CA Access Control for Virtual Environments

企业管理指南

r2.0

ca technologies

第三方通知

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

示例脚本和示例 SDK 代码

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

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

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- [set the eACee variable for your book]
- CA Access Control
- CA User Activity Reporting Module
- Identity Manager

文档约定

CA Access Control 文档使用以下约定：

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

文档在解释命令语法和用户输入（以等宽字体显示）时还会使用以下特殊约定：

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

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

示例：命令表示法约定

下面的代码说明了在本指南中使用命令约定的方式：

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

在该示例中：

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

文件位置约定

CA Access Control 文档使用以下文件位置约定：

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

联系技术支持

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

目录

第 1 章： 简介

此部分包含以下主题：

关于本指南

本指南提供了有关企业管理、报告以及 CA Access Control 企业管理 基于 Web 界面的信息。 CA Access Control 企业管理 的企业管理和报告包括特权帐户密码管理、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

该指南适合于使用 CA Access Control for Virtual Environments 的安全、系统和虚拟管理员，他们要使用其企业管理、第三方程序集成和报告的功能：

- 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)
- 与第三方程序集成。

企业管理

CA Access Control 企业管理 是基于 Web 的用户界面，通过它，您可以执行整个企业中的访问相关管理任务。 您可以执行大量管理任务。 例如，您可以通过企业，从中央位置部署访问策略、管理个人主机、管理特权帐户、生成企业报告等。

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。

企业视图

使用 CA Access Control 企业管理 查看相关信息，并管理来自中央位置的虚拟和物理计算机及 PUPM 端点。 CA Access Control 企业管理 全局查看会显示每个受管设备最后更新的详细信息。 通过全局查看，您也可以修改受管设备和安全组的设置。

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。

企业报告

通过 CA Access Control 企业管理 报告选项，您可以查看中央位置中的每个 PUPM 端点和受管设备的安全状态。 可以排定或按需从端点和受管设备收集数据。 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 for Virtual Environments 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 随付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 主机管理器**－定义受管设备和逻辑安全组。

  CA Access Control 主机管理器可以创建受管设备和安全组，将设备分配给安全组，并修改组。 CA Access Control 主机管理器无法定义策略或部署策略，但是他们可以使用全局查看来查看策略。

- **CA Access Control 策略部署器**－在整个环境中部署策略。

  CA Access Control 策略部署器将策略分配给主机和主机组，升级和降级策略，并重置主机配置。CA Access Control 策略部署器可以访问部署审核。 他们可以查看策略和主机，但也无法定义。 他们可以访问全局查看。

- **CA Access Control 策略管理器**－创建策略。

  CA Access Control 策略管理器创建、修改、查看和删除策略。 他们无法将策略部署到主机或主机组，但他们可以查看且可以访问全局查看。

- **CA Access Control 用户管理员**－管理 CA Access Control 企业管理 中的用户和组。 他们也可以将 CA Access Control 企业管理 角色分配给用户。

  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**－管理 CA Access Control 企业管理。

  系统管理员可以在 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**－管理英语报告。 具有该角色的用户可以排定和查看报告。

- **CA Enterprise Log Manager 用户**－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**－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**－指派工作项。 具有该角色的用户可以将工作项指派给用户。

- **自己管理员**－管理自己的用户帐户。 具有该角色的用户可以在他们的帐户上执行管理操作。 他们可以更改帐户密码、修改他们的用户信息、查看他们分配的角色、提交任务以及正在等待他们批准的项。

  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. 19)。
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，用户可以立即访问他们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。

请注意下列事项：

- 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. 19)。
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. 21)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. 21)。

   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. 22)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. 21)。

   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. 22)，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. 24)
添加选项卡 (p. 24)
配置字段、事件和角色使用 (p. 25)

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. 26)
组类型 (p. 29)

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. 34)
查看任务详细信息 (p. 38)
查看事件详细信息 (p. 38)
清除已提交的任务 (p. 38)
将消息队列审核消息传递到 Windows 事件日志 (p. 40)
将消息队列审核消息传递到 UNIX 系统日志 (p. 42)
配置审核收集器 (p. 158)

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. 35)，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. 37)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. 37)

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*《Identity Manager 管理指南》*。

第 3 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。

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. 21)

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：

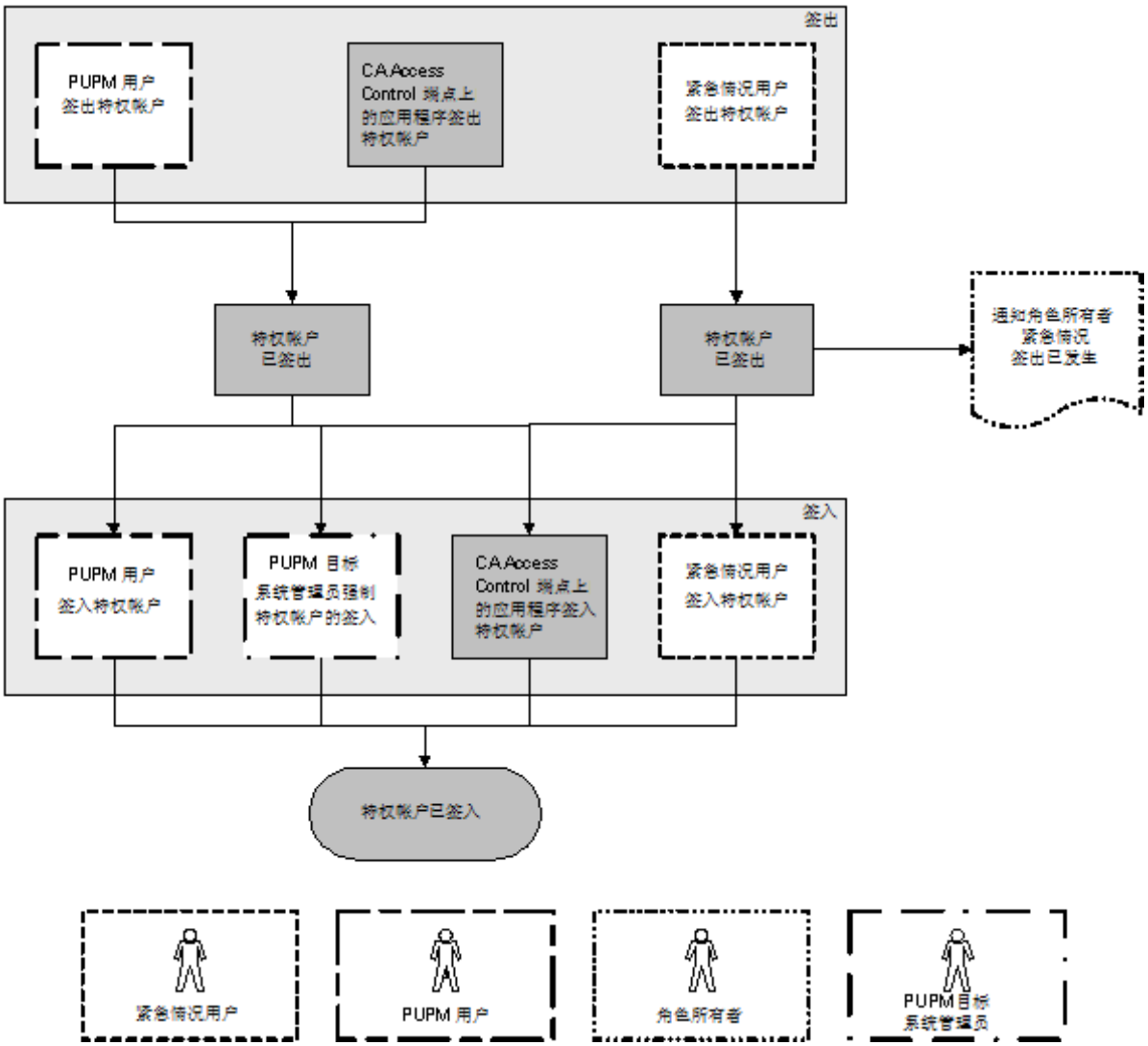
1. 用户使用下列方式之一签出特权帐户：
   - 具有“PUPM 用户”角色的用户签出特权帐户。
   - 具有“紧急情况”角色的用户执行紧急情况签出。
   - CA Access Control 端点上的应用程序（例如 CLI 密码使用方）签出特权帐户。

