CA Access Control for Virtual Environments

集成指南

r2.0

第三方通知

包含 AIX(TM)、Java(TM) 2 技术版、1.4 版模块的 IBM(R) 32 位运行时环境

示例脚本和示例 SDK 代码

CA Access Control 产品随附的示例脚本和示例 SDK 代码均“按原样”提供，仅供参考之用。 在特定环境下，可能需要对它们进行调整，而且在生产系统中部署它们之前，未经事先测试和验证不应将其用于生产。

CA Technologies 不向这些示例提供支持，而且对于这些脚本可能会引起的任何错误概不负责。

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA Access Control 企业版
- CA Access Control
- [assign the value for UARM in your book]
- Identity Manager

文档约定

CA Access Control 文档使用以下约定：

格式	含义
等宽字体	代码或程序输出
斜体	重点或新术语
粗体	必须完全按照显示内容键入的文本
正斜杠 (/)	用于描述 UNIX 和 Windows 路径的独立于平台的目录分隔符

文档在解释命令语法和用户输入（以等宽字体显示）时还会使用以下特殊约定：

格式	含义
斜体	您必须提供的信息
用方括号括起来 ([])	可选运算符
用大括号括起来 ({})	强制运算符集
用管道符 (|) 分隔的选项。	分隔可选运算符（选择一项）。 例如：下面的示例*既*可以表示用户名，*也*可以表示组名： `{username|groupname}`
...	指明前面的项或项组可以重复
下划线	默认值

格式	含义
前面带空格的行尾反斜杠 (\)	有时，在本指南中，一行无法容纳一个命令。 在这些情况下，行结尾处的空格加上反斜杠 (\) 就表示该命令延续到下一行。 **注意：**请勿复制反斜杠字符，并且请省略换行符。 这些不是实际命令语法的一部分。

示例：命令表示法约定

下面的代码说明了在本指南中使用命令约定的方式：

```
ruler className [props({all|{propertyName1[,propertyName2]...})]
```

在该示例中：

- 命令名称 (ruler) 以常规等宽字体显示，必须按照显示内容键入。
- *className* 选项以斜体显示，因为它是一个类名（例如 USER）的占位符。
- 即使不带有方括号中的第二部分，您也可以运行该命令，方括号表示该运算符是可选的。
- 使用可选参数 (props) 时，可以选择关键字 *all*，也可以指定一个或多个属性名（以逗号分隔）。

文件位置约定

CA Access Control 文档使用以下文件位置约定：

- *ACVEInstallDir*—默认 CA Access Control for Virtual Environments 安装目录：
  - /opt/CA/AccessControlServer/VirtualAppliance
- *ACInstallDir*—默认 CA Access Control 安装目录。
  - [set the alternate Installation Path variable]
- *ACSharedDir*—CA Access Control for UNIX 使用的默认目录。
  - /opt/CA/SharedComponents
- *ACServerInstallDir*—默认 CA Access Control 企业管理 安装目录。
  - /opt/CA/AccessControlServer
- *JBoss_HOME*—默认 JBoss 安装目录。
  - /opt/jboss-4.2.3.GA

联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

目录

第 1 章： 简介

此部分包含以下主题：

关于本指南

本指南提供有关如何计划、配置和将 CA Access Control for Virtual Environments 与 CA 和第三方产品集成方面的信息。 而且，本指南提供有关如何为高可用性和灾难恢复计划和配置 CA Access Control for Virtual Environments 的信息。

第 2 章： 与 ObserveIT Enterprise 集成

此部分包含以下主题：

关于 ObserveIT 集成

CA Access Control for Virtual Environments 与 ObserveIT Enterprise 的 集成可扩展您对由特权帐户针对您组织中的服务器进行访问尝试的控制。 ObserveIT Enterprise 会话记录软件会记录目标系统上的用户活动。 记录在用户签出特权帐户密码并登录到端点的时刻开始。 记录在会话终止（例如，用户签入特权帐户密码时）时结束。

已纪录的会话存储在您准备的专用数据库中。 您可以使用 ObserveIT 查看器，从 CA Access Control 企业管理 直接重放已纪录的会话。

您可以从以下链接中的 ObserveIT 系统获取 ObserveIT Enterprise 会话记录程序：

http://www.observeit-sys.com/download.asp

您可以在下列链接中找到 ObserveIT Enterprise 文档：

https://support.ca.com/cadocs/

注意：有关 ObserveIT 的更多信息，请参阅位于 ObserveIT Enterprise 安装介质上的 ObserveIT 文档。

如何设置该集成

执行几个步骤将 CA Access Control for Virtual Environments 与 ObserveIT Enterprise 会话记录软件集成。 在集成的结尾，ObserveIT 会记录所有 PUPM 会话。

注意：有关如何完成步骤 1 - 5 的更多信息，请参阅 ObserveIT 安装介质上的 ObserveIT Enterprise 文档。

完成以下步骤：

1. 查看 ObserveIT Enterprise 系统和安装要求。

   确认您使用的服务器满足安装 ObserveIT Enterprise 的最低系统要求。

2. 准备中央数据库

   已纪录的会话存储在专用的 Microsoft SQL Server 上。

3. 配置 Internet Information Server (IIS)。

   ObserveIT Enterprise 应用程序服务器使用 IIS 来处理代理发送的元数据。

4. 安装 ObserveIT Enterprise 服务器组件。

   ObserveIT 应用程序服务器、代理和管理控制台也进行安装。

5. 配置 ObserveIT Enterprise 应用程序服务器。

   配置记录设置。

6. 在企业管理服务器上部署会话记录脚本。

   脚本会启用触发会话记录的 PUPM 自动登录。

7. 创建服务帐户。

   创建要使用的企业管理服务器服务帐户

8. 定义到 CA Access Control 企业管理 中的 ObserveIT Enterprise 应用程序服务器的连接。

   配置连接设置来启用会话记录。

如何准备集成

在完成 ObserveIT Enterprise 应用程序服务器的安装后，准备用于 CA Access Control for Virtual Environments 集成的服务器。 在准备 ObserveIT Enterprise 应用程序服务器后，服务器已配置为开始记录和保存 PUPM 会话。

完成以下步骤：

1. 打开管理控制台。
2. 创建服务帐户。

   CA Access Control for Virtual Environments 使用服务帐户连接到 ObserveIT Enterprise 应用程序服务器。

打开管理控制台

在安装和开始 ObserveIT Enterprise 之后，您可以启动基于 Web 的管理控制台。

打开管理控制台

1. 使用浏览器打开 ObserveIT Enterprise 管理控制台。 输入以下 URL：

   http://observeit_server_name:port/ObserveIT

   示例：

   http://observeit_server:4884/ObserveIT

2. 使用您在安装过程中指定的管理员凭据进行登录。

   此时打开 ObserveIT Enterprise 管理控制台。

注意：您也可以通过依次单击“开始”、“程序”、“ObserveIT”、“ObserveIT WebConsole”打开 ObserveIT Enterprise 管理控制台。

创建服务帐户

CA Access Control 企业管理 使用服务帐户来验证 ObserveIT Enterprise 应用程序服务器以便记录用户活动。 当在 CA Access Control 企业管理 中配置 ObserveIT Enterprise 应用程序服务器连接设置时，提供服务帐户凭据。

创建服务帐户

1. 在 ObserveIT Enterprise 管理控制台中，依次选择“配置”、“控制台用户”。

   此时打开控制台用户屏幕。

2. 选择“创建用户”。

   此时打开“添加控制台用户”窗口。

3. 输入用户名、密码，然后确认密码。
4. 将身份验证方法设为“ObserveIT.Authentication”，将用户角色设为“Admin”。
5. 单击“添加”。

   服务帐户即被创建。

注意：有关用户管理的更多信息，请参阅位于 ObserveIT Enterprise 安装介质上的 *ObserveIT 文档*。

部署会话记录脚本

用户会话记录与 PUPM 自动登录协同工作。 当用户签出特权帐户密码并选择登录到端点时，会打开一个远程管理软件并自动让用户登录。 CA Access Control 企业管理 通过使用基于端点类型的会话记录脚本来控制远程管理程序。

例如，当用户选择登录到 Windows 端点时，CA Access Control 企业管理 使用的脚本会打开远程桌面软件来连接到端点。

要记录 ObserveIT Enterprise 应用程序服务器上的会话，您要在企业管理服务器上部署会话记录脚本。

部署会话记录脚本

1. 从 CA 支持网站中下载会话记录脚本，并将其保存在临时目录中。
2. 在企业管理服务器上，导航到以下目录，其中 *JBoss_HOME* 指定了安装 JBoss 的目录：

   JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/sso_scripts

3. 将会话记录脚本复制到 sso_scripts 目录。

   建议您在覆盖该目录中的文件之前先进行备份。

4. 选择使用新文件覆盖现有文件。

现在，您可以配置到 ObserveIT Enterprise 应用程序服务器的连接设置。

定义到 ObserveIT 的连接

为了完成与 ObserveIT Enterprise 的集成，您配置 CA Access Control 企业管理 中到 ObserveIT Enterprise 应用程序服务器的连接设置。

