PWD=Password1;HOST NAME=database;PORT=3306"</code>
<code>-dbkey</code>	群集密钥。	<code>-dbkey abc1234</code>

示例：

以下示例说明如何使用现有 CMS 将服务器设置备份到 BIAR 文件中。

```
-backup "C:\Users\Administrator\Desktop\my.biar"
-cms mycms:6400
-username Administrator
-password Password1
```

示例：

以下示例说明如何显示 BIAR 文件的内容。

```
-displaycontents "C:\Users\Administrator\Desktop\mybiar.biar"
```

示例：

以下示例说明如何从 BIAR 文件恢复设置。恢复服务器设置时，必须使用临时 CMS。

```
-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
```

第 14 章 复制 BI 平台部署

14.1 系统复制概述

本章介绍如何为测试、备用或其他目的创建 BI 平台部署的副本。

相关主题

- 第 462 页上的“[备份和恢复概览](#)”

14.2 术语

术语	定义
源系统	原始 BI 平台部署。
目标系统	要创建的新部署。
系统复制	针对现有 BI 平台部署创建副本的操作。
同质系统复制	创建复制系统（其中源系统与目标系统具有相同类型的操作系统和数据库）的操作。BI 平台只支持同质系统复制。
异质系统复制	创建复制系统（其中源系统与目标系统使用不同类型的操作系统或数据库，但基于相同的数据）的操作。
数据库复制	使用数据库供应商工具创建 CMS 系统或审核数据库的副本的操作。

14.3 系统复制的使用情况

下表介绍用户可能希望通过已有给定资源实现的目标，并引导用户使用最恰当的解决方案。

目标	所需资源	解决方案
<p>目标：相同复制</p> <p>我想为备用或测试目的创建一个具有相同硬件配置和 IP 地址/计算机名称的复制系统。</p>	<ul style="list-style-type: none"> 与源系统具有相同硬件的目标系统和 源系统的备份或对要从中创建备份的源系统的访问。 	<p>使用本指南中所详细说明了的系统备份和恢复工作流，请参阅第 466 页上的“备份整个系统”过程。从源系统的备份重新创建目标系统。</p>
<p>目标：复制</p> <p>我想为备用、测试或培训创建一个硬件及 IP 地址/计算机名称与源系统不同的重复系统。</p>	<ul style="list-style-type: none"> 源系统（运行中或已停止）或源系统数据库与文件的备份。 和 第 487 页上的“从源系统导出”中详细介绍的系统信息。 	<p>使用系统复制工作流，从第 485 页上的“计划复制系统”开始，并遵循本章其余部分的说明。</p> <p>注意： 可以在具有相同版本、支持包和修补程序级别的现有 BI 平台部署的计算机上创建目标系统，或在未安装 BI 平台的干净计算机上创建目标系统。</p>

相关主题

- 第 466 页上的[“备份”](#)
- 第 485 页上的[“计划复制系统”](#)

14.4 计划复制系统

一个系统副本不一定反映当前系统情况。可创建系统的一个副本并等待，然后继续在目标系统上重新创建副本，也可使用源系统的上一个备份作为目标系统的基础。这意味着副本代表着创建副本时的系统。例如，如果等待一个月，那么副本将重新创建一个月之前的系统。

在回顾了前一节中的使用案例并确定了最适合自己需求的情况后，应开发一个系统复制计划。

创建系统复制计划

计划复制系统时，应事先确定以下内容：

- 源系统是否在复制时停止或变为主动？（可在任一情况下完成该过程。）
 - 如果停止源系统，那么需要停机多长时间？
 - 计划测试时间以确保目标系统的完整性。
- 要使用哪些数据库工具进行数据库备份和恢复。
- 目标系统要部署在哪些计算机上，以及每个节点的承载位置。
- 要复制哪些可选组件。
- 要用于目标 CMS 数据库的数据库类型，以及要复制的任何其他可选数据库。

还应考虑以下内容：

- 源系统安装了哪些 BI 平台组件。可以使用安装程序的“添加/删除” > “修改”功能查看当前安装的组件列表。
- 如果在和源系统不同的硬件设置上安装目标系统，可能需要调整目标系统以获得更佳性能。有关如何提高系统性能的信息，请参阅《SAP BusinessObjects Business Intelligence sizing companion guide》（SAP BusinessObjects Business Intelligence 规模设置指南）。
- 可能希望目标系统根据源系统数据库之外的报表数据库制定报表。在这种情况下，用户需要更改报表数据库的数据库连接信息。为此，可以保留相同的 DSN 名称，但在目标系统上将 DSN 指向其他数据库。

所需的源系统组件

- CMS 系统数据库
- FRS 文件存储
- 语义层配置文件
- 审核数据库（可选）
- 监控数据库（可选）
- 生命周期管理子版本数据库（可选）

14.5 注意事项与限制

制作 BI 平台部署的副本时应注意以下事项。

方面	注意事项
SAP Business Warehouse 集成	如果在集成环境中使用 BI 平台和 SAP ERP 或 BW, 请在复制系统之前阅读 SAP 系统复制文档。系统复制指南位于 http://www.sdn.sap.com/irj/sdn/systemcopy (需要进行 SMP 登录)。选择 SAP NetWeaver 版本; 相关复制指南可在安装指南文件夹中查找。
程序版本	源系统和目标系统必须具有相同的版本、支持包和修补程序级别。
内容和配置设置	只能复制整个源系统; 不能选择性地复制内容或系统配置设置。
安装路径	源位置和目标位置中的安装路径必须相同: 例如, 如果源系统安装在 C:\SAP BusinessObjects Enterprise XI 4.0, 则目标系统也必须安装在 C:\SAP BusinessObjects Enterprise XI 4.0。
主机操作系统	源操作系统和目标操作系统必须相同。
CMS 数据库软件类型	CMS 源数据库和目标数据库必须为同一类型。在完成系统复制后, 便可以选择更改为支持的其他数据库类型。
审核数据库软件类型	如果复制审核数据, 则源审核数据库与目标审核数据库的类型必须相同。创建副本后, 可以建立一个不同类型的新数据库。 注意: 如果建立新数据库, 现有事件并不会复制到该数据库中, 而只有新事件将记录到新数据库中。
Web 层自定义	复制过程不会从源系统中复制 Web 层组件。如果自定义了 Web 层 (例如, 修改了 custom 文件夹中的 .properties 文件), 则必须将那些自定义手动应用到目标系统。
这些说明未涵盖的主题	此工作流不描述如何导出或导入数据库。请使用数据库供应商工具进行数据库复制与恢复。

在系统复制过程中, 将会复制以下数据:

- CMS 资源库数据库。(包含报表、分析、文件夹、权限、用户和用户组、服务器设置以及其他 BI 内容和系统内容)
- 审核数据库。(包含 BI 平台服务器或客户端应用程序触发的审核事件)
- 监控数据库。(包含来自量度、探测器和监测器的趋势数据)
- 生命周期管理数据库。(包含报表的不同版本、分析、其他 BI 资源以及版本信息)

注意:

有关数据库及其内容的说明, 请参阅本指南第 32 页上的 [“数据库”](#) 一节。

- 语义层配置文件

Web 层配置、搜索索引以及上面未明确提及的任何数据不会予以复制。

文件恢复副本的注意事项

如果是为了恢复被意外删除的文件这一特定目的而复制系统, 则还应注意以下事项:

使用备份在生产系统的第 491 页上的 [“导入一个目标系统”](#) 过程中执行这些步骤。

- 不要安装所有节点，而只安装将包含 CMS 及其数据库的第一个节点。
- 不要安装审核数据库、LCM 数据库或监控数据库。
- 不要重新创建指向审核数据库或报表数据库的连接。

使用 LCM 升级要从目标系统恢复到源系统的对象。

14.6 系统复制过程

以下过程将指导用户完成 BI 平台部署复制过程的两个阶段。

14.6.1 从源系统导出

需要记下源系统的以下信息。如果希望记下这些信息，可以使用位于第 989 页上的 [“系统复制工作表”](#) 的工作表。

属性	位置
CMS 群集密钥（请确保该记录的安全）。	安装 BI 平台时由系统管理员创建。
节点的名称。	转到 CMC 的“服务器”选项卡，在左侧树中展开“节点”。
部署中每台计算机的计算机名称和 BI 平台安装文件夹。	转到 CMC 的“服务器”选项卡，右键单击 CMS 并选择“占位符”。查看 %INSTALLROOTDIR% 占位符的值。
BI 平台管理员密码（请确保该记录的安全）。	安装 BI 平台时由系统管理员创建。

属性	位置
<p>CMS 可能使用的所有数据库连接，以及这些连接所关联的用户名和密码。如果要复制此信息，可能会包含审核数据库。请确保为群集中的所有计算机获取此信息。</p> <p>注意： 如果要复制审核数据库，还需要审核数据库连接名称和凭据。</p>	<p>转到 CMC 的“服务器”选项卡，右键单击 CMS 并选择“量度”。</p> <p>查看以下量度：</p> <ul style="list-style-type: none"> • 系统数据库连接名称 • 系统数据库服务器名称 • 系统数据库用户名 • 数据源名称 • 审核数据库连接名称（可选） • 审核数据库用户名（可选）
<p>对于群集中的每台计算机，任何其他数据库连接（例如，Universe 和报表所使用）的详细信息（客户端类型、版本）。请确保包含用户名和密码。</p>	<p>对于直接创建自数据库的 Crystal 报表，请使用 SAP Crystal Reports 2011 或 SAP Crystal Reports for Enterprise 设计器查看连接信息。对于 Universe 连接信息，请使用信息设计工具 (.unx) 或 Universe 设计工具 (.unv)。</p>
<p>源系统的版本、支持包和修补程序级别。</p>	<p>在 Windows 上，这可通过查看“删除或更改”程序工具来确定。</p> <p>在 Unix 上，可以使用 BI 平台安装目录中的 modifyOrRemoveProducts.sh 实用程序。</p>
<p>部署中每个输入 FRS 和输出 FRS 的文件存储位置。</p>	<p>转到 CMC 的“服务器”选项卡，右键单击输入或输出 FRS 并选择“属性”。查看“文件存储目录”属性。</p> <p>注意： 如果值以 % 开头，则这是一个占位符，需要单击“占位符”并记下该占位符下列出的目录。</p>

属性	位置
计划复制生命周期管理 (LCM) 时 LCM 数据库文件夹和 LCM 子版本文件夹的位置。	<p>Windows 安装中 LCM 数据库的默认文件夹为安装目录\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOVERRIDE, 在 Unix 上, 则为安装目录/sap_bobj/data/LCM/LCMOverride。</p> <p>Windows 安装中 LCM 子版本文件的默认位置为:</p> <ul style="list-style-type: none"> • 安装目录\SAP BusinessObjects Enterprise XI 4.0\CheckOut • 安装目录\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository <p>在 Unix 上, 此类位置则为:</p> <ul style="list-style-type: none"> • 安装目录/check_out (此目录只在使用子版本签出文件后创建)。 • \$HOME/LCM_Repository
如果计划复制监控数据库, 则监控数据库文件夹。	<p>这是在 CMC 中设置的。转到 CMC 的“应用程序”管理区域, 选择“监控应用程序” > “属性”并查看“趋势数据库备份目录”。</p> <p>Windows 安装中的默认文件夹为安装目录\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB, 在 Unix 上, 则为安装目录/sap_bobj/Data/TrendingDB。</p>
语义层文件夹路径。	<p>在 Windows 安装中, 默认文件夹路径为安装目录\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionsServer\。</p>

记录上述信息之后:

- 1 使用数据库供应商备份工具创建以下数据库的备份副本:
 - CMS 系统数据库
 - 审核数据库 (可选)
- 2 使用文件备份工具, 备份以下文件集合:
 - FRS 输入和输出文件存储。
 - 监控趋势数据库 (可选)。通过备份工作表上记录的监控文件夹中的文件可实现此操作。在 Windows 上, 该位置默认为: 安装目录\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB。在 Unix 上为: 安装目录/sap_bobj/Data/TrendingDB。
 - 生命周期管理数据库 (可选)。通过备份工作表上记录的数据库文件夹中的文件可实现此操作。在 Windows 上, 该位置默认为: 安装目录\SAP BusinessObjects Enterprise XI 4.0\Data\LCM\LCMOVERRIDE。在 Unix 上为: 安装目录/sap_bobj/data/LCM/LCMOverride。
 - 生命周期管理子版本数据库 (可选)。通过备份工作表上记录子版本文件夹中的文件可实现此操作。在 Windows 上, 此类位置默认为:

- 安装目录\SAP BusinessObjects Enterprise XI 4.0\CheckOut
- 安装目录\SAP BusinessObjects Enterprise XI 4.0\LCM_Repository。

而在 Unix 上, 这些位置为:

- 安装目录/check_out (此目录只在使用子版本签出文件后创建)。
- \$HOME/LCM_Repository
- 语义层文件夹中的配置文件: connectionServer 文件夹中的 cs.cfg 文件及其任何子文件夹中的任何 .sbo 和 .prm 文件。

注意:

有关此工作流的限制和详细说明, 请参阅第 467 页上的 [“热备份”](#) 一节。

- 3 用户可定制以下文件。如果已定制任何文件, 则应备份源系统中的文件, 然后将这些文件恢复到目标系统上的相同文件夹:
 - BO_trace.ini 安装到:
 - [安装目录]SAP BusinessObjects Enterprise XI 4.0/conf
 - clientSDKOptions.xml 安装到:
 - [安装目录]SAP BusinessObjects Enterprise XI 4.0/java/lib
 - [安装目录]SAP BusinessObjects Enterprise XI 4.0/win32_x86
 - [安装目录]SAP BusinessObjects Enterprise XI 4.0/win64_x64
 - CRConfig.xml 安装到:
 - [安装目录]SAP BusinessObjects Enterprise XI 4.0/java
 - mdas.properties 安装到:
 - [安装目录]/SAP BusinessObjects Enterprise XI 4.0/java/pjs/services/MDAS/resources/com/businessobjects/multidimensional/services
 - WDeploy 配置文件安装到 [安装目录]SAP BusinessObjects Enterprise XI 4.0/wdeploy/conf:
 - config.apache
 - config.jboss7
 - config.sapappsvr73
 - config.tomcat6
 - config.tomcat7
 - config.weblogic11
 - config.websphere7
 - config.websphere8
 - wdeploy.conf
- 4 用户可定制以下 Web 层文件。如果已更改其中任何文件, 则应备份源系统中的文件。之后, 需要恢复这些文件或将更改重新应用到目标系统。
 - BO_trace.ini 安装到:
 - [安装目录]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/BOE/WEB-INF/TraceLog
 - [安装目录]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/conf
 - clientaccesspolicy.xml 安装到:
 - [安装目录]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT

- clientSDKOptions.xml 安装到：
 - [安装目录]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/clientapi/WEB-INF/lib
 - [安装目录]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/dswsbobje/WEB-INF/lib
 - crossdomain.xml 安装到：
 - [安装目录]SAP BusinessObjects Enterprise XI 4.0/warfiles/webapps/ROOT
 - [安装目录]tomcat/webapps/ROOT
 - config/custom 文件夹（在 Web 层中）中的任何定制文件。备份这些文件，将定制传送到目标系统。
- 5 备份手动添加到源系统的任何自定义扩展；例如，发布扩展、自定义库等等。

将上面记录的信息与数据库和文件的副本放在一起。建议保留另一份副本，以便在将来的系统复制过程需要时进行更新。

14.6.2 导入一个目标系统

此过程假定已经创建了要在目标系统中使用的源部署数据库和系统文件的备份副本。所有备份文件都必须来自相同的备份集。还需要在“从源系统导出”中记下的详细信息（例如，群集密钥和数据库凭据）。

如果目标系统驻留在某个网络位置并可访问源系统的资源，则应确保目标系统在经过重新配置之前不会尝试访问这些资源。为此，可以在目标系统与源系统资源之间设置防火墙，或者在启动目标系统时使源系统处于停止状态。在首次启动目标系统之后，可以删除防火墙或启动源系统。

如果目标系统已经安装了 BI 平台，请确保其版本、支持包和修补程序级别与创建副本时的源系统相同。还要确保它使用与源系统相同的安装路径。

- 1 在目标系统上，创建指向要放置 CMS 资源库、审核数据库和报表数据库的一个或多个数据库的连接。

注意：

虽然连接可以指向不同的数据库，但它们必须具有与源系统相同的连接名称或 DSN，并使用与源系统相同的凭据。

- 2 使用数据库工具将 CMS 系统数据库和审核数据库（如果需要）从源系统备份恢复到目标数据库中。

如果目标系统上的 Universe 或报表需要使用不同的报表数据库，可修改数据库连接以指向该数据库。

如果需要有关此步骤的进一步说明，请参阅第 472 页上的 [“恢复系统”](#) 主题。

- 3 如果目标主机系统上安装了 BI 平台，请跳到步骤 4。如果未安装 BI 平台，则在目标主机系统上安装 BI 平台并牢记以下步骤：
 - a 安装与源系统相同的程序版本、支持包和修补程序级别。

- b 使用与源系统相同的安装路径。
- c 选择与源系统所安装的组件相同的组件。
- d 当安装程序提示创建 CMS 数据库（以及审核数据库，如果适用）时，选择“使用现有数据库”选项并输入在步骤 1 中设置的连接名称和凭据。

注意：

请不要选择重新初始化 CMS 数据库。

- e 当提示输入“节点名称”时，请使用与源系统相同的名称、端口号、平台管理员密码和群集密钥。
- 有关完整的安装说明，请参阅《SAP BusinessObjects Business Intelligence 平台安装指南》。当系统完成安装后，请转到步骤 6。

注意：

如果未从源系统复制审核数据，可以通过在安装过程中配置审核创建一个新审核数据库。

- f 在 CCM 中停止所有节点。
- 4 如果目标系统上已安装 BI 平台，请在 CCM 中停止所有节点。在目标系统 CMS 主机计算机上启动 CCM。
 - 5 如果已经安装了 BI 平台，则使用“重新创建节点”选项添加一个新节点。
 - a 使用来自源系统的“节点名称”和“SIA 端口号”。
 - b 选择“启动新的临时 CMS”。
 - c 选择一个新的“CMS 端口号”（可以是任何空闲端口）和“CMS 数据库类型”（与所恢复的数据库类型相匹配）。
 - d 输入步骤 1 中 CMS 数据库所恢复到的连接的详细信息。
 - e 输入来自源系统的群集密钥。
 - f 输入来自源系统的管理员密码。
 - 6 将输入和输出 FRS 文件存储恢复到目标系统文件存储中。使用源系统上使用的相同文件夹。
 - 7 将监控数据库文件夹（如果希望复制监控信息）恢复到源系统上使用的相同文件夹。
 - 8 将 LCM 数据库文件夹（如果希望复制 LCM 信息）恢复到源系统上使用的相同文件夹。
 - 9 将 LCM 子版本文件（如果希望复制 LCM 信息）恢复到源系统上使用的相同文件夹。
 - 10 将语义层/连接配置服务器文件恢复到源系统上使用的相同文件夹。
 - 11 重新启动目标系统主机计算机。
 - 12 如果在步骤 3 中在目标系统上安装了 BI 平台，请应用匹配源系统所需的任何支持包或修补程序。
 - 13 如果目标系统要在多台主机计算机上运行，请为每台主机计算机重复步骤 1 - 11。
请在安装附加 BI 平台节点时使用“扩展安装”选项，并切记应当为目标系统中的附加节点使用与源系统相同的节点名称。
 - 14 如果目标系统 CMS 数据库要使用与源系统不同的数据库类型，请使用 CCM 执行第 419 页上的[“将数据从一个 CMS 系统数据库复制到另一个系统数据库”](#)，并指定要用于副本的数据库作为目标。
 - 15 恢复在程序“从源系统中导出”第 3 步中备份的全部用户可定制文件。
 - 16 恢复在程序“从源系统中导出”第 4 步中备份的全部用户可定制文件。

“Web 层”指用户可执行定制的 WDeploy 阶段区域，以及部署到应用程序服务器的 Web 层内容。

将更改应用到目标系统时，不要将更改应用到应用程序服务器目录；将更改应用到 WDeploy 阶段区域，然后使用 WDeploy 将 Web 层重新部署到应用程序服务器。

WDeploy 阶段区域在 Windows 上的位置如下：安装目录/SAP BusinessObjects Enterprise XI 4.0/warfiles。

17. 恢复在程序“从源系统中导出”第 5 步中备份的全部扩展。

执行 BI 平台的系统复制后：

1. 目标上第一个节点的安装将创建一个临时 CMS，它会在安装结束时停止运行。请使用 CMC，转到“服务器”页面并删除此 CMS。

记忆：

如果不移除源系统，或要与目标系统同时使用，建议在目标系统上重新命名相应群集。

2. 在目标 CMS 数据库上运行 Repository Diagnostic Tool。
3. 适用情况下，在目标系统上配置 Windows AD 单一登录（SSO）。请参阅第 263 页上的[“BI 平台 AD 身份验证 SSO”](#)。
4. 适用情况下，在目标系统上配置 SLD。有关详细信息，请参阅 SAP 注释 1508421：“SAP SLD Data Supplier for Apache Tomcat”（针对 Apache Tomcat 的 SAP SLD 数据提供者）。
5. 对目标系统执行健全性检查以确保其完整性。
6. 执行一次充分的重建索引。

第 15 章 版本管理

15.1 管理 BI 资源的不同版本

升级管理应用程序可用于管理 BI 平台资源库中 BI 资源的不同版本。该工具包含 Subversion 和 ClearCase 两个版本控制系统，方便用户进行维护操作。

要管理作业或 InfoObject 的不同版本，请执行以下步骤：

1. 登录 CMC 应用程序并选择“版本管理”。
2. 从“版本管理”窗口的左面板中选择文件夹，以查看要对其版本进行管理的作业或 InfoObject。
3. 选择 InfoObject，然后单击“添加到 VM”。

注意：

单击“添加到 VM”后，即会在版本管理系统（VMS）资源库中创建该对象的基础版本。对于后续的签入操作，基础版本是必需的。


4. 对于文档的后续更改，要确定以递增方式更改的文档的版本，请单击“签入”。这将更新 VMS 资源库中的文档。

将出现“签入注释”对话框。

5. 输入注释，然后单击“确定”。
选定 InfoObject 的版本号变更会显示在版本管理系统列和内容管理系统列中。
6. 要从 VMS 获取文档的最新版本，请选择所需的 InfoObject，然后单击“获取最新版本”。
VMS 资源库中的最新版本将导入 CMS。
7. 要创建最新版本的副本，则单击“创建副本”。
VMS 资源库中将创建所选版本的副本。
8. 选择“历史记录”可查看选定 InfoObject 的所有可用版本。

将出现“历史记录”窗口。将显示以下选项：

- 获取版本 — 如果存在多个版本，且需要使用 BI 资源的某一特定版本，则可以选择所需的 InfoObject 并单击“获取版本”。
- 获取版本副本 — 通过此选项可获取选定版本的副本。
- 导出版本副本 — 通过此选项可获取选定版本的副本并将其保存到本地系统。

- 比较 — 通过此选项可比较作业的两个版本的元数据信息。有关更多信息，请参阅“比较同一作业的不同版本”。
- 9 选择一个 InfoObject，并单击“锁定”以锁定该 InfoObject，或单击“解锁”以取消锁定 InfoObject，或者单击“删除”以删除 VMS 资源库中的所有内容版本。CMS 中的内容不受影响。
注意：
 如果锁定某一 InfoObject，则无法对该 InfoObject 执行任何操作。
 10. 当 CMS 中的版本新于 VMS 中的版本时，更新的 InfoObject 旁边会显示一个指示符。将光标置于该指示符之上时，将显示工具提示，指明 CMS 中的 InfoObject 已更新。
 11. 要查看 VMS 中存在但 CMS 中不存在的所有已签入资源的列表，请单击“查看已删除的资源”。单击任意已删除的资源，以查看该资源的历史记录。可以选择某个已删除的资源，然后单击“获取版本”以查看该资源的特定版本。可以单击“获取版本副本”来获取选定资源的副本。
 单击“删除”会同时从 VMS 资源库中永久删除对象。
注意：
 如果使用“获取版本”或“获取版本副本”，则资源将从 VMS 缺失文件列表移动到 CMS 中。
 12. 选择某个 InfoObject，然后单击  查看该 InfoObject 的属性。或者，可以右击 InfoObject 并执行步骤 4 至 16。

15.2 使用版本管理设置选项

可以通过中央管理控制台设置版本管理系统设置。用户可以配置 Subversion 和 ClearCase 参数。

要设置 Subversion 管理系统，请执行以下步骤：

- 1 在 CMC 主页中选择“应用程序”。
- 2 双击“VMS”。将出现“版本管理设置”屏幕。
- 3 选择“VMS 设置”。
- 4 从“版本管理系统”下拉列表中，选择“Subversion”。
 在升级管理工具安装过程中提供的服务器端口号、密码、资源库名称、服务器名称、用户名、工作区目录名称和安装目录名称将显示在相应的字段中。
- 5 如有必要，可修改这些字段。
 请确保所输入的安装路径一直扩展到 .exe 文件所在的目录级别。在 Windows 上为：安装目录\SAP BusinessObjects Enterprise XI 4.0\subversion；在 Unix 上为：安装目录/sap_bobj/enterprise_40/subversion/bin
- 6 可通过分别单击“http”或“svn”单选按钮，使用 http 或 svn 协议访问 Subversion 资源库。
- 7 可以通过单击“测试 VMS”验证所输入的 VMS 设置。
- 8 单击“保存”。

注意：

- 如果想要将 Subversion 用作默认 VMS，则选择“用作默认 VMS”。
- 如果已按照步骤 3 修改字段，请重新启动服务器智能代理。

15.2.1 在 Windows 上设置 ClearCase 版本管理系统

要在 Windows 上设置 ClearCase 版本管理系统，请执行以下步骤：

- 1 在“管理选项”窗口中，单击“VMS 设置”。
- 2 从“版本管理系统”下拉列表中，选择“ClearCase”。
- 3 输入以下详细信息：
 - ClearCase 映射驱动器 — 输入驱动器名称。默认为驱动器 M。例如：M:
 - VOB 标记名 — 输入版本化对象库（VOB）的名称。例如：FridayVB
 - 查看存储目录 — 输入共享文件夹的路径。例如：\\HostName\FolderName

注意：

主机名不能写为 localhost。

- 4 单击“保存”。

15.2.2 在 Unix 上设置 ClearCase 版本管理系统

要在 Unix 系统中设置 ClearCase 版本管理系统，请执行以下步骤：

- 1 在“管理选项”窗口中，单击“VMS 设置”。
- 2 在“版本管理系统”下拉列表中，选择“ClearCase”。
- 3 输入以下详细信息：
 - ClearCase 映射驱动器 — 输入 MVFS 所在文件夹的名称。默认为 /view
 - VOB 标记名 — 输入 VOB 名称以及 VOB 所在的文件夹。例如：VobFolder/VobName
 - 查看存储目录：输入创建视图所在目录的路径。

如果要将 ClearCase 用作默认版本管理系统，可选择“用作默认 VMS”。

15.3 比较同一作业的不同版本

可以通过以下步骤查看同一作业的两个版本之间的差异：

- 1 登录到 CMC 应用程序。
- 2 在 CMC 主页中，选择“版本管理”。
- 3 在“版本管理”屏幕中，选择需要比较版本的 InfoObject。
- 4 单击“历史记录”。
- 将出现“历史记录”页面，其中显示了所选 InfoObject 的所有版本。
- 5 选择任意两个版本进行比较。
- 6 单击“比较”。
- 比较过程随即开始，并且将以橙色突出显示差异，而缺少的对象则以红色突出显示。
- 7 单击“保存”，以保存差异报告。

15.4 升级 Subversion 内容

如果具有使用以前版本的 BI 平台创建的旧 Subversion 内容，可通过以下步骤将内容升级为最新版本：

- 1 登录到 SAP BusinessObjects Enterprise 3.x 计算机上的 VMS。
- 2 签入任何对象。例如，签入 Administrator 和 Guest 对象两次。
- 3 在 CMC 中，单击“用户”并验证 VMS 和 CMS 版本号中显示的是 2。
- 4 从 VMS 注销。
- 5 转到命令提示符，导航到 C:\Program Files\Subversion\bin，并运行导出命令：`svnadmin dump c:/LCM_repository/svn_repository > dumrepo`
- 6 将 dumrepo 文件复制到 BI 平台所在的计算机上
- 7 转到 BI 平台所在计算机上的命令提示符，导航到 C:\Program Files (x86)\SAP，并执行以下命令：
`svnadmin.exe load "C:/Program Files (x86)/SAP BusinessObjects/SAPBusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository" < c:/dumrepo`
`svnadmin.exe upgrade "C:/Program Files (x86)/SAP BusinessObjects/SAP BusinessObjects Enterprise XI 4.0/LCM_repository/svn_repository"`
- 8 命令成功执行后，重新启动 SIA。
- 9 登录到 CMC 并单击“版本管理”。
- 10 单击“用户”，并验证 VMS 版本为 2。
- 11 选择 Administrator 对象并单击“获取最新版本”。
- 12 现在，VMS 和 CMS 上便具有相同版本了。

第 16 章 升级管理

16.1 欢迎使用升级管理

16.1.1 概述

升级管理应用程序可用于在各个资源库之间移动商务智能（BI）资源，管理资源的依赖项以及回滚目标系统的已升级资源（如果需要）。它还支持对同一 BI 资源的不同版本进行管理。

升级管理应用程序与中央管理控制台相集成。仅当源系统和目标系统上安装了相同版本的 BI 平台时，才能将 BI 资源从一个系统升级到另一个系统。

16.1.2 功能

升级管理应用程序支持以下功能：

- 升级 — 此功能用于在目标系统中创建或更新 InfoObject。除升级 InfoObject 以外，通过该功能还可执行以下任务：
 - 创建新作业
 - 复制现有作业
 - 编辑作业
 - 计划作业升级
 - 查看作业的历史记录

- 导出为 LCMBIAR
- 导入 BIAR/LCMBIAR
- 管理依赖项 — 此功能用于选择、过滤和管理要升级的作业中 InfoObject 的依赖项。
- 计划 — 此功能用于为作业升级指定一个时间，而不是作业一经创建就立即升级。可使用以下任一参数为作业升级指定时间：每小时、每天、每周或每月。
- 安全设置 — 此功能用于升级 InfoObject 及其关联的安全权限，如有必要，也可以升级与应用程序权限关联的 InfoObject。
- 测试升级 — 此功能用于检查或测试升级，以便确保在实际升级 InfoObject 之前执行了所有的预防性措施。
- 回滚 — 此功能用于在作业升级后将目标系统恢复到其先前状态。可对整个作业或作业的一部分进行回滚。
- 审核 — 升级管理工具生成的事件存储在审核数据库中。通过审核功能可以监控审核数据库中记录的事件。
- LCM 覆盖设置 — 此功能可通过作业升级来扫描和升级覆盖。

16.1.3 应用程序访问权限

本节介绍升级管理应用程序的应用程序访问权限。

- 可在 CMC 中设置对升级管理应用程序的访问权限。
- 可设置对升级管理应用程序中各种功能的应用程序粒度权限。

要在升级管理应用程序中设置特定权限，请执行以下步骤：

- 1 登录到 CMC，并选择“应用程序”。
- 2 双击“升级管理”。
- 3 单击“用户安全性”并选择用户。可以查看或为用户分配安全权限。
- 4 提供以下升级管理特定权限：
 - 允许访问以编辑覆盖
 - 允许访问以包含安全
 - 允许访问 LCM 管理
 - 允许访问以管理依赖项
 - 创建作业
 - 删除作业
 - 编辑作业
 - 编辑 LCMBIAR
 - 导出为 LCMBIAR
 - 导入 LCMBIAR
 - 升级作业
 - 回滚作业

- 查看并选择 BOMM (BusinessObjects 元数据) 对象
 - 查看并选择业务视图
 - 查看并选择日历
 - 查看并选择连接
 - 查看并选择配置文件
 - 查看并选择 QaaWS
 - 查看并选择报表对象
 - 查看并选择安全设置
 - 查看并选择 Universe
- 。 5 如果希望为选定用户分配权限，请选择相应权限并单击“指定安全性”。

升级管理应用程序访问权限即在 CMC 中设置完毕。

16.1.4 升级管理中的 WinAD 支持

为使升级管理应用程序正常工作，必须将以下内容添加到所有自适应作业服务器的所有 `javaargs` 参数中：

```
Djava.security.auth.login.config=<path>\bsclogin.conf,Djava.security.krb5.conf=<path>\krb5.ini
```

记忆：

在部署上指定到 `bsclogin.conf` 和 `krb5.ini` 的正确路径。

16.2 升级管理工具入门

16.2.1 访问升级管理应用程序

要访问升级管理应用程序，请在 CMC 主页中选择“升级管理”。

只要用户具有“升级作业”文件夹的查看权限，就可以启动升级管理应用程序。但是，要创建、计划或升级作业，用户必须由管理员授予额外的权限。

16. 2. 2 用户界面组件


本章介绍升级管理工具中的 GUI 组件。

- 升级管理工作区工具栏
- 工作区面板
- 树面板
- 详细信息面板
- 信息对象列表和作业查看器页面

升级管理工作区工具栏

下表列出了升级管理工作区工具栏中包含的选项，并介绍使用这些选项可执行的任务：

选项	说明
	用于创建新文件夹。新文件夹将创建为“升级作业”文件夹中的子文件夹。
	用于从选定作业或文件夹的当前位置复制和删除该作业或文件夹。
	用于从作业或文件夹的当前位置复制该作业或文件夹。
	用于将复制的作业或文件夹粘贴到新位置。
	用于删除现有作业。
	用于刷新主页，以获取可进行升级的作业或文件夹的更新列表。
属性	用于修改选定作业的属性。可以修改选定作业的标题、说明和关键字。
历史记录	用于查看选定作业的历史记录。
新建作业	用于创建新作业。
导入	用于导入 BIAR 文件或覆盖文件。
编辑	用于编辑选定作业。

选项	说明
升级	用于升级选定作业。
回滚	用于从目标系统中检索已升级的作业。
	用于在作业列表的各页面之间导航。可以使用此选项导航单个页面，或输入相应的页码来导航至特定页面。
搜索	用于搜索特定作业。可以按作业的名称、关键字、说明或所有这三个参数来搜索作业。
升级作业	用于查看已升级的作业。
升级状态	根据已升级作业的状态（例如成功、失败或部分成功）显示这些作业。

工作区面板

升级管理主页中的“工作区”面板显示新建作业的列表。可以使用此面板查看作业名称、作业状态、作业创建信息、升级摘要、测试升级摘要、依赖项管理屏幕和目标系统的相关信息。

树面板

升级管理主页中的树面板显示树结构，其中包括“升级作业”文件夹和“升级状态”文件夹。新建的作业显示在“升级作业”文件夹下的层次结构中。“升级状态”文件夹根据已升级作业的状态显示这些作业。

详细信息面板

此面板还包括“首选项”链接，管理员和用户可通过该链接设置工具首选项。“帮助”和“关于”链接可用于获取有关使用升级管理工具的更多信息。

信息对象列表和作业查看器页面

信息对象列表是动态生成的树列表，包含要升级的 InfoObject 的列表。它还将 InfoObject 分类为用户组、Universe、连接等等。作业查看器页面用于查看已添加到作业中的 InfoObject。

16.2.3 使用“设置”选项

“设置”选项使用户可以在将 InfoObject 从一个 BI 平台部署升级至另一个 BI 平台部署和 SAP 部署之前，配置设置。本节介绍如何使用设置选项。

在“升级作业”屏幕中单击“设置”下拉菜单。此下拉菜单将显示以下选项：

- 管理系统 — 此选项可用于添加升级管理活动所需的所有系统。

- 回滚设置 — 此选项可用于选择为其启用回滚的系统。
- 作业设置 — 此选项可用于选择在“依赖项”页面中查看完整的实例。还可用于管理作业实例清除活动。
- CTS 设置 — 此选项可用于为增强变更和传输系统（CTS+）集成添加 Web 服务和 SAP BW 系统信息。
- LCM 覆盖设置 — 此选项可用于为 Crystal Reports 和 Universe 连接扫描、升级和编辑数据库连接信息。还可以在这里编辑 QAANA URL。

16.2.3.1 使用“管理系统”选项

本节介绍如何使用“管理系统”选项。此选项可用于添加或删除主机系统。

要添加主机系统，请执行以下步骤：

- 1 在“管理选项”窗口中，单击“管理系统”选项。
将出现“管理系统”窗口。此窗口显示主机名、端口号、显示名称和说明的列表。
- 2 单击“添加”。
将出现“添加系统”对话框。
- 3 在相应字段中添加主机名、端口号、显示名称和说明。
注意：
选择“标记为来源”选项将系统标识为源系统，即连接信息所来自的系统。
- 4 单击“确定”，以添加该系统。
主机系统即被添加到列表中。

注意：

要删除主机系统，请选择要删除的主机系统，然后单击“删除”。

相关主题

- 第 503 页上的[“使用“回滚设置”选项”](#)
- 第 504 页上的[“使用“作业设置”选项”](#)

16.2.3.2 使用“回滚设置”选项

默认情况下，在系统级别启用回滚过程。通过“回滚设置”选项可在系统级别禁用回滚过程。

要在系统级别禁用回滚过程，请执行以下步骤：

- 。 1 在“回滚”窗口中的主机系统列表内，选择要用于禁用回滚进程的主机系统。
- 。 2 单击“保存并关闭”以保存修改。

相关主题

- 第 504 页上的[“使用“作业设置”选项”](#)

16.2.3.3 使用“作业设置”选项

通过“作业设置”选项可指定系统中能够存在的作业实例数量。可以指定以下选项之一：

- 作业实例数超过 N 时删除作业实例 — 此选项可用于指定系统中可存在的每个作业的最大作业实例数。
- 删除生成于 N 天前的作业实例 — 此选项可用于指定必须删除指定天数之前创建的所有作业实例。

从“显示创建的作业”下拉列表中，选择时间间隔，以查看在指定期间创建的作业。

要设置“作业设置”选项，请执行以下步骤：

- 。 1 选择该选项，然后输入首选值。
- 。 2 单击“保存”以保存更新后的更改。

可以单击“默认设置”来设置默认值，然后可单击“关闭”以关闭窗口。

注意：

仅当下次执行该作业时才会删除原有的作业实例。

相关主题

- 第 495 页上的[“使用版本管理设置选项”](#)

16.2.3.4 使用“LCM 覆盖设置”选项

“LCM 覆盖设置”选项可用于通过作业升级或 BIAR 文件来升级覆盖。

注意：

- 下列步骤中将使用术语“系统”。有三种类型的系统：
 - 来源：这是源系统，作为任何连接信息的原始系统。
 - 中央 LCM：这是默认要连接的系统。
 - 目标：这是 BI 资源升级到的最终系统。
- 从 BI 平台 4.0 SP4 版本起，覆盖数据存储在运行 PJS 服务的计算机上创建的本地中心数据库中。为防止维护多个数据库产生重复数据输入和不一致的覆盖数据，可以为所有 PJS 服务器的覆盖数据库设置一个单独位置。在 CMC 的“应用程序”页面中，右键单击“升级管理”并选择“LCM 覆盖设置”。显示承载 LCM 服务的所有 PJS 服务器的列表时，确保所有目录都指向相同位置。

16.2.3.4.1 升级覆盖

升级覆盖之前添加主机系统。有关添加主机系统的信息，请参见第 503 页上的 [“使用“管理系统”选项”](#)。

要升级覆盖，请执行以下步骤：

- 1 在“管理选项”窗口中，单击“覆盖设置”选项。
将出现“覆盖设置”窗口。
- 2 如果登录到中央升级管理系统，请从该系统中注销。
- 3 单击“登录”以连接到“来源”系统。
将出现“登录到系统”窗口。
- 4 选择标记为“来源”的源系统以扫描对象，并使用有效凭据登录到该系统。
- 5 从“扫描”旁边的“开始”下拉列表中，选择“开始”选项。
开始扫描过程。将显示“list of unique connections”（唯一连接列表）。

注意：

要计划扫描以适合您的首选项，请从下拉列表中选择“重复发生设置”选项。

- 6 在覆盖列表中，将要升级的对象的状态更改为“活动”，并单击“保存”。
- 7 单击“升级覆盖”。
将在显示目标系统列表的地方出现“升级覆盖”屏幕。
- 8 单击“登录”，以使用有效凭证登录到目标系统。
您可以指定多个目标系统。
- 9 单击“升级”。
即可完成覆盖的升级。

注意：

如果在 InfoObject 升级过程中目标系统覆盖失败，系统会将作业状态设置为“部分成功”，并为对象设置“覆盖失败”警告状态。

10. 从“来源”系统注销。
11. 从“覆盖设置”屏幕，单击“登录”。
将出现“登录到系统”窗口。
12. 使用有效凭据登录到其中一个目标系统。
所有升级对象列表显示在“覆盖列表”。这些对象的状态为“不活动”。
13. 为要编辑的对象单击“选择”复选框，并单击“编辑”。
14. 更新所需值，并单击“完成”。
15. 将对象的状态更改为“活动”，并单击“保存”。

16.2.3.4.2 使用 BIAR 文件升级覆盖

升级覆盖之前添加主机系统。有关添加主机系统的信息，请参见第 503 页上的 [“使用“管理系统”选项”](#)。

要通过 BIAR 文件升级覆盖，请执行以下步骤：

1. 在“管理选项”窗口中，单击“覆盖设置”选项。
将出现“覆盖设置”窗口。
2. 如果登录到中央 LCM 系统，请从该系统中注销。
3. 单击“登录”以连接到“来源”系统。
将出现“登录到系统”窗口。
4. 在“覆盖设置”屏幕中，选择标记为“来源”的源系统以扫描对象，并使用有效凭据登录到系统。
5. 从“扫描”旁边的“开始”下拉列表中，选择“开始”选项。
扫描进程开始。显示覆盖列表。

注意：

要计划扫描以适合您的首选项，请从下拉列表中选择“重复发生设置”选项。

6. 在覆盖列表中，将所需对象的状态更改为“活动”，并单击“保存”。
7. 单击“升级覆盖”。
将在显示目标系统列表的地方出现“升级覆盖”屏幕。
8. 要使用密码加密 BIAR 文件，单击“密码加密”复选框。
“密码”和“确认密码”字段启用。

9. 在“密码”字段中输入密码。在“确认密码”字段中重新输入相同密码。
10. 单击“导出”，并将覆盖 BIAR 文件保存到文件系统。
11. 通过 LCM 工具登录到目标系统，并单击“导入” > “覆盖文件”。
将出现“导入 LCMBIAR 文件”窗口。
12. 单击“浏览”浏览 BIAR 文件。
13. 在“密码”字段中输入 BIAR 文件的密码。

注意：

只有当您所选的 BIAR 文件使用了密码加密时，才会显示“密码”字段

14. 单击“确定”。即可完成覆盖的升级。
15. 从来源系统注销。
16. 从“覆盖设置”屏幕，单击“登录”。
将出现“登录到系统”窗口。
17. 使用有效凭据登录到目标系统。
导入的对象列表显示在“覆盖列表”中。这些对象的状态为“不活动”。
18. 为要编辑的对象单击“选择”复选框，并单击“编辑”。所编辑的对象将由一个图标表示。

注意：

单击图标可删除覆盖对象。

19. 更新所需值，并单击“完成”。
20. 将对象的状态更改为“活动”，并单击“保存”。

16.2.3.4.3 使用 CTS+ 升级覆盖

升级覆盖之前添加主机系统。有关添加主机系统的信息，请参见第 503 页上的 [“使用“管理系统”选项”](#)。

要通过 CTS+ 升级覆盖，请完成以下步骤：

注意：

使用 SAP 身份验证启动升级管理工具，以便可以使此选项。

1. 在“管理选项”窗口中，单击“覆盖设置”选项。
将出现“覆盖设置”窗口。
2. 如果登录到中央 LCM 系统，请从该系统中注销。
3. 单击“登录”以连接到“来源”系统。
将出现“登录到系统”窗口。

- 4 选择标记为“来源”的源系统以扫描对象，并使用有效凭据登录到该系统。
- 5 从“扫描”旁边的“开始”下拉列表中，选择“开始”选项。
开始扫描过程。将显示“覆盖列表”。

注意：

要计划扫描以适合您的首选项，请从下拉列表中选择“重复发生设置”选项。

- 6 在覆盖列表中，将要升级的对象的状态更改为“活动”，并单击“保存”。
- 7 单击“升级覆盖”。
将在显示目标系统列表的地方出现“升级覆盖”屏幕。
- 8 从“升级选项”下拉列表中，选择“使用 CTS+ 升级”。
- 9 单击“升级”。
10. 通过完成以下步骤将覆盖释放到目标系统：
 - a 登录 CTS+ 的域控制器并打开“传输组织器” Web UI。有关使用传输组织器 Web UI 的更多信息，请参阅http://help.sap.com/saphelp_nw70ehp1/helpdata/en/b5/6d03660d3745938cd46d6f5f9cef2e/frameset.htm。
 - b 如果请求状态为“Modifiable”（可修改），则请单击“释放”，以释放覆盖的传输请求。有关释放非 ABAP 对象的传输请求的更多信息，请参阅http://help.sap.com/saphelp_nw70ehp1/helpdata/en/55/07c497db8140ef8176715d4728eec1/frameset.htm。
 - c 关闭“传输组织器” Web UI。
11. 通过完成以下步骤将覆盖导入目标系统：
 - a 登录到 CTS+ 的域控制器。
 - b 调用 STMS 事务，进入传输管理系统。
 - c 单击“导入概览”图标。
将出现“导入概览”屏幕，可查看来自所有系统的导入队列项目。
 - d 单击目标 LCM 系统的系统 ID。
可以看到可被导入到系统的传输请求列表。
 - e 单击“刷新”。
 - f 导入相关传输请求。有关更多信息，请参阅http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a39e7acc11d1899e0000e829fbbd/frameset.htm
12. 即可完成覆盖的升级。
13. 使用有效凭据登录到其中一个目标系统。
所有已升级对象的列表将显示在“覆盖列表”中。这些对象的状态为“不活动”。
14. 为要编辑的对象单击“选择”复选框，并单击“编辑”。
15. 更新所需值，并单击“完成”。
16. 将对象的状态更改为“活动”，并单击“保存”。

16.2.3.5 使用 CTS 设置选项

可以使用此选项向自己的架构中添加 Web 服务并管理 BW 系统。有关使用 CTS 设置选项以及设置 CTS 以用于升级管理应用程序的更多信息，请参阅第 540 页上的 [“在升级管理工具中配置 CTS+ 设置”](#) 一节。

16.3 使用升级管理工具

启动升级管理应用程序时，默认情况下，用户将进入“升级作业”页面。

“升级作业”主页屏幕包含各种用于执行以下任务的选项卡：

- 选择“新建作业”以选择与作业相关的过程。还可以右击主页屏幕，然后从列表中选择与作业相关的过程。
- 选择“导入” > “导入文件”直接从文件系统导入 BIAR 文件或 LCMBIAR，而不是执行创建新作业的整个过程。
- 选择“导入” > “覆盖文件”以导入覆盖文件。
- 选择“编辑”以编辑现有作业。
- 选择“升级”以将作业从源系统升级到目标系统，或将作业导出到 BIAR 文件。
- 选择“回滚”以从目标系统恢复已升级的作业。
- 选择“历史记录”以查看作业的先前升级实例。
- 选择“属性”以查看选定作业实例的属性，例如标题、ID、文件名、说明等等。

“升级作业”应用程序区域显示系统中存在的作业的列表，以及各个作业的以下信息：

- 名称：显示已创建作业的名称。
- 状态：显示作业的状态，如已创建、成功、部分成功、正在运行或失败。
- 创建时间：显示作业的创建日期和时间。
 - 上次运行时间：显示上次升级作业的日期和时间。
 - 源系统：显示将从中升级作业的系统的名称。
 - 目标系统：显示作业将升级到的系统的名称。
- 创建者：显示创建特定作业的用户名称。

注意：

升级管理应用程序使用 SAP BusinessObjects Business Intelligence 平台 SDK 完成所有活动。


16.3.1 创建和删除文件夹

本节介绍如何在升级作业主页中创建和删除文件夹。

16.3.1.1 创建文件夹

本节介绍如何创建文件夹。

要创建文件夹，请执行以下步骤：

- 。 1 在升级管理工具栏中，单击 。
- 。 2 在“创建文件夹”对话框中，输入文件夹名称。
- 。 3 单击“确定”。

新文件夹即被创建。


相关主题

- 第 511 页上的[“创建作业”](#)
- 第 510 页上的[“删除文件夹”](#)

16.3.1.2 删除文件夹

本节介绍如何删除文件夹。

要删除文件夹，请执行以下步骤：

- 。 1 在“升级作业”主页中选择一个文件夹或作业。
- 。 2 单击 。

将出现“删除”对话框。

- 。 3 单击“确定”。

选定文件夹即被删除。

相关主题

- 第 511 页上的[“创建作业”](#)

16.3.2 创建作业

本节介绍如何使用升级管理工具创建新作业。

下表阐述可用于创建新作业的 GUI 元素和字段：

字段	说明
名称	待创建作业的名称。
说明	待创建作业的说明。
关键字	待创建作业的内容关键字。
作业保存于	显示默认选定的文件夹。
源系统	要从中升级作业的 BI 平台系统的名称。
目标系统	要将作业升级到的 BI 平台系统的名称。
用户名	登录源系统或目标系统时必须使用的登录 ID。
密码	登录源系统或目标系统时必须使用的密码。
身份验证	登录源系统或目标系统时使用的身份验证类型。 升级管理工具支持以下身份验证类型： <ul style="list-style-type: none"> • Enterprise • Windows AD • LDAP • SAP

注意：

在创建作业之前，请确保已经在目标系统中编辑和更新了覆盖（如果有），以便自动更新 BI 平台内容。有关更多信息，请参见“使用‘覆盖设置’选项”。

要使用升级管理工具创建新作业，请执行以下步骤：

- 1 启动升级管理工具。
- 2 在“升级作业”主页中，单击“新建作业”选项卡。
- 3 在相应字段中输入作业的名称、说明和关键字。

注意：

“说明”、“关键字”和“目标系统”字段是非必填字段。

- 。 4 在“作业保存于”字段中，浏览并选择要保存作业的文件夹。

注意：

默认情况下，在单击“新建作业”之前，“作业保存于”字段将填充文件夹窗格中突出显示的文件夹的名称。

- 。 5 从“选择依赖项”下拉列表中选择选项以将依赖项添加到作业。必须明确选择要升级的依赖项。例如，如果从“选择依赖项”下拉列表中选择“所有 Universe”，则会显示依赖项列表中包含的所有 Universe。然后可以逐个选择依赖项。
- 。 6 从各自的下拉列表中选择源系统和目标系统。

如果系统名称未包含在下拉列表中，则单击“登录到新 CMS”选项。将启动一个新窗口。输入系统名称以及用户名和密码。

- 。 7 单击“创建”。

新建作业存储于源系统的 CMS 资源库中。

注意：

如果创建的作业以文件夹作为主对象并且是重复性作业，该作业将在下一次运行时包含添加到文件夹的任何内容。

相关主题

- 第 504 页上的[“使用“LCM 覆盖设置”选项”](#)

16.3.2.1 登录新 CMS

本节介绍如何登录到新 CMS。

要登录到新 CMS，请执行以下步骤：

- 1 启动升级管理应用程序。
- 2 创建新作业。
有关创建新作业的更多信息，请参阅第 511 页上的[“创建作业”](#)。
- 3 从“源系统”下拉列表中选择“登录到新 CMS”。
将出现“登录到系统”对话框。
- 4 输入用户凭据，选择相应的身份验证类型，然后单击“登录”。
- 5 从“目标系统”下拉列表中选择“登录到新 CMS”。
- 6 输入用户凭据，选择相应的身份验证类型，然后单击“登录”。

相关主题

- 第 514 页上的[“编辑作业”](#)

- 第 514 页上的[“将 Infoobject 添加到作业中”](#)
- 第 517 页上的[“资源库连接时升级作业”](#)
- 第 521 页上的[“计划作业升级”](#)

16.3.3 通过复制现有作业来创建新作业

本节介绍如何通过复制现有作业来创建新作业。

要通过复制现有作业来创建新作业，请执行以下步骤：

- 1 启动升级管理应用程序。
- 2 在“升级作业”主页中，单击“新建作业”。
- 3 单击“复制现有作业”选项。

将出现“复制现有作业”窗口，其中显示“升级作业”文件夹中作业的列表。

- 4 从列表中选择所需作业，然后单击“创建”。

将显示该作业的名称、关键字和说明。如有必要，可以修改这些字段。但不能更改源系统的名称。

- 5 在“作业保存于”字段中，浏览并选择要保存该作业的文件夹，然后单击“创建”。

新作业即被创建，并出现“添加对象 - 作业名称”页面。

相关主题

- 第 514 页上的[“将 Infoobject 添加到作业中”](#)
- 第 514 页上的[“编辑作业”](#)
- 第 517 页上的[“资源库连接时升级作业”](#)

16.3.4 搜索作业

升级管理工具中的搜索功能可用于查找资源库中可用的作业。

要搜索作业，请执行以下步骤：

- 1 在主页的“搜索”字段中，输入要查找的文本。
- 2 单击“搜索”字段旁的列表，以指定搜索参数。可以指定以下搜索参数：

- 搜索标题 — 此选项允许用户按作业名称来搜索作业。
 - 搜索关键字 — 此选项允许用户按作业关键字来搜索作业。
 - 搜索说明 — 此选项允许用户按作业说明来搜索作业。
 - 搜索所有字段 — 此选项允许用户按作业的标题、关键字和说明来搜索作业。
- 。 3 单击“搜索”图标。

相关主题

- 第 514 页上的“[将 Infoobject 添加到作业中](#)”
- 第 514 页上的“[编辑作业](#)”

16.3.5 编辑作业

本节介绍如何编辑作业。

注意：

编辑作业不同于创建新作业。

要编辑作业，请执行以下步骤：

- 。 1 启动升级管理应用程序。
- 。 2 在“升级作业”主页中，选择要编辑的作业。
- 。 3 单击“编辑”。

将显示选定作业的详细信息。可以根据需要添加或删除 InfoObject、管理依赖项或升级作业。

编辑作业时，不能更改源系统名称。

相关主题

- 第 514 页上的“[将 Infoobject 添加到作业中](#)”
- 第 517 页上的“[资源库连接时升级作业](#)”
- 第 521 页上的“[计划作业升级](#)”

16.3.6 将 Infoobject 添加到作业中

每个作业都必须包括一组 InfoObject 及其依赖项。因此，将作业升级到目标系统之前必须将 InfoObject 添加到该作业。

注意：

升级基于业务视图 Infoobject（数据连接、数据基础、业务元素和业务视图）的 Crystal 报表时，必须包括安全信息（数据连接上的 DataAccess 权限以及数据基础和业务元素上的 ViewDataField 权限），才能查看目标系统上报表中的数据。

注意：

将 InfoObject 添加到作业时，必须登录到目标系统。

要将 InfoObject 添加到作业，请执行以下步骤：

- 1 启动升级管理工具。
- 2 创建新作业。

有关创建新作业的信息，请参阅第 511 页上的 [“创建作业”](#)。

- 3 单击“添加对象”。

将出现“添加对象”对话框，并显示对象列表。

- 4 导航至要从中选择 InfoObject 的文件夹。

将显示选定文件夹中 InfoObject 的列表。

- 5 选择要添加到作业的 InfoObject，然后单击“添加”。

如果要在添加 InfoObject 后退出“添加对象 - 源系统名称”对话框，请单击“添加并关闭”。该 InfoObject 即被附加到作业，并关闭“添加对象 - 源系统名称”对话框。

将 InfoObject 添加到作业后，可以右击“作业查看器”页面，然后选择与作业相关的过程，以继续执行升级任务。可使用“作业查看器”页面的“管理依赖项”选项，管理选定 InfoObject 的依赖项。

注意：

- 在“作业查看器”页面的左面板将显示信息对象列表，以平面树结构形式显示作业及其依赖项。
- 添加 InfoObject 后单击“保存”保存更改。否则，当用户关闭选项卡时将被提示选择保存作业。

最佳做法：SAP BusinessObjects 建议选择少量 InfoObject（一次不超过 100 个），以便升级实现升级管理工具的最佳性能。

相关主题

- 第 515 页上的[“管理作业的依赖项”](#)
- 第 517 页上的[“资源库连接时升级作业”](#)
- 第 521 页上的[“计划作业升级”](#)

16.3.7 管理作业的依赖项

本节说明如何管理 InfoObject 的依赖项。

要管理 InfoObject 的依赖项，请执行以下步骤：

- 1 启动升级管理工具。
- 2 创建新作业。

有关创建新作业的信息，请参阅第 511 页上的 [“创建作业”](#)。

- 3 将所需的 InfoObject 添加到新作业。


将出现“升级作业”屏幕。

- 4 单击“管理依赖项”。

将出现“管理依赖项”窗口。此窗口显示 InfoObject 及其依赖项的列表。要只查看尚未选择的对象依赖项，请单击“仅显示未选定的依赖项”复选框。

- 5 从“选择依赖项”下拉列表中选择选项以将依赖项添加到作业。默认情况下不选择依赖项，用户必须明确选择要升级的依赖项。

例如，如果从“仅显示未选定的依赖项”下拉列表中选择“所有 Universe”，则会选择依赖项列表中包括的所有 Universe。也可以逐个选择依赖项。

可单击“类型” 查看 InfoObject 的受支持过滤选项。将出现一个下拉列表。此列表显示支持的过滤选项。选择过滤选项，然后单击“确定”。即会显示过滤后的 InfoObject。

从“依赖项”列选择依赖项时，依赖项会自动移动到“作业中的对象”列。

也可以在“搜索依赖项”字段中键入依赖项名称来搜索依赖项。

有关搜索依赖项的更多信息，请参阅第 516 页上的 [“搜索依赖项”](#)

- 6 单击“应用更改”更新依赖项列表，单击“应用更改并关闭”保存更改。

工具会自动计算依赖项对象。这些依赖项基于 InfoObject 关系或 InfoObject 属性进行计算。在此版本的工具中，不会对不符合这两个条件的依赖项进行计算。

注意：

如果选择某文件夹进行升级，则选定文件夹中的内容被视为主要资源。

相关主题

- 第 517 页上的 [“资源库连接时升级作业”](#)

16.3.8 搜索依赖项

升级管理工具中的高级搜索功能可用于查找资源库中可用 InfoObject 的依赖项。

要搜索 InfoObject 的依赖项，请执行以下步骤：

- 。 1 启动升级管理。
- 。 2 创建新作业或编辑现有作业。

如果已创建新作业，则将 InfoObject 添加到该作业。如果要编辑现有作业，可根据需要添加对象。

- 。 3 单击“管理依赖项”。
- 。 4 在“搜索依赖项”字段中，输入想要查找的依赖项的名称。
- 。 5 单击“搜索”图标。

相关主题

- 第 515 页上的[“管理作业的依赖项”](#)

16.3.9 资源库连接时升级作业

本节介绍在资源库已连接的情况下，如何将作业从源系统升级到目标系统。

下表列出可使用升级管理工具升级的 InfoObject 类型：

类别	可以升级的对象类型
报表	Crystal 报表、Web Intelligence、Dashboards、QaaWS、Explorer
第三方对象	多信息文本、文本文档、Microsoft Excel、Microsoft Power Point、Microsoft Word、Flash、Adobe Acrobat
用户	用户和用户组
服务器	服务器组
Business Intelligence 平台	文件夹、程序、事件、配置文件、对象包、超级链接、类别、警报、收件箱文档、个人和收藏文件夹
Universe、工作区	Universes UNV、连接
EPM 仪表盘	Universe、连接、报表、仪表盘和分析

类别	可以升级的对象类型
业务视图	数据基础
联盟 <ul style="list-style-type: none"> 复制列表 复制作业 	“复制列表”可升级以下对象：Flash、.txt、讨论区、Dashboards、.pdf、超级链接、.xls、对象包、Crystal 报表、Web Intelligence 文档、Universe、程序、连接、DataFoundation、业务视图、.rtf、配置文件、事件、用户和 userGroups。“复制连接”可升级复制作业、远程连接、发布、讨论和 Pioneer 连接
BI 服务	Web Intelligence 文档、Universe 和连接
新 InfoObject	Crystal 报表 (rpt/rptr)、Pioneer、Dashboard Design、DSL Universe (UNX)、WebI、Explorer、Data Federation、Data Steward、BI 工作区等

要升级作业，请执行以下步骤：

- 1 启动升级管理。
- 2 在“升级作业”主页中，选择要升级的作业。
还可以右击主页屏幕，然后单击“升级”。
- 3 在“源”和“目标”系统下拉列表中，选择源系统和目标系统。

注意：

首先确保已登录到源系统和目标系统，然后再执行升级过程。

- 4 在“更改管理 ID”字段中，输入相应的值，然后单击“保存”。

注意：

更改管理 ID 用于获取与记录、审核、作业历史记录等相关的信息。升级管理工具可用于将每个作业创建实例映射到“更改管理 ID”。更改管理 ID 是用户在创建新作业时，在作业定义中设置的属性。该工具会自动为每个作业生成 ID。

- 5 如有需要，选择“安全设置”。将显示以下选项：
 - 不升级安全设置 — 这是默认选项。
 - 升级安全设置 — 此选项用于升级作业及其关联的安全权限。
 - 升级对象安全性 — 此选项用于升级对象和文件夹的安全性
 - 升级用户安全性 — 此选项用于升级属于作业一部分的用户的权限
 - 包括应用程序权限 — 仅在选择“升级安全设置”时才启用此选项。如果作业中的对象继承任何应用程序权限，则该作业与这些权限一起升级。

也可以单击“查看安全设置”查看作业中 InfoObject 的安全依赖项。

- 6 单击“测试升级”，以确保源系统和目标系统中各 InfoObject 的 CUID 没有冲突。升级详细信息显示在“成功”、“失败”和“警告”选项卡下。第一列显示要升级的对象，第二列显示每个 InfoObject 的升级状态。升级管理工具将选定对象分类为用户、组、Universe 等。

注意：

此选项不提交任何 InfoObject 进行升级。

测试升级的结果可以是以下任一种结果：

- 已覆盖 — 目标系统中的 InfoObject 被源系统中的 InfoObject 覆盖。
- 已复制 — 源系统中的 InfoObject 被复制到目标系统。
- 已撤消 — InfoObject 未从源系统升级到目标系统。
- 警告 — 目标系统中的 InfoObject 是较新版本，可以从作业中删除该 InfoObject。但如果想要升级，该 InfoObject 仍会被升级。

7 如果要计划作业实例的升级，请单击“计划作业”。

8 单击“升级”。

选定作业即被升级。

如果不想升级作业，可使用“保存”选项保存修改，如安全设置、更改管理 ID 和计划设置。

16.3.10 使用 BIAR 文件升级作业

升级是指将 BI 资源从一个资源库传送到另一个资源库的活动。如果已连接源系统和目标系统，升级管理工具将使用 WAN 或 LAN 升级 InfoObject。但是，即使未连接源系统和目标系统，升级管理工具也支持升级 InfoObject。

在未连接源系统和目标系统的情况下，升级管理工具使用以下方法将作业升级到目标系统：将作业从源系统中导出到一个 BIAR 文件，然后将该作业从 BIAR 文件导入目标系统。

本节介绍如何将作业导出到 BIAR 文件，然后将作业从 BIAR 文件导入目标系统。

注意：

不能使用通过导入向导工具创建的 BIAR 文件。

相关主题

- 第 519 页上的[“将作业导出到 BIAR 文件”](#)
- 第 520 页上的[“从 BIAR 文件导入作业”](#)

16.3.10.1 将作业导出到 BIAR 文件

本节介绍如何将作业导出到 BIAR 文件。

要将作业导出到 BIAR 文件，请执行以下步骤：

1. 启动升级管理工具，并创建新作业。
有关创建新作业的更多信息，请参阅第 511 页上的 [“创建作业”](#)。
2. 在“目标”下拉列表中，选择“输出到 LCMBIAR 文件”选项，然后单击“创建”。
3. 单击“添加对象”，将 InfoObject 添加到作业。
可以使用“管理依赖项”选项来管理选定作业的依赖项。
4. 单击“升级”。
将出现“升级”窗口。
5. 根据需要修改这些选项，然后单击“导出”。
BIAR 文件即被创建。可将 BIAR 文件保存到文件系统或 FTP 位置。
6. 在“目标”下拉列表中，选择“输出到 LCMBIAR 文件”，然后单击“LCMBIAR 文件目标”。
将出现“LCMBIAR 文件目标”窗格。
7. 执行以下步骤之一：
 - 选择“文件系统”。
 - 选择“FTP”，在主机、端口、用户名、密码、目录和文件名字段中输入相应的详细信息。
8. 要使用密码加密 LCMBIAR 文件，单击“加密密码”复选框。
9. 在“密码”字段中输入密码。
10. 在“确认密码”字段重新输入密码。
11. 单击“导出”。
根据步骤 7 中选择的选项，BIAR 文件被导出到文件系统或 FTP 位置。
12. 可以制定将作业导出到 BIAR 文件的计划。有关更多信息，请参阅第 521 页上的 [“计划作业升级”](#) 一节。

相关主题

- 第 514 页上的[“将 Infoobject 添加到作业中”](#)
- 第 515 页上的[“管理作业的依赖项”](#)

16.3.10.2 从 BIAR 文件导入作业

可以从典型的 BIAR 文件或从 LCMBIAR 文件中导入作业。将 BIAR 文件从存储设备复制到目标系统。

要导入 BIAR 文件，请执行以下步骤：

1. 启动升级管理应用程序。
2. 在“升级作业”主页中，单击“导入” > “导入文件”。

将出现“从文件导入”窗口。

- 3 可以从本地计算机或从任何其他源计算机中导入 BIAR 文件。

- 要从本地计算机导入 BIAR 文件，请执行以下步骤：

- a 选择“文件系统”。
- b 单击“浏览”，然后从文件系统中选择一个 BIAR 文件。

注意：

如果存在同名的作业，将显示“确认保存”弹出对话框。单击“是”将覆盖现有作业；单击“否”将使用新 CUID 和名称 Jobname_copy 创建作业。

- c 在“密码”字段中，输入 LCMBIAR 文件的密码。

注意：

只有对 LCMBIAR 文件使用了密码加密，才会显示“密码”字段。

- d 单击“创建”。该作业即被创建。

- 要从启用了 FTP 的任何源计算机导入 BIAR 文件，请执行以下步骤：

- a 选择“FTP”。
- b 分别在“主机”、“端口”、“用户名”、“密码”、“目录”和“文件名”字段中输入相应的详细信息，并单击“确定”。

注意：

可以仅导入 LCMBIAR 或升级 BIAR 文件。

- 4 单击“升级”。

将出现“升级 - 作业名称”窗口。

- 5 从“目标”下拉列表中，选择目标系统。如果选择“登录到新 CMS”，则提示用户提供凭据。确认目标系统的登录凭据。
- 6 单击“升级”，将内容升级到目标系统。

也可以单击“测试升级”选项来查看要升级的对象以及升级状态。

相关主题

- 第 515 页上的[“管理作业的依赖项”](#)

16.3.11 计划作业升级

本节介绍如何计划作业实例的升级。同时还介绍如何指定重复发生选项和参数。

要计划作业实例的升级，请执行以下步骤：

- 1 在“升级”对话框中，单击“计划”选项。

- 2 设置所需计划选项，然后单击“计划”。

如果在完成作业升级计划后向现有文件夹中添加 InfoObject，则这些 InfoObject 在计划的时间也将升级至目标。

将作业导出到 BIAR 文件时，可以制订目标计划。

提示：

完成 InfoObject 升级后，可以通过单击 infoobject 并选择“历史记录”查看所有正在运行的 infoobject 实例。

作业的升级也可基于事件触发器进行。

可以基于作业升级状态（例如成功/部分成功/失败）选择电子邮件通知。有关各种计划选项和配置通知的详细信息，请参阅“计划”一节。

相关主题

- 第 519 页上的[“将作业导出到 BIAR 文件”](#)

16.3.11.1 更新重复发生和待定作业升级实例




在升级管理工具中，可使用“重复发生和待定实例”选项跟踪和更新计划作业升级实例的状态。

要跟踪和更新计划作业升级实例，请执行以下步骤：

- 1 启动升级管理工具。
- 2 在“升级作业”主页中，选择一个作业。
- 3 单击“历史记录”。
- 4 单击“重复发生和待定实例”。

将出现“重复发生和待定实例的作业历史记录”窗口。此窗口显示重复发生和待定作业升级实例的列表。

根据需要，可以使用以下选项：

- 单击“已升级的实例”以查看计划作业升级实例的列表。
- 单击“暂停”选项以暂停计划升级。
- 单击“恢复”选项以恢复暂停的计划作业升级实例。
- 单击“重新计划”选项以重新计划作业升级实例。
- 单击  以删除计划作业升级实例。
- 单击  以刷新计划作业升级实例的状态。
- 可以使用  选项导航单一页面，也可以通过输入相应页码导航至特定页面。

注意：

“重复发生和待定实例的作业历史记录”窗口中的状态列显示作业升级实例的状态，例如重复发生、待定等。

相关主题

- 第 523 页上的“[回滚作业](#)”

16.3.12 查看作业的历史记录

本节介绍如何查看作业历史记录。

注意：

要查看作业的历史记录，必须确保作业的状态为以下状态之一：

- 成功
- 失败
- 部分成功

要查看作业的历史记录，请执行以下步骤：

- 1 启动升级管理工具。

将出现“升级作业”主页。

- 2 执行以下任意操作：

- 右击要查看历史记录的作业，然后选择“历史记录”。
- 选择要查看历史记录的作业，然后单击“历史记录”选项卡。

将显示作业实例、作业名称、源系统和目标系统的名称、升级作业的用户 ID 以及作业状态（成功、失败或部分成功）。

可使用“状态”列中显示的链接查看作业状态。

16.3.13 回滚作业

“回滚”选项允许用户在作业升级后将目标系统恢复到其先前状态。

要回滚某作业，请执行以下步骤：

- 1 启动升级管理工具。
将出现“升级作业”主页。
- 2 执行以下任意操作：
 - 右击要回滚的作业，然后选择“回滚”。
 - 选择要回滚的作业，然后单击“回滚”选项卡。将出现“回滚”窗口。
- 3 选择要回滚的作业，然后单击“完全回滚”。
该作业即被回滚。

只能回滚作业升级的最新实例。不能同时回滚两个作业实例。

16.3.13.1 使用“部分回滚”选项

升级管理工具可用于从目标系统完全或部分回滚作业中的 InfoObject。

要部分回滚 InfoObject，请执行以下步骤：

- 1 启动升级管理工具。
将出现“升级作业”主页。
- 2 执行以下任意操作：
 - 右击要回滚的作业，然后选择“回滚”。
 - 选择要回滚的作业，然后单击“回滚”选项卡。将出现“回滚”窗口。
- 3 从列表中选择作业，然后单击“部分回滚”。

选定作业中 InfoObject 的列表将显示在“作业查看器”页面中。

- 4 选择要回滚的 InfoObject，然后单击“回滚”。

注意：

必须确保回滚了作业中的所有 InfoObject，然后才能回滚下一个作业中的 InfoObject。

警告：

如果作业与安全设置一同升级，则在 InfoObject 的部分回滚期间，选定的依赖项 InfoObject 的安全设置可能不会回滚到其先前状态。

相关主题

- 第 494 页上的“[管理 BI 资源的不同版本](#)”

16.3.13.2 密码到期后回滚作业

本节介绍如何在用于升级作业的密码到期后回滚作业。

要在密码到期后回滚作业，请执行以下步骤：

- 。 1 选择要回滚的作业，然后单击“回滚”。
- 。 2 在“回滚”窗口中，选择“完全回滚”。

将显示一条错误消息。此消息说明作业无法回滚。系统还会提示用户登录到源系统或目标系统。

- 。 3 输入新的登录凭据，然后单击“登录”。

将出现一个对话框，指明回滚过程完成。

注意：

使用源系统或目标系统凭据升级的作业将自动更新。

相关主题

- 第 525 页上的“[密码到期后回滚 InfoObject](#)”
- 第 524 页上的“[使用“部分回滚”选项](#)”

16.3.13.2.1 密码到期后回滚 InfoObject

本节介绍如何在源系统和目标系统的密码到期后回滚 InfoObject。

要在密码到期后回滚 InfoObject，请执行以下步骤：

- 。 1 选择要回滚的作业，然后单击“回滚”。

将出现“回滚”窗口。

- 。 2 选择“部分回滚”选项。

将显示一条错误消息。此消息说明 InfoObject 无法回滚。系统还会提示用户登录到源系统或目标系统。

- 。 3 输入新的登录凭据，然后单击“登录”。

将出现“作业查看器”页面。此页面显示 InfoObject 列表。

- 。 4 选择所需的 InfoObject，然后单击“回滚”。

注意：

使用源系统或目标系统凭据升级的作业将自动更新。

相关主题

- 第 523 页上的[“回滚作业”](#)
- 第 524 页上的[“使用“部分回滚”选项”](#)
- 第 525 页上的[“密码到期后回滚作业”](#)

16.4 管理 Infoobject 的不同版本


版本管理应用程序可用于管理 BI 平台资源库中 BI 资源的版本。该工具同时支持 Subversion 和 ClearCase 版本管理系统。本节介绍如何使用升级管理控制台工具中的版本管理功能。

要创建并管理 InfoObject 的不同版本，请执行以下步骤：

- 1 启动升级管理应用程序。
- 2 在主页中，从下拉列表中选择“版本管理”。
将出现“登录到系统”对话框。
- 3 输入登录凭据，然后单击“登录”。
将出现“版本管理”窗口。

注意：

只有在已配置了版本管理系统（VMS）的情况下才能登录到该系统。

- 4 如果要更改主机系统，请单击 。
将出现“登录到系统”对话框。
- 5 输入用户凭据，然后单击“登录”。
- 6 从“版本管理”窗口的左面板中选择文件夹，以查看要对其版本进行管理的 InfoObject。
- 7 选择 InfoObject，然后单击“添加到 VM”。

注意：

单击“添加到版本管理系统”后，即会在 VMS 资源库中创建该对象的基础版本。对于后续的签入操作，基础版本是必需的。

- 8 单击“签入”以更新 VMS 资源库中的文档。
将出现“签入注释”对话框。
- 9 输入注释，然后单击“确定”。

选定 InfoObject 的版本号变更会显示在 VMS 列和内容管理系统列中。

10. 要从 VMS 获取文档的最新版本，请选择所需的 InfoObject，然后单击“获取最新版本”。

11. 要创建最新版本的副本，则单击“创建副本”。

选定版本的副本即被创建。

12. 选择“历史记录”可查看选定资源的所有可用版本。

将出现“历史记录”窗口。将显示以下选项：

- 获取版本 — 如果存在多个版本，且需要使用 BI 资源的某一特定版本，则可以选择所需的资源并单击“获取版本”。
- 获取版本副本 — 通过此选项可获取选定版本的副本。
- 导出版本副本 — 通过此选项可获取选定版本的副本并将其保存到本地系统。

13. 选择 InfoObject，然后单击“锁定”以锁定该 InfoObject，而单击“解锁”可解除锁定该 InfoObject。

注意：

如果锁定某一 InfoObject，则无法对该 InfoObject 执行任何操作。

14. CMS 和 VMS 同步 — InfoObject 的 CMS 版本更新后，已更新的 InfoObject 旁边将出现一个指示符。将光标置于该指示符之上时，将显示工具提示，指明 CMS 中的 InfoObject 已更新。

15. 要查看 VMS 中存在但 CMS 中不存在的所有已签入资源的列表，请单击“查看已删除的资源”。


单击任意已删除的资源，以查看该资源的历史记录。可以选择某个已删除的资源，然后单击“获取版本”以查看该资源的特定版本。可以单击“获取版本副本”来获取选定资源的副本。

注意：

如果使用“获取版本”或“获取版本副本”选项，资源将从 VMS 缺失文件列表移动到 CMS 中。

警告：

如果删除父文件夹，则无法恢复其所包含的子对象和文件夹。

16. 选择某资源，然后单击  查看该资源的属性。

或者，可以右击 InfoObject 并执行步骤 4 至 16。

16.4.1 版本管理应用程序访问权限

本节介绍版本管理应用程序的应用程序访问权限。

- 可在 CMC 中设置对版本管理应用程序的访问权限。
- 可设置对版本管理应用程序中各种功能的应用程序粒度权限。

要在版本管理应用程序中设置特定权限，请完成以下步骤：

1. 登录到 CMC 并选择“应用程序”。
2. 双击“版本管理”。

- 。 3 单击“用户安全性”并选择用户。可以查看或为所选用户分配安全权限。
- 。 4 现在可以使用以下版本管理特定权限：
 - 允许签入
 - 允许创建副本
 - 允许删除修订版
 - 允许获取修订版
 - 允许锁定和解锁
 - 视图和版本 BOMM 对象
 - 视图和版本业务视图
 - 视图和版本日历
 - 视图和版本连接
 - 视图和版本配置文件
 - 视图和版本 QaaWS
 - 视图和版本报表对象
 - 视图和版本安全对象
 - 视图和版本 Universe
 - 查看已删除的资源
- 。 5 如果希望为选定用户分配权限，请选择相应权限并单击“指定安全性”。

16.4.2 备份和恢复 Subversion 文件

本节介绍执行 Subversion 文件备份和恢复的建议步骤。备份和恢复计划包含相应预防措施，当系统由于自然灾害或灾难事件发生故障时将采取这些措施。

16.4.2.1 备份 Subversion 文件

执行以下步骤，以备份 Subversion 文件：

- 1 在 Windows 上，转到安装目录\SAP BusinessObjects Enterprise 4.0\CheckOut，或在 Unix 上，转到安装目录/sap_bobj/enterprise_40/subversion/checkout
- 2 复制 CheckOut 文件夹并将其存储在任意备份设备中。
- 3 复制整个 LCM_Repository 并将其存储在任意备份设备中。

16.4.2.2 恢复 Subversion 文件

请完成以下步骤，以恢复 Subversion 文件：

- 1 从先前的备份位置恢复 CheckOut 文件夹。

注意：

在 CMC 中，单击“应用程序” > “版本管理” > “VMS 设置”，并确保在“工作区目录”字段中输入正确的签出路径。

- 2 从先前的备份位置恢复 LCM_Repository 文件夹。

注意：

在 CMC 中，单击“应用程序” > “版本管理” > “VMS 设置”，并确保在“安装目录”字段中输入正确的签出路径。

16.5 使用命令行选项

升级管理工具的命令行选项使用户可以通过输入命令行将对象从一个 BI 平台部署升级到另一个 BI 平台部署。

升级管理工具通过命令行选项支持以下作业升级：

- 将现有 LCM 作业模板导出到带有加密密码的 LCMBIAR
- 将现有 LCM 作业模板导出到无加密密码的 LCMBIAR
- 使用现有作业模板升级
- 导入并升级现有 LCMBIAR
- 导出单个/多个平台查询
- 升级多个平台查询
- 执行系统到系统升级

16.5.1 在 Windows 上运行命令行工具

要运行命令行工具，请执行以下步骤：

- 1 启动命令行窗口或外壳。
- 2 导航到相应目录。

例如，Windows 上的目录路径为：C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib

- 3 执行以下操作之一：

- 执行 LCMCLI，确保在运行程序前已设置了 Java 路径。

命令：java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <属性文件>

- 运行以下位置的 BAT 文件：C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win64_x64\scripts\lcm_cli.bat

命令：lcm_cli.bat -lcmproperty <属性文件>

注意：

收到提示后输入有效密码。

升级管理命令行工具将 properties 文件作为参数。properties 文件包含必需的参数，以便向升级管理工具传送下列信息：要执行的操作、连接到哪个 BI 平台部署、连接方法以及要升级的对象等。

文件必须为 <文件名称>.properties 格式

例如，Myproperties.properties

16.5.2 在 UNIX 上运行命令行工具

要运行命令行工具，请执行以下步骤：

- 1 启动 shell。
- 2 导航到相应目录。

例如，/usr/u/qaunix/Aurora604/sap_bobj/enterprise_40/java/lib

- 3 执行以下操作之一：

- 执行 LCMCLI，确保在运行程序前已设置了 Java 路径。

命令：java -cp "lcm.jar" com.businessobjects.lcm.cli.LCMCLI <属性文件>

- 从 <安装目录路径>\sap_bobj\lcm_cli.sh 中运行 BAT 文件

命令：lcm_cli.sh -lcmproperty <属性文件>

注意：

收到提示后输入有效密码。

16.5.3 命令行工具参数

下表介绍了适用于升级管理应用程序的命令行选项的参数和允许的值。

参数	允许的值	说明	必需与可选
action	Export、Promote 示例：action=export	该选项可用于指定 CLI 必须执行的操作。此操作可执行以下任何操作： <ul style="list-style-type: none"> 将 LCMBIAR 文件中的对象或升级管理作业升级到 BI 平台系统。 将对象从 BI 平台系统导出到 LCM-BIAR 文件。 	必需
consolelog	真或假	此参数用来在命令日志中显示用户执行命令的完整日志。	可选
Destination_authentication	secEnterprise、secWinAD、secLDAP、secSAPR3 示例：Destination_authentication=<身份验证>	该参数指定要使用的身份验证类型。	可选。 如果未指定身份验证类型，则使用 secEnterprise。
Destination_clientID	客户端 ID 示例：Destination_clientID=<系统 ID>	该参数仅用于 SAP 身份验证。	对于 SAP 身份验证是必需的。

参数	允许的值	说明	必需与可选
Destination_CMS	任意格式文本。 示例: Destination_CMS=<CMSname: 端口号>	用户可使用该参数指定工具必须连接到的 CMS。	如果 action=export, 则必需
Destination_password	任意格式文本。 示例: Destination_password=<密码>	该参数指定用户帐户的关联密码。	如果 action=promote, 则必需
Destination_systemID	系统 ID 示例: Destination_systemID=<系统 ID>	该参数仅用于 SAP 身份验证。	对于 SAP 身份验证是必需的。
Destination_userName	任意格式文本。 示例: Destination_username=<用户名>	该参数指定工具连接到 BI 平台 CMS 时必须使用的用户帐户。 注意: 支持委派的管理员。	如果 action=promote, 则必需
exportLocation	任意格式文本。必须具有 .lcmbar 扩展名 示例: exportLocation=C:/Backup/New.lcmbar	用户可使用该参数来指定在导出和打包对象之后用于放置 LCM-BIAR 文件的位置。	如果 action=export, 则必需
exportDependencies	假、真 示例: exportDependencies=<真或假>	此参数指定工具收集的对象相关性, 以进行导出。仅与 Source_CMS 标记配合使用时适用。	可选, 如果 action=promote or export, 则使用 如未指定, 默认值为假。

参数	允许的值	说明	必需与可选
exportQuery	<p>任意格式文本。使用 CMS 查询语言格式。</p> <p>示例: export Query1=select*from ci_Infoobjects where si_name='Xtreme 雇员' and si_kind='Webi'</p> <p>注意: 在一个属性文件中可以具有任意数量的查询,但是这些查询必须命名为 exportQuery1、exportQuery2 等等。</p>	<p>这些是工具应执行的查询,用以收集导出的所需的对象。</p>	<p>可选 (如果 action=export, 则使用)</p>
exportQueriesTotal	<p>正整数 export QueriesTotal=<整数></p>	<p>用户可使用该参数来指定要执行的导出查询数。如果有 x 个导出查询并且要全部执行,则必须将该参数值设置为 x。</p>	<p>可选 (如果 action=export, 则使用)</p> <p>如未指定,默认值等于 1</p>
importLocation	<p>任意格式文本。必须具有 .lcmbar 扩展名</p> <p>示例: importLocation=C:/Backup/New.lcmbar</p>	<p>用户可使用该参数来指定包含待升级对象的 LCMBAR 文件的位置。</p>	<p>如果 action=promote, 则必需</p>
includeApplicationSecurity	<p>假、真</p> <p>示例: includeApplicationSecurity=<真或假></p>	<p>该参数将向工具发出指令,要求导出或导入与选定应用程序关联的安全性。</p>	<p>可选 (如未指定,默认值为假)。</p> <p>如果 action=promote 或 export, 则使用</p>

参数	允许的值	说明	必需与可选
includeSecurity	假、真 示例: includeSecurity=<真或假>	该参数将向工具发出指令, 要求导出或导入与选定对象和选定用户关联的安全性。如果使用访问级别, 这也将导出/导入它们。	可选 (如未指定, 默认值为 false)。 如果 action=promote 或 export, 则使用
JOB_CUID	已保存的 LCM 作业的 GUID。	该参数指令工具将作业中的所有对象导出为 LCMBIAR 文件。	可选 (如果 action=export 或 promote, 则使用)
lcmbiarpassword	任意格式文本。 示例: java -jar upgradeManagementTool.jar -mode livetobiar -biarfile "C:\TEMP\abc.biar" -lcmbiarpassword "testpassword"	此参数使用密码加密和解密 BIAR 文件。	可选, 如果未指定或字符串为空, 表示没有加密
lcmproperty	属性文件保存位置的完整路径 lcm_cli.bat -lcmproperty <属性文件的路径>	此参数为执行命令需要的值, 保存在一个文件中	必需
LCM_authentication	secEnterprise、secWinAD、secLDAP、secSAPR3 示例: LCM_authentication=<authentication>	该参数指定要使用的身份验证类型。	可选。 如果未指定身份验证类型, 则使用 secEnterprise。

参数	允许的值	说明	必需与可选
LCM_clientID	客户端 ID 示例: LCM_clientID=<客户端 ID>	该参数用于 SAP 身份验证。	对于 SAP 身份验证是必需的。
LCM_CMS	任意格式文本。 示例: LCM_CMS=<CMSname:端口号>	用户可使用该参数为升级管理应用程序指定 CMS。	如果 action=promote 或 export, 则必需
LCM_password	任意格式文本。 示例: LCM_password=<密码>	用户可使用该参数来指定用户帐户的密码。	如果 action=promote 或 export, 则必需
LCM_systemID	系统 ID 示例: LCM_systemID=<系统 ID>	该参数用于 SAP 身份验证。	对于 SAP 身份验证是必需的。
LCM_userName	任意格式文本。 示例: LCM_userName=<用户名>	用户可使用该参数指定工具连接到升级管理应用程序 CMS 所必须使用的帐户用户名。 注意: 支持委派的管理员	如果 action=promote 或 export, 则必需
Source_authentication	secEnterprise、secWinAD、secLDAP、secSAPR3 示例: Source_authentication=<身份验证>	该参数指定要使用的身份验证类型。	可选。 如果未指定身份验证类型, 则使用 secEnterprise。

参数	允许的值	说明	必需与可选
Source_clientID	SAP 客户端 ID 示例: Source_clientID=<系统 ID>	该参数仅用于 SAP 身份验证。	对于 SAP 身份验证是必需的。
Source_CMS	任意格式文本。 示例: Source_CMS=<CMSname: 端口号>	用户可使用该参数指定工具必须连接到的 CMS。	如果 action=export, 则必需
Source_password	任意格式文本。 示例: Source_password=<密码>	该参数指定用户帐户的关联密码。	如果 action=export, 则必需
Source_systemID	SAP 系统 ID 示例: Source_systemID=<系统 ID>	该参数仅用于 SAP 身份验证。	对于 SAP 身份验证是必需的。
Source_userName	任意格式文本。 示例: Source_userName=<用户名>	该参数指定工具连接到 BI 平台 CMS 时必须使用的用户帐户。 注意: 支持委派的管理员。	如果 action=export, 则必需
stacktrace	真或假 示例: stacktrace=<真或假>	用户可使用该参数来跟踪所有调用。	可选 (如未指定, 默认值等于 false)

注意:

- 类似于在导出前创建作业, 命令行选项会即时创建临时作业。此作业名称可包含 Query_<用户>_<时间戳>。这仅特定于 exportQuery。
- 导出的 LCMBIAR 文件命名约定可以包含 <作业名>_<时间戳>.lcmbar, 以便在 exportLocation 文件中未指定 LCMBIAR 名称时保持唯一性。
- 只能通过升级管理应用程序回滚作业。没有对回滚作业的命令行支持。

16.5.4 示例属性文件

以下为示例 properties 文件：

示例：

```
importLocation=C:/Backup/CR.lcmbiar
action=promote
LCM_CMS=<CMS 名称:端口号>
LCM_userName=<用户名>
LCM_password=<密码>
LCM_authentication=<身份验证>
LCM_systemID=<ID>
LCM_clientID=<客户端 ID>
Destination_CMS=<CMS 名称:端口号>
Destination_userName=<用户名>
Destination_password=<密码>
Destination_authentication=<身份验证>
Destination_systemID=<ID>
Destination_clientID=<客户端 ID>
lcmbiarpassword=<密码>
```

注意：

如果该 properties 文件没有任何个人信息，LCM 命令行界面将在控制台中提示提供相同信息。

16.6 使用增强更改和传输系统

更改和传输系统（CTS）组织和自定义 ABAP 工作台中的开发项目，然后在系统架构中的 SAP 系统之间传输这些更改。增强更改和传输系统（CTS+）是 CTS 的加载项，该加载项升级所有启用了 CTS+ 的非 ABAP 资源库的非 ABAP 内容。

BI 平台信息对象可使用 SAP Business Warehouse 内容作为数据源。CTS+ 与升级管理工具集成后，可使用 CTS 传输请求来升级作业，从而处理 BI 平台资源库，处理方式与 SAP Business Warehouse（BW）资源库类似。CTS+ 允许在系统架构内传输非 SAP 对象。例如，在开发系统中创建的对象可以附加到传输请求中并转发给架构内的其他系统。

有关更改和传输系统的更多信息，请参阅http://help.sap.com/saphelp_nw70ehp1/helpdata/en/3b/dfba3692dc635ce10000009b38f839/frameset.htm。

有关 CTS+ 和非 ABAP 传输的更多信息，请参阅http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bb/6fab6036a146baa58e42fac032ab7b/frameset.htm。

16.6.1 先决条件

以下是通过 CTS+ 将商务智能内容从一个系统传输到另一个系统的前提条件：

- 。 1 安装了 SAP BusinessObjects Business Intelligence 平台 4.0（BI 平台）。
- 。 2 安装了 SAP Solution Manager 7.1 或 SAP Solution Manager 7.0 EHP1（最低为 SP25），并作为 CTS+ 的域控制器，至少用于配置 SAP BusinessObjects 系统。

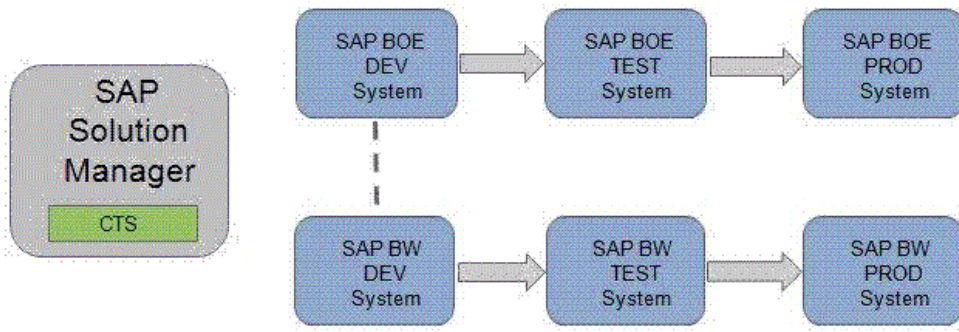
有关配置传输域的更多信息，请参阅http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a0a77acc11d1899e0000e829fbbd/frameset.htm。

- 。 3 为 SAP Solution Manager 安装了 CTS 插件（CTS 插件来源于 SL 工具集 1.0 SP02。建议使用最新版本的 CTS 插件。）

有关安装所需 CTS 插件的更多信息，请参阅 SAP 注释：<https://service.sap.com/sap/support/notes/1533059>

- 。 4 安装了 SAP Business Warehouse 7.0（SPS 24 或更高版本）系统。有关更多信息，请参阅 SAP 注释 <https://service.sap.com/sap/support/notes/1369301>。
- 。 5 更改和传输系统（CTS）中配置了 SAP Business Warehouse（SAP BW）传输架构。

16.6.2 配置 BI 平台和 CTS+ 集成



作为更改和传输系统一部分的传输管理系统（TMS）用于在架构内的 SAP 系统之间传输更改。它管理连接的系统及其路线，以及导入到系统中的数据。有关传输管理系统的更多信息，请参阅 http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a0137acc11d1899e0000e829fbbd/frame set.htm。

CTS+ 可用于从外部收集文件并在传输架构内进行分发。传输组织器 Web UI 是 CTS+ 的一部分，用于管理传输请求及其所包含的对象。有关更多信息，请参阅 http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a0137acc11d1899e0000e829fbbd/frame set.htm

可以使用 CTS 传输请求将 BI 平台升级管理与 CTS+ 和 SAP BW 相集成。

注意：

要启用 BI 平台与 SAP Solution Manager 的集成，需要在 SAP Solution Manager 架构中定义“BOLM”应用程序类型。

执行以下步骤以集成 BI 平台与 CTS+：

- 1 激活 CTS 导出 Web 服务
- 2 在升级管理工具中配置 CTS 设置
- 3 在 SAP Solution Manager 中配置 BI 平台导入系统

相关主题

- 第 539 页上的“[激活 CTS 导出 Web 服务](#)”
- 第 540 页上的“[在升级管理工具中配置 CTS+ 设置](#)”
- 第 538 页上的“[配置 BI 平台和 CTS+ 集成](#)”

16.6.2.1 激活 CTS 导出 Web 服务

若要配置 BI 平台系统，您需要在 SOA Management Web 工具中激活 CTS 导出 Web 服务。

- 1 若要启动应用程序，请在 SAP Solution Manager 中输入事务代码 SOAMANAGER。
要了解 SOA Management 和服务端点的配置，请参阅 SAP Help Portal，网址为：
http://help.sap.com/saphelp_nw70ehp1/helpdata/en/33/06820d9d174c2884576bd78ac5629d/frame_set.htm
所需身份验证完成后，将在 Web 浏览器中打开 SOA Management Console。
- 2 在“Service Administration”（服务管理）选项卡中选择“Single Service Configuration”（单项服务配置）。
CTS 导出 Web 服务名为 EXPORT_CTS_WS
- 3 在“Configuration”（配置）选项卡中创建或编辑服务端点。
- 4 在“Security”（安全性）选项卡中配置传输协议和身份验证方法。
- 5 在“Transport Settings”（传输设置）选项卡中，定义备选访问 URL 以更方便地访问服务端点。

16.6.2.2 在升级管理工具中配置 CTS+ 设置

下面的部分将介绍为使用升级管理工具设置 CTS+ 时，需要在 CMC 应用程序中执行的配置步骤。

- 1 在“升级作业”页面中，单击“CTS 设置”，再单击“BW 系统”。
- 2 在“BW 系统”页面中，单击“添加”向系统架构中添加 BW 系统。
- 3 在“添加系统”页面中，输入以下详细信息：
 - “主机 BW SID”：指定主机 SAP BW/ABAP 计算机的系统 ID (SID)。
 - “主机名”：指定主机计算机的 IP 地址。
 - “系统编号”：输入主机系统的系统编号。
 - “客户端”：是指客户端计算机的系统详细信息。
 - “用户”和“密码”：在这两个字段中指定客户端计算机上的用户名和密码。
 - “语言”：在此字段中指定语言选择。
- 4 单击“保存”将系统添加到系统架构中。

注意：

将 BW 系统添加到系统架构中后，可以使用“BW 系统”页面中的“编辑”或“删除”修改系统架构中的系统。

- 5 在“升级作业”页面中，单击“CTS 设置”，再单击“Web 服务设置”。
- 6 在“Web 服务设置”页面中，输入 Web 服务 URL 和用户详细信息。

注意：

如果不清楚这些详细信息，可向 Solution Manager 管理员索取。

- 7 单击“保存”和“关闭”以完成添加 Web 服务设置。
- 8 在 BI 源系统中创建映射文件。

在 BI 平台开发系统中完成以下步骤以创建一个文本文件，其中包含用于启用映射的连接详细信息：

- a 在 BI 平台升级管理 CMS 中，转到根目录并在路径 <SAP BusinessObjects Business Intelligence 平台安装路径>/SAP BusinessObjects Business Intelligence platform 4.0/ 中创建一个名为 LCM 的文件夹。
- b 创建名为 LCM_SOURCE_CMS_SID_MAPPING.properties 的文本文件，并在该文件中输入以下内容之一：
 - <包含域的 SAP BusinessObjects Business Intelligence 平台源系统的完整名称>@<CMS 端口号> = <CTS 配置中使用的源系统的逻辑名称>
 - <SAP BusinessObjects Business Intelligence 平台源系统的 IP 号>@<CMS 端口号> = <CTS 配置中使用的源系统的逻辑名称>

例如：

DEWDFTH04171S@6400=WJ3

10.208.112.177@6400=WJ3

DEWDFTH04171S.pgdev.sap.corp@6400=WJ3

注意：

在群集环境中，将 LCM_SOURCE_CMS_SID_MAPPING.properties and LCM_SID_RFC_MAPPING.properties 文件复制到运行自适应处理服务器的系统中。

有关针对非 ABAP 系统执行配置步骤的更多信息，请参阅

http://help.sap.com/saphelp_nw70/helpdata/en/d4/3bab83106941f08ad1f2e1ec14375e/frameset.htm。

16.6.2.3 在 SAP Solution Manager 中配置 BI 平台导入系统

- 1 登录到 SAP Solution Manager 系统。
- 2 输入事务 stms，并按 Enter 键。
- 3 将应用程序类型配置为 BOLM。
 - a 转到“Overview”（概览） > “Systems”（系统）。
 - b 转到“Extras”（额外） > “Application Type”（应用程序类型） > “Configure”（配置）。
 - c 选择“New Entries”（新建条目）。
 - d 在“Application Type”（应用程序类型）字段中输入 BOLM。
 - e 输入描述。
 - f 在“Support Details”（支持详细信息）字段中输入 <http://service.sap.com> (ACH: BOJ-BIP-DEP)
 - g 选择“Table View”（表视图） > “Save”（保存）。
 - h 选择“Yes”（确定）确认该提示。
- 4 要使用其他语言，可按以下方式维护翻译的文本：

- a 选择“Goto”（转到）>“Translation”（翻译）。
- b 选择翻译文本的目标语言。
- c 在“Description”（说明）和“Support Details”（支持详细信息）字段中输入翻译后的值。
- d 确认对话框。
- e 选择“Continue”（继续）。
- f 选择“Table View”（表视图）>“Save”（保存）。
- g 收到提示后确认。

此时，TMS 域对 CTS 中商务智能内容使用的支持已就绪。

- 5 在 CTS+ 中，将 BI 平台源系统定义为导出系统。

注意：

有关创建非 ABAP 系统作为源系统的更多信息，请参阅 http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2flabeeaf4f8e4/frame set.htm (http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2flabeeaf4f8e4/frame set.htm)。

- 6 在 CTS+ 中，通过完成以下步骤配置 BI 平台导入系统：

注意：

可以定义一个 SID 作为对 BI 平台导入系统的引用。

- a 创建一个非 ABAP 系统作为导入系统。
有关更多信息，请参阅http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2flabeeaf4f8e4/frame set.htm (http://help.sap.com/saphelp_nw70ehp1/helpdata/en/bf/e4626214504be18b2flabeeaf4f8e4/frame set.htm)
- b 指定部署方法为“Others”（其他），并取消选择所有其他选项。
- c 单击“Save”（保存）。
- d 确认分发对话框。
将出现用于配置导入系统设置的表视图。
- e 选择“Edit”（编辑）>“New Entries”（新条目）。
- f 在“Change View CTS: System details for handling of application types”（更改视图 CTS: 有关处理应用程序类型的系统详细信息）屏幕中，执行以下步骤：
 - 1 在“Deploy Method”（部署方法）字段中选择“application specific Deployer (EJB)”（应用程序特定部署器 (EJB)）。
 - 2 在“Deploy URI”（部署 URI）字段中输入以下 URI: `http://<BOE (http://%3cboe/) web server name>:<Webserver port>/BOE/LCM/CTServlet?&cmsName=<BOE destination name>:<CMSport>&authType=<BOE authentication type>`

其中：

- “BOE web server name”是运行 BI 平台 Web 服务器的计算机的名称或 IP 地址。
- “Web server port”是 BI 平台应用程序服务器的端口号。
- “BOE destination name”是运行 BI 平台中央管理服务器 (CMS) 的计算机的名称。
- “CMS port”是 CMS 的端口号。
- “BOE authentication type”是用于导入商务智能内容的用户身份验证类型。受支持的身份验证类型包括 secEnterprise、secLDAP、secWinAD 和 secSAPR3。

- 3 在 “User”（用户）字段中，输入 BI 平台用户名。
- 4 在 “Password”（密码）字段中，输入 BI 平台密码。
- 5 选择 “Save”（保存）以保存设置。

如果需要多个导入系统，请重复上述步骤，以创建所需的全部目标系统。要在创建目标系统之后配置源系统与目标系统之间的传输路线，请参阅http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a1df7acc11d1899e0000e829fbbd/frameset.htm。

16.6.2.4 从 BI 平台导出到 CTS+

16.6.2.4.1 为 CTS+ 配置 SSL

要为 CTS+ 配置 SSL，必须在应用程序服务器 ABAP 上配置 SSL。

记忆：

确保应用程序服务器上已安装 SAP Cryptographic Library。

- 1 使用事务代码 rz10，然后配置 “配置文件” 参数以使用 SSL。
 - a 将以下参数添加到实例配置文件 SM1_DVWEBMGS00_PAPGVMWIN044:

```
ssf/name=SAPSECULIB
# HTTPS port
icm/server_port_1=PROT=HTTPS,PORT=8443,TIMEOUT=30,PROCTIMEOUT=600
# 0: Do not use certificates 1: Allow certificates (default) 2: Require certificates
icm/HTTPS/verify_client=1
```

- 2 如果 SSL 服务器 PSE 不存在，可通过命令行新建。
 - a 设置 SECUDIR 变量:

```
set SECUDIR=D:\usr\sap\SM1\DVWEBMGS00\sec
```

- b 使用以下参数运行 sapgenpse:

```
sapgenpse get_pse -p SAPSSLS.pse
```

注意：

请勿指定 PIN，使用应用程序服务器的全限定域名作为可分辨名称（DN）中的常用名（CN）。

记忆:

确保运行 ICM 的操作系统用户拥有 PSE 读取权限。

- 3 将证书请求发送至认证机构 (CA)。
 - a 为 CA 选择 SAPNetCA PKCS#7, 并为命令选择验证证书请求。
 - b 附上证书请求。
 - c 将证书请求响应保存至文件, 例如 smlsslcert.crt。
- 4 使用以下参数将证书请求响应导入到 SSL 服务器 PSE:

```
sapgenpse import_own_cert -c smlsslcert.crt -p SAPSSL.pse
```
- 5 使用事务代码 smicm, 然后单击“管理” > “ICM” > “软退出” > “全局”以重新启动 ICM。

注意:
也可使用 SAP MMC 重新启动整个 SM1 系统。
- 6 使用“Internet 通信管理器监控器 - 服务显示”选项卡验证 HTTPS 服务是否在 ICM 上运行。
- 7 测试 SSL 连接。

16.6.2.4.2 配置客户端 SSL 证书

要配置客户端 SSL 证书, 必须将服务器证书或信任的 CA 证书导入 JVM 密钥库。

- 1 备份<安装目录>\win64_x64\sapjvm\jre\lib\security 目录中的 cacerts 文件。
- 2 使用以下参数将 SAPNetCA 证书导入承载 BOE.war 文件的 Tomcat JVM:

```
<INSTALLDIR>\win64_x64\sapjvm\jre\bin\keytool.exe -import -file SAPNetCA.cer -keystore cacerts
```

注意:

可以从 SAP 图像信任的 CA 库中下载 SAPNetCA 证书。默认密钥库密码为 changeit。

- 3 重新启动 Tomcat。

16.6.2.4.3 配置 CTS+ 导出 Web 服务

要配置 CTS+ 导出 Web 服务 (EXPORT_CTS_WS), 必须创建一个 HTTPS 端点。

- 1 使用事务代码soamanager，在“提供者安全性”选项卡的“通信安全性”下，选择“SSL over HTTP（传输通道安全性）”，并在“传输通道身份验证”下，选择“用户 ID/密码”。
- 2 在“传输设置”选项卡的“传输绑定”下，选择“计算协议HTTPS”。

16.6.2.4.4 为 SSL 配置升级管理

记忆：

将服务器证书或信任的 CA 证书导入 JVM 密钥库。

- 1 在 CMC 的“升级管理”选项卡上，单击“设置” > “CTS 设置” > “Web 服务设置”。
- 2 确保 Web 服务 URL 参数包含 https://

注意：

如果无法到达指定的 URL，则“通过 CTS 升级”不会显示在“作业目标”菜单或“覆盖”窗口中。如果升级管理与 CTS+ 之间的 SSL 握手失败，则会显示一个错误。

16.6.2.5 从 CTS+ 导入到 BI 平台

16.6.2.5.1 为 SSL 配置 CTS+

要为 SSL 配置 CTS+，必须创建一个 SSL 服务器 PSE，并将 SAP CA 证书导入到服务器中。有关更多信息，请参阅“To configure SSL for CTS+”（为 CTS+ 配置 SSL）。

注意：

如果 SSL 客户端 PSE 不存在，则系统会默认选择 SSL 服务器 PSE。

相关主题

- 第 543 页上的[“为 CTS+ 配置 SSL”](#)

16.6.2.5.2 配置 BI 平台 Tomcat 以使用 HTTPS

要配置 BI 平台 Tomcat 以使用 HTTPS，必须在安装 BI 平台的计算机上执行以下步骤。

1. 创建一个服务器密钥对、一个证书和一个密钥库。

- a. 使用以下参数运行<安装目录>\win64_x64\sapjvm\jre\bin\keytool.exe:

```
keytool -genkey -alias server -keyalg RSA -keysize 1024 -keystore serverkeystore.jks -storetype JKS  
keytool -certreq -keyalg RSA -alias server -file server.csr -keystore serverkeystore.jks
```

- b. 收到提示后，请输入以下信息:

- 您的名字和姓氏
- 您所在组织单位的名称
- 您所在组织的名称
- 您所在城市或位置的名称
- 您所在州或省的名称
- 此单元对应的 2 个字母的国家/地区代码

将显示一个格式化字符串（例如 CN=John Smith, OU=Accounting, O=SAP, L=Vancouver, ST=BC, C=CA）。输入 yes 并按“回车键”确认。

2. 将服务器证书请求发送至认证机构（CA）。有关更多信息，请参阅“To configure SSL for CTS+”（为 CTS+ 配置 SSL）。
3. 使用以下参数将签署的服务器证书导入服务器密钥库:

```
keytool -import -alias server -keystore serverkeystore.jks -trustcacerts -file server.crt
```

4. 配置 Tomcat 配置文件 server.xml，以启用 HTTPS 并使用已创建的服务器密钥库。
5. 重新启动 Tomcat，并通过浏览器访问以下 URL 验证连接: https://<SERVERNAME>:8443

相关主题

- 第 543 页上的[“为 CTS+ 配置 SSL”](#)

16.6.2.5.3 升级测试和生产系统以使用 HTTPS

要在测试和生产系统上启用 HTTPS，请在 CTS+ 的 “CTS: System details for handling of application types”（CTS：处理应用程序类型的系统详细信息）显示视图中，确保 “Deploy URI”（部署 URI）参数包含 https://

16.6.3 使用 CTS 升级作业

本节介绍升级管理应用程序使用更改传输系统将源系统中的 BI 平台中央管理服务器（CMS）对象升级到目标系统中的工作流程。要使用 CTS 升级作业，请完成以下步骤：

- 1 使用 SAP 身份验证启动升级管理应用程序并创建一个作业。

有关创建新作业的更多信息，请参阅以下相关链接中的 “创建作业” 部分。

注意：

在源系统登录屏幕中，确保将 “SAP” 选作身份验证类型。

- 2 从 “目标” 下拉列表中，选择 “使用 CTS+ 升级” 选项。



- 3 单击 “创建”。

将出现 “从以下系统添加对象：” 屏幕。在此处，文件夹和子文件夹以树状结构显示。

- 4 导航至要从中选择 InfoObject 的文件夹。

- 5 选择要添加到作业中的 InfoObject，并单击 “添加”。如果要添加 InfoObject 并在之后退出 “添加对象” 屏幕，请单击 “添加并关闭”。

InfoObject 即被附加到该作业，并将出现 “升级作业” 屏幕。

注意：

在 “升级作业” 屏幕上，可以执行以下操作：

- 使用 “添加对象” 选项将更多 InfoObject 添加到作业中。有关更多信息，请参阅 “将 InfoObject 添加到作业”。
- 使用 “管理依赖项” 选项管理所选信息对象的依赖项。对象的 SAP BW 依赖项显示在 UI 上并可供用户选择。

有关更多信息，请参阅 “管理作业依赖项”。

- 6 单击 “升级”。

将出现“升级”屏幕，其中显示了当前设置的默认传输请求的 ID、所有者和简短描述。

7. 可以使用“传输请求”超级链接执行以下操作：

- 查看传输请求的详细信息。
 - 更改默认传输请求的设置。
 - 选择其他传输请求。
 - 创建传输请求。
- a. 单击“传输请求”超级链接，以打开“传输组织器” Web 用户界面。
 - b. 如果提示输入登录凭据，请使用 CTS 域控制器系统的有效用户凭据登录。
 - c. 刷新“升级”屏幕，以查看更新。

有关使用“传输组织器” Web UI 的更多信息，请参阅

http://help.sap.com/saphelp_nw70ehp1/helpdata/en/b5/6d03660d3745938cd46d6f5f9cef2e/frame_set.htm。

8. 要查看 SAP BW 对象依赖项的详细信息，请单击“Second level dependencies”（二级依赖项）超级链接。

注意：

单击“Second level dependencies”（二级依赖项）超级链接时，仅显示请求中锁定的对象。如果已释放请求，则无法查看任何依赖项。此外，如果没有活动的二级依赖项，此超级链接将禁用。

9. 单击“升级”。

10. 关闭作业。

将显示升级管理主屏幕。此时，所创建作业的状态将为“已导出到 CTS+”。

11. 通过完成以下步骤将 BI 平台对象释放到目标系统：

- a. 单击显示在想要升级作业状态列中的链接。
将出现“升级状态”窗口。
- b. 单击“请求状态”。
将出现“传输组织器” Web UI。
- c. 如果请求状态为“Modifiable”（可修改），请单击“释放”，以释放 BI 平台对象的传输请求。有关释放包含非 ABAP 对象的传输请求的更多信息，请参阅
http://help.sap.com/saphelp_nw70ehp1/helpdata/en/55/07c497db8140ef8176715d4728eec1/frame_set.htm。
- d. 关闭“传输组织器” Web UI。

12. 要查看 SAP BW 对象的依赖项，请单击“List of BW dependencies”（BW 依赖项列表）超级链接。

注意：

建议向 SAP BW 团队咨询，以获取有关 SAP BW 依赖项及其释放情况的更新，因为这些对象由该团队负责。

13. 关闭“升级状态”窗口。

14. 通过完成以下步骤将 BI 平台对象导入到目标系统：

- a. 登录到 CTS+ 域控制器。
- b. 调用 STMS 事务，进入传输管理系统。
- c. 单击“导入概览”图标。
将出现“导入概览”屏幕，可查看来自所有系统的导入队列项目。

- d 选择目标 LCM 系统的系统 ID。
可以看到可被导入到系统的传输请求列表。
 - e 单击“刷新”。
 - f 导入相关传输请求。有关更多信息, 请参阅http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a39e7acc11d1899e0000e829fbbd/frameset.htm
有关导入 BOLM 内容的传输请求的一般信息, 请参阅
http://help.sap.com/saphelp_nw70ehp1/helpdata/en/09/ca0f3a878f46e9a5a32e666131d2ba/frameset.htm。
15. 如果所选对象具有 SAP BW 依赖项, 请执行以下步骤:
- a 通过完成以下步骤将 SAP BW 依赖项释放到目标系统:
 - 1 登录到 SAP BW 源系统。
 - 2 调用 SE09 事务。将出现“传输组织器”屏幕。
 - 3 单击“显示”。将显示 SAP BW 请求。
 - 4 单击 SAP BW 请求并将其展开, 以查看为依赖项创建的任务。
 - 5 右击与主 SAP BW 对象相关的请求, 并选择“Release Directly”(直接释放)。重复此步骤, 分别释放与每个依赖项相关的任务。
 - 6 右击与主 BW 对象相关的请求并选择“Release Directly”(直接释放)。
 - 7 刷新该屏幕, 直到释放所有请求。

注意:
双击请求日志可以进行查看。
 - b 通过完成以下步骤将 SAP BW 依赖项导入目标系统:
 - 1 登录到 SAP BW 目标系统。
 - 2 调用 STMS 事务, 进入传输管理系统。
 - 3 单击“导入概览”图标。将显示“导入概览”屏幕。
 - 4 双击 SAP BW 目标的系统 ID。可以看到可被导入到系统的传输请求列表。
 - 5 导入相关传输请求。有关更多信息, 请参阅http://help.sap.com/saphelp_nw70ehp1/helpdata/en/44/b4a39e7acc11d1899e0000e829fbbd/frameset.htm
有关传输导入队列的更多信息, 请参阅http://help.sap.com/saphelp_nw70ehp1/helpdata/en/65/8a99386185c064e10000009b38f8cf/frameset.htm。
16. 登录到目标系统以查看所升级作业的状态。
- 有关 Generic CTS 的联机文档的信息, 请参阅 http://help.sap.com/saphelp_ctsplug100/helpdata/en/52/700dbe608e4752a8e2e96a1876f865/frameset.htm

相关主题

- 第 511 页上的“[创建作业](#)”
- 第 515 页上的“[管理作业的依赖项](#)”

第 17 章 差异可视化工具

17.1 升级管理工具中的差异可视化工具

差异可视化工具可用于查看支持的文件类型（LCM BIAR）和/或支持的对象类型（LCM 作业）的两个版本之间的差异。可以使用该功能来确定文件或对象之间的差异，以便开发和维护不同报表类型。该功能会给出源版本和目标版本之间的比较状态。例如，如果用户报表的前一个版本是准确的，而当前版本并不准确，则可以比较和分析文件以便评估实际问题。

下面是可从中检测文件或对象的可视化差异的三种类型：

- “已删除” — 在报表中，如果一个文件版本缺少某个元素，差异类型将显示为“已删除”。例如，元素可以是行、节实例或者块。
- “已修改” — 在报表中，如果在源版本和目标版本之间存在不同的值，差异的类型将显示为“已修改”。例如，值可以是单元内容或区域设置变量的结果。
- “已插入” — 在报表中，如果某个元素仅存在于目标版本中，但源版本中却没有，那么差异的类型将显示为“已插入”。

下面是支持差异可视化工具的对象类型。

- LCMBIAR
- LCM 作业

可以比较以下组合：

- LCM 作业与另一个 LCM 作业
- LCM 作业与 LCMBIAR 文件
- LCMBIAR 文件与另一个 LCMBIAR 文件
- LCMBIAR 文件与 LCM 作业

首选项

在差异可视化工具主页中，可以设置首选项，如产品区域设置、首选查看区域设置、每页的最大对象数、时区和未保存数据的提示。

主页

差异可视化工具主页包含以下选项卡和窗格：

- 新建比较 — 该选项卡可用于在对象之间创建新比较

- 搜索比较 — 该字段可用于搜索已比较的对象
- 比较窗格 — 该窗格列出过滤器和差异选项卡
- 比较：差异窗格 — 该窗格将列出所比较的对象与比较名称、日期/事件和差异状态

17.1.1 使用差异可视化工具比较对象或文件

差异可视化工具选项可用于比较 BIAR 文件和对象。

要使用差异可视化工具比较文件，请执行以下步骤：

- 1 登录到 CMC 应用程序。
- 2 在 CMC 主页的“管理”选项卡下，单击“差异可视化工具”链接。
“差异可视化工具”页面随即出现。已比较的文件将存储在“差异”文件夹或用户创建的任何子文件夹中。

注意：

要创建新的子文件夹，请单击“文件夹”图标。

- 3 选择“新建比较”。
“差异可视化工具 — 比较”屏幕随即出现。
- 4 从“参考”下的“选择系统”中选择参考系统。
可以连接到以下参考系统之一：

- CMS
- VMS
- 本地文件系统

- 5 单击“浏览”选择要比较的对象或本地系统中的文件。
- 6 从“目标”下的“选择系统”中选择目标系统。
可以连接到以下参考系统之一：

- CMS
- VMS
- 本地文件系统

注意：

如果登录到 CMS 或 VMS，参考系统中的选定对象也可自动匹配参考系统中的同名对象。

- 7 单击“浏览”选择要比较的对象或本地系统中的作业。
- 8 单击“添加”。

选择用来进行比较和添加到信息对象列表的对象。

如果向信息对象列表添加了多对对象，那么可以将这些对象安排在以后某个时间进行比较。但是，如果信息对象列表仅包含一对对象，即可比较这些对象。

要比较文件，请继续下一步。要计划比较，请参见第 553 页上的 [“计划比较”](#)。

9. 单击“比较”可比较对象或文件夹。

注意：

LCMBIAR/LCM 作业文件的比较包括：

- LCMBIAR 元数据：比较作业详细信息，如名称、创建者、时间等等。
- 主要对象：通过 CUID 比较在 LCMBIAR 中显式选定的每个对象与目标 LCMBIAR 中的类似对象。
- 依赖对象：通过 CUID 比较文件中选定的依赖对象与目标中的类似对象。

如果选择了非 LCMBIAR 或 LCM 作业对象，将显示以下错误消息：“未找到插件”。

比较进程即时启动，而差异（如果有）将显示在“差异可视化工具的查看器”中。差异将以橙色突出显示，而缺少的对象则以红色突出显示。

也可使用过滤器选项按类型查看具有差异或公共属性的比较对象。

10. 单击“保存”，以保存差异报告。
11. 指定要保存报表的位置，并单击“确定”。

17.1.2 在版本管理系统中比较对象或文件

可以通过使用差异可视化工具选项在版本管理系统中比较升级管理作业或文件夹。

要在版本管理系统中比较对象，请完成以下步骤：

1. 登录到 CMC 应用程序。
2. 在 CMC 主页的“管理”选项卡下，单击“差异可视化工具”链接。
“差异可视化工具”页面随即出现。已比较的文件将存储在“差异”文件夹或用户创建的任何子文件夹中。
- 注意：**
要创建新的子文件夹，请单击“文件夹”图标。
3. 选择“新建比较”。
“差异可视化工具 — 比较”屏幕随即出现。
4. 从“参考”下的“选择系统”下拉菜单中选择“登录到 VMS”。
5. 输入 VMS 的登录凭据，并单击“登录”。
“自动选择目标系统”对话框随即出现。
6. 若要设置另一目标系统，请单击“否”；若要将目标系统设置为与参考系统相同，请单击“是”。
7. 单击“浏览”从参考和目标系统中选择要比较的对象或作业。
8. 单击“添加”。

为比较选定的对象将在“新建比较”窗格中列出。

可以立即比较文件，或者计划以后比较。要比较文件，请继续下一步。要计划比较，请参见第 553 页上的 [“计划比较”](#)。

- 。9 单击“比较”可比较作业或文件夹。

比较进程即时启动，而差异（如果有）将显示在“差异可视化工具的查看器”中。差异将以橙色突出显示，而缺少的对象则以红色突出显示。

也可使用过滤器选项按类型查看具有差异或公共属性的比较对象。

- 。01 单击“保存”，以保存差异报告。
- 。11 指定要保存报表的位置，并单击“确定”。

17.1.3 计划比较

要计划比较文件或对象，请执行以下步骤：

- 1 单击“计划”。
- 将出现“计划”窗口。
- 2 从“运行比较”列表中选择计划比较的频率。
- 3 在相应字段中指定允许的重试次数和重试时间间隔。

注意：

仅在指定重试次数时才可指定重试时间间隔。

- 4 指定报表名称，并单击“浏览”以浏览想要保存报表的位置。
- 将出现“作业保存于”窗口。
- 5 选择保存报表所需的文件夹，然后单击“确定”。

注意：

用户必须相应地指定比较日期和时间，具体取决于从“运行比较”列表中选择的事项。

- 6 单击“计划”。

用户稍后可在差异可视化工具的查看器中查看比较对象或差异报表。“已比较差异”页面显示文件夹和文件列表，或显示比较报表。

“已比较差异”页面还包含以下选项：

- 历史记录：“历史记录”选项可用于查看比较的历史记录。
- 重新运行：“重新运行”选项可用于再次运行比较。
- 计划：“计划”选项可用于计划比较。

第 18 章 管理应用程序

18.1 通过 CMC 管理应用程序

18.1.1 概述

利用 CMC 的“应用程序”管理区域，无需进行任何编程即可更改 Web 应用程序（如 CMC 和 BI 启动板）的外观和功能。也可以修改用户、组和管理员的应用程序访问权限，方法是修改与每个对象关联的权限。

本节提供了有关如何管理各种设置的上下文信息、程序和说明。以下应用程序包含可以通过 CMC 修改的设置：

- Analysis (OLAP 版)
- 警报应用程序
- BI 启动板
- BI 工作区
- 中央管理控制台
- 协作（凭借 SAP Jam 或 SAP StreamWork）
- Crystal Reports 配置
- Dashboards
- 讨论区
- 信息设计器
- 监控应用程序
- 多租户
- OpenDocument
- 平台搜索应用程序
- 升级管理

- 报表转换工具
- SAP BusinessObjects Mobile
- 翻译管理工具
- Universe 设计工具
- 升级管理工具
- 差异可视化工具
- Web Intelligence
- Web 服务
- 微件

18.1.2 应用程序的常规设置

18.1.2.1 设置用户对应用程序的权限

可以使用权限来控制用户对应用程序中某些功能的访问。通过 CMC 中的“应用程序”区域，可以将主体分配到某个应用程序的访问控制列表、查看主体拥有的权限，以及修改主体对某个应用程序拥有的权限。有关权限管理的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》。

18.1.2.2 在 CMC 中设置 Web 应用程序跟踪日志级别

要跟踪其他 Web 应用程序，必须手动配置相应的 BO_trace.ini 文件。

1. 在 CMC 的“应用程序”区域，右击应用程序，选择“跟踪日志设置”。

注意：

这些应用程序具备跟踪日志设置：BI 启动板、CMC、OpenDocument、升级管理、版本管理、差异可视化和 Web 服务。

将显示“跟踪日志设置”对话框。

- 2 从“日志级别”列表中选择设置。
- 3 单击“保存并关闭”。

新的跟踪日志级别将在下次登录 Web 应用程序后生效。

相关主题

- 第 823 页上的[“跟踪日志级别”](#)

18.1.2.2.1 跟踪日志级别

下列跟踪日志级别可用于 BI 平台组件：

级别	说明
未指定	跟踪日志级别通过其他方式（通常为 .ini 文件）指定。
无	未发生跟踪。
低	跟踪日志过滤器允许记录错误消息，但忽略警告和状态消息。记录组件启动、关闭、启动请求和结束请求消息的重要状态消息。建议不要为调试使用此级别。
中	跟踪日志过滤器设置为包括错误、警告和大多数状态消息。过滤掉重要性很低或极其冗长的状态消息。此级别对于调试来说不够详细。
高	不过滤任何消息。建议为调试使用此级别。 警告： 该跟踪日志级别将严重影响系统资源，增加 CPU 使用量，并消耗存储空间。

18.1.3 应用程序特定设置

18.1.3.1 管理 CMC 应用程序设置

18.1.3.1.1 身份验证和程序对象

请留意将程序对象添加到资源库时存在的潜在安全风险。程序对象运行所依据帐户的文件权限级别将确定该程序可对文件进行什么修改（如果有）。

您可以控制用户可运行的程序对象的类型，也可以配置运行程序对象所必需的凭据。

启用或禁用某种程序对象类型

作为第一层安全保障，您可以配置可供使用的程序对象的类型。

所有平台上的身份验证

在 CMC 的“文件夹”管理区域中，必须为程序运行所依据的帐户指定凭据。利用此功能，可以为程序设置特定的用户帐户，并向其分配适当的权限，以便使用该帐户运行程序对象。

或者，将程序对象添加到 BI 平台的用户可以将自己的凭据分配给程序对象，以便程序能够访问系统。因此，程序将依据该用户帐户运行，并且程序的权限将被限制为用户的权限。如果选择不为程序对象指定用户帐户，程序将依据默认系统帐户运行，该帐户通常具有本地权限，但没有网络权限。

注意：

默认情况下，当您计划程序对象时，如果未指定凭据，作业将失败。要提供默认的凭据，请在“应用程序”管理区域中选择“CMC”。选择“操作” > “程序对象权限”，然后选择“使用以下操作系统凭据进行计划”，并输入默认用户名和密码。

Java 程序的身份验证

BI 平台允许为所有程序对象设置安全性。对于 Java 程序，BI 平台会强制使用 Java 策略文件，该文件具有与适用于不安全代码的 Java 默认值一致的默认设置。使用 Java 策略工具（Java 开发工具包附带）修改 Java 策略文件以适合您的特定需求。

Java 策略工具包含两个基本代码项。第一个条目指向 BI 平台 Java SDK，并使程序对象对所有 BI 平台 JAR 文件都具有完全访问权限。第二个基本代码项适用于所有本地文件。它针对不安全代码使用的安全设置与针对不安全代码的 Java 默认设置相同。

注意：

- Java 策略的设置对同一计算机上的所有自适应作业服务器均适用。
- 默认情况下，Java 策略文件安装在 BI 平台安装根目录中的 Java SDK 目录下。例如，Windows 上的典型位置是：C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\conf\crystal-program.policy。

18.1.3.1.1 启用或禁用某种程序对象类型

- 1 在“应用程序”区域中，选择“中央控制管理台”。
 - 2 单击“操作” > “程序对象权限”。
- 将会出现“程序对象权限”对话框。
- 3 在“允许用户”区域中，选择希望用户能够运行的程序对象的类型。

可以选择“运行脚本/二进制文件”或“运行 java 程序”。

如果选择了“运行 java 程序”，则可以选中或清除“使用身份模拟”复选框。此选项为 Java 程序提供了用于登录到 Business Intelligence 平台的标记。

- 4 单击“保存并关闭”。

18.1.3.1.2 向系统注册处理扩展

注意：

此功能不适用于 Web Intelligence 文档。

您必须使您的代码库可用于将处理相关“计划”或“查看”请求的每台计算机，然后才能将处理扩展应用于特定对象。安装 BI 平台将在每个作业服务器、处理服务器和报表应用程序服务器（RAS）上为处理扩展创建一个默认目录。建议您将处理扩展复制到每台服务器上的默认目录。在 Windows 上，该默认目录为 C:\Program Files\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\win32_x86\ProcessExt。在 Unix 上的目录为 sap_bobj/ProcessExt。

提示：

可以共享处理扩展文件。

取决于您写入扩展的功能，请将库复制到以下计算机上：

- 如果处理扩展仅拦截“计划”请求，请将库复制到以自适应作业服务器方式运行的每台计算机上。
- 如果处理扩展只拦截“查看”请求，请将库复制到以 Crystal Reports 处理服务器或 RAS 方式运行的每台计算机上。
- 如果处理扩展拦截“计划”和“查看”请求，请将库复制到以自适应作业服务器、Crystal Reports 处理服务器或 RAS 方式运行的每台计算机上。

注意：

如果只有对特定服务器组做出的“计划”/“查看”请求才需要处理扩展，则只需要将库复制到组中的每台处理服务器。

18.1.3.1.2.1 向系统注册处理扩展

- 1 转到 CMC 的“应用程序”管理区域。
 - 2 选择“中央控制管理台”。
 - 3 单击“操作” > “处理扩展”。
- 将出现“处理扩展：CMC”对话框。
- 4 在“名称”字段中，输入处理扩展程序的显示名称。
 - 5 在“位置”字段中，键入处理扩展的文件名以及任何其他路径信息。
 - 如果将处理扩展复制到每台相应计算机上的默认目录中，则只需要输入文件名（但不带文件扩展名）。
 - 如果将处理扩展复制到默认目录下的子文件夹，请按以下方式键入位置：子文件夹/文件名
 - 6 使用“说明”字段来添加有关处理扩展的信息。
 - 7 单击“添加”。

提示：

若要删除处理扩展，请从“现有扩展”列表中选择该扩展，然后单击“删除”。（确保没有任何重复性作业基于此处理扩展，因为基于此处理扩展的任何将来的作业都会失败。）

- 8 单击“保存并关闭”。

处理扩展便会注册到 CMC 中。

现在，您即可选择此处理扩展以将它的逻辑应用于特定对象。

18.1.3.1.2.2 在多台服务器之间共享处理扩展

注意：

此功能不适用于 Web Intelligence 文档或在 SAP Crystal Reports for Enterprise 中创建的报表。

如果要将所有处理扩展放在一个位置，则可以覆盖每台自适应作业服务器、Crystal Reports 处理服务器和 RAS 的默认处理扩展目录。首先，将处理扩展复制到可供所有服务器访问的网络驱动器上的一个共享目录。从每台服务器的计算机中映射（或安装）网络驱动器。

注意：

Windows 上映射的驱动器只有在重新启动计算机后才会生效。

如果同时在 Windows 和 Unix 上运行服务器，则必须将每个处理扩展的 .dll 和 .so 版本复制到共享目录中。此外，在 Windows 和 Unix 计算机上必须都能够（通过 Samba 或某些其他文件共享系统）看到共享的网络驱动器。

最后，更改每台服务器的命令行以修改默认处理扩展目录。要更改命令行，请转到 CMC 中的“服务器”选项卡，选择服务器并打开其“属性”页面。将 `-report_ProcessExtPath absolute path` 添加到命令行。将 `absolute path` 替换为新文件夹的路径，并使用适合于运行服务器的操作系统的路径约定（例如，`M:\code\extensions`、`/home/shared/code/extensions` 等）。

要修改默认的处理扩展目录，请使用 CMC 停止服务器。然后，打开服务器的“属性”来修改命令行。完成后再次启动服务器。

18.1.3.1.3 管理 CMC 选项卡访问

18.1.3.1.3.1 委派的管理和 CMC 选项卡访问

通常，一名 BI 平台系统管理员可以管理大量文档、文件夹、用户、服务器和其他对象。但是，大型企业环境的资源可能会超出单个管理员的负担能力。这时，希望仅专注于高优先级任务的系统管理员可以创建委派的管理员，将部分管理任务分配给他们（例如，管理某个部门或租户内容）。与系统管理员不同，委派的管理员执行的任务有限，对系统中的对象所具备权限也较少。

中央管理控制台的默认配置允许用户访问所有可用的 CMC 选项卡。系统管理员可以管理 CMC 选项卡访问，控制主体（用户或用户组）能够看到哪些选项卡。为改进委派的管理员的用户体验和工作流，系统管理员还可以隐藏任何委派的管理员用不到的 CMC 选项卡。

警告：

CMC 选项卡访问的管理只影响 CMC 用户界面的外观。隐藏 CMC 选项卡并不是一项安全措施，因为这不会设置或修改选项卡内对象的安全权限。要确保用户无法对未经授权的对象执行未经授权的操作（例如，通过中央配置管理器或基于 BI 平台 SDK 的第三方软件管理服务器），必须为对象（例如服务器对象）设置适当的安全权限。

相关主题

- 第 562 页上的[“管理其他用户的 CMC 选项卡访问”](#)
- 第 564 页上的[“管理为其他用户或用户组配置 CMC 选项卡访问的权限”](#)

18.1.3.1.3.2 使用 CMC 选项卡访问

18.1.3.1.3.2.1 管理其他用户的 CMC 选项卡访问

系统管理员始终可以访问所有 CMC 选项卡。请遵循以下原则来管理主体可以访问的 CMC 选项卡：

- 为简化管理流程，减少维护和故障排除的需求，建议管理员在用户组级别（而不是用户级别上）管理 CMC 选项卡访问。
- 对于具有顶级文件夹的 CMC 选项卡，管理员在授予对某个选项卡的访问权限时，必须同时授予对该选项卡顶级文件夹的“查看”权限。以下 CMC 选项卡支持顶级文件夹：
 - “访问级别”
 - “日历”
 - “类别”
 - “（Universe）连接”
 - “加密密钥”
 - “事件”
 - “联盟”
 - “文件夹”

- “收件箱”
 - “OLAP 连接”
 - “个人类别”
 - “个人文件夹”
 - “配置文件”
 - “复制列表”
 - “服务器和组”
 - “临时存储”
 - “Universe”
 - “用户和组”
 - “Web 服务查询”
- 为提高系统安全性，仅管理员组成员可访问下列 CMC 选项卡。作为系统管理员，管理员组成员可访问所有 CMC 选项卡，无论 CMC 选项卡访问权限如何。CMC 选项卡访问权限用于控制委派的管理员（即管理员组成员外的用户）对 CMC 选项卡的访问。
 - 审核
 - 身份验证
 - 加密密钥
 - 许可密钥
 - 监控
 - 会话
 - 设置
 - 用户属性管理

警告：

CMC 选项卡访问的管理只影响 CMC 用户界面的外观。隐藏 CMC 选项卡并不是一项安全措施，因为这不会设置或修改选项卡内对象的安全权限。要确保用户无法对未经授权的对象执行未经授权的操作（例如，通过中央配置管理器或基于 BI 平台 SDK 的第三方软件管理服务器），必须为对象（例如服务器对象）设置适当的安全权限。

18.1.3.1.3.2.1.1 管理其他用户的 CMC 选项卡访问

- 1 登录到 CMC。
- 2 在“用户和组”选项卡中，右击某个主体并选择“CMC 选项卡配置”。

注意：

如果 CMC 选项卡访问不受限制，则会显示以下消息：警告：CMC 选项卡访问目前不受限制。要限制 CMC 访问，单击“应用程序”选项卡，选择“CMC”，然后设置 CMC 选项卡访问为受限。CMC 选项卡受限之后，这些设置将生效。您仍然可以配置 CMC 选项卡访问。但是，配置要在限制 CMC 选项卡访问之后才会生效。

在“Configure CMC Tab Access”（配置 CMC 选项卡访问）对话框中，将显示一个表：

- 或 表示主体可以访问哪些 CMC 选项卡。
- “继承”表示选项卡访问权限继承自父用户组。
- “显式”表示选项卡访问权限是在主体级别上显式指定的。

3 检查 CMC 选项卡访问权限。要修改权限，可以使用工具栏上的按钮：

- 单击“授予”以显式授予对某个选项卡的访问权限。
- 单击“拒绝”以显式拒绝对某个选项卡的访问权限。
- 单击“继承”以使用继承的访问权限。

注意：

单击按钮可立即将更改应用于主体。

4 完成时，单击“关闭”。

新生效的选项卡访问权限将显示在表的“权限”列中。

相关主题

- 第 566 页上的“[限制 CMC 选项卡访问](#)”

18.1.3.1.3.2.1.2 继承 CMC 选项卡访问

对于 CMC 选项卡访问权限和配置其他用户或用户组的 CMC 选项卡访问的权限，其应用和继承方式与其他 BI 平台安全权限相同。如果主体没有明确指定的选项卡访问权限，他们将继承自己所在用户组的选项卡访问权限。

如果某个用户是两个用户组的成员，选项卡访问权限的计算方式与所有其他 BI 平台权限相同。例如，如果在一个组中授予了对某个 CMC 选项卡的访问权限，但在另一个组中为拒绝，则主体将不能访问该 CMC 选项卡。

注意：

- 对于继承某个用户组的权限的所有用户或用户组，如果其 CMC 选项卡访问权限设置为“继承”，则修改该用户组的 CMC 选项卡访问权限将更改其相同的选项卡访问权限。
- 在用户级别上设置的选项卡访问权限将始终取代继承自用户组的选项卡访问权限。

18.1.3.1.3.2.1.3 委派的管理员用户组

可以创建一组委派的管理员用户组以简化 CMC 选项卡管理。为避免逐个配置 CMC 选项卡访问，可以使现有用户或用户组成为委派的管理员用户组的成员。建议采用以下配置，但针对特定业务需求可以对其进行修改。

注意：
如果权限设置为“继承”，则多个组的成员身份会导致权限增加。

委派的管理员用户组	建议的权限
系统管理员	授予对所有选项卡的访问权限。
用户管理员	授予对“访问级别”、“文件夹”、“收件箱”、“个人文件夹”、“个人类别”、“查询结果”、“会话”和“用户和组”的访问权限。将所有其他选项卡设置为“继承”。
内容管理员	授予对“日历”、“类别”、“事件”、“文件夹”、“实例管理器”、“个人类别”、“个人文件夹”、“配置文件”、“查询结果”和“Universe”的访问权限。将所有其他选项卡设置为“继承”。
服务器管理员	授予对“服务器”和“应用程序”的访问权限。将所有其他选项卡设置为“继承”。

18. 1. 3. 1. 3. 2. 1. 4 管理为其他用户或用户组配置 CMC 选项卡访问的权限

在大型企业环境中，系统管理员可能需要将 CMC 选项卡访问管理委托给某个委派的管理员。或者，在多租户系统中，每个租户可能有一个委派的管理员负责管理其他用户和用户组对 CMC 选项卡的访问。

- 1 登录到 CMC。
 - 2 在“用户和组”选项卡中，右击某个主体并选择“CMC 选项卡配置”。
- 在“配置 CMC 选项卡”对话框中，将为该主体显示“配置其他用户（或用户组）对 CMC 选项卡的访问”。

注意：
如果授予此权限，该主体将能够管理对其具有“安全地修改权限”权限的用户对 CMC 选项卡（仅限主体具有访问权限的选项卡）的访问。此外，通过将“配置其他用户（或用户组）对 CMC 选项卡的访问”权限授予主体对其具有“安全地修改权限”权限的用户，主体还可以进一步将 CMC 选项卡访问管理委派给其他用户。

- 或 表示主体是否具有为其他用户或用户组配置 CMC 选项卡的权限。
 - “继承”表示权限继承自父用户组。
 - “显式”表示权限是在主体级别上显式指定的。
- 3 检查配置其他用户或用户组对 CMC 选项卡的访问的权限。要修改权限，可以从列表中选择以下设置之一：
- 单击“授予”以显式授予管理其他用户或用户组对 CMC 选项卡的访问的权限。
 - 单击“拒绝”以显式拒绝管理其他用户或用户组对 CMC 选项卡的访问的权限。
 - 单击“继承”以继承管理其他用户或用户组对 CMC 选项卡的访问的权限。

注意：

从列表中选择某个设置将立即更改主体的权限。

- 4 完成时，单击“关闭”。

系统将显示新生效的权限。

相关主题

- 第 560 页上的[“委派的管理和 CMC 选项卡访问”](#)
- 第 563 页上的[“继承 CMC 选项卡访问”](#)

18.1.3.1.3.2.1.5 添加用户或用户组的自定义选项卡

必须先将 CMC 选项卡设置为“受限”，才能添加用户或用户组的“自定义”选项卡。

- 1 在 CMC 中，转到“用户和组”管理区域。
- 2 右击用户或用户组，并选择“CMC 选项卡配置”。

将出现“配置 CMC 选项卡”对话框，列出每个 CMC 选项卡标题及其用户组的权限级别。

如果对话框顶部以红色显示以下警告消息，则必须先将 CMC 选项卡访问设置为受限，才可以添加“自定义”选项卡：

警告：CMC 选项卡访问当前不受限制。要限制 CMC 访问，单击“应用程序”选项卡，选择“CMC”，然后设置 CMC 选项卡访问为受限。CMC 选项卡为受限之后，这些设置将生效：

- 3 （如有必要）设置 CMC 选项卡为受限：
 - a 在 CMC 的“应用程序”管理区域，右击“中央管理控制台”并选择“CMC 选项卡访问配置”。
 - b 在“CMC 选项卡访问”中，选择“受限”选项，然后单击“保存并关闭”。
- 4 在用户组的“配置 CMC 选项卡”对话框中，从列表中为每个 CMC 选项卡选择“授予”、“拒绝”或“继承”。

每更改一个选项卡的权限时，“配置 CMC 选项卡”对话框将更新用户组配置其他用户或用户组选项卡访问的权限。

- 5 单击“关闭”。

18.1.3.1.3.2.2 限制 CMC 选项卡访问

建议先为主体配置 CMC 选项卡访问，然后再限制 CMC 选项卡访问。如果在配置之前限制选项卡访问，用户在管理员授予其访问权限之前将无法访问任何 CMC 选项卡。

为确保与以前的 BI 平台版本保持一致，CMC 选项卡访问在安装 BI 平台之后的初始状态下是不受限制的，能够访问 CMC 的任何用户均可以访问所有可用的选项卡。为防止用户访问其无权访问的选项卡，系统管理员可以限制 CMC 选项卡访问。

在紧急情况下或者要对 CMC 选项卡访问配置进行故障排除时（例如，委派的管理员无法访问某个重要的 CMC 选项卡），可以取消 CMC 选项卡访问限制。

- 1 登录到 CMC。
- 2 在“应用程序”选项卡中，右击“中央管理控制台”并选择“CMC 选项卡访问配置”。这将显示“CMC 选项卡访问”对话框。
- 3 配置 CMC 选项卡访问规则。
 - 要将用户限制为只能访问具备权限的选项卡，请选择“受限”。
 - 要允许用户访问所有选项卡，请选择“不受限”。

- 4 完成后，单击“保存并关闭”。

CMC 选项卡访问规则将应用于系统。

相关主题

- 第 566 页上的“[CMC 选项卡访问故障排除](#)”

18.1.3.1.3.2.3 CMC 选项卡访问故障排除

要防止未经授权的访问或解决用户对 CMC 选项卡访问受限的问题，可以对用户的 CMC 选项卡访问权限进行故障排除。

- 1 以管理员身份登录 CMC。

注意：

确保您有权访问要进行故障排除的选项卡，并具有该用户的“安全地修改权限”权限。

- 2 在“用户和组”选项卡中，右击某个主体并选择“CMC 选项卡配置”。
系统显示“Configure CMC Tab Access”（配置 CMC 选项卡访问）窗口。
- 3 检查有效的 CMC 选项卡访问权限。您可以明确授予或拒绝对可用选项卡的访问权限。
如果 CMC 选项卡访问权限是继承的，但有效的选项卡访问权限与用户需求不匹配：
 - a 编译选定主体所在的所有用户组的列表。
 - b 为用户从中继承选项卡访问权限的每个组重复步骤 1-3。
 - c 根据需要在主体级别或在组级别下更正 CMC 选项卡访问权限。

注意：

在组级别上执行此任务，将影响该用户组中所有用户以及从该用户组继承权限的用户组中所有用户的 CMC 选项卡访问权限，只要这些用户将 CMC 选项卡访问设置为“继承”。

- 4 完成时，单击“关闭”。

相关主题

- 第 562 页上的[“管理其他用户的 CMC 选项卡访问”](#)
- 第 563 页上的[“继承 CMC 选项卡访问”](#)

18.1.3.2 管理讨论设置

在 BI 平台中，可以在 CMC 的“应用程序”区域中指定讨论线索的系统级别设置。

对于“讨论区”应用程序，可以通过多种方式管理并与讨论线索交互，包括：

- 根据指定搜索标准搜索讨论线索。
- 排序讨论线索的搜索结果。
- 删除讨论线索。

注意：

用户权限设置不可用于讨论区应用程序。但是，可以设置对个别报表的权限。

18.1.3.2.1 搜索一个讨论线索

默认情况下，“讨论区”页显示所有讨论线索的标题。只显示根级别线索。

要分页浏览讨论线索的列表，请使用“上一页”和“下一页”按钮。也可以搜索一个特定线索或线索组。

- 1 转到 CMC 的“应用程序”区域，然后选择“讨论区”。
- 2 单击“管理” > “管理线索”。
- 将显示“注释管理”对话框。
- 3 在“字段名称”列表中，选择一个选项。

选项	说明
线索标题	按线索标题进行搜索。
创建日期	按创建日期进行搜索。
上次修改日期	按上次修改日期进行搜索。
作者	按作者进行搜索。

- 4 在第二个列表上改进搜索。

注意：
搜索不区分大小写。

- 如果选择了“线索标题”或“作者”，请从第二个字段中的以下选项进行选择。

选项	说明
是	搜索线索标题或作者姓名与您在第三个字段中键入的文本完全匹配的讨论线索。
不是	搜索线索标题或作者姓名与您在第三个字段中键入的文本不完全匹配的讨论线索。
包含	搜索在线索标题或作者姓名的任何部分中包含搜索文本字符串的讨论线索。
不包含	搜索在线索标题的任何部分中不包含文本字符串的讨论线索。

- 如果选择了“创建日期”或“上次修改日期”，请选择以下其中一个选项，然后指定搜索日期。

选项	说明
之前	搜索在搜索日期之前创建或修改的讨论线索。
之后	搜索在搜索日期之后创建或修改的讨论线索。
介于	搜索在两个搜索日期之间创建或修改的讨论线索。

- 5 要进一步改进搜索，请使用第三个文本字段。
 - 如果在前两个字段中选择了基于文本的搜索，请键入文本字符串。
 - 如果选择了基于日期的搜索，请在相应的字段中输入一个或多个日期。
- 6 单击“搜索”。

18.1.3.2.2 对讨论线索的搜索结果进行排序

在搜索讨论线索时，可以选择希望如何显示搜索结果。例如，可以按字母升序对搜索结果进行排序，并选择每页显示多少个结果。

- 1 转到 CMC 的“应用程序”区域，然后选择“讨论区”。
- 2 单击“管理” > “管理线索”。
- 将显示“注释管理”对话框。
- 3 在“排序依据”列表中，选择一个排序选项。

选项	说明
线索标题	按讨论线索的标题排序。
创建日期	按讨论线索的创建日期排序。
上次修改日期	根据讨论线索的上次修改日期排序。
作者	按特定讨论线索的作者排序。

- 4 在第二个列表中，选择是以升序还是降序显示记录。
- 5 在第三个文本字段中，输入要在每页中显示的讨论线索结果的个数。
默认为每页 10 个结果。
- 6 单击“搜索”。

18.1.3.2.3 删除讨论线索

在 BI 平台中，可以在 CMC 的“应用程序”区域中删除任何讨论线索。

- 1 转到 CMC 的“应用程序”区域，然后选择“讨论区”。
- 2 单击“管理” > “管理线索”。
将显示“注释管理”对话框。
- 3 在结果列表中，搜索并选择要删除的讨论线索。
- 4 单击“删除”。

18.1.3.3 管理 BI 启动板设置

在 BI 平台中，在 CMC 的“应用程序”区域中，选择“管理” > “属性”，查看 BI 启动板的显示选项。

对于 BI 启动板，可向用户或组授予以下功能：

- 更改首选项
- 组织文件夹
- 搜索
- 按对象类型过滤对象列表
- 查看“收藏夹”文件夹

例如，如果已使用标准命名规则创建用户文件夹，则可能不允许用户组织其各自的文件夹。

注意：

默认情况下，所有用户都能访问以上功能。

18.1.3.3.1 更改 BI 启动板的显示设置

- 1 转到 CMC 的“应用程序”区域，然后双击“BI 启动板”。
随后将显示“BI 启动板属性”对话框。
- 2 要为 BI 启动板用户启用讨论区，请选择“启用讨论区”复选框。
- 3 要启用过滤器进行计划，请选中“在“计划”页上显示“过滤器”选项卡”复选框。
在计划 Crystal 报表时，此设置控制用户是否可以键入记录或组选择公式。
- 4 单击“保存并关闭”。

18.1.3.4 管理 Web Intelligence 设置

可以通过设置 Web Intelligence 应用程序的属性控制用户有权限访问 Web Intelligence 文档的哪些功能。

18.1.3.4.1 修改 Web Intelligence 的显示设置

- 1 转到 CMC 的“应用程序”区域，然后选择“Web Intelligence”。
- 2 单击“管理” > “属性”。
将出现“属性”对话框。
- 3 定义以下任意显示选项。

选项	说明
维和明细	使用此区域中的选项来定义添加的数据如何在报表中显示；更改字体样式、文本颜色和背景颜色。单元格预览会自动显示所做的更改。完成后单击“确定”。
波动值（数字度量）	使用此区域中的选项来修改页面标题并设置其格式；更改字体样式、文本颜色和背景颜色。单元格预览会自动显示所做的更改。完成后单击“确定”。
“嵌入式图像的属 性”	输入嵌入式图像的最大大小。
快速显示模式属性	在适当的字段中，输入最大纵向记录数、最大横向记录数、最小页面宽度、最小页面高度、右填充值和下填充值。

选项	说明
自动保存设置	设置文档的自动保存时间间隔。每次手动或自动保存文档时，都会重置该时间间隔。当手动保存文档时，还会删除自动保存的文档。
自动刷新	<p>在选择 Web Intelligence 文档属性的“自动刷新”时，启用 Web Intelligence 文档的自动刷新功能。</p> <p>有关详细信息，请参阅《SAP BusinessObjects Web Intelligence 用户指南》。</p>
自动合并	<p>在选择 Web Intelligence 文档属性“自动合并维”时，启用维的自动合并功能。</p> <p>有关详细信息，请参阅《SAP BusinessObjects Web Intelligence 用户指南》。</p>
打开安全权限设置时自动刷新文档	使用此选项可使 Web Intelligence 在打开时自动刷新文档，而无需在 Web Intelligence 文档属性中启用“打开时刷新”。选择此选项即选择安全权限“文档 — 禁用打开时自动刷新”。
智能视图	<p>当用户在 Web Intelligence 中打开文档时，该选项确定显示哪个文档版本。</p> <ul style="list-style-type: none"> 查看最新的实例 <p>打开对象的最新实例。例如，如果计划文档每小时刷新一次，且文档上次保存和关闭是在五小时前，则将打开最新的实例。当用户保存该实例时，原始文档则相应地进行更新。</p> <ul style="list-style-type: none"> 查看对象 <p>无论是否可能已发生任何计划的刷新，文档均将以其上次保存时的相同状态打开。</p>

- 4 单击“保存并关闭”。

注意：

要将所做的选择恢复为默认的显示变量，请单击“重置”。

18.1.3.5 管理警报设置

在 BI 平台中，可以在 CMC 的“应用程序”区域中指定警报的系统级别设置。

对于“警报”应用程序，可以通过下列操作控制和定义系统用户访问警报的方式：

- 为警报预订者启用“我的警报”文件夹
- 启用通过电子邮件发送警报消息，并设置警报消息的格式
- 设置系统中的警报数量限制
- 设置警报消息的到期期限

相关主题

- 第 555 页上的“[设置用户对应用程序的权限](#)”

18.1.3.5.1 修改警报目标属性

- 1 在 CMC 的“应用程序”区域中，双击“警报应用程序”。
- 2 单击“管理” > “属性”。
将显示“警报”对话框。
- 3 （必需）然后执行下列任一操作：
 - 选择“启用我的警报”，警报预订者可在 BI 启动板的“我的警报”区域中收到通知。
 - 选择“启用电子邮件”，警报预订者可通过电子邮件收到通知。
随后将显示警报的全球电子邮件选项。
- 4 如果已选择“启用电子邮件”，请执行以下操作：
 - 在“发件人”框中，输入将发出警报通知的电子邮件地址。
预订者将收到此电子邮件地址发送的警报电子邮件。使用系统能够识别的有效电子邮件地址。
 - 在“收件人”框中，输入警报预订者的电子邮件地址。
默认情况下，所有系统的警报均将发送至此电子邮件地址。
提示：
请勿指定电子邮件地址或收件人。使用 %SI_EMAIL_ADDRESS% 占位符。
 - 在“抄送”框中，输入应接收警报抄送副本的每个收件人的电子邮件地址。
 - 在“主题”框中，输入包含警报的电子邮件所使用的默认主题标题。
 - 在“正文”框中，输入包含警报的电子邮件所包含的默认消息。

- 选择“添加附件”，可默认将附件添加到包含警报的电子邮件中。
例如，选择此选项将添加含触发警报的相关 Crystal 报表。
- 如果已选择“添加附件”，则可在“文件名”中选择“自动生成”或“特定名称”来指示如何命名电子邮件中的附件。

5 单击“保存并关闭”。

相关主题

- 第 555 页上的[“设置用户对应用程序的权限”](#)
- 第 572 页上的[“管理警报设置”](#)

18.1.3.5.2 修改警报默认属性

- 1 转到 CMC 的“应用程序”区域，然后选择“警报应用程序”。
- 2 单击“管理” > “属性” > “默认设置”。
- 3 为下列属性设置相应的值。

选项	说明
到期期限	指定警报消息应在系统中保留多长时间后才删除。
警报消息数上限	指定系统支持的警报消息数上限。当消息数达到该阈值时，系统将删除 20% 的警报消息（从最旧的消息开始删除）。

4 单击“保存并关闭”。

相关主题

- 第 572 页上的[“管理警报设置”](#)

18.1.3.6 管理微件设置

SAP BusinessObjects 微件是一个桌面应用程序，可供用户向桌面添加小型应用程序，以便轻松访问 BI 平台上的商务智能内容和 SAP NetWeaver Application Server 上的 Web Dynpro 应用程序。

从 CMC 的“应用程序”区域中，可以控制用户在其桌面上创建和使用微件的权限，以及用户从桌面上的微件应用程序中搜索 BI 平台资源库的能力。

可以授予用户或组以下权限：

使用微件

编辑由微件创建的对象

修改用户对于对象的访问权限

注意：

默认情况下，所有一般用户都能访问以上功能。

18.1.3.7 管理 SAP BusinessObjects Explorer 设置

通过在 CMC 的“应用程序”区域中设置 SAP BusinessObjects Explorer 的安全权限，可以定义用户能够其使用哪些功能。

18.1.3.7.1 修改 SAP BusinessObjects Explorer 应用程序属性

- 1 转到 CMC 的“应用程序”区域。
- 2 单击“管理” > “属性”。
将出现“属性”对话框。
- 3 定义以下任意 SAP BusinessObjects Explorer 设置：
 - 书签有效性
 - 高级配置
- 4 单击“保存并关闭”。

18.1.3.8 文档历史记录

下表概述了最重要的文档更改。

版本	日期	说明
SAP BusinessObjects Business Intelligence 平台 4.1	2013 年 5 月	<p>添加 SAP Jam 支持。当集成时，SAP Jam 为 BI 启动板添加了社交媒体和协作功能。</p> <p>为用户和组添加其他 SAP StreamWork 访问权限。SAP StreamWork “源” 面板包括实例和时间的下拉列表以及关注或取消关注源的按钮。关注 SAP StreamWork 中的模板文档时，将自动关注所有相关的实例。仅针对 SAP StreamWork 中的实例发布实例评论。</p> <p>可以在选项卡上或通过链接打开文件和实例的 OpenDocument 链接。通过 OpenDocument 链接查看文档或实例时，打开 SAP StreamWork “源” 面板以监控或回复文档源。</p> <p>将“添加文件扩展名”复选框添加到“目标”对话框中。</p>
SAP BusinessObjects Business Intelligence 平台 4.1 支持包 1	2013 年 8 月	<p>本指南已更新，现包括以下信息：</p> <p>注意： 一次可运行 BI 启动板的一个会话。使用选项卡（或窗口，具体取决于用户配置）查看多个对象和应用程序。</p>

18.1.3.9 管理协作应用程序集成

在 BI 平台中，使用 CMC 的“应用程序”区域启用和配置与 SAP Jam 或 SAP StreamWork 的协作。

协作应用程序的 Enterprise 代理需要以下附加配置：

- 建立与服务提供者的 HTTPS 连接
- 满足身份验证的先决条件

由于已应用不同的身份验证程序（SAML 2.0 和 OAuth 1.0a），因此该文档的大部分内容都由说明所组成。配置协作应用程序后，SAP Jam 或 SAP StreamWork 源将在 BI 启动板中可用。

目标读者

需要将 BI 平台与 SAP Jam 或 SAP StreamWork 协作应用程序相集成的 BI 平台管理员。

18.1.3.10 协作先决条件

这些先决条件对 BI 平台和协作应用程序的要求进行汇总。

- BI 平台必须至少安装一个中央管理服务器（CMS）。
- 必须在 CMC 中配置协作应用程序（SAP Jam 或 SAP StreamWork）。
- 必须定义协作应用程序（SAP Jam 或 SAP StreamWork）Enterprise 组织。
- SAP Jam 或 SAP StreamWork 用户必须归属 Enterprise 组织。

注意：

只有在设置使用企业预置 LDAP/AD 目录服务的用户时才需要 SAP StreamWork Enterprise 代理。

18.1.3.11 BI 平台配置

18.1.3.11.1 协作配置选项

此表汇总了 BI 平台中用于集成 SAP Jam 或 SAP StreamWork 的 CMC 选项。

以下选项将显示在 CMC 中“属性：协作”对话框中：要访问这些选项，请转到“应用程序”选项卡，单击“协作”，然后从“管理”菜单中选择“属性”。

选项	说明
启用协作	选中此复选框，然后选择“SAP Jam”或“SAP StreamWork”。
连接 URL	键入指向协作应用程序的 URL。
唯一标识 提供程序 ID	<p>输入一个值以用于 BI 平台部署。此值将与在协作应用程序的管理控制台中配置集成所用的证书相关联。</p> <p>注意： 声明单一登录标识的应用程序必须配置为管理 OAuth 应用程序。</p>
标识提供 程序 Base64 证书	<p>单击“生成”时，将在“标识提供程序 Base64 证书”字段中创建一个证书。在 SAP StreamWork 管理控制台中使用此证书生成一个 OAuth 使用者密钥。此证书将建立协作应用程序和 BI 平台之间的信任关系。外部标识提供程序本身由一个 X509 证书标识，后者用于签名所有标识声明。该证书必须采用 Base64 编码。</p>
OAuth 使 用程序密钥	使用此字段输入在协作应用程序管理控制台中生成的有效 OAuth 使用程序密钥。

选项	说明	
使用代理连接	<p>选中此框以启用通过代理连接。必须在“HTTP 代理主机”和“端口”框中提供代理主机的相关信息。</p> <p>提示： 要支持从协作应用程序服务器到公司网络的入站连接，DMZ 中必须包含反向代理。</p> <p>注意： 要向反向代理添加从 SSL 证书提供方处获得的受信任证书，反向代理必须具备域名或子域名。</p>	
	HTTP 代理主机	<p>在反向代理配置中，键入可访问协作应用程序的外部地址。例如，可使用 <code>https://ReverseProxy/</code>，其中 ReverseProxy 为反向代理的域名或子域名。</p> <p>协作应用程序使用此地址向 BI 平台发送信息。反向代理使用此地址将接收自协作应用程序的信息重定向至含协作应用程序 Enterprise 代理的计算机上。</p>
	端口	将协作应用程序 Enterprise 代理配置为侦听端口 8443。

18.1.3.11.2 在 CMC 中启用并配置协作。

必须有效连接至协作应用程序（SAP Jam 或 SAP StreamWork）管理控制台才可执行此任务。需要从该控制台传递和检索安全详细信息。

出于安全原因，以下默认帐户无法向 SAP Jam 或 SAP StreamWork 发送内容或制定内容计划：

- Guest
- SAdmin
- Administrator
- WaaWSServletPrincipal

- 1 在 BI 平台的中央管理控制台（CMC）中，转到“应用程序”区域，然后双击“协作”。
- 2 在“属性：协作”对话框中，选择“启用协作”复选框，然后选择“SAP Jam”或“SAP StreamWork”。
- 3 在“连接 URL”框中，键入连接至协作应用程序的 URL。

- 4 在“唯一标识提供程序 ID”框中，为 BI 平台部署键入唯一标识提供程序值。
记录该标识提供程序值；它将用于配置协作应用程序。
- 5 单击“生成”（如果已创建证书，则单击“重新生成”）。
在“标识提供程序 Base64 证书”框中创建证书。该证书值将用于配置协作应用程序。
- 6 在“OAuth 使用程序密钥”框中，键入有效的 OAuth 使用程序密钥。
将在协作应用程序中创建 OAuth 使用程序密钥。
- 7 如果正在通过代理连接运行 SAP Jam 或 SAP StreamWork 的服务器，请执行以下操作：
 - a 选择“使用代理连接”复选框。
 - b 在“HTTP 代理主机”框中，键入服务器的代理主机名称。
 - c 在“端口”框中，键入服务器的端口号。
- 8 单击“保存并关闭”。

18.1.3.12 SAP Jam 配置

18.1.3.12.1 为 SAP Jam 注册新的 SAML 受信任 IDP

在注册新的 SAML 受信任 IDP 之前：

- 必须在 SAP Jam 中添加并配置公司。
- 必须拥有与 SAP Jam 中的公司相关联的有效 SAP Jam 用户帐户。
- 必须拥有 SAP Jam 中的公司的公司管理权限以及 BI 平台和 BI 启动板的完整管理员权限。
- 必须将 BI 启动板作为 OAuth 客户端与 SAP Jam 一起注册，该客户端充当 SAP Jam 内 BI 启动板的角色。

注意：

每个用户均须使用唯一的电子邮件地址在 SAP Jam 中注册，该电子邮件地址与 BI 启动板中用户的 Enterprise 电子邮件地址相对应。电子邮件地址将在 BI 平台与 SAP Jam 中进行一一映射。

- 1 从 SAP Jam 右上角的“Administrator”（管理员）菜单中选择“Admin”（管理）。
系统将显示与 SAP Jam 中的公司相关的信息（包括 SAP Jam 许可）。备注此信息。
- 2 从“Admin”（管理）菜单中，选择“SAML Trusted IDP”（SAML 受信任 IDP），然后单击“Register your identity provider”（注册标识提供程序）。

必须对 BI 启动板中创建的 IDP 进行注册。

- 3 (必填) 在 “IDP ID” (IDP ID) 框中, 输入在 BI 平台中配置 SAP Jam 时创建的唯一标识提供程序值。

如果尚不具备该值, 请与外部应用程序管理员联系。

例如, 键入 <公司名称>_<系统ID>_<客户端>

- 4 在 “Single Sign-On URL” (单一登录 URL) 框中, 输入直接访问 SAP Jam 的 URL。
SAP Jam 通过唯一标识提供程序使用此 URL 进行单一登录。
- 5 在 “Single Log-Out URL” (单一注销 URL) 框中, 输入 SAP Jam 注销后显示的 URL。
SAP Jam 通过唯一标识提供程序使用此 URL 进行单一注销。
- 6 在 “Default Name ID Format” (默认名称 ID 格式) 框中, 输入要在身份验证请求中使用的名称 ID 格式。
- 7 在 “Default Name ID Policy SP Name Qualifier” (默认名称 ID 策略 SP 名称限定符) 框中, 输入要在身份验证请求中使用的 SP 名称限定符。
- 8 (必填) 在 “Allowed Assertion Scope” (允许的断言范围) 列表中, 选择 “Users in my company” (我公司的用户)。
此选项指定 SAP Jam 从 IDP 处接收其断言的用户集。
- 9 (必填) 在 “X509 Certificate (Base64)” (X509 证书 (Base64)) 框中, 输入在 BI 平台中配置 SAP Jam 时生成的 Base64 证书值。

如果尚不具备该值, 请与外部应用程序管理员联系。

10. 单击 “Register” (注册)。

18.1.3.12.2 为 SAP Jam 创建 OAuth 客户端

在创建 OAuth 使用程序密钥之前:

- 必须在 SAP Jam 中添加并配置公司。
- 必须拥有与 SAP Jam 中的公司相关联的有效 SAP Jam 用户帐户。
- 必须拥有 SAP Jam 中的公司的公司管理权限以及 BI 平台和 BI 启动板的完整管理员权限。
- 必须将 BI 启动板作为 OAuth 客户端与 SAP Jam 一起注册, 该客户端充当 SAP Jam 内 BI 启动板的角色。

注意:

每个用户均须使用唯一的电子邮件地址在 SAP Jam 中注册, 该电子邮件地址与 BI 启动板中用户的 Enterprise 电子邮件地址相对应。电子邮件地址将在 BI 平台与 SAP Jam 中进行一一映射。

- 1 从 SAP Jam 右上角的 “Administrator” (管理员) 菜单中选择 “Admin” (管理)。
系统将显示与 SAP Jam 中的公司相关的信息 (包括 SAP Jam 许可)。

- 2 在“Admin”（管理）菜单中，选择“OAuth Clients”（OAuth 客户端），然后单击“Add OAuth Client”（添加 OAuth 客户端）。
- 3 在“Register a new OAuth Client”（注册新的 OAuth 客户端）对话框的“Name”（名称）框中，输入在 BI 平台中配置 SAP Jam 时创建的唯一标识提供程序值。
如果尚不具备该值，请与外部应用程序管理员联系。
当 SAP Jam 以用户身份操作时，它将显示应用程序名称作为所输入 URL 的超级链接。
例如，键入<公司名称>_<系统ID>_<客户端>_<应用程序>
- 4 在“Integration URL”（集成 URL）框中，输入直接访问 BI 启动板的 URL。
当 SAP Jam 以用户身份操作时，它将显示应用程序名称作为此 URL 的超级链接。
- 5 在“X509 Certificate (Base64)”（X509 证书 (Base64)）框中，输入在 BI 平台中配置 SAP Jam 时生成的 Base64 证书值。
如果尚不具备该值，请与外部应用程序管理员联系。
若将此框留空，SAP Jam 将提供使用程序密钥。
- 6 单击“Save”（保存）。
已生成 OAuth 使用程序密钥。备注 BI 平台管理员要使用的 OAuth 使用程序密钥值。

18.1.3.13 SAP StreamWork 配置

18.1.3.13.1 SAP StreamWork 集成图例

此图表显示集成 SAP StreamWork 时所需的 BI 平台、SAP StreamWork 和 SAP StreamWork Enterprise 代理组件。

工作流描述集成系统所涉及的步骤，以及用户可在集成后执行的操作概览。

- 在 SAP StreamWork Enterprise 代理中，用户可将 LDAP 的 Enterprise 用户设置到 SAP StreamWork。
- 在 BI 平台的 CMC 中，管理员可创建用户并将用户映射到 Enterprise 用户。
- 在 BI 启动板中，用户可创建活动并在浏览器中进行查看，而无需创建帐户或登录至 SAP StreamWork。

- 在 BI 启动板中，用户可查看并响应 SAP StreamWork 源。

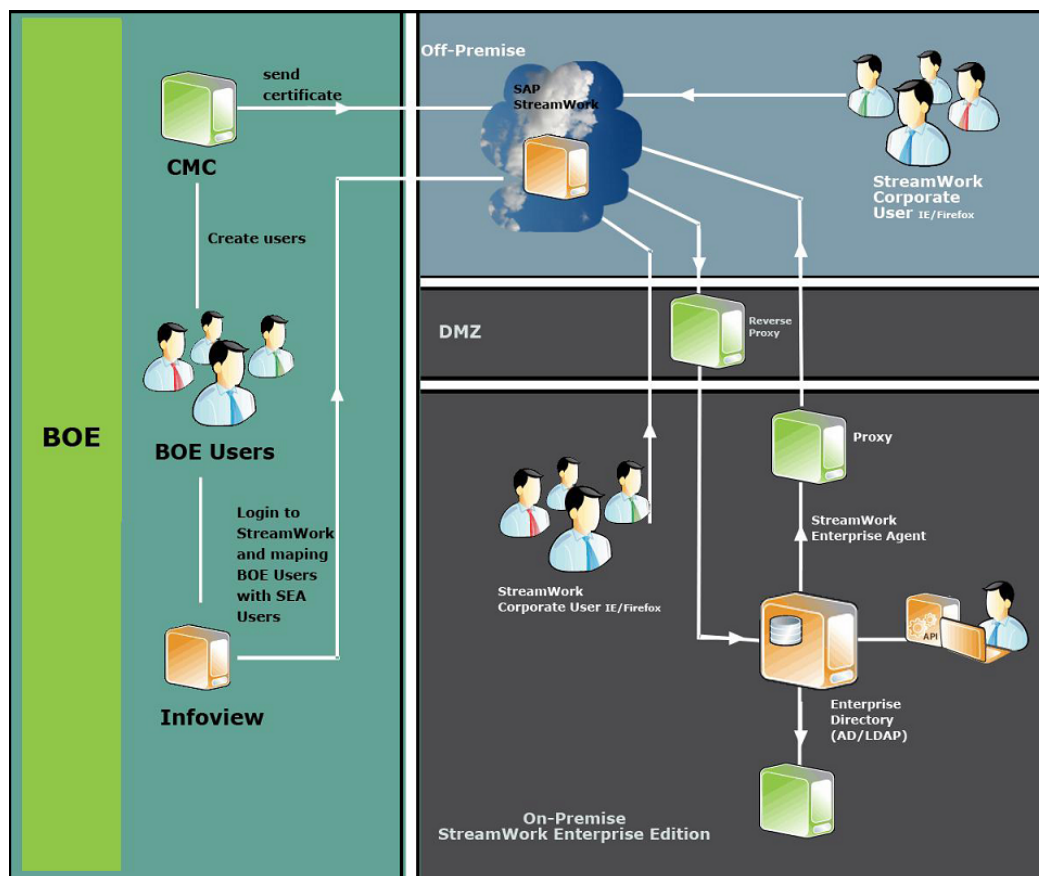


图 18-1: 系统架构

18.1.3.13.2 为 SAP StreamWork 创建 OAuth 使用程序密钥

在创建 OAuth 使用程序密钥之前，必须具备 SAP StreamWork Enterprise 组织的管理员权限。

- 1 在 SAP StreamWork 管理控制台的“Admin”（管理）选项卡中，选择“SAML Trusted IDP”（SAML 受信任 IDP），然后使用已指定为 Enterprise 组织管理员的帐户登录至 SAP StreamWork。
- 2 单击“Register your identity provider”（注册标识提供程序）。
- 3 选择“Click here to create a new administrative OAuth application”（单击此处创建新的管理 OAuth 应用程序），并接受使用条款协议。

- 4 在“Register a new Application OAuth application”（注册新的应用 OAuth 应用程序）窗口中，执行以下操作：
 - a 在“Application Name”（应用程序名称）框中，输入要在集成中使用的应用程序实例名称。
此信息标识以用户身份进行操作时所需的程序，例如：为用户发布 SAP StreamWork 源。用户必须能够识别此应用程序名称。
 - b 在“Integration URL”（集成 URL）框中，输入直接访问 BI 启动板的 URL。
 - c 在“Base64 X509 Certificate”（Base64 X509 证书）框中，输入在 BI 平台中央管理控制台（CMC）中对 SAP StreamWork 进行配置时生成的 Base64 证书值。
如果尚不具备该值，请与外部应用程序管理员联系。
- 5 单击“Register”注册。
已生成 OAuth 使用程序密钥。备注 BI 平台管理员要使用的 OAuth 使用程序密钥值。
- 6 单击“Back”（后退），显示 SAML 受信任标识提供程序。
- 7 在“Register a new SAML Trusted Identity Provider”（注册新的 SAML 受信任标识提供程序）窗口中，执行以下操作：
 - a 在“Display Name”（显示名称）框中，为 BI 平台部署输入名称。
此名称将针对 SAP StreamWork 用户予以显示。
 - b 在“IDP ID”（IDP ID）框中，输入在 BI 平台中对 SAP StreamWork 进行配置时创建的唯一标识提供程序值。
如果尚不具备该值，请与外部应用程序管理员联系。
 - c 在“Base64 X509 Certificate”（Base64 X509 证书）框中，输入在 BI 平台中对 SAP StreamWork 进行配置时生成的 Base64 证书值。
如果尚不具备该值，请与外部应用程序管理员联系。
- 8 单击“Register”注册。

18.1.3.13.3 将 SAP StreamWork 添加到 BI 工作区

SAP StreamWork 是隐藏的，必须手动使其显示在 BI 启动板模块的列表中，该列表可添加到 BI 工作区。

- 1 在 C:\BusinessObjects\tomcat\work\Catalina\localhost\BOE\eclipse\plugins\webpath.PerformanceManagement\web\WEB-INF\lib\asdk-ivdm_ext.jar\conf-syst\conf-syst\ 中找出 home-analyticlist.xml 文件。

文件内容应该以下列文本开始：

```
<?xml version="1.0" encoding="UTF-8"?>
```



```

<CHOICE>
  <!--<SW_ACTIVITIES NAME="$MSG_SW_ACTIVITIES$" DESCRIPTION="$MSG_SW_ACTIVITIESDESC$"/>-->
  <!--SW_FEED NAME="$MSG_SW_FEED$" DESCRIPTION="$MSG_SW_ACTIVITIESDESC$"/-->
  <HOMEINBOX NAME="$MSG_HOMEINBOX$" DESCRIPTION="$MSG_HOMEINBOXDESC$"/>
  <HOMEAPPLICATIONS NAME="$MSG_HOMEAPPLICATIONS$" DESCRIPTION="$MSG_HOMEAPPLICATIONSDESC$"/>
  <HOMERECENTLYRUNDOCS NAME="$MSG_HOMERECENTLYRUNDOCS$" DESCRIPTION="$MSG_HOMERECENTLYRUNDOCSDESC$"/>
  <HOMERECENTDOCS NAME="$MSG_HOMERECENTDOCS$" DESCRIPTION="$MSG_HOMERECENTDOCSDESC$"/>
  <HOMEALERTS NAME="$MSG_ALERTNOTIFICATIONS$" DESCRIPTION="$MSG_ALERTNOTIFICATIONSDESC$"/>
</CHOICE>

```

- 2 从 SW_ACTIVITIES NAME= 和 SW_FEED NAME= 行中删除 ! -- 。
- 3 重新启动 Tomcat 服务器。
“SAP StreamWork 订阅源”将在 BI 工作区模块库、BI 启动板中的 “BI 启动板模块” 列表中显示。

18.1.3.14 管理平台搜索设置

在 BI 平台中，可以在 CMC 的 “应用程序” 区域中指定平台搜索应用程序的系统级别设置。

相关主题

- 第 693 页上的 [“索引建立失败列表”](#)
- 第 688 页上的 [“在 CMC 中配置应用程序属性”](#)

18.1.3.14.1 在 CMC 中配置应用程序属性

若要配置平台搜索应用程序属性，请完成以下步骤：

- 1 转到 CMC 的“应用程序”区域。
- 2 选择“平台搜索应用程序”。
- 3 单击“管理” > “属性”。将出现“属性”对话框。
- 4 配置平台搜索设置：

选项	说明
搜索统计信息	平台搜索提供以下搜索统计信息： <ul style="list-style-type: none">• 索引建立状态：显示索引建立进程的状态。• 已建立索引的文档数：显示已建立索引的文档数。• 上次建立索引的时间戳：显示上次为该文档建立索引时的时间戳。
停止/启动索引建立	<p>要从持续爬网切换到计划爬网或用于维护目的时，可以使用“开始建立索引”或“停止建立索引”选项来启动或停止索引建立流程。</p> <p>要停止建立索引，请单击“停止建立索引”。</p>
默认索引区域设置	<p>平台搜索使用在 CMC 中指定的区域设置为所有未本地化的 BI 文档建立索引。文档实现本地化后，将使用相应语言的分析器建立索引。</p> <p>搜索基于客户端的产品区域设置，并且为客户端的产品区域设置分配权重。</p> <p>可以在 CMC 配置属性中配置权重。</p>

选项	说明
爬网频率	<p>可以使用以下选项为整个 BI 平台资源库建立索引：</p> <ul style="list-style-type: none">持续爬网：通过该选项，每当添加、修改或删除对象时都可以随时为资源库建立索引。持续爬网使用户可以查看或使用最新的 BI 平台内容。默认设置下，持续爬网会根据用户所执行的操作不断地更新资源库。持续爬网无需用户干预即可运作，从而减少了对文档建立索引所需的时间。计划的爬网：通过该选项，可以根据“计划”选项设置的计划来建立索引。 <p>有关如何计划对象的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 CMC 联机帮助》中“平台搜索”的“计划对象”部分。</p> <p>注意：</p> <ul style="list-style-type: none">如果选择“计划的爬网”并将“重复发生”设置为“立即”以外的其他选项，则平台搜索将显示计划下次对文档建立索引的日期和时间戳。如果选择“计划的爬网”，则会启用“开始建立索引”按钮，而禁用“停止建立索引”按钮。计划完成后，“停止建立索引”按钮将禁用。

选项	说明
索引位置	<p>索引存储在以下位置中的共享文件夹中：</p> <ul style="list-style-type: none">主索引位置（索引和拼写程序）：主索引和拼写程序索引存储在此位置中。在搜索过程中，主索引用于检索初始结果，而拼写程序索引用于检索建议。在群集式 BI 平台部署中，此位置应该位于可以从群集的所有节点访问的共享文件系统上。永久性数据位置（内容存储）：内容存储位于此位置中。它是从主索引位置中创建的，并与之保持同步。内容存储用于生成构面，并处理从主索引位置生成的初始提示。在群集 BI 平台部署中，每个节点都会生成内容存储。 <p>永久性数据位置是唯一受群集环境影响的索引位置，这是因为它包含内容存储文件夹。如果计算机只有一种搜索服务，则只有一个内容存储位置。例如，{bobj.enterprise.home}\data\PlatformSearchData\workspace\<服务器名称>\ContentStores。</p> <p>不过，如果在群集环境中有多搜索服务，则每个搜索服务将有一个内容存储位置。例如，如果有两个服务器实例在运行，则内容存储位置将如下所示：</p> <ul style="list-style-type: none">a {bobj.enterprise.home}\data\PlatformSearchData\workspace\<服务器名称>\ContentStores。b {bobj.enterprise.home}\data\PlatformSearchData\workspace\<服务器名称 1>\ContentStores。 <ul style="list-style-type: none">非永久性数据位置（临时文件，增量索引）：在增量索引与主索引合并之前，此位置中会临时创建和存储增量索引。此位置的索引在与主索引合并后即被删除。此外，此位置中将创建替代文件（提取器的输出），并在其转换为增量索引之前临时存储这些文件。 <p>注意：</p> <ul style="list-style-type: none">所有索引位置必须是共享位置。需要单击“停止建立索引”，才能修改索引位置。如果修改索引位置，则需要将内容复制到新位置，否则现有索引信息将丢失。

选项	说明
索引建立级别	<p>可以通过以下方式设置索引建立级别来微调搜索内容：</p> <ul style="list-style-type: none"> 平台元数据：仅为平台元数据信息（如文档的标题、关键字和说明）创建索引。 平台和文档元数据：此索引包括平台元数据以及文档元数据。文档元数据包括创建日期、修改日期和作者姓名。 全部内容：此索引包括平台元数据、文档元数据和其他内容，例如： <ul style="list-style-type: none"> 文档中的实际内容 提示和 LOV 内容 统计图、图形和标签 <p>注意： 修改索引建立级别时，将为整个 BI 平台资源库刷新重新初始化索引建立。</p>
内容类型	<p>可以选择以下内容类型来建立索引：</p> <ul style="list-style-type: none"> Crystal Reports Web Intelligence Universe BI 工作区 Microsoft PowerPoint Adobe Acrobat 多信息文本 文本 Microsoft Word Microsoft Excel
重新建立索引	<p>此选项将删除现有索引，并重新建立整个资源库的索引。</p> <p>不管建立索引是在运行还是已停止，都可以选择“重新建立索引”选项。现有索引在将更改保存到属性页时被删除。不过，如果建立索引当前已停止，索引在重新开始建立索引前不会开始重建。</p> <p>如果不希望平台搜索重新为文档建立索引，则需要清除“重新建立索引”选项，然后单击“开始建立索引”。</p>

选项	说明
从索引建立范围排除的文档	<p>“从索引建立范围排除的文档”选择将从索引建立范围排除文档。例如，用户可能希望将极大的 Crystal 报表设置为不可搜索，以确保报表应用程序服务器资源不会过载。同样，也可能不希望对包含数百个性化报表的发布建立索引。</p> <p>通过排除特定文档，可以防止从平台搜索对其进行访问。值得注意的是，如果在将某个文档放入该组之前已对其建立索引，则此文档可能仍然是可搜索的文档。为确保“从索引建立范围排除的文档”组中的文档不可搜索，必须重新建立索引。</p> <p>默认情况下，只有管理员帐户拥有“从索引建立范围排除的文档”选项的完全控制权限。具有以下权限的其他用户只能向“从索引建立范围排除的文档”组中添加文档：</p> <ul style="list-style-type: none"> 对目录的查看和编辑权限 直接编辑文档

5 单击“保存并关闭”。

注意：

如果用户未选择“重新建立索引”选项而更改了索引建立级别或者选择或取消选择了提取器，则索引会以增加方式更新，而不删除现有索引。

18.1.3.15 配置 BEx Web 集成

BEx Web 应用程序是 SAP NetWeaver Business Warehouse (BW) 的 Business Explorer (BEx) 中基于 Web 的应用程序，用于在 Web 上提供数据分析、报表创建和分析应用程序。

Business Explorer 属于 SAP NetWeaver Business Intelligence 套件，可以为战略分析提供灵活的报表创建和分析工具，并为决策制定提供支持。这些工具包括查询、报表创建和分析功能。具有访问权限的员工既可以在 Web 中，也可以在 Microsoft Excel 中从不同角度对历史数据或当前数据进行各种详细级别的评估。

用户通过 SAP NetWeaver Portal 或 SAP BusinessObjects Business Intelligence 平台的 BI 启动板访问数据。BEx Web 应用程序的作者可以直接从 BEx Web Application Designer 的 BI 启动板中执行 Web 应用程序。

若要在 BI 平台中集成 BEx Web 应用程序，请执行下列配置步骤：

- 1 在中央管理控制台 (CMC) 中为 BEx Web 应用程序设置服务器。
可以为 BEx Web 应用程序使用常规服务器或独立的服务器。

提示:

由于许多其他服务通常都会使用通用服务器，所以我们建议为 BEx Web 应用程序设置单独的服务器。

- 2 配置服务器设置。
- 3 检查与 BW 系统的连接。
- 4 要确保作者可以直接从 BEx Web Application Designer 的 BI 启动板中运行 BEx Web 应用程序，请确保在 BW 系统的“Connected Portals”（连接的门户）表（RSPOR_T_PORTAL）中进行相关设置。

在配置 BI 平台服务器后，用户可以在 BI 启动板中打开 BEx Web 应用程序。他们可以在此处浏览数据，并将 BEx Web 应用程序作为书签保存在 Web 浏览器收藏夹中。

限制:

从以下 SAP NetWeaver 版本开始支持集成:

- SAP NetWeaver 7.0 Enhancement Package 1 Support Package Stack 8
- SAP NetWeaver 7.3 Support Package Stack 1

由于此集成不需要 SAP NetWeaver Java 堆栈，所以下列限制适用:

- 不支持信息传播。
- 由于不需要 SAP NetWeaver 的门户和 Knowledge Management，所以 BEx Web 应用程序中不支持文档集成和门户主题的使用。
- 不支持“报表”Web 项目。建议使用 SAP Crystal Reports 进行格式化的报表创建。
- 要创建打印版的 BEx Web 应用程序，需要使用 SAP Business Explorer 的导出库。Adobe 文档服务（ADS）不可用。
- 在 BI 平台中集成的 BEx Web 应用程序只能包含 BW 主系统中存储的数据源。在系统管理中，定义配置为 BI 平台中的 BW 主系统的系统。
- BI 平台和 SAP NetWeaver BW 系统之间未启用单一登录。对于每个 BI 平台会话，BEx Web 应用程序用户需要登录相应的 BW 主系统。
- 不支持来自 BEx Web 应用程序或到 BEx Web 应用程序的报表对报表接口。不会执行相应的命令。
- 不支持基于 BEx 查询或查询视图以及使用 SAP BusinessObjects Dashboards 创建的仪表盘。

有关 BEx Web 应用程序的更多信息，请参阅 SAP Help Portal（网址为 <http://help.sap.com>）：“SAP NetWeaver 7.3” > “SAP NetWeaver Library: Function-Oriented View” > “Business Warehouse” > “SAP Business Explorer” > “BEx Web” > “Analysis & Reporting: BEx Web Applications”。

有关在 BI 启动板中访问和保存 BEx Web 应用程序的更多信息，请参阅位于 <http://help.sap.com> 的《BI 启动板用户指南》。

相关主题

- 第 592 页上的“[为 BEx Web 应用程序启动服务器](#)”
- 第 592 页上的“[为 BEx Web 应用程序启动独立的服务器](#)”
- 第 592 页上的“[配置服务器设置](#)”
- 第 593 页上的“[检查与 BW 系统的连接](#)”
- 第 594 页上的“[配置 BEx Web Application Designer 和 BI 平台之间的连接](#)”

18.1.3.15.1 为 BEx Web 应用程序启动服务器

在能够执行此任务之前，自适应处理服务器必须处于“已停止”状态。

- 1 登录到中央管理控制台（CMC）。
- 2 选择“服务器”。
- 3 展开“服务类别”节点，并选择“分析服务”。
- 4 选择“自适应处理服务器”并在上下文菜单中选择“选择服务”。
- 5 从“可用服务”列表将“BEx Web 应用程序服务”移到右侧的“服务”列表中。
- 6 通过重新启动自适应处理服务器重新启动 BEx Web 应用程序服务。

18.1.3.15.2 为 BEx Web 应用程序启动独立的服务器

- 1 登录到中央管理控制台（CMC）。
- 2 选择“服务器”。
- 3 展开“服务类别”节点，并选择“Analysis Services”。
- 4 选择“自适应处理服务器”并在上下文菜单中选择“克隆服务器”。
- 5 为服务器输入名称（例如 AdaptiveProcessingServer）并在“克隆到节点”框中选择所需节点。
- 6 选择克隆的服务器并在上下文菜单中选择“选择服务”。
- 7 在“可用服务”列表中选择“BEx Web 应用程序服务”，并将其移到右侧的“服务”列表中。
- 8 通过重新启动新的自适应处理服务器启动 BEx Web 应用程序服务。

18.1.3.15.3 配置服务器设置

- 1 登录到中央管理控制台（CMC）。

- 2 选择“服务器”。
- 3 展开“服务类别”节点，并选择“Analysis 服务”。
- 4 选择承载 BEx Web 应用程序服务的服务器，并在上下文菜单中选择“属性”。
- 5 在“BEx Web 应用程序服务”区域的“BEx Web 应用程序服务配置”下，进行以下设置：
 - a 检查最大客户端会话数，如有必要，可进行更改。
 - b 在“SAP BW 主系统”下，输入在 BI 平台中创建的到 BW 系统的 OLAP 连接名称。默认名称为“SAP_BW”。
 - c 输入在 BW 系统的“Configuration of RFC Connections”（配置 RFC 连接）（事务代码 sm59）下输入的“JCo 服务器 RFC 目标”的名称。
 - d 输入在 BW 系统的“Configuration of RFC Connections”（配置 RFC 连接）（事务代码 sm59）下定义的“JCo 服务器网关主机”的名称。
 - e 输入在 BW 系统的“Configuration of RFC Connections”（配置 RFC 连接）（事务代码 sm59）下定义的“JCo 服务器网关服务”的名称。
 - f 检查“JCo 服务器连接计数”，如有必要，可进行更改。
- 6 选择“保存并关闭”。
- 7 选择承载 BEx Web 应用程序服务的服务器，并在上下文菜单中选择“重新启动服务器”。要应用所选设置，必须重新启动服务器。

注意：

重新启动服务器之前，必须已在 ABAP 系统中创建了 RFC 目标。

相关主题

- 第 594 页上的“[在 ABAP 系统中创建 RFC 目标](#)”

18.1.3.15.4 检查与 BW 系统的连接

- 1 登录到中央管理控制台（CMC）。
- 2 选择“OLAP 连接”。
- 3 检查是否建立了与 BW 系统的连接。否则，单击“新建连接”按钮，设置一个连接。连接的默认名称为 SAP_BW。也可以输入其他名称。
- 4 请确保选择了“身份验证”下的“预定义”并输入了必要的用户名和密码。

注意：

此用户帐户对于 JCo 服务器 RFC 目标是必需的，通过该用户帐户可集成 BEx Web Application Designer、BW 系统和 BI 平台。

提示：

为保证连接安全，请确保只有管理员拥有访问该连接的权限。

- 。 a 为此，请右击到 BW 系统的连接（默认名称为“SAP_BW”），并选择“用户安全性”。
- 。 b 进行必要的安全设置，如果可能，仅将访问权授予管理员。

18.1.3.15.5 配置 BEx Web Application Designer 和 BI 平台之间的连接

为确保作者可以直接在 BEx Web Application Designer 的 BI 启动板中运行 BEx Web 应用程序，需要在 BW 系统的“Connected Portals”（连接的门户）表（RSPOR_T_PORTAL）中进行相关设置。

- 1 在 BW 系统中，调用事务 SM30（“Table View Maintenance”（表视图维护））。
- 2 在“Table/View”（表/视图）下，输入 RSPOR_T_PORTAL。
- 3 选择“Maintain”（维护）。
- 4 若要创建新条目，请选择“New Entries”（新建条目）。
- 5 进行以下设置：
 - a 为确保 BW 系统和 BI 平台之间实现集成，必须在事务 SM59 中创建 RFC 目标。在“目标”下输入此 RFC 目标。
 - b 选择“Standard Portal”（标准门户）。这将确保始终在 BI 平台中调用 Web Application Designer 中的 Web 应用程序。
 - c 在“URL Prefix”（URL 前缀）下，输入访问 BI 平台 Web 应用程序容器服务器（WACS）的 URL，其中包括协议、主机名和端口，例如 http://<wacs><域>:<端口>。
 - d 在“平台”下，选择“BOE”。
 - e 如果希望激活“导出 SAP Business Explorer 库”，请选择“Use SAP Export Lib (PDF)”（使用 SAP 导入库（PDF）），这样便可从 BEx Web 应用程序中导出 PDF、PostScript 和 PCL 文件。
- 6 保存您的输入。

相关主题

- 第 594 页上的“[在 ABAP 系统中创建 RFC 目标](#)”

18.1.3.15.5.1 在 ABAP 系统中创建 RFC 目标

要集成 BW 系统和 BI 平台，需要一个 RFC 目标。此 RFC 目标可以保证 BW 系统和 BI 平台之间的通信。

- 1 调用“Configuration of RFC Connections”（配置 RFC 连接）（事务代码 SM59）。
- 2 选择“创建”。
- 3 维护 RFC 目标：
 - a 输入 RFC 目标的名称。
 - b 选择“T for TCP/IP connection”（T: TCP/IP 连接）作为连接类型。
 - c 输入说明。
可根据情况维护 RFC 目标说明的语言。
 - d 在“Technical Settings”（技术设置）下，选择“Registered Server Program”（注册的服务器程序）作为激活类型。
 - e 在“Technical Settings”（技术设置）下，输入程序 ID。
该程序 ID 必须与在 BI 平台服务器中创建此 BW 系统的目标时所指定的程序 ID（JCo 服务器 RFC 目标）相同。
 - f 在“网关选项”的“技术设置”下，输入 BI 平台服务器用于和 BW 系统进行通信的网关主机和网关服务。
- 4 在“Logon & Security”（登录和安全性）表页面上，激活“Send SAP Logon Ticket”（发送 SAP 登录权证）选项。
- 5 保存您的输入。

相关主题

- 第 592 页上的[“配置服务器设置”](#)

18.1.3.16 配置 SAP HANA 单一登录

在 BI 平台 CMC 的“应用程序”区域中，可为 SAP HANA 数据库连接配置单一登录（SSO）。使用 SAML（安全性断言标记语言）实现 SSO。

建立 BI 平台会话之后，即可生成 SAML 权证，该权证可用于登录 SAP HANA，而无需用户提供密码。

这是连接到 SAP HANA 数据源所涉及到的基本工作流程。

- 1 管理员在 CMC 中的 SAP HANA 和 BI 平台之间配置信任。
- 2 用户可凭借任何受支持的身份验证提供程序登录 BI 平台。
- 3 如果 SAP HANA 和 BI 平台用户 ID 相匹配，则 BI 平台便能够生成 SAML 断言，SAP HANA 可以接受该断言来为当前用户建立连接。传递到 SAP HANA 的用户 ID 是 BI 平台已登录用户的用户 ID。
- 4 BI 平台客户端应用程序创建了 SAP HANA 连接。

注意:

在使用 SAML 配置 SAP HANA 单一登录之前，必须在 SAP HANA 计算机上配置 SSL。有关详细信息，请参阅 SAP HANA 文档。

18.1.3.16.1 创建 SAP HANA 连接

- 1 获得 SAP HANA 数据库相关参数。
 - a 打开 SAP HANA Studio 应用程序。
 - b 打开系统的属性页面，找到数据库连接的 URL。
 - c 记录主机名称和端口号。
在第 2 步需要此信息。
 - 2 在 BI 平台中配置 SAP HANA 连接。
 - a 转到 CMC 的“应用程序”区域，然后双击“HANA 身份验证”。
 - b 在“HANA 身份验证”对话框中，单击“创建连接”按钮。
随后将打开“创建 HANA 身份验证连接”对话框。
 - c 输入在第 1 步中记录的主机名称和端口号。
 - d 在“唯一标识提供程序 ID”字段中，指定将用于 BI 平台部署的值。
 - e 单击“生成”。
在“标识提供程序 Base64 证书”框中创建证书。
 - 3 配置 SAP HANA 部署。
 - a 使用 SAP HANA Studio 应用程序，运行此 SQL 命令，以启用 BI 平台作为 ID 提供程序：

创建 SAML 提供程序 UNIQUE ID，具有主题 'C=CA, ST=BC, O=SAP, OU=BOE, CN=UNIQUE ID' 发行者 'C=CA, ST=BC, O=SAP, OU=BOE, CN=UNIQUE ID'

UNIQUE ID 是在第 2 步中指定的“唯一标识提供程序 ID”。
 - b 为安装 SAP HANA 时创建的用户将证书从 CMC 复制到 ~/.ssl 目录的 trust.pem 文件中。
用户名为 <3个字符代码>adm。例如，SAP HANA 实例标识符为 xyz，用户名为 xyzadm。
- 注意:**
- 此时，可验证 key.pem 文件是否在 ~/.ssl 目录中。如果不存在，则未正确地配置 SAP HANA 来使用 SSL。在使用 SAML 配置 SAP HANA 单一登录之前，必须在 SAP HANA 计算机上配置 SSL。有关详细信息，请参阅 SAP HANA 文档。
- c 重启 SAP HANA。
 - d 使用这些命令，在 SAP HANA 中创建一个用户，BI 平台可为该用户生成权证：

```
CREATE USER HANAUserName PASSWORD HANAUserPassword;
ALTER USER HANAUserName ENABLE SAML;
ALTER USER HANAUserName ADD IDENTITY 'BIPUserName' FOR SAML PROVIDER BIPUniqueIdentityProviderID;
```

BIPUserName 为 BI 平台用户的全称。

示例:

```
CREATE USER Administrator PASSWORD Abcd1234;  
ALTER USER Administrator ENABLE SAML;  
ALTER USER Administrator ADD IDENTITY 'Administrator' FOR SAML PROVIDER BIPDeployment1;
```

另外，还可使用现有用户，并只运行上述 ALTER 命令。

4 测试 SAP HANA 配置。

- a 转到 CMC 的“应用程序”区域，然后双击“HANA 身份验证”。
- b 在“HANA 身份验证”对话框中，打开在第 2 步创建的连接。
随后将打开“编辑 HANA 身份验证连接”对话框。
- c 在“为以下用户测试连接”下，输入用户名并单击“测试连接”按钮，以验证连接设置是否有效。
例如，输入用户名“Administrator”。如果设置无效，则会显示错误消息。可以尝试以下故障排除步骤：
 - 确保 trust.pem 文件中任何其他证书均不包含与 CN 属性值相同的“主题”或“颁发者”。要查看证书的组件，可在 Internet 上搜索 x509 证书解码器，找到证书解码器。
 - 尝试这些命令，以检查 HANA 端配置：

```
select * from "SAML_PROVIDERS"  
select user_name, is_saml_enabled from users where user_name = '<UserName>'  
select * from "PUBLIC"."SAML_USER_MAPPINGS"
```

注意:

如果 key.pem 文件不在 .ssl 目录中，则说明未正确地配置 SAP HANA 以使用 SSL。

18. 1. 3. 16. 2 SAP HANA 连接设置

下表汇总了 CMC 中用于配置 SAP HANA 连接的设置。

设置	说明
HANA 主机名称	请提供 SAP HANA 主机的名称。
HANA 端口	请提供 SAP HANA 主机的端口号。
唯一标识提供程序 ID	指定 HANA 安装内的唯一名称。HANA 安装将接受来自该标识提供程序名称正确签署的权证来登录。

设置	说明
标识提供程序 Base64 证书	单击“生成”时，将在“标识提供程序 Base64 证书”字段中创建一个证书。将该证书复制到 SAP HANA 部署中的 trust.pem 文件。该证书将在 SAP HANA 与 BI 平台之间建立信任关系。外部标识提供程序本身由一个 X509 证书标识，后者用于签名所有标识声明。该证书必须采用 Base64 编码。

18.2 通过 BOE.war 属性管理应用程序

18.2.1 BOE WAR 文件

通过覆盖 BOE.war 文件的默认属性，可以修改 BI 平台 Web 应用程序的设置。在承载 Web 应用程序服务器的计算机上部署该文件。有关如何部署文件的详细信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

BOE.war 文件中所包含的属性可控制默认登录行为的规范、默认身份验证方法和单一登录的设置。可以指定两种类型的属性：

- 全局属性 — 这些属性会影响 BOE.war 文件中所包含的所有 Web 应用程序。
- 应用程序特定属性 — 仅影响特定 Web 应用程序的属性设置。

若要修改任何默认属性，请使用自定义配置目录保存全局或应用程序特定的属性的新设置。默认情况下，该目录位于：C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom。

请勿修改 config\default 目录中的属性。

注意：

在某些 Web 应用程序服务器上，如与 BI 平台捆绑在一起的 Tomcat 版本，可以直接访问 BOE.war。在这种情况下，可以直接设置自定义设置，而无需取消部署 WAR 文件。当无法直接访问已部署的 Web 应用程序时，必须取消部署该文件，然后进行自定义和重新部署。有关更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

18.2.1.1 全局 BOE.war 属性

下表列出了 BOE.war 的默认 global.properties 文件中所包括的设置。若要覆盖任何设置，请在以下路径中新建一个文件：C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom。

设置	默认值	说明
persistentcookies.enabled	persistentcookies.enabled=true	启用或禁用 Web 应用程序登录页上的永久性 Cookie。
siteminder.authentication	siteminder.authentication=secLDAP	指定与 SiteMinder 一起使用的身份验证方法。只能选择 secLDAP 和 secwinAD 选项。
siteminder.enabled	siteminder.enabled=false	启用和禁用与 SiteMinder 一起使用的身份验证。
sso.enabled	sso.enabled=false	为 BI 平台启用和禁用单一登录 (SSO)。
sso.sap.primary	sso.sap.primary=false	如果要将 SAP SSO 用作应用程序的主要单一登录机制，则设置为 true。仅适用于 SAP 和 SiteMinder SSO 同时使用的情况。
max.tree.children.threshold	max.tree.children.threshold=200	指定阈值，树列表控件在该阈值处不会显示所有的节点，而显示“太多子项”的消息。
trusted.auth.shared.secret	无	指定用于检索受信任的身份验证秘密的会话变量名称。仅在使用 Web 会话传递共享秘密时适用。
trusted.auth.user.param	无	指定用于为受信任的身份验证检索用户名的变量。可设置为以下一个： <ul style="list-style-type: none"> 标题 URL 参数 Cookie 会话

设置	默认值	说明
trusted.auth.user.retrieval	无	指定用于为受信任的身份验证检索用户名的方法。可设置为以下一个： <ul style="list-style-type: none"> “REMOTE_USER” “HTTP_HEADER” “COOKIE” “QUERY_STRING” “WEB_SESSION” “USER_PRINCIPAL” 设置为空可禁用“受信任的身份验证”。
trusted.auth.user.namespace.enabled	trusted.auth.user.namespace.enabled=false	启用和禁用对现有用户帐户的动态别名绑定。如果属性设置为 true，则“受信任的身份验证”会使用别名绑定对登录到 BI 平台的用户进行身份验证。利用别名绑定，应用程序服务器可用作 SAML 服务提供商，从而启用“受信任的身份验证”以提供到系统的 SAML SSO。如果设置为 false，则“受信任的身份验证”会使用名称匹配对用户进行身份验证。
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	用于启用或禁用 Windows AD 身份验证的 Vintela 设置。
pinger.showWarningDialog.cmc	pinger.showWarningDialog.cmc=true	指定是否显示其中的消息指示当前会话很快将在 CMC 中过期的警告对话框。
pinger.showWarningDialog.bi-launchpad	pinger.showWarningDialog.bilaunchpad=true	指定是否显示其中的消息指示当前会话很快将在 BI 启动板中过期的警告对话框。
pinger.warningPeriod.pingIncrementsInSeconds	pinger.warningPeriod.pingIncrementsInSeconds=15	指定在显示会话到期警告时 Web 服务器请求的发送频率。这对于将应用程序中的警告对话同步是至关重要的。
pinger.warningPeriod.lengthInMinutes	pinger.warningPeriod.lengthInMinutes=5	指定应在会话到期前的多长时间内开始显示警告。
logoff.on.websession.expiry	logoff.on.websession.expiry=true	指定当 Web 会话到期时是否将所有应用程序会话注销。
pinger.enabled	pinger.enabled=true	启用或禁用会话到期警告消息机制。

设置	默认值	说明
system.com.sap.bip.jcomanager.destinations.maxsize	system.com.sap.bip.jcomanager.destinations.maxsize=1000	指定缓存的 Java 连接的最大数量。
httpproxy.username	httpproxy.username=myusername	指定登录 HTTP 代理服务器的用户名。
httpproxy.password	httpproxy.password=mypassword	指定登录 HTTP 代理服务器的密码。
logon.embed.secret	无	嵌入 BI 平台应用程序的门户和 BI 平台应用程序服务器之间的共享秘密，用于确定 BI 平台应用程序是否可安全地嵌入到其他页面中。
logon.embed.timeout	logon.embed.timeout=300	BI 平台应用程序（如 BI 启动板）拒绝嵌入门户前的秒数。确保 BI 平台 Web 服务器和门户服务器计算机上的系统时钟均在各自的此秒数范围之内。
iview.autologoff	iview.autologoff=true	设置为 true，为 SAP NetWeaver iViews 启用即时自动注销。
pinger.showWarningDialog	pinger.showWarningDialog=true	指定是否显示其中的消息指示当前会话即将过期的警告对话框。不适用于 CMC 和 BI 启动板。

18.2.1.2 BI 启动板属性

下表列出了 BOE.war 文件的默认 bilaunchpad.properties 文件中所包括的设置。若要覆盖任何设置，请在以下路径中新建一个文件：C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom。

设置	说明																		
app.name	指定应用程序的显示名称。该名称将显示在 Web 应用程序标题页和登录屏幕上。默认值: app.name=BI launch pad																		
app.name.short	指定应用程序的显示名称。该名称将显示在 Web 应用程序标题页和登录屏幕上。默认值: app.name.short=BI launch pad																		
app.url.name	指定应用程序的 URL 名称, 前面带有 "/" 字符。默认值: app.url.name=/BI																		
authentication.default	<p>指定用于对访问应用程序的用户进行身份验证的默认身份验证方法。可以针对此设置使用以下任意方法:</p> <table> <tr> <th>身份验证</th><th>设置值</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>secpcenterprise</td></tr> <tr> <td>JD Edwards</td><td>secPSE1</td></tr> <tr> <td>Siebel</td><td>secSiebel7</td></tr> <tr> <td>Oracles EBS</td><td>secOraApps</td></tr> </table> <p>默认值: authentication.default=secEnterprise</p>	身份验证	设置值	Enterprise	secEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpcenterprise	JD Edwards	secPSE1	Siebel	secSiebel7	Oracles EBS	secOraApps
身份验证	设置值																		
Enterprise	secEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpcenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel7																		
Oracles EBS	secOraApps																		
authentication.visible	指定登录到 BI 启动板的用户是否可以查看和更改身份验证方法。默认值: authentication.visible=false																		
cms.default	指定默认的 CMS 名称。默认值: cms.default=[主机的名称]																		
cms.visible	指定登录到 BI 启动板的用户是否可以查看和更改 CMS 名称。默认值: cms.visible=true																		
dialogue.prompt.enabled	指定当用户导航离开输入页时是否应在对话框中提示用户。默认值: dialogue.prompt.enabled=false																		
logontoken.enabled	指定是否在用户登录到 BI 启动板后启用会话的标记创建。标记将存储在 Cookie 中。默认值: logontoken.enabled=false																		
SMTPFrom	<p>将对象计划到目标时, 启用或禁用“从”字段。默认值: SMTPFrom=true</p> <p>当该值设置为 false 时, 将不会显示“从”字段, 并且系统将尝试按以下顺序检索“从”电子邮件值:</p> <ul style="list-style-type: none"> 1 首先, 从报表对象的报表默认设置中检索。 2 其次, 从登录用户的用户配置文件中的电子邮件地址中检索。 3 最后, 从作业服务器的默认设置中检索。 																		

设置	说明
url.exit	指定在终止用户的 BI 启动板会话后用于重定向用户的 URL。此设置仅适用于已通过外部验证流程登录到应用程序的用户。
disable.locale.preference	启用或禁用用户查看以修改 BI 启动板的本地查看首选项。默认值: disable.locale.preference=false
extlogon.allow.logoff	用户结束其 BI 启动板会话后, 启用或禁用自动注销用户会话。如果希望用户注销 BI 启动板时不自动终止用户会话, 则设置为 false。默认值: extlogon.allow.logoff=true
logon.allowInsecureEmbedding	指定是否允许其他页面嵌入该应用程序 (作为框架), 而无需传递有效的嵌入标记。默认: logon.allowInsecureEmbedding=false
sso.types.and.order	<p>指定要启用的 SSO 类型以逗号分隔的列表及其执行顺序。</p> <p>空列表表示将使用传统的排序。</p> <p>如果已指定列表, 将忽略传统选项。</p> <p>有效选项: vintela、trustedIIS、trustedHeader、trustedParameter、trustedCookie、trustedSession、trustedUserPrincipal、trustedVintela、trustedX509、sapSSO 和 siteminder。</p> <p>如果不需要, 请指定: none</p>

18.2.1.3 OpenDocument 属性

下表列出了 BOE.war 文件的默认 opendocument.properties 文件中所包括的设置。若要覆盖任何设置, 请在以下路径中新建一个文件: C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom。

设置	说明																		
app.name	指定应用程序的显示名称。该名称将显示在 Web 应用程序标题页和登录屏幕上。默认值: app.name=SAP BusinessObjects OpenDocument																		
app.name.short	指定应用程序的显示名称。该名称将显示在 Web 应用程序标题页和登录屏幕上。默认值: app.name.short=OpenDocument																		
authentication.default	<p>指定用于对访问应用程序的用户进行身份验证的默认身份验证方法。可以针对此设置使用以下任意方法:</p> <table border="1"> <thead> <tr> <th>身份验证</th><th>设置值</th></tr> </thead> <tbody> <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>secpenterprise</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> </tbody> </table> <p>默认值: authentication.default=secEnterprise</p>	身份验证	设置值	Enterprise	secEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpenterprise	JD Edwards	secPSE1	Siebel	secSiebel7	Oracles EBS	secOraApps
身份验证	设置值																		
Enterprise	secEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel7																		
Oracles EBS	secOraApps																		
authentication.visible	指定登录到 OpenDocument 的用户是否可以查看和更改身份验证方法。默认值: authentication.visible=false																		
cms.default	指定默认的 CMS 名称。默认值: cms.default=[主机的名称]																		
cms.visible	指定登录到 OpenDocument 的用户是否可以查看和更改 CMS 名称。默认值: cms.visible=true																		
logontoken.enabled	指定是否在用户登录到 OpenDocument 后启用会话的标记创建。标记将存储在 Cookie 中。默认值: logontoken.enabled=false																		
extlogon.allow.logoff	在用户结束其 OpenDocument 会话后, 启用或禁用自动注销用户会话。如果希望用户注销 OpenDocument 后不自动终止用户会话, 则设置为 false。默认值: extlogon.allow.logoff=true																		

设置	说明
SAPLogonToken.enabled	指定是否允许 RESTful Web 服务 SAP 登录标记进行身份验证后进入 BI 平台。通过 RESTful Web 服务 URL 成功登录后，请求标头中的 X-SAP-LogonToken 值会指定 SAP 登录标记。默认值：SAPLogonToken.enabled=true
logon.allowInsecureEmbedding=false	指定是否允许其他页面嵌入该应用程序（作为框架），而无需传递有效的嵌入标记。默认：logon.allowInsecureEmbedding=false
sso.types.and.order	<p>指定要启用的 SSO 类型以逗号分隔的列表及其执行顺序。</p> <p>空列表表示将使用传统的排序。</p> <p>如果已指定列表，将忽略传统选项。</p> <p>有效选项：serializedSession、sapLogonToken、trustedIIS、trustedHeader、trustedParameter、trustedCookie、trustedSession、trustedUserPrincipal、trustedVintela、vintela、infoview、trustedX509、sapSSO 和 siteminder。</p> <p>如果不需要，请指定：none</p>

18.2.1.4 CMC 属性

下表列出了 BOE.war 的默认 cmc.properties 文件中所包括的设置。若要覆盖任何设置，请在以下路径中新建一个文件：C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\config\custom。

设置	说明																		
app.url.name	指定应用程序的 URL 名称，前面带有 "/" 字符。默认值：app.url.name=/CMC																		
authentication.default	<p>指定用于对访问应用程序的用户进行身份验证的默认身份验证方法。可以针对此设置使用以下任意方法：</p> <table> <tr> <th>身份验证</th><th>设置值</th></tr> <tr> <td>Enterprise</td><td>secEnterprise</td></tr> <tr> <td>LDAP</td><td>secLDAP</td></tr> <tr> <td>Windows AD</td><td>secWinAD</td></tr> <tr> <td>SAP</td><td>secSAPR3</td></tr> <tr> <td>PeopleSoft</td><td>secpssenterprise</td></tr> <tr> <td>JD Edwards</td><td>secPSE1</td></tr> <tr> <td>Siebel</td><td>secSiebel7</td></tr> <tr> <td>Oracles EBS</td><td>secOraApps</td></tr> </table> <p>默认值：authentication.default=secEnterprise</p>	身份验证	设置值	Enterprise	secEnterprise	LDAP	secLDAP	Windows AD	secWinAD	SAP	secSAPR3	PeopleSoft	secpssenterprise	JD Edwards	secPSE1	Siebel	secSiebel7	Oracles EBS	secOraApps
身份验证	设置值																		
Enterprise	secEnterprise																		
LDAP	secLDAP																		
Windows AD	secWinAD																		
SAP	secSAPR3																		
PeopleSoft	secpssenterprise																		
JD Edwards	secPSE1																		
Siebel	secSiebel7																		
Oracles EBS	secOraApps																		
authentication.visible	指定登录到 CMC 的用户是否可以查看和更改身份验证方法。默认值：authentication.visible=false																		
cms.default	指定默认的 CMS 名称。默认值：cms.default=[主机的名称]																		
cms.visible	指定登录到 CMC 的用户是否可以查看和更改 CMS 名称。默认值：cms.visible=true																		
dialogue.prompt.enabled	指定当用户导航离开输入页时是否应在对话框中提示用户。默认值：dialogue.prompt.enabled=false																		
logontoken.enabled	指定是否在用户登录到 CMC 后启用会话的标记创建。标记将存储在 Cookie 中。默认值：logontoken.enabled=false																		
SMTPFrom	<p>将对象计划到目标时，启用或禁用“从”字段。默认值：SMTPFrom=true</p> <p>当该值设置为 false 时，将不会显示“从”字段，并且系统将尝试按以下顺序检索“从”电子邮件值：</p> <ul style="list-style-type: none"> 1 首先，从报表对象的报表默认设置中检索。 2 其次，从登录用户的用户配置文件中的电子邮件地址中检索。 3 最后，从作业服务器的默认设置中检索。 																		

18.3 自定义 BI 启动板和 OpenDocument 登录入口点

可以自定义 BI 启动板和 OpenDocument Web 应用程序的登录页。例如，可以将登录页自定义为使用公司徽标或公司样式表，也可以创建支持受信任的身份验证的自定义登录页。

若要自定义登录页，请修改存储在 BOE.war Web 应用程序的 BI 启动板和 OpenDocument 应用程序区域的 custom.jsp 文件，然后将 BOE.war Web 应用程序重新部署到 BI 平台系统。用户可通过导航到唯一的 URL 访问自定义登录入口点。

若要使用这些示例，则需要熟悉部署 BI 平台 Web 应用程序的相关操作。有关更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

18.3.1 BI 启动板和 OpenDocument 文件位置

BI 启动板和 OpenDocument Web 应用程序封装在 BOE.war Web 存档文件中。BOE.war 存档的位置在 BOE.properties 文件中进行定义。

BOE.properties 文件在 Windows 系统中的位置如下：

- BOE 安装目录\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf\apps\BOE.properties

BOE.properties 文件在 Unix 系统中的位置如下：

- BOE 安装目录/sap_bobj/enterprise_xi40/wdeploy/conf/apps/BOE.properties

下表定义了 BI 启动板和 OpenDocument 应用程序的 BOE.war Web 存档文件中的公用文件的位置。

表18-5: BI 启动板文件位置

注意：
BI 启动板 Web 应用程序之前称为 InfoView。

文件类型	位置
自定义登录脚本	WEB-INF\eclipse\plugins\webpath.InfoView\web\custom.jsp
附加文件的目录	WEB-INF\eclipse\plugins\webpath.InfoView\web\noCacheCustomResources
自定义登录 URL	http://<服务器名>:<端口>/BOE/BI/custom.jsp

表18-6: OpenDocument 文件位置

文件类型	位置
自定义登录脚本	WEB-INF\eclipse\plugins\webpath.OpenDocument\web\opendoc\custom.jsp
附加文件的目录	WEB-INF\eclipse\plugins\webpath.OpenDocument\web\noCacheCustomResources
自定义登录 URL	http://<服务器名>:<端口>/BOE/OpenDocument/opendoc/custom.jsp

18.3.2 定义自定义登录页

可以自定义 BI 平台登录页的入口点。例如，可以创建显示公司徽标和使用公司样式表的自定义登录页。

编辑 custom.jsp 文件以自定义用户的登录体验，并将支持文件放入 noCacheCustomResources 文件夹中。

此示例说明了如何创建将用户重定向到标准登录页的自定义登录页。

- 1 创建一个包含自定义登录代码的文件，并在 noCacheCustomResources 文件夹中将其另存为 custom.js。

此示例定义了一个可将用户重定向到标准登录页的函数，即 logon.jsp。

```
function load() {window.location = "logon.jsp";}
```

- 2 编辑 custom.jsp 文件以自定义登录页。

此示例会显示一则欢迎消息和一个调用在 custom.js 文件中定义的加载方法的超链接。

```
<!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 重新部署 BOE.war Web 应用程序，并重新启动 Web 服务器。

18.3.3 登录时添加受信任的身份验证

若要启用受信任的身份验证，请在 `custom.jsp` 文件中将受信任用户设置为会话属性，并且在 `global.properties` 文件的副本中修改身份验证设置。`global.properties` 文件的自定义副本的值将覆盖默认值。

- 1 编辑 `custom.jsp` 文件以设置一个定义受信任用户的会话属性。

```
request.getSession().setAttribute("TrustedUserAttribute", "TrustedUser");
```

- 2 通过将 `WEB-INF\config\default\global.properties` 复制到 `WEB-INF\config\custom\global.properties` 创建 `global.properties` 文件的自定义副本。
- 3 修改 `WEB-INF\config\custom\global.properties` 以启用单一登录（SSO）。

```
sso.enabled=true
```

- 4 修改 `WEB-INF\config\custom\global.properties` 以设置受信任的身份验证的参数，其中包括受信任用户会话变量和共享秘密。
用系统的共享秘密替换 "...".

