CA Access Control

集成指南

12.8

第三方通知

示例脚本和示例 SDK 代码

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

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

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA Access Control
- CA ControlMinder
- CA Single Sign-On (eTrust SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management（CA NSM，以前为 Unicenter NSM 和 Unicenter TNG）
- CA Software Delivery（以前为 Unicenter Software Delivery）
- Unicenter Service Desk（以前为 Unicenter Service Desk）
- CA User Activity Reporting Module（以前是 [set the CALM variable for your book]）
- Identity Manager

文档约定

CA ControlMinder 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

格式	含义
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
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 ControlMinder 文档使用以下文件位置约定：

- *ACInstallDir*—默认 CA ControlMinder 安装目录。
  - Windows—C:\Program Files\CA\AccessControl\
  - UNIX—/opt/Ca/AccessControl/

- *ACSharedDir*—CA ControlMinder for UNIX 使用的默认目录。
  - UNIX—/opt/CA/AccessControlShared
- *ACServerInstallDir*—默认 CA Access Control 企业管理 安装目录。
  - /opt/CA/AccessControlServer
- *DistServerInstallDir*—默认分发服务器安装目录。
  - /opt/CA/DistributionServer
- *JBoss_HOME*—默认 JBoss 安装目录。
  - /opt/jboss-4.2.3.GA

联系技术支持

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

文档更改

从最新版本以来对该文档进行了以下更新：

- 与 ObserveIT Enterprise 集成
- 与 RSA SecurID 的集成
- 与多个 LDAP 服务器一起使用
- 与 CA SiteMinder 集成
- 与 CA AuthMinder 集成
- CA ControlMinder REST API

目录

第 9 章： CA ControlMinder REST API 93

第 1 章： 关于本指南

本部分提供有关如何将 CA Access Control 与第三方软件集成的信息。其中包括 CA User Activity Reporting Module、CA Directory、CA SiteMinder、CA AuthMinder、RSA SecurID 和 ObserveIT Enterprise。

第 2 章： 与 CA User Activity Reporting Module 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。

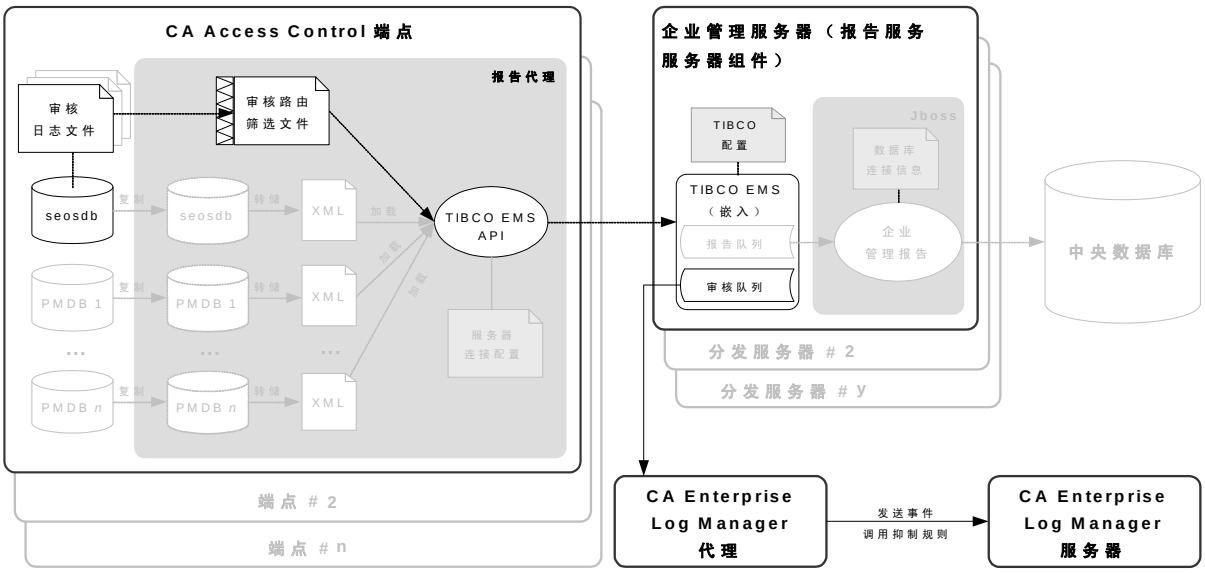
CA User Activity Reporting Module 集成体系结构

通过与 CA User Activity Reporting Module 集成，可以从每个端点发送 CA ControlMinder 审核事件，以便 CA User Activity Reporting Module 进行收集和报告。

您可以配置 CA ControlMinder，将审核事件从本地端点上的审核文件发送到分发服务器上的远程审核队列。然后可以将 CA User Activity Reporting Module 连接器配置为与审核队列连接，并从审核队列调用事件（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 ControlMinder 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：

- 每个包含 CA ControlMinder 数据库 (seosdb) 的端点都安装有报告代理组件。
- 报告代理收集来自端点的审核数据，并将它们发送到分发服务器。
- 分发服务器将审核数据累积在审核队列中。
- CA User Activity Reporting Module 代理从审核队列收集事件，并将其发送到 CA User Activity Reporting Module 服务器进行处理。

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。

注意：默认情况下，CA Access Control 企业管理 在企业管理服务器上安装分发服务器。为了实现高可用性，您可以在单独的计算机上安装分发服务器。

[set the CALM variable for your book] 集成组件

[set the CALM variable for your book] 集成使用以下 CA ControlMinder 组件。这些组件是 CA ControlMinder 企业报告服务的一部分：

- *报告代理*是一种 Windows 服务或 UNIX 后台进程，在每个 CA ControlMinder 或 UNAB 端点上运行，并将信息发送到驻留在分发服务器上的已配置消息队列中的队列。对于 [set the CALM variable for your book] 集成，报告代理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*是分发服务器的一个组件，配置用于接收报告代理发送的端点信息。为了进行报告，消息队列使用 CA ControlMinder Web 服务将端点数据库快照转发给中央数据库。要实现冗余和故障转移，您可以使用多个分发服务器收集和转发信息。

注意：默认情况下，CA Access Control 企业管理 在企业管理服务器上安装分发服务器。

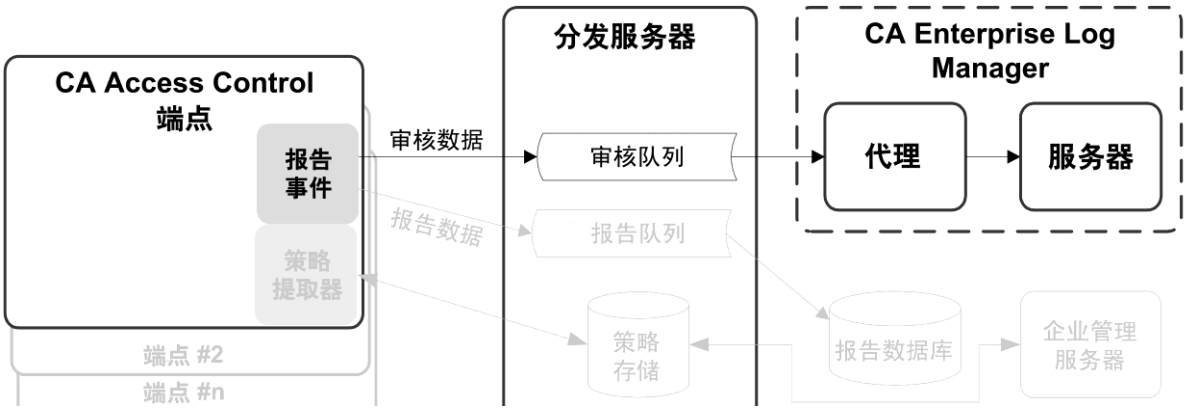
[set the CALM variable for your book] 集成还使用以下 [set the CALM variable for your book] 组件：

- *[set the CALM variable for your book] 代理*是通过连接器配置常规服务，其中每台连接器都从单个事件源中收集原始事件，然后将事件发送到 [set the CALM variable for your book] 服务器进行处理。对于 CA ControlMinder 审核数据，代理将部署 CA ControlMinder 连接器。
- *CA ControlMinder 连接器*是适用于 CA ControlMinder 审核事件源的即取即用的 [set the CALM variable for your book] 集成。连接器允许从 CA ControlMinder 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 [set the CALM variable for your book] 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 [set the CALM variable for your book] 组件的详细信息，请参阅 [set the CALM variable for your book] 文档。

审核数据如何从 CA ControlMinder 流向 [set the CALM variable for your book]

要了解 CA ControlMinder 如何与 [set the CALM variable for your book] 集成，以及配置此集成时需要考虑的事项，首先需要考虑 CA ControlMinder 与 [set the CALM variable for your book] 之间的审核数据流。下图说明了 CA ControlMinder 如何将审核事件传递给分发服务器上的消息队列，[set the CALM variable for your book] 代理的 CA ControlMinder 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 [set the CALM variable for your book] 服务器：



1. 报告代理从本地端点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. 由 [set the CALM variable for your book] 代理部署的 [set the CALM variable for your book] 连接器与审核队列连接，并从该队列调用事件（消息）。
3. [set the CALM variable for your book] 连接器和代理使用数据映射和解析文件将事件映射到通用事件语法 (CEG)，然后应用抑制规则和总结规则，之后再将事件传递到 [set the CALM variable for your book] 服务器。
4. [set the CALM variable for your book] 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 [set the CALM variable for your book] 工作原理的详细信息，请参阅 [set the CALM variable for your book] 文档。

如何为 CA ControlMinder 设置 [set the CALM variable for your book]

要使用 [set the CALM variable for your book] 创建包含来自所有 CA ControlMinder 端点的审核数据的报告，请首先实施企业报告。您必须在与 [set the CALM variable for your book] 进行集成之前实施企业报告，因为实施企业报告在您的端点上启用了报告代理。实施了企业报告后，请为 CA ControlMinder 设置 [set the CALM variable for your book]。

要为 CA ControlMinder 安装 [set the CALM variable for your book]，请执行以下步骤：

1. 安装 [set the CALM variable for your book] 服务器。

   注意：有关详细信息，请参阅*《[set the CALM variable for your book] 实施指南》*。

2. 在分发服务器上或其附近安装 [set the CALM variable for your book] 代理。

   分发服务器必须可以访问代理，并可以通过指定的端口与其进行通讯。代理还必须可以访问 [set the CALM variable for your book] 服务器。

   注意：安装 [set the CALM variable for your book] 代理之前请验证操作系统是否支持 [set the CALM variable for your book] 代理。有关安装该代理的详细信息，请参阅*《[set the CALM variable for your book] 代理安装指南》*。

3. 安装 CA Access Control 企业管理。

   注意：有关详细信息，请参阅*《实施指南》*。

4. 为代理创建一个连接器。

   安装 [set the CALM variable for your book] 代理并与 [set the CALM variable for your book] 服务器进行通讯后，创建一个连接器并对其进行配置，使连接器可以访问 CA ControlMinder 事件源（分发服务器上的审核队列）。

   注意：下列主题说明了 CA ControlMinder 事件收集所需的设置，包括为成功集成而必须配置的连接器详细信息和连接器配置要求。有关如何创建连接器的详细信息，请参阅*《[set the CALM variable for your book] 管理指南》*和*联机帮助*。

5. 创建从 CA Access Control 企业管理 到 [set the CALM variable for your book] 的连接。

6. （可选）配置审核收集器。

7. 为审核收集配置 CA ControlMinder 端点。

连接器详细信息

在计算机上安装 [set the CALM variable for your book] 代理后，该计算机会显示在 [set the CALM variable for your book] 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 ControlMinder 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*《[set the CALM variable for your book] 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 ControlMinder 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*《[set the CALM variable for your book] 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 *[set the CALM variable for your book] 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*《[set the CALM variable for your book] 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 ControlMinder 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 ControlMinder”。

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 [set the CALM variable for your book] 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 [set the CALM variable for your book] 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 ControlMinder 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 [set the CALM variable for your book] 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 ControlMinder 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 [set the CALM variable for your book] 筛选事件

您可以使用筛选文件阻止 CA ControlMinder 将日志文件中的每条审核记录发送到 [set the CALM variable for your book]。筛选文件指定了不发送到 [set the CALM variable for your book] 的审核记录。

注意：此筛选文件可以阻止 CA ControlMinder 将指定的审核事件发送到分发服务器，但不会使 CA ControlMinder 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 [set the CALM variable for your book] 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 ControlMinder 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“[set the CALM variable for your book] 代理连接器配置”页面中配置 CA ControlMinder 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 [set the CALM variable for your book] 检索。

[set the CALM variable for your book] 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 ControlMinder 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 ControlMinder 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 ControlMinder 设置为保留审核日志文件的时间戳备份。这样，CA ControlMinder 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 [set the CALM variable for your book] 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 ControlMinder 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 ControlMinder 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 ControlMinder 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 ControlMinder 会保护这些文件。

为 [set the CALM variable for your book] 集成配置现有的 Windows 端点

安装和配置了 CA Access Control 企业管理 后，您可以启用和配置报告代理，将端点配置为用于将审核数据发送到分发服务器。

注意： 安装 CA ControlMinder 时，通过报告代理可以将端点配置为收集并发送审核数据。此过程说明了如果在安装时没有配置此选项，可通过何种方式将现有的端点配置为发送审核数据。

为 [set the CALM variable for your book] 集成配置现有的 Windows 端点

1. 请依次单击“开始”、“控制面板”、“添加/删除程序”。

   将显示“添加或删除程序”对话框。

2. 滚动浏览程序列表，然后选择 CA ControlMinder。

3. 单击“更改”。

   将显示 CA ControlMinder 安装向导。

   按照向导提示修改 CA ControlMinder 安装，以便启用报告代理功能和审核传递子功能。

   核实您同时指定保留带时间戳的审核日志文件备份。

注意：启用报告代理和审核传递之后，可以修改 CA ControlMinder 配置设置以更改与性能相关的设置。执行此操作之前，应了解报告代理如何收集审核事件并将它们传递到分发服务器 (p. 22)。有关报告代理配置设置的详细信息，请参阅 *《参考指南》*。