定义到 ObserveIT 的连接

1. 在 CA Access Control 企业管理 中，依次选择“系统”、“连接管理”、“会话记录”、“创建连接”。

   将显示“创建连接”屏幕。

2. 输入以下详细信息：

   连接说明

   定义连接的自由文本说明

   播放 URL

   定义 ObserveIT Enterprise 应用程序服务器 URL

   示例：http://observeit_host:4884/observeit/

   用户 ID

   定义服务帐户用户名

   密码

   定义服务帐户密码

   高级

   指定以下高级连接设置：

   查看器页面

   指定是否显示一条消息，表示该会话记录在屏幕的顶端

   查看器参数

   指定 ObserveIt 查看器窗口的宽度和高度

ActiveX URL

指定 ObserveIT Enterprise ActiveX 文件所在位置的完整路径名。 默认情况下，指定到 ObserveIT 应用程序服务器的 URL。

示例：
http://observeit_host:4884/ObserveIT/AgentInstall/Agent.cab#version=1,0,0,0

服务器 URL

指定 ObserveIT Enterprise 应用程序服务器存储已纪录会话的位置的完整路径名。默认情况下，指定到 ObserveIT 应用程序服务器的 URL。

示例： http://observeit_host:4884/ObserveITApplicationServer

3. 单击“提交”。

CA Access Control 企业管理 将创建连接。

第 3 章： 记录 PUPM 会话

此部分包含以下主题：

如何记录会话

每个 PUPM 会话都被记录下来并存储在 ObserveIT Enterprise 数据库上。每个会话都被分为单个的片段，您可以从整个纪录的会话中分别播放。

以下过程说明了如何记录 PUPM 会话：

1. 用户从 CA Access Control 企业管理 中签出特权帐户密码，并选择自动登录到端点。

   如果这是首次使用该选项，用户需要安装 ActiveX。
2. 此时打开一个远程管理会话，而用户无需输入密码即可登录。
3. 安装在端点上的 ObserveIT 代理开始记录用户活动，并将片段发送到 ObserveIT Enterprise 应用程序服务器，该服务器将数据保存在数据库中。
4. 用户关闭远程管理会话，而 ObserveIT 代理也停止记录。
5. 已纪录的会话在 CA Access Control 企业管理 中显示。

重要说明！ 要使 Internet Explorer 能够下载 ActiveX，请在“本地 Intranet 区域”或“受信任区域”中指定 ObserveIT Enterprise 主机名，然后将“下载已签名的 ActiveX 控件”安全选项设为“启用”。

注意：有关会话记录的更多信息，请参阅位于 ObserveIT Enterprise 安装介质上的 *ObserveIT 文档*。

记录会话的位置

ObserveIT Enterprise 应用程序服务器将 PUPM 会话记录到专用的 Microsoft SQL Server 上。 ObserveIT 数据库服务器使用两个专用的数据库。 第一个数据库命名为 ObserveIT，承载着配置和元数据。 第二个数据库命名为 ObserveIT_Data，存储 ObserveIT 代理在已纪录会话期间收集的快照。

注意：有关会话记录的更多信息，请参阅位于 ObserveIT Enterprise 安装介质上的 *ObserveIT 文档*。

播放会话

从 CA Access Control 企业管理 播放已纪录的 PUPM 会话。 当选择播放会话时，CA Access Control 企业管理 在新窗口中播放已纪录的会话。 播放器窗口中包含用来导航该会话的控制按钮。 您还可以在已纪录的会话中执行自由的文本搜索。

注意：有关自由文本搜索的更多信息，请参阅位于 ObserveIT Enterprise 安装介质上的 *ObserveIT 文档*。

播放会话

1. 在 CA Access Control 企业管理 中，依次选择“特权帐户”、“审核子任务”。

   此时“审核特权帐户”任务显示在可用任务的列表中。

2. 选择“审核特权帐户”

   此时打开“审核特权帐户”搜索窗口。

   注意：确认已为您分配了 PUPM 审核管理员角色。

3. 指定搜索标准、输入要显示的行数，然后单击“搜索”。

   将显示满足您搜索标准的任务。

4. 单击会话详细信息列中的播放图标可播放该会话。

   此时打开播放器窗口，从会话的开头播放该会话。

   注意：使用窗口底部的控件可导航该会话。

第 4 章： 实施企业报告

此部分包含以下主题：

企业报告功能

CA Access Control 企业管理 通过 CA Business Intelligence 公用报告服务器（CA Access Control 报告门户）提供报告功能。 通过企业报告，您可以从一个中央位置查看每个端点（用户、组和资源）的安全状态。 CA Access Control 报告介绍了每个端点上用于确定哪些用户可以执行哪些操作的规则和策略以及所有策略偏差。

配置完成后，CA Access Control 企业报告可以独立运行，它连续从每个端点收集数据并将信息存储在中央服务器中，无需手工干预。 可以排定或根据需要从每个端点收集数据。 无需连接到每个端点找出谁有权访问哪项资源。 无论收集服务器处于启动还是关闭状态，每个端点均会报告其状态。

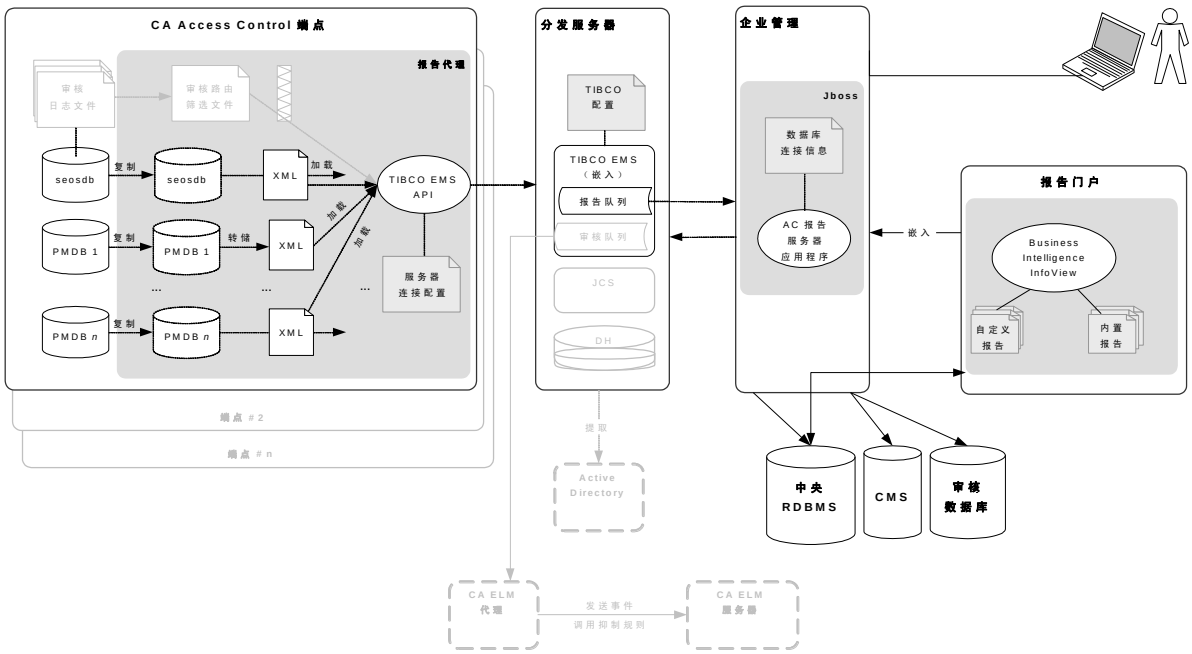
报告服务体系结构

CA Access Control 报告服务可为 CA Access Control 企业报告提供基于服务器的平台。 您可以使用此平台创建包含所有 CA Access Control 端点数据的报告。 可以通过启用了 Web 的应用程序来查看和管理创建的报告。

通过报告服务，您可以在现有 CA Access Control 基础结构的顶层构建报告环境。

注意：有关企业报告的详细信息，请参阅*《企业管理指南》*。

下图显示了报告服务组件的体系结构。 该图还显示了组件之间的数据流。



上图说明了以下内容：

- 每个包含 CA Access Control 数据库 (seosdb) 和任意数量的策略模型 (PMDB) 的端点均已安装报告代理组件。
- 报告代理从端点收集数据，并将数据发送到分发服务器进行处理。
- 在简单的企业模型中，一个分发服务器处理所有端点数据并将其发送至中央数据库进行存储。 您也可以复制分发服务器组件，用于在大型企业环境中进行容错以及更快地进行处理。
- 中央数据库 (RDBMS) 存储端点数据。
- 通过报告门户，您可以访问中央数据库中的数据以生成内置报告，或查询数据以生成自定义报告。

如何设置报告服务服务器组件

要使用企业报告，请安装和配置 CA Access Control 报告服务服务器组件。 安装和配置服务器组件之后，在每个端点上配置报告代理。

注意：报告代理安装和配置是 CA Access Control 和 [assign the value for unab in your book] 端点安装的一部分，不包含在该过程中。