```
trusted.auth.user.param=TrustedUserAttribute  
trusted.auth.user.retrieval=WEB_SESSION  
trusted.auth.shared.secret="..."
```

有关更多详细信息，请参阅为 Web 应用程序配置受信任的身份验证的相关主题。

- 5 重新部署 Web 应用程序并重新启动 Web 服务器。
- 6 在 CMC 中，启用受信任的身份验证。
在“身份验证”选项卡中，双击“Enterprise”，然后选择复选框“已启用受信任的身份验证”。

相关主题

- 第 212 页上的[“启用受信任的身份验证”](#)
- 第 216 页上的[“为 Web 应用程序配置受信任的身份验证”](#)

18.4 自定义 Web Intelligence 界面

在 CMC 中，可自定义用户组 Web Intelligence 界面元素的外观，例如，整个工具栏或工具栏的特定条目，并自定义对特定文档模式的访问权。

默认情况下，系统将显示所有界面元素。如果不想显示特定元素，则可在 CMC 中取消选择这些元素：在“用户和组”选项卡中，选择一个用户或组，然后单击“操作” > “自定义”。

自定义部分包含以下选项卡：

- 功能

在该选项卡上，可选择与功能有关的隐藏按钮，例如：“刷新”。

- 用户界面元素

在此选项卡中，可选择要隐藏的个别界面元素，如工具栏或选项卡，或其子元素（例如，按钮命令）。

注意：

自定义适用于所有 Web Intelligence 应用程序客户端：Web、Java Applet 和胖客户端。

18.4.1 “功能”选项卡

功能项目	说明	影响以下界面项目
刷新	用户可以刷新文档，以从数据源更新数据。	在阅读和设计模式下使用“标准操作组”工具栏中的“刷新”按钮。
钻取	用户可在文档中向上和向下钻取数据。	“钻取”按钮可用于以下位置： <ul style="list-style-type: none">• 阅读模式下的“分析组”工具栏。• 设计模式中“分析”选项卡下的“交互”子选项卡。
阅读模式	用户可在阅读模式下查看文档。	“阅读”按钮位于以下位置： <ul style="list-style-type: none">• 应用程序上下文菜单• 应用程序控制工具栏
设计模式	用户可在设计模式下查看文档。	“设计”按钮位于以下位置： <ul style="list-style-type: none">• 应用程序上下文菜单• 应用程序控制工具栏
数据模式	用户可在数据模式下查看文档。	“数据”按钮位于以下位置： <ul style="list-style-type: none">• 应用程序上下文菜单• 应用程序控制工具栏

18.4.2 “用户界面元素”选项卡

用户可自定义的一些界面元素将在随后小节的图表中加以确定。使用下表来确定图表中的元素项目。

“用户界面元素”项目	子元素项目	说明	图表编号
启动屏幕		选择此项目，可隐藏用户打开 Web Intelligence 时显示的屏幕。	
应用程序上下文菜单		选择此项目，可隐藏用户右击 Web Intelligence 屏幕时显示的菜单。	1
	应用程序模式	选择此项目，可在“应用程序上下文菜单”中隐藏应用程序模式更改选项。	1a
	过滤器栏	选择此项目，可在“应用程序上下文菜单”中隐藏“过滤器栏”选项。	1b
	大纲	选择此项目，可在“应用程序上下文菜单”中隐藏“大纲”选项。	1c
	公式栏	选择此项目，可在“应用程序上下文菜单”中隐藏“公式栏”选项。	1d
	侧面板	选择此项目，可在“应用程序上下文菜单”中隐藏“侧面板”选项。	1e
	报表选项卡	选择此项目，可在“应用程序上下文菜单”中隐藏“报表选项卡”选项。	1f
	状态栏	选择此项目，可在“应用程序上下文菜单”中隐藏“状态栏”选项。	1g
侧面板		选择此项目，可隐藏报表面板旁的“侧面板”，以允许用户访问各种信息选项卡。	2
	文档摘要	选择此项目，可在“侧面板”中隐藏“文档摘要”选项卡。	2a
	导航图	选择此项目，可在“侧面板”中隐藏“导航图”（在 HTML 界面中称为“报表导航图”）选项卡。	2b
	输入控件	选择此项目，可在“侧面板”中隐藏“输入控件”选项卡。	2c

“用户界面元素”项目	子元素项目	说明	图表编号
	用户提示输入	选择此项目，可在“侧面板”中隐藏“用户提示输入”选项卡。	2d
	可用对象	选择此项目，可在“侧面板”中隐藏“可用对象”选项卡。	2e
	文档结构和过滤器	选择此项目，可在“侧面板”中隐藏“文档结构和过滤器”选项卡。	2f
	Web 服务发布者	选择此项目，可在“侧面板”中隐藏“Web 服务发布者”选项卡。	2g
	数据	选择此项目，可在“侧面板”中隐藏“数据”选项卡。	2h
状态栏		选择此项目隐藏“状态栏”，用户可在其中查看文档操作状态相关信息，并可执行缩放、页面导航以及“公式栏”激活等任务。	3
	“报表”下拉列表	选择此项目，可在“状态栏”中隐藏“报表”下拉列表。	3a
	打印状态图标	选择此项目，可在“状态栏”中隐藏打印状态图标列表。	3b
	跟踪数据更改	选择此项目，可在“状态栏”中隐藏“跟踪数据更改”状态。	3c
	页面导航	选择此项目，可在“状态栏”中隐藏“页面导航”栏。	3d
	分页模式	选择此项目，可在“状态栏”中隐藏“分页模式”按钮。	3e
	缩放列表	选择此项目，可在“状态栏”中隐藏“缩放百分比”下拉列表。	3f
	缩放滑块	选择此项目，可在“状态栏”中隐藏“缩放滑块”栏。	3g
	工作区状态	选择此项目，可在“状态栏”中隐藏“工作区状态”指示符。 注意： 如果工作区出现问题，“工作区状态”指示符（  ）将在“缩放滑块”和“上次刷新日期”之间显示。	不显示
	上次刷新日期	选择此项目，可在“状态栏”中隐藏文档刷新日期。	3i
	连接状态	选择此项目，可在“状态栏”中隐藏 Web Intelligence 胖客户端连接状态。	3j

“用户界面元素”项目	子元素项目	说明	图表编号
报表分区		选择此项目，可在 Web Intelligence 中隐藏“报表区”。	4
	报表选项卡	选择此项目，可在报表分区中隐藏“报表”选项卡。	4a
	双向页面滚动	选择此项目，可在“报表区”页面右下角隐藏双向页面滚动功能。	4b
	公式栏	选择此项目，可在报表分区顶部隐藏“公式栏”。	4c
阅读模式工具栏		选择此项目，可隐藏在阅读模式下显示的工具栏。	5
	Web Intelligence 下拉列表	选择此项目，可在阅读模式下隐藏 Web Intelligence 下拉列表。	5a
	文件组	选择此项目，可在阅读模式下隐藏“文件组”工具栏。	5b
	标准操作组	选择此项目，可在阅读模式下隐藏“标准操作组”工具栏。	5c
	分析组	选择此项目，可在阅读模式下隐藏“分析组”工具栏。	5d
设计模式工具栏		选择此项目，可隐藏在设计模式下显示的工具栏和选项卡。	6
	“文件”选项卡	选择此项目，可在阅读模式下隐藏“文件”选项卡。	6a
	“属性”选项卡	选择此项目，可在阅读模式下隐藏“属性”选项卡。	6b
	标准操作组	选择此项目，可在阅读模式下隐藏“标准操作组”工具栏。	6c
	“报表元素”选项卡	选择此项目，可在阅读模式下隐藏“报表元素”选项卡。	6d
	“格式”选项卡	选择此项目，可在阅读模式下隐藏“格式”选项卡。	6e
	“数据访问”选项卡	选择此项目，可在阅读模式下隐藏“数据访问”选项卡。	6f
	“分析”制表符	选择此项目，可在阅读模式下隐藏“分析”选项卡。	6g
	“页面设置”选项卡	选择此项目，可在阅读模式下隐藏“页面设置”选项卡。	6h

“用户界面元素”项目	子元素项目	说明	图表编号
初始工具栏		选择此项目，可隐藏用户在打开 Web Intelligence 应用程序时显示的初始工具栏。	7
	Web Intelligence 下拉列表	选择此项目，可在初始工具栏中隐藏 Web Intelligence 下拉列表。	7a
	文件组	选择此项目，可在初始工具栏中隐藏“文件组”工具栏。	7b
应用程序控制工具栏		选择此项目，可隐藏在 Web Intelligence 上层工具栏中显示的“应用程序控制工具栏”。	8
	应用程序模式按钮	选择此项目，可在 Web Intelligence 上层工具栏中隐藏应用程序模式按钮（“阅读”、“设计”和“数据”）。	8a
	工具	选择此项目，可在 Web Intelligence 上层工具栏中隐藏“工具”图标。	8b
	帮助	选择此项目，可在 Web Intelligence 上层工具栏中隐藏“帮助”图标。	8c
	收盘	选择此项目，可在 Web Intelligence 上层工具栏中隐藏“关闭”图标。	8d

初始屏幕

在 CMC 用户和组自定义中，用户可选择隐藏显示的 Web Intelligence 初始屏幕。下图显示用户打开 Web Intelligence 时默认显示的初始屏幕。



图 18-2：初始屏幕（英文示例）

应用程序上下文菜单

以下图表显示可在右击上下文菜单中隐藏的项目。

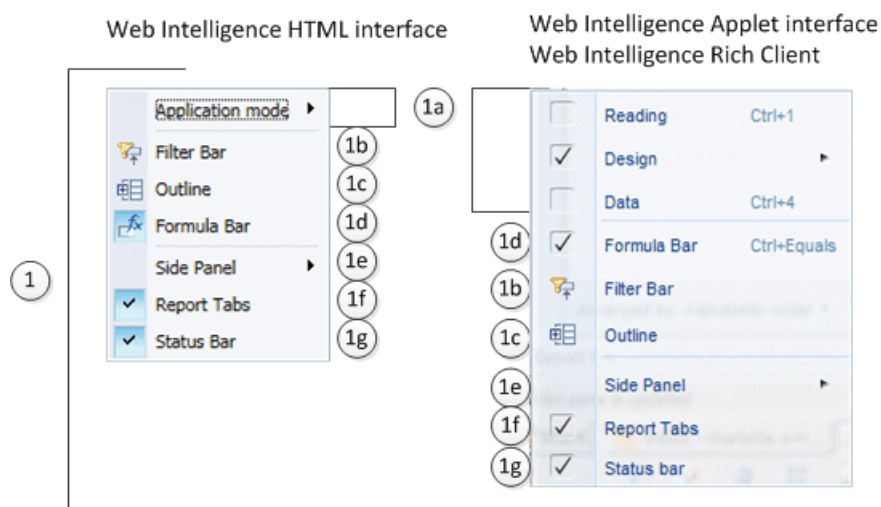
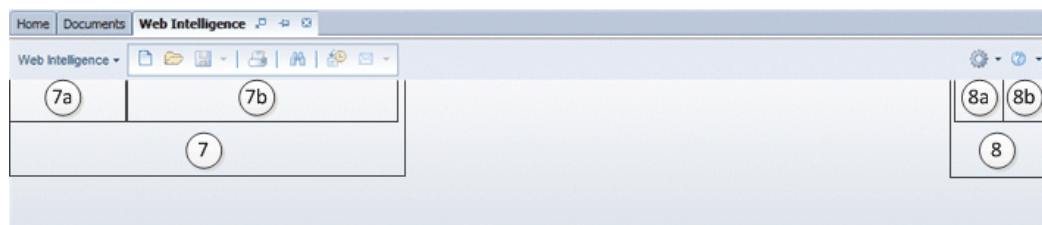


图 18-3: 应用程序上下文菜单（英文示例）

初始工具栏

以下图表显示在未打开任何文档时，可在 Web Intelligence 的工具栏中隐藏的项目。

Web Intelligence Applet interface
Web Intelligence Rich Client

Web Intelligence HTML interface

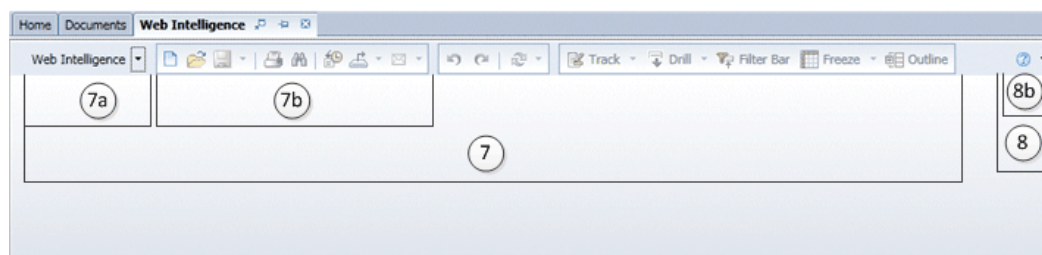
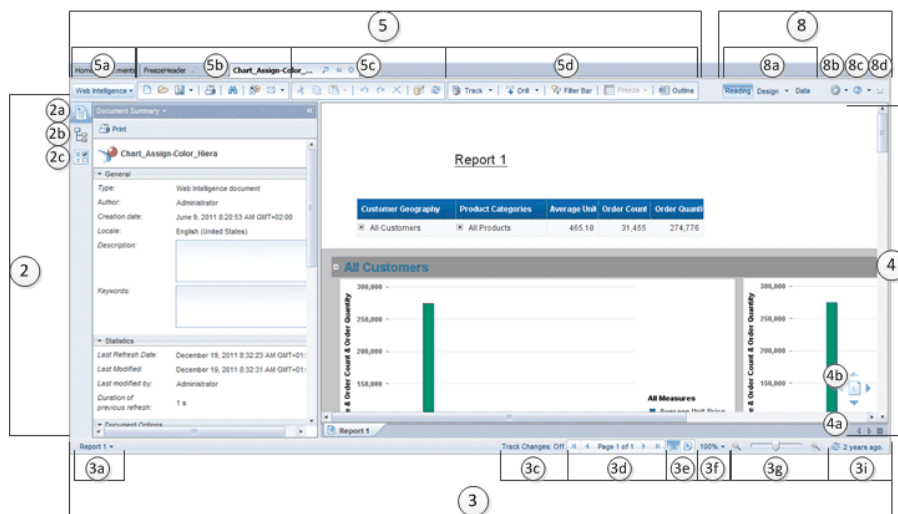


图 18-4: 初始工具栏（英文示例）

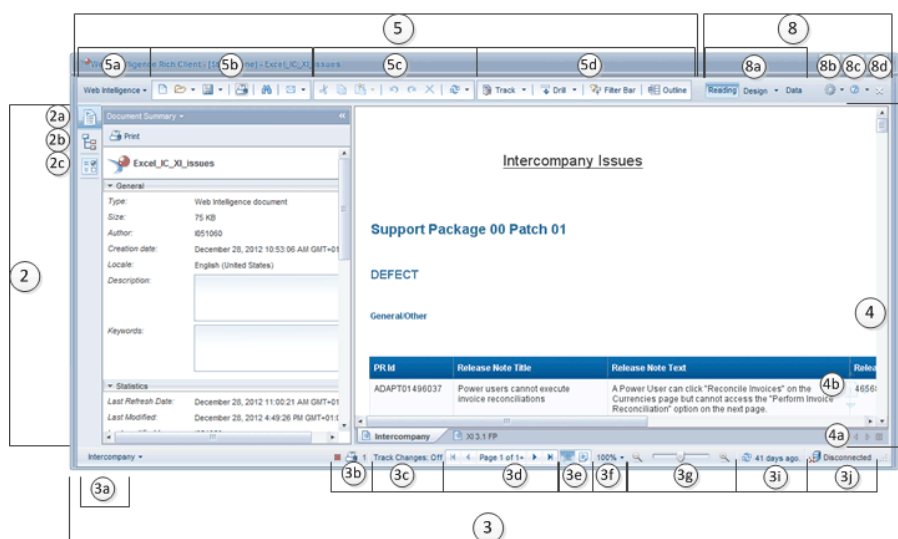
阅读模式

以下图表显示可在 Web Intelligence 阅读模式下隐藏的项目。

Web Intelligence Applet interface



Web Intelligence Rich Client



Web Intelligence HTML interface

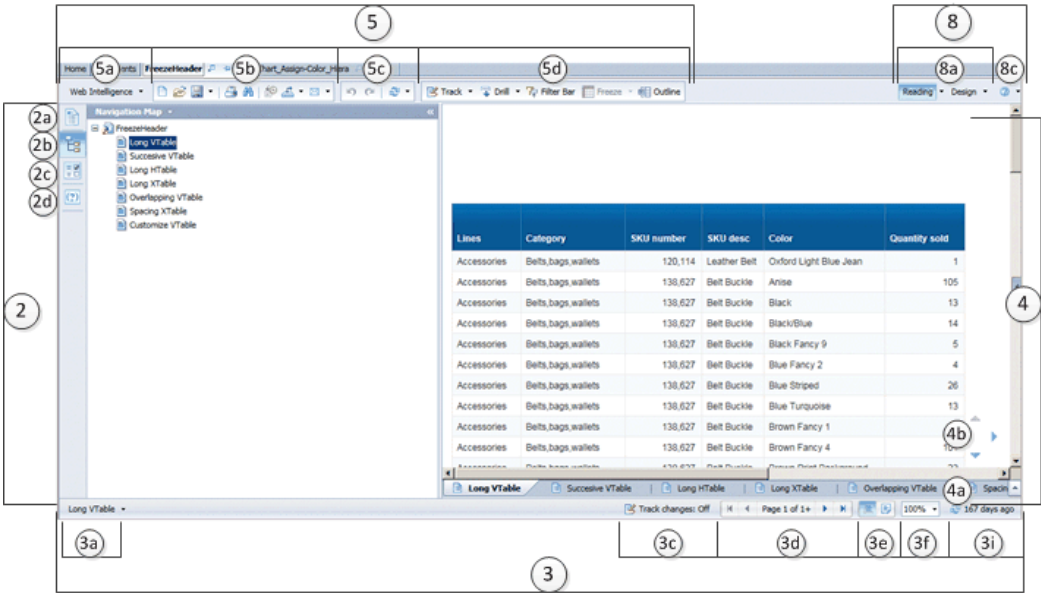
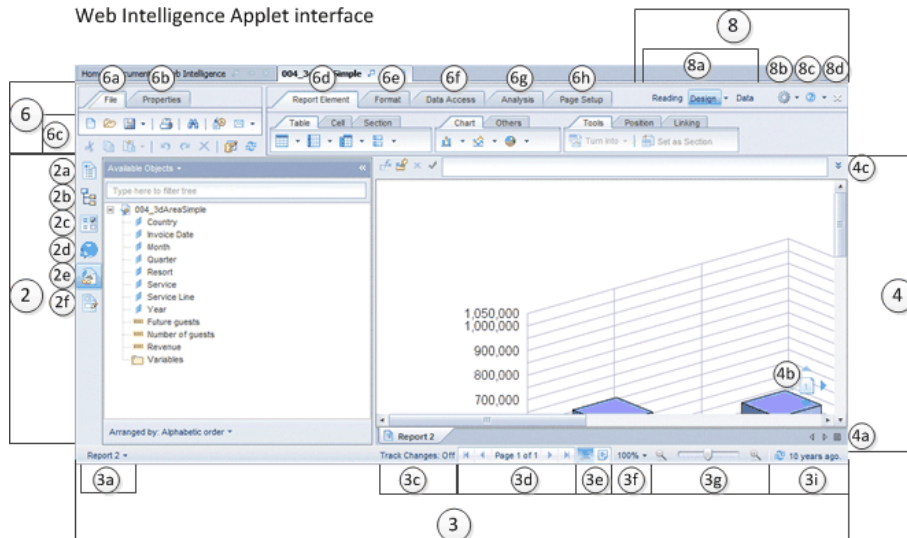


图 18-5：阅读模式（英文示例）

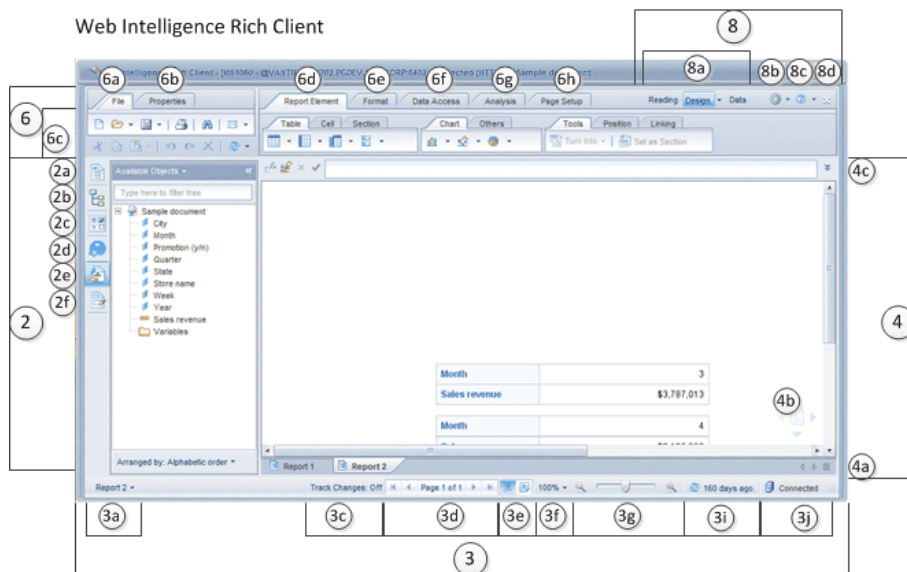
设计模式

以下图表显示可在 Web Intelligence 设计模式下隐藏的项目。

Web Intelligence Applet interface



Web Intelligence Rich Client



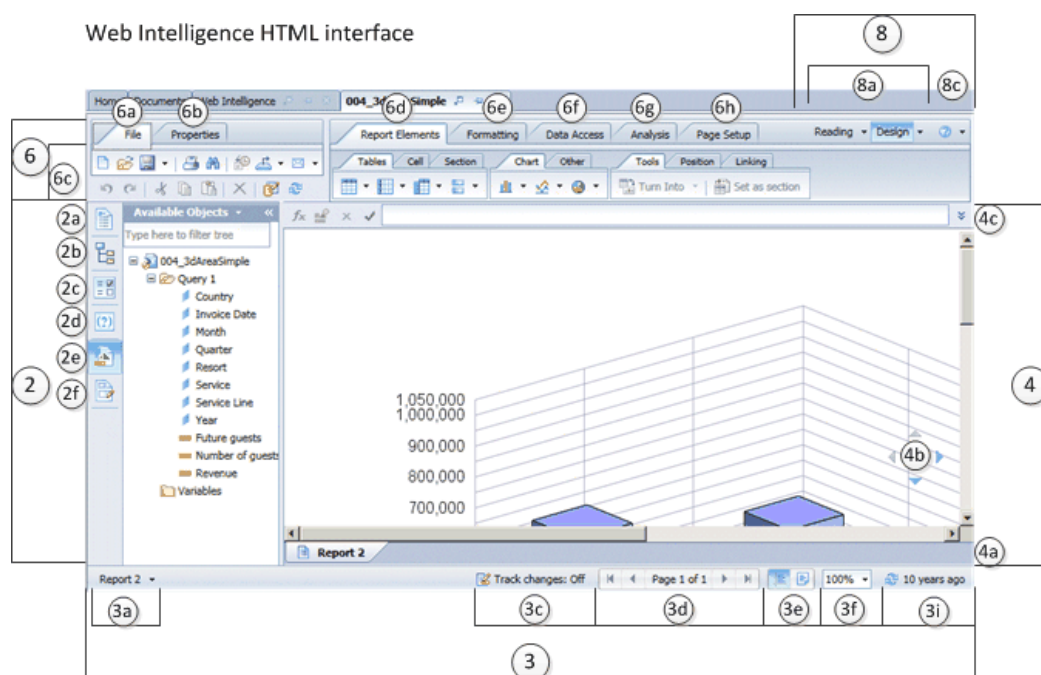
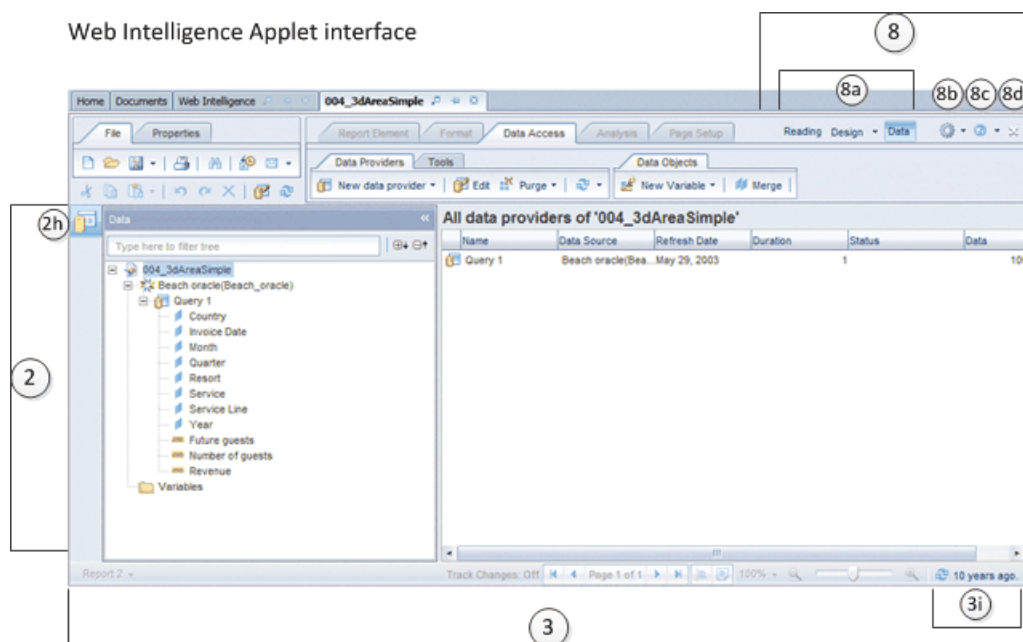


图 18-6: 设计模式 (英文示例)

数据模式

以下图表显示可在 Web Intelligence 数据模式下隐藏的项目。

Web Intelligence Applet interface



Web Intelligence Rich Client

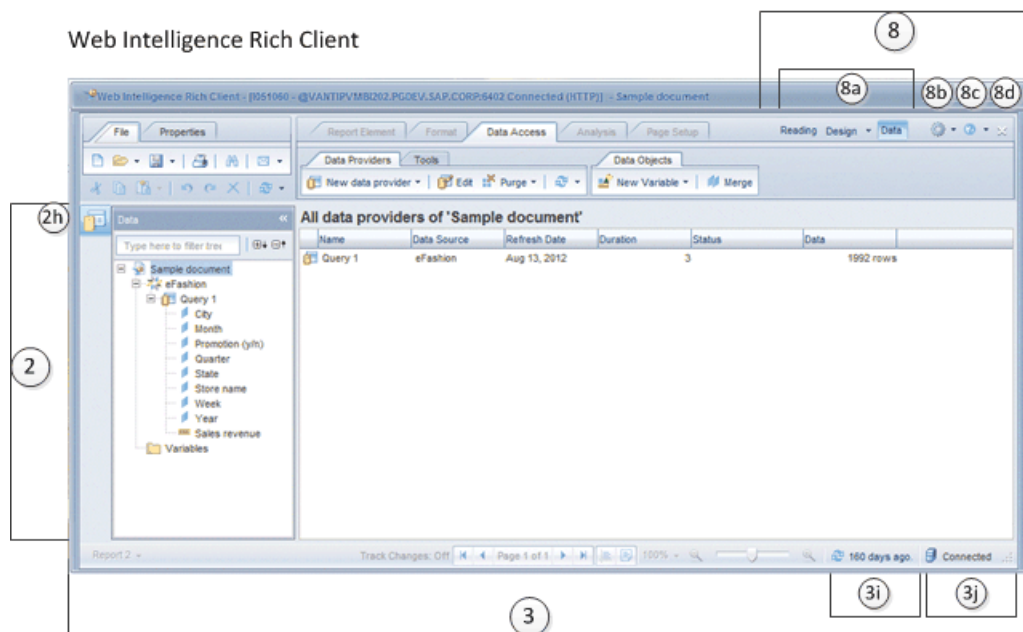


图 18-7：数据模式（英文示例）

18.4.3 自定义 Web Intelligence 界面外观

用户可通过隐藏所选“用户组”所有成员中的菜单项、子项目和功能来自定义 Web Intelligence 用户界面的外观。

- 1 以管理员身份登录 CMC。
- 2 从“组织”列表中，选择“用户和组”。
- 3 在“组层次结构”列表中，选择一个用户组。
- 4 从“管理”列表中，选择“属性”。
- 5 在侧面板中，选择“自定义”。
- 6 执行以下操作之一：
 - 要在 Web Intelligence 中隐藏项目，可在“用户界面元素”或“功能”选项卡中将其选中。
 - 要在 Web Intelligence 中显示隐藏的项目，则可在“用户界面元素”或“功能”选项卡中取消选择这些项目。
- 7 单击“保存并关闭”。

保存自定义后，所选组的所有用户均将在下次登录 BI 启动板及打开 Web Intelligence 看到这些更改。

注意：

我们建议用户以已定义组中的用户身份登录 BI 启动板，启动 Web Intelligence，并验证该界面是否符合自定义设置。

第 19 章 管理连接和 Universe

19.1 管理连接

连接是一组指定参数集，用于定义一个或多个 SAP BusinessObjects 应用程序访问关系数据库或 OLAP 数据库的方式。诸如服务器名称、数据库、用户名和密码等连接详细信息都可以安全地存储在 BI 平台资源库的“连接”文件夹中。

设计者根据连接定义 Universe。查询、分析和报告应用程序的用户可以使用 Universe 访问数据库，而无需了解有关数据库中基础数据结构的任何信息。

用户可使用以下应用程序创建连接：

- Universe 设计工具。连接存储在资源库中。
- 信息设计工具。可以在本地创建连接，然后发布至资源库，或者直接在资源库中创建和编辑连接。

注意：

有关如何管理 OLAP 数据源连接的信息，请参阅《SAP BusinessObjects Analysis (OLAP 版) 管理员指南》。

有权限允许用户创建、编辑和删除连接。

可以授予用户对 Universe 连接的访问权限，并允许用户创建和查看使用 Universe 和连接的文档。

相关主题

- 第 120 页上的“[在 CMC 中管理对象的安全设置](#)”
- 第 891 页上的“[连接权限](#)”

19.1.1 删除 Universe 连接

提示：

可以在 Universe 设计工具和信息设计工具中删除连接。

- 1 在“连接”区域中，从列表中选择一个 Universe 连接。
- 2 单击“管理” > “删除”。

19.2 管理 Universe

Universe 是经过组织的元数据对象集合，供业务用户以非技术语言分析公司数据并根据这些数据生成报表。这些对象包括维、度量、层次关系、属性、预定义计算、函数和查询。元数据对象层在关系数据库表模式或 OLAP 多维数据集上构建，因此对象直接映射到数据库结构。Universe 包含到数据源的连接，因此查询和分析工具的用户可以连接到 Universe，并使用 Universe 中的对象运行查询和创建报表，而无需了解有关数据库中基础数据结构的信息。

可以使用以下工具创建 Universe：

- Universe 设计工具。使用这一工具创建的 Universe 可以通过 .unv 扩展名来区分，因此称为 .unv Universe。 .unv Universe 在安全的连接中定义，存储于资源库 Universe 文件夹中。
- 信息设计工具。使用这一工具创建的 Universe 基于新的语义层。通过 .unx 扩展名来区分，因此称为 .unx Universe。 .unx Universe 在本地创建并发布至资源库 Universe 文件夹中。设计者可以使用信息设计工具安全编辑器定义对象级别的安全性。

可以授予用户对应用程序和 Universe 的权限，允许其创建、编辑和删除 Universe 以及设计 Universe 的安全性。

可以授予用户对 Universe 的权限，允许其创建和查看使用 Universe 的文档。

相关主题

- 第 120 页上的“[在 CMC 中管理对象的安全设置](#)”
- 第 902 页上的“[Universe 设计工具权限](#)”
- 第 887 页上的“[Universe \(.unv\) 权限](#)”
- 第 903 页上的“[信息设计工具权限](#)”
- 第 889 页上的“[Universe \(.unx\) 权限](#)”

19.2.1 删除 Universe

提示：

还可以在信息设计工具中删除 Universe。

- 1 在 CMC 的 “Universe” 区域中，选择列表中的一个 Universe。
- 2 单击 “管理” > “删除”。
- 3 如果提示确认，请单击 “确定”。

第 20 章 监控

20.1 关于监控

通过监控应用程序，您可针对报表和通知捕获 BI 平台服务器的运行时和历史量度。监控应用程序有助于系统管理员确定应用程序是否工作正常，以及响应时间是否为期望值。通过提供关键业务量度，监控应用程序可以支持您更深入地了解 BI 平台。

监控允许您执行以下任务：

- 检查每台服务器的性能：可借助监测器进行检查，检测器会用红绿灯显示每台服务器的状态。系统管理员可以为这些监测器设置阈值，并可在超过阈值时接收到警报。这有助于在即将出现故障或断开的情况下采取主动措施。
- 查看关键系统的关键绩效指标（KPI）：这有助于监控活动和资源。这些 KPI 显示在监控应用程序的“仪表盘”页面中。
- 基于服务器组、服务类别和 Enterprise 节点查看图形和表格格式的整个 BI 平台部署。
- 在仪表盘屏幕上查看最近的故障。
- 检查系统可用性和响应时间：利用探测器可以模拟工作流，以检查 BI 平台部署中的服务器和服务是否按预期运转。通过定期分析这些探测器的往返时间，系统管理员可以评估系统使用模式。
- 分析 CMS 的峰值负载和峰值期间：这有助于系统管理员确定是否需要更多的许可或系统资源。
- 与其他企业应用程序集成：BI 平台监控应用程序可以与其他企业应用程序（例如 SAP Solution Manager 和 IBM Tivoli Monitoring）集成。

相关主题

- 第 946 页上的[“关于服务器量度附录”](#)

20.2 监控术语

下面列出了与监控应用程序有关的术语：

趋势

为发现趋势这一目的记录或显示历史数据。

仪表盘

“仪表盘”页面为系统管理员提供了用于监视所有服务器性能的集中式视图。它提供有关系统 KPI、最近的警报、监测器以及基于监测器状态的相应图形的实时信息。

监测器

监测器提供 BI 平台环境中服务器和工作流的实时状态和历史趋势。用户可将阈值和警报与监测器关联起来可以使用探测器、服务器、SAPOSCOL 或派生量度中的数据创建监测器。

派生量度

派生量度是将两个或两个以上的现有量度合并为一个数学等式而创建的量度。可根据用户需要创建量度，然后使用该量度创建监测器。

拓扑量度

拓扑量度可提供 BI 平台中每种服务类别的净状态。例如，Crystal Reports 服务可提供与 Crystal Reports 服务器相关的所有监测器的综合运行状态。

健康状态

健康状态值如下所述：

- “0” — 危险
- “1” — 警告
- “2” — 良好

KPI

KPI（关键性能指标）是 BI 平台中的标准量度。它们提供有关计划和登录会话的信息。例如，“运行中作业数”的数字越大，表明服务器的性能越好。相反，“挂起作业数”的数字越大，表明系统的性能越差、负载越重。

探测器

探测器可以监控各种服务，并模拟 BI 平台组件的不同功能。通过计划使探测器按指定时间间隔运行，系统管理员可以跟踪 BI 平台提供的关键服务的可用性和性能。这些数据还可用于能力计划。

红绿灯

红绿灯是一个图标，显示绿色、黄色或红色以指示任何时刻检测器的状态。用户可以选择设置两种或三种监测器状态。

趋势图

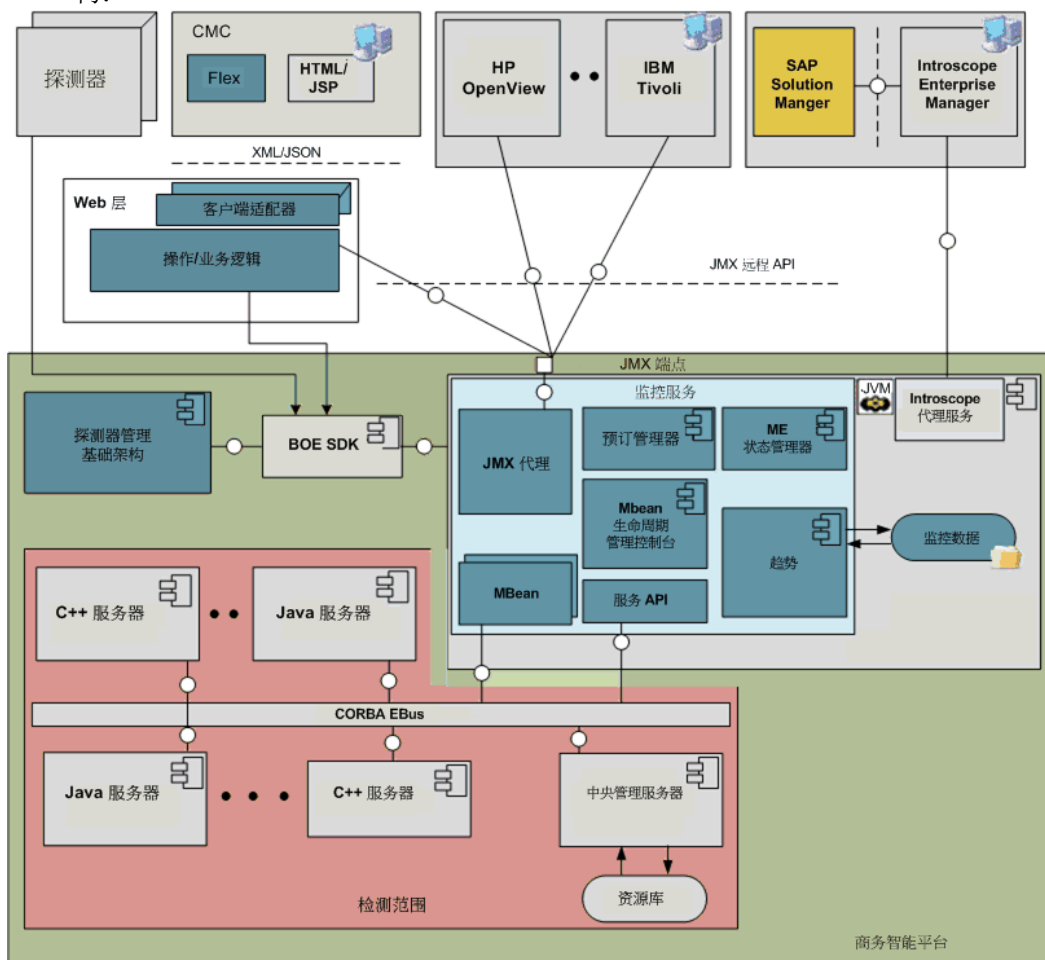
趋势图是探测器和服务器所生成历史量度数据的图形表示。它有助于系统管理员以不同的时间间隔监控系统，并且评估系统使用模式。

警报

警报是在超出为应用于监测器的不同度量设置的用户定义阈值时，由监控应用程序生成的通知。可以选择通过电子邮件接收警报，或在“仪表板”页面上进行查看。

20.2.1 体系结构

本节概述了监控体系结构，并简要介绍了各组件所扮演的角色。下面以图形方式显示了监控体系结构：



下面列出了体系结构中的高级组件：

- 自适应处理服务器（APS）
- Java 管理扩展（JMX）代理/服务器
- MBean
- JMX 客户端
- 管理控制台
- 趋势数据库

监控服务承载于自适应处理服务器上。该应用程序基于 JMX 技术。

监控服务提供监控应用程序中的可用核心服务。监控服务提供以下服务：

- 提供 JMX 代理服务。
- 为 SAP BusinessObjects 服务器动态创建 MBean。
- 为 MBean 提供生命周期管理。
- 提供一种注册新探测器的机制。
- 允许用户使用服务器的量度创建复杂的阈值条件。
- 提供阈值通知机制并发送警报。
- 存储历史数据。

承载于自适应作业服务器中的探测器计划服务管理探测器的运行和计划。因此，需要运行自适应作业服务器，才能运行探测器。

监控应用程序还提供 JMX 或远程方法调用 (RMI) URL 端点。IBM Tivoli Monitoring 等其他企业应用程序可通过使用 JMX 远程 API 连接到监控应用程序并访问 BI 平台量度。监控应用程序使用专用 Derby 数据库，以存储用于趋势目的的历史数据。有关趋势数据库模式的信息，请参见第 986 页上的[“趋势数据库模式”](#)。

20.3 配置监控的数据库支持

本节介绍如何设置监控以及根据监控数据制定报表。

注意：

只有选择“写入趋势数据库”设置的监测器将监控信息写入趋势数据库。

有两个数据库选项用于记录监控信息：

- 在嵌入式 Derby 数据库中记录信息（默认选项）。

监控应用程序包括一个嵌入式 Apache Derby 数据库，通常称作“趋势数据库”，默认情况下在其中存储监控信息。用户可根据 Derby 数据库制定报表；但它不提供故障切换或传统的关系数据库备份和恢复工具。此外，必须手动刷新 Derby 数据库才能返回最新信息。

- 将信息记录到审核数据库（CMS 在其中存储审核数据的关系数据库）。

不使用默认的 Derby 数据库，可选择使用审核数据库存储 (ADS)，后者通常被称为审核数据库。可使用随 BI 平台提供的审核数据库，或配置为审核数据库的另一个支持的数据库。使用审核数据库允许用户根据审核数据和监控信息制定报表。捕捉关系数据库中的数据可提供备份和恢复功能，以及数据的实时可用性。

相关主题

- 第 629 页上的[“使用 Derby 数据库的配置”](#)
- 第 629 页上的[“使用审核数据库的配置”](#)

20.3.1 使用 Derby 数据库的配置

默认情况下，监控应用程序在嵌入式 Derby 数据库存储监控数据。如果要使用 Derby 数据库，请确认 CMC 中的以下数据库设置：

- 1 在 CMC 主页的“管理”区域中，单击“应用程序”。
- 2 双击“监控应用程序”打开属性页面。
- 3 在“趋势数据库设置”区域中，检查是否已选中使用嵌入式数据库。

要在 Derby 数据库中运行查询以创建报表和执行数据分析，Derby 数据库需要一个 Universe。Universe 将随附 BI 平台部署通过 CMC 的以下位置予以提供：Universes > Monitoring TrendData Universes。

20.3.2 使用审核数据库的配置

如果要为监控数据使用审核数据库，需要执行额外配置步骤，如下所示：

- 如果 Derby 趋势数据库存在现有数据，需要将 Derby 数据库迁移到审核数据库，然后配置 BI 平台以便在审核数据库中记录监控信息。这些是用户需要遵守的高级步骤：有关详细信息，请参阅相关主题。
 - 1 迁移 Derby 数据库。
 - 2 配置 SBO 文件并添加别名。
 - 3 切换到审核数据库。
 - 4 重新启动承载监控服务的自适应处理服务器。
 - 5 在监控仪表盘上，确保一切都按预期工作。检查在数据库中创建的这些监控表：
 - MOT_MES_DETAILS
 - MOT_MES_METRICS
 - MOT_TREND_DATA
 - MOT_TREND_DETAILS
- 如果在趋势数据库中没有任何数据，即采用新安装，则无需迁移数据库；只需配置 BI 平台以便在审核数据库中记录监控信息。这些是用户需要遵守的高级步骤：有关详细信息，请参阅相关主题。
 - 1 检查审核数据库是否工作，以及审核是否正常运行。
 - 2 在 ADS 中创建监控表。
 - 3 配置 SBO 文件并添加别名。
 - 4 切换到审核数据库。

- 5 重新启动承载监控服务的自适应处理服务器。
- 6 在监控仪表盘上，确保一切都按预期工作。检查在数据库中创建的这些监控表：
 - MOT_MES_DETAILS
 - MOT_MES_METRICS
 - MOT_TREND_DATA
 - MOT_TREND_DETAILS

注意：

如果将监控数据记录到审核数据库并希望根据此数据制定报表，需要开发一个自定义 Universe。这些随 BI 平台提供的 Universe 仅用于嵌入式 Derby 数据库。

相关主题

- 第 630 页上的[“将 Derby 数据库迁移到审核数据库”](#)
- 第 633 页上的[“配置 SBO 文件”](#)
- 第 634 页上的[“在 SBO 文件中添加别名”](#)
- 第 635 页上的[“切换到审核数据库”](#)
- 第 631 页上的[“在 ADS 中创建监控表”](#)

20.3.2.1 将 Derby 数据库迁移到审核数据库

如果希望将审核数据库用于监控数据，并且 Derby 趋势数据库中存在现有数据，则需要将 Derby 数据库迁移到审核数据库。

开始迁移数据前，请检查这些先决条件：

- 审核数据库有效，并且审核正常运行。
- 您已具有足够的权限，并且在目标数据库中具有数据库客户端应用程序，可以创建新表并导入 CSV 转储文件等。
- 审核数据库支持逗号分隔值（CSV）文件的导入。

按下列步骤执行数据库迁移：

- 1 第 631 页上的[“备份 Derby 数据库”](#)
- 2 第 631 页上的[“将数据导出到 CSV 文件”](#)
- 3 第 631 页上的[“在 ADS 中创建监控表”](#)
- 4 第 632 页上的[“将内容恢复到目标数据库”](#)

注意：

在群集方案中，用户应为所有监控实例使用相同的 Derby 数据库实例。如果用户在群集方案中具备多个 Derby 数据库实例，则用户应只从一个 Derby 实例导入数据。从多个 Derby 实例导入数据会导致数据不一致，因此不建议如此操作。

20.3.2.1.1 备份 Derby 数据库

- 1 在 CMC 主页的“管理”区域中，单击“应用程序”。
 - 2 双击“监控应用程序”打开属性页面。
 - 3 在“趋势数据库设置”区域中，输入要将 Derby 趋势数据库备份到的文件位置，然后单击“保存”。
 - 4 在“运行数据库备份任务”旁边，单击“立即”。
- 如果数据库备份成功，将显示一个确认消息。此外，检查针对备份位置输入的文件夹位置，并检查备份文件是否已放置在那里。

20.3.2.1.2 将数据导出到 CSV 文件

本节说明如何生成迁移所需的 CSV 转储文件。CSV 文件包含嵌入式 Derby 数据库数据内容的逗号分隔值。

- 1 在 CMC 主页的“管理”区域中，单击“应用程序”。
- 2 双击“监控应用程序”打开属性页面。
- 3 在“趋势数据库设置”区域的“将嵌入式数据库中的数据导出为 CSV 文件”旁边，单击“导出”。

以下四个 CSV 文件将在默认趋势数据库位置中生成，即 <BOE 安装目录>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB:

- Mot_Mes_Details.csv
- Mot_Trend_Data.csv
- Mot_Trend_Details.csv
- Mot_Mes_Metrics.csv

20.3.2.1.3 在 ADS 中创建监控表

按下列步骤准备目标审核数据库：

- 1 安装 BI 平台之后，在<安装目录>\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Data\TrendingDB 位置可找到有关所有支持的 CMS 审核数据库的 DDL。从中可以找到 7 个具有相应数据库名称的不同（.sql 扩展名）文件。例如，针对 Oracle 的Oracle.sql，针对 Sybase ASE 数据库的 Sybase ASE.sql 等。
- 2 现在，转到目标数据库（此处的目标数据库指已配置 CMS 审核的数据库）并运行 .sql 文件。系统已创建以下四个监控表：MOT_TREND_DETAILS、MOT_TREND_DATA、MOT_MES_DETAILS 和 MOT_MES_METRICS。所需索引也会随表一起创建。

如果所有表均使用 .sql 文件中提及的正确数据类型创建，则系统将创建监控应用程序所需的数据库计划。

20.3.2.1.4 将内容恢复到目标数据库

若要将内容恢复至目标数据库，则需执行以下步骤：

- 1 启用“身份插入”。

监控表包含大量“身份”列。这些列的值是自动生成的。部分数据库（例如 MS SQL Server 和 Sybase ASE）不允许向这些列中显式插入值。但在数据迁移过程中，即使是标识列的值也需要迁移。因此，用户必须通过使用以下 SQL 命令启用这些值的显式插入：SET IDENTITY_INSERT <表名称> ON。

- 2 将 CSV 转储文件导入目标表。

数据库客户端提供的所有软件都支持用户通过使用菜单选项或命令将数据从 CSV 导入到表中。用户需要使用此选项将数据从 CSV 文件导入到对应的表中。将数据文件按以下顺序导入新表：

- a MOT_TREND_DETAILS
- b MOT_TREND_DATA
- c MOT_MES_DETAILS
- d MOT_MES_METRICS

- 3 禁用“身份插入”。

完成数据导入后，用户需要使用以下 SQL 命令禁用该表的标识插入：SET IDENTITY_INSERT <表名称> OFF。

导入数据之后，用户必须禁用表中的“身份插入”，才能在下一个表中启用“身份插入”。这是因为“身份插入”操作仅可在一个表中启用一次。

注意：

启用或禁用“身份插入”仅适用于 MS SQL Server 和 Sybase ASE。对于 Oracle、MaxDb、DB2、MySQL 或 SQL Anywhere 等其他数据库，不要求执行此操作。您可以直接将数据导入至表中。

20.3.2.2 配置 SBO 文件

在内部，监控应用程序使用连接服务器库，连接服务器需要 SBO 配置以建立与数据库驱动程序的连接。需要在 SBO 文件中指定数据库驱动程序及其位置以建立此连接。

示例：

- 如果在 CMC “审核” 页面中配置的“连接名称”字段是一个 ODBC DSN，则应在以下文件中配置驱动程序：<安装目录>\dataAccess\connectionServer\odbc<数据库类型>.sbo。
- 如果用于审核的数据库是 SAP HANA，则需要在其中配置驱动程序的文件为：<安装目录>\dataAccess\connectionServer\odbc\newdb.sbo。
- 如果用于审核的数据库是 MS SQL Server，则需要在其中配置驱动程序的文件为：<安装目录>\dataAccess\connectionServer\odbc\sqlsrv.sbo。
- 如果用于审核的数据库是 DB2，则需要在其中配置驱动程序的文件为：<安装目录>\dataAccess\connectionServer\odbc\db2iseries.sbo。
- 如果在 CMC “审核” 页面中配置的“连接名称”字段为 <主机名><端口号><数据库名>，则应在以下文件中配置驱动程序 JAR：dataAccess\connectionServer\jdbc<数据库类型>.sbo。

配置 SBO 文件

通常，SBO 文件中已经配置了 ODBC 库，只需添加别名即可。如果未配置，请按照以下示例在 SBO 文件中执行配置：

示例：

- 如果用于审核的数据库版本是 SAP HANA，则 SBO 中的配置应为：

```
<DataBase Active="Yes" Name="SAP HANA database 1.0" Platform="MSWindows">
  <Aliases>
    <Alias>SAP High-Performance Analytic Appliance (SAP HANA) 1.0</Alias>
    <Alias>Hana</Alias>
  </Aliases>
  <Libraries>
    <Library Platform="MSWindows">dbd_wnewdb</Library>
    <Library Platform="MSWindows">dbd_newdb</Library>
  </Libraries>
  <Parameter Name="Driver Name">HDBODBC</Parameter>
</DataBase>
```

- 如果用于审核的数据库版本是 MS SQL Server 2008，则 SBO 中的配置应为：

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
  <Libraries>
    <Library>dbd_wmssql</Library>
    <Library>dbd_mssql</Library>
  </Libraries>
  <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
  <Parameter Name="CharSet Table" Platform="Unix">datadirect</Parameter>
  <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
  <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
</DataBase>
```

- 如果用于审核的数据库版本是 DB2，则 SBO 中的配置应为：

```
<DataBase Active="Yes" Name="DB2 UDB for iSeries v5">
<!-- You can add an alias here if you are using some connections that are defined with an older database engine -->
<Alias>DB2/400 V5</Alias>
<Alias>DB2/400 V4</Alias>
<Alias>DB2 for iSeries v4</Alias>
<Alias>DB2</Alias>
</Aliases>
```

- 如果用于审核的数据库版本是 MySQL 5，则 SBO 应包含此项：

```
<DataBase Active="Yes" Name="MySQL 5">
  <JDBCdriver>
    <ClassPath>
      <Path>C:\mysqljdbcdriver.jar</Path>
    </ClassPath>
    <Parameter Name="JDBC Class">com.mysql.jdbc.Driver</Parameter>
    <Parameter Name="URL Format">jdbc:mysql://$DATASOURCE$/$DATABASE$</Parameter>
  </JDBCdriver>
  <Parameter Name="Driver Capabilities">Query,Procedures</Parameter>
  <Parameter Name="Force Execute">Always</Parameter>
  <Parameter Name="Extensions">mysql5,mysql,jdbc</Parameter>
</DataBase>
```

有关在 SBO 文件中配置驱动程序的更多信息，请参阅《数据访问指南》。

20.3.2.3 在 SBO 文件中添加别名

此外，在配置驱动程序时，用户还需要在 SBO 中用于审核的数据库版本下添加别名。下表列出了针对指定数据库应使用的别名。

数据库名称	要在 SBO 中使用的别名
SAP HANA	HANA
Microsoft SQL Server	MS SQL Server
My SQL	MySQL
SAP Max DB	MaxDB
IBM DB2	DB2
Sybase SQL Anywhere	Sybase SQL Anywhere
Sybase Adaptive Server Enterprise	Sybase Adaptive Server Enterprise
Oracle	Oracle

当监控应用程序在 SBO 中搜索这些名称时，应使用指定名称。

示例：

如果用于审核的数据库是 MS SQL Server 2008，则需要按如下所示向 SBO 中添加别名：

```
<DataBase Active="Yes" Name="MS SQL Server 2008">
  <Aliases>
    <Alias>MS SQL Server</Alias>
  </Aliases>
  <Libraries>
    <Library>dbd_wmssql</Library>
    <Library>dbd_mssql</Library>
  </Libraries>
  <Parameter Name="Extensions">sqlsrv2008,sqlsrv,odbc</Parameter>
  <Parameter Name="CharSet Table" Platform="Unix">datadirect</Parameter>
  <Parameter Name="Driver Name">SQL (Server|Native Client)</Parameter>
  <Parameter Name="SSO Available" Platform="MSWindows">True</Parameter>
</DataBase>
```

20.3.2.4 切换到审核数据库

切换数据库，以便监控趋势信息存储在审核数据库中。

- 1 在 CMC 主页的“管理”区域中，单击“应用程序”。
- 2 双击“监控应用程序”打开属性页面。
- 3 在“趋势数据库设置”区域中，选择“使用审核数据库”。

20.4 配置属性

本部分描述监控应用程序属性，以及用户可如何编辑这些属性。

要查看监控应用程序的配置属性：

- 1 转到 CMC 的“应用程序”选项卡。
- 2 右击“监控应用程序”并选择“属性”。将出现“监控应用程序属性”窗口。配置属性的说明见下表：

节	字段	说明
	启用监控应用程序	选择此选项可启用监控功能。如果取消选择此选项，除探测器外的所有监控功能都将禁用。探测器趋势也将被禁用。
	默认 JMX 代理端点 URL (IIOP)	这包含使用 IIOP 协议的默认 JMX 代理端点 URL。如果在启用监控后重新启动服务器，则自动生成该 URL。这是用于监控服务的默认协议。此为只读字段。
RMI	启用 JMX RMI 协议	默认情况下，将禁用此选项。如果启用此选项，必须提供 RMI 端口号。此端口将同时用于 RMI 注册表项和 RMI 连接器端口。此端口必须可供服务使用，否则将无法启动服务。提供 RMI 端口号后，请重新启动服务器。重新启动服务器后，将生成 RMI JMX 代理端点 URL。此只读属性包含使用 RMI 协议的 JMX 代理端点 URL。使用此 URL 可从其他客户端连接到监控。
主机量度	启用主机量度	<p>默认情况下，将禁用此选项。如果启用此选项，则必须提供 SAPOSCOL 二进制文件的安装路径。</p> <p>要启用主机量度，需安装 SAPOSCOL。有关如何安装 SAPOSCOL 的更多信息，请参阅第 638 页上的 “安装 SAPOSCOL”。</p>

节	字段	说明
趋势数据库设置	使用审核数据库	<p>选择此选项，在 CMS 审核数据库中存储量度的趋势历史记录。</p> <p>注意： CMS 审核数据库必须已配置为支持此功能。</p>
	使用嵌入式数据库	选择此选项，在监控应用程序附带的嵌入式数据库中存储量度/监测器趋势历史记录。
	数据库大小超过此值（MB）时删除早期数据	当数据库超过该指定大小后，将清除趋势数据库的数据。会为此数据库创建大小为 30% 的缓冲区。例如，如果用户将此属性设置为 100 MB，则在系统检查数据库增大到超过 100 MB 时，将清理数据，直到数据库为 70 MB 为止。
	每天运行数据库清理任务的时间	数据库清除任务在指定时间启动。当数据库超过指定的最大规模时，将对数据库进行清理。
	备份趋势数据库间隔	指定趋势数据库每次备份之间的小时数。设置此值后，系统启动时或者每次重新启动 APS 时以及在每个指定间隔内都会备份。
	趋势数据库备份目录	默认情况下不指定位置。也可以指定位置；但要提供绝对路径而非相对路径。如果是共享位置，则应提供访问该共享位置的权限。
	运行数据库备份任务	单击此选项后将启动数据库备份任务。在选择此选项之前指定数据库备份目录位置。
	将嵌入式数据库中的数据导出为 CSV 文件	单击“导出”按钮，将数据库导出为以逗号为分隔值的文件。
	趋势数据库位置	默认情况下，趋势数据库位置为安装目录\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0/Data/TrendingDB。还可以指定其他位置；但是，请提供绝对路径而非相对路径。在群集环境中，该位置可以是共享位置，并且应提供访问此位置的权限。

节	字段	说明
其他设置	量度刷新时间间隔（秒）	<p>可指定的最小时间间隔为 15 秒。此时间间隔管理以下事项：</p> <ul style="list-style-type: none"> 监测器的预订计算：警告和危险规则使用指定时间间隔进行连续计算。 计算监测器状态：如果监测器的“事件”设置选择了以下选项，则以指定时间间隔持续计算监测器状态：每次警告或危险规则求得的值为真时更改监测器状态。 趋势期间：使用指定时间间隔持续记录图表的历史模式。
	监控 UI 自动刷新时间间隔（秒）	<p>此时间间隔将在监控用户界面（包括仪表盘、监测器列表和探测器）中用于自动刷新。最短时间间隔为 15 秒。自动刷新不会影响图形中实时模式下的持续时间，默认情况下该持续时间设置为 15 秒。</p>
	警报提醒频率（天）	指定生成警报提醒前的天数。

- 。 3 单击“保存”。

注意：

更改除启用和禁用监控应用程序之外的任何这些属性时，必须重新启动承载监控服务的自适应处理服务器。

安装 SAPOSCOL

执行以下步骤以安装 SAPOSCOL：

- 1 从 SAP Marketplace (<http://service.sap.com>) 上下载 SAPHOSTAGENT710_XX.SAR。
- 2 通过执行 `SAPCAR.EXE -xvf SAPHOSTAGENT710_XX.SAR` 命令抽取 SAPHOSTAGENT710_XX.SAR。
- 3 通过执行 `saphostexec.exe -install` 命令安装 saphostexec。saphostexec 作为服务安装之后，将会启动 SAPOSCOL。
- 4 通过执行 `saposcol -s` 命令检查 SAPOSCOL 状态。

20.4.1 JMX 端点 URL

监控应用程序提供了 JMX 端点 URL，其他客户端可通过该 URL 使用 JMX 远程 API 进行连接。默认情况下，JMX 连接性是通过 IIOP（Internet 对象请求代理间协议）或 CORBA（公用对象请求代理体系结构）传输提供的。此连接 URL 显示在监控应用程序的属性页面中。由于能够通过 IIOP 连接，因此不需要担心防火墙和必须暴露端口的问题。默认情况下，CORBA 端口是可用的。在 JMX 客户端上需要有下表中列出的 Jar 文件才能够连接到这些 JMX 客户端：

Jar 文件
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

另一个选项是通过默认 RMI 端口进行连接。有关如何通过 RMI 端口进行连接的更多信息，请参见第 635 页上的 [“配置属性”](#)。

20.4.2 监控探测器的 HTTPS 身份验证

支持监控探测器的 HTTPS 服务器身份验证，并且在使用前需要以下配置：

- 。 1 将服务器证书导入客户端的信任库。这有助于客户端（探测器）检查服务器的身份：运行此命令：`<安装根目录>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\lib> keytool -import -alias ca -keystore "<安装根目录>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\lib\security\cacerts" -file ca.cer`

ca.cer 是服务器的自签署证书，或生成服务器证书的证书机构（通常是内部 CA）的证书。如果通过广为人知的 CA 生成服务器的证书，则无需导入它，并可跳过此步。这是因为服务器的证书将由该 CA 检查，默认情况下其公钥已经在信任库中。
- 。 2 将 BI 启动板探测器设置中的“URL 基址”更改为 `https://<URL>/BOE/BI`，其中 <URL> 指证书中使用的主机名称。

不支持用于监控探测器的 HTTPS 客户端身份验证。

20.4.3 探测器的密码加密

使用探测器时，要确保加密密码，通过命令行创建探测器时您必须将 `true` 参数添加到每个监控探测器的密码参数。有关更多信息和语法示例，请参阅 CMC 帮助中的“通过命令行管理探测器”这一主题。

20.5 与其他应用程序集成

IBM Tivoli Monitoring 等企业解决方案可以作为通过 JMX 端点 URL 连接的 JMX 客户端集成监控应用程序。在集成后，可以从客户端用户界面查看 SAP BusinessObjects 量度。

20.5.1 将监控应用程序与 IBM Tivoli 集成

要将监控应用程序与 IBM Tivoli 集成，需要创建、安装并配置 IBM Tivoli Monitoring 代理。请执行以下步骤创建 IBM Tivoli Monitoring 代理：

- 。 1 安装 IBM Tivoli Monitoring Agent Builder 6.2.1 版软件。

- 。 2 创建新代理。有关如何创建新代理的信息，请参阅 IBM Tivoli Monitoring 代理用户指南。
- 。 3 在“Defining data monitoring types”（定义数据监控类型）步骤中，选择“Monitoring Data Categories”（监控数据类别）区域中的“Data from a server”（来自服务器的数据），然后选择“数据源”区域中的“JMX”。
- 。 4 单击“Next”（下一步）。
- 。 5 在“JMX Information”（JMX 信息）窗口中，单击“Browse”（浏览）以查看 MBean 服务器上的所有 JMX MBean。

注意：

如果是第一次运行浏览器，则需要添加新连接。

- 。 6 在“Java Management Extensions (JMX) Browser”（Java 管理扩展 (JMX) 浏览器）窗口中，单击“Connection Name”（连接名称）旁边的“+”，以添加新连接。
- 。 7 在“MBean Server Connection Wizard”（MBean 服务器连接向导）窗口中，选择“Standard JMX Connections (JSR-160)”（标准 JMX 连接 (JSR-160)）。
- 。 8 在“Connection Properties”（连接属性）窗口中，提供以下信息：

字段	说明
连接名称	符合 JSR-160 的服务器
用户 ID	用于登录 BI 平台的用户名
密码	用于登录 BI 平台的密码
服务 URL	提供 JMX 端点 URL

- 。 9 单击“Finish”（完成）。
- 。01 在“MBean Key Properties”（MBean 键属性）区域，选择“Domain”（域）和“Type”（类型）。

所有 MBean 将出现在下面的文本字段中。

- 。11 选择域为“Servers”（服务器）的所有 MBean，每次选择一个 MBean，以便列出属性。如果可能有多个相同类型的 MBean，请选择一个键属性。例如，如果服务器有两个实例正在运行，则每个实例的 PID 均可以是键属性。
- 。21 选择一个服务器，然后在“JMX Agent-Wide Options”（JMX 代理方面的选项）窗口中选择 JMX 属性组的选项。
- 。31 在“Data Source Definition”（数据源定义）窗口中，选择用户添加的代理，然后单击“Add to Selected”（添加到选定项）。用户将转到代理创建周期的开始，用户需要重复以上步骤添加其他要监视的服务器。
- 。41 创建代理后，需要安装代理。有关如何安装代理的更多信息，请参阅 IBM Tivoli Monitoring 代理用户指南（图 154 后面的内容）。本部分给出关于在本地安装代理以及关于创建代理可安装解决方案的信息。

注意：

如果使用 Agent Builder 创建 BI 平台的代理，则必须在同一系统上安装 BI 平台。然而，如果使用某个已创建代理的安装程序文件安装该代理，则不需要安装 BI 平台监控；原因是配置时可以提供带有 JMX 端点的任何系统的详细信息。

执行以下步骤配置已安装的代理：

- 。 1 在 TEMS 模式中打开“Manage Tivoli Enterprise Monitoring Services”（管理 Tivoli Enterprise 监控服务）。将看到代理已安装。
- 。 2 右击代理模板，并选择“Configure using defaults”（使用默认值配置）。
- 。 3 选择实例名称。

可通过使用两种不同协议配置代理：RMI 和 BOEIIOP。

要使用 RMI 协议：

- 单击“Next”（下一步）。不要对 Java 参数进行任何更改。
- 提供 JMX 凭据的值，如用户 ID、密码和服务 URL。有关更多信息，请参阅“Related Topics”（相关主题）中的“Configuration Properties”（配置属性）。
- 单击“OK”（确定）。

要使用 BOEIIOP 协议：

- 将 bcm.jar 和 cryptojFIPS.jar 文件从 %安装目录%\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\java\lib 复制到系统中的某个文件夹内。
- 将下表中列出的 jar 文件复制到其他文件夹。
- 在 Java 参数中，将 JVM 参数设置为 Djmx.remote.protocol.provider.pkgs = com.businessobjects.sdk.monitoring 和 -Djmx.boeiiop.bcm.dir=< 文件夹位置，该位置为已复制了 bcm.jar 和 cryptojFIPS.jar 文件的位置。
- 选择“Next”（下一步）。
- 提供 JMX 凭据的值，如用户 ID、密码和服务 URL。有关更多信息，请参阅“Related Topics”（相关主题）中的“Configuration Properties”（配置属性）。
- 将<“Jar Directories”>（Jar 目录）值设置为复制表中提供的 Jar 文件列表的文件夹。
- 单击“OK”（确定）。

Jar 文件
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

Jar 文件
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 在“Manage Tivoli Enterprise Monitoring Services”（管理 Tivoli Enterprise 监控服务）窗口中，右击代理并选择“Start”（开始）。
- 。 5 打开 IBM Tivoli Enterprise Portal Desktop/Browser Client。在“Navigator”（浏览器）窗口中出现一个按钮。
- 。 6 单击“Navigator”（浏览器）按钮。
代理即添加到“Navigator”（浏览器）中。

相关主题

- 第 635 页上的[“配置属性”](#)

20.5.2 将监控应用程序与 SAP Solution Manager 集成

要将监控应用程序与 SAP Solution Manager 集成，需要在用户系统上安装 [Wily Introscope](#)，并使其运行。必须将 SAP Solution Manager 配置为用于 Introscope 工作站。在 BI 平台安装期间执行下列步骤：

- 。 1 在“配置与 Introscope Enterprise Manager 的连接”步骤中，提供主机名和端口的详细信息。在安装 BI 平台时，Introscope 代理将安装在 C:\Program Files (x86)\SAP Business Objects\SAP BusinessObjects Enterprise XI 4.0\java\Wiley。
- 。 2 启动 Introscope 工作站并单击“New Investigator”（新建调查者）。可以在配置的代理程序 JMX 节中查看 SAP BusinessObjects 服务器量度和探测器虚拟量度。

注意：

可以配置 Introscope (IS) 代理，方法是依次选择“CMC” > “服务器” > “服务器节点” > “点位符”。还可以在此处为 IS 代理配置 IS Enterprise Manager 主机和端口，以便与监控应用程序进行通信。有关更多信息，请参阅 CMC 帮助中的“管理服务器”。

对于 IS 中提供的 JMX 度量，请确保自适应处理服务器实例上同时提供了 IS 代理服务 and 监控服务。

如果启用 IS 检测，则会自动启用代码检测。

20.6 用于监控服务器的群集支持

监控应用程序支持群集，提供故障切换功能。

有了群集支持，在任何给定时间内都将只有一个服务处于活动状态，而所有其他服务都将处于被动状态。如果群集环境中有两个监控服务 s1 和 s2，则只有一个可用。s1 和 s2 都尝试变为主动，但其中一个成功时，另一个服务将变为不活动或被动。

被动服务定期（每分钟）检查主动服务的可用性。如果活动服务不可用，被动服务会立即尝试成为活动服务。

注意：

建议在单独的自适应处理服务器（APS）实例上承载监控服务，以避免 APS 出现故障或性能低下。

20.7 疑难解答

本节将针对监控应用程序使用过程中可能出现的各种问题提供详细的分步解决方法。

20.7.1 仪表盘

CMC 页面上不显示监控链接

- 检查用户是否具有足够的访问权。
- 确保将用户添加到“监控用户”或“管理员”组，或属于这些组的任何其他组。

关键绩效指标（KPI）在监控仪表盘上不可见

- 选择“服务器属性” > “量度”，检查所需量度是否可见。
- 确保中央管理服务器按预期做出响应。

无法启动监控应用程序

下载并安装最新的 Flash Player。

20.7.2 警报

无法在“警报”页面上接收警报

- 检查是否选中警报应用程序属性中的“启用我的警报”选项。
- 确保具有足够的访问权限接收警报。
- 检查最近的警报在监控仪表盘上是否可见。

注意：

可以向设置的电子邮件 ID 发送 Crystal Reports 文档，以检测 SMTP 是否正常工作。

无法接收电子邮件通知

- 检查是否选中警报应用程序属性中的“启用电子邮件”选项。
- 检查接收电子邮件警报的电子邮件地址设置是否恰当。
- 检查 SMTP 服务器是否工作正常。
- 确保已启用自适应作业服务器实例。
- 检查自适应作业服务器实例目标中的 SMTP 设置。

20.7.3 监测器列表

无法接收监测器的历史数据

- 在监控应用程序“属性”页面上检查轮询时间间隔。
- 检查记录文件夹中的跟踪文件。

- 检查是否在 CMC “应用程序”页面上指定了“趋势数据库位置”。对于群集环境，确保用户具有访问共享位置的权限。有关更多信息，请参阅“相关主题”中的“配置属性”。
- 检查服务器和客户端的系统时间在特定时区内是否相同。

获取已同步的实时数据时发生错误

检查自适应处理服务器实例是否正在运行。

禁用“监测器列表”选项卡

- 检查监控服务是否正在运行。
- 检查错误消息的监控服务日志。
- 检查服务器及其量度在 jConsole 中是否可见。

相关主题

- 第 635 页上的[“配置属性”](#)

20.7.4 探测器

无法计划探测器

- 检查承载探测器计划服务的 AdaptiveJobServer 实例是否正在运行。
- 确保用于 Crystal Reports 和 Web Intelligence 文档的报表 CUID 是正确的。
- 确保用户具有管理权限或是管理员组的成员。
- 检查用户是否具有足够的权限打开、刷新、导出相应探测器中使用的 Crystal Reports 或 Web Intelligence 文档。

探测器计划状态为“挂起”

- 检查是否安装了探测器计划服务实例。
- 检查承载探测器计划服务的 AdaptiveJobServer 实例是否正在运行。

从数据库检索趋势数据时出错

检查自适应处理服务器实例是否正在运行。

probeRun.bat 运行失败

- 检查是否设置了 java_home。
- 检查是否在命令提示符中输入了正确的参数。

注意：

在命令提示符中输入 probeRun.bat - help，以检查是否所有参数都正确。

20.7.5 量度

未列出主机量度

- 确保 SAPOSCOL 正在运行。
- 确保在监控应用程序“属性”页面中选择了“启用主机量度”选项。
- 重新启动自适应处理服务器实例，使更改生效。
- 确保“SAPOSCOL 二进制文件的安装路径”正确。

检索 JMX 客户端时出错

检查自适应处理服务器实例是否正在运行。

“量度”页面上的 SAPOSCOL 量度值为零。

- 确保 SAPOSCOL 正在运行。
- 在安装了 SAPOSCOL 的主机上执行以下命令：
 - 1 `saposcol -s`，可检查状态
 - 2 `saposcol -m`，可获取 SAPOSCOL 所收集数据的快照

20.7.6 图形

图形显示实时模式和历史模式的不同时间。

确保服务器和客户端的系统时间在特定时区内相同。

对于群集方案而言，图形数据不显示在历史模式中

确保所有自适应处理服务器实例都指向相同的 Derby 数据库位置。

第 21 章 审核

21.1 概述

审核可用于保留服务器和应用程序上重大事件的记录，从而能够帮助用户了解正在访问的信息及其访问和更改的方式，以及正在执行这些操作的用户。这些信息被记录在“审核数据存储”（ADS）数据库中。将数据写入到 ADS 之后，即可按需设计自定义报表。可在 SAP Community Network 上查找示例 Universe 和报表<http://scn.sap.com/>。

对于本章而言，审核方是指负责记录或存储有关事件信息的系统，被审核方是指执行可审核事件的任何系统。在有些情况下，单个系统可以既是审核方也是被审核方。

审核工作原理

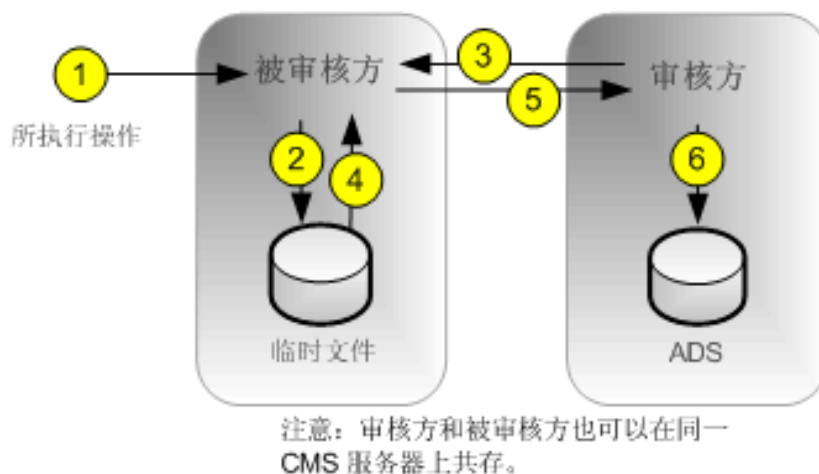
中央管理服务器（CMS）充当系统审核方，而每个触发可审核事件的服务器或应用程序充当被审核方。在触发审核事件时，被审核方将生成一个记录，并将其存储在本地临时文件中。CMS 定期与被审核方通信，以便请求这些记录并将数据写入 ADS。

CMS 还控制在不同计算机上发生的审核事件的同步。每个被审核方将为其记录的审核事件提供一个时间戳。为了确保不同服务器上的事件的时间戳保持一致，CMS 将定期向被审核方广播自己的系统时间。然后，被审核方会将此时间与他们的内部时钟进行比较。如果存在差异，被审核方将为后续的审核事件校准它们记录的时间。

根据被审核方的类型，系统将使用下列其中一种工作流来记录事件。

服务器审核

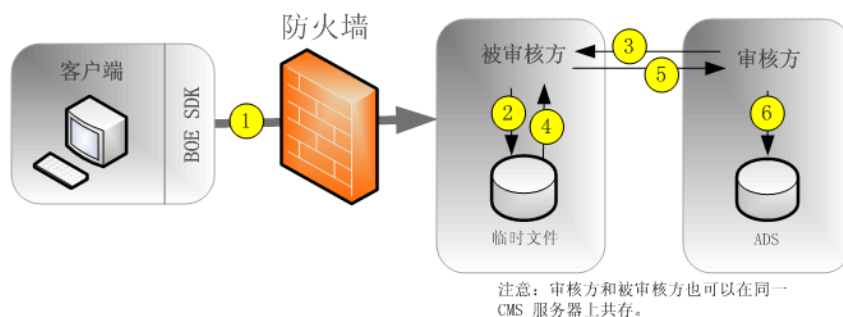
对于服务器生成的事件，CMS 可同时充当“被审核方”和“审核方”。



- 1 服务器执行一个可审核事件。
- 2 被审核方将事件写入一个临时文件中。在执行第 3 步之前，可重复执行第 1 和第 2 步。
- 3 审核方定期轮询被审核方，并请求批量审核事件。
- 4 被审核方从临时文件中获取事件。
- 5 被审核方将事件传给审核方。
- 6 审核方将事件写入 ADS 并发出信号通知被审核方从临时文件中删除事件。

通过 CORBA 进行的客户端连接的客户端登录审核

其中包括如 SAP BusinessObjects Web Intelligence 等应用程序。



- 1 该客户端连接至作为被审核方的 CMS。客户端提供其 IP 地址和计算机名称，被审核方随后将对该地址和计算机名称进行验证。

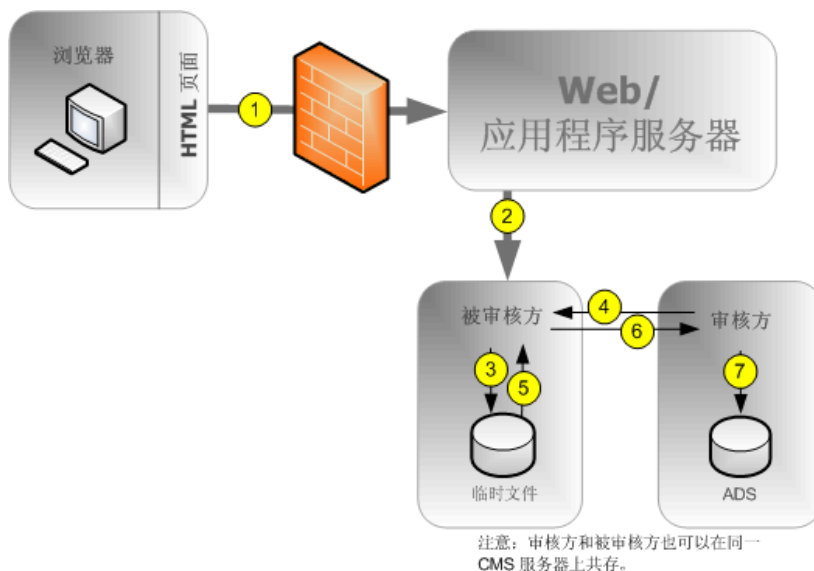
注意：

应在客户端与 CMS 之间的防火墙中打开一个端口。有关防火墙的更多详细信息，请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》中的安全性章节。

- 2 被审核方将事件写入一个临时文件中。在执行第 3 步之前，可重复执行第 1 和第 2 步。
- 3 审核方定期轮询被审核方，并请求批量审核事件。
- 4 被审核方从临时文件中获取事件。
- 5 被审核方将事件传给审核方。
- 6 审核方将事件写入 ADS 并发出信号通知被审核方从临时文件中删除事件。

通过 HTTP 连接的客户端的客户端登录审核

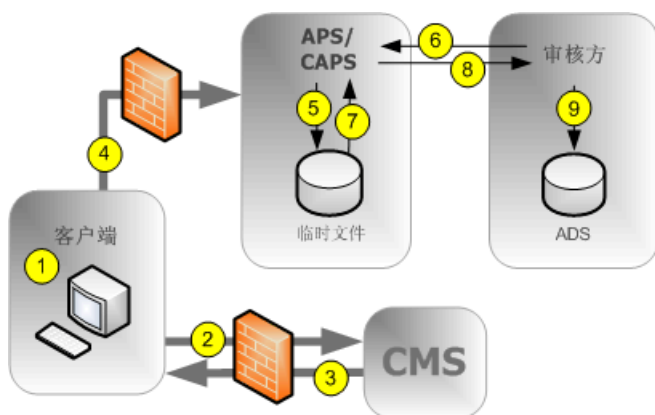
其中包括在线应用程序，如 BI 启动板、中央管理控制台、SAP BusinessObjects Web Intelligence 等。



- 1 浏览器连接至 Web 应用程序服务器，登录数据被提交至 Web 应用程序服务器。
- 2 BI 平台 SDK 将登录请求随浏览器计算机的 IP 地址和名称一起提交到被审核方（CMS）。
- 3 被审核方将事件写入一个临时文件中。在执行第 4 步之前，可重复执行第 1 到第 3 步。
- 4 审核方定期轮询被审核方，并请求批量审核事件。
- 5 被审核方从临时文件中获取事件。
- 6 被审核方将事件发送给审核方。
- 7 审核方将事件写入 ADS 并发出信号通知被审核方从临时文件中删除事件。

通过 CORBA 连接的客户端的非登录审核

当通过 CORBA 连接时，此 workflow 适用于审核 SAP BusinessObjects Web Intelligence 事件。



- 1 用户执行可能会被审核的操作。
- 2 客户端与 CMS 联系，确认是否已配置审核该操作。

- 3 如果该操作被设置为需要审核，则 CMS 会将该信息通知客户端。
- 4 客户端将事件信息发送到客户端审核代理服务（CAPS），此服务在自适应处理服务器中承载。

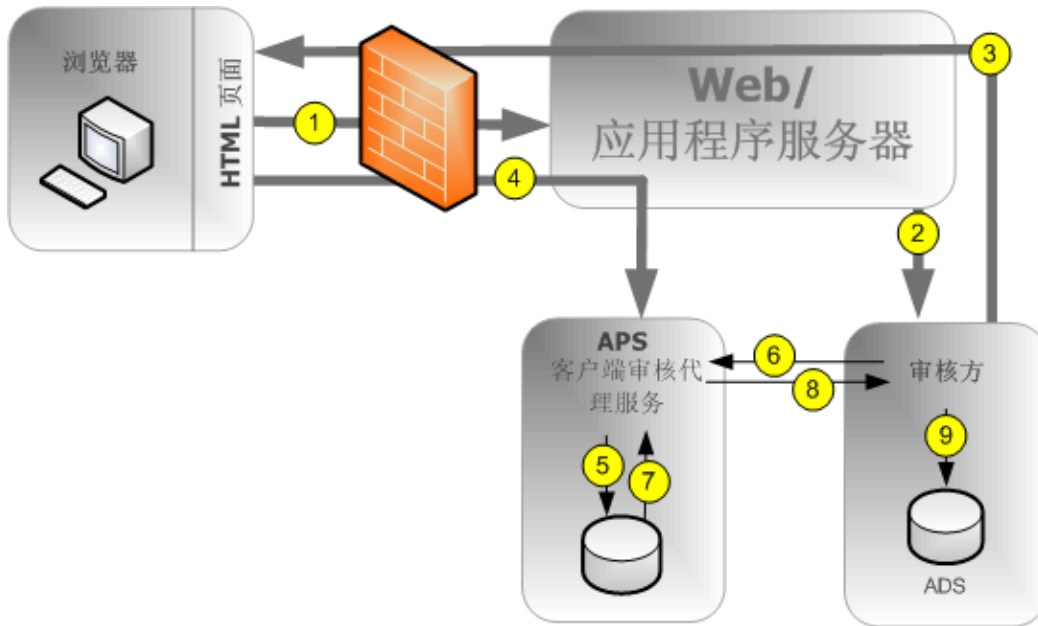
注意：

应在每个客户端和承载 CAPS 的每个自适应处理服务器之间以及每个客户端和 CMS 之间打开防火墙中的一个端口。有关防火墙的更多详细信息，请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》中的安全性章节。

- 5 CAPS 将事件写入一个临时文件中。在执行第 6 步之前，可重复执行第 1 到第 5 步。
- 6 审核方定期轮询 CAPS，并请求批量审核事件。
- 7 CAPS 从临时文件中获取事件。
- 8 CAPS 将事件信息发送到审核方。
- 9 审核方将事件写入 ADS 并发出信号通知 CAPS 从临时文件中删除事件。

通过 HTTP 连接的客户端的非登录审核

当通过 HTTP 连接时，此工作流程适用于审核 SAP BusinessObjects Web Intelligence 事件（登录事件除外）。



注意：审核方和被审核方也可以在同一 CMS 服务器上共存。

- 1 用户引发一个可能可审核的事件。客户端应用程序与 Web 应用程序服务器联系。
- 2 Web 应用程序查看该事件是否被配置为需要审核。

注意：

虽然图中显示与审核方 CMS 联系，但与群集中的任何 CMS 联系均可获取此信息。

- 3 CMS 将审核配置信息返回给 Web 应用程序服务器，后者将此信息传回给客户端应用程序。
- 4 如果事件被配置为需要审核，则客户端将事件信息发送给 Web 应用程序服务器，后者将此信息传送到自适应处理服务器（APS）中承载的客户端审核代理服务（CAPS）。
- 5 CAPS 将事件写入一个临时文件中。在执行第 6 步之前，可重复执行第 1 到第 5 步。
- 6 审核方定期轮询 CAPS，并请求批量审核事件。

- 7 CAPS 从临时文件中获取事件。
- 8 CAPS 将事件信息发送到审核方。
- 9 审核方将事件写入 ADS 并发出信号通知 CAPS 从临时文件中删除事件。

支持审核的客户端

下列客户端应用程序支持审核：

- 中央管理控制台（CMC）
- BI 启动板
- OpenDocument
- Analysis
- Live Office Web 服务提供者
- Web Intelligence 胖客户端

注意：

必须至少有一个 CAPS 实例正在运行，这样才能从上面列出的客户端收集审核事件。

上面未列出的客户端不会直接生成事件，但可以审核服务器因运行客户端应用程序而执行的某些操作。

审核一致性

大多数情况下，如果正确安装审核、正确配置审核、审核安全可靠，并且使用了所有客户端应用程序的正确版本，审核将恰当一致地记录所有指明的系统事件。但是，务必要记住，某些系统和环境情况可能会对审核产生反面影响。

在事件发生后，始终会有一段延迟，然后事件才会最终传送到 ADS。遇到 CMS 或审核数据库不可用或者网络连接失败等情况还可能增加延迟。

系统管理员应尽力避免以下任何情况，这些情况可能会导致审核记录不完整：

- 存储审核数据的磁盘达到最大容量。应确保有大量的磁盘空间可用于审核数据库和被审核方临时文件。
- 在被审核方服务器传送所有审核事件之前从网络中错误地移除了该服务器。应确保从网络中移除服务器时留出足够的时间将审核事件传输到审核数据库。
- 删除或修改被审核方临时文件。
- 硬件或磁盘错误。
- 被审核方或审核方主机计算机出现物理损坏。

还有一些情况可能会使审核事件无法到达 CMS 审核方。这些情况可能包括：

- 用户使用旧客户端版本。
- 防火墙配置不恰当可能阻止审核信息的传送。

注意：

- 由客户端应用程序生成的事件包含从客户端方提交的信息，即系统信任区域以外的信息。因此，在某些情况下，该信息可能不如系统服务器所记录的信息可靠。
- 如果要部署中删除某个服务器，则应先禁用该服务器，但让其继续运行并连接到网络，直至临时文件中的所有事件都有机会传输至审核数据库中。服务器的“队列中的当前审核事件数”量度将显示等待传送的审核事件的数量。当此量度达到零时，可停止服务器。临时文件的位置由该节点的 %DefaultAuditingDir% 占位符定义。有关占位符的更多详细信息，请参阅“服务器管理”章节。

- 如果希望使用客户端审核，则建议为客户端审核代理服务创建专用的自适应处理服务器。这样可以确保实现最佳的系统性能。为增加系统的容错率，您可能还会考虑在多个 APS 上运行 CAPS。

相关链接

第 966 页上的 [“服务器和节点占位符”](#)

21.2 CMC 审核页

CMC 中的“审核”页具有以下区域：

- 状态摘要
- 设置事件
- 设置事件详细信息
- 配置

21.2.1 审核状态

审核“状态摘要”显示一组量度，帮助优化审核配置并提醒用户可能影响审核数据完整性的任何问题。状态汇总位于中央管理控制台中“审核”页面的顶部。

在如下情境中，汇总也显示警告：

- 与审核数据存储（ADS）数据库的连接不可用。
- 没有正在运行或已启用的客户端审核代理服务，这将无法收集客户端事件。
- 被审核方具有无法检索的事件（将标识受影响的服务器）。这通常表明某个服务器未正常停止或关闭，并且仍具有临时文件中的事件。

注意：

状态摘要量度标记为绿色、黄色或红色，以指示审核功能的正常状态。

审核状态量度

量度	详细信息
ADS 上次更新时间	审核方 CMS 上次结束轮询被审核方的审核事件的日期和时间。
审核线索利用率	<p>审核方 CMS 从被审核方收集数据所用的轮询周期百分比，剩余部分为两次轮询之间剩余的时间。</p> <p>如果此值达到 100%，该数字将显示为黄色，表明在下一轮询应该开始时审核方仍在从被审核方收集数据。这可能导致事件延迟到达 ADS。</p> <p>如果这种情况频繁发生或持续存在，则建议更新部署以便允许 ADS 数据库以更高速率接收数据（例如，更快的网络连接或功能更强大的数据库硬件），或者减少系统跟踪的审核事件数。</p>
上次轮询周期持续时间	<p>上一轮询周期的持续时间（以秒为单位）。这表明上一轮询周期内事件数据到达 ADS 的最长延迟时间。</p> <ul style="list-style-type: none"> 如果在 20 分钟（1200 秒）以内，该数字将显示为绿色背景。 如果介于 20 分钟与 2 小时（7200 秒）之间，它将显示为黄色背景。 如果超过 2 小时，它将显示为红色背景。 <p>如果这种情况持续不断，且您觉得延迟时间太长，则建议更新部署以便允许 ADS 数据库以更高速率接收数据（例如，更快的网络连接或功能更强大的数据库硬件），或者减少系统跟踪的审核事件数。</p>
CMS 审核方	当前充当审核方的 CMS 的名称。
ADS 数据库连接名称	审核方 CMS 当前用于连接到审核数据存储（ADS）的数据库连接的名称。对于 SQL Anywhere、SQL Server 和 SAP HANA 服务器，它将显示 ODBC 连接的名称。对于其他数据库类型，它将显示为服务器名称后接数据库名称和连接端口。
ADS 数据库用户名	用户名和审核方 CMS 将用于登录 ADS 数据库。

21.2.2 配置审核事件

CMC 的“审核”页面可用于激活审核和选择整个系统内将要审核的事件。

如果对某些事件或事件详细信息不感兴趣，则可不选择这些内容以提高系统性能。

注意：

如果在安装 BI 平台时选择不配置 ADS 连接，则需要在配置审核事件之前设置与数据库的连接。若未连接，则仍将收集事件，但连接之后，这些事件将写入 ADS。要关闭审核，应将级别设置为关闭。请参见“审核数据存储配置设置”。

21.2.2.1 配置审核事件

- 1 在中央管理控制台中，选择“审核”选项卡。
将出现“审核”页面。
- 2 将“设置事件”滑块设置为所需级别。
下表显示了滑块的不同设置及每个级别捕获的事件。

审核级别	捕获的事件
禁用	无
最小	<ul style="list-style-type: none"> • 登录 • 注销 • 权限修改 • 自定义访问级别已修改 • 审核修改
默认	“最小”事件，加上： <ul style="list-style-type: none"> • 查看 • 刷新 • 提示 • 创建 • 删除 • 修改 • 保存 • 搜索 • 编辑 • 运行 • 交付
完全	“最小”和“默认”事件，加上： <ul style="list-style-type: none"> • 触发 • 超范围钻取 • 检索的页面 • LCM 配置 • 回滚 • VMS 添加 • VMS 检索 • VMS 签入 • VMS 签出 • VMS 导出 • VMS 锁定 • VMS 取消锁定 • VMS 删除 • 多维数据集连接 • MDAS 会话 <p>注意： 如果安装了加载项，则可能存在更多事件。</p>
自定义	选择一组自定义的事件。

3 如果选择了“自定义”，请在“设置事件”滑块下方的列表上单击要捕获的事件。

- 4 在“设置事件详细信息”下，单击要为事件记录的可选详细信息。记录的详细信息越少，系统性能越高。

详细信息	说明
查询	若已设定，将为查询数据库的任何事件记录“查询”事件详细信息（详细信息 ID 25）。
文件夹路径详细信息	若已设定，将捕获以下详细信息： <ul style="list-style-type: none"> 对象文件夹路径（详细信息 ID 71） 顶层文件夹名称（详细信息 ID 72） 容器文件夹名称（详细信息 ID 64）
权限详细信息	若已设定，将捕获以下详细信息： <ul style="list-style-type: none"> 权限已添加（详细信息 ID 55） 权限已删除（详细信息 ID 56） 权限已修改（详细信息 ID 57）
用户组详细信息	若已设定，将捕获以下详细信息： <ul style="list-style-type: none"> 用户组名称（详细信息 ID 16） 用户组 ID（详细信息 ID 15）
属性值详细信息	若已设定，在更新对象属性时，将捕获“属性值”事件详细信息（详细信息 ID 29）。仅为 CMC、BI 启动板或 SharePoint 事件生成此详细信息。

- 5 单击“保存”。

注意：

对于客户端审核，在作出更改与系统开始为任何新事件记录数据之前可能需要等待 2 分钟。请确保允许在实现系统更改时出现此延迟。

21.2.3 审核数据存储配置设置

如果在安装 BI 平台时选择不设置审核数据库，或者希望更改数据库位置或设置，则可以使用以下步骤配置与 ADS 的连接。

也可以在此配置审核事件在数据库中的保留时间。

如果从低于 SAP BusinessObjects Enterprise XI 3.x 的版本执行了升级，并且安装了 Business Objects Metadata Manager (BOMM) 的 3.x 版本，则建议将 ADS 配置为使用与 BOMM 相同的数据库或表空间。

注意：

如果使用现有 DB2 9.7 Workgroup 作为审核数据库，请确保将数据库帐户配置为页面大小大约 8 kB。

21.2.3.1 配置审核数据存储数据库设置

- 1 在中央管理控制台上，选择“审核”选项卡。
- 2 在“配置”区域的“ADS 数据库”标题下方，选择要为审核数据设置的数据库类型。
- 3 在“连接名称”字段中，输入已为审核数据库配置的连接的名称。

数据库类型	连接名称
IBM DB2	服务名称
Microsoft SQL Server	ODBC DSN
MySQL	服务器主机名，端口，数据库名称
Oracle	TNS 服务名称
SAP HANA	ODBC DSN
SAP MaxDB	服务器主机名，端口，数据库名称
Sybase Adaptive Server Enterprise	服务名称
Sybase SQL Anywhere	ODBC DSN

- a 如果要使用采用 Windows 身份验证的 Microsoft SQL 数据库，请启用“Windows Authentication”（Windows 身份验证）选项。
- 4 在“用户名”和“密码”字段中，输入希望审核方 CMS 在登录到数据库时使用的用户名和密码。如果 IBM DB2 由 BI 平台安装为默认数据库，请将“用户名”和“密码”字段留空。
- 5 在“删除以下天数前的事件（天）”字段中，输入希望信息在数据库中保留的天数。（最小值 1，最大值 109,500。）

警告：

时间早于此处设置的天数的数据将从 ADS 中永久删除；无法恢复此类数据。如果想保持长期记录，可以考虑定期将记录移至存档数据库。

- 6 在数据库连接丢失的情况中，如果要手动将审核方 CMS 重新连接到数据库，请取消选择“ADS 自动重新连接”选项。

注意：

如果未选中该选项，则需要在连接丢失时手动建立与 ADS 的连接。通过重新启动 CMS 或启用“ADS 自动重新连接”均可完成上述操作。事件将被记录下来，但仍存储在临时文件中，直到重新与 ADS 建立连接。