   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。

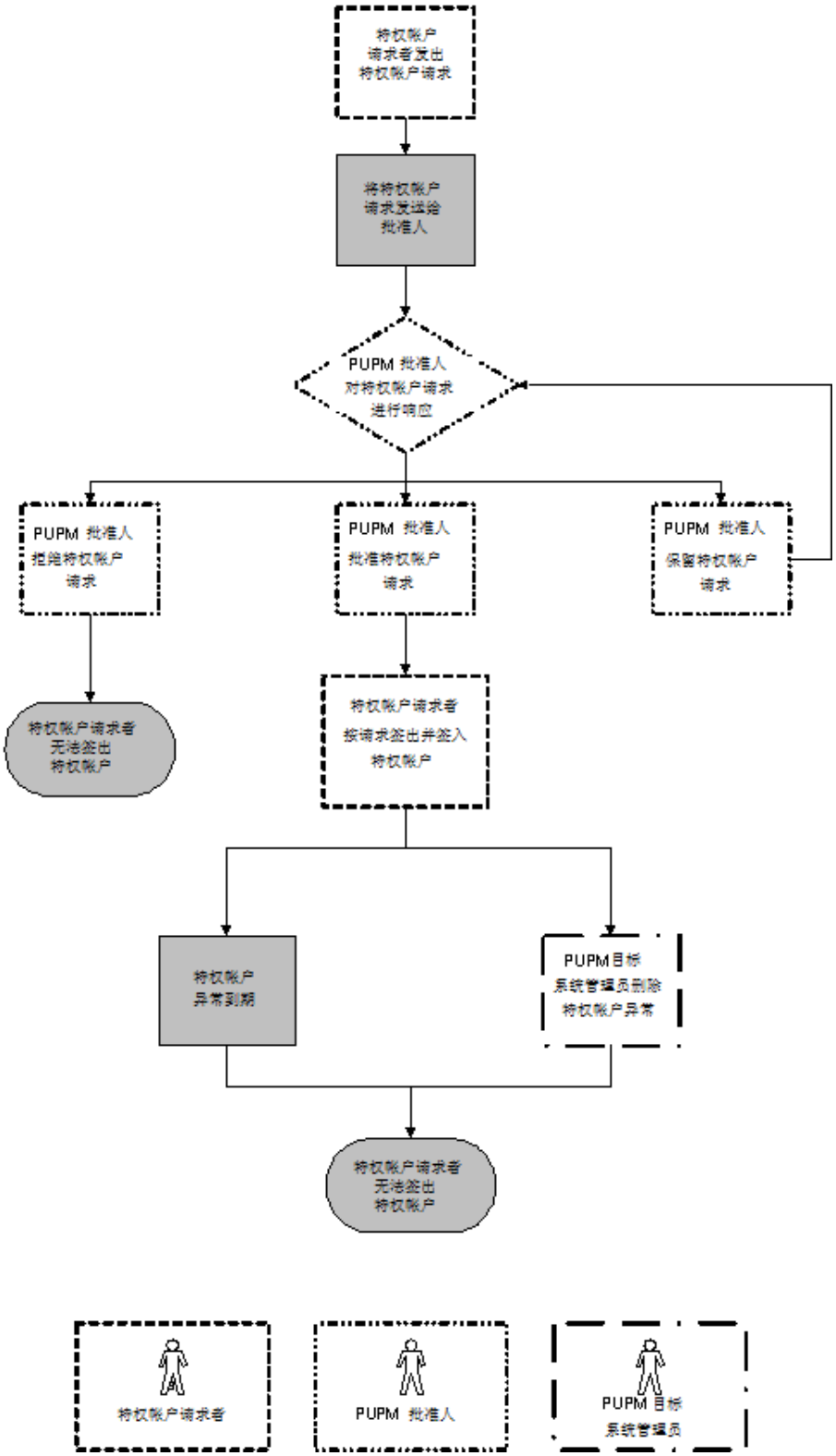
     具有“特权帐户请求”角色的用户被授予特权帐户异常，并且可以签出和签入特权帐户。

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。

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. 33)
审核特权帐户 (p. 130)

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. 134)

如何将 PUPM 端点与 CA User Activity Reporting Module 集成

通过将您的 PUPM 端点与 CA User Activity Reporting Module 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。

完成以下步骤：：

1. 在 CA Access Control 企业管理 中：
   a. 配置到 CA User Activity Reporting Module 的连接。
   b. 指定每个 PUPM 端点的 CA User Activity Reporting Module 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 User Activity Reporting Module 选项卡。
2. 配置 CA User Activity Reporting Module 以便能够从 PUPM 端点不断收集信息。

注意：有关如何配置 CA User Activity Reporting Module 的详细信息，请参阅 CA User Activity Reporting Module 文档。

更多信息：

在 PUPM 端点上查看审核事件 (p. 134)

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。

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 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 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 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。

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。

.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。

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。

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。

第 4 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。

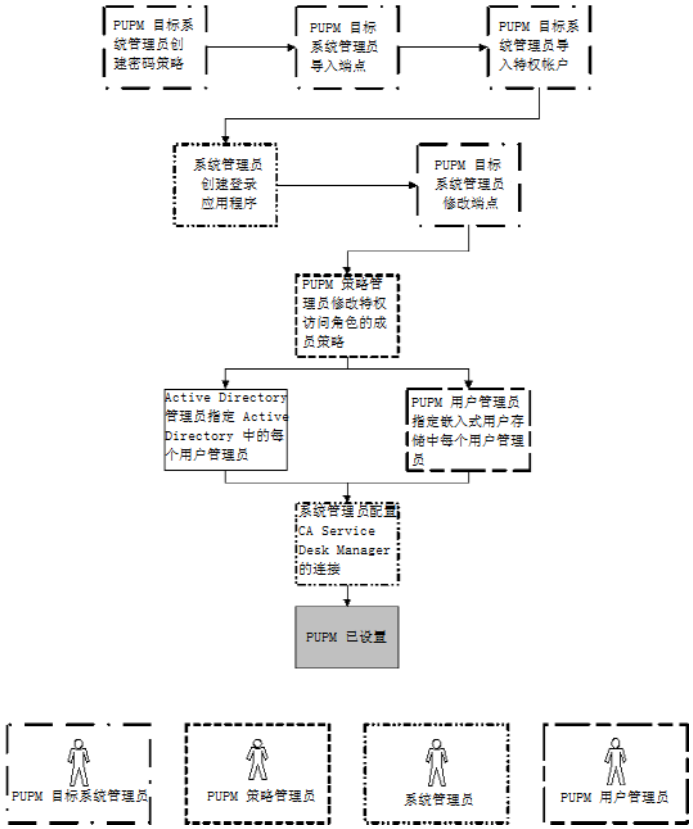
6. （嵌入式用户存储）PUPM 用户管理员为每个用户指定了管理员。

   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 Unicenter Service Desk 的连接。