要设置报告服务服务器组件，请执行以下步骤：

1. 如果尚未安装和配置企业管理服务器，请执行此操作。
2. 设置报告门户计算机 (CA Business Intelligence)。

   您可以在 CA Support 网站上找到 CA Business Intelligence 安装文件。
3. 在报告门户上部署 CA Access Control 报告数据包。
4. 配置到 CA Business Intelligence 的连接。
5. 创建快照定义。

   您现在可在 CA Business Intelligence 和 CA Access Control 企业管理 中生成和查看报告。

注意：有关生成和查看报告的详细信息，请参阅*《企业管理指南》*。

如何设置报告门户计算机

通过报告门户，您可以访问 CA Access Control 企业管理 存储在中央数据库中的端点数据以生成内置报告，或查询数据以生成自定义报告。 报告门户使用 CA Business Intelligence。

注意：如果已拥有旧版本的报告门户或 CA Business Intelligence 或 [assign the value for boe in your book] XI 的独立安装，则可以使用现有安装而无需升级。

重要说明！ 如果您使用 Oracle Database 11g，请安装 CA Access Control 企业版 报告门户（光盘 2）DVD 的 \boeXIR2_SP5 目录下提供的 BusinessObjects XI Release 2.1 SP5 修补程序。

要设置报告门户，请执行以下操作：

1. 如果使用 Oracle 数据库，请在报告门户计算机上安装完整的 Oracle 客户端。
2. 如果尚未设置，请设置中央数据库和分发服务器。

   注意：在安装企业管理服务器时，设置中央数据库和分发服务器。
3. (UNIX) 如果报告门户计算机是 Solaris 或 Linux 计算机，请为 CA Business Intelligence 安装准备 UNIX 计算机 (p. 24)。
4. 同步报告门户计算机和企业管理服务器的系统时间。

   如果不同步系统时间，CA Access Control 企业管理 生成的报告将一直处于挂起或重复状态。
5. 为操作系统安装 CA Business Intelligence。

   您可以在 CA Access Control 企业版 报告门户光盘上找到 CA Business Intelligence 安装文件。

   注意：默认情况下，Windows 报告门户使用 Microsoft SQL Server 身份验证来验证连接。 如果要使用域用户账户设置进行身份验证，您可以将报告门户配置为在 Windows 身份验证中运行 (p. 31)。

   报告门户已设置，您现在可以部署 CA Access Control 报告数据包。

注意：有关 CA Business Intelligence 的详细信息，请参阅 CA Technologies 支持提供的 *《CA Business Intelligence 安装指南》*。

示例：在 Windows 上安装 CA Business Intelligence

以下过程说明了如何在 Windows 上安装 CA Business Intelligence：

注意：安装大约要花费 1 小时才能完成。

1. 将 CA Access Control 企业版 Report Portal for Windows DVD 插入光盘驱动器中。
2. 导航到 \Disk1\InstData\VM 文件夹并双击 install.exe。

   将启动 CA Business Intelligence 安装向导。

3. 使用下表完成该安装向导：

信息	操作
安装语言	选择要使用的支持的安装语言，然后单击“确定”。 **注意：**要使用任何支持的非英语语言进行安装，需要使用已本地化的操作系统。
许可协议	选择“我接受本许可协议的条款”，然后单击“下一步”。
安装类型	选择“典型安装”，然后单击“下一步”
非 Root 凭据	输入非 root 用户名和密码。
BusinessObjects XI 管理员密码	键入两次 P@ssw0rd 以设置和确认密码，然后单击“下一步”。 **注意：**有关密码规则，请参阅 *《CA Business Intelligence 安装指南》*，CA Access Control 企业版 总目录中提供该指南。
Web 服务器配置	单击“下一步”接受默认值。
CMS 数据库设置	输入以下信息，然后单击“下一步”： ■ **MySQL Root 密码:** P@ssw0rd ■ **用户名:** cadbusr ■ **密码:** C0nf1dent1al ■ **数据库名:** MySQL1 **注意：**CA Business Intelligence 中央管理服务器 (CMS) 仅用于内部管理目的。
启用审核	单击“下一步”接受默认值。
审核数据库设置	输入以下信息，然后单击“下一步”： ■ **用户名:** cadbusr ■ **密码:** C0nf1dent1al ■ **数据库名:** MySQL1
查看设置	查看设置，然后单击“安装”来完成安装。

将开始安装，完成该过程最多将花费一小时。

重要说明！ CA Business Intelligence 中央管理服务器 (CMS) 仅用于内部管理目的，并不包含用于生成和显示报告的报告数据。 安装 CA Access Control 企业管理 时定义的报告数据库包含报告代理上传到分发服务器的数据。 有关 CMS 的详细信息，请参阅*《CA Business Intelligence 安装指南》*。

准备 CA Business Intelligence 安装的 Solaris 和 Linux

在 Solaris 或 Linux 上安装 CA Business Intelligence 之前，您必须针对此安装准备计算机。 在准备计算机时，应为 CA Business Intelligence 安装创建非 root 用户，并验证 Oracle RDBMS 是否对 CA Business Intelligence 安装公开，并设置环境变量。

完成以下步骤：

1. 以 root 用户身份登录。
2. 创建非 root 用户。 CA Business Intelligence 安装需要非 root 用户。

   例如：输入以下命令来创建名为 bouser 的用户，该用户属于“other”组：

   ```
   groupadd other
   useradd -d /home/bouser -g other -m -s /bin/bash -c bouser bouser
   passwd bouser
   ```

   出现提示时，为所定义的用户输入并确认密码。
3. (Linux) 确认 LANG 环境变量已配置如下：

   ```
   LANG=en US.utf8
   ```
4. 以创建的非 root 用户身份登录。
5. 输入以下命令以验证 ORACLE_HOME 和 TNS_ADMIN 环境变量是否已正确设置：

   ```
   echo $ORACLE_HOME
   echo $TNS_ADMIN
   ```

   如果输出不为空，则表明这些环境变量有效。 例如：

   ```
   /opt/oracle/app/oracle/product/10.2.0/client_1
   /opt/oracle/app/oracle/product/10.2.0/client_1/admin/network
   ```

   如果命令输出为空，请验证是否针对您创建的非 root 用户设置了这些变量。 例如：按如下所示编辑 /home/bouser/.profile：

   ```
   ORACLE_HOME=/opt/oracle/app/oracle/product/10.2.0/client_1
   export ORACLE_HOME
   TNS_ADMIN=$ORACLE_HOME/network/admin
   export TNS_ADMIN
   ```

6. 确认非 root 用户的 LD_LIBRARY_PATH 包含以下路径：

   ```
   $ORACLE_HOME/lib:$ORACLE_HOME/lib32
   ```

   例如：键入以下命令并在输出中搜索以下路径：

   ```
   echo $LD_LIBRARY_PATH
   ```

   如果这些路径缺失，请将它们添加到 LD_LIBRARY_PATH。 例如：按如下所示编辑 /home/bouser/.profile：

   ```
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib:$ORACLE_HOME/lib32
   export LD_LIBRARY_PATH
   ```

7. 确认 LD_LIBRARY_PATH 和 TNS_ADMIN 中的文件夹是可访问的，如下所示：

   ```
   ls -l $ORACLE_HOME
   ls -l $TNS_ADMIN/tnsnames.ora
   ```

   上述命令不应返回**权限已被拒绝**错误。 如果返回此错误，您必须授予适当的权限。 例如：root/oracle 用户应运行以下命令：

   ```
   chmod -R +xr $ORACLE_HOME
   ```

8. 使用 TNS Ping 实用程序确认 Oracle 连接有效，如下所示：

   ```
   $ORACLE_HOME/bin/tnsping service_name
   ```

   TNS Ping 的输出类似于以下示例：

   ```
   TNS Ping Utility for Solaris: Version 10.2.0.1.0 - Production on 07-MAY-2008
   09:17:02
   版权所有 (c) 1997, 2005, Oracle。  保留所有权利。
   使用的参数文件:
   /opt/oracle/app/oracle/oracle/product/10.2.0/client_1/network/admin/sqlne
   t.ora
   使用了 TNSNAMES 适配器解析别名
   正在尝试连接 (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST
   = 172.16.234.75)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME =
   service_name)))
   OK (30 msec)
   ```

   现在，您可在 Solaris 或 Linux 上安装 CA Business Intelligence。

为 CA Business Intelligence 安装准备 Linux

在 Linux 上安装 CA Business Intelligence 之前，您必须准备计算机。 在准备计算机时，应为 CA Business Intelligence 安装创建非 root 用户并设置环境变量。

注意：确认您使用的 Linux 版本受 CA Business Intelligence 支持。

为 CA Business Intelligence 安装准备 Linux

1. 创建非 root 用户。 CA Business Intelligence 安装需要非 root 用户。

   例如：输入以下命令，以创建名为 bouser 的用户并设置密码：

   ```
   useradd -d /home/bouser -m -s /bin/bash -c bouser bouser
   passwd bouser
   ```

2. 确认 LANG 环境变量已配置如下：

   ```
   LANG=en US.utf8
   ```

报告数据包部署

报告数据包是一个 .BIAR 文件，用于部署 CA Access Control 标准报告。 它包含报告门户的部署构件和描述符集合。 要使用这些标准报告，您需要将报告数据包文件导入 BusinessObjects InfoView。