为 CA User Activity Reporting Module 集成配置现有的 UNIX 端点

安装和配置了 CA Access Control 企业管理 后，您可以启用和配置报告代理，将端点配置为用于将审核数据发送到分发服务器。

注意：在您安装 CA ControlMinder 时，您可以配置端点进行收集和发送审核数据。该程序说明如果在安装时没有配置该选项，配置现有端点用于发送审核数据的方式。

请按下列步骤操作

1. 运行 *ACSharedDir*/lbin/report_agent.sh：

   ```
   report_agent config -server hostname [-proto {ssl|tcp}] [-port port_number
   [-rqueue queue_name] -audit -bak
   ```

   如果忽略任何配置选项，则使用默认设置。

   注意：有关 report_agent.sh 脚本的详细信息，请参阅 *《参考指南》*。

2. 在数据库中创建 *+reportagent* 用户。

   该用户应有 ADMIN 和 AUDITOR 属性和对本地终端的 *写入*访问权限。您还应将 epassword 设置为报告代理共享密钥（安装分发服务器时定义的共享密钥）。

3. 为报告代理过程创建 SPECIALPGM。

   SPECIALPGM 将 root 用户映射到 +reportagent 用户。

注意：在启用报告代理和审核路由之后，您可以修改 CA ControlMinder 配置设置来更改性能相关的设置。执行此操作之前，应了解报告代理如何收集审核事件并将它们传递到分发服务器 (p. 22)。有关报告代理配置设置的详细信息，请参阅 *《参考指南》*。

示例：使用 selang 为 CA User Activity Reporting Module 集成配置 UNIX 端点

下列的 selang 命令向你显示，假定您启用和配置了报告代理，创建必要报告代理用户，并为报告代理过程指定特定安全权限的方式：

```
eu +reportagent admin auditor logical epassword(Report_Agent) nonative
auth terminal (terminal101) uid( +reportagent) access(w)
er specialpgm (/opt/CA/AcessControl/bin/ReportAgent) Seosuid(+reportagent) \

Nativeuid(root) pgmtype(none)
```

CA ControlMinder 事件的查询和报告

CA ControlMinder 的查询、报告和操作警报编组到 [set the CALM variable for your book] 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 [set the CALM variable for your book] 产品页面，然后单击“CA Enterprise Log Manager - Reports - Complete List”链接。

如何在 CA ControlMinder 中启用 [set the CALM variable for your book] 报告

在可以查看 CA Access Control 企业管理 中的 [set the CALM variable for your book] 报告之前，您必须在 CA Access Control 企业管理 中启用 [set the CALM variable for your book] 报告功能，导出和添加 [set the CALM variable for your book] 证书，并配置从 CA Access Control 企业管理 到 [set the CALM variable for your book] 的连接。

1. 通过配置高级设置启用 [set the CALM variable for your book] 报告。
2. 导出 [set the CALM variable for your book] 受信任证书并添加到密钥存储 (p. 28)。
3. 配置到 [set the CALM variable for your book] 的连接 (p. 29)。
4. （可选）配置审核收集器 (p. 31)。

   如果要将 共享帐户管理 审核事件发送到 [set the CALM variable for your book]，请配置审核收集器。

将 [set the CALM variable for your book] 受信任证书添加到密钥存储

[set the CALM variable for your book] 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 [set the CALM variable for your book] 源，从而验证数据的可靠性。

要查看 CA Access Control 企业管理 中的 [set the CALM variable for your book] 报告，首先要导出证书，然后再将其添加到密钥存储。

将 [set the CALM variable for your book] 受信任证书添加到密钥存储

1. 以 https://*host*:*port* 的格式在 Web 浏览器中输入 [set the CALM variable for your book] 服务器的 URL

   此时将显示安全警告对话框。

2. 单击“查看证书”。

   此时将显示“证书”对话框。

3. 单击“详细信息”、“复制到文件”。

   此时将显示证书导出向导。

4. 按照以下说明完成向导：

   - **导出文件格式**－选择“Base64 编码 X.509 (.CER)”。
   - **要导出的文件**－定义导出的证书文件的完整路径名。

     例如：C:\certificates\computer.base64.cer

   此时将显示一条消息，指示导出已成功完成。

5. 将证书导入密钥存储。例如：

   ```
   C:\jdk1.5.0\jre\lib\security>c:\jdk1.5.0\bin\keytool.exe -import -file
   computer.base64.cer -keystore
   C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\custom\ppm\tru
   ststore\ssl.keystore
   ```

6. 输入密钥存储密码。默认密码为“secret”。

7. 单击“是”信任证书。

   证书即可添加到密钥存储。

配置到 [set the CALM variable for your book] 的连接

CA Access Control 企业管理 可通过与 [set the CALM variable for your book] 通讯来显示含有 CA ControlMinder 相关信息的报告。要显示这些报告，您需要配置到 [set the CALM variable for your book] 的连接。

配置到 [set the CALM variable for your book] 的连接

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。

   “管理 [set the CALM variable for your book] 连接”任务会显示在可用任务列表中。
2. 单击“管理 [set the CALM variable for your book] 连接”。

   将显示“管理 [set the CALM variable for your book] 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 [set the CALM variable for your book] 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 [set the CALM variable for your book] 主机的名称。

   示例： host1.comp.com

   端口号

   定义 [set the CALM variable for your book] 主机用于通讯的端口。

   默认值： 5250

证书颁发机构签名的 SSL 证书

指定到 [set the CALM variable for your book] 的连接是否使用由证书颁发机构签名的 SSL 证书。

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 [set the CALM variable for your book] 连接设置。

示例：获得 [set the CALM variable for your book] 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 [set the CALM variable for your book] 连接设置时需要提供的 [set the CALM variable for your book] 证书信息。

1. 使用以下格式在 Web 浏览器中输入 [set the CALM variable for your book] 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 [set the CALM variable for your book] 的有效用户名和密码。

3. 选择“注册”选项以在 [set the CALM variable for your book] 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 共享帐户管理 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 [set the CALM variable for your book]。

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 3 章： 与 ObserveIT Enterprise 集成

此部分包含以下主题：

关于本指南

此章向您说明如何将 CA Access Control 与 ObserveIT Enterprise 会话记录程序相集成。此章说明您要记录 共享帐户管理 会话的过程和步骤。

此章针对要使用 ObserveIT Enterprise 会话记录功能的 CA ControlMinder 的安全和系统管理员。

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

第 4 章： 关于 ObserveIT 集成

CA ControlMinder 与 ObserveIT Enterprise 的 集成可扩展您对由特权帐户针对您组织中的服务器进行访问尝试的控制。ObserveIT Enterprise 会话记录软件会记录目标系统上的用户活动。当用户签出特权帐户密码并登录到端点时将开始记录，而在会话终止时（例如，当用户签入该特权帐户密码时）会结束记录。

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

通过以下链接可以从 ObserveIT 系统下载 ObserveIT Enterprise：

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

您可以在以下位置找到 ObserveIT Enterprise 文档：

产品文档

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

如何设置该集成

将 CA ControlMinder 与 ObserveIT Enterprise 会话记录软件相集成需要您采取几个步骤。在集成结束时，ObserveIT Enterprise 软件会记录所有的 共享帐户管理 会话。

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

执行以下操作来设置集成：

1. 查看 ObserveIT Enterprise 系统和安装要求。

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

2. 准备中央数据库

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

3. 配置 Internet Information Server (IIS)。

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

4. 安装 ObserveIT Enterprise 服务器组件。

   ObserveIT 应用程序服务器、代理和管理控制台也进行安装。

5. 配置 ObserveIT Enterprise 应用程序服务器。

   配置记录设置。

6. 在企业管理服务器上部署会话记录脚本。

   脚本会启用触发会话记录的 共享帐户管理 自动登录。

7. 创建服务帐户。

   创建要使用的企业管理服务器服务帐户

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

   配置连接设置来启用会话记录。

如何准备集成

在完成 ObserveIT Enterprise 应用程序服务器的安装后，准备用于 CA ControlMinder 集成的服务器。在准备 ObserveIT Enterprise 应用程序服务器后，服务器已配置为开始记录和保存 共享帐户管理 会话。

执行以下操作来准备集成：

1. 打开管理控制台。
2. 创建服务帐户。

   CA ControlMinder 使用服务帐户连接到 ObserveIT Enterprise 应用程序服务器。

打开管理控制台

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

打开管理控制台

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

   http://observeit_server_name:port/ObserveIT

   示例：

   http://observeit_server:4884/ObserveIT

2. 使用您在安装过程中指定的管理员凭据进行登录。

   此时打开 ObserveIT Enterprise 管理控制台。

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

创建服务帐户

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

创建服务帐户

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

   此时打开控制台用户屏幕。

2. 选择“创建用户”。

   此时打开“添加控制台用户”窗口。

3. 输入用户名、密码，然后确认密码。

4. 将身份验证方法设为“ObserveIT.Authentication”，将用户角色设为“Admin”。

5. 单击“添加”。

   服务帐户即被创建。

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

部署会话记录脚本

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

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

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

部署会话记录脚本

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

   JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/sso_scripts
3. 将会话记录脚本复制到 sso_scripts 目录。

   建议您在覆盖该目录中的文件之前先进行备份。
4. 选择使用新文件覆盖现有文件。

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

定义到 ObserveIT 的连接

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

定义到 ObserveIT 的连接

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

   将显示“创建连接”屏幕。

2. 输入以下详细信息：

   连接说明

   定义连接的自由文本说明

   播放 URL

   定义 ObserveIT Enterprise 应用程序服务器 URL

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

   用户 ID

   定义服务帐户用户名

   密码

   定义服务帐户密码

   高级

   指定以下高级连接设置：

   查看器页面

   指定是否显示一条消息，表示该会话记录在屏幕的顶端

   查看器参数

   指定 ObserveIt 查看器窗口的宽度和高度

   ActiveX URL

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

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

服务器 URL

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

示例：http://observeit_host:4884/ObserveITApplicationServer

3. 单击“提交”。

CA Access Control 企业管理 将创建连接。

如何记录会话

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

以下过程说明了如何记录 共享帐户管理 会话：

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

   如果这是首次使用该选项，用户需要安装 ActiveX。

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

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

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

记录会话的位置

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

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

播放会话

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

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

播放会话

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

   此时“审核特权帐户”任务显示在可用任务的列表中。

2. 选择“审核特权帐户”

   此时打开“审核特权帐户”搜索窗口。

   注意：确认已为您分配了 共享帐户管理 审核管理员角色。

3. 指定搜索标准、输入要显示的行数，然后单击“搜索”。

   将显示满足您搜索标准的任务。

4. 单击会话详细信息列中的播放图标可播放该会话。

   此时打开播放器窗口，从会话的开头播放该会话。

   注意：使用窗口底部的控件可导航该会话。

第 5 章： 与 RSA SecurID 的集成

此部分包含以下主题：

如何将 CA Access Control 企业管理 与 RSA SecurID 集成

如果贵组织使用 RSA SecurID 对用户进行身份验证，则可以使用 RSA SecurID 的功能来对用户登录到 CA Access Control 企业管理 进行身份验证。将企业管理服务器与 RSA SecurID 集成时，CA Access Control 企业管理 不会对登录的用户进行身份验证。CA Access Control 企业管理 检测到第三方程序完成了用户身份验证。

以下过程说明如何将 CA Access Control 企业管理 与 RSA SecurID 集成：

1. 准备企业管理服务器。
2. 安装支持的 Web 服务器：
   - 包含应用程序请求路由 (ARR) 模块的 Windows Internet Information Server 7.0。
   - 包含代理模块的 Linux-Apache 2.2.6 Web 服务器
3. 将 Web 服务器配置为反向代理服务器 (p. 45)。

   Web 服务器充当所有登录身份验证请求的反向代理服务器。
4. 将 RSA SecurID 配置为阻止对 CA Access Control 企业管理 的所有网络访问（从 Web 服务器访问除外）。

   RSA SecurID 可防止用户直接访问 CA Access Control 企业管理。
5. 安装企业管理服务器组件。
6. 在 CA Access Control 企业管理 中，为每位将要登录到 CA Access Control 企业管理 的 RSA SecurID 用户定义一个用户帐户。

   只需要针对那些您要授予 CA Access Control 企业管理 访问权限的用户进行定义。

   重要说明！ 如果使用的是 Active Directory，则不需要完成此步骤。

7. 在以下服务器上安装 RSA 身份验证代理：
   - (Linux) 企业管理服务器
   - Web 服务器

   RSA 身份验证代理会拦截用户访问请求，并将请求转发到 RSA 身份验证管理器。
8. 配置 RSA Web 代理，以启用 CA Access Control 企业管理 的单点登录 (SSO)。
9. 在专用主机上安装 RSA 身份验证管理器。