   与 Unicenter Service Desk 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。

完成以下步骤：

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. 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。

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。

6. 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。

创建特权帐户

创建特权帐户以便在受管和断开的系统上管理帐户密码。 通过使用特权帐户，用户可以签出和签入特权帐户密码，创建特权帐户。

要创建多个帐户，请使用发现特权帐户向导以便在端点上搜索特权帐户。 如果要创建一个帐户，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。

完成以下步骤：

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，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

定义并确认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。

单击“提交”。

CA Access Control 企业管理 创建新的特权帐户。

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. 78)

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。

完成以下步骤：

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。 以下字段需加以说明：

   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：在您选择端点类型时，要求您提供 PUPM 需要的凭据以便管理管理该端点的特权帐户。 您选择的端点类型会影响您必须提供的连接信息。

   受管设备

   （可选）指定是否将 PUPM 端点与 CA Access Control for Virtual Environments 受管设备关联

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“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 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. 82)
VMware ESX/ESXi 连接信息 (p. 83)
Windows Agentless 连接信息 (p. 87)
Identity Manager 配给连接信息 (p. 101)
断开端点的连接信息 (p. 103)

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。

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 CA Access Control for Virtual Environments 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。

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。

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. 59)

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. 88)

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. 88)

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。

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”。

   “权限”对话框关闭。 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。

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

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. 80)。 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. 73)。

   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。

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：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。

Identity Manager 配给连接信息

Identity Manager 配给连接器允许您管理在配给服务器中定义的 Identity Manager 端点。 在 PUPM 中创建 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 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
```

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 Identity Manager 密码策略强制选项的更多信息，请参阅 *《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 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 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 Identity Manager 配给管理器 (p. 102)

针对 PUPM 配置 Identity Manager 配给管理器

您必须为 PUPM 配置 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 Identity Manager r12.5 和 r12.5 SP1 端点。

针对 PUPM 配置 Identity Manager 配给管理器

1. 登录到 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 Identity Manager - Provisioning Server 和 Identity Manager - Connector Server (Java) 服务。

   已为 PUPM 配置了 Identity Manager 配给管理器。

修改 Identity Manager 配给连接器搜索限制

当您运行“特权帐户发现”向导时，Identity Manager 配给连接器会针对您在 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 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。 请执行以下操作：
   a. 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

   b. 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 并运行，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。

请注意下列事项：

- 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。

完成以下步骤：

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. 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登录应用程序列表。

   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。

   注意：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：

修改 Windows Server 2008 端点以便使用登录应用程序 (p. 91)

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。

完成以下步骤：

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“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“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“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 Identity Manager 配给服务器中的定义完全一致。 该属性适用于“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

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. 96)

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。

创建特权帐户 CSV 文件

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“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。

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。

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。

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. 120)

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")

```
LaunchProcessAsUser (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.LaunchProcessAsUser("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。

第 5 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. 131)，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. 37)

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. 131)，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. 57)

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 6 章： 使用特权帐户

此部分包含以下主题：

签出特权帐户密码

可以签出特权帐户密码，以登录帐户所属的端点。 签出特权帐户时，可以选择来显示密码、将密码复制到剪贴板或登录端点。

如果要使用 SSH 连接 SSH 设备端点，而 PUPM 使用不同的帐户连接和管理该端点，则应签出这两个帐户。 使用连接帐户的凭据连接 SSH 设备端点，然后使用管理帐户的凭据通过 su 命令切换到该帐户。

签出特权帐户密码

1. 依次单击“主页”、“我的帐户”、“我的特权帐户”。

   此时出现“我的帐户”页面，其中显示可供您签出的帐户。

2. （可选）选择搜索所使用的属性，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精简列表。

3. 选择要签出的帐户及端点，然后从“操作”菜单中选择以下选项之一：
   - 选择“签出”以签出密码
   - 选择配置用来登录端点的“登录应用程序”
   - 选择“显示密码”以显示密码
   - 选择“复制到剪贴板”以将密码复制到剪贴板
   - 选择“高级登录”以配置要登录的端点的登录应用程序和主机名

   CA Access Control 企业管理 将提交任务并根据您选择的选项继续操作。

   如果选择了登录到端点，CA Access Control 企业管理 将显示一条确认消息，并在端点上打开一个窗口供您完成登录。

   注意：如果这是您第一次尝试登录该端点，在连接端点前将打开一个对话框，请求您确认操作。

   重要说明！ 在 Microsoft Windows 2008 服务器上，启用 Microsoft Internet Explorer 浏览器安全性设置中的“ActiveX 控件自动提示”。 如果禁用该选项，浏览器将阻止 ActiveX 文件运行远程桌面应用程序。

更多信息：

PUPM 到 UNIX 端点的连接方式 (p. 95)

签入特权帐户密码

从受管端点注销后，应签入特权帐户密码。 当您签入特权帐户密码后，CA Access Control 企业管理 可能会更改该密码（如果已配置）。

签入特权帐户密码

1. 依次单击“主页”、“我的帐户”、“我的特权帐户”。

   此时出现“我的特权帐户”页面，其中显示可供您签入的帐户。
2. （可选）选择搜索所使用的属性，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精简列表。
3. 选择要签入的帐户密码，并从“操作”菜单中选择“签入”。

   CA Access Control 企业管理 即会提交任务以签入帐户。

更多信息：

签出特权帐户密码 (p. 137)
请求特权帐户的访问权限 (p. 139)

请求特权帐户的访问权限

如果需要特权帐户密码，而您的用户帐户没有可签出帐户的特权访问权限，您可以提交请求来签出该帐户。 CA Access Control 企业管理 会将您的请求转发给可以批准或拒绝您的请求的批准人。 一经批准，您即可签出该特权帐户。

请求特权帐户的密码

1. 依次单击“主页”、“我的帐户”、“特权帐户请求”。

   此时出现“特权帐户请求: 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. 选择要签出的特权帐户，然后单击“选择”。

4. 完成请求，然后单击“提交”。 您可能还需要提供 Unicenter Service Desk 票单号。

   此时会打开一个窗口，通知您该请求已经提交。

   请求将转发给批准人，在批准或拒绝前，该请求将保持未决状态。如果请求得到批准，您可以签出特权帐户。

回应特权帐户请求

如果分配了默认的 PUPM 批准人角色或与之相当的角色，您可以回应由用户提交的未决特权帐户访问请求。 您可以通过以下操作之一进行回应：

- **批准**－批准请求并允许用户签出特权帐户。
- **拒绝**－拒绝特权帐户请求。
- **保留项目**－保留该请求，将来再加以考虑。 保留请求时，CA Access Control 企业管理 将从其他批准人的工作列表中删除该工作项目。 以后可以返回到该项目进行批准或拒绝。
- **发布项目**－发布该请求，以供其他人回应。 您只能发布先前为自己保留的项目。

