CA Access Control 高级版

企业管理指南

12.6

第三方通知

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 高级版
- CA Access Control
- CA Single Sign-On (CA SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management（CA NSM，以前为 Unicenter NSM 和 Unicenter TNG）
- CA Software Delivery（以前为 Unicenter Software Delivery）
- CA Service Desk Manager（以前为 Unicenter Service Desk）
- CA User Activity Reporting Module（以前是 CA Enterprise Log Manager）
- CA 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

格式	含义
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
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：

- *ACInstallDir*—默认 CA Access Control 安装目录。
  - Windows—C:\Program Files\CA\AccessControl\
  - UNIX—/opt/CA/AccessControl/
- *ACSharedDir*—CA Access Control for UNIX 使用的默认目录。
  - UNIX—/opt/CA/AccessControlShared

- *ACServerInstallDir*—默认 CA Access Control 企业管理 安装目录。
  - /opt/CA/AccessControlServer
- *DistServerInstallDir*—默认分发服务器安装目录。
  - /opt/CA/DistributionServer
- *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。

文档更改

从上一版本以来对该文档进行了以下更新：

- 规划您的 PUPM 实施 (p. 105)
  - Connector Xpress 示例：配置 SUN ONE 端点 (p. 127)－新主题说明如何在 Connector Xpress 中配置 SUN ONE 端点
  - Connector Xpress 示例：在 Java 连接器服务器中注册 SUN One 端点类型 (p. 129)－新主题说明如何在 Java 连接器服务器中注册 SUN ONE 端点类型
- 实施特权帐户 (p. 141)
  - Sybase 服务器连接信息 (p. 158)－新主题指定 Sybase 服务器端点类型连接信息
  - VMware ESX/ESXi 连接信息 (p. 160)－新主题指定 VMWare ESX/ESXi 端点类型连接信息
  - 创建端点 CSV 文件 (p. 186)－更新主题包括其他行
  - 创建特权帐户 CSV 文件 (p. 191)－更新主题包括其他行

目录

第 1 章： 简介

此部分包含以下主题：

关于本指南

本指南提供了有关 CA Access Control 高级版 中的企业管理、报告以及 CA Access Control 企业管理 基于 Web 界面的信息。 CA Access Control 的企业管理和报告包括高级策略管理、报告和全局查看企业查看器。

为了简化术语，在本指南中我们将此产品称为 CA Access Control。

使用本指南的用户

本指南面向要使用 CA Access Control 的企业管理和报告功能的安全管理员和系统管理员而编写：

- 企业策略管理
- 企业报告
- 用于处理企业主机访问管理的基于 Web 的界面。
- 特权用户密码管理 (PUPM)

Enterprise Management

CA Access Control 企业管理 是基于 Web 的用户界面，使您能够执行整个企业中的访问相关管理任务。 使用 CA Access Control 企业管理，您可以执行大量管理任务，例如从一个中央位置部署整个企业的访问策略、管理单个主机、管理特权帐户、生成企业报告等等。

企业管理界面

CA Access Control 企业管理 界面是您的企业管理工具，包含管理企业所需的一切内容。 CA Access Control 企业管理 界面包含的工具用于配置主机、创建和分配策略、管理用户、组和管理任务以及配置和管理整个企业中特权帐户的访问。 此外，您还可以获取对企业报告和审核功能的访问权限。

集中策略管理

使用 CA Access Control 企业管理 的集中策略管理功能创建不知名策略并将其分配给企业中的主机或主机组。 CA Access Control 企业管理 界面使用向导可以分配企业范围策略，并显示每台主机上的部署进程的状态。

此外，您还可以使用 CA Access Control 企业管理 集中策略管理功能来排除策略部署进程的故障、取消分配、升级或降级现有策略。

企业视图

您可以使用 CA Access Control 企业管理 来查看相关信息并从中央位置管理 CA Access Control、PUPM 和 UNAB 主机。 CA Access Control 企业管理 全局查看显示有关每台主机类型、主机上次更新时间、每台主机上配置的设备类型等信息，并让您可以远程修改主机的设置并对其进行管理。

特权用户密码管理

特权用户密码管理 (PUPM) 是一种进程，企业可通过该进程保护、管理和跟踪与企业中权限最高的用户相关的所有活动。

CA Access Control 企业管理 从中央位置向受管理设备上的特权帐户提供基于角色的访问管理。 CA Access Control 企业管理 提供特权帐户和应用程序 ID 密码的安全存储，并基于策略控制对特权帐户和密码的访问。

此外，CA Access Control 企业管理 还管理特权帐户和应用程序密码生命周期，并允许删除配置文件和脚本中的任何密码。

UNAB 管理

通过 UNIX 身份验证代理 (UNAB)，您可以使用 Active Directory 数据存储登录到 UNIX 计算机。 这意味着您可以将单个存储库用于所有的用户，使他们能够使用相同的用户名和密码登录所有平台。

将 UNIX 帐户与 Active Directory 相集成可实施严格的身份验证和密码策略，将基本的 UNIX 用户和组属性传输到 Active Directory。 这让您可以在管理 Windows 用户和组的同时，从单一点管理 UNIX 用户和组。

使用 CA Access Control 企业管理 集中策略管理功能，通过创建和分配包含一整套登录规则的登录策略来控制对 UNIX 主机的访问。

企业报告

通过 CA Access Control 企业管理 报告服务，您可以在一个中央位置查看每个端点（用户、组和资源）的安全状态。 可以在排定时间或在需要时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。

设置 CA Access Control 报告服务后，该服务将独立运行，从每个端点收集数据并将其报告给中央服务器，然后继续报告端点状态而无需手工干预。 这意味着无论收集服务器处于开机还是关机状态，每个端点均会报告其状态。

CA Access Control 企业管理 随附了现成的一套预定义报告，显示了有关每个端点的一系列信息。 此外，您还可以自定义现有的报告和创建自己的报告，以便显示您有兴趣查看的信息。

第 2 章： 管理 CA Access Control 企业管理

此部分包含以下主题：

管理范围

在 CA Access Control 企业管理 中，可通过分配管理角色和特权访问角色为用户和管理员分配权限。 角色包含与 CA Access Control 企业管理 中的应用程序功能对应的任务。

角色可简化权限管理。 您可以为用户分配角色，而不是将该用户与其所执行的每项任务关联在一起。 用户可以执行其分配角色的所有任务。 然后，可通过添加任务来编辑该角色。 现在，具有该角色的每个用户都可以执行新任务。 如果从角色中删除了某项任务，用户将不能再执行该任务。

用户登录到 CA Access Control 企业管理 时，可看到基于其角色的选项卡。 用户只能看到分配给其角色的选项卡和任务。

可以为不同的用户分配单独的角色，以防一个用户能够完成所有任务。这可能会有助于您的组织遵守职责独立的要求。 但是，可以为一个用户分配多个角色。

CA Access Control 企业管理 中的管理角色

CA Access Control 企业管理 中的预定义管理角色提供了一组基本的管理角色，您可以根据具体要求将这些角色分配给您企业的管理员。 现有 CA Access Control 企业管理 附带了以下管理角色：

- **CA Access Control 主机管理员**－负责定义主机和逻辑主机组。

  该管理角色允许用户创建主机和主机组，为主机组分配主机，以及对其进行修改。 它不允许用户定义策略或部署策略，但允许用户查看策略，并提供了对“全局查看”的访问权限。

- **CA Access Control 策略部署员**－负责在环境中部署策略。

  该管理角色允许用户将策略分配给主机和主机组、升级和降级策略、重置主机配置，以及访问部署审核。 它允许用户查看策略和主机，但不允许对其进行定义，并提供了对“全局查看”的访问权限。

- **CA Access Control 策略管理员**－负责创建策略。

  该管理角色允许用户创建、修改、查看和删除策略。 该管理角色不允许用户将策略部署到主机或主机组，但是允许用户查看策略，以及访问“全局查看”。

- **CA Access Control 用户管理员**－负责 CA Access Control 企业管理 中的用户管理：创建和管理用户和组，以及为用户分配 CA Access Control 企业管理 角色。

  注意：CA Access Control 用户管理员不能创建新管理角色。 只有“系统管理员”可以创建新管理角色。

- **系统管理员**－负责管理 CA Access Control 企业管理。

  具有此管理角色的用户可以在 CA Access Control 企业管理 中执行、创建和管理所有任务。

  此角色可用于实施阶段，以针对紧急情况定义组织中的实际管理角色。 建议您将此角色分配给最少数量的用户，最好只分配给一个用户，并密切监控该用户的操作。

- **报告**－负责管理英语报告。 具有该角色的用户可以排定和查看报告。

- **UNAB 管理员**－负责管理 UNAB。 具有该角色的用户可以配置 UNAB 主机和主机组，管理登录授权策略，以及解决迁移冲突。

  注意：分配了“系统管理员”角色的用户还会被分配“UNAB 管理员”角色。

- **CA Enterprise Log Manager 用户**－负责查看 CA Enterprise Log Manager 报告。 具有该角色的用户可以查看 CA Enterprise Log Manager 报告。

- **CA Enterprise Log Manager 管理**－负责管理 CA Enterprise Log Manager 报告。 具有该角色的用户可以在 CA Access Control 企业管理 中管理 CA Enterprise Log Manager 报告，并管理到 CA Enterprise Log Manager 服务器的连接。

- **指派管理员**－负责指派工作项。 具有该角色的用户可以将工作项指派给用户。

- **自主管理员**－负责管理其自己的用户帐户。 具有该角色的用户可以对其帐户执行管理操作：更改帐户密码、修改其用户配置文件、查看其分配的角色、提交的任务及正在等待其批准的项目。

  注意：默认情况下，系统中的每个用户都会被分配“自主管理员”角色。

创建管理角色

如果 CA Access Control 企业管理 中的预定义管理角色不适合您的组织要求，您可以创建新的管理角色。

创建管理角色

1. 在 CA Access Control 企业管理 中，执行如下操作：
   a. 单击“用户和组”。
   b. 单击“角色”子选项卡。
   c. 在左侧的任务菜单中展开管理角色树。

      此时“创建管理角色”任务会显示在可用任务列表中。
2. 单击“创建管理角色”。

   此时将显示“创建管理角色: 选择管理角色”页面。
3. （可选）按如下方式选择一个现有管理角色来创建新管理角色作为其副本：
   a. 选择“创建角色副本”。
   b. 选择要搜索的属性，键入筛选值，然后单击“搜索”。

      此时将显示匹配筛选条件的管理角色的列表。
   c. 选择要用作新管理角色基础的对象。
4. 单击“确定”。

   将显示“创建管理角色”任务页面。 如果管理角色是从现有对象创建的，则对话框字段中会预先填充来自现有对象的值。
5. 在该对话框的“配置文件”选项卡中填写以下字段：

   名称

   定义策略的名称。

   说明

   角色的文本说明。

   已启用

   指定角色是否可以分配给用户和组。

6. 按如下方式将任务添加到角色：
   a. 单击“任务”选项卡。
   b. （可选）从“筛选”任务下拉列表中选择任务类别

      此类别的任务即会加载。

      注意：该任务类别与 CA Access Control 企业管理 中显示此类别中任务的选项卡匹配。
   c. 从“添加任务”下拉列表中选择一项任务。

      该任务即被添加到角色。
   d. 重复步骤 b 至 c 以将更多的任务添加到角色。
7. 添加成员和范围规则 (p. 25)。
8. 单击“提交”。

   该角色即已创建。

特权访问角色

CA Access Control 企业管理 中的特权访问角色提供了一组基本角色，您可以根据具体要求将这些角色分配给您企业中的管理员和用户。 现有 CA Access Control 企业管理 附带了以下特权访问角色：

- **紧急情况**－具有该角色的用户可以启动紧急情况特权帐户密码签出。 通过紧急情况签出，用户可以立即访问自己没有特权访问权限的端点。 默认情况下，该角色将分配给 CA Access Control 企业管理 中的所有用户。
- **端点特权访问角色**－具有该角色的用户可以对指定端点类型执行特权帐户任务。 您第一次定义新类型的端点时，CA Access Control 会创建相应的端点特权访问角色。 例如：您第一次在 CA Access Control 企业管理 中创建 Windows 端点时，CA Access Control 会创建 Windows Agentless Connection 端点特权访问角色。
- **特权帐户请求**－具有该角色的用户可以提交或删除特权帐户密码的请求。 默认情况下，该角色将分配给 CA Access Control 企业管理 中的所有用户。
- **PUPM 批准人**－具有该角色的用户可以响应 CA Access Control 企业管理 用户已经提交的特权访问请求。 默认情况下，该角色将分配给 CA Access Control 企业管理 中的所有用户。
- **PUPM 审核管理员**－具有该角色的用户可以审核特权帐户活动并管理 CA Enterprise Log Manager 审核收集参数。
- **PUPM 策略管理员**－具有该角色的用户可以管理角色成员和成员策略、分配角色所有者，以及创建和删除角色。

- **PUPM 目标系统管理员**－具有该角色的用户可以管理密码策略和特权帐户，并可执行特权帐户发现向导以发现端点上的特权帐户。
- **PUPM 用户**－具有该角色的用户可以签入和签出其可以使用的特权帐户密码。 默认情况下，该角色将分配给 CA Access Control 企业管理 中的所有用户。
- **PUPM 用户管理员**－具有该角色的用户可以管理 CA Access Control 企业管理 用户和组及密码策略，以及管理用户的工作项。

将特权访问角色分配给用户时，应当注意以下方面：

- 要响应特权帐户请求，用户必须具有“PUPM 批准人”角色，而且必须是请求用户的管理员。
- 如果用户具有“紧急情况”、“特权帐户请求”或“PUPM 用户”角色，但还没有端点特权访问角色，则该用户无法访问任何端点。 实际上，该用户无法执行任何任务。
- 如果用户具有端点特权访问角色，但没有任何其他角色，则该用户无法执行任何任务。

创建特权访问角色

特权访问角色定义角色成员、管理员和所有者可在使用 PUPM 时执行的任务，例如：签入和签出特权帐户。 如果 CA Access Control 企业管理 中的预定义特权访问角色不适合您的组织要求，您可以创建新的角色。

创建特权访问角色

1. 在 CA Access Control 企业管理 中，执行如下操作：
   a. 单击“用户和组”。
   b. 单击“角色”子选项卡。
   c. 在左侧的任务菜单中展开特权访问角色树。
      此时“创建特权访问角色”任务会显示在可用任务列表中。
2. 单击“创建特权访问角色”。
   此时出现“创建角色: 选择特权访问角色”页面。

3. （可选）按如下方式选择一个现有的特权访问角色来创建新角色作为其副本：
   a. 选择“创建角色副本”。
   b. 选择要搜索的属性，键入筛选值，然后单击“搜索”。
      此时将显示匹配筛选条件的特权访问角色的列表。
   c. 选择要用作新特权访问角色基础的对象。
4. 单击“确定”。
   将显示“创建管理角色”任务页面。 如果管理角色是从现有对象创建的，则对话框字段中会预先填充来自现有对象的值。
5. 在该对话框的“配置文件”选项卡中填写以下字段：
   名称
      定义策略的名称。
   说明
      角色的文本说明。
   已启用
      指定角色是否可以分配给用户和组。
6. 按如下方式将任务添加到角色：
   a. 单击“任务”选项卡。
   b. （可选）从“筛选”任务下拉列表中选择任务类别
      此类别的任务即会加载。
      注意：该任务类别与 CA Access Control 企业管理 中显示此类别中任务的选项卡匹配。
   c. 从“添加任务”下拉列表中选择一项任务。
      该任务即被添加到角色。
   d. 重复步骤 b 至 c 以将更多的任务添加到角色。
7. 添加成员和范围规则 (p. 25)。
8. 单击“提交”。
   该角色即已创建。

用于将角色分配给用户的方法

可以使用以下方法将角色分配给用户：

- 通过使用“修改角色成员/管理员”任务，在角色中添加或删除多个用户。
- 通过使用“修改用户”任务上的“管理角色”选项卡或“特权访问角色”选项卡，在单一用户中添加或删除角色。
- 使用“修改管理角色”任务或“修改特权访问角色”选项卡上的“成员”选项卡修改角色的成员策略。

如何将用户添加到管理角色中

一旦创建管理角色，即可将成员和管理员添加到该角色中。 属于某角色的成员会分配属于该角色的权限。 下列步骤是将成员添加到角色中的先决条件：

1. 修改管理角色成员策略定义来定义该规则的成员。

   通过修改角色成员策略，您可以将属于其他角色成员的用户添加到您正在修改的角色中。

   示例： *其中“登录名”= "Administrator" 或“管理角色”= "SystemManager"*

2. 确认管理员是否可以将成员添加到该角色或将其从中删除。
3. 定义当用户被添加到该角色或将其从中删除时执行的操作。

   示例： *将 SystemManager 添加到“管理角色”中，从“管理角色”中删除 SystemManager*。

4. 修改管理策略以便将用户作为管理员添加到管理规则中的该角色，并为该用户分配管理员权限。

   作为角色管理员添加的用户有权将成员添加到该角色中。

   现在，您可以将成员添加到该角色中。

添加成员和范围规则

定义角色的配置文件和任务后，可添加成员、管理员和所有者。

添加成员和范围规则

1. 单击“成员”选项卡，并执行以下操作：
   a. 单击“添加”。
   b. 为成员策略 (p. 27)指定“成员规则”和“范围规则”，然后单击“确定”。
   c. （可选）选择“管理员可以添加和删除该角色的成员”，并指定添加操作和删除操作 (p. 27)。

   该角色的成员策略即已创建。
2. 单击“管理员”选项卡，并执行以下操作：
   a. 单击“添加”。
   b. 指定“管理规则”和“范围规则”，并为管理策略 (p. 28)指定管理员权限，然后单击“确定”。
   c. （可选）选择“管理员可以添加和删除该规则的管理员”，并指定添加操作和删除操作 (p. 27)。

   该角色的管理策略即已创建。
3. 单击“所有者”选项卡，单击“添加”，指定一项所有者规则 (p. 28)，然后单击“确定”。

   该策略的所有者规则即已创建。

成员策略

*成员策略*定义可以执行某一角色的任务的用户。 成员策略包含以下内容：

- **成员规则**－定义可以执行该角色的用户
- **范围规则**－定义用户可以管理的对象

例如：管理角色、连接、特权帐户以及策略都属于对象。 可以在范围规则中指定许多其他对象。 每个成员策略可以具有多个成员规则，每个成员规则可以具有多个范围规则。

示例：纽约 CA Access Control 主机管理员的成员策略

Don Hailey 是 Forward, Inc 公司的 IT 经理，并且具有“系统管理员”管理角色。 Don 想创建一个管理角色，仅允许具有“CA Access Control 主机管理员”管理角色的纽约员工管理 Forward, Inc 纽约办公室中的主机和主机组。 所有纽约员工都是 NY 员工组的成员，纽约的所有主机和主机组的名称均以字母 NY 开头。

Don 将创建以下成员策略。 该成员策略包含两个成员规则。 第一个成员规则不包含范围规则。 第二个成员规则包含两个范围规则：

- 成员规则 1－管理角色包含“AC 主机管理员”。
- 成员规则 2－作为“NY 员工”组的成员的用户；范围规则－名称以“NY”开头的主机，以及名称以“NY”开头的主机组。

添加和删除操作

如果指定某管理角色的管理员可以在该角色中分配和取消分配用户，必须为该管理角色指定添加和删除操作。

添加和删除操作包含以下内容：

- **添加操作**－确保用户符合角色成员规则之一的条件
- **删除操作**－确保用户不再符合角色成员规则之一的条件

管理策略

*管理策略*指定身为管理角色的管理员的用户。 管理角色管理员可管理管理角色的成员策略，并可在该管理角色中添加和删除用户和组。

管理策略包含以下内容：

- **管理规则**－定义身为角色的管理员的用户
- **范围规则**－定义管理员可以管理的用户
- **管理员的权限**－指定管理员是否可以管理该管理角色的成员和管理员

角色所有者

角色所有者可在管理角色中添加和删除任务。 只能定义一个所有者规则，但可以在该所有者规则中指定不同组的成员。

创建管理任务

如果 CA Access Control 企业管理 中的预定义管理任务不适合您的组织要求，您可以创建管理任务。

创建管理任务

1. 选择“用户和组”选项卡，选择“任务”链接，然后单击“创建管理任务”。

   此时出现“创建管理任务: 选择管理任务”页面。

2. 选择“新建管理任务”，然后单击“确定”。

   此时出现“创建管理任务”页面的“配置文件”选项卡。

   注意：要创建现有管理任务的副本，请选择“创建管理任务副本”，搜索要复制的管理任务，选择该管理任务，然后单击“确定”。

3. 输入任务名称和说明。 请注意，将光标置于标记字段中时，名称便会出现在该字段中。

4. 从菜单中选择该任务在任务列表中的位置。

5. 选择该任务所属的类别。

6. （可选）选择顺序和最多三项 (3) 任务的类别名。

7. 选择该任务所属的主要对象。 主要对象是该任务可以出现在其中的最高类别。

8. 选择要与该任务关联的操作。

9. 选择是否将用户和帐户与该任务进行同步。

10. 请选择以下选项之一：

    隐藏在菜单中

    选择不显示该任务。

    公共任务

    选择使该任务对所有用户可用。

    启用审核

    选择为该任务启用审核事件日志。

    启用工作流

    选择启用工作流。

    启用 Web 服务

    选择启用使用 Web 服务访问该任务。

    工作流流程

选择要与该任务关联的工作流流程。

11. 选择任务优先级。
12. 选择“提交”。

    CA Access Control 企业管理 将创建管理任务。

更多信息：

添加搜索屏幕 (p. 30)
添加选项卡 (p. 30)
配置字段、事件和角色使用 (p. 31)

添加搜索屏幕

选择要与该任务关联的搜索屏幕。 在此选项卡中，可以选择在该任务中使用现有搜索屏幕，或创建新搜索屏幕显示信息并提供特定于该任务的搜索选项。

添加搜索屏幕

1. 选择浏览按钮以搜索现有搜索屏幕，或创建新搜索屏幕。

   注意：要创建现有搜索屏幕的副本，请选择“从其他任务复制范围”，搜索要复制的管理任务，选择该管理任务，然后单击“确定”。
2. 选择“新建”以创建新的搜索屏幕。
3. 选择要创建的搜索屏幕的类型。
4. 输入所需信息，然后单击“确定”。

   新搜索屏幕即会被添加到该任务。

添加选项卡

使用选项卡屏幕选择要用于该任务的选项卡控制器以及将在该任务中显示的选项卡。

添加选项卡

1. 选择要在该任务中使用的选项卡控制器。

   注意：要创建现有选项卡定义的副本，请选择“从其他任务复制选项卡”，搜索要复制的管理任务，选择该管理任务，然后单击“确定”。
2. 从菜单中选择将在该任务中显示的选项卡。
3. 单击“提交”。

   CA Access Control 企业管理 即会将该选项卡添加到新任务中。

配置字段、事件和角色使用

字段、事件和角色使用选项卡来显示有关该任务访问的字段、与该任务关联的事件以及显示该任务的用户角色的信息。 不能更改这些字段中显示的信息。

可以通过更改设置来更改这些选项卡显示的信息。 例如：要更改显示该任务的管理角色，请将管理角色设置修改为包括或排除该任务。

用户、组和管理角色

创建用户时，可为其分配一个或多个“*管理角色*”或“*特权访问角色*”。 管理角色包含与 CA Access Control 企业管理 中的应用程序功能对应的任务。 将管理角色分配给某用户后，该用户可以执行该管理角色中包含的任务。 通过这些任务，用户可以执行 CA Access Control 功能，例如：创建策略、部署策略、创建主机组以及管理其他用户。

特权访问角色定义与受管端点上的特权帐户管理相对应的任务。 将特权访问角色分配给某用户后，该用户可以执行特权帐户管理任务，例如：签入和签出特权帐户密码。

要使管理更容易，可以创建用户组，并将管理角色分配给组。 然后，该组中的每个用户都可以完成该管理角色中的所有任务。

更多信息：

创建用户 (p. 32)
组类型 (p. 35)

Active Directory 限制

如果使用 Active Directory 作为用户存储，您将无法在 CA Access Control 企业管理 中创建和删除用户和组。 您在界面中看不到以下任务，您也无法将这些任务分配给管理角色或特权访问角色：

- 创建用户
- 删除用户
- 修改角色成员/管理员
- 创建组
- 删除组

您将管理角色分配给 Active Directory 用户时，CA Access Control 企业管理 会修改用户配置文件并注意到在注册地址字段中被分配给该用户的管理角色。

注意：您可以选择在用户 DN: 参数中定义具有只读权限的用户。 但是，如果为用户定义只读权限，您无法在 CA Access Control 企业管理中将管理角色或特权访问角色分配给用户。 您另外修改每个角色的成员策略来指向 Active Directory 组。

创建用户

用户可在 CA Access Control 企业管理 中执行任务。 安装 CA Access Control 企业管理 时，可创建具有“系统管理员”角色的用户。 启动 CA Access Control 企业管理 以强制实施职责独立时，可创建其他用户。

注意：如果使用 Active Directory 作为用户存储，将无法在 CA Access Control 企业管理 中创建用户。

创建用户

1. 在 CA Access Control 企业管理 中，单击“用户和组”。

   此时“创建用户”任务会显示在可用任务列表中。

2. 单击“创建用户”。

   此时出现“创建用户: 选择用户”窗口。

3. （可选）按如下方式选择一个现有用户来创建新用户作为其副本：
   a. 选择“创建用户副本”。
   b. 选择要搜索的属性，键入筛选值，然后单击“搜索”。
      此时将显示匹配筛选条件的用户的列表。
   c. 选择要用作新用户基础的对象。
4. 单击“确定”。

   将显示“创建用户”任务页面。 如果用户是从现有对象创建的，则对话框字段中会预先填充来自现有对象的值。
5. 填写“配置文件”选项卡中的字段。 以下字段需加以说明：

   用户 ID

   定义标识 CA Access Control 企业管理 用户的字符串。这是用户用来登录的名称。

   密码必须更改

   指定强制用户在首次登录时更改密码。

   已启用

   指定用户是否可以登录到 CA Access Control 企业管理。
6. （可选）按如下方式单击“管理角色”选项卡，将管理角色分配给用户：
   a. 单击“添加管理角色”。
      此时出现“选择管理角色”部分。
   b. 键入筛选值，然后单击“搜索”。
      此时将显示匹配筛选条件的角色的列表。
   c. 选择要分配给用户的管理角色，然后单击“选择”。

   管理角色即会被分配给用户。
7. （可选）按如下方式单击“特权访问角色”选项卡以将特权访问角色分配给用户：
   a. 单击“添加特权访问角色”。
      此时出现“选择特权访问角色”部分。
   b. 键入筛选值，然后单击“搜索”。
      此时将显示匹配筛选条件的角色的列表。
   c. 选择要分配给用户的特权访问角色，然后单击“选择”。

   特权访问角色即会被分配给用户。

8. （可选）按如下方式单击“组”选项卡，将用户添加到组中：
   a. 单击“添加组”。
      此时出现“选择组”部分。
   b. 键入筛选值，然后单击“搜索”。
      此时将显示匹配筛选条件的组的列表。
   c. 选择要分配给用户的组，然后单击“选择”。
   该用户即被添加到组。
9. 单击“提交”。
   用户即已创建。

重置用户密码

用户帐户在几次登录尝试失败被锁定时，或者用户丢失或忘记了密码时，需要重置用户密码。

重置用户密码

1. 在 CA Access Control 企业管理 中，单击“用户和组”。
   此时“重置用户密码”会显示在可用任务列表中。
2. 单击“重置用户密码”。
   此时会打开“重置用户密码”搜索页面。
3. 键入搜索查询，然后单击“搜索”。
   查询会根据搜索条件显示结果。
4. 选择用户帐户，然后单击“选择”。
   此时会打开重置密码窗口。
5. 在“确认密码”字段中键入帐户密码。
6. （可选）选择“密码必须更改”选项。
7. 单击“提交”。
   此时 CA Access Control 企业管理 会重置用户密码。

启用或禁用用户

启用用户帐户后，用户便可以使用帐户凭据登录到 CA Access Control 企业管理。 禁用用户帐户可防止该用户访问 CA Access Control 企业管理，并在系统中保留用户配置文件。

启用或禁用用户

1. 在 CA Access Control 企业管理 中，单击“用户和组”。

   此时“启用/禁用用户”任务会显示在可用任务列表中。

2. 单击“启用/禁用用户”。

   此时出现“启用/禁用用户”页面。

3. 定义搜索查询，然后单击“搜索”。

   此时出现与搜索查询相匹配的用户的列表。

4. 按如下方式指定要禁用和启用的用户帐户：

   - 清除某个用户以禁用该帐户。
   - 选择某个用户以启用该帐户。

5. 单击“选择”。

   此时出现一个总结了指定更改的屏幕。

6. 单击“是”确认所做的修改。

   CA Access Control 企业管理 即会提交任务以执行所请求的更改。

组类型

可以创建多种类型的组或这些类型的组合：

- **静态组**

  以交互方式添加的用户的列表。

- **动态组**

  用户如果符合某个 LDAP 查询即属于组。（需要一个 LDAP 目录作为用户存储）。

  注意：要查看动态组查询字段，您必须通过编辑关联的配置文件屏幕将其包括在任务中。

- **嵌套组**

  包含其他组的组。（需要一个 LDAP 目录作为用户存储）。

  注意：要查看用户所属的静态组、动态组和嵌套组，请使用“用户”对象的“组”选项卡。 此选项卡显示在“查看用户”和“修改用户”任务中。

创建静态组或动态组

可以将静态组中的一组用户关联起来。 可通过在组成员资格列表中添加或删除用户来管理组。 要查看组的成员，请使用“查看组”或“修改组”任务中的“成员资格”选项卡。

可使用 CA Access Control 企业管理 通过定义 LDAP 筛选查询来创建动态组，以确定运行时的组成员资格。

注意：“成员资格”选项卡仅显示显式添加至组中的成员。 如果使用 Active Directory 作为用户存储，则无法在 CA Access Control 企业管理 中创建组。

创建静态组或动态组

1. 作为具有组管理权限的用户登录 CA Access Control 企业管理。
2. 依次选择“组”、“创建组”。

   此时出现“创建组”搜索屏幕。
3. 选择创建一个组，然后单击“确定”。

   此时出现组配置文件选项卡。
4. 输入组名和说明。
5. 导航到“成员资格”选项卡。

   注意：只有具有“修改组”任务的管理员才能更改组的动态成员资格。
6. 单击“添加用户”。

   此时会打开“选择用户”搜索窗口。
7. 输入搜索查询，然后单击“搜索”。

   查询会根据搜索条件返回结果。
8. 选择一个用户，然后单击“选择”。

   导航到“管理员”选项卡。
9. 单击“提交”。

   此时出现一条消息，通知您此过程已成功完成。

   注意：将某个用户分配为组管理员时，请验证该管理员的角色是否具有管理该组的相应范围。

LDAP 筛选查询－定义动态组查询参数

可使用 CA Access Control 企业管理 通过定义 LDAP 筛选查询来创建动态组，以确定运行时的组成员资格。

该筛选查询具有以下格式：

LDAP:///*search_base_DN*??*search_scope*?*searchfilter*

search_base_DN

定义在 LDAP 目录中开始搜索的起始点。 如果未在查询中指定基本 DN，则该组的组织为默认的基本 DN。

search_scope

指定搜索的范围，其中包括：

- **sub**－返回基本 DN 及以下级别的条目。
- **one**－返回比您在 URL 中指定的基本 DN 低一个级别的条目。
- **base**－改为使用 one，忽略 base 作为搜索选项。

使用 *one* 或 *base* 仅获取基本 DN 组织中的用户。

使用 *sub* 获取基本 DN 组织以及树中的所有下级组织下的所有用户。

searchfilter

定义您希望应用到搜索范围内的条目的筛选。 输入搜索筛选时，请使用标准 LDAP 查询语法，如下所示:

([*logical_operator*]*Comparison*)

logical operator

定义逻辑运算符。 可以为以下项之一：

- **|**－逻辑“或”
- **&**－逻辑“与"
- **!**－逻辑“非”

Comparison

定义 *AttributeOperatorValue*

- *Attribute*－定义 LDAP 属性的名称。
- *Operator*－指定比较运算符。 可以为以下项之一：**=**（等于）、**<=**（小于或等于）、**>=**（大于或等于）或 **~=**（约等于）。
- *Value*－定义属性数据的值。

示例：(&(city=Boston)(state=Massachusetts))

默认值：(objectclass=*)

创建动态查询时，请注意以下事项：

- “LDAP”前缀必须小写，例如：

  ```
  ldap:///o=MyCorporation??sub?(title=Manger)
  ```

- 不能指定 LDAP 服务器主机名或端口号。 所有搜索都在您为环境配置的 LDAP 目录中进行。

示例：示例 LDAP 查询

以下为 LDAP 查询示例：

说明	查询
所有经理用户。	ldap:///o=MyCorporation??sub?(title=Manger)
纽约西部分支机构的所有经理	ldap:///o=MyCorporation??one?(&(title=Manager) (office=NYWest))
所有配有手机的技术人员	ldap:///o=MyCorporation??one? (&(employeetype=technician) (mobile=*))
员工编号在 1000 到 2000 之间的所有员工	ldap:///o=MyCorporation, (& (ou=employee) (employeenumber >=1000) (employeenumber <=2000))
所有在公司任职超过 6 个月的帮助中心管理员	ldap:///o=MyCorporation,(& (cn=helpdeskadmin) (DOH => 2004/04/22) **注意：**此查询要求您为用户入职日期创建一个 DOH 属性。

注意： > 和 <（大于和小于）比较按词典编纂顺序而非算术顺序进行。 有关其用法的详细信息，请参阅 LDAP 目录服务器相关文档。

修改组成员

可使用该选项来添加或删除成员和组。 可使用以下过程来修改组的成员列表。

修改组成员

1. 作为具有组管理权限的用户登录 CA Access Control 企业管理。
2. 依次选择“组”、“修改组成员”。

   此时出现“修改组成员”屏幕。
3. 选择一个组，然后单击“选择”。

   此时会打开组成员列表。

4. 要删除一个成员，请清除该成员名旁边的复选框。
5. 要添加一个成员，请单击“添加用户”。
   a. 键入搜索查询，然后单击“搜索”。

      搜索查询将根据搜索条件显示结果。
   b. 选择用户，然后单击“选择”。

      该用户即被添加为组成员。
6. 要添加一个组，请单击“添加组”按钮。
   a. 键入搜索查询，然后单击“搜索”。

      搜索查询将根据搜索条件显示结果。
   b. 选择组，然后单击“选择”。

      此时会添加该组。
7. 单击“提交”。

   此时出现一条确认消息，通知您已成功完成任务。

审核数据

审核数据为在 CA Access Control 企业管理 环境中执行的操作提供了历史记录。 审核数据示例包括：

- 指定时间段的系统活动。
- 在特定时间段内修改的对象的列表。
- 分配给用户的角色
- 为特定用户帐户执行的操作

审核数据是针对 *事件*生成的。 事件是由 CA Access Control 企业管理 任务生成的操作。 例如：“创建用户”任务可以包括 AssignAccessRoleEvent 事件。

CA Access Control 企业管理 将审核数据存储在中央数据库中。 可以配置一个审核收集器，以便将审核数据传送到 CA Enterprise Log Manager。

注意：有关与 CA Enterprise Log Manager 集成的更多信息，请参阅*《实施指南》*。

更多信息：

搜索提交的任务 (p. 40)
查看任务详细信息 (p. 44)
查看事件详细信息 (p. 44)
清除已提交的任务 (p. 44)
将消息队列审核消息传递到 Windows 事件日志 (p. 46)
将消息队列审核消息传递到 UNIX 系统日志 (p. 48)

搜索提交的任务

提交的任务提供有关 CA Access Control 企业管理 环境中任务的信息。 您可以搜索和查看有关 CA Access Control 企业管理 执行的操作的高级详细信息。 各个详细信息屏幕提供每项任务和事件的其他相关信息。

您可以根据任务的状态取消或重新提交任务。

提交的任务可让您全程跟踪任务的处理。

搜索提交的任务

1. 在 CA Access Control 企业管理 中，依次单击“系统”、“审核”子选项卡。

   此时“查看提交的任务”任务会显示在可用任务列表中。

2. 单击“查看提交的任务”。

   将显示“查看提交的任务”页面。

3. 指定搜索条件 (p. 41)，输入要显示的行数，然后单击“搜索”。

   将显示满足您搜索条件的任务。

搜索查看提交的任务的属性

要查看已提交进行处理的任务，您可以使用“查看提交的任务”中的搜索功能。 您可以根据以下条件搜索任务：

启动人

将启动任务的用户名标识为搜索条件。 根据用户名进行搜索。 要确保您输入了有效的用户名，请使用“验证”按钮。

批准人

将任务批准人姓名标识为搜索条件。 根据用户名进行搜索。 要确保您输入了有效的用户名，请使用“验证”按钮。

注意：如果您选择了“批准任务执行者”条件筛选任务，则默认情况下，也将启用“显示批准任务”条件。

任务名称

将任务名称标识为搜索条件。 可以通过指定条件（例如：等于、包含、始于或终于“任务名称”字段的值）来细化搜索。 例如：您可以选择等于条件，然后在文本字段中输入“创建用户”，以此指定搜索条件“任务名称等于‘创建用户’”。

任务状态

将任务状态 (p. 43)标识为搜索条件。您可以启用“任务状态等于”，然后选择条件，以此选择任务状态。 您可以根据以下条件进一步细化搜索：

- 已完成
- 进行中
- 失败
- 已拒绝
- 部分完成
- 已取消
- 已排定

任务优先级

将任务优先级标识为搜索条件。您可以启用“任务优先级等于”，然后选择条件，以此选择任务优先级。 您可以根据以下条件进一步细化搜索：

低

指定您可以搜索具有低优先级的任务。

中

指定您可以搜索具有中优先级的任务。

高

指定您可以搜索具有高优先级的任务。

执行对象

标识在所选对象实例上执行的任务。 如果您未选择一个对象实例，则将显示在该对象所有实例上执行的任务。

注意：仅当在“配置提交的任务”屏幕上填充“配置执行对象”字段时，才显示该字段。 您可以使用此屏幕配置“提交的任务”选项卡。

日期范围

标识要搜索的提交的任务的日期范围。 您必须提供“起始”和“截止”日期。

显示未提交的任务

标识处于“审核”状态的任务。标识已启动其他任务的任务或还未提交的任务。 如果您选择了此选项卡，将审核并显示所有此类任务。

显示批准任务

标识必须在工作流流程中批准的任务。

更多信息：

任务状态说明 (p. 43)

任务状态说明

已提交的任务处于以下所说明的状态之一。 您可以根据任务的状态执行诸如取消或重新提交任务之类的操作。

注意：要取消或重新提交任务，必须将“查看提交的任务”配置为根据任务状态显示取消和重新提交按钮。

进行中

发生以下任一情况时显示该状态：

- 工作流已启动但尚未完成
- 在当前任务之前启动的任务正在进行中
- 嵌套任务已启动但尚未完成
- 主要事件已启动但尚未完成
- 次要事件已启动但尚未完成

您可以取消处于此状态下的任务。

注意：取消任务会取消当前任务的所有未完成的嵌套任务和事件。

已取消

您取消任何进行中的任务或事件时，将显示该状态。

已拒绝

CA Access Control 企业管理 拒绝工作流流程中的事件或任务时，将显示该状态。 您可以重新提交已拒绝的任务。

注意：重新提交任务时，CA Access Control 企业管理 将重新提交所有已失败或已拒绝的嵌套任务和事件。

部分完成

您取消某些事件或嵌套任务时，将显示该状态。 您可以重新提交部分完成的事件或嵌套任务。

已完成

任务完成时，将显示该状态。 当前任务的嵌套任务和嵌套事件完成之后，该任务才算完成。

失败

任务、嵌套任务或嵌套在当前任务中的事件无效时将显示该状态。任务失败时将显示该状态。 您可以重新提交已失败的任务。

已排定

将该任务排定在稍后的日期执行时，将显示该状态。 您可以取消处于此状态下的任务。

查看任务详细信息

CA Access Control 企业管理 提供任务详细信息，如提交的任务的状态、嵌套任务和与任务关联的事件。

查看提交的任务的详细信息

1. 单击“查看提交的任务”页面中选定任务旁边的右键头图标。

   将显示任务详细信息。

   注意：事件和嵌套任务（如果有）将显示在“任务详细信息”页面中。您可以查看每个任务和事件的任务详细信息。

2. 单击“关闭”。

   此时“任务详细信息”选项卡会关闭，CA Access Control 企业管理 会显示具有任务列表的“查看提交的任务”选项卡。

查看事件详细信息

CA Access Control 企业管理 提供事件详细信息，如已提交事件的状态、事件属性和有关事件的任何其他信息。

查看提交的事件的详细信息

1. 单击“查看任务详细信息”页面中某个事件旁边的右箭头图标。

   将显示事件详细信息。

2. 单击“关闭”。

   将关闭“事件详细信息”页面。

清除已提交的任务

CA Access Control 企业管理 在中央数据库中存储审核数据，包括 PUPM 审核数据。 但是，如果在中央数据库中存储大量审核数据，数据库性能可能会受到影响。 要提高数据库性能，可以使用“清除已提交的任务”向导将提交的任务从中央数据库中删除。

重要说明！ 清除已提交的任务会从数据库中删除审核数据。 为了避免数据丢失，建议您在运行清除任务之前，将审核事件传递到 CA Enterprise Log Manager。

可以将清除任务排定为立即运行或周期性地运行。 清除已提交的任务可能会消耗大量系统资源。 建议您将此任务排定为在业务时间之外运行。

清除已提交的任务

1. 在 CA Access Control 企业管理 中，执行如下操作：
   a. 单击“系统”。
   b. 单击“任务”子选项卡。
   c. 单击“清除已提交的任务”。

      此时出现“清除已提交的任务: 重现”页面。
2. 请执行下列操作之一：
   - 要立即运行任务，请选择“立即执行”，然后单击“下一步”。

     此时出现“清除已提交的任务: 清除已提交的任务”页面。
   - 要创建周期性的日程排定，请选择“排定新作业”并填写显示的字段。 以下字段需加以说明：

     时区

     指定企业管理服务器的时区。

     如果您与服务器处于不同的时区，在排定新作业时，既可选择您的时区，也可选择服务器时区。 在修改现有作业时不能更改时区。

     按周排定

     指定任务在一周中的某一天或某几天的特定时间运行。

     按 24 小时格式指定时间，如 17:15。

     高级排定

     允许您使用 cron 表达式来指定任务运行的时间。

     单击“下一步”。

     此时出现“清除已提交的任务: 清除已提交的任务”页面。
3. 填写以下字段：

   最小时长

   指定 CA Access Control 企业管理 从中央数据库删除处于最终状态（“已完成”、“已失败”、“已拒绝”、“已取消”或“已中止”）的任务的最短时限。

   审核超时

   （可选）指定 CA Access Control 企业管理 从中央数据库删除处于审核状态的任务的最短时限。

   注意：处于审核状态的任务尚未提交。

时间限制

（可选）指定 CA Access Control 企业管理 执行清除操作所用的最长时间。

任务限制

（可选）指定 CA Access Control 企业管理 从中央数据库删除的最大任务数。

单击“完成”。

CA Access Control 企业管理 将在您指定的时间从中央数据库删除提交的任务。

将消息队列审核消息传递到 Windows 事件日志

在 Windows 上有效

您可以配置企业管理服务器将消息队列审核消息传递到 Windows 事件日志。 每次当企业管理服务器将审核消息写入审核日志时，就会将相应的事件发送给事件日志。

将消息队列审核消息传递到 Windows 事件日志

1. 如果 JBoss 应用程序服务器正在运行，请将其停止 。
2. 导航到下列目录，其中 *JBOSS_HOME* 表示您安装 JBoss 的目录：

   JBOSS_HOME\server\default\conf\
3. 打开 jboss-log4j.xml 文件。
4. 在类中添加名为 "ENTM_NTEventLog" 的指示器。

   指示器指定用于审核以及显示数据的方式的类。
5. 创建名为 "EventLog" 的日志。

   您将指示器绑定的记录器指定为审核消息的输入通道。
6. 保存并关闭文件。
7. 将 NTEventLogAppender.dll 文件复制到 Windows System32 目录。

   注意：您可以在 Apache log4j 1.2.16 捆绑包中找到 NTEventLogAppender.dll 文件。 可以从 Apache 日志记录服务网站下载 Apache log4j 1.2.16。
8. 启动 JBoss 应用程序服务器。

   现在，企业管理服务器将消息队列审核消息传递到 Windows 事件日志。

示例：修改 jboss-log4j.xml 文件以将消息队列审核消息发送到 Windows 事件日志

以下片段显示 jboss-log4j.xml 文件，这些文件已配置为将消息队列审核消息传递到 Windows 事件日志：

```
 <appender name="ENTM_NTEventLog"
                       class="org.apache.log4j.nt.NTEventLogAppender">
    <param name="Source" value="CA Access Control Enterprise Management"/>
    <layout class="org.apache.log4j.SimpleLayout"/>
</appender>

<logger name="EventLog">
    <appender-ref ref="ENTM_NTEventLog"/>
</logger>
```

在该示例中，您进行以下更改：

- 按名称 "ENTM_NTEventLog" 添加新的指示器
- 按名称 "org.apache.log4j.nt.NTEventLogAppender" 添加类
- 定义 param 名称："Source"
- 定义值："CA Access Control Enterprise Management"
- 定义布局类："org.apache.log4j.SimpleLayout"
- 定义记录器名称："EventLog"
- 定义指示器 ref ref："ENTM_NTEventLog"

将消息队列审核消息传递到 UNIX 系统日志

在 UNIX 上有效

您可以配置企业管理服务器将消息队列审核消息传递到 UNIX 系统日志。 每次当企业管理服务器将审核消息写入审核日志时，就会将相应的事件发送给系统日志。

将消息队列审核消息传递到 UNIX 系统日志

1. 如果 JBoss 应用程序服务器正在运行，请将其停止 。
2. 导航到下列目录，其中 *JBOSS_HOME* 表示您安装 JBoss 的目录：

   ```
   JBOSS_HOME\server\default\conf\
   ```

3. 打开 jboss-log4j.xml 文件。
4. 在类中添加名为 "ENTM_UNIXEventLog" 的指示器。

   指示器指定用于审核以及显示数据的方式的类。
5. 创建名为 "EventLog" 的日志。

   您将指示器绑定的记录器指定为审核消息的输入通道。
6. 保存并关闭文件。
7. 打开 /etc/syslog.conf 文件，并确认系统日志将消息传递到 /var/log/messages 文件。
8. 打开 /etc/sysconfig/syslog 参数文件，并确认远程模式选项出现在以下条目中：

   ```
   SYSLOGD_OPTIONS="-m 0-r"
   ```

9. 重新启动系统日志后台程序。 运行以下命令：

   ```
   /etc/rc.d/init.d/syslog restart
   ```

   系统日志后台进程启动。
10. 启动 JBoss 应用程序服务器。

    现在，企业管理服务器会将消息队列审核消息传递到 UNIX 系统日志。

示例：修改 jboss-log4j.xml 文件以将消息队列审核消息发送到 UNIX 系统日志

以下片段显示在创建 LogAppender 对象后显示 jboss-log4j.xml 文件：

```
<appender name="ENTM_UNIXSysLog"
                        class="org.apache.log4j.net.SyslogAppender">
    <param name="Facility" value="USER"/>
    <param name="FacilityPrinting" value="false"/>
    <param name="SyslogHost" value="localhost"/>
    <layout class="org.apache.log4j.PatternLayout">
        <param name="ConversionPattern" value="%p - [CA AC ENTM]: %m%n"/>
    </layout>
</appender>

<logger name="EventLog">
    <appender-ref ref="ENTM_UNIXSysLog"/>
</logger>
```

在该示例中，您进行以下操作：

- 添加指示器："ENTM_UNIXSysLog"
- 创建类："org.apache.log4j.net.SyslogAppender"
- 定义 param 名称 "Facility" 和值 "USER"
- 定义 param 名称："FacilityPrinting"具有值"假的"
- 定义 param 名称 "SyslogHost" 以及值 "localhost"
- 定义布局类："org.apache.log4j.PatternLayout"
- 定义 param 名称："ConversionPattern" 以及值 "%p - [CA AC ENTM]: %m%n"
- 定义记录器名称："EventLog"
- 定义 appender-ref: ref="ENTM_UNIXSysLog"

电子邮件通知

电子邮件通知从电子邮件模板生成，向 CA Access Control 企业管理 用户通知系统中的事件。 如果您启用电子邮件通知，CA Access Control 企业管理 可以在以下情况之一发生时生成电子邮件通知：

- 需要批准或拒绝的事件处于挂起状态。
- 批准人批准事件。
- 批准人拒绝事件。
- 事件启动、失败或完成。
- 创建或修改 CA Access Control 企业管理 用户。

注意：有关如何启用电子邮件通知的详细信息，请参阅 *《实施指南》*。

电子邮件模板

CA Access Control 企业管理 从电子邮件模板生成电子邮件通知。 每个电子邮件模板都包含以下信息：

- **递送信息** — 电子邮件收件人的列表。
- **主题** — 用于电子邮件的主题行的文本。
- **内容** — 电子邮件正文。 正文通常包括静态文本和变量，CA Access Control 企业管理 根据触发电子邮件的任务或事件来解析这些内容。

电子邮件模板位于以下目录，其中 *JBoss_home* 是您安装 JBoss 的目录：

JBoss_home/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default

emailTemplates 目录包含五个子目录。 每个文件夹都与一个事件状态相关联。 下表列出每个子目录中的电子邮件模板的用途：

子目录	内容
Approved	■ CertifyRoleEvent.tmpl — 过时。 ■ CheckOutAccountPasswordEvent.tmpl — 通知收件人：特权帐户密码请求已批准。 ■ CreatePrivilegedAccountExceptionEvent.tmpl — 通知收件人：特权帐户密码请求已批准，期限为设定的时间段（该模板与特权帐户请求任务相对应）。 ■ defaultEvent.tmpl — 通知收件人：事件已批准。 ■ defaultTask.tmpl — 通知收件人：任务已批准。 ■ ForgottenPasswordEvent.tmpl — 过时。 ■ SelfRegisterUserEvent.tmpl — 过时。
Completed	■ AccumulatedProvisioningRolesEvent.tmpl — 过时。 ■ CertificationNonCertifiedActionCompletedNotificationEvent.tmpl — 过时。 ■ CertificationNonCertifiedActionPendingNotificationEvent.tmpl — 过时。 ■ CertificationRequiredFinalReminderNotificationEvent.tmpl — 过时。 ■ CertificationRequiredNotificationEvent.tmpl — 过时。 ■ CertificationRequiredReminderNotificationEvent.tmpl — 过时。 ■ CheckOutAccountPasswordEvent.tmpl — 通知收件人他们签出的特权帐户的密码。 ■ CreateProvisioningUserNotificationEvent.tmpl — 过时。 ■ defaultEvent.tmpl — 通知收件人：CA Access Control 企业管理 已完成事件。 ■ defaultTask.tmpl — 通知收件人：CA Access Control 企业管理 已完成任务。 ■ ForgottenPassword.tmpl — 过时。 ■ ForgottenUserID.tmpl — 过时。 ■ Self Registration.tmpl — 过时。

子目录	内容
Invalid	■ AssignProvisioningRoleEvent.tmpl — 过时。 ■ DefaultEvent.tmpl — 通知收件人：事件失败。 ■ DefaultTask.tmpl — 通知收件人：任务失败。
Pending	■ BreakGlassCheckOutAccountEvent.tmpl — 通知批准人：已执行紧急情况签出。 ■ CertifyRoleEvent.tmpl — 过时。 ■ CheckOutAccountPasswordEvent.tmpl — 通知批准人：特权帐户签出请求需要予以注意。 ■ defaultEvent.tmpl — 通知批准人：工作列表中所列的项目需要予以注意。 ■ defaultTask.tmpl — 通知批准人：任务需要予以注意。 ■ ModifyUserEvent.tmpl — 过时。
Rejected	■ CertifyRoleEvent.tmpl — 过时。 ■ CheckOutPasswordEvent.tmpl — 通知收件人：特权帐户密码请求已被拒绝。 ■ CreatePrivilegedAccountExceptionEvent.tmpl — 通知收件人：在设定的时间段内访问特权帐户的用户请求已被拒绝（该模板与特权帐户请求任务相对应）。 ■ defaultEvent.tmpl — 通知收件人：事件已被拒绝。 ■ defaultTask.tmpl — 通知收件人：任务已被拒绝。 ■ ForgottenPasswordEvent.tmpl — 过时。 ■ SelfRegisterUserEvent — 过时。

电子邮件通知的工作原理

电子邮件通知向 CA Access Control 企业管理 用户通知系统中的事件。 以下过程说明了电子邮件通知的工作原理：

1. 在事件发生时，CA Access Control 企业管理 会检查是否为该事件启用了电子邮件通知。
2. 如果电子邮件通知已启用，CA Access Control 企业管理 会在相应的子目录中查找事件类型。

   例如，如果即将发送电子邮件进行特权帐户请求的批准，CA Access Control 企业管理会在 "Approved" 子目录中查找。
3. CA Access Control 企业管理 会检查与事件具有相同名称的电子邮件模板子目录，然后执行以下操作之一：
   - 如果存在与事件具有相同名称的电子邮件模板，CA Access Control 企业管理 会将该电子邮件模板发送给收件人。
   - 如果不存在与事件具有相同名称的电子邮件模板，CA Access Control 企业管理 会将 defaultEvent.tmpl 电子邮件模板发送给收件人。

注意：有关如何配置电子邮件通知设置的详细信息，请参阅*《实施指南》*。

自定义电子邮件模板

CA Access Control 企业管理 从电子邮件模板生成电子邮件通知。 您可以自定义电子邮件模板来适合您企业的要求。

自定义电子邮件模板

1. 在可编辑的表单中打开模板。
2. 通过执行以下操作之一或全部，来编辑电子邮件模板：
   - 在模板的正文中键入静态文本。
   - 使用电子邮件模板 API 中的变量在模板中指定动态内容。
3. 保存并关闭该模板。

注意：有关电子邮件模板 API 的更多信息，请参阅*《CA Identity Manager 管理指南》*。

第 3 章： 查看企业实施

此部分包含以下主题：

全局查看

通过 CA Access Control 企业管理 中的“全局查看”，可查看在连接的 DMS 上进行管理的 CA Access Control 的企业实施。

使用“全局查看”可以：

- 标识向连接的 DMS 报告的端点。
- 标识端点类型，端点类型可以是 CA Access Control、PMDB、PUPM 和 UNAB 中的一个或多个。
- 查看每个端点上次将检测信号发送至 DMS 的时间。
- 查看有关端点的更多详细信息，例如：部署了哪些策略、操作系统是什么以及端点上有哪些受管设备。
- 打开 CA Access Control 端点管理 来管理 CA Access Control 端点。
- 修改 UNAB 主机或 PUPM 受管设备。

查看企业 CA Access Control 实施

使用 CA Access Control 企业管理 可以显示 CA Access Control 的企业实施。 该企业“全局查看”是所有端点、它们所编组到的逻辑主机组、这些端点上的部署策略以及它们所拥有的受管设备的快照。

查看企业 CA Access Control 实施

1. 在 CA Access Control 企业管理 中，单击“全局查看”选项卡，然后单击左侧任务菜单中的“全局查看”链接。

   将显示“全局查看”页面，其中显示了“搜索”区域。

2. （可选）定义搜索条件。

   可以使用两种类型的搜索：

   - **简单**－使用简单搜索可定义主机名掩码，并指定筛选结果所依据的端点类型。
   - **高级**－单击“高级”链接还可以按指定主机组、分配的策略，受管设备名掩码以及受管设备类型来筛选结果。