   RSA 身份验证管理器可对用户访问请求进行身份验证。

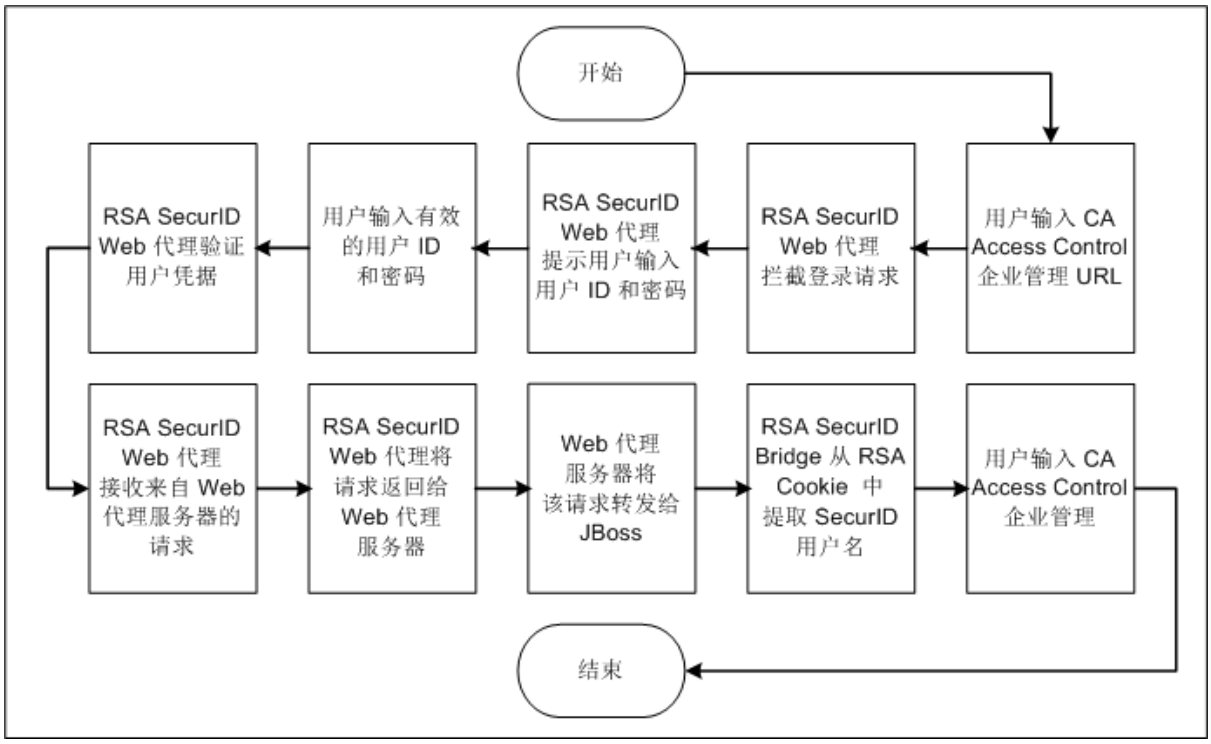
每当用户尝试登录到 CA Access Control 企业管理 时，RSA SecurID 会提示用户输入有效 RSA SecurID 凭据而不是 CA Access Control 企业管理 用户帐户详细信息。如果通过身份验证，RSA SecurID 会将用户登录到 CA Access Control 企业管理。

注意：有关 RSA SecurID Web 代理和身份验证管理器的详细信息，请参阅 RSA SecurID 网站。

RSA SecurID 如何对用户登录进行身份验证

将企业管理服务器与 RSA SecurID 集成后，每当用户登录 CA Access Control 企业管理 时，RSA SecurID 将对登录请求进行身份验证。如果 RSA SecurID 验证了用户登录，该用户将自动获取对 CA Access Control 企业管理 的访问权限。

下图说明了 RSA SecurID 如何对用户登录到 CA Access Control 企业管理进行身份验证：



将 Web 服务器配置为反向代理服务器

当用户尝试登录 CA Access Control 企业管理 时，RSA SecurID 会拦截请求，并提示用户输入有效的 SecurID 用户名和密码。安装的 Web 服务器充当反向代理服务器，用于接收来自企业管理服务器上的 RSA 身份验证 Web 代理的登录请求，并将这些请求转发到 RSA 身份验证管理器。

*反向代理*是其他服务器的网关，使一个 Web 服务器可以通过另一个 Web 服务器提供内容。

示例：将 Windows Server 2008 上的 Internet 信息服务 7.0 配置为反向代理服务器

在本示例中，系统管理员 Steve 在装有应用程序请求路由 (ARR) 模块的 Windows Server 2008 上安装了企业管理服务器和 Internet 信息服务 (IIS) 7.0。通过 ARR 模块，IIS 可以充当代理服务器。

1. Steve 启用了 Internet 信息服务服务器上的 IIS 代理设置：
   a. 依次选择“开始”、“管理工具”、“Internet 信息服务 (IIS) 管理器”

      随后将打开“Internet 信息服务 (IIS) 管理器”控制台。
   b. 从左侧窗格中选择主机，展开操作窗格，然后选择“应用程序请求路由缓存”图标。

      随后将打开“应用程序请求路由缓存”管理控制台。
   c. 从操作窗格中选择“服务器代理设置”。
   d. 选中“启用代理”复选框，然后单击“应用”。

      Steve 已启用 IIS 代理设置。

2. Steve 将 IIS 配置为将请求转发到企业管理服务器：
   a. 展开“站点”菜单，然后选择默认网站。
   b. 突出显示“URL 重写”图标，然后从“操作”菜单中选择“打开功能”。

      随后将打开“URL 重写”配置控制台。
   c. 从“操作”菜单中选择“添加规则”。

      随后将打开“添加规则”窗口。
   d. 在“入站规则”下方，选择“空白规则”，然后单击“确定”。

      随后将打开“编辑入站规则”配置窗口。
   e. 指定规则名称，然后从“模式”菜单中选择 (iam.+)。
   f. 向下滚动到“操作”部分，然后从“操作类型”菜单中选择“重写”。
   g. 在“URL 重写”字段中使用以下格式输入 CA Access Control 企业管理 URL。

      ```
      http://enterprise_host:8080/{R:0}
      ```
   h. 单击“应用”创建规则。

      现已创建新的入站规则。
   i. 从“模式”菜单使用 (castyles.+) 重复步骤 c 到 h。

      Steve 已将 IIS 配置为将请求转发到企业管理服务器。
3. Steve 配置 RSA SecurID，以保护 Web 服务器：
   a. 在“Internet 信息服务 (IIS) 管理器”控制台中选择“默认网站”，然后双击 RSA SecurID 图标。

      随后将打开 RSA SecurID 设置窗口。
   b. 选中以下复选框：
      - 在此服务器上启用 RSA SecurID Web 访问身份验证功能
      - 保护此资源
   c. 从“操作”菜单中选择“应用”

4. Steve 配置 RSA Web 代理，以启用 CA Access Control 企业管理 的单点注销 (SSO)：

   a. 打开 regedit 实用程序并导航到以下位置：

      ```
      HKEY_LOCAL_MACHINE\SOFTWARE\SDTI\RSAWebAgent
      ```

   b. 在名称 RSAUSERCustomHeader 下方，创建类型为 DWORD 的注册表键。

   c. 将注册表键值设置为 1

   Steve 已将 Internet 信息服务配置为反向代理服务器。

示例：将 Apache Web Server 2.2.6 配置为 Red Hat Enterprise Linux 5.0 上的反向代理服务器

在本示例中，系统管理员 Steve 已在 Red Hat Enterprise Linux 5.0 上安装企业管理服务器。Steve 现在需要安装 Apache Web Server 2.2.6 并将其配置为反向代理服务器。

1. Steve 执行了以下操作，以使用代理模块来安装和配置 Apache Web Server 2.2.6：

   a. 按以下方法配置 Apache Web Server 2.2.6 安装以安装代理模块：

      ```
      tar -zxvf httpd_2.2.6.tar.gz
      ./configure --prefix=/usr/local/apache --enable-proxy
      --enable-proxy-http
      make
      make install
      ```

      现已使用代理模块安装了 Apache Web Server 2.2.6。

2. Steve 通过执行以下操作来配置反向代理：

   a. 导航到 Apache Web 服务器的 conf 目录。

   b. 打开 httpd.conf 文件进行编辑。

   c. 找到 LoadModule 条目列表，并添加以下部分：

      ```
      # Used for proxy to the Enterprise Management Server
      ProxyPass       /iam http://196.168.1.1:8080/iam
      ProxyPass       /castylesr5.1.1
      http://192.168.1.1:8080/castylesr5.1.1
      ProxyPassReverse/iam http://192.168.1.1:8080/iam
      ```

   d. 保存并关闭文件。

   e. 重新启动 Apache Web 服务器。

   Steve 已将 Apache Web Server 2.2.6 配置为充当反向代理服务器。

3. Steve 配置 RSA Web 代理，以忽略用于 cookie 验证的 Web 浏览器 IP 地址：

   a. 导航到 RSA Web 代理安装目录：

      `/usr/local/apache/rsawebagent/`

   b. 运行 RSA Web 代理配置实用程序。

   c. 从列表中选择当前使用的 RSA 服务器。

   d. 浏览到第二个配置屏幕。

   e. 确认已启用“忽略用于 cookie 验证的浏览器 IP 地址”。

   Steve 已将 RSA Web 代理配置为忽略用于 cookie 验证的 Web 浏览器 IP 地址。

4. Steve 配置 RSA Web 代理，以启用 CA Access Control 企业管理 的单点注销 (SSO)：

   a. 打开 Linux Web 代理分发，然后查找以下文件：

      `rsacookieapi.tar`

   b. 将文件复制到临时目录，然后提取文件内容。

   c. 查找以下文件：

      - RSACookieAPI.jar
      - librsacookieapi.so

   d. 将 librsacookieapi.so 文件复制到以下位置，其中 *JBOSS_HOME* 表示 Steve 安装 Jboss 的位置：

      JBOSS_HOME`/server/default/deploy/IderntityMinder.ear/library`

   e. 将 RSACookieAPI.jar 文件复制到以下位置：

      `JBOSS_HOME/server/default/deploy/IderntityMinder.ear/user_console.war/WEB-INF/lib/`

   Steve 已将 RSA Web 代理配置为启用 CA Access Control 企业管理 的 SSO。

第 6 章： 与多个 LDAP 服务器一起使用

此部分包含以下主题：

简介

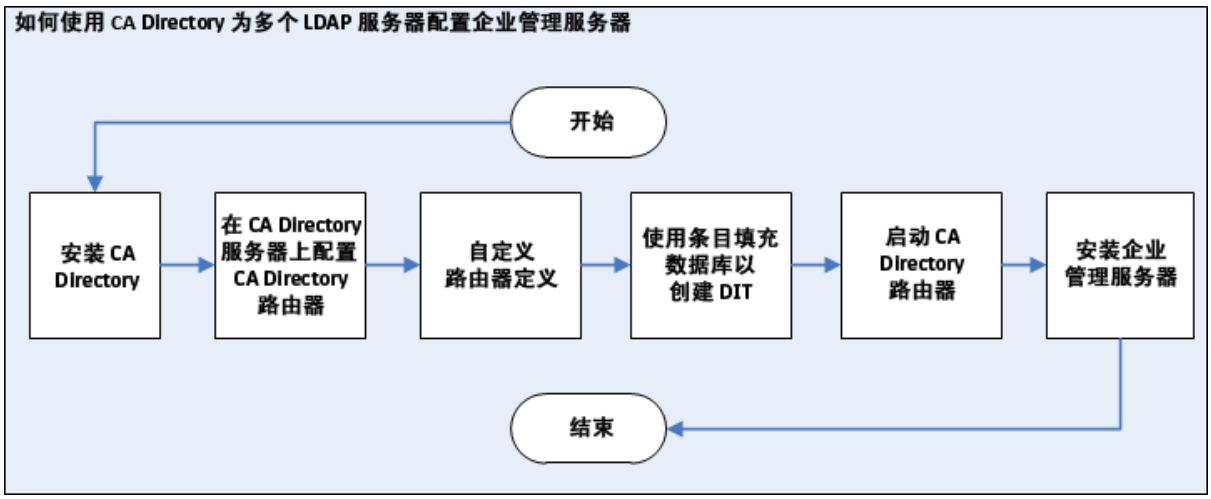
此章中该信息描述系统或数据库管理员如何将 CA Access Control 企业管理 配置为使用 CA Directory 与多个 LDAP 服务器一起使用。通过与多个 LDAP 服务器一起使用，管理员可以将多个 LDAP 用户存储集成到单个企业范围的用户存储。

如何配置多个 LDAP 服务器

CA Directory 支持将 LDAP 服务器集成到分布式目录主干。

CA Directory 提供名为 DXlink 的实用程序，该实用程序在多个 LDAP 目录服务器上启用搜索。

下图说明如何使用 CA Directory 为多个 LDAP 服务器配置 CA Access Control 企业管理：



您执行下列步骤，使用 CA Directory 为多个 LDAP 服务器配置企业管理服务器：

1. 安装 CA Directory
2. 配置 CA Directory 路由器 (p. 53)
3. 自定义 CA Directory 路由器定义 (p. 55)
4. 为数据库填充实体，创建 DIT (p. 58)
5. 启动 CA Directory
6. 安装企业管理服务器，以 Active Directory 作为用户存储

   重要说明！当您安装企业管理服务器时，请指定以下内容：

   - 主机名－指定 CA Directory 主机名
   - 端口号 -- 指定 25389
   - 基本 DN－指定环境中所有 Active Directory 服务器所共有的 DN。如不适用，请将该字段保留为空。
   - (Linux) 搜索根－指定环境中所有 Active Directory 服务器所共有的 DN。如不适用，请将该字段保留为空。
   - 管理帐户－指定 Active Directory 域之一的管理帐户。

注意：登录到 CA Access Control 企业管理 时，请验证您是否指定正在使用的管理帐户是成员的域名。

配置 CA Directory 路由器

CA Directory 将请求路由到相当于后缀的 Active Directory，该后缀在客户端请求中定义为 CA ControlMinder 使用的 Active Directory。CA Directory 使用 DXlink 实用程序路由请求。

在您完成该程序之前，您已安装两个 Active Directory 用户存储，例如：acdir1 以及 acdir2 以及名为“dsarouter”的 CA Directory。

遵循这些步骤:

1. 从 CA Directory 服务器，打开命令提示符窗口
2. 运行以下命令：

   `dxnewdsa -s 1 cadirhost-adrouter 25389`

   -s *1*

   指定 1 MB 的数据库大小

   cadirhost -adrouter

   定义路由的名称。

   25389

   指定路由器端口
3. 使用以下命令停止路由器：

   `dxserver stop cadirhost-adrouter`
4. 使用以下命令安装路由器：

   `dxserver install cadirhost-adrouter`

5. 导航到下列目录，其中 *DXHOME* 是该目录（安装路由器）的名称：

   DXHOME/config/knowledge

6. 复制 cadirhost-router.dxc 文件，如下所示：

   a. 将一个文件重命名为 acdir1-dxlink.dxc

   b. 将第二个文件重命名为 acdir2-dxlink.dxc

   c. 编辑 acdir1-dxlink.dxc 文件，如下所示：

```
set dsa "acdir1-dxlink" =
{
    prefix            = <dc "acdir1"><dc "com">
    dsa-name          = <cn "acdir1-dxlink">
    dsa-password      = "secret"
    ldap-dsa-name     = <dc "acdir1"><dc "com"><cn "users"><cn
"Administrator">
    ldap-dsa-password = "{CADIR}yKW2cVbG"
    address           = tcp "acdir1" port 389
    auth-levels       = clear-password
    trust-flags       = allow-check-password, no-server-credentials
    link-flags        = dsp-ldap, ms-ad
};
```

   ldap-dsa-name

   指定用于绑定到 Active Directory 的可分辨名称 (DN)

   ldap-dsa-password

   为 DN 定义加密密码

   注意：使用 dxpassword 实用程序加密密码。例如：dxpassword -P CADIR <*password*>。

   address

   指定 Active Directory 域控制器地址

   d. 编辑 acdir2-dxlink.dxc，如下所示：

```
set dsa "aclabcail-dxlink" =
{
    prefix            = <dc "acdir2"><dc "com">
    dsa-name          = <cn "acdir2-dxlink">
    dsa-password      = "secret"
    ldap-dsa-name     = <dc "acl"><dc "aclab"><cn "users"><cn
"Administrator">
    ldap-dsa-password = "{CADIR}yKW2cVbG"
    address           = tcp "acdir2" port 389
    auth-levels       = clear-password
    trust-flags       = allow-check-password, no-server-credentials
    link-flags        = dsp-ldap, ms-ad
};
```