注意：程序包向后兼容报告门户的以前版本。 您不需要升级报告门户就可以使用最新版本的报告数据包。 您还可以部署已本地化的报告数据包，各程序包均作为独立的 .biar 文件来提供。

在报告门户上部署报告数据包

要使用标准 CA Access Control 报告，请将报告程序包文件导入 BusinessObjects InfoView。

注意：该过程介绍如何在尚未部署程序包的任何先前版本的情况下在报告门户上部署报告数据包。

完成以下步骤：

1. 确认中央数据库、分发服务器和报告门户已设置。

   注意：确认 JAVA_HOME 变量已在报告门户计算机上设置。

2. 将 CA Business Intelligence for Windows DVD 插入光盘驱动器，然后导航到 \Disk1\cabi\biconfig 文件夹。

3. 将 biconfig 目录的内容复制到临时目录。
4. 将适用于您操作系统的 CA Access Control 企业版 Server Components DVD 插入光盘驱动器并导航至 \ReportPackages 文件夹。
5. 将以下文件从光盘复制到同一临时目录：
   - \ReportPackages*RDBMS**import_biar_config*.xml
   - \ReportPackages*RDBMS**AC_BIAR_File*.biar

   RDBMS

   定义用于 CA Access Control 报告的 RDBMS 类型。

   值：Oracle、MSSQL2005

   ***import_biar_config*.xml**

   为 RDBMS 定义导入配置文件 (.xml) 的名称。

   值：import_biar_config_oracle10g.xml、
   import_biar_config_oracle11g.xml、
   import_biar_config_mssql_2005.xml

   注意：如果使用 MS SQL Server 2008 作为中央数据库，请配置 import_biar_config_mssql_2005.xml 文件。

   ***AC_BIAR_File*.biar**

   根据您的语言和 RDBMS 定义 CA Access Control 报告文件 (.biar) 的名称。

   注意：RDBMS 的导入配置文件的 <biar-file name> 属性指向该文件。 默认情况下，该属性被设置为 RDBMS 的英文版名称。
6. 编辑 *import_biar_config*.xml 文件的副本。 定义以下 XML 属性：

   <biar-file name>

   定义 CA Access Control 报告文件 (.biar) 的完整路径名。 您在上一步中复制了该文件。

   <networklayer>

   定义 RDBMS 支持的网络层。

   值 (Windows)：
   - OLE DB—针对 MS SQL Server 身份验证模式。
   - Oracle OCI
   - ODBC—针对 Windows 身份验证模式。

   值 (UNIX)：Oracle CLI

<rdms>

定义用于 CA Access Control 报告的 RDBMS 类型。

值 (Oracle OCI)： Oracle 10 或 Oracle 11

值 (ODBC)： 常规 ODBC 数据源

值 (OLE DB)：MS SQL Server 2005 或*除* Oracle 10 或 Oracle 11 之外的任意值

注意：如果您使用 MS SQL Server 2008，请为该属性指定 MS SQL Server 2005。 有关可为该属性指定的值的详细信息，请参阅 CA Business Intelligence 文档。

<username>

定义您在为企业管理准备中央数据库时所创建的 RDBMS 管理用户的用户名。

<password>

定义您在为企业管理准备中央数据库时所创建的 RDBMS 管理用户的密码。

<datasource>

定义以下项之一：

- (Oracle) 数据库的名称
- （SQL Server 2005 或 2008）您创建的数据库
- (ODBC) 您创建的 DSN

重要说明！ 指定的数据库名称是由 CA Access Control 报告使用而不是由 CA Business Intelligence CMS 使用。

<server>

定义 SQL Server 2005 或 2008 计算机的名称。 对于 Oracle Database 10g、11g 和 ODBC，请将该值保留为空。

7. 请执行下列操作之一：

   - (Windows) 打开命令提示符窗口，然后输入以下命令：

     ```
     System_Drive:\BO\biconfig.bat -h host_name -u user_name -p password -f ac_biar_config.xml
     ```

     host_name

     定义报告门户主机名。

user_name

定义您在安装报告门户时配置的报告门户管理员。

password

定义报告门户管理员的密码。

例如：

```
biconfig.bat -h reportportal.comp.com -u Administrator -p P@ssw0rd -f
C:\BO\import_biar_config_oracle11g.xml
```

- (UNIX) 设置脚本文件 biconfig.sh 的执行权限并执行，如下所示：

  temp_dir/biconfig.sh -h *host_name* -u *user_name* -p *password* -f *ac_biar_config*.xml

  例如：

  ```
  biconfig.sh -h reportportal.comp.com -u Administrator -p P@ssw0rd -f
  /tmp/rp/import_biar_config_orcl.xml
  ```

批处理文件将 CA Access Control 报告导入 InfoView。 导入可能需要几分钟时间才能完成。 日志文件 (biconfig.log) 在与批处理文件相同的文件夹中创建，指示导入是否成功。

示例：Oracle Database 11g 导入配置文件示例

以下代码段是 Oracle Database 11g 的已编辑导入配置文件 (import_biar_config_oracle11g.xml) 的示例：

```
<?xml version="1.0"?>
<biconfig version="1.0">
  <step priority="1">
    <add>
      <biar-file name="c:\temp\AccessControl_R12.5_EN_ORCL_22_JUN_2009.biar">
        <networklayer>Oracle OCI</networklayer>
        <rdms>Oracle 11</rdms>
        <username>root</username>
        <password>P@ssw0rd</password>
        <datasource>orcl</datasource>
        <server></server>
      </biar-file>
    </add>
  </step>
</biconfig>
```

示例： Microsoft SQL Server 2005 导入配置文件示例

以下代码段是 MS SQL Server 2005 的已编辑导入配置文件 (import_biar_config_mssql2005.xml) 的示例：

```
<?xml version="1.0"?>
<biconfig version="1.0">
  <step priority="1">
    <add>
      <biar-file name="c:\temp\AccessControl_R12.5_EN_SQL_11_JUN_2009.biar">
        <networklayer>OLE DB</networklayer>
        <rdms>MS SQL Server 2005</rdms>
        <username>dbAdmin</username>
        <password>P@ssw0rd</password>
        <datasource>r125db</datasource>
        <server>rdbms.org</server>
      </biar-file>
    </add>
  </step>
</biconfig>
```

报告门户的 Windows 身份验证配置

在 Windows 上有效

在您安装报告门户 (CA Business Intelligence) 并选择使用 Microsoft SQL Server 作为 CMS 数据库时，身份验证模式设置为 SQL Server 身份验证。Microsoft SQL Server 身份验证使用 SQL 用户帐户来验证数据库连接。

如果贵组织使用 Active Directory，您可以将身份验证方法修改为 Windows 身份验证。 在 Windows 身份验证中，验证 CMS 数据库的连接时使用的是域用户帐户而不是本地用户帐户。

在 Windows 身份验证中验证连接可提供在所有报告门户组件之间进行通讯的安全方法。 您可以从报告门户中部署的报告数据包删除明文密码，因为您对包含用户凭据的数据库配置了 ODBC 连接。

重要说明！ Windows 身份验证要求您同时使用 Internet Information Server (IIS) 和 Microsoft SQL Server。

如何将报告门户配置为在 Windows 身份验证中运行

了解修改报告门户数据库连接身份验证模式时所采取的步骤，可帮助您以 Windows 身份验证方式实施报告门户。

执行以下操作配置 Windows 身份验证的报告门户：

1. 准备 Microsoft SQL Server 数据库的受支持版本，以用作 CMS 数据库。
2. 使用默认的用户和核对过程准备 CA Business Intelligence CMS 数据库。
3. 创建系统 DSN 并指定使用 SQL Server 身份验证。

   系统 DSN 用来连接到报告门户 CMS 数据库。
4. 将 Active Directory 用户添加到本地 Administrators 组。

   指定的该用户用于在将报告门户配置为以 Windows 身份验证模式运行时进行身份验证。
5. 将 ASP.NET Web 服务扩展设置为“已允许”。
6. 安装报告门户 (CA Business Intelligence) (p. 21)。 在安装期间执行以下操作：
   a. 选择以自定义模式安装 CA Business Intelligence。
   b. 指定 Microsoft SQL Server 2005 作为数据库。
   c. 指定 IIS 作为 Web 服务器。
7. 配置 Windows 身份验证的报告门户。

   配置 CA Business Intelligence 服务，以使用 Active Directory 用户账户以 Windows 身份验证模式进行身份验证。
8. 使用 Windows 身份验证为 CA Access Control 报告数据库创建系统 DSN。

   系统 DSN 用来连接到 CA Access Control 报告门户。
9. 在报告门户上部署报告数据包。

配置 Windows 身份验证的报告门户

安装报告门户后，即可将报告门户配置为以 Windows 身份验证模式运行。 配置报告门户，以使用 Active Directory 用户帐户并修改系统 DSN 连接参数。

配置 Windows 身份验证的报告门户

1. 以操作系统管理员身份登录到报告门户主机。
2. 将报告门户 CMS 的系统 DSN 修改为 Windows NT 身份验证。
3. 选择“开始”、“程序”、“BusinessObjects XI Release 2”、“Business Objects Enterprise”、“中央配置管理器”。