- 7 单击“保存”。
- 8 重启群集中的所有 CMS。

注意：

页面顶部的“状态摘要”显示当前的 ADS 值，该值在重启 CMS 前和“ADS 数据库”部分中的值不同。

21.3 审核事件

下表显示了系统中的所有审核事件，并对每个事件进行了简要介绍。接着列出了创建事件的服务类型。

事件	说明以及生成事件类型的服务器和客户端
审核修改	修改系统的审核设置。 <ul style="list-style-type: none"> 中央管理服务
创建	将新对象添加到系统中。 <ul style="list-style-type: none"> 中央管理服务 Crystal Reports 查看和修改服务 Desktop Intelligence 信息引擎服务 生命周期管理 Web Intelligence Web Intelligence 公用服务 Web Intelligence 核心服务 Web Intelligence 处理服务
多维数据集连接	执行 OLAP 多维数据集连接操作。 <ul style="list-style-type: none"> 多维分析服务
自定义访问级别已修改	修改权限信息。 <ul style="list-style-type: none"> 中央管理服务

事件	说明以及生成事件类型的服务器和客户端
删除	<p>从系统中删除对象。</p> <ul style="list-style-type: none"> 中央管理服务 生命周期管理服务
传送	<p>将对象发送/传送到目标。</p> <ul style="list-style-type: none"> 身份验证更新计划服务 中央管理服务 Crystal Reports for Enterprise 计划服务 Crystal Reports 计划服务 Desktop Intelligence 目标传送计划服务 平台搜索计划服务 探测器计划服务 程序计划服务 安全性查询计划服务 用户和组导入计划服务 Web Intelligence 计划和发布服务
超范围钻取	<p>Web Intelligence 文档的用户已向下钻取到超出报表预加载数据范围的详细信息级别。</p> <ul style="list-style-type: none"> Web Intelligence Web Intelligence 处理服务 Web Intelligence 公共服务 Web Intelligence 核心服务 信息引擎服务
编辑	<p>更改对象的内容。</p> <ul style="list-style-type: none"> BI 工作区应用程序 Desktop Intelligence 信息引擎服务 Web Intelligence Web Intelligence 公用服务 Web Intelligence 核心服务 Web Intelligence 处理服务
LCM 配置	<p>更改生命周期管理控制台（LCM）的详细配置。</p> <ul style="list-style-type: none"> 生命周期管理
登录	<p>用户登录到系统。</p> <ul style="list-style-type: none"> 中央管理服务
注销	<p>用户退出系统。</p> <ul style="list-style-type: none"> 中央管理服务

事件	说明以及生成事件类型的服务器和客户端
修改	更改对象的文件属性。 <ul style="list-style-type: none"> • Web Intelligence • 生命周期管理 • 中央管理服务
MDAS 会话	执行多维分析服务操作。 <ul style="list-style-type: none"> • 多维分析服务
检索页面	SAP Crystal Web Intelligence 客户端从资源库中检索其他信息。 <ul style="list-style-type: none"> • Web Intelligence 处理服务 • Web Intelligence 公共服务 • Web Intelligence 核心服务 • 信息引擎服务
提示	为对象提示输入信息。 <ul style="list-style-type: none"> • Crystal Reports 高速缓存服务 • Crystal Reports for Enterprise 计划服务 • Crystal Reports 计划服务 • 仪表盘高速缓存服务 • Desktop Intelligence • 信息引擎服务 • Live Office • Web Intelligence • Web Intelligence 公用服务 • Web Intelligence 核心服务 • Web Intelligence 处理服务
刷新	根据用户请求，从数据库更新对象中的数据。 <ul style="list-style-type: none"> • Crystal Reports 高速缓存服务 • Crystal Reports for Enterprise 计划服务 • Crystal Reports 计划服务 • 仪表盘高速缓存服务 • Desktop Intelligence • 信息引擎服务 • Live Office • Web Intelligence • Web Intelligence 公用服务 • Web Intelligence 核心服务 • Web Intelligence 处理服务
检索	从资源库中检索对象。 <ul style="list-style-type: none"> • 中央管理服务 • Desktop Intelligence

事件	说明以及生成事件类型的服务器和客户端
权限修改	更改用户、组或对象的安全信息。 <ul style="list-style-type: none"> 中央管理服务
回滚	LifeCycle Manager 用于将对象还原到之前版本。 <ul style="list-style-type: none"> 生命周期管理
运行	运行作业。 <ul style="list-style-type: none"> 身份验证更新计划服务 Crystal Reports for Enterprise 计划服务 Crystal Reports 计划服务 Desktop Intelligence 目标传送计划服务 LCM 计划服务 生命周期管理 平台搜索计划服务 探测器计划服务 程序计划服务 发布计划服务 复制服务 安全性查询计划服务 用户和组导入计划服务 视觉差异计划服务 Web Intelligence 计划和发布服务
保存	在更新或更改之后保存对象。 <ul style="list-style-type: none"> Analysis (OLAP 版) Crystal Reports 高速缓存服务 Crystal Reports for Enterprise 计划服务 Crystal Reports 计划服务 Crystal Reports 查看和修改服务 Dashboards Desktop Intelligence 信息引擎服务 生命周期管理 多维分析服务 SAP BusinessObjects Mobile Web Intelligence Web Intelligence 公用服务 Web Intelligence 核心服务 Web Intelligence 处理服务

事件	说明以及生成事件类型的服务器和客户端
搜索	执行搜索。 <ul style="list-style-type: none">• 搜索服务• Explorer• 生命周期管理
触发	触发了文件事件。 <ul style="list-style-type: none">• 事件服务• 中央管理服务
查看	查看对象。 <ul style="list-style-type: none">• Analysis (OLAP 版)• BI 启动板• BI 工作区应用程序• CMC• Crystal Reports 高速缓存服务• Crystal Reports 查看和修改服务• 仪表盘高速缓存服务• Desktop Intelligence• 信息引擎服务• OpenDocument• SAP BusinessObjects Mobile• Web Intelligence• Web Intelligence 公用服务• Web Intelligence 核心服务• Web Intelligence 处理服务
VMS 添加	将对象添加到 LCM 版本管理系统。 <ul style="list-style-type: none">• 生命周期管理
VMS 签入	将对象签入 LCM 版本管理系统。 <ul style="list-style-type: none">• 生命周期管理
VMS 签出	将对象签出 LCM 版本管理系统。 <ul style="list-style-type: none">• 生命周期管理
VMS 导出	从 VMS 中导出资源。 <ul style="list-style-type: none">• 生命周期管理
VMS 锁定	锁定 VMS 中的资源。 <ul style="list-style-type: none">• 生命周期管理

事件	说明以及生成事件类型的服务器和客户端
VMS 取消锁定	取消锁定 VMS 中的资源。 • 生命周期管理
VMS 检索	从 LCM 版本管理系统中检索对象。 • 生命周期管理
VMS 删除	从 LCM 版本管理系统中删除对象。 • 生命周期管理

按服务类型划分的事件

服务类型	生成的事件类型
身份验证更新计划服务	<ul style="list-style-type: none"> • 传送 • 运行
BI 启动板	查看
中央管理服务	<ul style="list-style-type: none"> • 审核修改 • 创建 • 自定义访问级别已修改 • 删除 • 传送 • 登录 • 注销 • 修改 • 检索 • 权限修改 • 触发
中央管理控制台	查看
Crystal Reports 计划服务	<ul style="list-style-type: none"> • 传送 • 提示 • 刷新 • 运行 • 保存
Crystal Reports 高速缓存服务	<ul style="list-style-type: none"> • 提示 • 刷新 • 保存 • 查看

服务类型	生成的事件类型
Crystal Reports for Enterprise 计划服务	<ul style="list-style-type: none">• 传送• 提示• 刷新• 运行• 保存
Crystal Reports 计划服务	<ul style="list-style-type: none">• 传送• 提示• 刷新• 运行• 保存
Crystal Reports 查看和修改服务	<ul style="list-style-type: none">• 创建• 保存• 查看
仪表盘高速缓存服务	<ul style="list-style-type: none">• 提示• 刷新• 查看
仪表盘应用程序	<ul style="list-style-type: none">• 保存
Desktop Intelligence (客户端)	<ul style="list-style-type: none">• 传送• 提示• 检索• 运行
Desktop Intelligence 计划程序流程	<ul style="list-style-type: none">• 传送• 运行
目标传送计划服务	<ul style="list-style-type: none">• 传送• 运行
事件服务	触发
信息引擎服务	<ul style="list-style-type: none">• 创建• 超范围钻取• 编辑• 检索的页面• 提示• 刷新• 保存• 查看

服务类型	生成的事件类型
LCM 计划服务	运行
LCM 服务	<ul style="list-style-type: none"> • 创建 • 删除 • LCM 配置 • 修改 • 回滚 • 运行 • 保存 • VMS 添加 • VMS 签入 • VMS 签出 • VMS 删除 • VMS 导出 • VMS 锁定 • VMS 检索 • VMS 取消锁定 • 搜索
Live Office	<ul style="list-style-type: none"> • 提示 • 刷新
多维分析服务	<ul style="list-style-type: none"> • 多维数据集连接 • MDAS 会话 • 保存
OpenDocument	查看
平台搜索计划服务	<ul style="list-style-type: none"> • 传送 • 运行
平台搜索服务	搜索
探测器计划服务	<ul style="list-style-type: none"> • 传送 • 运行
程序计划服务	<ul style="list-style-type: none"> • 传送 • 运行
发布计划服务	运行
复制服务	运行
安全性查询计划服务	<ul style="list-style-type: none"> • 运行 • 交付

服务类型	生成的事件类型
用户和组导入计划服务	<ul style="list-style-type: none">• 运行• 交付
视觉差异计划服务	运行
Web Intelligence 应用程序	<ul style="list-style-type: none">• 创建• 超范围钻取• 编辑• 修改• 提示• 刷新• 保存• 查看
Web Intelligence 公用服务	<ul style="list-style-type: none">• 创建• 超范围钻取• 编辑• 检索的页面• 提示• 刷新• 保存• 查看

服务类型	生成的事件类型
Web Intelligence 核心服务	<ul style="list-style-type: none"> • 创建 • 超范围钻取 • 编辑 • 检索的页面 • 提示 • 刷新 • 保存 • 查看
Web Intelligence 处理服务	<ul style="list-style-type: none"> • 创建 • 超范围钻取 • 编辑 • 检索页面 • 提示 • 刷新 • 保存 • 查看
Web Intelligence 计划和发布服务	<ul style="list-style-type: none"> • 传送 • 运行

事件属性和详细信息

BI 平台记录的每个事件都包括一组事件属性和详细信息。

即使在信息不适用于特定事件而使某些事件属性不具有值的情况下，事件属性也会始终随事件一起生成。在 ADS 中，事件属性包含在存储事件的表中，因此在创建报表时可使用事件属性对事件进行排序或分组。

事件详细信息记录未包含在事件属性中的附加事件信息。如果事件详细信息与特定事件无关，则不生成该事件详细信息。有一组可在相关的情况下为所有事件类型生成的公共事件详细信息。还有可为特定事件类型生成的多组附加事件详细信息。例如，提示事件记录在事件详细信息中为提示输入的值，但任何其他事件类型均不会生成提示值事件详细信息。在 ADS 中，详细信息存储在与父事件链接的单独的表中。

在某些情况下，事件详细信息可包含多个值。可使用组 ID 将这些详细信息进行分组。请参阅相关主题，了解有关组 ID 的详细信息。

将以审核方 CMS 区域设置的默认语言记录任何多语种数据（如对象或文件夹名称）。

相关主题

- 第 977 页上的“[审核数据存储表](#)”

21.3.1 审核事件和详细信息

下面部分列出了所有事件类型，并描述这些事件所特有的全部属性和事件详细信息。本节开始部分列出了所有事件类型所共有的属性和详细信息。

注意：

有些客户端程序不具有特有的事件，需借助公共事件和平台事件捕获相关操作信息。

通用事件属性和详细信息

以下各表显示为所有事件记录的属性和事件详细信息。

注意：

此表中的属性为审核数据存储中 ADS_EVENT 表中的列。

事件属性	说明
Event_ID	事件的唯一标识符。
Client_Type_ID	执行事件的应用程序类型的标识符
Service_Type_ID	显示触发事件的服务或应用程序类型的 ID。
Start_Time	事件启动的日期和时间（GMT 时间）。
Duration	事件的持续时间（以毫秒为单位）。
Session_ID	触发事件的会话的 ID。
Event_Type_ID	事件的类型（例如，1002 表示“查看”）。
Status_ID	记录操作是成功还是失败（“0” = 成功，“1” = 失败）。有些事件将具有其他状态类型，这将在介绍这些事件时进行详细说明。
Object_ID	受影响对象的 CUID（如适用）。针对触发事件的警报事件的 CUID。 注意： 所有未保存在 CMS 资源库中的对象都将具有标识 0。例如，这些对象可能是尚未保存到 CMS 数据库的文档，或以本地方式存储在客户端计算机上的文档。将需要使用 Object_Name 属性区别这些对象。
User_ID	执行事件的用户 CUID。
User_Name	执行事件的用户的用户名。
Object_Name	受影响对象的名称（如适用）。用于触发事件的警报事件的名称。
Object_Type_ID	对象类型的 CUID（例如文档、文件夹等）。

事件属性	说明
Object_Folder_Path	受影响对象在 CMS 资源库中所在文件夹的完整路径。例如 Sales/North America/East Coast
Folder_ID	存储对象的文件夹的 CUID。
Top_Folder_Name	存储受影响对象的顶层文件夹的名称。例如，如果对象位于 Sales/North America/East Coast 中，则值将为 Sales。
Top_Folder_ID	受影响对象所在的顶层文件夹的 CUID。例如，如果对象位于 Sales/North America/East Coast 中，则值将为文件夹 Sales 的 CUID。
Cluster_ID	记录事件的 CMS 群集的 CUID。
Action_ID	可用于捆绑由单一用户操作启动的一系列事件的唯一标识符。

注意：

此表中的属性为审核数据存储中 ADS_EVENT_DETAIL_TYPE_STR 表中的列。

事件详细信息	ID	说明
错误	1	仅在操作失败时记录；尝试所产生的任何错误消息文本。
元素 ID	2	驻留在容器对象（例如 Live Office 文档或仪表盘）中的对象的名称。
元素名称	3	为驻留在容器对象（例如 Live Office 文档或仪表盘）中的对象生成的 ID。
元素类型 ID	5	正在查看或修改的容器对象中的对象的类型。仅在适用的情况下生成。
父文档 ID	12	<ul style="list-style-type: none"> 对于文档实例：父文档的 CUID。 对于父文档：父文档自己的 CUID。
Universe ID	13	由文档或对象使用的 Universe 的 CUID。如果使用多个 Universe，则为每一个 Universe 都生成事件详细信息。
Universe 名称	14	由文档/对象使用的 Universe 的名称。如果使用多个 Universe，则为每一个 Universe 都生成事件详细信息。
用户组名称	15	执行操作的用户所属的用户组名称。如果用户属于多个组，则为每个组都生成事件详细信息。
用户组 ID	16	执行操作的用户所属的用户组 ID。如果用户属于多个组，则为每个组都生成事件详细信息。

公共事件

以下事件类型是所有 SAP BusinessObjects 服务器与客户端所共有的。

查看

用户查看文档/对象。

- 事件类型 ID: 1002

事件详细信息	ID	说明
大小	17	作为事件主题的对象的大小（以字节为单位）。
容器 ID	32	对象所驻留的容器对象（例如仪表盘的 CUID（如适用）。
容器类型	33	用于对象的容器的应用程序类型（如适用）。

注意：

如果使用搜索服务，则在文档索引过程中可能会注意到由“系统帐户”用户生成的大量“查看”事件。这是由搜索索引建立服务打开文档以构建搜索索引造成的。

刷新

从数据库刷新某个对象。

- 事件类型 ID: 1003

事件详细信息	ID	说明
大小	17	作为事件主题的对象的大小（以字节为单位）。 注意： 对于“按需查看 Crystal Reports”，这将设置为 0。
行数	63	数据库服务器返回的记录数。 注意： 对于“按需查看 Crystal Reports”，这将设置为 0。
查询	25	记录用于刷新数据的 SQL 查询（可选，在 CMC 中设置）。
Universe 对象名称	31	文档或对象使用的 Universe 的名称。将为文档或对象访问的每个 Universe 生成事件详细信息。
文档范围	36	记录文档的发布设置中所计划范围的相关信息（例如：国家/地区 = 美国，角色 = 经理）。仅适用于发布工作流。
发布实例 ID	37	此发布实例的 ID 仅适用于发布工作流。
Live Office 对象类型	10701	标识 Live Office 文档中正在刷新的对象的类型（例如 Crystal 报表）。仅为 Live Office 文档生成。

提示

为提示输入值。

- 事件类型 ID: 1004

事件详细信息	ID	说明
提示名称	26	分配给提示的名称（例如“日期”）。将为文档或对象中的每个提示分别生成详细信息，并对其进行分组。
提示值	27	为提示输入的值。将为输入的每个值分别生成详细信息。可将这些详细信息分组，并追溯到提示名称。
文档范围	36	文档计划范围的信息（例如：国家/地区 = 美国，角色 = 经理）。
发布实例 ID	37	此发布实例的 ID 仅适用于发布工作流。
设计时的名称	90	Dashboards 文档在设计时的名称。仅为 Dashboards 刷新或包括提示的 Dashboards 或 Live Office 文档生成。
Live Office 对象类型	10701	标识 Live Office 文档中正在刷新的对象的类型（例如 Crystal 报表）。仅为其中的嵌入式对象包括提示的 Live Office 文档生成。

创建

用户创建了一个对象。

- 事件类型 ID: 1005

事件详细信息	ID	说明
大小	17	作为事件主题的对象的大小（以字节为单位）。
覆盖	21	记录文档或对象是新建的还是覆盖了现有对象（0 = 新文档或对象，1 = 覆盖现有文档或对象）。
打开时刷新	23	记录文档或对象是否设置为打开时自动刷新（0 = 不刷新，1 = 打开时刷新）。仅在适用的情况下生成。
说明	24	记录文档或对象的说明字段中的任何信息。

删除

用户删除了一个对象。

- 事件类型 ID: 1006

修改

用户修改了对象的一个或多个文件属性。

- 事件类型 ID: 1007

事件详细信息	ID	说明
属性名称	28	已修改的属性的名称。将为每个已修改的属性生成事件详细信息。
属性值	29	文档或对象的任何已修改属性的新值。将为每个已修改的属性生成事件详细信息。

保存

以文档或对象的现有格式或其他格式将其以本地方式或远程方式保存或导出到 CMS 资源库。

- 事件类型 ID: 1008
- 状态:
 - “0”表示对象已本地保存成功。
 - “1”表示尝试失败。
 - “2”表示对象已成功保存或导出到资源库。
 - “3”表示对象已成功保存或导出到一个新格式。

事件详细信息	ID	说明
大小	17	已保存或导出的对象的大小（以字节为单位）。
文件名	18	保存文档或对象时使用的全名。如果客户端应用程序以本地方式保存文件，则该名称也会包括文件路径。
覆盖	21	记录文档或对象是新建的还是覆盖了现有文件。“0”= 新文档或对象，“1”= 覆盖现有文档或对象。
格式	22	指定已保存/导出文档的格式，以常见的三个字母文件扩展名显示（例如“doc”表示 Microsoft Word 文件，“pdf”表示 Adobe PDF 文件）。
打开时刷新	23	记录文档或对象是否设置为打开时自动刷新（“0”= 不刷新，“1”= 打开时刷新）。仅在适用的情况下记录。

搜索

执行了搜索。

- 事件类型 ID: 1009

事件详细信息	ID	说明
关键字	19	已执行搜索的关键字。
类别	20	搜索中使用的类别（如适用）。
行数	63	搜索返回的行数。

编辑

用户编辑了对象的内容。

- 事件类型 ID: 1010

事件详细信息	ID	说明
大小	17	作为事件主题的对象的大小（以字节为单位）。
查询	25	如果编辑时修改了 SQL 查询，则记录新的查询。（此设置为可选项，可在“CMC 审核”页面上进行选择。）
Universe 对象名称	31	文档或对象使用的 Universe 的名称。将为文档或对象访问的每个 Universe 分别生成详细信息。
容器 ID	32	使用对象的容器（例如仪表盘）的 CUID（如适用）。
容器类型	34	用于对象的容器的应用程序类型（如适用）。
容器文件夹路径	64	对象容器的文件夹路径（如适用）。

运行

运行了作业。

- 事件类型 ID: 1011
- 状态：
 - “0”表示作业成功执行
 - “1”表示作业失败
 - “2”表示作业失败，但将重试
 - “3”表示作业被取消

事件详细信息	ID	说明
大小	17	已运行文档的大小（以字节为单位）。
文档范围	36	文档计划范围的信息（例如：国家/地区 = 美国，角色 = 经理）。

传送

传送了对象。

- 事件类型 ID: 1012

事件详细信息	ID	说明
大小	17	已传送对象的大小（以字节为单位）。
目标类型	35	文档或对象实例的目标。例如，电子邮件、FTP、非托管磁盘、收件箱或打印机。
文档范围	36	文档计划范围的信息（例如国家/地区 = 美国，角色 = 经理）
发布实例 ID	37	此文档或对象实例的 ID。
域	38	记录通过电子邮件分发的文档/对象的 SMTP 服务器域名（如适用）。
主机名	39	记录通过电子邮件或 FTP 分发的文档/对象的 SMTP 或 FTP 主机的名称（如适用）。
端口	40	记录通过电子邮件或 FTP 分发的文档/对象的 SMTP 或 FTP 服务器域端口（如适用）。
发件人地址	41	记录通过电子邮件分发的文档/对象的发件人地址（如适用）。
收件人地址	42	记录通过电子邮件分发的文档/对象的收件人地址（如适用）。还将指定该地址是否包含在“收件人”、“抄送”或“密件抄送”字段中。将为每个目标收件人生成事件详细信息。
文件名	18	记录通过电子邮件或 FTP 分发或直接写入磁盘（不属于 Business Objects 部署）的文档/对象的文件名。
帐户名称	45	这将记录以下信息之一： <ul style="list-style-type: none"> 对于“收件箱”传送对象，记录 BusinessObjects 用户帐户名称列表。 对于“FTP”传送对象，记录 FTP 帐户名称。 对于“非托管磁盘”传送对象，记录所用的登录帐户。 对于“SMTP”传送对象，记录用于 SMTP 服务器的登录帐户。
打印机名称	46	向其传送文档或对象的打印机的名称（如适用）。
份数	47	文档或对象的打印份数（如适用）。
收件人姓名	48	用户名或文档或对象的收件人。将为每个目标收件人生成事件详细信息。

事件详细信息	ID	说明
警报事件 ID	92	警报事件的 CUID。仅在通过警报提示事件时生成。
警报事件名称	93	警报事件的名称。仅在通过警报提示事件时生成。
传送类型	75	指示传送的启动方式： <ul style="list-style-type: none">“0”表示计划“1”表示发送到目标“2”表示发布“3”表示已触发警报

检索

从 CMS 中检索了对象。

- 事件类型 ID: 1013

登录

用户登录。

- 事件类型 ID: 1014
- 状态：
 - “0”表示并发用户许可登录成功
 - “1”表示登录尝试失败
 - “2”表示命名用户许可登录成功
 - “3”表示非用户（系统）登录成功

事件详细信息	ID	说明
并发用户数	50	触发事件时系统上的用户数。
客户端报告的客户端主机名	51	客户端报告的客户端主机名。
服务器解析的客户端主机名	52	服务器解析的客户端主机名。如果无法解析客户端主机名，则不记录任何值。
客户端报告的客户端 IP 地址	53	客户端报告的客户端 IP 地址。
服务器解析的客户端 IP 地址	54	服务器解析的客户端 IP 地址。如果无法解析客户端 IP，则不记录任何值。

注销

用户注销。

- 事件类型 ID: 1015

事件详细信息	ID	说明
并发用户数	50	触发事件时系统上的并发用户数。

触发

触发了文件事件。

事件类型 ID: 1016

事件详细信息	ID	说明
文件名	18	正在监控和触发事件的文件的名称。

21.3.1.1 平台事件

下列事件特定于 BI 平台。

权限修改

对象的一个或多个权限已修改。

事件类型 ID: 10003

事件详细信息	ID	说明
添加的权限	55	所添加权限的类型、新权限的范围（哪些对象）以及适用的对象类型。信息将采用以下示例所示的结构：added right=Export; new value=Granted; scope=Current object; applicable object type=all object types。
删除的权限	56	所删除权限的类型、新权限的范围（哪些对象）以及适用的对象类型。信息将采用以下示例所示的结构：removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types。
修改的权限	57	所修改权限的类型、新权限的范围（哪些对象）以及适用的对象类型。信息将采用以下示例所示的结构：modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types。
主体	118	修改其安全权限的用户或用户组（主体）的 ID。
主体名称	119	修改其安全权限的用户或用户组（主体）的名称。

自定义访问级别已修改

自定义访问级别已修改。

事件类型 ID: 10004

事件详细信息	ID	说明
添加的权限	55	所添加权限的类型、新权限的范围（哪些对象）以及适用的对象类型。信息将采用以下示例所示的结构：added right=Export; new value=Granted; scope=Current object; applicable object type=all object types
删除的权限	56	所删除权限的类型、新权限的范围（哪些对象）以及适用的对象类型。信息将采用以下示例所示的结构：removed right=Export; previous value=Denied; scope=Current object; applicable object type=all object types。
修改的权限	57	所修改权限的类型、新权限的范围（哪些对象）以及适用的对象类型。信息将采用以下示例所示的结构：modified right=Export; previous value=Granted; scope=Current object; applicable object type=all object types。
主体	118	修改其安全权限的用户或用户组（主体）的 ID。

审核修改

更改了系统的审核设置。

事件类型 ID: 10006

事件详细信息	ID	说明
事件类型 ID	58	记录启用或禁用的审核事件类型的 ID。如果在一个操作中启用或禁用了多个事件类型，则会为每个事件类型生成一个事件详细信息。
操作	59	记录启用或禁用了哪些审核事件。
新审核级别	60	如果详细信息的审核级别发生更改，则记录新的级别设置（例如，禁用、最小或默认）。
旧审核级别	61	如果详细信息的审核级别发生更改，则记录以前的级别设置（例如，禁用、最小或默认）。
审核选项	62	如果启用或禁用了某个可选详细信息，将记录所修改的详细信息以及是否已将其启用或禁用。如果在一个操作中启用或禁用了多个详细信息，则会为每个修改的详细信息生成一个详细信息记录。
ADS 连接	78	<p>如果更改了审核数据存储的连接，它将使用以下格式记录新的连接设置：DBType=Oracle, DBName=MyADS, Username=USR1, Password="*****", SS0=off, DBReconnect=on。将仅记录发生更改的详细信息。例如，如果只更新了用户名，则仅记录 Username="new"。</p> <p>注意： 在数据库中，密码信息将始终用 * 隐藏起来。</p>
自动删除时间间隔	105	此项详细信息将记录对 CMC 的“审核”页面中“删除以下天数前的事件”字段所做的任何更改。它可控制审核信息在 ADS 中的保留天数。

21.3.1.2 SAP BusinessObjects Web Intelligence 事件

以下事件是特定于 SAP BusinessObjects Web Intelligence 组件的。

超范围钻取

用户的钻取操作超出了报表的范围。

- 事件类型 ID: 10201

事件详细信息	ID	说明
对象实例	11	记录该事件是计划的更新还是用户查看对象的结果（“0”是用户查看对象的结果；“1”是计划的对象刷新的结果）。
行数	63	数据库服务器返回的行数。
查询	25	记录用于刷新数据的查询（可选，在 CMC 中设置）。
Universe 对象名称	31	文档使用的 Universe 的名称。针对文档访问的每个 Universe 都将记录一个实例。
Universe ID	32	文档使用的 Universe 的 CUID。针对文档访问的每个 Universe 都将记录一个实例。

检索页面

检索了 Web Intelligence 文档页面。

- 事件类型 ID: 10202

21.3.1.3 SAP BusinessObjects Analysis (OLAP 版) 事件

MDAS 会话

执行 MDAS 会话操作

- 事件类型 ID: 10300
- 状态:
 - “0” = 成功打开了一个新会话。
 - “1” = 新会话失败。
 - “2” = 关闭了一个现有会话。

MDAS 多维数据集连接

执行多维数据集连接操作。

- 事件类型 ID: 10301
- 状态:
 - “0” = 成功打开了一个新连接。
 - “1” = 新连接失败。
 - “2” = 关闭了一个现有连接。

事件详细信息	ID	说明
连接 ID	94	连接的唯一标识符。
连接名称	95	连接的名称。
提供者类型	96	多维数据集提供者的类型。
多维数据集名称	97	所使用的多维数据集的完整名称。

21.3.1.4 SAP BusinessObjects 生命周期管理控制台事件

以下事件是 SAP BusinessObjects 生命周期管理组件所独有的。

SAP BusinessObjects 生命周期管理控制台通用详细信息

所有生命周期管理事件都具有以下附加事件详细信息。

事件详细信息	ID	说明
元素群集	6	当生命周期管理控制台对位于不同群集中的对象执行操作时受影响群集的 CUID。系统将为每个受影响的群集生成一个事件详细信息。
元素注释	7	有关对象的附加信息。
主元素	8	如果元素是主元素，此项详细信息将设为“1”；如果元素为从属元素，则设为“0”。
元素状态	9	如果操作元素失败，此项详细信息将设为“1”；否则设为“0”。
操作	10	说明所执行操作的类型（例如“添加”、“删除”或“修改”）。

SAP BusinessObjects 生命周期管理控制台配置

生命周期管理的配置发生更改。

- 事件类型 ID: 10900

事件详细信息	ID	说明
配置	100	用户查看了生命周期管理控制台配置。配置显示为逗号分隔的值对，例如：rollback settings=enabled, port=900。
之前配置	101	如果修改某个对象的生命周期管理控制台设置，则会记录之前的配置设置。使用与配置相同的格式。
之后配置	102	如果修改某个对象的生命周期管理控制台设置，则会记录新的配置设置。使用与配置相同的格式。
VMS 类型	10900	版本管理系统的类型。

回滚

对象回滚为以前的版本管理系统（VMS）版本。

- 事件类型 ID: 10901

VMS 添加

向 VMS 添加资源。

- 事件类型 ID: 10902

事件详细信息	ID	说明
版本	104	在版本管理系统中记录文档的版本号。

VMS 检索

从 VMS 中检索资源。

- 事件类型 ID: 10903

事件详细信息	ID	说明
还原删除的对象	103	表明是否从系统中删除了检索的对象。 “0”表示未删除对象；“1”表示删除了对象。
版本	104	在 VMS 中记录文档的版本号。

VMS 签入

将资源签入到 VMS 中。

- 事件类型 ID: 10904

事件详细信息	ID	说明
版本	104	在 VMS 中记录文档的版本号。

VMS 签出

从 VMS 中签出资源。

- 事件类型 ID: 10905

事件详细信息	ID	说明
版本	104	在 VMS 中记录文档的版本号。

VMS 导出

从 VMS 中导出资源。

- 事件类型 ID: 10906

事件详细信息	ID	说明
版本	104	在 VMS 中记录文档的版本号。

VMS 锁定

锁定 VMS 中的资源，以防止用户进行编辑。

- 事件类型 ID: 10907

事件详细信息	ID	说明
版本	104	在 VMS 中记录文档的版本号。
锁定者	10901	执行该操作的用户的用户名。

VMS 取消锁定

取消锁定 VMS 中的资源，允许用户对其进行编辑。

- 事件类型 ID: 10908

事件详细信息	ID	说明
版本	104	在 VMS 中记录文档的版本号。
取消锁定者	10902	执行该操作的用户的用户名。

VMS 删除

从 VMS 中删除资源。

- 事件类型 ID: 10909

事件详细信息	ID	说明
版本	104	在版本管理系统中记录文档的版本号。

第 22 章 平台搜索

22.1 了解平台搜索

利用平台搜索可以在 SAP BusinessObjects Business Intelligence 平台资源库中搜索内容。该工具可将搜索结果分组为若干类别，并按照搜索结果的相关性顺序对搜索结果进行排名，从而过滤搜索结果。

在此版本的 BI 平台中，平台搜索增强了以下功能：

- 搜索 BI 平台和 Explorer 内容。
- 如果找不到现有文档，则查询是否要创建文档。
- 同时支持持续索引建立和基于计划的索引建立。
- 支持在群集环境中建立索引。
- 设置和修改索引建立级别。
- 提供高级搜索配置选项。
- 支持多语言搜索和索引建立。
- 提供高级搜索语法。
- 支持元数据、内容和动态构面。
- 支持基于系统负载的自我康复。

注意：

如果从之前版本迁移到新版本，则索引不会迁移。

22.1.1 平台搜索 SDK

平台搜索支持使用公共 SDK 充当客户端应用程序和平台搜索之间的接口。它是面向公众提供的，可帮助用户自定义搜索服务并将其与应用程序相集成。

当搜索请求参数通过客户端应用程序发送给 SDK 层时，SDK 层会将请求参数转换为 XML 编码格式，并将其传递给平台搜索服务。

有关平台搜索 API 的更多信息，请参阅《Business Intelligence platform Java API Reference》（Business Intelligence 平台 Java API 参考）。

22.1.2 群集环境

平台搜索具有在群集环境中跨多个节点分担负载的能力。群集环境中的部署可优化系统资源并提升服务器性能。

平台搜索对搜索功能和索引建立功能均支持水平和垂直群集化。利用群集化环境，它可优化搜索和索引过程的性能。

负载平衡

平台搜索同时支持对索引建立和搜索的负载平衡。在群集环境中，可以在多个节点上执行索引建立以及搜索请求，以分担负载。每个节点均独立工作，以建立内容索引并创建增量索引。不过，群集中只有一个节点充当主索引，并将增量索引合并到主索引。所有节点均可访问主索引。这允许同时处理多个搜索请求。

故障转移

故障转移机制确保用户可继续搜索，并且索引操作不会中断。如果群集中的某个节点由于技术故障或与维护相关的活动而无法使用时，其他节点会自动处理索引建立和搜索请求。

22.2 设置平台搜索

22.2.1 部署 OpenSearch

平台搜索支持 OpenSearch 标准，从而使客户端应用程序能够使用 OpenSearch 标准和格式与平台搜索进行通信。默认情况下，OpenSearch 不随 SAP BusinessObjects Business Intelligence 套件一

起安装，因此用户需要将其作为单独的 WAR 文件（opensearch.war）手动部署到应用程序服务器（如 Tomcat），或者使用 WDeploy 工具进行部署。安装程序会将此文件复制到安装目录\warfiles\OpenSearch 目录中。

注意：

- 客户端程序与平台搜索进行通信时，需遵循 OpenSearch 标准。
- 安装 BI 平台时，会默认安装 Tomcat 应用程序服务器。

22.2.1.1 手动部署

要在 BI 平台环境下部署 OpenSearch，请执行以下步骤：

- 1 转到以下位置：安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\。
- 2 将 OpenSearch 文件夹复制到安装目录\tomcat\webapps\。
- 3 更改 \OpenSearch\WEB-INF\config.properties 文件中的配置参数：
 - CMS：CMS 名称及端口号：<CMS 名称>：<端口号>。
 - OpenDocURL：OpenDocument 应用程序的 URL：http://<Tomcat主机>:<连接器端口>/BOE/OpenDocument/opendoc/openDocument.jsp。
 - Proxy.rpurl：如果要使用反向代理，则需要反向代理服务器名称。
 - Proxy.opendoc.rpurl：如果要使用反向代理，则需要 opendoc 反向代理服务器名称。
- 4 重新启动 Tomcat 应用程序服务器以部署 OpenSearch。

22.2.1.2 使用 WDeploy 部署

要使用 WDeploy 部署 OpenSearch，请执行以下步骤。

注意：

对于 Windows 和 Unix，命令分别用 wdeploy.bat <参数>和 wdeploy.sh <参数> 表示。

- 1 用所需的 Web 应用程序服务器参数（如安装目录、实例名称、管理端口、管理用户名和管理密码）更新位于安装目录\SAP BusinessObjects Enterprise XI 4.0\wdeploy\conf 下的config. 应用程序服务器文件。
- 2 更改安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\OpenSearch\WEB-INF\config.properties 文件中的配置参数：
 - CMS：CMS 名称及端口号：<CMS 名称>：<端口号>。

- OpenDocURL: OpenDocument 应用程序的 URL: `http://<Web 应用程序服务器主机>:<连接器端口>/BOE/OpenDocument/opensdoc/openDocument.jsp`。
 - Proxy.rpurl: 如果要使用反向代理, 则需要反向代理服务器名称。
 - Proxy.opensdoc.rpurl: 如果要使用反向代理, 则需要 opensdoc 反向代理服务器名称。
- 3 从安装目录\SAP BusinessObjects Enterprise XI 4.0\wdeploy 位置执行wdeploy.bat <Web 应用程序服务器> -Dapp_source_tree=<OpenSearch Web 应用程序的父文件夹> -DAPP=OpenSearch deploy 命令。

例如, 以下命令可将 OpenSearch 部署到 WebSphere 7 Web 应用程序服务器:

```
wdeploy.bat websphere7 -Dapp_source_tree="INSTALLDIR\SAP BusinessObjects Enterprise XI 4.0\warfiles" -DAPP=OpenSearch deploy
```

- 4 重新启动应用程序服务器。

22.2.2 配置反向代理

若要在位于反向代理服务器后面的 Web 应用程序服务器上部署 Web 应用程序, 请对反向代理服务器进行配置, 以将传入的 URL 请求映射到正确的 WAR 文件。

为了说明配置步骤, 我们用 Apache 2.2 反向代理服务器作为示例。为 OpenSearch 配置 Apache 2.2 反向代理服务器:

- 1 设置反向代理并更改 OpenSearch 的 WEB-INF\config.properties 文件。
- 2 启用以下上下文参数, 并相应地更改其值。
 - proxy.rpurl: 这是 OpenSearch 的反向代理 URL (如 `http://机器 IP 地址/RP/OpenSearch/`)。
 - proxy.opensdoc.rpurl: 这是 OpenDoc 的反向代理 URL (如 `http://机器 IP 地址/RP/BOE/`)。
- 3 用下列设置更新位于 Apache 反向代理安装文件夹中的 httpd.conf 文件:
 - ProxyPass /RP/BOE/OpenDocument/ `http://<Tomcat 主机>:<连接器端口>/BOE/OpenDocument/`
 - ProxyPass /RP/OpenSearchRP/ `http://<Tomcat 主机>:<连接器端口>/OpenSearch/`
 - ProxyPassReverseCookiePath /BOE /RP/BOE
 - ProxyPassReverseCookiePath /OpenSearchRP /RP/OpenSearchRP
- 4 重新启动 Apache 2.2 反向代理服务器。

22.2.3 在 CMC 中配置应用程序属性

若要配置平台搜索应用程序属性, 请完成以下步骤:

- 1 转到 CMC 的“应用程序”区域。
- 2 选择“平台搜索应用程序”。
- 3 单击“管理” > “属性”。将出现“属性”对话框。
- 4 配置平台搜索设置：

选项	说明
搜索统计信息	<p>平台搜索提供以下搜索统计信息：</p> <ul style="list-style-type: none"> 索引建立状态：显示索引建立进程的状态。 已建立索引的文档数：显示已建立索引的文档数。 上次建立索引的时间戳：显示上次为该文档建立索引时的时间戳。
停止/启动索引建立	<p>要从持续爬网切换到计划爬网或用于维护目的时，可以使用“开始建立索引”或“停止建立索引”选项来启动或停止索引建立流程。</p> <p>要停止建立索引，请单击“停止建立索引”。</p>
默认索引区域设置	<p>平台搜索使用在 CMC 中指定的区域设置为所有未本地化的 BI 文档建立索引。文档实现本地化后，将使用相应语言的分析器建立索引。</p> <p>搜索基于客户端的产品区域设置，并且为客户端的产品区域设置分配权重。</p> <p>可以在 CMC 配置属性中配置权重。</p>
爬网频率	<p>可以使用以下选项为整个 BI 平台资源库建立索引：</p> <ul style="list-style-type: none"> 持续爬网：通过该选项，每当添加、修改或删除对象时都可以随时为资源库建立索引。持续爬网使用户可以查看或使用最新的 BI 平台内容。默认设置下，持续爬网会根据用户所执行的操作不断地更新资源库。持续爬网无需用户干预即可运作，从而减少了对文档建立索引所需的时间。 计划的爬网：通过该选项，可以根据“计划”选项设置的计划来建立索引。 <p>有关如何计划对象的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 CMC 联机帮助》中“平台搜索”的“计划对象”部分。</p> <p>注意：</p> <ul style="list-style-type: none"> 如果选择“计划的爬网”并将“重复发生”设置为“立即”以外的其他选项，则平台搜索将显示计划下次对文档建立索引的日期和时间戳。 如果选择“计划的爬网”，则会启用“开始建立索引”按钮，而禁用“停止建立索引”按钮。 计划完成后，“停止建立索引”按钮将禁用。

选项	说明
索引位置	<p>索引存储在以下位置中的共享文件夹中：</p> <ul style="list-style-type: none">主索引位置（索引和拼写程序）：主索引和拼写程序索引存储在此位置中。在搜索过程中，主索引用于检索初始结果，而拼写程序索引用于检索建议。在群集式 BI 平台部署中，此位置应该位于可以从群集的所有节点访问的共享文件系统上。永久性数据位置（内容存储）：内容存储位于此位置中。它是从主索引位置中创建的，并与之保持同步。内容存储用于生成构面，并处理从主索引位置生成的初始提示。在群集 BI 平台部署中，每个节点都会生成内容存储。 <p>永久性数据位置是唯一受群集环境影响的索引位置，这是因为它包含内容存储文件夹。如果计算机只有一种搜索服务，则只有一个内容存储位置。例如，{bobj.enterprise.home}\data\PlatformSearchData\workspace\<服务器名称>\ContentStores。</p> <p>不过，如果在群集环境中有多于一个搜索服务，则每个搜索服务将有一个内容存储位置。例如，如果有两个服务器实例在运行，则内容存储位置将如下所示：</p> <ul style="list-style-type: none">a {bobj.enterprise.home}\data\PlatformSearchData\workspace\<服务器名称>\ContentStores。b {bobj.enterprise.home}\data\PlatformSearchData\workspace\<服务器名称 1>\ContentStores。 <ul style="list-style-type: none">非永久性数据位置（临时文件，增量索引）：在增量索引与主索引合并之前，此位置中会临时创建和存储增量索引。此位置的索引在与主索引合并后即被删除。此外，此位置中将创建替代文件（提取器的输出），并在其转换为增量索引之前临时存储这些文件。 <p>注意：</p> <ul style="list-style-type: none">所有索引位置必须是共享位置。需要单击“停止建立索引”，才能修改索引位置。如果修改索引位置，则需要将内容复制到新位置，否则现有索引信息将丢失。

选项	说明
索引建立级别	<p>可以通过以下方式设置索引建立级别来微调搜索内容：</p> <ul style="list-style-type: none"> 平台元数据：仅为平台元数据信息（如文档的标题、关键字和说明）创建索引。 平台和文档元数据：此索引包括平台元数据以及文档元数据。文档元数据包括创建日期、修改日期和作者姓名。 全部内容：此索引包括平台元数据、文档元数据和其他内容，例如： <ul style="list-style-type: none"> 文档中的实际内容 提示和 LOV 内容 统计图、图形和标签 <p>注意： 修改索引建立级别时，将为整个 BI 平台资源库刷新重新初始化索引建立。</p>
内容类型	<p>可以选择以下内容类型来建立索引：</p> <ul style="list-style-type: none"> Crystal Reports Web Intelligence Universe BI 工作区 Microsoft PowerPoint Adobe Acrobat 多信息文本 文本 Microsoft Word Microsoft Excel
重新建立索引	<p>此选项将删除现有索引，并重新建立整个资源库的索引。</p> <p>不管建立索引是在运行还是已停止，都可以选择“重新建立索引”选项。现有索引在将更改保存到属性页时被删除。不过，如果建立索引当前已停止，索引在重新开始建立索引前不会开始重建。</p> <p>如果不希望平台搜索重新为文档建立索引，则需要清除“重新建立索引”选项，然后单击“开始建立索引”。</p>

选项	说明
从索引建立范围排除的文档	<p>“从索引建立范围排除的文档”选择将从索引建立范围排除文档。例如，用户可能希望将极大的 Crystal 报表设置为不可搜索，以确保报表应用程序服务器资源不会过载。同样，也可能不希望对包含数百个性化报表的发布建立索引。</p> <p>通过排除特定文档，可以防止从平台搜索对其进行访问。值得注意的是，如果在将某个文档放入该组之前已对其建立索引，则此文档可能仍然是可搜索的文档。为确保“从索引建立范围排除的文档”组中的文档不可搜索，必须重新建立索引。</p> <p>默认情况下，只有管理员帐户拥有“从索引建立范围排除的文档”选项的完全控制权限。具有以下权限的其他用户只能向“从索引建立范围排除的文档”组中添加文档：</p> <ul style="list-style-type: none">对目录的查看和编辑权限直接编辑文档

5 单击“保存并关闭”。

注意：

如果用户未选择“重新建立索引”选项而更改了索引建立级别或者选择或取消选择了提取器，则索引会以增加方式更新，而不删除现有索引。

22.3 使用平台搜索

22.3.1 为 CMS 资源库中的内容建立索引

索引建立是持续过程，包括以下顺序任务：

- 1 爬网：爬网机制轮询 CMS 资源库，并确定发布、修改或删除的对象。这可以通过两种方式进行：持续爬网和计划的爬网。

有关持续爬网和计划爬网的更多信息，请参阅“相关主题”中的“配置应用程序属性”主题。

- 2 提取：提取机制根据文档类型调用提取器。在资源库中，每种文档类型都有专用提取器。通过定义新提取器插件，可以搜索新文档类型。上述每个提取器均可伸缩，足以从包含众多记录的大型文档中提取内容。

支持以下提取器：

- 元数据提取器
- Crystal 报表提取器
- Web Intelligence 提取器
- Universe 提取器
- 第三方提取器（MS Office 2003、2007 和 PDF 文档）

有关可搜索文档类型的更多信息，请参阅“相关主题”中的“可搜索的内容类型”主题。

- 3 索引建立：索引建立体制通过第三方库（称为 Apache Lucene Engine）索引所有提取的内容。建立索引所需的时间变化不定，具体取决于系统中的对象数量，以及文档的大小和类型。

要使索引建立成功运行，以下服务器必须正在运行并且已启用：

- 输入文件资源库服务器（IFRS）
- 输出文件资源库服务器（OFRS）
- 中央管理服务器（CMS）
- 承载平台搜索服务的自适应处理服务（APS）。

如果选择的对象类型是 Web Intelligence 或 Crystal 报表，则必须为所选的各个对象类型运行和启用对应的 Web Intelligence 处理服务器或 Crystal Reports 应用程序服务器。

- 4 内容存储：内容存储包含从主索引中提取的信息，例如，ID、CUID、名称、类型和实例，其格式易于读取。这有助于加快搜索过程。

相关主题

- 第 688 页上的“[在 CMC 中配置应用程序属性](#)”
- 第 695 页上的“[可搜索的内容类型](#)”

22.3.2 索引建立失败列表

索引建立失败列表显示未能编入索引的文档列表。平台搜索提供三次对文档建立索引的机会。如果对文档建立索引失败，则在索引建立失败列表中列出该文档。

要查看索引建立失败列表，请按以下步骤操作：

- 1 转到 CMC 的“应用程序”区域。
- 2 选择“平台搜索应用程序”。
- 3 选择“操作”>“索引建立失败列表”。

将出现“平台搜索应用程序”对话框，其中显示包含以下详细信息的文档列表：

- 标题：显示未能建立索引的文档的标题。
- 类型：显示文档类型（如 Crystal 报表和 Web Intelligence）的名称和文档位置。
- 失败类型：显示错误代码及文档索引建立失败的原因。单击“更多”信息超级链接了解有关错误原因堆栈跟踪的更多信息。
- 最后尝试时间：显示最后一次尝试为文档建立索引的时戳。

22.3.3 搜索结果

22.3.3.1 搜索前

22.3.3.1.1 建议查询

使用平台搜索时，用户可以尝试查找特定问题的答案，而不是查找特定对象。BI 平台资源库中提供的报表中可能有这些问题的答案。

平台搜索会分析资源库中 Universe 的结构和现有报表，并将此信息与用户提供的搜索请求进行比较，以建议新的 SAP BusinessObjects Web Intelligence 查询，从而帮助用户找到解决其问题的方法。

为创建潜在报表，平台搜索会为维、度量、条件和过滤器值匹配所有 Universe 中的词。

平台搜索会在以下有关 Universe 或者现有 SAP BusinessObjects Web Intelligence 文档的信息中查找匹配项：

- Universe 中与搜索输入中的字词相匹配的度量。

在某个度量与搜索词之一匹配时，会在所产生的 Web intelligence 文档中使用该度量。

- Universe 中与搜索输入中的字词相匹配的维名称。

在某个维名称与搜索词之一匹配时，所产生的 Web Intelligence 文档会分解该维上的信息。

- 查询过滤器可用于聚焦文档中显示的数据。这些查询过滤器是通过分析搜索输入而生成的。
 - 如果某 Universe 条件的名称与搜索词之一匹配，则会将该条件用作过滤器。
 - 如果现有的 Web Intelligence 文档中包含名称与搜索词匹配的字段值，则会通过历史报表中具有匹配值的维来创建一个过滤器，并使用“等于”作为条件运算符。

如果平台搜索已找到了足够多的匹配项，以致于所产生的文档包含两个结果字段和一个过滤器，则查询会被视为准备运行。在这种情况下，用户可以单击以查看完成的报表。

如果 Universe 和文档之间的匹配项数量不足，则可以在运行之前编辑查询。

如果有多个 Universe 与搜索输入匹配，或者相同的字词出现在两个不同的匹配项中（例如在维名称中和作为过滤器值），则平台搜索会建议多个查询。

22.3.3.1.2 可搜索的内容类型

利用平台搜索可以搜索发布到 BI 平台的内容。下面列出了对象类型及其对应的索引内容：

对象类型	索引内容
Crystal 报表（2008 和 2011）	标题、说明、选择公式、已保存的数据、任何节中的文本字段、参数值和子报表。
Web Intelligence 文档	标题、说明、报表中使用的 Universe 过滤器的名称、保存的数据、报表中以本地方式定义的过滤器条件中的常量、报表中使用的 Universe 度量的名称、报表中使用的 Universe 对象的名称、记录集中的数据和单元格中的静态文本。
Microsoft Excel 文档（2003 和 2007）	<p>所有非空单元格中的数据、文档属性的“摘要”页面上的字段（标题、主题、作者、公司、类别、关键字和备注），以及文档页眉和页脚中的文本。</p> <p>对于使用计算或公式的单元格，可以搜索求值后的值。对于数字或日期/时间值，行数据是可搜索的。</p>

对象类型	索引内容
Microsoft Word 文档（2003 和 2007）	所有段落和表中的文本、文档属性的“摘要”页面上的字段（标题、主题、作者、公司、类别、关键字和备注）、文档页眉和页脚中的文本，以及数字文本。
RTF、PDF、PPT 和 TXT 文件	可以搜索这些文件中的所有文本。
LCMJob、AFDashboard Page、Dashboards、ObjectPackage、Web 服务查询（QaaWS）、配置文件、讨论区、InformationDesigner、SAP BusinessObjects BI 平台微件、MDAnalysis、发布、Flash、分析和超链接	元数据内容是可搜索的。
事件	<p>所有事件都是可搜索的，如自定义事件、系统事件、Crystal Reports 事件和监控事件。如果事件与源相关联，则平台搜索会将源和事件一同显现出来。</p> <p>注意： 平台搜索支持 Crystal Reports for Enterprise 的事件。</p>

对象类型	索引内容
BI 工作区	<ul style="list-style-type: none"> • 将为以下 BIW 模块的标题、说明和内容建立索引： <ul style="list-style-type: none"> • 文本模块 • Web 页模块 • 导航列表模块 • 查看器模块 • 复合模块的标题和说明将建立索引。 • 工作区模板模块只会为标题建立索引。 • 对于组模块，将为其中所含模块的标题和元数据建立索引。 • BI 工作区中 InfoObject 模块的标题、说明和 CUID 将建立索引。 <p>注意： 由于仅为嵌入式 InfoObject 模块的标题和说明建立索引，因此尝试搜索 InfoObject 内容时不会返回对嵌入模块的引用。例如，如果 CR 插入到 BI 工作区中，将为其标题和说明建立索引。搜索 CR 内容的任何尝试均不会返回对嵌入模块的引用。</p> <ul style="list-style-type: none"> • 如果 BI 工作区包含多个选项卡和子选项卡，还会为每个选项卡和子选项卡的标题和内容建立索引。
下一代 CR	<p>标题、说明、选择公式、已保存的数据、任何节中的文本字段、参数值和子报表。</p> <p>不支持下一代 CR 报表中的以下对象：</p> <ul style="list-style-type: none"> • 交叉表报表 • 统计图数据提取 • 图像和关联的元数据提取 • 嵌入式 OLE（例如，嵌入在 CR 中的 Word 文档） • Flash 对象提取 <p>此外，无法从下一代 CR 报表中逐页读取数据。</p>

对象类型	索引内容
Universe	<p>数据内容是可搜索的。</p> <p>注意：</p> <p>默认启用 Universe 索引建立选项。如果发现平台搜索用来建立 Universe 内容索引的查询运行缓慢，并且影响数据库服务器的性能，则建议在中央管理控制台（CMC）中禁用 Universe 索引建立选项。为 Universe 内容建立索引时平台搜索使用的查询示例：“Select distinct SampleColumnName from SampleTableName LIMIT 1000”（从 SampleTableName LIMIT 1000 中选择不同的 SampleColumnName）。</p> <p>按照以下步骤禁用 Universe 索引建立：</p> <ul style="list-style-type: none">。 1 登录到中央管理控制台（CMC）。。 2 选择“应用程序”。。 3 导航到平台搜索应用程序，选择“属性”。。 4 导航到内容类型，取消选中“Universe”。。 5 选择“保存并关闭”。

注意：

仅支持 15 MB 以内的第三方文档（MS Office 2003 和 2007 以及 PDF 文档）。

22.3.3.2 搜索

用户从 BI 启动板或任何其他使用平台搜索 SDK 的应用程序中搜索关键字时，会从主索引中查找搜索词。搜索引擎根据用户的查看权限仅显示用户有访问权限的文档。

22.3.3.3 搜索后

22.3.3.3.1 构面

通过将搜索结果分组为若干个类别或对象类型相似的若干个构面，并在为搜索词返回的结果中按类别出现的次数对其进行排名，平台搜索可细化搜索结果。利用构面可以导航到确切的结果。

平台搜索根据 InfoObject 元数据、文档元数据和文档内容生成构面。它只显示那些有两个以上文档与指定查询匹配的构面。构面根据与搜索查询匹配的文档动态显现，并按文档计数进行排序。

按照以下常见方面或类别对文档进行分组：

- 个人或公共（如 HR、公司和财务）：基于 BI 平台文档类别。
- 文档类型：基于文档类型，如 Web Intelligence、Crystal Reports、Microsoft Word（2003 和 2007）、Microsoft Excel（2003 和 2007）和 Dashboards。
- Universe 和连接：取决于内容源。
- 日期：包括上次刷新日期（年、季度和月）。
- 时间：包括上次刷新时间，如 24 小时和上周。
- 作者：创建文档的用户的名称。

22.3.3.3.2 规范化搜索结果排名

平台搜索会根据搜索到的词条位置对文档进行排名。它根据内容在文档中的出现位置将内容分组为以下类别：

- 。 1 平台元数据
- 。 2 文档元数据
- 。 3 内容元数据
- 。 4 内容

可以在 CMC 中为上述类别配置权重。

22.3.3.3.2.1 自定义用于排名搜索结果的权重

平台搜索功能允许基于内容在文档中出现的位置为按类别分组的内容设置权重，从而可以为所需类别设置较高的值以更快速地检索相关搜索结果。

要设置权重，请执行以下步骤：

- 1 在 CMC 的“管理”区域，单击“应用程序”。
- 2 打开“平台搜索应用程序”。
- 3 选择“排名”。

显示不同内容类别的权重，如平台元数据、文档元数据、内容元数据和内容。“用户区域设置”是在 BI 启动板首选项中的区域设置。

- 4 设置权重以满足要求。
- 5 单击“保存”。

在升级方案中，如果需要对已编制索引的文档进行排名，则需重新生成索引。有关更多信息，请参阅第 688 页上的 [“在 CMC 中配置应用程序属性”](#) 一节中关于重新建立索引的信息。

22.3.3.3.3 多语言支持

平台搜索提供多语言支持，这样就可以用所需语言建立内容的索引、检索搜索结果和获取建议。为了建立所有未本地化 BI 平台文档的索引，它使用 CMC 中“默认索引区域设置”的区域设置。

本地化信息对象后，平台搜索将使用相应语言分析器为文档建立索引。

搜索以设置为客户端的“产品区域设置”的区域设置为基础。平台搜索在检索搜索结果时会为客户端产品区域设置赋予更多权重。可以在 CMC 中配置权重。

22.3.3.3.4 建议

平台搜索会为拼写错误的搜索查询提供建议。如果原始搜索查询未输出任何结果，则平台搜索会根据已建立索引的内容建立最有可能的搜索词。

建议显示为带超链接的关键字。单击超级链接，以查看包含关键字（可能与原始查询相匹配）的文档列表。这些建议都是根据各种客观因素通过运算法则确定的。

如果有多个词与原始请求匹配，平台搜索会使用在 CMC 中设置为“默认索引区域设置”的语言提供前三项建议。

注意：

在下述情况下，平台搜索不会生成建议：

- 搜索查询包含三个以下字母
- 属性搜索，如类型：Crystal 报表
- Universe 元数据和内容
- 多字节语言，如中文、日语和韩语

22.3.3.3.5 联合 SAP BusinessObjects Explorer 中的搜索结果

平台搜索会联合来自 SAP BusinessObjects Explorer 和曲面信息空间以及 BI 平台内容的搜索请求。

SAP BusinessObjects Explorer 中的搜索结果按元数据类别进行分组。信息空间支持的构面包括类型、位置和刷新时间。

SAP BusinessObjects Explorer 为搜索查询中的每个搜索词将词频发送到平台搜索。平台搜索使用词频的平方根总和计算相关性。将生成的值作为匹配度分配给各个信息空间。然后，按匹配度对结果进行排序并发送到客户端。

22.4 平台搜索与 SAP NetWeaver Enterprise Search 相集成

SAP NetWeaver Enterprise Search 7.20 及更高版本可以使用基于 OpenSearch (RSS 和 ATOM) 的搜索服务。它可以将搜索请求委派给远程搜索服务提供者系统。在这种情况下，OpenSearch 是服务提供者，NetWeaver Enterprise Search 是搜索结果使用者，而 SAP BusinessObjects 平台搜索则为搜索服务提供者。

如果用户提交搜索请求，SAP NetWeaver Enterprise Search 会将该搜索请求直接转发给 OpenSearch 提供者。提供者将答复搜索请求，并将回答返回给 SAP NetWeaver Enterprise Search。然后，其与其他搜索对象连接器收到的结果合并，形成搜索结果并显示在用户界面中。

要集成 SAP NetWeaver Enterprise Search 和平台搜索，需要执行以下步骤：

- 。 1 在 SAP NetWeaver Enterprise Search 中创建连接器。
- 。 2 将用户角色导入到 BI 平台

22.4.1 在 SAP NetWeaver Enterprise Search 中创建连接器

可以使用 OpenSearch 类型的搜索对象连接器集成外部搜索提供者，这些提供者提供可通过 OpenSearch 使用的搜索功能。

要在 SAP NetWeaver Enterprise Search 中创建连接器，需要以下先决条件：

- 。 1 OpenSearch 说明服务 URL。
- 。 2 OpenSearch 说明服务的格式只能是 RSS 或 ATOM。

执行以下步骤，在 SAP NetWeaver Enterprise Search 中创建连接器：

- 1 启动管理主控室并选择“Create”（创建）。
- 2 选择 OpenSearch 作为搜索对象连接器类型。
- 3 选择“下一步”。
- 4 输入 OpenSearch 提供者的 OpenSearch 说明服务 URL。
- 5 选择下列任意身份验证设置，以启动说明服务 URL：
 - 无身份验证：不进行身份验证。
 - SAP 身份验证断言权证：此用户用于通过 SSO 的身份验证。
 - 用户/密码：预定义用户用于身份验证。
- 6 从 OpenSearch URL 设置中选择“Launch Search URL”（启动搜索 URL）。
然后对合适的搜索服务验证 OpenSearch 说明服务。系统自动输入搜索 URL 模板的值和相关说明。
- 7 选择下列任意身份验证设置以设置连接器：
 - 无身份验证：不进行身份验证。
 - SAP 身份验证断言权证：此用户用于通过 SSO 的身份验证。
 - 用户/密码：预定义用户用于身份验证。
- 8 选择“下一步”。
将出现汇总对话框，显示为此搜索对象连接器输入的值。
- 9 选择“Previous”（上一步）以修改设置，或者选择“Cancel”（取消）放弃所有输入的数据。
10. 选择“Finish”（完成）以保存设置。

22.4.2 将用户角色导入 BI 平台

执行以下步骤，以便将用户角色导入 BI 平台：

注意：

管理员必须知道用户详细信息、系统信息、应用程序主机信息和用户凭据。

- 1 转到 CMC 的“身份验证”区域。
- 2 选择“SAP”。
- 3 在“权利系统”选项卡上指定以下信息：
 - 系统
 - 客户端
 - 应用程序服务器
 - 系统编号
 - 用户名
 - 密码
 - 语言
- 4 选择“更新”。
- 5 选择“角色导入”选项卡并导入用户角色。
- 6 选择“更新”。
- 7 在 CMC 中选择“管理” > “用户安全性”，以分配适当的用户权限。

22.5 从 NetWeaver Enterprise Search 中搜索

要从 SAP NetWeaver Enterprise Search 中搜索结果，请执行以下步骤：

- 1 登录到 SAP NetWeaver Enterprise Search 应用程序。
- 2 选择“高级搜索”。
- 3 选择为平台搜索创建的连接器。
- 4 搜索关键字。

如果关键字存在匹配项，则该关键字的合并结果包含平台搜索中的结果。

22.6 审核

审核所有从使用平台搜索服务的客户端应用程序发送的搜索请求事件和搜索响应。对于平台搜索，审核将在服务级别实施。

平台搜索服务必须与客户端审核代理服务在同一服务器上运行才能发送审核事件。

平台搜索有一个事件类型 ID 1009 和四个平台搜索特定事件详细信息类型 ID:

- Keyword searched (ID: 19)
- Number of Search Results (ID: 63)
- Facet Search (ID: 20)
- Search Exception (ID: 1)

除以上详细信息外，还有一些标准事件详细信息，例如 sessionCuid 和 userCuid，它们在任何 BI 平台模块的任何审核中均受支持。

下面举例解释了审核在平台搜索中的工作原理。

如果搜索“销量”之类的关键字，搜索结果的总数可能是 5。在此情况下，将审核以下事件：

- 事件类型 ID 1009
- 事件详细信息类型 ID 19，带有“销量”值
- 事件详细信息类型 ID 63，带有值 5
- 会话 CUID
- 用户 CUID
- 状态，带有值 0，此值表示成功状态
- 开始时间
- 持续时间
- 对象 ID，带有值 0，原因是此事件是服务端审核

生成构面时，如果选择一个或多个构件，将审核以下事件：

- 事件类型 ID 1009
- 事件详细信息类型 ID 19，带有“销量”值
- 事件详细信息类型 ID 63，带有值 5
- 事件详细信息类型 ID 20，带有逗号分隔的构面串
- 会话 CUID
- 用户 CUID
- 状态，带有值 0，此值表示成功状态
- 开始时间
- 持续时间
- 对象 ID，带有值 0，原因是此服务是服务端审核

如果由于某个无效条目（例如，“*a”）而导致搜索异常，将审核以下事件详细信息：

- 事件类型 ID 1009
- 事件详细信息类型 ID 19，带有“销量”值
- 事件详细信息类型 ID 63，带有值 0
- 事件详细信息类型 ID 1，带有异常消息
- 会话 CUID
- 用户 CUID
- 状态，带有值 1，此值表示失败状态
- 开始时间
- 持续时间

- 对象 ID，带有值 0，原因是此服务是服务端审核

22.7 疑难解答

22.7.1 自我康复

平台搜索有自己的自我康复机制。它会持续监控搜索服务的内存使用情况。当内存使用情况超出阈值时，则自动停止索引建立。当内存使用情况回落到合理限值后，则自动启动。不过，用户在此过程中可以继续搜索，但在特定时间段内不能建立索引。默认情况下，平台搜索会根据文档类型配置任何时候均可建立索引的文档的数量。基于 CPU 和内存等系统资源开始建立索引。

22.7.2 问题方案

本节提供针对使用平台搜索检索搜索结果时可能发生的各种问题的分步解决方法。

无法从包含关键词的新添加文档中检索搜索结果

- 检查平台搜索是否支持所提交文档的文档类型。如果不支持文档类型，则不会为文档建立索引。

有关受支持文档类型的更多信息，请参阅下面列出的相关主题可搜索内容类型。

- 检查是否为“爬网频率”选择了该选项。如果将“爬网频率”设置为“持续爬网”，则立即选取文档建立索引。如果将“爬网频率”设置为“计划的爬网”，则仅在计划的时间周期建立索引。

有关爬网频率的更多信息，请参阅下面列出的相关主题配置应用程序属性。

- 检查索引建立失败列表，以验证是否为文档成功建立了索引。如果此列表中显示该文档，则需要对其进行修改并重新提交，以便平台搜索使用该文档建立索引。

注意：

通过添加或删除某个字段，然后再次保存该字段，您可以修改文档。这会在 BI 平台资源库中更新文档的时间戳，并开始重新为该文档建立索引。

有关索引建立失败的文档的更多信息，请参阅下面列出的相关主题索引建立失败列表。

- 检查自适应处理服务器跟踪日志中包含的有关索引建立失败的信息。
- 。 1 转到安装目录\SAP BusinessObjects Enterprise XI 4.0\logging\ 目录，其中包含具有 .glf 扩展名的 APS 跟踪日志。
- 。 2 打开跟踪日志文件并搜索需要为其建立索引的文档 SI_ID。

注意：

可以从文档属性中找到文档 SI_ID。

无法检索 Crystal Reports 文档

平台搜索仅针对版本 2008 和 2011 为 Crystal Reports 内容建立索引。它不会为 Crystal Reports for Enterprise 建立内容索引。

但对于 Crystal Reports for Enterprise，可以搜索属于文档属性的文档元数据，如标题、说明和关键词。

如果文档包含可建立索引的内容，则需要按照上述章节 无法从包含关键字的新添加文档中检索搜索结果中列出的步骤执行相同的过程。

无法检索 SAP BusinessObjects Explorer 信息空间

检查 SAP BusinessObjects Explorer 服务器是停止了还是禁用了。为平台搜索启用服务器，以对 SAP BusinessObjects Explorer 的搜索结果进行检索。

SAP NetWeaver Enterprise Search 无法在 BI 平台资源库中检索结果。

- 检查平台搜索是否使用 BI 启动板检索搜索结果，以确定问题是否是由平台搜索和 SAP NetWeaver Enterprise Search 的集成所造成的。
- 检查是否在 Web 应用程序服务器上正确部署了 OpenSearch。用于验证 OpenSearch 部署的具体步骤取决于所用 Web 应用程序服务器的类型。
- 检查是否在 SAP NetWeaver Enterprise Search 配置中正确创建或配置了连接器。需要对 SAP NetWeaver Enterprise Search 使用正确的连接器，以联合平台搜索的结果。
- 检查分别运行 SAP NetWeaver Enterprise Search 和 BI 平台资源库的计算机之间的通信是否正确。如果分布式环境中出现任何网络问题，则 SAP NetWeaver Enterprise Search 可能会无法联合结果。
- 检查添加到 BI 平台的 SAP NetWeaver Enterprise Search 用户是否具有适当的权限。要验证用户的权限，请转到 CMC 的“身份验证”区域，并选择“SAP”。

相关主题

- 第 693 页上的[“索引建立失败列表”](#)
- 第 688 页上的[“在 CMC 中配置应用程序属性”](#)
- 第 695 页上的[“可搜索的内容类型”](#)

第 23 章 联盟

23.1 联盟

联盟是一种跨站点复制工具，可以在全局环境中处理多个 BI 平台部署。

可以从一个 BI 平台部署中创建和管理内容，并按重复性计划跨地理地点将内容复制到其他 BI 平台部署。用户既可以完成单向复制作业，也可以完成双向复制作业。

用户能够进行如下操作，从而从联盟中获得好处：

- 减少网络通信量
- 从一个位置创建和管理内容
- 提高最终用户的性能

在使用联盟复制内容时，用户能够：

- 简化多个部署的管理需要
- 为跨国公司在各地的机构提供一致的权限策略
- 更快地获取信息并在数据所在的远程站点处理报表
- 通过更快地检索本地和分散的数据，从而节省时间
- 同步多个部署中的内容，而无需编写自定义代码

联盟允许用户拥有单独的安全模型、生命周期、测试和部署次数，以及不同的业务所有者和管理员。例如，可以委派限制销售应用程序管理员更改人力资源应用程序的管理功能。

可以利用联盟复制各种各样的对象，如下表中所述。

类别	可复制的对象类型	其他注释
业务视图	业务视图管理器、DataConnection、LOV、数据基础等	支持所有对象（尽管在个别级别不受支持）。
报表	Crystal 报表、Web Intelligence 和 Dashboard Design	支持 Full Client 加载项和模板。
第三方对象	Excel、PDF、PowerPoint、Flash、Word、文本、多信息文本和 Shockwave Flash 文件	
用户	用户、组、收件箱、收藏夹和个人类别	
Business Intelligence 平台	文件夹、事件、类别、日历、访问级别、超级链接、快捷方式、程序、配置文件、对象包、第三方	
Universe	Universe、连接和 Universe 限制	

以下方案重点介绍组织如何能够使用联盟的两个示例。

方案 1：零售（集中式设计）

ACME 商店想要使用单向复制方法将月销售报表发送到不同的商店位置。源站点的管理员创建一个报表，每个目标站点的管理员将复制该报表，并依据商店的数据库运行该报表。

提示：

可以将保留每个对象的复制信息的本地化实例发送回源站点。例如，它将应用相应的徽标、数据库连接信息等。

方案 2：远程计划（分布式访问）

数据位于源站点。待定复制作业将发送到源站点运行。完成的复制作业随后将发送回目标站点以供查看。例如，目标站点上可能没有报表数据，但用户可以将报表设置为在源站点上运行，然后再将完成的报表发送回目标站点。

23.2 联盟术语

以下术语表介绍与联盟相关的词语，并且可以为其导航和使用提供帮助。

BI 应用程序

相关的商务智能（BI）内容的逻辑分组，具有特定的用途，面向特定的用户。BI 应用程序不是对象。一个 BI 平台部署可以承载多个 BI 应用程序，每个应用程序都可以有独立的安全模型、生命周期、测试和部署时间安排，以及独立的业务所有者和管理员。

单向复制

仅按一个方向复制对象：从源站点到目标站点。在目标站点所做的任何更新保留在该目标站点上。

双向复制

与单向复制的行为相同，但双向复制还将沿着两个方向发送所做的更改。对源站点所做的更新被复制到每个目标站点。目标站点上的更新和新对象被发送到源站点。

复制

在 BI 平台系统之间复制内容的过程。

复制作业

一个对象，其中包含有关复制计划、要复制的内容以及复制内容时应满足的任何特殊条件的信息。

复制列表

要复制的对象的列表。复制列表涉及 BI 平台部署中将被一起复制的其他内容，如用户、组和报表等。

复制刷新

刷新复制列表中的所有对象，而不管上次修改的版本。

复制包

复制包创建于传输过程中，其中包含复制作业中的对象。它可以包含所有在复制列表中定义的对象，就像在快速变化的环境或初始复制的情况下一样。或者，如果对象与复制作业的计划相比并不频繁更改，则复制包可以包含复制列表的一个子集。复制包作为一个 BI 应用程序资源（BIAR）文件实施。

复制对象

从源站点复制到目标站点的对象。目标站点上所有复制的对象将标有复制图标。如果存在冲突，则以冲突图标标记对象。

多个源站点

多个站点可作为一个源站点。例如，多个开发中心通常具有多个源站点。不过，每次复制只能有一个源站点。

本地

连接用户或管理员的本地系统。例如，目标站点的管理员对目标站点而言被视为本地。

本地运行的已完成实例

在目标站点上处理并随即发送回源站点的实例。

源站点

内容所源自的 BI 平台系统：

目标站点

从源站点拉取复制 BI 平台内容的 BI 平台系统

远程

一个非用户本地系统的系统。例如，源站点对目标站点的用户和管理员而言被视为远程。

远程计划

从目标站点发送到源站点的计划请求。可以远程对目标站点上的报表进行计划，这样就可以将报表实例发回到源站点中进行处理。然后将完成的实例返回到目标站点。

远程连接

包含用于连接到BI 平台部署的信息的对象，这些信息包括用户名和密码、CMS 名称、WebService URI 和清除选项。

23.3 管理安全权限

由于联盟在独立的部署之间复制内容，并且需要与其他管理员进行协作，因此，在开始使用联盟之前，必须了解安全设置。

各独立部署中的管理员必须互相配合才能启用联盟功能。复制内容后，管理员可以对其进行更改。

为完成某些任务对源部署和目标部署所需的特定权限：

- 在源站点上所需的权限
- 在目标站点上所需的权限
- 对联盟特定对象所需的权限
- 联盟方案

提示：

在启用联盟之前，建议阅读本章内容。

23.3.1 在源站点上所需的权限

本节说明对源站点执行的操作，以及连接到源站点的用户帐户的必需权限。此帐户是在目标站点上的远程连接对象中输入的帐户。

操作	说明	所需的权限
单向复制	只从源站点向目标站点执行复制。 注意： 需要具有对所有复制的对象（包括依赖项计算自动复制的对象）的查看和复制权限。	<ul style="list-style-type: none">要复制的所有对象的查看和复制权限对复制列表的查看权限
双向复制	执行从源站点到目标站点的复制，然后执行从目标站点到源站点的复制。	<ul style="list-style-type: none">要复制的所有对象的查看和复制权限对复制列表的查看权限用户对象的修改权限权限，用于复制任何密码更改
计划	允许基于目标站点在源站点上执行远程计划。	<ul style="list-style-type: none">针对要远程计划的所有对象的“计划”权限

相关主题

- 第 711 页上的“[在目标站点上所需的权限](#)”

23.3.2 在目标站点上所需的权限

本节说明对目标站点应用的操作，以及运行复制作业的用户帐户的必需权限。此帐户是创建复制作业的用户的帐户。

注意：

与其他可计划的对象一样，可以代表其他人计划复制作业。

操作	说明	所需的权限
所有对象	复制对象（无论是单向复制还是双向复制）。	<ul style="list-style-type: none">所有对象的查看、添加、编辑和修改权限权限修改用户密码权限，适用所有用户对象
初次复制	第一次运行复制作业时，目标站点上不存在任何对象。因此，运行复制作业的用户帐户必须对将在其中添加内容的所有顶层文件夹以及对象具有权限。	<ul style="list-style-type: none">对所有顶层文件夹和默认对象的查看、添加、编辑和修改权限权限

相关主题

- 第 710 页上的“[在源站点上所需的权限](#)”

23.3.3 联盟特定的权限

本节详细介绍联盟特定的方案。

操作	说明	所需的权限
对象清除	对象清除删除目标站点上的对象。	<ul style="list-style-type: none"> 用于运行复制作业的帐户需要对可能要删除的所有对象具有删除权限。
禁用某些对象的清除	<p>从源站点中复制某些对象后，在源站点中删除了这些对象的情况下，可能不希望从目标站点中删除这些对象。可以通过权限预防在目标站点上删除这些对象。例如，当目标站点上的用户独立于源站点上的用户开始使用某个对象时，则可以选择此选项。</p> <p>例如，如果目标站点上的用户使用某个复制的 Universe 创建他们自己的本地报表，在从源站点中删除了该 Universe 的情况下，您可能不希望在目标站点中丢失该 Universe。</p>	<ul style="list-style-type: none"> 否定运行复制作业的用户帐户对要保留的对象的删除权限。
在源站点上不做任何修改的双向复制	<p>在某些情况下，可能会选择双向复制，但不希望修改源站点上的某些对象，即使在目标站点上更改了这些对象。这样做的原因有：对象较特殊，仅应由用户在源站点上更改；希望启用远程计划，但不希望所做的更改传播回去。</p> <p>注意：</p> <p>对于远程计划，可以创建一个仅处理远程计划对象的作业。但在这种情况下，仍将复制祖先对象，包括报表、包含报表的文件夹和该文件夹的父文件夹。在目标站点上所做的任何更改都会复制到源站点，而在源站点上所做的更改也会复制到目标站点。</p>	<ul style="list-style-type: none"> 否定用于连接的用户帐户对远程连接对象的编辑权限。

23.3.4 复制对象的安全性

要保留对象的安全权限，必须同时复制对象及其用户或组。否则，这些对象必须已在要复制到的站点上存在，而且在每个站点上都要有相同的唯一标识符（CUID）。

如果复制对象而不复制用户或组，或者对象在要复制到的站点上已不存在，则将会删除对象的权限。

示例：

为组 A 和组 B 分配了对对象 A 的权限。组 A 具有查看权限，组 B 具有拒绝查看权限。如果复制作业仅复制组 A 和对象 A，则在目标站点上对象 A 将只对与其关联的组 A 拥有“查看”权限。

复制对象时，如果未复制所有组以及对对象的显式权限，则具有潜在的安全风险。上例突显出一个潜在的风险。如果用户 A 既属于组 A 又属于组 B，则该用户将无权查看源站点上的对象 A。但是，用户 A 将被复制到目标站点，因为此用户同时属于这两个组。在复制到目标站点之后，因为未复制组 B，所以用户 A 将有权查看目标站点上的对象 A，但无法查看源站点上的对象 A。

引用未包括在复制作业中或尚未存在于目标站点上的其他对象的对象将显示在一个日志文件中。该日志文件指明，该对象引用了未经复制的对象并丢弃了该引用。

为特定用户或组仅将对象的安全性从源站点复制到目标站点。可以在目标站点上设置所复制对象的安全性，但这些设置不会复制到源站点。

23.3.5 复制使用访问级别的安全设置

为了保持一致，权限必须按访问级别定义。必须同时复制对象、用户或组和访问级别，或者，这些内容必须已在要复制到的站点上存在。

如果对象为某用户或组分配未包含在复制作业中或尚未存在于目标站点上的显式权限，则在日志文件中将显示该对象，其中表明该对象分配了未进行复制的权限，这些权限已被丢弃。

此外，可以选择自动复制用于导入的对象的访问级别。在复制列表上可以使用此选项。

注意：

不会复制默认访问级别，但会保持引用。

23.4 复制类型和模式选项

取决于所选择的复制类型和复制模式，可以选择创建以下四种不同的复制作业之一：

- 单向复制
- 双向复制
- 从源刷新
- 从目标刷新

23.4.1 单向复制

通过单向复制，可以仅按一个方向复制内容，即从源站点到目标站点。对复制列表中位于源站点上的对象所做的任何更改均被发送到目标站点。但是，对目标站点上的对象所做的更改不会发送回源站点。

单向复制对于以下部署是理想之选：部署了一个中央 BI 平台，可在其中创建、修改和管理对象。其他部署使用中央部署的内容。

要创建单向复制，请选择以下选项：

- 复制类型 = 单向复制
- 复制模式 = 正常复制

23.4.2 双向复制

通过双向复制，可以在源站点和目标站点之间双向复制内容。在复制过程中，对源站点上的对象所做的任何更改会复制到目标站点，而在目标站点上所做的更改会复制到源站点。

注意：

要执行远程计划和将本地运行的实例复制回源站点，必须选择双向复制模式。

如果有多个 BI 平台部署，而且在这些部署中的源和目标站点上创建、修改、管理和使用内容，则双向复制最为高效。它还帮助同步多个部署。

要创建双向复制，请选择以下选项：

- 复制类型 = 双向复制
- 复制模式 = 正常复制

相关主题

- 第 738 页上的“[远程计划和本地运行的实例](#)”

23.4.3 从源刷新或从目标刷新

在单向或双向复制模式中复制内容时，复制列表上的对象被复制到目标站点。但是，在每次运行复制作业时并非可以复制所有对象。

联盟具有一个优化引擎，用于帮助更快完成复制作业。它使用对象的版本和时间戳的组合来确定自上次复制以来是否修改了对象。此项检查是针对在复制列表中明确选择的对象以及在依赖项检查过程中复制的所有对象而执行的。

但是，在某些情况下，优化引擎可能会漏掉一些对象，因此将不会复制这些对象。在这些情况下，可以使用“从源刷新”和“从目标刷新”，以便不考虑时间戳强制复制作业复制内容及其依赖项。

“从源刷新”只将内容从源站点发送到目标站点。“从目标刷新”只将内容从目标站点发送到源站点。

示例：

下面三个示例介绍了使用“从源刷新”和“从目标刷新”的情况，其中某些对象将由于优化而缺失。

第 1 种情况：将包含其他对象的对象添加到正在复制的区域。

源站点中的文件夹 A 被复制到目标站点。现在该文件夹存在于源站点和目标站点中。某个用户在源站点上将包含报表 B 的文件夹 B 移动或复制到文件夹 A 中。在下次复制过程中，联盟将会发现文件夹 B 的时间戳已经发生了更改，并将将该文件夹复制到目标站点中。但是，报表 B 的时间戳未发生更改。因此，常规的单向或双向复制作业将漏掉报表 B。

为了确保正确复制文件夹 B 的内容，应该使用一次“从源刷新”复制作业。此后，常规的单向或双向复制作业将正确复制文件夹 B 的内容。如果此示例中的情况相反，即在目标站点上移动或复制文件夹 B，则使用“从目标刷新”。

第 2 种情况：使用生命周期管理器或 BIAR 命令行添加新对象。

使用生命周期管理器或 BIAR 命令行将对象添加到所复制的区域中时，常规的单向或双向复制作业可能不会选取对象。之所以发生这种现象，是因为在使用生命周期管理器或 BIAR 命令行时，源系统和目标系统上的内部时钟可能不同步。

注意：

建议在源站点上将新对象导入到所复制的区域中之后运行“从源刷新”复制作业。建议在目标站点上将新对象导入到所复制的区域中之后运行“从目标刷新”复制作业。

第 3 种情况：在计划的复制时间之间进行操作。

如果将对象添加到所复制的区域中，但是无法等到下一个计划复制时间，则可以使用“从源刷新”和“从目标刷新”复制作业。通过选择已向其中添加对象的区域，可以快速复制内容。

注意：

- 这种情况对于大型复制列表而言可能代价高昂，因此，建议不要经常使用此选项。例如，不必创建复制作业以按照小时计划采用从源刷新或从目标刷新模式进行刷新。应在立即运行或不频繁执行的计划中使用这两个模式。
- 在某些情况下无法使用冲突解决方案，其中包括：从源刷新（“目标站点优先”选项被锁定）或从目标刷新（“源站点优先”选项被锁定）。

23.5 复制第三方用户和组

在联盟中，可以复制第三方用户和组，具体来说就是 Active Directory (AD) 以及 LDAP 用户和组。

提示：

如果计划复制这些类型的用户和组或其个人内容（如收藏夹文件夹或收件箱），请阅读本节。

映射用户和组

- 1 在源站点上映射用户和组，以便联盟正确复制它们。
- 2 将映射的用户和组复制到目标站点。

注意：

不要在目标站点上单独映射组和用户。如果这样做，它们在目标站点和源站点上将具有不同的唯一标识符（CUID），因此联盟功能将无法匹配用户或组。

示例：

管理员在源站点和目标站点上映射组 A 与用户 A。组 A 和用户 A 在源站点和目标站点上具有不同的唯一标识符。在复制过程中，联盟功能无法对它们进行匹配，组 A 或用户 A 因别名冲突而不会被复制。

注意：

- 在复制第三方用户和组之前，必须将目标站点设置为使用 AD 或 LDAP 身份验证。但是，还必须将目标站点配置为使用 AD 或 LDAP，以便它可以与目录服务器或域控制器进行通信。
- 首次复制 AD 或 LDAP 组后，此组中的用户将无法在刷新 AD/LDAP 组图形之前登录。大约每 15 分钟将自动发生一次此操作。要手动刷新 AD/LDAP 组图形，请转到 CMC 的“身份验证”页，双击“Windows AD”或“LDAP”，然后单击“更新”。
- 请小心复制第三方组。将新用户添加到目录服务器中的组时，他们将可以登录到这两个站点。AD 或 LDAP 身份验证的此安全性问题与联盟无关。

如果分别登录到目标站点和源站点，或使用 CMC 身份验证页上的更新按钮在这两个站点上更新组成员资格，则会在这两个站点上创建用户帐户。这些帐户将具有不同的唯一标识符，因此联盟将无法正确复制它们。

注意：

请务必在一个站点上创建帐户，然后将其复制到另一个站点。

23.6 复制 Universe 和 Universe 连接

使用联盟在各个 BI 平台部署间复制 Universe 时，提前做好计划非常重要。Universe 对象在没有基础 Universe 连接的情况下无法正常工作。

Universe 连接对象包含连接到报表数据库所需的信息。要正常工作，Universe 连接对象必须包含有效信息并允许建立数据库连接。

注意：

如果正使用双向复制，并且在含 Universe 连接的情况下将 Universe 从源站点复制到目标站点，则在后续复制中，可能会将原站点上原站点的 Universe 与 Universe 连接之间的关系覆盖或移除掉。为了避免发生这种情况，请始终随 Universe 一起复制 Universe 连接。

要确保随 Universe 一同复制从属的 Universe 连接，在创建或修改含有 Universe 的复制列表时，请始终选择以下选项：

- 包括选定 Universe 使用的连接
- 包括选定 Universe 需要的 Universe

注意：

如果覆盖或删除了 Universe 与其 Universe 连接之间的关系，请在 Universe Designer 中打开 Universe，在“文件” > “参数”下面，修改连接信息。

以下两个示例演示了复制 Universe 及其相关 Universe 连接的过程。

示例：

当复制 Universes 和 Universe 连接时，必须确保源站点上的连接环境与目标站点上的连接环境相匹配。

例如，如果 Universe 连接使用一个名为 TestODBC 的 ODBC 连接，则目标环境中需要具有一个名为 TestODBC 的正确配置的 ODBC 连接。ODBC 连接可以解析到相同数据库或不同数据库。为了确保使用此连接的 Universe 不会遇到连接问题，数据库的模式必须相同。

示例：

如果希望目标站点上复制的 Universe 所使用的数据库与源站点上 Universe 使用的不同，请复制 Universe 连接，但要使目标站点上的连接信息指向需要的数据库。

例如，如果源站点上的 Universe 连接使用名为“测试”且指向 DatabaseA 的 ODBC 连接，请确保目标站点上也具有名为“测试”的 ODBC 连接，但连接指向 DatabaseB 。

23.7 管理复制列表

复制列表包括 BI 平台部署中的用户、组和报表等可以一起复制的内容。可从 CMC 访问复制列表。

下表说明了可以复制的内容类型。

类别	支持的对象
资源库对象	包括业务视图、数据连接、LOV、数据基础等的对象。 注意： 支持所有对象（尽管在个别级别不受支持）。
报表	Crystal 报表、Web Intelligence 文档和 Dashboards 对象。 注意： 支持 Full Client 加载项和模板。
第三方对象	Excel、PDF、PowerPoint、Flash、Word、文本文件、多信息文本文件、Shockwave Flash 文件。
用户	用户、组、收件箱、收藏夹、个人类别。
Business Intelligence 平台	文件夹、事件、类别、日历、自定义角色、超级链接、快捷方式、程序、配置文件、对象包、第三方。
Universe	Universe、连接、Universe 限制。

注意：

必须在源站点上创建以下对象，然后将其复制到目标站点。如果在目标站点上创建这些对象然后将它们复制到源站点，这些对象在源站点上将不起作用。

- 业务视图
- 业务元素
- 数据基础
- 数据连接
- 值列表
- Universe 过载

23.7.1 创建复制列表

复制列表位于 CMC 的复制列表区域。可以在创建的文件夹和子文件夹中安排复制列表。

23.7.1.1 创建复制列表文件夹

- 1 转到 CMC 的“复制列表”区域。
- 2 单击“复制列表”。
- 3 单击“管理” > “新建” > “文件夹”。
将出现“创建文件夹”对话框。
- 4 键入文件夹名称，然后单击“确定”。
此时便可在此文件夹中创建复制列表。

23.7.1.2 创建复制列表

- 1 转到 CMC 的“复制列表”区域。
- 2 选择要用于保存新复制列表的文件夹。
- 3 单击“管理” > “新建” > “新建复制列表”。
将出现“新建复制列表”对话框。
- 4 键入复制列表的标题和说明。
- 5 要查看高级选项，单击“复制列表属性”链接。
这允许用户指定将哪些依赖项从源站点自动复制到目标站点。
- 6 按下表中所述选择所需的选项。

依赖项对象选项	定义
包括选定的用户的个人文件夹	复制所选用户的个人文件夹及文件夹内容。
包括选定的用户的个人类别	复制所选用户的个人类别。
包括选定的报表的 Universe	复制所选报表对象依赖的所有 Universe。
包括选定的用户组的成员	复制所选组内的用户。
包括选定的 Universe 所需的 Universe	复制依赖其他 Universe 的所有 Universe。
包括选定的用户的收件箱	复制所选用户的收件箱及收件箱内容。

依赖项对象选项	定义
包括选定的 Universe 的用户组	复制与 Universe 限制关联的用户组。
包括选定的对象的访问级别集合	复制用于任何所选对象的所有访问级别。
包括选定的类别的文档	复制包含在所选类别中的所有文档（包括 Word、Excel 和 PDF）。
包括选定的 Flash 对象的受支持依赖项	复制 Flash 对象依赖的所有 Crystal 报表、超级链接、Web Intelligence 文档或 Universe。
包括选定的用户和用户组的配置文件	复制与所选用户或组关联的所有配置文件。
包括选定的 Universe 所使用的连接	复制所选对象使用的所有 Universe 连接对象。

注意：

BI 平台中的某些对象依赖于其他对象。例如：Web Intelligence 文档依赖于其结构和内容等的基础 Universe。如果复制 Web Intelligence 文档，但不选择该报表所使用的 Universe，则在目标站点上将无法执行复制作业，除非已在该站点上复制了该 Universe。但是，如果启用“包含选定报表的 Universe”，则联盟将自动复制该报表所依赖的 Universe。

7. 单击“下一步”。
8. 选择要添加到复制列表的一个或多个对象。
 - 使用箭头按钮添加或删除“可用对象”文件夹中的对象。
 - 或者，单击“全部复制”下的“资源库对象”复制所有业务视图、业务元素、数据基础、数据连接、值列表以及资源库对象（包括报表图像和函数）。

注意：

无法复制位于可用对象文件夹下的顶层文件夹。

9. 单击“保存并关闭”。

23.7.2 修改复制列表

创建复制列表后，可以修改其属性或对象。

23.7.2.1 修改复制列表中的属性

- 1 转到 CMC 的“复制列表”区域。
- 2 选择要修改的“复制列表”。
- 3 单击“管理” > “属性”。
将出现“常规属性”对话框。
- 4 修改标题和说明也可以在“常规属性”对话框打开时修改复制列表的其他区域。
- 5 如果要修改依赖项选项，请在导航列表上单击“复制列表属性”。
- 6 单击“保存并关闭”。

相关主题

- 第 719 页上的“[创建复制列表](#)”

23.7.2.2 修改复制列表中的对象

- 1 转到 CMC 的“复制列表”区域。
- 2 选择“复制列表”。
- 3 单击“操作” > “管理复制列表”。
将出现“管理复制列表”对话框，其中显示复制列表包含的对象的列表。
- 4 根据需要添加或删除对象。
- 5 单击“保存并关闭”。

相关主题

- 第 719 页上的“[创建复制列表](#)”

23.8 管理远程连接

远程连接对象包含连接到远程 BI 平台部署所需的信息。

注意：

远程连接对象是在目标站点 BI 平台部署中创建的。远程连接为源站点。

可在 CMC 的“联盟”区域中查看远程连接。

23.8.1 创建远程连接

联盟中的远程连接将连接到远程 BI 平台部署。要建立与要复制的内容所在的源站点的连接，首先必须在目标站点上创建一个远程连接。

可以创建文件夹和子文件夹以用于安排各远程连接。

23.8.1.1 创建远程连接文件夹

- 1 转到 CMC 的“联盟”区域。
- 2 单击“远程连接”。
- 3 单击“管理” > “新建” > “文件夹”。
将出现“创建文件夹”对话框。
- 4 键入文件夹名称，然后单击“确定”。
此时便可在此文件夹中建立远程连接。

23.8.1.2 创建远程连接

要连接到远程 BI 平台部署，必须在联盟中创建一个远程连接。

- 1 转到 CMC 的“联盟”区域。
- 2 单击“远程连接”。
- 3 单击“管理” > “新建” > “新建远程连接”。
将出现“新建远程系统连接”对话框。

4 根据需要输入标题、说明和相关字段：

注意：

除了“说明”和“将清除对象的数量限制为：”之外，其他所有字段都是必填字段。

字段	说明
标题	远程连接对象的名称。
说明	远程连接对象的说明。（可选）
远程系统 Web 服务 URI	在 Java 应用程序服务器上自动部署的联盟 Web 服务的 URL。可以在 BI 平台中使用任何联盟 Web 服务，无论它们是源站点、目标站点还是另一个部署。请使用以下格式： http://应用程序服务器的计算机名称:端口/dswsbobje。 示例：http://mymachine.mydomain.com:8080/dswsbobje
远程系统 CMS	要连接到的 CMS（可通过联盟 Web 服务访问）的名称。它将被视为源站点的 CMS。格式为：CMS 名称:端口。 示例：mymachine:6400 注意： 如果正在使用默认端口 6400，则指定端口是可选步骤。
用户名	用于连接到源站点的用户名。 注意： 请确保正在使用的用户名对源站点部署中的复制列表具有查看权限。
密码	用于连接到源站点的用户帐户的密码。
身份验证	用于连接到源站点的帐户身份验证的类型。选项包括：Enterprise、AD 或 LDAP。
清除频率（以小时计）	使用此远程连接对象的复制作业执行对象清除的频率。请仅输入正整数。单位为小时。默认值为 24。
将清除对象的数量限制为	复制作业所清除的对象数量。（可选）

5 单击“确定”。

相关主题

- 第 730 页上的[“管理对象清除”](#)

23.8.2 修改远程连接

创建远程连接后，可以修改其属性和安全选项。

要修改远程连接，请执行以下步骤：

- 1 转到 CMC 的“联盟”区域。
- 2 单击“远程连接”。
- 3 双击想要修改的远程连接。

将出现“远程连接属性”对话框。可以修改以下属性：



- 标题
- 说明
- 远程系统 Web 服务 URI
- 远程系统 CMS
- 用户名
- 密码
- 身份验证
- 清除频率（以小时计）
- 将清除对象的数量限制为

- 4 指定更改。
- 5 单击“保存并关闭”。

23.9 管理复制作业

复制作业是按计划运行的一种对象，用于在联盟中的两个 BI 平台部署之间复制内容。

注意：

目标站点上的已复制对象将标有如下所示的复制图标： 如果存在冲突，对象将标有如下所示的冲突图标：

可以在 CMC 的“联盟”区域中的“远程连接”文件夹中查看复制作业列表。

23.9.1 创建复制作业

在联盟中的两个 BI 平台部署间复制内容需要使用复制作业。每个复制作业只能有一个远程连接和一个关联的复制列表。

23.9.1.1 创建复制作业

- 1 转到 CMC 的“联盟”区域。
- 2 单击“远程连接”。
- 3 选择“远程连接”以包含新的复制作业。

警告：

CMC 必须能够连接到远程连接 URI 中的 Web 服务，才能继续使用向导。

- 4 单击“管理” > “新建” > “新建复制作业”。
- 将出现“新建复制作业”对话框。
- 5 键入该复制作业的标题和说明。
- 6 单击“下一步”。
- 将出现源站点上可用“复制列表”的列表。
- 7 选择想要用于复制作业的“复制列表”。
- 8 单击“下一步”。
- 9 按下表所述选择配置选项。

选项	说明
在目标上启用对象清除	<p>在删除了源站点上的源对象的情况下，强制复制作业删除目标站点上的所有已复制对象。</p> <p>注意： 对象清除不会删除使用依赖项复制的对象或在复制列表中选定的对象。</p>
单向复制	指定仅从源站点向目标站点复制对象。复制后对源站点上的对象所做的任何更改都将被复制到目标站点，但是，在目标站点上所做的更改不会被复制回源站点。
双向复制	指定双向复制对象；即从源站点复制到目标站点，以及从目标站点复制到源站点。复制后对一个站点上的这些对象所做的更改将被自动复制到另一个站点。
源站点优先	指定在检测到源站点上的对象与该对象在目标站点上的复制版本之间发生冲突时，源站点上的版本优先。
无自动冲突解决	指定不采取任何操作来解决所检测到的任何冲突。
目标站点优先（仅可用于双向复制）	指定在检测到源站点上的对象与该对象在目标站点上的复制版本之间发生冲突时，目标站点上的版本优先。
正常复制	指定复制作业以正常方式执行。
从源刷新	将所有内容从源站点复制到目标站点，而不管内容是否已更改。可以复制整个复制列表，也可以只复制该列表的一部分。
从目标刷新（仅可用于双向复制）	将所有内容从目标站点复制到源站点，而不管内容是否已更改。可以复制整个复制列表，也可以只复制该列表的一部分。
复制所有对象（仅对于双向复制可见）	<p>复制整个复制列表。</p> <p>注意： 这是最完整的选项，但是执行该操作所需的时间最长。</p>
复制远程计划（仅对于双向复制可见）	将待定远程实例从目标站点复制到源站点，并将完成的实例从源站点强制复制到目标站点。
复制文档模板	复制不是实例的所有对象（本地运行或为远程计划选中的报表）。这包括用户、组、文件夹和报表等。
复制本地运行的已完成实例	仅将已完成实例从目标站点复制到源站点。

10. 单击“确定”。

相关主题

- 第 730 页上的[“管理对象清除”](#)
- 第 732 页上的[“管理冲突检测和解决”](#)
- 第 738 页上的[“远程计划和本地运行的实例”](#)

23.9.2 计划复制作业

创建复制作业后，可以将其计划为运行一次或重复运行。也可以从一个源站点计划一个目标站点上的多个复制作业。

注意：

如果计划一个目标站点上的多个复制作业，则每次只能有一个复制作业连接到源站点。所有其他尝试连接的复制作业都将转为待定状态，在能够自动连接到源站点之前，这些作业将一直保持待定状态。

23.9.2.1 计划复制作业

1. 转到 CMC 的“联盟”区域。
2. 选择要计划的“复制作业”。
3. 单击“操作” > “计划”。
4. 选择所需的计划选项。

23.9.3 修改复制作业

在联盟中创建复制作业之后，可以修改其属性。

23.9.3.1 修改复制作业

1. 转到 CMC 的“联盟”区域。

- 2 单击“远程连接”文件夹。
- 3 选择包含要修改的“复制作业”的“远程连接”对象。
- 4 选择要修改的“复制作业”。
- 5 单击“管理” > “管理对象属性”。
- 6 根据需要查看和编辑“属性”、“计划”、“历史记录”、“复制列表”以及“用户安全性”。

节	说明
属性	修改复制作业的名称、说明及其他常规属性和选项。
计划	将复制作业设置为按重复计划运行。
历史记录	查看和管理复制作业的所有实例。
复制列表	更改所选的复制列表。
用户安全性	对复制作业设置权限。

23.9.4 在复制作业完成后查看日志

每次运行复制作业时，联盟都会自动生成一个日志文件，将在目标站点上创建该文件。日志文件使用 XML 1.1 标准并且需要一个支持 XML 1.1 的 Web 浏览器。

查看复制日志：

- 1 转到 CMC 的“联盟”区域。
 - 2 单击“所有复制作业”。
 - 3 从列表中选择一个复制作业。
 - 4 单击“属性”。
- 复制作业的“属性”页面将打开。
- 5 单击“历史记录”。
 - 6 单击日志文件的“实例时间”以查看成功的复制作业，或单击“失败”状态以查看失败的复制作业的日志文件。
 - 7 选择所需的实例以查看日志文件。

日志文件以 XML 格式生成，并使用 XSL 结构将信息格式设置为 HTML 页面。

可以从运行服务器智能代理（包含自适应作业服务器）的计算机中访问 XML 日志。可在以下位置找到日志文件：

- 在 Windows 上为安装目录\SAP BusinessObjects Enterprise XI 4.0\logging
- 在 Unix 上为安装目录/sap_bobj/logging

23.10 管理对象清除

在联盟中，应该在复制过程的整个生命周期执行对象清除，以确保从源站点中删除的所有对象也从每个目标站点中删除。

对象清除涉及两个元素：远程连接和复制作业。远程连接对象定义常规的清除选项，而复制作业则在相应的时间间隔过后执行清除。

23.10.1 如何使用对象清除

使用同一个远程连接的各独立复制作业在对象清除过程中将共同工作。这意味着复制作业将清除其复制列表内的对象，以及其他复制列表内使用同一个远程连接的对象。只有当复制作业的父项是同一个远程连接对象时，远程连接才被认为是同一个远程连接。

示例：

复制作业 A 和 B 复制对象 A 和对象 B。它们均从同一个源站点进行复制，并且使用同一个远程连接。如果源站点删除对象 B，则复制作业 A 将确保对象 B 被删除。即使复制作业 B 复制对象 B，该对象也将从目标站点中删除。当复制作业 B 执行时，它便不再需要运行对象清除。

注意：

在对象清除过程中，只会删除目标站点上的对象。如果从源站点删除某个作为复制一部分的对象，则会从目标站点删除该对象。但是，如果从目标站点中删除某个对象，则在对象清除过程中不会从源站点中删除该对象，即使复制作业处于双向复制模式也是如此。

对于从复制列表中删除或移除的对象，不会从目标站点中删除它们。要正确移除复制列表中指定的对象，应在目标站点和源站点上都删除该对象。通过依赖项计算复制的对象不会被删除。

23.10.2 对象清除的限制

在远程连接对象中，可以定义复制作业一次清除的对象数量。联盟将自动跟踪清除作业的结束位置。这样，在下次运行复制作业时，它会在该位置开始下一个清除作业。

提示：

要更快地完成复制作业，请限制要清除的对象数量。

示例：

复制作业 A 和 B 正在复制对象 A 和对象 B。这两个对象均从同一个源站点复制，并且使用同一个远程连接。

如果源站点删除对象 B，且对象限制设置为 1，则在下次运行复制作业 A 时，它将只检查是否删除了对象 A。这样，将不会检查对象 B，并且将不会删除该对象。

接着，复制作业 B 将会运行，并在复制作业 A 结束的位置开始清除对象。它将检查是否删除了对象 B，并从目标站点移除该对象。可以在远程连接对象的属性“将清除对象的数量限制为：”上找到此选项

注意：

如果未选择此选项，则所有使用此远程连接的复制作业都将检查所有对象以确定是否有可能执行清除。

23.10.3 对象清除频率

可以在远程连接的“清除频率”字段中设置复制作业执行对象清除的频率。

注意：

必须输入正整数，该值表示两次对象清除处理操作相隔的小时数。

示例：

复制作业 A 和 B 复制对象 A 和对象 B。这两个对象均从同一个源站点复制，并且使用相同的远程连接。

如果已从源站点中删除对象 B，并且所有以下条件都为真，则复制作业将检查对象 A 是否已删除。

- 对象限制为 1
- 清除频率为 150 个小时
- 再次运行复制作业 A

因为对象限制为 1，将不会检查或删除目标站点上的对象 B。

复制作业 A 执行完初始检查 150 小时后开始下一个清除作业。虽然复制作业 A 和 B 可能会在达到 150 小时的限制之前执行许多次，但这两个作业都不会尝试运行对象清除。在 150 小时后，下一