您已配置 CA Directory 路由器。

自定义 CA Directory 路由器定义

在配置 CA Directory 路由器之后，您需要自定义 CA Directory 路由器定义。

遵循这些步骤:

1. 导航到以下目录，其中 *DXHOME* 是安装 CA Directory 的目录：

   DXHOME/config/limits

2. 请执行以下操作：

   a. 创建 default.dxc 文件的副本，并将原始文件重命名为 dsarouter-adrouter.dxc

   b. 从文件中删除 ReadOnly 标志

   c. 打开 dsarouter-adrouter.dxc 文件并修改以下字段：

   ```
   # 大小限制
   set max-users = 255;
   set max-local-ops = 100;
   set max-op-size = 0;

   # 时间限制
   set max-bind-time = none;
   set bind-idle-time = 3600;
   set max-op-time = 600;
   ```

   保存并关闭文件。

3. 导航至以下目录：

   DXHOME/config/settings

4. 请执行以下操作：

   a. 创建 default.dxc 文件的副本，并将原始文件重命名为 dsarouter-adrouter.dxc

   b. 从文件中删除 ReadOnly 标志

   c. 打开 dsarouter-adrouter.dxc 文件并修改以下字段：

   ```
   # 目录信息库
   set alias-integrity = true;
   # 分配控件
   set multi-casting = true;
   set always-chain-down = false;
   # 安全控件
   set min-auth = clear-password;
   set allow-binds = true;
   set ssl-auth-bypass-entry-check = false;
   # 常规控件
   set op-attrs = true;
   set transparent-routing = true;
   ```

   保存并关闭文件

5. 导航至以下目录：

   ```
   DXHOME/config/knowledge
   ```

6. 打开或创建 dsarouter-adrouter.dxc 文件并删除 auth 级字符串值“anonymous”以只启用清除密码登录。例如：

   ```
   set dsa "cadirhost-adrouter" =
   {
   prefix        = <>
   dsa-name      = <cn "cadirhost-adrouter">
   dsa-password  = "secret"
   address       = tcp "cadirhost" port 25389
   disp-psap     = DISP
   snmp-port     = 25389
   console-port  = 25390
    auth-levels   = clear-password
   ```

   保存并关闭文件。

   重要说明！如果您在定义 IPv4 和 IPv6 地址的服务器上安装 CA Directory，则在 tcp 值中指定 IPv6 和 IPv4 地址类型。例如：address = tcp "fe80::20d:56ff:fed4:8300%5" port 19389, tcp "192.168.1.1" port 19389

7. 创建名为 adrouter.dxa 的文件并添加下列行，然后保存并关闭文件：

   ```
   source "dsarouter-adrouter.dxc";
   source "acdir1-dxlink.dxc";
   source "acdir2-dxlink.dxc";
   ```

8. 导航至以下目录：

   ```
   DXHOME/config/logging
   ```

9. 请执行以下操作：

   a. 创建 default.dxc 文件副本

   b. 将原始文件重命名为 dsarouter-adrouter.dxc

   c. 删除该 ReadOnly 标志

10. 导航至以下目录：

    ```
    DXHOME/config/servers
    ```

11. 请执行以下操作：

    a. 编辑 *cadirhost*-adrouter.dxi，如下所示修改下列行，然后保存并关闭文件：

       ```
       #
       # 由 DXnewdsa 写入的初始化文件
       #
       # 记录和跟踪
       source "../logging/cadirhost-adrouter.dxc";
       ```

```
# 架构
clear schema;
source "../schema/default.dxg";
# 知识
clear dsas;
source "../knowledge/adrouter.dxg";
# 操作设置
source "../settings/cadirhost-adrouter.dxc";
# 服务限制
source "../limits/cadirhost-adrouter.dxc";
# 访问控制
clear access;
source "../access/default.dxc";
# ssl
source "../ssld/default.dxc";
# 复制协议（很少使用）
# source "../replication/";
# 多次写入 DISP 恢复
set multi-write-disp-recovery = false;
# 网格配置
set dxgrid-db-location = "data";
set dxgrid-db-size = 1;
set cache-index = all-attributes;
set lookup-cache = true;
```

注意：将 *cadirhost* 替换成 CA Directory 主机名。

您已自定义 CA Directory 路由器定义。

填充 CA Directory 数据库创建 DIT

您可以选择使用实体填充 CA Directory 数据库，以创建目录信息树 (DIT)。通过 DIT 您可以从上而下浏览组织的分层结构。

遵循这些步骤:

1. 在托管 CA Directory 路由器的服务器上，创建文件名为 input.ldif 的文件，输入以下实体，例如：

```
dn: dc=com
objectClass: domain
objectClass: top
dc: com

dn: dc=company,dc=com
objectClass: domain
objectClass: top
dc: company

dn: dc=demo
objectClass: domain
objectClass: top
dc: demo
```

2. 保存并关闭文件。
3. 打开命令提示符窗口并运行以下命令：

```
dxloaddb cadirhost-adrouter input.ldif
```

4. 运行以下命令以启动 CA Directory 路由器：

```
dxserver start cadirhost-adrouter
```

注意：将 *cadirhost* 替换成 CA Directory 主机名。

您已经以实体填充了 CA Directory 数据库，创建 DIT。

第 7 章： 与 CA SiteMinder 集成

此部分包含以下主题：

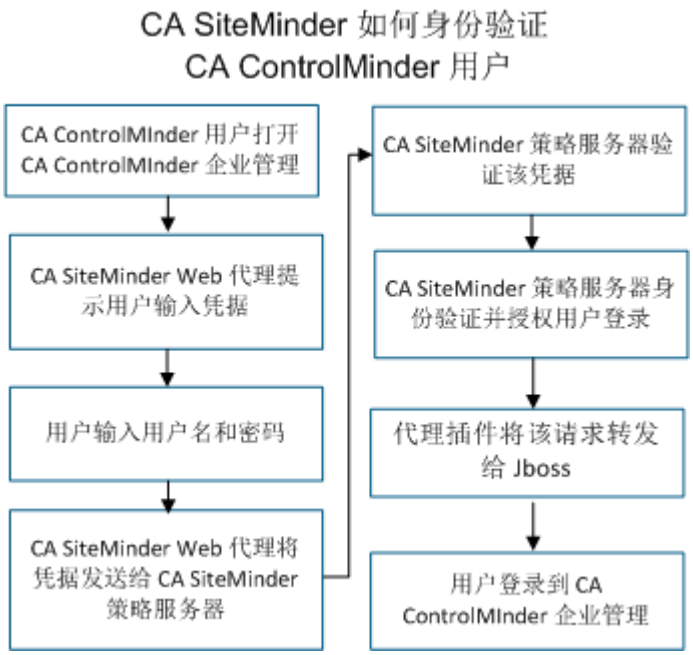
简介

该章中的信息描述系统、网络或安全管理员如何保护 CA Access Control 企业管理 以及 CA SiteMinder。CA SiteMinder 可以从 CA SiteMinder 目录验证用户，并且允许 CA ControlMinder 用户登录到 CA Access Control 企业管理。通过使用 CA SiteMinder 保护 CA Access Control 企业管理，管理员可以使用 CA SiteMinder 高级用户身份验证方法。

CA SiteMinder 验证 CA ControlMinder 用户的方式

在您使用 CA SiteMinder 保护 CA Access Control 企业管理 时，每次用户登录到 CA Access Control 企业管理，CA SiteMinder 都会验证登录请求。如果 CA SiteMinder 授权登录请求，那么用户获得访问 CA Access Control 企业管理 权限。

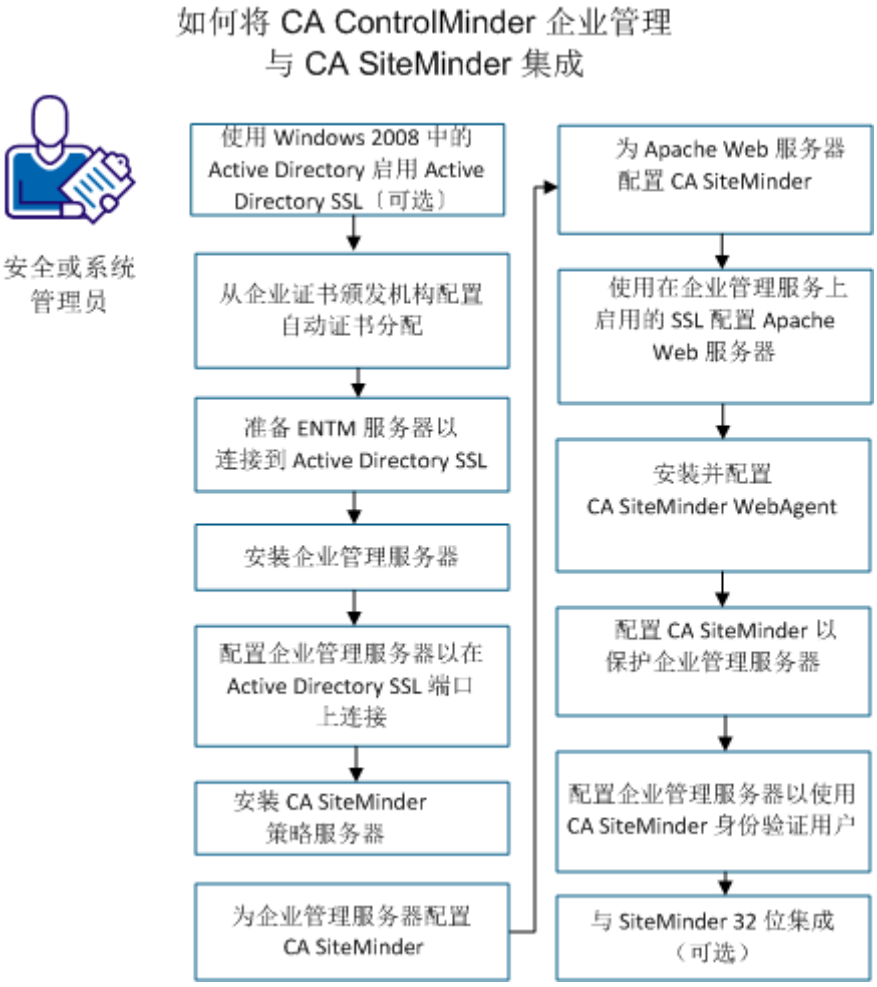
下图说明 CA SiteMinder 验证和授权 CA ControlMinder 用户登录到 CA Access Control 企业管理 的方式：



如何与 CA SiteMinder 集成

可以将 CA Access Control 企业管理与 CA SiteMinder 集成，以利用 CA SiteMinder 高级用户身份验证和授权功能。

下图说明系统或安全管理员将 CA Access Control 企业管理 与 CA SiteMinder 集成的方式：



遵循这些步骤:

1. 使用 Windows 2008 中的 Active Directory 启用 Active Directory SSL (p. 61)（可选）
2. 配置自动从企业证书颁发机构分配证书 (p. 63)
3. 准备企业管理服务器以连接到 Active Directory SSL (p. 63)
4. 安装企业管理服务器 (p. 65)

   注意：在安装企业管理服务器之前，通过安装和配置必备软件来让计算机做好准备。
5. 配置企业管理服务器以在 Active Directory SSL 端口连接 (p. 69)
6. 安装 CA SiteMinder 策略服务器 (p. 71)
7. 为企业管理服务器配置 CA SiteMinder (p. 72)
8. 配置企业管理服务器上的 Apahce Web 服务器代理插件 (p. 72)
9. 为 Apache Web 服务器配置 CA SiteMinder (p. 74)
10. 配置 CA SiteMinder Web 代理 (p. 76)
11. 配置 CA SiteMinder 以保护企业管理服务器 (p. 77)
12. 配置企业管理服务器以使用 CA SiteMinder 验证用户身份 (p. 79)
13. 与 32 位 CA SiteMinder 集成 (p. 82)

注意：有关 CA SiteMinder 策略服务器、Web 代理和管理员 UI 的详细信息，请参阅 CA SiteMinder 文档。

使用 Windows 2008 中的 Active Directory 启用 Active Directory SSL（可选）

要在使用 Active Directory 时对 CA ControlMinder 企业管理和用户之间的通信进行加密，请配置企业管理以使用 SSL。

注意：如果您正在使用 Windows 2008 上的 Active Directory，此步骤是可选的。

遵循这些步骤:

1. 在 Active Directory 计算机上，打开“服务器管理器”。从下拉菜单选择“角色”和“添加角色”，然后单击“下一步”。

   此时将打开添加角色向导的“开始之前”窗口。
2. 按以下步骤完成该向导：

   a. 选中“默认情况下跳过此页”框，然后单击“下一步”。

b. 选择“Active Directory 证书服务”，然后单击“下一步”。

此时将打开“选择角色服务”窗口。

c. 选择“证书颁发机构”，然后单击“下一步”。

此时将打开“指定安装类型”窗口。

d. 选择“企业”，然后单击“下一步”。

此时将打开“指定 CA 类型”窗口。

e. 选择“根 CA”，然后单击“下一步”。

此时将打开“设置私钥”窗口。

f. 选择“新建私钥”，然后单击“下一步”。

此时将打开“为 CA 配置加密”窗口。

g. 选择合适的加密服务提供商、哈希算法和密钥长度，然后单击“下一步”。

此时将打开“配置 CA 名称”窗口。

h. 输入公用名称，然后单击“下一步”。

此时将打开“有效期”屏幕。

i. 使用默认有效期（五年），然后单击“下一步”。

此时将打开“证书数据库”屏幕。

j. 使用默认证书数据库和登录位置，然后单击“下一步”。

此时将打开“确认安装选择”屏幕。

k. 复查安装选择，然后单击“安装”。

将安装角色，安装完成。

3. 单击“完成”并重新启动计算机。
4. 单击“开始”，选择“管理工具”和“证书颁发机构”。

将启动“证书颁发机构”应用程序并打开“证书颁发机构”窗口。

5. 在左侧的“证书颁发机构”下拉菜单中，在“证书”文件夹下找到您的证书以确认证书已颁发。

配置自动从企业证书颁发机构分配证书

您可以使用自动注册来安装计算机证书。对于计算机证书的自动分配，请配置 Active Directory 域的“组策略”。

遵循这些步骤:

1. 在域控制器上，打开“Active Directory 用户和计算机”控制台。
2. 双击“Active Directory 用户和计算机”，右键单击您的 CA 域名，然后单击“属性”。
3. 在“组策略”选项卡上，单击“默认域策略”和“编辑”。
4. 导航到“计算机配置”、“Windows 设置”、“安全设置”、“公钥策略”、“自动证书申请设置”。
5. 右键单击“自动证书申请设置”。
6. 选择“新建”，然后单击“自动证书申请”。

   此时将打开“自动证书申请”向导。
7. 单击“下一步”。
8. 在“证书模板”中，单击“计算机”和“下一步”。

   您的企业根 CA 将出现在列表中。
9. 依次单击“CA”、“下一步”和“完成”。

   您现在可以将证书导入企业管理中。要创建 CA 计算机的计算机证书，请在命令提示符中键入以下命令：

   `gpupdate /target:Computer`。

准备企业管理服务器以连接到 Active Directory SSL

在与 Active Directory 一起使用时，您可以配置 CA ControlMinder 企业管理以使用 SSL 来加密企业管理和用户之间的通信。

遵循这些步骤:

1. 在 Active Directory (AD) 计算机上，执行以下操作：

   A. 从“c:\Windows\system32”中复制 ldp.exe 文件，并将其粘贴到企业管理服务器上的相同位置。

   B. 从“C:\Windows\System32\en-US”中复制 ldp.exe.mui 文件，并将其粘贴到企业管理服务器上的相同位置。

   注意：这些步骤是启动企业管理服务器上的 ldp.exe 工具所必需的。

2. 依次单击“开始”、“运行”并键入 ldp.exe。

   此时将打开 ldp.exe 连接窗口。

3. 单击“连接”和“连接”。

   此时将打开“连接”屏幕。

4. 输入您的 Active Directory 主机名和非 SSL 端口号（例如：服务器：ad1.forward.inc，端口：389），然后单击“确定”。

   连接已完成。

5. 选中 SSL 框，然后单击“确定”。

   与 Active Directory 的连接已确认。

   注意：在您检查 Active Directory SSL 连接之前，请导入 Active Directory 证书，并将其安装在企业管理服务器的根证书中。要导入 AD 证书，必须在您的 Active Directory 上配置 SSL。有关详细信息，请参阅《*实施指南*》。

6. 在 Active Directory 计算机上，依次单击“开始”、“管理工具”、“证书颁发机构”。

7. 单击“认证”，右键单击“RootCA”，然后从下拉菜单中单击“属性”。

   此时将打开“RootCA 属性”窗口。

8. 单击“查看证书”按钮。

9. 在“详细信息”选项卡上，单击“复制到文件”按钮。

   此时将打开证书导出向导。

10. 完成证书导出向导。

    证书导出向导完成时，证书文件将复制到您的 Active Directory 计算机。

11. 浏览到 Active Directory 计算机上的证书位置，并将证书文件复制到您的企业管理服务器。

12. 在您的企业管理服务器上，双击复制的证书。

13. 单击“安装证书向导”，然后单击“下一步”。

14. 选择“将所有的证书放入下列存储”，然后单击“浏览”。

    此时将打开“选择证书存储”窗口。

15. 选择“受信任的根证书颁发机构”，单击“确定”和“下一步”。

    此时将打开“正在完成证书导入向导”窗口。

16. 单击“完成”和“确定”。

    证书导入向导完成。

17. 要检查 SSL Active Directory 连接，请在企业管理服务器上依次选择“开始”、“运行”、ldp.exe。

    此时将打开 ldp.exe 连接窗口。

18. 单击工具栏中的“连接”，然后单击“连接”。

    此时将打开“连接”窗口。

19. 指定服务器和 SSL 端口号，选中“SSL”框，然后单击“确定”。

    此时将打开确认到 Active Directory 的连接是否成功的 ldaps://(服务器名称) 窗口。

在 Windows 上安装 CA Access Control 企业管理

安装 CA Access Control 企业管理 时，将会安装所有企业管理服务器组件。在安装 CA Access Control 企业管理 之前，您必须准备企业管理服务器。

建议使用先决条件工具包安装程序来启动 CA Access Control 企业管理 安装。该安装程序将会安装第三方必备软件，然后启动 CA Access Control 企业管理 安装。

注意：不能使用网络安装方式安装 CA Access Control 企业管理。请将 CA Access Control 服务器组件 DVD 的光盘 1 目录的整个内容复制到安装目录，或将驱动器映射到此 DVD。

在 Windows 上安装 CA Access Control 企业管理

1. 如果 JBoss 应用程序服务器正在运行，请将它停止。
2. 如果在装有 CA ControlMinder 的计算机上安装 CA Access Control 企业管理，请停止 CA ControlMinder 服务。
3. 将适用于 Windows 的 CA Access Control 服务器组件 DVD 插入光盘驱动器。
4. 在“产品资源管理器”中展开“组件”文件夹，选择 CA Access Control 企业管理，然后单击“安装”。

   将启动 InstallAnywhere 安装程序。

a. （可选）指定安装期间要使用的自定义 FIPS 密钥的完整路径名。

b. 打开命令提示符窗口，并在适用于 Windows 的 CA Access Control 服务器组件 DVD 上导航到 CA Access Control 企业管理 安装可执行文件。该文件位于：

```
\EnterpriseMgmt\Disk1\InstData\NoVM
```

c. 使用以下参数运行 CA Access Control 企业管理 安装可执行文件：

```
-DFIPS_KEY=full_pathname_to_FIPS_key
```

例如：要使用位于 C:\tmp\FIPS.key 的自定义 FIPS 密钥进行安装，请执行以下操作：

```
E:\EnterpriseMgmt\Disk1\InstData\NoVM\install_EntM_r125.exe
-DFIPS_KEY=C:\tmp\FIPSkey.dat
```

重要说明！ 如果安装 CA Access Control 企业管理 for High Availability，请在主要和次要企业管理服务器上指定相同的 FIPS 密钥。如果安装支持 FIPS 的 CA Access Control 企业管理 for High Availability，请指定自定义 FIPS 密钥。

将启动 InstallAnywhere 安装程序。

5. 按照需要完成该向导。以下安装输入需加以说明：

选择安装文件夹

定义安装文件夹的完整路径。

默认值：\ProgramFiles\CA\AccessControlServer\

注意：在 64 位操作系统上，默认安装文件夹是：

```
\Program Files(x86)\CA\AccessControlServer\
```

Java 开发工具包 (JDK)

定义现有 JDK 的位置。

注意：如果在使用 CA Access Control 第三方组件 DVD 安装必备软件后立即启动 CA Access Control 企业管理 安装，此向导页面将不会出现。安装实用程序将根据您在必备软件安装过程中提供的值配置本页面上的安装设置。

JBoss 应用程序服务器信息

定义要安装应用程序的 JBoss 例程。

要执行此操作，请定义以下内容：

- JBoss 文件夹，该文件夹是安装 JBoss 的顶级目录。

  例如：在 Windows 上为 C:\jboss-4.2.3.GA，在 Solaris 上为 /opt/jboss-4.2.3.GA。

- URL，这是您进行安装所在的计算机的 IP 地址或主机名。
- JBoss 使用的端口。
- JBoss 用于安全通讯 (HTTPS) 的端口。
- 命名端口号。

注意：如果在使用 CA Access Control 第三方组件 DVD 安装必备软件后立即启动 CA Access Control 企业管理 安装，此向导页面将不会出现。安装实用程序将根据您在必备软件安装过程中提供的值配置本页面上的安装设置。

通讯密码

（仅主企业管理服务器）定义用于 CA ControlMinder 企业管理服务器组件之间通讯的密码。

注意：CA Access Control 企业管理 使用通讯密码管理消息队列密钥存储和管理员帐户、处理 CA Access Control 企业管理 与端点之间的通讯以及管理 Java 连接服务器。

数据库信息

定义 RDBMS 的连接详细信息：

- **数据库类型**－指定支持的 RDBMS。
- **主机名**－定义安装 RDBMS 的主机的名称。
- **端口号**－定义指定的 RDBMS 所使用的端口。安装程序将为 RDBMS 提供默认端口。
- **服务名**－(Oracle) 定义用于在系统中标识 RDBMS 的名称。例如：对于 Oracle Database 10g，默认为 *orcl*。
- **数据库名称**－(MS SQL) 定义创建的数据库的名称。
- **用户名**－定义准备数据库时创建的用户的名称。

  注意：在准备数据库时已向此用户授予了适当的数据库权限。
- **密码**－定义在准备数据库时创建的用户的 RDBMS 密码。

安装程序先检查数据库的连接，然后再继续。

用户存储类型

定义 CA Access Control 企业管理 使用的用户存储类型。选择以下选项之一：

- **嵌入式用户存储**－CA Access Control 企业管理 将用户信息存储在 RDBMS 中。
- **Active Directory**－在下一屏幕中指定连接详细信息。
- **其他用户存储**－在 CA Access Control 企业管理 安装完成后指定用户存储配置信息。

注意：要将登录授权策略部署至 UNAB，必须选择“Active Directory”或者“其他用户存储”作为用户存储。如果选择“Active Directory”或“其他用户存储”作为用户存储，将无法在 CA Access Control 企业管理 中创建或删除用户和组。有关 UNAB 和 Active Directory 限制的详细信息，请参阅*《企业管理指南》*。

Active Directory 设置

定义 Active Directory 用户存储设置：

- **主机**－定义 Active Directory 的域控制器主机名。
- **端口**－定义默认情况下用于对 Active Directory 进行 LDAP 查询的端口，例如：389。
- **搜索根**－定义搜索根，例如：ou=DomainName、DC=com。

  注意：在目录树中，请将“搜索根”设置为至少高于为“用户 DN”和“系统用户”指定的用户可分辨名称 (DN) 一个节点。否则，企业管理启动时可能不会显示任何选项卡。
- **用户 DN**－定义用于管理 CA Access Control 企业管理 的 Active Directory 用户帐户名称。例如：CN=Administrator、cn=Users、DC=DomainName、DC=Com。

  注意：此用户将发出针对 Active Directory 的 LDAP 查询。您可以选择为此参数定义具有只读权限的用户。但是，如果定义了具有只读权限的用户，将无法在 CA Access Control 企业管理 中向用户分配管理角色或特权访问角色。而是由您修改每个角色的成员策略以指向 Active Directory 组。

- **密码**—定义用于管理 CA Access Control 企业管理 的 Active Directory 用户帐户的密码。

安装程序会先检查与 Active Directory 的连接，然后再继续。

注意: 您可以使用 DSQUERY 目录查询实用程序发现用户可分辨名称（用户 DN）。您必须在 Active Directory 服务器上运行此查询。例如：

```
dsquery user -name administrator
"CN=Administrator,CN=Users,DC=lab.DC=demo"
```

系统用户

（仅适用于 Active Directory）定义 CA Access Control 企业管理 中被分配了“系统管理员”管理角色的 Active Directory 用户的 DN。

示例：CN=SystemUser、ou=OrganizationalUnit、DC=DomainName、DC=Com

注意：默认情况下，具有“系统管理员”管理角色的用户可以在 CA Access Control 企业管理 中执行、创建和管理所有任务。有关“系统管理员”管理角色的更多信息，请参阅*《企业管理指南》*。

管理员密码

（仅适用于嵌入式用户存储）定义*超级管理员*（即 CA Access Control 企业管理 管理员）的密码。记录此密码，以便在安装完成时登录到 CA Access Control 企业管理。

注意：您可在此步骤中创建嵌入式用户存储中的超级管理员用户。在 CA Access Control 企业管理 中，将为超级管理员用户分配“系统管理员”管理角色。您首次登录 CA Access Control 企业管理 时便是以超级管理员身份登录的。有关“系统管理员”管理角色的更多信息，请参阅*《企业管理指南》*。

完成向导后，即已安装 CA Access Control 企业管理。重新启动计算机以完成 CA Access Control 企业管理 安装。

6. 选择“是，重新启动我的系统”，然后单击“完成”。

   计算机重新启动。现在可以为企业配置 CA Access Control 企业管理。

配置企业管理服务器以在 Active Directory SSL 端口连接

遵循这些步骤:

1. 停止 JBoss 服务并将服务“启动类型”设置为“手工”。
2. 导航至以下目录：

   ```
   JBoss_HOME/default/deploy/IdentityMinder.ear/management_cons
   ole.war/WEB-INF
   ```

3. 以编辑模式打开 web.xml 文件。
4. 设置 AccessFilter 部分的 <param-value>true</param-value>，然后保存并关闭。

   注意：此步骤是启用 Identity Manager 管理控制台所必需的。
5. 启动 JBoss 服务。
6. 使用 Web 浏览器，打开 Identity Manager 管理控制台，并单击“继续”。
7. 依次单击“目录”、“ac-dir”、“导出”，然后单击“保存”。
8. 指定想要保存 ac-dir.xml 文件和备份该 xml 文件的位置。
9. 以编辑模式打开其中一个 ac-dir.xml 文件并进行以下更改：