您还可以添加其他批准人并再分配该工作项目，以便他们也会在其未决批准中收到该项目。

注意：紧急情况签出请求显示在“正在等待我的批准”请求列表中。 但您不需要批准或拒绝这些请求。 这些请求仅作为通知信息显示，指明用户已签出紧急情况帐户。

注意：要响应特权帐户请求，用户必须具有 PUPM 批准人特权访问角色，而且必须是请求用户的管理员。

回应特权帐户请求

1. 依次单击“主页”、“我的帐户”、“正在等待我的批准”。

   此时出现未决特权帐户请求的列表。

2. 单击要考虑的未决请求。

   此时出现“批准特权帐户请求”页面。

3. （可选）要为该请求添加批准人，请执行以下步骤：

   a. 单击“添加受派人”。

      此时会打开“选择用户”搜索窗格。

   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. 选择要添加的用户，然后单击“选择”。

      该用户即被添加到批准人列表中。

4. （可选）按如下方式查看请求的详细信息并修改必需的参数：
   a. 单击“特权帐户”选项卡。

      此时出现“特权帐户”选项卡，其中显示详细的帐户和请求信息。
   b. 使用“有效截止时间”字段覆盖签出截止时间超时。
   c. 使用“票单号”字段查看 Unicenter Service Desk 票单。
   d. 键入注释，以解释您对请求的回应。
5. 请执行下列操作之一：
   - 单击“批准”。

     请求将获得批准并从未决请求列表中删除，请求人此时即可签出特权帐户。
   - 单击“拒绝”。

     请求将遭到拒绝并从未决请求列表中删除。
   - 单击“保留项目”。

     请求将为您保留，并从其他批准人的未决请求列表中删除。
   - 单击“发布项目”。

     请求将发布给所有其他批准人。 您只能发布先前保留的项目。

紧急情况

使用紧急情况任务可以*立即*访问您没有特权访问权限的端点。

注意：如果不需要立即访问该端点，可以请求特权帐户的访问权限，并等待请求获得批准。

紧急情况

1. 依次单击“主页”、“我的帐户”、“我的特权帐户”。

   此时出现“我的帐户”页面，其中显示可供您签出的帐户。

2. 在“选择帐户”字段中，选择“高级”。

   此时出现高级搜索选项。

3. 选择包括紧急情况帐户，并选择“搜索”。

   此时将显示匹配筛选条件的特权帐户的精简列表。

4. 从“操作”菜单中选择要签出的特权帐户。

5. 填写理由，然后单击“签出”。

   CA Access Control 企业管理 将提交任务，如果成功，将在确认消息中显示帐户密码。

注意：签出密码后，以下选项也将显示在“操作”菜单中：“签出”、“登录应用程序”及“显示密码”。

签入紧急情况特权帐户密码

从受管端点注销后，应签入紧急情况特权帐户密码。

签入紧急情况特权帐户密码

1. 依次单击“主页”、“我的帐户”、“我的特权帐户”。

   此时出现“我的帐户”页面，其中显示可供您签入的帐户。

2. 在“选择帐户”字段中，选择“高级”。

   此时出现高级搜索选项。

3. 选择包括紧急情况帐户，并选择“搜索”。

   此时将显示匹配筛选条件的特权帐户的精简列表。

4. 选择要签入的帐户，并从“操作”菜单中单击“签入”。

   CA Access Control 企业管理 即会提交任务以签入帐户。

第 7 章： 与 CA Enterprise Log Manager 集成

此部分包含以下主题：

关于 CA User Activity Reporting Module

CA User Activity Reporting Module 注重于 IT 遵从和保障。 通过它，您可以对 IT 活动进行收集、正常化、汇总和报告，还可在可能发生违规行为时生成报警（要求用户采取相应措施）。 您可以通过不同的安全和非安全设备收集数据。

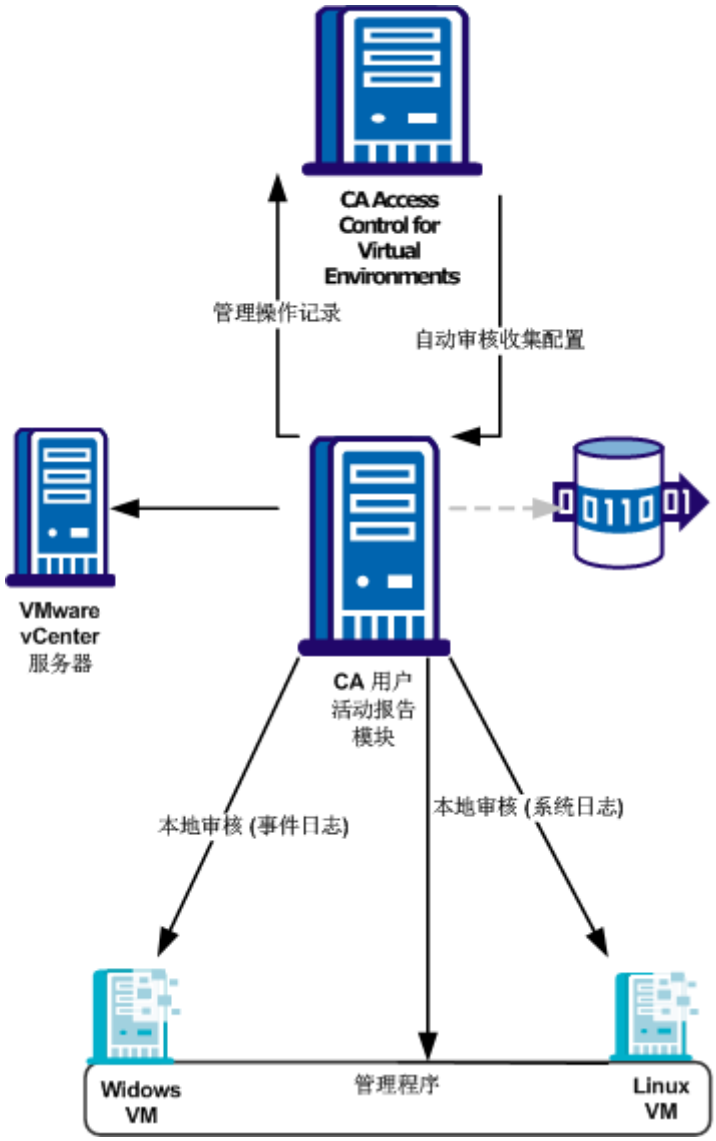
CA User Activity Reporting Module 集成体系结构

通过与 CA User Activity Reporting Module 集成，您可以从每个受管设备收集审核事件由 CA User Activity Reporting Module 进行报告。

您可以配置每个管理设备以将审核事件收集到本地计算机上的审核文件中。 然后，您可以配置 CA User Activity Reporting Module，从中调用事件（消息）。 CA User Activity Reporting Module 会处理这些事件，并将它们发送到 CA User Activity Reporting Module 服务器。

CA Access Control for Virtual Environments 安装支持 CA User Activity Reporting Module 集成。

下图显示了 CA User Activity Reporting Module 集成组件的体系结构。



上图说明了以下内容：

- 每个受管设备将审核数据收集到本地文件
- 应用审核收集策略时，CA User Activity Reporting Module 调用受管设备的将审核记录
- CA User Activity Reporting Module 收集 CA Access Control for Virtual Environments 中所做的管理操作的审核记录
- CA User Activity Reporting Module 从 VMware vCenter 服务器和管理程序收集审核记录