   注意：默认情况下，“全局查看”将显示对 CA Access Control 企业管理 连接到的 DMS 定义的所有端点的结果。

3. 单击“执行”。

   将按以下类别之一显示符合所定义条件的结果：

   - **按主机名列出结果**－这些是在 DMS 上定义的主机（端点）。 这是结果的默认显示类别。
   - **按主机组列出结果**－这些是所定义的逻辑主机组。
   - **按策略列出结果**－这些是在端点上部署的策略。
   - **按受管设备列出结果**－这些是端点上的受管设备。

打开 CA Access Control 企业管理 以管理端点

CA Access Control 企业管理 支持单点登录 (SSO)，您可以轻松登录 CA Access Control 端点管理 以管理 CA Access Control 企业管理 管理的任何端点。

如果您希望设置自动登录以管理 Windows 端点，请确认您在 CA Access Control 企业管理 和 CA Access Control 端点中使用相同的用户名和密码，而且您具有使用 CA Access Control 端点管理 管理端点的终端访问权限。

注意：要设置自动登录以管理 UNIX 端点，需要为 CA Access Control 端点管理 SSO 配置该端点。

打开 CA Access Control 企业管理 以管理端点

1. 使用“全局查看”查看要管理的一个或多个端点。
2. 单击“操作”列中的“管理”。

   此时将打开 CA Access Control 端点管理，并将自动输入端点主机名和您的凭据。 如果 CA Access Control 端点管理 中不存在您登录所用的 CA Access Control 企业管理 用户，则需要手动输入凭据。

更多信息：

查看企业 CA Access Control 实施 (p. 56)
为 CA Access Control 端点管理 SSO 配置 UNIX 端点 (p. 57)

为 CA Access Control 端点管理 SSO 配置 UNIX 端点

通过 CA Access Control 企业管理 可轻松登录 CA Access Control 企业管理，以管理 CA Access Control 企业管理 管理的任何端点。 在自动登录中，使用您的 Active Directory 凭据登录到 CA Access Control 企业管理。 CA Access Control 企业管理 会保留这些凭据，并在您打开 CA Access Control 端点管理 管理端点时向端点提供这些凭据。 使用 CA Access Control 端点管理 自动登录到 CA Access Control 依赖于您用来验证 CA Access Control 企业管理 的用户帐户。

注意：要配置自动登录到 UNAB 端点，请确认 CA Access Control 企业管理 和 UNAB 使用相同的 Active Directory。

重要说明！ 配置您想在 Active Directory 中用作 UNIX 用户的用户。

为 CA Access Control 端点管理 SSO 配置 UNIX 端点

1. 在 CA Access Control 端点上，打开 seos.ini 文件，找到 [OS_User] 部分，然后将标记 osuser_enabled 的值设为 **1**。

   企业用户和组被启用。

2. 找到 [seos] 部分，然后将标记 auth_login 的值设为 **pam**。

   使用的登录授权方式是 PAM。

3. 创建 CA Access Control 端点管理 计算机的 TERMINAL 记录。

   CA Access Control 端点管理 计算机被分配了 TERMINAL 访问。

4. 将您用来登录到 CA Access Control 企业管理 的用户帐户配置为 XUSER，并为其分配 ADMIN 属性。 使用以下格式：*<DOMAIN-NAME>user_account*。

5. 使用读取和写入访问权限在 TERMINAL 类中定义超级用户的 ACL。例如：

   ```
   Defaccess          : R, W
   ACLs               :
       Accessor                Access
       DOMAIN\user(XUSER  ) R, W
   ```

   用户可以使用 CA Access Control 企业管理 服务器管理端点。

修改 PUPM 端点

使用 CA Access Control 企业管理 全局查看，可以修改 PUPM 端点受管设备的设置。 受管设备是您使用特权帐户进行管理的应用程序。 PUPM 端点会将这些特权帐户存储在密码数据库中，并使用基于角色的管理系统授予对帐户的访问权限。 受管设备可以安装在 PUPM 端点本身或企业中。

修改 PUPM 端点

1. 依次选择“全局查看”、“全局查看”任务。

   此时将显示“全局查看”搜索屏幕。

2. 键入查询，然后单击“执行”。

   查询即会显示搜索结果。

3. 单击要修改的 PUPM 端点所在行的向下箭头（显示）图标。

   扩展信息将显示端点上的受管设备。

4. 单击“修改”以修改端点设置。

   此时出现“修改端点”窗口，其中显示了端点设置。

5. 修改端点设置并单击“提交”。

   此时将显示一条消息，通知您任务已完成。

更多信息：

创建端点 (p. 151)

第 4 章： 集中管理策略

此部分包含以下主题：

策略类型

在 CA Access Control 企业管理 中，使用三种类型的策略来管理 CA Access Control 端点和 UNAB 主机：CA Access Control 策略，UNAB 配置策略以及 UNAB 登录策略。

使用 CA Access Control 策略创建统一的策略，用于在整个企业中控制对资源的访问以及设置对 CA Access Control 端点的访问者权限。

使用 UNAB 登录策略在企业中管理对 UNIX 主机的访问。 登录策略控制用户对运行 UNAB 的 UNIX 主机的登录。 CA Access Control 企业管理 根据您填写的授权列表自动创建、分配和部署登录策略。

您使用 UNAB 配置策略来设置远程 UNAB 主机上的配置文件中标记的值，从而便于在组织中部署和配置 UNAB 主机。

更多信息：

管理 UNAB 登录授权 (p. 246)
配置 UNAB 主机或主机组 (p. 247)

集中管理策略的方法

您可以使用 CA Access Control 采用以下方式从一台计算机管理多个数据库：

- **基于规则的自动策略更新** - 您在中央数据库 (PMDB) 中定义的常规规则会自动传播给已配置的层级结构中的数据库。

  注意：仅此方法提供双重控制，并且仅适用于 UNIX。 有关基于规则的自动策略更新的双重控制信息，可以在*《端点管理指南：用于 UNIX》*上找到。 有关基于规则的自动策略更新的信息，可以在*《端点管理指南：用于 Windows》*上找到。

- **高级策略管理** - 根据主机或主机组分配将您部署的策略（规则组）传播到所有数据库。 您还可以取消部署（删除）策略以及查看部署状态和部署偏差。 要使用此功能，您需要安装并配置额外的组件。

  注意：有关高级策略管理的信息，可以在*《企业管理指南》*中找到。

高级策略管理

您所创建的策略（selang 命令）可以进行存储，然后以您定义的方式部署到企业中。 使用此基于策略的方式，您可以存储策略，然后将其分配至主机或主机组。 分配完成后，策略将立即排队以进行部署。 您也可以直接在主机或主机组上部署和取消部署策略版本。

中央数据库（部署映射服务器 (DMS)）收集有关您企业的策略、版本、分配和部署的所有信息。 因此，您可以轻松报告部署状态、部署偏差和部署层级结构。

注意：双重控制*不*适用于此方式，仅适用于 UNIX。 有关详细信息，请参阅*《端点管理指南：用于 UNIX》*。

基于策略的高级管理的工作原理

通过基于策略的高级管理，您可以存储、部署和取消部署策略版本，并在以后查看部署状态、部署偏差和部署分布。

基于策略的高级管理的工作原理如下：

1. 创建一个策略。

   每个策略都包含一对 selang 命令脚本。 第一个脚本称为*部署脚本*，它包含一组用于构建策略的 selang 命令。 第二个脚本称为*取消部署脚本*，它包含从端点数据库取消部署（删除）策略所需的命令。

2. 使用 CA Access Control 企业管理 或 policydeploy 实用工具将策略详细信息存储在 DMS 中，然后，CA Access Control 使用自动版本控制来存储策略。

   策略详细信息包括策略说明、部署脚本和取消部署脚本以及策略依存关系。

3. 根据 DMS 上是否已存在策略，CA Access Control 将执行以下操作之一：

   - 如果 DMS 上不存在策略名称，CA Access Control 会创建第一个版本的策略 *(policy_name*#01) 和逻辑策略对象（GPOLICY 类），然后将策略版本添加为逻辑策略的成员。
   - 如果 DMS 上已存在策略名称，CA Access Control 会将找到的最高策略版本增加一来创建新的策略版本，并将该策略版本添加为逻辑策略（GPOLICY 对象）的成员。

4. 当确定时机恰当时，使用 CA Access Control 企业管理 或 policydeploy 实用工具将保存的策略部署到目标数据库上。 CA Access Control 在 DMS 上自动创建部署任务（DEPLOYMENT 对象）。

   注意：CA Access Control 会部署最新且最终确定的存储策略的版本。您创建的新策略版本不会自动发送到分配的主机。 您需要将分配的主机手动升级到最新的策略版本。

   注意：在您创建 UNAB 登录和步骤策略后，CA Access Control 企业管理 会自动部署这些策略。 您可以仅将 UNAB 登录和配置策略分配给 UNAB 主机。

5. CA Access Control 在 DMS 上自动创建部署程序包（GDEPLOYMENT 对象）。

   部署程序包对上一步中创建的所有部署任务分组。

6. DMS 将部署任务发送到分发主机 (DH)。

7. 端点定期检查新策略部署任务（使用 policyfetcher），从 DH 提取挂起的部署任务，并在目标数据库上执行每个规则(部署脚本中指定的 selang 命令）。

8. 端点使用部署任务状态（失败、成功）、失败命令生成的 selang 结果消息和 HNODE 上的策略状态更新 DH。

   注意：如果策略部署出现错误，您可以使用 CA Access Control 企业管理 中的部署审核来详细了解失败命令的 selang 输出。 否则，您需要查看策略部署出现错误的计算机上的日志文件。

9. DH 将在存储部署任务状态和策略状态的 DMS 上更新这些信息。

注意：UNAB 登录策略和 UNAB 配置策略与基于策略的高级管理的工作原理不同。

更多信息：

策略依存关系 (p. 79)
策略验证 (p. 79)
分配路径 (p. 76)
控制主机访问和配置 UNAB 的方式 (p. 245)

部署方法如何影响部署任务

将存储的策略部署到目标数据库的时，CA Access Control 在 DMS 上自动创建部署任务。 部署任务（DEPLOYMENT 对象）是工作命令，由 DMS 生成，用于在端点上执行。 每个工作命令都用于一个端点，并包含有关需要部署到端点上的策略版本的信息。

注意：CA Access Control 使用不同的部署方法来部署 UNAB 登录和配置策略。

您用来部署存储策略的方式会影响 CA Access Control 创建的部署任务。以下内容显示选择不同方法的结果：

- 将策略（GPOLICY 对象）分配到一个或多个主机

  对于每台主机，CA Access Control 都创建最新且最终确定的策略版本的部署任务。

- 将策略（GPOLICY 对象）分配到一个或多个主机组

  对于每个属于某一主机组成员的主机，CA Access Control 都创建最新且最终确定的策略版本的部署任务。

- 将主机添加到已分配存储策略（GPOLICY 对象）的主机组

  对于新主机，CA Access Control 会创建最新且最终确定的策略版本的部署任务。

- 将策略重新部署到主机

  CA Access Control 为主机创建最新且最终确定的策略版本的部署任务。

- 还原 HNODE 上的策略（重新部署应部署到该主机的策略）

  对于每个应该部署到主机的策略，CA Access Control 都创建在该主机上有效的的策略版本的部署任务。

- 升级一个或多个主机上部署的策略

  对于每台主机，如果存储在主机上的版本比部署在主机上的版本新，CA Access Control 会创建最新且最终确定的策略版本的部署任务。

示例：将策略分配给主机

如果将策略 IIS 分配到主机 host1.comp.com 和 host2.comp.com，则 CA Access Control 将创建两个部署任务：一个用于在 host1.comp.com 上部署最新的 IIS 策略版本，另一个用于在 host2.comp.com 上部署最新的 IIS 策略版本。

示例：将策略分配给主机组

主机组“服务器”有两个成员：hostA.comp.com 和 hostB.comp.com。 如果将策略 IIS 分配到主机组“服务器”，则 CA Access Control 将创建两个部署任务：一个用于在 hostA.comp.com 上部署最新的 IIS 策略版本，另一个用于在 hostB.comp.com 上部署最新的 IIS 策略版本。

示例：将主机添加到已经分配策略的主机组

主机组“服务器”有两个分配的策略（IIS 和 ORACLE）。 如果您将 test.comp.com 主机添加到主机组中，则 CA Access Control 将创建两个部署任务：一个用于在 test.comp.com 上部署最新的 IIS 策略版本，另一个用于在 test.comp.com 上部署最新的 ORACLE 策略版本。

示例：还原主机

主机分配了两个策略：policy1 和 policy2。 如果您还原主机，则 CA Access Control 将创建两个部署任务：一个用于部署最新且最终确定的 policy1 版本，另一个用于在主机上部署最新且最终确定的 policy2 版本。

示例：升级部署的策略

策略 IIS 部署在两个主机上，host1.comp.com 和 host2.comp.com，但是最新版本的策略 IIS 没有部署到 host1.comp.com 上。 如果您在两个主机上都升级策略 IIS，CA Access Control 会仅创建一个部署任务，用于在 host1.comp.com 上部署最新的 IIS 策略版本。

更多信息：

控制主机访问和配置 UNAB 的方式 (p. 245)

DMS 上承载的端点数据

当您配置高级策略管理的环境时，企业中的端点将通过配置的 DH 向 DMS 通知以下三个方面的状态更改：

- 策略部署和取消部署

  当正在部署或取消部署策略时，端点会发送通知。 接下来以下详细信息会根据操作结果进行更新：

  - 策略详细信息
  - 部署状态（成功、失败等）
  - 无法执行的策略命令的 selang 命令输出
  - HNODE 策略状态（已部署、部署失败等）

- 主机心跳

  每个端点会以固定的可配置时间间隔将检测信号发送给在线主机的帐户。

- 偏差状态

  每个检测信号发送之后，端点将计算策略偏差，然后发送结果（找到或未找到偏差）。

  注意：如果 policyfetcher 发现端点和 DH 之间的部署和偏差状态发生冲突，会根据您从端点接收的信息解决冲突。

端点更新 DMS 的方式

每个端点都通过您配置的 DH 将检测信号（主机状态）、策略状态和偏差状态通知发送到 DMS。 这些 DMS 通知将按照以下方式处理：

1. DH 将通知消息存储在更新文件中。

   这些是来自端点的心跳和策略部署及取消部署通知。

2. DH 与其订户 DMS 通信：

   - 如果 DMS 不可用，则 DH 尝试定期与 DMS 通信，直至所有消息都成功发送出去。
   - 如果 DMS 可用，则 DH 发送存储的通知。

3. DMS 存储从每个 DH 接收到的信息以供将来使用。

   每次创建报告时，CA Access Control 都会在 DMS 上检索信息。

注意：UNAB 端点使用不同的过程来更新 DMS。

更多信息：

控制主机访问和配置 UNAB 的方式 (p. 245)

高级策略管理类

CA Access Control 使用特定的类让 DMS 执行以下操作：

- 保留部署在每台计算机上的策略状态的最新映射
- 将部署信息发送到 DH，以便端点可以获取它应当包含的策略部署的相关信息。

注意：有关这些类可包含属性的详细信息，请参阅*《selang 参考指南》*。

DEPLOYMENT 类

DEPLOYMENT 类中的每个对象都代表一个策略*部署任务*。 将策略分配到主机或从主机取消分配时，或者直接部署或取消部署策略时，CA Access Control 将在 DMS 上自动创建部署任务。 当您向已分配策略的主机组添加（分配）主机或从其删除（取消分配）主机、降级或升级主机上的策略以及重置或还原主机时，也会创建部署任务。

端点使用该对象作为工作命令：它们根据挂起 DEPLOYMENT 对象中的信息部署或取消部署策略版本。 每个工作命令都用于一个端点，并包含有关需要部署到端点上的策略版本的信息。 此外，DEPLOYMENT 对象具有表示部署是否成功的状态属性，以及包含策略部署任务的 selang 命令输出的结果属性 (result_message)。

注意：如果存在其他分配途径而导致 HNODE 上已存在策略，则部署任务会为空（没有操作状态）。

更多信息：

分配存储的策略版本 (p. 87)
对已分配的策略取消分配 (p. 88)
为已分配的主机升级至最新策略版本 (p. 88)
为已分配的主机降级至特定的策略版本 (p. 89)

GDEPLOYMENT 类

GDEPLOYMENT 类中的每个对象都代表一个*部署程序包*。 部署程序包在 DMS 上自动创建，并将由于相同事务（策略分配、升级等）对特定主机创建的所有部署任务分组到一起。 这意味着您执行的每个事务都会创建必需数量的部署任务（DEPLOYMENT 对象），并将这些任务按主机进行分组（GDEPLOYMENT 对象）。

通过部署程序包，您可以跟踪策略部署并排除其问题，以及记录触发因素（启动部署的原因）。

HNODE 类

HNODE 类中的每个对象都代表您企业中的一个端点。 它保留有关它所表示的特定节点、所从属的主机组以及上次检测到的联机时间的信息。此外，每个 HNODE 对象均保留其所表示节点上有效的策略版本（通过直接或间接分配）的信息，以及每个策略的状态（已部署、部署出错等）信息。

HNODE 对象的名称是实际的主机名。 例如，myhost.mydomain.com

GHNODE 类

GHNODE 类中的每个对象都代表一组 CA Access Control 节点（HNODE 对象）。 这使您可以出于部署策略的目的，将端点分组至逻辑组中。 每个 GHNODE 对象均保留有关已分配至其所代表节点的策略信息。

POLICY 类

POLICY 类中的每个对象都代表一个策略（GPOLICY 对象）版本，该策略可以部署在任意主机（HNODE 对象）或逻辑主机组（GHNODE 对象）上。它包含有关存储关联策略脚本的位置（在哪个 RULESET 对象中）和要部署该策略的节点或节点组的信息。

该对象名称为策略名加上版本号后缀（*策略名称*#*xx*）。

GPOLICY 类

GPOLICY 类中的每个对象都代表一个逻辑策略。 它包含有关属于此策略的策略版本（POLICY 对象）以及该策略分配到的主机和主机组的信息。

该对象名称为逻辑策略名称。

RULESET 类

RULESET 类中的每个对象都保留与策略版本相关联的部署和取消部署（删除）脚本。

该对象名称基于各自的 POLICY 对象名称。

主机和主机组

要使用高级策略管理，需定义 CA Access Control 的企业实施。 要执行此操作，请创建 HNODE 对象以代表端点（或主机），并创建 GHNODE 对象以代表逻辑主机组。 根据主机的属性和策略需求，主机可以为多个逻辑主机组中的成员。 例如：如果具有同时运行 Red Hat 操作系统和 Oracle 的主机，则这些主机可以为 Red Hat 逻辑主机组的成员，应用基线 Red Hat 访问控制策略，也可以为 Oracle 逻辑主机组的成员，应用 Oracle 访问控制策略。

将端点定义为企业中的主机

要向端点部署策略并查看其部署状态，需要在管理企业所用的部署映射服务器 (DMS) 上定义端点。 在启用了高级策略管理的端点上安装 CA Access Control 时，在 DMS 上会自动创建代表此端点的 HNODE 记录。 仅当要在端点上安装 CA Access Control 之前模拟环境时，才应在 DMS 上手动定义端点。

重要说明！ 您必须将完全限定主机名用作 HNODE 名称，否则端点不收集其部署。

将端点定义为企业中的主机

1. 在 CA Access Control 企业管理 中，单击“策略管理”，再单击“主机”子选项卡，然后在左侧的任务菜单中展开主机树。

   此时“创建主机”任务会显示在可用任务列表中。

2. 单击“创建主机”。

   此时将显示“创建主机: 主机搜索”屏幕。

3. 确认选择了“创建类型为‘主机’的新对象”，并单击“确定”。

   将显示“创建主机”任务页面。

4. 填写对话框中的以下字段：

   名称

   定义端点（HNODE 对象）的名称。 此名称在 DMS 上必须是唯一的（强制性）。

   说明

   （可选）定义主机的业务说明（自由文本）。 使用此字段记录有助于您识别该端点的任何信息。

   IP 地址

   （可选）定义主机的 IP 地址。

5. 单击“提交”。

   将提交该任务，如果提交成功，将随即显示一条消息，指明已创建新主机 (HNODE)。

主机组自动分配的工作原理

如果您安装 CA Access Control 的同时在端点上启用了高级策略管理，CA Access Control 企业管理 会自动将主机分配到主机组。 CA Access Control 企业管理 根据主机类型、操作系统、安装的 CA Access Control 版本或您定义的任何其他通用属性等条件将主机分配到主机组。 然后，可以将策略分配给主机组。

注意：当在 Linux 端点上安装 CA Access Control 时，该端点会被自动分配给“所有 Linux 主机”主机组。 如果在该端点上安装了 UNAB，也会自动将其分配给“所有 UNAB 主机”主机组。

CA Access Control 企业管理 以下列方式自动将主机分配到主机组：

1. 配置了高级策略管理的端点将检测信号发送到企业管理服务器。

   检测信号包含有关端点属性的信息。

2. 企业管理服务器根据主机组分配条件来评估端点属性，然后将主机分配给适当的主机组。

您可以使用“全局查看”查看分配给每台主机组的主机。

默认的即用型主机组

下表列出 CA Access Control 企业管理 中的默认的即用型主机组：

主机组名称	说明
AIX 5.2	所有 AIX 5.2 主机的默认主机组
AIX 5.3	所有 AIX 5.3 主机的默认主机组
AIX 6.1	所有 AIX 6.1 主机的默认主机组
所有 Linux 主机	所有 Linux 主机的默认主机组
所有 UNAB 主机	所有 UNIX 主机的默认主机组
所有 Windows 主机	所有 Windows 主机的默认主机组
ESX Server 3.x	所有 ESX Server 3.x 主机的默认主机组
ESX Server 4.x	所有 ESX Server 4.x 主机的默认主机组
HP-UX 11.23	所有 HP-UX 11.23 主机的默认主机组
HP-UX 11.31	所有 HP-UX 11.31 主机的默认主机组
RedHat 3	所有 RedHat 3 主机的默认主机组
RedHat 4	所有 RedHat 4 主机的默认主机组
RedHat 5	所有 RedHat 5 主机的默认主机组
SLES 9	所有 SLES 9 主机的默认主机组
SLES 10	所有 SLES 10 主机的默认主机组
sels 11	所有 SLES 11 主机的默认主机组
Solaris 8	所有 Solaris 8 主机的默认主机组
Solaris 9	所有 Solaris 9 主机的默认主机组
Solaris 10	所有 Solaris 10 主机的默认主机组
Windows Server 2003	所有 Windows Server 2003 主机的默认主机组
Windows Server 2003 R2	所有 Windows Server 2003 R2 主机的默认主机组
Windows Server 2008	所有 Windows Server 2008 主机的默认主机组
Windows Server 2008 R2	所有 Windows Server 2008 R2 主机的默认主机组

修改主机组自动分配条件

CA Access Control 企业管理 使用预定义的条件（例如，操作系统类型）自动将主机分配到主机组。 默认情况下，CA Access Control 企业管理 自动将每台主机添加到主机操作系统对应的主机组中。 例如，CA Access Control 企业管理 自动将 Windows Server 2003 R2 主机分配给“所有 Windows 主机”和“Windows Server 2003 R2”主机组。 您可以指定 CA Access Control 企业管理 用来自动分配主机到主机组的其他条件。

修改主机组自动分配条件

1. 打开企业管理服务器上的 selang 窗口并连接到 DMS。
2. 使用以下 selang 命令编辑主机组并指定分配条件：

```
editres GHNODE host_group_name criteria+(attribute=value)

editres GHNODE host_group_name criteria+(attribute!=value)

editres GHNODE host_group_name
criteria+(attribute=value)&&(attribute=value)

editres GHNODE host_group_name criteria+(attribute1=value1)

editres GHNODE host_group_name criteria+(attribute2=value2)

editres GHNODE host_group_name criteria-(attribute=value)
```

host_group_name

指定您分配该条件的目标主机组的名称。

attribute=value

指定主机组分配属性和值。 该参数可以具有以下值：

HNODE_IP=*IP_address*

指定 CA Access Control 企业管理 将定义的 IP 地址添加到主机组分配条件中。

示例：HNODE_IP=172.24.123.456

NODE_TYPE={AC Windows | AC UNIX | AC UNAB}

指定 CA Access Control 企业管理 将指定的端点类型添加到主机组分配条件中。

HNODE_VERSION={ACW | ACU | ACUNAB}:*version*

指定 CA Access Control 企业管理 将定义的端点版本添加到主机组分配条件中。

示例：HNODE_VERSION=ACW:12.53

该示例指定 CA Access Control 企业管理 将版本 12.53.1178 的 CA Access Control Windows 端点添加到主机组分配条件中。

ATTRIBUTES=("*attribute*")

指定 CA Access Control 企业管理 将定义的属性信息添加到主机组分配条件中。

示例：ATTRIBUTES=(Microsoft_Windows_Server_2003_R2)

注意：您可以在“值”字段中指定星号。

您已经修改您所指定主机组的分配条件。

示例：按照版本将主机分配给组

在该示例中，您将名为“所有 Windows 12.53 主机”的主机组的分配条件修改为仅自动分配安装了 CA Access Control 版本 12.53 的 Windows 主机：

```
editres GHNODE ("All Windows 12.53 hosts") criteria+(HNODE_VERSION=ACW:12.53)
```

示例：按照类型和版本将主机分配给组

在该示例中，您将名为“所有 UNIX 主机”的主机组的分配条件修改为根据其类型 (ACUNIX) 和 CA Access Control 版本自动分配主机：

```
editres GHNODE ("All UNIX hosts") criteria+(NODE_TYPE=AC
UNIX&&HNODE_VERSION=ACU:12.53)
```

示例：按照类型或版本将主机分配给组

在该示例中，您将名为“所有 UNAB 主机”的主机组的分配条件修改为根据类型 (UNAB) 或 UNAB 版本自动分配主机：

```
editres GHNODE ("All UNAB Hosts") criteria+(NODE_TYPE=ACUNAB)
editres GHNODE ("All UNAB Hosts") criteria+(HNODE_VERSION=ACUNAB:12.53)
```

示例：按照类型排除主机

在该示例中，您将名为“非 UNIX 主机”的主机组的分配条件修改为自动排除所有 AC UNIX 类型的主机：

```
editres GHNODE ("Non UNIX Hosts") criteria+(NODE_TYPE!=AC UNIX)
```

示例：删除分配的条件

在该示例中，您删除先前分配给名为“所有 Windows 主机”的主机组的 NODE_TYPE 条件：

```
editres GHNODE ("All Windows Hosts") criteria-(NODE_TYPE=AC Windows)
```

注意：要显示主机的有效属性，可以查看 DMS 审核文件并找到主机检测信号。 使用 seaudit -a -fn pmd.audit 命令显示 DMS 审核文件。

定义逻辑主机组

要管理一组相关端点上的策略，可以将端点定义为逻辑主机组，然后对整个组执行高级策略管理操作。 可以创建有意义的主机组之前，必须在 DMS 中定义端点。

注意：以下步骤将说明如何使用 CA Access Control 企业管理 在 DMS 上定义逻辑主机组。

定义逻辑主机组

1. 在 CA Access Control 企业管理 中，单击“策略管理”，再单击“主机”子选项卡，然后在左侧的任务菜单中展开主机组树。

   此时“创建主机组”会显示在可用任务列表中。

2. 单击“创建主机组”。

   此时将显示“创建主机组: 主机组搜索”屏幕。

3. 确认选择了“创建类型为‘主机组’的新对象”，并单击“确定”。

   将显示“创建主机组”任务页面。

4. 填写对话框中的以下字段：

   名称

   定义逻辑主机组（GHNODE 对象）的名称。

   说明

   （可选）定义主机组的业务说明（自由文本）。 使用此字段记录有助于您识别该主机组的任何信息。

5. 单击“主机选择”，然后单击“添加”。

   将显示“添加成员”对话框。

6. 选择希望添加至该主机组的端点，然后单击“选择”

   “添加成员”对话框将关闭，所选端点将添加至所定义的逻辑主机组的成员列表中。

7. 单击“提交”。

   将提交该任务，如果提交成功，将随即显示一条消息，指明已创建新主机组 (HNODE)。

导入主机组

导入主机组可帮助您将现有的 PMDB 结构迁移到高级策略管理。 在导入主机组时，将创建主机或将主机加入到主机组。 主机与 PMDB 订户相对应。

注意：高级策略管理环境不支持层级主机组。 从 PMDB 导入主机组时，会将所有订户均归入同一主机组中。 CA Access Control 企业管理 不创建与订户 PMDB 相对应的主机。

对于您加入主机组的每个 PMDB 订户，CA Access Control 企业管理 会检查在 DMS 上是否已存在与订户相对应的主机（HNODE 对象）。 如果 DMS 上存在相应的主机，CA Access Control 会将该主机添加到主机组。 如果 DMS 上不存在相应的主机，CA Access Control 会创建新的主机，并将新主机添加到主机组中。

如果您不具有访问端点的权限，则端点不显示在向导中，并且您无法将相应的主机添加到主机组中。

导入主机组

1. 在 CA Access Control 企业管理 中，执行如下操作：

   a. 单击“策略管理”。

   b. 单击“主机”子选项卡。

   c. 在左侧的任务菜单中展开主机组树。

      此时“主机组导入”任务会显示在可用任务列表中。

2. 单击“主机组导入”。

   将显示“PMDB 主机登录”页面。

3. 键入用户名、密码和 PMDB 的名称，然后单击“登录”。

   注意：以 *PMDBname@host* 格式指定 PMDB 名称，例如 master_pmdb@example

   此时，“主机组导入”向导将显示在“常规”任务阶段中。

4. 完成此向导，然后在阅读完摘要后单击“完成”。

   CA Access Control 将主机添加到主机组中。 如果 DMS 中不存在主机，CA Access Control 会为主机创建一个 HNODE 对象，再将其添加到主机组 (GHNODE) 中。

   注意：在您将主机添加到现有主机组中时，CA Access Control 会将分配给主机组的任何策略自动部署到该主机。

分配路径

*分配路径*将说明对特定主机或主机组进行的策略分配。 可通过两种路径将策略分配至主机：

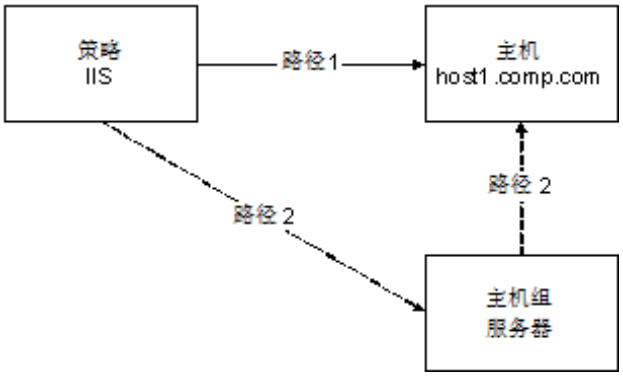
- 直接将策略分配至主机。
- 将策略分配至主机所属的主机组。
- 主机加入到具有一个或多个已分配策略的主机组。

分配路径非常重要，因为当存在多个分配路径时，会影响高级策略管理，如下所述：

- 如果删除一个分配路径，CA Access Control 不会对该策略进行取消部署，因为主机和该策略之间仍存在其他分配路径。
- 如果添加了一个分配路径，将创建部署程序包和部署任务用于跟踪和管理。 但是，部署任务的状态为*无操作*，因此不会在端点上启动策略部署。

示例：策略 IIS 的多种分配途径

下图显示策略 IIS 的多种分配途径的示例。 主机 host1.comp.com 是主机组“服务器”的成员。 途径 1 显示当您直接将策略 IIS 分配给主机 host1.comp.com 时的分配途径。 途径 2 显示当您将策略 IIS 分配给主机组“服务器”时的分配途径：



示例：删除任务途径

在前一个图中，策略 IIS 被分配给主机组“服务器”和主机 host1.comp.com。 如果从“服务器”主机组中删除 host1.comp.com，就删除了途径 2。 但是，CA Access Control 不从 host1.comp.com 上取消部署策略 IIS，因为该策略仍被直接分配给该主机（途径 1）。

如何创建和部署策略

使用基于策略的高级管理，您可以存储策略的草稿版本，然后按照要求进行审查和修改，然后部署审批过的策略版本。

要使用 CA Access Control 企业管理 部署经审批的策略版本，请执行以下操作：

1. 在 DMS 上存储策略版本。

   有了存储的策略版本后，可以对策略进行审查和部署。

2. 审查策略。

   一旦存储了策略版本，您应让规则与审查的策略相关联。

3. 最终确定策略。

   最终确定策略后，即可将其分配到希望部署该策略的主机或主机组。

4. 通过可用的分配途径之一将策略分配给端点：

   - 将存储的策略分配到主机或主机组。
   - 将主机分配给已经分配了策略的逻辑主机组。

   一旦分配了策略，CA Access Control 就能够自动部署最新且最终确定的策略版本。

注意：您遵照不同的过程创建和部署 UNAB 登录和配置策略。

更多信息：

管理 UNAB 登录授权 (p. 246)
配置 UNAB 主机或主机组 (p. 247)
分配路径 (p. 76)

管理要求

要在 DMS 上存储策略或分配这些策略，您和您使用的计算机必须具有相应权限。

要在 DMS 中存储策略，请执行以下操作：

- 用于管理 DMS 的*计算机*或者运行 policydeploy 实用程序的计算机必须具有 DMS 的终端权限（TERMINAL 类）。
- *您*必须具有对 DMS 上 POLICY、GPOLICY 和 RULESET 类的子管理权限。

将策略分配到主机或主机组：

- 您管理 DMS 的*计算机*需要有 DMS 的终端权利（TERMINAL 类）。
- *您*必须具有对 DMS 上 DEPLOYMENT、GDEPLOYMENT、POLICY、GPOLICY、HNODE 和 GHNODE（如果要将策略分配到主机组）类的子管理权限。

注意：有关端点权限和子管理权限的更多信息，请参阅《*适用于 UNIX 的端点管理指南*》和《*适用于 Windows 的端点管理指南*》。

策略依存关系

通过高级策略管理，您可以强制安排部署和取消部署策略的顺序。

使用策略依存关系，您可以将依存于一个或多个其他策略的策略定义为直至所有先决条件策略均部署后，才可进行部署。 同样，如果一个或多个依存性策略仍处于部署状态，则无法将先决条件策略取消部署。

可在创建或修改策略时定义策略依存关系。

策略验证

当启用策略验证时，CA Access Control 会检查在部署策略之前，该策略不包含错误。 如果 CA Access Control 在策略部署脚本中发现错误，则不会在端点上执行策略脚本。 这确保策略部署不会出现错误，并让您可以跟踪端点上的脚本错误。 默认情况下禁用策略验证。

如果不启用策略验证而您部署策略出现错误，某些策略命令可能仍然执行而不管其他命令中的错误。

策略验证仅检查 CA Access Control 数据库命令，即 AC 环境下的 selang 命令。 策略验证不检查本机、配置或策略模型环境中的命令。 如果某策略同时包含 AC 环境和其他环境的命令，策略验证仅检查 AC 环境中的命令。

策略验证无法检查取消部署脚本。

策略部署的工作原理

策略验证确认策略可以在没有错误的情况下部署，然后再将其实际部署到端点上。

注意：默认情况下不启用策略验证。

以下过程说明了策略验证的工作原理：

1. 将某策略分配到主机或主机组。
2. 在每个端点上，CA Access Control 企业管理 都验证该策略。
3. 会出现以下情况之一：
   - 如果策略不包含错误，CA Access Control 企业管理 将策略部署到端点。

     端点会更新策略状态为*已部署*的 DMS。
   - 如果策略脚本包含错误，CA Access Control 企业管理 *不会*将策略部署到端点。

     端点会更新策略状态为*未执行*的 DMS。 DMS 也会将与具有脚本错误的策略相对应的每个部署任务的状态更新为*失败*。

     注意：您可以使用 CA Access Control 企业管理 中的“部署审核”功能来查看出现错误的脚本。

启用策略验证

策略验证确保策略可以在没有错误的情况下部署，然后再将其实际部署到端点上。

要启用策略验证，请将 policyfetcher 部分中 policy_verification 配置的值设为 1。

策略验证随即启用。

创建和存储策略版本

在 DMS 上创建和存储的每个策略都会自动获得一个版本号。 当您第一次存储策略时，它将收到版本号“01”。 例如：您第一次存储策略 *myPolicy* 时，CA Access Control 企业管理 将创建名为 *myPolicy* 的 GPOLICY 对象，以及名为 *myPolicy#01* 的 POLICY 对象。 每次您存储 DMS 上已存在的策略时，该策略的最新存储版本将以一为单位递增，以创建新的策略版本。 例如：您第二十八次存储 *myPolicy* 的一个版本时，CA Access Control 企业管理 将创建名为 *myPolicy#28* 的 POLICY 对象。

注意：此过程将说明如何使用 CA Access Control 企业管理 创建和存储策略版本。 此过程不适用于 UNAB 登录和配置策略。

创建和存储策略版本

1. （可选）使用 selang 部署命令创建新的脚本文件。

   这些是构建希望部署在企业中端点上的策略时必需的命令。

   重要说明！ 策略部署不支持设置用户密码的命令。 不要将这类命令包含在您的部署脚本文件中。 虽然可支持本地 selang 命令，但不会显示在偏差报告中。

2. （可选）用 selang 取消部署命令创建新的脚本文件。

   这些是从企业中端点上取消部署（删除）策略必需的命令。

3. 在 CA Access Control 企业管理 中，单击“策略管理”，再单击“策略”任务，然后在左侧的任务菜单中展开策略树。

   将显示“策略”任务。

4. 单击“创建策略”。

   此时将显示“创建策略: 策略搜索”屏幕。

   注意：如果希望创建现有策略的新版本，请转而单击“修改策略”，然后搜索要修改的策略。

5. 单击“确定”。

   将显示“创建策略”任务页面。

6. 填写对话框中的以下字段：

   名称

   定义策略（GPOLICY 对象）名称。此名称在 DMS 上必须是唯一的（强制性），在企业中也必须唯一（非强制性，但如果已存在相同名称的策略，您将无法将策略部署到主机）。

   说明

   （可选）定义策略的业务说明（自由文本）。 使用此字段记录该策略的用途，以及有助于您识别该策略的任何其他信息。

7. 单击“策略脚本”选项卡，然后使用以下方法之一提供部署和取消部署脚本：
   - 在相应字段中键入部署和取消部署脚本。

     如果未创建带有部署命令的脚本文件，请使用该选项。
   - 从现有的 selang 脚本文件加载命令：
     a. 单击“浏览”，找到包含要使用的 selang 脚本的文件。
     b. 单击“加载”以使用您所选择的文件的内容填充脚本字段。
8. （可选）提供此策略版本的说明。

   使用此字段提供有关用于此策略版本的部署脚本的具体信息。
9. （可选）选择“最终确定提交”。

   此选项指定您创建的新策略版本可以进行部署。 如果未完成部署脚本的创建，请取消选定此选项。

   注意：如果未选择此选项，您可以修改部署脚本，而无需建新的策略版本。 不过，不能部署未经最终确定的策略版本。
10. 单击“策略依存关系”选项卡，然后单击“添加”。

    将显示“添加成员”对话框。
11. 选择希望作为先决条件添加到该策略的策略，然后单击“选择”。

    “添加成员”对话框将关闭，所选策略将添加至所创建策略的成员列表中。
12. 单击“提交”。

    将提交该任务，如果提交成功，将随即显示一条消息，指明已创建新策略版本。 您遵照不同的过程创建和部署 UNAB 登录和配置策略。

注意：您也可以使用 policydeploy 实用程序来执行该任务。 有关 policydeploy 实用程序的更多信息，请参阅*《参考指南》*。

更多信息：

管理 UNAB 登录授权 (p. 246)
配置 UNAB 主机或主机组 (p. 247)

创建定义变量的策略

通过创建和部署定义变量的策略，您可以在许多端点上定义同样的变量。

创建定义变量的策略

1. 使用定义变量的 selang 部署命令创建脚本文件。 使用以下 selang 命令定义每个变量：

   ```
   editres ACVAR ("variable_name") value("variable_value")
   ```

2. （可选）将使用变量的 selang 命令添加到脚本文件中。

   注意：您必须定义策略中的每个变量，然后才能在该策略的后续规则中引用这些变量。 使用以下格式引用变量："<!*variable*>"

3. 在 DMS 上存储策略。

示例：创建定义变量的策略

在该示例中，下列策略定义了名为 jboss_home 且具有 /opt/jboss 值的变量，并且创建规则来授权用户 Mark 访问 /opt 目录中的任何资源（该目录是通过 JBoss 访问的）。

```
editres ACVAR ("jboss_home") value("/opt/jboss")
authorize FILE /opt/* uid(Mark) access(all) via(pgm("<!jboss_home>/jboss"))
```

当端点编译该策略时，会创建以下规则：

```
authorize FILE /opt/* uid(Mark) access(all) via(pgm(/opt/jboss/jboss))
```

示例：创建定义多个变量值的策略

下列策略定义了名为 jboss_home 且具有 C:\JBoss 值的变量，将 C:\Program Files\JBoss 值添加到 jboss_home 变量中，并创建访问规则：

```
editres ACVAR ("jboss_home") value("C:\JBoss")
editres ACVAR ("jboss_home") value+("C:\Program Files\JBoss")
editres FILE ("<!jboss_home>\bin") defacc(none) audit(a)
```

当端点编译该策略时，会创建以下规则：

```
editres FILE ("C:\JBoss\bin") defacc(none) audit(a)
editres FILE ("C:\Program Files\JBoss\bin") defacc(none) audit(a)
```

示例：使用变量将同样的策略部署到 Windows 和 UNIX 端点

下列示例说明了虽然 JBoss 在每个操作系统上的安装位置不同，但是仍可使用变量将相同的 JBoss 策略部署到 Windows 和 UNIX 端点。 该示例定义了两个 jboss_home 变量，这些变量定义每个操作系统的 JBoss 安装位置：

1. 定义两个 jboss_home 变量，这些变量定义每个操作系统的 JBoss 安装位置。
   - 创建定义 Windows 上的 JBoss 安装位置的策略，并将该策略部署到 Windows 端点：

     ```
     editres ACVAR ("jboss_home") value("C:\JBoss")
     ```

   - 创建定义 UNIX 上的 JBoss 安装位置的策略，并将该策略部署到 UNIX 端点：

     ```
     editres ACVAR ("jboss_home") value("/opt/jboss")
     ```

2. 创建使用 jboss_home 变量保护 JBoss 安装位置的策略，并将该策略部署到 Windows 和 UNIX 端点：

   ```
   editres FILE "<!jboss_home>" defacc(none) audit(all)
   ```

   - 当 Windows 端点编译策略时，会创建以下规则：

     ```
     editres FILE "C:\JBoss" defacc(none) audit(all)
     ```

   - 当 UNIX 端点编译策略时，会创建以下规则：

     ```
     editres FILE "/opt/jboss" defacc(none) audit(all)
     ```

查看与策略关联的规则

一旦策略存储在 DMS 上，您就可以在部署中查看规则，并为每个策略版本取消部署脚本。

查看与策略关联的规则

1. 在 CA Access Control 企业管理 中，单击“策略管理”，再单击“策略”子选项卡，然后在左侧的任务菜单中展开策略树。

   将显示“策略”任务。

2. 单击“查看策略”。

   此时将显示“查看策略: 策略搜索”屏幕。

3. 定义搜索范围，然后单击“搜索”。

   将显示与定义的搜索范围匹配的策略列表。

4. 选择要查看的策略，然后单击“选择”。

   将显示“查看策略: *策略名称*”页面。 在不同的选项卡上，您可以查看该策略的属性，包括其名称和说明、最新版本的部署和取消部署脚本、此策略的现有全部策略版本列表、所有策略依存关系，以及有关该策略的创建和更新事件的一般信息。

5. 单击“版本历史记录”选项卡。

   将显示策略版本列表，每个版本均带有部署和取消部署脚本的链接。

6. 请执行以下操作之一：

   - 单击“部署脚本”链接。

     将显示带有部署脚本的弹出窗口。

   - 单击“取消部署脚本”链接。

     将显示带有取消部署脚本的弹出窗口。

注意：您也可以使用 policydeploy 实用程序来执行该任务。 有关 policydeploy 实用程序的更多信息，请参阅 *《参考指南》*。

导入策略

导入策略时，CA Access Control 企业管理 从本地 CA Access Control 数据库或 PMDB 导出 selang 规则，并在 DMS 上创建和存储包含规则的策略。 这允许您将保护一个端点的规则转换为可以保护许多端点的策略，并且帮助您将 PMDB 迁移到高级策略管理。

注意：您从其中导出规则的端点或 PMDB 必须位于安装了 CA Access Control r12.0 或更高版本的主机上。 要从更早的 CA Access Control 版本导入策略，请首先升级端点。

导入策略

1. 在 CA Access Control 企业管理 中，执行如下操作：

   a. 单击“策略管理”。

   b. 单击“策略”子选项卡。

   c. 在左侧的任务菜单中展开策略树。

      此时“策略导入”任务会显示在可用任务列表中。

2. 单击“策略导入”。

   此时将显示“主机登录”页面。

3. 键入用户名、密码和您要从其中导出规则的 PMDB 或主机的名称，然后单击“登录”。

   注意：以 *PMDBname@host* 格式指定 PMDB 名称，例如 master_pmdb@example

   “策略导入过程”向导将显示在“常规”任务阶段中。

4. 填写以下字段，然后单击“下一步”。

   名称

   定义策略的名称。 此名称在 DMS 上必须是唯一的（强制性），在企业中也必须唯一（非强制性，但如果已存在相同名称的策略，您将无法将策略部署到主机）。

   说明

   （可选）定义策略的业务说明（自由文本）。 使用此字段记录该策略的用途，以及有助于您识别该策略的任何其他信息。

   策略类

   指定要导出其规则的类，以包含在策略中。 如果在“选定列表”列中未指定任何类，将导出所有类并包含在策略中。

   导出依存类

   指定以导出依赖于在“选定列表”列中指定类的所有类。 如果您不选择该选项，CA Access Control 仅导出您在“选定列表”列中指定的类。

   将显示“策略脚本”阶段。

5. 检查导出的规则，并根据需要进行修改，然后单击“下一步”。

   将显示“摘要”阶段。

6. 单击“完成”。

   该策略即已创建。

分配存储的策略版本

可以将最终确定的策略版本分配给特定主机或主机组。 分配后的策略将自动部署，您可以通过 DMS 监控其状态。

注意：此过程不适用于登录和配置策略。

分配存储的策略版本

1. 在 CA Access Control 企业管理 中，单击“策略管理”，再单击“策略”子选项卡，在左侧的任务菜单中展开分配树，然后单击“分配策略”。

   在“策略选择”任务阶段将显示“分配策略”向导。

2. 完成此向导，然后在阅读完摘要后单击“完成”。

   CA Access Control 将提交策略分配任务。 策略分配至主机（直接分配或通过逻辑主机组成员资格分配）后，CA Access Control 将立即为每台主机创建 DEPLOYMENT 任务以进行检索。

注意：您也可以使用 policydeploy 实用程序来执行该任务。 有关 policydeploy 实用程序的更多信息，请参阅 *《参考指南》*。

策略维护

可以对已部署的策略执行以下操作：

- 从分配的主机对该策略取消分配
- 将主机升级至最新策略版本
- 将主机降级至早期策略版本
- 确认该策略在部署过程中没有发生错误
- 删除策略或策略版本

使用 CA Access Control 企业管理 或 policydeploy 实用程序执行这些操作。

对已分配的策略取消分配

可以从特定主机或主机组对已分配的策略取消分配。 取消分配后的策略将自动取消部署。

对已分配的策略取消分配

1. 在 CA Access Control 企业管理 中，单击“策略管理”，再单击“策略”子选项卡，在左侧的任务菜单中展开分配树，然后单击“取消分配策略”。

   在“策略选择”任务阶段将显示“取消分配策略”向导。

2. 完成此向导，然后在阅读完摘要后单击“完成”。

   CA Access Control 将提交策略分配任务。 策略从主机取消分配（直接取消分配或通过逻辑主机组成员资格取消分配）后，CA Access Control 将立即为每台主机创建 DEPLOYMENT 任务以进行检索。

注意：您也可以使用 policydeploy 实用程序来执行该任务。 有关 policydeploy 实用程序的更多信息，请参阅 *《参考指南》*。

为已分配的主机升级至最新策略版本

新的策略版本不会自动发送至已分配的主机或已部署该策略的主机。需要手动为已部署该策略的主机升级至最新版本。

为已分配的主机升级至最新策略版本

1. 在 CA Access Control 企业管理 中，单击“策略管理”，再单击“策略”子选项卡，在左侧的任务菜单中展开分配树，然后单击“升级策略”。

   在“策略选择”任务阶段将显示“升级策略”向导。

2. 完成此向导，然后在阅读完摘要后单击“完成”。

   CA Access Control 将提交策略升级任务。 对于主机上要进行升级的策略，CA Access Control 将为该主机创建 DEPLOYMENT 任务以进行检索。

   注意：选择要升级的主机组时，CA Access Control 企业管理 只允许您从包含已部署旧版本策略的主机的主机组中进行选择。

注意：您也可以使用 policydeploy 实用程序来执行该任务。 有关 policydeploy 实用程序的更多信息，请参阅 *《参考指南》*。

为已分配的主机降级至特定的策略版本

如果您无意中将错误的策略版本分配给一个或多个主机，或者希望返回到特定主机上的策略的旧版本，则可以对策略进行降级。

为已分配的主机降级至特定的策略版本

1. 在 CA Access Control 企业管理 中，单击“策略管理”，再单击“策略”子选项卡，在左侧的任务菜单中展开分配树，然后单击“降级策略”。

   在“策略选择”任务阶段将显示“降级策略”向导。

2. 完成此向导，然后在阅读完摘要后单击“完成”。

   CA Access Control 将提交策略降级任务。 对于主机上要进行降级的策略，CA Access Control 将为该主机创建 DEPLOYMENT 任务以进行检索。

注意：您也可以使用 policydeploy 实用程序来执行该任务。 有关 policydeploy 实用程序的更多信息，请参阅 *《参考指南》*。

删除的策略

您可以从 DMS 上删除逻辑策略（GPOLICY 对象）或策略版本（POLICY 对象）。 当删除策略版本时，CA Access Control 企业管理 还删除与策略版本相关联的部署和取消部署脚本（RULESET 对象）。 当删除逻辑策略时，您会删除与逻辑策略相关联的每个策略版本及其相关脚本。

您不能还原删除的逻辑策略或策略版本。

无法删除的策略

在以下情况下，您将无法删除策略：

- 无法删除策略的一个或多个策略版本。
- 策略是另一策略的先决条件。

  在删除策略之前，必须先删除对该策略的任何依存关系。
- 策略已在主机上进行分配或部署。

  您必须从主机上取消分配或取消部署该策略，然后才能将其删除。

您无法删除的策略版本

如果以下任意情况为真，您就无法删除策略版本：

- 策略版本在主机上有效（已分配或已部署）。

  您必须从主机上取消分配或取消部署该策略版本，然后才能将其删除。

- 策略版本在 DMS 上有状态。

  您必须从主机上取消分配或取消部署该策略版本，然后才能将其删除。 如果您无法取消分配或取消部署策略版本，则必须手工将其从主机中删除。

- 策略的状态为“已取消部署，但存在失败”。

  您必须删除该状态才能删除策略版本。

示例：您无法删除的策略版本

以下内容是您无法删除的策略版本的示例，因为他们在 DMS 上具有状态，但是在该主机上无效：

- 部署失败
- 未执行

在这两种情况下，您必须先从主机中手工删除策略版本，然后再删除策略版本。

注意：有关主机 (HNODE) 上的策略状态的更多信息，请参阅*《参考指南》*。 有关删除策略版本的状态的更多信息，请参阅*《疑难解答指南》*。

删除策略

当策略不再分配给主机或主机组时，您可以将该策略从 CA Access Control 企业管理 中删除。

重要说明！ 删除策略（GPOLICY 对象）时，CA Access Control 企业管理 会删除该策略的所有策略版本（POLICY 对象）以及与每个策略版本相关联的 RULESET 对象。

删除策略

1. 在 CA Access Control 企业管理 中，单击“策略管理”，再单击“策略”子选项卡，然后在左侧的任务菜单中展开策略树。

   将显示“策略”任务。

2. 单击“删除策略”。

   此时将显示“删除策略: 策略搜索”屏幕。

3. 定义搜索范围，然后单击“搜索”。

   将显示与定义的搜索范围匹配的策略列表。

4. 选择要删除的策略，然后单击“选择”。

   此时显示一条消息，询问您是否要删除该策略。

5. 单击“是”。

   该策略现已删除。

注意：您也可以使用 policydeploy 实用程序来执行该任务。 有关 policydeploy 实用程序的更多信息，请参阅*《参考指南》*。

更多信息：

无法删除的策略 (p. 89)

删除策略版本

您可以删除不再需要的已保存的策略版本（POLICY 对象）。 当删除策略版本（POLICY 对象）时，CA Access Control 企业管理 会删除与该策略版本相关的所有部署脚本和取消部署脚本。

要删除策略版本，请运行以下命令：

```
policydeploy -delete name#xx [-dms list]
```

-delete *name#xx*

删除指定的策略版本。

-dms *list*

（可选）指定以逗号分隔的 DMS 节点的列表，从这些节点删除策略版本。 如果未指定 DMS 节点，则 policydeploy 实用程序将使用在本地 CA Access Control 数据库中指定的 DMS 节点的列表。

示例：删除 IIS 5 保护策略版本

下列示例向您显示如何从 DMS 中删除未分配的策略版本 IIS5#05。 在该示例中，策略版本 IIS5#05 未分配给任何主机或主机组，并存储在 crDMS@cr_host.company.com DMS 节点上。

要删除 IIS 5 保护策略版本，请打开命令提示符窗口并运行 policydeploy 实用工具：

```
policydeploy -delete IIS5#05
```

策略版本 IIS5#05 从 crDMS@cr_host.company.com DMS 节点中删除。

变量

变量让您可以将相同的策略部署到具有不同配置和不同操作系统的端点上。 例如，尽管 CA Access Control 在每个操作系统上的安装位置不同，但您仍可以使用变量将相同的策略部署在 Windows 和 Solaris 端点上。

创建变量的方式

变量是 ACVAR 类中的对象，并且可以有多个值。 端点上的每个变量都必须有唯一名称，策略中的每个变量也必须有唯一名称。 使用以下任何一个方式创建变量：

- 使用 CA Access Control 端点管理 定义端点上的变量。
- 创建定义变量的策略，并将该策略部署到许多端点

重要说明！ 您只能创建使用策略中的变量的规则。 如果您直接使用包含变量的规则更新 CA Access Control 数据库，数据库将无法编译该规则，而 CA Access Control 也无法实施该规则。 您必须先定义变量，然后才能在策略脚本引用它。

变量类型

CA Access Control 支持用户定义的变量和内置变量：

- 用户定义的变量是您在 CA Access Control 数据库中定义的变量。
- 内置变量是 CA Access Control 在安装期间创建的变量。 您不能修改内置变量。

用户定义的变量

CA Access Control 支持以下用户定义的变量：

静态变量

定义 CA Access Control 端点上的固定位置。

您可以定义具有相同名称和不同值的静态变量，但是每个变量都必须存在于单独的端点上和单独的策略中。

注意： 如果您在创建变量时不指定变量类型，CA Access Control 则会创建静态变量。

注册表值变量

(Windows) 根据注册表值定义 CA Access Control 端点上的位置。

注意：您只能定义指向 REG_SZ 或 REG_EXPAND_SZ 注册表类型的注册表变量。

示例：下列规则定义了名为 jboss_home 的注册表变量：

```
editres ACVAR ("jboss_home") value("HKLM\Software\Jboss\home") type(regval)
```