   ```
   <LDAP searchroot="DC=cmlab,DC=ca,DC=corp" secure="true"/>
   <Connection host="KUMVI10-TEST.cmlab.ca.corp" port="636"/>
   <Container objectclass="top,organizationalUnit"
   attribute="ou" value=""/>
   ```
10. 依次单击“目录”、“ac-dir”和“更新”按钮。
11. 浏览到您编辑的 ac-dir.xml 文件，然后单击“完成”。

    ac-dir 将使用新端口值进行更新。将在底部记录错误。
12. 单击“继续”。
13. 停止 JBoss 服务。
14. 备份以下位置的 ssl.keystore 文件：

    JBoss_HOME/server/default/deploy/IdentityMinder.ea/custom/ppm/truststore。
15. 使用以下命令将证书导入 JBoss 密钥存储：

    ```
    keytool -import -keystore
    "jBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/
    ppm/truststore/ssl.keystore" -alias "<ALIAS NAME>" -file
    "<Certificate File Name>.cer"
    ```
16. 输入证书密码“secret”。

    注意：在导入期间必须信任证书。
17. 使用以下行更新 run.bat 文件：

    ```
    set JAVA_OPTS=%JAVA_OPTS% -Xms256m –Xmx1408m
    -Djavax.net.ssl.trustStore="%SYSTEMDRIVE%\jboss-4.2.3.GA\ser
    ver\default\deploy\IdentityMinder.ear\custom\ppm\truststore\
    ssl.keystore"。
    ```
18. 保存文件，然后启动 JBoss。
19. 使用 Web 浏览器打开 Identity Manager 管理控制台。

20. 转到“目录”、“ac-dir”以检查并确认您的企业管理环境正与 SSL 连接。
21. 使用 SSL 端口访问企业管理 URL，并确认您能登录到企业管理。

安装 CA SiteMinder 策略服务器

要管理用户界面，请使用安装向导安装以下组件：

- CA SiteMinder 管理先决条件
- 管理用户界面 (UI)
- 策略服务器

遵循这些步骤:

1. 从管理 UI 中，双击“adminui-pre-req-12.51-win32”，然后单击“下一步”。

   此时将打开管理 UI 先决条件安装程序。

2. 完成该向导。

   此时将打开管理 UI 安装程序向导。

3. 完成管理 UI 安装程序向导。

   管理 UI 安装完成。CA SiteMinder 管理 UI 将自动打开，并且您已准备好安装策略服务器。

4. 在管理 UI 中，双击“ca-ps-12.51-win32”，然后单击“下一步”。

   将启动策略服务器向导。

5. 完成策略服务器安装向导。以下安装输入没有自带说明：

   - 在“选择功能”窗口中，选中“策略存储”框。
   - 在“策略存储”窗口中，选中“关系数据库”框。
   - 在“选择密码服务”窗口中，选中“基本密码服务”框。

   策略服务器安装完成。

   注意：初次登录管理 UI 需要对策略服务器注册管理 UI，以在两个组件之间创建受信任关系。要对策略服务器注册管理 UI，请运行 XPSRegClient 实用程序，以提供注册超级用户帐户名和 Siteminder 用户密码 (*password*-adminui-setup)。在您第一次连接时，策略服务器将验证凭据，并且创建与管理 UI 的受信任关系。

为企业管理服务器配置 CA SiteMinder

以下过程说明如何为企业管理服务器配置 CA SiteMinder 以利用 CA SiteMinder 高级用户身份验证和授权功能。

1. 使用 CA SiteMinder 管理员接口完成以下内容：
2. 依次进入“开始”、“所有程序”、“CA”、“CA SiteMinder”、“CA SiteMinder 管理 UI”。

   “CA SiteMinder 管理 UI”打开，提示用户输入用户名和密码。
3. 登录到 CA SiteMinder 管理 UI。
4. 选择“基础架构”、“主机”、“主机配置”、“创建主机配置”、“创建主机配置类型对象的副本”。
5. 选择“DefaultHostSettings 对象”，然后单击“确定”。
6. 填写以下字段：
   - **名称**－*acentmnode*-HCO
7. 移动到“配置值”框，单击“添加”并输入 CA SiteMinder 策略服务器的主机名，如下所示：

   主机：*policyserver.company.com*
8. 单击“提交”。

您已配置代理对象。接下来，安装并配置 CA SiteMinder Web 代理。

配置企业管理服务器上已启用 SSL 的 Apache Web 服务器

以下步骤说明如何在 Windows（2003、2008 或 2012）Server 上安装企业管理服务器。

首先，使用向导安装 Apache HTTP Server 2.2.22。

遵循这些步骤:

1. 要配置具有 SSL 的 Apache Web 服务器，请运行包含 openssl 的 apache2.x 的“httpd-2.2.22-win32-x86-openssl-0.9.8t.msi”安装程序。
2. 根据说明完成 Apache HTTP Server 2.2 安装向导。以下安装输入没有自带说明：
   - **服务器信息**－使用所有默认值。
   - **选择类型**－选择“典型”。

   注意：要解决端口冲突错误，请在下一步中提供唯一端口号。

接下来，配置 Apache Web 服务器代理插件：

遵循这些步骤:

1. 停止企业管理服务器上的 JBoss 应用程序服务器。
2. 导航至以下目录：

   APACHE_HOME/conf

   APACHE_HOME

   安装 Apache Web 服务器的目录。
3. 要启用代理模块并包括代理配置，请编辑 httpd.conf 文件：
   a. 取消注释以下行：

      ```
      LoadModule proxy_module modules/mod_proxy.so
      LoadModule proxy_http_module modules/mod_proxy_http.so
      ServerName
      ```

   b. 在全局配置部分的结尾处添加下列行：

      ```
      Include conf/extra/httpd-proxy-entm.conf
      ```
4. 导航至以下目录：

   APACHE_HOME/conf/extra
5. 创建名为 httpd-proxy-entm.conf 的文件，并添加下列内容，然后保存并关闭文件：

   ```
   # Proxy to CA AC ENTM
   <IfModule proxy_module>
     <IfModule proxy_http_module>
          # /iam section BEGIN
       <Proxy /iam>
         Order allow,deny
         Allow from all
       </Proxy>
       ProxyPass /iam http://acentmnode.example.com:8080/iam
       ProxyPassReverse /iam
   http://acentmnode.example.com:8080/iam
       ProxyPass /iam/
   http://acentm.examplenode.com:8080/iam/
       ProxyPassReverse /iam/
   http://acentmnode.example.com:8080/iam/
          # /iam section END
   ```

```
        # /castylesr5.1.1 section BEGIN
      <Proxy /castylesr5.1.1>
        Order allow,deny
        Allow from all
      </Proxy>
      ProxyPass /castylesr5.1.1
http://acentmnode.example.com:8080/castylesr5.1.1
      ProxyPassReverse /castylesr5.1.1
http://acentmnode.example.com:8080/castylesr5.1.1
      ProxyPass /castylesr5.1.1/
http://acentmnode.example.com:8080/castylesr5.1.1/
      ProxyPassReverse /castylesr5.1.1/
http://acentmnode.example.com:8080/castylesr5.1.1/
        # /castylesr5.1.1 section END
    </IfModule>
</IfModule>
```

注意：将 *acentmnode.example.com:port* 替换为服务器（您安装了企业管理服务器）的实际主机名和端口。

6. 重新启动 Apache Web 服务器。
7. 启动 JBoss 应用程序服务器。
8. 要确认 Apache Web 服务器成功转发请求，请浏览到企业管理服务器。使用以下 URL：

   `http://enterprise_host:port/iam/ac`

您已在企业管理服务器上配置启用 SSL 的 Apache Web 服务器代理插件。

为 Apache Web 服务器配置 CA SiteMinder

在配置企业管理服务器上的 Apache Web 服务器代理插件之后，为 Apache Web 服务器配置 CA SiteMinder

遵循这些步骤:

1. 在 CA SiteMinder 管理员界面中，依次选择“基础架构”、“代理”、“代理”、“创建代理”、“创建类型为‘代理’的新对象”。
2. 填写以下字段，然后单击“提交”：
   - **名称**－webserver-agent
   - **说明**－Web 服务器节点 Web 代理
   - **选择代理类型**－SiteMinder
   - **代理类型**－Web 代理
   - **支持 4.x 代理**－选中

   您已配置 Web 代理对象。

3. 依次选择“基础架构”、“代理”、“代理配置对象”、“创建代理配置”、“创建类型为‘代理配置’的对象副本”。
4. 选择“ApacheDefaultSettings”，单击“确定”，并执行以下操作：
   a. 填写以下字段：
      - **名称**－webservernode-ACO
   b. 从“参数”列表中，编辑“#DefaultAgentName”字段并删除名称值中的 # 字符。
   c. 如下设置代理名称值：
      - **DefaultAgentName**－webserver-agent
   d. 编辑 #LogoffUri 和 #LogOffURI 并删除名称值中的 # 字符。
   e. 如下设置值：
      - **LogoffUri**－/iam/logout.jsp
      - **LogOffURI**－/iam/logout.jsp

   注意：有关代理参数的详细信息，请参阅《CA SiteMinder Agent Configuration Guide》。
5. 单击“提交”。

   您已创建代理配置对象。

安装和配置 CA SiteMinder Web 代理

以下内容说明如何安装和配置 Apache Web 服务器的 CA SiteMinder Web 代理。

遵循这些步骤:

1. 执行以下操作以安装 CA SiteMinder Web 代理：
   a. 使用“ca-wa-12.51-win32.exe”文件，在您的企业管理服务器上安装 CA SiteMinder Web 代理。
   b. 根据说明完成安装向导并重新启动计算机。

      CA SiteMinder Web 代理已安装。
2. 接下来，执行以下操作以使用之前定义的主机和代理对象配置来配置 CA SiteMinder Web 代理：
   a. 转到“开始”、“所有程序”、“CA”、“SiteMinder”、“Web 代理配置向导”。
   b. 当出现提示时，选择“是，我想现在进行主机注册”。
   c. 输入 CA SiteMinder 管理用户名和密码。
   d. 在“信任主机名和配置对象”窗口中，执行以下步骤：
      a. 将“受信任主机名”定义为您要对 CA SiteMinder 注册的企业管理服务器。
      b. 定义之前创建的“主机配置对象”。示例：webservernode-HCO
   e. 定义策略服务器 IP 地址并单击“添加”。
   f. 选择“FIPS 兼容模式”。
   g. 在“主机配置文件位置”中单击“下一步”。

      将对 CA SiteMinder 服务器注册 Web 代理。
   h. 选择“Web 服务器:Apache 2.2.xx”。
   i. 选择您之前在 CA SiteMinder 服务器上创建的“代理配置对象”。
   j. 将“SSL 身份验证”选择为“无高级身份验证”。
   k. 选择 Yes 以启用 Web 代理。

      将安装 Web 代理。
   l. 重新启动 Apache Web 服务器

      CA SiteMinder Web 代理已配置。

配置 CA SiteMinder 以保护企业管理服务器

以下内容说明如何配置 CA SiteMinder 以保护企业管理服务器登录会话。配置用户存储，以便 CA SiteMinder 保护身份验证方案和域策略。

遵循这些步骤:

1. 请执行以下操作：
   a. 转到“开始”、“所有程序”、“CA”、“SiteMinder”、“CA SiteMinder 管理 UI”。

      此时将打开“CA SiteMinder 管理 UI”，并提示您输入用户名和密码。

   b. 输入 CA SiteMinder 管理员用户帐户的凭据。
   c. 选择“基础架构”、“目录”、“用户目录”、“创建用户目录”。
   d. 填写“常规”框中的以下字段：
      - **名称**－ac-dir
      - **说明**－访问控制用户存储
   e. 移到目录设置框并完成以下字段：
      - **命名空间**－LDAP
      - **服务器**－*directory_hostname:port*
   f. 移到管理员凭据并完成以下字段：
      - **要求凭据**－选中
      - **用户名**－绑定用户完全 DN
      - **密码**－*密码*
      - **确认密码**－*密码*
   g. 移到 LDAP 设置框并完成以下字段：
      - **根**－*searchroot*
      - **范围**－子树
      - **开始**－(&(sAMAccountName=
      - **结束**
        －)(objectclass=top)(objectclass=person)(objectclass=organizationalperson)(objectclass=user))
   h. 移到用户属性框并完成以下字段：
      - **通用 ID**－与 %USER_ID% 一致的属性名称
2. 单击“提交”。

CA SiteMinder 创建用户目录对象。

3. 选择“查看用户目录”、“ac-dir”、“查看内容”。

   用户存储条目出现。

4. 依次选择“基础架构”、“身份验证”、“身份验证方案”、“创建身份验证方案”，完成以下字段：
   - **名称**－ac-basic-auth
   - **说明**－CA Access Control 企业管理 基本身份验证
   - **身份验证方案类型**－基本模板
   - **保护级别**－5
   - **库**－smauthdir
5. 单击“提交”

   CA SiteMinder 创建身份验证方案对象。

6. 依次选择“策略”、“域”、“域”、“创建域”。
7. 指定域名。
8. 移到“用户目录”框，并单击“添加/删除”。
9. 将 ac-dir 从“可用成员”列表移到“选定成员”列表，然后单击 OK。
10. 依次选择“策略”、“领域”、“创建领域”并填写以下字段：
    - **名称**－ac-realm
    - **代理**－*webserver*-agent
    - **资源筛选**－/iam/
    - **默认资源保护**－受保护
    - **身份验证方案**－ac-basic-auth
11. 移到“规则”框，选择“创建”并完成以下字段：
    - **名称**－ac-rule
    - **资源**－*
    - **允许访问**－选择
    - **Web 代理操作**－Get, Post
12. 单击“确定”和“完成”。
13. 依次选择“策略”、“域”、“域策略”、“创建”，并填写“常规”选项卡中的以下字段：
    - **名称**－ac-policy
14. 移到“用户”选项卡并选择“添加全部”

15. 移动到“规则”选项卡，单击“添加规则”，选择“ac-rule”，然后单击“确定”。
16. 单击“确定”和“提交”创建域。

您已经配置域和领域策略。

配置企业管理服务器以使用 CA SiteMinder 验证用户身份

以下步骤说明如何为 CA SiteMinder 集成配置企业管理服务器。

注意：开始此过程之前，请在 Windows x64 操作系统上完成以下步骤：

- 从 DVD06142621E\JDK-1.6.30_x86 安装 32 位 Java
- 要指向 32 位 Java，请在 \jboss-4.2.3.GA\bin 中找到 run_idm.bat 文件并修改 JAVA_HOME 值。
- 从 \Program Files (x86)\CA\webagent\java 中复制以下文件：`smconapi.jar`、`smjavaagentapi.jar`、`smjavasdk2.jar`
- 将文件放入以下目录：\jboss-4.2.3.GA\server\default\lib