   将打开中央配置管理器，显示 CA Business Intelligence 服务。
4. 停止所有 CA Business Intelligence 服务。
5. 将服务“登录身份”设置修改为 Active Directory 用户凭据。 对所有 CA Business Intelligence 服务执行该操作。

   重要说明！ 不要更改 WinHTTP Web Proxy Auto-Discovery 和 World Wide Web Publishing 服务的设置。
6. 启动所有 CA Business Intelligence 服务。

   报告门户现已配置为以 Windows 身份验证模式进行身份验证。

   注意：您可以通过 Microsoft SQL Server 活动监视器来确认与报告数据库的连接使用 Active Directory 用户帐户。

示例：修改 CA Business Intelligence 服务“登录身份”连接设置

以下示例为您展示了如何将 CA Business Intelligence 连接服务器服务“登录身份”凭据由系统帐户修改为 Active Directory 帐户。

1. 右键单击列表中的连接服务器服务并选择“属性”。

   将打开连接服务器服务属性窗口。
2. 在“登录身份”部分，删除“系统帐户”选项中的标记。

   连接设置字段已启用。
3. 输入 Active Directory 用户名、密码，并确认密码。

   示例：域/用户名

   单击“确定”。 服务连接设置已更改。
4. 退出中央配置管理器。

系统 DSN 连接配置示例

系统 DSN 连接设置定义连接到数据库所需的参数。 在以下示例中，创建以 SQL Server 身份验证模式对用户连接进行身份验证的系统 DSN，因为在安装报告门户时，它仅支持 SQL 身份验证。 在安装 CA Business Intelligence 之前，配置 CMS 数据库系统 DSN。

在以下示例中，为报告门户 CMS 数据库创建系统 DSN：

1. 选择“开始”、“设置”、“控制面板”、“管理工具”、“数据源 (ODBC)”。

   将打开 ODBC 数据源管理器。
2. 从“系统 DSN”选项卡中选择“创建”。

   将打开“选择新的数据源”窗口。
3. 向下滚动并选择“SQL Server”，然后单击“完成”。

   将打开“创建 SQL Server 的新数据源”向导。
4. 输入连接名称、说明和 SQL Server 名称。 单击“下一步”。
5. 选择使用 SQL Server 身份验证。
6. 输入用来连接到 SQL Server 的管理员用户凭据。 单击“下一步”。
7. 选择“更改默认数据库”选项，并从列表中选择报告门户 CMS 数据库。 单击“下一步”。
8. 单击“完成”。 选择测试连接，然后单击“确定”。

   系统 DSN 已创建。

在以 Windows 身份验证模式运行的报告门户上部署报告数据包

在 Windows 上有效

要使用标准 CA Access Control 报告，您需要将报告数据包文件导入 BusinessObjects InfoView。

注意：该过程介绍如何在尚未部署程序包的任何先前版本的情况下在报告门户上部署报告数据包。

在报告门户上部署报告数据包

1. 确认中央数据库、分发服务器和报告门户已设置。

   注意：确认 JAVA_HOME 变量已在报告门户计算机上设置。

2. 为 CA Access Control 报告数据库创建系统 DSN，并指定使用 Windows NT 身份验证。

   创建的系统 DSN 用来连接到 CA Access Control 报告数据库。在配置报告数据包时指定系统 DSN。

3. 将适用于您操作系统的 CA Access Control 企业版 Server Components DVD 插入光盘驱动器并导航至 \ReportPackages 文件夹。

4. 将 biconfig.zip 的内容提取到临时目录。

5. 将以下文件从光盘复制到同一临时目录：

   - \ReportPackages*RDBMS**import_biar_config*.xml
   - \ReportPackages*RDBMS**AC_BIAR_File*.biar

   RDBMS

   定义用于 CA Access Control 报告的 RDBMS 类型。

   值：MSSQL2005。

   ***import_biar_config*.xml**

   为 RDBMS 定义导入配置文件 (.xml) 的名称。

   值：import_biar_config_mssql_2005.xml

   注意：如果使用 MS SQL Server 2008 作为中央数据库，请配置 import_biar_config_mssql_2005.xml 文件。

   ***AC_BIAR_File*.biar**

   根据您的语言和 RDBMS 定义 CA Access Control 报告文件 (.biar) 的名称。

   注意：RDBMS 的导入配置文件的 <biar-file name> 属性指向该文件。 默认情况下，它被设置为 RDBMS 的英文版名称。

6. 编辑 *import_biar_config*.xml 文件的副本。 定义以下 XML 属性：

   重要说明！ 从文件中删除用户名、密码和服务器字段。

   <biar-file name>

   定义 CA Access Control 报告文件 (.biar) 的完整路径名。 这是您在上一步中复制的文件。

   <networklayer>

   定义 RDBMS 支持的网络层。

   值：ODBC。

<rdms>

定义用于 CA Access Control 报告的 RDBMS 类型。

值： 通用 ODBC 数据源

<datasource>

定义已创建的 DSN

重要说明！ 指定的数据库名称是由 CA Access Control 报告使用而不是由 CA Business Intelligence CMS 使用。

7. 打开命令提示符窗口并输入以下命令：

```
System_Drive:\BO\biconfig.bat -h host_name -u user_name -p password -f
ac_biar_config.xml
```

host_name

定义报告门户主机名。

user_name

定义您在安装报告门户时配置的报告门户管理员。

密码

定义报告门户管理员的密码。

例如：

```
biconfig.bat -h reportportal.comp.com -u Administrator -p P@ssw0rd -f
C:\BO\import_biar_config_mssql_2005.xml
```

示例：配置为使用 Windows 身份验证的示例 Microsoft SQL Server 2005 导入配置文件

以下代码段是在以 Windows 身份验证模式运行的报告门户上部署的 MS SQL Server 2005 的已编辑导入配置文件 (import_biar_config_mssql2005.xml) 示例。

```
<?xml version="1.0"?>
<biconfig version="1.0">
        <step priority="1">
                <add>
                        <biar-file name="c:\temp\biconfig\
                        AccessControl_R12.5_EN_JP_KR_SQL_6_DEC_2009.biar">
                                <networklayer>ODBC</networklayer>
                                <rdms>Generic ODBC datasource</rdms>
                                <datasource>acdb</datasource>
                        </biar-file>
                </add>
        </step>
</biconfig>
```

为大型部署配置 BusinessObjects

要在较大部署上运行 CA Access Control 报告，需要更改 BusinessObjects 默认配置。 更改 BusinessObjects 页面服务器可创建的并发连接的最大数目（默认值为 20,000）。 还需更改输入参数选择列表中显示的值的最大数目。

为大型部署配置 BusinessObjects

1. 更改 BusinessObjects 页面服务器可创建的并发连接数：
   a. 在报告门户计算机上，单击“开始”、“程序”、“Crystal Enterprise”、“Crystal 配置管理器”。

      将打开 BusinessObjects 配置管理器。

   b. 右键单击“Crystal 页面服务器”并选择“停止”。

   c. 右键单击“Crystal 页面服务器”并选择“属性”。

   d. 确认以下文本显示在“可执行文件的路径”字段的 *-restart* 之后：

      ```
      -maxDBResultRecords 0
      ```

   e. 重新启动 BusinessObjects 页面服务器。

2. 更改显示在报告的输入参数选择列表中的值的最大数：
   a. 打开 Windows 注册表编辑器。

   b. 导航到以下注册表键：

      ```
      HKEY_CURRENT_USER/Software/Business Objects/Suite 11.5/Crystal Reports/Database
      ```

   c. 依次单击“编辑”、“新建”、“DWORD 值”。

      将显示 REG_DWORD 类型的新注册表项。

   d. 将该项重命名为 *QPMaxLOVSize*。

   e. 双击该项并将其“数值数据”编辑为 1000。

      已设置新注册表项。

   f. 打开 BusinessObjects 中央管理控制台 (CMC)。

   g. 导航至“服务器”管理区域。

h. 单击要更改其设置的 Web Intelligence 报告服务器。

“Web Intelligence 报告服务器”页面将在“属性”选项卡中打开。

i. 将以下值修改为大于 1000 的值，或根据需要进行修改：

- 值批次大小列表
- 用于自定义排序的值列表的最大大小

单击“应用”提交更改，并重新启动服务器，以使更改立即生效。

配置到 CA Business Intelligence 的连接

CA Access Control 企业管理 通过 CA Business Intelligence 公用报告服务器（CA Access Control 报告门户）提供报告功能。 安装报告门户和部署报告后，需要配置从 CA Access Control 企业管理 到 CA Business Intelligence 的连接。 使用 Identity Manager 管理控制台配置该连接。

配置到 CA Business Intelligence 的连接

1. 启用 Identity Manager 管理控制台。
2. 打开 Identity Manager 管理控制台。
3. 单击“环境”、“ac-env”、“高级设置”、“报告”。

   将显示“报告属性”窗口。
4. 输入数据库和业务对象属性。

   重要说明！ CA Business Intelligence 中央管理服务器 (CMS) 仅用于内部管理目的，并不包含用于生成和显示报告的报告数据。 有关 CMS 的详细信息，请参阅 *《CA Business Intelligence 安装指南》*。