在策略中部署该规则时，Windows 端点使用 HKLM\Software\Jboss\home 注册表项的值来解析变量值。

操作系统变量

根据操作系统环境值定义 CA Access Control 端点上的位置。

示例：下列规则定义了名为 jboss_home 的操作系统变量：

```
editres ACVAR ( “jboss_home” ) value( “JBOSS_HOME” ) type(osvar)
```

在策略中部署该规则时，端点使用 JBOSS_HOME 操作系统环境变量的值来解析变量值。

内置变量

CA Access Control 在安装过程期间在 CA Access Control 数据库中创建内置变量。 您不能修改或删除内置变量，但是您可以在策略中使用内置变量。 内置变量是动态的并取决于 CA Access Control 端点上的系统设置。 当相应的系统设置有所变化时，内置变量的值会随之变更。

注意：当导出 CA Access Control 数据库时，内置变量不包括在输出中。当创建 DMS 或 PMDB 时，CA Access Control 不创建内置变量。

CA Access Control 支持以下内置变量：

<!HOSTNAME>

标识本地计算机的完全限定主机名。

<!HOSTIP>

标识主机 IP 地址（一个或多个）。

<!AC_ROOT_PATH>

标识 CA Access Control 安装路径。

<!AC_REGISTRY_KEY>

(Windows) 标识 CA Access Control 根注册表项。

<!USER_OS_ADMIN>

标识本地计算机上操作系统的管理员。

<!DOMAINNAME>

标识本地计算机的域名。

<!DNSDOMAINNAME>

标识本地计算机的 DNS 域名。

示例：在策略中使用内置变量

该示例创建网络资源规则：

```
authorize TCP 8333 uid(*) host(<!HOSTNAME>) access(WRITE)
```

您将策略部署到端点 host1.example.com 且端点编译策略时，它会创建以下规则：

```
authorize TCP 8333 uid(*) host(host1.example.com) access(WRITE)
```

使用变量的准则

当使用变量时，应当遵守以下准则：

- 您不能删除被其他变量或策略使用的变量。
- 变量可以有多个值。 您可以添加和删除变量值。
- 变量可以进行嵌套。 例如，下列规则定义了名为 ac_data 且包含内置的 <!AC_ROOT_PATH> 变量的变量：

  ```
  editres ACVAR ac_data value("<!AC_ROOT_PATH>\data")
  ```

  当具有 CA Access Control 默认安装的 Windows 端点编译该规则时，会创建以下规则：

  ```
  editres ACVAR ac_data value("C:\Program Files\CA\AccessControl\data")
  ```

- 每个变量只能有一种类型，例如，您无法定义既是静态变量又是注册表值变量的变量。
- 您不能部署包含未定义变量的策略。 如果您使用未定义的变量部署策略，CA Access Control 会将该策略的部署状态更改为“部署挂起”。要部署该策略，您必须定义此未定义的变量，然后重新部署该策略。

  注意：要找到策略中未定义的变量，请查看该策略的 DEPLOYMENT 对象。 不管您已经启用还是禁用了策略验证，CA Access Control 都会检查未定义的变量。

- CA Access Control 无法解析组合了 CA Access Control 变量和 Windows 系统变量的规则。 例如，CA Access Control 无法解析定义了名为 var1 的变量的以下规则：

  ```
  editres ACVAR var1 value("%SYSTEMROOT%\temp")
  ```

  要创建将 %SYSTEMROOT% 定义为 CA Access Control 变量且保护 %SYSTEMROOT%\temp 的策略，请使用以下规则：

  ```
  editres ACVAR var1 value("SYSTEMROOT") type(osvar)
  editres ACVAR var2 value("<!var1>\temp")
  ```

- CA Access Control 无法解析相互依赖的变量。 例如，CA Access Control 无法解析以下示例中的变量 var1 和 var2：

  ```
  editres ACVAR var1 value("<!var2>")
  editres ACVAR var2 value("<!var1>")
  ```

- 当使用斜线来定义变量中的目录时，对于 Windows 和 UNIX 端点，CA Access Control 会按照正确的方向解析斜线。
- 如果使用 selang 规则来定义变量，则必须使用策略将规则部署到端点。 如果使用 selang 规则在端点上直接更新 CA Access Control 数据库，CA Access Control 则无法编译这些规则。 例如，如果您已经在端点上定义名为 jboss_home 的变量，而您直接使用下列的 selang 规则更新数据库：

  ```
  editres FILE <!jboss_home> audit(all)
  ```

  CA Access Control 会无法编译该规则，而是在数据库中创建命名 <!jboss_home> 的 FILE 对象。

在 UNIX 端点上使用操作系统变量的准则

在 UNIX 上有效

CA Access Control 操作系统变量（类型为 osvar 的 ACVAR 对象）使用 UNIX 环境变量的值。 因为每个 UNIX 进程都有其自己的一组环境变量，因此建议您不要在 UNIX 端点上使用操作系统变量。

如果确实在 UNIX 端点上使用操作系统变量，则必须在启动 CA Access Control 之前设置和导出必要的环境变量。 在 UNIX 端点上使用操作系统变量时，应当遵守以下准则：

- 如果您在计算机启动时使用 rc 启动脚本来启动 CA Access Control，请确认脚本在启动 CA Access Control 之前设置和导出了环境变量。
- 如果用户停止和重新启动 CA Access Control，用户则必须在重新启动 CA Access Control 之前设置和导出其会话中的环境变量。

在 Windows 端点上使用操作系统变量的准则

在 Windows 上有效

CA Access Control 操作系统变量（类型为 osvar 的 ACVAR 对象）使用 Windows 环境变量的值。

在 Windows 端点上使用操作系统变量时，应当遵守以下准则：

- 环境变量必须是系统变量。
- 如果您更改 Windows 环境变量的值，在 CA Access Control 重新启动之前不会识别此更改。 在 Windows 的某些版本中，您还必须重新启动计算机以便任何 Windows 服务和 CA Access Control 识别此更改。

端点解析变量的方式

变量让您可以将相同的策略部署到具有不同配置和不同操作系统的端点上。 以下过程说明了在已经创建和部署策略之后，CA Access Control 端点解析策略中的变量的方式：

1. 当 policyfetcher 提取策略时，CA Access Control 会检查策略中的变量是否已在策略或 CA Access Control 数据库中进行了定义。 将会发生以下情况之一：
   - 如果变量没有在策略或数据库中定义，CA Access Control 会将策略状态更改为“部署挂起”。

     注意：要部署该策略，您必须定义此未定义的变量，然后重新部署该策略。
   - 如果变量在策略或数据库中有定义，CA Access Control 会编译该策略并实施其包含的规则。
2. 对于每个检测信号，policyfetcher 会检查变量值是否已在 CA Access Control 数据库中更改。将会发生以下情况 之一：
   - 如果没有更改任何变量值，policyfetcher 会重复第 2 步。
   - 如果变量值已经更改，CA Access Control 会将端点上使用更改变量的任何策略的状态都更改为“不同步”。

     注意：要清除策略的“不同步”状态，您必须重新部署该策略。

排除策略部署故障

将策略分配给主机时，只有 policyfetcher 检索部署任务并运行策略脚本之后，才会在分配的端点上部署该策略。 因此，在端点上传输或部署策略时，可能会由于多种原因而导致部署错误。

为了解决策略部署错误，高级策略管理为您提供了一些故障排除操作。您可以使用 CA Access Control 企业管理 或 policydeploy 实用程序执行这些操作。 在 CA Access Control 企业管理 中，故障排除操作位于“策略管理”选项卡的“策略”子选项卡中。

故障排除操作如下所述：

- **重新部署**－创建包含策略脚本的一项新部署任务并将该任务部署到端点。

  在端点上部署策略出现错误时可使用该选项。 即，selang 策略脚本执行失败。 需要先手动解决端点上脚本错误的原因，才能重新部署策略。

  注意：该选项仅在 CA Access Control 企业管理 中提供，在 policydeploy 实用程序中不受支持。

- **取消部署**－从指定端点取消部署策略，但不从相应主机取消分配该策略。

  使用该选项可从端点中删除未分配给 DMS 上的主机的任何策略。

- **重置**－重置端点。 CA Access Control 可重置主机状态、取消部署所有有效策略，以及删除所有 GPOLICY、POLICY 和 RULESET 对象。

  使用该选项可从所有策略部署清除端点及其在 DMS 上的状态。

  注意：该选项不会从端点或 DMS 中删除 DEPLOYMENT 或 GDEPLOYMENT 对象，因为您可能需要使用这些对象来进行审核。在重置端点之后，可使用 dmsmgr -cleanup 功能删除 DEPLOYMENT 对象和 GDEPLOYMENT 对象。 在重置端点之后，可以照常将策略分配给该端点。

- **还原**－在指定主机上取消部署任何策略，然后还原应该在主机上部署（分配或直接部署）的所有策略，方法是创建新部署任务并将这些任务发送到主机执行。

  当您在端点上重新安装 CA Access Control 或操作系统时，或者当您从备份还原端点时，可使用该选项来重新部署 DMS 指示在该端点上有效的所有策略。

如何删除过时的端点

DMS 将存储有关您企业的信息。 如果在从计算机中卸载 CA Access Control 时从企业删除该计算机，则 DMS 仍将包含对该节点的引用。 作为例行维护程序，您应从这些过时节点中清除 DMS。

要删除过时的节点，请执行以下操作之一：

- 请在 DMS 计算机上运行 dmsmgr 实用程序来执行例行清理：

  `dmsmgr -cleanup number_of_days -dms name`

  number_of_days

  定义 CA Access Control 节点处于不可用状态的最少天数。

- 也可以通过在 DMS 计算机上输入以下 selang 命令来手工删除特定的节点：

  `rr HNODE HNODE_name`

重要说明！ 删除节点时，CA Access Control 将删除所有与 HNODE 相关的部署任务，删除所有部署任务程序包（除非它们具有其他部署任务成员），只有此时才会删除 HNODE 对象。

查看部署审核信息

CA Access Control 企业管理 可提供策略部署审核。 通过该审核可以查看策略部署－一个部署任务的描述性列表。 该列表详细说明了每个部署任务的触发条件、何时创建任务，以及涉及哪类部署。 对于每个部署任务，您可以进一步查找以下详细信息：该部署任务为哪个主机和策略对而创建、部署的策略版本、部署任务的状态（已排队、已成功或已失败）和 selang 输出（部署命令的结果）。

查看部署审核信息

1. 在 CA Access Control 企业管理 中，执行如下操作：
   a. 单击“策略管理”。
   b. 单击“策略”子选项卡。
   c. 在左侧的任务菜单中展开部署树。

   此时“部署审核”任务会显示在可用任务列表中。
2. 单击“部署审核”。

   将显示“部署审核”页面。

3. 定义部署审核的范围，然后单击“执行”。

   CA Access Control 企业管理 将于您所定义的范围内检索有关部署的信息，并在短暂延迟后显示结果。

4. （可选）单击部署触发器，以查看相关联的部署任务的有关详细信息。

策略偏差计算器的工作原理

通过高级策略管理，可查看应部署在端点（由于策略部署的原因）上的访问规则和已成功部署在同一端点上的实际规则之间的差异。 也可解决对策略对象进行的属性添加和更改。 您可以利用这些信息解决与策略部署相关联的问题。

在端点上运行策略偏差计算时，将执行以下操作：

1. 在本地主机中检索应在端点上部署的规则列表。

   它们是按本地 RULESET 对象中定义的方式为每个部署的策略指定的规则，而本地 RULESET 对象与每个部署的策略版本的 POLICY 对象关联。

2. 请检查是否已将每条规则应用于端点。

   重要说明！ 偏差计算不会检查是否应用了本地规则。 它还忽略从数据库中删除对象（用户或对象属性、用户或资源授权，或者实际用户或资源）的规则。 例如，计算无法验证是否应用了以下规则：
   rr FILE /etc/passwd

3. （可选）将本地策略对象与 DMS 上的策略对象进行比较。

   正常情况下，偏差计算器只检查本地主机上的偏差。 如果指定 *-strict* 选项，则偏差计算也会将与本地 HNODE 对象关联的策略和与 DMS 上的 HNODE 对象关联的策略进行比较。 包括以下内容：

   a. 与代表本地主机的 HNODE 对象相关联的策略列表

   b. 每个与 HNODE 对象关联的 POLICY 对象的策略状态

   c. 每个与 HNODE 对象关联的 POLICY 对象的策略签名

4. 输出以下两个文件：

   - *ACInstallDir*/data/devcalc/deviation.log

     记录在最后一次偏差计算过程收集到的错误消息。

   - *ACInstallDir*/data/devcalc/deviation.dat

     策略及其偏差的列表。 您可以在端点上使用 selang 命令 *get devcalc* 获取此文件的内容。

   注意：CA Access Control 还会发送审核事件，使用 *seaudit -a* 可查看此类事件。 有关 seaudit 实用程序的详细信息，请参阅 *《参考指南》*。

5. 将发现的任何偏差通知 DMS。

   通过为本地 CA Access Control 数据库指定的 DH 将通知发送给 DMS。

偏差计算触发器

应当定期执行偏差计算，以使 DMS 包含有关策略偏差状态的最新信息。 如果您在端点上启用高级策略管理，policyfetcher 会在每个检测信号之后触发偏差计算。

注意：默认运行的偏差计算不考虑添加到端点的项。 要查看这些项目，请更改 devcalc_command 配置设置以便以 *精确*模式运行偏差计算。

建议您修改 policyfetcher 设置以便进行策略偏差计算的间隔能够满足您的要求。

策略偏差日志和错误文件

在每次偏差计算过程中，策略偏差计算都会编写新的日志。 该日志还包含错误消息，存储在 *ACInstallDir*/data/devcalc/deviation.log

如果您在报告中看到的偏差结果（从 DMS 检索得到）不是从最后一次运行偏差计算得到的，请使用该日志。 它可以帮助您诊断为什么偏差计算结果没有发送到 DMS 的原因。

示例：偏差日志和错误文件

下面是一个偏差日志和错误文件示例：

```
start time: Mon Jan 23 13:04:48 2006
WARNING, \"检索 DH 主机名失败，将在本地存储偏差\"
found deviation(s) for policy 'iis8#02'
end time: Mon Jan 23 13:05:04 2006
```

策略偏差数据文件

策略偏差计算编写一个包含策略及其偏差的列表的数据文件。 该数据文件存储在 *ACInstallDir*/data/devcalc/deviation.dat

注意：该数据文件中包含的策略列表取决于进行偏差计算的策略（默认情况下，所有策略和所有策略版本都在端点上）。

重要说明！ 偏差计算不会检查是否应用了本地规则。 它还忽略从数据库中删除对象（用户或对象属性、用户或资源授权，或者实际用户或资源）的规则。 例如，计算无法验证是否应用了以下规则：
rr FILE /etc/passwd

偏差状态发送到 DMS（无论是否存在偏差），但实际偏差在本地存储。创建报告时，可以从此文件中检索实际偏差结果，并将其添加到报告中。

在策略偏差数据文件中包含以下行：

日期

显示偏差计算的时间戳。 日界行始终是偏差报告的第一行。

格式：DATE, *DDD MMM DD hh:mm:ss YYYY*

Strict

指定用 -strict 选项运行偏差计算。

格式：STRICT, *DMS@hostname*, *策略名称*#*xx*, [1|0]

[1|0] 表示是否在与本地 HNODE 对象关联的策略以及与 *DMS@hostname*（第一个可用 DMS）上的 HNODE 对象关联的策略之间找到偏差，(1) 表示已找到，(0) 表示没有找到。

Policy Start

启动定义该策略版本偏差的策略块。

格式：POLICYSTART, *策略名称*#*xx*

Difference

说明为策略找到的偏差。 出现偏差的策略名称显示在此行上面最近的*策略行*中。

有八种类型的偏差，四种显示缺少的元素，而另外四种显示添加的元素，如下表所示：

偏差类型	格式
未找到类	DIFF, -(*class_name*), (*), (*), (*)

偏差类型	格式
未找到对象	DIFF, (*class_name*), -(*object_name*), (*), (*)
已添加对象	DIFF, (*class_name*), +(*object_name*), (*), (*)
未找到属性	DIFF, (*class_name*), (*object_name*), -(*property_name*), (*)
已添加属性	DIFF, (*class_name*), (*object_name*), +(*property_name*), (*)
缺少属性值	DIFF, (*class_name*), (*object_name*), (*property_name*), *-(expected_value*)
已添加属性值	DIFF, (*class_name*), (*object_name*), (*property_name*), *+(value*)

注意：当偏差计算器检测到缺少类时，也会为所有缺失对象、属性和值创建偏差行。

Policy End

结束定义该策略的偏差的策略块。

格式：POLICYEND, *policy_name#xx*, [1|0]

[1|0] 表示是否找到偏差，(1) 表示找到，(0) 表示没有找到。

警告

说明警告。

格式：WARNING, "*warning_text*"

示例：偏差数据文件

以下示例显示了偏差数据文件的摘录内容：

```
Date, Sun Mar 19 08:30:00 2006
WARNING, "检索 DH 主机名失败，将在本地存储偏差"
POLICYSTART, iis8#02
DIFF, (USER), (iispers), (*), (*)
POLICYEND, iis8#02, 1
```

显示缺少元素的偏差

偏差计算器可将缺少的元素与添加的新元素区分开。 缺少的元素是指在指定策略中明确定义但本地主机中不存在的 CA Access Control 元素。这些缺少的元素可能为：类、对象、属性和值。

任意缺少的元素组合都定义了一个层级结构要求。 例如，如果 Policy1 具有以下规则：

```
eu mytestuser2 operator
```

偏差计算器要求满足以下隐性要求：

- 类 USER 必须存在

  该规则定义了属于 USER 类的用户。

- USER 对象 mytestuser2 必须存在

  该规则明确涉及 USER 类的 mytestuser2 对象。

- 属性 OBJ_TYPE 必须存在

  该规则使用操作符参数设置 USER 对象的 OBJ_TYPE 参数。

- 将值 Operator 分配给 OBJ_TYPE 属性

  该规则明确地设置该值。

显示添加元素的偏差

偏差计算器可将缺少的元素与添加的新元素区分开。 添加的元素是指在本地定义但指定策略中不存在的 CA Access Control 元素。 这些添加的元素可能为：类、对象、属性和值。

如果本地异常已执行如下操作，则将包括添加偏差：

- 将新值添加到策略内所提及对象的属性。
- 将新属性添加到策略内所提及的对象。

注意：新对象（任何策略均未提及的对象）不会被视为添加；这同样适用于新类。

显示已修改元素的偏差

当偏差数据文件中没有单一偏差行显示修改时，就会发生显示已修改元素的偏差。 要识别修改，需要查找适用于同一元素的连续删除和添加行。 例如，在偏差数据文件的以下提取项中，具有 Operator 值的 mytestuser 已被修改为具有 Auditor 和 Administrator 两个值：

```
DIFF, (USER), (mytestuser2), (OBJ_TYPE), -(Operator)
DIFF, (USER), (mytestuser2), (OBJ_TYPE), +(Auditor)
DIFF, (USER), (mytestuser2), (OBJ_TYPE), +(Administrator)
```

第 5 章： 规划您的 PUPM 实施

此部分包含以下主题：

特权用户密码管理

特权用户密码管理 (PUPM) 是一种进程，企业可通过该进程保护、管理和跟踪与企业中权限最高的用户相关的所有活动。

PUPM 从中央位置向目标端点上的特权帐户提供基于角色的访问管理。PUPM 提供特权帐户和应用程序 ID 密码的安全存储，并基于您定义的策略控制对特权帐户和密码的访问。 此外，PUPM 管理特权帐户和应用程序密码生命周期，并让您可以从配置文件和脚本中删除密码。

什么是特权帐户？

特权帐户是一种不被分配给单个帐户且有权访问关键任务数据和进程的帐户。 系统管理员使用特权帐户在目标端点上执行管理任务，特权帐户也被嵌入到服务文件、脚本和配置文件中以便于无人处理。

特权帐户难以控制，因为他们不会被分配给可识别的用户，这会出现审核和跟踪困难。 这是让关键任务系统接触到意外损害和恶意活动的漏洞。 组织必须将这些特权帐户的数量减少到满足运营需求的下限。

通过删除或使应用程序不可访问，管理员可以绕过大多数内部控制来访问受限信息并引起拒绝服务 (DOS) 攻击。 此外，使用特权帐户执行的活动难以与可识别的用户帐户相关联。

特权访问角色和特权帐户

使用特权访问角色来指定每名用户可以在 CA Access Control 企业管理 中执行的 PUPM 任务以及每名用户可以签入和签出的特权帐户。 CA Access Control 企业管理 附带有预定义的特权访问角色。 您可以修改预定义的角色来适合企业需求，也可以创建全新的角色。

当用户登录到 CA Access Control 企业管理 时，仅会看与其角色相对应的任务和特权帐户。

更多信息：

特权访问角色 (p. 22)

使用特权访问角色

为企业设置 PUPM 之前，您应当考虑下列几点：

- 建议您使用 Active Directory 作为用户存储，并修改每个角色的成员策略以便指向 Active Directory 中的组。 要将用户添加到您以这种方式设置的角色或将其从中删除，可将用户添加到 Active Directory 组或从中删除用户。 这会降低管理上的开销。
- 如果使用 Active Directory 作为用户存储，则无法使用 CA Access Control 企业管理 来创建或删除用户或组。 您只能在 Active Directory 中创建和删除用户和组。
- 如果角色定义了成员策略，而当 PUPM 用户管理器将此特定角色分配给用户，但是该用户不适合成员策略的范围时，那么 CA Access Control 不会将此角色分配给该用户。 在成员策略中定义的规则优先于 PUPM 用户管理器的分配。
- 要回应特权帐户请求，用户必须有“PUPM 批准人”角色，并且是提出请求的用户的经理。 如果使用嵌入式用户存储，您可以在 CA Access Control 企业管理 中的“创建用户”和“修改用户”任务中指定用户的经理。
- 在预先设置中，CA Access Control 会将“紧急情况”、“PUPM 批准人”、“特权帐户请求”以及“PUPM 用户”角色分配给所有用户。 要更改该行为，请修改每个角色的成员策略。
- 您可以修改角色的范围规则以定义该角色可以访问的特定端点和特权帐户。 通过范围规则，您可以在整个企业中实施对特权帐户的细化访问。 范围规则在角色的成员策略中进行定义。

更多信息：

成员策略 (p. 27)

特权访问角色如何影响签出和签入任务

您签出特权帐户在端点上执行管理任务，并在您完成端点上的操作时签入特权帐户。

重要说明！ 用户必须有端点特权访问角色才能在端点类型上执行任务。 端点特权访问角色使用授权访问帐户指定用户可以执行任务的端点类型。 例如，如果您将 Windows Agentless 端点特权访问角色分配给用户，用户可以在使用授权帐户的 Windows 端点上执行端点任务。 如果您将“紧急情况”、“授权帐户请求”或“PUPM 用户”角色分配给用户，您还必须为其分配端点特权访问角色，否则用户将不能完成任何任务。

以下过程说明了特权访问角色如何影响用户执行的签出和签入任务：

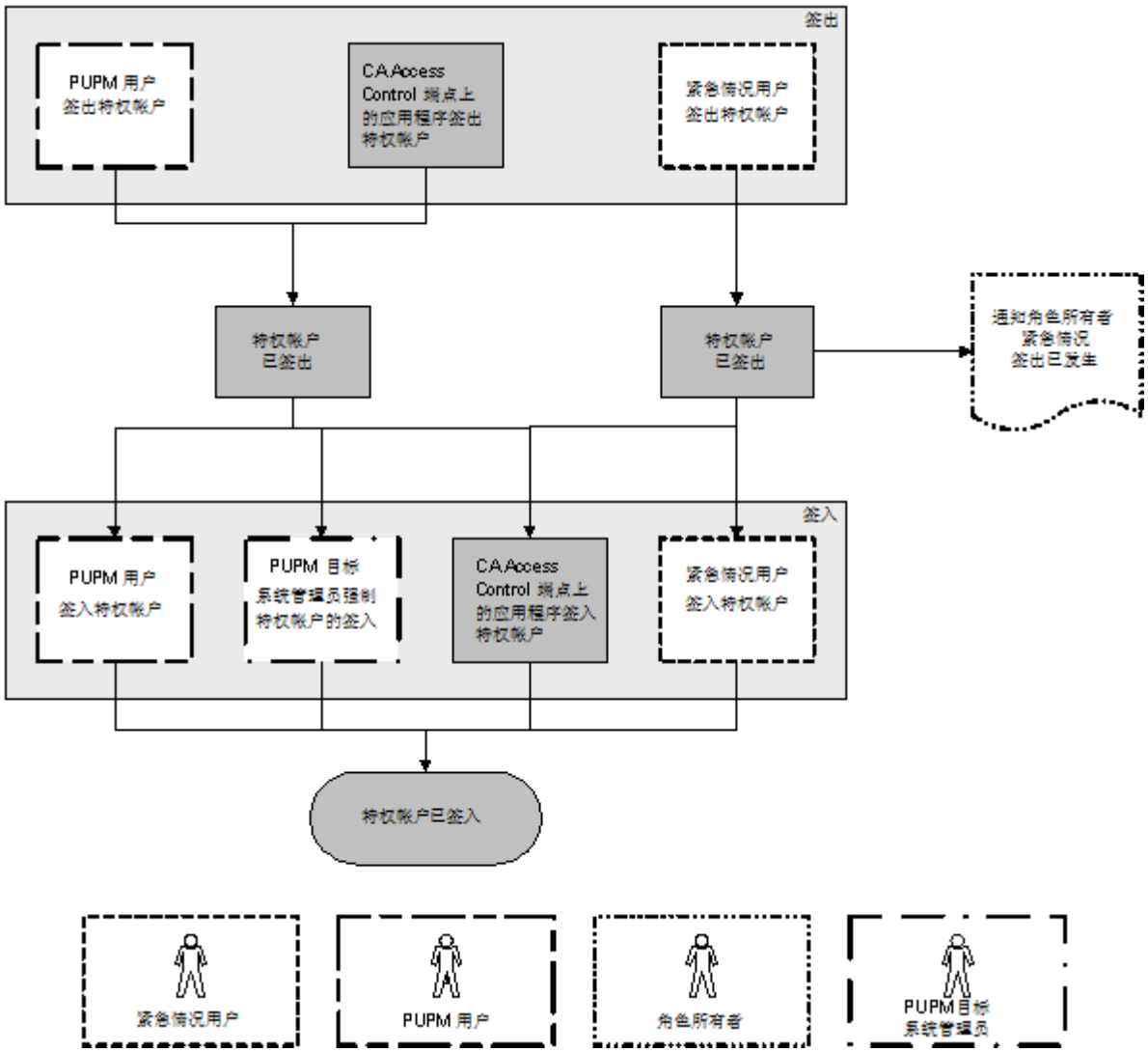
1. 用户使用下列方式之一签出特权帐户：
   - 具有“PUPM 用户”角色的用户签出特权帐户。
   - 具有“紧急情况”角色的用户执行紧急情况签出。
   - CA Access Control 端点上的应用程序（例如 CLI 密码使用方）签出特权帐户。

   特权帐户被签出。

   注意：如果用户执行紧急情况签出，CA Access Control 会向角色所有者发送通知消息。 角色所有者可以选择将信息添加到该消息中用于审核。
2. 用户使用下列方式之一签入特权帐户：
   - 具有“PUPM 用户”角色的用户签入特权帐户。
   - 具有“紧急情况”角色的用户签入特权帐户。
   - CA Access Control 端点上的应用程序签入特权帐户。
   - 具有“PUPM 目标系统管理员”角色的用户强制签入特权帐户。

   特权帐户被签入。

下图说明特权访问角色如何影响用户执行的签入和签出任务：



示例：签出特权帐户

您具有“系统管理员”角色。 您为 Joe 分配“PUPM 用户”角色和 Windows Agentless Connection 端点特权访问角色。 Joe 登录到 CA Access Control 企业管理，仅会看到让其签出和签入 Windows 端点上的特权帐户的任务。

示例：特权帐户的紧急情况

您具有“系统管理员”角色。 您为 Fiona 分配“紧急情况”角色和 Oracle Server 连接端点特权访问角色。 Fiona 需要对 Oracle 端点进行即时访问。 她登录到 CA Access Control 企业管理，仅会看到让她在 Oracle 端点上执行紧急情况签出的任务。 Fiona 执行 Oracle 特权帐户的紧急情况签出，CA Access Control 将通知消息发送到“紧急情况”角色所有者。

注意：默认情况下，“紧急情况”角色所有者是“系统管理员”管理角色。

特权访问角色如何影响特权帐户请求任务

如果用户无法签出特权帐户而且不需要对该帐户进行即时访问，用户可以提交特权帐户请求。 用户的经理可以批准或拒绝特权帐户请求。 该主题说明了用户需要哪种特权访问角色来执行特权帐户请求任务。

重要说明！ 用户必须有端点特权访问角色才能在端点类型上执行任务。 端点特权访问角色使用授权访问帐户指定用户可以执行任务的端点类型。 例如，如果您将 Windows Agentless 端点特权访问角色分配给用户，用户可以在使用授权帐户的 Windows 端点上执行端点任务。 如果您将“紧急情况”、“授权帐户请求”或“PUPM 用户”角色分配给用户，您还必须为其分配端点特权访问角色，否则用户将不能完成任何任务。

以下过程说明了特权访问角色如何影响用户可以执行的特权帐户请求任务：

1. 具有“特权帐户请求”角色的用户请求对特权帐户的访问。
2. CA Access Control 将特权帐户请求发送给用户的经理，该经理还具有“PUPM 批准人”角色。

   注意：用户必须具有“PUPM 批准人”角色*并且*是用户的经理才能接收特权帐户请求。

3. 具有“PUPM 批准人”角色的用户对特权帐户请求作出响应，并执行以下操作之一：

   - 拒绝特权帐户请求。

     具有“特权帐户请求”角色的用户无法签出特权帐户。

   - 保留特权帐户请求。

     没有其他用户可以批准或拒绝特权帐户请求。 具有“特权帐户请求”角色的用户无法签出特权帐户，直到“PUPM 批准人”选择批准该请求。

   - 批准特权帐户请求。

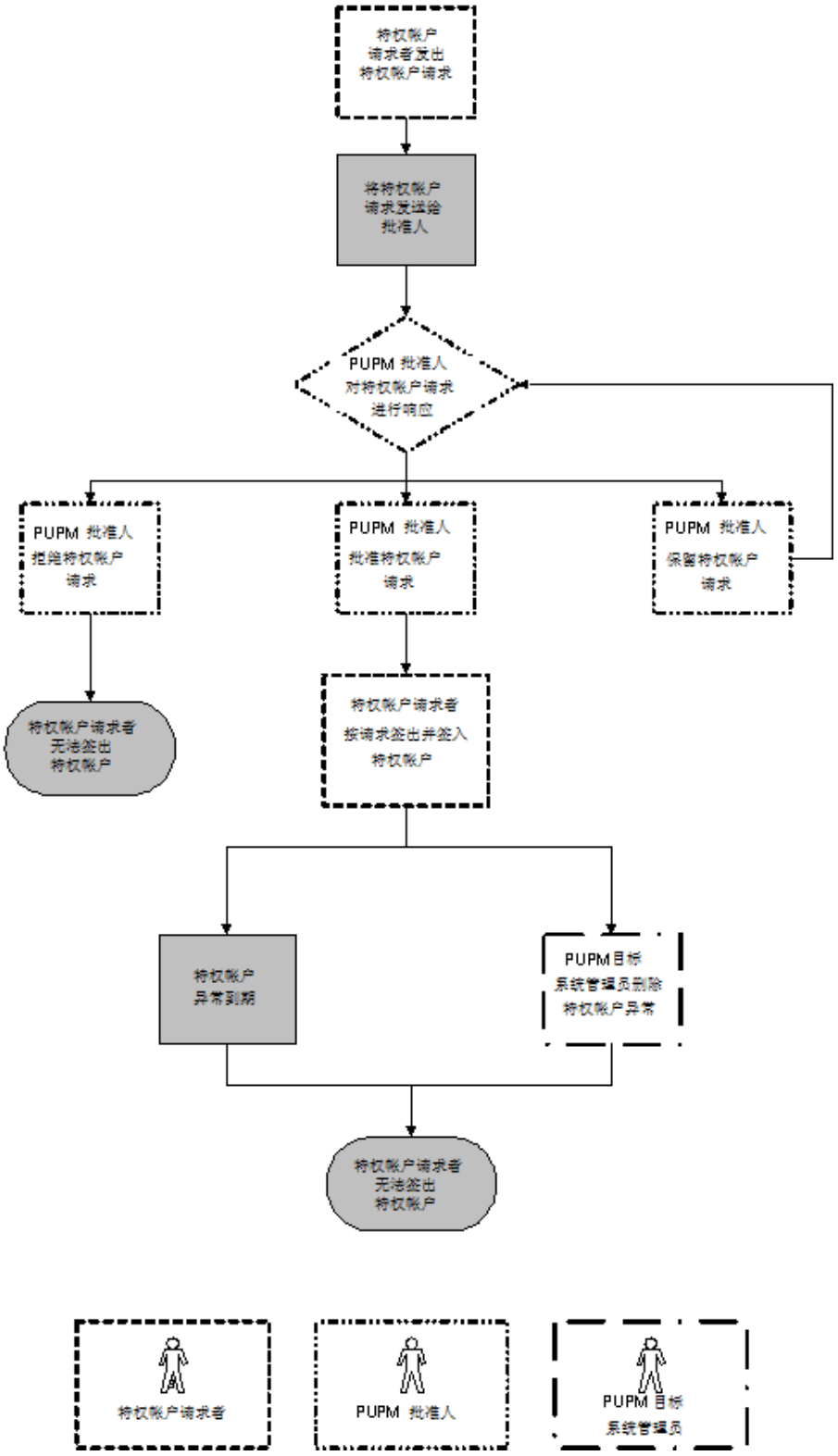
     具有“特权帐户请求”角色的用户被授予特权帐户异常，并且可以签出和签入特权帐户。

4. 特权帐户异常由于以下某项原因而到期：

   - 到达了在特权帐户异常中指定的截止时间。
   - 具有“PUPM 目标系统管理员”角色的用户删除特权帐户异常。

   具有“特权帐户请求”角色的用户无法再签出特权帐户。

下图说明了特权访问角色如何影响用户可以执行的特权帐户请求任务：



示例：提出特权帐户请求和对其作出响应

您具有“系统管理员”角色。 您为 Alice 分配“特权帐户请求”角色和 SSH 设备连接端点特权访问角色。 Bob 是 Alice 的经理，您为 Bob 分配“PUPM 批准人”角色。

Alice 登录到 CA Access Control 企业管理，仅会看到让她针对 UNIX 端点上的帐户提交特权帐户请求的任务。 Alice 针对 UNIX 端点上的 example_ux 帐户提交特权帐户请求。

Bob 登录到 CA Access Control 企业管理，仅会看到让他回应特权帐户请求的任务。 Bob 批准 Alice 的授权访问请求，并指定特权帐户异常在下午 6 点之前有效。 现在，Alice 可以签入和签出 example_ux 特权帐户。 下午 6 点时，特权帐户异常到期，而 Alice 不能再签出 example_ux 特权帐户。

在紧急情况处理期间会发生什么事情

用户需要立即访问其无权管理的帐户时，会执行紧急情况签出。

紧急情况帐户是未按照用户角色分配给用户的特权帐户。 但是如果有需要，用户可以获得帐户密码。

在紧急情况签出过程中，会给角色管理员发送一个通知消息，通知管理员发生紧急情况签出过程，不过管理员无法批准也无法停止该过程。

签出的紧急情况帐户会添加到用户在“主页”选项卡“紧急情况”选项中的“我的签出特权帐户”选项卡中。

注意：只有具有紧急情况特权访问角色的用户才可以执行紧急情况处理。

密码使用方

*密码使用方*是使用特权帐户和服务帐户来执行脚本、连接到数据库或管理 Windows 服务、排定任务或 RunAs 命令的应用程序、Windows 服务和 Windows 排定任务。 *服务帐户*是 Windows 服务使用的内部帐户。 例如，Windows 服务可以使用 NT AUTHORITY\LocalService 服务帐户登录到操作系统。

通过密码使用方，您可以从应用程序脚本中删除硬编码密码，并在端点上实施密码策略。 例如，您可以在 Windows 端点上为每个排定任务创建密码使用方，并且指定每个密码使用方使用相同的密码策略。 然后，PUPM 将以密码策略中指定的时间间隔更改每个排定任务的密码。

PUPM 使用下列方法向密码使用方提供特权帐户密码：

- 按需 — 当密码使用方发送对特权帐户密码的请求时，例如，当特权帐户使用 ODBC 连接到数据库时，此时需要身份验证。

  注意：您必须在启用了“PUPM 集成”功能的 PUPM 端点上安装 CA Access Control 才能使用按需获取密码的密码使用方。

- 当密码更改 — 当对于 CA Access Control 企业管理 中的密码使用方来说发生密码更改事件时，例如，当密码策略指定服务帐户的密码在固定的时间段后必须更改时。

  注意：您不需要在 PUPM 端点上安装 CA Access Control 即可使用在密码更改时获取密码的密码使用方。

各种类型的密码使用方

密码使用方表示了您在 PUPM 端点上运行的应用程序、Windows 服务或 Windows 排定任务。 除了“软件开发工具包”密码使用方之外，所有其他密码使用方都获得特权帐户密码，但是不签出或签入密码。

PUPM 按照需要向下列密码使用方提供特权帐户密码：

- **软件开发工具包 (SDK/CLI)** — 当端点上的脚本执行“软件开发工具包”密码使用方时，该密码使用方会请求特权帐户密码。

  使用“软件开发工具包”密码使用方来替换脚本中的硬编码密码。

  注意：与其他密码使用方不同，“软件开发工具包”密码使用方可以签出和签入特权帐户密码。

- **数据库（ODBC、JDBC、OLEDB、OCI、.NET）** — 当在端点上运行的程序连接到数据库时，“数据库”密码使用方会请求特权帐户密码。

  使用“数据库”密码使用方来替换连接到数据库的程序中的硬编码密码。

- **Windows 运行身份** — 当用户执行 RunAs 应用程序来替代特权帐户并执行特定命令时，“Windows 运行身份”密码使用方会请求密码。

  使用“Windows 运行身份”密码使用方让用户替代特权帐户并在没有特权帐户密码的情况下执行命令。

注意：您必须在启用了“PUPM 集成”功能的 PUPM 端点上安装 CA Access Control 才能使用按需获取密码的密码使用方。

PUPM 在密码更改时为以下密码使用方提供特权帐户密码：

- **Windows 排定任务** —“Windows 排定任务”密码使用方使用服务帐户来管理排定任务。 无论何时在 CA Access Control 企业管理 中发生密码更改事件，PUPM 都会强制该任务进行密码更改。

  使用“Windows 排定任务”密码使用方来设置密码策略并自动化排定任务的密码更改。

- **Windows 服务** —“Windows 服务”密码使用方使用服务帐户来运行 Windows 服务。 无论何时在 CA Access Control 企业管理 中发生密码更改事件，PUPM 都会强制该服务帐户进行密码更改。

  使用“Windows 服务”密码使用方来设置密码策略并自动化 Windows 服务的密码更改。 服务必须由您可以更改其密码的帐户运行，例如，您计算机的管理员帐户或域帐户。

注意：您不需要在 PUPM 端点上安装 CA Access Control 即可使用在密码更改时获取密码的密码使用方。

更多信息：

创建密码使用方 (p. 199)

密码使用方按需获取密码的方式

当关联的特权帐户验证其他应用程序时，密码使用方从 PUPM 检索密码。 按需获取密码的密码使用方将密码请求转发到 PUPM 代理，该代理使用消息队列与 CA Access Control 企业管理 进行通信。

“软件开发工具包”、“数据库”和“Windows 运行身份”密码使用方按需获取密码。 您使用按需获取密码的密码使用方来替换脚本中的硬编码密码。 无论何时应用程序提供密码用于身份验证时，PUPM 都会将硬编码密码替换成特权帐户密码。

注意：您必须在启用了“PUPM 集成”功能的 PUPM 端点上安装 CA Access Control 才能使用按需获取密码的密码使用方。

以下过程说明了密码使用方按需获取特权帐户密码的方式：

1. 应用程序使用硬编码密码来尝试连接到需要用户身份验证的系统。
2. 密码使用方会拦截连接尝试。

   例如，OCI 密码使用方会拦截连接到 Oracle 数据库的尝试。

3. PUPM 代理检查缓存。 会出现以下情况之一：
   - 如果请求已缓存，PUPM 代理将特权帐户密码转发给密码使用方。 密码使用方将硬编码密码替换成特权帐户密码。 应用程序使用特权帐户密码登录到系统。 该过程在此步骤完成。 CA Access Control 企业管理 不写入密码检索的审核记录。
   - 如果请求没有缓存，PUPM 代理会将密码请求转发给 CA Access Control 企业管理。
4. CA Access Control 企业管理 接收消息并检查密码使用方是否有权获取特权帐户密码。
5. 会出现以下情况之一：
   - 如果密码使用方有权获取密码，CA Access Control 企业管理 会将特权帐户密码发送到 PUPM 代理。 PUPM 代理将硬编码密码替换为特权帐户密码。 应用程序使用特权帐户密码登录到系统。 CA Access Control 企业管理 写入事件的审核记录。
   - 如果密码使用方无权获得密码，CA Access Control 企业管理 会将错误消息发送到 PUPM 代理。 PUPM 代理不将密码转发给应用程序，因此应用程序使用硬编码密码登录到系统。

PUPM 将密码更改通知给密码使用方的方式

当 CA Access Control 企业管理 中发生密码更改事件时（例如，当密码策略指定密码必须在固定的事件段后更改时），PUPM 会强制密码使用方进行密码更改。 CA Access Control 企业管理 使用 JCS 与当密码更改时获得密码的密码使用方进行通信。

只有“Windows 排定任务”和“Windows 服务”密码使用方在密码更改时获得密码。

注意：您不需要在 PUPM 端点上安装 CA Access Control 即可使用在密码更改时获取密码的密码使用方。

以下过程说明了 PUPM 将密码更改通知密码使用方的方式：

1. 密码更改事件生成新的密码。
2. CA Access Control 企业管理 在中央数据库中搜索使用密码的密码使用方。
3. JCS 使用当您创建端点时提供的管理员凭据登录到每个受到影响的端点。

4. JCS 尝试更改端点上的密码使用方的密码。 会出现以下情况之一：
   - JCS 更改端点上的密码使用方的密码并且可以选择重新启动服务。

     注意：您在创建密码使用方时指定 JCS 是否重新启动服务。
   - JCS 无法更改端点上的密码使用方的密码。 CA Access Control 企业管理 在启动更改密码事件的任务中编写通知消息。
5. CA Access Control 企业管理 写入密码更改的审核记录。

   注意：您使用“查看提交的任务”查看 PUPM 审核记录。 如果 JCS 无法更改密码使用方的密码，您可以使用“同步密码使用方”来重试密码更改。

更多信息：

同步密码使用方 (p. 238)

密码使用方的实施注意事项

在您实施密码使用方之前，请考虑以下情况：

- 要使用“软件开发工具包”、“数据库”、“Windows 运行身份”密码使用方，您必须在 PUPM 端点上安装启用了“PUPM 集成”功能的 CA Access Control。
- 要使用 JDBC 数据库密码使用方，连接到数据库的应用程序必须使用 JRE 1.5 或更高版本。
- 要使用 OCI 数据库密码使用方，连接到数据库的应用程序必须使用 OCI8 或更高版本。
- 要将 ODBC 或 OLEDB 数据库密码使用方与非默认的驱动程序结合使用，您必须联系 CA Technologies 支持。

  注意：在 ApplyOnProcess 注册表项中 ODBC 或 OLEDB 插件的注册表子项中定义了默认的驱动程序。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。
- 要使用 Java PUPM SDK 密码使用方，您编写的 Java 应用程序必须使用 JRE 1.5 或更高版本。
- 要使用 .NET PUPM SDK 密码使用方，您必须在端点上安装 .NET Framework 2.0 或更高版本。
- 当您发现服务帐户来创建“Windows 服务”或“Windows 排定任务”密码使用方时，CA Access Control 仅会发现由您可以更改其密码的帐户运行的服务。

- 要发现是域帐户的服务帐户，您必须创建表示帐户所在的域控制器 (DC) 的 PUPM 端点。 该端点必须具有以下属性：
  - 端点类型 — Windows Agentless
  - 是否 Active Directory — 真
  - 主机域 — DC 所属的域名
  - 用户域 — DC 上定义的用户所属的域名

    注意：仅当管理帐户来自的域不同于这些帐户所在的域时才会指定用户域。

更多信息：

发现服务帐户 (p. 197)

PUPM 审核记录

CA Access Control 企业管理 记录事件的审核数据，例如，用户签入特权帐户密码的时间。 CA Access Control 企业管理 还记录失败事件的审核数据。 例如，如果当您签出特权帐户密码但是不接受 ActiveX 下载时选择了自动登录，CA Access Control 企业管理 会记录自动登录失败的原因。 CA Access Control 企业管理 将 PUPM 审核数据存储在中央数据库中。

更多信息：

审核数据 (p. 39)
审核特权帐户 (p. 234)

密码使用方审核记录

每次当密码使用方提出密码请求而 PUPM 代理从企业管理服务器获取密码时，CA Access Control 企业管理 都会写入审核记录。 当密码使用方提出密码请求而请求失败时，CA Access Control 企业管理 也会写入审核记录，例如，当密码使用方对无权访问的密码提出请求时。

当密码使用方提出密码请求而端点上的 PUPM 代理从缓存获取密码时，CA Access Control 企业管理 不写入审核记录。

PUPM 导送程序审核记录

PUPM 导送程序将执行以下任务。 CA Access Control 企业管理 为 PUPM 导送程序执行的每个操作创建一个审核记录：

- 导送程序文件夹轮询－指定 PUPM 导送程序是否将轮询文件夹中的 CSV 文件成功上传到 CA Access Control 企业管理。
- 导送程序过程 CSV 文件－指定 CA Access Control 企业管理 是否成功处理了上传的 CSV 文件，并提供一个进度指示器，以便跟踪 CA Access Control 企业管理 在 CSV 文件中处理的行数。

此外，CA Access Control 企业管理 还为所导入的 CSV 文件中的每一行创建一个审核记录。 每一行都代表一个创建或修改 PUPM 端点或特权帐户的任务。 审核记录用于跟踪每项任务的状态。 这些任务可具有以下状态：

- **已完成**－CA Access Control 企业管理 完成了任务，如创建了特权帐户。
- **已失败**－CA Access Control 企业管理 处理了任务，但是没有完成，如无法在不存在的端点上创建特权帐户。
- **已审核**－CA Access Control 企业管理 尚未处理或完成任务，如因未指定 ACCOUNT_NAME 属性而无法创建特权帐户。

具有系统管理员角色的用户可以使用“查看提交的任务”任务来查看每项任务的状态。

PUPM 端点上的审核事件

CA Access Control 企业管理 会记录企业管理服务器上发生的事件的审核数据。 如果将您的 PUPM 端点与 CA Enterprise Log Manager 相集成，您还可以在端点上记录每个特权帐户会话的审核事件。

在用户签出特权帐户并使用该帐户登录到端点后，该集成让您可以跟踪特权帐户在端点上执行的操作。 这些操作记录在审核事件中，而审核事件收集在 CA Enterprise Log Manager 报告中。 您可以在 CA Access Control 企业管理 中查看这些 CA Enterprise Log Manager 报告。

例如，在用户签出名为 privileged1 的帐户之后，您想查看该用户执行的操作。 使用 CA Access Control 企业管理 中的“审核特权帐户”任务查找 privileged1 帐户签出的审核记录。 然后，从该审核记录进行深入查询，并查看 privileged1 帐户在端点上所执行活动（例如，打开和关闭程序）的 CA Enterprise Log Manager 报告。

更多信息：

在 PUPM 端点上查看审核事件 (p. 238)

如何将 PUPM 端点与 CA Enterprise Log Manager 相集成

通过将您的 PUPM 端点与 CA Enterprise Log Manager 相集成，您可以记录端点上每个特权帐户会话的审核事件。 集成让您还可以在 CA Access Control 企业管理 中查看 PUPM 端点上特权帐户审核事件的 CA Enterprise Log Manager 报告。

要将您的 PUPM 端点与 CA Enterprise Log Manager 相集成，请执行如下操作：

1. 在 CA Access Control 企业管理 中：
   a. 配置到 CA Enterprise Log Manager 的连接。
   b. 指定每个 PUPM 端点的 CA Enterprise Log Manager 主机名和事件日志名称。

      要指定主机名和事件日志名称，请使用“创建端点”或“修改端点”任务的 CA Enterprise Log Manager 选项卡。
2. 配置 CA Enterprise Log Manager 以便能够从 PUPM 端点不断收集信息。

注意：有关如何配置到 CA Enterprise Log Manager 的连接的更多信息，请参阅 *《实施指南》*。 有关如何配置 CA Enterprise Log Manager 的更多信息，请参阅 CA Enterprise Log Manager 文档。

更多信息：

创建端点 (p. 151)
在 PUPM 端点上查看审核事件 (p. 238)

CA Service Desk Manager 集成

PUPM 能够与 CA Service Desk Manager 进行通信以便作为特权帐户请求和审批流程的一部分接受和验证票单。 当与 CA Service Desk Manager 相集成时，PUPM 针对活动的票单验证对特权帐户密码的每个请求。 通过将 PUPM 与 CA Service Desk Manager 相集成，您可以为包括多个审批流程的特权帐户请求创建验证过程。

特权帐户请求与 CA Service Desk Manager 的集成方式

了解 PUPM 与 CA Service Desk Manager 的集成方式可帮助您设置到 CA Service Desk Manager 的连接并实施验证过程。

要将 PUPM 与 CA Service Desk Manager 相集成，请执行以下操作：

1. 部署并配置 CA Service Desk Manager。
2. 从 CA Access Control 企业管理 配置到 CA Service Desk Manager 的连接。
3. 使用 CA Service Desk Manager 打开一个服务台票单，请求对特权帐户的访问权限。
4. 使用 CA Service Desk Manager 批准服务台请求。
5. 在 CA Access Control 企业管理 中创建特权帐户请求，并提供 CA Service Desk Manager 票单号。
6. 批准或拒绝特权帐户请求。

配置到 CA Service Desk Manager 的连接

可在 CA Access Control 企业管理 中定义到 CA Service Desk Manager 的连接，以将 PUPM 与 CA Service Desk Manager 集成在一起。

配置到 CA Service Desk Manager 的连接

1. 在 CA Access Control 企业管理 中，依次选择“系统”、“连接管理”、“CA Service Desk Manager”、“管理的 CA Service Desk Manager 连接”。

   此时会打开“管理的 CA Service Desk Manager 连接”窗口。

2. 使用以下内容填写表单：

   连接名称

   定义连接名称。

   默认值：主 CA Service Desk Manager 连接

   连接类型

   指定连接类型。

   默认值：CA Service Desk Manager

   连接说明

   为连接指定说明。

主机名

定义 CA Service Desk Manager Web 服务 URL。

默认值：
http://*host_name*:8080/axis/services/USD_R11_WebService?wsdl

用户 ID

定义用来连接至 CA Service Desk Manager 的用户 ID。

注意：用户必须有权限通过 Web 服务 API 查询服务台票单。

密码

为用户 ID 定义密码。

强制

指定用户在请求访问特权帐户时是否必须输入票单号。

注意：如果未选定，则在请求访问特权帐户时不会强制用户输入票单号。

已启用

指定连接是否已启用。

注意：如果未选定，则请求特权帐户任务中不会显示票单号字段。

高级

指定是否要定义高级设置。 如果选择此选项，将显示以下字段：

票单类型

定义用于请求特权帐户密码的 CA Service Desk Manager 票单的类型。

限制： cr、iss、chg

默认值： cr

注意： 该字段区分大小写。

票单查询

定义用于验证票单的自定义查询。指定任意有效的 CA Service Desk Manager 查询。

示例： active=1 AND status='OP

注意： 如果将该字段留空，CA Access Control 企业管理 会枚举所有服务台票单来验证请求者票单。

3. 单击“提交”。

   此时 CA Access Control 企业管理 会测试连接设置并创建连接器服务器。

注意： 有关 CA Service Desk Manager 的更多信息，请参阅 CA Service Desk Manager 文档。

更多信息：

特权帐户请求与 CA Service Desk Manager 的集成方式 (p. 120)

实施注意事项

下列主题列出了在实施 PUPM 之前应当考虑的项目。

特权帐户密码的电子邮件通知

有时，当用户尝试签出密码时，CA Access Control 企业管理 挂起的时间要比 20 秒长，例如，当网络很慢时。 如果 CA Access Control 企业管理 挂起长于 20 秒，则屏幕超时且密码不会显示给用户。 而 CA Access Control 企业管理 将密码用电子邮件的方式发送给用户。

要帮助确保用户收到密码，请执行以下操作：

- 配置 CA Access Control 企业管理 的电子邮件通知设置。
- 确认用户存储中记录了每个 PUPM 用户的有效电子邮件地址。

注意：有关配置电子邮件通知的详细信息，请参阅 *《实施指南》*。

Windows Agentless 端点上的域用户限制

如果您配置本地计算机上的域用户，PUPM 无法更改域用户的密码。 该限制是由于 Windows 行为引起的。

用于管理 Active Directory 端点的最小权限

在 Windows 上有效

如果要使用 PUPM Windows Agentless 端点类型来管理 Active Directory 端点，且不想指定域管理员帐户，那么您可以指定管理常规用户帐户所需的具有最小权限的指派用户帐户。

示例：指派 Active Directory 用户管理 Windows Server 2008 上的其他 Active Directory 用户的权限

以下示例向您显示如何为常规用户指派管理 Windows Server 2008 上的其他常规 Active Directory 用户的权限。

1. 选择“开始”、“管理工具”、“组件服务”

   此时打开组件服务控制台。

2. 扩展“组件服务”列表，选择“计算机”，然后右键单击“我的电脑”并选择“属性”。

   “我的电脑”属性窗口将打开。

3. 导航到“COM 安全”选项卡并执行以下操作：
   a. 单击“访问权限”部分中的“编辑默认值”按钮
   b. 单击“添加”，找到用户帐户，分配访问权限
   c. 在“启动和激活权限”部分中选择“编辑默认值”。
   d. 单击“添加”，找到用户帐户，分配访问权限。
   e. 在“允许”列下，选择“本地和远程访问”和“本地和远程激活”选项。
   f. 单击“确定”，退出属性窗口。
4. 依次选择“开始”、“管理工具”、“Active Directory 用户和计算机”。 请执行以下操作：
   a. 从用户列表，右键单击用户帐户。
   b. 移到“成员”选项卡，并选择“添加”到组。
   c. 作为下列组的成员添加用户，然后单击“确定”：
      - 域用户
      - 分发 COM 用户

   您已为指派用户配置安全属性。 现在为您希望此用户管理的容器配置安全属性。
5. 从 Active Directory 用户和组控制台，右键单击“用户”文件夹并选择“属性”。
6. 移到“安全”选项卡，选择“添加用户”，然后单击“高级”。

   “高级安全设置”窗口将打开。 请执行以下操作：
   a. 在“权限”选项卡中，选择用户，并单击“编辑”。

      将打开权限条目窗口。
   b. 从“应用到”列表中选择后代用户对象并应用以下权限：
      - 列出内容
      - 读取所有属性
      - 写入所有属性
      - 读取权限
      - 修改权限
      - 更改密码
      - 重置密码
   c. 单击“确定”，退出属性窗口。