注意：CA User Activity Reporting Module 集成依赖于报告服务组件。 因此，体系结构包括不用于 CA User Activity Reporting Module 集成的其他报告服务组件和功能。 这些组件和功能在图表中显示为灰色。

CA User Activity Reporting Module 集成组件

CA User Activity Reporting Module 集成使用以下 CA Access Control for Virtual Environments 组件。 这些组件是 CA Access Control 企业报告服务的一部分：

- *报告代理*在每个受管设备上运行并将信息发送到驻留在 VPM 服务器上已配置的消息队列上的队列。 对于 CA User Activity Reporting Module 集成，报告代理在排定的时间从审核日志文件中收集审核消息，然后将这些事件发送到配置的分发服务器上的审核队列。
- *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信息。 对于报告，消息队列将 CA Access Control for Virtual Environments 数据库快照转发到中央数据库。

注意：默认情况下，CA Access Control for Virtual Environments 在 CA Access Control 服务器上安装分发服务器。

CA User Activity Reporting Module 集成还使用以下 CA User Activity Reporting Module 组件：

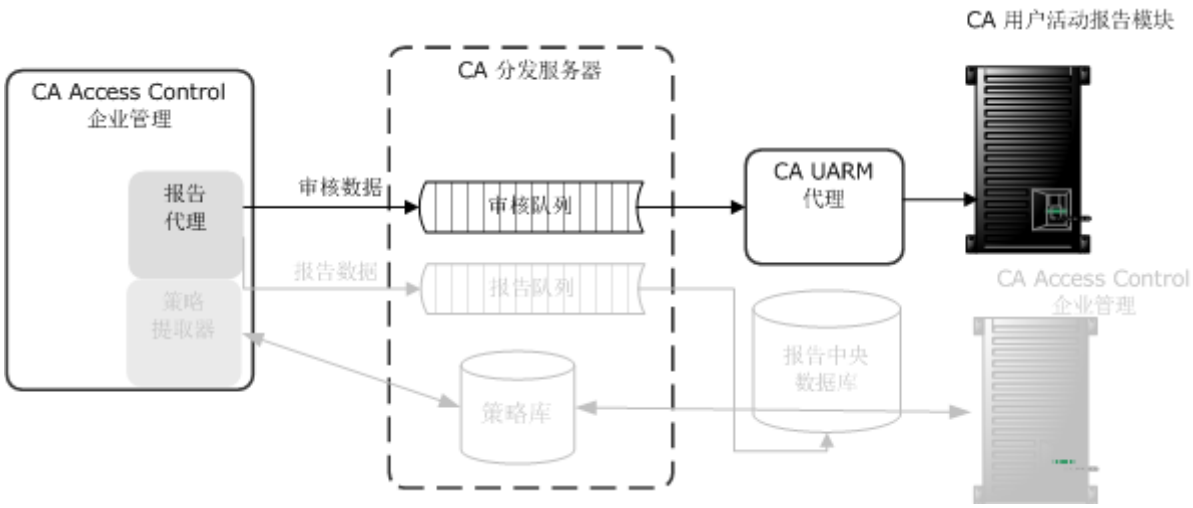
- *CA Access Control for Virtual Environments 连接器*是适用于 CA Access Control 审核事件源的即取即用的 CA User Activity Reporting Module 集成。 连接器允许从分发服务器收集原始事件，并能够基于规则将转换的事件传输到事件日志存储，在这里事件将插入热数据库。

- *收集服务器*是一个 CA User Activity Reporting Module 服务器，可以执行以下操作：细化传入的事件日志、将它们插入热数据库、将达到配置大小的热数据库压缩至暖数据库，并根据配置的计划将暖数据库自动存档到相关的管理服务器。

注意：有关 CA User Activity Reporting Module 组件的详细信息，请参阅 CA User Activity Reporting Module 文档。

审核数据如何从 CA Access Control for Virtual Environments 流向 CA User Activity Reporting Module

要了解 CA Access Control for Virtual Environments 如何与 CA User Activity Reporting Module 集成，以及配置此集成时需要考虑的事项，首先需要考虑 CA Access Control for Virtual Environments 与 CA User Activity Reporting Module 之间的审核数据流。 下图说明了 CA Access Control for Virtual Environments 如何将审核事件传递给分发服务器上的消息队列，CA User Activity Reporting Module 的 CA Access Control 连接器会在该消息队列中调用、映射、转换事件，然后将事件发送到 CA User Activity Reporting Module 服务器：



1. 报告代理从本地审核文件中收集审核事件，应用任何筛选策略，然后将事件置入位于分发服务器上的审核队列。
2. CA User Activity Reporting Module 连接器与审核队列连接，并从该队列调用事件（消息）。

3. CA User Activity Reporting Module 使用数据映射和解析文件将事件映射到通用事件语法 (CEG)，然后在将事件传递到 CA User Activity Reporting Module 服务器之前应用抑制规则和总结规则。
4. CA User Activity Reporting Module 服务器接收事件，并可能会在存储事件之前应用其他抑制规则和总结规则。

注意：有关 CA User Activity Reporting Module 工作原理的详细信息，请参阅 CA User Activity Reporting Module 文档。

如何为 CA Access Control for Virtual Environments 设置 CA User Activity Reporting Module

要使用 CA User Activity Reporting Module 创建包含来自所有虚拟机的审核数据的报告，请首先实施企业报告。 您必须在与 CA User Activity Reporting Module 进行集成之前实施企业报告，因为实施企业报告在 CA Access Control 服务器上启用了报告代理。 实施了企业报告后，请为 CA Access Control for Virtual Environments 设置 CA User Activity Reporting Module。

要为 CA Access Control for Virtual Environments 安装 CA User Activity Reporting Module，请执行以下步骤：

1. 安装 CA User Activity Reporting Module 服务器

   注意：有关详细信息，请参阅 *《CA User Activity Reporting Module 实施指南》*。
2. 在 CA User Activity Reporting Module 中配置 CA User Activity Reporting Module API 证书

   从 CA Access Control 企业管理 创建与 CA User Activity Reporting Module 的连接时，您指定证书的详细信息
3. 配置 UARM 连接器 (p. 148)
4. 在 CA User Activity Reporting Module 中配置审核收集配置文件

   您可以配置自定义审核收集配置文件或使用默认的收集配置文件
5. 从 CA Access Control 企业管理 创建与 CA User Activity Reporting Module 的连接

   您配置连接设置，以便启用 CA User Activity Reporting Module 从受管设备收集审核记录
6. 在 CA Access Control 企业管理 中配置审核收集策略

连接器详细信息

在计算机上安装 CA Enterprise Log Manager 代理后，该计算机会显示在 CA Enterprise Log Manager 服务器管理界面中（例如：要查看“默认代理组”中的计算机，请单击“管理”、“日志收集”、“代理资源管理器”、“默认代理组”、*computer_name*）。 此时必须创建连接器。 此主题说明了*必须*在连接器创建向导的“连接器详细信息”页面上配置的设置。

Integration

指定要用作模板的集成。

选择适当的 CA Access Control 集成。

示例：AccessControl_R12SP5_TIBCO

可以选择性更改连接器的名称并添加说明。 然后可以将抑制规则应用到由连接器处理的事件。

注意：有关其他自定义事件收集的可选设置的信息，请参阅 *《CA Enterprise Log Manager 管理指南》*和*联机帮助*。

抑制规则和总结规则

创建连接器并指定连接器详细信息之后，可以选择性应用连接器创建向导的“应用抑制规则”页面上的抑制规则。

CA Access Control 的抑制规则和总结规则的理想模型名称是 Host IDS/IPS。 创建规则时，请根据需要选择“事件类别”、“事件类”和“事件操作”的值以识别事件。