个复制作业将执行并尝试运行清除。然后，它将确定对象 B 已在源站点上删除，然后在目标站点上也删除该对象。

启用和禁用选项

每个复制作业都可以参与对象清除。使用复制作业上的“在目标上启用对象清除”选项可指示作业是否运行对象清除。某些情况下，可能不希望高优先级复制作业参与对象清除，以便可以尽快地执行这些作业。为此，请禁用对象清除。

相关主题

- 第 730 页上的[“对象清除的限制”](#)

23.11 管理冲突检测 and 解决

在联盟中，如果在源站点和目标站点上都更改了对象的属性，则会发生冲突。对象的顶层属性和嵌套属性都将接受冲突检查。例如，如果在源站点和目标站点上都修改了某个报表或报表的名称，则可能会发生冲突。

某些情况不会造成冲突。例如，如果在源站点上修改了某个报表的名称，而在目标站点上修改了复制版本的说明，则更改会合并在一起，不会发生任何冲突。

23.11.1 单向复制冲突的解决方法

在单向复制中，可以选择两种方法来解决冲突。

源站点优先

如果在单向复制过程中发生冲突，则源站点对象优先。源站点的信息会覆盖对目标站点上的对象所做的任何更改。例如，如果在源站点和目标站点上都修改了某个报表，则在下一次复制作业后，目标站点上的修改会被源站点上的版本覆盖。

注意：

由于自动解决了冲突，因此不会在日志文件中生成冲突，并且冲突不会出现在冲突对象列表中。

无自动冲突解决

如果发生了冲突，并且选择了无自动冲突解决，则冲突不会得到解决，同时，不会生成日志文件，并且冲突不会出现在冲突对象列表中。

管理员可以在 CMC 的“联盟”区域中访问存在冲突的所有复制对象的列表。存在冲突的对象会按它们用于连接到源站点的远程连接分组在一起。要访问这些列表，请转到 CMC 的“联盟”区域中的“复制错误”文件夹，并选择所需的远程连接。目标站点上所有复制的对象将标有复制图标。如果存在冲突，则以冲突图标标记对象。“属性”页面中还将出现一条警告消息。

注意：

- 当使用远程连接的复制作业完成时，列表将更新。它包含使用其特定远程连接的所有复制作业的所有存在冲突的对象。
- 具有 CMC 和复制作业实例访问权限的任何用户都能访问保存在日志文件目录中的 XML 日志。将标记目标站点对象的图标以指明冲突。在处理过程中，将创建一个冲突日志。

Abdul 在源站点上修改报表 A。Maria 在目标站点上修改复制的版本。下次运行复制作业时，报表将处于冲突状态，因为已在两个站点上更改了它，而且冲突将得不到解决。

将会保留目标报表，而且不会复制对源站点上的报表所做的更改。后续的复制作业将按相同的方式行事，直至解决了冲突为止。在手动解决冲突之前，将不会复制源站点上的任何更改。

注意：

在这种情况下，不会复制整个对象。将不复制可能不存在冲突的其他更改。

要手动解决冲突，可选择三种方法：

1. 创建一个复制作业，该作业只复制存在冲突的对象。它必须使用相同的远程连接对象和复制列表。
要保留源站点更改，请创建一个复制作业。然后将复制模式设置为“从源刷新”，并将“自动冲突解决”设置为“源站点优先”。
要保留目标站点更改，请创建一个复制作业，将“复制类型”设置为双向复制，将“复制模式”设置为“从目标刷新”，并将“自动冲突解决”设置为“目标站点优先”。
注意：
在复制模式中，设置“从源刷新”或“从目标刷新”，以便只在复制列表上选择存在冲突的对象。这样，将不会复制其他对象。接着，计划复制作业运行，该作业将复制选定的对象并按指定方式解决冲突。
2. 创建一个复制作业，该作业只复制存在冲突的对象。它将需要使用相同的远程连接对象。但是，与选项 1 不同，可以在源站点上创建新的复制列表。只使用存在冲突的对象，并创建将使用此重点复制列表的新复制作业。
要保留源站点更改，请将“自动冲突解决”设置为“源站点优先”。
要保留目标站点更改，请将“自动冲突解决”设置为“目标站点优先”，并将“复制类型”设置为“双向复制”。
3. 对于单向复制作业，只能删除目标站点上的对象。复制作业下次执行时，它会将对象从源站点复制到目标站点。

注意：

删除对象时要小心，因为依赖于该对象的其他对象可能会被删除、停止工作或失去安全性。建议使用选项 1 和 2。

23.11.2 双向复制冲突的解决方法

在双向复制冲突中，可以选择三个选项来解决冲突：

- 源站点优先
- 目标站点优先
- 无自动冲突解决

源站点优先

如果发生冲突，源站点将优先，并覆盖对目标站点所做的任何更改。

示例：

Lily 将报表的名称更改为报表 A。Malik 将目标站点上复制版本的名称更改为报表 B。下一次复制作业运行后，目标站点上的复制版本将恢复为报表 A。

这不会在日志文件中生成冲突，并且冲突不会出现在冲突对象列表中，因为已按照用户在源站点上的指示解决了冲突。

目标站点优先

如果发生冲突，目标站点将保留其更改，并覆盖对源站点所做的更改。

示例：

Kamal 将报表的名称修改为报表 A。Peter 将目标站点上复制版本的名称修改为报表 B。复制作业运行时，将会检测到冲突。目标报表的名称保留为报表 B。

在双向复制中，所做的更改还将发送回源站点。在此方案中，源站点会更新，并且其报表名称将更改为报表 B。这不会在日志文件中生成冲突，并且冲突将不会出现在冲突对象列表中，因为已按照用户的指示解决了冲突。

无自动冲突解决

如果选择无自动冲突解决，则冲突将不会得到解决。将会在管理员日志文件中记录冲突，而管理员可以手动解决它。

注意：

- 将会标记对象的图标，以指明存在冲突。
- 尽管在双向复制中会将更改同时复制到源站点和目标站点，但只会用冲突图标标记目标站点的版本。

注意：

具有 CMC 和复制作业实例访问权限的任何用户都能访问输出在日志文件目录中的 XML 日志。将标记目标站点对象的图标以指明冲突。在处理过程中，将创建一个冲突日志。

管理员可以在 CMC 的“联盟”区域中访问存在冲突的所有复制对象的列表。存在冲突的对象会按它们用于连接到源站点的远程连接分组在一起。要访问这些列表，请转到“CMC” > “联盟” > “复制错误” > “远程连接”。

注意：

当使用远程连接的复制作业完成时，列表将更新。它包含使用其特定远程连接的所有复制作业的所有存在冲突的对象。目标站点上所有复制的对象将标有复制图标。如果存在冲突，则以冲突图标标记对象。

示例：

Michael 在源站点上修改报表 A。Damien 在目标站点上修改复制的版本。下次运行复制作业时，此报表将处于冲突状态，因为已在两个站点上更改了它，而且将不解决此冲突。

将会保留目标报表，而且不会复制对源站点上的报表所做的更改。后续的复制作业将按相同的方式行事，直至解决了冲突为止。在管理员或委派的管理员手动解决冲突之前，不会复制在源站点上所做的任何更改。

注意：

- 在这种情况下，不会复制整个对象。将不复制不存在冲突的其他更改。
- 具有 CMC 和复制作业实例访问权限的任何用户都能访问输出在日志文件目录中的 XML 日志。将标记目标站点对象的图标以指明冲突。在处理过程中，将创建一个冲突日志。

管理员可以在 CMC 的“联盟”区域中访问存在冲突的所有复制对象的列表。存在冲突的对象会按它们用于连接到源站点的远程连接分组在一起。要访问这些列表，请转到“CMC” > “联盟” > “复制错误” > “远程连接”。

注意：

当使用远程连接的复制作业完成时，列表将更新。它包含使用其特定远程连接的所有复制作业的所有存在冲突的对象。目标站点上所有复制的对象将标有复制图标。如果存在冲突，则以冲突图标标记对象。

要手动解决冲突，可选择三种方法：

1. 创建一个复制作业，该作业只复制存在冲突的对象。它必须使用相同的远程连接对象和复制列表。
要保留源站点更改，请创建一个复制作业。然后将“复制模式”设置为从源刷新，并将“自动冲突解决”设置为源站点优先。
要保留目标站点更改，请创建一个复制作业，将“复制类型”设置为“双向复制”，将“复制模式”设置为“从目标刷新”，并将“自动冲突解决”设置为“目标站点优先”。

注意：

在“复制模式”中，设置“从源刷新”或“从目标刷新”，以便只在复制列表上选择存在冲突的对象。这样，将不会复制其他对象。接着，计划复制作业运行，该作业将复制选定的对象并按指定方式解决冲突。

- 2 创建一个复制作业，该作业只复制存在冲突的对象。它将需要使用相同的远程连接对象。但是，与选项 1 不同，可以在源站点上创建新的复制列表。只使用存在冲突的对象，并创建将使用此重点复制列表的新复制作业。

要保留源站点更改，请将“自动冲突解决”设置为“源站点优先”。

要保留目标站点更改，请将“自动冲突解决”设置为“目标站点优先”，并将“复制类型”设置为“双向复制”。

- 3 删除不希望位于站点上的对象。

注意：

删除对象时要小心，因为依赖于该对象的其他对象可能会被删除、停止工作或失去安全性。建议使用选项 1 和 2。

要保留目标站点更改，可以删除源站点上的对象。复制作业下次执行时，它会将对象从目标站点复制到源站点。

注意：

删除源站点的副本时请小心，因为复制该对象的其他目标站点可能会在将副本复制回之前执行其复制作业。这将会导致其他目标站点删除其副本，在副本返回之前，它将不可用。

要保留源站点更改，可以删除目标站点上的对象。

23.12 在联盟中使用 Web 服务

联盟使用 Web 服务在源站点和目标站点之间发送对象以及对对象所做的更改。在安装 BI 平台的过程中将会自动安装和部署特定于联盟的 Web 服务。但是，可能需要在 Web 服务中修改属性或自定义部署以便改善功能，如本节中所述。

提示：

要改进文件管理和功能，请在联盟中启用文件高速缓存。

23.12.1 会话变量

如果要在一个复制作业中传输大量内容文件，可能需要增加联盟 Web 服务的会话超时周期。

此属性位于 `dsws.properties` 文件中：

应用程序服务器安装目录\dswebobje\Web-INF\classes

例如：

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswebobje\WEB-INF\classes
```

要激活会话变量，请输入：

```
session.timeout = x
```

其中x是所需的时间，x的单位为秒。如果未指定，则默认值为 1200 秒或 20 分钟。

仅在运行 Web 应用程序服务器的计算机上重新部署修改的 Web 应用程序后，新属性才会生效。使用 WDeploy 在 Web 应用程序服务器上重新部署 WAR 文件。有关使用 WDeploy 的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

23.12.2 文件高速缓存

通过使用文件高速缓存，Web 服务可以处理非常大的附件，但不会在内存中对附件进行缓冲。如果在传输大量数据的过程中未启用文件高速缓存，则可能会使用所有的 Java 虚拟机内存，因此复制可能会失败。

注意：

文件高速缓存将会降低性能，因为 Web 服务对文件进行处理，而不是对内存进行处理。可以结合使用这两种选择，将要传输的大量数据发送到文件，将要传输的较少量数据发送到内存。

要启用文件高速缓存，请修改位于以下位置的 Axis2.xml 文件：

应用程序服务器安装目录\dswebobje\Web-Inf\conf

例如：

```
C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI
4.0\warfiles\webapps\dswebobje\WEB-INF\conf
```

输入以下内容：

```
<parameter name="cacheAttachments" locked="false">true</parameter>
<parameter name="attachmentDIR" locked="false">临时目录</parameter>
<parameter name="sizeThreshold" locked="false">4000</parameter>
```

注意：

阈值大小的单位为字节。

仅在运行 Web 应用程序服务器的计算机上重新部署修改的 Web 应用程序后，新属性才会生效。使用 WDeploy 在 Web 应用程序服务器上重新部署 WAR 文件。有关使用 WDeploy 的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

23.12.3 自定义部署

联盟 Web 服务可以自动进行部署并需要激活 federation、biplatform 和 session 服务。要禁用联盟或任何其他 Web 服务，请修改对应的 Web 服务的 service.xml 文件。

BI 平台 Web 服务位于：

应用程序服务器安装目录\dswsbobje\WEB-INF\services

示例：

C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\services

取消激活 Web 服务：

- 在 service.xml 文件的服务名称标记中添加 activate 属性并将其设置为 False
- 重新启动 Java 应用程序服务器

例如，要禁用联盟：

services.xml 文件位于：

C:\Program Files\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\services\federator\META-INF

将服务名称从：

```
<service name="Federator">
```

更改为：

```
<service name="Federator" activate="false">
```

仅在运行 Web 应用程序服务器的计算机上重新部署修改的 Web 应用程序后，新属性才会生效。使用 WDeploy 在 Web 应用程序服务器上重新部署 WAR 文件。有关使用 WDeploy 的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。

23.13 远程计划和本地运行的实例

本节介绍了远程计划、本地运行的实例和实例共享。这些功能允许报表在数据所在之处运行，并将完成的实例发送到适当的位置。

23.13.1 远程计划

通过使用联盟功能，可以在目标站点上计划报表，然后在源站点上处理它。完成的实例将返回到目标站点。

要启用远程计划，请按正常方式计划报表，并启用“在源站点运行”选项。要启用此选项，请单击“计划” > “计划服务器组” > “在源站点运行”。创建了计划实例后，它们将处于待定阶段。

在远程计划的过程中，将忽视在目标站点上提交的信息，而且报表实例仍将处于待定阶段。

在为远程计划启用下一个管理报表的复制作业时，它会将此实例复制到源站点以进行处理。在计划程序处理此实例之前，实例将保持待定状态。同时，发送此实例的复制作业将返回任何以前完成的实例和对象更改。

在源站点上处理完此实例后，实例将恢复为完成状态。在为远程计划启用下一个管理报表的复制作业时，它将使用完成的实例来更新目标站点上的副本。更新之后，将完成目标站点上的实例。

注意：

复制作业必须运行两次，以便带回一个完成的实例。

示例：

- 。 1 Tom 对报表 A 制定了计划以便实施远程计划。
- 。 2 在目标站点上创建报表 A，并将其置于待定状态。
- 。 3 运行复制作业 A。首先，它将源站点中的更改复制到目标站点（包括以前完成的实例）。其次，它将处于待定状态的实例复制到源站点，并将要复制的更改从目标站点复制到源站点。
- 。 4 在源站点，计划程序选取处于待定状态的实例，并将其发送到适当的作业服务器进行处理。然后在源站点上处理实例，并将其置于完成状态。
- 。 5 再次运行复制作业 A。在它将从源站点复制到目标站点时，将选取报表 A 的已完成实例，并将所做的更改应用于目标站点上的版本。
- 。 6 在此任务完成后，即完成了目标站点上的版本。

远程计划仅与双向复制作业一起使用，并且必须启用“复制远程计划”。此选项位于“复制作业属性”页上的“复制过滤器”区域中。在一些情况下，可能会想比复制“复制列表”上的其他对象更频繁地复制远程计划的作业。为此，请创建两个复制作业。启用其中一个复制远程计划的复制作业，以创建一个仅关注远程计划的复制作业。启用另一个复制文档模板或复制所有对象（无过滤器）的复制作业。

注意：

启用远程计划时，完成的实例和失败的实例均出现在源站点和目标站点上。

如果目标站点上的某用户将报表计划为远程计划，并且该用户在源站点上不存在，则实例将在源站点上失败。失败实例的所有者将是用于连接到源站点的远程连接对象的用户帐户。

虽然可能只能为远程计划配置某个复制作业，但是，它将始终复制报表实例的祖先对象。这就意味着，如果在两次复制之间进行了任何更改，则它将复制实际的报表、报表文件夹等。如果不希望将目标站点上的这些更改复制到源站点，可以使用安全权限控制复制哪些更改。

相关主题

- 第 710 页上的“[管理安全权限](#)”

23.13.2 本地运行的实例

本地运行的实例是通过目标站点上的报表处理的报表实例。借助联盟功能，可以将目标站点中的已完成实例复制到源站点。

要允许复制作业将完成的实例和失败的实例从目标站点复制到源站点，请单击“复制作业属性” > “复制过滤器” > “复制本地运行的已完成实例”。

在一些情况下，可能希望复制作业仅复制本地运行的实例。为此，请启用复制本地运行的已完成实例。

注意：

在复制作业上启用本地运行的实例后，完成的实例和失败的实例均将复制到源站点。这意味着，源站点和目标站点上都将有副本。

绝不会复制待定的实例。

如果本地运行的实例的所有者在源站点上不存在，则此所有者将为在远程连接对象中用于进行连接的用户帐户。

23.13.3 实例共享

在复制作业中启用远程计划和本地运行的实例时，如果有一个源站点，但是有多个复制相同报表的目标站点，则可能会发生实例共享。

示例：

报表 A 在源站点上出现，而目标站点 A 和 B 均复制它。在这两个目标站点上都将发生实例共享：

- 通过“复制远程计划”和/或“复制本地运行的已完成实例”启用复制作业。通过上述复制作业复制报表 A。
- 在目标站点上将报表 A 计划为在源站点运行和/或在本地运行

如果目标站点 A 和 B 均复制报表 A，并且与它们对应的复制作业将复制远程计划和/或本地运行的实例，则目标站点 A 将与目标站点 B 共享在目标站点 A 上处理的任何实例以及/或者在源站点上代表目标站点 A 处理的任何实例。

同样，目标站点 B 将与目标站点 A 共享在目标站点 B 以及/或者在源站点上处理的任何实例。最终，源站点以及目标站点 A 和 B 将具有一组相同的实例。

在很多情况下，实例共享是理想之选。例如，当其他站点的用户需要访问同类部署中的信息时。在这种情况下，为了阻止本地站点的用户查看实例，请确保设置了正确的安全权限。例如，在报表对象中应用权限，使用户只能看到他们所拥有的实例。

注意：

所有对象都遵守 BI 平台安全规则。要确保用户和组只能查看相应的实例，建议设置权限，使用户只能查看自己所拥有的实例。例如，在报表对象中应用权限，使用户只能看到他们所拥有的实例。

相关主题

- 第 710 页上的“[管理安全权限](#)”

23.14 导入和升级复制的内容

某些情况下，可以选择将复制的内容从一个 BI 平台系统导入或升级到另一个系统。本节论述联盟中的这些功能。

注意：

对象迁移最好由管理员组的成员执行，尤其是管理员用户帐户。要迁移一个对象，可能同时需要迁移很多相关对象。委派管理员帐户可能无法为所有对象获取需要的安全权限。

23.14.1 导入复制的内容

如果使用生命周期管理器将内容从一个 BI 平台部署导入到另一个部署，生命周期管理器将不会导入与所导入的复制对象关联的任何复制特定信息。这意味着，在导入之后，对象就好像从未复制过一样。这特定于目标站点上的复制对象，以下方案中描述了这一点。

示例：

BI 平台 A 是联盟过程中的目标站点。使用生命周期管理器将报表 A（系统 A 上的一个复制的报表）从系统 A 导入到 BI 平台 B。

结果：将报表 A 复制到 BI 平台 B 后，该报表不包含任何复制的信息。将不再用复制图标标记报表 A。如果对象在 BI 平台 A 上存在冲突，它在系统 B 上将不存在冲突。实质上它将被视为源自系统 B 的对象。

注意：

CUID 可能相同，也可能不相同，具体情况取决于在生命周期管理器中选择的导入选项。

23.14.2 导入复制的内容并继续复制

在导入复制的内容之后，可能需要将导入的对象纳入联盟过程中。存在以下两种方案：将导入的对象所在的系统视为源站点，或者将该系统视为目标站点。要将此系统视为源站点，请按正常方式继续执行联盟。

要将此系统视为目标站点并从源站点复制导入的对象，则必须：

- 确保在使用生命周期管理器时保留了对象的 CUID。
- 确保第一个复制作业的冲突解决方法设置为“源优先”或“目标优先”。

提示：

不要使用生命周期管理器将对象从一个目标站点导入到另一个目标站点，因为只使用联盟来复制对象将更有效，所以强烈建议这样做。

示例：

在 BI 平台系统 A 上创建了报表 A。系统 X 使用了联盟将报表 A 从系统 A 复制到系统 X。然后，生命周期管理器将报表 A 从系统 X 导入到系统 Y。

计划：系统 Y 希望将联盟设置为系统 A，并在复制过程中保留报表 A。系统 Y 为目标，系统 A 为源。

操作：将报表 A 从系统 X 导入到系统 Y 时，必须保留报表 A 的 CUID。此外，当第一个复制作业执行时，它将尝试复制报表 A。由于对象在系统 Y 上已存在，因此复制操作将导致冲突。要指定待使用的版本，必须将冲突解决模式设置为源成功或目标成功。

注意：

在本例中，建议只使用联盟来复制对象，而不是使用生命周期管理器将对象从一个目标站点导入到另一个目标站点。报表 A 将从系统 A 复制到系统 Y，并且不必使用生命周期管理器从系统 X 导入到系统 Y。

23.14.3 从测试环境中升级内容

在任何组织中，测试通常是在将任何内容转入生产环境中之前完成的。在生产计算机上设置联盟之前，通常要测试开发或测试环境中 BI 平台系统之间的联盟。在测试环境中创建了源站点和目标站点以及内容之后，可以使用以下步骤将此设置升级到生产计算机：

- 1 使用生命周期管理器将内容从测试环境中的源站点升级到生产环境中将充当源站点的计算机。

注意：

使用生命周期管理器时，不能选择复制列表对象。

- 2 在生产环境中的源站点上创建复制列表，并包括所需的内容。
- 3 从以下两个选项中进行选择：
 - A) 在生产环境中将充当目标站点的生产计算机上创建远程连接对象和相应的复制作业。
 - B) 使用生命周期管理器将远程连接和复制作业从 Dev/QA 环境中的目标站点导入到将充当目标站点的生产计算机。然后，编辑导入的远程连接以指向生产环境中将充当源站点的计算机。

23.14.4 将目标站点重新指向新位置

如果将远程连接对象编辑为指向一个新系统，则一旦从源站点复制了某个对象，就必须始终从该源站点复制该对象，而不能从其他 BI 平台复制，对于从远程连接对象之外的其他 BI 平台系统复制的对象，任何进行复制的尝试都会失败。要从其他源站点复制对象，请首先将该对象从目标站点中删除。

注意：

创建了复制对象的副本后，副本的 CUID 将发生变化，并且副本将不包含任何复制信息。

23.15 最佳做法

可以使用联盟优化复制作业的性能。

如果单一复制作业中有大量对象，可采取其他步骤以确保其成功运行。通常，在每个复制作业中应能复制多达 32,000 个对象。但是，某些部署可能需要复制规模更大或更小的配置。

1) 获得专用的 Web 服务提供者

在联盟中，复制的内容使用 Web 服务发送。在 BI 平台的默认安装中，所有 Web 服务均利用相同的 Web 服务提供者。较大的复制作业可能会占用 Web 服务提供者较长时间，因而减慢了响应其他 Web 服务请求及其服务的任何应用程序的速度。

如果计划同时复制大量对象，或者计划依次运行多个复制作业，则可以考虑将联盟 Web 服务部署在它自己的 Java 应用程序服务器上（此服务器使用计划者自己的 Web 服务提供者）。

要进行此操作，请使用 BI 平台安装程序来安装 Web 服务。必须已运行 Java 应用程序服务器，否则，请安装完整的 Web 层组件选项，这将安装 Web 服务和 Tomcat。

注意：

- 必须提供现有 CMS 的信息（例如主机名、端口和管理员密码）。
- 将需要在远程连接的 URI 字段中使用这个新的 Web 服务提供者的 URI。

2) 增加 Java 应用程序服务器的可用内存

如果单个复制作业复制许多对象，或者如果与其他应用程序共享 Java 应用程序服务器，请增加 Java 应用程序服务器的可用内存。

如果部署了 BI 平台和 Tomcat，则默认的可用内存为 1 GB。要增加 Tomcat 的可用内存：

在 Windows 中：

- 1 单击“开始” > “程序” > “Tomcat” > “Tomcat 配置”。
- 2 选择“Java”。
- 3 在“Java Options”（Java 选项）框中，找到 -Xmx1024M
- 4 将 -Xmx1024M 增加到所需的大小。

示例：

要将内存增加到 2GB，请输入：-Xmx2048M

在 Unix 中：

- 1 在 <BOE_Install_Dir>/setup/ 中，用首选的文本编辑器打开 env.sh。将 -Xmx1024m 参数增大到所需的大小。

2 找到以下行

```
# if [ -d "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for Tomcat
JAVA_OPTS="-Dbobj.enterprise.home=${BOBJEDIR}enterprise120
-Djava.awt.headless=true"

if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" =
"SunOS" -o "$SOFTWARE" = "Linux" ];
then
  JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
fi
export JAVA_OPTS
# fi
```

3 将 -Xmx1024m 参数增大到所需的大小。

示例：

要将内存增加到 2GB，请输入：-Xmx2048m

提示：

对于其他 Java 应用程序服务器，请参阅 Java 应用程序服务器的文档以增加可用内存。

3) 减小所创建的 BIAR 文件的大小。

联盟使用 Web 服务在源站点和目标站点之间复制内容。对象被集合起来，然后压缩为 BIAR 文件，以便提高传输效率。

复制大量对象时，请将 Java 应用程序服务器配置为创建较小的 BIAR 文件。联盟会将对象打包并压缩为多个较小的 BIAR 文件，以便要复制的对象数量不受限制。

要减小所创建的 BIAR 文件的大小，请将以下 Java 参数添加到 Java 应用程序服务器中：

```
Dbobj.biar.suggestSplit
and
Dbobj.biar.forceSplit
```

bobj.biar.suggestSplit 建议了适当的 BIAR 文件大小（它将设法实现此大小）。建议的新值为 90MB。

bobj.biar.forceSplit 将强制 BIAR 文件不得超过给定的大小。建议的新值为 100MB。

注意：

除非应用程序服务器耗尽内存，而且无法再增加其最大堆大小，否则无需更改默认的 BIAR 文件大小设置。

对于 Tomcat Windows：

- 1 要打开“Tomcat 配置”工具，请单击“开始” > “程序” > “Tomcat” > “Tomcat 配置”。
- 2 选择“Java”。
- 3 在“Java Options”（Java 选项）框中，在结尾添加以下行：

```
-Dbobj.biar.suggestSplit=90
-Dobj.biar.forceSplit=100
```

对于 Tomcat Unix/Linux：

- 1 用首选的文本编辑器打开 env.sh。它位于 <BOE_Install_Dir>/setup/ 中

2 找到以下行：

```
# if [ -d "$BOBJEDIR"/tomcat ]; then
# set the JAVA_OPTS for tomcat
JAVA_OPTS="-Dboj.enterprise.home=${BOBJEDIR}enterprise120 -Djava.awt.headless=true"

if [ "$SOFTWARE" = "AIX" -o "$SOFTWARE" = "SunOS" -o "$SOFTWARE" = "Linux" ]; then
  JAVA_OPTS="$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m"
fi
export JAVA_OPTS
# fi
```

添加所需的 BIAR 文件大小参数。

示例：JAVA_OPTS="\$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m -Dboj.biar.suggestSplit=90 -Dboj.biar.forceSplit=100"

对于其他 Java 应用程序服务器，请查阅文档以添加 Java 系统属性。

4) 增大套接字超时值。

自适应作业服务器负责运行复制作业。在复制作业的执行期间，自适应作业服务器会建立与源站点的连接。从源站点接收大量信息时，自适应作业服务器用于接收信息的套接字不得超时。

默认值为 90 分钟。如果需要，可以增加套接字超时值。

要增大自适应作业服务器上的套接字超时值：

- 1 打开中央管理控制台（CMC）
- 2 导航到“服务器”部分，然后选择“自适应作业服务器”。
- 3 单击“属性”。
- 4 在以下行的结尾添加命令行参数：
 - Windows: -javaArgs Xmx1000m,Xincgc,server,Dboj.federation.WSTimeout=<以分钟计的超时值>
 - Unix: -javaArgs Xmx512m,Dboj.federation.WSTimeout=<以分钟计的超时值>

相关主题

- 第 747 页上的[“错误消息疑难解答”](#)
- 第 736 页上的[“在联盟中使用 Web 服务”](#)
- 第 746 页上的[“当前版本限制”](#)

23.15.1 当前版本限制

联盟是一款灵活的工具，但是，某些限制可能会影响其在生产过程中的性能。本节重点说明为了优化联盟操作而可以改变的几个方面。

- 最大对象数

每个复制作业均在 BI 平台部署之间复制对象。建议在单个复制作业中复制的最大对象数为 100,000。虽然一个复制作业处理的对象可以超过 100,000 个，但联盟只支持最多复制 100,000 个对象。

- 权限

在联盟中，仅从源站点将权限复制到目标站点。建议在源站点上设置这两个部署公共的用户权限，并使用双向复制将这些权限复制到目标站点。在用户所在站点上的 BI 平台部署中，将如常管理特定站点上的用户权限。

- 业务视图和关联的对象

BI 平台可以存储业务视图、业务元素、数据基础、数据连接和值列表（LOV）。这些对象用于增强 Crystal Reports 的功能。

如果首先在目标站点上创建这些对象，然后使用双向复制将它们复制到源站点，则它们可能无法正常工作，而且它们的数据可能无法出现在 Crystal Reports 中。

建议在源站点上创建业务视图、业务元素、数据基础、数据连接和 LOV，然后将它们复制到目标站点。更新目标站点或源站点上的对象（权限允许），而所做的更改将正确地双向复制。

- Universe 限制

BI 平台可以存储 Universe 限制。如果在目标站点上创建 Universe 限制，然后使用双向复制将它们复制到源站点，则它们可能无法正常工作。

要解决此问题，请先在源站点上创建 Universe 限制，然后将它们复制到目标站点。接着，在源站点上设置有关 Universe 限制的任何安全设置，然后将这些设置复制到目标站点。

- 对象清除

对象清除会删除已在另一个站点上删除的对象。目前只能执行从源站点到目标站点的对象清除。

- 联盟日志文件

联盟日志文件将写入到使用 XML 1.1 标准的 XML 文件中。要用浏览器查看日志文件，浏览器必须支持 XML 1.1。

相关主题

- 第 730 页上的“[管理对象清除](#)”

23.15.2 错误消息疑难解答

本节包含在使用联盟时的极少数情况下可能会遇到的错误消息。这些消息将出现在复制作业日志中，或出现在报表的功能区中。

1) 无效的 GUID

错误示例：错误 2008-01-10T00:31:08.234Z GUID ASX00Fyvy0FJnRcD0dZNTZg（在对象编号 1285 上的属性 SI_PARENT_CUID 中找到）不是有效的 GUID。

此错误表示正在复制某个对象，但未随其一起复制父对象，而且该对象在目标站点上并未存在。例如，正在复制某个对象，但未复制包含它的文件夹。之所以未复制父对象，可能是因为复制对象的帐户在父对象上没有足够的权限。

2) Crystal Reports 在源站点上未显示任何数据

如果 Crystal 报表 使用原来在目标站点上创建然后复制到源站点的业务视图、业务元素、数据基础、数据连接或值列表（LOV），则可能会发生此错误。

3) 未正确应用 Universe 限制。

如果报表使用 Universe，而后者包含原来在目标站点上创建然后复制到源站点的 Universe 限制，则可能会发生此错误。

4) Java 内存不足

错误示例：java.lang.OutOfMemoryError。

如果 Java 应用程序服务器在处理复制作业时已用完内存，则可能会发生此错误。复制作业可能太大，或者 Java 应用程序服务器可能没有足够的内存。

解决方法是，通过将联盟 Web 服务移到专用的计算机上来增加 Java 应用程序服务器的可用内存，或者减少在一个复制作业中复制的对象数量。

5) 套接字超时

错误示例：与源站点通信时出错。读取超时。

从源站点发送到目标站点上的自适应作业服务器的信息所用的时间比规定的超时值长。增大自适应作业服务器上的套接字超时值，或者减少在复制作业中复制的对象数量。

6) 查询限制

错误示例：目标站点出现 SDK 错误。不是有效的查询。（FWB 00025）……查询字符串超过查询长度限制。

如果同时复制太多对象，以及联盟提交了对于 CMS 太大而无法处理的查询，则可能会发生此错误。来自源站点的对象将提交到目标站点。但是，将不会提交任何需要提交到源站点的更改。按照规定解决冲突，但不会在对象上设置手动解决冲突的标志。在目标站点上提交的对象将继续正确工作。

要解决此问题，请减少在一个复制作业中复制的对象数量。

7) 复制作业超时

错误示例：无法在指定的时间间隔内计划对象。

如果复制作业在等待另一个复制作业完成时超时，则可能会收到此消息。如果多个复制作业同时连接到同一个源站点，则可能会发生此错误。失败的复制作业将尝试在其下一个计划时间再次运行。

要解决此问题，请将失败的复制作业计划为在不会与其他连接到同一个源站点的复制作业冲突的时间运行。

8) 复制限制

错误示例：目标站点出现 SDK 错误。数据库访问错误。……内部查询处理器错误：查询处理器在查询优化期间用完了堆栈空间。在 ExecWithDeadlockHandling 中执行查询时出错。

如果超过了可以同时复制的受支持对象的数量，则可能会收到此消息。要解决此问题，请减少在复制作业中复制的对象数量，然后再次运行此作业。

9) 已删除对象

错误示例：检查安全权限时遇到错误或打包对象时遇到错误。

如果从复制包中删除了对象，则可能会显示此消息。在联盟查询需要复制的对象时，但在它检查权限和打包对象之前，可能会发生此错误。

10) 自适应处理服务器

错误示例：作业处理服务器中出错。

如果联盟加载的类太多，并且没有足够的内存来处理复制作业，则可能会发生此错误。

要解决此问题，需要执行以下两个步骤：

- 。 1 在自适应处理服务器的命令行参数中，添加以下行：-javaArgs "XX:MaxPermSize=256m"。
- 。 2 将以下参数添加到要针对联盟功能连接到的 Java 应用程序服务器中，以减小要使用的 BIAR 文件的大小：
 - -Dbobj.biar.suggestSplit=100m
 - -Dbobj.biar.forceSplit=100m

11) 对象管理器空间

错误示例：无法生成推送包。出现输入 / 输出异常：“没有在设备上留出空间”。

当联盟使用的临时目录没有足够的磁盘空间时，会发生此错误。要解决此问题，请在临时目录中创建额外的空间，或者使用其他位置作为临时目录。

要在源站点上为临时目录指定其他位置，请将以下行添加到 Java 应用程序服务器的配置文件中：
-Dbobj.tmp.dir=TempDir。

要在目标站点上为临时目录指定其他位置，请将以下行添加到自适应处理服务器的命令行参数中：
-javaArgs -Dbobj.tmp.dir=TempDir。

在以上示例中，TempDir 是想要使用临时目录的位置。

12) Universe 错误

错误示例：调用 processDPCommands API 时出现内部错误。

如果已经复制的 Universe 具有无效的“Universe 与 Universe 连接之间的关系”，或者缺少这种关系，则可能会发生此错误。要解决此问题，请运行复制作业，同时选择“从源刷新”选项，并验证是否复制了 Universe 连接。

或者，可以在 Universe Designer 中打开 Universe，编辑该 Universe 的连接，然后重新提交该 Universe。

相关主题

- 第 744 页上的“[最佳做法](#)”
- 第 746 页上的“[当前版本限制](#)”

第 24 章 ERP 环境补充配置

24.1 针对 SAP NetWeaver 集成的配置

24.1.1 与 SAP NetWeaver Business Warehouse (BW) 集成

24.1.1.1 概述

本节介绍如何配置 BW 以启用和管理从 SAP NetWeaver Business Warehouse 到 BI 平台的报表发布。

在开始本节之前，请确保在 CMC 中已完成 SAP 身份验证插件的配置。

相关主题

- 第 280 页上的“[配置 SAP 身份验证](#)”

24.1.1.1.1 在 BI 平台中设置文件夹和安全性

在 BI 平台中定义权利系统时，系统将创建一个与用户的 SAP 系统相匹配的逻辑文件夹结构。向 BI 平台导入角色和发布内容时，会创建相应的文件夹。管理员则不必创建这些文件夹。如果用户在配置 SAP 身份验证插件、将角色导入到 CMC 以及将内容发布到 BI 平台时定义了权利系统，系统就会创建这些文件夹。

注意：

BI 平台管理员负责将正确的权限分配给这些文件夹：

- SAP 顶层文件夹

确保“Everyone”组具有对 SAP 顶层文件夹的受限访问权限。

- 系统 ID 文件夹

为主体发布器分配 CMC 中的以下权限：

- 将对象添加到文件夹
- 查看对象
- 编辑对象
- 修改用户拥有的对象权限
- 删除对象

提示：

为更便于管理权限，可以创建一个包括这些权限的自定义发布器访问级别，然后在相关系统 ID 文件夹中为主体发布器授予此访问级别。

相关主题

- 第 126 页上的“[使用访问级别](#)”
- 第 112 页上的“[权限在 BI 平台中如何运作](#)”

24.1.1.1.2 了解默认的文件夹安全模式

当从 SAP 向 BI 平台发布内容时，该平台会自动创建角色、文件夹和报表的其余层次结构。系统会在按照系统 ID、客户端编号和角色名称命名的文件夹中组织报表：

- 当用户定义权利系统时，该系统将创建顶层文件夹（即 SAP 2.0 和系统（SID）文件夹）。
- 从 BW 发布角色时，系统会根据需要创建“角色”文件夹（作为组导入 BI 平台中）。
- 系统将为每个接收所发布内容的角色创建一个“内容”文件夹。

- 安全性是基于每个报表对象设置的，因此用户只能查看属于其角色的报表。

管理员负责将权限分配给不同角色的成员。内容管理工作台用于从 SAP BW 中管理报表发布功能。您可以在 SAP BW 系统使用特定 BI 平台系统识别角色，发布报表以及在 SAP BW 和 BI 平台部署之间同步报表。

内容文件夹

BI 平台将按照 CMC 中的定义为添加到权利系统的每个角色导入一个组。

为确保将适当的默认权限授予内容承载角色的所有成员，请在内容管理工作台中为 BI 平台中定义每个权利系统授予相应权限。要启动内容管理工作台，请运行事务处理 /CRYSTAL/RPTADMIN:

- 1 在内容管理工作台中，展开“Enterprise 系统”，然后展开“可用系统”。
- 2 双击所需的系统。
- 3 单击“布局”选项卡。
- 4 将“报表的默认安全策略”设置为“查看”。
- 5 将“角色文件夹的默认安全策略”设置为“按需查看”。
- 6 单击“确定”。

对于所有内容角色，这些设置都反映在 BI 平台中。这些角色也就是接收所发布内容的角色。现在，这些角色的成员将能够查看发布给其他角色的报表的计划实例，并且将能够刷新发布给他们所属角色的报表。

注意：

强烈建议您保持角色活动的区别。例如，虽然可以由管理员角色进行发布，但更好的做法是只由发布者角色进行发布。此外，发布角色的功能只是定义哪些用户可以发布内容。因此，发布角色不应包含任何内容；发布者应发布到正常的角色成员可以访问的内容承载角色。

24.1.1.2 配置 BW 发布器

BW 发布器允许单独或成批地从 BW 向 BI 平台发布 Crystal 报表（.rpt 文件）。

在 Windows 上，可以使用下列任一方法配置 BW 发布器：

- 使用承载 BI 平台的计算机上的服务启动 BW 发布器。BW 发布器服务将根据需要启动 BW 发布器的实例。
- 使用本地 SAP 网关启动 BW 发布器，以创建 BW 发布器实例。

在考虑了每个配置的优缺点之后，必须根据自己的站点要求来选择配置方法。在 BI 平台中完成 BW 发布器的配置之后，必须在内容管理工作台中配置发布。

24.1.1.3 将 BW 发布器配置为服务

本节介绍如何通过将 BW 发布器作为服务的方式支持报表从 BW 到 BI 平台的发布，请执行以下过程。

24.1.1.3.1 分布 BW 发布器安装

本节介绍 BW 发布器服务的分布以及如何分离 BW 发布器与其他 BI 平台组件。

可以通过在同一 BI 平台系统中的两台计算机上安装 BW 发布器服务来平衡 BW 发布负载。

在承载 BI 平台的计算机上安装 BW 发布器时，请将每一台计算机配置为使用相同的程序 ID 和 SAP 网关主机及网关服务。在创建使用此程序 ID 的 RFC 目标后，BW 会在承载 BI 平台的计算机上平衡发布负载。此外，当一个 BW 发布器不可用时，BW 将继续使用其余的 BW 发布器。

可以在包括多台 BW 应用程序服务器的任何配置中添加附加的系统冗余级别。将每台 BW 应用程序服务器配置为运行 SAP 网关。对于每台服务器，请在承载 BI 平台的计算机上安装单独的 BW 发布器服务。将每个 BW 发布器服务配置为使用单独 BW 应用程序服务器的网关主机和网关服务。在此配置中，即使一个 BW 发布器或一台应用程序服务器发生故障，BW 发布仍可继续进行。

如果要将 BW 发布器与其他 BI 平台组件分离，请使用独立 SAP 网关安装 BW。

在这种情况下，必须在安装 BW 发布器的计算机上安装本地 SAP 网关。另外，BW 发布器需要访问 BI 平台（SDK）和 Crystal Reports 打印引擎。因此，如果在专门的计算机上安装 BW 发布器和本地 SAP 网关，则还必须安装 SIA 服务器。

24.1.1.3.2 启动 BW 发布器：Unix

运行 BW 发布器脚本以创建一个或多个发布器实例对发布请求进行处理。建议启动一个发布器实例。

启动 BW 发布器之后，它将与用户在运行 BI 平台安装程序时指定的 SAP 网关服务建立连接。

24.1.1.3.3 启动 BW 发布器：Windows

在 Windows 上，使用中央配置管理器（CCM）启动 BW 发布器服务。启动 BW 发布器服务时，它会创建一个发布器实例为来自 BW 系统的发布请求提供服务。如果发布请求的数量增加，BW 发布器自动产生更多的发布器来满足需求。

24.1.1.3.4 配置 BW 发布器服务的目标

要启用 BW 发布器，必须在 BW 服务器上配置 RFC 目标，以便与 BW 发布器服务进行通信。如果有 BW 群集，请在每台服务器上配置 RFC 目标，在每次配置时都将 BW 的中心实例作为网关主机。

如果希望从 BW 发布到多个 BI 平台系统部署，请在每个 BI 平台部署中为此 BW 发布器服务创建单独的 RFC 目标。除了相同的网关主机和网关服务之外，必须对每个目标使用唯一的程序 ID。

24.1.1.3.5 使用本地 SAP 网关配置 BW 发布器

注意：

如果 BI 平台安装在 Unix 上，请不要使用此配置。在 Unix 上使用此方法可能会导致不可预测的系统行为。

要启用从 BW 到 BI 平台的报表发布，并使用本地 SAP 网关，请执行以下过程：

- 第 756 页上的 [“安装本地 SAP 网关”](#)。
- 第 756 页上的 [“配置 BW 发布器的目标”](#)。

24.1.1.3.6 安装本地 SAP 网关

必须在安装了 BW 发布器的计算机上安装本地 SAP 网关。建议 SAP BASIS 管理员安装这些 SAP 网关之一。

有关安装本地 SAP 网关的最新指导，请参阅 SAP 演示 CD 附带的 SAP 安装指导。

有关经过测试的环境的详细列表，请查阅产品分发介质附带的 platforms_EN.txt 文件。此文件包含应用程序服务器、操作系统、SAP 组件等的特定版本和 Service Pack 要求。

安装了 SAP 网关后，请使用 regedit 来验证 HKEY_CURRENT_USER\Environment 子键下的 TMP 和 TEMP 注册表项。两个注册表项应拥有相同的字符串值，而且该值必须是有效的绝对目录路径。如果两个项的值包含 %USERPROFILE% 变量，请将其替换为绝对目录路径。通常，这两个注册表项都被设置为 C:\WINDOWS\TEMP

24.1.1.4 配置 BW 发布器的目标

要启用 BW 发布器，您必须配置 RFC 目标，以便为 BW 提供您安装本地 SAP 网关和 BW 发布器的计算机的位置。

24.1.1.5 在内容管理工作台中配置发布

内容管理工作台用于从 SAP BW 中管理报表发布功能。您可以在 SAP BW 系统中使用特定 BI 平台系统识别角色，发布报表以及在 SAP BW 和 BI 平台部署之间同步报表。一旦您设置了 SAP 身份验证，并配置了 BW 发布器，请执行本节介绍的函数以启用发布。这些说明将指导您完成下列任务：

- 为内容管理工作台的不同用户设置正确的身份验证。
- 与发布内容的 BI 平台建立连接。
- 定义哪些角色可向各 BI 平台发布内容。

- 从 BW 向 BI 平台发布内容。

24.1.1.6 可访问内容管理工作台的用户

有三类用户可以访问内容管理工作台：

- 内容使用者，属于内容承载角色，能够查看报表。除了查看报表之外，他们无权执行任何其他操作。
- BI 平台内容发布者，能够在 BW 中查看、发布、修改和（可选）删除报表。
- BI 平台管理员，能够在内容管理工作台中执行所有任务。这些任务包括定义BI 平台系统、发布报表和执行报表维护。

24.1.1.7 在 BW 中为指定内容发布者创建角色

当配置 BW 以便与 BI 平台集成时，请评估当前的角色结构是否允许将特定的 BW 用户快速指定为 BI 平台系统的内容发布者或系统管理员。

建议为以说明性方式创建的任何新角色加上标记。说明性角色名称的示例包括 BOE_CONTENT_PUBLISHERS 和 SBOP_SYSTEM_ADMINISTRATORS。

提示：

可以向管理员用户分配全部或部分系统管理权限。

要修改在 BI 平台中向这些新角色（或任何现有角色）授予的权限，必须首先设置 SAP 身份验证，并导入角色。然后，可以通过使用中央管理控制台修改每个导入角色的权限。

有关创建角色的详细信息，请参阅 SAP 文档。有关在管理内容中的角色使用的更多信息，请参阅下面的章节：

- 第 287 页上的 [“导入 SAP 角色”](#)。
- 第 751 页上的 [“在 BI 平台中设置文件夹和安全性”](#)。
- 第 752 页上的 [“了解默认的文件夹安全模式”](#)。

24.1.1.8 配置对内容管理工作台的访问

对于可访问内容管理工作台的每种类型的用户，都必须在 BW 中应用适当的授权组。下表中列出了这些授权。

表24-1：管理用户的授权

授权对象	字段	值
S_RFC S_TCODE	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH、SH3A、SUNI
	ACTVT	Execute (16)
	TCD	/CRYSTAL/RPTADMIN、RSCR_MAINT_PUBLISH
S_TABU_CLI	CLIIDMAINT	X
S_TABU_DIS	ACTVT	Change、Display (02、03)
	DICBERCLS	&NC&
	JOBACTION	DELE、RELE
	JOBGROUP	，
S_RS_ADMWB	ACTVT	Execute (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	Create new、Change、Display、Delete (01、02、03、06)

授权对象	字段	值
ZCNTADMJOB	ACTVT	Create new、Delete (01、06)
ZCNTADMRPT	ACTVT	Display、Delete、Activate、Maintain、Check (03、06、07、23、39)

表24-2：内容发布者的授权

授权对象	字段	值
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/CE_SYNCH、SH3A、SUNI
	ACTVT	Execute (16)
	TCD	/CRYSTAL/RPTADMIN
S_BTCH_JOB	JOBACTION	DELE、RELE
	JOBGROUP	，
	ACTVT	Execute (16)
	RSADMWBOBJ	WORKBENCH
ZCNTADMCES	ACTVT	Display (03)
ZCNTADMJOB	ACTVT	(New、Delete) 01、06

授权对象	字段	值
ZCNTADMRPT	ACTVT	Display、Activate、Main- tain、Check (03、07、23、39) Delete (可选) (06) Edit (可选) (02)

可以选择是否授予内容发布者在 BW 内容管理工作台中删除报表的权限。但是请注意，在 BW 中删除报表也会在 BI 平台中删除该报表。如果发布者没有足够的权限在平台中删除报表，则会导致出现错误。

内容使用者的授权

授权对象	字段	值
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SH3A、SUNI
	ACTVT	Execute (16)
	TCD	/CRYSTAL/RPTADMIN
S_RS_ADMWB	ACTVT	Execute (16)
	RSADMWBOBJ	WORKBENCH
	ACTVT	Display (03)

24.1.1.9 定义 BI 平台系统

您必须在内容管理工作台中为要将报表发布到的每个 BI 平台系统创建系统定义。

24.1.1.9.1 添加 BI 平台系统

- 1 执行事务 /crystal/rptadmin 以访问内容管理工作台。
- 2 从“操作”窗格中，选择“Enterprise 系统”。
- 3 双击“添加新系统”。
- 4 在“系统”选项卡上：
 - 在“别名”字段中，键入一个说明性名称。请避免使用空格或特殊字符，因为如果在配置为 Enterprise Portal 时使用别名，这些字符需要特殊对待。
 - 键入正在运行 CMS 的计算机的名称。如果将 CMS 配置为侦听非默认端口，请键入 CMS 名称:端口
 - 如果要从没有明确分配给 BI 平台系统的任何角色向此系统发布报表，请选择“默认系统”。只能设置一个默认 BI 平台系统。

在所有可用系统的列表中，默认系统以绿色复选标记表示。

- 5 单击“保存”。
- 6 在“RFC 目标”选项卡上，添加与此系统关联的每个 RFC 目标。
要添加目标，请单击“插入行”按钮。在出现的列表中，双击 RFC 目标的名称。

注意：

一个 BI 平台系统可以有多个目标，以增加系统冗余。请参阅“分布 BW 发布器安装”。

- 7 选中位于所添加的目标名称旁的复选框，并单击“Verify BOE definition”（验证 BOE 定义）。
该测试将验证 BW 能够与指定的 BW 发布器联系，并能够使用 Crystal 权利用户帐户登录此系统。
- 8 在“HTTP”选项卡上：
 - 如果已为 HTTPS 配置了连接到 BI 平台的 Web 服务器，则可在“协议”字段中键入“http”或“https”。
 - 在“Web 服务器主机和端口”字段中，键入承载 BI 启动板的 Web 服务器的完全限定域名或 IP 地址。对于使用 Java 应用程序服务器的安装，请包括端口号。例如，键入“boserver01.businessobjects.com:8080”。
 - 在“路径”字段中，键入“SAP”
该路径实际上是 Web 服务器在引用 BI 平台 Web 内容的 sap 子文件夹时所使用的虚拟路径。只有在自定义了 Web 环境和平台 Web 内容文件位置的情况下，才提供替代值。
不要在此条目的开头或末尾包含正斜线。
- 在“查看器应用程序”字段中，键入查看器应用程序的名称。

要使用默认 BI 平台查看器（使用 Java 版的 BI 启动板），请键入 “openDocument.jsp”

如果使用默认 ASP.NET 配置在 Windows 上安装 BI 平台，请键入 report/report_view.aspx，以使用默认浏览器。

9. 在“语言”选项卡上，选择将发布到此系统的报表的语言。
10. 在“角色”选项卡中，添加希望与此 BI 平台系统关联的内容承载角色。
请参阅“导入 SAP 角色”。
11. 单击“插入行”按钮。

即可显示一个可以添加到此系统的角色的列表。

注意：

每个角色只能发布到一个 BI 平台系统。如果要添加到此 BI 平台系统的角色没有显示在该列表中，请单击“取消”以返回到“角色”选项卡，并单击“重新分配角色”。

12. 选择要发布到此系统的角色，然后单击“确定”。
13. 在“布局”选项卡中，为发布到此 BI 平台系统的报表和角色文件夹选择默认安全设置。

注意：

- 在 BI 平台中会为发布到该系统的每个角色自动创建一个文件夹。该文件夹包含在该角色下发布的报表的快捷方式。
- 一旦您配置了 BI 平台系统，更改此处的默认安全级别不会影响已发布的角色文件夹或报表的安全级别。要更改已发布到平台的所有角色和内容的默认安全级别，请删除系统中的角色文件夹和快捷方式。（这将不会删除实际的报表。）在此处更改安全设置，并重新发布角色和报表。

14. 单击底部的“确定”按钮，保存设置并在内容管理工作台中创建 BI 平台系统。

现在即可从 BW 向 BI 平台发布报表。

相关主题

- 第 754 页上的[“分布 BW 发布者安装”](#)
- 第 287 页上的[“导入 SAP 角色”](#)

24.1.1.10 使用内容管理工作台发布报表

将报表保存到 BW 之后，可以使用内容管理工作台发布该报表。可以使用内容管理工作台发布单独的报表，也可以发布保存到特定角色的所有报表。只有拥有 Crystal 内容发布者权限的用户（请参阅第 782 页上的[“创建并应用授权”](#)）才能使用内容管理工作台发布和维护报表。

24.1.1.11 发布角色或报表

- 1 执行事务 /crystal/rptadmin 以访问内容管理工作台。
- 2 从“操作”窗格上，选择“发布报表”。
- 3 要找到保存到 BW 系统的内容，请双击“选择要发布的报表和角色”。
即可出现一个对话框，用于帮助过滤可用角色和报表。
- 4 从该列表中，选择包含要显示内容的一个或多个系统。

注意：




该列表包含在此 BW 系统上定义的所有可用系统。

- 5 接下来，过滤结果以限制将要显示的报表和角色的数量。使用这些选项：
 - 对象版本
选择“A: 激活的”显示可以发布的所有报表。选择空白选项则显示所有报表。（其余选项是 SAP 保留项。）
 - 对象状态
选择“ACT 活动，可执行”只显示已经发布的报表。选择“INA 非活动，不可执行”只显示没有发布的报表。将该字段留空将显示所有报表。（其余选项是 SAP 保留项。）
 - 角色过滤器
如果在此框内键入文本，则将只显示与在此键入的内容匹配的角色。使用 * 作为通配符。例如，要显示以字母 d 开头的所有角色，请键入“d*”。
 - 报表说明
如果在此框内键入文本，则将只显示那些说明中包含在此键入的内容的报表。使用 * 作为通配符，用来匹配任意数量的字符。使用 + 作为通配符，用来匹配 0 或 1 个字符。例如，要显示说明中包含 revenue 一词的所有报表，请键入 *revenue*。
- 6 单击“确定”。

符合条件的报表的列表将显示在右侧面板中。

这些报表按层次结构排列：BI 平台系统 > 在该系统上的角色 > 保存到该角色的报表。

层次结构中的每一项都使用一个红色、黄色或绿色的点来标记。在层次结构中级别较高的项目反映了它们所包含项目的状态，最不利的状况被过滤到层次结构的顶层。例如，如果角色中的一个报表是黄色的（激活），而剩下的所有报表都是绿色的（已发布），那么角色显示为黄色（激活）。

-  绿色：项目已完全发布。如果项目是一个 BI 平台系统或角色，则该项目中的所有报表都已发布。
-  黄色：项目是激活的，但未发布。如果该项目是一个报表，则它可用于发布。如果该项目是角色或 BI 平台系统，则所有内容都是活动的，并且尚未发布角色或系统所包含的至少一个项目。
-  红色：该项目是 SAP 内容，无法使用内容管理工作台进行发布。在使用 BW 管理工作台激活内容之前，内容不可用于发布。

7. 选择您希望发布的报表。

要发布角色中的所有报表，请选择该角色。要在 BI 平台系统上发布所有角色，请选择该系统。

注意：

当您选择一个角色（或系统）时，该角色（或系统）中包含的所有报表都将被选中。要清除该选择，请清除该角色（或系统）复选框，然后单击“刷新”。

8. 单击“发布”。

注意：

后台发布的作为系统资源进行处理的报表会变为可用。要使用此选项，请单击“在后台”，而不是“发布”。

9. 单击“刷新”以更新内容管理工作台内的 BI 平台系统、角色和报表状态的显示。

提示：

要查看报表，请右击该报表，然后选择“查看报表”。要查看该报表使用了哪些查询，请右击该报表，然后选择“使用的查询”。

注意：

将报表发布到 BI 平台后，如果要覆盖所发布的报表，请单击“覆盖”。

相关主题

- 第 764 页上的[“计划后台发布”](#)

24.1.1.12 计划后台发布

在后台立即或作为计划的作业来发布报表可以节约系统资源。建议在后台发布报表，以提高系统响应能力。

作为计划的作业定期发布报表会同步 BW 和 BI 平台部署之间的报表信息。建议计划所有报表（或包含这些报表的角色）。还可以通过使用“报表维护”操作的“更新状态”选项，手动同步角色和报表。有关详细信息，请参阅第 765 页上的[“更新报表状态”](#)。

24.1.1.13 更新已发布报表的系统信息

BW 发布器使用在此处输入的 SAP 系统信息来更新已发布报表的数据源。可以选择使用本地 BW 应用程序服务器；如果要使用负载均衡配置，则可以使用中央 BW 实例。

24.1.1.14 维护报表

报表维护任务包括：在 BI 平台和 BW 之间同步有关报表的信息（更新状态）、删除不需要的报表（删除报表）以及更新从以前版本的 BI 平台中迁移的报表（迁移后处理）。

24.1.1.14.1 更新报表状态

如果在 BI 平台系统上对已发布的报表进行更改（例如更改将报表发布到的角色），则在同步 BI 平台与 BW 之前，BW 中不会体现所做的更改。用户可以计划一个发布作业，定期将 BI 平台与 BW 同步（请参阅第 764 页上的 [“计划后台发布”](#)），也可以使用“报表维护”工具手动更新报表状态。

24.1.1.14.2 删除报表

使用内容管理工作台从 BW 中删除已发布的报表时，还将从 BI 平台中删除该报表。用户只有获得删除 BW 和 BI 平台系统上的报表所需的授权，才能删除报表。

注意：

如果用户有权在 BW 上删除报表，但无权在发布报表的 BI 平台系统上删除报表，则可能会遇到错误。

24.1.1.15 配置 SAP http 请求处理程序

要启用在 BW 中查看报表，必须将 BW 配置为使用 HTTP 请求处理程序。该处理程序包括在内容管理工作台。这样，当 BW 用户从 SAPGUI 中打开 Crystal 报表时，BW 能够通过 Web 正确地路由查看请求。

使用事务 SICF 访问 BW 系统上活动的虚拟主机和服务的列表。在 default_host 层次结构中的 BW 下创建名为 ce_url 的新节点，然后将 /CRYSTAL/CL_BW_HTTP_HANDLER 添加到处理程序列表中。可能需要在创建该服务之后手动激活它。

24.1.1.16 针对处理 SAP 数据的配置

24.1.1.16.1 以 SAP 的批处理模式处理计划的报表

对于 Windows 安装，可以使用 SAP 的批处理模式在 BI 平台中运行计划的报表。在将特定环境变量设为 1 时，InfoSet 和 OpenSQL 的驱动程序可使用 SAP 的批处理或后台模式运行报表。相关的环境变量为：

- CRYSTAL_INFOSET_FORCE_BATCH_MODE（用于 InfoSet 驱动程序）
- CRYSTAL_OPENSQL_FORCE_BATCH_MODE（用于 OpenSQL 驱动程序）

但是，建议您只在有 BI 平台分布式安装时使用该功能。当将这些环境变量设为 1 时，驱动程序均使用 SAP 的批处理模式运行报表，这与实际运行报表的报表创建组件无关。因此，如果在运行 BI 平台服务器组合的计算机上创建这些环境变量作为系统环境变量，驱动程序会以批处理模式运行所有报表（包括来自 Crystal Reports 处理服务器和报表应用程序服务器的按需报表请求）。

要确保驱动程序仅以批处理模式运行计划的报表（由自适应作业服务器运行的报表），请不要在运行 BI 平台服务器组合的计算机上设置系统环境变量。而应该按照下面的步骤为每个自适应作业服务器自定义环境变量。

注意：

在 BI 平台中计划报表的 SAP 用户可能需要 SAP 中的其他授权。

相关主题

- 第 805 页上的“[使用 Open SQL 查询以批处理方式计划报表](#)”

24.1.1.16.2 以 SAP 的批处理模式处理计划的报表

- 1 利用以下内容，在“记事本”之类的文本编辑器中创建批处理脚本（.bat 文件）：

```
@echo off
set CRYSTAL_INFOSET_FORCE_BATCH_MODE=1
set CRYSTAL_OPENSQ_L_FORCE_BATCH_MODE=1
%*
```

此脚本会将环境变量的值设为 1，然后执行从命令行传递到此脚本的任何参数。

- 2 将该文件以 jobserver_batchmode.bat 文件名保存到每台自适应作业服务器计算机的某个文件夹中。
 - 3 登录到中央管理控制台（CMC）。
 - 4 选择“服务器”。
 - 5 展开“服务类别”节点，并选择“分析服务”。
 - 6 选择“自适应处理服务器”，并在上下文菜单中选择“属性”。
- 此时，将弹出“属性”页面。
- 7 定位至“属性”页面中的“命令行参数”字段。

这就是自适应作业服务器的命令。例如：

```
"\\SERVER01\C$\Program Files\SAO Business Objects\SAP BusinessObjects Enterprise\win32_x86\JobServer.exe" -service -name SERVER01.report -ns SERVER01 -objectType BusinessObjects Enterprise.Report -lib procReport -restart
```

- 8 将保存在自适应作业服务器计算机上的 jobserver_batchmode.bat 文件的完整路径放在该默认命令前面。

在本例中，批处理文件保存在名为 SERVER01 的计算机上，如下所示：

```
C:\Crystal Scripts\jobserver_batchmode.bat
```

自适应作业服务器的新命令为：

```
"\\SERVER01\C$\Crystal Scripts\jobserver_batchmode.bat" "\\SERVER01\C$\Program Files\SAP Business Objects\SAP  
BusinessObjects Enterprise 12.0\win32_x86\JobServer.exe" -service -name SERVER01.report -ns SERVER01  
-objectType BusinessObjects Enterprise.Report -lib procReport -restart
```

这个新启动命令会首先启动该批处理文件。然后，该批处理文件会在执行自适应作业服务器的原命令前设置所需的环境变量。这样，就可以确保自适应作业服务器可用的环境变量不同于负责按需创建报表的服务器（Crystal Reports 处理服务器和报表应用程序服务器）可用的环境变量。

9. 单击“保存并关闭”。
10. 右键单击自适应作业服务器，并在上下文菜单中选择“启动”。

注意：

如果自适应作业服务器启动失败，请验证您的新启动命令。

24.1.1.17 针对 SAP 传输的配置

24.1.1.17.1 概述

BI 平台包括以下这些传输：

- OpenSQL 连接传输
- InfoSet 连接传输
- 行级安全定义传输
- 群集定义传输
- 内容管理工作台传输
- BW 查询参数个性化传输
- MDX 传输
- ODS 传输

传输有两个不同的集：Unicode 兼容传输和 ANSI 传输。如果您运行的是 BASIS 系统 6.20 或更高版本，请使用 Unicode 兼容传输。如果您运行的是 BASIS 系统 6.20 之前的版本，请使用 ANSI 传输。所有安装的传输都位于产品分发介质上的以下目录中：\Collaterals\Add-Ons\SAP\Transports\。

注意：

在检查可能存在的安装冲突时，请确保 SAP 系统中没有这些对象名称存在。默认情况下，对象使用 /crystal/ 命名空间，因此用户不必自己创建此命名空间。如果手动创建了 /crystal/ 命名空间，则会提示用户输入用户无法访问的许可证修复密钥。

24.1.1.17.2 配置传输

要设置 BI 平台数据访问或 BW 发布器组件，必须将相应的传输导入 SAP 系统中。在与 SAP 系统进行通信时，这些组件会使用这些传输文件的内容。

SAP 系统上所需的安装与配置过程必须由熟悉更改和传输系统且拥有 SAP 系统管理权限的 BASIS 专家执行。根据您所运行的 BASIS 版本，导入传输文件的具体过程可能不同。有关的特定过程性详细信息，请参阅 SAP 文档。

当您第一次部署数据访问组件时，默认情况下，任何用户均可访问您的所有 SAP 表。为保护用户可访问的 SAP 数据，请使用安全定义编辑器。

在导入传输后，您必须配置相应的用户访问级别。创建所需的授权，并通过配置文件或角色将这些授权应用于将设计、运行或计划 Crystal 报表的 SAP 用户。

相关主题

- 第 782 页上的“[创建并应用授权](#)”

24.1.1.17.2.1 传输类型

传输有两个不同的集：Unicode 兼容传输和 ANSI 传输。如果您运行的是 BASIS 系统 6.20 或更高版本，请使用 Unicode 兼容传输。如果您运行的是 BASIS 系统 6.20 之前的版本，请使用 ANSI 传输。所有安装的传输都位于产品分发上的以下目录中：\Collaterals\Add-Ons\SAP\Transports\。transports.txt 文件列出了 Unicode 兼容和 ANSI 传输文件。

下面描述了各种传输类型：

- OpenSQL 连接传输

OpenSQL 连接传输使 OpenSQL 驱动程序能够连接到 SAP 系统并依据 SAP 系统创建报表。

- 行级安全定义传输

这种传输提供安全定义编辑器，该工具用作 OpenSQL 连接传输中 /crystal/auth 表的图形界面。

- 群集定义传输

这种传输提供群集定义工具。此工具使您能够为 ABAP 数据群集定义建立元数据资源库。这些定义为 OpenSQL 驱动程序提供所需的信息以便依据这些数据群集创建报表。

注意：

ABAP 数据群集与群集表不同。群集表是已经在 DDIC 中定义的。

- InfoSet 连接传输

InfoSet 连接传输使 InfoSet 驱动程序能够访问 InfoSet 和 SAP 查询。

- 内容管理工作台传输

这种传输为 BW 系统提供内容管理功能。它只能作为 UNICODE 兼容传输使用。

- BW 查询参数个性化传输

这种传输提供对基于 BW 查询的报表个性化和默认参数值的支持。

- BW MDX 连接传输

此传输使 MDX 查询驱动程序能够访问 BW 多维数据集和查询。此传输与 BW 3.0B 修补程序 27 或更高版本以及 BW 3.1C 修补程序 21 或更高版本兼容。

- ODS 连接传输

此传输使 ODS 查询驱动程序能够访问 ODS 数据。此传输与 BW 3.0B 修补程序 27 或更高版本以及 BW 3.1C 修补程序 21 或更高版本兼容。

24.1.1.17.2.2 检查冲突

当导入传输文件时，这些文件的内容会自动在 SAP BusinessObjects 命名空间下注册。为此，最新版本 R/3 和 MY SAP ERP 保留了 SAP BusinessObjects 命名空间。但是，某些对象（如授权对象、授权类和旧有对象）的对象名可能不包含相应的前缀。建议用户在导入传输文件之前先检查这些对象类型是否发生冲突。

如果 SAP 系统中已经存在函数组、任何功能模块或任何其他对象，则在导入 SAP BusinessObjects 传输文件前必须解析命名空间。有关适合您的 SAP 版本的过程，请参阅 SAP NetWeaver 文档。

24.1.1.17.2.3 导入传输文件

阅读位于产品分发介质上以下目录中的 transports_EN.txt 文件：\Collaterals\Add-Ons\SAP\Transports\。此文本文件列出了构成每种传输的文件的确切名称。（transports 目录下的 cofiles 和 data 目录与您的 SAP 服务器上的 .../trans/cofiles 和 .../trans/data 目录相对应。）

在导入行级安全定义或群集定义传输前，您必须导入 OpenSQL 连接传输。其他传输可以按任意顺序导入。

注意：

- 将文件从 CD 复制到服务器后，请确保在导入传输前所有文件均为可写文件。如果导入文件是只读文件，导入将失败。
- 由于传输是二进制文件，因此，在 Unix 安装上，必须通过 FTP 以二进制模式添加这些文件（以避免损坏文件）。此外，您还必须具有 Unix 服务器的写权限。

24.1.1.17.2.4 传输

24.1.1.17.2.4.1 OpenSQL 连接传输

OpenSQL 连接传输使驱动程序能够连接到 SAP 系统并依据 SAP 系统创建报表。

对象	类型	说明
/CRYSTAL/BC	包	开发类

对象	类型	说明
/CRYSTAL/OPENSQL	函数组	OpenSQL 函数
/CRYSTAL/OSQL_AUTH_FORMS	程序	辅助程序
/CRYSTAL/OSQL_EXECUTE	程序	辅助程序
/CRYSTAL/OSQL_TYPEPOOL PROG	程序	辅助程序
/CRYSTAL/OSQL_TYPEPOOLS	程序	辅助程序
/CRYSTAL/OSQL_UTILS	程序	辅助程序
ZSSI	授权对象类	报表创建授权对象
ZSEGREPORT	授权对象	报表创建授权对象
/CRYSTAL/OSQL_CLU_AC TKEY_ENTRY	表	群集元数据
/CRYSTAL/OSQL_FCN_PARAM	表	函数元数据
/CRYSTAL/OS QL_FCN_PARAM_FIELD	表	函数元数据
/CRYSTAL/OSQL_FIELD_ENTRY	表	表元数据
/CRYSTAL/OSQL_OBJECT_EN TRY	表	表元数据
/CRYSTAL/OSQL_RLS_CHK_EN TRY	表	RLS 元数据

对象	类型	说明
/CRYSTAL/OSQL_RLS_FCN_ENTRY	表	RLS 元数据
/CRYSTAL/OSQL_RLS_VAL_ENTRY	表	RLS 元数据
ZCLUSTDATA	表	群集元数据
ZCLUSTID	表	群集元数据
ZCLUSTKEY	表	群集元数据
ZCLUSTKEY2	表	群集元数据
/CRYSTAL/AUTHCHK	表	RLS 元数据
/CRYSTAL/AUTHFCN	表	RLS 元数据
/CRYSTAL/AUTHKEY	表	RLS 元数据
/CRYSTAL/AUTHOBJ	表	RLS 元数据
/CRYSTAL/AUTHREF	表	RLS 元数据
ZSSAUTHCHK	表	以前的 RLS 元数据
ZSSAUTHOBJ	表	以前的 RLS 元数据
ZSSAUTHKEY	表	以前的 RLS 元数据
ZSSAUTHREF	表	以前的 RLS 元数据
ZSSAUTH FCN	表	以前的 RLS 元数据

24.1.1.17.2.4.2 InfoSet 连接传输

InfoSet 连接传输使 InfoSet 驱动程序能够访问 InfoSet。这种传输与 R/3 4.6c 及更高版本兼容。如果运行的是 SAP R/3 4.6a 或更低版本，请不要导入这种传输。

对象	类型	说明
/CRYSTAL/BC	包	开发类
/CRYSTAL/FLAT	函数组	InfoSet 封装函数
/CRYSTAL/QUERY_BATCH	程序	批处理模式执行
/CRYSTAL/QUERY_BATCH_STREAM	程序	流式批处理模式执行。

24.1.1.17.2.4.3 行级安全定义传输

这种传输提供安全定义编辑器，该工具用作 OpenSQL 连接传输中 /CRYSTAL/AUTH 表的图形界面。

对象	类型	说明
/CRYSTAL/BC	包	开发类
/CRYSTAL/TABMNT	函数组	用于函数限制的表维护视图的函数组

对象	类型	说明
/CRYSTAL/RLSDEF	程序	主程序
/CRYSTAL/RLS_INCLUDE1	程序	含有模块定义的包含程序
/CRYSTAL/RLS_INCLUDE2	程序	含有子例程定义的包含程序
TDDAT [/CRYSTAL/AUTHFCN]	表内容	表维护定义
TVDIR [/CRYSTAL/AUTHFCN]	表内容	表维护定义
/CRYSTAL/AUTHFCNS	传输和维护对象的定义	表维护定义
/CRYSTAL/RLS	事务	主程序事务
/CRYSTAL/RLSFCN	事务	主程序在内部调用的辅助程序事务。

24. 1. 1. 17. 2. 4. 4 群集定义传输

这种传输提供群集定义工具。此工具使您能够为 ABAP 数据群集定义建立元数据资源库。这些定义为 OpenSQL 驱动程序提供所需的信息以便依据这些数据群集创建报表。

注意：
ABAP 数据群集与群集表不同。群集表是已经在 DDIC 中定义的。

对象	类型	说明
ZCIMPRBG	程序	主程序

对象	类型	说明
ZCRBGTOP	程序	包含程序
ZCDD	事务	主程序事务

24.1.1.17.2.4.5 内容管理工作台传输

这种传输为 BW 系统提供内容管理功能。它只能作为 Unicode 兼容传输使用。

对象	类型	说明
/CRYSTAL/BC	包	开发类
/CRYSTAL/CL_BW_HTTP_HANDLER	类	多个识别 CE 的 HTTP 请求处理程序
/CRYSTAL/OBJECT_STATUS_DOM	域	报表活动
/CRYSTAL/OBJ_POLICY_DOM	域	CE 对象安全
/CRYSTAL/OBJECT_STATUS	数据元素	报表活动
/CRYSTAL/OBJ_POLICY	数据元素	CE 对象安全
/CRYSTAL/CE_SYNC	函数组	发布者存根
/CRYSTAL/CA_MSG	消息类	状态消息

对象	类型	说明
/CRYSTAL/CE_SYNCH_FORMS	程序	程序组件
/CRYSTAL/CONTENT_ADMIN	程序	程序组件
/CRYSTAL/CONTENT_ADMIN_CLASS_D	程序	程序组件
/CRYSTAL/CONTENT_ADMIN_CLASS_I	程序	程序组件
/CRYSTAL/CONTENT_ADMIN_CTREE	程序	程序组件
/CRYSTAL/CONTENT_ADMIN_FORMS	程序	程序组件
/CRYSTAL/CONTENT_ADMIN_MODULES	程序	程序组件
/CRYSTAL/CONTENT_ADMIN_PAIS	程序	程序组件
/CRYSTAL/CONTENT_ADMIN_PBOS	程序	程序组件
/CRYSTAL/CONTENT_ADMIN_TAB_FRM	程序	程序组件
/CRYSTAL/CONTENT_ADMIN_TOP	程序	程序组件
/CRYSTAL/PUBLISH_WORKER	程序	程序组件
/CRYSTAL/PUBLISH_WORKER_DISP	程序	程序组件

对象	类型	说明
/CRYSTAL/PUBLISH_WORKER_DISP_I	程序	程序组件
/CRYSTAL/PUBLISH_WORKER_FORMS	程序	程序组件
/CRYSTAL/PUBLISH_WORKER_PROC	程序	程序组件
/CRYSTAL/PUBLISH_WORKER_PROC_I	程序	程序组件
/CRYSTAL/PUBLISH_WORKER_SCREEN	程序	程序组件
/CRYSTAL/CA_DEST	表	应用程序状态
/CRYSTAL/CA_JOB	表	应用程序状态
/CRYSTAL/CA_JOB2	表	应用程序状态
/CRYSTAL/CA_LANG	表	应用程序状态
/CRYSTAL/CA_PARM	表	应用程序状态
/CRYSTAL/CA_ROLE	表	应用程序状态
/CRYSTAL/CA_SYST	表	应用程序状态
/CRYSTAL/MENU_TREE_ITEMS	结构	应用程序状态
/CRYSTAL/REPORT_ID	表	应用程序状态
/CRYSTAL/RPTADMIN	事务	主程序事务

对象	类型	说明
/CRYSTAL/EDIT_REPORT	程序	报表编辑封装
/CRYSTAL/EDIT_REPORT	函数组	报表编辑函数
ZSSI	授权对象类	Crystal 授权
ZCNTADMCES	授权对象	CE 操作
ZCNTADMRPT	授权对象	报表操作
ZCNTADMJOB	授权对象	后台作业操作

24.1.1.17.2.4.6 ODS 连接传输

此传输使 ODS 查询驱动程序能够访问 ODS 数据。此传输与 BW 3.0B 修补程序 27 或更高版本以及 BW 3.1C 修补程序 21 或更高版本兼容。

对象	类型	说明
/CRYSTAL/BC	包	开发类
/CRYSTAL/ODS_REPORT	函数组	ODS 函数

24.1.1.17.2.4.7 BW 查询参数个性化传输

这种传输提供对基于 BW 查询的报表个性化和默认参数值的支持。

对象	类型	说明
/CRYSTAL/BC	包	开发类
/CRYSTAL/PERS_VAR	结构	变量定义
/CRYSTAL/PERS_VALUE	结构	值定义
/CRYSTAL/PERS	函数组	个性化函数

24.1.1.17.2.4.8 BW MDX 连接传输

此传输使 MDX 查询驱动程序能够访问 BW 多维数据集和查询。此传输与 BW 3.0B 修补程序 27 或更高版本以及 BW 3.1C 修补程序 21 或更高版本兼容。

对象	类型	说明
/CRYSTAL/BC	包	开发类
/CRYSTAL/MDX	函数组	MDX 函数
/CRYSTAL/MDX_STREAM_LAYOUT	表定义	数据集结构
/CRYSTAL/CX_BAPI_ERROR	类	例外

对象	类型	说明
/CRYSTAL/CX_METADATA_ERROR	类	例外
/CRYSTAL/CX_MISSING_STREAMINFO	类	例外
/CRYSTAL/CX_NO_MORE_CELLS	类	例外
/CRYSTAL/CX_NO_MORE_MEMBERS	类	例外
/CRYSTAL/CX_NO_MORE_PROPERTIES	类	例外
/CRYSTAL/CX_SAVE_SESSION_STATE	类	例外
/CRYSTAL/MDX_APPEND_DATA	类	数据集处理器
/CRYSTAL/MDX_READER_BASE	类	数据集处理器
/CRYSTAL/MDX_READ_DIMENSIONS	类	数据集处理器
/CRYSTAL/MDX_READ_MEASURES	类	数据集处理器
/CRYSTAL/MDX_READ_PROPERTIES	类	数据集处理器
/CRYSTAL/MDX_AXIS_LEVELS	表类型	元数据结构
/CRYSTAL/MDX_PROPERTY_KEYS	表类型	元数据结构

对象	类型	说明
/CRYSTAL/MDX_PROPERTY_VALUES	表类型	元数据结构
/CRYSTAL/MDX_STREAM_LAYOUT_TAB	表类型	元数据结构

24.1.1.18 授权概述

本节提供一个 SAP 授权列表，依据我们的经验和测试，这些授权是在集成的 SAP 环境中执行常见 BI 平台任务所必需的。根据具体实现，可能还会需要其他授权对象或字段。

必须从每个授权对象创建一个授权并定义相应的字段值。然后就可以将相应的授权作用于 SAP 用户的配置文件（或角色）。下面的部分介绍所需的授权并提供必需的字段值。有关您的 SAP 版本特定的详细过程信息，请参阅 您的 SAP 文档。

注意：

- 本节中的信息仅做指导之用。
- ZSEGREPORT 授权对象属于 ZSSI 对象类，当导入支持 Open SQL 查询所需的 SAP 集成传输文件时会安装该对象类。

24.1.1.18.1 创建并应用授权

必须创建并应用每位用户使用 SAP Desktop Intelligence Integration 访问信息所需的授权。创建、配置及应用授权的具体步骤取决于已安装的 SAP 版本。本节提供了 SAP 授权列表，依据我们的经验和测试环境，这些授权是在集成的 SAP NetWeaver ABAP 环境中使用 BI 平台执行常见任务所必需的。根据具体实现，可能还会需要其他授权对象或字段。

相关主题

- 第 756 页上的“[在内容管理工作台中配置发布](#)”

24.1.1.19 BW 中的操作

本节介绍 BW 中的各种操作。

24.1.1.19.1 Crystal Reports 中的操作

24.1.1.19.1.1 从 BW 角色中的查询创建新报表

授权对象	字段	值
S_USER_AGR	ACT_GROUP	USER_ROLE*
	ACTVT	01、02、06

授权对象	字段	值
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 是指用户所属的任何角色的名称。可以在此字段中输入多个值。

* QUERY_OWNER 是指查询的所有者的名称。如果指定名称，则只能依据该所有者的查询创建报表。
输入 * 可以依据任何所有者的查询创建报表。

** 对于 INFO_AREA、INFO_CUBE 或 COMP_ID，可以输入 * 代表任意值。如果指定一个特定值，则只能依据包含这些信息区域、多维数据集和部件 ID 的查询创建报表。

24.1.1.19.1.2 从 BW 角色打开现有报表

授权对象	字段	值
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SUSO、SUNI、RSCR、SH3A、RFC1、RZX0、RZX2、RS_PERS_BOD、/CRYSTAL/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 是指创建报表所依据的查询的所有者名称。如果输入查询所有者的名称，则只能依据该所有者的查询创建报表。可以输入 * 代表任意查询所有者。

** 对于 INFO_AREA、INFO_CUBE 或 COMP_ID，可以输入 * 代表任意值。如果指定一个特定值，则只能依据包含这些信息区域、多维数据集和部件 ID 的查询创建报表。

24.1.1.19.1.3 预览或刷新报表

授权对象	字段	值
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 是指创建报表所依据的查询的所有者名称。如果输入查询所有者的名称，则只能依据该所有者的查询创建报表。可以输入 * 代表任意查询所有者。

** 对于 INFO_AREA、INFO_CUBE 或 COMP_ID，可以输入 * 代表任意值。如果指定一个特定值，则只能依据包含这些信息区域、多维数据集和部件 ID 的查询创建报表。

24.1.1.19.1.4 验证数据库（刷新报表中的表定义）

授权对象	字段	值
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 是指创建报表所依据的查询的所有者名称。如果输入查询所有者的名称，则只能依据该所有者的查询创建报表。可以输入 * 代表任意查询所有者。

** 对于 INFO_AREA、INFO_CUBE 或 COMP_ID，可以输入 * 代表任意值。如果指定一个特定值，则只能依据包含这些信息区域、多维数据集和部件 ID 的查询创建报表。

24.1.1.19.1.5 设置数据源的位置

授权对象	字段	值
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 是指创建报表所依据的查询的所有者名称。如果输入查询所有者的名称，则只能依据该所有者的查询创建报表。可以输入 * 代表任意查询所有者。

** 对于 INFO_AREA、INFO_CUBE 或 COMP_ID，可以输入 * 代表任意值。如果指定一个特定值，则只能依据包含这些信息区域、多维数据集和部件 ID 的查询创建报表。

24. 1. 1. 19. 1. 6 将报表保存到 BW 角色

授权对象	字段	值
S_USER_AGR	ACT_GROUP	USER_ROLE*
	ACTVT	01、02、06

授权对象	字段	值
S_CTS_ADMI	CTS_ADMFCT	TABL

* USER_ROLE 是指用户所属的任何角色的名称。可以在此字段中输入多个值。

24.1.1.19.1.7 在向 BW 保存报表时准备报表以供翻译

授权对象	字段	值
S_USER_AGR	ACT_GROUP	USER_ROLE*
	ACTVT	01
S_CTS_ADMI	CTS_ADMFCT	TABL

* USER_ROLE 是指用户所属的任何角色的名称。可以在此字段中输入多个值。

24.1.1.19.1.8 保存报表并同时将其发布到 BI 平台

授权对象	字段	值
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 ***
S_RS_COMP1	RSZCOMPID	COMP_ID ***
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER **
	ACTVT	16

* USER_ROLE 是指用户所属的任何角色的名称。可以在此字段中输入多个值。

** QUERY_OWNER 是指创建报表所依据的查询的所有者名称。如果输入查询所有者的名称，则只能依据该所有者的查询创建报表。可以输入 * 代表任意查询所有者。

** 对于 INFO_AREA、INFO_CUBE 或 COMP_ID，可以输入 * 代表任意值。如果指定一个特定值，则只能依据包含这些信息区域、多维数据集和部件 ID 的查询创建报表。

24.1.1.19.1.9 启动 BEx 查询设计器

授权对象	字段	值
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_CTS_ADMI	CST_ADMFCT	TABL

* QUERY_OWNER 是指创建报表所依据的查询的所有者名称。如果输入查询所有者的名称，则只能依据该所有者的查询创建报表。可以输入 * 代表任意查询所有者。

** 对于 INFO_AREA、INFO_CUBE 或 COMP_ID，可以输入 * 代表任意值。如果指定一个特定值，则只能依据包含这些信息区域、多维数据集和部件 ID 的查询创建报表。

24.1.1.19.2 BI 启动板中的操作

24.1.1.19.2.1 使用 SAP 凭据登录到 BI 平台

授权对象	字段	值
S_ADMI_FCD	S_ADMI_FCD	STOR、STOM

24.1.1.19.2.2 按需查看 SAP BW 报表

授权对象	字段	值
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

授权对象	字段	值
S_RS_ODSO	RSINFOAREA	INFO_AREA**
	RSODSOBJ	OCRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* QUERY_OWNER 是指创建报表所依据的查询的所有者名称。如果输入查询所有者的名称，则只能依据该所有者的查询创建报表。可以输入 * 代表任意查询所有者。

** 对于 INFO_AREA、INFO_CUBE 或 COMP_ID，可以输入 * 代表任意值。如果指定一个特定值，则只能依据包含这些信息区域、多维数据集和部件 ID 的查询创建报表。

24.1.1.19.2.3 从查看器刷新报表

授权对象	字段	值
S_RS_COMP	RSINFOAREA	INFO_AREA**
	RSINFOCUBE	INFO_CUBE**
	RSZCOMPTP	REP
	RSZCOMPID	COMP_ID**

授权对象	字段	值
S_RS_COMP1	RSZCOMPID	COMP_ID**
	RSZCOMPTP	REP
	RSZOWNER	QUERY_OWNER*
	ACTVT	16
S_RS_ODSO	RSINFOAREA	INFO_AREA**
	RSODSOBJ	OCRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* QUERY_OWNER 是指创建报表所依据的查询的所有者名称。如果输入查询所有者的名称，则只能依据该所有者的查询创建报表。可以输入 * 代表任意查询所有者。

** 对于 INFO_AREA、INFO_CUBE 或 COMP_ID，可以输入 * 代表任意值。如果指定一个特定值，则只能依据包含这些信息区域、多维数据集和部件 ID 的查询创建报表。

24.1.1.19.2.4 计划报表

授权对象	字段	值
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	OCRM_OLVM
	RSODSPART	DATA
	ACTVT	03

* QUERY_OWNER 是指创建报表所依据的查询的所有者名称。如果输入查询所有者的名称，则只能依据该所有者的查询创建报表。可以输入 * 代表任意查询所有者。

** 对于 INFO_AREA、INFO_CUBE 或 COMP_ID，可以输入 * 代表任意值。如果指定一个特定值，则只能依据包含这些信息区域、多维数据集和部件 ID 的查询创建报表。

24.1.1.19.2.5 读取报表参数中的动态选取列表

授权对象	字段	值
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST、RSOB
	ACTVT	16

24.1.1.19.3 SAP NetWeaver (ABAP) 中的操作

24.1.1.19.3.1 在使用 OpenSQL 驱动程序的 Crystal Reports 内

本节介绍从 Crystal Reports 内使用 Open SQL 驱动程序可执行的各种 SAP NetWeaver (ABAP) 活动。

24. 1. 1. 19. 3. 2 登录 SAP 服务器

授权对象	字段	值
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST、/CRYSTAL/OPENSQL
	ACTVT	16

24. 1. 1. 19. 3. 3 创建新报表

授权对象	字段	值
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST、/CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	01

24. 1. 1. 19. 3. 4 打开或预览现有报表

授权对象	字段	值
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST、/CRYSTAL/OPENSQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

24. 1. 1. 19. 3. 5 验证数据库（刷新报表中的表定义）

授权对象	字段	值
S_ADMI_FCD	S_ADMI_FCD	STOR、STOM
ZSEGREPORT	ACTVT	02

授权对象	字段	值
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQ
	ACTVT	16

24.1.1.19.3.6 设置数据源的位置

授权对象	字段	值
ZSEGREPORT	ACTVT	02
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/OPENSQ
	ACTVT	16

24.1.1.19.4 使用 InfoSet 驱动程序和依据 InfoSet 创建报表的 Crystal Reports 中的操作

24. 1. 1. 19. 4. 1 登录 SAP 服务器

授权对象	字段	值
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

24. 1. 1. 19. 4. 2 通过 SAP NetWeaver（ABAP）上的 InfoSet 创建新报表

授权对象	字段	值
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	/CRYSTAL/FLAT、SKBW、AQRC
	ACTVT	16
S_CTS_ADMI	CTS_ADMFCT	TABL

注意：
同时添加足够的授权以查看数据行。例如 P_ORIG 或 P_APAP。

相关主题

- 第 801 页上的“[设置数据源的位置](#)”

24.1.1.19.4.3 验证数据库（刷新报表中的表定义）

授权对象	字段	值
S_ADMI_FCD	S_ADMI_FCD	STOR、STOM

24.1.1.19.4.4 设置数据源的位置

授权对象	字段	值
P_ABAP	REPID	AQTGSYSTGENERATESY、 SAPDBPNP
	COARS	2

24.1.1.19.5 使用 InfoSet 驱动程序和依据 ABAP 查询创建报表的 Crystal Reports 中的操作

24.1.1.19.5.1 登录 SAP 服务器

授权对象	字段	值
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST
	ACTVT	16

24.1.1.19.5.2 通过 SAP NetWeaver 上的 ABAP 查询创建新报表

授权对象	字段	值
P_ABAP	REPID	AQTG02=====P6、 SAPDBPNP
	COARS	2
S_ADMI_FCD	S_ADMI_FCD	STOR、STOM

授权对象	字段	值
S_TABU_DIS	ACTVT	03
	GROUP	表组的名称

24. 1. 1. 19. 5. 3 验证数据库

授权对象	字段	值
S_ADMI_FCD	S_ADMI_FCD	STOR、STOM
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SKBW
	ACTVT	16

24. 1. 1. 19. 5. 4 设置数据源的位置

授权对象	字段	值
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	表组的名称

24.1.1.19.6 BI 平台中的操作

24.1.1.19.6.1 以对话方式计划报表（使用 OpenSQL 查询）

授权对象	字段	值
S_USER_GRP	CLASS	
	ACTVT	03
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST、RFC1、/CRYSTAL/OPEN SQL
	ACTVT	16
ZSEGREPORT	ACTVT	02

注意：

CLASS 的值为空。

24.1.1.19.6.2 使用 Open SQL 查询以批处理方式计划报表

授权对象	字段	值
S_USER_GRP	CLASS	
	ACTVT	03

授权对象	字段	值
S_RFC	RFC_TYPE	FUGR
	RFC_NAME	SYST、RFC1、/CRYSTAL/OPEN SQL、SH3A
	ACTVT	16
S_BTCH_JOB	JOBGROUP	， ，
	JOBACTION	RELE
ZSEGREPORT	ACTVT	02
S_BTCH_ADM	BTCADMIN	Y

注意：
CLASS 的值为空。

24.1.1.19.6.3 Crystal 权利系统

授权对象	字段	值
文件访问授权 (S_DATASET)	活动 (ACTVT)	Read、Write (33、34)
	物理文件名 (FILENAME)	* (代表所有值)
	ABAP 程序名 (PROGRAM)	*

授权对象	字段	值
RFC 访问的授权检查 (S_RFC)	活动 (ACTVT)	16
	要保护的 RFC 名称 (RFC_NAME)	BDCH、STPA、SUSO、SUUS、 SU_USER、SYST、SUNI、 PRGN_J2EE、/CRYSTAL/SECURITY
	要保护的 RFC 对象类型 (RFC_TYPE)	函数组 (FUGR)
用户主维护：用户组 (S_US ER_GRP)	活动 (ACTVT)	Create 或 Generate 和 Display (03)
	用户主维护中的用户组 (CLASS)	<p>*</p> <p>注意： 为获得更高的安全性，可以 明确列出其成员需要访问 BI 平 台的用户组。</p>

24.1.1.19.6.4 运行和设计 BW BEx 查询

基于 BW BEx 查询从 Universe 中创建报表时，如果包含日期维，则系统管理员需要为设计 Universe 的用户和运行报表的用户授予 S_RS_I0BJ 权限。

授权对象	字段	值
S_RS_IOBJ	ACTVT	03
	RSIOBJ	
	RSIOBJ_CAT	
	RSIOBJ_PART	

24.2 针对 JD Edwards 集成的配置

24.2.1 为 SAP Crystal Reports 配置单一登录（SSO）

默认情况下，BI 平台将配置为允许 SAP Crystal Reports 用户使用单一登录（SSO）访问 JD Edwards EnterpriseOne 数据。

24.2.1.1 为 JD Edwards 和 SAP Crystal Reports 取消激活 SSO

- 1 在中央管理控制台（CMC）中，单击“应用程序”。
- 2 双击“Crystal Reports 配置”。
- 3 单击“单一登录选项”。

- 4 选择 crdb_pseone。
- 5 单击“删除”。
- 6 单击“保存并关闭”。
- 7 在 CMC 的“服务器”页面，选择“Crystal Reports 服务”并单击“重新启动服务器”。

24.2.1.2 为 JD Edwards 和 SAP Crystal Reports 激活 SSO

如果为 JD Edwards 和 SAP Crystal Reports 取消激活了 SSO，并希望重新激活它。

- 1 在中央管理控制台（CMC）中，单击“应用程序”。
- 2 双击“Crystal Reports 配置”。
- 3 单击“单一登录选项”。
- 4 在“使用以下驱动程序时，使用单一登录上下文进行数据库登录”下面，键入 crdb_pseone。
- 5 单击“添加”。
- 6 单击“保存并关闭”。
- 7 在 CMC 的“服务器”页面，选择“Crystal Reports 服务”并单击“重新启动服务器”。

24.2.2 为 JD Edwards 集成配置安全套接字层

可以在 BI 平台和 JD Edwards EnterpriseOne 部署中对客户端和服务器之间的所有网络通信使用安全套接字层（SSL）。

在 BI 平台使用 JD Edwards EnterpriseOne 数据需要对 SSL 配置进行部分更改。与其他 BI 平台服务器和客户端的 SSL 配置相似，将以下密钥和证书文件存储在一个可通过部署了 BI 平台的计算机访问的安全位置（在相同目录下）。

- 受信任的证书文件（cacert.der）。
- 生成的服务器证书文件（servercert.der）。
- 服务器密钥文件（server.key）。
- 密码短语文件（passphrase.txt）。

24.2.2.1 针对 SSL 启用 JD Edwards EnterpriseOne 数据连通性

注意：

以下过程中描述的所有值均区分大小写。

- 1 启动中央配置管理器（CCM）。
- 2 停止服务器智能代理（SIA）。
- 3 双击 SIA 打开“属性”对话框。
- 4 单击“协议”选项卡。
- 5 选择“启用 SSL”。
- 6 为“SSL 证书文件夹”选择包含 SSL 证书的目录。
- 7 为“服务器 SSL 证书文件”选择 servercert.der。
- 8 为“SSL 受信任证书文件”选择 cacert.der。
- 9 为“SSL 私钥文件”选择 server.key。
- 10 为“SSL 私钥密码短语文件”选择 passphrase.txt。
- 11 单击“应用”。
- 12 启动“服务器智能代理”。

必须重新启动 BI 平台报表服务器（如自适应作业服务器），才能使这些更改生效。

24.2.2.2 SSL 配置的属性文件

属性文件 sslconf.properties 包含 BI 平台使用的必需证书和密钥的所有信息。例如：

```
[default]
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

默认情况下，sslconf.properties 文件应放在 BI 平台的安装文件夹中：C:\Program Files\Business Objects\BusinessObjects 13.0。

24.3 针对 PeopleSoft Enterprise 集成的配置

24.3.1 为 SAP Crystal Reports 和 PeopleSoft Enterprise 配置单一登录 (SSO)

默认情况下，BI 平台将配置为允许 SAP Crystal Reports 用户使用单一登录 (SSO) 访问 PeopleSoft Enterprise 数据。

24.3.1.1 为 PeopleSoft Enterprise 和 SAP Crystal Reports 取消激活 SSO

- 1 在中央管理控制台 (CMC) 中，单击“应用程序”。
- 2 双击“Crystal Reports 配置”。
- 3 单击“单一登录选项”。
- 4 选择 `crdb_psenterprise`。
- 5 单击“删除”。
- 6 单击“保存并关闭”。
- 7 在 CMC 的“服务器”页面，选择“Crystal Reports 服务”并单击“重新启动服务器”。

24.3.1.2 为 PeopleSoft Enterprise 和 SAP Crystal Reports 激活 SSO

如果为 PeopleSoft Enterprise 和 SAP Crystal Reports 取消激活 SSO，并希望重新激活它。

- 1 在中央管理控制台 (CMC) 中，单击“应用程序”。
- 2 双击“Crystal Reports 配置”。
- 3 单击“单一登录选项”。
- 4 在“使用以下驱动程序时，使用单一登录上下文进行数据库登录”下面，键入 `crdb_psenterprise`。
- 5 单击“添加”。
- 6 单击“保存并关闭”。
- 7 在 CMC 的“服务器”页面，选择“Crystal Reports 服务”并单击“重新启动服务器”。

24.3.2 配置安全套接字层通信

可以为 BI 平台部署的客户端和服务端之间的所有网络通信使用安全套接字层（SSL）协议。

与其他 BI 平台服务器和客户端的 SSL 配置相似，将以下密钥和证书文件存储在一个可通过部署了 BI 平台的计算机访问的安全位置（在相同目录下）。

- 受信任的证书文件（cacert.der）。
- 生成的服务器证书文件（servercert.der）。
- 服务器密钥文件（server.key）。
- 密码短语文件（passphrase.txt）。

24.3.2.1 SSL 配置的属性文件

属性文件 `sslconf.properties` 包含 BI 平台组件使用的必需证书和密钥的所有信息。例如：

```
[default]
businessobjects.ora.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

`sslconf.properties` 文件应放在 BI 平台产品的安装文件夹中，该文件夹的默认路径为：`C:\Program Files\Business Objects\BusinessObjects 12.0 Integration Kit for PeopleSoft\`。

24.3.2.2 针对 SSL 启用 PeopleSoft 查询服务器

注意：

以下过程中描述的所有值均区分大小写。

- 在注册表项下为每个查询服务器配置两个注册表值，例如：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Business
Objects\Suite 12.0\Integration Kit for
PeopleSoft\QRY\Instances\aname]
    "CommunicationProtocol"="ssl"
    "SSL Configuration File"="C:\Program
Files\Business Objects\BusinessObjects 12.0 Integration Kit for
PeopleSoft\sslconf.properties"
```

必须重新启动 BI 平台报表服务器（如自适应作业服务器），才能使这些更改生效。

24.3.2.3 针对 SSL 启用安全桥

注意：

以下过程中描述的所有值均区分大小写。

- 将以下参数添加到 crpsepmsecuritybridge.bat 文件中，运行带这些参数的此 .bat 文件。

```
-Dbusinessobjects.orb.oci.protocol=ssl
-DcertDir="d:\ssl"
-DtrustedCert=cacert.der
-DsslCert=servercert.der
-DsslKey=server.key
-Dpassphrase=passphrase.txt
```

请确保将参数添加到 .bat 文件的正确位置，即紧接在 java.exe 之后，且在提供的 -jar 参数之前。例如：

```
@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\javask\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"
```

下表显示了与这些示例相对应的说明：

DcertDir=d:\ssl	用于存储所有证书和密钥的目录。
DtrustedCert=cacert.der	受信任的证书文件。如果指定多个文件，请用分号加以分隔。
DsslCert=clientcert.der	SDK 使用的证书。

DsslKey=client.key	SDK 证书的私钥。
Dpassphrase=passphrase.txt	存储私钥的密码短语的文件。

24.3.3 为 PeopleSoft 系统调优性能

要确保在依据 PeopleSoft 查询创建报表时获得最佳性能，了解 Crystal Reports 和 BI 平台如何执行查询很重要。

在刷新或运行基于 PeopleSoft 查询的报表时，会建立与 PeopleSoft 服务器的连接：

- 在 PeopleSoft Enterprise (PeopleTools 8.46 或更新版本) 环境中，会建立与 PeopleSoft 分析服务器的连接。
- 在 PeopleSoft Enterprise (PeopleTools 8.21-8.45) 环境中，会建立与 PeopleSoft 应用程序服务器的连接。

24.3.3.1 建议

在最佳部署中，会设置一个或多个只处理报表请求的 PeopleSoft 分析或应用程序服务器。在这些服务器的每一个中，Min Instances 和 Max Instances 的设置控制着任一时间可以处理的报表请求数。此设置提供了以下优点：

- 在 PeopleSoft 服务器中，报表请求和其他事务请求之间不会出现争用现象。
- 不禁用处理事务请求的服务器即可在处理报表请求的服务器上执行维护。

在报表请求和事务请求均由相同的 PeopleSoft 分析或应用程序服务器处理的环境中，必须将 BI 平台配置为不同时运行多于一个的报表。否则，如果所有 PSANALYTICSRV 或 PSAPPSRV 过程均用于运行报表，则用户将无法进行任何事务请求。

注意：

- 有关如何限制计划的报表作业和按需查看报表作业数量的信息，请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》中的“管理和配置服务器”。

- 不能将系统配置为限制可能同时尝试访问服务器的 Crystal Reports 用户的数量。

如果出现了性能问题，请使用 Psadmin 配置工具来确定请求是否正在排队。此外，监控 PeopleSoft 分析或应用程序服务器计算机上的系统资源。如果由于缺少物理内存而使用了虚拟内存，则处理速度也可能会变慢。

24.3.3.2 PeopleSoft 服务器

在 PeopleSoft 分析服务器中，刷新或运行报表的过程是 PSANALYTICSRV 过程。在 PeopleSoft 应用程序服务器中，刷新或运行报表的过程是 PSAPPSRV 过程。可用 PSANALYTICSRV 或 PSAPPSRV 过程的数量决定可以同时运行的报表的数量。

典型的 PeopleSoft 分析或应用程序服务器配置文件包含以下信息：

```
Min Instances=3  
Max Instances=5
```

在此示例中，随时可用的 PSANALYTICSRV 或 PSAPPSRV 过程的最小数量为三，而且能够增加到最多五个过程。这些设置不一定意味着总是可以同时运行五个报表；这些过程也可能用于处理系统中的其他任务。如果没有 PSANALYTICSRV 或 PSAPPSRV 过程可用于处理请求，则请求会被放入队列中，直到有可用过程为止。

注意：

PeopleSoft 应用程序服务器的配置文件通常还包含 Service Timeout 参数，该参数指定已排队的请求为了等待可用的过程而等待多长时间。如果在为该参数指定的时间内没有过程可用，则请求超时。

24.4 配置 Siebel 集成

24.4.1 配置 Siebel 以与 SAP BusinessObjects Business Intelligence 平台相集成

BI 平台集成提供了到 Crystal Reports 的链接，支持用户通过将 BusinessObjects Business Intelligence 套件内容嵌入到 Siebel 应用程序中。完成安装和配置后，用户可通过新的菜单项在 Siebel 应用程序中启动 BI 启动板。

默认情况下，所需文件安装在以下文件夹中：C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\。

注意：

子文件夹 Siebel 7.7 和 Siebel 8.0 分别包含使用 Siebel 版本 7.7 和 8.0 的文件。

24.4.1.1 导入 BI 平台 Siebel 集成项目

- 1 启动 Siebel Tools。
- 2 单击“Tools（工具）” > “Import from Archive（从存档中导入）”。
- 3 当提示需要存档文件时，浏览到集成产品安装的 Siebel Files 文件夹。
默认情况下为安装目录\SAP BusinessObjects Enterprise XI 4.0\Samples\siebel\Siebel Files\。
- 4 转到相应的子文件夹（Siebel 7.7 或 Siebel 8.0），并选择 BusinessObjectsEnterprise.sif 文件。
将出现“Import Wizard”（导入向导）。
- 5 单击“将存档文件中的对象定义与资源库中的定义合并”。
- 6 通过向导屏幕完成集成项目的导入过程。
将集成项目添加到资源库。
- 7 锁定“BusinessObjects Integration”项目。

24.4.2 创建 Crystal Reports 菜单项

- 1 在 Siebel Tools 中，锁定“Menu”（菜单）项目。
- 2 在“Object Explorer”（对象资源管理器）中，选择“Menu Item”（菜单项）对象。