   您已在用户容器中为用户配置了安全属性。

7. 从命令提示符窗口，运行命令 wmimgmt 来打开 WMI 控制台。 请执行以下操作：

   a. 右键单击“WMI 控件”，然后选择“属性”。

      将打开“WMI 控件属性”窗口。

   b. 移到“安全”选项卡并扩展根目录。

   c. 选择目录，然后单击“安全”按钮。

   d. 单击“添加”，添加正在编辑的用户帐户，然后添加针对根命名空间和子命名空间的读取安全的下列权限：

      - 部分写入
      - 提供商写入
      - 启用帐户
      - 远程启用

   e. 关闭 WMI 控制台。

8. 从命令提示符窗口，运行 regedit 实用程序并找到以下注册表项：

   HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

   HKEY_CLASSES_ROOT\CLSID\{233664b0-0367-11cf-abc4-02608c9e7553}

9. 右键单击每个注册表项，然后选择“权限”

   将打开权限窗口。

10. 将用户添加到列表中，并将完全控制分配给键和所有子对象

11. 单击“确定”以关闭 regedit 实用程序。

    您已为常规 Active Directory 用户指派管理其他常规 Active Directory 用户的权限。

连接器服务器

CA Access Control 企业管理 与连接器服务器进行通信，以便搜索和管理 PUPM 端点上的特权帐户。 CA Access Control 企业管理 使用 Java 连接器服务器 (JCS) 与 PUPM 端点的 CA Access Control 进行通信。 默认情况下，当您安装 CA Access Control 企业管理 时，JCS 是作为分发服务器的一部分而安装的。

要使用 PUPM 管理 CA Identity Manager 配给端点，您必须在 CA Access Control 企业管理 中创建 Identity Manager 配给类型连接器服务器。

注意：有关创建连接器服务器的更多信息，请参见*《联机帮助》*。

Connector Xpress 概述

Connector Xpress 是一种 CA Identity Manager 实用工具，用于管理动态连接器、将动态连接器映射到端点以及建立端点的传递规则。 您可以使用它来配置动态连接器以便配给和管理 SQL 数据库和 LDAP 目录。

通过 Connector Xpress，即使没有创建由配给管理器管理的连接器所需的专业技术，您也可以创建和部署自定义连接器。

使用 Connector Xpress，您还可以设置、编辑和删除连接器服务器配置（Java 和 C++）。

对 Connector Xpress 的主输入是端点系统的本机架构。 例如，您可以使用 Connector Xpress 连接到 RDBMS 并检索数据库的 SQL 架构。 然后，可以使用 Connector Xpress 从本机架构中与身份管理和配给相关的部分构建映射。 映射说明了配给层如何表示本机架构的元素。

注意：有关 Connector Xpress 的更多信息，请参阅 *《Connector Xpress 指南》*。

如何为 PUPM 实施 Connector Xpress

要管理非默认 PUPM 端点类型的端点，您可以使用 Connector Xpress 创建新的端点类型并管理特权帐户密码。 例如，当想管理位于 Microsoft SQL Server 数据库表的特权帐户密码时，创建类型为 SQL 的端点。 默认的 PUPM SQL 端点类型旨在管理 SQL Server 上的特权帐户，并非管理数据库中的单个表。

完成以下步骤：

1. 安装 Connector Xpress。

   注意：有关如何安装 Connector Xpress 的更多信息，请参阅 CA 支持 上 CA Identity Manager 总目录中提供的 *《Connector Xpress 指南》*。

2. 在 Connector Xpress 中配置新的端点类型。
3. 将新的端点类型注册到 Java 连接器服务器。

   注册新的端点类型以便使 Java 连接器服务器能够管理该端点类型。

4. 将新的端点类型加载到企业管理服务器。

   加载该端点类型以便使其在 CA Access Control 企业管理 中可用。

5. 在 CA Access Control 企业管理 中创建新端点类型的 PUPM 端点。
6. 在新的端点上发现特权帐户密码。

Connector Xpress 示例：配置 SUN ONE 端点

在该示例中，系统管理员 Steve 在 Connector Xpress 中创建 SUN ONE 端点类型以便连接到 SUN ONE 目录。

Steve 已经在企业管理服务器主机上安装 Connector Xpress。 Steve 执行以下操作：

1. 在“开始”菜单中依次选择“程序”、“CA”、“Identity Manager”、“Connector Xpress”。

   此时出现“Identity Manager Connector Xpress”主菜单。

2. 单击“设置数据源”。

   此时打开“设置数据源”窗口。

3. 单击“添加”。

   此时打开“源类型”窗口，显示可用的源。

4. 选择“JNDI”，然后单击“确定”。

   此时打开“编辑源”窗口。

5. 输入以下详细信息：

   - 名称－SUN ONE
   - 服务器名称－服务器 1
   - 端口－389
   - 绑定 DN－uid=user1、ou=cont1、ou=ldapConnector、dc=company、dc=com

     重要说明！ 指定现有的目录用户帐户，而不是目录管理器帐户，它不直接位于基本 DN 下。

   - 基本 DN－ou=ldapConnector、dc=company、dc=com

6. 单击“测试”来验证连接设置。

   此时打开“输入数据源的密码”窗口。

7. 输入管理员帐户密码，然后单击“确定”。

   如果没有发现任何错误，此时出现一条确认消息。 新的数据源即已创建。 Steve 现在创建新的项目。

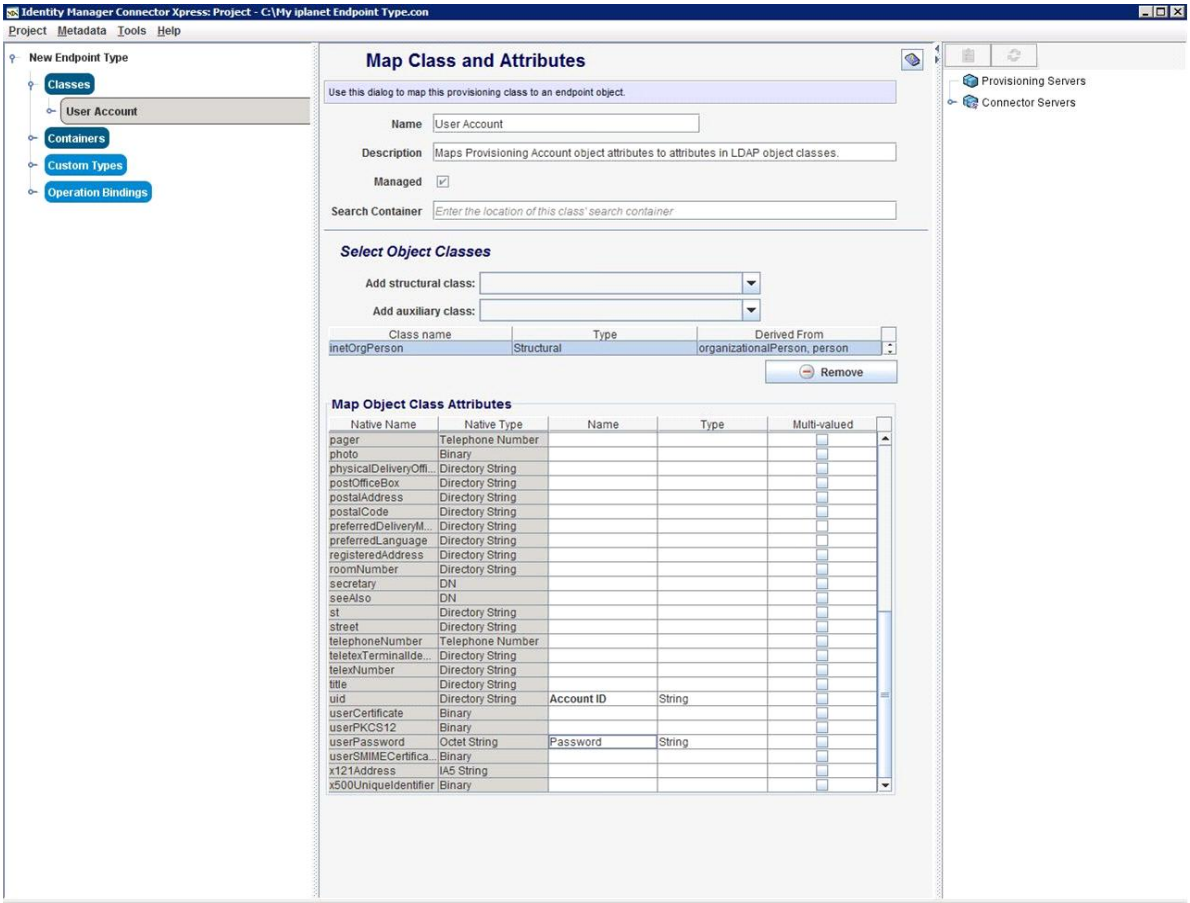
8. 依次选择“项目”、“新建”、“数据源”、“编辑”并输入管理员帐户密码。

   此时打开“端点类型详细信息”屏幕。

9. 输入端点名称和说明，双击“类”图标，然后选择“用户详细信息”选项。

   此时打开“映射类和属性”窗口。

10. 在选择对象类中，添加结构的类 inerOrgPerson，并映射以下属性：
    - cn－帐户 ID
    - sn－姓氏
    - uid－帐户 ID
    - userPassword－用户帐户密码



11. 保存项目，保存端点类型定义。

    Steve 已经在 Connector Xpress 中配置了新的 SUN ONE 端点类型。 现在，他将该端点类型注册到 Java 连接器服务器。

Connector Xpress 示例：在 Java 连接器服务器中注册 SUN One 端点类型

在该示例中，系统管理员 Steve 在 Java 连接器服务器中注册 Connector Xpress 中创建的端点类型。 他注册新的端点类型以便将其显示在 CA Access Control 企业管理 中。 Steve 执行以下操作：

1. 在“Identity Manager Connector Xpress”项目窗口中，右键单击“连接器服务器”选项并选择“添加服务器”。

   此时打开“连接器服务器详细信息”窗口。

2. 指定 Java 连接器服务器主机名，然后单击“确定”。

   注意：Java 连接器服务器属于分发服务器的一部分。 默认情况下，企业管理服务器在该服务器上安装分发服务器。 此时打开“所需的连接器服务器密码”窗口。

3. 输入企业管理服务器通信密码。

   您在安装企业管理服务器时指定了通信密码。 此时显示现有的端点类型的列表。

4. 右键单击“端点类型”，然后选择“创建新的端点类型”。

   此时打开“创建新的端点类型”窗口。

5. 输入端点类型名称，然后单击“确定”。

   如果没有发现任何错误，Connector Xpress 会创建新的端点类型。

Steve 已将新的端点注册到 Java 连接器服务器。 现在，他将新的端点类型加载到企业管理服务器。

更多信息：

Connector Xpress 示例：将端点类型加载到企业管理服务器 (p. 133)

Connector Xpress 示例：配置 JDBC 端点

在该示例中，系统管理员 Steve 在 Connector Xpress 中创建 JDBC 端点类型以便连接到 Microsoft SQL Server。

Steve 已经在企业管理服务器主机上安装 Connector Xpress。 Steve 执行以下操作：

1. 在“开始”菜单中依次选择“程序”、“CA”、“Identity Manager”、“Connector Xpress”。

   此时出现“Identity Manager Connector Xpress”主菜单。

2. 单击“设置数据源”。

   此时打开“设置数据源”窗口。

3. 单击“添加”。

   此时打开“源类型”窗口，显示可用的源。

4. 选择“JDBC”，然后单击“确定”。

   此时打开“编辑源”窗口。

5. 输入以下详细信息：

   - 数据源名称 — SQL Server
   - 数据库类型 — Microsoft SQL Server
   - 用户名 — sa
   - 服务器名称 — mysql
   - 端口 — 1433
   - 数据库 — users

6. 单击“测试”来验证连接设置。

   此时打开“输入数据源的密码”窗口。

7. 输入 sa 用户帐户密码，然后单击“确定”。

   如果没有发现任何错误，此时出现一条确认消息。 新的数据源即已创建。 现在，Steve 配置了新的端点类型。

8. 返回“Identity Manager Connector Xpress”主菜单，然后选择“新建项目”。

   此时出现“选择新项目的数据源”窗口。

9. 选择他创建的数据源，然后单击“确定”。

   此时打开“端点类型详细信息”窗口。

10. 输入端点名称和说明，双击“类”图标，然后选择“用户详细信息”选项。

    此时打开“映射类和属性”窗口。

11. 在“选择架构和表”部分中，选择以下内容：

    - 对于“架构”，选择 dbo
    - 对于“表”，选择 sqlConnector 表。

    即会显示映射的列。

12. 在“映射列”部分中，在“名称”列中输入以下值：

    - 在 uname 行中，输入帐户 ID
    - 在 upassword 行中，输入密码

13. 依次选择“项目”、“保存”保存端点类型定义。

Steve 已经在 Connector Xpress 中配置了新的 JDBC 端点类型。 现在，他将该端点类型注册到 Java 连接器服务器。

Connector Xpress 示例：在 Java 连接器服务器中注册 JDBC 端点

在该示例中，系统管理员 Steve 在 Java 连接器服务器中注册 Connector Xpress 中创建的端点类型。 他注册新的端点类型以便将其显示在 CA Access Control 企业管理 中。 Steve 执行以下操作：

1. 在“Identity Manager Connector Xpress”项目窗口中，右键单击“连接器服务器”选项并选择“添加服务器”。

   此时打开“连接器服务器详细信息”窗口。

2. 指定 Java 连接器服务器主机名，然后单击“确定”。

   注意：Java 连接器服务器属于分发服务器的一部分。 默认情况下，企业管理服务器在该服务器上安装分发服务器。 此时打开“所需的连接器服务器密码”窗口。

3. 输入企业管理服务器通信密码。

   您在安装企业管理服务器时指定了通信密码。 此时显示现有的端点类型的列表。

4. 右键单击“端点类型”，然后选择“创建新的端点类型”。

   此时打开“创建新的端点类型”窗口。

5. 输入端点类型名称，然后单击“确定”。

   如果没有发现任何错误，Connector Xpress 会创建新的端点类型。

Steve 已将新的端点注册到 Java 连接器服务器。 现在，他将新的端点类型加载到企业管理服务器。

Connector Xpress 示例：将端点类型加载到企业管理服务器

在该示例中，系统管理员 Steve 将已创建的新端点类型加载到企业管理服务器。 在 Steve 加载新的端点类型之后，他就能够从 CA Access Control 企业管理 配置和管理该端点。 Steve 执行以下操作：

1. 停止 JBoss 应用程序服务器。
2. 请执行下列操作之一：
   - (JDBC) 编辑文件 conXpressnamespace_config.xml.template。
   - (SUN One) 编辑 iplanetnamespace_config.xml

   该文件位于以下目录，其中 *JBoss_HOME* 表示 JBoss 的安装目录：

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/custom/ppm/namespaceConfigs/
3. 找到 <endpointType> 参数，然后删除默认值：'REPLACE_WITH_ENDPOINT_TYPE'。
4. 输入 Connector Xpress 中所指定的端点类型名称。
5. 在下列的目录中，在名称 conXpress_*Endpoint_Type*_namespace_config.xml 下保存文件：

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/custom/ppm/namespaceConfigs/
6. 启动 JBoss 应用程序服务器。

Steve 将新的端点类型加载到企业管理服务器。 现在，他可以在 CA Access Control 企业管理 中定义该类型的端点，并在该端点上发现特权帐户。

Connector Xpress 限制

当在 Connector Xpress 中创建的端点类型上运行"发现特权帐户"向导之前，您应当考虑以下内容：

- 定义与您在 Connector Xpress 中创建的类型相同的端点（例如，SQL Server 端点）并提供端点管理员帐户凭据。 当 CA Access Control 企业管理 创建端点时，也创建断开连接的特权帐户。
- 在端点类型菜单中指定您在 Connector Xpress 中创建的端点类型。 在 URL 字段中指定数据库名称，如下例所示。
- 将"用户登录"和"密码"字段留空。 选中"使用以下特权帐户"并选择具有权限的特权帐户连接到端点。 使用 CA Access Control 企业管理 为您先前定义的端点创建的断开连接的特权帐户。

示例：端点 URL 字段中的 SQL Server 数据库名称

下列示例向您显示包含 SQL Server 数据库名称的 URL 域：

```
jdbc:sqlserver://server.company.com:1433;database=database_name
```

PUPM SDK

通过 PUPM SDK，您可以编写签出和签入特权帐户密码的应用程序。 有两种类型的 PUPM SDK：密码使用方 SDK 和 Web 服务 SDK。

下表概述两种类型的 SDK 之间的差异：

功能	密码使用方 SDK	Web 服务 SDK
编程语言	Java .NET	Java
用户身份验证	是	否
密码缓存	是	否
在端点上需要 CA Access Control	是	否

使用案例：PUPM SDK

通过 PUPM SDK，您可以在脚本中自动化对特权帐户密码的管理。 如果不想修改包含硬编码密码的脚本，您可以编写定期替换脚本中的密码的应用程序。

例如，您在端点上有十个脚本包含相同特权帐户的硬编码密码。 您不想修改这些脚本。 您可以使用 PUPM SDK 编写应用程序，该应用程序在适当的停机时间签出特权帐户密码，在每个脚本中更新密码，然后签入该密码。 定期更改密码可帮助提高特权帐户的安全性。

如果您创建应用程序来执行该任务，请确认 CA Access Control 企业管理在签出或签入时没有更改特权帐户密码。 您可以使用“查看特权帐户”任务来验证该信息。

注意：您也可以使用 CLI 密码使用方来替换脚本中的硬编码密码。 例如，如果您想手工更新文件中的硬编码密码，则使用 CLI 密码使用方。

密码使用方 SDK 应用程序获取密码的方式

通过密码使用方 SDK，您可以编写获取、签入和签出特权帐户密码的应用程序。 要使用密码使用方 SDK，您必须执行以下操作：

- 在应用程序运行的端点上安装 CA Access Control
- 在 CA Access Control 企业管理 中定义该应用程序的密码使用方

有两种类型的密码使用方 SDK：

- Java PUPM SDK
- .NET PUPM SDK

密码使用方 SDK 应用程序与 PUPM 代理进行通信，然后该代理使用消息队列与 CA Access Control 企业管理 通信。 PUPM 代理使用 SSL 通信和端口 7243 与消息队列进行通信。

以下过程说明了密码使用方 SDK 应用程序获取密码的方式：

1. 应用程序将密码请求发送到 PUPM 代理。
2. PUPM 代理接收密码请求。 CA Access Control 验证运行该应用程序的用户的身份，并且检查缓存。 会出现以下情况之一：
   - 如果密码请求已缓存，PUPM 代理会将特权帐户密码发送给该应用程序。 该过程在此步骤完成。 CA Access Control 企业管理 不写入密码请求的审核记录。
   - 如果密码请求没有缓存，PUPM 代理会将密码请求和运行该应用程序的用户的名称发送到 CA Access Control 企业管理。
3. CA Access Control 企业管理 接收请求，并检查是否存在授权该应用程序获得特权帐户密码的密码使用方。

   密码使用方指定应用程序的路径、该应用程序可以请求的特权帐户、可以运行该应用程序的用户以及可以运行该应用程序的主机。

4. 会出现以下情况之一：
   - 如果该应用程序有权获取密码，CA Access Control 企业管理 会将特权帐户密码发送到 PUPM 代理。
   - 如果该应用程序无权获得密码，CA Access Control 企业管理 会将错误消息发送到 PUPM 代理。

   在这两种情况下，CA Access Control 企业管理 都会写入事件的审核记录。
5. PUPM 代理将特权帐户密码或错误消息发送到应用程序。

   如果应用程序在首次已经获得特权帐户密码，PUPM 代理会缓存该密码。

注意：当特权帐户的密码更改时，CA Access Control 企业管理 将密码更改事件广播到各个端点。 当端点接收广播信息时，PUPM 代理会从缓存中删除特权帐户密码。

更多信息：

如何配置端点以便使用密码使用方 SDK 应用程序 (p. 226)

Java PUPM SDK

Java PUPM SDK 是一种密码使用方 SDK，让您可以编写获取、签出和签入特权帐户密码的 Java 应用程序。 您可以在安装 CA Access Control 的 Windows 和 UNIX 端点上使用 Java PUPM SDK。 您编写的 Java 应用程序必须使用 JRE 1.5 或更高版本。

Java PUPM SDK 位于以下目录：

ACInstallDir/SDK/JAVA

该目录包含以下文件：

- PupmJavaSDK.jar — 包括在您的 Java 应用程序中的 SDK 库。
- CAPUPMCLientCommons.jar — 当运行应用程序时，必须包括在类路径中的支持库。
- jsafeFIPS.jar — 当运行应用程序时，必须包括在类路径中的支持库。

- CAPUPM.properties.SAMPLE — 您可以编辑用来更改默认应用程序属性的示例文件。

  如果编辑该文件，您必须命名新文件 CAPUPM.properties，并在运行应用程序时将文件名包括在类路径中。

  注意：建议在您修改该文件前先联系 CA Support。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

- Samples — 一个文件夹，包含签出和签入特权帐户密码的示例 Java 应用程序。

如果想要应用程序记录运行时事件和信息，您还必须在类路径中包括 log4j 库。 您必须在 CA Access Control 企业管理 中创建该应用程序的“软件开发工具包 (SDK/CLI)”密码使用方，然后该应用程序才能获取、签出和签入特权帐户密码。

更多信息：

如何配置端点以便使用密码使用方 SDK 应用程序 (p. 226)

.NET PUPM SDK

在 Windows 上有效

.NET PUPM SDK 是一种密码使用方 SDK，让您可以编写获取、签出和签入特权帐户密码的 C# 应用程序。 尽管您可以获取、签出和签入驻留在任何操作系统上的特权帐户密码，但是您仅可以在安装 CA Access Control 的 Windows 端点上使用 .NET PUPM SDK。 您必须在端点上安装 .NET Framework 2.0 或更高版本才能使用 .NET PUPM SDK。

.NET PUPM SDK 位于以下目录：

ACInstallDir\SDK\DOTNET

该目录包含以下文件：

- Pupmcsharpsdk.dll — 包括在您的 C# 应用程序中的 SDK 库。
- Examples — 一个文件夹，包含签出和签入特权帐户密码的示例应用程序。

  每个示例应用程序都包含未编译的示例（.cs 文件）和编译的示例（.exe 文件）。

您必须在 CA Access Control 企业管理 中创建该应用程序的“软件开发工具包 (SDK/CLI)”密码使用方，然后该应用程序才能获取、签出和签入特权帐户密码。

更多信息：

如何配置端点以便使用密码使用方 SDK 应用程序 (p. 226)

Web 服务 PUPM SDK

通过 Web 服务 PUPM SDK，您可以编写签入和签出特权帐户密码的 Java 应用程序。 您可以在未安装 CA Access Control 的端点上（例如，在大型机端点上）使用 Web 服务 PUPM SDK。

在您可以使用 Web 服务 PUPM SDK 应用程序签出或签入特权帐户密码之前，您必须创建一个用户代表 CA Access Control 企业管理 中的应用程序，并为该用户分配适当的特权访问角色。

您必须在端点上安装以下组件才能使用 Web 服务 PUPM SDK：

- Apache Ant 1.7
- Apache Axis 1.4
- Java SDK 1.4.2
- （可选）集成开发环境 (IDE)，例如 Eclipse

Web 服务 PUPM SDK 位于以下目录：

ACServerInstallDir/IAM Suite/Access Control/tools/samples/webservice/Axis

该目录包含 Web 服务 PUPM SDK 的以下组件：

- Readme.txt — 包含有关如何配置环境、生成 Java 示例和运行 Java 示例的说明的文件。
- build.xml — Apache Ant 构建脚本，
- build.properties — 在 build.xml 中设置属性的文件。
- CheckInPrivilegedAccount.java — 签入特权帐户密码的示例 Java 应用程序。
- CheckOutPrivilegedAccount.java — 签出特权帐户密码的示例 Java 应用程序。
- client-config.wsdd — 一个文件，配置 Axis 将所有传入和传出的 XML 消息保存在名为 axis.log 的文件。

  注意：该目录还包含让您可以执行其他管理任务（例如，创建或删除特权帐户）的示例 Java 应用程序。

更多信息：

如何配置端点以便使用 Web 服务 PUPM SDK 应用程序 (p. 228)

Web 服务 SDK 应用程序获取密码的方式

通过 Web 服务 PUPM SDK，您可以编写签入和签出特权帐户密码的 Java 应用程序。 您不需要在 Web 服务 PUPM SDK 应用程序运行的端点上安装 CA Access Control。 但是，与密码使用方 SDK 不同，Web 服务 PUPM SDK 不缓存密码或验证用户。

Web 服务 PUPM SDK 应用程序使用 SOAP（简单对象访问协议）和端口 18080 直接与企业管理服务器进行通信。

重要说明！ 建议您使用加强的身份验证协议（如 NTLM）来验证应用程序和企业管理服务器之间的连接。

以下过程说明了 Web 服务 PUPM SDK 应用程序获取密码的方式：

1. 该应用程序登录到 CA Access Control 企业管理。

   应用程序登录时使用的用户名和密码在应用程序中有所定义。
2. 该应用程序请求特权帐户的密码。
3. CA Access Control 企业管理 会检查分配给代表该应用程序的用户的特权访问角色。
4. 会出现以下情况之一：
   - 如果具有该特权访问角色的用户可以获得特权帐户密码，CA Access Control 企业管理 将密码发送给该应用程序。
   - 如果具有该特权访问角色的用户不能获得特权帐户密码，CA Access Control 企业管理 将错误消息发送给该应用程序。
5. 应用程序从 CA Access Control 企业管理 中注销。

更多信息：

如何配置端点以便使用 Web 服务 PUPM SDK 应用程序 (p. 228)

第 6 章： 实施特权帐户

此部分包含以下主题：

如何设置特权帐户

特权用户密码管理 (PUPM) 是一个流程，组织可通过该流程保护、管理和跟踪与组织中权限最高的帐户相关的所有活动。 在开始使用特权帐户密码之前，您需要完成几个步骤来为 PUPM 设置 CA Access Control 企业管理。 用户随后即可开始使用您定义的特权帐户。

以下过程说明企业中的用户为设置特权帐户而必须完成的任务。 用户必须具有指定角色才能完成流程的每个步骤。 具有“系统管理员”管理角色的用户可以执行此流程中的每个 CA Access Control 企业管理 任务。

注意：在开始该流程之前，请确认已在 CA Access Control 企业管理 中启用了电子邮件通知。 如果 CA Access Control 企业管理 无法为用户显示密码，它会将密码通过电子邮件发送给用户。

要设置特权帐户，用户需执行以下操作：

1. PUPM 目标系统管理员创建密码策略。 密码策略为特权帐户设置密码规则和限制。
2. PUPM 目标系统管理员在 CA Access Control 企业管理 中创建端点。 端点是由特权帐户管理的设备。 您可以在 CA Access Control 企业管理 中创建端点，或使用 PUPM 导送程序来导入端点。
3. PUPM 目标系统管理员为每个端点创建特权帐户。 通过创建特权帐户 CA Access Control 企业管理 可以管理这些帐户。 您可以在 CA Access Control 企业管理 中创建特权帐户，或使用 PUPM 导送程序来导入特权帐户。
4. （可选）系统管理员创建登录应用程序，PUPM 目标系统管理员修改 PUPM 端点以使用此登录应用程序。 登录应用程序允许用户从 CA Access Control 企业管理 登录到特权帐户。

5. PUPM 策略管理员修改特权访问角色的成员策略。 成员策略定义了可以执行某一角色的任务的用户。

   注意：如果使用 Active Directory 作为用户存储，建议您修改每个成员策略，使其与相应的 Active Directory 组对应。 随后可以通过从相应的 Active Directory 组添加或删除用户，在角色中添加或删除用户。 这会降低管理开销。

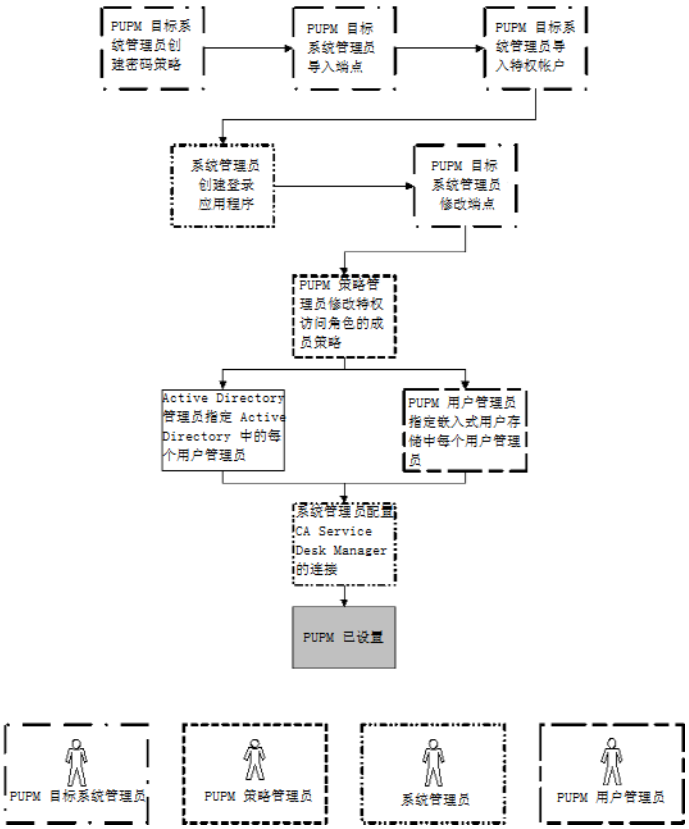
6. （嵌入式用户存储）PUPM 用户管理员为每个用户指定了管理员。

   注意：只有管理员才能批准用户提出的特权帐户请求。 如果使用 Active Directory 作为用户存储，请确认已在 Active Directory 中指定了每名用户的管理员。

7. （可选）系统管理员配置到 CA Service Desk Manager 的连接。

   与 CA Service Desk Manager 相集成您可为特权帐户请求创建多个审批流程。

下图说明执行每个流程步骤的特权访问角色：



发现特权帐户

建议您按固定时间间隔运行特权帐户发现过程，以扫描端点上的新特权帐户。 通过发现特权帐户过程您可以同时创建多个特权帐户。 CA Access Control 企业管理 会将所发现的帐户显示在一个表中，这样您便可以轻易识别您已用 PUPM 管理的那些帐户。

第一次在某端点类型上发现特权帐户时，CA Access Control 企业管理 会自动创建一个端点特权访问角色，以便在该端点类型上使用特权帐户。例如：您第一次在 Windows Agentless 端点上发现特权帐户时，CA Access Control 企业管理 会自动创建 Windows Agentless 连接端点特权访问角色。

发现特权帐户

1. 在 CA Access Control 企业管理 中，依次单击“特权帐户”、“帐户”、“发现特权帐户向导”。

   此时出现“发现特权帐户向导: 选择特权帐户”页面。

2. 从列表中选择“端点类型”。

3. 选择要搜索的属性，键入筛选值，然后单击“搜索”。

   此时将显示匹配筛选条件的端点的列表。

4. 选择要管理的特权帐户。

   下表列标题需加以说明：

   发现的帐户

   指定帐户是否已为 CA Access Control 企业管理 所知。已知帐户包括 CA Access Control 企业管理 已经管理的帐户，以及 CA Access Control 企业管理 用来管理端点的管理员帐户。

   是端点管理员

   指定 CA Access Control 企业管理 是否使用此帐户来管理端点。

   重要说明！ 在选择端点管理员帐户时要慎重。 CA Access Control 企业管理 可以自动更改其管理的特权帐户的密码。 如果选择端点管理员帐户，您可能无法登录到端点上的特权帐户，也无法对其进行管理。

   单击“下一步”。

   此时出现“发现特权帐户向导: 常规帐户详细信息”页面。

5. 填充该对话框中的字段。 以下字段需加以说明：

断开系统

指定帐户是否起源于断开的系统。

如果选择该选项，PUPM 不管理帐户， 而会仅充当断开系统的特权帐户的密码存储库。每次更改密码时，还需要在受管端点上手动更改帐户密码。

密码策略

指定要应用于特权帐户或服务帐户的密码策略。

签出到期

定义签出帐号到期之前的持续时间（分钟）。

独占帐户

指定是否任何时候只有单个用户可以使用该帐户。*独占帐户*是对特权帐户施加的限制，限制每次只允许单个用户使用该帐户。

签出时更改密码

指定是否要 CA Access Control 企业管理 在每次签出特权帐户时更改其密码。

注意：该选项不适用于服务帐户。

签入时更改密码

指定是否要 CA Access Control 企业管理 在每次用户或程序签入特权帐户时，或签出周期到期时更改特权帐户的密码。

注意：如果帐户不是独占帐户，则仅在*所有*用户都已签入该帐户时 CA Access Control 企业管理 才生成新的特权帐户密码。

注意：该选项不适用于服务帐户。

服务帐户

指定发现的帐户是否是服务帐户。

注意：您也可以使用“发现服务帐户向导”来发现服务帐户。

单击“完成”。

如果没有错误，CA Access Control 企业管理 会提交任务并创建选定的特权帐户。

更多信息：

发现服务帐户 (p. 197)

创建特权或服务帐户

可创建特权帐户和服务帐户来在受管和断开的系统上管理帐户密码。可以将特权帐户和服务帐户用于以下几个不同用途：

- 要允许用户签出和签入特权帐户密码，请创建特权帐户。
- 要设置 CLI、数据库或 Windows RunAs 密码使用方，需创建特权帐户。
- 要设置 Windows 服务和 Windows 排定任务密码使用方，需创建服务帐户。

  注意：不能签出和签入服务帐户密码。

要创建多个帐户，请使用发现特权帐户向导和发现服务帐户向导在端点上搜索特权帐户和服务帐户。 要创建一个帐户，请在该窗口中提供特权帐户详细信息或服务帐户详细信息。

请按下列步骤操作：

1. 在 CA Access Control 企业管理 中，依次单击“特权帐户”、“帐户”、“创建特权帐户”。

   此时出现“创建特权帐户: 选择特权帐户”页面。

2. （可选）按如下方式选择一个现有特权帐户来创建特权帐户作为其副本：

   a. 选择“创建类型为‘特权帐户’的对象副本”。

   b. 针对搜索选择属性，键入筛选器值，然后单击“搜索”。

      此时将显示匹配筛选条件的特权帐户的列表。

   c. 选择要用作新特权帐户基础的对象。

3. 单击“确定”。

   此时出现“创建特权帐户”任务页面的“常规”选项卡。 如果特权帐户是从现有对象创建的，则对话框字段中会预先填充来自现有对象的值。

4. 填写“常规”选项卡中的以下字段：

   帐户名称

   定义要用来指代此特权帐户的名称。

   注意：大型机系统（例如 RACF、ACF 和 Top Secret）使用的用户名区分大小写。 以大写字母输入帐户名称。

断开帐户

指定帐户是否起源于断开的系统。

如果选择该选项，PUPM 不管理帐户， 而会仅充当断开系统的特权帐户的密码存储库。每次更改密码时，还需要在受管端点上手动更改帐户密码。

帐户类型

指定帐户是共享（特权）帐户还是服务帐户。

注意：在创建服务帐户时，PUPM 不会尝试更改帐户密码。

端点名称

指定特权帐户或服务帐户所在的已定义端点的名称。 CA Access Control 企业管理 仅列出属于您指定类型的端点。

端点类型

指定特权帐户或服务帐户所在的端点的类型。

容器

指定特权帐户或服务帐户的容器的名称。 *容器*是一个类，其实例是其他对象的集合。容器采用一种遵循特定访问规则的有组织的方式来存储对象。

密码策略

指定要应用于特权帐户或服务帐户的密码策略。

密码

定义要用于新特权帐户的密码。

注意：新密码必须遵守指定的密码策略。

签出到期

定义签出帐号到期之前的持续时间（分钟）。

独占帐户

指定是否任何时候只有单个用户可以使用该帐户。*独占帐户*是对特权帐户施加的限制，限制每次只允许单个用户使用该帐户。

签出时更改密码

指定是否要 CA Access Control 企业管理 在每次签出特权帐户时更改其密码。

注意：该选项不适用于服务帐户。

签入时更改密码

指定是否要 CA Access Control 企业管理 在每次用户或程序签入特权帐户时，或签出周期到期时更改特权帐户的密码。

注意：如果帐户不是独占帐户，则仅在*所有*用户都已签入该帐户时 CA Access Control 企业管理 才生成新的特权帐户密码。

注意：该选项不适用于服务帐户。

仅登录应用程序签出

指定是否仅在为端点定义了登录应用程序时才允许密码签出。

注意：在启用了该选项时，用户无法显示密码，也无法将密码复制到剪贴板。

5. （可选）移到“密码使用方”选项卡。

如果配置，CA Access Control 企业管理 则显示使用特权帐户的密码使用者。

6. （可选）单击“信息”选项卡，并填写该选项卡中的字段。

您可以在该选项卡中指定端点特有的属性，并在定义或修改特权访问角色时使用这些属性。

当访问特权角色的成员登录 CA Access Control 企业管理 时，用户根据在特权访问角色中定义的属性获取对特权访问帐户的访问权限。

所有者

指定端点所有者的名称。

部门

指定部门名称。

示例：开发部

自定义 1...5

指定最多五个自定义的端点特定属性。

注意：在特权访问角色的“成员”选项卡“成员策略”部分的“成员规则”窗口中，指定自定义属性。

7. 单击“提交”。

CA Access Control 企业管理 会创建新的特权帐户或服务帐户。

创建密码策略

特权帐户的密码策略是一组规则和限制，这些规则和限制决定了允许的特权帐户密码。 例如：您可以配置策略，要求密码的长度至少有八个字符，并且包含一个数字和字母。 密码策略也决定了 CA Access Control 企业管理 自动创建新帐户密码的时间间隔。

注意：CA Access Control 企业管理 附带了一个您可以使用的预定义密码策略。 建议您定义适合于每个端点且符合安全要求的密码策略。

要创建密码策略，

1. 在 CA Access Control 企业管理 中，依次单击“特权帐户”、“密码策略”、“创建密码策略”。

   此时出现“创建密码策略: 配置标准搜索屏幕”页面。

2. （可选）按如下方式选择一个现有密码策略来创建密码策略作为其副本：

   a. 选择“创建类型为‘特权帐户密码策略’的对象副本”，并单击“搜索”。

      此时出现密码策略的列表。

   b. 选择要用作新密码策略基础的对象。

3. 单击“确定”。

   此时出现“创建密码策略”任务页面。 如果密码策略是从现有对象创建的，则对话框字段中会预先填充来自现有对象的值。

4. 为密码策略键入一个名称和可选说明。

5. （可选）清除“已启用”。

   默认情况下，新密码策略处于启用状态。 如果您在创建的策略尚未得到批准，可以选择清除该复选框让策略处于禁用状态。

6. 定义密码组成规则。

7. （可选）定义密码到期时间间隔。

   这是一个固定时间间隔，CA Access Control 企业管理 会按此时间间隔自动更改密码。 默认情况下，到期时间间隔处于禁用状态（设置为零）。

8. （可选）以 24 小时时间格式定义时间，CA Access Control 企业管理可以按此时间更改密码。

   例如：如果为服务帐户创建一个密码策略，则可以指定 CA Access Control 企业管理 只能在周日晚上 10:00 到 11:59 之间 (22:00–23:59) 更改帐户密码。

9. 单击“提交”。

   CA Access Control 企业管理 会创建密码策略。

更多信息：

密码组成规则 (p. 149)

密码组成规则

在创建密码策略时，可以定义对新密码的内容要求。

重要说明！ 在配置密码组成规则时，设置要求时需要考虑最大密码长度。 如果所需字符的总数超过最大密码长度，则会拒绝所有密码。

CA Access Control 企业管理 为特权帐户提供了以下密码组成规则：

最小密码长度

定义密码必须包含的最少字符数。

最大密码长度

定义密码可以包含的最多字符数。

最多重复字符

定义密码可以包含的重复字符的最多数目。

例如：如果将该值设置为 3，密码中不能出现字符串“aaa”，但可以出现“aa”。

大写字母（模式为 u）

指定密码是否可以包含大写字母，如果可以包含，定义密码必须包含的大写字母的最少数目。

小写字母（模式为 c）

指定密码是否可以包含小写字母，如果可以包含，定义密码必须包含的小写字母的最少数目。

字母（模式为 l）

指定密码是否可以包含字母字符，如果可以包含，定义密码必须包含的字母字符的最少数目。

数字（模式为 d）

指定密码是否可以包含数字，如果可以包含，定义密码必须包含的数字的最少数目。

字母或数字（模式为 a）

指定密码是否可以包含字母数字字符，如果可以包含，定义密码必须包含的字母数字字符的最少数目。

标点（模式为 P）

指定密码是否可以包含标点或特殊字符（非字母数字字符），如果可以包含，定义密码必须包含的标点或特殊字符的最少数目。

任何（模式为 *）

指定密码可以包含任何字符。 如果选择该选项，CA Access Control 企业管理 会自动选择所有其他字符内容定义。

使用模式

指定由您定义密码必须使用的模式，而不是定义字符内容定义。

示例：

- **uuuuu**—匹配 ASDKF 或 IUTYE
- **ucdddp**—匹配 Rv671* 或 Uc194^
- **********—匹配 lkI&5Jj@ 或 sffIU*&1
- **llllaaaa**—匹配 yuUI1Uo3 或 qWcV1Er6

禁用字符

定义在创建或修改特权帐户密码时不能使用的字符。

PUPM 端点和特权帐户的创建

下列主题说明了如何创建端点、创建和发现特权帐户以及在 CA Access Control 企业管理 中创建登录应用程序。

如果您想创建或修改多个 PUPM 端点或特权帐户，请考虑使用 PUPM 导送程序。 通过 PUPM 导送程序，您可以在单个步骤中导入许多端点或特权帐户，并可以自动化 PUPM 端点和特权帐户的管理。

创建端点

通过在 CA Access Control 企业管理 中创建端点定义您可以管理端点并发现该端点上的特权帐户和服务帐户。

请按下列步骤操作：

1. 在 CA Access Control 企业管理 中，依次单击“特权帐户”、“端点”、“创建端点”。

   此时出现“创建端点: 选择端点”页面。

2. （可选）按如下方式选择一个现有端点来创建端点作为其副本：

   a. 选择“创建类型为‘端点’的对象副本”。

   b. 针对搜索选择属性，键入筛选器值，然后单击“搜索”。

      此时将显示匹配筛选条件的端点的列表。

   c. 选择要用作新端点基础的对象。

3. 单击“确定”。

   此时出现“创建端点”任务页面的“常规”选项卡。 如果端点是从现有对象创建的，则对话框字段中会预先填充来自现有对象的值。

4. 填充该选项卡中的字段。 以下字段没有自带说明：

   名称

   定义端点的逻辑名称。

   注意：该字段定义了端点的名称在 CA Access Control 企业管理 中的显示方式。 可在选择端点类型时指定连接信息。

   说明

   （可选）定义要为该端点记录的信息（自由文本）。

   端点类型

   指定特权帐户或服务帐户所在的端点的类型。

   注意：在选择端点类型时，会有其他打开的对话框要求您提供凭据，PUPM 需要这些凭据来管理该端点类型上的特权帐户。 您选择的端点类型会影响您必须提供的连接信息。

5. （可选）单击“登录应用程序”选项卡并填写该选项卡中的字段。

   登录应用程序

   指定要分配给该端点的登录应用程序。

   注意：需要先创建一个登录应用程序，之后才能将其分配给端点。 您可以为同一端点分配多个登录应用程序。

6. （可选）单击“CA Enterprise Log Manager”选项卡，并填写该选项卡中的字段。

   使用该选项卡您可以在 CA Access Control 企业管理 中查看 PUPM 端点上的特权帐户审核事件的 CA Enterprise Log Manager 报告。 如果尚未配置到 CA Enterprise Log Manager 的连接，则不会出现此选项卡。

   主机名

   按 CA Enterprise Log Manager 中的说明定义主机名。

   如果没有在该字段中键入值，CA Access Control 企业管理 会使用您在“常规”选项卡的“名称”字段中指定的主机名。

   事件日志名称

   按 CA Enterprise Log Manager 中的说明定义事件日志名称。例如：Windows Agentless 端点的事件日志名称可能是 NT-Security。

   如果没有在该字段中键入值，在 CA Access Control 企业管理 中查看特权帐户审核事件报告时，会显示所有端点类型的审核事件。

   注意：有关事件日志名称的更多信息，请参阅 CA Enterprise Log Manager 文档。

7. （可选）单击“信息”选项卡，并填写该选项卡中的字段。

   您可以在该选项卡中指定端点特有的属性，并在定义或修改特权访问角色时使用这些属性。

   当访问特权角色的成员登录 CA Access Control 企业管理 时，用户根据在特权访问角色中定义的属性获取对特权访问帐户的访问权限。

   所有者

   指定端点所有者的名称。

   部门

   指定部门名称。

   示例：开发部

   自定义 1...5

   指定最多五个自定义的端点特定属性。

   注意：在特权访问角色的“成员”选项卡“成员策略”部分的“成员规则”窗口中，指定自定义属性。

8. 单击“提交”。

   CA Access Control 企业管理 尝试使用您提供的凭据连接到端点。 如果连接成功，则会创建端点。 否则，您会收到一条连接错误消息。

相关主题：

PUPM 访问控制的连接信息 (p. 153)
MS SQL Server 连接信息 (p. 155)
Oracle Server 连接信息 (p. 156)
VMware ESX/ESXi 连接信息 (p. 160)
Windows Agentless 连接信息 (p. 160)
SSH 设备连接信息 (p. 168)
SAP R3 连接信息 (p. 175)
CA Identity Manager 配给连接信息 (p. 176)
断开端点的连接信息 (p. 179)
创建登录应用程序 (p. 179)

PUPM 访问控制的连接信息

PUPM 端点类型的访问控制允许您管理特权访问控制帐户。

当您创建此类端点时，请提供以下信息，以使 CA Access Control 企业管理 可以连接到端点：

用户登录

定义该端点的管理用户的名称。PUPM 使用该帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。

注意：如果您指定“高级”选项，PUPM 不使用“用户登录”帐户来执行管理任务。相反，PUPM 使用指定的特权帐户在端点上执行管理任务。

密码

定义该端点的管理用户的密码。

主机

定义该端点的主机名。

主机域

指定该主机所属的域的名称。

示例：Domain.com

高级

指定是否要使用特权管理帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。 例如：您可以指定一个可以在多个端点上执行管理任务的特权域帐户。

如果指定该选项，PUPM 不使用“用户登录”帐户来执行管理任务。

IBM AS/400 连接信息

IBM AS/400 端点类型允许您管理特权 IBM AS/400 受管帐户。

您为 IBM AS/400 端点指定的管理用户必须有以下特权：

- 查看其他用户帐户
- 查看自己的用户帐户
- 查看其他用户帐户密码

当您创建此类端点时，请提供以下信息，以使 CA Access Control 企业管理 可以连接到端点：

名称

指定端点的名称

重要说明！ 端点名称必须与主机名匹配

用户登录

定义该端点的管理用户的名称。PUPM 使用该帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。

注意：如果您指定“高级”选项，PUPM 不使用“用户登录”帐户来执行管理任务。 相反，PUPM 使用指定的特权帐户在端点上执行管理任务。

密码

定义该端点的管理用户的密码。

主机

定义该端点的主机名。

注意：如果 CA Access Control 安装在端点上，建议您指定该属性的 CA Access Control 主机名。 您可以使用“全局查看”来查看端点的 CA Access Control 主机名。

重要说明！ 主机名必须与端点名称匹配

高级

指定是否要使用特权管理帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。 例如：您可以指定一个可以在多个端点上执行管理任务的特权域帐户。

如果指定该选项，PUPM 不使用“用户登录”帐户来执行管理任务。

MS SQL Server 连接信息

MS SQL Server 终端类型允许您管理特权 Microsoft SQL Server 帐户。

您为 MS SQL Server 端点指定的管理用户必须满足以下条件：

- 具有 securityadmin 服务器角色

注意：具有 securityadmin 服务器角色的用户无法修改 serveradmin 和 sysadmin 服务器角色。

当您创建此类端点时，请提供以下信息，以使 CA Access Control 企业管理 可以连接到端点：

用户登录

定义该端点的管理用户的名称。PUPM 使用该帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。

注意：如果您指定“高级”选项，PUPM 不使用“用户登录”帐户来执行管理任务。相反，PUPM 使用指定的特权帐户在端点上执行管理任务。

密码

定义该端点的管理用户的密码。

URL

定义 CA Access Control 企业管理 可以用来连接到端点的 URL。URL 指定数据库服务器的特定类型。

格式：jdbc:sqlserver://*servername*:*port*

示例：jdbc:sqlserver://localhost:1433

注意：有关 URL 的格式的更多信息，请参阅您的端点文档。

主机

定义该端点的主机名。

注意：如果 CA Access Control 安装在端点上，建议您指定该属性的 CA Access Control 主机名。 您可以使用“全局查看”来查看端点的 CA Access Control 主机名。

端口

（可选）指定服务器侦听端口号。 指定的端口号必须与您在 URL 中指定的端口号匹配。

示例： 1433

实例名称

（可选）指定数据库实例名称。

高级

指定是否要使用特权管理帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。 例如：您可以指定一个可以在多个端点上执行管理任务的特权域帐户。

如果指定该选项，PUPM 不使用“用户登录”帐户来执行管理任务。

Oracle Server 连接信息

Oracle Server 端点类型允许您管理特权 Oracle 数据库帐户。

您为 Oracle Server 端点指定的管理用户必须具有 ALTER USER 和 SELECT ANY DIRECTORY 系统权限。

当您创建此类端点时，请提供以下信息，以使 CA Access Control 企业管理 可以连接到端点：

用户登录

定义该端点的管理用户的名称。PUPM 使用该帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。

注意： 如果您指定“高级”选项，PUPM 不使用“用户登录”帐户来执行管理任务。相反，PUPM 使用指定的特权帐户在端点上执行管理任务。

密码

定义该端点的管理用户的密码。

URL

定义 CA Access Control 企业管理 可以用来连接到端点的 URL。URL 指定数据库服务器的特定类型。

格式： jdbc:oracle:*drivertype*:@*hostname*:*port*:*service*

示例： jdbc:oracle:thin:@ora.comp.com:1521:orcl

注意： 有关 URL 的格式的更多信息，请参阅您的端点文档。

主机

定义该端点的主机名。 这是完全限定主机名。

注意：如果 CA Access Control 安装在端点上，建议您指定该属性的 CA Access Control 主机名。 您可以使用“全局查看”来查看端点的 CA Access Control 主机名。

高级

指定是否要使用特权管理帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。 例如：您可以指定一个可以在多个端点上执行管理任务的特权域帐户。

如果指定该选项，PUPM 不使用“用户登录”帐户来执行管理任务。

Sybase Server 连接信息

Sybase Server 端点类型允许您管理特权 Sybase Server 帐户。

重要说明！ 请验证已正确配置了数据库且端口 2638 已开放用于连接。

当您创建此类端点时，请提供以下信息，以使 CA Access Control 企业管理 可以连接到端点：

用户登录

定义该端点的管理用户的名称。PUPM 使用该帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。

注意：如果您指定“高级”选项，PUPM 不使用“用户登录”帐户来执行管理任务。 相反，PUPM 使用指定的特权帐户在端点上执行管理任务。

密码

定义该端点的管理用户的密码。

URL

定义 CA Access Control 企业管理 可以用来连接到端点的 URL。URL 指定数据库服务器的特定类型。

格式：jdbc:sybase:Tds:*servername*:*port*

示例：jdbc:sybase:Tds:localhost:2638

注意：有关 URL 的格式的更多信息，请参阅您的端点文档。

主机

定义该端点的主机名。

注意：如果 CA Access Control 安装在端点上，建议您指定该属性的 CA Access Control 主机名。 您可以使用“全局查看”来查看端点的 CA Access Control 主机名。

高级

指定是否要使用特权管理帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。 例如：您可以指定一个可以在多个端点上执行管理任务的特权域帐户。

如果指定该选项，PUPM 不使用“用户登录”帐户来执行管理任务。

RACF 连接信息

RACF 类型允许您管理特权 RACF 帐户。

当您创建此类端点时，请提供以下信息，以使 [assign the value for eACVPM in your book] 可以连接到端点：

用户登录

定义该端点的管理用户的名称。PUPM 使用该帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。

注意：如果您指定“高级”选项，PUPM 不使用“用户登录”帐户来执行管理任务。相反，PUPM 使用指定的特权帐户在端点上执行管理任务。

示例：*cn=user1,host=RACF,o=company,c=com*

密码

定义该端点的管理用户的密码。

主机

定义该端点的主机名。

注意：如果 CA Access Control 安装在端点上，建议您指定该属性的 CA Access Control 主机名。 您可以使用“全局查看”来查看端点的 CA Access Control 主机名。

基域名

定义在 LDAP 目录中开始搜索的起始点

示例：*host=RACF,o=company,c=com*

URL

定义 CA Access Control 企业管理 可以用来连接到端点的 URL。URL 指定数据库服务器的特定类型。

示例：ldap://*host_name.company.com:5*91

高级

指定是否要使用特权管理帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。 例如：您可以指定一个可以在多个端点上执行管理任务的特权域帐户。

如果指定该选项，PUPM 不使用“用户登录”帐户来执行管理任务。

注意：指定一个对自己及对其他用户帐户都有管理权限的用户帐户。

VMware ESX/ESXi 连接信息

VMware ESX/ESXi 端点类型允许您管理特权 VMware ESX/ESXi 帐户。

当您创建此类端点时，请提供以下信息，以使 [assign the value for eACVPM in your book] 可以连接到端点：

用户名

定义该端点的管理用户的名称。CA Access Control 企业管理 使用该帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。

注意：如果您指定“高级”选项，PUPM 不使用“用户登录”帐户来执行管理任务。 相反，PUPM 使用指定的特权帐户在端点上执行管理任务。

密码

定义该端点的管理用户的密码。

主机

定义该端点的主机名。

高级

指定是否要使用特权管理帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。 例如：您可以指定一个可以在多个端点上执行管理任务的特权域帐户。

如果指定该选项，PUPM 不使用“用户登录”帐户来执行管理任务。

Windows Agentless 连接信息

Windows Agentless 端点类型允许您管理特权 Windows 帐户。

注意：如果您在本地计算机上配置域用户，PUPM 无法更改该域用户的密码。 该限制是由于 Windows 行为引起的。

当您创建此类端点时，请提供以下信息，以使 CA Access Control 企业管理 可以连接到端点：

用户登录

定义该端点的管理用户的名称。PUPM 使用该帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。

注意：如果您指定“高级”选项，PUPM 不使用“用户登录”帐户来执行管理任务。相反，PUPM 使用指定的特权帐户在端点上执行管理任务。

密码

定义该端点的管理用户的密码。

主机

定义该端点的主机名。

示例：myhost-ac-1

主机域

指定该主机所属的域的名称。

注意：只使用前缀指定主机域名。 例如：如果完整域名是 company.com，您只输入前缀 company。

是 Active Directory

指定用户帐户是否是 Active Directory 帐户。

用户域

指定用户所属的域的名称。

注意：只使用前缀指定用户域名。 例如：如果完整域名是 company.com，您只输入前缀 company。

重要说明！ 如果想使用 PUPM 自动登录功能登录端点，则验证是否指定了主机域名。 如果端点是工作组的成员，请指定主机名，而不是工作组名称。

高级

指定是否要使用特权管理帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。 例如：您可以指定一个可以在多个端点上执行管理任务的特权域帐户。

如果指定该选项，PUPM 不使用“用户登录”帐户来执行管理任务。

针对 PUPM 配置 Windows Agentless 端点

下列主题说明了在可以实施 PUPM 之前，您可能需要在您的 Windows Agentless 端点上执行的其他配置步骤。

更多信息：

Windows Agentless 端点上的域用户限制 (p. 123)