注意：有关其他自定义事件收集的可选设置的信息，请参阅 *《CA Enterprise Log Manager 管理指南》*和*联机帮助*。 有关字段标识或各个值的详细信息，请参阅 *CA Enterprise Log Manager 联机帮助*中的“通用事件语法参考”。

连接器配置要求

创建连接器并指定连接器详细信息之后，可以配置连接器。 此主题说明了为开始收集事件，*必须*在连接器创建向导的“连接器配置”页面上配置的设置。

注意：有关其他自定义事件收集的可选设置的信息，请参阅*《CA Enterprise Log Manager 管理指南》*和*联机帮助*。

TIBCO Server

按以下格式指定消息队列（TIBCO 服务器）的主机名或 IP 地址：

协议://*服务器 IP 或名称*:*端口号*

消息队列安装在 CA Access Control 企业管理 上。

- 定义以下值：

  ssl://ACentmserver:7243

端口值和通讯方式是 CA Access Control 企业管理 使用的默认端口。如果您在安装 CA Access Control 企业管理 之后配置了不同值，请使用新配置的端口和通讯方式值。

TIBCO 用户

指定消息队列身份验证的用户名。CA Access Control 定义了一个名为“reportserver”的默认用户。

TIBCO 密码

指定消息队列身份验证的密码。输入您在安装 CA Access Control 企业管理 时在“通讯密码”对话框中定义的密码。

事件日志名称

为事件源指定日志名称。

接受默认名称“CA Access Control”。

PollInterval

指定当消息队列不可用或断开连接时代理轮询事件之前等待的秒数。

SourceName

指定“消息队列”队列的标识符。

接受默认标识符“queue_audit”。

TIBCO 队列

指定日志传感器从中读取消息（事件）的“消息队列”队列的名称。

接受默认名称“queue/audit”。

收集的线程数

指定日志传感器为读取“消息队列”消息而衍生的线程数。

调整该值时，应考虑“消息队列”队列中的事件数和 CA Enterprise Log Manager 代理系统的 CPU。

限制：最小值为 1。 日志传感器可以衍生的最大线程数为 20。

配置设置如何影响报告代理

对于 CA Enterprise Log Manager 集成，报告代理会定期从审核日志文件中收集端点审核消息，然后将这些事件传递到配置的分发服务器上的审核队列。 可以通过调整报告代理设置来影响性能。

注意：报告代理是 CA Access Control 企业报告服务的一部分，还负责发送数据库快照以用于端点报告。 此进程只说明报告代理为将审核事件传递到 CA Enterprise Log Manager 而执行的操作。

当您启用了审核收集时（将 audit_enabled 配置设置设为 1），报告代理会执行以下操作：

- 读取端点审核文件中的记录并将这些记录提交到内存，以收集新的审核记录。

  报告代理会读取您在 audit_read_chunk 配置设置中定义的审核记录数，然后在等待 audit_sleep 配置设置中定义的持续时间之后再次读取审核文件。 报告代理会读取活动审核日志*和*所有备份审核文件中之前的未读记录。 然后记住满足在审核筛选文件中定义的审核筛选的记录（audit_filter 配置设置）。

- 将内存中的一组审核记录发送到 audit_queue 配置设置中定义的分发服务器消息队列。

  如果满足以下条件之一，报告代理将发送审核记录：

  - 内存中的记录数达到由 audit_send_chunk 配置设置定义的数量。
  - 因最近一次发送审核记录而过去的时间量等于 audit_timeout 配置设置所定义的时间间隔。

示例：审核收集和传递的默认报告代理设置

此示例说明了我们如何设置默认报告代理配置设置，为何种环境设置这些设置以及它们如何影响性能。

我们希望一般环境为每秒 30 个事件 (EPS)。 因此，报告代理每过一秒钟会读取 30 个事件。 要降低对其他正在运行的应用程序（CPU 使用率和上下文开关参数）产生的影响，我们可以将报告代理设置为每 10 秒钟读取 300 个事件，如下所示：

```
audit_sleep=10
audit_read_chunk=300
```

CA Access Control 在报告代理和分发服务器之间传输消息所使用的消息总线对大数据包（发送时间间隔较长）的处理效果要好于对小数据包（发送时间间隔较短）的处理效果。 以下配置设置指定报告代理在收集的审核记录达到定义的数量时将这些记录发送到分发服务器。 假设每秒 30 个事件，如果希望报告代理大约每隔一分钟（60 秒）发送一次审核记录，我们需要按如下所示设置报告代理：

```
audit_send_chunk=1800
```

但是，在夜间或在其他时间，如果每秒的事件数小于 30，则每分钟的事件数将少于 1800。 要验证报告代理是否仍然定期将审核记录发送到分发服务器，我们将发送审核记录的最大时间间隔设置为 5 分钟，如下所示：

```
audit_timeout=300
```

从 CA Enterprise Log Manager 筛选事件

您可以使用筛选文件阻止 CA Access Control 将日志文件中的每条审核记录发送到 CA Enterprise Log Manager。 筛选文件指定了不发送到 CA Enterprise Log Manager 的审核记录。

注意：此筛选文件可以阻止 CA Access Control 将指定的审核事件发送到分发服务器，但不会使 CA Access Control 停止将审核事件写入本地文件。 要从本地审核文件中筛选出审核事件，请修改由 logmgr 部分的 AuditFiltersFile 配置设置定义的文件（默认为 audit.cfg）中的筛选规则。

要从 CA Enterprise Log Manager 中筛选事件，请编辑端点上的审核筛选文件。 如果要将相同的筛选规则应用于多个端点，建议您创建审核筛选策略，然后将该策略分配给希望策略生效的端点。

注意：有关详细信息，请参阅*《参考指南》*。

示例：审核筛选策略

此示例为您展示了审核筛选策略的格式：

```
env config
er config auditrouteflt.cfg line+("FILE;*;*;R;P")
```

此策略会将以下行写入 auditrouteflt.cfg 文件：

```
FILE;*;*;R;P
```

此行可筛选用于记录在任何访问者试图对任何文件资源进行读取时，得到允许的访问尝试的审核记录。 CA Access Control 不会将这些审核记录发送到分发服务器。

使用 SSL 进行安全通讯

安装 CA Access Control 企业管理 时，您可以选择使用 SSL 保护分发服务器与报告代理之间通讯的安全，或选择不保护通讯安全。 无论选择哪个选项，在端点上安装报告代理时都必须指定相同选项。

例如：如果使用 SSL 加密报告代理与分发服务器之间的通讯（默认），则必须在安装 CA Access Control 企业管理 时提供身份验证信息，如报告代理与分发服务器进行通讯所必需的密码。

此密码为在端点上以及在“CA Enterprise Log Manager 代理连接器配置”页面中配置 CA Access Control 报告代理时提供的密码。

安装报告代理时必须提供相同的信息。 只有能够提供正确证书和密码信息的报告代理才能将事件写入分发服务器上的审核队列，从而供 CA Enterprise Log Manager 检索。