注意：

如果“Menu”（菜单）对象未出现在“Object Explorer”（对象资源管理器）中，则单击 Siebel Tools 中的“View”（视图）>“Option”（选项），然后单击“Object Explorer”（对象资源管理器）选项卡，并选择“Menu”（菜单）对象。

3 在“Menus”（菜单）列表中，选择“Generic Web”（通用 Web）菜单。

4 单击“Menu Items”（菜单项）列表标题。

5 单击“Edit（编辑）”>“New Record（新记录）”。

6 相应地定义新的菜单项。建议值如下：

- 名称：视图 — Crystal Reports
- 命令：Crystal Reports
- 备注：SAP BusinessObjects 集成报表菜单
- 非活动：False

7 使用位置编号选择该菜单项在“View”（视图）菜单中的位置。

为便于选择位置编号，可按位置对菜单项进行排序。

8 现在即可添加区域设置记录以根据需要对标题进行本地化。

现在即可重新编译 Siebel 应用程序。请参阅第 817 页上的 [“重新编译 Siebel 应用程序”](#)。

24.4.2.1 重新编译 Siebel 应用程序

安装 BI 平台并使用户能够通过 Siebel 菜单项访问其命令后，必须按照平常步骤重新编译 Siebel 应用程序。有关详细信息，请参阅 Siebel Bookshelf。

重新编译完 Siebel 应用程序后，重新生成其 JavaScript 文件。在 Siebel 7.7 及更高版本中，在重新编译的过程中可以自动重新生成 JavaScript 文件。

由于编译 Siebel 资源库所需的步骤是在 Siebel Tools 工作站中执行，因此用户需要将生成的 JavaScript 从 Siebel Tools 工作站部署到 Siebel 服务器中。通常情况下，取决于 Siebel 的安装位置，可在以下位置找到生成的 JavaScript 文件：

```
C:\sea77\tools\PUBLIC\ENU\srf1096416329_444
```

该示例文件夹名称 srf1096416329_444 由 Siebel Tools 生成，并与生成的资源库文件唯一对应。

应将 JavaScript 文件部署在 Siebel 服务器上，取决于 Siebel 的安装位置，JavaScript 文件通常位于以下位置：

```
C:\sea77\SWEApp\PUBLIC\ENU\srf1096416329_444
```

确保保留 Siebel Tools 生成的文件夹名称。

此外，必须更新 Siebel 服务器计算机上的 Siebel 配置文件以允许此服务。在 Siebel 服务器计算机上找到相应的配置文件。例如，如果运行的是英文版本的 Siebel Call Center，则使用 `ua gent.cfg`。默认情况下，此文件可在 Siebel 7.7 中找到，位置为 `C:\sea77\siebsrvr\bin\ENU\ua gent.cfg`。

然后将以下行添加到配置文件的 SWE 节的末尾：

```
ClientBusinessServiceNUMBER = BusinessObjects Integration Service
```

`ClientBusinessService` 编号按顺序编排。如果 SWF 节中没有其他 `ClientBusinessServices`，则将<编号>设置为 0。否则，将<编号> 设置为第二大的值。

对于 Siebel 8.x 或更高版本：

- 1 登录到 Siebel Tools，并在“Object Explorer”（对象资源管理器）中找到 Siebel Universal Agent 应用程序对象。
- 2 展开应用程序对象以显示“Application User Prop”（应用程序用户属性）对象。
- 3 为每个要声明的业务服务创建新记录，按如下所示为其设置 Name 和 Value 属性：
 - Name = `ClientBusinessServiceX`
 - Value = `BusinessObjects Integration`

现在即可创建调用导入的 Siebel 命令的 Crystal Reports 菜单项。

24.4.3 上下文感知

上下文感知功能用于向用户展现很可能与其当前任务相关的报表。在这种情况下，对于直接从 Siebel 客户端应用程序访问 Crystal Reports 的用户，会向其自动显示已被设计为包含 Siebel 数据的报表。

24.4.3.1 配置上下文感知

在配置上下文感知之前，请确保已完成以下操作。

- 安装 Siebel 集成产品
 - 配置 Siebel 与 BI 平台相集成
- 1 打开中央管理控制台（CMC）。
 - 2 单击“身份验证”。
 - 3 双击“Siebel”。
- 将出现 Siebel 映射界面。

- 4 单击“域”。
将出现域映射界面。
- 5 记下与要使用的 Siebel 服务器对应的域名。
- 6 关闭 Siebel 映射界面。
- 7 打开 BI 启动板。
- 8 在 PublicFolders\Siebel 下创建一个新文件夹，并将其名称设置为 CMC 中的 Siebel 域名。
- 9 将包含 Siebel 信息的所有报表都放置在此文件夹下。

24.4.3.2 为上下文感知指定 URL

- 1 重新生成应用程序的 JavaScript 文件之后，转到 BI 平安装目录的 Siebel Files 文件夹，其默认位置为：C:\Program Files\Business Objects\SAP BusinessObjects Enterprise XI\Siebel Files\。
- 2 复制 BusinessObjectsEnterpriseServer.html 文件。然后找到 genbscript 程序生成的新 JavaScript 文件所在的公共文件夹，并将 BusinessObjectsEnterpriseServer.html 的副本放置到相应语言的子文件夹中。

例如，如果应用程序的 JavaScript 文件生成到 Siebel 服务器上的 c:\sea752\SWEApp\PUBLIC\ENU 文件夹中，则将 BusinessObjectsEnterpriseServer.html 文件复制到 c:\sea752\SWEApp\PUBLIC\ENU 文件夹中。

- 3 使用文本编辑器（如记事本）从公共文件夹打开 BusinessObjectsEnterpriseServer.html 文件，并找到如下行：

```
Var userDomain = "SIEB78"
```

```
var destAddr = "http://SAP BusinessObjects server:8080/BOE/BI/logon/siebelStart.do"
```

注意：

- 如果修改 userDomain 或 destAddr 变量，则必须清除浏览器缓存的 Web 页以确保浏览器能够指向正确的目标地址。
- userDomain 区分大小写。

24.4.3.3 验证上下文感知

- 1 在 Siebel Tools 中，单击“调试” > “开始”。

- 2 导航到任意屏幕，然后单击“View”（视图）菜单。

新的 Crystal Reports 菜单项应出现在菜单上。

- 3 单击“Crystal Reports”菜单项。

BI 平台打开 BI 启动板窗口，连接到此窗口需要提供用户名和密码。这仅在会话超时之前的首次登录时需要。在 html 和 Siebel 身份验证中配置的域名应该已填写。

注意：

此步骤只是验证已进行到目前的安装。在将 Siebel 职责映射到 BI 平台之前，无法使用 Siebel 身份验证登录到 BI 平台。

24.4.3.4 向 BI 平台添加文件夹

BI 平台 Integration for Siebel 需要将某些文件夹添加到 BI 启动板中才能完全启用上下文感知功能。

为了能够正常运行，上下文文件夹的结构应如下所示：公共文件夹\Siebel\域名。只有域名子文件夹中存储的且在 Siebel 系统中被配置为与特定 SAP BusinessObjects 业务元素相关联的报表会显示为上下文感知功能的一部分。此处使用的 <域名> 必须为在身份验证配置中为 Siebel 配置的域名，且必须与在 Siebel 端的 BusinessObjectsEnterpriseServer.html 文件中配置的值相同。

注意：

需要使用 Siebel Tools 完成此节中的步骤。

24.4.4 为 SAP Crystal Reports 和 Siebel 配置单一登录（SSO）

默认情况下，BI 平台将配置为允许 SAP Crystal Reports 用户使用单一登录（SSO）访问 Siebel 数据。

24.4.4.1 为 Siebel 和 Crystal Reports 取消激活 SSO

- 1 在中央管理控制台（CMC）中，单击“应用程序”。
- 2 双击“Crystal Reports 配置”。
- 3 单击“单一登录选项”。
- 4 选择 `crdb_siebel`。
- 5 单击“删除”。
- 6 单击“保存并关闭”。
- 7 重新启动 SAP Crystal Reports。

24.4.4.2 为 Siebel 和 SAP Crystal Reports 激活 SSO

如果为 Siebel 和 SAP Crystal Reports 取消激活 SSO，并希望重新激活它。

- 1 在中央管理控制台（CMC）中，单击“应用程序”。
- 2 双击“Crystal Reports 配置”。
- 3 单击“单一登录选项”。
- 4 在“使用 SSO 上下文进行数据库登录...”下，键入“`crdb_siebel`”。
- 5 单击“添加”。
- 6 单击“保存并关闭”。
- 7 重新启动 SAP Crystal Reports 服务器。

24.4.5 配置安全套接字层通信

在 Siebel 和 BI 平台部署中，可以为客户端和服务器之间的所有网络通信使用安全套接字层（SSL）协议。

与其他 BI 平台服务器和客户端的 SSL 配置相似，将以下密钥和证书文件存储在一个 Siebel 部署中的计算机可以访问的安全目录下。

- 受信任的证书文件（`cacert.der`）。
- 生成的服务器证书文件（`servercert.der`）。
- 服务器密钥文件（`server.key`）。
- 密码短语文件（`passphrase.txt`）。

SSL 配置的属性文件

属性文件 `sslconf.properties` 包含所有关于 Integration for Siebel 组件使用的必需证书和密钥的信息。例如：

```
businessobjects.orb.oci.protocol=ssl
certDir=d:/ssl
trustedCert=cacert.der
sslCert=servercert.der
sslKey=server.key
passphrase=passphrase.txt
```

默认情况下，`sslconf.properties` 文件应放入安装 BI 平台产品的文件夹中：C:\Program Files\Business Objects\SAP BusinessObjects Enterprise XI\。

第 25 章 管理和配置日志

25.1 记录组件的跟踪消息

日志

BI 平台生成系统级消息，并将其写入日志文件。系统管理员可使用这些日志文件监控性能或调试错误。

跟踪

BI 平台也可生成跟踪（记录在监控组件运行期间发生的事件），并在采用 .glf 扩展名的日志文件中收集这些跟踪。跟踪事件的范围包括从状态消息到严重的异常错误。SAP 支持员工和开发人员可使用跟踪报告 BI 平台组件（服务器和 Web 应用程序）的性能，以及监控组件的活动。

在设置组件的跟踪日志级别时，要确定发送至日志文件的信息的类型和详细程度。跟踪日志级别是将跟踪抑制在指定阈值下的一个过滤器。通过监控组件跟踪日志，可确定是否必须更改组件或其配置的当前实例，以便在增加的工作负载下操作。

注意：

可使用任何文本编辑器查看 BI 平台日志文件。

25.2 跟踪日志级别

下列跟踪日志级别可用于 BI 平台组件：

级别	说明
未指定	跟踪日志级别通过其他方式（通常为 .ini 文件）指定。
无	未发生跟踪。
低	跟踪日志过滤器允许记录错误消息，但忽略警告和状态消息。记录组件启动、关闭、启动请求和结束请求消息的重要状态消息。建议不要为调试使用此级别。
中	跟踪日志过滤器设置为包括错误、警告和大多数状态消息。过滤掉重要性很低或极其冗长的状态消息。此级别对于调试来说不够详细。
高	不过滤任何消息。建议为调试使用此级别。 警告： 该跟踪日志级别将严重影响系统资源，增加 CPU 使用量，并消耗存储空间。

25.3 为服务器配置跟踪

日志消息是软件系统事件和状态的永久性记录。对监控的 BI 平台部署的跟踪将写入特定的 .glf 日志文件，并存储在记录目录中。

- 在 Windows 上，默认位置为 安装目录\SAP BusinessObjects Enterprise XI 4.0\logging
- 在 Unix 上，默认位置为安装目录/sap_bobj/logging

.glf 日志文件的名称包括一个速记标识符、服务器名称和一个数字参考，例如 aps_mysia.AdaptiveProcessingServer_trace.000012.glf。当日志文件的大小达到 10MB 的阈值时，系统将为所监控的服务器创建新的跟踪日志文件。此外，同时保留五个日志文件。随着新日志文件的创建，将删除旧的日志文件。

可以通过为特定服务器或服务器组设置跟踪日志级别，确定日志文件中所收集的跟踪消息的严重性和重要性。

注意：

要修改特定服务器或服务器组的跟踪日志级别，请使用中央管理控制台（CMC）中的跟踪日志服务。要修改其他参数，请在 B0_trace.ini 文件中手动更改跟踪日志级别和其他设置。

25.3.1 在 CMC 中设置日志级别

可为服务器调整跟踪日志级别，而不影响其他跟踪设置。

- 1 在 CMC 的“服务器”区域中，访问服务器。
 - 从特定类别中选择服务器。
 - 单击导航窗格中的“服务器列表”以访问完整的服务器列表，然后选择服务器。
- 2 右击所选服务器并选择“属性”。
- 3 在“跟踪日志设置”区域中，从“日志级别”列表中选择一项设置。
- 4 单击“保存并关闭”。

新的跟踪日志级别将立即生效。

要为日志文件指定不同的输出目录，请在“命令行参数”区域包括 `-loggingPath target_directory` 参数。重新启动服务器使此设置生效。

相关主题

- 第 823 页上的[“跟踪日志级别”](#)

25.3.2 为 CMC 中的多个服务器设置日志级别

- 1 在 CMC 的“服务器”区域中，访问多个服务器。
 - 从特定类别中选择服务器。
 - 单击导航窗格中的“服务器列表”以访问完整的服务器列表。按住 Ctrl 并单击多个服务器以进行选择。
- 2 右击所选服务器，并选择“编辑公用服务”。
- 3 在“跟踪日志设置”区域中，从“日志级别”列表中选择一项设置。
- 4 单击“确定”。

新的跟踪日志级别将立即生效。

要为日志文件指定不同的输出目录，请在“命令行参数”区域包括 `-loggingPath target_directory` 参数。重新启动服务器使此设置生效。

相关主题

- 第 823 页上的[“跟踪日志级别”](#)

25.3.3 使用 B0_trace.ini 文件配置服务器跟踪

默认情况下，B0_trace.ini 文件只记录错误和断言。

- 1 打开 B0_trace.ini 文件。
 - 在 Windows 上，默认位置为安装目录\SAP BusinessObjects Enterprise XI 4.0\conf\
 - 在 Unix 上，默认位置为 安装目录/sap_bobj/enterprise_xi40/conf/
- 2 取消注释“Trace Syntax and Setting”（跟踪语法和设置）一节中的行。
- 3 修改服务器跟踪参数。以下参数用于配置服务器跟踪：

参数	可能的值	说明
sap_log_level	log_information log_warning log_error log_fatal log_none	<p>确定日志消息的严重性。默认日志严重性为 log_error。</p> <p>日志严重性遵循一定的层次结构，log_information 为最高级，log_none 为最低级。设置日志严重性级别时，将显示该级别和更低级别的所有消息。例如，如果将严重性设置为 log_warning，包括 log_warning、log_error 和 log_fatal 的消息将写入日志文件。</p> <p>注意： log_information 和 log_warning 可缩短为 log_info 和 log_warn。</p>
sap_trace_level	trace_debug trace_path trace_information trace_error trace_none	<p>确定跟踪消息的严重性。默认跟踪严重性为 trace_error。</p> <p>跟踪严重性遵循一定的层次结构，trace_debug 为最高级，trace_none 为最低级。设置跟踪严重性级别时，将显示该级别和更低级别的所有消息。例如，如果将跟踪严重性设置为 trace_path，包括 trace_path、trace_information 和 trace_error 的消息将写入日志文件。</p> <p>注意： trace_information 可缩短为 trace_info。</p>

- 4 保存并关闭 B0_trace.ini 文件。

经常读取 BO_trace.ini 文件。对 BO_trace.ini 文件的更改在保存后五分钟内生效。如果重新启动 CMS，对 BO_trace.ini 文件的更改将立即生效。

示例：

BO_trace.ini

```
sap_log_level=log_warning;  
sap_trace_level=trace_path;
```

25.3.3.1 为特定服务器配置跟踪

BO_trace.ini 文件为 BI 平台服务器指定跟踪参数。其中的设置会影响所有托管服务器。管理员可以使用 BO_trace.ini 文件为特定服务器设置特定的跟踪参数。

警告：

CMC 中为特定服务器指定的新跟踪日志级别设置将覆盖 BO_trace.ini 中的全部设置。

- 1 打开 BO_trace.ini 文件。
 - 在 Windows 上，默认位置为安装目录\SAP BusinessObjects Enterprise XI 4.0\conf\
 - 在 Unix 上，默认位置为 安装目录/sap_bobj/enterprise_xi40/conf/
- 2 使用 if 语句为特定服务器指定跟踪设置。例如：

```
if (process == "aps_MySIA.ProcessingServer") {  
    sap_log_level=log_warning;  
    sap_trace_level=trace_path;  
}
```

提示：

必须为跟踪设置指定流程，以应用到特定服务器。

- 3 保存并关闭 BO_trace.ini 文件。

将在五分钟内实施修改后的设置。

25.4 为 Web 应用程序配置跟踪

对监控 BI 平台部署的跟踪将写入特定的 .glf 日志文件，并存储在承载 Web 应用程序文件夹的计算机上的目录中。

- 在 Windows 上，默认位置为：C:\SBOPWebapp_应用程序_IP 地址_端口\，例如 C:\SBOPWebapp_BI launchpad_192.0.2.0_8080\

- 在 Unix 上，默认位置为：\$userHome/SBOPWebapp_应用程序_IP 地址_端口/，例如 \$userHome/SBOPWebapp_CMC_192.0.2.0_8080/

默认情况下，CMC 中的 Web 应用程序的跟踪日志级别设置为“未指定”。在 CMC 中，跟踪日志设置适用于以下应用程序：

- 中央管理控制台
- BI 启动板
- OpenDocument
- Web 服务

注意：

要修改特定服务器或服务器组的跟踪日志级别，请使用中央管理控制台（CMC）中的跟踪日志服务。要修改其他参数，请在 BO_trace.ini 文件中手动更改跟踪日志级别和其他设置。此文件随 BOE.war 和 dswebobje.war 文件一起部署在 Web 应用程序服务器上。

在配置 BO_trace.ini 文件之前，必须使用 WDeploy 工具从 Web 应用程序服务器上取消部署现有 Web 应用程序。在配置 BO_trace.ini 之后，必须将其与 Web 应用程序一起重新部署在 Web 应用程序服务器上。有关使用 WDeploy 准备、部署和取消部署 Web 应用程序的更多信息，请参阅《SAP BusinessObjects Enterprise Business Intelligence 平台 Web 应用程序部署指南》。

25.4.1 在 CMC 中设置 Web 应用程序跟踪日志级别

要跟踪其他 Web 应用程序，必须手动配置相应的 BO_trace.ini 文件。

- 1 在 CMC 的“应用程序”区域，右击应用程序，选择“跟踪日志设置”。

注意：

这些应用程序具备跟踪日志设置：BI 启动板、CMC、OpenDocument、升级管理、版本管理、差异可视化和 Web 服务。

将显示“跟踪日志设置”对话框。

- 2 从“日志级别”列表中选择设置。
- 3 单击“保存并关闭”。

新的跟踪日志级别将在下次登录 Web 应用程序后生效。

相关主题

- 第 823 页上的[“跟踪日志级别”](#)

25.4.2 使用 BO_trace.ini 文件配置跟踪设置

BO_trace.ini 文件随 BOE 和 dswsbobje.war 文件一起部署在 Web 应用程序服务器上。可使用 BO_trace.ini 为 BI 平台应用程序指定跟踪参数。因此，此文件并非始终可访问，用户必须从 Web 应用程序服务器中解除受影响的 Web 应用程序的部署。

- 1 可以使用 Wdeploy 取消 Web 应用程序在您的 Web 应用程序服务器上的部署。有关使用 WDeploy 取消部署 Web 应用程序的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。
 - 如果使用随 BI 平台安装提供的 Tomcat Web 应用程序服务器，则无需解除 Web 应用程序的部署。而是可以直接修改该文件。
 - BOE.war 文件的跟踪配置文件位于安装目录\Tomcat\webapps\BOE\WEB-INF\TraceLog
 - dswsbobje.war 文件的跟踪配置文件位于安装目录\Tomcat\webapps\dswsbobje\WEB-INF\conf

注意：

如果使用捆绑式 Tomcat Web 应用程序服务器，请跳到第 2 步。

- 2 访问 BO_trace.ini 文件的预先部署版：
 - BOE.war 文件的配置文件的预先部署版默认位置为安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
 - dswsbobje.war 文件的配置文件的预先部署版默认位置为安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf
- 3 打开 BO_trace.ini 文件。
 - 在 Windows 上，默认位置为安装目录\SAP BusinessObjects Enterprise XI 4.0\conf\
 - 在 Unix 上，默认位置为 安装目录/sap_bobj/enterprise_xi40/conf/
- 4 修改服务器跟踪参数。以下参数用于配置服务器跟踪：

参数	可能的值	说明
sap_log_level	log_information log_warning log_error log_fatal log_none	<p>确定日志消息的严重性。默认日志严重性为 log_error。</p> <p>日志严重性遵循一定的层次结构，log_information 为最高级，log_none 为最低级。设置日志严重性级别时，将显示该级别和更低级别的所有消息。例如，如果将严重性设置为 log_warning，包括 log_warning、log_error 和 log_fatal 的消息将写入日志文件。</p> <p>注意： log_information 和 log_warning 可缩短为 log_info 和 log_warn。</p>
sap_trace_level	trace_debug trace_path trace_information trace_error trace_none	<p>确定跟踪消息的严重性。默认跟踪严重性为 trace_error。</p> <p>跟踪严重性遵循一定的层次结构，trace_debug 为最高级，trace_none 为最低级。设置跟踪严重性级别时，将显示该级别和更低级别的所有消息。例如，如果将跟踪严重性设置为 trace_path，包括 trace_path、trace_info 和 trace_error 的消息将写入日志文件。</p> <p>注意： trace_information 可缩短为 trace_info。</p>

- 5 保存并关闭 BO_trace.ini 文件。
 - 6 使用 WDeploy 在承载 Web 应用程序服务器的计算机上部署 .war 文件。
- 修改的跟踪设置将在下次登录 Web 应用程序时生效。

25.4.2.1 为特定 Web 应用程序配置跟踪

BO_trace.ini 文件随 BOE 和 dswebobje.war 文件一起部署在 Web 应用程序服务器上。可使用 BO_trace.ini 为 BI 平台应用程序指定跟踪参数。因此，此文件并非始终可访问，用户必须从 Web 应用程序服务器中解除受影响的 Web 应用程序的部署。下面是 Web 应用程序及其关联的 .war 文件：

Web 应用程序	WAR 文件	预部署位置
中央管理控制台	BOE. war	安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
BI 启动板	BOE. war	安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
OpenDocument	BOE. war	安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
Web 服务	dswsbobje. war	安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf

1. 可以使用 Wdeploy 取消 Web 应用程序在您的 Web 应用程序服务器上的部署。有关使用 WDeploy 取消部署 Web 应用程序的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台 Web 应用程序部署指南》。
 - 如果使用随 BI 平台安装提供的 Tomcat Web 应用程序服务器，则无需解除 Web 应用程序的部署。而是可以直接修改该文件。
 - BOE. war 文件的跟踪配置文件位于安装目录\Tomcat\webapps\BOE\WEB-INF\TraceLog
 - dswsbobje. war 文件的跟踪配置文件位于安装目录\Tomcat\webapps\dswsbobje\WEB-INF\conf

注意：

如果使用捆绑式 Tomcat Web 应用程序服务器，请跳到第 2 步。

2. 访问 BO_trace.ini 文件的预先部署版：
 - BOE. war 文件的配置文件的预先部署版默认位置为安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\BOE\WEB-INF\TraceLog
 - dswsbobje. war 文件的配置文件的预先部署版默认位置为安装目录\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps\dswsbobje\WEB-INF\conf
3. 打开 BO_trace.ini 文件。
 - 在 Windows 上，默认位置为安装目录\SAP BusinessObjects Enterprise XI 4.0\conf\
 - 在 Unix 上，默认位置为 安装目录/sap_bobj/enterprise_xi40/conf/
4. 使用 if 语句为特定 Web 应用程序指定跟踪设置。例如：

```
if (device_name == "Webapp_opendocument_trace") {
    sap_log_level=log_warning;
    sap_trace_level=trace_path;
}
```

必须为跟踪设置指定流程，以应用到特定 Web 应用程序服务器。在初始安装后，以下 Web 应用程序可用：

Web 应用程序	设备名称
BI 启动板	WebApp_BIlaunchpad
中央管理服务器	WebApp_CMC
OpenDocument	WebApp_OpenDocument

以下参数用于配置 Web 应用程序服务器跟踪：

参数	可能的值	说明
sap_log_level	log_information log_warning log_error log_fatal log_none	<p>确定日志消息的严重性。默认日志严重性为 log_error。</p> <p>日志严重性遵循一定的层次结构，log_information 为最高级，log_none 为最低级。设置日志严重性级别时，将显示该级别和更低级别的所有消息。例如，如果将严重性设置为 log_warning，包括 log_warning、log_error 和 log_fatal 的消息将写入日志文件。</p> <p>注意： log_information 和 log_warning 可缩短为 log_info 和 log_warn。</p>
sap_trace_level	trace_debug trace_path trace_information trace_error trace_none	<p>确定跟踪消息的严重性。默认跟踪严重性为 trace_error。</p> <p>跟踪严重性遵循一定的层次结构，trace_debug 为最高级，trace_none 为最低级。设置跟踪严重性级别时，将显示该级别和更低级别的所有消息。例如，如果将跟踪严重性设置为 trace_path，包括 trace_path、trace_info 和 trace_error 的消息将写入日志文件。</p> <p>注意： trace_information 可缩短为 trace_info。</p>

5 保存并关闭 B0_trace.ini 文件。

6 使用 WDeploy 在承载 Web 应用程序服务器的计算机上部署 .war 文件。

25.5 为升级管理工具配置跟踪

无法使用 CMC 执行升级管理工具的跟踪配置。必须使用 B0_trace.ini 文件执行升级管理工具的跟踪。

- 在 Windows 上，默认位置为安装目录\SAP BusinessObjects Enterprise XI 4.0\conf\
- 在 Unix 上，默认位置为 安装目录/sap_bobj/enterprise_xi40/conf/

25.5.1 为升级管理工具配置跟踪

1. 打开 B0_trace.ini 文件。
 - 在 Windows 上，默认位置为安装目录\SAP BusinessObjects Enterprise XI 4.0\conf\
 - 在 Unix 上，默认位置为 安装目录/sap_bobj/enterprise_xi40/conf/
2. 取消注释“Trace Syntax and Setting”（跟踪语法和设置）一节中必需的行。
3. 使用 if 语句指定跟踪设置。例如：

```
if (process == "upgrademanagementtool") {  
    sap_log_level=log_warning;  
    sap_trace_level=trace_path;  
}
```

提示：

必须将该进程指定为 upgrademanagementtool，这样跟踪设置才能应用于升级管理工具。

4. 保存并关闭 B0_trace.ini 文件。

将在五分钟内实施修改后的设置。

25.6 为 BI 平台客户端应用程序配置跟踪

可在下列客户端上激活跟踪：

- Universe 设计工具
- 信息设计工具
- Web Intelligence 胖客户端

可通过为每个客户端类型编辑 .ini 文件来设置这些组件的跟踪。这些 .ini 文件的运行方式与本章其他部分中描述 B0_trace.ini 文件相同。有关修改 .ini 文件的详细信息，请参阅第 826 页上的[“使用 B0_trace.ini 文件配置服务器跟踪”](#)。

这些文件需位于为这些应用程序配置的工作目录中（默认情况下为 <安装目录>\SAP BusinessObjects）。如果不存在，可能需要创建这些文件。文件名称如下：

- Universe 设计工具：designer_trace.ini
- 信息设计工具：B0_Trace.ini
- Web Intelligence 胖客户端：WebIRichClient_trace.ini

请参阅这些产品的文档了解详细信息。

第 26 章 集成到 SAP Solution Manager

26.1 集成概述

BI 平台中已添加支持功能，通过该功能可实现与 SAP Solution Manager 的集成。以下 SAP Solution Manager 组件可用于为您的 BI 平台部署提供支持：

- 解决方案架构目录
- Solution Manager 诊断
- CA Wily Introscope
- SAP Passport

注意：

要访问 SAP BusinessObjects 的 SAP Support Portal，请转到：<https://websmp205.sap-ag.de/bosap-support>

26.2 SAP Solution Manager 集成检查列表

下表汇总了使 SAP Solution Manager 能够为 BI 平台提供支持所必需的事项。

SAP Solution Manager 支持	BI 平台所需信息
SLD 注册	<ul style="list-style-type: none"> 必须安装 SAPHOSTAGENT 以便能够注册 BI 平台服务器。 <p>注意： 如果已经安装了 SAPHOSTAGENT，BI 平台安装程序将自动注册服务器。</p> <ul style="list-style-type: none"> 必须为提供后端服务器报告的数据提供者创建一个 connect.key 文件。 （可选）对于 WebSphere 6.1 或 7 的 SLD 注册，必须在每台 WebSphere Web 应用程序服务器上安装 SLDREG 注册工具。有关更多信息，请参阅 SAP 注释 1482727。 （可选）对于 SAP NetWeaver 7.2 的 SLD 注册，应在每个 NetWeaver 主机上安装 SLDREG。有关更多信息，请参考 SAP 注释 1018839。 （可选）对于 Apache Tomcat 的 SLD 注册，必须在每个 Tomcat 服务器上安装 SLDREG。有关更多信息，请参阅 SAP 注释 1508421。
SMD 集成	<ul style="list-style-type: none"> 必须在 BI 平台服务器的所有主机上安装 SMD 代理（DIAGNOSTICS.AGENT）。 必须在 BI 平台中启用 SMAdmin 用户帐户。
性能检测	<ul style="list-style-type: none"> 必须配置 Introscope 代理以连接 Enterprise Manager。可以使用 BI 平台安装程序或 CMC 节点占位符配置连接。 必须安装 SMD 代理。 必须配置 BI 平台以连接 SMD 代理。可以使用 BI 平台安装程序或 CMC 节点占位符配置连接。
SAP Passport	<ul style="list-style-type: none"> 您需要下载并安装 SAP Passport 客户端工具。

26.3 管理系统架构目录注册

26.3.1 在系统架构中注册 BI 平台

系统架构目录 (SLD) 是与软件生命周期管理相关的系统架构信息的中央资源库。SLD 包含系统架构的说明, 即当前安装的系统 and 软件组件。SLD 数据提供者在 SLD 服务器上注册系统并保持信息的最新状态。管理和业务应用程序访问 SLD 中存储的信息以便在协作计算环境中执行任务。

系统架构目录数据提供者 (SLD-DS) 是负责向 SLD 服务器注册 BI 平台服务器的应用程序。针对每个平台安装实例都会提供一个特定数据提供者, 用于提供有关以下组件的报告:

- BI 平台服务器
- WebSphere Web 应用程序服务器上所承载的 Web 应用程序和服务。

注意:

SAP NetWeaver 具有一个内置 SLD-DS 提供者, 可注册 NetWeaver 应用程序服务器以及所承载的 Web 应用程序和服务。此 SLD-DS 与 SAP NetWeaver 环境中所集成的 BI 平台部署相关。

负责提供有关 BI 平台服务器的报告的 SLD-DS 要求安装并配置 SLDREG 程序。SLDREG 程序是在安装 SAPHOSTAGENT 工具时安装的。有关如何访问和安装 SAPHOSTAGENT 的更多信息, 请参阅《SAP BusinessObjects Business Intelligence 平台安装指南》中的“准备”部分。安装 SLDREG 后, 您需要创建一个 connect.key 文件, 使其能够访问 SLD 服务器。

有关如何为 WebSphere 配置特定数据提供者的信息, 请参阅《Web 应用程序部署指南》。

在 BI 平台安装过程中, 注册 BI 平台所需的信息存储在一个配置文件中。该文件包含 SLD DS 用于连接到 BI 平台数据库的信息。

26.3.1.1 为 SLD 数据提供者创建 connect.key 文件

在为 SLD 数据提供者创建 connect.key 文件之前, 您需要下载并安装 SAPHOSTAGENT。有关更多详细信息, 请参阅《SAP BusinessObjects Business Intelligence 平台安装指南》中的“准备”一节。

注意:

connect.key 文件是为提供 BI 平台服务器报告的数据提供者进行 SLD 注册所必需的。

- 1 打开命令行控制台。
- 2 导航到默认 SAPHOSTAGENT 安装路径。
 - 在 Windows 上为: Program Files\SAP\hostctrl\exe
 - 在 Unix 上为: /usr/sap/hostctrl/exe
- 3 运行以下命令:
`sldreg -configure connect.key`
- 4 输入以下配置详细信息

- User name
- Password
- 主机
- 端口号
- 指定使用 HTTP

sldreg 工具将创建 connect.key 文件，数据提供者会自动使用该文件将信息发送至 SLD 服务器。

26.3.2 何时会触发 SLD 注册？

在以下情况下，提供 BI 平台后端服务器报告的数据提供者将调用 SLD 注册进程：

- 重新启动 BI 平台部署中的服务器节点。
- 向部署中添加新服务器或节点。
- 删除服务器或节点。

注意：

如果删除服务器或节点，SLD 注册进程不会修改 SLD 服务器上的内容。要在删除服务器或节点时更新 SLD 服务器，请从 SLD 删除系统，然后通过重新启动 BI 平台重新发送。

可以手动调用 WebSphere SLD 注册的数据提供者，也可以将其设置为按指定时间间隔运行，例如每隔 24 小时。有关配置此数据提供者的更多信息，请参考 SAP 注释 482727。

26.3.3 记录 SLD 连接

数据提供者配置文件

系统将为 BI 平台部署创建一个用于 SLD 注册的配置文件。该文件（sldparserconfig.properties）位于以下目录中：<安装目录>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/。

记录 SLD 连接

BI 平台部署中的 SLD 服务器与数据提供者之间的连接是通过 sldreg 工具和 connect.key 文件进行控制的。

注意：

日志文件名指定为 sldparserconfig.properties 文件中的一个属性。

提供 BI 平台后端服务器报告的 SLD 数据提供者的日志文件默认位于以下位置：<安装目录>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/bobjsldds.log。每次执行数据提供者时都会覆盖该文件。

sldreg 的日志文件默认位于以下位置：<安装目录>/SAP BusinessObjects Enterprise XI 4.0/java/lib/bobj-sld-ds/log。sldreg 日志文件名无法修改，且采用以下格式：sldreg_Timestamp.log。

每次数据提供者调用 sldreg 时都会创建一个新的日志文件。

26.4 管理 Solution Manager 诊断代理

26.4.1 Solution Manager 诊断（SMD）概述

SAP Solution Manager 的 Solution Manager 诊断（SMD）组件可提供集中分析和监控整个系统架构的所有功能。如果安装了 SMD 代理，则可由 SMD 服务器监控 BI 平台。SMD 代理（DIAGNOSTICS.AGENT）可为 SMD 收集之后可用于根本原因分析的信息。所收集并发送到 SMD 服务器的信息包括后端服务器配置和服务器日志文件的位置。

26.4.2 使用 SMD 代理

BI 平台不安装 SMD 代理。该代理（DIAGNOSTICS.AGENT）可从以下位置下载：<http://service.sap.com/swdc>。

有关安装和配置该代理的信息位于：<http://service.sap.com/diagnostics>

使用 SMD 代理的指导原则

使用 SMD 代理监控 BI 平台时，请遵循以下指导原则：

- 所监控系统和代理的安装顺序并不重要。您可以选择在安装和部署 BI 平台之前或之后安装 SMD 代理。

- 安装 SMD 代理时，请记下主机名和侦听端口。这些对于将 BI 平台配置为受监控的系统是非常重要的。如果在安装所监控系统之前已经安装了代理，则可在 BI 平台的安装设置过程中提供配置信息。您也可以将来使用部署中的中央控制台通过节点的占位符提供这些信息。
- 如果后端服务器部署在分布式系统中，则应在承载后端服务器的每台计算机上安装 SMD 代理。
- 非 Java 服务器的性能检测要求使用 SMD 代理。
- 您必须激活 SMAAdmin 用户帐户以使 SMD 服务器能够访问 CMS。

26.4.3 SMAAdmin 用户帐户

每个 BI 平台部署都会创建一个用户帐户来帮助完成 SMD 集成。SMD 服务器使用该只读帐户登录 CMS 并收集有关部署的服务器配置和其他信息。

SMAAdmin 帐户默认未激活。

26.4.3.1 激活 SMAAdmin 帐户

- 1 在 CMC 的“用户和组”管理区域中，选择“用户列表”。
这时将显示用户列表。
- 2 找到“SMAAdmin”用户帐户。
- 3 单击“管理” > “属性”。
将出现“属性”对话框。
- 4 清除“已禁用帐户”选框。
- 5 单击“保存并关闭”。

26.5 管理性能检测

26.5.1 BI 平台的性能检测

您可以使用作为 SAP Solution Manager 一部分的 CA Wily Introscope 度量 BI 平台的性能检测结果。在安装该平台时，您的部署可以使用以下资源

- Introscope 代理：Introscope 代理可收集来自 BI 平台 Java 后端服务器的性能量度。这些代理还可收集来自周围计算环境的信息。然后，它们会将这些量度报告给 Enterprise Manager。
- 系统为检测过程提供了相应文件。一组文件用于非 Java 服务器的检测，另一组文件用于 Java 服务器的检测。在 SAP Solution Manager 一侧，需要具有 Enterprise Manager (EM) 组件。EM 充当在应用环境中收集的所有 Introscope 性能数据和量度的中央资源库。EM 将处理性能数据并将其提供给用户以进行生产监控和诊断。

26.5.2 为 BI 平台设置性能检测

可通过两种方式为在 BI 平台后端服务器上运行的工作流设置性能检测。

- 1 在 BI 平台的安装设置过程中。您需要知道 SMD 代理的主机名和侦听端口。有关更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台安装指南》。如果选择此选项，当您完成所监控系统的部署后，将默认运行检测。
- 2 安装 BI 平台后，您可以在中央管理控制台（CMC）中通过节点属性中的占位符为 SMD 代理提供配置信息。

注意：

对于非 Java 服务器上的工作流的检测，必须安装有 SMD 代理（DIAGNOSTICS.AGENT）。

相关主题

- 第 838 页上的“[使用 SMD 代理](#)”

26.5.2.1 配置用于检测的节点

如果在 BI 平台的安装设置过程中没有为 SMD 代理和 Enterprise Manager 提供配置信息，请按以下说明操作。

- 1 转到 CMC 的“服务器”区域。
- 2 在导航面板中，单击“节点”。
这时将显示所有可用节点。
- 3 右击要执行检测的节点并选择“占位符”。
随即显示“占位符”对话框。
- 4 修改以下占位符的值。

占位符	说明
%IntroscopeAgentEnableInstrumentation%	启用或禁用 Java 服务器上的检测。如果在安装设置过程中为 Enterprise Manager 提供了配置详细信息，则该项将设置为启用。设置为“真”以启用检测。
%IntroscopeAgentEnterpriseManagerHost%	安装 Enterprise Manager 的计算机的主机名。
%IntroscopeAgentEnterpriseManagerPort%	Enterprise Manager 使用的侦听端口。
%IntroscopeAgentEnterpriseManagerTransport%	Enterprise Manager 使用的通信协议。支持的协议包括 TCP、SSL、HTTP Tunnel 和 HTTPS。
%NCSInstrumentLevelThreshold%	用于设置非 Java 服务器的检测级别。如果希望关闭检测，则设为 0。设为大于 0 的任何值将激活检测。
%SMDAgentHost%	安装 SMD 代理（DIAGNOSTICS.AGENT）的计算机的主机名。
%SMDAgentPort%	SMD 代理使用的侦听端口。

- 5 单击“保存并关闭”。
- 6 重新启动节点。
重新启动节点后，所提供的新值将传播至所有托管服务器。

26.5.3 Web 层的性能检测

BI 平台不包含 Web 层组件的检测数据。

26.5.4 检测日志文件

将 BI 平台部署配置为运行检测后，系统便会在特定位置记录相关消息。通过检查日志文件可以验证检测状态。

对于 Java 后端服务器的检测，日志文件位于以下目录：<安装目录>/SAP BusinessObjects Enterprise XI 4.0/java/wily/logs。针对每个 Java 进程会创建一个单独的 .log 文件。该文件夹还包含 AutoProbe.log 文件，这些文件指定为检测加载的方法。

对于非 Java 后端服务器的检测，日志文件位于以下目录：<安装目录>/SAP BusinessObjects Enterprise XI 4.0/logging/。在 Unix 上，日志文件位于 <sap_bobj>\logging\ 目录中。非 Java 服务器的检测相关日志文件将保存为 .trc 文件。

对于 Web 应用程序服务器的检测，日志文件位于以下目录：<安装目录>/SAP BusinessObjects Enterprise XI 4.0/java/wily/webapp/logs。此文件夹中会显示两种类型的日志文件：Introscope.log 和 Autoprobe.log。

26.6 使用 SAP Passport 进行跟踪

除了跟踪 BI 平台组件（如服务器和 Web 应用程序）外，跟踪机制还支持对特定操作的跟踪。端到端跟踪分析功能可分析单个事务的性能。通过将特定操作的所有跟踪信息整合在一起，SAP 支持人员可以查看所有跟踪数据，而不会因其他操作的相关跟踪信息分散精力。

SAP Passport

支持 BI 平台端到端跟踪的机制是一款名为 SAP Passport 的工具。SAP Passport 客户端工具可为特定工作流的所有 HTTP 请求注入一个唯一标识符，此标识符将转发给该工作流中使用的所有服务器。SAP 支持人员可以使用此唯一标识符汇总该工作流的端到端跟踪消息。

注意：

如果在 CMC 和 BO_trace.ini 配置文件中指定的跟踪日志级别高于在 SAP Passport 客户端工具（SAPClientPlugin.exe）中指定的跟踪日志级别，则会使用前者。

您可以在后端服务器、Web 应用程序和 Web 服务的日志中找到 Passport。

SAP Passport 客户端工具并不作为 BI 平台的一部分进行安装。要访问和下载该工具，请转到 <http://service.sap.com/swdc>。

第 27 章 命令行管理

27.1 Unix 脚本

本节详细介绍 SAP BusinessObjects Business Intelligence 平台的 Unix 分发介质附带的各种管理工具和脚本。本节主要供您参考。概念和配置过程在本指南中有更为详细的论述。

BI 平台的 UNIX 分发介质包含若干脚本，它们提供了 Windows 版本的中央配置管理器（CCM）中的所有可用配置选项。而其他许多脚本为您提供了特定于 Unix 的选项，或者充当您自己的脚本的模板。另外，还有若干 BI 平台使用的次要脚本。下面说明了每个脚本，并在适当的地方提供了命令行选项。

27.1.1 脚本实用程序

本节说明如何借助帮助管理脚本在 UNIX 上使用 BI 平台。本帮助的其余部分论述了可以利用这些脚本执行的每个任务背后的概念。本参考部分为您提供了主要的命令行选项和它们的参数。

27.1.1.1 ccm.sh

ccm.sh 脚本安装在安装程序的 安装目录/sap_bobj 目录中。此脚本为您提供命令行版本的中央配置管理器。本节列出了命令行选项并提供了一些示例。

注意：

- 方括号 [] 中的参数是可选的。

- 如果不确定服务器智能代理的名称，请查看 `ccm.config` 文件中的 `Command` 属性，然后使用出现在 `-name` 选项后面的值。
- 只有安装了 BI 平台的用户才能启动 `ccm.sh` 脚本。
- 由其他身份验证信息指示的参数在第二张表中提供。

CCM 选项	有效参数	说明
<code>-help</code>	不适用	显示命令行帮助。
<code>-start</code>	all 或 SIA 名称	将每个服务器智能代理作为进程启动。all 选项将启动计算机上的所有节点，包括属于不同群集的所有节点。
<code>-stop</code>	all 或 SIA 名称	通过终止其进程 ID 来停止每个服务器智能代理。all 选项将启动计算机上的所有节点，包括属于不同群集的所有节点。
<code>-restart</code>	all 或 SIA 名称	通过终止其进程 ID 来停止每个服务器智能代理，然后启动每个 SIA。all 选项将启动计算机上的所有节点，包括属于不同群集的所有节点。
<code>-managedstart</code>	全限定的服务器名称[其他身份验证信息]	启动服务器。
<code>-managedstop</code>	全限定的服务器名称[其他身份验证信息]	停止服务器。
<code>-managedrestart</code>	全限定的服务器名称[其他身份验证信息]	停止服务器，然后启动服务器。
<code>-managedforceterminate</code>	全限定的服务器名称[其他身份验证信息]	在未完成当前处理请求的情况下立即停止服务器。
<code>-enable</code>	全限定的服务器名称[其他身份验证信息]	启用已启动的服务器，使其向系统注册并开始侦听适当的端口。使用全限定格式的服务器名称。

CCM 选项	有效参数	说明
-disable	全限定的服务器名称[其他身份验证信息]	禁用服务器，使其停止响应 BI 平台请求，但仍然作为进程处于启动状态。使用全限定格式的服务器名称。
-display	[其他身份验证信息]	报告群集中所有服务器的当前状态，包括服务器名称、主机名、进程 ID、说明、是否正在运行以及是否已启用。

下表描述了构成由 [其他身份验证信息] 指示的参数的选项。

注意：

对于改进的安全性，必须始终为帐户凭据提供 Enterprise 身份验证。不支持其他类型的身份验证。

身份验证选项	有效参数	说明
-cms	cms 名称:端口#	指定您想登录到的 CMS。如果未指定，则 CCM 会默认为本地计算机和默认端口（6400）。
-username	用户名	指定提供 BusinessObjects Business Intelligence 平台管理权限的帐户。如果未指定，则会尝试默认的 Administrator 帐户。
-password	密码	指定相应的密码。如果未指定，则会尝试空密码。 注意： 要指定 -password 参数，还必须指定 -username 参数。

CCM 从 ccm.config 文件中读取启动字符串和其他配置值。

相关主题

- 第 846 页上的“[ccm.config](#)”

27.1.1.1.1 示例

以下两个命令将启动和启用所有 BI 平台服务器。中央管理服务器（CMS）在本地计算机和默认端口（6400）上启动：

```
ccm.sh -start all
ccm.sh -enable all
```

以下两个命令将启动和启用所有 BI 平台服务器。CCM 将启用群集中的所有服务器，其中 CMS 在计算机 MACHINE01 和端口 6701 上运行：

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701
```

以下两个命令将启动和启用具有名为 SysAdmin 的指定管理帐户和所提供密码的所有 BI 平台服务器：

```
ccm.sh -start all
ccm.sh -enable all -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

以下命令将使用指定的管理帐户登录，并禁用正运行于另一台计算机上的自适应作业服务器：

```
ccm.sh -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

27.1.1.1.2 ccm.config

此配置文件定义在运行 CCM 的命令时 CCM 使用的启动字符串和其他值。此文件由 CCM 本身和其他 BI 平台脚本实用程序维护。通常只在需要修改服务器智能代理的命令行时才编辑此文件。强烈建议在手动编辑前先备份此文件。

相关主题

- 第 853 页上的“[命令行概述](#)”

27.1.1.2 cmsdbsetup.sh

`cmsdbsetup.sh` 脚本安装在所安装程序的 `sap_bobj` 目录中。该脚本提供基于文本的程序，可用于执行以下任务。

- 配置 CMS 系统数据库
- 重新初始化 CMS 系统数据库
- 从其他数据源复制数据
- 更改群集密钥
- 更改群集名称

注意：

在运行此脚本之前，请备份当前的 CMS 系统数据库以及输入和输出文件资源库的内容。有关更多信息，请参阅“Backing up and Restoring Your System”（备份与恢复系统）。另请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》中“服务器维护”一章中的“将中央管理服务器组成群集”，以了解有关 CMS 群集和配置 CMS 数据库的更多信息。

此脚本将提示执行者输入服务器智能代理（SIA）的名称。要查看 SIA 的名称，请参阅 `ccm.config` 文件中 SIA 的命令属性。SIA 的当前名称显示在 `-name` 选项之后。或者，可以通过 `serverconfig.sh` 文件使用选项 8。

相关主题

- 第 357 页上的[“将中央管理服务器组成群集”](#)
- 第 462 页上的[“备份和恢复概览”](#)

27.1.1.3 `serverconfig.sh`

`serverconfig.sh` 脚本安装在所安装程序的 `sap_bobj` 目录中。此脚本提供基于文本的程序，可用于执行以下操作。

- 添加节点
- 删除节点
- 修改节点
- 移动节点
- 备份服务器配置
- 恢复服务器配置
- 修改 Web 层配置
- 列出所有节点

27.1.1.3.1 在 Unix 上添加/删除/修改/列出节点

- 1 转到安装程序的 安装程序/sap_bobj 目录。
- 2 发出以下命令：

```
./serverconfig.sh
```

此脚本为您显示选项列表：

- a 添加节点
 - b 删除节点
 - c 修改节点
 - d 移动节点
 - e 备份服务器配置
 - f 恢复服务器配置
 - g 修改 Web 层配置
 - h 列出所有节点
- 3 输入对应于您想执行的操作的数字。
 - 4 如果您要添加、删除或修改服务器，则向此脚本提供它所需的任何其他信息。

27.1.2 脚本模板

27.1.2.1 startservers

`startservers` 脚本安装在安装程序的安装目录/sap_bobj 目录中。此脚本可用作您自己的脚本的模板：它作为一个示例提供，向您说明如何设置自己的脚本，以通过运行一系列 CCM 命令来启动 BI 平台服务器。有关编写用于服务器的 CCM 命令的详细信息，请参阅 第 843 页上的 [“ccm.sh”](#)。

27.1.2.2 stopservers

`stopservers` 脚本安装在安装程序的安装目录 `/sap_bobj` 目录。此脚本可用作您自己的脚本的模板：它作为一个示例提供，向您说明如何设置自己的脚本，以通过运行一系列 CCM 命令来停止 BI 平台服务器。有关编写用于服务器的 CCM 命令的详细信息，请参阅第 843 页上的 [“ccm.sh”](#)。

27.1.3 BI 平台使用的脚本

当运行主 BI 平台脚本实用程序时，这些次要脚本通常在后台运行，用户无需亲自运行。

`bobjrestart.sh`

此脚本由 CCM 在内部运行，从而管理服务器智能代理节点。请勿自行运行此脚本。

`env.sh`

将 `env.sh` 脚本安装到您的安装目录 `sap_bobj/setup` 中。此脚本用于设置某些其他脚本所需的 BI 平台环境变量。BI 平台脚本根据需要运行 `env.sh`。有关更多详细信息，请参阅《SAP BusinessObjects Business Intelligence 平台安装指南》。

`env-locale.sh`

`env-locale.sh` 脚本用于在不同的编码类型（例如 UTF8 或 EUC 或 Shift-JIS）之间转换脚本语言字符串。此脚本由 `env.sh` 根据需要运行。

`initlaunch.sh`

`initlaunch.sh` 脚本运行 `env.sh` 以设置 BI 平台环境变量，然后运行已作为该脚本的命令行参数添加的任何命令。此脚本主要供 SAP BusinessObjects 用作调试工具。

`postinstall.sh`

`postinstall.sh` 脚本安装在所安装程序的脚本目录中。用户无需亲自运行此脚本。

`setup.sh`

`setup.sh` 脚本安装在所安装程序的根目录中。此脚本提供一个基于文本的程序，可支持用户设置 BI 平台安装。此脚本在用户安装 BI 平台时自动运行。它提示用户输入初次设置 BI 平台时所需的信息。

有关在安装 BI 平台时如何响应此设置脚本的完整详细信息，请参阅《SAP BusinessObjects Business Intelligence 平台安装指南》。

setupinit.sh

将 setupinit.sh 脚本安装到安装目录 /sap_bobj/init 中。此脚本将运行控制脚本复制到 rc# 目录，以允许自动启动。如果希望 BI 平台服务器随其安装所基于的计算机同步启动和停止，请在 setup.sh 脚本完成后运行此脚本。

注意：
您必须具有 root 权限才能运行此脚本。

27.2 Windows 脚本

本节详细介绍了 BI 平台的 Windows 分发介质附带的各种管理工具和脚本。 本节主要供您参考。概念和配置过程在本指南中有更为详细的论述。

BI 平台的分发介质包括中央配置管理器（CCM）的 Windows 版本。除与 GUI 交互外，还可以选择从带有管理服务器选项的命令行中运行可执行的 CCM。

27.2.1 ccm.exe

将 ccm.exe 可执行文件安装到您的安装目录 安装目录\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64 中。可以直接从命令行运行可执行文件来执行某些操作。本节列出了命令行选项并提供了一些示例。

- 注意：**
- 在使用 ccm.exe 的命令行选项与单个服务器交互之前，必须运行服务器智能代理（SIA）和中央管理服务器（CMS）。
 - 方括号 [] 中的参数是可选的。
 - 由其他身份验证信息指示的参数在第二张表中提供。

CCM 选项	有效参数	说明
-help	不适用	显示命令行帮助。

CCM 选项	有效参数	说明
-managedstart	all 或全限定的服务器名称 [其他身份验证信息]	启动服务器。
-managedstop	all 或全限定的服务器名称 [其他身份验证信息]	停止服务器。
-managedrestart	all 或全限定的服务器名称 [其他身份验证信息]	停止服务器，然后启动服务器。
-managedforceterminate	all 或全限定的服务器名称 [其他身份验证信息]	在未完成当前处理请求的情况下立即停止服务器。
-enable	all 或全限定的服务器名称 [其他身份验证信息]	启用已启动的服务器，使其向系统注册并开始侦听适当的端口。
-disable	all 或全限定的服务器名称 [其他身份验证信息]	禁用服务器，使其停止响应 BI 平台请求，但仍然作为进程处于启动状态。
-display	[其他身份验证信息]	报告群集中所有服务器的当前状态，包括服务器名称、主机名、进程 ID、说明、是否正在运行以及是否已启用。

下表描述了构成由 [其他身份验证信息] 指示的参数的选项。

注意：

对于 Enterprise 身份验证，必须始终提供帐户的凭据。

身份验证选项	有效参数	说明
-cms	cms 名称:端口#	指定您想登录到的 CMS。如果未指定，则 CCM 会默认为本地计算机和默认端口（6400）。

身份验证选项	有效参数	说明
-username	用户名	指定提供 BI 平台管理权限的帐户。如果未指定，则会尝试默认的 Administrator 帐户。
-password	密码	指定相应的密码。如果未指定，则会尝试空密码。 注意： 要指定 -password 参数，还必须指定 -username 参数。
-authentication	身份验证类型	指定身份验证类型。仅支持 secEnterprise。

CCM 从 ccm.config 文件中读取启动字符串和其他配置值。

27.2.1.1 示例

以下示例假设服务器智能代理（SIA）和中央管理服务器（CMS）已启动并且正在运行。在使用 ccm.exe 的命令行选项与单个服务器交互之前，可以使用以下 Windows 命令启动 SIA 服务。

```
net start "Server Intelligence Agent (NODENAME)"
```

SIA 还可以使用 net stop "Server Intelligence Agent (NODENAME)" 停止。

该命令将启动所有 BI 平台服务器：

```
ccm.exe -managedstart all
```

此命令启动自适应作业服务器。CMS 在端口 6701 而不是在默认端口上启动：

```
ccm.exe -managedstart MACHINE01.AdaptiveJobServer -cms MACHINE01:6701
```

此命令利用名为 SysAdmin 的指定管理帐户启用自适应作业服务器。

```
ccm.exe -enable MACHINE01.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

此命令以指定的管理帐户登录以禁用正在另一台计算机上运行的自适应作业服务器：

```
ccm.exe -disable MACHINE02.AdaptiveJobServer -cms MACHINE01:6701 -username SysAdmin -password 35%bC5@5
```

27.3 服务器命令行

27.3.1 命令行概述

本节列出控制每个 BI 平台服务器行为的命令行选项。

当通过中央管理控制台（CMC）启动或配置服务器时，使用包括一组典型选项和值的默认命令行启动（或重新启动）该服务器。在大多数情况下，您无需直接修改默认命令行。此外，可以通过 CMC 中的各种服务器配置屏幕对最常见的设置进行操作。本节提供每个服务器支持的命令行选项的完整列表以供参考。如果需要进一步自定义 BI 平台的行为，可以直接修改每个服务器的命令行。

在本节中，方括号 [] 中提供的值是可选的。

注意：

下表列出了受支持的命令行选项：BI 平台服务器使用这些表中未列出的许多内部选项。不能修改这些内部选项。

27.3.1.1 查看或修改服务器的命令行

- 1 使用中央管理控制台（CMC）停止服务器。
- 2 右击该服务器并选择“属性”。
- 3 在“属性”屏幕上，修改该服务器的命令行，然后单击“保存并关闭”。
- 4 启动服务器。

27.3.2 适用于所有服务器的标准选项

除非另有说明，否则这些命令行选项适用于所有 SAP BusinessObjects Business Intelligence 平台服务器。有关每种类型的服务器特定的选项，请参阅本节其余的部分。

选项	有效参数	行为
<code>-requestPort</code>	端口	<p>指定服务器侦听的端口。服务器向 CMS 注册此端口。如果未指定，服务器将选择大于 1024 的任何空闲端口。</p> <p>注意： 不同的服务器将此端口用于不同的目的。在更改之前，请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》中有关更改默认服务器端口号的一节。</p>
<code>-loggingPath</code>	绝对路径	指定创建日志文件的路径。

27.3.2.1 Unix 信号处理

在 UNIX 上，BI 平台后台程序将处理以下信号：

- SIGTERM 将使服务器正常关机（退出代码 = 0）。
- SIGSEGV、SIGBUS、SIGSYS、SIGFPE 和 SIGILL 将导致快速关机（退出代码 = 1）。

27.3.3 中央管理服务器

本节提供特定于 CMS 的命令行选项。在 Windows 上，服务器的默认路径为安装目录\BusinessObjects Enterprise XI 4.0\win64_x64\CMS.exe。

在 UNIX 上，服务器的默认路径为安装目录/sap_bobj/enterprise_xi40/platform/boe_cmsd。

选项	有效参数	行为
-threads	数字	指定 CMS 初始化和使用的工作线程数。该值可以介于 12 至 150 之间，默认情况下设置为 50。
-reinitializedb		导致 CMS 删除系统数据库，并只使用默认的系统对象重新创建系统数据库。重新创建数据库时，其中的所有现有数据都将丢失。
-quit		在处理完 -reinitializedb 选项后强制 CMS 退出。
-receiverPool	数字	指定 CMS 所创建的用于接收客户端请求的线程数。客户端可以是另一台 SAP BusinessObjects 服务器、报表发布向导、Crystal Reports 或您创建的自定义客户端应用程序。默认值为 5。通常情况下，您不需要增加该值，除非您创建了一个具有许多客户端的自定义应用程序。
-maxobjectsincache	数字	指定 CMS 存储在其内存高速缓存中的最大对象数。增加对象数将会减少数据库调用的次数，并显著提高 CMS 的性能。但是，将太多对象放在内存中可能会导致 CMS 用于处理查询的剩余内存太少。上限为 100000。

选项	有效参数	行为
<code>-ndbqthreads</code>	数字	指定将请求发送到数据库的 CMS 工作线程数。每个线程都连接到数据库，因此必须小心不要超出数据库容量。多数情况下，应将最大值设置为 20。
<code>-oobthreads</code>	数字	如果群集包含超过八个的 CMS 群集成员，请确保每个 CMS 的命令行均包含此选项。指定群集中的 CMS 服务数量。此选项确保群集可以承受沉重的负载。

相关主题

- 第 853 页上的“[适用于所有服务器的标准选项](#)”

27.3.4 Crystal Reports 处理服务器和 Crystal Reports 高速缓存服务器

从命令行控制 Crystal Reports 处理服务器和 Crystal Reports 高速缓存服务器的方式基本相同。命令行选项确定服务器是作为处理服务器、高速缓存服务器还是同时作为这两个服务器启动。仅适用于一种服务器类型的选项会在下面加以注释。

在 Windows 上，服务器的默认路径为：

- 安装目录\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\cacheserver.exe。
- 安装目录\BusinessObjects Business Intelligence platform XI 4.0\win64_x64\pageserver.exe。

在 Unix 上，服务器的默认路径为：

- 安装目录/sap_bobj/enterprise_xi40/平台/boe_cachesd。
- 安装目录/sap_bobj/enterprise_xi40/平台/boe_procd。

选项	有效参数	行为
<code>-cache</code>		启用高速缓存服务器功能。

选项	有效参数	行为
-deleteCache		服务器每次启动和停止时删除缓存目录。
-report_ProcessExtPath	绝对路径	指定处理扩展的默认目录。有关详细信息，请参阅《SAP BusinessObjects Business Intelligence 平台 管理员指南》。

相关主题

- 第 853 页上的[“适用于所有服务器的标准选项”](#)

27.3.5 Dashboards 处理服务器和 Dashboards 高速缓存服务器

从命令行控制 Dashboards 处理服务器和 Dashboards 高速缓存服务器的方式基本相同。命令行选项确定服务器是作为处理服务器、高速缓存服务器还是同时作为这两个服务器启动。仅适用于一种服务器类型的选项会在下面加以注释。

在 Windows 上，服务器的默认路径为：

- 安装目录\SAP BusinessObjects\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\xccache.exe。
- 安装目录\SAP BusinessObjects\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\xcproc.exe。

在 Unix 上，服务器的默认路径为：

- 安装目录/sap_bobj/enterprise_xi40/<platform>_64/boe_xccached。
- 安装目录/sap_bobj/enterprise_xi40/<platform>_64/xcprocd。

选项	有效参数	行为
-cache		启用高速缓存服务器功能。

选项	有效参数	行为
-dir	绝对路径	指定高速缓存服务器的高速缓存目录和处理服务器的临时目录。创建的目录为 absolutepath/cache 和 absolutepath/temp
-deleteCache		服务器每次启动和停止时删除缓存目录。
-psdir	绝对路径	指定处理服务器的临时目录。此选项优先于 -dir。
-refresh	分钟数	共享缓存页面指定的分钟数。
-auditMaxEventsPerFile	数字	在高速缓存服务器上，指定审核日志文件中记录的审核操作的最大数目。默认值为 500。如果超过此最大记录数目，服务器将打开一个新日志文件。

相关主题

- 第 853 页上的“[适用于所有服务器的标准选项](#)”

27.3.6 作业服务器

本节介绍特定于自适应作业服务器的命令行选项。

在 Windows 上，服务器的默认路径为安装目录\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\JobServer.exe。

在 Unix 上，服务器的默认路径为安装目录/sap_bobj/enterprise_xi40/PLATFORM/boe_jobsd。

选项	有效参数	行为
<code>-dir</code>	绝对路径	指定作业服务器的数据目录。
<code>-maxJobs</code>	数字	设置服务器可处理的最大并发作业数量。默认值为 5。
<code>-requestJSChildPorts</code>	下限-上限	<p>指定子进程应在防火墙环境中使用的端口范围。例如，6800-6805 将子进程限制到 6 个端口。</p> <p>注意： 要使此选项生效，还必须指定 <code>-requestPort</code> 设置。</p>
<code>-report_ProcessExtPath</code>	绝对路径	<p>指定处理扩展的默认目录。有关详细信息，请参阅《SAP BusinessObjects Business Intelligence 平台 管理员指南》。</p>

相关主题

- 第 853 页上的“[适用于所有服务器的标准选项](#)”

27.3.7 自适应处理服务器

自适应处理服务器使用为 SAP Java 虚拟机（SAP JVM）定义的参数。请参阅 SAP JVM 文档以了解更多信息。

27.3.8 报表应用程序服务器

本节介绍报表应用程序服务器特定的命令行选项。

在 Windows 上，服务器的默认路径为安装目录\SAP BusinessObjects Business Intelligence platform 4.0\win32_x86\crystalras.exe。

在 Unix 上，服务器的默认路径为安装目录/sap_bobj/enterprise_xi40/PLATFORM/ras/boe_crystalrasd。

选项	有效参数	行为
-ipport	端口	指定在独立模式下（在 BI 平台外部）运行时用于接收 TCP/IP 请求的端口号。
-report_ProcessExtPath	绝对路径	指定处理扩展的默认目录。有关详细信息，请参阅《SAP BusinessObjects Business Intelligence 平台 管理员指南》。

选项	有效参数	行为
<code>-ProcessAffinityMask</code>	掩码	<p>使用掩码来精确指定 RAS 在多处理器计算机上运行时将使用哪些 CPU。</p> <p>该掩码采用格式 0xffffffff，其中每个 f 代表一个处理器，处理器列表的阅读顺序为从右到左（也就是说，最后一个 f 代表第一个处理器）。将每个 f 替换为 0（不允许使用 CPU）或 1（允许使用 CPU）。</p> <p>例如，如果在一台有 4 个处理器的计算机上运行 RAS 并要使用第三个和第四个处理器，请使用掩码 0x1100。若要使用第二个和第三个处理器，请使用 0x0110。</p> <p>注意：</p> <ul style="list-style-type: none">• RAS 使用字符串中第一个允许的处理器，最多可使用您的许可允许的最大处理器数。如果有两个处理器许可，则 0x1110 的作用和 0x0110 相同。• 掩码的默认值是 -1，它的意义与 0x1111 相同。

相关主题

- 第 853 页上的“[适用于所有服务器的标准选项](#)”

27.3.9 Web Intelligence 处理服务器

本节介绍 Web Intelligence 处理服务器特定的命令行选项。

在 Windows 上，服务器的默认路径为 安装目录\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\WIReportServer.exe。

在 Unix 上，服务器的默认路径为 安装目录/sap_bobj/enterprise_xi40/PLATFORM/WIReportServer。

选项	有效参数	行为
-ConnectionTimeout Minutes	分钟数	指定多少分钟后服务器将超时。
-MaxConnections	数字	指定服务器允许同时存在的最大同时连接数。
-DocExpressEnable		在查看 Web Intelligence 文档时启用对文档进行高速缓存。
-DocExpressRealTime CachingEnable		启用对 Web Intelligence 文档进行实时高速缓存。
-DocExpressCache DurationMinutes	分钟数	指定内容存储在高速缓存中的时间（以分钟为计）。
-DocExpressMaxCache SizeKB	千字节	指定文档高速缓存的大小。
-EnableListOfValues Cache		启用对每个值列表用户会话进行高速缓存的功能
-ListOfValuesBatchSize	数字	指定每个值列表批次可返回的值的最大数量。
-UniverseMaxCacheSize	数字	指定要高速缓存的 Universe 数。
-WIDMaxCacheSize	数字	指定可存储在高速缓存中的最大 Web Intelligence 文档数。

相关主题

- 第 853 页上的“[适用于所有服务器的标准选项](#)”

27.3.10 输入文件资源库服务器和输出文件资源库服务器

本节介绍输入文件资源库服务器和输出文件资源库服务器特定的命令行选项。

在 Windows 上，服务器的默认路径为安装目录\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\fileserver.exe。

在 Unix 上，提供这两个服务器的程序默认路径为安装目录/sap_bobj/enterprise_xi40/platform/boe_filesd。默认情况下，服务器智能代理将为输入文件资源库服务器启动 boe_filesd 的一个实例，并为输出文件资源库服务器启动一个实例。

选项	有效参数	行为
<code>-rootDir</code>	绝对路径	<p>设置服务器托管的各个子文件夹和文件的根目录。相对于此根目录对用于引用文件资源库服务器中文件的文件路径进行解释。</p> <p>注意： 所有输入文件资源库服务器必须共享相同的根目录，所有输出文件资源库服务器必须共享相同的根目录（否则可能出现不一致的实例）。此外，输入根目录不得与输出根目录相同。建议您使用 RAID 阵列或替代硬件解决方案复制根目录。</p>

选项	有效参数	行为
<code>-tempDir</code>	绝对路径	<p>设置 FRS 用于传输文件的临时目录的位置。如果要控制 FRS 临时目录的位置，或者 FRS 生成的默认临时目录名称超出了文件系统路径限制（使 FRS 无法启动），请使用此命令行选项。</p> <p>注意： 不要为此选项指定现有目录。FRS 启动时将清空指定的目录，FRS 关闭时将删除该目录。如果使用现有目录，该目录将被清空和删除。</p>
<code>-maxidle</code>	分钟数	<p>指定清除空闲会话之前的分钟数。</p>

相关主题

- 第 853 页上的“[适用于所有服务器的标准选项](#)”

27.3.11 事件服务器

本节介绍事件服务器特定的命令行选项。

在 Unix 上，服务器的默认路径为安装目录\SAP BusinessObjects Business Intelligence platform 4.0\win64_x64\EventServer.exe。

在 Unix 上，服务器的默认路径为安装目录/sap_bobj/enterprise_xi40/platform/boe_eventsd。

选项	有效参数	行为
-cleanup	分钟数	指定服务器清除侦听器代理的频率（以分钟为单位）。该值表示执行两次清除操作所花费的时间量。例如，如果将值指定为 10，则每五分钟将清除一次代理。

相关主题

- 第 853 页上的“[适用于所有服务器的标准选项](#)”

第 28 章 资源库诊断工具

28.1 资源库诊断工具概述

资源库诊断工具（RDT）是一个命令行工具，此工具可以扫描、诊断和修复中央管理服务器（CMS）系统数据库与文件资源库服务器（FRS）文件存储之间可能存在的项，或者存储在 CMS 数据库内的 InfoObject 元数据中可能存在的项。

在正常操作过程中，CMS 系统数据库具有不一致之处是不正常的。但是，在发生意外事件（例如，灾难恢复、备份还原或网络中断）时可能存在不一致之处。在这些事件过程中，执行任务时 CMS 系统数据库可能会中断。这可能导致 CMS 系统数据库中存在与对象的不一致之处。

RDT 将扫描 CMS 系统数据库，并找出对象（如报表、用户、用户组、文件夹、服务器、Universe、Universe 连接和其他对象）中的不一致项。

RDT 将扫描两种类型的不一致。

- 对象与文件之间的不一致。

这些不一致可能存在于 CMS 数据库中的 InfoObject 与文件资源库中的相应文件之间。例如，存储在 FRS 中的文件在 CMS 系统数据库中可能缺少对应的对象。

- InfoObject 元数据不一致。

这些不一致可能存在于 CMS 数据库内 InfoObject 的对象定义（元数据）中。例如，InfoObject 可能会引用在 CMS 数据库中不存在的另一个 InfoObject。

基于运行 RDT 时提供的参数，该工具将执行以下两项功能：

- 它将扫描 CMS 系统数据库和 FRS 文件存储，报告不一致之处，输出 XML 格式的日志文件并建议用于修复不一致之处的操作。
- 它将扫描并修复在 CMS 系统数据库和 FRS 中找到的不一致之处，并将所执行的操作输出到 XML 格式的日志文件中。

28.2 使用资源库诊断工具

在任何安装有中央配置管理器（CCM）的计算机上都可以使用资源库诊断工具（RDT）。此命令行工具将扫描、诊断和修复可能存在于中央管理服务器（CMS）系统数据库与文件资源库服务器（FRS）文件存储之间的不一致项或可能存在于 InfoObject 元数据中的不一致项。

建议备份 CMS 数据库和 FRS 文件存储，并在停止 SAP BusinessObjects Business Intelligence 平台服务后对备份版本运行 RDT。如果无法进行此操作，则可在活动数据库中运行 RDT。

如果要在活动数据库中运行 RDT，请注意以下事项：

- RDT 在运行时将使用一个数据库连接。
- RDT 仅检查其开始运行时的一致性。RDT 运行期间发生的任何不一致情况均不会予以记录或修复。
- 建议运行 RDT 的主机计算机的内存要高于处理 RDT 事务的常规系统建议值：
 - InfoObject 数等于或少于 50,000 的数据库应额外具有 350 MB 内存用于处理
 - InfoObject 数在 50,000 到 400,000 之间的数据库应额外具有 1.7 GB 内存用于处理
 - InfoObject 数在 400,000 到 1,000,000 之间的数据库应额外具有 4 GB 内存用于处理
- RDT 不必从 CMS 服务器运行。在单独的计算机上运行 RDT 可降低对系统性能的影响。
- 该工具在运行时可能会对数据库性能产生一定影响。

RDT 不要求运行 CMS 服务，RDT 可直接针对 CMS 数据库运行。

28.2.1 使用资源库诊断工具

1. 如果要在 Windows 计算机上运行此工具，请打开命令窗口并运行以下命令。

安装目录\SAP BusinessObjects Enterprise XI 4.0\win64_x64\reposcan.exe arguments，其中 arguments 是要指定参数的列表。

2. 如果要在 Unix 计算机上运行此工具，请打开 /usr/bin/sh 兼容外壳，并运行以下命令。

. 安装目录/sap_bobj/enterprise_xi40/platform/boe_reposcan.sh arguments，其中 platform 是 linux_x64、solaris_sparcv9、hpux_ia64 或 aix_rs6000_64，而 arguments 是要指定的参数的列表。

资源库诊断工具将在资源库中扫描不一致项。基于所指定的参数，该工具将诊断并记录不一致项，或者将修复不一致项并记录它所执行的操作。

Repo_Scan_yyyy_mm_dd_hh_mm_ss.xml 列出了工具找出的不一致。如果让工具修复它所找到的差异，则该工具还将创建文件 Repo_Repair_yyyy_mm_dd_hh_mm_ss.xml。此文件详细说明修复了哪些对象以及删除的任何孤立文件。如果存在无法修复的不一致情况，也会列出这些信息。

可以通过 `outputdir` 参数指定日志文件的路径。如果未指定此参数，则日志文件在 Windows 上的默认目录为 `安装目录\SAP BusinessObjects Enterprise XI 4.0\reposcan`，在 Unix 上为 `./sap_bobj/enterprise_xi40/reposcan`。

注意：

此应用程序还提供了一个默认的 XSL 文件，该文件与 XML 文件一起使用以产生 HTML 页面。在 Windows 上，XSL 文件存储于 `<安装目录>\SAP BusinessObjects Enterprise XI 4.0\reposcan`，在 Unix 上存储于 `./sap_bobj/enterprisexi_40/reposcan`。

有关警告消息以及 RDT 在发现不一致项时执行的建议操作的列表，请参阅 “CMS 元数据中的不一致项” 和 “CMS 与 FRS 之间的不一致项”。

相关主题

- 第 874 页上的[“CMS 元数据中的不一致项”](#)
- 第 873 页上的[“ CMS 与 FRS 之间的不一致”](#)

28.2.2 资源库诊断工具参数

RDT 接受下表中的参数：

注意：

执行时命令行参数将覆盖任何参数文件条目。

表28-1：常规参数

参数	可选或必需	说明
dbdriver	必需	<p>用于连接到 CMS 数据库的驱动程序类型。接受的值包括：</p> <ul style="list-style-type: none">• db2databasesubsystem• maxdbdatabasesubsystem• mysqldatabasesubsystem• oracledatabasesubsystem• sqlserverdatabasesubsystem• sybasedatabasesubsystem• sqlanywheredatabasesubsystem

参数	可选或必需	说明
connect	必需	<p>用于连接到 CMS 数据库的连接详细信息。</p> <p>例如：-connect "UID=root;PWD=密码;DSN=dsn;HOSTNAME=主机名;PORT=端口号"</p>
dbkey	必需	<p>输入 BI 平台部署的群集密钥。</p> <p>如果不知道群集密钥，请通过下述步骤重置群集密钥：</p> <p>注意： 如果计算机位于群集中，则需要为所有群集成员执行这些步骤。先备份 CMS 数据库和文件存储，然后继续。</p> <ol style="list-style-type: none"> 1 启动中央配置管理器（CCM）。 2 在 CCM 中，右击服务器智能代理（SIA）并选择“停止”。在 SIA 状态为“已停止”之前，请勿继续到步骤 3。 3 右击 SIA 并选择“属性”。 4 在“配置”选项卡上，单击“CMS 群集密钥配置”旁的“更改”。 5 将显示一条警告消息。单击“是”以继续。 6 在“更改群集密钥”对话框中，在“新群集密钥”和“确认新群集密钥”字段中输入相同的八字符密钥。 <p>注意：</p> <ul style="list-style-type: none"> • 如果忽略 dbkey 参数，或者如果群集密钥不正确，RDT 将不会运行。 • CCM 中显示的群集密钥是加密的，在 dbkey 参数中无法使用。 <p>有关群集密钥的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》中的“BI 平台安全”。</p>
inputfrsdir	必需	<p>输入文件资源库服务器的文件路径。</p> <p>注意： 将使用登录时所用的用户帐户执行此命令行工具。该用户帐户必须拥有对文件位置的完全控制权限。</p>

参数	可选或必需	说明
outputfrsdir	必需	<p>输出文件资源库服务器的文件路径。</p> <p>注意： 将使用登录时所用的用户帐户执行此命令行工具。该用户帐户必须拥有对文件位置的完全控制权限。</p>
outputdir	可选	<p>RDT 在其中编写日志文件的文件路径。</p> <p>在 Windows 上，默认值为安装目录\SAP BusinessObjects Enterprise XI 4.0\reposcan，在 Unix 上，默认值为 ./sap_bobj/enterprise_xi40/reposcan。</p>
count	可选	<p>要扫描的近似错误数。这有助于确保实现最佳性能。计数上限为 $2e31 - 1$。值 0 被解释为整个资源库。</p> <p>默认值为 0。</p>
repair	可选	<p>指示 RDT 修复可能发现的所有不一致项。默认行为是只报告不一致项，但不执行任何修复。如果命令行上存在 -repair 参数，则 RDT 将报告并修复所有不一致项。</p> <p>警告： 该过程将删除资源库数据库中的任何孤立对象或文件。</p>
scanfrs	可选	<p>指定 RDT 是否在 CMS 和 FRS 中扫描不一致项。可接受的值为 True 和 False。</p> <p>默认值为 True。</p>
scancms	可选	<p>指定 RDT 是否在 CMS 中扫描 InfoObject 之间的不一致项。可接受的值为 True 和 False。</p> <p>默认值为 True。</p>

参数	可选或必需	说明
submitterid	可选	<p>指定用户 ID 以替换计划对象的丢失或无效的 ID。如果未提供值，则 RDT 不会替换无效的 ID。如果提供的用户 ID 在 CMS 中不存在，则 RDT 会提示您输入一个有效的 ID。</p> <p>仅在修复模式下运行 RDT 时才使用此参数。</p>
startid	可选	<p>指定在 CMS 数据库中开始进行扫描的对象。例如，如果已经扫描了资源库中的前 500 个对象，则可以设置 -startid=501 以从第 501 个对象开始进行新的扫描。</p> <p>默认值为 1。</p>
optionsfile	可选	<p>指定参数文件的文件路径。参数文件是一个列出了每个命令行选项及其值的文本文件。该文件中每行都应该有一个参数。</p> <p>注意： 借助此选项，用户可以按以上所述在一个文本文件中设置所有参数。然后使用此选项指向此参数文件，而不必在命令行中输入这些参数。</p>
syscopy	可选	<p>复制资源库数据库时使用此参数。必须在新创建的副本上运行该工具，这将更新副本以防止其与源系统服务器进行群集。如果副本无法与源系统通信，则不必执行此操作。它只能与强制性参数一起使用，而不能与列表中的其他可选参数组合使用。</p> <p>注意： 请注意，不要在源系统上使用 syscopy 参数运行 RDT。</p>

如果资源库诊断工具正在活动的群集 CMS 上运行，则使用下列参数。

表28-2：对群集的 CMS 使用 RDT

参数	可选或必需	说明
requestport	可选	<p>RDT 用于与 CMS 通信的端口号。接受正整数。默认情况下，该工具使用的值来自运行 RDT 的计算机的操作系统。</p>

参数	可选或必需	说明
numericip	可选	确定 RDT 是否将数字 IP 地址（而不是主机名）用于 CMS 与运行 RDT 的计算机之间的通信。可接受的值为 True 和 False。 默认值为 False。
ipv6	可选	运行 RDT 的计算机的 ipv6 名称。接受字符串。 默认值是运行 RDT 的计算机的主机名。
port	可选	运行 RDT 的计算机的 ipv4 名称。接受字符串。 默认值是运行 RDT 的计算机的主机名。
threads	可选	要使用的线程的数目。接受正整数。 默认值为 12。

当 RDT 使用 SSL 与它所扫描的 CMS 数据库通信时，使用以下参数。

表28-3：将 RDT 与 SSL 一起使用

参数	可选或必需	说明
protocol	可选	指定是否应该在 SSL 模式下运行此工具。 仅接受值 ssl。
ssl_certdir	可选	包含 SSL 证书的目录。
ssl_trustedcertificate	可选	证书的文件名。
ssl_mycertificate	可选	签名的证书的文件名。
ssl_mykey	可选	包含 SSL 私钥的文件的文件名。
ssl_mykey_passphrase	可选	包含 SSL 密码短语的文件的文件名。

示例：

以下示例将在 CMS 和 FRS 中扫描两种类型的不一致项，并修复它所发现的不一致项。

```
reposcan.exe
-dbdriver mysqldatabasesubsystem
-connect UID=root;PWD=Password1;DSN=myDsn;HOSTNAME=myHostname;PORT=3306
-inputfrsdir C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\FileStore\Input
-outputfrsdir C:\Program Files (x86)\SAP BusinessObjects\SAP BusinessObjects Enterprise XI 4.0\FileStore\Output
-dbkey cluster key
-repair
```

28.3 CMS 与 FRS 之间的不一致

下表描述资源库诊断工具（RDT）所识别的可能存在于中央管理服务器（CMS）数据库和文件资源库服务器（FRS）之间的不一致项。此表具有以下 4 个列：

- 警告消息

写入扫描和修复日志文件中的警告消息。

- 不一致

关于 RDT 所找到的对象不一致的解释。

- 建议

RDT 在发现不一致时建议执行的操作。这可以在扫描日志文件中找到。

- 操作

RDT 所执行的用于修复不一致项的操作。这可以在修复日志文件中找到。

警告消息	不一致	建议	操作
对象名称 对象 对象类型（对象 ID = ID）正在引用 FRS（文件名）中不存在的文件。	对象存在于 CMS 数据库中，但 FRS 中没有对应的文件。	允许应用程序删除此对象。此对象的任何后代对象也将被删除。	从资源库中删除此对象。
文件文件名存在于输入或输出 FRS 中，但资源库中没有对应的 InfoObject。	此文件存在于 FRS 中，但 CMS 数据库中也没有对应的文件。	允许应用程序删除未链接的文件。	未执行任何操作。
对象类型 对象 对象名称（对象 ID = ID）具有文件文件名。存储的文件大小为大小字节，这与实际的文件大小大小字节不匹配。	该文件的大小与 InfoObject 文件大小不匹配。	允许应用程序使用正确的文件大小更新对象。	将对象更新为具有正确的文件大小。
此目录未包含任何文件。	FRS 文件夹为空。	允许应用程序删除目录。	删除空文件夹。

28.4 CMS 元数据中的不一致项

下表描述了资源库诊断工具（RDT）所识别的可能存在于中央管理服务器（CMS）系统数据库内对象元数据中的不一致项。此表具有以下 4 个列：

- 警告消息

写入扫描和修复日志文件中的警告消息。

- 不一致

关于 RDT 所找到的对象不一致的解释。

- 建议

RDT 在发现不一致时建议执行的操作。这可以在扫描日志文件找到。

- 操作

RDT 所执行的用于修复不一致项的操作。这可以在修复日志文件找到。

警告消息	不一致	建议	操作
对象类型对象 对象名称（对象 ID = ID）缺少父对象（父对象 ID = ID）。	对象缺少父对象 ID，或者对象的父对象 ID 无效。	允许应用程序将对象移到“BOE Repair”文件夹。	将对象及其子对象移到“BOE Repair”文件夹。
对象类型 对象 对象名称（对象 ID = ID）缺少所有者对象（所有者对象 ID = ID）。	对象缺少所有者对象 ID，或者对象的所有者对象 ID 无效。	允许应用程序将对象分配给管理员。	将对象分配给管理员。
对象类型 对象 对象名称（对象 ID = ID）缺少提交者对象（提交者对象 ID = ID）。	对象缺少提交者对象 ID，或者对象的提交者对象 ID 无效。	<p>RDТ 所显示的建议取决于是否为 -submitterid 参数提供了值。</p> <ul style="list-style-type: none"> 如果提供此参数，则建议为允许应用程序用提供的提交者 ID 更新对象。 如果未提供此参数，则建议为重新计划对象或使用 -submitterid 命令行替换无效的提交者 ID。 	<p>如果提供 -submitterid 参数值，则 RDТ 会将该值应用于对象的提交者 ID。</p> <p>如果没有为此参数提供值，则 RDТ 不会采取任何操作。重新计划对象时，CMS 将应用新 ID。</p>
对象类型 对象 “对象名称” 上一个成功实例的（对象 ID = ID）属性引用了缺少的对象（上一个成功实例对象 ID = ID）。	对象缺少上一个成功实例，或对象的上一个成功实例无效。	允许应用程序重新计算属性。	重新计算属性。
对象类型 对象 “对象名称”（对象 ID = ID）缺少日历对象（日历对象 ID = ID）。	对象引用了不存在的日历。	使用现有的日历重新计划对象。此应用程序不会执行任何操作。	未执行任何操作。
对象类型对象 “对象名称”（对象 ID = ID）缺少必需的计划服务器组（服务器组对象 ID = ID）。	首选的服务器不存在。	重新计划对象并选择一个现有的服务器组。此应用程序不会执行任何操作。	未执行任何操作。

警告消息	不一致	建议	操作
对象类型对象“对象名称”（对象 ID = ID）的挂起事件列表缺少的对象（事件对象 ID = ID）。	此对象正在等待的一个或多个事件不存在。	重新计划对象以等待现有事件对象。此应用程序不会执行任何操作。	未执行任何操作。
对象类型 对象“对象名称”（对象 ID = ID）的待触发事件列表包含缺少的对象（事件对象 ID = ID）。	此对象触发的事件不存在。	允许应用程序从对象的待触发事件列表中删除缺少的事件。	从对象的待触发事件列表中删除缺少的事件。
对象类型 对象“对象名称”（对象 ID = ID）的访问控制列表引用了缺少的主体（主体对象 ID = ID）。	孤立的访问控制项。	允许应用程序从对象的访问控制列表中删除缺少的主体。	从对象的访问控制列表中删除缺少的主体。
对象类型 对象“对象名称”（对象 ID = ID）的访问控制列表引用了缺少的访问级别（访问级别对象 ID = ID）。	孤立的访问控制项。	允许应用程序从对象的访问控制列表中删除缺少的访问级别。	从对象的访问控制列表中删除缺少的访问级别。
对象类型 对象 对象名称（对象 ID = ID）具有多个收藏夹文件夹。	特定用户帐户具有多个收藏夹文件夹。	允许应用程序将多个文件夹合并成一个收藏夹文件夹。	所有收藏夹文件夹已合并到一个收藏夹文件夹中。
对象类型 对象 对象名称（对象 ID = ID）包含无效的输入文件条目（文件）。	该对象的输入文件列表中包含无效的条目。	允许工具删除对象输入文件列表中的无效条目。	从对象输入文件列表中删除无效的条目。
对象类型 对象 对象名称（对象 ID = ID）包含无效的输入文件条目（文件）。	该对象的输出文件列表中包含无效的条目。	允许工具删除对象输出文件列表中的无效条目。	从对象输出文件列表中删除无效的条目。

警告消息	不一致	建议	操作
对象类型 对象 对象名称 (对象 ID = ID) 缺少必需的高速缓存服务器组 (服务器组对象 ID = ID)。	该对象缺少必需的高速缓存服务器组。	重新计划对象并选择一个现有的服务器组。	未执行任何操作。
对象类型 对象 对象名称 (对象 ID = ID) 缺少必需的计划服务器组 (服务器组对象 ID = ID)。	该对象缺少必需的处理服务器组。	重新计划对象并选择一个现有的服务器组。	未执行任何操作。
对象类型 对象 对象名称 (对象 ID = ID) 的配置文件列表中包含缺少的对象 (配置文件对象 ID = ID)。	该对象的配置文件列表中包含缺少的对象。	请使用现有配置文件更新发布。此应用程序不会执行任何操作。	未执行任何操作。

第 29 章 权限附录

29.1 关于权限附录

本权限附录列出并说明了可以在 BI 平台系统中对不同对象设置的大部分权限。对于需要一种以上的权限才能在对象上执行任务的情况，本附录也提供了有关所需的其他权限和必须在哪些对象上拥有这些权限的信息。有关设置权限的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》中的“设置权限”一章。

29.2 常规权限

本节中的权限适用于多种对象类型。这些权限中有许多还具有等效的所有者权限。所有者权限只适用于其权限正在接受检查的对象的所有者。

以下权限只适用于可以计划的对象：

- “计划文档运行”权限。
- “代表其他用户进行计划”权限。
- “计划到目标”权限。
- “查看文档实例”权限。
- “删除实例”权限。
- “暂停并继续文档实例”权限。
- “重新计划实例”权限。

权限	说明
查看对象	允许查看对象及其属性。如果对于某个对象没有此权限，则会在 BI 平台系统中隐藏该对象。此权限是所有任务都需要的基本权限。
将对象添加到文件夹	允许将对象添加到文件夹。此权限也适用于行为类似于文件夹的对象，例如收件箱、收藏夹文件夹或对象包。
编辑对象	允许编辑对象内容以及对象和文件夹的属性。
修改用户拥有的对象权限	允许修改对象的安全设置。
安全地修改用户拥有的对象权限	允许向其他用户授予自己已拥有的对象权限或访问级别。要这样做，还需要在用户和对象本身上拥有此权限。有关此权限的更多信息，请参阅《SAP BusinessObjects Business Intelligence 平台管理员指南》中的“设置权限”一章。
定义服务器组以便处理作业	<p>允许指定在处理对象时要使用的服务器组。此权限仅适用于可以为其指定处理服务器的对象。</p> <p>要指定服务器组，还需要有对象的“编辑对象”权限。</p>
删除对象	允许删除对象及其实例。
将对象复制到另一文件夹	<p>允许在 CMS 中的其他文件夹内创建对象的副本。要这样做，还需要具有对目标文件夹的“将对象添加到文件夹”权限。</p> <p>注意： 复制对象时，未复制对象上的显式安全性；新对象将继承目标文件夹的安全设置，但必须重新设置显式安全性。</p>
复制内容	允许将对象复制到联合部署中的另一个系统。
计划文档运行	允许计划对象。
代表其他用户进行计划	<p>允许为其他用户或组计划对象。为其计划对象的用户或组将成为对象实例的所有者。</p> <p>要为其他用户或组计划对象，还需要有以下权限：</p> <ul style="list-style-type: none"> • 用户或组的此权限。 • 对象的“计划文档运行”权限。

权限	说明
计划到目标	<p>允许执行以下操作：</p> <ul style="list-style-type: none">• 将对象计划到默认 Enterprise 位置以外的目标。• 修改为计划指定的默认目标。 <p>要将对象计划到目标，还需要有以下权限：</p> <ul style="list-style-type: none">• 要计划的对象的“计划文档运行”权限。• 收件人收件箱的“将对象添加到文件夹”权限（如果要计划到收件箱目标）。• 要计划的对象的“将对象复制到另一文件夹”权限（如果要将副本而不是快捷方式发送到收件箱目标）。
查看文档实例	<p>允许查看对象实例。此权限是在对象实例上执行的所有任务都需要的基本权限。</p>
删除实例	<p>允许只删除对象实例。如果拥有“删除对象”权限，则不需要此权限就能删除实例。</p>
暂停并继续文档实例	<p>允许暂停或继续正在运行的对象实例。</p>
重新计划实例	<p>允许重新计划对象实例。</p>

相关主题

- 第 137 页上的[“所有者权限”](#)
- 第 136 页上的[“在修改用户拥有的对象权限选项之间进行选择”](#)

29.3 特定对象类型的权限

29.3.1 文件夹权限

要使权限管理变得更轻松，建议设置文件夹权限，以便文件夹的内容继承安全设置。文件夹权限包含以下这些：

- 应用于文件夹对象的常规权限。
- 特定于类型的权限，计划用于文件夹的内容（例如 Crystal 报表的“打印报表数据”权限）。

相关主题

- 第 118 页上的[“特定于类型的权限”](#)

29.3.2 类别

本节中的权限是在公共类别和个人类别的上下文具有特定意义的常规权限。

注意：

类别中的对象不继承在类别上设置的权限。

权限	说明
将对象添加到文件夹	允许在类别中创建新的类别。不需要此权限就能将对象添加到类别。
编辑对象	<p>允许执行以下操作：</p> <ul style="list-style-type: none">• 修改类别属性。• 将类别作为子类别移入另一个类别中。• 将对象添加到类别。• 从类别中删除对象。 <p>要将类别作为子类别移入另一个类别中，还需要有以下权限：</p> <ul style="list-style-type: none">• 原始类别的“删除对象”权限。• 目标类别的“将对象添加到文件夹”权限。
删除对象	允许删除类别。

29.3.3 Desktop Intelligence 文档

本节中的权限仅适用于 Desktop Intelligence 文档。

权限	说明
使用值列表	允许用户使用值列表。
下载对象相关文件	允许用户下载与对象相关联的文件。
导出报表数据	允许用户以 Excel、PDF 和 CSV 格式导出文档。如果没有此权限，则需要有“另存为 CSV”、“另存为 Excel”或“另存为 PDF”权限；这些权限允许仅以指定的格式导出文档。
查看 SQL	允许用户查看为查询生成的 SQL。
刷新报表数据	允许用户刷新文档数据。
刷新值列表	允许用户在创建提示或查看文档时刷新提示的值列表。要这样做，还需要有文档的“使用值列表”权限。

PDF、XLS、RTF 以及文本的特定文档权限：

权限	说明
将对象添加到文件夹	允许用户向文件夹中添加对象。该权限还适用于类似文件夹的对象，如：收件箱、收藏夹或对象包。
将对象复制到另一文件夹	允许用户在 CMS 中的其他文件夹中创建对象副本。为此，还需要具有针对目标文件夹的“将对象添加到文件夹”权限。
删除实例	仅允许用户删除对象实例。如果拥有“删除对象”权限，则不需要此权限即可删除实例。
删除对象	允许用户删除该类别。
编辑对象	允许用户修改类别属性、将类别作为子类别移至另一类别内、向类别内添加对象、从类别内移除对象。
修改用户拥有的对象权限	允许用户为该对象上的任意用户修改任意权限。

权限	说明
暂停并继续文档实例	允许用户暂停或继续正在运行的对象实例。
复制内容	允许用户将对象复制到联合部署中的其他系统。
重新计划实例	允许用户重新计划对象实例。
安全地修改用户拥有的对象权限	仅针对用户被授予的权限，允许用户执行授予、拒绝或还原至未指定状态的操作。
查看文档实例	允许用户查看对象实例。此权限是在对象实例上执行的所有任务都需要的基本权限。
查看对象	允许用户查看类别及其包含的子类别。

29.3.4 注释

注释允许用户使用讨论区应用程序评论其他对象。注释在讨论线索中链接在一起；这些讨论线索被视为它们所讨论的对象的子对象。可以在对象级别或文件夹级别设置权限，以控制讨论线索的使用。

本节中的权限仅适用于注释。

权限	说明
允许讨论线索	此权限允许执行以下操作： <ul style="list-style-type: none">• 开始和答复讨论线索。• 查看有关讨论线索的注释。• 修改或删除张贴的注释。

29.3.5 Crystal 报表

本节中的权限仅适用于 Crystal 报表。

注意：

仅当 Crystal 报表位于 BI 平台环境中时，这些权限才适用。在将 Crystal 报表下载到本地磁盘时，这些权限无效。要防止出现此问题，可以拒绝 Crystal 报表的“下载与对象关联的文件”权限。

权限	说明
打印报表数据	允许打印报表。
刷新报表数据	允许刷新报表数据。
导出报表数据	当在 Crystal Reports 查看器中联机查看报表时，允许将报表数据导出为任何格式。 要导出 RPT 格式的报表数据，还需要有“下载与对象关联的文件”权限。
下载与对象关联的文件	此权限允许执行以下操作： <ul style="list-style-type: none">• 导出 RPT 格式的报表。• 在 Crystal Reports 设计器中打开报表。• 将 RPT 格式的报表计划到外部目标。

29.3.6 Web Intelligence 文档

本节中的权限仅适用于 Web Intelligence 文档。

权限	说明
使用值列表	允许使用值列表。
导出报表数据	允许将文档数据导出为 Excel、PDF 和 CSV 格式。如果没有此权限，则需要有“另存为 CSV”、“另存为 Excel”或“另存为 PDF”权限；这些权限允许仅以指定的格式导出文档。
查询脚本 — 启用查看（SQL、MDX）	允许查看查询脚本（SQL 和 MDX）。
刷新报表数据	允许刷新文档数据。
编辑查询	允许编辑文档中的查询。
刷新值列表	创建提示或查看文档时，允许刷新用于提示的值列表。要这样做，还需要有文档的“使用值列表”权限。
另存为 CSV	允许仅将文档导出为 CSV 文件。如果已经有文档的“导出报表数据”权限，则不需要此权限。
另存为 Excel	允许仅将文档导出为 Excel 文件。如果已经有文档的“导出报表数据”权限，则不需要此权限。
另存为 PDF	允许仅将文档导出为 PDF 文件。如果已经有文档的“导出报表数据”权限，则不需要此权限。
发送至	允许将文档发送给计划程序、BI 平台收件箱，或作为电子邮件中的超级链接发送。此权限还允许 Web Intelligence 胖客户端用户以电子邮件附件形式发送文档。

29.3.7 用户和组

在 BI 平台环境中，可以像为其他对象设置权限一样为用户和组设置权限。本节中的权限是特定于类型的权限（仅适用于用户和组对象），或者是在用户和组的上下文中具有特定意义的常规权限。

注意：

- 用户和子组可以通过组成员资格继承权限。

- 用户帐户的创建者被视为帐户的所有者。但是，在创建用户帐户后，此帐户的预定用户也被视为所有者。

权限	说明
编辑对象	<p>允许执行以下操作：</p> <ul style="list-style-type: none"> • 编辑用户或组的属性。 • 管理组成员资格。 <p>要向另一个组添加用户或组，需要有该用户或组以及目标组的此权限。</p>
更改用户密码	<p>允许执行以下操作：</p> <ul style="list-style-type: none"> • 更改用户帐户的密码。要这样做，还需要具有对用户帐户的“编辑对象”权限。 • 更改另一个用户帐户的密码。要这样做，还需要具有对用户帐户的“编辑对象”权限和“修改用户拥有的对象权限”权限。 <p>注意：</p> <ul style="list-style-type: none"> • 此权限不会影响以下用户密码设置： <ul style="list-style-type: none"> • 密码从不过期 • 用户必须在下一次登录时更改密码 • 用户不能更改密码 • 此权限不适用于 BusinessObjects Universe 的数据源凭据。
预订发布	<p>允许将用户作为收件人添加到发布。</p>
代表其他用户进行计划	<p>允许代表用户计划对象，以便用户成为对象实例的所有者。要这样做，还需要有对象的“代表其他用户进行计划”权限。</p>
添加或编辑用户属性	<p>允许更改用户电子邮件地址或自定义用户属性。</p> <p>该权限适用于用户。</p>
添加或编辑用户属性（所有者权限）	<p>允许用户对象所有者更改用户电子邮件地址或自定义用户属性的值。</p> <p>该权限适用于用户。</p>

29.3.8 访问级别

本节中的权限仅适用于访问级别。

权限	说明
将访问级别用于安全性分配	允许在将主体添加到对象的访问控制列表时分配访问级别。为此，还需要具有对主体和对象的“修改用户拥有的对象权限”权限或“安全地修改用户拥有的对象权限”权限。如果授予了“安全地修改用户拥有的对象权限”权限，则还必须授予自己相同的对象访问级别。

相关主题

- 第 136 页上的[“在修改用户拥有的对象权限选项之间进行选择”](#)

29.3.9 Universe (.unv) 权限

本节中的权限适用于使用 Universe 设计工具创建的 Universe 或 .unv Universe。本节中所列出的权限是特定于类型的权限（仅适用于 Universe），或者是在 Universe 的上下文具有特定意义的常规权限。

注意：

仅当在 Universe 设计工具应用程序中从 CMS 导入 Universe 时，Universe 权限才适用。在将 Universe 保存到本地磁盘时，这些权限不适用。

权限	说明
将对象添加到文件夹	允许向 Universe 添加限制集或对象。要这样做，还需要有“编辑访问限制”权限。
查看对象	允许访问和查看 Universe。
编辑对象	此权限允许执行以下操作： <ul style="list-style-type: none">在 CMC 或 Universe 设计工具中编辑 Universe。锁定或取消锁定 Universe。 要取消锁定 Universe，还需要有“取消锁定 Universe”权限。
删除对象	允许删除 Universe。
翻译对象	允许使用翻译管理工具保存已翻译的 Universe 对象名称。 注意： 如果已被授予明确的编辑对象权限，且翻译对象的权限未被明确拒绝，则可以保存翻译。
新建值列表	此权限允许执行以下操作： <ul style="list-style-type: none">将新的值列表与对象关联。编辑现有的值列表。 注意： 此权限不会阻止创建级联值列表。
打印 Universe	允许打印 Universe。
显示表或对象值	允许查看与 Universe 中的表或对象关联的值。
编辑访问限制	允许为 Universe 编辑访问限制（Universe 限制）。

权限	说明
取消锁定 Universe	<p>允许执行以下操作：</p> <ul style="list-style-type: none"> 如果 Universe 被另一个用户锁定，则取消锁定 Universe。 从 CMS 导出 Universe。 <p>要取消锁定 Universe，还需要有“编辑对象”权限。</p>
数据访问	<p>允许从 Universe 检索数据和刷新基于 Universe 的文档。要这样做，还需要具有 Universe 设计工具应用程序、文档和 Universe 连接的此权限。</p>
创建和编辑基于 Universe 的查询	<p>允许创建基于 Universe 的文档和编辑基于 Universe 的查询。</p>

29.3.10 Universe (.unx) 权限

本节中的权限适用于使用信息设计工具创建的 Universe 或 .unx Universe。本节中所列出的权限是特定于类型的权限（仅适用于 Universe），或者是在 Universe 的上下文中具有特定意义的常规权限。

注意：

Universe 权限仅适用于已发布至资源库的 Universe。在将 Universe 保存至本地文件夹时，这些权限不适用。

权限	说明
查看对象	<p>允许访问和查看 Universe。</p>
编辑对象	<p>允许重新发布 Universe。</p>
删除对象	<p>允许删除 Universe。</p>
检索 Universe	<p>允许获取已发布的 Universe 并在信息设计工具中编辑基础资源（业务层和数据基础）。</p> <p>注意： 还必须被授予信息设计工具应用程序权限“检索 Universe”。</p>

权限	说明
编辑安全配置文件	<p>允许在信息设计工具安全编辑器中为 Universe 插入、编辑和删除安全配置文件。</p> <p>注意： 查看安全配置文件或更改安全配置文件聚合选项不需要此权限。</p>
分配安全配置文件	允许在信息设计工具安全编辑器中为用户和组分配和取消分配安全配置文件。
数据访问	<p>允许从 Universe 检索数据和刷新基于 Universe 的文档。</p> <p>在信息设计工具中，此权限允许在查询面板中预览结果集。</p>
创建和编辑基于此 Universe 的查询	<p>允许创建和编辑基于 Universe 的查询。</p> <p>在信息设计工具中，此权限允许在 Universe 上打开查询面板并运行查询。</p>
为所有用户保存	<p>允许为所有用户保存 Universe。</p> <p>注意： 还必须被授予了信息设计工具应用程序权限“为所有用户保存”。</p>

29.3.11 Universe 对象访问级别

设计者使用 Universe 设计工具创建 Universe 或者使用信息设计工具创建业务层时，会为 Universe 中的每个对象分配一个对象访问级别。对象访问级别包括：

- 公共（默认）
- 受控制
- 受限
- 保密
- 专用

Universe 在资源库中发布之后，则可以根据在应用程序中分配的对象访问级别授予对 Universe 对象的访问权限。例如，可以对 Everyone 用户组授予“公共”访问权限。这样，Everyone 组的用户就可以查看 Universe 中被指定为“公共”的对象。