遵循这些步骤:

1. 在企业管理服务器上：
   a. 停止 JBoss 应用程序服务器。
   b. 导航到以下目录，其中 *JBOSS_HOME* 是 JBoss 的安装目录：

      JBOSS_HOME`/server/default/deploy/IdentityMinder.ear/user_console.war/WEB-INF`

   c. 打开 web.xml 文件并找到“FrameworkAuthFilter”部分。
   d. 将值修改为 false，然后保存并关闭文件。例如：

```
<filter>
  <filter-name>FrameworkAuthFilter</filter-name>

<filter-class>com.netegrity.webapp.authentication.Framew
orkLoginFilter</filter-class>
  <init-param>
    <param-name>Enable</param-name>
    <param-value>false</param-value>
  </init-param>
</filter>
```

2. 导航至以下目录：

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/policyserver.rar/META-INF

3. 请执行以下操作：

   a. 打开 ra.xml 文件，并将值设置为 true 来启用连接，如下所示：

   ```
   <config-property>
    <config-property-name>Enabled</config-property-name>

   <config-property-type>java.lang.String</config-property-type>
    <config-property-value>true</config-property-value>
   </config-property>
   ```

   b. 根据 CA SiteMinder 策略服务器配置来配置 FIPS 模式，如下所示：

   ```
   <config-property>
     <config-property-name>FIPSMode</config-property-name>

   <config-property-type>java.lang.String</config-property-type>
     <config-property-value>false</config-property-value>
   </config-property>
   ```

   c. 定义 CA SiteMinder 策略服务器主机名、IP 地址和端口号，如下所示：

   ```
   <config-property>

   <config-property-name>ConnectionURL</config-property-name>

   <config-property-type>java.lang.String</config-property-type>

   <config-property-value>policyservernode.example.com,44441,44442,44443</config-property-value>
   </config-property>
   ```

   d. 定义管理用户帐户设置，如下所示：

   ```
   <config-property>
     <config-property-name>UserName</config-property-name>

   <config-property-type>java.lang.String</config-property-type>

   <config-property-value>siteminder</config-property-value>
   </config-property
   ```

e. 运行以下目录中的密码工具：

```
/CA/AccessControlServer/IAMSuite/AccessControl/tools/Pas
swordTool
```

例如：

```
pwdTools -FIPS -p <clear_text_password> -k
JBoss_HOME/server/default/deploy/IdentityMinder.ear/conf
ig/com/netegrity/config/keys/FIPSKey.dat
```

f. 将 AdminSecret 定义为以下加密命令的输出，如下所示：

```
<config-property>

<config-property-name>AdminSecret</config-property-name>

<config-property-type>java.lang.String</config-property-
type>

<config-property-value>{AES}:gSez2/BhDGzEKWvFmzca4w==</c
onfig-property-value>
</config-property>
```

g. 将 AgentName 定义为 CA Access Control 企业管理 节点代理名称：

```
<config-property>
  <config-property-name>AgentName</config-property-name>

<config-property-type>java.lang.String</config-property-
type>

<config-property-value>webserver-agent</config-property-
value>
</config-property>
```

h. 使用下列密码工具命令加密 CA Access Control 企业管理 共享密钥：

```
ACServerInstallDir/IAMSuite/AccessControl/tools/Password
tool/pwdtools.bat -FIPS -p <your_shared_secret> -k
JBoss_HOME/server/default/deploy/IdentityMinder.ear/conf
ig/com/netegrity/config/keys/FIPSKey.dat
```

i. 将 AgentSecret 定义为以下命令的加密输出：

```
<config-property>

<config-property-name>AgentSecret</config-property-name>

<config-property-type>java.lang.String</config-property-
type>

<config-property-value>{AES}:gSez2/BhDGzEKWvFmzca4w==</c
onfig-property-value>
</config-property>
```

4. 保存并关闭文件。
5. 导航至以下目录：

   JBoss_HOME/bin

6. 编辑 run_idm.bat，并设置对 JBoss 安装路径的 %PATH% 变量：例如：

```
set
PATH=%PATH%;C:\jboss-4.2.3\server\default\deploy\IdentityMin
der.ear\library;%SystemRoot%\SYSTEM32;%SystemRoot%;%SystemRo
ot%\SYSTEM32\WBEM
```

7. 保存并关闭文件。
8. 启动 JBoss 应用程序服务器。

   您已经为 CA SiteMinder 集成配置了企业管理服务器。现在您可以浏览到 CA Access Control 企业管理 URL，并验证 CA SiteMinder 是否保护登录会话。

与 32 位 CA SiteMinder 集成

要将 64 位 CA ControlMinder 12.8 与 32 位 CA SiteMinder 集成，请遵循除配置 Web 代理步骤以外的基本配置步骤。在完成基本配置之后，执行以下步骤以允许 64 位 CA ControlMinder dll 与 32 位 CA SiteMinder dll 文件通信：

遵循这些步骤:

1. 下载最新的 Web 代理版本（12.51 CR01 32 位）。
2. 安装 Web 代理，并根据说明继续配置，跳过安装 Web 代理的步骤。

   注意：在安装之后，由于 DLL 不匹配，JBoss 将产生错误。

3. 停止 JBoss 服务。
4. 在 JBoss 计算机上安装最新的 CA SiteMinder SDK (12.51 CR01)。
5. 安装之后，导航到文件夹 \Program Files (x86)\CA\sdk 并将 bin64 文件夹中的所有 DLL 复制到 *JBoss 文件夹* /server/default/deploy/IdentityMinder.ear/library。
6. 将 lib64 文件夹中的内容复制到 *JBoss 文件夹* /server/default/deploy/IdentityMinder.ear/library。

7. 将以下五个 jar 从 java64 复制到 *JBoss 文件夹* /server/default/deploy/IdentityMinder.ear/library：
   - smagentapi.jar
   - smjavaagentapi.jar
   - SmJavaApi.jar
   - smjavasdk2.jar
   - imsjavasdk.jar
8. 如果在 /server/default/deploy/IdentityMinder.ear/library 中出现 msvcr71.dll，将其删除。
9. 确保 PATH 环境变量的第一个路径为 \Program Files (x86)\CA\sdk\bin64。
10. 下载最新的 Web 代理版本（12.51 CR01 64 位）。
11. 安装但不配置 Web 代理（选择“稍后配置”）。
12. 重新启动计算机。
13. 从 PATH 环境变量中删除 \Program Files\CA\webagent\win32\bin 路径。
14. 重新启动 Apache 服务器。

第 8 章： 与 CA AuthMinder 集成

此部分包含以下主题：

关于 CA AuthMinder 集成

CA ControlMinder 与 CA AuthMinder 集成，以便向操作系统的特权用户和其他本机用户提供强身份验证选项。

CA ControlMinder 系统管理员通过将用户添加到组中，限制来自终端的交互式会话。为了获得写入文件的权限，此组中的用户必须使用 CA ArcotID OTP（一次性密码）验证自己。

身份验证之后，CA ControlMinder 不将创建的规则应用于本机用户（“根”），而是根据其内部身份将规则应用于用户。CA ControlMinder 区分非限制、受限制和升级的用户，并将特定规则应用于他们。

- interactive_restricted 组的用户 *名*交互登录时，CA ControlMinder 标识他为“restricted_*name*”。

  示例：

  - 根用户交互式登录时，CA ControlMinder 将规则应用于用户“restricted_root”（如果指定）或应用“_default”限制的规则。
  - 根用户非交互式登录时，CA ControlMinder 将规则应用于根用户。
- 来自 interactive_restricted 组的用户将自己提升为企业名称时，CA ControlMinder 识别他为“*name2*”。

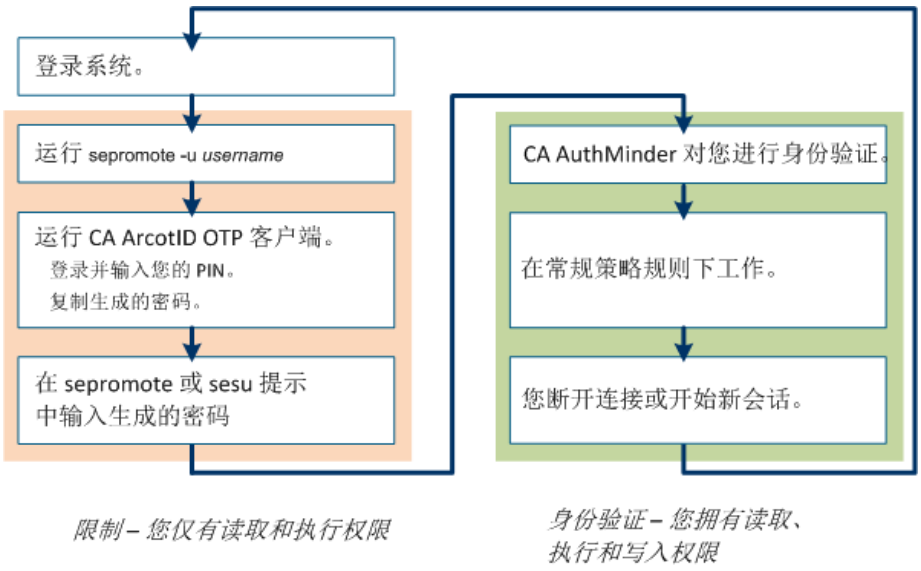
  示例：

  - 根提升为“name2”时，CA ControlMinder 将规则应用于用户“name2”。

从用户角度看到的强身份验证

通知 interactive_restricted 组中的用户，他们必须验证 CA ControlMinder 端点以便对文件获得写入权限，并可以使用 sesu 切换用户。为了验证自己的身份，用户将运行 sepromote 实用程序，并输入一次性密码 (OTP)。

注意：有关 sesu 和 sepromote 实用程序的更多信息，请参阅《*CA ControlMinder 参考指南*》的“实用程序”一章。



从用户角度来看，强身份验证如何工作：

1. 您（interactive_restricted 组中的用户）登录系统。

   您会收到您处于受限制模式的消息。Interactive_restricted 组的用户可以读取文件并执行指令。他们无法修改除了他们有权修改的预定义非文件列表 (p. 91)之外的任何文件。该消息将提醒您运行 sepromote 实用程序以删除限制。

2. 您想请求写入访问，并运行 sepromote 实用程序以进行身份验证。
   `sepromote -u username`

   sepromote 实用程序将提示您输入一次性密码。

3. 运行 CA ArcotID OTP 桌面客户端（或 CA ArcotID OTP 移动应用程序）。登录，输入您的 PIN，并生成通行码。

   注意：通行码生成是脱机过程。您的 OTP 客户端不需要连接到 CA AuthMinder 来生成通行码。

4. 在 sepromote 提示时输入密码。

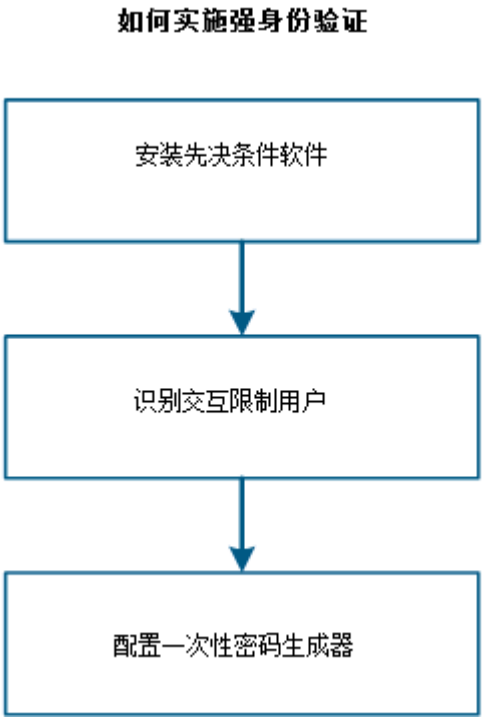
   CA AuthMinder 将验证通行码，且 sepromote 将验证您的身份。您现在在常规策略规则下工作。

5. 在断开连接和开始新会话时，您必须再次进行身份验证。

注意：如果具有当前 CA ControlMinder 版本的系统中的已验证用户登录到旧版本系统，他们将无法保留其强身份验证。

如何实施强身份验证

要实施强身份验证，您设置 CA AuthMinder 服务器、CA Adapter 和 CA ArcotID OTP 客户端。交互式受限用户需要写入权限时，他们使用一次性密码验证自己。



遵循这些步骤:

1. 安装先决条件软件 (p. 88)
2. 识别交互式受限用户 (p. 90)
3. 配置一次性密码生成器 (p. 90)

安装先决条件软件

要实施强身份验证，设置 CA AuthMinder 服务器、CA Adapter 和 CA ArcotID OTP 桌面或移动客户端。

注意：有关安装和配置必要软件的更多信息，请参阅 support.ca.com 上 CA AuthMinder 总目录中的以下文档：

- *CA AuthMinder Windows 安装指南*或 *CA AuthMinder UNIX 安装指南*
- *CA Adapter Windows 安装指南*或 *CA Adapter UNIX 安装指南*
- *CA ArcotID OTP 客户端安装指南*

安装第三方软件。

遵循这些步骤:

1. 安装 JDBC Drivers 4.0 for SQL Server (JAR)。
2. 安装 Oracle JDK。
3. 安装 Apache Tomcat 应用程序服务器。

安装 CA AuthMinder 服务器。

遵循这些步骤:

1. 配置 CA AuthMinder，以便使用配置 CA ControlMinder 端点所使用的相同用户目录。
2. 验证是否配置 MS SQL Server 使用“SQL Server 身份验证”的身份验证方法。
3. 创建新的数据库并配置数据库大小以便可以自动增加。推荐的数据库名称是“arcotdb”。