Windows Agentless 端点上的防火墙配置

在 Windows Server 2008 和 Windows 7 Enterprise 上有效

PUPM Windows Agentless 连接器使用端口 135（DCOM 端口）连接到 Windows Agentless 端点。 PUPM Windows Agentless 连接器属于 JCS 的一部分。 在连接器连接到端点之后，它使用动态端口（大于 1000）进行与 WMI (Windows Management Instrumentation) 服务的通信。

如果 Windows Agentless 端点上启用了 Windows 防火墙，该防火墙就可以同时阻止到端口 135 和动态端口的连接。 如果 Windows 防火墙阻止这些连接，企业管理服务器则无法与端点进行通讯。 因此，您在端点上无法创建 Windows Agentless 端点，或发现服务帐户和排定任务。

如果启用了 Windows 防火墙，必须配置该防火墙以便 PUPM Windows Agentless 连接器可以连接到端点。 在配置防火墙时，打开端口 135 并指定防火墙允许来自动态 RPC 端口的流量到达 WMI 服务。

更多信息：

如何针对 PUPM 配置 Windows 防火墙 (p. 162)

如何针对 PUPM 配置 Windows 防火墙

在 Windows Agentless 端点上有效

PUPM Windows Agentless 连接器使用端口 135（DCOM 端口）连接到 Windows Agentless 端点。 在连接器连接到端点之后，它使用动态端口（大于 1000）进行与 WMI (Windows Management Instrumentation) 服务的通信。

如果启用了 Windows 防火墙，您必须配置该防火墙以便 PUPM Windows Agentless 连接器可以连接到端点。 如果您不配置防火墙，企业管理服务器则无法与端点进行通信。

要针对 PUPM 配置 Windows 防火墙，请执行如下操作：

1. 打开端口 135。
2. 创建防火墙规则，以便防火墙允许任何来自动态 RPC 端口的流量到达 WMI 服务。

   使用下列示例中的信息帮助您配置 Windows 防火墙。

示例：打开端口 135

下列示例向您显示如何在 Windows Server 2008 计算机上打开端口 135。

1. 依次单击“开始”、“控制面板”、“Windows 防火墙”。

   将显示“Windows 防火墙”对话框。

2. 单击“更改设置”。

   此时出现“Windows 防火墙设置”对话框。

3. 单击“例外”选项卡，然后单击“添加端口”。

   此时出现“添加端口”对话框。

4. 按如下方式填写该对话框：

   - 在“名称”字段中，键入 **DCOM_TCP135**
   - 在“端口号”字段中，键入 **135**
   - 在“协议”部分中，选择“TCP”

   单击“确定”。

   “例外”选项卡中显示 DCOM_TCP135 规则。

5. 单击“确定”。

   “Windows 防火墙设置”对话框关闭。 您已经打开了端口 135。

示例：创建允许来自动态 RPC 端口的流量到达 WMI 服务的防火墙规则

下列示例向您显示如何在 Windows Server 2008 计算机上创建防火墙规则。 该防火墙规则允许来自动态 RPC 端口的流量到达 WMI 服务。

1. 依次单击“开始”、“管理工具”、“高级安全 Windows 防火墙”。

   此时打开“高级安全 Windows 防火墙”对话框。

2. 右键单击左侧窗格中的“入站规则”，然后单击“新建规则”。

   此时出现“新建入站规则向导”。

3. 完成“新建入站规则向导”。 *接受除*以下页面以外所有页面上的默认设置：

   a. 在“规则类型”页面上，选择“自定义”。

   b. 在“程序”页面上，执行如下操作：

      - 选择所有程序。
      - 单击“自定义”。

        此时打开“自定义服务设置”对话框。

      - 选择“适用于此服务”，选择“Windows Management Instrumentation”，然后单击“确定”。

c. 在“范围”页面上，在“此规则匹配哪些远程 IP 地址”部分中执行如下操作：

- 选择这些 IP 地址，然后单击“添加”。

  此时出现“IP 地址”对话框。

- 在“IP 地址或子网”中输入分发服务器的 IP 地址，然后单击“确定”。

d. 在“名称”页面上，在“名称”字段中键入新规则的名称。

完成该向导之后，您已经创建了防火墙规则，这样该防火墙就会允许任何来自动态 RPC 端口的流量到达 WMI 服务。

更多信息：

Windows Agentless 端点上的防火墙配置 (p. 162)

针对 PUPM 配置 Windows Server 2008 R2 x64 端点

在 Windows Server 2008 上有效

要在 Windows Server 2008 R2 x64 端点上使用 PUPM，您必须在端点上执行其他配置步骤。

请按下列步骤操作：

1. 打开 Windows 注册表。
2. 导航到以下注册表项，并为每个注册表项执行步骤 3-6：

   `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

   `HKEY_CLASSES_ROOT\CLSID\{233664b0-0367-11cf-abc4-02608c9e7553}`

   注意：您可以使用“编辑”菜单中的“查找”选项来搜索这些注册表项。
3. 右键单击每个注册表项，然后选择“权限”。

   此时显示“权限”对话框。
4. 单击“高级”。

   此时出现“高级安全设置”对话框。
5. 依次单击“所有者”选项卡、“将所有者更改为:”字段中的“Administrators”、“应用”，然后单击“确定”。

   “高级安全设置”对话框关闭。

6. 在“权限”对话框中选择“组或用户名称”中的“Administrators”，然后在“Administrators 的权限”窗口的“允许”列中选择“完全控制”复选框。
7. 单击“确定”。
8. 依次单击“开始”，“管理工具”，“本地安全策略”。

   “本地安全策略”管理控制台将打开。
9. 依次选择“本地策略”，“安全选项”。

   可用的安全选项列表出现。
10. 找到以下安全策略：
    - 网络安全：针对基于 NTLM SSP（包括安全 RPC）客户端的最小会话安全
    - 网络安全：针对基于 NTLM SSP（包括安全 RPC）客户端的最小会话安全
11. 右键单击每个策略，然后选择“属性”。

    本地安全设置选项卡将打开。
12. 确认没有选择“需要 128 位加密”选项。
13. 单击“确定”并退出。

    您已经针对 PUPM 配置了 Windows Server 2008 R2 x64 端点。 您可能还需要配置防火墙并将权限添加到 DCOM。

修改 Windows Server 2008 端点以便使用登录应用程序

在 Windows Server 2008 上有效

在 Windows Server 2008 计算机上，Microsoft 更改了“ActiveX 控件的自动提示”选项的默认值。 在 Windows Server 2008 计算机上，该选项的默认值为“已禁用”。 在 Windows 的先前版本上，该选项的默认值为“已启用”。 该选项影响了本地 Intranet 和受信任的站点区域的安全设置。

要修改 Windows Server 2008 端点以便使用登录应用程序，请为本地 Intranet 和受信任的站点区域更改“ActiveX 控件的自动提示”选项的值。

注意：如果不更改该选项的值，则无法在 Windows Server 2008 计算机上使用自动登录。

更多信息：

创建登录应用程序 (p. 179)

针对 PUPM 配置 Windows 7 Enterprise 端点

在 Windows 7 Enterprise 上有效

如果想在 Windows 7 端点上使用 PUPM，请在该端点上执行其他配置步骤。

完成以下步骤：

1. 打开 Windows 注册表。
2. 导航到以下注册表项，并为每个注册表项执行步骤 3-6：

   HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

   HKEY_CLASSES_ROOT\CLSID\{233664b0-0367-11cf-abc4-02608c9e7553}

   注意：您可以使用“编辑”菜单中的“查找”选项来搜索这些注册表项。
3. 右键单击注册表项，然后选择“权限”。

   此时显示“权限”对话框。
4. 单击“高级”。

   此时出现“高级安全设置”对话框。
5. 依次单击“所有者”选项卡、“将所有者更改为:”字段中的“Administrators”、“应用”，然后单击“确定”。

   “高级安全设置”对话框关闭。
6. 在“权限”对话框中选择“组或用户名称”中的“Administrators”，然后在“Administrators 的权限”窗口的“允许”列中选择“完全控制”复选框。
7. 单击“确定”并关闭 Windows 注册表。
8. 依次打开 Windows“控制面板”、“管理工具”、“服务”。

   此时打开 Windows“服务”控制台。
9. 右键单击“Remote Registry”服务，然后选择“属性”

   此时打开“属性”对话框。
10. 将“启动类型”更改为“自动”，然后选择“启动”。

    此时启动“Remote Registry”服务。
11. 在“运行”命令行窗口运行 DCOMCNFG 命令。

    此时打开“组件服务”窗口。
12. 依次选择“控制台根目录”、“组件服务”、“计算机”。
13. 右键单击“我的电脑”，然后选择“属性”。

    此时打开“属性”对话框。

14. 单击“COM 安全”选项卡，然后在“访问权限”部分下单击“编辑默认值”。

    此时打开“默认安全”对话框。

15. 在“组或用户名称”窗口中选择“Administrators”，然后选择“本地访问”和“远程访问”的“允许”复选框。

16. 单击“确定”，然后在“启动和激活权限”部分中重复步骤 14 和步骤 15。

17. 单击“确定”并关闭“组件服务”控制台。

    您已针对 PUPM 配置了 Windows 7 Enterprise 端点。 您还可能需要配置防火墙

修改管理员批准模式

在 Windows Server 2008 和 Windows 7 上有效

PUPM 端点管理任务运行在后台，且需要本地管理员帐户的访问权限。如果 PUPM 端点管理员没有访问该本地管理员帐户的权限，那么您必须允许所有端点管理员以管理员批准模式运行。

重要说明：如果已禁用该策略设置，安全中心会通知您，操作系统的总体安全性已减少。

请按下列步骤操作：

1. 依次选择“控制面板”、管理工具、“本地安全策略”

   “本地安全”窗口打开。

2. 浏览到本地策略、安全选项

   此时会打开策略窗格。

3. 右键单击“用户帐户控制”：以管理员批准模式运行所有管理员并选择“属性”

   将出现“属性”对话框

4. 更改操作方式以禁用，并单击“确定”

   “属性”对话框将关闭。

5. 重新启动您的计算机以应用更改。

   您的后台端点管理任务现在成功运行。

质询和响应身份验证协议限制

在 Windows Agentless 端点上有效

质询/响应用于网络登录的身份验证协议会影响身份验证协议的级别以及端点用于进行客户端/服务器通信的会话安全。 有三种用于网络登录的 Windows 质询/响应身份验证协议：

- LM — LAN Manager 质询/响应
- NTLM — Windows NT 质询/响应
- NTLMv2 — 第二版的 NTLM

LAN Manager 身份验证级别设置控制端点使用的质询/响应身份验证协议。 该设置的默认值是“发送 LM 和 NTML 响应”。 仅当 LAN Manager 身份验证级别设置的值是“发送 LM 和 NTML 响应”时，企业管理服务器才能与 Windows 端点进行通信。 例如，当该设置的值是“仅发送 NTLMv2 响应\拒绝 LM 和 NTLM”时，企业管理服务器无法与 Windows 端点进行通信。

仅当端点上的 LAN Manager 身份验证级别设置是“发送 LM 和 NTML 响应”时，您才能创建 Windows Agentless 端点。 如果无法创建 Windows Agentless 端点，您可能需要更改端点上的质询和响应身份验证协议。

SSH 设备连接信息

SSH 设备类型允许您管理特权 UNIX 帐户。

重要说明！ 在您配置 PUPM SSH 端点之前，先在端点上禁用隧道明文密码，然后再配置端点设置。

当您创建此类设备时，请提供以下信息，以使 CA Access Control 企业管理 可以连接到设备：

用户登录

定义该端点的管理用户的名称。PUPM 使用该帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。

注意：如果您指定“高级”选项，PUPM 不使用“用户登录”帐户来执行管理任务。相反，PUPM 使用指定的特权帐户在端点上执行管理任务。如果您指定操作管理员帐户，PUPM 会使用该帐户在端点上执行管理任务。

密码

定义该端点的管理用户的密码。

主机

定义该端点的主机名。

使用 Telnet

指定使用 Telnet（而不是 SSH）连接到 SSH 设备。

操作管理员用户登录

（可选）定义端点的操作管理员用户的名称。PUPM 使用该帐户在端点上执行管理任务，例如，发现和更改特权帐户的密码。 如果您不指定操作管理员用户，PUPM 会使用用户登录帐户在端点上执行管理任务。

如果为使用检查点防火墙的 SSH 端点指定操作管理员用户，则请指定专家用户。 但是，您无法使用 PUPM 更改端点上的专家帐户的密码。该限制意味着，专家帐户必须是 PUPM 中的断开帐户。

操作管理员密码

（可选）定义操作管理员用户的密码。

配置文件

指定 SSH 设备 XML 配置文件的名称。您可以根据需要自定义 XML 文件。

注意：如果您不指定该字段的值，CA Access Control 企业管理 将使用 ssh_connector_conf.xml 文件。

高级

指定是否要使用特权管理帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。 例如：您可以指定一个可以在多个端点上执行管理任务的特权域帐户。

如果指定该选项，PUPM 不使用“用户登录”帐户来执行管理任务。

PUPM 到 UNIX 端点的连接方式

当创建端点时，您指定 PUPM 用来连接到端点并执行管理任务（如发现和更改特权帐户的密码）的管理员帐户。 对于 UNIX 帐户，最合适的管理员帐户通常是 root。 但是，PUPM 使用 SSH 连接到 UNIX 端点，而某些组织禁止用户和应用程序以 root 用户身份进行 SSH 连接。

要克服该问题，您可以在创建“SSH 设备”端点时同时指定一个连接帐户和一个操作管理员帐户。 （PUPM 使用“SSH 设备”作为 UNIX 端点的端点类型。）通过使用两个帐户，您还可以使用与操作管理员帐户相比具有更少权限的连接帐户。

以下过程说明了 PUPM 使用这些帐户连接到“SSH 设备”端点的方式：

1. PUPM 使用连接帐户的凭据连接到端点。
2. PUPM 使用操作管理员帐户的凭据切换到该帐户。

   例如，如果操作管理员帐户是 root 帐户，PUPM 使用 root 凭据切换到 root 帐户。
3. PUPM 以操作管理员身份执行管理任务。

   例如，如果操作管理员帐户是 root 帐户，PUPM 以 root 用户身份执行管理任务。

当您查看“SSH 设备”端点上的特权帐户时，连接帐户和操作管理员帐户都被列为端点管理员帐户。

如何创建自定义的 SSH 设备端点

如果 PUPM 用来发现特权帐户的默认设置不适用于“SSH 设备”端点，您可以创建自定义的“SSH 设备”端点。

要创建自定义的“SSH 设备”端点，请执行以下操作：

1. 自定义“SSH 设备”XML 文件。
2. 在 CA Access Control 企业管理 中创建“SSH 设备”端点 (p. 151)。 在“配置文件”字段中，输入您创建的 XML 文件的名称。

   使用自定义的设置创建了“SSH 设备”端点。
3. 在您创建的端点上运行特权帐户发现向导 (p. 143)。

   CA Access Control 企业管理 使用您在 XML 文件中定义的参数搜索端点中的特权帐户。
4. 审阅 JCS 连接器日志文件 (jcs_stdout.log) 和 JCS 连接器错误文件 (jcs_sterr.log)。 文件位于：

   ACServerInstallDir/Connector Server/logs
5. 如果需要，请修改 XML 文件以解决出现在日志文件中的错误。

注意：有关 SSH 设备 XML 文件的格式的详细信息，请参阅 *《参考指南》*。

各种类型的 SSH 设备 XML 配置文件

CA Access Control 提供以下“SSH 设备”XML 配置文件。 您自定义这些文件来适应您的企业要求：

- **aix_connector_conf.xml** — 针对是 AIX 端点的 SSH 设备定义配置设置。
- **checkpoint_connector_conf.xml** — 针对使用检查点防火墙的 SSH 设备定义配置设置。
- **Cisco-UCS_connector_conf.xml** — 针对是 Cisco UCS 端点的 SSH 设备定义配置设置。
- **device_connector_conf.xml** — 针对诸如路由器类的设备定义配置设置。
- **nis_connector_conf.xml** — 针对与 NIS 服务器一起使用的 SSH 设备定义配置设置。

  注意：将本地 root 帐户用作已连接的用户。 请执行以下操作：

  a. 创建 NIS 端点 (nis_endpoint_1) 并使用默认 XML 文件定义 root 帐户。 (ssh_connector_conf.xml)

  b. 创建其他 NIS 端点 (nis_endpoint_2) 并使用“高级”选项定义第一个 NIS 端点的 root 帐户。
- **ssh_connector_conf.xml** — 当您配置使用 passwd 命令更改帐户密码的 SSH 设备时，请使用该文件。

  注意：将本地用户（例如 root）指定为已连接的用户。
- **sudo_connector_conf.xml** — 当您配置使用 sudo 和 passwd 命令的 SSH 设备时，请使用该文件。

自定义 SSH 设备 XML 文件

“SSH 设备”XML 文件定义 PUPM 连接到“SSH 设备”端点、发现用户帐户以及更改端点上的特权帐户密码的方式。CA Access Control 提供几个不同的“SSH 设备”XML 文件。 这些文件包含 PUPM 用来连接到各种类型的“SSH 设备”端点的默认设置。

如果“SSH 设备”端点使用备用方法更改端点上的特权帐户密码，您自定义“SSH 设备”XML 文件来指定非默认设置。 例如，自定义“SSH 设备”XML 文件，以便为使用非标准方法发现用户帐户并更改特权帐户密码的路由器、交换机或防火墙创建端点。

完成以下步骤：

1. 在 CA Access Control 企业管理 上，找到想要自定义的 XML 文件。 这些文件位于以下目录中：

   ACServerInstallDir/Connector Server/conf/override/sshdyn

2. 复制想要自定义的文件，然后打开新文件进行编辑。

   注意：将新文件保存在相同的目录中。

3. 修改文件中的参数来适应您的企业要求。

   文件中的每个 <item> 元素都定义了特定命令的参数。 PUPM 使用这些命令在端点上获取用户和更改密码。 修改 <item> 元素可定义 PUPM 发送给端点的命令。 您也可以修改 PUPM 用来连接到端点的设置。

4. 保存并关闭文件。

   您已经针对端点自定义了“SSH 设备”XML 文件。

注意：有关 SSH 设备 XML 文件的格式的详细信息，请参阅 *《参考指南》*。

注意：如果您使用的是中文、日文或朝鲜语字符自定义文件，您应当使用 UTF-8 编码来保存文件。

示例：SSH 设备 XML 文件如何定义 PUPM 命令

该示例说明了“SSH 设备”XML 文件中的某部分如何定义 PUPM 在“SSH 设备”端点上执行的命令。 该部分中的每个 <item> 元素都定义了特定操作的参数。 所有的 <item> 元素一起创建定义了 PUPM 与端点的交互方式的脚本。

每个 <item> 元素都以 sCommand 参数开头。 sCommand 参数定义了 PUPM 在端点上执行的命令。 sCommand 参数后面的参数定义了 PUPM 在该命令之后执行的任何其他操作。

该示例向您显示 Cisco-UCS_connector_conf.XML 文件中的某部分如何定义 PUPM 用来更改 Cisco 交换机上的特权帐户密码的命令。 Cisco-UCS_connector_conf.xml 文件位于以下目录：

ACServerInstallDir/Connector Server/conf/override/sshdyn

该示例仅显示 Cisco-UCS_connector_conf.xml 文件的一部分。 该文件中的其他元素配置到 Cisco 交换机的连接，并指定 PUPM 执行以获取用户的命令。

注意：有关 SSH 设备 XML 文件的格式的详细信息，请参阅 *《参考指南》*。

以下过程向您显示 PUPM 执行以更改 Cisco 交换机上的特权帐户密码的命令。 为了展示 <item> 元素如何配置 PUPM 执行的命令，在每个步骤的结尾提供了相应的 <item> 元素。

1. PUPM 指定更改特权帐户的密码。 PUPM 执行以下操作以完成该步骤：

   a. PUPM 发出以下命令：

      ```
      set password
      ```

   b. PUPM 会等待 500 毫秒。

   c. PUPM 等待接收 **word:** 文本字符串。 当接收到该字符串时，会进入下一步骤。

   以下 <item> 元素指定了 PUPM 在该步骤采取的操作：

   ```
   <item>
   <param name="sCommand" value="set password" />
   <param name="iWait" value="500" />
   <param name="sWaitForText" value="word:" />
   </item>
   ```

2. PUPM 指定特权帐户的新密码。 PUPM 执行以下操作以完成该步骤：

   a. PUPM 将新密码发送到端点。

      PUPM 不会将新密码写入日志文件。

   b. PUPM 会等待 500 毫秒。

   c. PUPM 等待接收 **word:** 文本字符串。 当接收到该字符串时，会进入下一步骤。

   以下 <item> 元素指定该命令的参数：

   ```
   <item>
   <param name="sCommand" value="[%%password%%]" />
   <param name="bHideSentLog" value="true" />
   <param name="iWait" value="500" />
   <param name="sWaitForText" value="word:" />
   </item>
   ```

3. PUPM 确认特权帐户的新密码。 PUPM 执行以下操作以完成该步骤：

   a. PUPM 将新密码重新发送到端点。

      PUPM 不会将新密码写入日志文件。

   b. PUPM 会等待 500 毫秒。

   c. PUPM 等待接收 **local-user* #** 文本字符串。 当接收到该字符串时，会进入下一步骤。

      如果 PUPM 接收到 **failure**、**invalid** 或 **error** 文本字符串，则密码更改失败。

   以下 <item> 元素指定该命令的参数：

   ```
   <item>
   <param name="sCommand" value="[%%password%%]" />
   <param name="bHideSentLog" value="true" />
   <param name="iWait" value="500" />
   <param name="sWaitForText" value="local-user* #" />
   <param name="sFailureResult" value="failure;invalid;error" />
   </item>
   ```

4. PUPM 提交特权帐户的新密码。 PUPM 执行以下操作以完成该步骤：

   a. PUPM 发出以下命令：

      ```
      commit-buffer
      ```

      PUPM 不会将该命令写入日志文件。

   b. PUPM 会等待 500 毫秒。

   c. PUPM 等待接收 **local-user #** 文本字符串。 当接收到该字符串时，密码更改已完成。

      如果 PUPM 接收到 **Error: Update failed:** 文本字符串，则密码更改失败。

   以下 <item> 元素指定该命令的参数：

   ```
   <item>
   <param name="sCommand" value="commit-buffer" />
   <param name="bHideSentLog" value="true" />
   <param name="iWait" value="500" />
   <param name="sWaitForText" value="local-user #" />
   <param name="sFailureResult" value="Error: Update failed:" />
   </item>
   ```

   密码更改已完成。

SAP R3 连接信息

PUPM SAP R3 端点类型允许您管理特权 SAP R3 帐户。 在 PUPM 中创建 SAP R3 端点之前，必须配置 SAP R3 连接器。

当您创建此类设备时，请提供以下信息，以使 CA Access Control 企业管理 可以连接到设备：

用户登录

定义该端点的管理用户的名称。PUPM 使用该帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。

注意：如果您指定“高级”选项，PUPM 不使用“用户登录”帐户来执行管理任务。相反，PUPM 使用指定的特权帐户在端点上执行管理任务。

密码

定义该端点的管理用户的密码。

主机

定义该端点的主机名。

系统 ID

定义 SAP R3 系统 ID。

系统编号

定义 SAP R3 系统编号。

客户端编号

定义 SAP R3 系统客户端编号。

高级

指定是否要使用特权管理帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。 例如：您可以指定一个可以在多个端点上执行管理任务的特权域帐户。

如果指定该选项，PUPM 不使用“用户登录”帐户来执行管理任务。

注意：有关系统 ID、系统编号和客户端编号的更多信息，请参阅 SAP R3 文档。

配置 SAP R3 连接器

您必须配置 SAP R3 连接器才可以使用 PUPM 来管理 SAP R3 端点上的特权帐户。

要配置 SAP R3 连接器，请在企业管理服务器或 Java 连接器服务器 (JCS) 安装所在的任何服务器上安装 SAP JCo 库。

您可以使用您的 SAP 登录从 SAP Marketplace 下载 SAP JCo 库。 确认所选择的 SAP JCo 库适用于您使用的系统平台。

示例：在 Windows 上安装 SAP JCo 库

下列示例向您显示如何在 x86 Windows 2003 Server 上安装 SAP JCo 库。

1. 将 sapjco-ntamd64-2.1.9.zip 解压缩到临时目录。
2. 将 sapjcorfc.dll 和 librfc32.dll 文件复制到 Windows system32 目录。

   注意：如果系统进行提示，请覆盖该目录中的任何现有文件。
3. 将 sapjco.jar 文件复制到 Java Connector Server extlib 目录。 该目录位于：

   ```
   [set the Access Path variable]\Connector Server\extlib
   ```
4. 重新启动 CA Identity Manager - Connector Server 服务。

   现在，您可以使用 PUPM 来管理 SAP R3 端点上的特权帐户。

更多信息：

SAP R3 连接信息 (p. 175)

CA Identity Manager 配给连接信息

CA Identity Manager 配给连接器允许您管理在配给服务器中定义的 CA Identity Manager 端点。 在 PUPM 中创建 CA Identity Manager 端点之前，您必须创建 Identity Manager 配给类型的连接器服务器。

注意：有关如何创建连接器服务器的更多信息，请参阅联机帮助。

注意：当您配置 CA Identity Manager 配给连接器服务器时，指定完全可辨别名称 etaadmin。

例如：

```
eTGlobalUserName=etaadmin,eTGlobalUserContainerName=Global
Users,eTNamespaceName=CommonObjects,dc=ProvisioningDomainName,dc=eta
```

CA Identity Manager 可以强制实施与在目标系统上配置的密码策略不同的密码策略。 如果您在目标系统上强制实施密码策略，PUPM 会更改用户密码。 但是，用户无法在端点上使用该密码。 确认目标系统上的密码策略符合 PUPM 密码策略。 有关 CA Identity Manager 密码策略强制选项的更多信息，请参阅《*CA Identity Manager 管理指南*》。

当您创建此类端点时，请提供以下信息，以使 CA Access Control 企业管理 可以连接到端点：

端点

定义端点的名称，使之与您在 CA Identity Manager 配给服务器中定义的名称完全相同。

仅当您在配给服务器中配置连接之后，CA Access Control 企业管理 才显示 CA Identity Manager 端点类型。

主机

定义该端点的主机名。 该名称是您想分配给该端点的逻辑名称。 CA Access Control 企业管理 在“全局查看”中使用此名称表示端点。

高级

指定是否要使用特权管理帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。 例如：您可以指定一个可以在多个端点上执行管理任务的特权域帐户。

如果指定该选项，PUPM 不使用“用户登录”帐户来执行管理任务。

更多信息：

针对 PUPM 配置 CA Identity Manager 配给管理器 (p. 177)

针对 PUPM 配置 CA Identity Manager 配给管理器

您必须为 PUPM 配置 CA Identity Manager 配给管理器才能使用 PUPM 来管理您在配给服务器中定义的 CA Identity Manager r12.5 和 r12.5 SP1 端点。

针对 PUPM 配置 CA Identity Manager 配给管理器

1. 登录到 CA Identity Manager 配给管理器。
2. 单击“系统”选项卡。
3. 选择想要配置的域，然后单击左侧窗格中的“域配置”。

   此时出现域配置树。

4. 展开“密码”树，选择“Enforce Synchronized Account Passwords”。

   此时出现“Enforce Synchronized Account Passwords”参数的“域配置”选项卡。

5. 单击“编辑”，将值更改为“No”，然后单击“确定”。
6. 单击“应用”。

   “Enforce Synchronized Account Passwords”的值已更改。

7. 重新启动 CA Identity Manager - Provisioning Server 和 CA Identity Manager - Connector Server (Java) 服务。

   已为 PUPM 配置了 CA Identity Manager 配给管理器。

修改 CA Identity Manager 配给连接器搜索限制

当您运行“特权帐户发现”向导时，CA Identity Manager 配给连接器会针对您在 CA Identity Manager 连接管理器中配置的每个端点返回多达 1000 个结果。 您可以修改默认搜索限制在每个查询中显示更多结果。

修改 CA Identity Manager 配给连接器搜索限制

1. 在企业管理服务器上，停止 Java 连接器服务器。 请执行下列操作之一：

   a. 在 Windows 中，打开“服务”窗口，选择 CA Identity Manager - Connector Server (Java) 服务并单击“停止”。

   b. 在 UNIX 中，导航到下列目录，其中 *ACServerInstallDir* 表示安装企业管理服务器的目录：

      ACServerInstallDir/Connector_Server/bin

   c. 运行以下命令：

      ```
      ./im_jcs stop
      ```

   Java 连接器服务器停止。

2. 打开 im_connector_conf.xml 文件进行编辑。 该文件位于以下目录：

   ACServerInstallDir/Connector_Server/conf/override/imdyn

3. 找到标记“I_SEARCH_SIZE_LIMIT”，并且将搜索限制指定为值。 例如：

   ```
   <param name="I_SEARCH_SIZE_LIMIT" value="1500" />
   ```

4. 保存并关闭文件。
5. 启动 Java 连接器服务器。

重要说明！ 指定比默认值高的搜索限制值可导致系统特性下降。

断开端点的连接信息

断开端点类型允许您存储驻留在断开端点上的特权帐户的密码。

PUPM 不登录到断开端点上的帐户，也不管理这些帐户。 相反，PUPM 仅用作端点上特权帐户的密码存储库。 每次更改 CA Access Control 企业管理 中断开端点上特权帐户的密码时，还必须在受管端点上手动更改帐户密码。

只能在断开端点上创建断开的帐户。 断开的帐户是 PUPM 不进行管理的帐户；例如：PUPM 不更改断开的帐户的密码。 此外，您无法使用“发现特权帐户向导”或“发现服务帐户向导”来发现断开端点上的帐户。

当您创建此类端点时，请提供以下信息，以使 CA Access Control 企业管理 可以连接到端点：

主机名

定义该端点的主机名。

创建登录应用程序

登录应用程序使用脚本在端点上执行一个应用程序，在您签出特权帐户密码后，该应用程序会使您自动登入特权帐户。 登录应用程序允许您配置 PUPM 自动登录。

您可以创建以下类型的登录应用程序。 每种类型的登录应用程序都是 Visual Basic 脚本：

- ORACLE_10G_WEB.vbs－允许您自动登录 Oracle 10g 数据库的企业管理器 Web 接口。
- ORACLE_10XE_WEB.vbs－允许您自动登录 Oracle XE 数据库的数据库主页 Web 接口。
- ORACLE_11G_WEB.vbs－允许您自动登录 Oracle 11g 数据库的企业管理器 Web 接口。
- PUTTY.vbs－允许您自动登录 SSH 设备端点。

  注意：您必须在计算机上安装 PuTTY 版本 0.60，才能使用 PuTTY 登录应用程序。
- RDP.vbs－允许您自动登录 Windows 端点。

当您使用自动登录功能在 Windows Agentless 端点上签出特权帐户密码时，CA Access Control 企业管理 会将主机域附加到特权帐户名称的前面。 在您为 Windows Agentless 端点创建登录应用程序之前，请验证以下各项：

- 如果端点是工作组的一部分，确认在“主机域”字段中指定了计算机名。
- 如果端点是域的一部分，确认在“主机域”字段中指定了域名。

  注意：您可以使用修改端点任务来修改“主机域”字段。

默认情况下，您必须有系统管理员角色才能创建登录应用程序。 仅可以在 Microsoft Internet Explorer 浏览器中使用登录应用程序。

创建登录应用程序

1. 在 CA Access Control 企业管理 中，依次单击“特权帐户”、“登录应用程序”、“创建登录应用程序”任务。

   此时出现“创建登录应用程序: 登录应用程序搜索”屏幕。
2. （可选）按如下方式选择一个现有登录应用程序来创建登录应用程序作为其副本：
   a. 选择“创建类型为‘登录应用程序’的对象副本”。
   b. 选择要搜索的属性，键入筛选值，然后单击“搜索”。

      此时将显示匹配筛选条件的登录应用程序的列表。
   c. 选择要用作新登录应用程序基础的对象。
3. 单击“确定”。

   此时出现“创建登录应用程序”任务页面。 如果登录应用程序是从现有对象创建的，则对话框字段中会预先填充来自现有对象的值。
4. 填写以下字段：

   名称

   定义要用来指代此登录应用程序的名称。

   说明

   （可选）定义要为该登录应用程序记录的信息（自由文本）。

脚本

定义用来启动登录应用程序的 Visual Basic 脚本。

注意：建议您不要自定义这些提供的脚本。

启用

指定已启用该登录应用程序。

单击“提交”。

CA Access Control 企业管理 将创建登录应用程序。 用户必须先在 CA Access Control 企业管理 中将端点修改为使用登录应用程序，然后才能使用该登录应用程序。 您需要在端点上执行其他配置步骤以使用终端集成，并需要在 Windows Server 2008 端点上使用登录应用程序。

更多信息：

配置终端集成 (p. 229)
修改 Windows Server 2008 端点以便使用登录应用程序 (p. 165)

如何导入 PUPM 端点和特权帐户

使用 PUPM 导送程序实现 PUPM 端点和特权帐户的自动管理。 PUPM 导送程序允许您通过一个步骤将许多 PUPM 端点和特权帐户导入 CA Access Control 企业管理。 也可以使用 PUPM 导送程序来创建或修改 PUPM 端点和特权帐户。

注意：您不能使用 PUPM 导送程序来删除 PUPM 端点和特权帐户。

重要说明！ 为避免在处理过程中出错，请在您导入特权帐户 CSV 文件之前，将端点 CSV 文件导入 PUPM。

要将 PUPM 端点和特权帐户导入到 CA Access Control 企业管理 中，请执行以下操作：

1. 配置导送程序属性文件。

   导送程序属性文件指定了轮询时间间隔以及轮询文件夹、已处理文件文件夹和错误文件文件夹的名称和位置。

2. （可选）写入限制对轮询文件夹、已处理文件的文件夹和错误文件的文件夹进行访问的 CA Access Control 规则。

   限制对这些文件夹的访问有助于防止未授权的用户访问端点的明文密码和特权帐户 CSV 文件。

3. 执行下面的一项或所有操作：
   - 创建端点 CSV 文件。
   - 创建特权帐户 CSV 文件。

   CSV 文件中的每一行都表示一个创建或修改 PUPM 端点或特权帐户的任务。 您必须创建单独的端点 CSV 文件和特权帐户 CSV 文件。

   注意：您可以在其他应用程序中配置一个自动化进程，以创建 CSV 文件。
4. （可选）开始轮询任务。

   轮询任务开始时，PUPM 导送程序将轮询文件夹中的 CSV 文件上传到 CA Access Control 企业管理，然后 CA Access Control 企业管理 会处理这些 CSV 文件。

   注意：如果您不手动启动轮询任务，PUPM 导送程序会在导送程序属性文件所指定的时间，在轮询文件夹中检查文件。
5. 当 CA Access Control 企业管理 处理完 CSV 文件时，查看错误文件的文件夹中的 CSV 文件是否有失败的任务。

   该文件列出失败的任务和 CA Access Control 企业管理 无法处理的任务。
6. 更正文件中的错误，并将文件保存到轮询文件夹中。
7. 开始轮询任务。
8. 重复步骤 5 - 7，直至导入全部 PUPM 端点和特权帐户。

PUPM 导送程序的工作原理

通过 PUPM 导送程序，您在一个步骤中即可创建或修改许多 PUPM 端点或特权帐户。 了解 PUPM 导送程序的工作原理可帮助您以最适合您企业的方式配置 PUPM，并帮助您排除可能发生的任何问题。

以下过程说明了 PUPM 导送程序的工作原理：

1. 您（或某自动化进程）在轮询文件夹中创建和保存一个或多个 CSV 文件。

   CSV 文件中的每一行都表示一个创建或修改 PUPM 端点或特权帐户的任务。 您分别为端点和特权帐户创建单独的 CSV 文件。
2. 当轮询任务开始时，PUPM 导送程序将轮询文件夹中的 CSV 文件上传到 CA Access Control 企业管理。 您可以配置轮询任务在指定的时间运行，也可以手工开始轮询任务。

   注意：如果 PUPM 导送程序无法重命名文件，则无法处理该文件。未处理的 CSV 文件仍然保留在轮询文件夹中。

3. CA Access Control 企业管理 重命名 CSV 文件 *original_timestamp*.csv，并将文件移至已处理文件的文件夹。

   注意：*original* 是初始 CSV 文件的名称，*timestamp* 是表示文件处理时间的时间戳。 例如，如果您将初始 CSV 文件命名为 endpoints.csv，CA Access Control 企业管理 则会将已处理文件的文件夹中的文件命名为 endpoints_091209130256.csv。

4. CA Access Control 企业管理 依次处理 CSV 文件的每一行。 对于 CSV 文件的每一行，会发生以下情况：

   - 如果 CA Access Control 企业管理 可以完成任务，它会：
     - 完成该任务，例如创建端点。
     - 创建该任务的审核记录。
   - 如果 CA Access Control 企业管理 无法完成任务，它会：
     - 将 CSV 文件中的行复制到错误文件文件夹的 CSV 文件中。
     - 将名为 FAILURE_REASON 的列添加到错误文件文件夹的 CSV 文件中。
     - 将任务失败的原因添加到 FAILURE_REASON 列。
     - 创建该任务的审核记录。

   错误文件文件夹中的 CSV 文件为您提供了一种便捷的方式来查看失败的任务。 该文件的名称也是 *original_timestamp*.csv。

   注意：已处理文件文件夹中的 CSV 文件列出了所有的已处理任务，但是没有指定任务的状态。 也就是说，该任务是完成还是已失败。

5. CA Access Control 企业管理 为 CSV 文件的每一行重复步骤 4。

配置导送程序属性文件

导送程序属性文件指定了轮询时间间隔以及轮询文件夹、已处理文件文件夹和错误文件文件夹的名称和位置。 JBoss 会在每次启动时读取导送程序属性文件。

配置导送程序属性文件

1. 如果 JBoss 应用程序服务器正在运行，请将其停止。
2. 在基于文本的编辑器中打开导送程序属性文件。 该文件位于以下位置，其中 *JBoss_home* 是您安装 JBoss 的位置：

   ```
   JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/default/feeder.properties
   ```

3. 启用下列参数之一：

FOLDER_POLLING_INTERVAL_IN_MINUTES

定义 PUPM 导送程序对轮询文件夹进行轮询的时间间隔（以分钟为单位）。 该参数在默认情况下处于启用状态。

限制：1-60

默认值：60

FOLDER_POLLING_CRON_EXPR

定义 PUPM 导送程序对轮询文件夹进行轮询的时间。将该参数指定为 Cron 表达式。

重要说明！ 如果您使用该参数，从 FOLDER_POLLING_CRON_EXPR 行中删除注释标记 (#)，并通过在该行的开头添加注释标记来禁用 FOLDER_POLLING_INTERVAL_IN_MINUTES 参数。

示例：FOLDER_POLLING_CRON_EXPR=0 0 23 ? * MON-FRI

该示例指定，PUPM 导送程序在周一到周五的下午 11 点对轮询文件夹进行轮询。

轮询时间间隔已配置。

4. （可选）编辑以下参数：

FOLDER_FOR_POLLING

定义轮询文件夹 — PUPM 导送程序对 CSV 文件进行轮询的文件夹。

默认：
JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/waitingToBeProcessed

注意：该文件夹必须位于企业管理服务器计算机上。 您必须指定该文件夹的绝对文件路径。

FOLDER_FOR_PROCESSED_FILES

定义已处理文件文件夹 — PUPM 导送程序在处理 CSV 文件之后将其移至的文件夹。

默认：
JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/processed

注意：该文件夹必须位于企业管理服务器计算机上。 您必须指定该文件夹的绝对文件路径。

FOLDER_FOR_ERROR_FILES

定义错误文件文件夹 — PUPM 导送程序将其无法处理的 CSV 文件移至的文件夹。

默认：
JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/failedToSubmit

注意：该文件夹必须位于企业管理服务器计算机上。 您必须指定该文件夹的绝对文件路径。

轮询文件夹的名称已配置。

5. 保存并关闭文件。

   导送程序属性文件已配置。

6. 重新启动 JBoss 应用程序服务器。

示例：导送程序属性文件

下列示例配置 PUPM 导送程序每 30 分钟一次来对轮询文件夹进行轮询，并定义轮询文件夹、已处理文件文件夹和错误文件文件夹的位置：

```
# feeder folder polling job configuration
# folder specified as FOLDER_FOR_POLLING will be checked every
FOLDER_POLLING_INTERVAL_IN_MINUTES minutes e.g. 60 equals every 1 hour (max value
is every hour)
FOLDER_POLLING_INTERVAL_IN_MINUTES=30
# if cron expression is supplied remark the FOLDER_POLLING_INTERVAL_IN_MINUTES
key
# FOLDER_POLLING_CRON_EXPR=
FOLDER_FOR_POLLING=C:\feeder\waitingToBeProcessed
FOLDER_FOR_PROCESSED_FILES=C:\feeder\processed
FOLDER_FOR_ERROR_FILES=C:\feeder\failedToSubmit
```

创建端点 CSV 文件

端点 CSV 文件中标头行之后的每一行都表示一个在 CA Access Control 企业管理 中创建或修改端点的任务。

重要说明！ 当创建 CSV 文件时，请确认没有其他应用程序使用该文件且该文件能够被重命名。 PUPM 导送程序仅处理能够重命名的 CSV 文件。

请按下列步骤操作：

1. 创建一个 CSV 文件，并以恰当的名称命名。

   注意：建议您创建端点 CSV 示例文件的一份副本。 示例文件位于以下目录，其中 *ACServer* 是您安装企业管理服务器的目录：

   ACServer/IAM Suite/Access Control/tools/samples/feeder

2. 创建指定端点属性名称的标头行。

   端点属性的名称如下所示。 某些端点属性仅对特定的端点类型有效：

   OBJECT_TYPE

   指定要导入的对象的类型。

   值：ENDPOINT

   操作_类型

   指定要执行的操作类型

   值：CREATE、MODIFY、DELETE

   %FRIENDLY_NAME%

   定义您在 CA Access Control 企业管理 中引用该端点的名称。

   DESCRIPTION

   定义想要为该端点记录的任何信息。

   ENDPOINT_TYPE

   指定该端点的类型。

   注意：您可以查看 CA Access Control 企业管理 中可用的端点类型。 在创建“CA Identity Manager 配给”类型的端点之前，您必须在 CA Access Control 企业管理 中创建“Identity Manager 配给”类型的连接器服务器。

   HOST

   定义该端点的主机名称。

LOGIN_USER

定义该端点的管理用户的名称。 该属性对任何“CA Identity Manager 配给”端点类型都*无效*，但是适用于所有其他的端点类型。

对于除“SSH 设备”以外的所有有效的端点类型：

- 如果您不指定特权管理帐户（IS_ADVANCE 属性），PUPM 会使用 LOGIN_USER 连接到端点并在端点上执行管理任务（例如，发现帐户和更改密码）。
- 如果您指定了特权管理帐户，PUPM 会忽略 LOGIN_USER 的任何值。

对于“SSH 设备”端点：

- 如果您不指定操作管理员 (OPERATION_ADMIN_USER_NAME) 或特权管理帐户，PUPM 会使用 LOGIN_USER 连接到端点并在端点上执行管理任务。
- 如果您指定了操作管理员，PUPM 会使用 LOGIN_USER 连接到端点，并使用操作管理员在端点上执行管理任务。
- 如果您指定了特权管理帐户，PUPM 会忽略 LOGIN_USER 的任何值。

PASSWORD

定义 LOGIN_USER 的密码。 该属性对“CA Identity Manager 配给”端点类型*无效*，但是适用于所有其他的端点类型。

URL

定义 CA Access Control 企业管理 用来连接到端点的 URL。 该属性适用于 MS SQL Server 和 Oracle Server 端点类型。

格式： (MS SQL Server) jdbc:sqlserver://*servername*:*port*

格式：(Oracle Server) jdbc:oracle:*drivertype*:@*hostname*:*port*:*service*

DOMAIN

指定该端点所属的域的名称。 该属性适用于 Access Control for PUPM 和 Windows Agentless 端点类型。

IS_ACTIVE_DIRECTORY

指定用户帐户是否是 Active Directory 帐户。 该属性仅适用于 Windows Agentless 端点类型。

限制： TRUE、FALSE

USER_DOMAIN

指定 LOGIN_USER 所属的域的名称。 该属性适用于 Windows Agentless 端点类型。

CONFIGURATION_FILE

指定您正在定义的“SSH 设备”XML 配置文件的名称。 该属性适用于“SSH 设备”端点类型。

注意：如果您不指定该属性的值，CA Access Control 企业管理 会使用默认配置文件 (ssh_connector_conf.xml)。

OPERATION_ADMIN_USER_NAME

（可选）定义端点的操作管理员用户的名称。 PUPM 使用该帐户在端点上执行管理任务，例如，发现和更改特权帐户的密码。 该属性适用于“SSH 设备”端点类型，如下所示：

- 如果您指定特权管理帐户（IS_ADVANCE 属性）和操作管理员，PUPM 会使用特权管理帐户连接到端点，并使用操作管理员在端点上执行管理任务。
- 如果您指定了 LOGIN_USER 和操作管理员帐户，PUPM 会使用 LOGIN_USER 连接到端点，并使用操作管理员在端点上执行管理任务。

如果为使用检查点防火墙的 SSH 端点指定操作管理员，您必须指定专家用户。 但是，您无法使用 PUPM 更改端点上的专家帐户的密码。 该限制意味着，专家帐户必须是 PUPM 中的断开帐户。

OPERATION_ADMIN_USER_PASSWORD

（可选）定义端点的操作管理员用户的密码。该属性适用于“SSH 设备”端点类型。

ENDPOINT

定义端点的名称，与其在 CA Identity Manager 配给服务器中的定义完全一致。该属性适用于“CA Identity Manager 配给”端点类型。

IS_ADVANCE

（可选）指定您是否想使用特权管理帐户连接到端点并在端点上执行管理任务（例如，发现帐户和更改密码）。 该属性适用于所有端点类型。

对于除“SSH 设备”以外的所有有效的端点类型，如果您指定了特权管理帐户（IS_ADVANCE 为 TRUE），PUPM 会使用特权管理帐户连接到端点并在端点上执行管理任务。

对于“SSH 设备”端点：

- 如果您指定特权管理帐户和操作管理员 (OPERATION_ADMIN_USER_NAME)，PUPM 会使用特权管理帐户连接到端点，并使用操作管理员在端点上执行管理任务。
- 如果您仅指定特权管理帐户，PUPM 会使用特权管理帐户连接到端点并在端点上执行管理任务。

限制： TRUE、FALSE

注意： 如果您将该属性的值设置为 TRUE，则不要指定 LOGIN_USER 的值。 但是，您必须指定 PROPERTY_ADMIN_ACCOUNT_ENDPOINT_TYPE、PROPERTY_ADMIN_ACCOUNT_ENDPOINT_NAME、PROPERTY_ADMIN_ACCOUNT_CONTAINER 以及 PROPERTY_ADMIN_ACCOUNT_NAME。

PROPERTY_ADMIN_ACCOUNT_ENDPOINT_TYPE

（可选）定义特权管理帐户在其上有所定义的端点的类型。

注意： 要使用授权管理帐户，您必须指定 IS_ADVANCE 为真。

PROPERTY_ADMIN_ACCOUNT_ENDPOINT_NAME

（可选）定义特权管理帐户在其上有所定义的端点的名称。 该端点必须存在于 CA Access Control 企业管理 中。

注意： 要使用授权管理帐户，您必须指定 IS_ADVANCE 为真。

PROPERTY_ADMIN_ACCOUNT_CONTAINER

（可选）定义特权管理帐户在其中有所定义的容器。 容器是一个类，其实例是其他对象的集合。

值： （Windows Agentless 和 Oracle Server）： Accounts

（SSH 设备）： SSH Accounts

（MS SQL Server）： MS SQL Logins

注意： 要使用授权管理帐户，您必须指定 IS_ADVANCE 为真。

PROPERTY_ADMIN_ACCOUNT_NAME

（可选）定义 PUPM 用来在端点上执行管理任务（例如，发现帐户和更改密码）的特权管理帐户的名称。特权帐户必须存在于 CA Access Control 企业管理 中。

注意： 要使用授权管理帐户，您必须指定 IS_ADVANCE 为真。

LOGIN_APPLICATION

指定登录应用程序的名称以与端点关联

OWNER_INFO

指定端点所有者的名称。

DEPARTMENT_INFO

指定部门名称。

CUSTOM1....5_INFO

指定多达五个特定客户属性。

3. 将端点任务行添加到 CSV 文件中。

   每一行都表示一个创建或修改端点的任务，并且必须有与标头行相同的属性。 这些属性的顺序必须与标头行中的相同。 如果某行没有某属性的值，则保留该字段为空。

4. 将文件保存到轮询文件夹。

   端点 CSV 文件已准备就绪，可供 PUPM 导送程序处理。

   注意：默认的轮询文件夹位于以下目录，其中 *JBoss_home* 是您安装 JBoss 的目录：

   JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/waitingToBeProcessed

示例：端点 CSV 文件

以下是端点 CSV 文件示例。 您可以在 *ACServer*/IAM Suite/Access Control/tools/samples/feeder 目录中找到更多的端点 CSV 文件示例。

```
OBJECT_TYPE,%FRIENDLY_NAME%,DESCRIPTION,ENDPOINT_TYPE,HOST,LOGIN_USER,
PASSWORD,URL,CONFIGURATION_FILE,DOMAIN,IS_ACTIVE_DIRECTORY,USER_DOMAIN,ENDPOI
NT

ENDPOINT,Oracle1,oracle 10g,Oracle Server,TEST10,
ORAADMIN1,ORAADMIN1,jdbc:oracle:thin:@TEST10:1521:RNDSRV,,,,,

ENDPOINT,local MSSQL1,local SQL server,MS SQL Server,
localhost,testAdmin,Password1@,jdbc:sqlserver://localhost:1433,,,,,

ENDPOINT,SSH_Device2,unix machine,SSH Device,TEST84,root,Password1@,,,,,,

ENDPOINT,IM_Access Control,Access Control via provisioning,Access
Control,TEST1,,,,,,,,TEST1
```

更多信息：

各种类型的 SSH 设备 XML 配置文件 (p. 171)
如何创建自定义的 SSH 设备端点 (p. 170)

创建特权帐户 CSV 文件

特权帐户 CSV 文件中标头行之后的每一行都表示一个在 CA Access Control 企业管理 中创建或修改特权帐户的任务。

重要说明！ 当创建 CSV 文件时，请确认没有其他应用程序使用该文件且该文件能够被重命名。 PUPM 导送程序仅处理能够重命名的 CSV 文件。

请按下列步骤操作：

1. 创建一个 CSV 文件，并以恰当的名称命名。

   注意：建议您创建特权帐户 CSV 示例文件的一份副本。 示例文件位于以下目录，其中 *ACServer* 是您安装企业管理服务器的目录：

   ACServer/IAMSuite/AccessControl/tools/samples/feeder

2. 创建指定特权帐户属性名称的标头行。

   特权帐户属性的名称如下所示：

   OBJECT_TYPE

   指定要导入的对象的类型。

   值：ACCOUNT_PASSWORD

   操作_类型

   指定要执行的操作类型

   值：CREATE、MODIFY、DELETE

   ACCOUNT_NAME

   定义您想在 CA Access Control 企业管理 上引用特权帐户的名称。

   注意：大型机系统（例如 RACF、ACF 和 Top Secret）和“SSH 设备”端点类型使用的用户名区分大小写。使用正确的大小写形式输入这些端点类型的帐户名称。 使用大写字母输入大型机系统和 Oracle Server 端点上的特权帐户的帐户名称。

   ENDPOINT_NAME

   指定特权帐户所在的端点的名称。 您必须定义 CA Access Control 企业管理 中的端点，然后才能创建该端点的任何特权帐户。

   NAMESPACE

   指定该端点的端点类型。

   注意：您可以查看 CA Access Control 企业管理 中可用的端点类型。 在创建“CA Identity Manager 配给”类型的端点之前，您必须在 CA Access Control 企业管理 中创建“Identity Manager 配给”类型的连接器服务器。

CONTAINER

指定特权帐户的容器的名称。容器是一个类，其实例是其他对象的集合。容器采用一种遵循特定访问规则的有组织的方式来存储对象。

值：（Windows Agentless 和 Oracle Server 端点）：Accounts

（SSH 设备端点）：SSH Accounts

（MS SQL Server 端点）：MS SQL Logins

DISCONNECTED_SYSTEM

指定特权帐户是否起源于断开的系统。

如果您指定 TRUE，PUPM 则不管理该帐户。而会仅充当断开系统的特权帐户的密码存储库。每次当您更改 PUPM 中的密码时，也在受管理的端点上手工更改帐户密码。

值：TRUE、FALSE

EXCLUSIVE_ACCOUNT

指定是否仅有单个用户可以在任何时候签出帐户。

如果您指定 TRUE，PUPM 则仅让单个用户在任何时候签出帐户。

值：TRUE、FALSE

NEW_PASSWORD

指定特权帐户的密码。 如果您不指定该属性的值，CA Access Control 企业管理 会生成一个遵守指定密码策略的密码。

注意：密码必须遵守密码策略。

PASSWORD_POLICY

指定特权帐户的密码策略。

注意：如果您指定的密码策略不存在，任务则会失败，而 CA Access Control 企业管理 也不会创建特权帐户。

OWNER_INFO

指定帐户所有者的名称。

DEPARTMENT_INFO

指定部门名称。

CUSTOM1....5_INFO

指定多达五个特定客户属性。

3. 将任务行添加到 CSV 文件中。

   每一行都表示一个创建或修改特权帐户的任务，并且必须有与标头行相同数量的属性值。 如果某行没有某属性的值，则保留该字段为空。

4. 将文件保存到轮询文件夹。

   特权帐户 CSV 文件已准备就绪，可供 PUPM 导送程序导入。

   注意：默认的轮询文件夹位于以下目录，其中 *JBoss_home* 是您安装 JBoss 的目录：

   JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/waitingToBeProcessed

示例：特权帐户 CSV 文件

以下是特权帐户 CSV 文件示例。 您可以在 *ACServer*/IAMSuite/AccessControl/tools/samples/Feeder 目录中找到更多的特权帐户 CSV 文件示例。

```
OBJECT_TYPE,ACCOUNT_NAME,ENDPOINT_NAME,NAMESPACE,CONTAINER,
DISCONNECTED_SYSTEM,EXCLUSIVE_ACCOUNT,NEW_PASSWORD,PASSWORD_POLICY

ACCOUNT_PASSWORD,demo1,local windows 2003,Windows Agentless,
Accounts,FALSE,FALSE,Password1@,default password policy

ACCOUNT_PASSWORD,demo2,local windows 2003,Windows Agentless,
Accounts,FALSE,FALSE,,default password policy

ACCOUNT_PASSWORD,disconnected1,local windows 2003,Windows Agentless,
Accounts,TRUE,FALSE,Password1@,default password policy
```

手动开始轮询任务

当轮询任务开始时，PUPM 导送程序会上传轮询文件夹中的 CSV 文件。 然后 CA Access Control 企业管理 会处理 CSV 文件中的每一行。

注意：如果您不手动启动轮询任务，PUPM 导送程序会在导送程序属性文件所指定的时间检查轮询文件夹。 您必须有系统管理员或 PUPM 目标系统管理员角色才能启动轮询任务。

手动启动轮询任务

1. 在 CA Access Control 企业管理 中，执行如下操作：
   a. 单击“特权帐户”。
   b. 单击“帐户”子选项卡。
      此时“导送程序文件夹轮询”任务会显示在可用任务列表中。
2. 单击“导送程序文件夹轮询”。
   此时出现“导送程序文件夹轮询”屏幕。
3. 单击“提交”。
   PUPM 导送程序在轮询文件夹中轮询 CSV 文件。

如何设置密码使用方

密码使用方是指使用特权帐户和服务帐户来执行脚本、连接到数据库或管理 Windows 服务、排定任务或 RunAs 命令的应用程序、Windows 服务和 Windows 排定任务。 密码使用方允许您从应用程序脚本中删除硬编码密码，并强制对服务帐户实施密码策略。