每个对象访问级别均授予比上一个级别更多的对象访问权限。“公共”是最低的级别。被授予“公共”访问权限的主体只能查看指定为“公共”的对象。被授予“受控制”访问权限的主体可以查看指定

为“公共”和“受控制”的对象。“专用”是最高级别的设置，它向主体授予对所有对象访问级别（即 Universe 中所有对象）的访问权限。

注意：

- 对象访问级别安全设置会覆盖 Universe 继承的任何安全设置。
- 对于 .unx Universe，对象访问级别安全设置会考虑安全配置文件中定义的对象安全性。有关安全配置文件的更多信息，请参阅《信息设计工具用户指南》。

相关主题

- 第 891 页上的“[分配 Universe 对象访问级别](#)”

29.3.11.1 分配 Universe 对象访问级别

要设置 Universe 对象访问级别安全性，需要有 Universe 的“修改用户拥有的对象权限”权限。

- 1 在 CMS 的“Universe”区域中，选择一个 Universe。
- 2 单击“操作” > “Universe 安全性”。
- 3 在“Universe 安全性”对话框中，为用户或组选择“对象级别安全性”列表中的对象访问级别。

29.3.12 连接权限

本节中的权限是特定于类型的权限（适用于 Universe 连接），或者是在 Universe 连接的上下文具有特定意义的常规权限。这些权限适用于在资源库中发布的连接。

关系连接权限

权限	说明
查看对象	允许查看连接。
编辑对象	允许编辑连接参数。
本地下载连接	<p>允许脱机模式下在 Web Intelligence 胖客户端中使用连接上创建的 Universe。</p> <p>允许在信息设计工具中使用本地的中间件驱动程序。为此，请在信息设计工具首选项中选择本地中间件选项，否则对数据库的查询将使用服务器中间件。</p> <p>在信息设计工具中编辑安全连接也需要此权限。</p>
删除对象	允许删除连接。

权限	说明
将对象复制到另一文件夹	允许将连接从一个文件夹复制到另一个文件夹。
数据访问	允许从连接中指定的数据库中检索内容。 在信息设计工具中，该权限允许用户从连接和数据基础编辑器中浏览表数据。用户还可以在查询面板中预览结果集。
使用存储过程的连接	允许使用为 Universe 连接指定的数据库中的存储过程。 注意： 此权限仅适用于 .unv Universe。

OLAP 连接权限

权限	说明
查看对象	允许查看连接。
编辑对象	允许用户在信息设计工具连接编辑器中编辑连接参数。
删除对象	允许删除连接。
将对象复制到另一文件夹	允许将连接从一个文件夹复制到另一个文件夹。

29. 3. 13 应用程序

29. 3. 13. 1 CMC

本节中的权限仅适用于 CMC。

权限	说明
登录到 CMC 并在 CMC 中查看此对象	允许登录到 CMC。
允许访问实例管理器	允许访问实例管理器。
允许访问关系查询	允许在 CMC 中运行关系查询。
允许访问安全性查询	允许在 CMC 中运行安全性查询。

29.3.13.2 BI 启动板

本节中的权限仅适用于 BI 启动板。

权限	说明
组织	允许执行以下操作： <ul style="list-style-type: none">• 移动和复制对象。• 将对象添加到收藏夹文件夹。• 创建对象的快捷方式。
发送到 Business Objects 收件箱	将对象发送到 BI 收件箱收件人。
发送到电子邮件目标	将对象发送到 BI 收件箱收件人。
发送到文件位置	将对象保存到文件位置。
发送到 FTP 位置	将对象保存到 FTP 位置。

29.3.13.2.1 协作应用程序权限

在 BI 平台中配置应用程序之后，本节中的权限将适用于 SAP Jam 或 SAP StreamWork。

权限	说明
对文档进行注释	允许对文档和实例进行注释
对用户自有文档进行注释	允许对自有文档和实例进行注释
查看用户自有文档的注释	允许查看自有文档和实例的注释
查看对文档的注释	允许查看文档和实例的注释

29.3.13.3 BI 工作区

本节中的权限仅适用于 BI 工作区。

权限	说明
创建和编辑 BI 工作区	允许用户创建新的 BI 工作区和编辑现有 BI 工作区。
创建和编辑模块	允许用户创建新的模块和编辑现有模块。
编辑 BI 工作区	允许用户编辑现有 BI 工作区。用户不能创建新的 BI 工作区。

29.3.13.4 Desktop Intelligence

本节中的权限适用于 SAP BusinessObjects Desktop Intelligence。

权限	说明
创建和编辑连接	允许用户新建连接或编辑现有连接。
数据提供者操作	允许用户修改查询或更改其所基于的 Universe。
编辑自由编写 SQL	允许用户编辑使用自由编写 SQL 脚本作为数据提供者的查询。执行该操作还须具备“使用自由编写 SQL”权限。
使用自由编写 SQL	允许用户创建使用自由编写 SQL 脚本作为数据提供者的查询。
刷新文档列表和类别	允许用户在启用该权限后刷新文档列表。
将文档发送到资源库	允许用户在 CMS 的公共文件夹或其个人文件夹中发布文档。
将文档发送到邮件	允许用户通过 Desktop Intelligence 以电子邮件形式发送文档。
检索文档	允许用户从 CMS 导入文档。
运行 VBA 代码	允许用户运行 VBA 代码。
安装加载项	允许用户安装或卸载 VBA 加载项。
管理所有公司类别	允许用户创建、编辑或删除类别中的任何文档。
管理我的公司类别	允许用户创建、编辑或删除 Desktop Intelligence 应用程序内的任何公司类别。
编辑分析范围	允许用户编辑“分析范围”
以钻取模式工作	允许用户向下钻取至报表中更加细化的分析层面。
以切片和切块模式工作	允许用户使用切片和切块面板。

权限	说明
编辑 VBA 代码	允许用户编辑报表中使用的 VBA 宏。
欧元转换器	允许用户将报表中的货币数额转换为欧元，或将欧元转换为其他货币数额。
复制到剪切板	允许用户剪切或复制文档内容。
贯穿钻取	允许用户通过检索新数据进一步钻取报表。
编辑欧元转换器汇率	允许用户修改欧元转换器函数所使用的欧元汇率。
Desktop Intelligence 报表交互	允许用户选择报表中的单个元素进行剪切、复制、清除或删除操作。
Desktop Intelligence 文档交互	允许用户在文档中重命名、复制、插入或删除报表。
打印文档	允许用户打印文档。
Refresh Desktop Intelligence content (刷新 Desktop Intelligence 内容)	允许用户刷新 Desktop Intelligence 内容。
使用模板	允许用户使用模板创建报表或将模板应用于现有内容。
创建模板	允许用户将文档另存为模板。
为所有用户保存文档	允许用户在没有离线使用安全限制的情况下保存文档，以便使所有用户都能够查看该本地保存的文档。
创建 Desktop Intelligence 文档	允许用户新建文档。
保存 Desktop Intelligence 文档	允许用户本地保存文档。
将文档发送到收件箱	允许用户向 BI 启动板收件箱发送文档。
使用用户对象	允许用户创建、编辑或删除用户对象。

权限	说明
刷新值列表	允许用户在获得此权限授权后刷新值列表。
使用值列表	允许用户使用和刷新文档中的值列表。
编辑值列表	允许用户编辑 Universe 中定义的值列表。
使用查询	允许用户新建基于 Universe 的查询。
编辑查询	允许用户编辑基于 Universe 的查询。
查看 SQL	允许用户查看为查询生成的 SQL。
编辑查询 SQL	允许用户修改查询的 SQL。
总是重新生成 SQL	允许在每次刷新时重新生成查询。
使用存储过程	允许用户使用存储过程作为数据提供者创建报表。
编辑存储过程	允许用户编辑存储过程参数。
使用个人数据文件	允许用户使用 Excel、dBase 或 ASCII 文本文件作为数据提供者创建报表。
编辑个人数据文件	允许用户编辑个人数据提供者。
安全地修改用户拥有的对象权限	仅允许用户针对被授予的权利执行授权、拒绝或还原至未指定状态等操作。

权限	说明
修改用户具有的对此对象的权限	允许用户为该对象上的任意用户修改任意权限。
编辑此对象	允许用户在 CMC 中修改应用程序的属性。
登录到 Desktop Intelligence 并在 CMC 中查看此对象	允许用户登录 Desktop Intelligence，并在 CMC 中查看对象。

29.3.13.5 Web Intelligence

本节中的权限仅适用于 SAP BusinessObjects Web Intelligence（包括胖客户端界面），并且可影响这些应用程序中的查看器和查询面板。

权限	说明
数据 — 启用数据跟踪	允许跟踪已更改的数据。
数据 — 启用已更改数据的格式设置	允许选择已更改数据的格式。
胖客户端界面 — 启用 Web Intelligence 胖客户端	允许使用胖客户端界面。
胖客户端界面 — 启用本地数据提供者	允许在胖客户端界面中使用个人数据提供者。
胖客户端界面 — 导出文档	允许在胖客户端界面中将文档导出至 CMS。
胖客户端界面 — 导入文档	允许在胖客户端界面中导入 CMS 内的文档。
胖客户端界面 — 从 BI 启动版安装	允许从 BI 启动板下载胖客户端界面。
胖客户端界面 — 打印文档	允许从胖客户端界面打印文档。
胖客户端界面 — 删除文档安全性	允许从胖客户端界面删除文档安全性。

权限	说明
胖客户端界面 — 为所有用户保存文档	允许从胖客户端界面为所有用户保存文档。
胖客户端界面 — 在本地保存文档	允许在胖客户端界面中将文档保存至本地磁盘。
胖客户端界面 — 通过邮件发送	允许在胖客户端界面中通过电子邮件发送文档。
胖客户端界面 — 启用本地数据提供者	允许在胖客户端界面中使用个人数据提供者。
文档 — 禁用打开时自动刷新	禁止在打开时自动刷新文档。
文档 — 启用自动保存	允许自动保存文档（如果管理员已在 CMC 中激活了自动保存）。
文档 — 启用创建	允许创建新文档。
文档 — 启用发布和内容管理	允许在 CMS 中发布文档。
交互式：报表创建 — 创建并编辑报警器	允许在交互式查看器中创建并编辑报警器。
界面 — 启用富 Internet 应用程序	允许使用富 Internet 应用程序查看和编辑界面（之前版本中的 Java 报表面板）。
界面 — 启用 Web 查看界面	允许使用 Web 查看界面（之前版本中的 DHTML 查看器）。
界面 — 启用 Web 查询面板	允许使用 Web 查询面板（查询 — 之前版本中的 HTML）。
常规 — 编辑“我的首选项”	允许在 BI 启动板中编辑首选项。
常规 — 启用右击菜单	允许使用右击菜单。
左窗格 — 启用文档摘要	允许在左窗格中显示文档摘要。
左窗格 — 启用文档结构和过滤器	允许在左窗格中显示文档结构和过滤器。
查询脚本 — 启用编辑（SQL、MDX）	允许编辑查询脚本（SQL 和 MDX）。
查询脚本 — 启用查看（SQL、MDX）	允许查看查询脚本（SQL 和 MDX）。

权限	说明
报表创建 — 创建和编辑拆分	允许创建和编辑拆分。
报表创建 — 创建和编辑条件格式设置规则	允许创建和编辑条件格式规则。
报表创建 — 创建和编辑预定义的计算	允许创建和编辑预定义计算。
报表创建 — 创建并编辑输入控件	允许创建和编辑输入控件。
报表创建 — 创建和编辑报表过滤器并使用输入控件	允许创建和编辑报表过滤器和输入控件。（禁用后不会在左窗格中显示“输入控件”窗格。）
报表创建 — 创建和编辑排序	允许创建和编辑排序。
报表创建 — 创建公式和变量	允许创建公式和变量。
报表创建 — 启用格式设置	允许编辑报表格式设置。如果此权限被拒绝，则用户无法使用设计和数据模式（已取消激活）。
报表创建 — 启用合并维	允许在报表和数据管理器中使用合并维同步数据。
报表创建 — 插入和删除报表、表、统计图和单元格	允许插入和删除报表、表、统计图和单元格。还可以规范和复制工作流（复制/粘贴）。

29.3.13.6 战略生成器

战略生成器是一个与仪表盘和分析应用程序相关的工具。本节中的权限仅适用于战略生成器，并且可能会影响 Performance Manager 中的目标管理或战略生成器中的特定功能。

权限	说明
创建、修改或删除目标	允许在 Performance Manager 中添加、编辑或删除目标。
查看目标	允许在包含目标的分析中查看目标。
对目标管理的访问权	允许在 Performance Manager 中的“目标管理”页上查看目标。
发布目标	允许在 Performance Manager 中发布目标。
对战略生成器的访问权	允许访问 Performance Manager 中的战略生成器工具。
创建、修改或删除角色	允许管理在战略生成器中用于将目标或 Metric 发布到特定读者的角色。
创建、修改或删除策略	允许创建战略，它们在战略生成器中链接角色以及发布目标和 Metric。

29.3.13.7 Universe 设计工具权限

本节中的权限适用于 Universe 设计工具应用程序。

权限	说明
检查 Universe 完整性	允许检查 Universe 完整性。
刷新结构窗口	允许刷新结构窗口。
使用表浏览器	允许使用表浏览器来查看数据库数据。
应用 Universe 约束	允许向导入的 Universe 的用户应用预定义的 Universe 约束。
链接 Universe	允许链接两个 Universe 和共享元素。
创建、修改或删除连接	允许创建、修改和删除存储在资源库中或作为个人连接或共享连接存储的 Universe 连接。

29.3.13.8 信息设计工具权限

本节中的权限适用于信息设计工具应用程序。

权限	说明
管理安全配置文件	<p>允许打开安全性编辑器。</p> <p>注意： 要使用安全配置文件，需要具有在 Universe 中授予的权限。</p>
共享项目	允许共享本地项目，并打开“Synchronize Project”（同步项目）视图以将共享项目与本地项目同步。
创建、修改或删除连接	<p>允许执行以下操作：</p> <ul style="list-style-type: none"> 从“已发布的资源”视图创建和删除受保护的连接 在连接编辑器中编辑连接 将连接发布至资源库
发布 Universe	允许将 Universe 发布至资源库。

权限	说明
检索 Universe	允许检索已发布至要编辑的本地项目的 Universe
为所有用户保存	允许在检索 Universe 时使用“为所有用户保存”选项。
计算统计信息	允许选择在其中计算和发布统计信息的表和列。

29.3.13.9 SAP BusinessObjects Business Intelligence 平台微件

本节中的权限仅适用于 SAP BusinessObjects Business Intelligence 平台应用程序的微件。

权限	说明
使用资源管理器	允许用户使用文档列表资源管理器浏览所有已连接的 BI 平台服务器上的内容。
使用警报收件箱	(不赞成使用) 允许使用警报收件箱。
使用搜索	允许用户使用内容搜索同时所有连接的 BI 平台资源库中进行搜索。

29.3.13.10 警报

本节中的权限仅适用于“警报”应用程序。

权限	说明
触发警报	<p>用于触发警报事件。</p> <p>要触发文档的警报，用户需要具备下列权限：</p> <ul style="list-style-type: none">• 对文档的查看和计划权限• 对相应事件的查看和触发权限
预订对象	<p>用于预订警报事件。</p> <p>要预订事件，用户需要具备下列权限：</p> <ul style="list-style-type: none">• 对相应事件的查看权限• 对用户自己帐户的预订权限 <p>要预订文档中的警报，用户需要具备下列权限：</p> <ul style="list-style-type: none">• 对文档的查看权限• 对文档的查看实例权限• 对相应事件的查看权限• 对用户自己帐户的预订权限

29. 3. 13. 11 Explorer

此节中的权限仅适用于 Explorer。

权限	说明
登录到 Explorer 并在 CMC 中查看此对象	允许您登录到 Explorer。必须具有此权限才能使用 Explorer 执行其他任务。
发掘信息空间	<p>允许发掘信息空间。</p> <p>若要执行此任务，还必须具有“登录到 Explorer 并在 CMC 中查看此对象”权限。</p>
发掘信息空间：导出为书签/电子邮件	<p>允许创建书签以及通过电子邮件发送书签。</p> <p>要执行此任务，还必须具有以下权限：</p> <ul style="list-style-type: none"> • 登录到 Explorer 并在 CMC 中查看此对象 • 发掘信息空间
发掘信息空间：导出为 CSV	<p>允许您将发掘的结果导出到 CSV 或 Excel 文件中。</p> <p>要执行此任务，还必须具有以下权限：</p> <ul style="list-style-type: none"> • 登录到 Explorer 并在 CMC 中查看此对象 • 发掘信息空间
发掘信息空间：导出为图像	<p>允许将发掘的结果导出成一个图像。</p> <p>要执行此任务，还必须具有以下权限：</p> <ul style="list-style-type: none"> • 登录到 Explorer 并在 CMC 中查看此对象 • 发掘信息空间
发掘信息空间：导出为 Web Intelligence	<p>允许将发掘的结果导出成一个查询。</p> <p>要执行此任务，还必须具有以下权限：</p> <ul style="list-style-type: none"> • 登录到 Explorer 并在 CMC 中查看此对象 • 发掘信息空间
管理信息空间	<p>允许访问“管理空间”菜单并执行相关任务。</p> <p>若要执行此任务，还必须具有“登录到 Explorer 并在 CMC 中查看此对象”权限。</p>
管理信息空间：创建新空间	<p>允许创建新信息空间。</p> <p>要执行此任务，还必须具有以下权限：</p> <ul style="list-style-type: none"> • 登录到 Explorer 并在 CMC 中查看此对象 • 管理信息空间

权限	说明
管理信息空间：修改空间	<p>允许修改或删除信息空间。</p> <p>要执行此任务，还必须具有以下权限：</p> <ul style="list-style-type: none">• 登录到 Explorer 并在 CMC 中查看此对象• 管理信息空间
管理信息空间：计划索引	<p>允许对信息空间数据的索引进行计划。</p> <p>要执行此任务，还必须具有以下权限：</p> <ul style="list-style-type: none">• 登录到 Explorer 并在 CMC 中查看此对象• 管理信息空间
管理信息空间：启动索引	<p>允许运行信息空间数据的索引。</p> <p>要执行此任务，还必须具有以下权限：</p> <ul style="list-style-type: none">• 登录到 Explorer 并在 CMC 中查看此对象• 管理信息空间

29. 3. 13. 12 SAP BusinessObjects Mobile

本节中的权限仅适用于 SAP BusinessObjects Mobile 应用程序。

权限	说明
登录 SAP BusinessObjects Mobile 应用程序	授予通过 Mobile 应用程序登录到 BI 平台并查看文档的访问权。
预订文档警报	<p>授予预订文档/重复发生警报的访问权。</p> <p>注意：</p> <ul style="list-style-type: none">• 如果用户先前已被授予了“预订文档警报”权限，但现在却被拒绝，则仍会继续收到预订的警报。若不想接收这些警报，则必须明确取消警报的预订。• 要为计划预订文档警报（或重复性实例），用户必须具有中央管理控制台（CMC）中“事件”下的“系统事件”文件夹的“完全控制”安全访问权。
将文档保存到本地存储设备	<p>授予将文档保存在 Mobile 设备上的访问权。</p> <p>注意：</p> <p>如果用户在获得“将文档保存到设备的本地存储”权限后将文档保存在设备上，即使用户的保存权限被剥夺，这些保存的文档仍会保留在设备上。但是，在同步过程中不会同步这些文档。</p>
将设备上的文档作为电子邮件发送	授予通过电子邮件发送报表的访问权。

有关更多信息，请参阅 《SAP BusinessObjects Mobile 安装和部署指南》。

第 30 章 服务器属性附录

30.1 关于服务器属性附录

此服务器属性附录列出并说明了可为每个 BI 平台服务器设置的属性。

30.1.1 公共服务器属性

本节中描述的服务器属性适用于所有服务器类型。

表30-1：请求端口属性

属性	说明	默认值
服务器名称	服务器的名称。	默认值是服务器所在的节点名称加上服务器名称。
ID、CUID	服务器的短 ID 和群集唯一 ID。只读。	这些值是自动生成的。
节点	服务器所在节点的名称。	此值是在安装过程中指定的。
说明	服务器的说明	默认值为服务器的名称。
命令行参数	服务器的命令行参数。	默认值取决于服务器类型。

属性	说明	默认值
请求端口	<p>指定服务器从中接收请求的端口。在配有防火墙的环境中，将服务器配置为仅侦听防火墙开放端口上的请求。如果为服务器指定端口，请确保该端口尚未由其他进程占用。</p> <p>注意： 如果选择了“自动分配”，则服务器将绑定到动态分配的端口。这意味着每次重新启动服务器时将其分配一个随机端口号。</p>	默认情况下，“自动分配”设置为“真”，并且“请求端口”为空。
自动分配	指定当重新启动服务器时服务器是否绑定到一个动态分配的端口。要将服务器绑定到特定端口，请将“自动分配”设置为“假”，并指定有效的“请求端口”。	默认值为“真”。

表30-2：自动启动属性

属性	说明	默认值
在服务器智能代理启动时自动启动此服务器	<p>指定在服务器智能代理（SIA）启动或重新启动时是否自动启动服务器。</p> <p>如果此值设置为“假”并且 SIA 启动或重新启动，则服务器将保持停止状态。</p>	默认值为“真”。

表30-3：主机标识符属性

属性	说明	默认值
自动分配	指定服务器是否绑定到一个自动分配的网络接口。如果设置为“假”，服务器将绑定到特定网络接口。如果设置为“真”，服务器将接受第一个可用 IP 地址上的请求。在多宿主计算机上，通过将此值设置为“假”并提供有效主机名或 IP 地址，可以指定要绑定到的特定网络接口。	默认值为“真”。
主机名	服务器绑定到的网络接口的主机名。如果指定了主机名，服务器将接受与该主机名相关联的所有 IP 地址上的请求。	默认情况下，“自动分配”设置为“真”，并且“主机名”为空。

属性	说明	默认值
IP 地址	服务器绑定到的网络接口的 IP 地址。IPv4 和 IPv6 协议均受支持。如果指定了 IP 地址，服务器将只接受该 IP 地址上的请求。	默认情况下，“自动分配”设置为“真”，并且“IP 地址”为空。

表30-4：配置模板属性

属性	说明	默认值
使用配置模板	指定是否使用配置模板。	默认值为“假”。
还原系统默认值	指定是否为此服务器还原原始默认设置。	默认值为“假”。
设置配置模板	指定是否使用当前服务的设置作为所有同一类型的服务的配置模板。如果设置为“真”，则会立即重新配置已指定为“使用配置模板”的所有同一类型的服务，以使用当前服务的设置。	默认值为“假”。

表30-5：跟踪日志服务属性

属性	说明	默认值
日志级别	<p>指定想要记录的消息的最低严重等级，并确定要在服务器日志文件中记录多少信息。</p> <p>可能的日志阈值级别包括：</p> <ul style="list-style-type: none"> • 未指定 • 无 • 低 • 中 • 高 	默认值为“未指定”。

相关主题

- 第 371 页上的[“使用配置模板”](#)
- 第 823 页上的[“跟踪日志级别”](#)

30.1.2 核心服务属性

“核心服务”类别包括以下服务器：

- 自适应作业服务器
- 自适应处理服务器
- 中央管理服务器
- 仪表盘服务器
- 仪表盘分析服务器
- 事件服务器
- 输入文件资源库服务器
- 输出文件资源库服务器
- Web 应用程序容器服务器

自适应作业服务器属性

表30-6：常规属性

属性	说明	默认值
临时目录	指定必要时在其中创建临时文件的目录。如果此目录没有足够的磁盘空间，则可能会遇到性能问题。为获得更好的性能，请确保此目录位于本地磁盘上。 注意： 必须重新启动服务器才能使更改生效。	%DefaultDataDir%

自适应作业服务器可承载许多不同服务。每项服务都具有以下属性

表30-7：服务属性

属性	说明	默认值
最大并发作业数	指定服务器允许的并发独立进程（子进程）的数量。您可以根据自己的报表创建环境自调整最大作业数。 默认设置对于大多数报表创建方案都是可接受的。适合自己的报表创建环境的理想设置取决于硬件配置、数据库软件和报表创建要求。	5
最大子请求数	指定重新启动前子进程要处理的作业数。	100

自适应处理服务器属性

表30-8：常规属性

属性	说明	默认值
服务启动超时（秒）	<p>指定服务器将等待服务启动的时间量（以秒为单位）。</p> <p>如果服务在指定的时间内未能启动，则有以下两个可能的原因：</p> <ul style="list-style-type: none"> 服务失败，举例来说，服务由于无法找到必需的资源（如数据库）或由于遇到端口冲突而失败。 服务在指定的时间内无法启动，举例来说，服务由于系统太慢而无法启动。 <p>要找出原因，请检查服务器日志文件。如果服务在指定的时间内无法启动，请考虑增大此值。</p>	1200

表30-9：客户端审核代理服务属性

属性	说明	默认值
无配置属性		

表30-10：安全标记服务属性

属性	说明	默认值
无配置属性		

表30-11：Insight to Action 服务属性

量度	说明	
每个用户会话的最大活动连接数	给定时间内用户可用的最大 SAP 服务器连接数。当用户打开具有 RRI 功能的报表或仪表盘时，将建立与 SAP 服务器的连接以确定可用 RRI 目标。	20
每个用户会话的最大空闲连接数	保持开放且可重新用于后续 RRI 请求的空闲连接数。增加此设置将分配附加系统资源。	20
连接最长等待时间（秒）	Insight to Action 框架在 SAP 服务器响应超时前的等待时间（秒）。	30

表30-12：发布服务属性

属性	说明	默认值
线程池大小	指定可同时运行的范围批处理线程数量。如果将该属性的值设置为 0，则线程池大小使用基于当前计算机上 CPU 核心数量的公式来确定。	0

表30-13：翻译服务属性

属性	说明	默认值
无配置属性		

表30-14：监控服务属性

属性	说明	默认值
无配置属性		

表30-15：平台搜索服务属性

属性	说明	默认值
无配置属性		

表30-16：发布后处理服务属性

属性	说明	默认值
无配置属性		

中央管理服务器属性

注意：

修改这些服务器属性中的任一属性时，都必须重新启动服务器才能使更改生效。

表30-17：中央管理服务属性

属性	说明	默认值
名称服务器端口	指定 CMS 侦听初始名称服务请求的端口。	6400

属性	说明	默认值
请求的系统数据库连接数	指定 CMS 尝试建立的 CMS 系统数据库连接的数量。如果服务器无法建立请求的所有数据库连接，CMS 将继续工作，但性能会降低，因为此时所能处理的并发请求要少一些。CMS 会尝试建立其他连接，直至建立所请求数量的连接。 CMS 的“已建立的系统数据库连接数”量度显示了已建立的当前连接数。	14
自动重新连接到系统数据库	指定 CMS 在服务中断时是否自动尝试重新建立与 CMS 数据库的连接。如果此值设置为“假”，将能够在继续操作之前检查 CMS 数据库的完整性；必须重新启动 CMS 才能重新建立数据库连接。	TRUE

表30-18：单一登录服务属性

属性	说明	默认值
单一登录有效期（秒）	指定与数据源间的 SSO 连接在过期之前保持有效的时间（秒）。这适用于运行此类报表的 Windows AD 用户：针对到数据源的 Windows AD SSO 进行了配置的报表。	86400

事件服务器属性

表30-19：事件服务属性

属性	说明	默认值
事件轮询时间间隔（秒）	指定服务器轮询触发事件的文件的间隔（秒）。	10 允许值的范围为 1 到 1200 秒。
清除时间间隔（分钟）	指定清除实用程序的运行频率（以分钟为单位）。	20

输入文件资源库服务器属性

表30-20：输入文件存储服务属性

属性	说明	默认值
文件存储目录	指定文件资源库对象的存储目录。 注意： 如果此目录没有足够的磁盘空间，则可能会遇到性能问题。	%DefaultInputFRS Dir/%
临时目录	指定必要时在其中创建临时文件的目录。 注意： 如果此目录没有足够的磁盘空间，则可能会遇到性能问题。为确保更好的性能，建议“临时目录”和“文件存储目录”位于相同的文件系统上。	%DefaultInputFRS Dir/temp%
最长空闲时间（分钟）	指定服务器在关闭不活动的连接之前等待的时间长度。将值设置得过低可能会导致用户的请求过早关闭。将值设置得过高可能会导致系统资源（如处理时间和磁盘空间）的过度消耗。	10
文件访问的最大重试次数	指定服务器尝试访问某个文件的次数。	1

输出文件资源库服务器属性

表30-21：输出文件存储服务属性

属性	说明	默认值
文件存储目录	指定文件资源库对象的存储目录。 注意： 如果此目录没有足够的磁盘空间，则可能会遇到性能问题。	%DefaultOutputFRS Dir/%
临时目录	指定必要时在其中创建临时文件的目录。 注意： 如果此目录没有足够的磁盘空间，则可能会遇到性能问题。	%DefaultOutputFRS Dir/temp%
最长空闲时间（分钟）	指定服务器在关闭不活动的连接之前等待的时间长度。将值设置得过低可能会导致用户的请求过早关闭。将值设置得过高可能会导致系统资源（如处理时间和磁盘空间）的过度消耗。	10

属性	说明	默认值
文件访问的最大重试次数	指定服务器尝试访问某个文件的次数。	1

Web 应用程序容器服务器属性

表30-22：常规属性

属性	说明	默认值
服务启动超时（秒）	<p>超时前 WACS 将等待其承载的服务启动的时间。如果已超时，则 WACS 将不提供尚未启动的服务。在速度较慢的计算机上，可以考虑指定一个较大的值。</p> <p>如果指定的值太小，且 WACS 在超时前未启动，请通过中央配置管理器（CCM）还原 WACS 的默认设置。</p>	1200

表30-23：跟踪日志服务属性

属性	说明	默认值
日志级别	<p>启用日志记录并将严重性和详细级别设置为“无”（仅记录严重事件）、“低”（记录启动、关闭以及开始和结束请求的消息）、“中”（记录错误、警告和大部分状态消息）或“高”（记录全部消息。仅用于调试。可能会增加 CPU 占用，从而影响性能。）</p> <p>可用菜单选择如下：</p> <ul style="list-style-type: none"> • 未指定 • 无 • 低 • 中 • 高 	未指定

表30-24：Business Process BI 服务属性

属性	说明	默认值
无配置属性		

表30-25：查询生成器服务属性

属性	说明	默认值
无配置属性		

表30-26：RESTful Web 服务 — 系统属性配置属性

属性	说明	默认值
显示错误堆栈	若启用，错误日志中会包含 RESTful Web 服务错误消息（出于调试目的）。其他情况下，出于对披露 BI 平台详细信息的安全考虑，不应使用此项。	未选中
一页的默认对象数	每页列出的条目数。开发人员可在 RESTful Web 服务 SDK 中以 &pageSize=<m> 参数覆盖此设置。	50
Enterprise 会话标记超时（分钟）	登录标记保持有效的到期时间。超出此时间后，必须生成一个新的登录标记。	60
会话池大小	这是指要同时存储的缓存会话数，可用于提高服务器性能。会话池可缓存活动的 RESTful Web 服务会话，当用户发送的另一请求使用 HTTP 请求标头中的相同登录标记时，便可以重复利用这些会话。	1000
会话池超时（分钟）	以分钟计的缓存会话到期时间。	2
启用 HTTP 基本身份验证	如果不启用此设置，则 RESTful Web 服务请求必须使用登录标记。如果启用此设置，用户在第一次进行 RESTful Web 服务请求时必须提供其用户名和密码。启用后，会出现“HTTP 基本身份验证作为默认基本身份验证方案”下拉菜单。	未选中
HTTP 基本身份验证作为默认基本身份验证方案	选中“启用 HTTP 基本身份验证”时，可以选择以下四种身份验证类型之一。请注意：除非使用 HTTPS 选项，否则用户名和密码将以明文格式传送。 接受的值包括： <ul style="list-style-type: none"> • secEnterprise • secDAP • SAPR3 • secWinAD 	空白。但是，如果选择“启用 HTTP 基本身份验证”，将默认为“secEnterprise”。

表30-27: RESTful Web 服务 — 跨源资源共享配置属性

属性	说明	默认值
允许源	该设置允许具有支持跨源资源共享浏览器的用户访问必须访问多个域名的 Java 脚本页面。添加每个域名，并用逗号隔开。例如：http://origin1.server.com:8080, http://origin2.server.com:8080。默认情况下，浏览器可以访问所有域名（*）。	*（星号）
最长寿命（分钟）	这是浏览器可缓存 HTTP 请求的最长时间。	1440

表30-28: RESTful Web 服务 — 受信任的身份验证配置属性

属性	说明	默认值
获取方法	<p>该设置是一个菜单，用来在使用 RESTful Web 服务 API /logon/trusted 时，设置获取受信任的身份验证登录标记所用的查询方法。</p> <ul style="list-style-type: none"> “HTTP_HEADER”用于请求标题为 accept=application/xml（或 application/json）的 GET 查询。 “QUERY_STRING”用来向使用 RESTful Web 服务 API 的 URL 查询末尾添加登录名，例如：/logon/trusted/?user=johndoe。 “COOKIE”在从 Web 浏览器 cookie 中获取登录名时使用。域、名、值和路径必须存储在 cookie 中。 	HTTP_HEADER
用户名参数	这是获取登录标记时用来识别受信任用户的标签。	X-SAP-TRUSTED-USER

表30-29: BOE Web 应用程序服务属性

属性类型	说明	默认值
身份验证类型	<p>用于对登录到 BI 启动板的用户进行身份验证的身份验证类型。</p> <p>接受的值包括：</p> <ul style="list-style-type: none"> AD Kerberos AD Kerberos SS0 Enterprise LDAP 	Enterprise

属性类型	说明	默认值
默认 AD 域	使用默认 Active Directory 域，以便用户在登录时无需提供域。例如，如果将默认域设置为 mydomain 且用户使用用户名 user 登录，则 Active Directory 登录权限将尝试对 user@mydomain.com 进行身份验证。	空白
服务主体名称	客户端使用服务主体名称（SPN）唯一标识服务的实例。Kerberos 身份验证服务使用 SPN 对服务进行身份验证。	空白
Keytab 文件	Keytab 文件的完整路径。利用密钥表文件可以对 Kerberos 过滤器进行配置，而不会在 Web 应用程序计算机上公开用户帐户的密码。	空白

表30-30: Web 服务 SDK 和 QaaWS 属性

属性	说明	默认值
启用 Kerberos Active Directory 单一登录	用于指明是否为 Web 服务 SDK 和 QaaWS 启用 Kerberos AD 单一登录。	假
默认 AD 域	使用默认 Active Directory 域，以便用户在登录时无需提供域。	空白
服务主体名称	客户端使用服务主体名称（SPN）唯一标识服务的实例。Kerberos 身份验证服务使用 SPN 对服务进行身份验证。	空白
Keytab 文件	Keytab 文件的完整路径。利用密钥表文件可以对 Kerberos 过滤器进行配置，而不会在 Web 应用程序计算机上公开用户帐户的密码。	空白

表30-31: HTTP 配置属性

属性	说明	默认值
绑定到所有 IP 地址	用于指明是否绑定到所有网络接口。如果服务器有多个 NIC，但想要绑定到特定的网络接口，请取消选中此属性。	真
绑定到主机名或 IP 地址	指定在其上提供 HTTP 服务的网络接口（IP 地址或主机名）。只有取消选中“绑定到所有 IP 地址”，才能指定值。	localhost

属性	说明	默认值
HTTP 端口	在其上提供 HTTP 服务的端口。	6405 允许值的范围为 1 到 65535。
最大 HTTP 标头大小	请求和响应 HTTP 标头的最大允许大小。	32768

表30-32：通过代理的 HTTP 的配置属性

属性	说明	默认值
启用 HTTP 代理	用于指定是否在 WACS 上启用 HTTP 代理连接器。通常会在具有反向代理的部署中检查此项。	假
绑定到所有 IP 地址	用于指明是否将 HTTP 代理端口绑定到所有网络接口。	真
绑定到主机名或 IP 地址	指定在其上提供 HTTP 代理服务的网络接口（IP 地址或主机名）。只有取消选中“绑定到所有 IP 地址”，才能指定值。	localhost
HTTP 端口	在其上提供反向代理部署中的 HTTP 服务的端口。只有选中“启用 HTTP 代理”，才能指定值。	6406 允许值的范围为 1 到 65535。
代理主机名	代理服务器的 IPv4 地址、IPv6 地址、主机名或完全限定的域名。只有选中“启用 HTTP 代理”，才能指定值。	空白
代理端口	正向或反向代理服务器的端口。只有选中“启用 HTTP 代理”，才能指定值。	0 允许值的范围为 1 到 65535。
最大 HTTP 标头大小	请求和响应 HTTP 标头的最大允许大小。	32768

表30-33：HTTPS 配置属性

属性	说明	默认值
启用 HTTPS	用于指明是否启用 HTTPS/SSL 通信。	假
绑定到主机名或 IP 地址	指定在其上提供 HTTPS 服务的网络接口（IP 地址或主机名）。只有选中“启用 HTTPS”，才能指定值。	localhost

属性	说明	默认值
HTTPS 端口	在其上提供 HTTPS 服务的端口。只有选中“启用 HTTPS”，才能指定值。	443 允许值的范围为 1 到 65535。
代理主机名	代理服务器的 IPv4 地址、IPv6 地址、主机名或完全限定的域名。只有选中“启用 HTTPS”，才能指定值。	空白
代理端口	正向或反向代理服务器的端口。只有选中“启用 HTTPS”，才能指定值。	0 允许的值范围为 1 到 65535。
协议	要使用的加密协议。只有选中“启用 HTTPS”，才能指定值。	TLS 允许的值为 TLS 或 SSL。
证书存储类型	包含证书以及私钥的证书存储的类型。在大多数情况下将为 PKCS12。只有选中“启用 HTTPS”，才能指定值。	PKCS12 允许的值为 PKCS12 或 JKS。
证书存储文件位置	证书文件的完整路径。只有选中“启用 HTTPS”，才能指定值。	空白
私钥访问密码	PKCS12 证书存储和 JKS 密钥存储具有受密码保护的私钥，用于防止未经授权的访问或盗窃行为。在此输入生成证书存储时指定的密码，以便 WACS 可以从证书存储访问私钥。只有选中“启用 HTTPS”，才能指定值。	空白
证书别名	证书存储内的证书的别名。如果未指定该属性，并且所使用的证书存储包含多个证书，则使用存储中的第一个证书。在大多数情况下无需指定值。只有选中“启用 HTTPS”，才能指定值。	空白
启用客户端身份验证	如果启用了客户端身份验证，则只有拥有存储在证书信任列表文件中的密钥的客户端才可以获得 WACS 服务。其他客户端均会遭到拒绝。只有选中“启用 HTTPS”，才能启用客户端身份验证。	假
证书信任列表文件位置	证书信任列表文件的完整路径。只有选中“启用 HTTPS”和“启用客户端身份验证”，才能指定值。	空白
证书信任列表私钥访问密码	用于保护对证书信任列表文件中私钥的访问的密码。只有选中“启用 HTTPS”和“启用客户端身份验证”，才能指定值。	空白
最大 HTTP 标头大小	请求和响应 HTTP 标头的最大允许大小。	32768

表30-34：并发属性（每个连接器）

属性	说明	默认值
最大并发请求数	每个连接器（HTTP、HTTP 代理或 HTTPS）可以同时处理的并发 HTTP 或 HTTPS 请求的数量。	150 允许值的范围为 1 到 1000。

表30-35：Active Directory 配置属性

属性	说明	默认值
Krb5.ini 文件位置	krb5.ini 文件的完整路径，该文件存储了 Kerberos 配置属性。	空白
bscLogin.conf 文件位置	bscLogin.conf 文件的完整路径。	空白

30.1.3 连接服务属性

连接服务类别包含以下服务：

- 本机连接服务（承载于独立的服务器上）
- 本机连接服务（32 位，承载于独立的服务器上）
- 自适应连接服务（承载于 APS 中）

所有服务均共享相同配置设置。

表30-36：Excel 数据访问服务属性

属性	说明	默认值
Excel 数据访问清除超时（秒）	指定服务在清除非活动客户端的会话之前要等待多长时间（秒）。	默认值为 1200 秒。
Excel 数据访问交换超时（秒）	指定服务在将非活动客户端的会话交换到硬盘上之前要等待多长时间（秒）。建议指定一个低于“Excel 数据访问清除超时（秒）”属性值的值。	默认值为 600 秒。

表30-37：服务操作属性

属性	说明	默认值
记忆： 更改下列“服务操作”属性后，无需重新启动服务器。		
连接池	启用或禁用连接池。 可能的值为： <ul style="list-style-type: none"> • 已启用 — 带超时设置 • 已启用 — 不带超时设置 • 已禁用 注意： 连接池是维持可重用状态连接的高速缓存功能，用于提高服务器性能。	已启用 — 带超时设置
连接池超时	为池中的连接指定最长空闲时间（以分钟为单位）。 注意： 此属性等同于 cs.cfg 文件的 Max Pool Time 参数。若禁用池，则相当于将 Max Pool Time 设置为 0。若不带超时启用池，则相当于将 Max Pool Time 设置为 -1。有关更多信息，请参阅《数据访问指南》。	60
临时对象不活动超时	指定未使用的临时对象在服务器中的保留时间（以分钟为单位）。在此时间过后，将删除该对象，并收回其资源。	60
临时对象计时器时间间隔	指定两次活动检查之间的时间间隔（以分钟为单位）。在达到固定时间间隔时，服务器将搜索要删除的候选对象。	5
启用 HTTP 分块	启用或禁用 HTTP 分块。 注意： HTTP 分块仅与三层部署相关。它会影响在打开/刷新文档时的性能，因为在提取大文档时，响应越大，来回通信次数就越少。若禁用 HTTP 分块，就相当于将“HTTP 块区大小”设置为 0。	已启用

属性	说明	默认值
HTTP 块区大小	指定由服务器生成的 HTTP 响应大小（以 KB 为单位）。	64

表30-38：低级别跟踪属性

属性	说明	默认值
记忆： 更改下列“低级别跟踪”属性后，无需重新启动服务器。		
启用作业跟踪	启用对“连接服务器”作业的跟踪。 注意： 它需要将“日志级别”属性设置为“高”。	已禁用
启用中间件跟踪	启用对所有中间件的跟踪。要跟踪特定中间件，必须配置 <code>cs.cfg</code> 文件并重新启动服务器。 注意： 它需要将“日志级别”属性设置为“高”。	已禁用

表30-39：活动数据源属性

属性	说明	默认值
警告： 更改下列“活动数据源”属性后，必须重新启动服务器。		

属性	说明	默认值
激活数据源	<p>允许您选择需要连接的数据源。此属性充当驱动程序的过滤器。指定活动数据源以加载要使用的驱动程序。</p> <p>警告： 默认服务器行为是加载所有可用驱动程序。使用此设置可专用化服务器。在网络上部署多个 CORBA 服务器时，此设置特别有用。</p> <p>记忆： 仅加载选定数据源的驱动程序。将忽略所有其他项。如果未选择任何数据源，服务器将加载所有可用驱动程序。</p> <p>注意： 在服务器量度中验证是否已激活选定数据源。网络层和数据库将显示在“连接服务量度”下方。</p>	取消选中
网络层	<p>指定连接使用的网络层。</p> <p>注意： 仅考虑未本地化的名称。在 driver.cfg 文件中可找到可用网络层列表，此文件位于 connectionserver-install-dir\connectionServer 目录下。</p>	<ul style="list-style-type: none"> Native CORBA 服务器的 ODBC 自适应 CORBA 服务器的 JDBC
数据库	<p>指定连接使用的数据库。</p> <p>注意： 仅考虑未本地化的名称。如果数据库为纯 ASCII 字符串，则可能是常规表达式。模式使用 GNU 正则表达式语法。使用 .* 模式可匹配任何字符。例如，MS SQL Server.*\$ 表达式表示使用所有 MS SQL Server 数据库。有关常规表达式的更多信息，请参阅 PERL Web 站点：http://www.perl.com/doc/manual/html/pod/perlre.html#Regular_Expressions。</p>	在输入数据库名称之前，此字段为空。

表30-40：自定义数据访问服务属性

属性	说明	默认值
自定义数据访问清除超时（秒）	指定服务在清除非活动客户端的会话之前要等待多长时间（秒）。	默认值为 1200 秒。

属性	说明	默认值
自定义数据访问交换超时（秒）	指定服务在将非活动客户端的会话交换到硬盘上之前要等待多长时间（秒）。建议指定一个低于“自定义数据访问清除超时（秒）”属性值的值。	默认值为 600 秒。

表30-41：单一登录服务属性

属性	说明	默认值
单一登录有效期（秒）	以秒为单位，指定 SSO 连接在过期之前的有效时间。	默认值为 86400 秒。

表30-42：生命周期管理服务属性

属性	说明	默认值
无配置属性		

表30-43：生命周期管理 ClearCase 服务属性

属性	说明	默认值
无配置属性		

表30-44：差异可视化服务属性

属性	说明	默认值
无配置属性		

相关主题

- 第 909 页上的“[公共服务器属性](#)”

30.1.4 Crystal Reports 服务属性

Crystal Reports 服务类别包含以下服务器：

- Crystal Reports 高速缓存服务器
- Crystal Reports 处理服务器
- Crystal Reports 2013 报表应用程序服务器属性
- Crystal Reports 2013 处理服务器

Crystal Reports 高速缓存服务器属性

同时适用于 Crystal Reports 高速缓存服务器和 Crystal Reports 处理服务器的任何属性均应设置为相同的值。例如，如果在高速缓存服务器上将“查看器刷新总是输出最新数据”设置为“真”，则在处理服务器上应将同一属性设置为“真”。

注意：

修改这些服务器属性中的任一属性时，都必须重新启动服务器才能使更改生效。

表30-45: Crystal Reports 高速缓存服务属性

属性	说明	默认值
查看器刷新总是输出最新数据	指定当用户显式刷新报表时是否忽略所有缓存的页面并从数据库中直接检索新数据。 注意： 可以对报表对象本身设置此属性，并且此属性可能因报表而异；对报表对象指定的值优先于服务器设置。要对报表对象指定值，请在 CMC 中选择报表，并单击“默认设置” > “查看服务器组”。	默认值为“假”。
在客户端之间共享报表数据	指定是否在不同的客户端之间共享报表数据。 注意： 可以对报表对象本身设置此属性，并且此属性可能因报表而异；对报表对象指定的值优先于服务器设置。	默认值为“真”。
空闲连接超时（分钟）	指定 Crystal Reports 高速缓存服务器等待空闲连接返回请求的时间量（分钟）。通常无需修改默认值。	默认值为 20 分钟。
安全高速缓存超时（分钟）	指定服务器在查询 CMS 之前使用缓存的登录凭据、报表参数和数据库连接信息处理请求的时间长短（秒）。	默认值为 20 分钟。

属性	说明	默认值
按需提供给客户端的最旧数据（秒）	<p>指定服务器使用缓存的数据满足来自按需报表的请求的时间量（以秒为单位）。</p> <p>如果服务器收到一个请求，且用为满足以前的请求而生成的数据可以满足这个请求，并且生成这些数据后流逝的时间小于此处设定的值，则服务器将重复使用这些数据满足随后的请求。当多个用户需要相同的信息时，用这种方式重复使用数据能够大幅改善系统性能。</p> <p>在设置此值时，请考虑用户收到最新数据的重要程度。如果收到最新数据对于所有用户非常重要（可能是因为重要数据的更改非常频繁），可能需要通过将此值设为 0 来禁止此类数据的重复使用。</p> <p>注意： 可以对报表对象本身设置此属性，并且此属性可能因报表而异；对报表对象指定的值优先于服务器设置。</p>	默认值为 0 秒。
最大高速缓存大小（KB）	指定用于缓存报表的硬盘空间量（KB）。如果服务器需要处理大量的报表或特别复杂的报表，则可能需要较大的高速缓存大小。	默认值为 256000 KB。
高速缓存文件目录	指定高速缓存文件目录的位置。	%DefaultDataDir%/CrystalReportsCachingServer/temp
Java VM 参数	指定可提供给 JVM 的命令行参数。	默认值为空。
DLL 名称	<p>指定当前加载的文档类型插件的名称。</p> <p>此属性是只读的。</p>	rasprocReport

Crystal Reports 处理服务器属性

同时适用于 Crystal Reports 高速缓存服务器和 Crystal Reports 处理服务器的任何属性均应设置为相同的值。例如，如果在高速缓存服务器上“查看器刷新总是输出最新数据”设置为“真”，则在处理服务器上应将同一属性设置为“真”。

注意：

修改这些服务器属性中的任一属性时，都必须重新启动服务器才能使更改生效。

表30-46: Crystal Reports 处理服务属性

属性	说明	默认值
空闲作业超时（分钟）	指定 Crystal Reports 处理服务器在两次请求给定作业之间等待的时间长度（分钟）。	默认值为 20 分钟。
子进程存在期内的最大作业数	指定每个子进程在每个生命周期内可管理的作业的最大数量。	默认值为 1000。
查看器刷新总是输出最新数据	<p>指定当用户显式刷新报表时是否忽略所有缓存的页面并从数据库中直接检索新数据。指定是否在不同的客户端之间共享报表数据。</p> <p>注意： 可以对报表对象本身设置此属性，并且此属性可能因报表而异；对报表对象指定的值优先于服务器设置。要对报表对象指定值，请在 CMC 中选择报表，并单击“默认设置” > “查看服务器组”。</p>	默认值为“假”。
在客户端之间共享报表数据	<p>指定是否在不同的客户端之间共享报表数据。指定是否在不同的客户端之间共享报表数据。</p> <p>注意： 可以对报表对象本身设置此属性，并且此属性可能因报表而异；对报表对象指定的值优先于服务器设置。</p>	默认值为“真”。
空闲连接超时（分钟）	指定 Crystal Reports 处理服务器等待空闲连接返回请求的时间量（分钟）。通常无需修改默认值。	默认值为 20 分钟。
最大并发作业数（0 代表自动配置）	指定允许在 Crystal Reports 处理服务器上以并发方式运行的独立作业的最大数量。如果将此属性的值设置为0，则服务器将基于运行服务器的计算机的 CPU 和内存应用一个适当的值。	默认值为 0。

属性	说明	默认值
按需提供给客户端的最旧数据（秒）	<p>指定服务器使用缓存的数据满足来自按需报表的请求的时间量（以秒为单位）。</p> <p>如果服务器收到一个请求，且用为满足以前的请求而生成的数据可以满足这个请求，并且生成这些数据后流逝的时间小于此处设定的值，则服务器将重复使用这些数据满足随后的请求。当多个用户需要相同的信息时，用这种方式重复使用数据能够大幅改善系统性能。</p> <p>在设置此值时，请考虑用户收到最新数据的重要程度。如果收到最新数据对于所有用户非常重要（可能是因为重要数据的更改非常频繁），可能需要通过将此值设为 0 来禁止此类数据的重复使用。</p> <p>注意： 可以对报表对象本身设置此属性，并且此属性可能因报表而异；对报表对象指定的值优先于服务器设置。</p>	默认值为 0。
最大预先启动子进程数	指定服务器允许的预先启动子进程的最大数量。如果此值过低，服务器将在进行请求时立即创建子进程，并且用户可能会感觉到延迟。如果此值过高，则空闲子进程可能会不必要地浪费系统资源。	默认值为 1 个子进程。
临时目录	<p>指定必要时在其中创建临时文件的目录。</p> <p>注意： 如果此目录没有足够的磁盘空间，则可能会遇到性能问题。</p>	%DefaultDataDir%/CrystalReportsProcessingServer/temp
Java 类路径	服务器需要的 Java 类的名称和路径。	%CommonJavaLibDir%/procCR.jar
Java 子 VM 参数	指定提供给服务器创建的子进程的命令行参数。	Dbusinessobjects.connectivity.directory=%CONNECTIONSERVER_DIR%, Dcom.businessobjects.mds.cs.ImplementationID=csEX

表30-47：单一登录服务属性

属性	说明	默认值
单一登录有效期（秒）	以秒为单位，指定 SSO 连接在过期之前的有效时间。	默认值为 86400 秒。

Crystal Reports 2013 报表应用程序服务器属性

注意：

修改这些属性中的任一属性时，都必须重新启动服务器才能使更改生效。

表30-48：Crystal Reports 2013 查看和修改服务属性

属性	说明	默认值
允许报表作业保持与数据库的连接，直至关闭报表作业	指定报表作业在进程执行之前是否将保持与数据库的连接。	默认值为“假”。
浏览数据大小（记录数）	指定在浏览特定字段的值时从数据库返回的非重复记录的数量。将首先从客户端的高速缓存中检索数据（如果有），然后再从服务器的高速缓存中检索数据。如果都没有，则将从数据库中检索数据。	默认值为 100 条记录。
空闲连接超时（分钟）	指定报表应用程序服务器（RAS）在超时之前等待来自空闲客户端的请求的时间量（以分钟为单位）。 将此值设得过低会导致用户的请求过早关闭，而将此值设得过高会影响服务器的可伸缩性（例如，如果未明确关闭 ReportClientDocument 对象，则服务器将会无谓地等待空闲作业关闭）。	默认值为 30 分钟。
批大小（记录数）	指定数据库在每次数据传输期间返回结果集中的多少行。 例如，如果请求 500 条记录，并且“批大小”属性设置为 100 条记录，则将分 5 批（每批 100 行）返回数据。要提高 RAS 的性能，必须了解网络环境、数据库和请求类型以便设置适当的批大小。	默认值为 100 条记录。

属性	说明	默认值
在预览或刷新报表时要读取的数据库记录数（-1 代表无限制）	<p>指定在查看或刷新报表时将读取的数据库记录的数量。此设置限制当用户运行查询或报表时服务器从数据库中检索的记录的数量。如果想要防止用户运行会返回过大记录集的按需报表，此设置特别有用。</p> <p>您可能宁愿计划此类报表，以使用户能更快获得这些报表，并减少这些大型查询带给数据库的负载。</p>	默认值为 20000 条记录。
最大并发报表作业数（0 代表无限制）	指定允许以并发方式在 RAS 上运行的独立作业的最大数量。	默认值为 75 个作业。
按需提供给客户端的最旧数据（分钟）	指定按需报表将提供缓存报表数据的时间量（分钟）。	默认值为 20 分钟。
临时目录	<p>指定必要时在其中创建临时文件的目录。</p> <p>注意： 如果此目录没有足够的磁盘空间，则可能会遇到性能问题。</p>	%Default DataDir%/CrystalReportsRasServer/temp

表30-49：单一登录服务属性

属性	说明	默认值
单一登录有效期（秒）	以秒为单位，指定 SSO 连接在过期之前的有效时间。	默认值为 86400 秒。

Crystal Reports 2013 处理服务器属性

注意：

修改这些属性中的任一属性时，都必须重新启动服务器才能使更改生效。

表30-50：Crystal Reports 2013 处理服务属性

属性	说明	默认值
空闲作业超时（分钟）	指定 Crystal Reports 处理服务器在两次请求给定作业之间等待的时间长度（分钟）。	默认值为 20 分钟。
子进程存在期内的最大作业数	指定每个子进程在每个生命周期内可管理的作业的最大数量。	默认值为 1000。

属性	说明	默认值
查看器刷新总是输出最新数据	<p>指定当用户显式刷新报表时是否忽略所有缓存的页面并从数据库中直接检索新数据。指定是否在不同的客户端之间共享报表数据。</p> <p>注意： 可以对报表对象本身设置此属性，并且此属性可能因报表而异；对报表对象指定的值优先于服务器设置。要对报表对象指定值，请在 CMC 中选择报表，并单击“默认设置” > “查看服务器组”。</p>	默认值为“假”。
在客户端之间共享报表数据	<p>指定是否在不同的客户端之间共享报表数据。指定是否在不同的客户端之间共享报表数据。</p> <p>注意： 可以对报表对象本身设置此属性，并且此属性可能因报表而异；对报表对象指定的值优先于服务器设置。</p>	默认值为“真”。
空闲连接超时（分钟）	指定 Crystal Reports 处理服务器等待空闲连接返回请求的时间量（分钟）。通常无需修改默认值。	默认值为 20 分钟。
最大并发作业数（0 代表自动配置）	指定允许在 Crystal Reports 处理服务器上以并发方式运行的独立作业的最大数量。如果将此属性的值设置为 0，则服务器将基于运行服务器的计算机的 CPU 和内存应用一个适当的值。	默认值为 0。
按需提供给客户端的最旧数据（秒）	<p>指定服务器使用缓存的数据满足来自按需报表的请求的时间量（以秒为单位）。</p> <p>如果服务器收到一个请求，且用为满足以前的请求而生成的数据可以满足这个请求，并且生成这些数据后流逝的时间小于此处设定的值，则服务器将重复使用这些数据满足随后的请求。当多个用户需要相同的信息时，用这种方式重复使用数据能够大幅改善系统性能。</p> <p>在设置此值时，请考虑用户收到最新数据的重要程度。如果收到最新数据对于所有用户非常重要（可能是因为重要数据的更改非常频繁），可能需要通过将此值设为 0 来禁止此类数据的重复使用。</p> <p>注意： 可以对报表对象本身设置此属性，并且此属性可能因报表而异；对报表对象指定的值优先于服务器设置。</p>	默认值为 0。

属性	说明	默认值
最大预先启动子进程数	指定服务器允许的预先启动子进程的最大数量。如果此值过低，服务器将在进行请求时立即创建子进程，并且用户可能会感觉到延迟。如果此值过高，则空闲子进程可能会不必要地浪费系统资源。	默认值为 1 个子进程。
临时目录	指定必要时在其中创建临时文件的目录。 注意： 如果此目录没有足够的磁盘空间，则可能会遇到性能问题。	%DefaultDataDir%/CrystalReports2013ProcessingServer/temp
允许报表作业保持与数据库的连接，直至关闭报表作业	指定报表作业在关闭之前是否将保持与数据库的连接。	默认值为“假”。
预览或刷新时读取的数据库记录数（0 代表无限制）	指定在查看或刷新报表时将读取的数据库记录的数量。此设置限制当用户运行查询或报表时服务器从数据库中检索的记录的数量。如果想要防止用户运行会返回过大记录集的按需报表，此设置特别有用。 您可能宁愿计划此类报表，以使用户能更快获得这些报表，并减少这些大型查询带给数据库的负载。	默认值为 20000。

表30-51：单一登录服务属性

属性	说明	默认值
单一登录有效期（秒）	以秒为单位，指定 SSO 连接在过期之前的有效时间。	默认值为 86400 秒。

30.1.5 分析服务属性

分析服务类别包含自适应处理服务器：

表30-52：多维分析服务属性

属性	说明	默认值
最大客户端会话数	<p>指定可在服务器上同时打开的 MDAS 会话的最大数量。</p> <p>如果打开的会话数达到此值，任何其他开始 MDAS 会话的尝试均会导致出现“服务器不可用”错误消息。可以根据自己的需求和可用硬件来更改此值以优化 MDAS 性能，但增大此值可能导致 MDAS 和数据库都出现性能问题。默认值 15 个会话是保守估计值。对于用户查询较小的安装，可以大幅增大此值，而对于用户查询较大的安装，则需要较低的值。</p>	默认值设置为 15。有效范围为 1 到 100。
查询返回的最大单元数	指定单个查询返回给用户的单元数。用户无法执行会返回过多单元（消耗大量内存）的查询。如果用户的查询超出此单元限制，用户将收到一条错误消息。	默认值为 100000 个单元。
过滤时返回的最大成员数	指定按成员过滤时检索的成员数。检索的成员数过大会消耗大量内存。	默认值为 100000 个成员。

表30-53：BEx Web 应用程序服务属性

属性	说明	默认值
最大客户端会话数	服务所允许的最大客户端会话数。	默认值为 15 个会话。
SAP BW 主系统	到 BI 平台中创建的 BW 系统的 OLAP 连接的名称。	默认值为 SAP_BW。
JCo 服务器 RFC 目标	在 BW 系统中输入的 JCo 服务器 RFS 目标的名称。	默认情况下，此值为空。
JCo 服务器网关主机	在 BW 系统中定义的 JCo 服务器网关主机的名称。	默认情况下，此值为空。
JCo 服务器网关服务	在 BW 系统中定义的 JCo 服务器网关服务的名称。	默认情况下，此值为空。
JCo 服务器连接计数	指定可用来为服务处理从 ABAP 到 Java 调用的自动创建的程序数。	默认值为 3 个连接。

30.1.6 数据联合服务属性

数据联合服务类别包含自适应处理服务器：

表30-54：数据联合服务属性

属性	说明	默认值
最大连接数	指定服务器上所允许的最大连接数。	默认值为 32767。
执行线程池大小	指定在某个给定时刻可并行执行的最大查询数。	默认值为 10。
连接不活动状态超时	指定在等待多长时间（秒）后关闭不活动的连接。	默认值为 10800 秒。
语句不活动状态超时	指定在等待多长时间（秒）后关闭不活动的查询语句。	默认值为 600 秒。

30.1.7 Web Intelligence 服务属性

Web Intelligence 服务类别包括以下服务器：

- 自适应处理服务器
- Web Intelligence 处理服务器

自适应处理服务器设置

表30-55：命令行参数

属性	说明	默认值
展开至级别	<p>指定从 BEx 查询中检索数据所至的级别。</p> <p>默认情况下，层次结构不会展开至给定级别。默认级别始终是“00级别”。可以通过将此参数添加到命令行来更改此行为，但如果设置的值过高，Web Intelligence 会检索所有层次结构数据，可能影响系统性能和稳定性。</p>	<p>-Dsap.sl.bics.expandToLevel=n</p> <p>n 可以是 0 至 99 之间的任意整数。如果 n=0，或未指定此参数，则层次结构将不使用“展开至级别”参数。</p>

表30-56: Web Intelligence 监控服务属性

属性	说明	默认值
启用监控	指定是否为服务启用了监控。	真
监控线程循环延迟 (秒)	指定服务每次尝试 Ping 客户端之前要等待的时间 (秒)。	300
默认监控资源的清除 超时(秒)	指定服务在清除非活动客户端的会话之前要等待多长时间(秒)。	1200
默认监控资源的交换 超时(秒)	指定服务在将非活动客户端的会话交换到硬盘上之前要等待多长时间(秒)。建议一个小于“默认监控资源的清除超时”属性值的值。	600
启用服务剖析		TRUE
启用服务活动监控		TRUE

表30-57: 可视化服务属性

属性	说明	默认值
可视化引擎清除超时 (秒)	指定服务在清除非活动客户端的会话之前要等待多长时间(秒)。	1200
可视化引擎交换超时 (秒)	指定服务在将非活动客户端的会话交换到硬盘上之前要等待多长时间(秒)。建议指定一个低于“可视化引擎清除超时(秒)”属性值的值。	600

表30-58: Rebean 服务属性

属性	说明	默认值
无配置属性		

表30-59: 文档恢复服务属性

属性	说明	默认值
无配置属性		

表30-60: DSL 桥服务属性

属性	说明	默认值
DSL 桥引擎清除超时 (秒)	指定服务在清除非活动客户端的会话之前要等待多长时间 (秒)。	1200

Web Intelligence 处理服务器属性

Web Intelligence 处理服务器属性分为以下几组服务:

- 信息引擎
- Web Intelligence 核心
- Web Intelligence 处理
- Web Intelligence 公用

阈值设置如各表中所述。

表30-61: 信息引擎服务属性

属性	说明	默认值
启用值列表高速缓存	指定是否在 Web Intelligence 处理服务器上为值列表启用高速缓存。	真
值列表批大小 (项)	指定每个值列表批的最大项数 (即值的个数)。	1000
最大自定义排序大小 (项数)	指定自定义排序中的最大项数。	100
Universe 高速缓存最大大小 (Universe 数)	指定 Web Intelligence 处理服务器上要高速缓存的 Universe 数。	20
最大值列表大小 (项数)	指定每个值列表的最大项数 (即值的个数)。	50000

表30-62: Web Intelligence 核心服务属性

属性	说明	默认值
回收前的超时 (秒)	以秒为单位, 指定当处理的总文档数超出“回收前的最大文档数”属性指定的值时, 服务器智能代理 (SIA) 停止并重新启动服务器之前的服务器空闲时间。	1200

属性	说明	默认值
空闲文档超时（秒）	以秒为单位，指定切换 Web Intelligence 处理服务器会话之前，等待的时间长度。因此，如果客户端在此段时间内未生成请求，会话将切换到硬盘上，释放出资源供活动会话使用。	300 有效范围为 100 到 10000 秒。
服务器轮询时间间隔（秒）	以秒为单位，指定在服务器轮询新线程请求之前必须经过的时间间隔。当服务器处于轮询阶段中时，它将执行清除操作（比如切换未使用的文档），以使服务器内存低于内存阈值上限。	120
每个用户的最大文档数	指定在任意给定时间，可与用户关联的最大活动会话数（Web Intelligence 文档数）。因此，如果为 5，则用户一次最多可以使用 5 个活动会话。	5 有效范围为 1 到 20。
回收前的最大文档数	指定在考虑回收服务器之前，可以处理的 Web Intelligence 文档数。如果处理的文档达到此数值，且服务器处于空闲状态，则将关闭服务器，服务器智能代理（SIA）将启动一个服务器新实例。但是，在启动服务器新实例之前，会出现时间延迟。这段时间延迟由“回收前的超时”属性定义。	50
允许文档导航图最大大小错误	指定是否限制“最大连接数”属性。如果启用此属性，服务器将识别为“最大连接数”属性设置的值；否则将忽略该属性。	真
空闲连接超时（分钟）	以分钟为单位，指定服务器等待空闲连接返回请求的时间长度。若值设置得过低，可能导致请求过早关闭。若值设置得过高，可能导致请求排队，而服务器在等待空闲请求关闭。	20
最大连接数	指定一次可打开的最大并发会话数。这是一个约数；此设置不计算已切换的非活动会话数，也不计算为分析会话数而创建的会话。如果达到此限值，且没有其他服务器可用于处理请求，用户将收到错误消息。 注意： 必须启用“允许文档导航图最大大小错误”属性，才能使服务器识别此属性。	50 有效范围为 5 到 65535。

属性	说明	默认值
启用内存分析	指定是否启用内存分析。如果启用此属性，则以下属性将处于活动状态，且由服务器识别： <ul style="list-style-type: none"> 内存最大阈值 内存上限 内存下限 <p>当服务器的进程内存超出“内存上限”时，唯一允许进行的操作是保存文档。当进程内存超出“内存最大阈值”时，所有操作都将停止和失败。</p>	真
内存下限（MB）	指定内存占用的下限。	3500
内存上限（MB）	指定内存占用的上限。	4500
内存最大阈值（MB）	指定内存占用的最大阈值。	6000
启用 APS 服务监控	启用自适应处理服务器上承载的 APS 服务对服务器的监控。	真
APS 服务 ping 失败重试计数	指定服务器在认为其无法访问 APS 服务之前要尝试访问 APS 服务的次数。	3
APS 服务监控线程周期	指定两次尝试访问 APS 服务之间的延迟周期。	300
启用当前活动日志	指定是否在服务器日志文件中生成完整的跟踪。 注意： 此属性仅可在排除问题故障时出于调试目的启用。在正常操作期间设置为“FALSE”	假

表30-63: Web Intelligence 处理服务属性

属性	说明	默认值
启用 HTTP URL	指定服务器是否能够访问远程存储的文件。	真
代理值	指定网络代理服务器的地址。仅当网络具有代理服务器且试图访问远程存储的文件时才需要指定一个值。	空白

表30-64: Web Intelligence 公共服务属性

属性	说明	默认值
高速缓存超时（分钟）	以分钟为单位，指定清空文档高速缓存内容之前，等待的时间长度。超时取决于每个文档的最近访问日期。	4370

属性	说明	默认值
文档高速缓存清除时间间隔（分钟）	指定依据“文档高速缓存最大大小”、“文档高速缓存最大缩减空间”和“高速缓存中的最大文档数”设置对文档高速缓存进行扫描和检查的时间间隔（以分钟为单位）。	120
禁用高速缓存共享	指定是否禁用高速缓存共享。高速缓存共享默认是启用的；这意味着所有 Web Intelligence 处理服务器实例将共享同一高速缓存。但如果希望 Web Intelligence 处理服务器的每个实例使用一个高速缓存，则应启用此属性。	假
启用文档高速缓存	指定是否启用文档高速缓存。如果启用此属性，将随计划的 Web Intelligence 文档预加载高速缓存。	真
启用实时高速缓存	指定是否启用实时高速缓存。如果启用了此属性，则可以动态加载高速缓存。因此，在查看 Web Intelligence 文档时，Web Intelligence 处理服务器会高速缓存这些文档。如果在文档中启用了预先高速缓存功能，则文档作为计划作业运行时，服务器还将高速缓存文档。	真
文档高速缓存最大大小（KB）	指定文档高速缓存的最大大小。达到此限值后，将基于“文档高速缓存最大缩减空间”属性来清空文档高速缓存。	1000000
文档高速缓存最大缩减空间（百分比）	指定百分之多少的高速缓存应保持清空状态，以便更新的操作和结果能够存储到高速缓存中。将清除上次访问时间最早的文档。	70
最大字符流大小（MB）	指定发送到 Web Intelligence 客户端的最大字符流大小。 注意： 如果超出“最大字符流大小”属性指定的值，将不创建 Web Intelligence 文档，客户端将收到错误消息。	5 有效范围为 1 到 65535 MB。
二进制流最大大小（MB）	以 MB 为单位，指定发送到 Web Intelligence 客户端的最大二进制流大小。 注意： 如果超出“二进制流最大大小”属性指定的值，将不创建 Web Intelligence 文档，客户端将收到错误消息。	50 有效范围为 1 到 65535 MB。
图像目录	指定图像目录的位置。	空白
输出高速缓存目录	指定高速缓存的位置。	空白

表30-65：常规属性

属性	说明	默认值
单一登录有效期 (秒)	以秒为单位，指定 SSO 连接在过期之前的有效时间。	86400

相关主题

- 第 943 页上的[“Web Intelligence 服务器内存阈值设置 ”](#)

30.1.7.1 Web Intelligence 服务器内存阈值设置

以下各节描述当达到“内存最大阈值”、“内存上限”或“内存下限”时 Web Intelligence 服务器上所发生的情况。

内存最大阈值

如果达到“内存最大阈值”限制，所有当前的操作都将中止。

内存上限

如果达到“内存上限”，则将发生以下服务器操作以释放资源和保护服务器：

- 服务器将阻止新连接和任何其他消耗内存的线程启动。只会允许“保存”Web Intelligence 文档的选项。发出要求分配内存的操作请求的用户将收到“服务器忙”消息，并且会收到应保存任何暂挂更改的通知。
- 服务器将启用系统清理以释放足够的资源，以便使分配的内存量低于“内存上限”属性设置的限制。
- 服务器将尝试删除只读文档。
- 如果在系统清理期间未释放出足够的内存，则服务器将开始关闭处于“查看”模式的文档。服务器将开始基于 LIFO 协议关闭文档；将首先从内存中清除最近的活动文档。服务器将继续关闭文档，直至达到安全级别；此级别是根据以下公式计算得出的：内存上限 — (20%*(内存上限))。例如，如果“内存上限”属性设置为 4500MB，则安全级别将为：

$$4500\text{MB} - .20 \times 4500\text{MB} = 3600\text{MB}$$

- 如果在关闭处于“查看”模式的文档时未释放出足够的内存，则服务器将开始关闭所有仍处于打开状态的文档，包括那些处于“编辑”模式的文档。服务器将开始基于 LIFO 协议关闭文档；将首先从内存中清除最近的活动文档。服务器将继续关闭文档，直至达到安全级别；此级别是根据以下公式计算得出的：内存上限 — (20%*(内存上限))。例如，如果“内存上限”属性设置为 4500MB，则安全级别将为：

$$4500\text{MB} - .20 \times 4500\text{MB} = 3600\text{MB}$$

内存下限

如果达到“内存下限”，服务器会将不活动的文档交换到硬盘上，从而为处于活动状态的文档分配额外的内存。

30.1.8 Dashboard Design 服务属性

仪表盘高速缓存服务器属性

表30-66：仪表盘高速缓存服务属性

属性	说明	默认值
最大高速缓存大小 (KB)	指定用于缓存查询的硬盘空间大小 (KB)。如果服务器需要处理大量查询或非常复杂的查询，则可能需要较大的高速缓存大小。	默认值为 256000 KB。
空闲连接超时 (分钟)	指定仪表盘高速缓存服务器等待空闲连接返回请求的时间 (以分钟为单位)。通常无需修改默认值。	默认值为 15 分钟。
客户端共享数据	指定是否在不同的客户端之间共享报表数据。	默认值为“真”。
按需提供给客户端的最旧数据 (秒)	<p>指定服务器使用缓存的数据满足来自按需查询的请求的时间量 (以秒为单位)。</p> <p>如果服务器收到一个请求，且用为满足以前的请求而生成的数据可以满足这个请求，并且生成这些数据后流逝的时间小于此处设定的值，则服务器将重复使用这些数据满足随后的请求。当多个用户需要相同的信息时，用这种方式重复使用数据能够大幅改善系统性能。</p> <p>在设置此值时，请考虑用户收到最新数据的重要程度。如果收到最新数据对于所有用户非常重要 (可能是因为重要数据的更改非常频繁)，可能需要通过将此值设为 0 来禁止此类数据的重复使用。</p> <p>注意： 可以对报表对象本身设置此属性；对报表对象指定的值优先于服务器设置。</p>	默认值为 0 秒。
安全高速缓存超时 (分钟)	指定服务器在查询 CMS 之前使用缓存的登录凭据、报表参数和数据库连接信息处理请求的时间长短 (分钟)。	默认值为 20 分钟。
Java VM 参数	指定可提供给 JVM 的命令行参数。	Xmx858M

仪表盘处理服务器属性

表30-67：仪表盘处理服务属性

属性	说明	默认值
最大并发作业数	指定允许以并发方式在服务器上运行的独立作业的最大数量。如果将此属性的值设置为0，则服务器将基于运行服务器的计算机的 CPU 和内存应用一个适当的值。	默认值为 0。
子进程存在期内的最大作业数	指定每个子进程在每个生命周期内可管理的作业的最大数量。	默认值为 10000。
最大预先启动子项数	指定服务器允许的预先启动子进程的最大数量。如果此值过低，服务器将在进行请求时立即创建子进程，并且用户可能会感觉到延迟。如果此值过高，则空闲子进程可能会无端浪费系统资源。	默认值为 1。
空闲连接超时（分钟）	以分钟为单位，指定服务器等待空闲连接返回请求的时间长度。通常无需修改默认值。	默认值为 15 分钟。
空闲作业超时（分钟）	指定服务器在两次请求给定作业之间等待的时间长短（分钟）。	默认值为 15 分钟。
Java 子 VM 参数	指定提供给服务器创建的子进程的命令行参数。	Xmx858M, Dswfinjection.lang.directory=%CommonJavaLibDir%, Dbusinessobjects.connectivity.directory=%CONNECTIONSERVER_DIR%

表30-68：单一登录服务属性

属性	说明	默认值
单一登录有效期（秒）	以秒为单位，指定 SSO 连接在过期之前的有效时间。	默认值为 86400 秒。

第 31 章 服务器量度附录

31.1 关于服务器量度附录

在此附录中，除特别声明外，术语“服务器”指 SAP BusinessObjects 服务器，而非安装或运行 SAP BusinessObjects Business Intelligence 平台的计算机。

服务器量度在未运行的服务器上不可用。

除本附录中描述的量度外，监控应用程序还可监控以下服务器状态：

服务器状态	说明
健康状态	健康状态表明服务器的一般健康状况。可能的值如下： <ul style="list-style-type: none">• 0 = 红色（危险）• 1 = 黄色（警告）• 2 = 绿色（正常）
服务器启用状态	此状态表明服务器是已启用还是已禁用。可能的值如下： <ul style="list-style-type: none">• 0 = 已禁用• 1 = 已启用
服务器运行状态	此状态表明服务器的运行状态。可能的值如下： <ul style="list-style-type: none">• 0 = 已停止• 1 = 正在启动• 2 = 正在初始化• 3 = 正在运行• 4 = 正在停止• 5 = 失败• 6 = 正在运行，但出现错误• 7 = 正在运行，但出现警告

相关主题

- 第 367 页上的“[分析服务器量度值](#)”

31.1.1 公用服务器量度

以下量度描述正在运行指定服务器的计算机。

表31-2：计算机特定量度

量度	说明
计算机名称	正在运行服务器的计算机的主机名。
操作系统	正在运行服务器的计算机的操作系统。
CPU 类型	正在运行服务器的计算机的中央处理单元类型。此量度在自适应处理服务器或 Web 应用程序容器服务器（WACS）上不可用。
CPU	服务器的可用 CPU 数。在多核硬件上，此量度可能报告逻辑 CPU 数，而非物理处理器数。此量度在自适应处理服务器或 Web 应用程序容器服务器（WACS）上不可用。
RAM (MB)	正在运行服务器的计算机上的可用内存量（以 MB 为单位）。此量度在自适应处理服务器或 Web 应用程序容器服务器（WACS）上不可用。
本地时间	本地时间。
磁盘大小 (GB)	用于安装 BI 平台的磁盘的大小（以 GB 为单位）。此量度在自适应处理服务器或 Web 应用程序容器服务器（WACS）上不可用。
已用磁盘空间 (GB)	用于安装 BI 平台的磁盘上的已用空间（以 GB 为单位）。这包括计算机上其他程序使用的磁盘空间，而非仅由 BI 平台所用的空间。此量度在自适应处理服务器或 Web 应用程序容器服务器（WACS）上不可用。

以下量度描述了指定的 SAP BusinessObjects 服务器。

表31-3：服务器特定量度

量度	说明
名称服务器	此服务器将其地址发布至的 CMS 服务器的名称和端口号。
已注册的名称	服务器的内部名称。这并非是在 CMC “服务器” 屏幕上显示的名称。
版本	服务器的版本。
开始时间	服务器最近一次启动的时间。
进程 ID	服务器的唯一进程 ID 号。运行服务器的计算机的操作系统生成此进程 ID。此进程 ID 可用于标识特定服务器。
主机名	服务器当前正在使用的主机名的列表，以逗号分隔。
主机 IP 地址	服务器侦听请求时所用的 IP 地址的列表，以逗号分隔。
请求端口	服务器用于从其他服务器接收请求的端口。如果服务器侦听多个 IP 地址上的请求，则服务器的请求端口将始终为同一端口。如果其他任何进程使用此请求端口，服务器将不会启动。请确保其他进程不会使用此端口。
繁忙的服务器线程数	当前用于某个请求的服务器线程数。如果此数字与服务器最大线程池大小相同，则表明系统无法并行处理更多请求，新请求可能需要等待繁忙的线程变为可用。

表31-4：审核量度

量度	说明
队列中的当前审核事件数	<p>被审核方已记录、但 CMS 审核方尚未获取的审核事件的数量。如果此数字持续升高，可能表明审核功能配置不正确，或者系统负载过高，并且生成审核事件的速度比审核方可以获取审核事件的速度更快。</p> <p>注意： 停止一个服务器时，要首先禁用它，然后等待此量度达到 0。否则，审核事件会滞留在队列中而无法到达审核数据存储器，直至重新启动服务器且 CMS 对其进行轮询。</p>

表31-5：日志记录服务量度

量度	说明
记录目录	此位置中提供服务器的日志文件。

31.1.2 中央管理服务器量度

下表描述中央管理服务器（CMS）的“量度”屏幕上显示的服务器量度。

表31-6：中央管理服务器量度

量度	说明
已建立了到审核数据库的连接	表明 CMS 是否与审核数据库有正常的连接。值为 1 表明存在连接。值为 0 表明与审核数据库不存在连接。如果 CMS 是审核方，则此值应为 1。如果为 0，请调查不能与审核数据库建立连接的原因。
CMS 审核方	表明 CMS 是否充当审核方。值为 1 表明 CMS 充当审核方。值为 0 表明 CMS 不充当审核方。
审核数据库连接名称	审核数据库连接的名称。这未必是审核数据库本身的名称。如果此量度为空，则表明无法建立与审核数据库的连接。
审核数据库用户名	用于连接到审核数据库的用户帐户的名称。
审核数据库的上次更新时间	CMS 最近一次成功启动以从被审核方获取事件的日期和时间。如果 CMS 为审核方，则此量度必须显示一个接近于“量度”屏幕加载时间的时间。如果此值超过屏幕加载时间两个多小时，则可能表示审核没有正常工作。
审核线程的上次轮询周期持续时间（秒）	上一轮询周期的持续时间（以秒为单位）。这表明上一轮询周期内事件数据到达审核数据库的最长延迟时间。 <ul style="list-style-type: none"> 值小于 20 分钟表明系统处于健康状态。 值介于 20 分钟到 2 小时之间表明系统繁忙。 值大于 2 小时表明系统非常繁忙。如果此情况持续，而您认为延迟时间过长，建议更新部署，从而使审核数据库能以更高速率接收数据，或减少系统跟踪的审核事件数。
审核线索利用率	审核方 CMS 从被审核方收集数据所用的轮询周期百分比。剩余时间为两次轮询之间剩余的时间。 <p>如果此值达到 100%，则在下一轮询应该开始时审核方仍在从被审核方收集数据。这可能导致事件延迟到达审核数据库。如果线索利用率频繁达到 100%，或者在几天内均保持此比率，建议您更新部署，从而使审核数据库能以更高速率接收数据，或减少系统跟踪的审核事件数。</p>
群集式 CMS 服务器	群集中运行中央管理服务器的主机名称和端口号列表（用分号分隔）。

量度	说明
并发用户建立的会话的数量	具有并发许可的用户的会话总数。
命名用户建立的会话的数量	具有命名许可的用户的会话总数。
启动后用户会话的峰值数	CMS 自启动以来处理的并发用户会话峰值数。
服务器建立的会话的数量	BI 平台服务器使用 CMS 创建的并发会话数。如果此数字大于 250，请再创建一个 CMS。
所有用户建立的会话的数量	在加载“量度”屏幕时，CMS 正在处理的并发用户会话数。此数字越大，正在使用系统的用户数越大。如果此数字大于 250，请再创建一个 CMS。
失败作业数	系统中的失败作业数。
挂起作业数	已计划、但因尚未到达计划时间或事件而未准备运行的作业数。
运行中作业数	当前正在运行的作业数。
已完成作业数	系统中的已完成作业数。
等待中作业数	系统中已计划、正在等待可用资源的作业数。
并发用户许可数	由密钥号码指定的并发用户许可的数量。
命名用户许可数	由密钥号码指定的命名用户许可的数量。
内部版本日期	CMS 的内部版本日期。
系统数据库连接名称	CMS 系统数据库连接的名称。这未必是 CMS 系统数据库本身的名称。
系统数据库服务器名称	在其中运行 CMS 系统数据库的服务器的名称。这未必是 CMS 系统数据库本身的名称。
系统数据库用户名	用于连接到 CMS 系统数据库的用户帐户的名称。
数据源名称	CMS 系统数据库连接的名称。
内部版本号	CMS 的内部版本号。此数字可用于确定用户安装的 SAP BusinessObjects Business Intelligence 平台的版本。
产品版本	CMS 的产品版本。
资源版本	CMS 的资源版本。
启动后平均提交响应时间（毫秒）	从服务器启动以来，CMS 执行提交操作所用的平均时间长度（以毫秒为单位）。如果响应时间大于 1000 毫秒，可能表明需要调整 CMS 或 CMS 系统数据库。
启动后平均查询响应时间（毫秒）	从服务器启动以来，CMS 执行查询操作所用的平均时间长度（以毫秒为单位）。如果响应时间大于 1000 毫秒，可能表明需要调整 CMS 或 CMS 系统数据库。

量度	说明
启动后最长提交响应时间（毫秒）	从服务器启动以来，CMS 执行提交操作所用的最长时间长度（以毫秒为单位）。如果响应时间大于 10000 毫秒，可能表明需要调整 CMS 或 CMS 系统数据库。
启动后最长查询响应时间（毫秒）	从服务器启动以来，CMS 执行查询操作所用的最长时间长度（以毫秒为单位）。如果响应时间大于 10000 毫秒，可能表明需要调整 CMS 或 CMS 系统数据库。
启动后的提交数	从服务器启动以来，向 CMS 系统数据库提交的次数。
启动后的查询数	服务器启动起来的数据库查询总数。如果此数字较大，可能表明系统较活跃，或系统负载较重。
启动后的用户登录数	服务器启动以来的用户登录次数。如果此数字较大，可能表明系统较活跃，或系统负载较重。
已建立的系统数据库连接数	CMS 可以建立的与 CMS 系统数据库的连接数。如果某个数据库连接丢失，CMS 会尝试恢复连接。如果建立的数据库连接数始终低于由“请求的系统数据库连接数”属性（“属性”屏幕中“中央管理服务”区域）指定的系统数据库连接数，则可能表明 CMS 无法获取更多连接，且系统运行没有达到最佳状态。一个潜在的解决方案是配置数据库服务器以允许 CMS 进行更多数据库连接。
当前使用的系统数据库连接	CMS 当前正在使用的与 CMS 系统数据库的连接数。当前正在使用的连接数可能小于或等于建立的系统数据库连接数。如果建立的连接数与使用的连接数在某段时间相同，则可能出现了瓶颈。通过增加“属性”屏幕中“请求的系统数据库连接数”属性的值，可以改善系统的性能。调整 CMS 系统数据库也可以改善性能。
挂起的系统数据库请求数	正在等待可用连接的 CMS 系统数据库的请求数。如果此数字较高，请考虑增加“请求的系统数据库连接数”属性的值。调整 CMS 系统数据库也可以改善性能。
CMS 系统高速缓存中的对象数	CMS 系统高速缓存中的当前对象总数。
CMS 系统 DB 中的对象数	CMS 系统数据库中的当前对象总数。
现有的并发用户帐户数	群集中具有并发许可的现有用户的总数。
现有的命名用户帐户数	群集中具有命名许可的现有用户的总数。

31.1.3 连接服务器量度

以下量度特定于连接服务器。

表31-7：连接服务量度

量度	说明
数据源	<p>在表中列出通过“属性”页面激活的数据源。显示每个网络层和数据库对的以下信息：</p> <ul style="list-style-type: none"> • 状态（“已加载”或“失败！”）：驱动程序的当前状态 • 可用连接：可以使用的池连接数 • 作业数（CORBA）：正在处理的作业数（2 层部署） • 作业数（HTTP）：正在处理的作业数（Web 层部署） <p>注意： 有关连接池的更多信息，请参阅《数据访问指南》。</p>

31.1.4 事件服务器量度

下表描述事件服务器的“量度”屏幕上显示的服务器量度。

表31-8：事件服务量度

量度	说明
监控文件列表	通过一个表列出了事件服务器正在监控的文件。“文件名”列显示文件的名称和路径。“上次通知时间”列显示服务器轮询并找到该文件存在的最新时间戳。
监控文件数	事件服务器当前监控的文件总数。

31.1.5 文件资源库服务器量度

下表描述输入文件资源库服务器和输出文件资源库服务器的“量度”屏幕上显示的服务器量度。

表31-9：文件存储服务量度

量度	说明
活动文件	文件资源库服务器中当前正在访问的文件数。
已写入的数据（MB）	已写入到服务器上的文件的总 MB 数。
已发送的数据（MB）	从服务器上的文件读取的总 MB 数。
活动文件的列表	一个表，其中列出了文件资源库服务器中当前正在访问的文件。
活动连接数	与客户端以及与其他服务器之间的活动连接的总数。
根目录中的可用磁盘空间（GB）	包含服务器可执行文件的磁盘上的可用空间总量（GB）
根目录中的空闲磁盘空间（GB）	包含服务器可执行文件的磁盘上的剩余可用空间总量（以 GB 为单位）。
根目录中的总磁盘空间（GB）	包含服务器可执行文件的磁盘上的总磁盘空间（GB）
根目录中的可用磁盘空间（%）	包含服务器可执行文件的磁盘上的可用磁盘空间量（%）。

31.1.6 自适应处理服务器量度

下表描述自适应处理服务器“量度”屏幕上显示的服务器量度。

表31-10：自适应处理服务器量度

量度	说明
传输层中的线程数	传输层所有线程池中的线程总数。
传输层线程池大小	共享传输层线程的总数。这些线程可以由自适应处理服务器上承载的任何服务使用。
可用处理器数	对运行该服务器的 Java 虚拟机（JVM）可用的处理器数。

量度	说明
最大内存 (MB)	Java 虚拟机将尝试使用的最大内存量 (以 MB 为单位)。
可用内存 (MB)	JVM 可用来分配新对象的内存量 (以 MB 为单位)。
内存总量 (MB)	Java 虚拟机中的内存总量 (以 MB 为单位)。此值会根据主机环境随时间变化。
CPU 使用百分比 (最近 5 分钟内)	在之前 5 分钟内服务器所使用 CPU 时间占总 CPU 时间的百分比。例如, 如果一个线程总共占用四 CPU 系统中的一个 CPU, 那么利用率为 25%。分配给 JVM 的所有处理器全部考虑在内。如果值大于 80%, 则表示可能出现了 CPU 瓶颈。
CPU 使用百分比 (最近 15 分钟内)	在之前 15 分钟内服务器所使用 CPU 时间占总 CPU 时间的百分比。例如, 如果一个线程总共占用四 CPU 系统中的一个 CPU, 那么利用率为 25%。分配给 JVM 的所有处理器全部考虑在内。如果值超过 70%, 则表示可能出现了瓶颈。
垃圾回收期间已停止系统的百分比 (最近 5 分钟内)	<p>在垃圾回收 (GC) 运行的最近 5 分钟内, 已停止系统的百分比。在此情况下, 在虚拟机执行需要独占访问的垃圾回收关键阶段时, 所有 APS 服务都将无法执行。</p> <p>通常, 较小的一位数值表明行为正常, 甚至欠载。如果此值随时间变为二位数, 可能表明存在吞吐量过低的问题, 需要进行调查。</p>
垃圾回收期间已停止系统的百分比 (最近 15 分钟内)	<p>在垃圾回收 (GC) 运行的最近 15 分钟内, 已停止系统的百分比。在此情况下, 在虚拟机执行需要独占访问的垃圾回收关键阶段时, 所有 APS 服务都将无法执行。</p> <p>通常, 较小的一位数值表明行为正常, 甚至欠载。如果此值随时间变为二位数, 可能表明存在吞吐量过低的问题, 需要进行调查。</p>
垃圾回收期间的页面错误数 (最近 5 分钟内)	前 5 分钟运行收集垃圾时出现的页面错误数。任何大于 0 的值均表明系统负载过重, 处于内存较低的状态。
垃圾回收期间的页面错误数 (最近 15 分钟内)	前 15 分钟运行收集垃圾时出现的页面错误数。任何大于 0 的值均表明系统负载过重, 处于内存较低的状态。
完全垃圾回收数	从服务器启动以来, 执行完全垃圾回收的次数。如果此值显著上升, 可能表明系统处于内存较低的状态。
JVM 锁争用数	包含等待访问的线程的同步对象的数量。始终大于 0 的任何值可能表明存在不会再次运行的线程。启动线程转储, 以获取有关该问题原因的更多信息。
JVM 调试信息	关于 SAP Java 虚拟机的调试信息, 包括状态、端口和附加客户端 (如果有)。
JVM 版本信息	关于 SAP Java 虚拟机的版本信息。

量度	说明
JVM 死锁线程计数器	发生死锁的线程数。对于大于 0 的任何值，均表明存在不会再次运行的线程。启动线程转储，以获取有关该问题原因的更多信息。
JVM 跟踪标记数	当前为 JVM 开启的跟踪标记数。这指明了 JVM 跟踪的级别。
服务	服务器承载的服务的列表，以逗号分隔。

表31-11: DSL 桥服务量度

量度	说明
DSLServiceMetrics.queryCount	客户端和服务之间打开的数据请求数
DSLServiceMetrics.activeConnectionCount	当前在客户端和服务之间打开的连接数。
DSLServiceMetrics.activeSessionCount	当前在客户端和服务之间打开的会话数。
DSLServiceMetrics.activeOLAPConnectionCount	当前在 OLAP 客户端和服务之间打开的连接数。

表31-12: 客户端审核代理服务量度

量度	说明
自服务器启动以来收到的审核事件数	自服务启动以来，服务收到的客户端审核事件的数量。此量度可用于验证是否正确配置了客户端审核功能。如果值大于 0，则表示正在通过此客户端审核服务成功路由来自客户端的审核事件。

表31-13: 平台搜索服务量度

量度	说明
服务启动后成功的提取尝试次数	平台搜索服务启动后提取文档的成功尝试次数。
上次索引更新时间戳	上次索引更新的日期和时间。
上一次内容存储生成时间戳	上一次生成内容存储的日期和时间。
服务启动后失败的提取尝试次数	平台搜索服务启动后提取文档的失败尝试次数。
服务可用	如果服务可用，则为“真”。否则，为“假”。
正在建立索引	如果正在建立索引，则为“真”。否则，为“假”。
已建立索引的文档数	显示服务启动后已建立索引的文档数。

表31-14：多维分析服务量度

量度	说明
会话计数	从 MDAS 客户端到服务器的当前连接数。
多维数据集计数	正用于向尚未超时的连接提供数据的数据源数目。
查询计数	MDAS 客户端与服务器之间打开的数据请求数。

表31-15：数据联合服务量度

量度	说明
正在运行的查询数	正在运行的查询总数（占用内存和不占用内存）。
连接数	指向数据联合查询引擎的用户连接总数。
从数据源传输的字节总数	从数据源读取的数据数量（以字节为单位）。
从数据源传输的记录总数	从数据源读取的行总数。
执行查询产生的字节总数	作为查询输出产生的数据数量（以字节为单位）。
执行查询产生的记录总数	作为查询输出产生的总行数。
占用内存的查询数	正在运行的占用内存的查询总数。
执行查询所用内存字节总数	正在运行的查询当前使用的内存量（以字节为单位）。
执行查询所用磁盘字节总数	正在运行的查询当前使用的磁盘空间量（以字节为单位）。
使用磁盘的查询数	正在运行的使用磁盘的查询总数。
等待资源的查询数	正在运行的当前等待执行的查询总数。
活动线程数	用于执行请求的活动线程总数。
元数据高速缓存所用内存的字节总数	用于高速缓存元数据、统计信息和连接器配置的内存量（以字节为单位）。
失败查询数	失败查询总数（引发异常）。
处于查询分析步骤的查询数	正在运行的当前处于分析步骤的查询总数。
处于查询优化步骤的查询数	正在运行的当前处于优化步骤的查询总数。
处于查询执行步骤的查询数	正在运行的当前处于执行步骤的查询总数。
已加载的连接器数	已加载于服务的连接器总数。
与已加载连接器间的活动连接数	指向已加载于服务的连接器的活动连接总数。

量度	说明
数据联合服务可用	如果服务可用，则为“真”。否则，为“假”。

表31-16：连接服务量度

量度	说明
数据源	<p>在表中列出通过“属性”页面激活的数据源。显示每个网络层和数据库对的以下信息：</p> <ul style="list-style-type: none"> 状态（“已加载”或“失败！”）：驱动程序的当前状态 可用连接：可以使用的池连接数 作业数（CORBA）：正在处理的作业数（2 层部署） 作业数（HTTP）：正在处理的作业数（Web 层部署） <p>有关连接池的更多信息，请参阅《数据访问指南》。</p>

表31-17：监控服务量度

量度	说明
过去 15 个周期的平均监测器状态计算时间（毫秒）	该监控服务实例计算过去 15 个周期的监测器状态所需的平均时间
用户创建的量度数	群集中所有用户创建的量度总数。
监测器数	群集中监测器的总数，包括已禁用和已启用的监测器。
serviceBean.monitoringAppPropEnabled	如果监控应用程序已启用，则为“真”。否则，为“假”。此量度与 CMC 中监控应用程序属性页面中的设置相匹配。
监控量度刷新闻隔（秒）	此监控服务实例当前使用的刷新闻隔。在服务启动时，该量度将初始化为当时 CMC 中监控应用程序属性页面中的设置，因此在其他时间，该量度可能与 CMC 页面上的当前设置不同。
服务可用	如果监控服务为活动状态，则为“真”。否则，为“假”。群集中仅有一个活动的监控服务。
计算趋势的量度数	监控数据库当前正在记录的量度总数。

表31-18：BEx Web 应用程序服务量度

量度	说明
会话计数	BEx Web 应用程序服务中的活动会话总计数

31.1.7 Web 应用程序容器服务器量度

下表描述 Web 应用程序容器服务器的“量度”屏幕上显示的服务器量度。

注意：

Web 应用程序容器服务器还具有在“自适应处理服务器量度”一节中描述的所有量度。

表31-19: Web 应用程序容器服务器量度

量度	说明
正在运行的 WACS 连接器列表	服务器上所有正在运行的连接器的列表。如果没有看到所有连接器（HTTP、HTTPS 和通过代理的 HTTP），这表明连接器未启用或启动失败。
WACS 连接器在启动时失败	是否存在任何失败的连接器。如果为“真”，则至少有一个连接器启动失败。如果为“假”，则所有连接器都在运行。当一个或多个连接器启动失败时，不运行服务器；必须解决服务器故障，才能确保所有连接器的启动都正常。

相关主题

- 第 953 页上的“[自适应处理服务器量度](#)”

31.1.8 自适应作业服务器量度

表31-20: 作业服务器量度

量度	说明
收到的作业请求数	应该已在服务器上运行的作业数。
并发作业数	当前正在服务器上运行的作业数。如果此数值较高，那么服务器处于繁忙状态。

量度	说明
峰值作业	在服务器上同时运行过的最大并发作业数。除非重新启动服务器，否则此数值不会降低。
创建作业的失败次数	服务器上失败的作业数。
临时目录	在其中创建临时文件的目录。此目录可在服务器的“属性”屏幕上指定。 如果此目录没有足够的磁盘空间，用户将遇到问题。
有效的文件系统目标默认设置	如果服务器可以向在该服务器“目标”屏幕中指定的文件系统目标发送文档，则为“真”。否则，为“假”。
有效的 FTP 目标默认设置	如果服务器可以向在该服务器“目标”屏幕中指定的 FTP 服务器目标发送文档，则为“真”。否则，为“假”。
有效的收件箱目标默认设置	如果服务器可以向在该服务器“目标”屏幕中指定的收件箱目标发送对象，则为“真”。否则，为“假”。
有效的电子邮件目标默认设置	如果服务器可以向在该服务器“目标”屏幕中指定的电子邮件目标发送对象，则为“真”。否则，为“假”。
计划服务	显示服务器上运行的所有服务的表。
子进程	显示服务器上运行的所有子进程的表。
有效的 SAP StreamWork 目标默认设置	如果服务器可向在该服务器“目标”屏幕中指定的 SAP StreamWork 目标发送对象，则为“真”。否则，为“假”。

下表描述服务器上运行的每个计划服务的量度。

表31-21：计划服务量度

量度	说明
计划服务	服务名称。
收到的作业请求数	应该已在服务上运行的作业数。
并发作业数	当前在服务上运行的并发作业数。如果此数值较高，那么服务处于繁忙状态。
峰值作业	在服务上同时运行过的最大并发作业数。
允许的最大并发作业数	服务允许的并发独立进程（子进程）的数量。 此目录可在服务器的“属性”屏幕上指定。
创建作业的失败次数	服务上失败的作业数。

下表描述服务器上运行的每个子进程的量度。

表31-22：子量度

量度	说明
计划服务	子进程名称。
进程 ID	子进程的标识符。
收到的作业请求数	应该已在子进程上运行的作业数。
并发作业数	当前在子进程上运行的并发作业数。正常情况下此数字必须为 1。
峰值作业	在子进程上同时运行过的最大并发作业数。
允许的最大作业数	子进程允许的并发作业数。
通信故障	父自适应作业服务器出现过的通信故障数。如果此数值较大，那么子进程将重新启动。
正在初始化	如果子进程处于初始化过程中，则为“真”。否则，为“假”。
关闭中	如果子进程处于关闭过程中，则为“真”。否则，为“假”。

31.1.9 Crystal Reports Server 量度

下表描述了 Crystal Reports 处理服务器和 Crystal Reports 2013 处理服务器的“量度”屏幕上显示的服务器量度。

表31-23：Crystal Reports 处理服务器量度

量度	说明
打开的作业数	该表列出了服务器上当前运行的作业。其中包括文档的 ID 和名称、运行作业的用户名、上次访问文档的日期和作业已经运行了多长时间。
已处理的请求数	自服务器启动以来，服务器已处理的请求总数。
打开的作业数	服务器及其子进程当前正在处理的作业数。

量度	说明
对象类型	服务器主要处理的 InfoObject 类型。此量度的值不会更改。
平均处理时间（毫秒）	自服务器启动以来，服务器用于处理最近所接收的 500 个请求的平均时间（以毫秒为单位）。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。
最长处理时间（毫秒）	在服务器处理的最近 500 个请求中，处理单个请求所用的最长时间（以毫秒为单位）。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。
最短处理时间（毫秒）	在服务器处理的最近 500 个请求中，处理单个请求所用的最短时间（以毫秒为单位）。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。
排队的请求数	等待处理或正在处理的请求数。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。
对象 DLL 名称	服务器的处理插件的名称。此量度的值不会变化。
打开的连接数	当前在服务器和客户端之间打开的连接数。
请求失败率	在服务器所收到的最近 500 个请求中，服务器未能成功处理的请求数百分比。
已传输的数据（KB）	自服务器启动以来，已传输到客户端的数据总量（以 KB 为单位）。
失败的请求数	自服务器启动以来，服务器无法完成的请求数。
最大子进程数	服务器允许的最大并发子进程数。

下表描述了 Crystal Reports 高速缓存服务器的“量度”屏幕上显示的服务器量度。

表31-24: Crystal Reports 高速缓存服务器量度

量度	说明
缓存命中率（%）	在最近 500 个请求中，为其提供了缓存数据的请求所占的百分比。
连接的处理服务器	罗列部署中的 Crystal Reports 处理服务器的表。其中包括服务器的名称以及服务器当前打开的连接数。
已处理的请求数	自服务器启动以来，服务器已满足的请求总数。
对象类型	服务器主要处理的 InfoObject 类型。此量度的值不会更改。
平均处理时间（毫秒）	自服务器启动以来，服务器用于处理最近所接收的 500 个请求的平均时间（以毫秒为单位）。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。

量度	说明
最长处理时间（毫秒）	在服务器处理的最近 500 个请求中，处理单个请求所用的最长时间（以毫秒为单位）。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。
最短处理时间（毫秒）	在服务器处理的最近 500 个请求中，处理单个请求所用的最短时间（以毫秒为单位）。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。
排队的请求数	等待处理或正在处理的请求数。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。
对象 DLL 名称	服务器的处理插件的名称。此量度的值不会变化。
高速缓存大小	服务器当前在磁盘上缓存的数据量（以 KB 为单位）。
打开的连接数	当前在服务器和客户端之间打开的连接数。
已传输的数据（KB）	自服务器启动以来，已传输到客户端的数据总量（以 KB 为单位）。

下表描述了 Crystal Reports 2013 报表应用程序服务器的“量度”屏幕上显示的服务器量度。

表31-25: Crystal Reports 2013 报表应用程序服务器量度

量度	说明
metric_currentdoccount 注意： 该量度在 CMC 的监控页面上显示为 document_s_。	服务器当前正在处理的文档数。
metric_totaldoccount 注意： 该量度在 CMC 的监控页面上显示为 document_s_。	自服务器启动以来，服务器已处理的文档数。
metric_currentagentthreadcount 注意： 该量度在 CMC 的监控页面上显示为 agent thread_s_。	服务器当前正在处理的线程数。
metric_totalagentthreadcount 注意： 该量度在 CMC 的监控页面上显示为 agent thread_s_。	自服务器启动以来，服务器已处理的线程数。