   注意：有关详细信息，可以从应用程序访问并参阅 *Identity Manager 管理控制台联机帮助*。

   重要说明！ 在“业务对象端口”字段中，输入报告门户使用的端口号。 默认端口为 8080。 在“业务对象报告”文件夹字段中，输入 CA Access Control r12。
5. 单击“保存”。

   CA Business Intelligence 设置已保存。

注意：有关 CA Business Intelligence 的详细信息，请参阅 CA Technologies 支持提供的 *《CA Business Intelligence 安装指南》*。

创建快照定义

报告基于从 CA Access Control 和 [assign the value for unab in your book] 端点收集并存储在中央数据库中的数据快照、CA Access Control 企业管理 中的 PUPM 数据以及用户存储中的数据。

必须先创建快照定义并捕获快照数据，然后才能运行和查看 CA Access Control 报告。 快照定义指定 CA Access Control 收集的报告数据以及数据收集的排定。

快照参数 xml 文件指定 CA Access Control 收集的报告数据。 默认情况下，该文件会指定报告快照中包括所有 CA Access Control 和 [assign the value for unab in your book] 端点、PUPM 数据以及用户存储中的数据。 您可以自定义快照参数 xml 文件以限制报告快照的范围。

要帮助确保报告包含最新的数据，请不要将此快照排定为比端点快照运行得更为频繁。 例如：如果您将端点配置为每周发送一次快照，而将 CA Access Control 企业管理 配置为每天都捕获快照，则将每周从端点收集一次报告数据，但每天都会从 PUPM 和用户存储中收集报告数据，因此报告中将显示过期的端点数据。

重要说明！ 不要启用多个快照定义。 如果启用了多个快照定义，CA Access Control 企业管理 无法成功运行所有报告。

注意：默认情况下，您必须具有“系统管理员”角色才能创建快照定义。

创建快照定义

1. 在 CA Access Control 企业管理 中，执行如下操作：
   a. 请单击“报告”。
   b. 单击“任务”子选项卡。
   c. 在左侧的任务菜单中展开管理快照定义树。
      此时“创建快照定义”任务会显示在可用任务列表中。
2. 单击“创建快照定义”。
   将显示“创建快照定义: 选择快照定义”页面。
3. 单击“确定”。
   将显示“创建快照定义”页面。

4. 填写“配置文件”选项卡中的以下字段：

快照定义名称

定义快照定义的名称。

快照定义说明

指定描述快照定义的任何其他信息。

已启用

指定 CA Access Control 企业管理 启用快照定义。

注意：如果不选中此复选框，CA Access Control 企业管理 将不会捕获快照，您也无法查看报告。 您一次只能启用一个快照。

标识符

指定用于定义报告快照范围的快照参数 XML 文件。

默认值：PPM_ALL.xml

保留最终个数

指定存储在中央数据库中的成功快照数。当数据库中的快照数达到所指定的数量时，CA Access Control 会删除旧快照。

注意：快照数量应大于零。 如果没有为该字段指定值，则 CA Access Control 将存储无限多的快照。 建议您最多存储三个成功的快照。

5. 单击“重现”选项卡并选择“排定”。

此时将显示排定选项。

6. 指定快照执行时间和重现模式，然后单击“提交”。

注意：建议您将此快照排定为运行频率小于来自 CA Access Control 和 [assign the value for unab in your book] 端点的快照。

将 CA Access Control 配置为按排定的时间和频率捕获快照。

注意：在创建快照定义之后，您可以选择按需捕获快照以及按照排定的时间和频率捕获快照。 有关捕获快照数据的详细信息，请参阅*《企业管理指南》*。

限制报告快照的范围

当 CA Access Control 企业管理 捕获报告快照时，它收集 CA Access Control 和 [assign the value for unab in your book] 端点的快照数据、CA Access Control 企业管理 的 PUPM 数据，以及用户存储数据。 CA Access Control 企业管理 收集报告数据后，将数据存储在中央数据库中。

快照参数 XML 文件指定 CA Access Control 企业管理 收集的报告数据。您可以通过自定义快照参数 XML 文件来限制报告快照的范围。

例如：如果使用 Active Directory 作为用户存储，CA Access Control 企业管理 将在捕获报告快照时收集每个 Active Directory 用户的数据。 该操作可能需要花费大量时间才能完成。 要减少捕获快照的时间，可以通过自定义快照参数 XML 文件来限制 Active Directory 快照的范围。

限制报告快照的范围

1. 导航到以下目录，其中 *JBOSS_HOME* 是 JBoss 的安装目录：

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/imrexport/sample

2. 复制 PPM_ALL.xml 文件，重命名新文件，并在同一目录中保存文件。

   您已创建新的快照参数 XML 文件。

3. 以可编辑格式打开新的快照参数 XML 文件。

4. 编辑 <!--IM COLLECTORS--> 部分的条目，以指定 CA Access Control 企业管理 从用户存储收集的数据的范围。

5. 以 (!--) 和 (--) 注释掉 <!--PUPM COLLECTORS--> 部分中不希望包含在报告快照中的 CA Access Control 企业管理 组件所对应的条目。

6. （可选）限制 Active Directory 快照的范围：

   a. 查看LDAP 查询如何限制报告快照 (p. 46)和LDAP 语法注意事项 (p. 46)主题。

      这些主题中的信息将帮助您按以下步骤定义正确的 LDAP 查询。

   b. 在 <!--PUPM COLLECTORS--> 部分找到以下元素：

      ```
      <export object="com.ca.ppm.export.ADUsersCollector">
      </export>
      ```

      该元素指定包含在快照中的 Active Directory 用户数据。

c. 编辑元素，以使它按如下所示，其中 *ldap_query* 指定 LDAP 查询，该查询定义为其收集数据的用户：

```
<export object="com.ca.ppm.export.ADUsersCollector">
        <where attr="%USER" satisfy="ANY">
                <value op="EQUALS">(ldap_query)</value>
        </where>
</export>
```

d. 在 <!--PUPM COLLECTORS--> 部分找到以下元素：

```
<export object="com.ca.ppm.export.ADGroupsCollector">
</export>
```

e. 编辑元素，以使它按如下所示，其中 *ldap_query* 指定 LDAP 查询，该查询定义为其收集数据的组：

```
<export object="com.ca.ppm.export.ADGroupsCollector">
        <where attr="%USER" satisfy="ANY">
                <value op="EQUALS">(ldap_query)</value>
        </where>
</export>
```

您已限制 Active Directory 快照的范围。

7. 保存并关闭新的快照参数 XML 文件。
8. 修改 CA Access Control 企业管理 中的快照定义，以使用新的快照参数 XML 文件。

运行捕获快照任务时，它仅收集快照参数 XML 文件中指定的数据。

示例：将报告快照的范围限制到 CA Access Control 端点

如果不使用 PUPM 和 [assign the value for unab in your book]，则可以限制报告快照的范围，以仅从 CA Access Control 端点收集数据。 要将数据收集的范围限制到 CA Access Control 端点，以 (!--) 和 (--) 注释 <-- PUPM COLLECTORS --> 部分下的所有条目，ReportIdMarkerCollector 条目*除外*。

以下是修改 PPM_ALL.xml 文件以注释 <-- PUPM COLLECTORS --> 部分的所有条目（除 ReportIdMarkerCollector 条目之外）后 PPM_ALL.xml 文件的片段：

```
<!--  PUPM COLLECTORS -->
        <!-- export object="com.ca.ppm.export.AccountPasswordCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.PPMRolesCollector">
                <exportattr attr="|rolemembers|" />
        </export -->

        <!-- export object="com.ca.ppm.export.
                PrivilegedAccountExceptionCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.PPMPasswordPolicyCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.ADUsersCollector">
        </export -->

        <export object="com.ca.ppm.export.PPMAccountUserAccessCollector">
        </export --!>

        <!-- export object="com.ca.ppm.export.ADGroupsCollector">
                <exportattr attr="|groupmembers|" />
        </export -->

        <export object="com.ca.ppm.export.ReportIdMarkerCollector">
        </export>
```

快照参数 XML 文件语法－限制报告快照

快照参数 XML 文件指定 CA Access Control 企业管理 收集的报告数据。您可以通过编辑快照参数 XML 文件来限制报告快照的范围。

CA Access Control 企业管理 仅为满足在快照参数 XML 文件中定义的条件的对象收集报告数据。 文件中的每个收集器都定义 CA Access Control 企业管理 收集的一组对象。

每个收集器都具有以下结构：

```
<export object=" ">
        <where attr=" " satisfy=" ">
                <value> </value>
        </where>
        <exportattr attr=" " />
</export>
```

注意：<where>/<value> 和 <exportattr> 元素可选。

每个收集器包含以下元素：

<export>

表明 CA Access Control 企业管理 收集的对象数据。例如：<export> 元素可以指定 CA Access Control 企业管理 收集用户数据。

<export> 元素可以包括一个或多个 <exportattr> 和 <where> 元素，以便仅收集满足特定条件的数据。 如果未指定任何 <exportattr> 或 <where> 元素，则 CA Access Control 企业管理 将为对象收集所有数据。