有两组密码使用方：

- 按需获得密码的密码使用方－数据库、Windows 运行身份、软件开发工具包
- 密码更改时获得密码的密码使用方－Windows 排定任务、Windows 服务

软件开发工具包密码使用方获得、签出及签入特权帐户密码。 所有其他类型的密码使用方可以获得特权帐户密码，但是不签出或签入密码。

以下过程说明企业中的用户为设置密码使用方而必须完成的任务。 用户必须具有指定角色才能完成流程的每个步骤。 具有“系统管理员”管理角色的用户可以执行此流程中的每个 CA Access Control 企业管理 任务。

要设置密码使用方，用户需执行以下操作：

1. 系统管理员按如下方式配置端点：

   a. 在使用数据库、Windows 运行身份和软件开发工具包密码使用方的端点上安装 CA Access Control。

      系统管理员在安装过程中启用 PUPM 集成功能。

      注意：无需在端点上安装 CA Access Control 即可使用 Windows 排定任务或 Windows 服务密码使用方。

   b. 在使用以下密码使用方的端点上，执行其他配置步骤：

      - 数据库 (JDBC)－准备端点以使用数据库 (JDBC) 密码使用方 (p. 215)。
      - 数据库（ODBC、OLEDB、OCI）－将端点配置为使用数据库（ODBC、OLEDB、OCI）密码使用方 (p. 221)。
      - 数据库 (.NET)－将端点配置为使用数据库 (.NET) 密码使用方 (p. 222)。
      - 软件开发工具包 (CLI)－将端点配置为使用 CLI 密码使用方 (p. 223)。
      - 软件开发工具包 (SDK)－将端点配置为使用 PUPM SDK (p. 226)。

   端点配置为使用密码使用方。

2. PUPM 目标系统管理员角色在 CA Access Control 企业管理 中创建密码策略。 密码策略为特权帐户和服务帐户设置密码规则和密码到期时间间隔。

3. PUPM 目标系统管理员在 CA Access Control 企业管理 中创建端点。端点是由特权帐户和服务帐户所管理的设备。 您可以在 CA Access Control 企业管理 中创建端点，或使用 PUPM 导送程序来导入端点。

   注意：如果在您设置特权帐户时已创建端点，则不执行该步骤。

4. 要创建数据库、Windows 运行身份或软件开发工具包密码使用方，用户应执行以下操作：

   a. PUPM 目标系统管理员在 CA Access Control 企业管理 中发现或创建特权帐户。

      该用户可以在 CA Access Control 企业管理 中发现和创建特权帐户，或使用 PUPM 导送程序导入特权帐户。

b. 系统管理员在 CA Access Control 企业管理 中创建数据库、Windows 运行身份和软件开发工具包密码使用方。

系统管理员将数据库、Windows 运行身份和软件开发工具包密码使用方与特权帐户相关联，这属于创建密码使用方任务的组成部分。

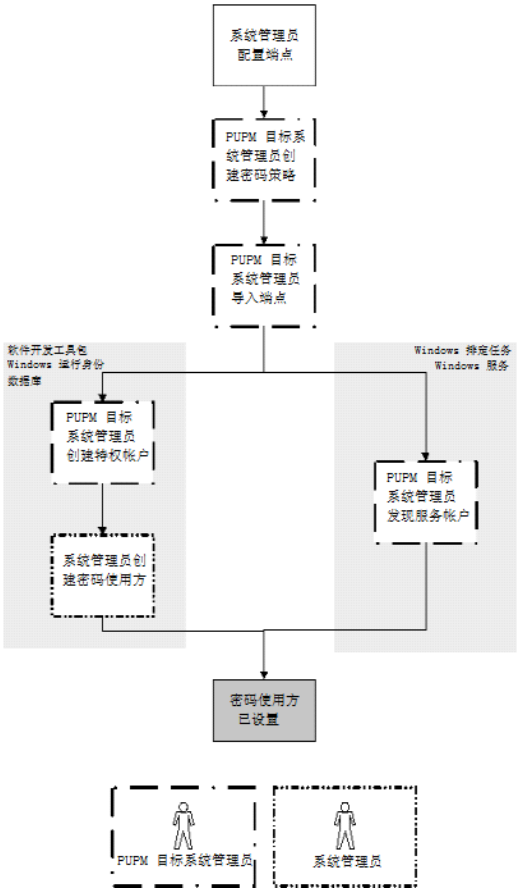
5. 为了创建 Windows 排定任务或 Windows 服务密码使用方，PUPM 目标系统管理员会发现服务帐户。

对于发现的每个服务和排定任务，CA Access Control 企业管理 都会为其创建密码使用方。

注意：CA Access Control 企业管理 仅发现由您可以更改密码的帐户所运行的服务。 例如：CA Access Control 企业管理 发现由您的计算机管理员帐户或域帐户所运行的服务，但不发现由 NT AUTHORITY\Local Service 帐户运行的发现服务。

现在便为您的企业设置了密码使用方。

下图说明执行每个流程步骤的特权访问角色：



发现服务帐户

*服务帐户*是 Windows 服务所使用的内部帐户。 这些服务为计算机提供核心操作系统和其他功能。 利用 CA Access Control 企业管理 管理服务帐户密码，您就可以保护这些服务，使其免受潜在的攻击。

您可以发现在 Windows Agentless 端点上管理服务和排定任务的服务帐户。 发现服务帐户允许您在 CA Access Control 企业管理 中同时创建多个服务帐户，并将密码使用方分配给这些服务帐户。 如果您不想为服务帐户创建密码使用方，则使用“创建特权或服务帐户”任务来创建服务帐户。

注意：要发现特权帐户，请使用“发现特权帐户向导”。

“发现服务帐户向导”不发现端点上的所有服务。 它仅发现由您可以更改其密码的帐户所运行的服务。 例如：CA Access Control 企业管理 发现由您的计算机管理员帐户或域帐户所运行的服务，但不发现由 NT AUTHORITY\Local Service 帐户运行的发现服务。

发现服务帐户

1. （可选）要发现是域帐户的服务帐户，请验证是否在 CA Access Control 企业管理 中定义了帐户所在的域控制器 (DC) 的以下属性：
   - 端点类型－Windows Agentless
   - 是 Active Directory－True
   - 主机域－DC 所属的域名
   - 用户域－DC 上定义的用户所属的域名

     注意：仅当管理帐户来自的域不同于这些帐户所在的域时才会指定用户域。

   “发现服务帐户向导”现在可以发现是域帐户的服务帐户。
2. 在 CA Access Control 企业管理 中，依次选择“特权帐户”、“帐户”、“发现服务帐户向导”。

   将打开“发现服务帐户向导”窗口。

   注意：“端点类型”字段的值是 Windows Agentless，因为 PUPM 仅在 Windows Agentless 端点上管理服务帐户。

3. 选择要搜索的属性，键入筛选值，然后单击“搜索”。

   此时将显示匹配筛选条件的服务帐户的列表，以及使用这些服务帐户的 Windows 服务和排定任务的列表。 如果向导发现来自未知域的帐户，将显示一条警告消息。

   注意：完成该过程会花费一些时间。 服务和排定任务列在“密码使用方”列中。 通过该列中的图标可以看出哪些密码使用方是服务，哪些是排定任务。

4. 选择想要密码使用方来管理的服务和排定任务，然后单击“下一步”。

   此时出现“常规帐户属性”窗口。

5. 选择要分配给服务和排定任务的密码策略，然后单击“下一步”。

   此时出现“摘要”窗口。

6. 查看摘要然后单击“完成”。

   如果没有出错，CA Access Control 企业管理 会提交任务并添加服务帐户。 在 CA Access Control 企业管理 添加服务帐户之后，它会自动为您选择的每项服务和排定任务创建密码使用方。 您可以使用合适的密码使用方任务来查看和修改密码使用方。

更多信息：

创建特权或服务帐户 (p. 145)
发现特权帐户 (p. 143)

创建密码使用方

密码使用方是指使用特权帐户和服务帐户来执行脚本、连接到数据库或管理 Windows 服务、排定任务或 RunAs 命令的应用程序、Windows 服务和 Windows 排定任务。

有两组密码使用方：

- 按需获得密码的密码使用方－软件开发工具包、数据库、Windows 运行身份

  注意：您必须在启用了“PUPM 集成”功能的 PUPM 端点上安装 CA Access Control 才能使用按需获取密码的密码使用方。

- 密码更改时获得密码的密码使用方－Windows 排定任务、Windows 服务

请提供不同信息以从各个组创建密码使用方。 默认情况下，您必须有系统管理员角色才能创建密码使用方。

注意：如果您创建类型为软件开发工具包、数据库和 Windows 运行身份的密码使用方，则需要完成该任务。 建议您使用“发现服务帐户向导”来创建 Windows 排定任务或 Windows 服务密码使用方。

创建密码使用方

1. 在 CA Access Control 企业管理 中，依次单击“特权帐户”、“密码使用方”、“创建密码使用方”。

   此时出现“创建密码使用方: 登录应用程序搜索屏幕”页面。

2. （可选）按如下方式选择一个现有密码使用方来创建密码使用方作为其副本：

   a. 选择“创建类型为‘密码使用方’的对象副本”。

   b. 选择要搜索的属性，键入筛选值，然后单击“搜索”。

      此时将显示匹配筛选条件的密码使用方的列表。

   c. 选择要用作新密码使用方基础的对象。

3. 单击“确定”。

   此时出现“创建密码使用方”任务页面。 如果密码使用方是从现有对象创建的，则对话框字段中会预先填充来自现有对象的值。

4. 填写“常规”选项卡中的以下字段：

名称

定义要用来指代此密码使用方的名称。

说明

（可选）定义要为该密码使用方记录的信息（自由文本）。

使用方类型

指定该密码使用方的类型。

应用程序路径

（软件开发工具包、数据库、Windows 运行身份、Windows 排定的任务）在端点上定义密码使用方的完整路径名。

- 对于软件开发工具包密码使用方，指定执行密码请求的应用程序的路径名。
- 对于数据库密码使用方，指定连接到数据库的应用程序的路径名。
- 对于 Windows 运行身份密码使用方，指定用户执行的应用程序的路径名。
- 对于 Windows 排定任务密码使用方，指定排定任务的路径名。

注意：您可以在路径名中使用通配符 (*) 和 CA Access Control 变量，例如：<!AC_ROOT_PATH>\bin\acpwd.exe。

服务名称

（Windows 服务）定义 Windows 服务的路径名。 指定路径名，使之与 Windows 服务属性页面中的路径名完全相同。

已启用

指定启用密码使用方，也就是说，PUPM 接受来自该使用方的请求，或对该使用方强制实施密码更改。

状态

（Windows 排定任务或 Windows 服务）指出上次密码更改成功还是失败。

最后的同步日期

（Windows 排定任务或 Windows 服务）显示最后成功的密码同步。

重新启动

（Windows 服务）指定是否在密码更改之后重新启动 Windows 服务。

5. 单击“特权帐户”选项卡，并指定与密码使用方相关联的特权帐户。

   如果您创建软件开发工具包、数据库或 Windows 运行身份类型的密码使用方，该密码使用方可以获得您指定的特权帐户的密码。

   如果您创建 Windows 排定任务或 Windows 服务类型的密码使用方，PUPM 会在这些特权帐户的密码发生更改时，强制为密码使用方更改密码。

6. 指定可以使用密码使用方的实体。 请执行下列操作之一：

   - 要创建软件开发工具包、数据库或 Windows 运行身份类型的密码使用方，请执行以下操作：

     a. 单击“主机”选项卡，并指定密码使用方可以从中获得特权帐户密码的主机或主机组，或选择“所有主机”，以授予所有主机或主机组访问特权帐户密码的权限。

        注意：可以在“名称”字段中键入主机或主机组的名称，或者单击“...”以搜索 CA Access Control 主机或主机组（HNODE 或 GHNODE 对象）。

     b. 单击“用户”选项卡，并指定可以请求特权帐户密码的用户或组，或选择“所有用户”，以使每个用户都请求特权帐户密码。

        指定端点上显示的用户或组的名称，例如：DOMAIN\user1。不要指定 CA Access Control 企业管理 用户或组。

   - 要创建 Windows 排定任务或 Windows 服务类型的密码使用方，请单击“端点”选项卡，并指定要在上面创建密码使用方的端点。

7. 单击“提交”。

   CA Access Control 企业管理 会创建密码使用方。

更多信息：

各种类型的密码使用方 (p. 113)

密码使用方示例：Windows 运行身份

通过 Windows RunAs 应用程序，用户可以借用特权帐户的权限以便执行特定任务。 您可以创建“Windows 运行身份”密码使用方,以便当用户执行 RunAs 时，PUPM 代理向 RunAs 应用程序直接提供特权帐户密码。“Windows 运行身份”密码使用方免除了用户知晓特权帐户密码来执行管理任务的需要。

您仅可以在 Windows Agentless 端点上创建“Windows 运行身份”密码使用方。

在下列示例中，备份任务被排定为每周运行一次。 该任务位于 C:\backup\backup.exe 并由管理员运行。 如果排定备份失败，系统管理员 Steve 想让用户 John 手工开始备份。 Steve 可以使用“Windows 运行身份”密码使用方让 John 在没有管理员密码的情况下开始备份任务。

以下过程说明了 Steve 和 John 在名为 win123_PUPM 的端点上创建和使用“Windows 运行身份”密码使用方所执行的步骤：

1. Steve 在 win123_PUPM 上安装启用了“PUPM 集成”功能的 CA Access Control。
2. Steve 在 CA Access Control 企业管理 中执行以下操作：
   a. 创建名为 win123_PUPM 的 Windows Agentless 端点。
   b. 在 win123_PUPM 端点上发现 Administrator 特权帐户。
   c. 使用以下参数创建“Windows 运行身份”密码使用方：
      - 名称 — win123_PUPM Backup RunAs
      - 使用者类型 — Windows 运行身份
      - 应用程序路径 — C:\backup\backup.exe
      - 帐户 — Administrator
      - 主机 — win123_PUPM
      - 用户 — Domain1\John

        注意： Steve 输入端点上显示的 John 的用户名。

   “Windows 运行身份”密码使用方已创建。
3. 排定的备份任务失败，然后 John 登录到 win123_PUPM 手工开始备份。 他使用以下参数执行 RunAs 命令开始备份任务：
   - 帐户 — Administrator
   - 密码 — 无密码

     注意： PUPM 代理忽略 John 针对密码提供的任何值。

   PUPM 代理会检查 John 先前所提出的开始备份任务请求的缓存。 因为这是 John 首次提出该请求，因此没有缓存该请求。 PUPM 代理从 CA Access Control 企业管理 检索特权帐户密码，并将其提供给 RunAs 应用程序。 备份任务开始。

密码使用方示例：Windows 排定任务

“Windows 排定任务”和“Windows 服务”密码使用方帮助您自动化服务帐户的密码更改。 服务帐户是 Windows 服务使用的内部帐户。 例如，如果您配置排定任务定期检查软件更新，排定任务则使用服务帐户登录到端点并执行该任务。

您仅可以在 Windows Agentless 端点上创建“Windows 排定任务”和“Windows 服务”密码使用方。 无需在端点上安装 CA Access Control 就可使用“Windows 服务”和“Windows 排定任务”密码使用方。

您仅可以为由您可以更改其密码的帐户运行的服务创建“Windows 服务”密码使用方。 例如，您可以为由您计算机的 Administrator 帐户运行的服务创建密码使用方；您不能为由 NT AUTHORITY\Local Service 帐户运行的服务创建密码使用方。

在下列示例中，系统管理员 Steve 想为某排定任务创建密码使用方，该排定任务检查名为 win456 的 Windows 端点上的软件更新。 排定任务使用 win456\ServiceAdmin 帐户登录到该端点。

Steve 在 CA Access Control 企业管理 中执行以下操作：

1. Steve 创建名为 30days 的密码策略。 该密码策略指定，CA Access Control 企业管理 每 30 天为服务帐户更改一次密码，并且仅可在周日的上午 1 点到上午 3 点之间更改密码。
2. Steve 创建名为 win456 的 Windows Agentless 端点。
3. Steve 使用服务帐户发现向导来发现 win456 端点上的 win456\ServiceAdmin 帐户，并将 30days 密码策略应用于该服务帐户。
4. CA Access Control 企业管理 使用以下参数创建“Windows 排定任务”密码使用方：
   - 名称 — win456 上的 UpdateTask (C:\WINDOWS\Tasks\UpdateTask.bat)
   - 使用者类型 — Windows 排定任务
   - 应用程序路径 — C:\WINDOWS\Tasks\UpdateTask.bat
   - 特权帐户 — win456\ServiceAdmin
   - 端点 — win456

   Steve 已创建密码使用方。 CA Access Control 企业管理 每次更改 win456\ServiceAdmin 帐户的密码时，JCS 都会登录到 win456 端点并更改软件更新排定任务的密码。 如果密码更改不成功，Steve 可以使用“同步密码使用方”任务来重试密码更改。

更多信息：

同步密码使用方 (p. 238)

PUPM 自动登录

通过 PUPM 自动登录，您可以签出特权帐户密码并一步登录到 PUPM 端点。 PUPM 自动登录不会在您签出后显示密码，但是会使用密码让您自动登录到端点上的特权帐户。 您可以在签出后在 CA Access Control 企业管理 中查看密码。

重要说明！ 您仅可以在 Microsoft Internet Explorer 浏览器中使用 PUPM 自动登录。

要管理自动登录，请在 CA Access Control 企业管理 中创建登录应用程序。 登录应用程序使用脚本在用户的计算机上打开一个窗口，并让用户登录到其签出的特权帐户。 例如，如果您使用 PuTTY 登录应用程序签出“SSH 设备”端点上的 root 帐户，CA Access Control 企业管理 会在您的计算机上打开一个 PuTTY 窗口，并让您登录到该端点上的 root 帐户。

自动登录的工作原理

通过 PUPM 自动登录，您可以签出特权帐户密码并一步登录到 PUPM 端点。

以下过程说明了 PUPM 如何让您自动记录到端点。 您必须在 CA Access Control 企业管理 中创建登录应用程序并将其分配给 PUPM 端点，然后才能开始该过程：

1. 签出特权帐户密码并选择 CA Access Control 企业管理 用来登录到端点的登录应用程序。
2. 如果您的计算机中没有安装 ActiveX，会发生以下情况：
   a. CA Access Control 企业管理 将 ActiveX 包发送到您的计算机。
   b. 安装 ActiveX。

      如果不安装 ActiveX，您无法自动登录到端点。
3. 一旦 ActiveX 安装完毕，ActiveX 会将在登录应用程序中定义的脚本文件从企业管理服务器下载到您的计算机。

   该脚本文件包含特权帐户密码。 脚本文件运行、连接到端点并自动输入特权帐户的凭据。

   注意： ActiveX 不在您的计算机上保存脚本文件。

4. 此时打开终端、Windows 远程桌面或 Internet 浏览器窗口。

   您登录到端点上的特权帐户。

5. 当完成该会话时，会发生以下情况之一：

   - 如果您在关闭远程窗口之前签入特权帐户密码，PUPM 会发送通知，告知它将在宽限期之后关闭窗口。 宽限期过后，PUPM 关闭窗口并结束该会话。

     注意：宽限期在脚本文件中有所定义。 您可以自定义脚本文件以延长或缩短宽限期。

   - 如果您关闭远程窗口并且没有签入特权帐户密码，PUPM 会发送通知，询问您是否想要签入密码。

更多信息：

创建登录应用程序 (p. 179)

如何自定义 PUPM 自动登录应用程序脚本

您可以通过自定义 PUPM 自动登录应用程序脚本来增强 PUPM 自动登录能力。 您使用 PUPM 自动登录 SDK 来创建自定义脚本，使用户能够自动地登录到端点。

以下过程说明自定义自动登录应用程序脚本的方式：

1. 创建 Visual BASIC 脚本

   您可以使用标准 COM 对象或 ACLauncher ActiveX 方式创建脚本。

2. 在 CA Access Control 企业管理 中配置登录应用程序，并将创建的脚本与应用程序关联

3. 将登录脚本与端点关联

更多信息：

PUPM 自动登录应用程序 Visual BASIC 脚本 (p. 206)

PUPM 自动登录应用程序 Visual BASIC 脚本

PUPM 自动登录应用程序使用 Visual Basic 脚本来启用自动用户登录。 您可以自定义 Visual Basic 脚本，以便创建新登录应用程序或修改现有登录应用程序。

从企业管理服务器下载到客户端计算机时，PUPM 自动登录应用程序脚本会包含 ActiveX 以值替换的变量。 企业管理服务器处理脚本，并以值替换关键字。 然后，ActiveX 执行客户端计算机上的脚本。

PUPM 自动登录应用程序脚本位于以下目录：

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

元素

PUPM 登录应用程序脚本包含以下键：

#host#

指定用户自动登录到的端点名称

#username#

指定签出特权帐户

#password#

指定要签出的特权帐户密码

#userdomain#

(Active Directory) 指定特权帐户域名

#isActiveServletUrl#

指定 ACLauncher ActiveX 用于检查帐户密码签入事件的 URL。

#CheckinUrl#

在用户注销端点的情况下，指定 ACLauncher ActiveX 用于签入帐户密码的 URL。

#SessionidUrl#

如果会话记录在 ObserverIT Enterprise，指定 ACLauncher ActiveX 用于发送已记录会话 ID 的 URL。

PUPM 自动登录应用程序脚本的以下片段显示变量如何出现：

```
Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")
hwnd = pupmObj.LauncheRDP("#host#", "#userDomain#\#userName#", "#password#")
' Set window close event
pupmObj.SetWindowCloseEvent(hwnd)
' Set server checkin event
pupmObj.SetServerCheckinEvent("#isActiveServletUrl#")
' Wait until one of the events signaled
rc = pupmObj.WaitForEvents()
If rc = 1 Then 'user has closed the window - notify the server side
        pupmObj.SendCheckinEvent("#CheckinUrl#")
ElseIf rc = 2 Then 'timeout elapsed - close the window
    call pupmObj.CloseWindow(hwnd, 0)
ElseIf rc = 3 Then 'the account was checkedin at the server side - close the window
    call pupmObj.CloseWindow(hwnd, 120)
End If
```

结构

PUPM 自动登录应用程序脚本结构如下所示：

- COM 对象的初始化

  ```
  Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")
  ```

- 自动登录应用程序的执行

  ```
  hwnd = pupmObj.LauncheRDP("#host#", "#userDomain#\#userName#",
  "#password#")
  ```

- Post execution tasks—password check in, interactive login or timeout

  ```
  ' Wait until one of the events signaled
  rc = pupmObj.WaitForEvents()
  If rc = 1 Then 'user has closed the window - notify the server side
      pupmObj.SendCheckinEvent("#CheckinUrl#")
  ElseIf rc = 2 Then 'timeout elapsed - close the window
      call pupmObj.CloseWindow(hwnd, 0)
  ElseIf rc = 3 Then 'the account was checkedin at the server side - close the
  window
      call pupmObj.CloseWindow(hwnd, 120)
  End If
  ```

要记录登录应用程序会话，请将记录说明添加到脚本中，如下所示：

- 在初始化部分， 添加以下内容：

```
Set observeIT = CreateObject("ObserverIT.AgentAPI.Proxy")
```

- 在应用程序执行部分，添加以下内容：

```
'Get application processid
processID = pupmObj.GetWindowProcessID(hwnd)
'Start recording
sessionid = observeIT.StartByProcessID(processID, true)
'Send the sessions if to the ENTM server
pupmObj.AssignSessionID "#SessionidUrl#" ,sessionId
```

- 在后执行部分，添加以下内容：

```
'Stop recording

observeIT.StopBySessionId sessionId, true
```

方法

ACLauncher ActiveX 使用以下方法：

```
LauncheRDP (BSTR bsHostName, BSTR bsUserName, BSTR bsPassword, VARIANT
*phWindow);
```

启动带有输入凭据的远程桌面会话并返回远程桌面窗口句柄

示例： Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test.LauncheRDP("hostname.com", "hostname\administrator", "password")

```
LaunchePUTTY (BSTR bsHostName, BSTR bsUserName, BSTR bsPassword, VARIANT
*phWindow);
```

启动带有输入凭据的 PuTTY 会话并返回 PuTTY 窗口句柄

示例： Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test。 LaunchePUTTY ("hostname.ca.com", "root", "password")

```
LaunncheProcessAsUser (BSTR bsApplication, BSTR bsCommandline, BSTR bsUsername,
BSTR bsPassword, VARIANT *phWindow);
```

启动带有输入凭据的过程并返回过程窗口句柄

示例： Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test.LauncheProcessAsUser("cmd.exe", "/k echo This console is run under %USERNAME% account...", "administrator" , "password")

```
GetWindowProcessID(VARIANT *phWindow, LONG *pProcessID);
```

返回指定窗口句柄的过程 ID

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") id = test.GetWindowProcessID(hwnd) test.Echo "Process ID = " & id

```
GetWindowTitle(VARIANT *phWindow, BSTR *pbsTitle);
```

返回指定窗口句柄的标题 ID

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") title = test.GetWindowTitle(hwnd)

```
CloseWindow(VARIANT *phWindow, LONG Seconds);
```

显示对话框，消息指定窗口将在 X 秒内关闭，并关闭指定窗口句柄的窗口

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.Sleep(5000) test.CloseWindow(hwnd, 60)

```
SetTimeoutEvent(LONG seconds);
```

为“WaitForEvents”方法指定超时。 一旦到达超时值，WaitForEvents 方法则从其阻止调用返回一个返回值，表示到达超时

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetTimeoutEvent(10)

```
SetWindowCloseEvent(VARIANT *phWindow);
```

指定“WaitForEvents”方法的窗口闭事件。 关闭窗口之后，“WaitForEvents”方法从其阻止调用返回并显示返回值，这些返回值表示窗口已关闭

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetWindowCloseEvent(hwnd)

```
SetServerCheckinEvent(BSTR bsURL);
```

将 PUPM 签入事件设置为块执行条件。 每 5 秒 ActiveX 查询 PUPM

示例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetServerCheckinEvent("http://server.com/__azy?djfhwek5jy34brfhwkeb") (replace with variable)

```
WaitForEvents(VARIANT *pRetVal);
```

阻止脚本执行，直到注册条件之一正确。

选项：1－用户已关闭窗口，2－已用超时时间，3－在服务器端密码签入

示例：Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetServerCheckinEvent("http://server.com/__azy?djfhwek5jy34brfhwkeb")

test.SetWindowCloseEvent(hwnd) test.SetTimeoutEvent(360) rc = test.WaitForEvents() If rc = 3 Then call test.CloseWindow(hwnd, 10) End If

```
SwitchToThisWindow(VARIANT *phWindow);
```

定位 Z 顺序顶端的窗口

示例：Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SwitchToThisWindow(hwnd)

```
SendCheckinEvent(BSTR bsURL);
```

用户关闭窗口时，发送签入事件

示例：Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password")

```
Sleep(LONG milliseconds);
```

暂停脚本执行

Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.Sleep(2000)

```
Echo(VARIANT* pArgs);
```

打印消息到屏幕

Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.Echo("Password Checkin")

高级登录

高级登录是自动登录的一种，让您可以签出在某个端点上定义的特权帐户并使用该账户登录到其他端点。 通过高级登录，您可以使用自动登录签出在 Active Directory 中定义的特权帐户。

例如，您在 Active Directory 中定义名为 example1 的 UNAB 端点，并将 example1 用户和组（包括 root）迁移到 Active Directory。 您将 root 用户定义为 CA Access Control 企业管理 中的特权帐户。 如果您在签出 root 时使用了自动登录，您则会登录到定义了 root 帐户的端点，这是 Active Directory 域控制器。 您在签出 root 时使用了高级登录，您可以选择登录到 example1 端点。

CA Access Control 企业管理 显示您已分配登录应用程序的每个端点的高级登录选项。 一旦将登录应用程序分配给端点，您不需要执行其他步骤即可配置高级登录。

终端集成

通过终端集成，您可以将您的 CA Access Control 端点与 PUPM 相集成，以便跟踪使用特权帐户的用户的活动。 仅当用户签出特权帐户密码并使用自动登录登录到 CA Access Control 端点时，终端集成才起作用。

终端集成使您可以提高安全性和责任制，如下：

- 要提高安全性，您可以指定用户必须使用 PUPM 自动登录来登录到端点。
- 要提高责任制，您可以指定当 CA Access Control 写入审核记录和作出授权决策时，要使用最初用户名，而不是特权帐户用户名。

如果您指定当 CA Access Control 写入审核记录和作出授权决策时要使用最初用户名，CA Access Control 会累积登录对话的审核模式。 累积的审核模式使用最初用户的审核模式和特权帐户的审核模式。 如果最初用户没有在 CA Access Control 数据库中定义，CA Access Control 会累积默认用户的审核模式和特权帐户的审核模式。

例如，您为某端点配置终端集成。 在该端点上，user1（最初用户）的审核模式是“失败”，而名为 privileged_user 的特权帐户的审核模式是“成功”。 当 user1 使用自动登录作为 privileged_user 登录到端点时，CA Access Control 将该登录对话的审核模式设为“失败，成功”。

您仅可以在安装了 CA Access Control 的“Windows Agentless”和“SSH 设备”端点上使用终端集成。 此外，用户必须使用自动登录签出特权帐户密码。

默认情况下，当您安装启用了“PUPM 集成”功能的 CA Access Control 时，会启用终端集成。 在安装 CA Access Control 之后，使用 CA Access Control 端点管理 配置端点上的终端集成。

示例：登录事件审核记录

以下示例显示了您配置终端集成的帐户的登录事件审核记录。 您指定用户必须使用 PUPM 自动登录来登录到端点。

事件类型：登录尝试
状态：已拒绝
用户名：example1\administrator
终端：example1.domain.com
程序：终端服务
日期：2010 年 5 月 27 日
时间：17:35
详细信息：该帐户需要自动登录
用户登录会话 ID：7dd2b3dc-8a1a-4ffa-8e7d-f9bc20d2b341
审核标志：OS 用户

示例：资源访问审核记录

以下示例显示了您配置终端集成的帐户的资源访问审核记录。 您指定当 CA Access Control 写入审核记录和作出授权决策时，要使用最初用户名，而不是特权帐户用户名。 最初用户名 (user1) 列在用户名字段中，而特权帐户 (administrator) 列在有效的用户名字段中。

事件类型：资源访问
状态：已拒绝
类：FILE
资源：C:\tmp\core.txt
访问：执行
用户名：domain\user1
终端：example1.domain.com
程序：C:\WINDOWS\system32\cmd.exe
日期：2010 年 2 月 02 日
时间：14:20
详细信息：没有允许访问的步骤
用户登录会话 ID：7dd2b3dc-8a1a-4ffa-8e7d-f9bc20d2b341
审核标志：OS 用户
有效的用户名：example1\administrator。

更多信息：

配置终端集成 (p. 229)
终端集成的实施注意事项 (p. 214)

终端集成的工作原理

通过终端集成，您可以将您的 CA Access Control 端点与 PUPM 相集成，以便增加提高安全性和责任制。

以下过程说明了终端集成的工作原理：

1. 用户使用自动登录签出 CA Access Control 企业管理 中的特权帐户密码。
2. CA Access Control 企业管理 从 DMS 检索端点详细信息，并将一条登录前消息发送到消息队列。 消息中包含特权帐户的名称、签出该帐户的用户的名称以及端点的名称。
3. CA Access Control 端点上的 PUPM 代理在消息队列中检索登录前消息。
4. 当用户使用特权帐户登录到端点时，CA Access Control 授权引擎会检查特权帐户的本地数据库记录并采取以下操作：
   a. 引擎会检查该帐户在登录前是否需要签出帐户，即用户是否必须使用自动登录才能登录到端点。 将会发生以下情况之一：
      - 如果需要签出帐户而 PUPM 代理没有收到特权帐户的登录前消息，引擎会拒绝该登录尝试。
      - 如果需要签出帐户而 PUPM 代理没有已收到特权帐户的登录前消息，引擎会在没有其他限制的情况下允许登录，例如，不存在防止登录的 TERMINAL 限制。
      - 如果不需要签出帐户，引擎会在没有其他限制的情况下允许登录。
   b. 引擎会检查是否必须使用用户原来的身份进行授权决策。 将会发生以下情况之一：
      - 如果必须使用用户原来的身份，引擎将使用最初用户名来评估资源访问请求并写入审核记录。
      - 如果不使用用户原来的身份，引擎将使用特权帐户名称来评估资源访问请求并写入审核记录。

更多信息：

配置终端集成 (p. 229)
终端集成的实施注意事项 (p. 214)

终端集成的实施注意事项

在实施终端集成之前，请考虑以下内容：

- 您可以在安装了 CA Access Control 的“Windows Agentless”和“SSH 设备”端点类型上配置终端集成。 您不能在其他端点类型上配置终端集成。
- (UNIX) CA Access Control 必须将 PAM 登录拦截用于用来连接端点的登录程序。 例如，如果用户使用 SSH 连接端点，CA Access Control 必须使用 PAM 登录拦截来拦截 SSH 登录。

  要指定 CA Access Control 将 PAM 登录拦截用于登录程序，请在登录程序的 LOGINAPPL 记录中设置 loginflags(pamlogin) 标记。 例如：

  ```
  editres loginappl SSH loginflags(pamlogin)
  ```
- 您仅能为特权帐户登录启用终端集成。 登录集成对服务帐户登录不起作用。
- 仅当您使用自动登录签出特权帐户时，终端集成才起作用。
- (UNIX) 您仅能将终端集成用于 SSH 登录。 存在该限制是因为终端集成只有在用户使用 PUPM 自动登录来签出特权帐户密码并登录到 CA Access Control 端点时才起作用，PUPM 仅提供 SSH 登录的登录脚本。

  如果您编写自定义脚本来创建其他登录类型的登录应用程序，并想启用其他登录类型的终端集成，请为相应的登录程序设置 LOGINAPPL 记录的 loginflags(pamlogin) 属性。

更多信息：

配置终端集成 (p. 229)

第 7 章： 配置 PUPM 端点

此部分包含以下主题：

准备 JBoss 应用程序以便使用数据库 (JDBC) 密码使用方

您可以使用 JDBC 数据库密码使用方来替换使用 JDBC 连接到数据库的应用程序中的硬编码密码。 无论何时应用程序提供密码进行身份验证，PUPM 代理都会从 CA Access Control 企业管理 获取特权帐户密码，并将硬编码密码替换为特权帐户密码。

在配置密码使用方使用的数据库之前，您应当准备端点以便使用 JDBC 密码使用方。

准备 JBoss 应用程序以便使用数据库 (JDBC) 密码使用方

1. 确认已在该端点上安装启用了“PUPM 集成”功能的 CA Access Control，且连接到数据库的应用程序使用 JRE 1.5 或更高版本。

   注意：安装 CA Access Control 的端点上安装了连接到数据库的应用程序。 您不需要在数据库主机上安装 CA Access Control。

2. 如果连接到数据库的应用程序正在运行，请将其停止。
3. 导航到下列目录，其中 *ACInstallDir* 是您安装 CA Access Control 的目录：

   ACInstallDir/SDK/JDBC

4. 找到以下文件：
   - CAJDBCService.sar
   - CAJDBCDriver.jar
   - CAPUPMClientCommons.jar
   - jsafeFIPS.jar

5. 将 CAJDBCService.sar 复制到下列目录，其中 *JBOSS_HOME* 是您安装 JBoss 的目录：

   JBOSS_HOME/server/default/deploy

6. 将文件 CAJDBCDriver.jar、CAPUPMClientCommons.jar 和 jsafeFIPS.jar 复制到下列目录：

   JBOSS_HOME/server/lib

7. 在企业管理服务器上，找到您为密码使用方定义的数据源 XML 文件。

8. 打开文件进行编辑。 请执行下列操作之一：

   - 针对 Microsoft SQL Server 自定义数据源配置文件 (p. 216)
   - 针对 Oracle 自定义数据源配置文件 (p. 217)

   自定义数据源配置文件以便指定数据库连接设置和数据源类。

9. 启动 CA Access Control。

   您已经配置端点以使用密码使用方。 现在，必须为 CA Access Control 企业管理 中的应用程序创建密码使用方。 创建密码使用方之后，启动该应用程序。

更多信息：

密码使用方示例：JDBC 数据库 (p. 218)
创建密码使用方 (p. 199)

针对 Microsoft SQL Server 自定义数据源配置文件

您可以配置 JDBC 数据库密码使用方来替换使用 JDBC 连接到 Microsoft SQL Server 数据库的应用程序中的硬编码密码。 已准备端点以使用 JDBC 密码使用方之后，请完成下列步骤。

针对 Microsoft SQL Server 自定义数据源配置文件

1. 找到 <driver-class> 标记，并将默认值替换为 JDBC 驱动程序类属性。 例如：

   ```
   <driver-class>com.ca.ppm.clients.jdbc.CAJDBCDriver</driver-class>
   ```

2. 找到 <connection-url> 标记，并将默认值替换为数据库连接设置。 例如：

   ```
   <connection-url>>@@@com.microsoft.sqlserver.jdbc.SQLServerDriver@@@jdbc:sqlserver://SQLServer1:1433;selectMethod=cursor;DatabaseName=tempdb</connection-url>
   ```

3. 启动 CA Access Control。

   您已将数据源配置文件自定义到 Microsoft SQL Server。 现在，必须为 CA Access Control 企业管理 中的应用程序创建密码使用方。 创建密码使用方之后，启动该应用程序。

针对 Oracle 自定义数据源配置文件

您可以配置 JDBC 数据库密码使用方来替换使用 JDBC 连接到 Oracle 数据库的应用程序中的硬编码密码。 已准备端点以使用 JDBC 密码使用方之后，请完成下列步骤。

针对 Oracle 自定义数据源配置文件

1. 找到 <xa-datasource-class> 标记，并将默认值替换为 CAJDBCDataSource 类属性。 例如：

   ```
   <xa-datasource-class>com.ca.ppm.clients.jdbc.CAJDBCDataSource</xa-datasource-class>
   ```

   重要说明！ 属性名必须与默认值保留相同的大小写形式。

2. 找到所有的 <xa-datasource-property name=> 标记。 例如：

   ```
   <xa-datasource-property
   name="URL">jdbc:oracle:oci8:@tc</xa-datasource-property>
   <xa-datasource-property name="User">scott</xa-datasource-property>
   <xa-datasource-property name="Password">tiger</xa-datasource-property>
   ```

3. 将这些属性组合到单个字符串中。 例如：

   ```
   <xa-datasource-property
   name="CAJDBCProperties">CAJDBCPropertyRealDatasourceClass="oracle.jdbc.xa.client.OracleXADataSource";URL="jdbc:oracle:oci8:@tc";User="scott";Password="tiger";</xa-datasource-property>
   ```

4. 启动 CA Access Control。

   您已为 Oracle 自定义了数据源配置文件。 现在，必须为 CA Access Control 企业管理 中的应用程序创建密码使用方。 创建密码使用方之后，启动该应用程序。

密码使用方示例：JDBC 数据库

在该示例中，系统管理员 Steve 使用 JBoss 应用程序服务器来运行包含明文密码的应用程序。 应用程序使用明文密码来验证到 Microsoft SQL Server 数据库的连接。 Steve 想修改 JBoss 应用程序服务器，以便每次当该应用程序连接到数据库时，都会从 PUPM 获取特权帐户密码。

Steve 已在 Windows 端点上安装了 JBoss 应用程序服务器版本 4.2.3.GA 和 Java Development Kit (JDK) 1.6.0_19。 端点被命名为 JBossEndpoint。 名为 JBossEndpoint\Administrator 的用户使用 run.bat 文件来启动 JBoss 应用程序服务器，该服务器上运行连接到 Microsoft SQL Server 数据库的应用程序。 应用程序使用 sa 帐户连接到数据库。

1. Steve 在 JBossEndpoint 上执行以下操作：
   a. 停止 JBoss。
   b. 安装启用了“PUPM 集成”功能的 CA Access Control。
   c. 导航至以下目录：

      ```
      C:\Program Files\CA\AccessControl\\SDK\JDBC
      ```

   d. 找到以下文件：
      - CAJDBCService.sar
      - CAJDBCDriver.jar
      - CAPUPMClientCommons.jar
      - jsafeFIPS.jar
   e. 将文件 CAJDBCService.sar 复制到下列目录：

      ```
      C:\jboss-4.2.3.GA\server\default\deploy
      ```

   f. 将文件 CAJDBCDriver.jar、CAPUPMClientCommons.jar 和 jsafeFIPS.jar 复制到下列目录：

      ```
      C:\jboss-4.2.3.GA\server\default\lib
      ```

   g. 导航至以下目录：
      ```
      C:\jboss-4.2.3.GA\server\default\deploy
      ```
   h. 打开下列文件进行编辑：
      - imworkflowdb-ds.xml
      - objectstore-ds.xml
      - reportsnapshot-ds.xml
      - userstore-ds.xml

i. 找到 <driver-class> 标记，并将默认值替换为 JDBC 驱动程序类属性。 例如：

```
<driver-class>com.ca.ppm.clients.jdbc.CAJDBCDriver</driver-class>
```

j. 找到 <connection-url> 标记，并将默认值替换为数据库连接设置。 例如：

```
<connection-url>>@@@com.microsoft.sqlserver.jdbc.SQLServerDriver@@@jdbc:sqlserver://SQLServer1:1433;selectMethod=cursor;DatabaseName=tempdb</connection-url>
```

k. 保存并关闭文件。

l. 启动 CA Access Control。

2. Steve 在 CA Access Control 企业管理 中执行以下操作：

a. 创建名为 JBossEndpoint_PUPM 的“Windows Agentless”类型的端点。

b. 在 JBossEndpoint_PUPM 端点上发现 sa 特权帐户。

c. 使用下列参数创建数据库密码使用方：

- 名称 — JBossEndpoint MS SQL 连接
- 使用者类型 — 数据库 (ODBC/JDBC/OLEDB/OCI)
- 应用程序路径 — C:\jboss-4.2.3.GA\bin\run.bat
- 帐户 — sa
- 主机 — JBossEndpoint
- 用户 — JBossEndpoint\Administrator

3. JBossEndpoint\Administrator 用户通过运行 run.bat 文件启动端点上的 JBoss 应用程序服务器。

JBoss 应用程序服务器启动，而应用程序尝试连接到 SQL Server。 PUPM 代理拦截该连接尝试，并向应用程序提供特权帐户密码。

4. Steve 在下列目录的 JBoss 日志文件中检查错误：

```
C:\jboss-4.2.3.GA\server\default\log
```

Oracle 数据库的其他信息

Tnsnames.ora 文件是 Oracle 配置文件，定义客户端用来连接到 Oracle 数据库的数据库地址。 Tnsnames.ora 文件可能包含多个主机名、端口、服务名称、实例名称或 SID。

PUPM 解析 $ORACLE_HOME 和 $TNS_ADMIN 环境变量，以便解析 tnsnames.ora 文件的完整路径。 环境变量在下列注册表项中有所定义：

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\PlugIns*plugin*\EnvironmentVariables

插件

指定拦截连接尝试的插件的名称。

值：OCIPlg、ODBCPlg、OLEDBPlg

每次当 PUPM 拦截 Oracle 数据库的连接尝试时，都会解析 tnsnames.ora 文件。 如果该文件包含任何这些属性的多个值，PUPM 代理会为每个可能的属性组合创建单独的网络。 PUPM 代理将所有的网络集发送到 CA Access Control 企业管理，CA Access Control 企业管理 获取与网络集最匹配的特权帐户密码。

示例：tnsnames.ora 文件中的网络集

以下内容是 tnsnames.ora 文件的示例：

```
SAMPLE_INSTANCE=
 (DESCRIPTION=
   (SOURCE_ROUTE=yes)
   (ADDRESS=(PROTOCOL=tcp)(HOST=host1)(PORT=1630))    # hop 1
   (ADDRESS_LIST=
     (FAILOVER=on)
     (LOAD_BALANCE=off)                                # hop 2
     (ADDRESS=(PROTOCOL=tcp)(HOST=host2a)(PORT=1630))
     (ADDRESS=(PROTOCOL=tcp)(HOST=host2b)(PORT=1630)))
   (ADDRESS=(PROTOCOL=tcp)(HOST=host3)(PORT=1521))    # hop 3
   (CONNECT_DATA=(SERVICE_NAME=Sales.example.com)))
```

当 PUPM 代理解析该 tnsnames.ora 文件时，会将以下网络集发送到 CA Access Control 企业管理：

- HOST=host1, PORT=1630
- HOST=host2a, PORT=1630
- HOST=host2b, PORT=1630
- HOST=host3, PORT=1521, SERVICE_NAME= Sales.example.com

配置端点以便使用数据库（ODBC、OLEDB、OCI）密码使用方

对于 Windows Agentless 端点有效

您可以使用 ODBC、OLEDB 或 OCI 数据库密码使用方来替换使用 ODBC、OLEDB 或 OCI 连接到数据库的应用程序中的硬编码密码。 当应用程序尝试连接到数据库时，PUPM 代理会拦截该连接尝试，并将硬编码密码替换为从 CA Access Control 企业管理 检索到的特权帐户密码。

应用程序必须驻留在安装了 CA Access Control 的 Windows Agentless 端点上。 如果您想创建 OCI 数据库密码使用方，请确认应用程序使用的是 OCI8 或更高版本。

PUPM 使用不同的插件来拦截每种类型的连接尝试。 例如，OCI 插件拦截使用 OCI 的连接尝试。 下列注册表项控制 CA Access Control 插件的行为：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\PlugIns
```

每个插件的设置位于以下子项中：

- OCI—Instrumentation\PlugIns\OCIPlg
- ODBC—Instrumentation\PlugIns\ODBCPlg
- OLEDB—Instrumentation\PlugIns\OLEDBPlg

配置端点以便使用数据库（ODBC、OLEDB、OCI）密码使用方

1. 确认在端点上安装了 CA Access Control 并启用了“PUPM 集成”功能。

   注意：安装 CA Access Control 的端点上安装了连接到数据库的应用程序。 您不需要在数据库主机上安装 CA Access Control。

2. 在端点上停止 CA Access Control。
3. 在连接类型适当的注册表子项中，执行以下操作：
   - 确认 OperationMode 注册表项的值为 1。

     该注册表项启用了插件。
   - 确认运行应用程序的进程名称是 ApplyOnProcess 注册表项的值。

     该注册表项指定插件应用的进程。 例如，如果您正在为 IIS 应用程序创建密码使用方，请确认 w3wp.exe 是注册表项的值。

     注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

4. 启动 CA Access Control。

   您已经配置端点以使用数据库密码使用方。 现在，必须为 CA Access Control 企业管理 中的应用程序创建数据库密码使用方。

   注意：如果您为 IIS 应用程序创建密码使用方，您必须指定 NT_AUTHORITY\NETWORK SERVICE 和 *hostname*\IUSR_*hostname* 用户可以使用该密码使用方来获取特权帐户密码，其中 *hostname* 是端点的名称。

配置端点以便使用数据库 (.NET) 密码使用方

在 Windows Agentless 端点上有效

您可以使用 .NET 数据库密码使用方来替换使用 .NET 连接到数据库的应用程序中的硬编码密码。 当应用程序尝试连接到数据库时，PUPM 代理会拦截该连接尝试，并将硬编码密码替换为从 CA Access Control 企业管理 检索到的特权帐户密码。

注意：应用程序必须驻留在安装了 CA Access Control 的 Windows Agentless 端点上。

PUPM 使用探查器加载插件来拦截每个连接尝试。 .NET 插件拦截使用 .NET 的连接尝试。 下列注册表项控制 CA Access Control .NET 的行为：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Instrumentation\
.NET\
```

探查器和插件的设置位于以下子项中：

- Profiler—Instrumentation\.NET\Profiler\
- Plugin—Instrumentation\.NET\Profiler\Plugin

配置端点以便使用 .NET 数据库密码使用方

1. 确认在端点上安装了 CA Access Control 并启用了“PUPM 集成”功能。

   注意：安装 CA Access Control 的端点上安装了连接到数据库的应用程序。 您不需要在数据库主机上安装 CA Access Control。

2. 在端点上停止 CA Access Control。

3. 在连接类型适当的注册表子项中，执行以下操作：

   - 确认 OperationMode 注册表项的值为 1。

     该注册表项启用了插件。

     重要说明！ 确认 OperationMode 注册表项针对探查器和插件设为 1。

   - 确认运行应用程序的进程名称是 ApplyOnProcess 注册表项的值。

     该注册表项指定插件应用的进程。 例如，如果您正在为 IIS 应用程序创建密码使用方，请确认 w3wp.exe 是注册表项的值。

     注意：建议您不要自行更改该注册表项的值。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

4. 启动 CA Access Control。

   您已经配置端点以使用数据库密码使用方。 现在，必须为 CA Access Control 企业管理 中的应用程序创建数据库密码使用方。

   注意：如果您为 IIS 应用程序创建密码使用方，请将 NT_AUTHORITY\NETWORK SERVICE 和 *hostname*\IUSR_*hostname* 指定为可以使用该密码使用方来获取特权帐户密码的用户，其中 *hostname* 是端点的名称。

配置端点以便使用 CLI 密码使用方

CLI 密码使用方是一种“软件开发工具包”密码使用方。 您可以使用 CLI 密码使用方将脚本中的硬编码密码替换为特权帐户密码。 CLI 密码使用方表示的脚本可获取、签出或签入特权帐户密码。 脚本会调用 PUPM 代理，该代理从 CA Access Control 企业管理 检索特权帐户密码。

使用 CLI 密码使用方编写 .bat 或 .sh 脚本，这些脚本受限于其功能而无法更改其他文件或脚本。 例如，您可以编写使用 acpwd 实用工具的脚本来手工更新文件中的硬编码密码。 还使用 CLI 密码使用方让用户可以从端点的命令行运行 acpwd 实用工具。

注意：您还可以使用 PUPM SDK 将脚本中的硬编码密码替换为特权帐户密码。 例如，使用 PUPM SDK 编写自定义脚本来替换多个文件中的密码。

配置端点以便使用 CLI 密码使用方

1. 确认在端点上安装了 CA Access Control 并启用了“PUPM 集成”功能。
2. 将以下命令添加到您的脚本中：

   ```
   acpwd {-checkout | -get} -account name -ep name -eptype type [-container name]
   -nologo
   ```

   注意：有关 acpwd 实用程序语法的详细信息，请参阅*《参考指南》*。
3. 修改您的脚本以便使用命令的输出（特权帐户密码）。

   您已经配置端点以使用 CLI 密码使用方。 现在，您必须在 CA Access Control 企业管理 中创建脚本的“软件开发工具包”(SDK/CLI) 密码使用方。

更多信息：

创建密码使用方 (p. 199)

CLI 密码使用方的工作原理

您可以使用 CLI 密码使用方将脚本中的硬编码密码替换为特权帐户密码。 CLI 密码使用方表示的脚本使用 acpwd 实用工具获取、签出或签入特权帐户密码。 还使用 CLI 密码使用方让用户可以从端点的命令行运行 acpwd 实用工具。 了解 CLI 密码使用方的工作原理可帮助您使用 acpwd 实用工具。

注意：要在脚本中或从命令行使用 acpwd 实用工具，您必须首先在 CA Access Control 企业管理 中将脚本或实用工具定义为“软件开发工具包”(SDK/CLI) 密码使用方。 该密码使用方定义允许获取特权帐户密码的用户的列表。

以下过程说明了 CLI 密码使用方的工作原理：

1. 以下列方式之一调用端点上的 acpwd 实用工具：
   - 用户从命令提示符窗口运行该实用工具。
   - 脚本或应用程序服务器运行并调用该实用工具。
2. acpwd 实用工具请求特权帐户密码。 PUPM 代理将该请求转发给 CA Access Control 企业管理 进行授权。
3. CA Access Control 企业管理 将特权帐户密码发送到端点。 PUPM 代理显示该密码，或将密码转发给原始程序并记录确认信息。

4. 您（脚本或应用程序服务器）或 CA Access Control 企业管理 重新签入该帐户密码，而 PUPM 代理会记录确认信息。
5. PUPM 代理会记录签入已成功的确认信息。

   注意：具有数字零 (0) 的确认信息表示 PUPM 代理已成功检索、签出或签入密码。 有关 acpwd 实用程序语法的详细信息，请参阅*《参考指南》*。

示例：获取密码的脚本

以下内容是提取的脚本示例，该脚本在 Windows 上获取特权帐户密码。 该示例假定，PUPM 代理已安装在 CA Access Control 端点上。

该示例脚本尝试使用从 CA Access Control 企业管理 获取的特权帐户密码，在 Windows 注册表中添加和删除条目。

```
set AdminUser=PowerUser
FOR /F "tokens=*" %%i IN ('"C:\Program Files\AccessControl\bin\acpwd.exe" -get
-account PowerUser
 -ep comp1_123 -eptype "Windows Agentless" -container "Windows Accounts" -nologo')
DO SET AdminPassword=%%i
set runasadmin="C:\utils\psexec.exe" -u %AdminUser% -p
%runasadmin% %AdminPassword% REG ADD "HKLM\SOFTWARE\PUPM Registry"
%runasadmin% %AdminPassword% REG DELETE "HKLM\SOFTWARE\PUPM Registry" /F
```

在该示例中，脚本运行 PUPM 代理来获取特权帐户密码。 该脚本包含帐户名称 (*PowerUser*)、端点名称 (*comp1_123*)、端点类型 (*Windows Agentless*)、用户（*Windows 帐户*）的容器名称。 该脚本指示 PUPM 代理仅显示密码，并使用该密码以管理用户身份运行 PsExec 程序来添加和删除注册表项。

如何配置端点以便使用密码使用方 SDK 应用程序

您可以使用密码使用方 SDK 为 CA Access Control 端点编写应用程序。 这些应用程序可获取、签出和签入特权帐户密码，并提供密码缓存和用户身份验证。

当运行应用程序时，应用程序会调用从 CA Access Control 企业管理 获取、签出或签入特权帐户密码的 PUPM 代理。

有两种类型的密码使用方 SDK：

- Java PUPM SDK — 使用该 SDK 可为 Windows 和 UNIX 端点编写 Java 应用程序。

  您编写的 Java 应用程序必须使用 JRE 1.5 或更高版本。

- .NET PUPM SDK — 使用该 SDK 可为 Windows 端点编写 C# 应用程序。

  您必须在端点上安装 .NET Framework 2.0 或更高版本才能使用 .NET PUPM SDK。

要配置端点来使用密码使用方 SDK 应用程序，请执行以下操作：

1. 确认在端点上安装了 CA Access Control 并启用了“PUPM 集成”功能。
2. 使用密码使用方 SDK 示例编写您的应用程序。 您可以在以下位置找到示例：
   - Java PUPM SDK—*ACInstallDir*/SDK/JAVA/Samples/PUPMJavaSDK/src/cpm/ca/pupm/javasdk/Tester.java
   - .NET PUPM SDK—*ACInstallDir*/SDK/DOTNET/Examples

   您已经配置端点以使用密码使用方 SDK 应用程序。 现在，您必须在 CA Access Control 企业管理 中创建应用程序的“软件开发工具包”(SDK/CLI) 密码使用方。

更多信息：

密码使用方 SDK 应用程序获取密码的方式 (p. 135)
Java PUPM SDK (p. 136)
.NET PUPM SDK (p. 137)
创建密码使用方 (p. 199)