CA Enterprise Log Manager 集成的审核日志文件备份

要收集审核数据，报告代理应根据其配置设置读取 CA Access Control 审核日志文件。 报告代理以配置的时间间隔从审核日志文件中读取读取已配置数量的审核记录。 在默认的传统安装中，或者如果安装过程中未启用审核日志传递，CA Access Control 将保留一个按大小触发的审核日志备份文件。 每次审核日志达到配置的最大大小时，都会创建一个备份文件，从而覆盖现有的审核日志备份文件。 因此，备份文件有可能在报告代理读取所有记录之前即被覆盖。

我们强烈建议您将 CA Access Control 设置为保留审核日志文件的时间戳备份。 这样，CA Access Control 在备份审核日志文件达到配置的应保留审核日志文件的最大值时，才会覆盖此类文件。 这是在端点上进行安装的过程中启用审核日志传递子功能时的默认设置。

示例：审核日志备份设置

此示例说明了建议的配置设置如何影响 CA Enterprise Log Manager 集成。 当您在端点上进行安装期间启用审核日志传递子功能时，CA Access Control 将设置以下 logmgr 部分配置设置：

```
BackUp_Date=yes
audit_max_files=50
```

在此示例中，CA Access Control 会设置审核日志文件的每个备份副本的时间戳，并且最多保留 50 个备份文件。 这样就为报告代理从文件中读取所有审核记录提供了大量机会，并且为您复制备份文件以便安全保留（如果需要）提供了大量机会。

重要说明！ 如果将 audit_max_files 设置为 0，CA Access Control 将不删除备份文件，并将持续累计文件。 如果希望通过外部程序管理备份文件，请记住，默认情况下 CA Access Control 会保护这些文件。

CA Access Control 事件的查询和报告

CA Access Control 的查询、报告和操作警报编组到 CA Enterprise Log Manager 界面中的服务器资源保护标签下。

注意：有关信息，请通过 http://ca.com/support 访问 CA Enterprise Log Manager 产品页面，然后单击“CA Enterprise Log Manager - Reports - Complete List”链接。

如何在 CA Access Control 中启用 CA Enterprise Log Manager 报告

在可以查看 CA Access Control 企业管理 中的 CA Enterprise Log Manager 报告之前，您必须在 CA Access Control 企业管理 中启用 CA Enterprise Log Manager 报告功能，导出和添加 CA Enterprise Log Manager 证书，并配置从 CA Access Control 企业管理 到 CA Enterprise Log Manager 的连接。

1. 通过配置高级设置启用 CA Enterprise Log Manager 报告。
2. 导出 CA Enterprise Log Manager 受信任证书并添加到密钥存储。
3. 配置到 CA Enterprise Log Manager 的连接。
4. （可选）配置审核收集器 (p. 158)。

   如果要将 PUPM 审核事件发送到 CA Enterprise Log Manager，请配置审核收集器。

将 CA User Activity Reporting Module 受信任证书添加到密钥存储

CA User Activity Reporting Module 报告使用受信任证书进行验证。 证书会验证报告中显示的信息是否源自受信任的 CA User Activity Reporting Module 源，从而验证数据的可靠性。

注意：在您启动该程序之前，获得并安装 CA User Activity Reporting Module 信任证书。 有关安装 CA User Activity Reporting Module 信任证书的更多信息，请参阅 CA User Activity Reporting Module 文档。

完成以下步骤：

1. 在企业管理服务器上，打开命令提示符窗口并导航到以下目录：

jbossInstallDir/server/default/deploy/IdentityMinder.ear/custom/ppm/truststore

1. 输入下面的命令：

   `keytool -import -file <certificate.cert> -keystore`

   -import

   指定实用程序读取证书，并将其存储在 keystore 中。

   -file

   指定信任证书文件的完整路径名。

   将显示密码提示符。

2. 输入密钥存储密码。 默认密码为“secret”。
3. 单击“是”信任证书。

   证书即可添加到密钥存储。

配置到 CA User Activity Reporting Module 的连接

CA Access Control 企业管理 可通过与 CA User Activity Reporting Module 通讯来显示含有 CA Access Control 相关信息的报告。 要显示这些报告，您需要配置到 CA User Activity Reporting Module 的连接。

完成以下步骤：

1. 在 CA Access Control 企业管理 中，执行如下操作：
   a. 单击“系统”。
   b. 单击“连接管理”子选项卡。
   c. 在左侧的任务菜单中展开 UARM 树。

   “管理 CA User Activity Reporting Module 连接”任务会显示在可用任务列表中。
2. 单击“管理 CA User Activity Reporting Module 连接”。

   将显示“管理 CA User Activity Reporting Module 连接: *PrimaryCALMServer*”任务页面。
3. 填充该对话框中的字段。 以下字段需加以说明：

   连接名称

   标识 CA User Activity Reporting Module 连接的名称。

   说明

   （可选）定义该连接的说明。

   主机名

   定义希望 CA Access Control 企业管理 运行所在的 CA User Activity Reporting Module 主机的名称。

   示例： host1.comp.com

   端口号

   定义 CA User Activity Reporting Module 主机用于通讯的端口。

   默认值： 5250

   验证信任根证书

   指定与 CA User Activity Reporting Module 的连接是否使用由证书授权签署的信任根证书。

   注意： 请确认您是否已安装 CA User Activity Reporting Module 信任根证书以确保适当的功能。

证书名称

定义证书的名称。

密码

定义证书密码。

4. 单击“提交”。

   CA Access Control 企业管理 将保存 CA User Activity Reporting Module 连接设置。

示例：获得 CA User Activity Reporting Module 证书信息

以下示例为您显示了如何获得在 CA Access Control 企业管理 中创建和管理 CA User Activity Reporting Module 连接设置时需要提供的 CA User Activity Reporting Module 证书信息。

1. 使用以下格式在 Web 浏览器中输入 CA User Activity Reporting Module URL：

   `https://host:port/spin/calmapi/products.csp`

   示例： https://localhost:5250/spin/calmapi/products.csp

2. 输入用于登录到 CA User Activity Reporting Module 的有效用户名和密码。

3. 选择“注册”选项以在 CA User Activity Reporting Module 中注册证书。

   将显示“新产品注册”屏幕。

4. 输入证书名称和密码，然后选择“注册”。

   此时将显示一条消息，通知您已成功注册证书。

配置审核收集器

CA Access Control 企业管理 可收集审核事件（包括 PUPM 审核事件），并将其存储在中央数据库中。 您可以将 CA Access Control 企业管理 配置为将审核事件发送到 CA Enterprise Log Manager。

配置审核收集器

1. 在 CA Access Control 企业管理 中，执行如下操作：
   a. 单击“系统”。
   b. 单击“连接管理”子选项卡。
   c. 在左侧的任务菜单中展开 ELM 树。

      此时“创建审核收集器”任务会显示在可用任务列表中。
2. 单击“创建审核收集器”。

   将显示“创建审核收集器: 审核收集器搜索”屏幕。
3. （可选）按如下方式创建现有审核收集器的副本：
   a. 选择“创建类型为‘ELM 发送者’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“ELM 发送者”列表。
   c. 选择要用作新审核收集器的基础的对象。
4. 单击“确定”。

   将显示“创建审核收集器”任务页面。 如果审核收集器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. 填充该对话框中的字段。 以下字段需加以说明：