31.1.10 Web Intelligence 服务器量度

表31-26: Web Intelligence 处理服务量度

量度	说明
高速缓存大小 (KB)	高速缓存中当前存储的数据量 (以 KB 为单位)。
缓存中的最大文档数	自服务器启动以来, 从高速缓存中删除的过期文档数。
高速缓存使用达到最大值次数	自服务器启动以来, 高速缓存达到服务器上所允许的最大大小的次数。
CPU 使用情况 (%)	自服务器启动以来, 服务器使用的 CPU 时间占 CPU 总时间的百分比。
总 CPU 时间 (秒)	自服务器启动以来, 服务器使用的 CPU 总时间 (以秒为单位)。
内存使用达到高阈值次数	自服务器启动以来, 内存使用达到高内存阈值的次数。
内存使用达到最大阈值次数	自服务器启动以来, 内存使用达到最大内存阈值的次数。
虚拟内存大小 (MB)	分配给服务器的总内存量 (以 MB 为单位)。
客户端当前调用次数	服务器正在处理的当前 CORBA 调用数。
远程扩展错误数	服务器无法连接到自适应处理服务器承载的远程扩展服务器的次数。
当前任务数	服务器上正在执行的当前任务数。
客户端总调用次数	自服务器启动以来, 服务器收到的 CORBA 呼叫总数。
总任务数	自服务器启动以来, 服务器上已经执行的任务总数。
空闲时间 (秒)	自服务器收到来自客户端的上一个请求以来已经过去的时间 (以秒为单位)。
当前活动会话数	能够接受来自客户端的请求的当前会话数。
从高速缓存中打开的文档数	直接从高速缓存中读取上次请求结果的文档数。
文档数	当前服务器上打开的文档数。
当前会话数	当前服务器上创建的会话数。
文档交换次数	清除线程为其计划了交换请求的文档数。

量度	说明
交换文档数	交换请求所交换的文档数。
会话超时次数	自服务器启动以来的超时会话数。
总会话数	自服务器启动以来在服务器上创建的会话数。
用户数	连接到服务器的用户总数。
活动线程数	服务器收到的请求提供服务的线程数（异步线程池）。
总线程数	自服务器启动以来创建的总线程数（异步线程池）。

31.1.11 Dashboards 服务器量度

表31-27: Dashboards 处理服务器量度

量度	说明
打开的作业数	该表列出了服务器上当前运行的作业。其中包括文档的 ID 和名称、运行作业的用户名、上次访问文档的日期和作业已经运行了多长时间。
已处理的请求数	自服务器启动以来，服务器已满足的请求总数。
打开的作业数	服务器及其子进程当前正在处理的作业数。
对象类型	服务器主要处理的 InfoObject 类型。此量度的值不会更改。
平均处理时间（毫秒）	自服务器启动以来，服务器用于处理最近所接收的 500 个请求的平均时间（以毫秒为单位）。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。
最长处理时间（毫秒）	在服务器处理的最近 500 个请求中，处理单个请求所用的最长时间（以毫秒为单位）。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。
最短处理时间（毫秒）	在服务器处理的最近 500 个请求中，处理单个请求所用的最短时间（以毫秒为单位）。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。
排队的请求数	等待处理或正在处理的请求数。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。

量度	说明
对象 DLL 名称	服务器的处理插件的名称。此量度的值不会变化。
打开的连接数	当前在服务器和客户端之间打开的连接数。
请求失败率	在服务器所收到的最近 500 个请求中，服务器未能成功处理的请求数百分比。
已传输的数据 (KB)	自服务器启动以来，已传输到客户端的数据总量（以 KB 为单位）。
失败的请求数	自服务器启动以来，服务器无法完成的请求数。
最大子进程数	服务器允许的最大并发子进程数。

表31-28：高速缓存服务器量度

量度	说明
缓存命中率 (%)	在最近 500 个请求中，为其提供了缓存数据的请求所占的百分比。
连接的处理服务器	罗列部署中的仪表盘处理服务器的表。其中包括服务器的名称以及服务器当前打开的连接数。
已处理的请求数	自服务器启动以来，服务器已满足的请求总数。
对象类型	服务器主要处理的 InfoObject 类型。此量度的值不会更改。
平均处理时间 (毫秒)	自服务器启动以来，服务器用于处理最近所接收的 500 个请求的平均时间（以毫秒为单位）。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。
最长处理时间 (毫秒)	在服务器处理的最近 500 个请求中，处理单个请求所用的最长时间（以毫秒为单位）。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。
最短处理时间 (毫秒)	在服务器处理的最近 500 个请求中，处理单个请求所用的最短时间（以毫秒为单位）。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。
排队的请求数	等待处理或正在处理的请求数。如果此数值一直较高且仍在增长，请考虑在其他计算机上创建附加服务器。
对象 DLL 名称	服务器的处理插件的名称。此量度的值不会变化。
高速缓存大小 (KB)	服务器当前在磁盘上缓存的数据量（以 KB 为单位）。
打开的连接数	当前打开的指向客户端的连接数。
已传输的数据 (KB)	自服务器启动以来，已传输到客户端的数据总量（以 KB 为单位）。

第 32 章 服务器和节点占位符附录

32.1 服务器和节点占位符

除 %SERVER_FRIENDLY_NAME% 和 %SERVER_NAME% 外，这些占位符适用于相同节点上的所有服务器。

表32-1：占位符

占位符	说明	默认值
%AuditingDatabaseConnection%	CMS 使用的审核数据库连接。	此值在安装过程中指定。
%AuditingDatabaseDriver%	用于连接到审核数据库的数据库驱动程序的类型。	在 Windows 上，默认值为 sqlserverauditdbss。
%BINDIR%	SAP BusinessObjects Business Intelligence 平台 64 位二进制文件所在的文件夹。	在 Windows 上，为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\win64_x64。在 Unix 上，为 <安装目录>/sap_bobj/enterprise_xi40/<平台>/
%BINDIR32%	SAP BusinessObjects Business Intelligence 平台 32 位二进制文件所在的文件夹。	在 Windows 上，为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\win32_x86。在 Unix 上，为 <安装目录>/sap_bobj/enterprise_xi40/<平台>/
%CACHESERVER_EXE%	Crystal Reports 高速缓存服务器的可执行文件的名称。	在 Windows 上，为 crcache.exe。在 Unix 上，为 boe_cr cached.bin。
%CMS_EXE%	中央管理服务器的可执行文件的名称。	在 Windows 上，为 cms.exe。在 Unix 上，为 boe_cmsd。

占位符	说明	默认值
%CONNECTIONSERVER32_EXE%	32 位连接服务器的可执行文件的名称。	在 Windows 上, 为 Connection Server32.exe。在 Unix 上, 为 ConnectionServer32。
%CONNECTIONSERVER_DIR%	连接服务器的根文件夹。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\dataAccess\connectionServer。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/dataAccess/connectionServer
%CONNECTIONSERVER_EXE%	64 位连接服务器的可执行文件的名称。	在 Windows 上, 为 Connection Server.exe。在 Unix 上, 为 ConnectionServer。
%CR2011_BINDIR%	Crystal Reports 2011 服务器二进制文件所在的目录。	在 Windows 上, 为 <安装目录>\SAP BusinessObjectsEnterprise XI 4.0\win32_x86。在 Unix 上, 该目录类似于: <安装目录>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9。
%CR2011_DefaultWorkingDir%	Crystal Reports 2011 服务器的默认工作目录。	在 Windows 上, 为 <安装目录>\SAP BusinessObjectsEnterprise XI 4.0\win32_x86。在 Unix 上, 该目录类似于: <安装目录>/sap_bobj/enterprise_xi40/dataAccess/connectionServer/solaris_sparcv9。
%CRYSTALRAS_EXE%	报表应用程序服务器的可执行文件的名称。	在 Windows 上, 为 crystal ras.exe。在 Unix 上, 为 boe_crystalrasd。
%CR_ODBCINI%	odbc.ini 文件的名称及其所在的路径。	在 Unix 上, 为 <安装目录>/bobj/odbc.ini。在 Windows 上, 这是一个空字符串。
%CommonJavaBundlesDir%	OSGI 共享捆绑包所在的文件夹。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\java\lib\bundles。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/java/lib/bundles。

占位符	说明	默认值
%CommonJavaLibDir%	公用 Java 库所在的文件夹。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\java\lib。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/java/lib。
%DLLEXT%	.dll 或 .so 文件的默认扩展名。	在 Windows 上, 为 .dll。在 Unix 上, 为 .so。
%DLLPATH%	安装了 SAP BusinessObjects Business Intelligence 平台的计算机上的环境变量的名称, 该变量指定解释器将在其中搜索可执行文件的目录。	在 Windows 上, 为 Path。在 Unix 上, 为 LD_LIBRARY_PATH。
%DLLPATH32%	在 Solaris 32 位系统上, 安装了 SAP BusinessObjects Business Intelligence 平台的计算机上的环境变量的名称, 该变量指定解释器将在其中搜索可执行文件的目录。	在 Solaris 计算机上为LD_LIBRARY_PATH_32。在其他操作系统上, 此占位符是一个空字符串。
%DLLPATH64%	在 Solaris 64 位系统上, 安装了 SAP BusinessObjects Business Intelligence 平台的计算机上的环境变量的名称, 该变量指定解释器将在其中搜索可执行文件的目录。	在 Solaris 计算机上为LD_LIBRARY_PATH_64。在其他操作系统上, 此占位符是一个空字符串。
%DLLPREFIX%	.dll 或 .so 文件的默认前缀。	在 Unix 上, 为 lib。在 Windows 计算机上, 此占位符是一个空字符串。
%DLLPRELOAD%	平台的 LD_PRELOAD 环境变量名称。	在 Unix 上, 为 LD_PRELOAD。在 Windows 计算机上, 此占位符是一个空字符串。
%DLLPRELOAD32%	32 位 AIX 系统的 LD_PRELOAD 环境变量名称。	在 AIX 上, 为 LDR_PRELOAD。在其他计算机上, 此占位符是一个空字符串。
%DLLPRELOAD64%	64 位 AIX 系统的 LD_PRELOAD 环境变量名称。	在 AIX 上, 为 LDR_PRELOAD64。在其他计算机上, 此占位符是一个空字符串。
%DP%	路径定界符。	在 Windows 上, 为 ;。在 Unix 上, 为 :。

占位符	说明	默认值
%DefaultAuditingDir%	在其中写入审核临时文件的目录。 为获得最佳性能，此位置应位于服务器的本地驱动器上。	在 Windows 上，为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\Auditing。在 Unix 上，为 <安装目录>/sap_bobj/data/Auditing/。
%DefaultDataDir%	作业服务器使用的临时目录。	在 Windows 上，为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\Data。在 Unix 上，为 <安装目录>/sap_bobj/data/。
%DefaultInputFRSDir%	输入文件资源库服务器的根文件夹。	在 Windows 上，为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Input。在 Unix 上，为 <安装目录>/sap_bobj/data/frsinput。
%DefaultLoggingDir%	日志文件的存储位置。	在 Windows 上，为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\logging。在 Unix 上，为 <安装目录>/sap_bobj/logging。
%DefaultOutputFRSDir%	输出文件资源库服务器的根文件夹。	在 Windows 上，为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\FileStore\Output。在 Unix 上，为 <安装目录>/sap_bobj/data/frsoutput。
%DefaultWorkingDir%	64 位服务器的工作目录	在 Windows 上，为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\win64_x64。在 Unix 上，为 <安装目录>/sap_bobj/enterprise_xi40/<平台>。
%DefaultWorkingDir32%	32 位服务器的工作目录	在 Windows 上，为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\win32_x86。在 Unix 上，为 <安装目录>/sap_bobj/enterprise_xi40/<平台>。
%EPM_LD_PRELOAD_ONCE%	平台的 LD_PRELOAD_ONCE 环境变量名称。	\$LD_PRELOAD_ONCE\$

占位符	说明	默认值
%EVENTSERVER_EXE%	事件服务器的可执行文件的名称。	在 Windows 上, 为 EventServer.exe。在 Unix 上, 为 boe_eventsd。
%EXEEXT%	可执行文件的默认扩展名。	在 Windows 上, 为 .exe。此占位符在 Unix 上不可用。
%EXEPATH%	安装了 SAP BusinessObjects Business Intelligence 平台的计算机上的环境变量的名称, 该变量指定解释器将在其中搜索可执行文件的目录。	在 Windows 上, 为 Path。在 Unix 上, 为 PATH。
%EnterpriseDir%	64 位 SAP BusinessObjects Business Intelligence 平台的安装位置。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/。
%EnterpriseDir32%	32 位 SAP BusinessObjects Business Intelligence 平台的安装位置。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/。
%ExternalJavaLibDir%	外部第三方 Java 库所在的文件夹。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\java\lib\external。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/java/lib/external。
%FILESERVER_EXE%	文件服务器的可执行文件的名称	在 Windows 上, 为 fileserv er.exe。在 Unix 上, 为 boe_filesd。
%HOARD_PATH%	内存管理器的位置。	默认情况下, 此项为空。
%HOARD_PRELOAD%	指定是否预先加载内存管理器。	默认情况下, 此项为空。
%INSTALLROOTDIR%	64 位 SAP BusinessObjects Business Intelligence 平台的安装文件夹。	此值在安装过程中指定。
%INSTALLROOTDIR32%	32 位 SAP BusinessObjects Business Intelligence 平台的安装文件夹。	此值在安装过程中指定。

占位符	说明	默认值
%IntroscopeAgentEnableInstrumentation%	指定是否对使用 Introscope Agent Enterprise Manager 的 Java 服务器启用检测。	可能的值为 True 或 False, 具体取决于在安装 SAP BusinessObjects Business Intelligence 平台时是否启用了 Introscope Agent Enterprise Manager。
%IntroscopeAgentEnterpriseManagerHost%	向其发送检测数据的 Introscope Agent Enterprise Manager 的主机名。	此值在安装过程中指定。
%IntroscopeAgentEnterpriseManagerPort%	向其发送检测数据的 Introscope Agent Enterprise Manager 的端口。	此值在安装过程中指定。
%IntroscopeAgentEnterpriseManagerTransport%	向 Introscope Agent Enterprise Manager 发送检测数据时使用的传输协议。允许的值包括: <ul style="list-style-type: none"> • TCP • HTTP • HTTPS • SSL 	TCP
%IntroscopeAgentEnterpriseManagerTransportHTTP%	通过 HTTP 向 Introscope Agent Enterprise Manager 发送检测数据时使用的类。	com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportHTTPS%	通过 HTTPS 向 Introscope Agent Enterprise Manager 发送检测数据时使用的类。	com.wily.isengard.postofficehub.link.net.HttpTunnelingSocketFactory
%IntroscopeAgentEnterpriseManagerTransportSSL%	通过 SSL 向 Introscope Agent Enterprise Manager 发送检测数据时使用的类。	com.wily.isengard.postofficehub.link.net.SSLSocketFactory
%IntroscopeAgentEnterpriseManagerTransportTCP%	通过 TCP 向 Introscope Agent Enterprise Manager 发送检测数据时使用的类。	com.wily.isengard.postofficehub.link.net.DefaultSocketFactory
%IntroscopeDir%	Introscope Agent Enterprise Manager 的安装文件夹。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\java\wily。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/java/wily。
%JAVAW_EXE%	无控制台窗口的 Java 虚拟机的可执行文件的名称。	在 Windows 上, 为 javaw.exe。在 Unix 上, 为 java。

占位符	说明	默认值
%JAVA_EXE%	Java 虚拟机的可执行文件的名称。	在 Windows 上, 为 java.exe。在 Unix 上, 为 java。
%JOBSEVERCHILD_EXE%	自适应作业服务器子进程可执行文件的名称。	在 Windows 上, 为 JobServer Child.exe。在 Unix 上, 为 boe_jobcd。
%JOBSEVER_EXE%	自适应作业服务器可执行文件的名称。	在 Windows 上, 为 JobServer.exe。在 Unix 上, 为 boe_jobcd。
%JdkBinDir%	JDK 二进制文件所在的文件夹。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\bin。在 Unix 上, 为 <安装目录>/sap_bobje/<平台>/sapjvm/bin。
%JreBinDir%	JRE 二进制文件所在的文件夹。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\win64_x64\sapjvm\jre\bin。在 Unix 上, 为 <安装目录>/sap_bobje/<平台>/sapjvm/jre/bin。
%JVM_ARCH_ENVIRONMENT%	表明计算机是在 32 位还是 64 位 JVM 上运行。	对于 32 位 Unix 计算机, 默认值为 -d32。对于 64 位计算机, 默认值为 -d64。在 Windows 计算机上, 这是一个空字符串。
%JVM_HEADLESS_MODE%	用于指定 JVM 是否以无头模式工作的命令行参数。	在 Windows 上, 为 “-Djava.awt.headless=false”。在 Unix 上, 为 “-Djava.awt.headless=true”
%JVM_HEAP_DUMP_ON_OUT_OF_MEMORY_ERROR%	指定在遇到 “内存不足” 错误时 JVM 要采取的操作的命令行参数。	“-XX:+HeapDumpOnOutOfMemoryError” “-XX:HeapDumpPath=%DefaultLoggingDir%” “-XX:+ExitVMOnOutOfMemoryError”
%JVM_SHARED_MEMORY_SEGMENT%	启用 JVM 扩展并设置 JVM 的实例号的命令行参数。	默认情况下, 此占位符为空。

占位符	说明	默认值
%LANGUAGEPACKSDIR%	安装有部署语言包的文件夹。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\Languages。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/Languages/。
%LANGUAGEPACKSDIR32%	32 位系统上安装有部署语言包的文件夹。	。在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\Languages。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/Languages/。
%LSTDir%	LST 配置文件的存储文件夹。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\conf\lst。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/conf/lst。
%MDAS_JVM_OS_STACK_SIZE%	指定多维分析服务的 JVM 堆栈大小。	默认情况下, 此占位符为空。
%NCSInstrumentLevelThreshold%	NCS 库的跟踪日志记录阈值级别。	默认情况下, 此值为 0。
%PAGESERVER_EXE%	用于 Crystal Reports 2011 处理服务器的可执行文件名称。	在 Windows 上, 为 crproc.exe。在 Unix 上, 为 boe_crprocd.bin。
%PJSContainerDir%	APS 容器 JARS 所在的文件夹。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\container。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/java/pjs/container。
%PJSServicesDir%	APS 服务 JARS 所在的文件夹。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\java\pjs\services。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/java/pjs/services。
%Platform%	运行 SAP BusinessObjects Business Intelligence 平台的计算机的操作系统。	运行 SAP BusinessObjects Business Intelligence 平台的计算机的操作系统。

占位符	说明	默认值
%Platform32%	运行 32 位 SAP BusinessObjects Business Intelligence 平台的计算机的操作系统。	运行 SAP BusinessObjects Business Intelligence 平台的计算机的操作系统。
%RasBinDir%	报表应用程序服务器的根文件夹。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\win32_x86。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/<平台>/ras。
%SERVER_FRIENDLY_NAME%	服务器的全名。	服务器的全名。
%SERVER_NAME%	服务器的全名。	服务器的全名。
%SMDAgentHost%	向其发送检测数据的 SMD 代理的主机名。	此值在安装过程中指定。
%SMDAgentPort%	向其发送检测数据的 SMD 代理的端口。	此值在安装过程中指定。
%TRACE_CONFIGFILE_INI%	BO_Trace.ini 文件的名称及其路径。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\conf\BO_trace.ini。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/conf/BO-trace.ini。
%WarFilesDir%	Web 应用程序文件的位置。	在 Windows 上, 为 <安装目录>\SAP BusinessObjects Enterprise XI 4.0\warfiles\webapps。在 Unix 上, 为 <安装目录>/sap_bobj/enterprise_xi40/warfiles/webapps。
%WEBI_LD_PRELOAD%	平台的 LD_PRELOAD 环境变量名称。	\$LD_PRELOAD\$
%WEBISERVER_EXE%	Web Intelligence 处理服务器的可执行文件的名称。	在 Windows 上, 为 wireportserver.exe。在 Unix 上, 为 WIReport Server。
%WEBI_LD_PRELOAD_ONCE%	平台的 LD_PRELOAD_ONCE 环境变量名称。	\$LD_PRELOAD_ONCE\$
%XCCACHE_EXE%	仪表盘高速缓存服务器的可执行文件的名称。	在 Windows 上, 为 xccache.exe。在 Unix 上, 为 boe_xccached。

占位符	说明	默认值
%XCPROC_EXE%	仪表盘处理服务器的可执行文件的名称。	在 Windows 上，为 xcproc.exe。 在 Unix 上，为 boe_xcprocd。

注意：

在节点级别可编辑以下占位符。有关说明和默认值请见上表。未显示在此列表中的占位符是只读的。

- %DefaultAuditingDir%
- %DefaultDataDir%
- %DefaultLoggingDir%
- %IntroscopeAgentEnableInstrumentation%
- %IntroscopeAgentEnterpriseManagerHost%
- %IntroscopeAgentEnterpriseManagerPort%
- %IntroscopeAgentEnterpriseManagerTransport%
- %NCSInstrumentLevelThreshold%
- %SMDAgentHost%
- %SMDAgentPort%

相关主题

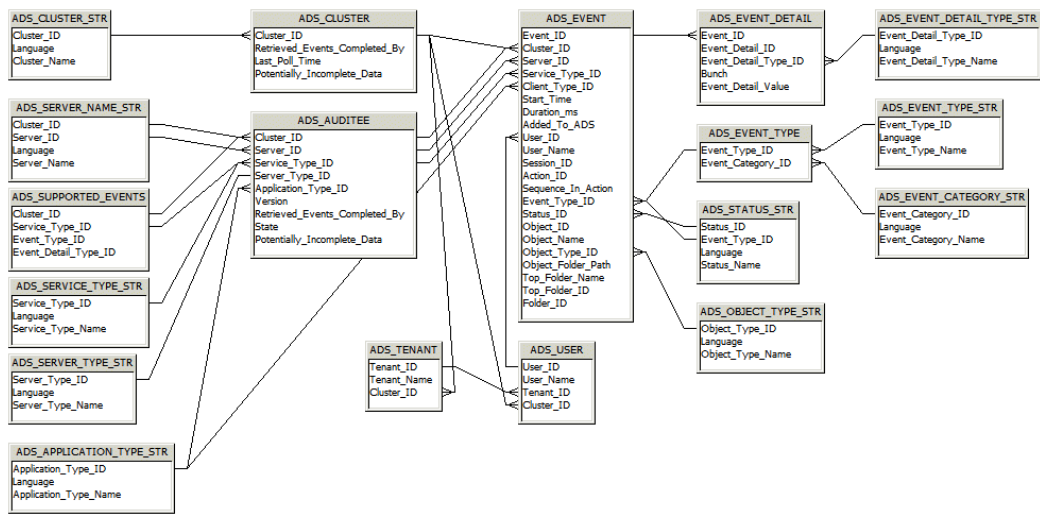
- 第 412 页上的“[查看和编辑节点的占位符](#)”

第 33 章 审核数据存储模式附录

33.1 概述

本附录为要访问审核数据存储表并提供相应报表的任何报表设计人员提供了一个参考。下面的图形和表说明显示了用于记录审核数据的表，以及这些表间的关系。

33.2 模式图



33.3 审核数据存储表

ADS_APPLICATION_TYPE_STR 表

此表提供客户端应用程序类型名称的多语种字典。

列名称	类型	键	说明
Application_Type_ID	字符 (64)	主键	应用程序的应用程序类型 CUID。
Language	字符 (10)	主键	记录应用程序类型时使用的语言代码；例如 EN 或 DE。
Applica tion_Type_Name	字符 (255)	NA	应用程序类型的文本名称；例如 Crystal Re- ports 或 Web Intelligence。

ADS_AUDITEE 表

此表记录属于部署一部分的所有被审核方服务器的属性信息。

列名称	类型	键	说明
Cluster_ID	字符 (64)	主键	被审核方所属群集的 GUID。

列名称	类型	键	说明
Server_ID	字符 (64)	<ul style="list-style-type: none"> 主键 外键 (来自 ADS_SERVER_NAME_SIR) 	触发事件的服务器的 CUID。如果事件由客户端触发，则记录负责处理事件的自适应处理服务器的 CUID。
Service_Type_ID	字符 (64)	<ul style="list-style-type: none"> 主键 外键 (来自 ADS_SERVICE_TYPE_SIR) 	触发事件的服务的服务类型 CUID。由客户端触发的事件将记录应用程序类型 CUID。
Server_Type_ID	字符 (64)	<ul style="list-style-type: none"> 主键 外键 (来自 ADS_SERVER_TYPE_SIR) 	触发事件的服务器的服务器类型 CUID。
Application_Type_ID	字符 (64)	<ul style="list-style-type: none"> 主键 外键 (来自 ADS_APPLICATION_TYPE_SIR) 	触发事件的客户端的应用程序类型 CUID。对于服务器事件，将记录服务类型的 ID。
Version	字符 (64)	NA	记录事件时，触发该事件的服务器或客户端的版本。
Retrieved_Events_Completed_By	日期时间	NA	审核方 CMS 上次向此被审核方轮询其临时文件的时间。这表示此被审核方在此日期/时间之前完成的所有事件都在 ADS 中。
State	整数	NA	被审核方所处的状态（运行中、未运行、已删除）。
Potentially_Incomplete_Data	整数	NA	显示此被审核方是否有未传输到 ADS 的事件。

ADS_CLUSTER 表

此表记录有关任何含有被审核方的群集的信息。

列名称	类型	键	说明
Cluster_ID	字符 (64)	<ul style="list-style-type: none"> 主键 外键 (来自 ADS_CLUSTER_STR) 	群集的 GUID。
Retrieved_Events_Completed_By	日期时间	NA	显示数据库中该群集审核信息的即时性。在任何给定时间，记录所有当前正在运行的被审核方服务器最早检索到的审核时间戳。这表示在此日期之前完成的所有事件都在 ADS 中。
Last_Poll_Time	日期时间	NA	审核方 CMS 上次轮询此群集中被审核方的时间。
Potentially_Incomplete_Data	整数	NA	表示群集内可能存在不完整的审核信息：“0” = 所有服务器都已正常传输数据；“1” = 群集中至少有一个正在运行或未运行的服务器设置了“Potentially_Incomplete_Data”标志，这意味着某个被审核方还有事件未传输到 ADS。

ADS_CLUSTER_STR 表

此表提供部署中不同群集的参考记录。

列名称	类型	键	说明
Cluster_ID	字符 (64)	主键	群集的唯一标识。
Language	字符 (10)	主键	群集的语言设置代码，例如 EN 或 DE。
Cluster_Name	字符 (255)	NA	群集的名称。

ADS_EVENT 表

此表记录每个事件的基本属性，并且是模式中其他各表的中央链接点。

列名称	字段类型	键	说明
Event_ID	字符 (64)	主键	为事件生成的唯一标识。
Cluster_ID	字符 (64)	外键 (来自 ADS_CLUSTER)	被审核方群集的 GUID。记录此信息是因为多个群集可能会使用相同的 ADS。

列名称	字段类型	键	说明
Server_ID	字符 (64)	外键 (来自 ADS_SERV- ER_NAME)	触发事件的服务器的 CUID。
Service_Type_ID	字符 (64)	外键 (来自 ADS_SER- VICE_TYPE_STR)	<ul style="list-style-type: none"> 触发事件的服务类型的 CUID。服务器上的服务将记录其服务类型 CUID。 客户端应用程序 (例如, BI 启动板或 Web Intelligence 胖客户端) 将记录其应用程序类型 CUID。
Client_Type_ID	字符 (64)	外键 (来自 ADS_APPLICA- TION_TYPE)	记录建立会话的客户端的客户端类型 ID。
Start_Time	日期时 间	NA	事件操作开始的日期和时间 (UTC) (包括毫秒)。
Duration_ms	整数	NA	操作的持续时间 (以毫秒为单位)。
Added_to_ADS	日期时 间	NA	在 ADS 中记录事件时的日期和时间 (UTC)。
User_ID	字符 (64)	NA	执行操作的用户的 CUID。
User_Name	字符 (255)	NA	与执行操作的用户的 ID 关联的名称。以审核方 CMS 的默认语言记录。
Session_ID	字符 (64)	NA	在期间触发事件的会话的 GUID。如果没有关联的会话, 则该字段将为空。
Action_ID	字符 (64)	NA	触发事件的用户操作的 ID。用于将由单一用户操作产生的事件进行分组。
Sequence_In_Action	整数	NA	对于多服务器 (或客户端和多服务器) 事件而言, 该字段为触发事件的序列中的服务器或客户端应用程序。在所有计划工作流中, 该序列 ID 将始终为 0。
Event_Type_ID	整数	外键 (来自 ADS_EVENT_TYPE)	事件的类型 (例如查看或保存)。
Status_ID	整数	外键 (来自 ADS_STA- TUS_STR)	操作的状态 (例如 “0” = 成功, “1” = 失败)。
Object_ID	字符 (64)	NA	对其执行操作的对象的 CUID。

列名称	字段类型	键	说明
Object_Name	字符 (255)	NA	对其执行操作的对象的名称。以审核方 CMS 的默认语言记录。
Object_Type_ID	字符 (64)	外键（来自 ADS_OB- JECT_TYPE_STR）	对其执行操作的对象类型的 CUID。
Object_Folder_Path	字符 (255)	NA	对其执行操作的对象的完整文件夹路径（例如 Country/Region/City）。以审核方 CMS 的默认语言记录。如果无法确定文件夹路径，则该值将设置为空。
Folder_ID	字符 (64)	NA	对其执行操作的对象的文件夹的 CUID。
Top_Folder_Name	字符 (255)	NA	对象的顶层文件夹的名称。例如，如果对象位于 Country/Region/City 中，则将记录 Country。
Top_Folder_ID	字符 (64)	NA	对象所驻留的顶层文件夹的 CUID。例如，如果对象位于 Country/Region/City 中，则将记录 Country 文件夹的 CUID。

ADS_EVENT_CATEGORY_STR 表

此表提供事件类别名称的多语种字典。

列名称	类型	键	说明
Event_Type_ID	整数	主键	事件类别 ID。
Language	字符 (10)	主键	记录事件类别名称时使用的语言代码；例如 EN 或 DE。
Event_Category_Name	字符 (255)	NA	事件类别的名称。

ADS_EVENT_DELETES

不要使用此表或依据此表创建报表。它只供内部系统使用，在以后版本中可能会被删除。

ADS_EVENT_DETAIL 表

此表记录事件详细信息属性。

列名称	类型	键	说明
Event_Detail_ID	整数	主键	事件详细信息的 GUID。

列名称	类型	键	说明
Event_ID	字符 (64)	<ul style="list-style-type: none"> 主键 外键（来自 ADS_EVENT） 	父事件 GUID。
Event_Detail_Type_ID	整数	外键（来自 ADS_EVENT_DETAIL_STR）	事件详细信息类型。
Bunch	整数	NA	<p>如果详细信息属于系列的一部分，则该字段用于将它们捆绑在一起。</p> <p>例如，如果报表有关于“州”和“国家/地区”的提示，则提示“国家/地区”时用户可以输入“美国”，提示“州”时输入“加利福尼亚”和“内华达”。这将产生两组事件详细信息。第一组包括：</p> <ul style="list-style-type: none"> 提示名称：国家/地区 提示值：美国 <p>第二组包括：</p> <ul style="list-style-type: none"> 提示名称：州 提示值：加利福尼亚 提示值：内华达
Event_Detail_Value	字符（长文本）	NA	事件详细信息的值。

ADS_EVENT_DETAIL_TYPE_STR 表

此表提供事件详细信息类型名称的多语种字典。

列名称	类型	键	说明
Event_Detail_ID	整数	主键	事件详细信息的事件详细信息类型 ID。
Language	字符 (10)	主键	记录事件详细信息名称时使用的语言代码；例如 EN 或 DE。
Event_Detail_Type_Name	字符 (255)	NA	事件详细信息类型的文本名称。

ADS_EVENT_TYPE 表

此表提供不同事件类别的参考记录。

列名称	类型	键	说明
Event_Type_ID	整数	<ul style="list-style-type: none"> 主键 外键（来自 ADS_EVENT_TYPE_STR） 	事件类型的唯一标识符。
Event_Category_ID	整数	<ul style="list-style-type: none"> 主键 外键（来自 ADS_EVENT_CATEGORY_STR） 	事件的类别。例如：公共、Web Intelligence 或生命周期管理。

ADS_EVENT_TYPE_STR 表

此表提供事件类型名称的多语种字典。

列名称	类型	键	说明
Event_Category_ID	整数	主键	事件的事件类型 ID。
Language	字符 (10)	主键	记录事件类别名称时使用的语言代码；例如 EN 或 DE。
Event_Type_Name	字符 (255)	NA	事件类型的文本名称；例如查看或登录。

ADS_OBJECT_TYPE_STR 表

此表提供事件对象名称的多语种字典。

列名称	类型	键	说明
Object_Type_ID	字符 (64)	主键	对象的对象类型 CUID
Language	字符 (10)	主键	记录对象类型名称时使用的语言代码，例如 EN 或 DE。
Object_Type_Name	字符 (255)	NA	对象类型的名称。

ADS_SERVER_NAME_STR 表

此表提供服务器名称的多语种字典。重命名服务器时将更新值。

列名称	类型	键	说明
Cluster_ID	字符（64）	主键	服务器所属群集的 GUID。
Server_ID	字符（64）	主键	服务器的 CUID。
Language	字符（10）	主键	服务器名称的语言代码；例如 EN 或 DE。
Server_Name	字符（255）	NA	服务器的名称。

ADS_SERVICE_TYPE_STR 表

此表提供服务类型名称的多语种字典。

列名称	类型	键	说明
Service_Type_ID	字符（64）	主键	服务的服务类型或服务类别 CUID。
Language	字符（10）	主键	记录服务类型名称时使用的语言代码，例如 EN 或 DE。
Service_Type_Name	字符（255）	NA	服务类型的名称。

ADS_STATUS_STR 表

此表提供事件状态名称的多语种字典。

列名称	类型	键	说明
Status_ID	整数	主键	操作状态的数值表示。
Event_Type_ID	整数	主键	事件的事件类型 ID。例如，1002 表示查看。
Language	字符（10）	主键	记录事件状态时使用的语言代码，例如 EN 或 DE。
Status_Name	字符（255）	NA	事件状态的文本说明，例如“成功”或“失败”。

ADS_SUPPORTED_EVENTS 表

此表记录每个服务类型或客户端应用程序类型受支持的事件及事件相关详细信息的列表。

列名称	类型	键	说明
Cluster_ID	字符（64）	主键	服务器所属的群集 GUID。

列名称	类型	键	说明
Service_Type_ID	字符 (64)	主键	触发事件的服务的服务类型 CUID。 如果事件由客户端应用程序触发，则记录应用程序类型 CUID。
Event_Type_ID	整数	外键 (来自 ADS_EVENT_TYPE)	所记录事件类型的 ID (例如保存的 ID)。
Event_Detail_Type_ID	整数	外键 (来自 ADS_EVENT_DETAIL_TYPE_STR)	用于标识为该事件捕获的事件详细信息类型的 CUID (例如文件路径)。

ADS_TENANT 表

此表记录租户名称与租户 ID 之间的关系。

列名称	类型	键	说明
Cluster_ID	字符 (64)	主键	群集的 GUID。
Tenant_ID	字符 (64)	主键	租户的 CUID。
Tenant_Name	字符 (255)	NA	租户的名称。

ADS_USER 表

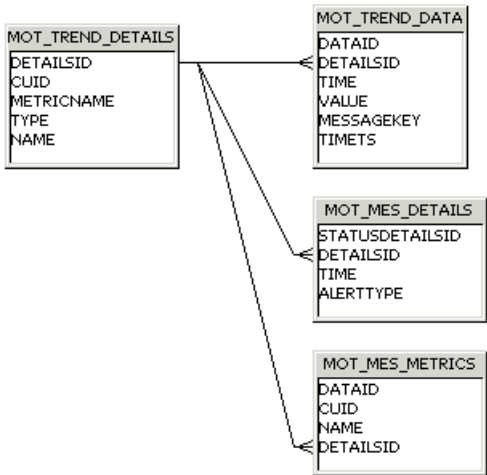
此表记录用户与租户之间的关系。

列名称	类型	键	说明
Cluster_ID	字符 (64)	主键	群集的 GUID。
User_ID	字符 (64)	主键	用户的 CUID。
User_Name	字符 (255)	NA	用户的名称。
Tenant_ID	字符 (64)	主键	租户的 CUID。

第 34 章 监控数据库模式附录

34.1 趋势数据库模式

下面的趋势数据库图形和表说明显示了记录量度、探测器和监测器数据的表，以及这些表间的关系。



MOT_TREND_DETAILS

此表记录有关托管实体、探测器和监测器的信息。例如，CUID 和量度名称。

列名称	类型	键	说明
DetailsId	INTEGER	主键 自动生成	
CUID	VARCHAR(64)	不适用	InfoObject 的 CUID 显示量度或与量度有关
MetricName	VARCHAR(255)	不适用	量度的名称

列名称	类型	键	说明
类型	VARCHAR(32)	不适用	“Subscription”、“ManagedEntityStatus”或“Probe”之一
名称	VARCHAR(255)	不适用	类型为“ManagedEntityStatus”时的监测器名称。否则，默认为“类型”中的相同字符串，全部为大写字母的除外；例如“PROBE”或“SUBSCRIPTION”。

MOT_TREND_DATA

此表记录来自量度、监测器和探测器的趋势数据。例如，量度值和时间。

列名称	类型	键	说明
DataId	INTEGER	主键 自动生成	
DetailsId	INTEGER	外键（来自MOT_TREND_DETAILS）	
Time 或 TimeT	BIGINT 或 NUMBER 或 FIXED Unix Epoch 日期	不适用	数据的收集时间。
值	FLOAT 或 DOUBLE 或 NUMBER	不适用	量度/预订的值
MessageKey	VARCHAR(32)	不适用	错误消息键或空（如成功）。对于监测器，也可以是“watchEnabled”或“watchDisabled”。它是一个“键”，因为它最终用于在显示 UI 前取回本地消息。
Ts	DATETIME 或 TIMESTAMP	不适用	数据写入数据库的时间

MOT_MES_DETAILS

此表记录有关预订超出的信息和警报传送信息。例如，超出时间和警报传送时间。

列名称	类型	键	说明
StatusDetailsId	INTEGER	主键 自动生成	

列名称	类型	键	说明
DetailsId	INTEGER	外键（来自 MOT_TREND_DE- TAILS）	
时间	BIGINT 或 NUM- BER Unix Epoch 日期	不适用	数据的收集时间。
AlertType	SMALLINT 或 NUMBER	不适用	预订通知传送类型（例如电子邮件）

MOT_MES_METRICS

此表将记录属于监测器方程式的监测器和度量信息。每个属于该监测器的度量均在此表中有一个条目。

列名称	类型	键	说明
DataId	INTEGER	主键 自动生成	
DetailsId	INTEGER	外键（来自 MOT_TREND_DE- TAILS）	
CUID	VARCHAR (64)	不适用	监测器的 GUID
名称	VARCHAR (255)	不适用	监测器的名称

第 35 章 系统复制工作表附录

35.1 系统复制工作表

属性	值
群集密钥。	
节点的名称。	
部署中每台计算机的计算机名称和 BI 平台安装文件夹。	
BI 平台管理员密码。	
CMS 数据库连接，与部署中每台计算机的连接相关联的用户名和密码。	
审核数据库连接，与部署中每台计算机的连接相关联的用户名和密码。	
对于部署中的每台计算机，Universe 和报表使用的源系统中每台计算机的任何其他数据库客户端连接的详细信息。	
对于部署中的每台计算机，数据库客户端类型和版本。	
版本、支持包和修补程序级别。	

属性	值
部署中每个输入 FRS 和输出 FRS 的文件存储位置。	
计划复制生命周期管理 (LCM) 时 LCM 数据库文件夹和 LCM 子版本文件夹的位置。	
如果计划复制监控数据库，则监控数据库文件夹。	
语义层文件夹路径。	

附录 A 更多信息

信息资源	位置
SAP BusinessObjects 产品信息	http://www.sap.com
SAP Help Portal	<p>导航到 http://help.sap.com/businessobjects/ 并在 “SAP BusinessObjects Overview” (SAP BusinessObjects 概述) 侧面板上单击 “All Products” (所有产品)。</p> <p>用户可以从 SAP Help Portal 访问涵盖所有 SAP BusinessObjects 产品及其开发信息的最新文档。用户可以下载 PDF 版本或可安装的 HTML 库。</p> <p>某些指南存储在 SAP Service Marketplace 中, 并且无法从 SAP Help Portal 获得。这些指南将在 Help Portal 上列出, 并附有指向 SAP Service Marketplace 的链接。拥有维护协议的客户有访问此站点的授权用户 ID。如要获得 ID, 请联系客户支持代表。</p>
SAP Service Marketplace	<p>http://service.sap.com/bosap-support > 文档</p> <ul style="list-style-type: none"> • 安装指南: https://service.sap.com/bosap-instguides • 发行说明: http://service.sap.com/releasenotes <p>SAP Service Marketplace 用于存储某些安装指南、升级和迁移指南、部署指南、发行说明以及所支持平台的文档。拥有维护协议的客户有访问此站点的授权用户 ID。请联系客户支持代表以获得 ID。如果是从 SAP Help Portal 重定向到 SAP Service Marketplace, 请使用左侧导航窗格中的菜单找到包含要访问的文档的类别。</p>
Docupedia	<p>https://cw.sdn.sap.com/cw/community/docupedia</p> <p>Docupedia 提供更多文档资源、协作编写环境, 以及交互式反馈渠道。</p>
开发人员资源	<p>https://boc.sdn.sap.com/</p> <p>https://www.sdn.sap.com/irj/sdn/businessobjects-sdklibrary</p>

信息资源	位置
SAP Community Network 上的 SAP BusinessObjects 文章	https://www.sdn.sap.com/irj/boc/businessobjects-articles 这些文章以前称为技术论文。
技术说明	https://service.sap.com/notes 这些技术说明以前称为知识库文章。
SAP Community Network 上的论坛	https://www.sdn.sap.com/irj/scn/forums
培训	http://www.sap.com/services/education 从传统的课堂学习到有针对性的电子学习讲座，我们都可以提供一套培训方案，满足您的学习需要，适合您喜欢的学习方式。
联机客户支持	http://service.sap.com/bosap-support SAP Support Portal 包含关于客户支持计划和服务的信息。它还包含指向各种技术信息和下载内容的链接。拥有维护协议的客户有访问此站点的授权用户 ID。如要获得 ID，请联系客户支持代表。
咨询	http://www.sap.com/services/bysubject/businessobjectsconsulting 从最初的分析阶段到交付部署项目为止，顾问将始终与您协同工作。我们提供各种主题（例如，关系数据库和多维数据库、连通性、数据库设计工具以及自定义嵌入技术）的专业技能。

索引

A

- Agent Builder 640
- Analysis (OLAP 版) 70
- 安全 37, 341, 498
 - Universe 对象 890
 - Web 服务器 143
 - Web 浏览器到 Web 服务器 144
 - 查询 123, 124
 - 处理扩展 147
 - 导入设置 315
 - 登录限制 146
 - 顶层文件夹 123
 - 防止恶意登录企图 145
 - 分布式 142
 - 管理 121
 - 管理设置 318
 - 环境保护 143
 - 会话跟踪 142
 - 活动信任关系 141
 - 审核 Web 活动 145
 - 自定义权限 341
- 安全插件 207, 280
 - LDAP 身份验证 224
 - Windows AD 身份验证 246
- 安全定义编辑器
 - 传输 769, 774
- 安全套接字层, 配置 821
- 安全套接字层 (SSL) 144, 158,
 - 162, 164, 223
 - 和 LDAP 223
 - 和负载均衡 142
 - 配置 809, 812
- 安全网络通信
 - BI 平台服务器 291
 - CMC 设置 299
 - SAP 密码库 291
 - 多处理环节发布 300
 - 服务器组 299
 - 工作流 295
 - 客户端与服务器 291
 - 配置 SAP 292
 - 配置服务器 297
 - 设置环境 295
 - 生成 PSE 296
- 安全网络通信 (SNC), 集成
 - 为 SNC 进行配置 301
- 安全性 314, 752
 - Guest 帐户限制 146
 - 插件 37, 207
 - 防火墙 144

安全性 (续)

- 密码限制 145
- 默认模式 752
- 文件夹级别 752
- 限制 146
- 应用 318
- 用户限制 146
- 在 BI 平台中 752

安装

- 默认安全级别 752
- 在 Windows 上的 SAP 网关 755

安装目录, 位置 382

B

- BackupCluster.bat 471
- backupcluster.sh 471
- BEx Web 应用程序 590
- BEx Web 应用程序服务 592
- BI 工作区 68
- BI 工作区, 权限 895
- BI 平台
 - 安全建议 140
 - 备份与恢复 466
 - 导入角色 287
 - 顶层文件夹, 权限 123
 - 服务器之间的通信 167
 - 跟踪, 记录 823
 - 跟踪日志级别 556, 823
 - 权限 112
 - 使用反向代理服务器的部署 193, 194
 - 灾难恢复计划 139
 - 主要身份验证过程 206
- BI 平台服务器 640
 - 配置 Kerberos 和浏览器 254
 - 针对防火墙配置 hosts 文件 178
- BI 启动板 68
 - 登录 104, 105
 - 管理 570
 - 控制访问 555
 - 配置 104
 - 权限 894
 - 自定义登录 607
 - 组首选项 105, 106
- BI 微件: 请参阅 SAP BusinessObjects Business Intelligence 平台微件 63
- BI 资源 498
- BIAR 文件 519
 - 导出作业 519
- BIAR 文件 (续)
 - 导入作业 520
- BO_trace.ini
 - 配置 826
- BOE WAR 文件 104, 105
- Business Process BI Service
 - 从 Web 应用程序容器服务器中删除 428
 - 添加到 Web 应用程序容器服务器 428
- BW
 - 启用查看 766
 - 与 BI 平台集成 751
- BW 发布器
 - 分布组件 754
 - 配置为服务 754
 - 在 Unix 上配置 754
- BW 发布器服务 754
 - 创建 RFC 目标 755
 - 配置 754
 - 启动 754
- 版本 498
- 版本管理 462, 495, 498
- 版本管理设置 495
- 版本管理系统 494
- 版本控制 39
- 保存
 - 新作业 511
 - 作业 513
- 保存的数据 128
- 报表
 - 发布 762
 - 以批处理模式 766
 - 更新数据源 765
 - 删除 765
- 报表查看器 69
- 报表对象
 - 权限 884
 - 用于创建/修改的权限 366
- 报表维护 765
- 报表应用程序服务器
 - 命令行选项 860
 - 所需的对象权限 366
- 报表转换工具 61
 - SSL 166
- 备份 BI 平台 462, 466
 - 服务器设置 469, 470, 471
 - 冷备份 466
 - 热备份 462, 466
 - 热备份: 启用 468
 - 热备份先决条件 467

比较不同版本 497
 比较不同版本的 LCM 497
 编辑作业 514
 编码, 登录标记 141
 变量
 AIX 20
 HP-UX 20
 Linux 20
 Solaris 20
 Unix 操作系统 20
 安装目录 20, 382
 脚本目录 20
 节点管理脚本 382
 别名
 创建 109
 现有的用户 109
 新用户 108
 分配给用户 109
 管理 108
 禁用 111
 删除 110
 部分回滚 524
 部署模板 82

C

CA Wily Introscope 39
 cacert.der 158, 159
 cakey.pem 158, 159
 CCM
 Windows 的 850, 852
 对于 Unix 843, 846
 节点 381
 重命名 394
 重新创建 389
 删除 392
 添加 385
 移动 396
 用户凭据, 更改 405
 启动、停止和重新启动服务器
 349, 351
 启用和禁用服务器 353
 删除服务器 357
 添加服务器 354
 ccm.config 846
 ccm.exe 850, 852
 ccm.sh 843, 846
 恢复服务器设置 479
 ClearCase 39
 CMC
 Windows 服务器依赖项, 添加 404
 管理服务器 344
 加密密钥 154
 克隆服务器 355, 356
 控制访问 555

CMC (续)
 启动、停止和重新启动服务器
 349, 350
 启用和禁用服务器 353
 权限 893
 删除服务器 357
 添加自定义选项卡 565
 委派的管理
 概述 560
 用户组 564
 选项卡访问
 概述 560
 管理为其他用户或用户组进行
 配置的权限 564
 权限, 继承 563
 为其他用户管理 561, 562
 限制 566
 疑难解答 566
 CMS 280, 308
 SAP HANA 数据库, 选择 414
 SQL Anywhere 数据库, 选择 413
 登录 512
 多宿主计算机疑难解答 379
 分布式安全 142
 更改群集名称 361
 会话变量 142
 跟踪 143
 身份验证 206
 量度 368
 命令行选项 855
 默认端口 379, 380
 配置 379, 380, 415, 416, 417,
 418
 启动 352
 启用和禁用其他服务器 353
 群集 357, 360
 安装新的群集成员 359
 要求 357
 身份验证 206
 属性 912
 添加到群集 358
 停止 352
 疑难解答 352
 作为名称服务器 379, 380
 CMS 系统数据库 413, 414, 415, 416
 SAP HANA 数据库, 选择 414
 SQL Anywhere 数据库, 选择 413
 备份 466
 重新创建 417, 418
 复制 419, 420
 更改密码 415
 删除 417, 418
 选择 415, 416
 cmsdbsetup.sh 847
 Cookie 142
 登录标记 141

Cookie (续)
 会话跟踪 142
 Crystal Reports 处理服务器 856
 命令行选项 856
 Crystal Reports: 请参见 SAP
 Crystal Reports 66
 Crystal 报表
 权限 884
 CTS 509
 CTS 传输 (CTS+) 39
 CTS 设置选项 509
 CTS 选项 509
 custom.jsp 608
 测试升级 498
 插件
 安全 37
 插件, 安全 207
 查看
 CMS 群集详细信息 368
 Web 应用程序容器服务器 (WACS)
 量度 457
 当前量度值 367
 系统量度值 368
 主体的权限 121
 作业历史记录 523
 查看当前帐户 90
 查询
 安全 123, 124
 查询 HTML 面板, 访问权限 571
 查找对象的依赖项 517
 产品, 系统配置向导 81
 超出时间 986
 程序对象
 启用, 禁用 557, 558
 身份验证 557
 重命名, 访问级别 130
 重新启动服务器 349, 350, 351
 初始化 CMS 系统数据库 417, 418
 处理层 369
 处理服务器
 Web Intelligence 861
 命令行选项 856, 857
 处理扩展 147
 共享 560
 注册 558
 传输 769, 770
 InfoSet 连接 769, 774
 OpenSQL 连接 771
 安全定义编辑器 769
 表 768
 参数个性化 769, 780
 程序 768
 导入 771
 对象 768
 概述 768
 函数组 768

传输 (续)

- 行级安全定义 774
- 检查冲突 770
- 内容管理工作台 776
- 群集定义 769, 775

创建

- 访问级别 129
- 服务器子组 363
- 文件夹 510
- 新作业 513
- 用户帐户 94
- 组 96
- 作业 511

- 从 NetWeaver Enterprise Search 中搜索 703

D

- Dashboard Builder 68
- Dashboards 处理服务器 857
 - 命令行选项 857
- Derby 数据库, 迁移 630
- Desktop Intelligence 文档
 - 权限 882
- dumrepo 497
- 大小调整和调优 82
- 单向复制 714, 715
- 单一登录 37, 207, 273, 280
 - BI 平台 207
 - Kerberos 272, 442, 443
 - 导入角色 287
 - 到数据库 209
 - 端到端 209
 - 服务帐户 265
 - 匿名 207
 - 设置
 - LDAP 232
 - SiteMinder 232, 273
 - 疑难解答 233
- 单一登录, 配置 JD Edwards 808
- 单一登录, 配置 PeopleSoft 811
- 单一登录, 为 Siebel 配置 820
- 单一登录, 针对 Oracle EBS 的配置 343
- 单一登录, 针对 SAP Netweaver 的配置 307
- 导出作业
 - BIAR 文件 519
- 导航树
 - 服务器 344
- 导入向导: 请参见升级管理工具 26, 65
- 导入作业
 - BIAR 文件 520
- 登录
 - BI 启动板 105

登录 (续)

- 防止恶意企图 145
- 工作流 71
- 新 CMS 512
- 自定义 607
- 登录标记 141
 - 分布式安全 142
 - 会话跟踪 142
 - 身份验证 206
- 登录次数, 登录标记 141
- 第三方安全插件 207
- 第三方对象 517
- 第三方用户, 复制 717
- 第三方组, 复制 717
- 顶层
 - 文件夹, 权限 123
- 动态链接库, 处理扩展 147
- 端到端单一登录 209
- 端到端跟踪 842
- 端口号
 - Web 应用程序容器服务器 (WACS) 458
 - 冲突 458, 459
 - 更改 379, 380
- 对象
 - 权限 752, 878
 - 查看 121
 - 设置 122
- 对象冲突
 - 单向复制 732
 - 双向复制 732, 734
- 多宿主计算机 376, 377
 - Web 应用程序容器服务器 (WACS) 456
- 多语言支持 700

E

- env-locale.sh 849
- env.sh 849
- Explorer 701
 - 权限 905
- Explorer: 请参阅 SAP BusinessObjects Explorer 66

F

- FIPS 兼容模式
 - 安全设置 148
 - 联邦信息处理标准 148
 - 在 Unix 上打开 149
 - 在 Windows 上打开 148
 - 在 Windows 上关闭 149
- 发布
 - 定义角色, 在 BW 中 757
 - 多个 BI 平台系统 760

发布 (续)

- 角色或系统中的报表 762
- 批处理模式中的报表 766
- 设置 756
- 使用角色的多个报表 762
- 在后台 764
- 在后台计划 764
- 发布, 分配权限 342
- 翻译管理工具 62
 - SSL 165
- 反. 向代理服务器
 - 配置 ISA 2006 197
- 反向代理服务器
 - Live Office 204
 - Tomcat 199
 - Web 服务 199, 200
 - 包含 Web 应用程序容器服务器 (WACS) 的部署 454
 - 部署 BI 平台 193, 194
 - 查看器 URL 204
 - 会话 cookie 201
 - 配置 Apache 2.2 196
 - 配置 BI 平台 194, 195
 - 配置 WebSEAL 6.0 196
 - 特殊配置 199
 - 与 Web 应用程序容器服务器 (WACS) 配合使用 455
 - 支持的 194
- 防火墙 144
 - Web 应用程序容器服务器 (WACS) 455
 - 服务器通信, 和 167
 - 配置 176
 - SAP 集成 187
 - 用于 Oracle 电子商务集成 189
 - 配置 Siebel 集成 192
 - 配置方案 181
 - 强制服务器通过名称注册 381
 - 调试 180
 - 为 JD Edwards EnterpriseOne 配置 188
 - 为 PeopleSoft Enterprise 配置 190
- 访问 112
 - BI 启动板 555
 - CMC 555
 - Universe 连接 622
 - 查询 HTML 面板 571
 - 服务器 365
 - 服务器组 365
 - 收件箱 104
 - 应用程序 555
 - 用户 103
 - 组 103
- 访问级别 112, 120, 134
- RAS 366

访问级别 (续)

- 查看 121
- 查看与按需查看 128
- 重命名 130
- 创建 129
- 分配到主体 122
- 复制 129
- 管理 134
- 跨站点管理 132
- 权限 887
- 任务, 所需的权限 126
- 删除 130
- 修改权限 130
- 与对象的关系 131
- 预定义 126

访问控制列表

- 查看 121
- 将主体添加到 122

非主要网络接口 378

分布

- BW 发布者组件 754

分析 65

分钟数, 登录标记 141

服务 44

- 错误 349
- 配置模板 371
- 与服务器对比 23, 40

服务类别 49, 344

服务器 32

BEx Web 应用程序服务属性

- JCo 服务器 RFC 目标 935
- JCo 服务器连接计数 935
- JCo 服务器网关服务 935
- JCo 服务器网关主机 935
- SAP BW 主系统 935
- 最大客户端会话数 935

bscLogin.conf 文件位置 912

Crystal Reports Server 属性

- Java VM 参数 928
- Java 类路径 928
- Java 子 VM 参数 928
- 安全高速缓存超时 928
- 按需提供给客户端的最旧数据 928
- 查看器刷新总是输出最新数据 928
- 单一登录有效期 928
- 高速缓存文件目录 928
- 空闲连接超时 928
- 空闲作业超时 928
- 临时目录 928
- 浏览数据大小 928
- 批大小 928
- 预览或刷新时读取的数据库记录数 928

服务器 (续)

Crystal Reports Server 属性 (续)

- 允许报表作业保持与数据库的连接, 直至关闭报表作业 928
- 在客户端之间共享报表数据 928
- 在预览或刷新报表时要读取的数据库记录数 928
- 子进程存在期内的最大作业数 928
- 最大并发报表作业数 928
- 最大高速缓存大小 928
- 最大预先启动子进程数 928

HTTP 端口 912

HTTPS 端口 912

IPv6 地址 375

Krb5.ini 文件位置 912

Unix 信号处理 854

Web Intelligence 服务器设置

- 内存上限 943
- 内存下限 943
- 内存最大阈值 943

Web Intelligence 服务属性

- APS 服务 ping 失败重试计数 937
- APS 服务监控线程周期 937
- Universe 高速缓存最大大小 937

代理值 937

- 单一登录有效期 937
- 二进制流最大大小 937
- 服务器轮询时间间隔 937
- 高速缓存超时 937
- 高速缓存中的最大文档数 937
- 回收前的超时 937
- 回收前的最大文档数 937
- 监控线程循环延迟 (秒) 937
- 禁用高速缓存共享 937
- 可视化引擎交换超时 (秒) 937
- 可视化引擎清除超时 (秒) 937
- 空闲连接超时 937
- 空闲文档超时 937
- 每个用户的最大文档数 937
- 默认监控资源的交换超时 (秒) 937
- 默认监控资源的清除超时 (秒) 937
- 内存上限 937
- 内存下限 937
- 内存最大阈值 937
- 启用 APS 服务监控 937
- 启用 HTTP URL 937
- 启用当前活动日志 937
- 启用监控 937
- 启用内存分析 937

服务器 (续)

Web Intelligence 服务属性 (续)

- 启用实时高速缓存 937
- 启用文档高速缓存 937
- 启用值列表高速缓存 937
- 输出高速缓存目录 937
- 图像目录 937
- 文档高速缓存清除时间间隔 937
- 文档高速缓存最大大小 937
- 文档高速缓存最大缩减空间 937
- 允许文档导航图最大大小错误 937
- 值列表批大小 937
- 值列表批大小 (项) 937
- 最大连接数 937
- 最大值列表大小 937
- 最大字符流大小 937
- 最大自定义排序大小 937
- 绑定到所有 IP 地址 912
- 绑定到主机名或 IP 地址 912
- 标准命令行选项 854
- 查看服务器的状态 348
- 重新启动 349, 350, 351
- 错误 349
- 代理端口 912
- 代理主机名 912
- 单一登录有效期 912
- 导航树 344
- 端口 912
- 端口偏移 912
- 多维分析服务属性
 - 查询返回的最大单元数 935
 - 过滤时返回的最大成员数 935
 - 最大客户端会话数 935
- 访问 365
- 分组 362
- 服务启动超时 912
- 更改 348
 - 状态 348
- 公共服务器属性
 - SIA 启动时自动启动此服务器 909
 - 还原系统默认值 909
 - 请求端口 909
 - 日志级别 909
 - 设置配置模板 909
 - 使用配置模板 909
 - 主机标识符 909
 - 自动分配 909
- 核心服务属性
 - bscLogin.conf 文件位置 912
 - CORS — 跨源资源共享 912
 - Enterprise 会话标记超时 912
 - HTTP 端口 912
 - HTTP 基本身份验证, 启用 912
 - HTTPS 端口 912

服务器 (续)

核心服务属性 (续)

Krb5.ini 文件位置 912
 pageSize 912
 SAPR3 912
 secDAP 912
 secEnterprise 912
 secWinAD 912
 绑定到所有 IP 地址 912
 绑定到主机名或 IP 地址 912
 代理端口 912
 代理主机名 912
 单一登录有效期 912
 端口 912
 端口偏移 912
 多域访问, Javascript 912
 服务启动超时 912
 跟踪日志服务 912
 会话池超时 912
 会话池大小 912
 监控代理的 URL 912
 可视化引擎交换超时 (秒) 912
 可视化引擎清除超时 (秒) 912
 空闲连接超时 912
 空闲瞬时对象超时 912
 连接最长等待时间 (秒) 912
 临时目录 912
 每个用户会话的最大活动连接数 912
 每个用户会话的最大空闲连接数 912
 名称服务器端口 912
 启用 HTTPS 912
 启用客户端身份验证 912
 清除时间间隔 912
 请求的系统数据库连接数 912
 日志级别 912
 事件轮询时间间隔 912
 私钥访问密码 912
 通过代理启用 HTTP 912
 文件存储目录 912
 文件访问的最大重试次数 912
 显示错误堆栈 912
 线程池大小 912
 协议 912
 一页的默认对象数 912
 证书别名 912
 证书存储类型 912
 证书存储文件位置 912
 证书信任列表私钥访问密码 912
 证书信任列表文件位置 912
 自动重新连接到系统数据库 912
 最长空闲时间 912
 最长寿命 912
 最大 HTTP 标头大小 912
 最大并发请求数 912

服务器 (续)

核心服务属性 (续)

最大并发作业数 912
 最大尝试次数 912
 最大子请求数 912
 活动, 记录 369
 记录活动 369
 监控代理的 URL 912
 节点 23, 40
 禁用 353
 可视化引擎交换超时 (秒) 912
 可视化引擎清除超时 (秒) 912
 克隆 355, 356
 空闲连接超时 912
 空闲瞬时对象超时 912
 连接服务器属性
 HTTP 块区大小 923
 激活数据源 923
 连接池 923
 连接池超时 923
 临时对象不活动超时 923
 临时对象计时器时间间隔 923
 启用 HTTP 分块 923
 启用中间件跟踪 923
 启用作业跟踪 923
 数据库 923
 网络层 923
 连接最长等待时间 (秒) 912
 列表 344
 临时目录 912
 每个用户会话的最大活动连接数 912
 每个用户会话的最大空闲连接数 912
 名称服务器端口 912
 命令行 853
 默认设置 373
 配置 369
 配置服务器以使用服务帐户 252
 配置模板 371
 设置 371
 应用 372
 启动 349, 350, 351
 自动 349, 350
 启用 353
 启用 HTTPS 912
 启用客户端身份验证 912
 清除时间间隔 912
 请求的系统数据库连接数 912
 日志级别 912
 删除 357
 设置 IP 地址 375
 设置服务帐户 245
 事件轮询时间间隔 912
 属性 370

服务器 (续)

数据联合服务属性

连接不活动状态超时 937
 语句不活动状态超时 937
 执行线程池大小 937
 最大连接数 937
 私钥访问密码 912
 添加 354
 停止 349, 350, 351
 通过代理启用 HTTP 912
 通过名称注册 381
 通信 167
 文件存储目录 912
 文件访问的最大重试次数 912
 协议 912
 性能设置 370
 修改组成员资格 364, 365
 仪表盘服务器属性
 Java VM 参数 944
 Java 子 VM 参数 944
 安全高速缓存超时 (分钟) 944
 按需提供给客户端的最旧数据 (秒) 944
 客户端共享数据 944
 空闲连接超时 944
 空闲连接超时 (分钟) 944
 空闲作业超时 944
 预览或刷新时读取的数据库记录数 944
 允许报表作业保持与数据库的连接, 直至关闭报表作业 944
 子进程存在期内的最大作业数 944
 最大并发作业数 944
 最大高速缓存大小 (KB) 944
 最大预先启动子进程数 944
 与服务对比 23, 40
 占位符 355
 证书别名 912
 证书存储类型 912
 证书存储文件位置 912
 证书信任列表私钥访问密码 912
 证书信任列表文件位置 912
 主机标识选项 374
 主机名 375
 状态 344, 348
 自动重新连接到系统数据库 912
 最长空闲时间 912
 最大 HTTP 标头大小 912
 最大并发请求数 912
 最大并发作业数 912
 最大尝试次数 912
 最大子请求数 912
 服务器类型 52, 57

服务器量度 946

Crystal Reports Server 量度

打开的连接数 960
 打开的作业数 960
 当前打开的报表作业数 960
 当前打开的连接数 960
 对象 DLL 名称 960
 对象类型 960
 高速缓存大小 960
 缓存命中率(%) 960
 排队的请求数 960
 平均处理时间(毫秒) 960
 请求失败率 960
 失败的请求数 960
 已传输的数据(KB) 960
 已满足的请求数 960
 最长处理时间(毫秒) 960
 最大子进程数 960
 最短处理时间(毫秒) 960

Web Intelligence 服务器量度

CPU 使用情况(%) 963
 当前会话数 963
 当前活动会话数 963
 当前任务数 963
 高速缓存大小(KB) 963
 高速缓存使用达到最大值次数 963
 缓存中的最大文档数 963
 会话超时次数 963
 活动线程数 963
 交换文档数 963
 客户端当前调用次数 963
 客户端总调用次数 963
 空闲时间(秒) 963
 内存使用达到高阈值次数 963
 内存使用达到最大阈值次数 963
 文档交换次数 963
 文档数 963
 虚拟内存大小(MB) 963
 用户数 963
 远程扩展错误数 963
 总 CPU 时间(秒) 963
 总会话数 963
 总任务数 963
 总线程数 963

Web 应用程序容器服务器量度

WACS 连接器在启动时失败 958
 正在运行的 WACS 连接器列表 958

查看 368

连接服务器量度

数据源 952

事件服务器量度

监控文件列表 952
 监控文件数 952

文件资源库服务器量度

根目录中的可用磁盘空间(%) 953
 根目录中的可用磁盘空间(GB) 953

服务器量度(续)

文件资源库服务器量度(续)

根目录中的空闲磁盘空间(GB) 953
 根目录中的总磁盘空间(GB) 953
 活动连接数 953
 活动文件 953
 活动文件的列表 953
 已发送的数据(MB) 953
 已写入的数据(MB) 953

仪表盘服务器量度

打开的连接数 964
 打开的作业数 964
 对象 DLL 名称 964
 对象类型 964
 高速缓存大小(KB) 964
 缓存命中率(%) 964
 排队的请求数 964
 平均处理时间(毫秒) 964
 请求失败率 964
 失败的请求数 964
 已处理的请求数 964
 已传输的数据(KB) 964
 最长处理时间(毫秒) 964
 最大子进程数 964
 最短处理时间(毫秒) 964

中央管理服务量度

CMS 审核方 949
 CMS 系统 DB 中的对象数 949
 CMS 系统高速缓存中的对象数 949
 并发用户建立的会话的数量 949
 并发用户许可数 949
 产品版本 949
 当前使用的系统数据库连接 949
 等待中作业数 949
 服务器建立的会话的数量 949
 挂起的系统数据库请求数 949
 挂起作业数 949
 命名用户建立的会话的数量 949
 命名用户许可数 949
 内部版本号 949
 内部版本日期 949
 启动后的查询数 949
 启动后的提交数 949
 启动后的用户登录数 949
 启动后平均查询响应时间(毫秒) 949
 启动后平均提交响应时间(毫秒) 949
 启动后用户会话的峰值数 949
 启动后最长查询响应时间(毫秒) 949
 启动后最长提交响应时间(毫秒) 949
 群集式 CMS 服务器 949
 审核数据库的上次更新时间 949
 审核数据库连接名称 949
 审核数据库用户名 949
 审核线程的上次轮询周期持续时间(秒) 949
 审核线索利用率 949

服务器量度(续)

中央管理服务量度(续)

失败作业数 949
 数据源名称 949
 所有用户建立的会话的数量 949
 系统数据库服务器名称 949
 系统数据库连接名称 949
 系统数据库用户名 949
 现有的并发用户帐户数 949
 现有的命名用户帐户数 949
 已建立的系统数据库连接数 949
 已建立了到审核数据库的连接 949
 已完成作业数 949
 运行中作业数 949
 资源版本 949

自适应处理服务器量度

CPU 使用百分比(最近 15 分钟内) 953
 CPU 使用百分比(最近 5 分钟内) 953
 DSLServiceMetrics.activeConnectionCount 953
 DSLServiceMetrics.activeOLAPConnectionCount 953
 DSLServiceMetrics.activeSessionCount 953
 DSLServiceMetrics.queryCount 953
 JVM 版本信息 953
 JVM 调试信息 953
 JVM 跟踪标记数 953
 JVM 死锁线程计数器 953
 JVM 锁争用数 953
 serviceBean.monitoringAppPropEnabled 953
 查询计数 953
 处于查询分析步骤的查询数 953
 处于查询优化步骤的查询数 953
 处于查询执行步骤的查询数 953
 传输层线程池大小 953
 传输层中的线程数 953
 从数据源传输的记录总数 953
 从数据源传输的字节总数 953
 等待资源的查询数 953
 多维数据集计数 953
 服务 953
 服务可用 953
 服务启动后成功的提取尝试次数 953
 服务启动后失败的提取尝试次数 953
 过去 15 个周期的平均监测器状态计算时间(毫秒) 953
 会话计数 953
 活动线程数 953
 计算趋势的量度数 953
 监测器数 953
 监控量度刷新间隔(秒) 953
 可用处理器数 953
 可用内存(MB) 953
 垃圾回收期间的页面错误数(最近 15 分钟内) 953

- 服务器量度 (续)
 - 自适应处理服务器量度 (续)
 - 垃圾回收期间的页面错误数 (最近 5 分钟内) 953
 - 垃圾回收期间已停止系统的百分比 (最近 5 分钟内) 953
 - 垃圾回收期间已停止系统的百分比 (最近 1 分钟内) 953
 - 连接数 953
 - 内存总量 (MB) 953
 - 上次索引更新时间戳 953
 - 上一次内容存储生成时间戳 953
 - 失败查询数 953
 - 使用磁盘的查询数 953
 - 收到的审核事件数 953
 - 数据联合服务可用 953
 - 完全垃圾回收数 953
 - 已加载的连接器数 953
 - 已建立索引的文档数 953
 - 用户创建的量度数 953
 - 与已加载连接器间的活动连接数 953
 - 元数据高速缓存所用内存的字节总数 953
 - 占用内存的查询数 953
 - 正在建立索引 953
 - 正在运行的查询数 953
 - 执行查询产生的记录总数 953
 - 执行查询产生的字节总数 953
 - 执行查询所用磁盘字节总数 953
 - 执行查询所用内存字节总数 953
 - 最大内存 (MB) 953
 - 自适应作业服务器量度
 - 并发作业数 958
 - 创建作业的失败次数 958
 - 峰值作业 958
 - 关闭中 958
 - 计划服务 958
 - 进程 ID 958
 - 临时目录 958
 - 收到的作业请求数 958
 - 通信故障 958
 - 有效的 FTP 目标默认设置 958
 - 有效的电子邮件目标默认设置 958
 - 有效的收件箱目标默认设置 958
 - 有效的文件系统目标默认设置 958
 - 允许的最大并发作业数 958
 - 允许的最大作业数 958
 - 正在初始化 958
 - 子进程 958
 - 服务器量度关于 (续)
 - 公用量度
 - CPU 947
 - CPU 类型 947
 - RAM (MB) 947
 - 版本 947
 - 本地时间 947
 - 操作系统 947
 - 服务器量度关于 (续)
 - 公用量度 (续)
 - 5 分钟磁盘大小 (GB) 947
 - 繁忙的服务器线程数 947
 - 计算机名称 947
 - 记录目录 947
 - 进程 ID 947
 - 名称服务器 947
 - 请求端口 947
 - 已用磁盘空间 (GB) 947
 - 已注册的名称 947
 - 主机 IP 地址 947
 - 主机名 947
 - 审核量度
 - 队列中的当前审核事件数 947
 - 服务器设置
 - ccm.sh
 - 备份服务器设置 470
 - 备份 469, 470, 471
 - 恢复 477, 479
 - 服务器属性 909
 - 服务器依赖项
 - 事件日志 404
 - 添加 404
 - 远程过程调用 404
 - 服务器占位符 966
 - 服务器智能代理 22
 - Windows 服务器依赖项, 添加 404
 - 节点 381, 384, 388, 392, 394
 - 重命名 394, 395
 - 重新创建 389, 390, 391, 393, 400
 - 删除 392, 393, 400
 - 添加 385, 386, 387, 388, 400
 - 新计算机, 添加 385
 - 移动 396, 397, 398, 399, 402
 - 用户凭据, 更改 405
 - 自动启动服务器 351
 - 服务器智能代理 (SIA)
 - 关闭工作流 72
 - 启动工作流 71
 - 服务器状态 344
 - 服务器组
 - 创建 362
 - 访问 365
 - 服务器的子组 362, 364
 - 节点 344
 - 子组 363
 - 服务帐户
 - 配置服务器 252
 - 设置 245
 - 委派 245
 - 负载均衡 142
 - Web 应用程序容器服务器 (WACS) 454
 - 和分布式安全 142
- 负载平衡 (续)
 - 群集 357
 - 添加 CMS 358
 - 复查, 系统配置向导 85
 - 复制 462
 - 第三方用户和组 717
 - 对象 707
 - 访问级别 129
 - 现有作业 513
 - 复制列表
 - 创建 719, 720
 - 管理 721
 - 修改 722
 - 依赖项选项 719, 720
 - 支持的对象 719
 - 复制作业
 - 查看 725
 - 创建 726
 - 计划 728
 - 配置选项 726
 - 修改 728
- G
 - Guest 帐户
 - 禁用 100
 - GWSETUP 755
 - 概述 685
 - 高级权限 113, 120, 122
 - 高速缓存服务器 856, 857
 - 个人安全环境
 - 请参阅 PSE 291
 - 跟踪
 - 端到端 842
 - 服务器 824
 - BO_trace.ini, 配置 826
 - 跟踪, 会话 142
 - 跟踪日志
 - 日志级别 556, 823
 - 跟踪日志级别
 - CMC 服务器, 设置用于 825
 - 更改管理 ID 517
 - 更新 514
 - 重复发生和待定
 - 作业实例 522
 - 状态
 - 计划作业升级 522
 - 工作流 70
 - 按需查看 SAP Crystal Reports 2011 报表 75
 - 按需查看 Web Intelligence 文档 78
 - 查看 Analysis 工作区 80
 - 查看非缓存的 SAP Crystal Reports 2011 报表页面 74
 - 查看缓存的 Crystal 报表页面 74

工作流 (续)

- 查看权限 121
- 访问控制列表, 将主体分配到 122
- 高级权限, 分配 122
- 关闭 SIA 72
- 计划的 Web Intelligence 文档 79
- 启动 SIA 71
- 设置 Crystal 报表计划 76
- 设置 Web Intelligence 文档计划 78
- 设置程序对象的计划 73
- 设置顶层文件夹权限 123
- 用户登录 71
- 运行计划的 SAP Crystal Reports 2011 报表 77
- 运行已计划的程序对象 73
- 共享库, 作为处理扩展 147
- 构面 699
- 故障转移 644
- 关键字 511
- 关系查询
 - 访问级别 131
- 管理
 - BI 启动板 555
 - CMC 555
 - 分配权限 341
 - 服务器和服务器组 365
 - 权限 134
 - 收件箱 104
 - 委派 134
 - 应用程序 555
 - 用户 103
 - 组 103
- 管理系统 503
- 管理选项 498
 - 覆盖设置 502
 - 管理系统 502
 - 回滚设置 502
 - 作业设置 502
- 管理依赖项 498, 514, 516
- 管理应用程序 554
 - BOE WAR 文件 598
 - 讨论线索, 删除 570
- 规范化搜索结果排名 699
- 过滤的 InfoObject 516

H

- hosts 文件, 针对 NAT 防火墙配置 178
- HTTP 142, 206
- HTTP 基本身份验证 448
- HTTPS
 - 配置 Web 应用程序容器服务器 (WACS) 429, 431, 455
- 行级安全, 处理扩展 147

- 红绿灯 625
- 后台程序, 信号处理 854
- 恢复
 - InfoObject 524
 - 系统默认值 373, 460
 - 作业 523
- 恢复 BI 平台 462
 - 服务器设置 477, 479
- 恢复 SAP BI 平台
 - 服务器设置 477
- 回滚 498
 - 升级管理中的作业 523
- 回滚 InfoObject
 - 密码到期后 525
- 回滚过程 525
- 回滚设置 504
- 回滚作业
 - 密码到期后 525
- 会话 142
 - 跟踪 142
- 会话变量 142
 - 身份验证 206
- 活动信任关系 141

I

- IPv6
 - CMC 373
 - 选项 373
 - 在 CMC 中设置地址 375
- idm.keytab 450
- idm.princ 450
- idm.realm 450
- InfoObject
 - 管理不同版本 494
- InfoSet 连接传输 769
- InfoView 68
- initlaunch.sh 849
- INSTALLDIR 20
- Introscope 643
- ISA 2006
 - 针对 Oracle 10gR3 进行配置 201
 - 针对 Sun Java 8.2 进行配置 201
 - 针对 Tomcat 5.5 进行配置 201
 - 针对 WebSphere CE 2.0 进行配置 201
- iView
 - 启用查看 766

J

- JAAS, 配置文件 256, 257, 436
- Java 管理扩展 (JMX) 627
- Java 应用程序服务器, Kerberos 254
- Java, Kerberos 260, 261
- JD Edwards EnterpriseOne 38

- JD Edwards EnterpriseOne 集成
 - 防火墙配置 188
- JMX MBean 640
- JMX 远程 API 638
- 基于浏览器的客户端 59
- 集成
 - SAP 39
 - SNC 301
- 计划 498
 - 作业升级 521
- 记录 369
 - Web 活动 145
 - 服务器活动 369
- 继承 114
 - CMC 选项卡访问权限 563
 - 权限覆盖 116
 - 文件夹 115
 - 限制 118
 - 终止 133
 - 组 114
- 加密密钥 150
 - CMC 154
 - 标记为已泄露 156
 - 查看 153
 - 撤销 157
 - 创建新的 156
 - 对象列表 155
 - 状态 154
- 加密人员 152
 - 添加成员 153
- 监测器 625
- 监控 625
- 监控, 模式图 986
- 监控代理 640
- 监控服务 635
- 监控服务器 644
- 检测 842
 - Web 层 841
 - 非 Java 服务器 840
- 概述 840
- 日志记录 842
- 验证 842
 - 占位符 841
- 建立索引 692
- 建议 700
- 健康状态 625
- 将 Derby 数据库迁移到审核数据库 630
- 脚本, Unix 843
- 脚本, Windows 850
- 脚本参数, 节点
 - 重新创建 400
 - 删除 400
 - 添加 400
 - 移动 402

节点 23, 40, 381
 CMC 344
 重命名 394
 CCM 394
 serverconfig.sh 395
 重新创建 400
 AddNode.bat 390
 addnode.sh 391
 CCM 389
 RemoveNode.bat 393
 removenode.sh 393
 serverconfig.sh 390
 方案 388
 群集 357
 删除 392, 400
 CCM 392
 serverconfig.sh 393
 添加 384, 400
 AddNode.bat 386
 addnode.sh 388
 CCM 385
 CMS 358
 serverconfig.sh 387
 到群集 359
 新计算机 385
 移动 396, 402
 CCM 396
 MoveNode.bat 397
 movenode.sh 399
 serverconfig.sh 398
 节点管理脚本, 位置 382
 节点占位符 966
 禁用

 Guest 帐户 100
 别名 111
 服务器 353
 警报 573, 625
 管理 573
 管理设置 573
 默认属性 574
 目标属性 573
 权限 904
 角色 757
 导入 287
 将权限分配给 341
 取消映射 312, 340
 为管理创建 757
 映射 287, 310, 312, 326, 328, 331, 337
 重新映射 333

K

Kerberos 254, 435
 Java 单一登录 272, 442, 443
 Krb5.ini 437

Kerberos (续)
 LDAP 241
 NetWeaver SSO 257
 配置文件 254, 435
 疑难解答 278, 438
 Kerberos 文件 242
 KPI (关键绩效指标) 625
 Krb5.ini 437
 可搜索的内容类型 695
 克隆
 Web 应用程序容器服务器 (WACS) 426
 服务器 355, 356
 客户端
 Data Federator。请参见数据联合管理工具 63
 Query as a Web Service 61
 SAP BusinessObjects Analysis (Microsoft Office 版) 65
 SAP BusinessObjects Business Intelligence 平台微件 63
 SAP BusinessObjects Dashboards 66
 SAP Crystal Reports 66
 Universe 设计工具 61
 Web 59
 Web Intelligence 胖客户端 60
 报表转换工具 61
 翻译管理工具 62
 数据联合管理工具 63
 信息设计工具 62
 信息设计器。请参见信息设计工具 62
 业务视图管理器 60
 桌面 59
 客户端, 基于浏览器 67
 Analysis (OLAP 版) 70
 BI 工作区 68
 BI 启动板 68
 SAP BusinessObjects Mobile 70
 SAP BusinessObjects Web Intelligence 69
 报表查看器 69
 中央管理控制台 (CMC) 25, 67
 客户端, 桌面
 升级管理工具 26, 65
 中央配置管理器 (CCM) 26, 64
 资源库诊断工具 26, 65
 跨源资源共享 (CORS) 449
 扩展, 处理 147

L

LDAP
 Kerberos 身份验证 241
 安全插件 224

LDAP (续)
 安全套接字层 (SSL) 223
 登录配置文件 242
 配置单一登录 232
 身份验证 223
 配置 224
 身份验证插件 224
 依据 Windows AD 映射 236
 帐户 223
 疑难解答 243
 主机
 管理多个 227
 配置 225, 228
 组
 映射 234
 Live Office
 反向代理服务器的配置 199
 logon.csp 206
 类别 106
 权限 881
 冷备份 462, 466
 历史记录 509
 连接 643
 联盟 707
 Web 服务 736, 737, 738
 本地运行的实例 738, 739, 740
 查看日志 729
 重新指向目标站点 741, 743
 从目标刷新 714, 715
 从源刷新 714, 715
 单向复制 714, 715
 导入和升级复制的内容 741, 742, 743
 第三方用户和组, 复制 717
 对象清除 730, 731
 访问级别 132
 复制大对象 744
 复制列表 719
 创建 719, 720
 管理 721
 文件夹 719, 720
 复制模式 714, 715
 复制作业 725
 创建 726
 计划 728
 修改 728
 管理安全性 710, 711, 712, 713, 714
 管理冲突 732, 734
 术语 708
 双向复制 714, 715
 提高性能 746
 疑难解答 747
 优点 707
 远程计划 738, 739, 740

联盟 (续)
 远程连接 722
 创建 723
 修改 725
 最佳做法 744
 量度 625, 986
 查看 367
 临时文件 84
 绿色复选标记, 用于默认系统 761
 裸机备份 462, 466

M

MBean 627
 Mobile
 权限 907
 Monitoring Data Categories 640
 密码 415, 416
 更改 102
 选项 102, 211
 用于 CMS 数据库 415
 限制 145
 密钥文件 158, 159
 命令行选项 531, 853, 861, 864
 CMS 855
 SSL 158
 报表应用程序服务器 860
 处理服务器 856, 857
 高速缓存服务器 856, 857
 事件服务器 864
 输入文件资源库服务器和输出文件
 资源库服务器 863
 所有服务器 854
 自适应作业服务器 858
 模板, 部署 82
 模式图, 趋势数据库 986
 默认安全模式 752
 默认设置
 端口 379, 380
 服务器 373
 目标站点
 访问级别 132
 目录服务器 224
 安全插件 224
 关于 LDAP 223

N

内存设置
 在 Web 应用程序容器服务器
 (WACS) 上进行更改 459
 内容管理工作台 760
 报表发布概述 756
 定义用户访问级别 758
 发布报表 762
 更新报表的数据源 765

内容管理工作台 (续)
 删除报表 765
 添加 BI 平台系统 760
 同步报表信息 764, 765
 应用授权 758
 在后台发布报表 764
 匿名单一登录 207

O

ODBC
 CMS 数据库
 连接 419
 odbcc.ini
 为 SQL Anywhere 创建 383
 OpenDocument
 自定义登录 607
 OpenSearch 686
 OpenSQL 连接 769
 OpenSQL 连接传输 769
 Oracle
 JAAS 257
 Java 选项 260
 Kerberos 254
 Oracle EBS
 更新别名 339
 更新角色 339
 Oracle 电子商务套件 38
 将角色映射到 BI 平台 337
 Oracle 电子商务套件集成
 防火墙配置 189

P

PeopleSoft Enterprise 38
 PeopleSoft Enterprise 集成
 防火墙配置 190
 PeopleSoft EPM 安全桥
 响应文件 316
 PeopleSoft 分析服务器 815
 PeopleSoft 响应文件 320
 参数 320
 PLATFORM64DIR 20
 PlatformServices.properties 360
 postinstall.sh 849
 PSANALYTIC 过程 815
 PSAPPSRV 过程 815
 PSE
 服务器端信任 291
 配置访问 298
 派生量度 625
 配置 635
 Apache 2.2 196
 CMS 群集 361
 CMS 数据库 415, 416
 CMS 系统数据库 417, 418

配置 (续)

ISA 2006 197
 WebSEAL 6.0 196
 安全套接字层 821
 处理层 369
 多台服务器 371
 反向代理服务器 194, 195
 防火墙 176
 节点 357
 配置模板 371
 群集 357
 受信任的身份验证 213
 应用程序层 369
 智能层 369
 配置 OpenSearch 687
 配置反向代理 688
 配置模板 371
 恢复系统默认值 373
 设置 371
 应用 372
 最佳做法 371
 配置模式 314
 配置审核, 参见审核 653
 配置文件参数 301
 配置向导请参阅系统配置向导 25, 81
 批量添加
 用户 99
 组 99
 票证 142
 登录标记 141
 用于分布式安全 142
 平台搜索 586, 688

Q

QaaWS 498
 Query as a Web Service 61
 企业资源规划 (ERP) 38
 启用
 服务器 353
 轻量级目录访问协议请参阅 LDAP 223
 趋势, 定义 625
 趋势数据库 627
 趋势数据库, 迁移 630
 趋势数据库模式图 986
 趋势图 625
 取消映射角色 312, 340
 全局系统量度 368
 权利系统 282
 权限 112, 341, 878
 BI 工作区 895
 BI 启动板 555, 894
 CMC 555, 893
 Crystal 报表 884
 Desktop Intelligence 文档 882
 Explorer 905

权限 (续)

- Mobile 907
- Universe (.unv) 887
- Universe (.unx) 889
- Universe 连接 891
- Universe 设计工具 902
- Web Intelligence 899
- Web Intelligence 文档 884
- 安全性查询 123, 124
- 报表应用程序服务器 366
- 查看 121
- 查看与按需查看 128
- 常规 878
- 顶层文件夹 123
- 发布权限 342
- 访问级别 112, 887
 - 复制的 132
 - 关系查询 131
 - 跨站点管理 132
 - 任务 126
 - 修改包含的权限 130
- 分配到主体 122
- 服务器 365
- 服务器组 365
- 高级权限 113, 122
- 管理 121, 134, 137
- 管理安全性 710, 711, 712, 713, 714
- 管理权限 341
- 继承 114
 - 文件夹 115
 - 终止 133
- 组 114
- 警报 904
- 类别 881
- 权限
 - 复制 710, 711, 712, 713, 714
- 权限覆盖 116
- 权限作用域 118
- 收件箱 104
- 所有者权限 137
- 特定于类型 118
- 微件 904
- 文件夹 880
- 限制作用域 118
- 信息设计工具 903
- 应用程序 555
- 用户 103, 885
- 有效权限 120
- 战略生成器 901
- 注释 883
- 组 103, 885
- 权限资源管理器 121
- 权限作用域 118
- 群集 357, 359
 - 查看详细信息 368

群集 (续)

- 更改名称 361
- 节点 357
- 添加 CMS 358
- 群集定义传输 769, 775
- 群集定义工具 769, 775
- 群集密钥 150
 - Dbinfo 文件 150
 - Unix 上重置 152
 - 概述 150
 - 在 Windows 上重置 151
- 群集支持 644, 686

R

- RAM 82
- restart.sh 849
- RESTful Web 服务 443
- RESTful Web 服务管理
 - TrustedPrincipal.conf 451
 - web.xml 450
- 会话池 447
- 会话池超时 447
- 会话池大小 447
- 命令行选项 445
- 配置基本 URL 444
- 启用错误消息堆栈 445
- 设置会话标记超时值 446
- 设置默认页面大小 446
- 受信任的身份验证的命令行选项 452
- RestoreCluster.bat 479
- restorecluster.sh 479
- RFC 目标 755
 - 用于 BW 发布者服务 755
 - 用于本地 SAP 网关 756
- RMI 协议 635
- 热备份 462, 466, 467
- 日志记录 842
 - 跟踪 823
 - 级别, 跟踪日志 556, 823
- 日志文件 84, 85
- 容量, 系统配置向导 82
- 软件开发工具包 (SDK) 34

S

- SAML
 - SSO 214
- SAP
 - 防火墙配置 187
 - 更新别名 289
 - 更新角色 289
 - 集成 39
- SAP Business Explorer 590

- SAP BusinessObjects Analysis (Microsoft Office 版) 65
- SAP BusinessObjects Business Intelligence 平台
 - Web 应用程序容器服务器 (WACS) 421
 - 文档 20
- SAP BusinessObjects Business Intelligence 平台服务器
 - 配置 Kerberos 和浏览器 435
- SAP BusinessObjects Business Intelligence 平台微件 63
- SAP BusinessObjects Dashboards 66
- SAP BusinessObjects Explorer 66, 575
 - 管理设置 575
 - 应用程序属性 575
- SAP BusinessObjects Mobile 70
- SAP BusinessObjects SDK 147
- SAP BusinessObjects Web Intelligence 69
- SAP Crystal Reports 66
- SAP ERP 38
- SAP HANA
 - 配置 SSO 237, 595
- SAP HANA 数据库
 - 为 CMS 选择 414
- SAP Jam
 - 权限 895
- SAP Jam 集成
 - 简介 577
 - 先决条件 577
- SAP Passport 842
- SAP Solution Manager 39
 - SLD 836
 - SMD 838
 - 概述 834
- SAP StreamWork
 - 权限 895
- SAP StreamWork 集成
 - 简介 577
 - 先决条件 577
- SAP 身份验证 280
 - CMC 选项 284
- SAP 网关 301
 - 安装 756
 - 分布组件 754
 - 和 SNC 301
 - 使用本地发布 755
- SAPGENPSE 298
- SCRIPTDIR 20
- SDK
 - 平台搜索 685
- serverconfig.sh 847, 848
 - 节点
 - 重命名 395

- serverconfig.sh (续)
 - 节点 (续)
 - 重新创建 390
 - 删除 393
 - 添加 387
 - 移动 398
- setup.sh 849
- setupinit.sh 849
- Siebel Enterprise 38
- Siebel 集成
 - Crystal Reports 菜单项, 创建 816
 - 集成项目 816
 - 配置防火墙 192
 - 重新编译 Siebel 应用程序 [充新编译 Siebel 应用程序] 817
- SiteMinder
 - BOE war 配置 233
 - Windows AD 273
 - 错误 233
 - 配置 LDAP 插件 232
 - 设置 LDAP 单一登录 232, 273
 - 疑难解答 233
- SMAAdmin 帐户 839
- SMD 838
 - SMD 代理 838
- SNC
 - 请参阅安全网络通信 291
- Solution Manager 625
 - SMAAdmin 帐户 839
- SPN 实用程序 245
- SQL Anywhere
 - 创建 odbc.ini 383
- SQL Anywhere 数据库
 - 为 CMS 选择 413
- SSL 158, 162, 164
 - sslconfig.exe 164
 - 报表转换工具 166
 - 翻译管理工具 165
 - 密钥 158, 159
 - 胖客户端 164
 - 配置 Web 应用程序容器服务器 (WACS) 429, 431
 - 配置服务器 158, 162, 164
 - 证书 158, 159
- SSL. 请参阅安全套接字层 (SSL) 223
- sslc.cnf 158
- sslc.exe 158
- startservers 848
- stopservers 849
- Subversion 39, 494
- Subversion 内容 497
- Subversion 设置 495
- Subversion 升级 497
- syslog 369
- 删除 417, 418, 503
 - CMS 系统数据库 417, 418
 - Universe 623
 - Universe 连接 622
 - Web 应用程序容器服务器 (WACS) 427
 - 别名 110
 - 访问级别 130
 - 服务器 357
 - 文件夹 510
 - 用户帐户 96
 - 组 99
 - 作业实例 504
- 上下文感知 818
 - 配置 818, 820
- 设置
 - 回滚过程 504
 - 作业实例 504
- 身份验证 37
 - Enterprise 209, 500
 - LDAP 223, 224, 500
 - Web 应用程序容器服务器 (WACS) 433
 - Windows AD 244, 500
 - 安全插件 207
 - 类型 93
 - 受信任的身份验证 212
 - 主要 206
- 审核 498
 - CMC 页 653
 - Web Intelligence 事件 679
 - Web 活动 145
 - 分析器事件 680
 - 公共事件 669
 - 量度 653
 - 配置 653
 - 平台事件 677
 - 审核数据存储
 - 模式表 977
 - 模式图 976
 - 生命周期管理控制台事件 681
 - 事件
 - 列表 659
 - 配置 654
 - 属性和详细信息 659
 - 数据库保持 657
 - 事件类型 669
 - MDAS 多维数据集连接 680
 - MDAS 会话 680
 - VMS 导出 681
 - VMS 检索 681
 - VMS 签出 681
 - VMS 签入 681
 - VMS 取消锁定 681
 - VMS 锁定 681
 - VMS 添加 681
- 审核 (续)
 - 事件类型 (续)
 - 超范围钻取 679
 - 回滚 681
 - 检索的页面 679
 - 权限修改 677
 - 审核修改 677
 - 自定义访问级别已修改 677
 - 事件类型 ID 669, 677, 679, 680, 681
 - 事件类型: 保存 669
 - 事件类型: 编辑 669
 - 事件类型: 查看 669
 - 事件类型: 触发 669
 - 事件类型: 传送 669
 - 事件类型: 创建 669
 - 事件类型: 登录 669
 - 事件类型: 检索 669
 - 事件类型: 删除 669
 - 事件类型: 搜索 669
 - 事件类型: 提示 669
 - 事件类型: 修改 669
 - 事件类型: 运行 669
 - 事件类型: 注销 669
 - 事件属性 669, 679, 680, 681
 - 事件详细信息 669, 677, 679, 680, 681
 - 事件详细信息 ID 669, 677, 679, 680, 681
 - 数据库连接设置 657
 - 体系结构 648
 - 信息流 648
 - 状态摘要 653
 - 审核日志文件 466
 - 审核数据库 466
 - 审核数据库, 迁移 Derby 数据库到 630
 - 审核文件 84
 - 升级 40, 497, 498
 - 升级 Subversion 内容 497
 - 升级管理 501
 - 升级管理的命令行选项 531
 - 升级管理工具 26, 65
 - 升级管理文件夹 500
 - 升级管理应用程序访问权限 499
 - 升级命令行选项 531
 - 升级选项 517
 - 升级作业 521
 - 使用 BIAR 文件 519
 - 资源库连接时 517
 - 升级作业页面 509
 - 实例共享 738, 739, 740
 - 实时数据 128
 - 使用 WDeploy 的 OpenSearch 687
 - 事件服务器 912
 - 命令行选项 864

- 事件日志 369, 404
- 视图 36
- 收件箱
 - 控制访问 104
- 受信任的身份验证 212, 609
 - SAML 214
 - 示例配置 219
 - 属性 216
 - 用户主体 221
- 授权
 - BI 平台中的权限 752
 - 内容管理工作台 758
 - 信息平台服务 281
 - 应用 782
 - 用于 SAP 数据访问 782
- 输出文件存储 84
- 输出文件资源库 23, 40, 912
- 输入文件存储 84
- 输入文件资源库 23, 40, 912
- 属性, 登录标记 141
- 数据
 - 保存的 128
 - 实时 128
- 数据安全
 - FIPS 兼容模式 148
 - 概述 147
 - 加密 150
 - 加密密钥 150
 - 两密钥加密 147
 - 默认数据处理模式 148
 - 群集密钥 150
 - 向后兼容性 148
- 数据访问
 - 安装概述 769
- 数据库 32
 - SAP HANA 数据库 414
 - SQL Anywhere 数据库 413
 - Uiverse 36
 - 初始化 CMS 417, 418
 - 单一登录访问 209
 - 视图 36
 - 为 CMS 选择 415, 416
- 数据库, 迁移 Derby 630
- 数据联合管理工具 63
- 数据文件 84
- 数据源连接 622
- 刷新模式选项, 对于联盟 714, 715
- 双向复制 714, 715
- 搜索 568, 692
 - 讨论线索 568
- 搜索参数 513
- 搜索选项 513
- 搜索依赖项 516, 517
- 所有者权限 137

T

- Tomcat
 - JAAS 256
 - Kerberos 254
- 探测器 625, 986
- 讨论区
 - 管理设置 567
- 讨论线索 568
 - 对搜索结果进行排序 569
 - 取消搜索 568
 - 搜索 568
- 套接字超时 744
- 特定权限
 - BI 工作区 895
- 特定于类型的权限 118
 - BI 启动板 894
 - CMC 893
 - Crystal 报表 884
 - Desktop Intelligence 文档 882
 - Uiverse (.unv) 887
 - Uiverse (.unx) 889
 - Uiverse 连接 891
 - Uiverse 设计工具 902
 - Web Intelligence 899
 - Web Intelligence 文档 884
 - 访问级别 887
 - 警报 904
 - 类别 881
 - 微件 904
 - 文件夹 880
 - 信息设计工具 903
 - 用户 885
 - 战略生成器 901
 - 注释 883
 - 组 885
- 体系结构 29, 627
 - 平台搜索 692
- 体系结构层 31
- 添加 357
 - CMS 358
 - 服务器 354
 - 群集成员 357
 - 用户到组 100
 - 主机系统 503
 - 子组 98
- 添加 InfoObject 514
- 添加 Web 服务 509
- 添加对象 519
- 调优和大小调整 82
- 通信 206
 - BI 平台服务器之间 167
 - 在浏览器和 Web 应用程序服务器之间 206
- 通知 627
- 通知传送 986

- 同步报表信息 764, 765
- 统计数据, 审核 Web 活动 145
- 图, 组件 30
- 托管的对象 315
 - BI 平台组 315, 319
 - PeopleSoft 角色 315, 319
 - Uiverse 315, 319
- 拓扑量度 625

U

- Uiverse 36, 516
 - 复制 718
 - 管理 623
 - 权限 (.unv) 887
 - 权限 (.unx) 889
- Uiverse Designer: 请参见 Uiverse
- 设计工具 61
- Uiverse 对象安全性 890
- Uiverse 连接
 - 复制 718
 - 管理 622
 - 权限 891
 - 删除 622
- Uiverse 设计工具 61
- Uiverse 设计工具, 权限 902
- Unix
 - syslog 369
- Unix 脚本, 概述 843

V

- Voyager 70
- Voyager: 请参见 SAP
- BusinessObjects Analysis 65

W

- WAR 文件
 - BI 平台 Web 应用程序 193, 194
 - BOE 194, 598, 599, 601, 603
 - BOE WAR 文件
 - BI 启动板属性 601
 - CMC 属性 605
 - OpenDocument 属性 603
 - 全局属性 599
 - dswebobje 194
- WDeploy 67
- Web Intelligence 571, 858
 - 查询 HTML 访问权限 571
 - 处理服务器 861
 - 权限 899
 - 应用程序权限 571
 - 自定义界面 609
- Web Intelligence 处理服务器 23, 40

Web Intelligence 胖客户端 60
 Web Intelligence 文档
 权限 884
 Web 服务 509
 从 Web 应用程序容器服务器中删除 428
 反向代理服务器的配置 199, 200
 会话变量 736
 添加到 Web 应用程序容器服务器 428
 文件高速缓存 736, 737
 自定义部署 736, 738
 Web 服务器
 保护安全 144
 Web 客户端 59
 Web 应用程序服务器 33
 身份验证 206
 Web 应用程序容器服务器 (WACS)
 33, 912
 AD Kerberos 438
 CMC 服务 421
 HTTPS 429, 431, 455
 JAAS 文件 436
 Kerberos 配置文件 435
 SSL 429, 431
 安装 425
 常见任务 422
 创建新服务器 426
 防火墙 455
 服务器错误 457
 负载平衡 454
 概述 421
 更改内存设置 459
 恢复系统默认值 460
 解决端口冲突 458, 459
 克隆 426
 连接器 421
 量度 958
 删除 424, 427
 删除 Web 服务 428
 属性 461
 添加 424
 添加 Web 服务到 428
 系统量度 457
 疑难解答 457
 与代理服务器配合使用 454, 455
 与其他 Web 服务器配合使用 453
 在多宿主计算机上 456
 WebLogic
 JAAS 配置文件 256
 Java 选项 260
 Kerberos 254
 WebSphere
 JAAS 257
 Java 选项 261
 WinAD 500

Windows
 服务器依赖项, 添加 404
 事件日志 369
 Windows AD
 Vintela 267, 268
 安全插件 246
 单一登录 265, 267, 268
 服务帐户 265
 启用 Kerberos 433, 434
 身份验证 244
 映射 LDAP 236
 帐户和组 250
 计划更新 250
 Windows 脚本, 概述 850
 完全回滚 523
 网络地址转换
 配置, 服务器 hosts 文件 178
 网络环境
 IPv4
 双 IPv4/IPv6 节点 374
 IPv6 374
 网络接口
 疑难解答 (针对多个) 378
 网络接口疑难解答 379
 微件
 管理设置 574
 权限 904
 委派的管理 134
 概述 560
 用户组 564
 文件夹
 创建 510
 对象权限
 继承 115
 权限 880
 文件夹, 系统配置向导 84
 文件夹继承 115
 权限覆盖 116
 文件系统
 备份 466
 文件资源库服务器 23, 40, 912
 备份 466
 命令行选项 863

X

Xcelsius请参见 SAP BusinessObjects
 Dashboards 66
 系统备份 462, 466
 系统架构目录 (SLD) 39
 connect.key 文件 836
 触发器 837
 验证注册 837
 注册 836

系统量度, 查看
 Web 应用程序容器服务器 (WACS) 457
 系统量度值, 查看 368
 系统配置向导 25, 81
 系统帐户 281
 限制 146
 Guest 帐户 146
 登录 146
 密码 145
 权限作用域 118
 用户 146
 相似性, 和 SSL 142
 响应时间 625
 响应文件 85, 86, 316
 创建 316
 应用 318
 向导 25
 向导, 系统配置 81
 协作
 权限 895
 协作应用程序集成
 简介 577
 先决条件 577
 信号处理 854
 信任, 活动信任关系 141
 信任让渡 142
 信息平台服务
 创建帐户 281
 发布权限 342
 管理权限 341
 信息设计工具 62
 信息设计工具, 权限 903
 性能 82, 625
 负载平衡 142
 群集 357
 性能建议 814
 修改作业 514
 许可密钥 90
 查看 89
 概述 89
 购买 89
 和 CMS 数据库迁移 419
 添加 90
 选项卡访问, CMC
 概述 560
 管理为其他用户或用户组进行配置
 的权限 564
 权限, 继承 563
 为其他用户管理 561, 562
 限制 566
 疑难解答 566
 自定义 565
 选择产品 81
 选择对象依赖项 516

组 (续)

- 将访问权授予 103
- 将权限分配给 122
- 将用户添加到 100
- 默认 92
- 权限 885
 - 继承 114
 - 权限覆盖 116
 - 在顶层文件夹上 123
- 终止继承 133
- 删除 99

组 (续)

- 添加, 批量 99
- 添加子组 98
- 修改 97
- 映射 310, 326, 331, 337
- 指定组成员资格 98
- 组件 769, 775
 - 群集定义工具 769, 775
- 组件图 30
- 作业
 - 编辑 514

作业 (续)

- 搜索 513
- 修改 514
- 作业历史记录
 - 查看 523
- 作业设置 504
- 作业实例
 - 删除 504
 - 设置 504
- 作业相关的过程 509