运行 Java PUPM SDK 应用程序

在配置端点来使用密码使用方 SDK 应用程序之后，您可以运行该应用程序以便获取、签出和签入特权帐户密码。

运行 Java PUPM SDK 应用程序

1. 确认您已经在 CA Access Control 企业管理 中创建应用程序的密码使用方。
2. 打开命令提示符窗口，然后导航到安装应用程序的文件夹。
3. 运行以下命令：

```
java -cp
PupmJavaSDK.jar;CAPUPMClientCommons.jar;jsafeFIPS.jar;[log4jLib];.
applicationName {explicit | keyvalues} {checkout | checkin} "endpointType"
"endpointName" "accountName" "accountContainer" flags
```

log4jLib

（可选）定义应用程序用来记录运行时事件和信息的 log4j 库的名称。

applicationName

定义 Java PUPM SDK 应用程序的名称。

explicit

指定命令为每个参数都提供明确的值。

keyvalues

指定命令使用密钥对/值对。

checkout

指定应用程序检索（获取或签出）特权帐户密码。

注意：*flags* 参数指定应用程序执行的获取或签出操作。

checkin

指定应用程序签入特权帐户密码。

endpointType

定义特权帐户在其上有所定义的端点的类型。

注意：您可以在 CA Access Control 企业管理 中使用“查看端点类型”任务来查看可用端点类型的列表。 定义端点类型，与其在 CA Access Control 企业管理 中显示的完全一致，例如“通过配给的 SAP R3”。

endpointName

定义特权帐户在其上有所定义的端点的名称。

accountName

定义特权帐户的名称。

accountContainer

定义特权帐户在其中有所定义的容器的名称。

如果特权帐户在容器中没有定义，请指定该参数的“帐户”。

flags

指定应用程序是签出还是获取特权帐户密码。

值：0 — 签出或签入特权帐户密码（GetOnly 标志为假）；1 — 获取特权帐户密码（GetOnly 标志为真）

应用程序对特权帐户密码执行指定操作并显示结果。

注意：您可以使用 semsgtool 实用工具查看 PUPM SDK 数字错误代码的文本说明。 有关 semsgtool 实用程序的详细信息，请参阅《参考指南》。

如何配置端点以便使用 Web 服务 PUPM SDK 应用程序

您可以使用 Web 服务 PUPM SDK 编写签出和签入特权帐户密码的 Java 应用程序。 因为应用程序直接与企业管理服务器进行通信，所以您不需要在应用程序运行的端点上安装 CA Access Control。

在端点上安装以下组件才能使用 Web 服务 PUPM SDK：

- Apache Ant 1.7
- Apache Axis 1.4
- Java SDK 1.4.2
- （可选）集成开发环境 (IDE)

重要说明！ 建议您使用加强的身份验证协议（如 NTLM）来验证应用程序和企业管理服务器之间的连接。

要配置端点以便使用 Web 服务 PUPM SDK，请执行以下操作：

1. 阅读 Web 服务 PUPM SDK 自述文件。

   该自述文件包含有关如何配置环境、生成 Java 示例和运行 Java 示例的说明。 自述文件位于：

   ACServerInstallDir/IAM Suite/Access Control/tools/samples/webservice/Axis

2. 使用 Java 示例编写您的 SDK 应用程序。

   您已经配置端点来使用 Web 服务 PUPM SDK 应用程序。 现在，您必须在 CA Access Control 企业管理 中创建代表应用程序的用户，并为该用户分配适当的特权访问角色。

更多信息：

Web 服务 SDK 应用程序获取密码的方式 (p. 139)
Web 服务 PUPM SDK (p. 138)

配置终端集成

通过终端集成，您可以将您的 CA Access Control 端点与 PUPM 相集成，以便跟踪签出特权帐户的用户的活动。 终端集成还让您指定，用户必须使用自动登录来登录到具有特权帐户的 CA Access Control 端点。

在配置终端集成之前，请验证以下各项：

- CA Access Control 企业管理 中存在您想为其配置终端集成的特权帐户。
- 该端点上已启用终端集成，也就是说，PUPMAgent 部分中的 EnableLogonIntegration 配置设置的值为 1。

  注意：默认情况下，当您安装启用了“PUPM 集成”功能的 CA Access Control 时，会启用终端集成。 如果您启用了终端集成，但是没有对其进行配置，CA Access Control 则不会对任何帐户实施终端集成。
- (UNIX) CA Access Control 将 PAM 登录拦截用于用来连接端点的登录程序。

  例如，如果用户使用 SSH 连接端点，请验证 CA Access Control 是否使用 PAM 登录拦截来拦截 SSH 登录。

  注意：有关 PAM 登录拦截和 LOGINAPPL 类的详细信息，请参阅 *《selang 参考指南》*。

下列步骤说明了如何为单个的特权帐户配置终端集成。 您可以使用策略为在多个端点上具有相同名称的特权帐户配置终端集成。

配置终端集成

1. 在 CA Access Control 端点管理 中，依次单击“用户”选项卡、“用户”子选项卡，然后搜索您想为其配置终端集成的特权帐户。

   注意：有关如何在 CA Access Control 端点管理 中管理用户的详细信息，请参阅*联机帮助*。

2. 选择特权帐户。

   此时出现“修改用户”任务页面的“常规”选项卡。

3. 在“帐户”部分中，选择下列选项中的一项或两项：

   使用原来的身份

   指定当 CA Access Control 写入审核记录并作出授权决策时，使用签出特权帐户的用户的名称，而不是特权帐户用户名。

   在登录前需要签出帐户

   指定用户必须使用自动登录来登录到具有该特权帐户的端点。通过自动登录，用户可以签出密码并从 CA Access Control 企业管理自动登录到端点。

4. 单击“保存”。

   您已为该特权帐户启用和配置终端集成。

示例：配置终端集成的策略

下列策略为名为 administrator 的帐户配置终端集成。 策略指定当 CA Access Control 写入审核记录并作出授权决策时使用最初用户名，还指定用户必须使用自动登录以 administrator 身份登录到端点：

```
editusr administrator pupm_flags(use_original_identity)
editusr administrator pupm_flags(required_checkout)
```

更多信息：

终端集成 (p. 211)
终端集成的工作原理 (p. 213)
终端集成的实施注意事项 (p. 214)

第 8 章： 管理特权帐户

此部分包含以下主题：

强制签入特权帐户密码

可以强制签入当前由一个或多个用户签出的特权帐户密码。

强制签入特权帐户密码

1. 依次单击“特权帐户”、“帐户”、“强制签入”。

   此时将显示“强制签入: 选择特权帐户”页面。

2. 选择要搜索的属性，键入筛选值，然后单击“搜索”。

   此时将显示匹配筛选条件的特权帐户的列表。 通过“由用户签出”列可以知道该特权帐户是否已被签出以及由谁签出。

3. 选择要签入的特权帐户密码，然后单击“选择”。

   此时显示确认消息。

4. 单击“是”确认更改。

   CA Access Control 企业管理 即会提交任务以签入帐户。

自动重置特权帐户密码

使用自动密码重置任务可重置选定特权帐户的密码。 启动时，CA Access Control 企业管理 会根据分配给选定帐户的密码策略为该帐户生成新的密码。

重要说明！ 重置帐户密码时，上一个密码会失效。 使用上一个密码的任何用户都必须签入该帐户再签出该帐户，才能继续登录到受管设备。

注意：该选项对于断开连接的帐户无效。

自动重置特权帐户密码

1. 依次单击“特权帐户”、“帐户”、“自动帐户重置”。

   此时将显示“自动帐户重置: 选择特权帐户”页面。
2. 选择要搜索的属性，键入筛选值，然后单击“搜索”。

   此时将显示匹配筛选条件的特权帐户的列表。
3. 选择要重置的特权帐户密码，然后单击“选择”。

   此时显示确认消息。
4. 单击“是”确认更改。

   CA Access Control 企业管理 即会提交任务以重置帐户密码。

手动重置特权帐户密码

使用手动密码重置任务可重置帐户密码，并手动为特权帐户生成新的密码。 新密码必须符合分配给选定特权帐户的密码策略。

重要说明！ 重置帐户密码时，上一个密码会失效。 使用上一个密码的任何用户都必须签入该帐户再签出该帐户，才能继续登录到受管设备。

强烈建议您仅在管理源自断开端点的特权帐户时使用手动密码重置。 每次更改断开端点的密码时，也要更改 CA Access Control 企业管理 存储的密码。

手动重置特权帐户密码

1. 依次单击“特权帐户”、“帐户”、“手动密码重置”。

   此时将显示“手动密码重置: 选择特权帐户”页面。
2. 选择要搜索的属性，键入筛选值，然后单击“搜索”。

   此时将显示匹配筛选条件的特权帐户的列表。

3. 选择要更改其密码的特权帐户，然后单击“选择”。

   此时将显示“手动密码重置”页面。

4. 键入新密码并进行确认，然后单击“提交”。

   CA Access Control 企业管理 即会提交任务以更改帐户密码。

删除特权帐户异常

*特权帐户异常*让用户可以签出他们无权签出的特权帐户。 一旦 PUPM 批准人批准了特权帐户访问请求，请求人就可以在请求有效期内签出特权帐户。 您可以删除特权帐户异常以防止用户能够签出应用了异常的帐户。 要删除特权帐户异常，您的帐户必须分配了默认的“特权帐户请求”或“PUPM 目标系统管理员”角色，或者分配了包含该任务的等效角色。

删除特权帐户请求

1. 在 CA Access Control 企业管理 中，依次单击“特权帐户”、“异常”和“删除特权帐户异常”。

   此时出现“删除特权帐户异常: 选择特权帐户异常”页面。

2. 针对搜索选择属性，键入筛选器值，然后单击“搜索”。

   此时出现匹配筛选条件的特权帐户异常的列表。

3. 选择您想删除的特权帐户异常，然后单击“选择”。

   此时显示一条确认消息，询问您是否要删除选定的特权帐户异常。

4. 单击“是”。

   特权帐户请求被删除。

手工密码提取

如果应用程序服务器未运行并且 PUPM 不可用，您无法使用 PUPM 来签出特权帐户。 您可以另外使用 pwextractor（PUPM 密码提取实用工具）从数据库导出特权帐户密码。 然后，可以使用密码照常登录到特权帐户，或者备份特权帐户密码。

如果您从数据库提取特权帐户密码，因为 PUPM 不可用，因此您无需在 PUPM 还原时完成任何恢复后继步骤。

在安装企业管理服务器时安装 pwextractor。 默认情况下，CA Access Control 规则不保护 pwextractor，但是您可以编写规则对其进行保护。

要使用 pwextractor，您必须：

- 有权使用数据库表
- 了解 PUPM 用来访问数据库的帐户的用户名和密码

  注意：您在安装企业管理服务器时提供这些凭据。

无论 CA Access Control 企业管理 是否运行以及应用程序服务器是否运行，您都可以使用 pwextractor。 您还可以远程运行 pwextractor。

注意：有关 pwextractor 的详细信息，请参阅 *《参考指南》*。

示例：从 Oracle 数据库提取特权帐户密码

下列示例从 Oracle 数据库提取特权帐户密码，并将输出写入文件 C:\tmp\pwd.txt。 架构名称为 orcl，且数据库位于主机 myhost.example.com。 企业管理服务器安装在 Windows 计算机上：

```
pwextractor.bat -h myhost.example.com -d orcl -t oracle -l joesmith -p P@ssw0rd
-f C:\tmp\pwd.txt
-k
C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\config\com\netegri
ty\config\keys\FipsKey.dat
```

审核特权帐户

您可以搜索和查看有关 CA Access Control 企业管理 执行的特权帐户操作的高级详细信息。 各个详细信息屏幕提供每项任务和事件的其他相关信息。 您可以根据任务的状态取消或重新提交任务。

审核特权帐户

1. 在 CA Access Control 企业管理 中，依次单击“特权帐户”、“审核”。

   此时“审核特权帐户”任务将显示在可用任务列表中。
2. 选择“审核特权帐户”。

   此时将打开“审核特权帐户”任务。
3. 指定搜索条件 (p. 235)，输入要显示的行数，然后单击“搜索”。

   将显示满足您搜索条件的任务。

搜索用于审核特权帐户的属性

要查看已提交进行处理的任务，可以使用“审核特权帐户”中的搜索功能。 您可以根据以下条件搜索任务：

启动人

将启动任务的用户名标识为搜索条件。 根据用户名进行搜索。 要确保您输入了有效的用户名，请使用“验证”按钮。

批准人

将任务批准人姓名标识为搜索条件。 根据用户名进行搜索。 要确保您输入了有效的用户名，请使用“验证”按钮。

注意：如果您选择了“批准任务执行者”条件筛选任务，则默认情况下，也将启用“显示批准任务”条件。

任务名称

将任务名称标识为搜索条件。 可以通过指定条件（例如：等于、包含、始于或终于“任务名称”字段的值）来细化搜索。 例如：您可以选择等于条件，然后在文本字段中输入“创建端点”，以此指定搜索条件“任务名称等于‘创建端点’”。

帐户名称

将帐户名称标识为搜索条件。 可以通过指定条件（例如：等于、包含、始于或终于“帐户名称”字段的值）来细化搜索。 例如：您可以选择等于条件，然后在文本字段中输入“管理员”，以此指定搜索条件“帐户名称等于‘管理员’”。

端点类型

将端点类型标识为搜索条件。 可以通过指定条件（例如：等于、包含、始于或终于“端点类型”字段的值）来细化搜索。 例如：您可以选择等于条件，然后在文本字段中输入 Windows Agentless，以此指定搜索条件“端点类型等于 Windows Agentless”。

端点名称

将端点名称标识为搜索条件。 可以通过指定条件（例如：等于、包含、始于或终于“端点名称”字段的值）来细化搜索。 例如：您可以选择等于条件，然后在文本字段中输入 exampleHost，以此指定搜索条件“端点名称等于 exampleHost”。

事件名称

将事件名称标识为搜索条件。 可以通过指定条件（例如：等于、包含、始于或终于“事件名称”字段的值）来细化搜索。 例如：您可以选择等于条件，然后在文本字段中输入 CheckInAccountPasswordEvent，以此指定搜索条件“事件名称等于 CheckInAccountPasswordEvent”。

任务状态

将任务状态标识为搜索条件。您可以启用“任务状态等于”，然后选择条件，以此选择任务状态。 您可以根据以下条件进一步细化搜索：

- 已完成
- 进行中
- 失败
- 已拒绝
- 部分完成
- 已取消
- 已排定

任务优先级

将任务优先级标识为搜索条件。您可以启用“任务优先级等于”，然后选择条件，以此选择任务优先级。 您可以根据以下条件进一步细化搜索：

低

指定您可以搜索具有低优先级的任务。

中

指定您可以搜索具有中优先级的任务。

高

指定您可以搜索具有高优先级的任务。

提交时间介于

标识要搜索的提交的任务的日期范围。必须提供“提交时间介于”字段中的“起始”和“截止”日期。

显示未提交的任务

标识处于“审核”状态的任务。标识已启动其他任务的任务或还未提交的任务。 如果选中此复选框，将审核并显示所有此类任务。

显示批准任务

标识必须在工作流流程中批准的任务。

更多信息：

任务状态说明 (p. 43)

任务状态说明

已提交的任务处于以下所说明的状态之一。 您可以根据任务的状态执行诸如取消或重新提交任务之类的操作。

注意：要取消或重新提交任务，必须将“查看提交的任务”配置为根据任务状态显示取消和重新提交按钮。

进行中

发生以下任一情况时显示该状态：

- 工作流已启动但尚未完成
- 在当前任务之前启动的任务正在进行中
- 嵌套任务已启动但尚未完成
- 主要事件已启动但尚未完成
- 次要事件已启动但尚未完成

您可以取消处于此状态下的任务。

注意：取消任务会取消当前任务的所有未完成的嵌套任务和事件。

已取消

您取消任何进行中的任务或事件时，将显示该状态。

已拒绝

CA Access Control 企业管理 拒绝工作流流程中的事件或任务时，将显示该状态。 您可以重新提交已拒绝的任务。

注意：重新提交任务时，CA Access Control 企业管理 将重新提交所有已失败或已拒绝的嵌套任务和事件。

部分完成

您取消某些事件或嵌套任务时，将显示该状态。 您可以重新提交部分完成的事件或嵌套任务。

已完成

任务完成时，将显示该状态。 当前任务的嵌套任务和嵌套事件完成之后，该任务才算完成。

失败

任务、嵌套任务或嵌套在当前任务中的事件无效时将显示该状态。任务失败时将显示该状态。 您可以重新提交已失败的任务。

已排定

将该任务排定在稍后的日期执行时，将显示该状态。 您可以取消处于此状态下的任务。

在 PUPM 端点上查看审核事件

如果将您的 PUPM 端点与 CA Enterprise Log Manager 相集成，您可以在端点上记录每个特权帐户会话的审核事件。 在 CA Enterprise Log Manager 报告中收集审核事件，您可以从 CA Access Control 企业管理 查看这些报告。 通过该报告，您可以跟踪特权帐户在用户签出帐户之后执行的操作。

您仅可以查看 CheckOutAccountPasswordEvent 或 CheckInAccountPasswordEvent 事件的 CA Enterprise Log Manager 报告。

在 PUPM 端点上查看审核事件

1. 在 CA Access Control 企业管理 中，依次单击“特权帐户”、“审核”。

   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”任务。

3. 指定搜索条件 (p. 235)，输入要显示的行数，然后单击“搜索”。

   此时显示满足您搜索条件的任务。

4. 对于选定的任务，单击“审核特权帐户”页面中“会话详细信息”列中的图标。

   注意：仅出现 CheckOutAccountPasswordEvent 或 CheckInAccountPasswordEvent 事件的图标。

   此时出现 CA Enterprise Log Manager 报告。 该报告包含您选择的特权帐户会话的审核事件。

5. 单击“预览”。

   该报告关闭，CA Access Control 企业管理 会显示具有任务列表的“审核特权帐户”页面。

更多信息：

PUPM 端点上的审核事件 (p. 118)
如何将 PUPM 端点与 CA Enterprise Log Manager 相集成 (p. 119)

同步密码使用方

CA Access Control 企业管理 中的服务帐户密码更改时，JCS 会尝试更改与该服务帐户关联的每个密码使用方的密码。 如果 JCS 未更改密码使用方的密码，可以使用“同步密码使用方”来重试密码更改。

同步密码使用方

1. 在 CA Access Control 企业管理 中，依次单击“特权帐户”、“密码使用方”、“同步密码使用方”。

   此时将显示“同步密码使用方”任务页面。

2. 选择要搜索的属性，键入筛选值，然后单击“搜索”。

   此时将显示匹配筛选条件的密码使用方的列表。

   注意：“端点类型”字段的值是 Windows Agentless，因为 PUPM 仅在 Windows Agentless 端点上管理服务帐户。

3. 选择要同步的密码使用方，然后单击“提交”。

   JCS 即会尝试更新选定密码使用方的密码。

   注意：JCS 会尝试五次 (5) 更新密码使用方。 如果 JCS 无法更新该密码使用方，它会被标记为不同步，需要您手动同步该密码使用方。

更多信息：

PUPM 将密码更改通知给密码使用方的方式 (p. 115)
密码使用方示例：Windows 排定任务 (p. 203)

还原端点管理员密码

每次更改管理员密码时，PUPM 都会根据密码更改的日期和时间将以前的密码存储在数据库中。 如果在无法连接到端点时从备份还原了端点，则当前管理员密码将与在该端点上设置的管理员密码不同。 要连接并登录到该端点，需要还原管理员密码，以匹配所使用备份的时间段。

还原端点管理员密码

1. 在 CA Access Control 企业管理 中，依次选择“特权帐户”、“端点”、“端点密码还原点”任务。

   此时将打开“端点密码还原点: 搜索端点”屏幕。

2. 选择要搜索的属性，键入筛选值，然后单击“搜索”。

   此时将显示匹配搜索条件的端点的列表。

3. 从该列表中选择一个端点，然后单击“选择”。

   此时将显示端点和管理员帐户详细信息。

4. 从“密码日期”菜单中选择要还原的管理员密码。

   “密码日期”菜单列出了每个密码更改的日期和时间。 选择最接近于所使用备份的日期的密码。

5. 单击“验证”。

   PUPM 即会尝试验证密码。 如果成功，会显示一条确认消息。

6. （可选）选择要重置的其他特权帐户密码。

7. 单击“提交”。

   PUPM 即会还原选定的密码，并将该密码设置为当前管理员密码。 如果您已经选择了其他特权帐户，PUPM 还会还原这些帐户密码。

显示先前的特权帐户密码

如果由于无法连接到端点而从备份还原了该端点，则该端点上的管理员帐户密码将与在 PUPM 数据库中存储的密码不同步。 要登录或连接到该端点，您必须具有所使用备份的时间段内的管理员密码。

每次更改密码时，PUPM 都会存储以前的密码，以便您能够选择以前使用的一个密码来连接到所还原的端点。

显示先前的特权帐户密码

1. 在 CA Access Control 企业管理 中，依次选择“特权帐户”、“帐户”、“显示先前的帐户密码”。

   此时将打开“显示先前的帐户密码: 选择特权帐户”搜索屏幕。

2. 选择要搜索的属性，键入筛选值，然后单击“搜索”。

   此时将显示匹配条件的端点和特权帐户的列表。

3. 从该列表中选择一个特权帐户，然后单击“选择”。

   此时出现一个屏幕，按日期顺序显示帐户详细信息和密码历史记录。

4. 从该列表中选择一个条目，然后单击“显示密码”。

   CA Access Control 企业管理 即会将特权帐户密码显示在屏幕的顶部。 您现在便可以使用该密码登录到端点。

5. 单击“关闭”。

第 9 章： 使用 UNAB

此部分包含以下主题：

UNAB 组件

UNIX 身份验证代理 (UNAB) 包含几个组件，这些组件管理和控制 Active Directory 用户对 UNIX 主机的访问。

- **UNAB 验证代理** — UNAB 验证代理 (uxauthd) 后台进程为与 Active Directory 的连接提供服务，并负责维护与 Active Directory 的安全连接以便进行用户身份验证和登录授权、Active Directory 的主机注册、用户和组迁移，还负责管理本地访问文件等等。
- **uxconsole** — uxconsole 是 UNAB 管理控制台，用来将 UNIX 主机注册到 Active Directory、迁移用户和组以及注册和激活 UNAB。
- **uxpreinstall** — uxpreinstall 实用工具确认 UNIX 计算机是否符合 UNAB 系统要求。 使用 uxpreinstall 实用工具来诊断可能的问题，并针对这些问题建议解决方案。
- **CA Access Control 企业管理** — CA Access Control 企业管理 使您能够从中央位置管理您的 UNAB 主机。 使用 CA Access Control 企业管理，您可以控制 Active Directory 用户对企业中每个 UNAB 主机的访问、管理主机登录授权、解决主机迁移冲突并生成报告。

设置 UNAB 的方式

了解 UNIX 身份验证代理 (UNAB) 如何控制对 UNIX 主机的访问，可在实施和配置过程中对您有所帮助。

在 UNIX 主机上安装 UNAB 之后，您将 UNAB 注册到 Active Directory 并激活 UNAB 来启用 UNIX 端点的企业用户身份验证。 然后，开始将本地用户和组迁移到 Active Directory 的迁移进程。

1. 将 UNIX 主机注册到 Active Directory。

   在这一阶段，UNAB 不拦截任何注册请求。

2. 定义允许或拒绝访问 UNIX 主机的企业用户和组。 通过从 CA Access Control 企业管理 创建登录授权策略来实现此目的。
3. 激活 UNAB 可启用 UNIX 主机的企业用户身份验证。
4. 将其他企业用户和组添加到 UNAB 登录授权策略中以便使新用户能够登录。

   在这一阶段，允许本地用户存储（例如：etc/passwd）中定义的用户以及 UNAB 登录授权策略允许的企业用户进行登录。

5. 将用户和组迁移到 Active Directory 中。

CA Service Desk Manager 验证用户的方式

根据您选择使用的集成模式，在 UNIX 主机上安装和配置 UNAB 之后，用户可以使用其 Active Directory 用户帐户或其本地用户帐户进行登录。

当用户尝试登录到正在运行 UNAB 的 UNIX 主机时，会发生以下情况：

1. 系统提示用户输入 Active Directory 或本地帐户用户名和密码。
2. UNAB 使用 Active Directory、登录授权策略或本地主机访问文件来验证用户凭据，并检查从用户帐户获取的其他信息。
3. 如果用户通过了验证，UNAB 将授予该用户对 UNIX 主机的访问权限。 否则，UNAB 会阻止该用户对主机的访问。

存储在 UNAB 端点上的信息

UNAB 验证用户之后，UNAB 会将以下信息存储在端点上：

- 用户名
- 采用 SHA-1 的哈希密码
- 用户类属性
- 用户帐户控制
- 上次成功登录的时间
- 上次失败登录的时间
- 自上次成功登录以来的失败登录数量

UNAB 将用户详细信息保存到 logon.db 文件中，而 NSS 数据库将用户和组属性保存到 nss.db 文件中，这两个文件都位于以下目录：

```
/opt/CA/uxauth/etc
```

控制主机访问和配置 UNAB 的方式

您可以控制用户和组对 UNIX 主机的访问并从 CA Access Control 企业管理 统一配置您的 UNAB 主机。 通过将访问权仅授予获准登录该主机的用户和组，来控制用户和组对 UNIX 主机的访问。

您以对主机的访问控制相同的配置方式来配置 UNAB 主机。 一次性使用 CA Access Control 企业管理 控制企业中 UNAB 主机的功能，并将其应用于所有主机。

在您分配用户和组登录授权或定义配置标记值之后，CA Access Control 企业管理 在策略中阐明这些信息并执行以下操作：

1. CA Access Control 企业管理 创建包含用户和组或配置参数列表的部署包，并将包分配给策略应用的主机或主机组。
2. CA Access Control 企业管理 将该包转发给分发服务器以便分发给主机。
3. UNAB 从分发服务器检索部署包，安装策略，然后将确认信息发送回 CA Access Control 企业管理。

注意：如果您同时将企业登录策略和 UNAB 登录策略部署到主机，那么企业登录策略要优先于 UNAB 登录策略。

管理 UNAB 登录授权

要控制到 UNAB 主机或主机组的用户登录，需要创建已获得访问权限的用户或组的列表。 然后使用一个策略来阐明此列表，CA Access Control 企业管理 会将此策略分配并部署到选定主机或主机组。 该登录策略名为 login@*hostName*。

注意：您可以使用“部署审核”任务来查看策略的部署状态。

管理 UNAB 登录授权

1. 在 CA Access Control 企业管理 中，执行如下操作：
   a. 单击“策略管理”。
   b. 单击“UNIX 身份验证代理”子选项卡。
   c. 根据需要展开左侧任务菜单中的“主机”或“主机组”树。
      此时出现可用任务列表。
2. 请执行下列操作之一：
   - 单击“管理主机登录授权”。
     此时出现“管理主机登录授权: 主机搜索”屏幕。
   - 单击“管理主机组登录授权”。
     此时出现“管理主机组登录授权: 主机组搜索”屏幕。
3. 键入要修改的主机或主机组的名称，然后单击“搜索”。
   此时将显示匹配筛选条件的主机或主机组的列表。
4. 选择要修改的主机或主机组，然后单击“选择”。
   此时出现“管理主机登录授权: *HostName*”或“管理主机组登录授权: *HostGroupName*”页面。
5. （可选）按如下方式添加用户：
   a. 从下拉菜单中选择“用户”。
   b. 以下列格式键入用户名：*域/用户*。
   c. 单击“添加”。
      所添加的用户会显示在“授权用户和组”列表中。

6. （可选）按如下方式添加组：
   a. 从下拉菜单中选择“组”。
   b. 键入要添加的组的名称。
   c. 单击“添加”。

      所添加的组会显示在“授权用户和组”列表中。
7. （可选）按如下方式删除用户和组：
   a. 在“授权用户和组”列表中选择要删除的用户和组。
   b. 单击“删除”。

      此时会从“授权用户和组”列表删除所选的用户和组。
8. 单击“提交”。

   此时 CA Access Control 企业管理 会为指定主机或主机组分配更新的用户和组列表。

配置 UNAB 主机或主机组

可以定义管理 UNAB 主机和主机组的配置设置。 CA Access Control 企业管理 可帮助您设置 UNAB 配置文件 (uxauth.ini) 或 CA Access Control 配置文件 (accommon.ini) 中的设置值。 在完成将值分配给配置设置之后，CA Access Control 企业管理 会创建一个包含更新的设置值的配置策略，并将其分配给主机或主机组。 该策略名为 config@*hostName*。

注意：您可以使用“部署审核”任务来查看策略的部署状态。

配置 UNAB 主机或主机组

1. 在 CA Access Control 企业管理 中，执行如下操作：
   a. 单击“策略管理”。
   b. 单击“UNIX 身份验证代理”子选项卡。
   c. 根据需要展开左侧任务菜单中的“主机”或“主机组”树。

      此时出现可用任务列表。
2. 请执行下列操作之一：
   - 单击“配置 UNAB 主机”。

     此时出现“配置 UNAB 主机: 主机搜索”屏幕。
   - 单击“配置 UNAB 主机组”。

     此时出现“配置 UNAB 主机组: 主机组搜索”屏幕。

3. 键入要修改的主机或主机组的名称，然后单击“搜索”。

   此时将显示匹配筛选条件的主机或主机组的列表。

4. 选择要修改的主机或主机组，然后单击“选择”。

   此时出现“UNAB 配置: *HostName*”或“UNAB 配置: *HostGroupName*”屏幕。

5. 选择要修改的部分和标记，然后单击“添加标记”。

   此时出现所选的配置标记。

6. 修改配置标记的值。

   注意：有关配置标记的更多信息，请参阅 *《参考指南》*。

7. （可选）选择要修改的其他部分和标记，单击“添加标记”，并根据需要修改配置标记的值。

8. 单击“提交”。

   此时 CA Access Control 企业管理 会设置选定 UNAB 主机或主机组上的配置标记的值。

确认 CA Access Control 企业管理 已将策略提交到主机

在阐明授权和配置列表之后，可以在部署审核选项中确认 CA Access Control 企业管理 已将更改提交到 UNAB 主机。

确认 CA Access Control 企业管理 已将策略提交到主机

1. 在 CA Access Control 企业管理 中，依次选择“策略管理”选项卡、“策略”任务并展开“部署”选项。

   此时会打开部署选项菜单。

2. 选择“部署审核”选项。

   此时会打开部署审核搜索屏幕。

3. 选择要显示的主机和策略，然后单击“执行”。

   查询即会显示搜索结果。

   注意：登录策略包含前缀 **login@**

4. 单击结果行以显示部署状态。

   此时 CA Access Control 企业管理 会显示部署任务的状态和输出。

如何将用户和组迁移到 Active Directory

通过将管理任务合并为单一的管理应用程序，将用户从 UNIX 主机迁移到 Active Directory 简化了 UNIX 主机上的用户和组管理。

要将用户和组迁移到 Active Directory，请执行以下操作：

1. 以仿真模式运行迁移过程。

   在仿真模式下，UNAB 不会将用户或组迁移到 Active Directory。 如果发现冲突，UNAB 将其记录在一个日志文件中，该文件就用户和组属性的可能冲突进行报告。 默认情况下，UNAB 冲突文件 (migrate.conflicts) 位于以下目录：

   ```
   /opt/CA/uxauth/log
   ```

2. 下载该冲突文件。

   您从 CA Access Control 企业管理 中采用 CVS 格式下载来自主机的冲突文件。

   注意：您必须等待下一个排定的报告快照完成才能下载该 CSV 文件。

3. 针对每个想要迁移到 Active Directory 的本地帐户创建 Active Directory 帐户。

   UNAB 仅迁移具有现有的 Active Directory 用户帐户的那些用户。

   注意：当您创建用户帐户时，不需要指定 UNIX 属性。 您不需要在 Active Directory 中创建组，迁移工具会在迁移过程中创建组。

4. 将解决冲突的 CSV 文件上传到主机。

   UNAB 重新开始迁移过程，尝试迁移已解析的帐户和组。

5. 迁移结束后再次查看冲突文件，以确认先前在该文件报告的用户帐户和组已成功迁移。

解决迁移冲突

UNAB 会将在迁移过程中发现的冲突记录到冲突文件中。 此文件详细记录了冲突的原因，这些冲突妨碍了用户和组从本地主机迁移到 Active Directory。

可将冲突文件导出成 CSV 文件，将此电子表格下载到计算机，然后复查并解决这些冲突。 以后可以将此修改过的电子表格上传回 CA Access Control 企业管理，CA Access Control 企业管理 再将其发送到消息队列。 UNAB 会检索文件，并重新启动迁移过程，以迁移以前未迁移的用户和组。

注意：如果迁移主机组，则无法下载冲突文件。 但可以上传修正过的冲突文件来解决迁移过程中的冲突。

解决迁移冲突

1. 在 CA Access Control 企业管理 中，执行如下操作：
   a. 单击“策略管理”。
   b. 单击“UNIX 身份验证代理”子选项卡。
   c. 根据需要展开左侧任务菜单中的“主机”或“主机组”树。

      此时出现可用任务列表。
2. 请执行下列操作之 一：
   - 单击“解决主机迁移冲突”。

     此时出现“解决主机迁移冲突: 主机搜索”屏幕。
   - 单击“解决主机组迁移冲突”。

     此时出现“解决主机组迁移冲突: 主机组搜索”屏幕。
3. 键入要为其解决冲突的主机或主机组的名称，然后单击“搜索”。

   此时将显示匹配筛选条件的主机或主机组的列表。
4. 选择要为其解决冲突的主机或主机组，然后单击“选择”。

   此时出现“UNAB 迁移: *HostName*”或“UNAB 迁移: *HostGroupName*”页面。

5. （可选）按如下方式下载主机迁移的冲突文件并解决冲突：
   a. 选择“下载 UNAB 迁移冲突详细信息”部分中的“导出和下载”链接。

      此时会打开一个对话框窗口。
   b. 导航到保存文件的位置并选择“保存”。

      CSV 文件会下载到指定位置。
   c. 打开 CSV 文件，解决文件中报告的冲突，然后保存并关闭文件。
6. （可选）创建并保存用于解决主机组迁移冲突的 CSV 文件。
7. 按如下方式上传用于解决主机或主机组迁移冲突的 CSV 文件：
   a. 选择“上传 UNAB 迁移解决方案”部分中的“浏览”按钮。

      此时会打开一个对话框窗口。
   b. 浏览至文件，然后单击“打开”。
   c. 单击“上传”。

      此时会上传文件。
8. 单击“提交”。

   CA Access Control 企业管理 会将文件发送到消息队列。 UNAB 从队列检索文件，并重新启动迁移过程，尝试迁移已解决的帐户和组。
9. 迁移结束后再次查看冲突文件，以确认先前该文件中报告的用户帐户和组已成功迁移。

注意：如果在 Active Directory 中存在名称相同的用户或组，则不能迁移用户或组。 例如：如果您尝试迁移名为 g1 的组，但是在 Active Directory 中存在名为 g1 的用户，则 UNAB 无法迁移该组。

示例：UNAB 冲突文件输出

下列示例摘自在迁移过程中创建的 UNAB 冲突文件输出：

```
*** CA UxAuth 迁移工具在 2009 年 7 月 2 日 10:16 找到的冲突详细信息 ***
组“ident”冲突：
    在 Active Directory 中找不到组“ident”，ID“101”。
组“nfsnobody”冲突：
    Active Directory 无法将成员添加到组“nfsnobody”，因为 UNIX 组“nfsnobody”包含不存在于 Active Directory 中的成员。
用户“john”冲突：
    用户“john”，ID“4321”，作为 UNIX 用户“johnm”存在于 Active Directory 中
    为 Active Directory 中的用户“john”分配主要组“555”，且 Unix 主要组是“4321”
    为 Active Directory 中的用户“john”分配主目录“/home/john”，且 Unix 主目录是“/home/johnm”
    为 Active Directory 中的用户“john”分配 shell“/bin/sh”，且 UNIX shell 是“/sbin/nologin”
    用户“john”的主要组“4321”未迁移
```

在该示例中，UNAB 报告了以下冲突：

- 在 Active Directory 中找不到组“ident”
- 组“nfsnobody”成员在 Active Directory 中不存在
- 用户“john”缺少以下属性：
  - 用户名 (john) 与 Active Directory 用户名 (johnm) 相冲突
  - 用户主要组 (4321) 与 Active Directory 组 (555) 相冲突
  - 用户主 UNIX 目录 (/home/johnm) 与 Active Directory 主目录设置 (/home/john) 相冲突
  - 用户 UNIX shell (.sbin/nologin) 与 Active Directory shell 属性 (/bin/sh) 相冲突
  - 用户主要组 (4321) 没有迁移到 Active Directory。

示例：UNAB 冲突解析文件

下列示例摘自您创建用于解决 UNAB 在冲突文件中报告的冲突的 UNAB 冲突解析 CSV 文件。 可使用 CA Access Control 企业管理 将 CSV 文件提交到 UNAB 主机：

解决方案实体类型	解决方案实体名称	解决方案操作	解决方案 AD 映射名称	冲突	UID	主目录	GID	成员属于	成员	GECOS
USER	超级用户		根	组迁移，无 AD	1	/home/superuser/	1			

在本例中，冲突解析 CSV 文件包含以下内容：

- 解决方案实体类型－USER
- 解决方案实体名称－超级用户
- 解决方案 AD 映射名称－根
- 冲突－在 Active Directory 中找不到用户组
- UID－1
- 主目录－/home/superuser/
- GID－1

注意：有关迁移用户的更多信息，请参阅*《实施指南》*。

显示用户信息

UNAB 可以显示有关用户帐户的信息，例如，帐户类型（本地或企业用户帐户）、登录状态（允许或已拒绝）和登录原因。 您可以选择显示本地和企业帐户的列表并显示帐户的详细信息。

显示用户信息

1. 导航到 bin 目录。 默认情况下，该目录在以下路径下：

   ```
   /opt/CA/uxauth/bin
   ```

2. 输入以下任何一条命令：

   ```
   ./uxconsole -manage -find -user <filter>
   ```

   ```
   ./uxconsole -manage -show -detail -user <filter>
   ```

   UNAB 根据您指定的选项显示用户详细信息。

   注意：您可以使用通配符 (*)。

注意：有关 uxconsole 实用程序的详细信息，请参阅 *《参考指南》*。

停止 UNAB

如果安装新版本的 UNAB 或更新操作系统，您需要停止 UNAB。

通过停止 uxauthd.sh 脚本来停止 UNAB。

停止 UNAB

1. 作为 root 用户登录 UNIX 计算机。
2. 导航到 UNAB bin 目录。
3. 输入下面的命令：

   ```
   ./uxauthd.sh -stop
   ```

   UNAB 后台进程即已停止。

查看 UNAB 状态

使用该选项来查看 UNAB 的当前状态。

查看 UNAB 状态

1. 以具有该计算机上的管理权限的用户身份登录到 UNIX 计算机。
2. 导航到 UNAB bin 目录。
3. 运行以下命令。

   ```
   ./uxconsole -status -detail
   ```

   出现一条消息通知您 UNAB 的当前状态。

注意：有关 uxconsole 实用程序的详细信息，请参阅 *《参考指南》*。

UNAB 调试文件

UNAB 配置文件的代理部分（在 uxauth.ini 文件中）定义代理在运行时收集的调试信息。 默认情况下，UNAB 在下列文件中收集调试信息，其中 *UNABInstallDir* 是您安装 UNAB 的目录：

UNABInstallDir/log/debug/agent_debug

只要 UNAB 配置文件中启用了调试机制，那么当 uxauthd 后台进程启动时，UNAB 代理就会将调试消息记录在调试文件中。

当使用 -debug 选项启动 UNAB 时，用户控制台中就会显示一条调试消息。

第 10 章： 创建报告

此部分包含以下主题：

安全标准

随着从纸质运行环境迁移到以电子媒介为主的运行环境，企业面临着电子数据受到本地和远程攻击的极大风险。 为解决此类问题，已经在以下领域实施了若干安全措施：常规全局安全、财务准确性和报告、私人财务信息和个人身份的安全保护、医疗相关信息的保护以及安全最佳实践的美国政府标准。

以下安全标准、法案和要求提供了由 CA Access Control 报告服务执行的最佳实践报告根源的有用总结：

Payment Card Industry Data Security Standard（PCI DSS，支付卡行业数据安全标准）

PCI DSS 是由主要的信用卡公司制订的一种行业标准，用于帮助避免欺诈和黑客攻击等安全问题。 接受、获得、存储、传送或处理信用卡和借记卡数据的公司必须遵守 PCI DSS。

Health Insurance Portability and Accountability Act（HIPAA，健康保险携带和责任法案）

HIPAA 是用于在工人更换或失去工作时保护健康保险范围的美国联邦法律。 HIPAA 还用于保护健康数据的安全性和隐私性。

Sarbanes-Oxley Act（Sarbanes-Oxley 法案）

SOX 是规定财务报告标准的美国联邦法律。 该法案适用于美国所有上市公司的董事会和管理层。

报告类型

您可以采用两种不同的报告类型查看有关 CA Access Control 数据和事件的信息：

- CA Access Control 报告 — 说明哪些用户可以执行哪些操作。

  CA Access Control 报告提供每个端点上 CA Access Control 数据库中的数据的相关信息，即您在端点上部署的规则和策略以及策略偏差。 您在 CA Business Intelligence 和 CA Access Control 企业管理 中查看 CA Access Control 报告。

- 审核报告 — 说明哪些用户执行了哪些操作。

  审核报告提供每个端点上审核日志文件 (seos.audit) 中的数据的相关信息，即有关端点上哪些用户执行了哪些操作的信息。 您在 CA Enterprise Log Manager 和 CA Access Control 企业管理 中查看审核报告。

  注意：有关在 CA Enterprise Log Manager 中查看审核报告的更多信息，请参阅 *《CA Enterprise Log Manager 概述指南》*。

注意：您必须安装和配置其他组件才能查看 CA Access Control 报告和 CA Access Control 审核报告。 有关详细信息，请参阅 *《实施指南》*。

报告服务

通过 CA Access Control 报告服务，您可以在一个中央位置查看每个端点（用户、组和资源）的安全状态。 可以在排定时间或在需要时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。 设置 CA Access Control 报告服务后，该服务将独立运行，从每个端点收集数据并将其报告给中央服务器，然后继续报告端点状态而无需手工干预。

CA Access Control 报告服务对于 BS 7799/ISO 17799、Sarbanes-Oxley (SOX)、Payment Card Industry (PCI)、Health Insurance Portability and Accountability Act (HIPAA)、Federal Information Security Management Act (FISMA) 等环境非常有用。 报告服务提供一种解决方案，使您无论在何种情况下都能了解在数以千计的端点中用户、组和资源访问的真实端点状态。

报告服务经过结构化，使您可以查询从每个端点收集的数据。 可以构建自定义报告用于多种用途，也可以使用 CA Access Control 提供的预先配置好的报告。 由于报告服务基于服务器，因此该服务可使您集中化报告存储和管理，另外还提供对报告的安全访问 (SSL)。 可以配置报告服务以获得高可用性。 可以将报告服务器组件安装在单个服务器上，也可以通过分布式配置的方式进行安装。

注意：报告服务组件不属于 CA Access Control 强制系统，它向现有实施添加价值，而且无需重新配置。

报告服务组件

报告服务包含以下核心组件：

- *报告代理*是一种 Windows 服务或 UNIX 后台进程，在每个 CA Access Control 或 UNAB 端点上运行，并将信息发送到驻留在分发服务器上的已配置消息队列中的队列。
- *消息队列*是分发服务器的组件，配置用来接收报告代理发送的端点信息。 对于报告，消息队列从中央数据库接收并向其转发端点数据库快照。 对于冗余和故障转移，可以使用多个分发服务器收集和转发信息。
- *中央数据库*是关系数据库管理系统 (RDBMS)，保存包括报告功能在内的 CA Access Control 企业管理 功能的信息。 可以使用多种工具查询存储在数据库中有关 CA Access Control 实施的数据。
- *报告门户*是用于服务 CA Access Control 报告的应用程序服务器。 该服务器使用 BusinessObjects InfoView 门户，可使您与存储在中央数据库的报告信息进行交互。
- CA Access Control 企业管理 服务器用于阅读消息队列中的报告数据，并将数据存储在中央数据库中。
- 包含内置报告，可使您轻松显示常用报告方案的数据。
- 您在上面运行 Web 浏览器来查看和管理报告的计算机。

注意：有关 CA Access Control 报告服务实施和体系结构的详细信息，请参阅 *《实施指南》*。

报告服务如何运行

报告服务让您可以检查从每个 CA Access Control 和 UNAB 端点、用户存储和 PUPM 策略存储中收集的数据。 要正确设置报告服务，您需要了解它如何收集、存储数据并通过数据生成报告。

报告服务执行以下操作：

- 从每个 CA Access Control 和 UNAB 端点收集数据。

  每个端点都将报告数据发送到分发服务器上的消息队列。

- 将数据存储在中央数据库中。

  CA Access Control 企业管理 从消息队列中检索报告数据，并将其存储在中央数据库中。

- 捕获报告数据的快照，并将其存储在中央数据库中。

  CA Access Control 企业管理 将 PUPM 报告数据作为快照的一部分捕获。

- 通过存储的数据生成报告。

  一旦中央数据库中有可用数据，使用报告门户来生成报告并查询存储的数据。 报告门户是 CA Technologies 版本的 BusinessObjects InfoView 门户，配置以连接到中央数据库并捆绑现成的 CA Access Control 报告。

注意：有关报告服务体系结构的信息，请参阅 *《实施指南》*。

如何从每个端点收集报告的数据

要生成报告，必须收集每个端点的数据。 报告服务使用安装在每个 CA Access Control 和 UNAB 端点的报告代理，在排定的时间或在需要时从每个端点收集数据。

注意：报告代理还负责收集和传递用于与 CA Enterprise Log Manager 集成的审核数据。 此过程仅对报告代理在端点上进行报告时所执行的操作进行了说明。

报告代理在每个端点上执行以下操作：

1. 执行偏差计算并向分发服务器发送结果。

   重要说明！ 如果将报告代理设置为定期运行且不需要更新 DMS，则您无需另外排定策略偏差计算。

2. 创建 CA Access Control 端点上的 CA Access Control 数据库 (seosdb) 和每个策略模型数据库 (PMDB) 的副本，或创建 UNAB 端点上的 UNAB 数据库的副本。

   这是报告代理创建的临时副本，以便可以在不影响 CA Access Control 性能的情况下处理数据。

3. 将每个数据库的数据转储为 XML 结构。

   这是对数据库中所有对象的转储，这意味着获得所有数据，而不仅仅是通过数据库界面实用程序（例如 selang）可见的数据。

4. 将 XML 版本的数据库发送到分发服务器。

   报告代理会将数据发送到分发服务器上的报告队列。

注意：报告的数据不是从 PUPM 端点上收集的。

如何处理和存储每个端点的数据

在每个端点收集数据后，会将其发送到分发服务器进行处理。 数据经处理后，将发送并存储在中央数据库中，用于生成报告。

分发服务器执行以下操作：

1. 从每个端点上的报告代理接收端点的整个数据库的 XML 转储。
2. 使用 Message Driven Bean (MDB) 根据数据库架构处理 XML 转储。

   每个传入的 XML 转储将转换为 Java 对象，以保存在中央数据库中。

3. 每个 Java 对象均将插入到中央数据库中。

   现在可从中央数据库检索来自每个端点的数据。

注意：端点数据必须由报告门户检索，即捕获在快照中，然后才可包含在报告中。

CA Access Control 企业管理 捕获快照的方式

CA Access Control 企业管理 必须将报告数据捕获在快照中（包括端点转储），然后数据才能在报告中显示。 CA Access Control 企业管理 捕获快照之后，您可以生成和查看 CA Access Control 报告。

CA Access Control 企业管理 会在快照定义中指定的时间执行以下操作来捕获快照：

- 将用户存储中的数据提取到中央数据库中。
- 将 PUPM 策略存储中的数据提取到中央数据库中。
- 为中央数据库中最新的端点快照做标记以便将其包括在快照中。

将端点快照发送到分发服务器

当您配置端点用于报告时，您指定报告代理收集端点上本地 CA Access Control 数据库和任何 PMDB 的排定快照的时间和将快照发送到分发服务器上的报告队列的时间。 如果不想等待排定时间，您可以立即将端点快照发送到分发服务器。

注意：您可以通过更改 accommon.ini 文件或 CA Access Control 注册表项 ReportAgent 部分中的排定配置设置来更改报告代理排定。

按照需要将端点快照发送到分发服务器

1. 在端点上打开命令提示符窗口。
2. (UNIX) 设置库路径环境变量，如下：
   a. 切换到 root 帐户。
   b. 将库路径环境变量设置为 *ACSharedDir*/lib。 默认情况下，*ACSharedDir* 是以下目录：

      ```
      /opt/CA/AccessControlShared
      ```

   c. 导出库路径环境变量。
3. (UNIX) 浏览至以下目录：

   ```
   ACSharedDir/bin
   ```

4. 在端点上运行报告代理。 请执行下列操作之一：
   - (Windows) 运行以下命令：

     ```
     ReportAgent -report snapshot
     ```

   - (UNIX) 运行以下命令：

     ```
     ./ReportAgent -report snapshot
     ```

   报告代理将 CA Access Control 数据库和任何本地 PMDB 的快照发送到分发服务器上的报告队列。

注意：有关为报告配置端点的更多信息，请参阅 *《实施指南》*。 有关 ReportAgent 部分的详细信息，请参阅 *《参考指南》*。 有关库路径环境变量的更多信息，请参阅 *《疑难解答指南》*。

如何在 CA Access Control 企业管理 中查看报告

以下过程说明了如何创建和查看 CA Access Control 报告，此报告提供了有关 PUPM、CA Access Control 和 UNAB 端点以及用户存储的信息。 还可以在 CA Business Intelligence 中查看 CA Access Control 报告。

要在 CA Access Control 企业管理 中查看报告，请执行以下操作：

1. 创建快照定义。

   快照定义指定 CA Access Control 收集的报告数据，并定义快照排定。

2. 确认您已经针对报告配置了 CA Access Control 和 UNAB 端点。

3. （可选）捕获快照数据。

   如果不想等待排定的快照，可以使用“捕获快照数据”任务立即收集快照。

4. 运行报告。

   报告即会创建。

5. 查看报告。

注意：有关创建快照定义以及针对报告配置端点的更多信息，请参阅*《实施指南》*。

捕获快照数据

通常，按照排定的时间间隔在快照中捕获报告数据。 如果您想按需捕获快照数据，请使用“捕获快照数据”任务将数据立即导出到中央数据库。

重要说明！ 如果要导出大量的数据，则导出快照数据可能花费大量的时间。 如果报告快照包含大量数据，建议您创建快照定义来排定您的快照。

注意：默认情况下，您必须具有“系统管理员”角色才能捕获快照数据。

捕获快照数据

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. 单击“捕获快照数据”。

      将显示“捕获快照数据”页面。
2. 选择要捕获的快照定义的名称，然后单击“提交”。

   CA Access Control 企业管理 即会将快照数据导出到中央数据库。

注意：您可以使用“查看提交的任务”任务来检查该任务的进度。 有关创建快照定义的更多信息，请参阅 *《实施指南》*。

在 CA Access Control 企业管理 中运行报告

CA Access Control 报告可提供有关 PUPM、CA Access Control 和 UNAB 端点以及用户存储中的数据的信息。

该报告包括 CA Access Control 企业管理 在快照中捕获的数据。 在 CA Access Control 企业管理 捕获快照之后，快照中的数据便可用于报告。 您必须先运行报告，然后才能对其进行查看。 默认情况下，您必须具有“系统管理员”或“报告”角色才能运行报告；对于要运行的报告，您必须具有特定的“报告”角色。

注意：不能在 CA Access Control 企业管理 中排定周期性报告。 但是，可以在 CA Business Intelligence 中排定周期性报告。 如果在 CA Business Intelligence 中排定报告，则无法在 CA Access Control 企业管理 中查看它；但是，如果在 CA Access Control 企业管理 中运行报告，则可以在 CA Business Intelligence 中查看它。

在 CA Access Control 企业管理 中运行报告

1. 在 CA Access Control 企业管理 中，执行如下操作：
   a. 请单击“报告”。
   b. 单击语言子选项卡。

      语言子选项卡是安装 CA Access Control 企业管理 所使用的语言的名称。 例如：如果用英语安装 CA Access Control 企业管理，则显示“英语”子选项卡。
   c. 在左侧的任务菜单中展开要运行的报告类型树。

      随即将显示报告列表。
2. 选择要运行的报告。

   此时将显示参数屏幕。
3. 提供所需的参数信息。

   输入参数信息时，请考虑以下方面：
   - 如果指定了某一数字参数，但却为该参数输入非数字值，则该报告将失败。
   - 如果指定了某一参数，但是中央数据库中没有该参数的任何值，则该报告为空。

     例如：如果定义了一个或多个用户的相关报告，但是中央数据库中没有任何用户数据，则该报告为空，因为没有要报告的用户数据。

   注意：按 Ctrl 的同时进行单击可选择多个参数。
4. 单击“提交”。

   该报告即被提交至报告服务器。

更多信息：

排定报告 (p. 268)

查看报告

CA Access Control 报告可提供有关 PUPM、CA Access Control 和 UNAB 端点以及用户存储中的数据的信息。 您必须先运行 CA Access Control 报告，然后才能进行查看。

注意：请在浏览器中启用第三方会话 cookie 以在 CA Access Control 企业管理 中查看报告。 默认情况下，您必须具有“系统管理员”或“报告”角色才能查看报告。

查看报告

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. 单击“查看我的报告”。
      此时将显示“查看我的报告: 配置管理报告”屏幕。
2. 搜索要查看的报告。
   此时将显示符合搜索条件的报告的列表。
3. 选择您想要查看的报告。
   报告即会显示。
4. （可选）单击“导出此报告”（左上角）将该报告导出为以下格式：
   - Crystal Reports
   - Excel
   - PDF
   - Word
   - RTF

   报告即会被导出。

管理快照

通过 CA Access Control 企业管理，可以查看、修改及删除快照定义。 当您查看或修改快照定义时，会显示“配置文件”、“重现”和“维护”选项卡。 仅在快照曾被捕获的情况下才会出现“维护”选项卡。

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。

要查看、修改或删除快照定义，请转至“报告”、“任务”、“管理快照定义”，然后单击要执行的任务。

注意：如果某快照定义正在用于将数据导出至中央数据库，则无法删除该快照定义。 删除正在使用的快照定义时，将数据导出至中央数据库的操作会停止，但该快照定义仍可用。

BusinessObjects InfoView 报告门户

*报告门户*是用于服务 CA Access Control 报告的应用程序服务器。 该服务器使用 BusinessObjects InfoView 门户，可使您与存储在中央数据库的报告信息进行交互。

打开 InfoView 以使用报告

使用 BusinessObjects InfoView 访问 CA Access Control 报告。 以下过程说明了如何访问报告界面 (BusinessObjects InfoView)。

打开 InfoView 以使用报告

1. 使用以下方式之一启动 InfoView：
   - 在安装了 BusinessObjects InfoView 的计算机上，依次选择“开始”、“程序”、“BusinessObjects XI 版本 2”、“BusinessObjects Enterprise”、“BusinessObjects Enterprise Java InfoView”。
   - 在任意计算机的浏览器中，导航至以下 URL：

     `http://ACRPTGUI_host:ACRPTGUI_port/businessobjects/enterprise115`

     ACRPTGUI_host - 安装了 InfoView 的计算机的名称或 IP 地址（报告门户）。

     ACRPTGUI_port - 用于访问 InfoView 的端口号，默认情况下为 9085。

   将显示 InfoView“登录”页面。
2. 输入安装 InfoView 时设置的凭据，然后单击“登录”。

   将显示 InfoView“主页”页面。

注意：有关使用 BusinessObjects InfoView 的详细信息，请参阅*《BusinessObjects Enterprise XI 版本 2 InfoView 用户指南》*。