   作业启用

   指定是否启用审核收集器。

   名称

   定义审核收集器的名称。

   队列 Jndi

   定义 CA Access Control 企业管理 将审核事件消息发送到的消息队列的名称。

   示例： *queue/audit*

   休眠

   定义两次数据库查询之间的时间间隔（分钟）。

   默认值： 1

超时

定义将审核事件消息发送到消息队列的收集器超时时间（分钟）。

默认值：10

注意：一旦超过超时时间，收集器将会发送消息，即使队列中的消息数未达到在“消息块大小”字段中定义的级别也是如此。

消息块大小

定义在将消息发送到队列之前数据库中累积的最大消息数。

默认值： 100

6. 单击“提交”。

CA Access Control 企业管理 将创建审核收集器。

第 8 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 for Virtual Environments 数据和事件的信息：

- CA Access Control for Virtual Environments 报告 — 说明哪些用户可以执行哪些操作。

  CA Access Control for Virtual Environments 报告提供每个受管设备上 CA Access Control for Virtual Environments 数据库中的数据相关信息，即您在端点上部署的策略以及策略偏差。 您在 [assign the value for cabi in your book] 和 CA Access Control 企业管理 中查看 CA Access Control for Virtual Environments 报告。

- 审核报告 — 说明哪些用户执行了哪些操作。

  审核报告提供每个受管设备上的数据相关信息，即有关哪个用户在端点上执行了何种操作的信息。 您在 VMware vSphere 客户端和 CA Access Control 企业管理 中查看 CA User Activity Reporting Module 的审核报告。

  注意：有关在 CA User Activity Reporting Module 中查看审核报告的更多信息，请参阅 *《CA User Activity Reporting Module 概述指南》*。

注意：必须安装查看 CA Access Control for Virtual Environments 报告和 CA Access Control for Virtual Environments 审核报告的其他组件。 有关详细信息，请参阅 *《产品指南》*。

报告服务

通过 CA Access Control for Virtual Environments 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。 可以排定或根据需要从每个端点收集数据。 无需连接到每个端点找出谁有权访问哪项资源。 设置 CA Access Control for Virtual Environments 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，也可以使用默认情况下 CA Access Control for Virtual Environments 提供的现有报告。 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 for Virtual Environments 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，并将信息发送到驻留在 CA Access Control 服务器上的已配置消息队列中的队列。
- *消息队列*是 CA Access Control 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。
- *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。
- 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。

报告服务如何运行

通过报告服务，您可以检查从每个受管设备、用户存储和 PUPM 策略存储收集的数据。 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：

- 从每个受管设备收集数据。

  每个受管设备将报告数据发送到消息队列。

- 将数据存储在中央数据库中。

  CA Access Control for Virtual Environments 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 for Virtual Environments 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 for Virtual Environments 报告。

收集报告数据的方式

要生成报告，必须收集每个受管设备的数据。 报告服务使用报告代理，在排定的时间或在需要时从该受管设备收集数据。

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 CA Access Control 服务器发送结果。
2. 在受管设备上创建 CA Access Control 数据库的副本。

   这是报告代理使用的临时副本，以便可以在不影响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。

   这是数据库中所有对象的转储，即捕获所有数据。

4. 将 XML 版本的数据库发送到 CA Access Control 服务器。

   报告代理会将数据发送到 CA Access Control 服务器上的报告队列。

更多信息：

配置设置如何影响报告代理 (p. 150)

处理和存储数据的方式

在每个受管设备上收集数据后，会将其发送到 CA Access Control 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。

CA Access Control 服务器执行以下操作：

1. 从报告代理接收整个数据库的 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。

如何在 CA Access Control 企业管理 中查看报告

该过程解释了如何创建和查看提供受管设备相关信息的 CA Access Control for Virtual Environments 报告。 还可以在 [assign the value for cabi in your book] 中查看 CA Access Control for Virtual Environments 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 for Virtual Environments 收集的报告数据，并定义快照排定。

2. 验证您是否已经配置了进行报告的受管设备。
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。

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。

执行以下操作：

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*在线帮助*。

在 CA Access Control 企业管理 中运行报告

该报告包括 CA Access Control for Virtual Environments 在快照中捕获的数据。 在 CA Access Control for Virtual Environments 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 [assign the value for cabi in your book] 中排定周期性报告。 如果在 [assign the value for cabi in your book] 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 [assign the value for cabi in your book] 中查看它。

执行以下操作：

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. 171)

查看报告

CA Access Control for Virtual Environments 报告提供受管设备的相关信息。 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。

执行以下操作：

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)。

完成以下步骤：

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。

运行报告

打开报告界面 (BusinessObjects InfoView) 后，即可选择并运行报告。

完成以下步骤：

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。

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》*。

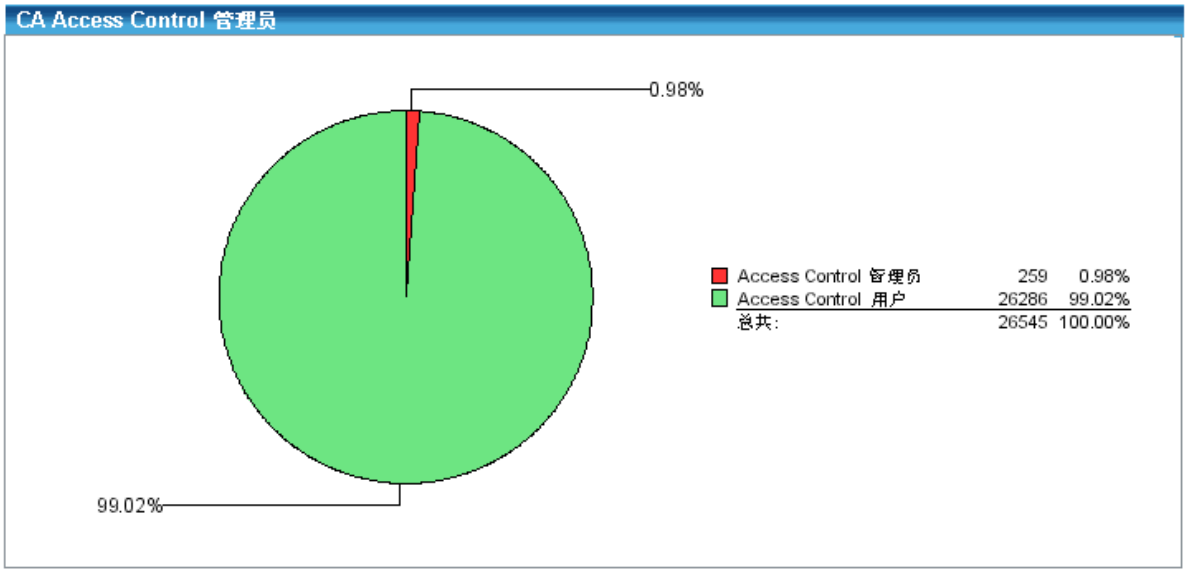
标准报告

默认情况下，CA Access Control for Virtual Environments 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。

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 Administrators

User Name	Full Name	Host ID	Has Administrator Mode	Has Password Manager Mode	Has Operator Mode
_seagent					
		SYSTEMA	yes		
		SYSTEMB	yes		
		SYSTEMC	yes		

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)

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
- 帐户
- 请求者
- 请求理由
- 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
- 帐户
- 请求者名称和 ID
- 请求理由
- 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
- 帐户
- 请求理由
- 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

CA User Activity Reporting Module 报告

CA User Activity Reporting Module 报告显示有关 CA Access Control for Virtual Environments 活动、资源管理等详细信息。

有关 CA User Activity Reporting Module 报告的详细信息，请参阅 CA User Activity Reporting Module 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。