<export> 元素只有对象参数。

<where>

根据 <value> 元素定义的条件筛选已收集的数据。 <where> 元素必须至少包含一个 <value> 元素。您可以指定多个 <where> 元素来精简筛选（它们充当 OR 元素）。

下表说明 <where> 元素的参数：

参数	说明
attr	表示要用于筛选的属性。

参数	说明
satisfy	表明要收集的对象或属性必须满足部分值还是所有值。 ■ ALL—属性或对象必须满足所有值评估。 ■ ANY—属性或对象必须至少满足一个值评估。

<value>

在 <where> 元素中定义要收集的属性或对象必须满足的条件。 <value> 元素要求操作符 (op) 参数。 操作符可以是 EQUALS 或 CONTAINS。

注意：在快照参数 XML 文件的 <!--PUPM COLLECTORS--> 部分中，可以在 <value> 元素中使用 LDAP 语法。 使用 LDAP 语法，可以指定 CA Access Control 企业管理 从 Active Directory 收集的用户和组数据。

<exportattr>

表示要收集的特定属性。使用 <exportattr> 元素为正在收集的对象收集属性子集。 例如：可以使用 <exportattr> 元素仅收集用户的 ID。

<exportattr> 元素具有 attr 参数。

下表所示属性可用于 <where> 元素或 <exportattr> 元素（按对象）：

对象	可以在 <where> 元素中使用的属性	可以在 <exportattr> 元素中使用的属性
role	可以使用 name 属性筛选。 name—其名称满足筛选的角色	您可以收集以下任何属性： ■ |tasks|—与该角色相关的所有任务 ■ |rules|—适用于该角色的所有成员、管理员、所有者和范围规则 ■ |users|—该角色的所有成员、管理员和所有者 ■ |rolemembers|—所有角色成员 ■ |roleadmins|—所有角色管理员 ■ |roleowners|—所有角色所有者

对象	可以在 <where> 元素中使用的属性	可以在 <exportattr> 元素中使用的属性
user	任何常见或物理属性以及以下任一属性： ■ |groups|—组的所有成员 ■ |roles|—角色的所有成员 ■ |orgs|—配置文件存在于满足筛选条件的组织的用户	您可以收集以下任何属性： ■ |all_attributes|—所有可用的用户属性 ■ |groups|—用户所属的或作为管理员管理的所有组 ■ |roles|—用户所属的、作为管理员或所有者的所有角色
group	任何常见或物理属性或以下属性： |groups|—满足筛选条件的某个组内的嵌套组列表	您可以收集任何常见或物理属性，或者以下任一属性： ■ |all_attributes|—在目录配置文件 (directory.xml) 中为组对象定义的所有属性 ■ |groups|—该组内的所有嵌套组 ■ |users|—该组的所有成员 ■ |groupadmins|—为指定组的管理员的所有用户 ■ |groupmembers|—属于指定组的所有用户 ■ |users|—所有组管理员和成员
organization	任何常见或物理属性	您可以收集任何常见或物理属性，或者以下任一属性： ■ |all_attributes|—在目录配置文件 (directory.xml) 中为组织对象定义的所有属性 ■ |orgs|—该组织内的所有嵌套组织 ■ |groups|—该组织内的所有组 ■ |users|—该组织内的所有用户

LDAP 查询如何限制报告快照中的用户和组数据

如果将 Active Directory 用作用户存储，则可以指定在报告快照中捕获的用户和组数据。

可以在按用户和组筛选 Active Directory 数据的快照参数 XML 文件中使用 LDAP 查询。 但是，无法使用按角色成员资格筛选 Active Directory 数据的 LDAP 查询。 只能在快照参数 XML 文件的 <!--PUPM COLLECTORS--> 部分使用 LDAP 查询

以下过程介绍了快照参数 XML 文件中的 LDAP 查询如何限制 CA Access Control 企业管理 收集的 Active Directory 数据。 该信息有助于编写正确的 LDAP 查询来限制报告快照。

当 CA Access Control 企业管理 捕获 Active Directory 报告快照时，它执行以下操作：

1. 仅为在以下元素的 LDAP 查询中指定的 Active Directory 用户收集数据：

   ```
   <export object="com.ca.ppm.export.ADUsersCollector">
   ```

   如果元素不包含 LDAP 查询，CA Access Control 企业管理 将在快照中包括所有 Active Directory 用户的数据。

2. 仅为在以下元素的 LDAP 查询中指定的 Active Directory 组收集数据：

   ```
   <export object="com.ca.ppm.export.ADGroupsCollector">
   ```

   如果元素不包含 LDAP 查询，CA Access Control 企业管理 将在快照中包括所有 Active Directory 组的数据。

   注意：CA Access Control 企业管理 不会为步骤 1 的查询未返回的任何用户收集数据。 如果用户是步骤 2 的查询返回的组成员，但是用户未由步骤 1 的查询返回，则 CA Access Control 企业管理 不会在 Active Directory 快照中包括用户的任何数据。

LDAP 语法注意事项

在编写 LDAP 查询来限制 Active Directory 快照的范围时，请考虑以下注意事项：

- 您可以在 LDAP 查询中使用以下逻辑操作符：
  - EQUAL TO (=)
  - OR (|)

- AND (&)

  注意：某些限制适用于与号 (&) 字符。

- NOT (!)
- 通配符 (*)

- 只能在以下上下文中使用与号字符 (&) 和左尖括号字符 (<)：
  - 作为标记分隔符
  - 在注释中
  - 在处理指令中
  - 在 CDATA 部分

使用字符串 **&** 或 Unicode 字符引用表示任何其他上下文中的与号字符。 使用字符串 **<** 或 Unicode 字符引用表示任何其他上下文中的左尖括号字符。

- 只能在字符串的结尾处使用右尖括号字符 (>)，用以标记 CDATA 部分的结尾 ( ]]>)。

  使用字符串 **>** 或 Unicode 字符引用表示任何其他上下文中的右尖括号字符。

示例：与号字符

以下快照参数 XML 文件片段指定在报告快照中包括所有 Active Directory 用户数据。 片段中的 LDAP 查询使用 & 字符串表示与号：

```
<export object ="com.ca.ppm.export.ADUsersCollector">
        <where attr="%USER%" satisfy="ANY">
                <value op="EQUALS">(&amp;(objectClass=user))</value>
        </where>
</export>
```

第 5 章： CA Access Control for Virtual Environments REST API

此部分包含以下主题：

基于 REST API

REST（表象化状态传输）描述软件的结构风格特征，依靠多媒体内在属性创建并修改 URL 上可访问的对象状态。

在 REST 方案中，文档（表示对象状态）在客户端和服务之间来回传递，假设两者均不知道任何实体，而不是在单个请求或响应中的实体。

要获得基于 REST API 的架构，请导航到下列 URL 并查看空页的源：

`https://hostname:18443/iam/api/1.0/restapi/schemas`

注意：有关架构的更多信息，请参阅本节中的示例。

基于 REST 身份验证

作为请求信息的一部分，CA Access Control for Virtual Environments REST 请求包括身份验证信息。 CA Access Control for Virtual Environments 支持 HTTP 基本身份验证方式。 您可以使用以下基本身份验证，例如：

```
Authorization: Basic c3VwZXJhZG1pbjpkZWZhdWx0c3VwZXJhZG1pbjpkZWZhdWx0
```

以上示例表示用户“superadmin”和密码“default”的基础 64 编码。

获取标记

要检索所有标记列表，请使用 GET 命令来获取全部标记。

将 HTTP GET 请求发送到下列 URL：

```
https://hostname:18443/iam/api/1.0/restapi/environment/ac/tags
```

要检索特定标记，请使用如下 GET 命令并指定标记名称。

将 HTTP GET 请求发送到下列 URL：

```
https://hostname:18443/iam/api/1.0/restapi/environment/ac/tags/<tag_name>
```

创建标记

使用 POST 命令创建标记。

将 HTTP POST 请求发送到下列 URL：

```
https://hostname:18443/iam/api/1.0/restapi/environments/ac/tags
```

HTTP 正文必须包含创建标记的以下信息：

```
<Tag>
  <Name>Tag Name</Name>
  <Description>Tag Description</Description>
</Tag>
```

<名称>

指定标记名称

<说明>

指定标记的说明

修改标记

修改要修改的标记，以便从受管设备分配或删除标记。

遵循这些步骤:

1. 使用 GET 命令检索标记状态：

   https://*hostname*:18443/iam/api/1.0/restapi/environments/ac/<tag_name>

   您得到响应 XML 文档，类似于以下内容：

   ```
   <Tag>
     <Name>testtag</Name>
     <Description />
     <Devices>
       <Device>
         <ID>vm-11</ID>
       </Device>
     </Devices>
   </Tag>
   ```

2. 使用修改的标记更新设备。

   将 HTTP PUT 命令发送到下列 URL：

   https://*hostname*:18443/iam/api/1.0/restapi/environments/ac/<tag_name>

删除标记

要删除标记，请使用 DELETE 命令。

将 HTTP DELETE 请求发送到下列 URL：

https://*hostname*:18443/iam/api/1.0/restapi/environments/ac/tags/</*tag_name*>

标记受管设备

您可以标记受管设备以将计算机添加到安全组并远程对它进行管理。

遵循这些步骤:

1. 获得 CA Access Control for Virtual Environments 用于受管设备的 ID。

   要得到 CA Access Control for Virtual Environments 用于受管设备的 ID，请使用筛选，并使用 REST 请求来检索设备详细信息。 例如：

   ```
   https://hostname:18443/iam/api/1.0/restapi/environments/ac/devices?managed-object-vcenter-uuid=54E79C3A-49D5-4958-A983-8B919F470CEC&managed-object-id=vm-394
   ```

   注意：在前一示例中，使用在 VMware 管理对象浏览器 (MOB) 中定义的筛选参数 vCenter UUID 和 VM UUID 传递。

   您得到响应 XML 文档，类似于以下内容：

   ```
   <Devices>
     <Device>
       <ID>vm-19</ID>
       <ParentID>esx-3</ParentID>
       <Name>ESXi in a box</Name>
       <Type>VirtualMachine</Type>
       <VirtualMachineProperties>
         <ManagedObjectID>vm-394</ManagedObjectID>

   <ManagedObjectVCenterUUID>54E79C3A-49D5-4958-A983-8B919F470CEC</ManagedObjectVCenterUUID>
         <GuestOSVersion>LINUX_REDHAT_5</GuestOSVersion>
         <GuestOSArchitecture>X86</GuestOSArchitecture>
         <GuestOSDescription>Red Hat Enterprise Linux 5 (64-bit)</GuestOSDescription>
       </VirtualMachineProperties>
       <SecurityGroups>
         <SecurityGroup>
           <ID>sg-13</ID>
           <Name>weiig01esxi01.ca.com</Name>
           <Description/>
           <Owner>superadmin</Owner>
         </SecurityGroup>
         <SecurityGroup>
           <ID>sg-15</ID>
           <Name>Discovered virtual machine</Name>
           <Description/>
           <Owner>superadmin</Owner>
         </SecurityGroup>
   ```

```
      <SecurityGroup>
        <ID>sg-22</ID>
        <Name>vSphere in a box</Name>
        <Description/>
        <Owner>superadmin</Owner>
      </SecurityGroup>
    </SecurityGroups>
  </Device>
</Devices>
```

设备的 ID 是在响应 XML 文件中所指定的 **vm-19**。

2. 使用分配的标记更新设备。

   将 HTTP PUT 命令发送到下列 URL：

   ```
   https://<host>:18443/iam/api/1.0/restapi/environments/ac/devices/<managed_device_ID>
   ```

   注意：HTTP 内容必须包含新分配的标记信息，除此以外，还包含设备的所有现有属性。 要获得现有属性，请在筛选设备的 CA Access Control for Virtual Environments ID 时从响应 XML 文件复制 <Device>...</Device> 标记之间的数据。

   带有新标记关系的 HTTP 内容示例：

   ```
   <Device>
     <ID>vm-19</ID>
     <ParentID>esx-3</ParentID>
     <Name>ESXi in a box</Name>
     <Type>VirtualMachine</Type>
     <VirtualMachineProperties>
       <ManagedObjectID>vm-394</ManagedObjectID>

   <ManagedObjectVCenterUUID>54E79C3A-49D5-4958-A983-8B919F470CEC</ManagedObjectVCenterUUID>
       <GuestOSVersion>LINUX_REDHAT_5</GuestOSVersion>
       <GuestOSArchitecture>X86</GuestOSArchitecture>
       <GuestOSDescription>Red Hat Enterprise Linux 5 (64-bit)</GuestOSDescription>
     </VirtualMachineProperties>
     <Tags>
       <Tag>
         <Name>testtag</Name>
         <Description>testtag2 description</Description>
       </Tag>
     </Tags>
     <SecurityGroups>
       <SecurityGroup>
         <ID>sg-13</ID>
         <Name>weiig01esxi01.ca.com</Name>
         <Description/>
         <Owner>superadmin</Owner>
       </SecurityGroup>
   ```

```
    <SecurityGroup>
      <ID>sg-15</ID>
      <Name>Discovered virtual machine</Name>
      <Description/>
      <Owner>superadmin</Owner>
    </SecurityGroup>
    <SecurityGroup>
      <ID>sg-22</ID>
      <Name>vSphere in a box</Name>
      <Description/>
      <Owner>superadmin</Owner>
    </SecurityGroup>
  </SecurityGroups>
</Device>
```

从受管设备中删除标记

您可以在受管设备上删除标记，以便从安全组中删除。

遵循这些步骤:

1. 获得 CA Access Control for Virtual Environments 用于受管设备的 ID。

   要获得 CA Access Control for Virtual Environments 用于受管设备的 ID，请使用筛选。 例如：

   ```
   https://hostname:18443/iam/api/1.0/restapi/environments/ac/devices?managed-object-vcenter-uuid=54E79C3A-49D5-4958-A983-8B919F470CEC&managed-object-id=vm-394
   ```

   注意：在前一示例中，传递在 VMware 管理对象浏览器 (MOB) 中定义的 vCenter UUID 和 VM UUID。

   您得到响应 XML 文档，类似于以下内容：

   ```
   <Devices>
     <Device>
       <ID>vm-19</ID>
       <ParentID>esx-3</ParentID>
       <Name>ESXi in a box</Name>
       <Type>VirtualMachine</Type>
       <VirtualMachineProperties>
         <ManagedObjectID>vm-394</ManagedObjectID>

   <ManagedObjectVCenterUUID>54E79C3A-49D5-4958-A983-8B919F470CEC</ManagedObjectVCenterUUID>
         <GuestOSVersion>LINUX_REDHAT_5</GuestOSVersion>
         <GuestOSArchitecture>X86</GuestOSArchitecture>
         <GuestOSDescription>Red Hat Enterprise Linux 5 (64-bit)</GuestOSDescription>
       </VirtualMachineProperties>
   ```

```
    <SecurityGroups>
      <SecurityGroup>
        <ID>sg-13</ID>
        <Name>weiig01esxi01.ca.com</Name>
        <Description/>
        <Owner>superadmin</Owner>
      </SecurityGroup>
      <SecurityGroup>
        <ID>sg-15</ID>
        <Name>Discovered virtual machine</Name>
        <Description/>
        <Owner>superadmin</Owner>
      </SecurityGroup>
      <SecurityGroup>
        <ID>sg-22</ID>
        <Name>vSphere in a box</Name>
        <Description/>
        <Owner>superadmin</Owner>
      </SecurityGroup>
    </SecurityGroups>
  </Device>
</Devices>
```

设备的 ID 是在响应 XML 文件中所指定的 **vm-19**。

2. 更新设备并删除标记，如下所示：

   a. 编辑第 1 步中的响应 XML 文件，并在 <Tags>...</Tags> 标记之间删除所有内容。

   b. 使用 HTTP PUT 命令，将更新的 XML 文件发送到下列 URL：

      ```
      https://<host>:18443/iam/api/1.0/restapi/environments/ac/devices/vm-19
      ```

示例：HTTP 架构

以下内容是支持的基于 REST API 命令的架构示例：

- HTTP POST：

  ```
  POST /iam/api/1.0/restapi/environments/ac/tags HTTP/1.1
  Content-type: application/xml; charset=UTF-8
  Authorization: Basic YWRtaW46ZGVmYXVsdA==
  Cache-Control: no-cache
  Pragma: no-cache
  Host: 10.112.196.244
  Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
  Connection: keep-alive
  Content-Length: 79

  <Tag><Name>testtag</Name><Description>testtag2
  description</Description></Tag>
  ```

- HTTP GET：

```
GET /iam/api/1.0/restapi/environments/ac/devices/vm-19 HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.169:9998
```

- HTTP PUT：

```
PUT /iam/api/1.0/restapi/environments/ac/devices/vm-19 HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 959

<Devices><Device><ID>vm-19</ID><ParentID>esx-3</ParentID><Name>ESXi in a
box</Name><Type>VirtualMachine</Type><VirtualMachineProperties><ManagedOb
jectID>vm-394</ManagedObjectID><ManagedObjectVCenterUUID>54E79C3A-49D5-49
58-A983-8B919F470CEC</ManagedObjectVCenterUUID><GuestOSVersion>LINUX_REDH
AT_5</GuestOSVersion><GuestOSArchitecture>X86</GuestOSArchitecture><Guest
OSDescription>Red Hat Enterprise Linux 5
(64-bit)</GuestOSDescription></VirtualMachineProperties><Tags><Tag><Name>
testtag</Name><Description>testtag2
description</Description></Tag></Tags><SecurityGroups><SecurityGroup><ID>
sg-13</ID><Name>weiig01esxi01.ca.com</Name><Description/><Owner>superadmi
n</Owner></SecurityGroup><SecurityGroup><ID>sg-15</ID><Name>Discovered
virtual
machine</Name><Description/><Owner>superadmin</Owner></SecurityGroup><Sec
urityGroup><ID>sg-22</ID><Name>vSphere in a
box</Name><Description/><Owner>superadmin</Owner></SecurityGroup></Securi
tyGroups></Device></Devices>
```

- HTTP DELETE：

```
DELETE /iam/api/1.0/restapi/environments/ac/tags/testtag HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```