运行报告

打开报告界面 (BusinessObjects InfoView) 后，即可选择并运行报告。

运行报告

1. 打开 InfoView。

   将显示 InfoView“主页”页面。
2. 依次展开“主页”、“公共文件夹”、“CA 报告”，然后单击左框中的“CA Access Control”。

   将显示 CA Access Control 页面。

3. 单击要查看报告的链接标题。

   将显示报告的页面，从中您可以输入其他值来定义要查看报告的范围。

4. 填写表中字段以定义要查看报告的范围，然后单击“确定”。

   将显示报告的输出页面。

   可以执行其他查询以影响报告的生成。 例如，可以包括“全部”从所有已知主机生成报告，也可以选择个别主机从单个主机生成报告。另外，还可以指定一个日期范围，以查看所有历史数据或仅查看特定日期范围内的数据。

   注意：可以使用 %（百分比）符号指定通配符值。 % 的使用是一种标准的 SQL 选择表示法，与其通常在通配符规范中的情况不一样，它*不*代表单个字符。

注意：有关使用 BusinessObjects InfoView 的详细信息，请参阅*《BusinessObjects Enterprise XI 版本 2 InfoView 用户指南》*。

排定报告

运行报告有多种方法。 可以通过单击报告标题并指定值来运行报告，也可以从多个选项中进行选择以排定报告。

排定报告

1. 打开 InfoView。

   将显示 InfoView“主页”页面。

2. 依次展开“主页”、“公共文件夹”、“CA 报告”，然后单击左框中的“CA Access Control”。

   将显示 CA Access Control 页面。

3. 单击要排定报告的标题下方的“排定”。

   将显示所选报告的“排定”页面。

4. 修改“运行对象”下拉列表中的选择，以指定想要所排定报告运行的时间。

5. 展开“参数”区域以指定运行报告所需的值：

   a. 单击“清空”以定义每个参数的值。

      将显示“输入提示值”区域的字段。

   b. 根据需要定义值，然后单击“确定”。

      将保存您所定义的值，以在运行报告时使用。

6. 单击“排定”以根据所选的排定选项运行报告。

   将显示“历史记录”页面，用于确认您设置的报告排定实例。

注意：有关使用 BusinessObjects InfoView 的详细信息，请参阅 *《BusinessObjects Enterprise XI 版本 2 InfoView 用户指南》*。

查看生成的报告

报告生成后，可以通过从 CA Access Control 报告列表中执行以下任一操作来查看报告：

- 单击“查看最新实例”以查看所需报告。
- 单击“历史记录”，然后单击日期和时间以选择要查看的报告实例。

注意：有关使用 BusinessObjects InfoView 的详细信息，请参阅 *《BusinessObjects Enterprise XI 版本 2 InfoView 用户指南》*。

查看报告状态

可通过查看已排定报告的状态来确定该报告是否已成功运行。

查看报告状态

1. 打开 InfoView。

   将显示 InfoView“主页”页面。

2. 依次展开“主页”、“公共文件夹”、“CA 报告”，然后单击左框中的“CA Access Control”。

   将显示 CA Access Control 页面。

3. 单击要查看报告的“历史记录”链接。

   将显示报告的“历史记录”页面，从中您可以查看报告运行的日期和时间的列表。

   该列表中的每个条目将显示以下内容：

   - 实例时间 - 报告运行的日期和时间
   - 标题 - 报告的标题
   - 运行人 - 运行报告的用户的名称
   - 参数 - 为运行该报告而选择的参数
   - 格式 - 报告的输出格式
   - 状态 - 报告的当前状态，例如“成功”
   - 重新排定 - 用于再次运行报告的链接

注意：有关使用 BusinessObjects InfoView 的详细信息，请参阅 *《BusinessObjects Enterprise XI 版本 2 InfoView 用户指南》*。

标准报告

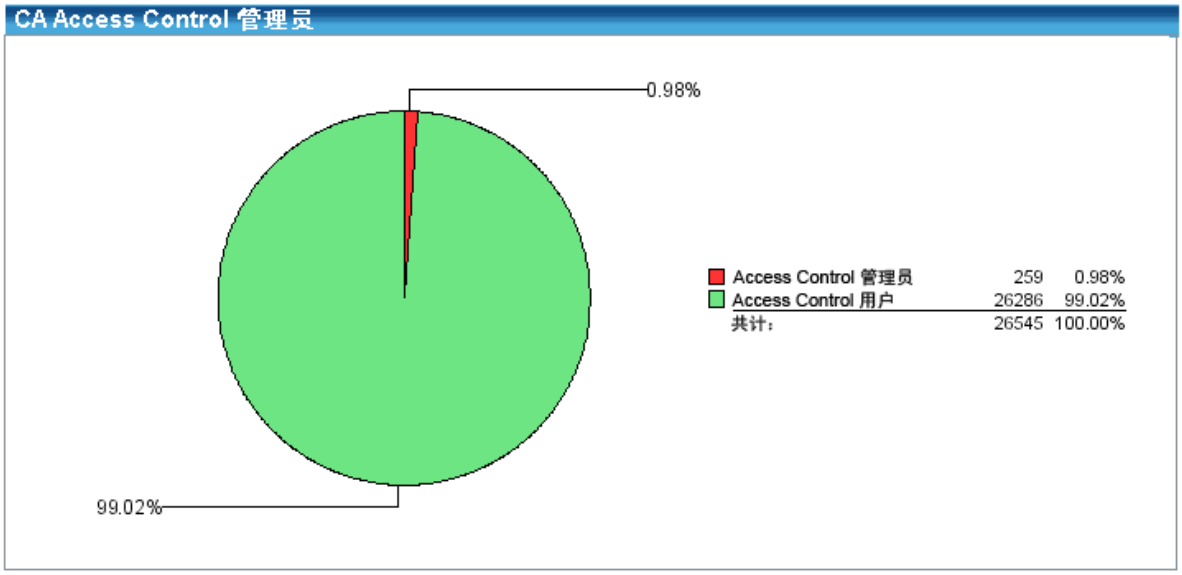
CA Access Control 报告服务附带有标准报告作为报告门户安装的一部分部署，是即时可用的。 报告分成以下类别：

- 帐户管理报告 (p. 272)
- 授权报告 (p. 276)
- 杂项报告 (p. 277)
- 策略管理报告 (p. 279)
- 密码策略报告 (p. 282)
- 特权帐户管理报告 (p. 283)
- UNIX 身份验证代理报告 (p. 288)

除了标准报告，您还可以使用不同功能扩充报告并制作类似的报告，也可以生成全新的报告。

报告的外观

报告输出会在适当时使用表格和图形。 例如，一些报告中包含让人一目了然的饼图，同时仍提供支持详细信息。 如下图中所示，“CA Access Control 管理员”报告提供了一个饼形图，用于指出多少端点用户是 CA Access Control 管理员。 如果管理员数与普通用户数之间的比例很高，则可能会面临安全风险，因此图形会快速显示是否存在安全风险。 在此示例中，图中占大部分的红色楔形具有重要意义，因为它显示了当前企业用户库中接近 1% 的用户均可以执行 CA Access Control 管理。



除了图形之外，每个报告还具有实际端点值的关联列表。 以下是 CA Access Control 管理员报告中此表的示例：

CA Access Control 管理员

用户名	全名	主机识别码	拥有管理员身份	拥有密码管理员身份	拥有操作员身份
_seagent					
		SYSTEMA	是		
		SYSTEMB	是		
		SYSTEMC	是		

帐户管理报告

标准帐户管理报告提供了对用户帐户的概述。

注意：报告标题是报告在 BusinessObjects InfoView 中显示的名称。

以下是标准帐户管理报告的列表：

CA Access Control 管理员

“CA Access Control 管理员”报告显示了具有 CA Access Control 管理权限的所有用户的列表。 这些用户包括具有 ADMIN、PWMANAGER 或 OPERATOR 属性的用户。 报告以饼形图显示摘要数据，以表格格式显示用户名的详细列表。

如果有大量用户均可以管理 CA Access Control，则可能会使企业面临安全风险。 当然，如果所评估的端点处于开发或测试环境中，那么，系统的多数用户是 CA Access Control 管理员是非常正常的。

CA Access Control 组用户成员资格

通过“CA Access Control 组用户成员资格”报告，您可查看用户组及其成员。 该报告以表格格式显示详细信息。

为了简化管理，CA Access Control 环境中的每个用户均可作为一个或多个当前定义的 CA Access Control 组的成员包括在内。 因为资源访问通常适用于组，所以应定期对组成员资格进行复查。

CA Access Control 组

“CA Access Control 组”报告显示组所在的已定义主机、组的说明及该组是否包含任何称为嵌套组的子组。

了解整个企业中有哪些组存在于哪些主机上有助于管理您的环境。 此外，了解哪些组包含其他组，对于确定为什么特定用户或组可以访问特定资源非常有用。

CA Access Control 不活动天数

“CA Access Control 不活动天数”报告显示在指定周期（例如 90 天）内未登录的用户。 还会显示这些用户是处于挂起状态，还是仍然能够访问系统。 该报告包括一个摘要饼形图，其中突出显示了帐户处于不活动状态但已挂起的用户，以及帐户处于不活动状态但未挂起的用户。

所有企业环境中的重要审核点将显示哪些用户当前具有访问环境的权限以及上次访问的时间。 除了显示用户上次访问资源、登录到端点的时间等之外，重要审核点还会显示帐户处于不活动状态的时间。 对于验证服务帐户的访问规律，以及识别在特定时间段内一直处于打开状态但未被访问的帐户，此报告非常有用。

CA Access Control 密码更改

“CA Access Control 密码更改”报告显示了必须在指定时间段内更改密码的用户帐户的列表。 该报告提供了一个摘要饼形图，其中列出了无需更改密码的用户帐户、需要更新密码的用户帐户，以及密码已到期的用户帐户。 该报告还提供详细信息，例如主机 ID 以及用户帐户的密码还剩多少天到期。

与了解到期密码的状态相类似的审核要求，是了解尚未更改密码的用户的列表所必须的。 使用此信息，即可确定可能即将到期的帐户将会面临的安全风险。

CA Access Control 密码到期

“CA Access Control 密码到期”报告显示了未在指定天数内更新密码的用户帐户。 该报告提供了一个摘要饼形图，其中标识了已更新密码的用户帐户、由于密码到期导致系统访问权限挂起的用户帐户，以及密码已到期但仍可访问系统的用户帐户。 该报告提供了未在最近 x 天内更改密码的用户帐户的详细信息，包括主机 ID、上次更改密码日期，以及用户帐户仍可访问系统的原因。

CA Access Control 能够通过提供额外的质量检查以及保留先前密码的历史记录，来增强端点密码保护，从而防止频繁重复使用。 作为此组件的一部分，密码上次更改日期将保留。 通过使用此密码质量模型组件，CA Access Control 可以确定企业中的哪些用户未在指定时间段内更改密码。 此报告的重要性在于，您可以使用它集中确定由于密码到期而导致的企业登录环境中可能存在的弱点。

CA Access Control 密码策略遵从（帐户）

“CA Access Control 密码策略遵从（帐户）”报告显示了密码未遵守密码策略（例如密码长度以及最少数字和字母字符数）的用户帐户。 该报告提供了一个摘要饼形图，其中标识了遵守策略和未遵守策略的用户帐户数。 该报告还以表格格式提供了未遵守策略的用户帐户的详细信息。

CA Access Control 密码策略遵从（主机）

“CA Access Control 密码策略遵从（主机）”报告显示了哪些主机的用户帐户密码未遵守密码策略（例如密码长度以及最少数字和字母字符数）。 该报告提供了一个摘要饼形图，其中标识了遵守策略和未遵守策略的主机数。 该报告还以表格格式提供了未遵守策略的主机以及这些主机上的用户帐户的详细信息。

CA Access Control 责任隔离

“CA Access Control 责任隔离”报告显示了违反责任隔离策略（例如用户不能既是管理员用户组的成员又是审核者用户组的成员）的用户帐户。 该报告提供了一个摘要饼形图，其中比较了遵守策略和未遵守策略的用户数。 该报告还包括未遵守策略的用户帐户的详细信息以及主机 ID。

所有企业环境中的所有端点均需由必须对操作系统和应用程序组件具有访问权限的用户来维护。 通常，系统管理员会从操作系统的角度来维护计算机，而应用程序管理员会从应用程序的角度来维护计算机。 例如，Solaris 系统管理员可以更新 UNIX 主机文件中的条目，而 Oracle DBA 可以维护 Oracle 数据库中的表。

此模型的优点在于，系统管理员危及应用程序安全的能力方面受到限制，而应用程序管理员危及操作系统安全的能力方面也受到限制。 通常，使同一人既为系统管理员又为应用程序管理员的做法并不好。

该报告可帮助识别用户属于代表不同角色的两个组的潜在冲突。 该组交集检测和报告对满足针对 ISO7799、SOX、PCI、HIPAA 和 DoD 的主要审核点之一来说非常有益。

CA Access Control 用户组成员资格

“CA Access Control 用户组成员资格报告”显示环境中每台主机的用户和组成员资格。 报告提供了用户及其所属组的详细信息，按主机排列。

CA Access Control 用户创建日期

“CA Access Control 用户创建日期”报告显示了环境中的指定主机或所有主机上于特定时间段创建的用户帐户。 该报告提供了有关用户帐户创建日期的详细信息，该信息先按主机排列，再按用户帐户排列。

CA Access Control 用户挂起日期

“CA Access Control 用户挂起日期”报告显示了环境中的指定主机或所有主机上于特定时间段挂起的用户帐户。 该报告提供了有关用户帐户挂起日期的详细信息，该信息先按主机排列，再按用户帐户排列。

CA Access Control 用户更新日期

“CA Access Control 用户更新日期”报告显示了环境中的指定主机或所有主机上于特定时间段更新的用户帐户。 该报告提供了有关用户帐户更新日期的详细信息，该信息先按主机排列，再按用户帐户排列。

授权报告

标准授权报告提供了对用户和资源授权的概述。

注意：报告标题是报告在 BusinessObjects InfoView 中显示的名称。

以下是标准授权报告的列表：

CA Access Control 基线资源遵从（主机）

“CA Access Control 基线资源遵从（主机）”报告显示对指定资源具有非默认访问权限的用户帐户。 该报告提供了一个摘要饼形图，其中显示了可进行非默认访问的主机数，以及具有非默认访问权限的用户帐户总数。 该报告还按主机提供了每个具有非默认访问权限的用户帐户的访问权限详细信息。

CA Access Control 组权限

“CA Access Control 组权限”报告显示用户组可以访问的所有资源的列表。 该报告按资源名称，以表格格式显示标识以下内容的详细列表：

- 主机 ID
- 访问权限
- 访问权限是默认授予还是通过使用程序授予
- 任何限制，例如可用日历的名称或其他时间限制
- 是否由于用户组拥有资源而授予访问权限

使用此报告，您可以确定哪些用户组对整个企业中或特定主机的已定义资源具有访问权限。 检查后，您可以决定是否更改访问权限以符合安全策略。

按组列出 CA Access Control 资源访问

“按组列出 CA Access Control 资源访问”报告显示了授予用户组对指定资源的访问权限。 该报告提供了一个对资源具有访问权限的所有用户组的详细列表，其中包括主机 ID、访问权限、是否授予默认访问权限以及其他任何限制条件（例如指定了日期和时间）。

按用户列出 CA Access Control 资源访问

“按用户列出 CA Access Control 资源访问”报告显示了授予用户帐户对指定资源的访问权限。 该报告提供了一个对资源具有访问权限的所有用户帐户的详细列表，其中包括主机 ID、访问权限、是否授予默认访问权限以及其他任何限制条件（例如指定了日期和时间）。

CA Access Control 用户权限

“CA Access Control 用户权限”报告显示用户的访问权限，按资源排列。 对于用户可以访问的每个资源，该报告都提供用户的访问类型、默认访问权限、用户可以用来访问资源的任何程序以及用户访问资源的时间限制。 该报告还指定用户是否是资源所有者。

杂项报告

标准杂项报告提供监控的文件、监控的程序的相关信息，以及 UNIX 主机在不重新启动系统的情况下卸载 CA Access Control 内核的准备情况。

注意：报告标题是报告在 BusinessObjects InfoView 中显示的名称。

以下是标准杂项报告的列表：

CA Access Control 监控的文件 (p. 277)
CA Access Control 监控的程序 (p. 278)
UNIX 主机卸载注意事项 (p. 278)
CA Access Control UNIX 卸载准备情况 (p. 279)

CA Access Control 监控的文件

“CA Access Control 监控的文件”报告显示企业中主机上的重要系统文件的状态。 该报告提供了一个摘要饼形图，其中指出了未在哪些主机上监控文件、在哪些主机上监控了文件但文件已修改，以及在哪些主机上监控了文件但文件仍处于受信任状态。 该报告还提供了文件的详细信息（例如主机 ID），因此您可以检查文件在该主机上的策略，也可以查看对文件的修改是否是由经授权的用户执行。

确保监控重要系统文件对于保护数据的完整性非常重要。 了解文件何时进行了更改可使您进行审核跟踪，因此您可以根据安全策略验证更改是否是由经授权的用户做出。

CA Access Control 监控的程序

“CA Access Control 监控的程序”报告显示了企业中主机上的重要程序的状态。 该报告提供了一个摘要饼形图，其中指出了未在哪些主机上监控程序、在哪些主机监控了程序但程序已修改，以及在哪些主机上监控了程序但程序仍处于受信任状态。 该报告还提供了程序的详细信息（例如主机 ID），因此您可以检查程序在该主机上的策略，也可以查看对程序的修改是否是由经授权的用户执行。

确保监控重要程序对于保护数据的完整性非常重要。 了解程序何时进行了更改可使您进行审核跟踪，因此您可以根据安全策略验证更改是否是由经授权的用户做出。

UNIX 主机卸载注意事项

“UNIX 主机卸载注意事项”报告显示了已拦截系统调用的 UNIX 主机，这些系统调用可能阻止您卸载 CA Access Control 内核。 在这些主机上，您需要重新启动计算机，然后才能卸载内核并升级 CA Access Control。

该报告列出进程和父进程 ID、程序名称、阻拦时间和每台主机卸载注意事项的阈值时间。 该报告还指定每个系统调用是阻拦还是非阻拦。

该报告将主机分为以下类别：

- **未就绪（溢出）** — 系统调用表超出其大小，需要重新启动来卸载内核。
- **未就绪（阻止系统调用）** — 阻止拦截的系统调用存在，需要重新启动来卸载内核。
- **可能（非阻止系统调用）** — 非阻止拦截的系统调用存在，可能不需要重新启动即可卸载内核。

CA Access Control UNIX 卸载准备情况

“CA Access Control UNIX 卸载准备情况”报告显示 UNIX 主机在不重新启动系统的情况下卸载 CA Access Control 内核并升级 CA Access Control 的准备情况。

该报告提供了摘要饼图，显示了准备好可以进行内核卸载、可能准备好进行内核卸载以及没有准备好进行内核卸载的主机的比例。 该报告还提供了每台主机的已拦截和非阻止的系统调用数。

该报告将主机分为以下类别：

- **未就绪（溢出）** — 系统调用表超出其大小，需要重新启动来卸载内核。
- **未就绪（阻止系统调用）** — 阻止拦截的系统调用存在，需要重新启动来卸载内核。
- **可能（非阻止系统调用）** — 非阻止拦截的系统调用存在，可能不需要重新启动即可卸载内核。
- **就绪** — 不存在拦截的系统调用，不需要重新启动即可卸载内核。
- **不适用** — 主机不是 UNIX 主机。
- **未知状态** — 没有提供该主机的任何信息。

策略管理报告

标准策略管理报告提供有关您的 CA Access Control 企业管理 策略的信息。

注意：报告标题是报告在 BusinessObjects InfoView 中显示的名称。

以下是标准策略管理报告的列表：

CA Access Control 策略分配

“CA Access Control 策略分配”报告显示了策略分配的详细信息，这些策略部署到指定 DMS 上定义的主机和主机组上。 该报告显示下列信息：

- 策略名
- 分配类型（主机或主机组）
- 部署策略的主机和主机组的名称

CA Access Control 策略部署记分卡

“CA Access Control 策略部署记分卡”报告显示指定策略的部署信息。 该报告提供摘要饼图以及下列信息：

- 正确部署策略的主机数。
- 部署策略出错或出现偏差的主机数。
- 面临风险（策略分配给主机，但是策略尚未部署到主机）的主机数。

该报告还提供策略部署的任何问题的详细信息，按主机排列。

CA Access Control 策略部署记分卡(按主机)

“CA Access Control 策略部署记分卡(按主机)”报告显示策略的部署信息，按主机排列。 该报告提供摘要饼图以及下列信息：

- 正确部署策略的主机数。
- 部署策略出错或出现偏差的主机数。
- 面临风险（策略分配给主机或主机所属的主机组，但是策略尚未部署到主机）的主机数。

该报告还提供策略部署的任何问题的详细信息，按主机排列。

CA Access Control 策略部署记分卡(按主机组)

“CA Access Control 策略部署记分卡(按主机组)”报告显示策略的部署信息，按主机排列组。 该报告提供摘要饼图以及下列信息：

- 主机组中正确部署策略的主机数。
- 主机组中部署策略出错或出现偏差的主机数。
- 主机组中面临风险（策略分配给主机组，但是策略尚未部署到主机）的主机数。

该报告还提供策略部署的任何问题的详细信息，按主机组排列。

CA Access Control 策略部署状态(按主机)

“CA Access Control 策略部署状态(按主机)”报告显示策略的状态信息，按主机排列。 该报告提供每个策略的版本信息，包括：

- 偏差状态
- 部署时间
- 部署策略的用户的名称。

CA Access Control 策略部署状态(按主机组)

“CA Access Control 策略部署状态(按主机组)”报告显示策略的状态信息，按主机组排列组。 该报告提供每个策略的版本信息，包括：

- 偏差状态
- 部署时间
- 部署策略的用户的名称。

该报告还列出主机组中部署了策略的主机。

CA Access Control 策略清单

“CA Access Control 策略清单”报告显示存储在 DMS 上的策略的快照，包括：

- 每个策略上次更新的时间
- 上次更新策略的用户的名称
- 已部署的策略版本号
- 最后确定的策略版本
- 策略依赖的任何策略的名称

注意：如果策略依赖于其他策略，除非部署了其所依赖的策略，否则无法对其进行部署。

CA Access Control 策略规则

“CA Access Control 策略规则”报告显示策略中每个规则的部署脚本和取消部署脚本，按策略名称排列。 该报告提供了上次更新规则的日期以及上次更新规则的用户的名称。 该报告还指定了该策略是否已最终确定并准备好进行部署，以及策略版本号。

CA Access Control 策略版本

“CA Access Control 策略版本”报告显示每个策略的版本信息，按策略名称排序。 对于每个策略，该报告都提供：

- 当前版本号
- 该版本的部署时间
- 部署当前版本的用户的名称

该报告还指定当前版本是否已最终确定。

CA Access Control 规则偏差(按主机)

“CA Access Control 规则偏差(按主机)”报告显示策略状态和规则偏差，按主机排列。 该报告提供每台主机上的策略列表，以及每个策略的状态、版本和偏差状态。 如果策略存在规则偏差，该报告会提供偏差的详细信息，即偏差应用的资源和属性的详细信息。

CA Access Control 规则偏差(按主机组)

“CA Access Control 规则偏差(按主机组)”报告显示策略状态和规则偏差，按主机组排列。 该报告提供每个主机组上的策略列表，以及每个策略的状态、版本和偏差状态。 如果策略存在规则偏差，该报告会提供该主机组的每个主机成员的偏差详细信息，即偏差应用的资源和属性的详细信息。

密码策略报告

密码策略报告提供有关 CA Access Control 中定义的密码策略的信息。

以下是标准密码策略报告的列表：

CA Access Control 特权帐户(按密码策略) (p. 283)
CA Access Control PUPM 密码策略 (p. 283)

CA Access Control 特权帐户(按密码策略)

该报告显示系统中所有特权帐户的列表及其相应的密码策略。 使用该报告，您可以确定哪些特权帐户与哪个密码策略相关联。 查看该报告之后，您可以确定是否正确分配了密码策略并根据需要采取更正操作。

该报告显示下列信息：

- 快照时间
- 密码策略名称
- 端点类型和名称
- 帐户名称
- 上次签出日期
- 上次密码更改

CA Access Control PUPM 密码策略

该报告会根据复杂性显示当前密码策略。 使用该报告，您可以确定现有密码策略的最大长度和最小长度以及其他策略参数是否符合安全标准。

该报告显示下列信息：

- 快照日期
- 密码策略名称和说明
- 最大长度
- 最小长度
- 密码策略参数

特权帐户管理报告

“特权帐户管理”报告提供特权帐户管理的详细信息视图。

以下是标准特权帐户管理报告的列表：

CA Access Control 特权帐户(按端点) (p. 284)
CA Access Control PUPM 角色和特权帐户(按用户) (p. 284)
CA Access Control 特权帐户请求(按端点) (p. 285)
CA Access Control 特权帐户请求(按批准人) (p. 286)
CA Access Control 特权帐户请求(按请求者) (p. 287)
CA Access Control PUPM 用户(按特权帐户) (p. 287)
CA Access Control PUPM 用户(按角色) (p. 288)

CA Access Control 特权帐户(按端点)

该报告按照端点类型和端点名称列出特权帐户。 使用该报告，您可以根据端点类型和名称查看特权帐户。 查看该报告之后，您可以确定每个端点相关联的特权帐户的数量。

该报告显示下列信息：

- 快照时间
- 端点类型和名称
- 帐户名称
- 上次签出用户
- 上次签出
- 上次密码更改

CA Access Control PUPM 角色和特权帐户(按用户)

该报告根据用户帐户显示特权访问角色和特权帐户的列表。 使用该报告，您可以根据关联角色和用户帐户查看特权帐户。

该报告显示下列信息：

- 快照时间
- 用户 ID
- 端点时间和名称
- 角色名称和说明
- 帐户名称
- 例外
- 上次密码更改

CA Access Control 特权帐户请求(按端点)

该报告按照端点类型和端点名称显示特权帐户请求的列表。 使用该报告，您可以查看为签出特权帐户及其相应的端点类型和名称而提出的请求。

该报告显示下列信息：

- 快照时间
- 端点类型和名称
- 主机名
- 帐户
- 请求者
- 请求理由
- 请求时间
- 批准时间
- 有效自
- 有效截止时间
- 批准人
- 批准人注释

注意：该报告仅显示活动的特权帐户请求。

CA Access Control 特权帐户请求(按批准人)

该报告根据批准人显示特权帐户请求的列表。 使用该报告，您可以查看特权帐户请求（特定用户已批准该请求）。 查看该报告之后，您可以更改批准人角色、分配其他用户或从角色中删除用户。

该报告显示下列信息：

- 快照时间
- 批准人用户 ID
- 端点类型和名称
- 主机名
- 帐户
- 请求者名称和 ID
- 请求理由
- 请求时间
- 批准时间
- 有效自
- 有效截止时间
- 批准人注释

注意：该报告仅显示活动的特权帐户请求。

CA Access Control 特权帐户请求(按请求者)

该报告根据请求特权帐户密码的用户来显示特权帐户请求。 使用该报告，您可以查看用户为签出特权帐户而提出的请求。 查看该报告之后，您可以确定签出请求的数量以及提出的用户。

该报告显示下列信息：

- 快照名称
- 批准人用户 ID
- 端点类型和名称
- 主机名
- 帐户
- 请求理由
- 请求时间
- 批准时间
- 有效自
- 有效截止时间
- 批准人
- 批准人注释

注意：该报告仅显示活动的特权帐户请求。

CA Access Control PUPM 用户(按特权帐户)

该报告根据端点类型和名称显示有权使用特权帐户的用户的列表。 使用该报告，您可以确定用户访问特权帐户的方式和每个特权帐户源自的端点类型和名称。

该报告显示下列信息：

- 快照类型
- 端点类型和名称
- 特权帐户名称
- 用户名
- 用户 ID
- 请求

CA Access Control PUPM 用户(按角色)

该报告显示用户及其相关特权帐户角色的列表。 使用该报告，您可以确定用户与特权帐户角色的关联方式，并决定当前状态是否满足安全标准。

该报告显示下列信息：

- 快照时间
- 角色名称
- 成员数量
- 用户名
- 用户 ID
- 电子邮件地址

UNIX 身份验证代理报告

UNAB 报告提供 UNAB 管理任务的详细信息视图。

以下是标准 UNIX 身份验证代理报告的列表：

CA Access Control UNAB 企业用户访问(按主机)

该报告按主机显示访问 UNAB 主机的企业用户的列表。 该报告向您提供访问每台主机的企业用户、他们上次的登录尝试以及有权访问主机的用户（或组）等相关信息。 查看该报告之后，您可以更改企业用户对主机的访问权限。

CA Access Control UNAB 访问主机(按企业用户)

该报告按用户显示访问 UNAB 主机的企业用户的列表。 该报告向您提供访问每台主机的企业用户、他们上次的登录尝试以及有权访问主机的用户（或组）等相关信息。 查看该报告之后，您可以更改企业用户对主机的访问权限。

CA Access Control UNAB 企业用户

该报告显示获准访问主机的企业用户的列表。 该报告显示当前的企业用户帐户、用户 ID、主目录和 shell 类型。 查看该报告之后，您可以更改用户属性并添加或删除企业用户。

CA Access Control UNAB 企业用户活动

该报告显示迁移和部分迁移的企业用户帐户的活动列表。 使用该报告，您可以查看 UNIX 主机上企业用户的活动。 该报告向您提供最近的成功和失败登录尝试、用户上次执行的成功密码更改等相关信息。

CA Access Control UNAB 企业组

该报告显示企业组的属性。 该报告向您提供企业组的详细信息（如组 ID）。

CA Access Control UNAB 主机(按主机组)

该报告按主机组显示 UNAB 主机。 该报告向您提供了 UNAB 主机的当前分组概述。

该报告包含以下属性：

- 主机组
- 主机名
- 总数

CA Access Control UNAB 本地组迁移状态

该报告显示每个组的每个端点的迁移过程状态。 使用该报告，您可以查看每台主机上的迁移过程的当前状态。

该报告显示下列信息：

- 主机名
- 迁移状态
- 组名称
- 组 ID
- 名称冲突
- GID 冲突
- 成员冲突
- 无 Active Directory 组冲突
- 条目数

CA Access Control UNAB 本地组摘要

该报告显示本地组属性的摘要。 该报告向您提供每个 UNAB 主机上出现的相同组的实例数的概览。

该报告显示下列信息：

- 主机数
- 组名称
- 组 ID
- 实例数

CA Access Control UNAB 本地用户摘要

该报告显示本地用户参数的摘要。 该报告中的信息显示单个用户帐户出现在 UNIX 主机上的实例数。

该报告显示下列信息：

- 主机数
- 用户名
- 用户 ID
- 组 ID
- 主目录
- 登录 shell
- 条目数

CA Access Control UNAB 本地组迁移状态(按组)

该报告按组显示本地组的迁移状态。 使用该报告，您可以查看每个组的迁移过程的当前状态。

CA Access Control UNAB 本地组迁移(按主机)

该报告按主机显示本地组的迁移状态。 该报告向您提供了每台主机上组的迁移状态的详细信息视图。

CA Access Control UNAB 本地用户迁移状态

该报告显示本地用户的迁移状态。 使用该报告，您可以查看每个用户的迁移状态，并在本地用户属性和企业用户属性之间进行比较。

CA Access Control UNAB 本地用户迁移状态(按主机)

该报告按主机显示本地用户的迁移状态。 使用该报告，您可以查看每台主机上的迁移状态。

CA Access Control UNAB 本地用户迁移状态(按用户)

该报告按用户显示本地用户的迁移状态。 使用该报告，您可以查看每个本地用户的迁移状态。

CA Access Control UNAB 非标准本地组(按组)

该报告按组显示非标准本地组的相关信息。 使用该报告，您可以查看本地属性不同于其企业属性的本地组的详细信息。

CA Access Control UNAB 非标准本地用户(按用户)

该报告按用户显示非标准本地用户的相关信息。 使用该报告，您可以查看本地属性不同于其企业属性的用户的相关信息。

CA Enterprise Log Manager 报告

CA Enterprise Log Manager 报告显示有关 CA Access Control 和 UNAB 帐户活动、资源管理等详细信息。

有关 CA Enterprise Log Manager 报告的详细信息，请参阅 CA Enterprise Log Manager 文档。

自定义报告

所有 CA Access Control 报告均使用 Crystal Reports Designer XI 创建。 创建后，这些报告在 BusinessObjects InfoView 中以基于 Web 的格式显示。 要自定义提供的报告，您必须拥有 Crystal Reports Designer XI。

注意：本指南中的说明提供了一些有助于您开始自定义报告的提示。 有关 Crystal Reports Designer XI 的详细信息，请参阅 *《BusinessObjects Enterprise XI 版本 2 Designer 指南》*。

CA Access Control Universe for BusinessObjects

CA Access Control Universe for BusinessObjects 提供 CA Access Control 报告服务中央数据库的简化视图。 Universe 是映射至数据库中数据的语义层。 该层将最终用户与数据库的复杂结构分离。 Universe 是类和对象的集合。

Universe 是使用 BusinessObjects Enterprise Designer 创建的。 CA Access Control Universe 由 CA Technologies 提供，用于简化从 CA Access Control 报告服务中央数据库中创建报告的过程。 您不应修改 CA Technologies 开发的 CA Access Control Universe。 如有必要，请创建副本以作为您自己 Universe 的基础。

查看 CA Access Control Universe

可以使用 BusinessObjects Designer 查看 CA Access Control Universe。

查看 CA Access Control Universe

1. 依次选择“开始”、“程序”、“Business Objects XI Release 2”、“BusinessObjects Enterprise”、“Designer”。

   将显示“用户身份验证”对话框，您可从中登录 BusinessObjects Designer。

2. 输入凭据，然后单击“确定”。

   将显示“快速设计”向导的欢迎屏幕。

3. 清除“启动时运行该向导”复选框，然后单击“取消”。

   将打开空的 Designer 会话。 标题栏中将显示用户名和存储库名称。

4. 依次单击“文件”、“打开”，浏览到包含 CA Access Control Universe 的目录，选择 *CA Access Control.unv* 文件，然后单击“打开”。

   CA Access Control Universe 将在当前 Designer 窗口中打开。

   注意：CA Access Control Universe 存储在指定为默认 Universe 文件存储的目录中，且位于 *CA Universe\CA Access Control* 下。

自定义标准报告

可以自定义任何标准报告。 例如，您可以更改标题、颜色、徽标和字体以满足您的需求。 必须在 Crystal Reports Designer XI 中打开报告才能进行更改。 每个报告都具有对应的 .rpt 文件。 打开该文件即可自定义报告。

自定义标准报告

1. 打开要在 Designer 中自定义的 .rpt 文件。

   将显示报告的“设计”视图。

2. 执行以下*任一*操作：

   - 要更改报告标题，请依次单击“文件”、“摘要信息”，然后在“标题”字段中输入标题。
   - 要自定义文本，请在“设计”视图中突出显示所需文本，然后双击该文本以进行编辑。
   - 要更改文本的显示方式，请在打开的报告中的文本上单击右键，选择“设置文本格式”，然后根据需要更改属性。

3. 保存自定义的 .rpt 文件。

   新的自定义报告将保存，并且随时均可发布。

发布自定义报告

必须使用 BusinessObjects InfoView 发布自定义报告。

发布自定义报告

1. 打开 BusinessObjects InfoView，并以管理员身份登录。

   将显示 InfoView“主页”页面。

2. 依次单击“新建”、“文件夹”，然后在“公共文件夹”下创建新文件夹。

   将显示“创建新文件夹”任务页面。

3. 输入自定义报告文件夹的名称和说明，然后单击“确定”。

   新文件夹将创建。

4. 在您所创建的新文件夹中，依次单击“新建”、“本地计算机文档”、“Crystal 报告”。

   将显示“从本地计算机添加文档”任务页面。

5. 为您自定义的 rpt 文件输入报告标题和路径名，然后单击“确定”。

   自定义报告将发布，并且可以立即从 BusinessObjects InfoView 中查看。 还可以像其他任何报告一样排定该报告。

第 11 章： 部署示例策略和最佳实践策略

此部分包含以下主题：

示例策略

CA Access Control 附带的示例策略向您提供了建议用于保护操作系统和应用程序资源的职责独立和最佳实践。 每个策略都是一个 selang 脚本，包括的注释说明了该策略的用途及其包含的规则。

示例策略提供了使用 CA Access Control 保护您的系统的基准。 将示例策略用作您自己的策略的基础可简化为组织创建策略的过程。您应当针对您的安全策略和环境自定义这些示例策略（操作系统策略取决于您已安装的实际操作系统软件包）。

自定义示例策略之后，使用 CA Access Control 企业管理 将策略部署到端点。

示例策略适用于下列的常用应用软件和操作系统：

- 应用程序有：
  - Apache
  - JBoss 应用程序服务器
  - CA Access Control Web 服务
  - Microsoft SQL Server 2005
  - Oracle Database 10g
- 操作系统有：
  - AIX
  - HP-UX

  - Red Hat Enterprise Linux
  - SuSe Linux Enterprise Server
  - Sun Solaris
  - Windows 2003
- 虚拟化系统有：
  - VMware ESX 服务器
  - Hyper-V
  - Solaris 10 区域

存储示例策略的位置

CA Access Control 将示例策略安装到下列目录：

ACInstallDir/samples/Policies/

ACInstallDir

定义 CA Access Control 的安装目录。

该位置上有三 (3) 个子目录：

- **Applications**—包含特定于应用程序的策略。
- **OS**—包含操作系统策略。
- **Virtualization**—包含虚拟化系统策略。

CA Access Control 以文本文件的形式提供策略，文件中包含执行该策略的 selang 脚本。 每个策略也都有一个匹配策略，您可以用来取消部署保护策略。 您从 CA Access Control 企业管理 部署和取消部署策略。

示例策略有以下命名约定：*OS_ACTION*

OS

定义策略适用于的操作系统。

ACTION

指定脚本采取的策略操作。

值：deploy 和 undeploy

例如，下列文件包含 Red Hat Enterprise Linux 4.0 的示例部署策略：
_LINUX40_deploy.txt

注意：应用程序策略没有取消部署脚本。

示例策略脚本

每个策略都是一个 selang 脚本，包括的注释说明了该策略的用途及其包含的规则。 编写示例策略脚本用于演示最佳实践：

- 备注

  示例策略带有注释以便帮助您了解示例策略各个部分的设置以便逐一实现。

- 容器

  示例策略将相关资源分组为一个单个的容器资源。 通过该方法，通用策略即可一次性应用于所有的相关资源。 策略规则 (ACL) 不需要应用于各个资源。 例如，策略可以使用容器对所有的系统配置文件进行分组。

  策略容器使用以下命名约定：POL_*container_name*。 您可以将这些容器视为子策略。 例如，OS 示例策略使用 POL_SYS_CONF 容器来保护操作系统配置文件。

- 角色

  为了简化用户管理，示例策略将 ACL 应用于角色。 每个角色都使用您可以增加实际用户的 CA Access Control 用户组。

  策略角色使用以下约定：ROL_*role_name*。 例如，示例策略将 ROL_SYSTEM 组用于内置系统用户（如 adm 和 lp）。 许多策略为这些用户分配广泛的权限（用于适当的系统操作），但也会让权限到期，这样用户就无法用其进行登录。

- 变量

  这样，当您部署这些变量时必须实施最小的更改，示例策略利用 CA Access Control 变量。 示例策略使用内置变量来保护本地系统资源，例如，本地主机的终端规则。 示例策略还使用用户定义的变量来简化策略更改。 例如，用户定义的变量可以包含管理用户的主目录。 如果管理用户使用不同的主目录，您只需针对所有受影响的规则进行一次性更改即可自动更改。

示例：策略脚本注释

来自 Solaris SPARC 9 示例策略的以下片段展示了示例策略的注释方式。使用 selang 语法规则并以哈希符号 (#) 开头的行是注释。

```
#
# * Home Directories Protection Policy *
# **************************************
#
# This policy uses the FILE class to protect the home
# directories of sensitive users so that only the owner
# of each directory can access it.
#
# Prerequisites:
#     None
#
# Roles:
#     None
#
# Containers:
#     POL_HOME_DIR      - home directories of sensitive users
#
# define container POL_HOME_DIR
# Protect home directories
editres   CONTAINER POL_HOME_DIR audit(<!POLICY_AUDIT_MODE>) owner(+nobody)
comment("AC Sample - Protect home directories")
authorize CONTAINER POL_HOME_DIR uid(* _undefined)   access(NONE)
editres ACVAR ("HOME_OS_ADMIN") value("/root") type(static)
editusr (<!USER_OS_ADMIN>)
# define specific FILE resources and connect them with POL_HOME_DIR
editres FILE ("<!HOME_OS_ADMIN>/*") audit(<!POLICY_AUDIT_MODE>) owner(+nobody)
defaccess(NONE) <!POLICY_WARNING_MODE>  comment("AC Sample")
authorize FILE ("<!HOME_OS_ADMIN>/*") uid(<!USER_OS_ADMIN>) access(ALL)
chres CONTAINER POL_HOME_DIR mem+("<!HOME_OS_ADMIN>/*") of_class(FILE)
```

示例：示例策略中的容器

下列 selang 输出显示 POL_SYS_FILES 的属性。 AIX 示例策略包含保护系统文件的子策略。

```
AC> sr container POL_SYS_FILES
Data for CONTAINER 'POL_SYS_FILES'
------------------------------------------------------------------------
ACLs              :
    Accessor                Access
    ROL_SYSADMIN  (GROUP  ) All
    ROL_SYSTEM    (GROUP  ) All
    *             (USER   ) R, Chdir
    _undefined    (USER   ) R, Chdir
```

```
Members           :
    /boot/*       (FILE  )
    /dev/kmem     (FILE  )
    /dev/mem      (FILE  )
    /dev/port     (FILE  )
Audit mode        : Failure
Owner             : +nobody       (USER  )
Create time       : 10-Dec-2008 10:32
Update time       : 10-Dec-2008 10:35
Updated by        : root          (USER  )
Comment           : AC Sample - Protect OS system files
```

示例：示例策略中的变量

来自 Red Hat Enterprise Linux 5 示例策略的以下片段展示了示例策略使用变量的方式。 在该片段中，示例策略定义了本地主机的可能名称和管理用户 root 的主目录。

```
#
# * AC Variables Definitions *
# ****************************
#
# The rules in this section define variables that policies use.
# Variables:
#     LOCALHOST             : list of possible names for local host
#     POLICY_AUDIT_MODE     : set policies audit mode
#     POLICY_DEFACCESS      : set defaccess of policies` resources
#
editres ACVAR ("LOCALHOST") value("localhost") type(static)
editres ACVAR ("LOCALHOST") value+("127.0.0.1")
editres ACVAR ("LOCALHOST") value+("0.0.0.0")
editres ACVAR ("POLICY_AUDIT_MODE")   value("FAILURE") type(static)
editres ACVAR ("POLICY_DEFACCESS")    value("ALL")     type(static)
```

更多信息：

用户定义的变量 (p. 92)
内置变量 (p. 93)
使用变量的准则 (p. 94)
端点解析变量的方式 (p. 96)

遵从性和最佳实践策略

通过遵从性和最佳实践策略，您可快速在端点上部署遵从性和最佳实践策略。 每个策略都是一个 selang 脚本，包括的注释说明了该策略的用途、其包含的规则及其使用的变量。

该规则遵守支付卡行业数据安全标准 (PCI DSS) 和安全评估步骤以及 VMWare VSphere 强化需求。

遵从性和最佳实践策略适用于以下操作系统和虚拟化平台：

- 操作系统
  - Red Hat Advanced Server Linux
  - SuSE Linux
  - SLES
  - AIX
  - HP-UX
  - Solaris
  - Windows 2003 R2
  - Windows 2008 R2
- 虚拟化平台
  - VMWare Server ESX
  - Solaris 10 上的 Solaris 区域
  - Hyper-V

存储遵从性和最佳实践策略的位置

企业管理服务器在安装期间将遵从性和最佳实践策略存储在 DMS 上。这会在您部署企业管理服务器的全新安装时自动完成。

从 CA Access Control 企业管理 的“策略管理”部分中管理遵从性和最佳实践策略。

在每次 CA Access Control 的新安装上，遵从性和最佳实践策略都存储在以下位置：

ACInstallDir/samples/Policies/OutOfTheBox

ACInstallDir

定义 CA Access Control 的安装目录。

CA Access Control 以文本文件的形式提供策略，文件中包含执行该策略的 selang 脚本。 每个策略也都有一个匹配策略，您可以用来取消部署保护策略。 您从 CA Access Control 企业管理 部署和取消部署策略。

示例策略有以下命名约定：*REGULATION_ACTION*

REGULATION

定义策略适用于的法规的名称。

ACTION

指定脚本采取的策略操作。

值： deploy 和 undeploy

例如，下列文件包含 PCI DSS 的第 7.1.1 小节的示例部署策略：pci_dss_7.1.1_deploy.txt

注意：遵从性和最佳实践策略独立于操作系统，并且适用于 Windows 和 UNIX 系统。

遵从性和最佳实践策略脚本

每个策略都是一个 selang 脚本，包括的注释说明了该策略的用途及其包含的规则：

- 备注

  示例策略带有注释以便帮助您了解示例策略各个部分的设置以便逐一实现。

- 变量

  遵从性和最佳实践策略独立于操作系统。 但是，资源组会随着系统的变化而有所不同。 为了克服该问题，资源表使用变量，而 ACL 在策略中使用变量。 当端点连接到企业管理服务器时，它会根据操作系统自动添加到匹配的主机组，策略即被部署到端点。

- 角色

  为了简化用户管理，示例策略将 ACL 应用于角色。 每个角色都使用您可以增加实际用户的 CA Access Control 用户组。

  策略角色使用以下约定：ROL_*role_name*。 例如，示例策略将 ROL_SYSTEM 组用于内置系统用户（如 adm 和 lp）。 许多策略为这些用户分配广泛的权限（用于适当的系统操作），但也会让权限到期，这样用户就无法用其进行登录。

示例：遵从性和最佳实践策略注释

来自 PCI_DSS_7.1.1 遵从性策略的以下片段展示了遵从性和最佳实践策略的注释方式。 使用 selang 语法规则并以哈希符号 (#) 开头的行是注释。

```
#
# * 2. Protect <!USER_OS_ADMIN> Logon and Access Control Administration *
# ************************************************************************
#
# This section uses the TERMINAL class to restrict administrator users from
# logging in directly (read access). Access Control administration is blocked as
# well (write access).
#
# To separate security administration from system administration, the policy
# sets READ access only to these special terminals.
#
editres   TERMINAL ("<!HOSTNAME>") audit(ALL) warning
authorize TERMINAL ("<!HOSTNAME>") uid("<!USER_OS_ADMIN>") deniedaccess(READ)
# The following line is commented because the warning mode in UNIX is not
# applicable for write access to class TERMINAL.
#authorize TERMINAL ("<!HOSTNAME>") uid("<!USER_OS_ADMIN>") deniedaccess(WRITE)
```

示例：遵从性和最佳实践策略角色

来自 PCI_DSS_7.1.1 遵从性策略的以下片段展示了策略将 ACL 应用于角色的方式。

```
#
# * 1. Role Definitions *
# ***********************
#
# The rules in this section define the roles that the policy uses.
#
#  * Define built-in OS users with the logical property. This prevents users
#    from logging in to the system.
#  * Create the user +nobody in CA Access Control only. CA Access Control
#    sets this user as the owner of many resources (to disable ownership
#    bypass). You cannot create this user in the native OS.
#  * Create at least one user in ROL_AC_ADMIN. Without this user you cannot
#    login into CA Access Control.
#    Note: By default, the rules add the superuser account to ROL_AC_ADMIN.
#          We recommend that you remove this user and add security
#          administrators to this group.
# Roles:
#     ROL_SYSTEM        : built-in OS users
#     ROL_SYSADMIN      : system administrators
#     ROL_RESTRICTED    : restricted users with permissions for specific tasks
#     ROL_AC_ADMIN      : CA Access Control administrators
#     ROL_AC_AUDITOR    : CA Access Control auditors
#     ROL_AC_OPERATOR   : CA Access Control operators
#     ROL_AC_SERVICE    : CA Access Control service managers
#     ROL_AC_PWMANAGER  : CA Access Control password managers
#

editgrp (ROL_SYSTEM ROL_SYSADMIN ROL_RESTRICTED ROL_AC_ADMIN ROL_AC_AUDITOR
ROL_AC_OPERATOR ROL_AC_SERVICE ROL_AC_PWMANAGER)
chgrp (ROL_SYSADMIN ROL_AC_ADMIN) audit(LOGINSUCCESS LOGINFAILURE FAILURE)
editusr (+nobody) comment("AC OOTB - Resource owner used for disabling ownership
bypass")
chusr (+nobody) owner(+nobody)
join ("<!USER_OS_ADMIN>") group(ROL_SYSTEM)
join ("<!USER_OS_ADMIN>") group(ROL_AC_ADMIN)
```

策略部署

当部署任何一个 CA Access Control 策略时，您应遵循一些通用步骤以确保策略的部署和执行符合预期而不会发生错误。 以下部分说明了您在部署示例策略前后应当采取的操作。

如何准备端点进行策略部署

在实施任何策略之前，您应当针对该策略准备端点。 这样，您以后便可以隔离特别与该策略相关的问题。

准备端点进行策略部署：

- 使用操作系统或应用程序的全新安装

  将最新可用的、厂商提供的操作系统版本和修补程序用于操作系统策略。 这样，您便可以在修改可能影响系统之前保护系统。 在应用策略之后，了解到该策略会保护系统免受恶意或意外更改的伤害，您就可以根据需要应用修补程序并配置系统。 同样的逻辑也适用于应用程序。

- 实施职责独立

  查看策略规则并添加其他角色（如果需要）。 创建您自己的策略，该策略定义角色、用户及其关系（角色成员资格）。 然后，可以在示例策略前后部署该策略。

  确保您没有为任何单一用户授予过多权限。 例如，默认情况下，超级用户被添加到 ROL_AC_ADMIN，其提供 CA Access Control 管理权限。 但是，最佳实践是删除该用户，然后另将安全管理员添加到该组中。

- 创建新的 CA Access Control 数据库，或备份您现有的数据库

  在您实施策略之前创建新的数据库。 这可确保策略规则不会发生冲突或更改数据库中的现有规则。 如果您无法创建新的数据库，则应备份数据库，以便可以将其还原到应用策略之前的状态。

- 将适当的管理角色分配给用户：系统管理员、安全管理员、应用程序管理员。

- 使用新的审核日志文件

  备份现有的审核日志文件，然后将其删除。 这可确保 CA Access Control 在记录新事件时将创建新的审核日志文件。 有了仅包含与您部署策略有关的事件的审核日志文件，可以帮助您更加快速地识别和隔离与策略相关联的问题。

- 设置 CA Access Control 用户定义的变量

  请确认预设的 CA Access Control 变量值（“AC 变量定义”部分）匹配您的环境，并根据需要添加或修改值。

如何以分阶段的方式部署策略

当部署策略时，可以采取几个操作来确保策略的部署和执行符合预期而不会发生错误。 在您已经准备好端点进行策略部署之后，建议您通过分阶段的策略部署来继续进行。

建议您首先在测试环境中部署策略，然后在已经根据需要调整策略之后，将其部署到生产环境中。

以分阶段的方式部署策略：

1. 在警告模式下部署策略

   策略现在处于活动状态，但是不实施其规则。 在实施策略之前，您可以检查审核日志以预览该目标策略的结果。

   注意：默认情况下，示例策略的脚本为所有策略规则设置“警告”模式。

2. 查看 CA Access Control 审核日志的警告消息

   在部署策略之后，任何违反的策略都会作为警告显示在审核日志中（假定您的策略规则使用“警告”模式）。

3. 在真实情况中使用系统并再次分析审核日志

   要有效地测试策略，您可以在计算机上执行常规操作过程（登录、启动和停止服务和应用程序等等）。 然后，您可以再次分析审核日志来查看是否出现任何新的警告。

4. 根据需要调整策略

   使用从审核日志收集的信息，您可以调整策略以实现环境中的预期使用。

5. 删除警告模式来启用策略

   一旦确信您的策略已就绪，可以在生产环境中实施规则，您就可以删除警告模式来启用该策略。

   现在，该策略现在成为活动状态。

注意：如果您想更改策略，应首先禁用策略实施（使用“警告”模式），对策略进行更改，然后当确信更改可以按照需要正常运行时，再重新激活该策略。

更多信息：

策略部署 (p. 308)
如何针对您的环境来自定义策略 (p. 308)
启用示例策略实施 (p. 309)

策略部署

因为示例和最佳实践策略包含 CA Access Control 变量，您必须使用高级策略管理方法对其进行部署。

注意：您不能在端点上以 selang 直接运行示例策略文件。

使用 CA Access Control 企业管理 在 DMS 上存储示例策略，然后根据需要将其分配给多个端点。

更多信息：

高级策略管理 (p. 62)
如何创建和部署策略 (p. 77)

如何针对您的环境来自定义策略

示例和最佳实践策略是作为您自己的安全策略的基础而提供的。 要部署策略，您应当针对环境对其进行自定义。

针对您的自定义策略：

- 查看 CA Access Control 和系统日志文件。

  查找并确认在部署进程期间发生的警告或错误，并且修改策略来解决这些问题。

- 将用户加入策略角色。

  策略使用角色进行授权。 您需要将组织中的用户分配到这些角色。

  重要说明！ 当取消部署策略时，不要删除您创建的用户或组。 这可能会影响使用该用户和组的其他策略中 ACL 列表和访问者关联的正常行为。

- （仅适用于 Windows）运行共存实用工具 eACoexist.exe。

  该实用工具识别 CA Access Control 与其他安装的程序之间的冲突，并且通过为该程序创建旁路来解决这些冲突。

启用示例策略实施

默认情况下，示例策略的脚本为所有策略规则设置“警告”模式。 当部署策略时，它处于活动状态，但是不实施其规则。 当您熟悉策略并根据需要对其进行自定义后，应当准备好启用该策略以便实施策略规则。

注意：该步骤说明了如何为单个策略启用策略实施。 有关如何在执行系统维护之后为多个策略启用策略实施的更多信息，请参阅您的操作系统的*《端点管理指南》*。

启用示例策略实施

1. 编辑策略脚本以将每个 **warning** 实例更改为 **warning-**。

   当运行为资源或访问者设置 warning- 的规则时，CA Access Control 会删除资源或访问者中的“警告”模式。

2. 部署已编辑的策略。

   策略实施已启用。

示例：启用 Windows 示例策略实施

以下片段来自 Windows 的示例 JBoss 策略。 策略被启用，因为 "warning" 变为 "warning-"。

```
# Protect JBoss files
# -------------------

# Protect JBoss files in the application directory.
# These rules apply protection to files that are not protected by other rules.
editfile     ("<!JBOSS_HOME>\*") owner(nobody) defaccess(NONE) warning- comment
("AC Sample - JBoss base dir")
authorize FILE ("<!JBOSS_HOME>\*") id(ROL_JBOSS_ADMIN) access(ALL)
via(pgm("<!JBOSS_HOME>\bin\*"))
authorize FILE ("<!JBOSS_HOME>\*") id(jboss_pgm)       access(READ,CHDIR)
via(pgm("<!JBOSS_HOME>\bin\*", "<!JBOSS_JAVA_PGM>"))
```

禁用示例策略实施

默认情况下，示例策略的脚本为所有策略规则设置“警告”模式。 当启用策略实施时，请删除“警告”模式。 要禁用策略实施，再重新引入“警告”模式。

注意：该步骤说明了如何为单个策略禁用策略实施。 有关如何在执行系统维护时为多个策略禁用策略实施的更多信息，请参阅您的操作系统的*《端点管理指南》*。

禁用示例策略实施

1. 编辑策略脚本以将每个 **warning-** 实例更改为 **warning**。

   当运行为资源或访问者设置 warning 的规则时，CA Access Control 会为资源或访问者设置“警告”模式。

2. 部署已编辑的策略。

   策略实施已禁用。