4. 打开 SQL Server Management Studio 并创建数据库用户：
   a. 浏览已创建数据库的 SQL 服务器。展开“安全”文件夹，然后单击“登录”。
   b. 右键单击“登录”，然后单击“新建登录”。
   c. 输入登录名称。推荐的名称是“arcotuser”。
   d. 指定 SQL Server 身份验证。
   e. 指定用于登录的密码和确认密码。
   f. 根据组织的密码策略，验证在此页面上是否指定其他密码设置。
   g. 将默认的数据库设置为您的 SQL 数据库“arcotdb”。
   h. 将用户映射设置为“arcotuser”（在“用户映射到此登录”部分）。
   i. 为默认数据库将用户映射 (SQL 2005) 设置到“db_owner”（在“arcotdb 的数据库角色成员”部分中）。

   您已安装 CA AuthMinder 服务器。

安装和配置 CA Adapter 和“自定义应用程序”：

遵循这些步骤:

1. 安装 CA Adapter。

   CA Adapter 安装也包括“自定义应用程序” Web 应用程序。
2. 访问 CA Adapter 配置向导，并作为主要身份验证方法使用“移动的 ArcotID OTP”创建 SAML 集成配置文件。
3. 通过访问以下 URL 运行自定义应用程序。
   `https://host_name:port/customapp/`
4. 单击“自定义应用程序”的左侧面板的“设置”。
5. 在“自定义应用程序”设置屏幕上填充各字段。
   a. 定义承载 CA AuthMinder 身份验证流管理器的应用程序服务器的协议、主机和端口。
   b. 通过选择集成配置文件“移动的 ArcotID OTP”来定义“流类型”。
   c. 单击“提交”。

您的 CA AuthMinder 安装已准备就绪与 CA ControlMinder 集成。

标识交互式受限用户

标识环境中需要强身份验证的用户。为他们提供必要的软件和凭据。

遵循这些步骤:

1. 将用户添加到 CA ControlMinder 访问者数据库中预定义的 interactive_restricted 组。

   注意：有关预定义组的详细信息，请参阅《*CA ControlMinder 端点管理指南*》中的“管理用户和组”一章。

2. 为这些用户提供自定义应用程序的 URL 及其 CA ArcotID OTP 凭据。告诉他们注册 CA ArcotID OTP（一次）。

3. 向这些用户通知有关如何使用 sesu 或 sepromote 对 CA ControlMinder 端点进行身份验证 (p. 86)的过程。

   注意：有关 sesu 和 sepromote 实用程序的更多信息，请参阅《*CA ControlMinder 参考指南*》的“实用程序”一章。

配置 CA ArcotID OTP 客户端

每次要编辑文件时，所有交互式的受限用户需要使用他们的 ArcotID OTP 凭据和生成的密码验证到 CA ControlMinder 端点。为了激活一次性密码生成器，他们需要配置 CA ArcotID OTP 移动或桌面客户端。

通知所有交互式受限用户通过执行以下程序一次，为 ArcotID OTP 注册他们自身。

遵循这些步骤:

1. 访问自定义应用程序 Web 应用程序。
   `https://hostname:port-number/customapp/`
2. 单击左侧面板的“自定义应用程序”。
3. 提交您的用户名（CA ControlMinder 端点需要验证的用户的用户名）。如果要求，请提交您的电子邮件地址。

   注意：默认情况下，CA ArcotID OTP 使用在 CA ControlMinder 和 CA AuthMinder 使用的用户目录中您的用户配置信息的电子邮件地址。

   CA ArcotID OTP 将电子邮件与激活代码一起发送以便确认您的身份。
4. 提交电子邮件和其他身份验证详细信息（如您的移动电话号码和安全问题的回复）中的激活代码。

   Web 应用程序显示您的激活详细信息：服务器 URL、用户标识符和激活代码。保留网页打开。

5. 在您的桌面或移动设备上激活 ArcotOTP，以便设置一次性密码生成器：

   a. 打开 CA ArcotID OTP 桌面客户端或 CA ArcotID OTP 移动应用程序。

   b. 单击“帐户”部分中的“添加”以添加新账户。

   c. 将身份验证值从“自定义应用程序”窗口复制和粘贴到“添加帐户”窗口，然后单击“保存”。例如：

      服务器 URL

      https://*hostname*:*port-number*/arcotafm/controller_aotp.jsp?profile=mobileotpprofile

      用户标识符

      jsmith

      激活代码

      12345678

   d. 设置 PIN 以保护您的凭据，然后单击“保存”。

   e. （可选）单击“提交”以完成自行注册。

   ArcotOTP 客户端显示您的帐户。

在 sepromote 提示您密码时，现在您已准备好生成 CA ArcotID OTP 客户端的一次性密码。

非限制文件的列表

Interactive_restricted 组的用户可以读取文件并执行指令。他们无法修改除了此预定义列表上的文件之外的任何文件。

以下文件有 AC_FILE_F_RESTRICTED_BYPASS 权限：

Linux

```
/selinux/use*
/selinux/contex**
/proc/*/loginuid
/dev/pt*
/dev/pts/*
/dev/nul*
/dev/tt*
/tmp/**
/var/run/utm*
/var/log/wtm*
/var/log/lastlo*
/proc/*/attr/exec
```

Solaris

```
/var/adm/lastlo*
/var/adm/wtmp*
/devices/pseudo/*
/var/adm/utmp*
/var/adm/sulo*
/etc/utmppip*
```

HP-UX

```
/etc/utmp*
/dev/tc*
/dev/ud*
/dev/ptm*
/dev/lo*
/dev/tt*
/var/spool/*
/var/adm/wtmp*
```

AIX

```
/etc/utm*
/dev/pt*
/dev/pts/*
/dev/nul*
/dev/tt*
/tmp/**
```

疑难解答

注意：有关详细的故障排除建议，请参阅《*CA AuthMinder Java 开发人员指南*》的“SDK 例外及错误代码”一章。

第 9 章： CA ControlMinder REST API

此部分包含以下主题：

基于 REST API

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

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

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

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

注意：有关架构的更多信息，请参阅本节中的示例。

您可以使用 REST 请求在自定义或第三方程序之间进行通讯，而 共享帐户管理 数据库忽略企业管理服务器用户界面。

HTTP 动词

如果可能，CA ControlMinder REST API 针对每个操作使用以下适当的 HTTP 动词。

GET

用于检索帐户、端点和帐户请求。

POST

用于创建帐户、端点和帐户请求。

PUT

用于更新帐户、端点和帐户请求。

DELETE

用于删除帐户、端点和帐户请求。

示例：HTTP 操作

以下内容是支持的基于 REST API 命令的架构示例：

- HTTP POST：

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

以下示例是创建帐户的 HTTP POST 正文内容：

```
<Account>
<Name>myaccount_name</Name>
<Disconnected>true</Disconnected>
<Type>Shared</Type>
<Container>MS SQL Logins</Container>
<PasswordPolicy>default password policy</PasswordPolicy>
<PasswordState>CheckedIn</PasswordState>
<Exclusive>false</Exclusive>
<ChangePasswordOnCheckOut>false</ChangePasswordOnCheckOut>
<ChangePasswordOnCheckIn>false</ChangePasswordOnCheckIn>
<LoginApplicationCheckoutOnly>false</LoginApplicationCheckoutOnly>
<Owner ownerType="Group">my_group</Owner>
</Account>
```

- HTTP GET：

```
GET /iam/api/1.0/restapi/environments/ac/endpoints/endpointname HTTP/1.1
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Host: 10.112.196.169:9998
```

- HTTP PUT：

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

以下示例是更新帐户的 HTTP PUT 正文内容：

```
<Account>
<Name>myaccount_name</Name>
<Disconnected>true</Disconnected>
<Type>Shared</Type>
```

```
<Container>MS SQL Logins</Container>
<PasswordPolicy>default password policy</PasswordPolicy>
<PasswordState>CheckedIn</PasswordState>
<Exclusive>false</Exclusive>
<ChangePasswordOnCheckOut>false</ChangePasswordOnCheckOut>
<ChangePasswordOnCheckIn>false</ChangePasswordOnCheckIn>
<LoginApplicationCheckoutOnly>false</LoginApplicationCheckoutOnly>
<Owner ownerType="Group">my_group</Owner>
</Account>
```

- HTTP DELETE：

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

基于 REST 身份验证

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

```
Authorization: Basic
c3VwZXJhZG1pbjpkZWZhdWx0c3VwZXJhZG1pbjpkZWZhdWx0
```

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

获取架构

要检索帐户请求架构，请将 HTTP GET 请求发送到以下 URL：

`https://<host_name>:18443/iam/api/1.0/restapi/schemas`

host_name

指定主机名称。

创建帐户

要创建帐户，请将 HTTP POST 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts
```

host_name

指定主机名称。

endpoint_name

指定端点名称。

以下示例显示创建帐户的 HTTP 正文内容：

```
<Account>

<Name>myaccount_name</Name>

<Disconnected>true</Disconnected>

<Type>Shared</Type>

<Container>MS SQL Logins</Container>

<PasswordPolicy>default password policy</PasswordPolicy>

<PasswordState>CheckedIn</PasswordState>

<Exclusive>false</Exclusive>

<ChangePasswordOnCheckOut>false</ChangePasswordOnCheckOut>

<ChangePasswordOnCheckIn>false</ChangePasswordOnCheckIn>

<LoginApplicationCheckoutOnly>false</LoginApplicationCheckoutOnly>

<Owner ownerType="Group">my_group</Owner>

</Account>
```

名称

指定帐户名称。

已断开连接

指定该帐户是否断开连接。

类型

指定帐户的类型。

容器

指定容器。

PasswordPolicy

指定为帐户实施的密码策略。

PasswordState

指定该帐户的密码状态。

注意：如果密码更改请求失败，则将该密码状态值指定为*不同步*。例如，如果密码重置任务正在运行，且数据库服务器关闭，则密码状态值*不同步*。

独占

指定帐户是否独占。

ChangePasswordOnCheckOut

指定在签出帐户时，是否更改密码。

ChangePasswordOnCheckIn

指定在签入帐户时，是否更改密码。

LoginApplicationCheckoutOnly

指定登录应用程序是否签出帐户。

所有者

定义所有者类型。

更新帐户

要更新帐户，请将 HTTP PUT 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

host_name

指定主机名称。

endpoint_name

指定端点名称。

account_name

指定帐户名称。

以下示例显示更新帐户的 HTTP 正文内容：

```
<Account>
<Name>myaccount_name</Name>
<Disconnected>true</Disconnected>
<Type>Shared</Type>
<Container>MS SQL Logins</Container>
<PasswordPolicy>default password policy</PasswordPolicy>
<PasswordState>CheckedIn</PasswordState>
<Exclusive>false</Exclusive>
<ChangePasswordOnCheckOut>false</ChangePasswordOnCheckOut>
<ChangePasswordOnCheckIn>false</ChangePasswordOnCheckIn>
<LoginApplicationCheckoutOnly>false</LoginApplicationCheckoutOnly>
<Owner ownerType="Group">my_group</Owner>
</Account>
```

名称

指定帐户名称。

已断开连接

指定该帐户是否断开连接。

类型

指定帐户的类型。

容器

指定容器。

PasswordPolicy

指定为帐户实施的密码策略。

PasswordState

指定该帐户的密码状态。

注意：如果密码更改请求失败，则将该密码状态值指定为*不同步*。例如，如果密码重置任务正在运行，且数据库服务器关闭，则密码状态值*不同步*。

独占

指定帐户是否独占。

ChangePasswordOnCheckOut

指定在签出帐户时，是否更改密码。

ChangePasswordOnCheckIn

指定在签入帐户时，是否更改密码。

LoginApplicationCheckoutOnly

指定登录应用程序是否签出帐户。

所有者

定义所有者类型。

删除帐户

要删除帐户，请将 HTTP DELETE 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

host_name

指定主机名称。

endpoint_name

指定端点名称。

account_name

指定帐户名称。

获取帐户

使用 GET 命令检索特定帐户。

注意：如果帐户被签出，您可以查看密码。

要检索特定帐户，请将 HTTP GET 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

使用帐户容器查询参数在检索帐户时指定支持端点的容器。

要检索有非默认的帐户容器的帐户，如 Active Directory，请将 HTTP GET 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>?account-container=<container>
```

host_name

指定主机名称。

endpoint_name

指定端点名称。

account_name

指定帐户名称。

容器

指定帐户容器名称。

获取帐户

要检索端点的特权帐户，请将 HTTP GET 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts
```

host_name

指定主机名称。

endpoint_name

指定端点名称。

签入帐户

要签入帐户，请将 HTTP PUT 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

host_name

指定主机名称。

endpoint_name

指定端点名称。

account_name

指定帐户名称。

以下示例显示签入帐户的 HTTP 正文内容：

```
<Account>

<PasswordState>Checked In</PasswordState>

</Account>
```

签出帐户

要签出帐户，请将 HTTP PUT 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

host_name

指定主机名称。

endpoint_name

指定端点名称。

account_name

指定帐户名称。

以下示例显示签出帐户的 HTTP 正文内容：

```
<Account>

<PasswordState>Checked Out</PasswordState>

</Account>
```

紧急情况帐户

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。

要紧急情况处理帐户，请将 HTTP 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>?breakglass-accounts=true
```

host_name

指定主机名称。

endpoint_name

指定端点名称。

account_name

指定帐户名称。

以下示例显示紧急情况签出帐户的 HTTP 正文内容：

```
<Account>

<PasswordState justification="my
justification">BreakGlass</PasswordState>

</Account>
```

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。

重置密码

要手动重置密码，请将 HTTP PUT 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

host_name

指定主机名称。

endpoint_name

指定端点名称。

account_name

指定帐户名称。

以下示例显示重置密码的 HTTP 正文内容：

```
<Account>
<Password auto="false">password</Password>
</Account>
```

自动重置密码

要自动重置帐户的密码，请将 HTTP PUT 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>
```

host_name

指定主机名称。

endpoint_name

指定端点名称。

account_name

指定帐户名称。

以下示例显示自动重置密码的 HTTP 正文内容：

```
<Account>
<Password auto="true"/>
</Account>
```

创建端点

要创建端点，请将 HTTP POST 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints
```

host_name

指定主机名称。

以下示例显示创建端点的 HTTP 正文内容：

```
<Endpoint>
   <Name>endpoint_name</Name>
   <EndpointType>MS SQL Server</EndpointType>
   <EndpointTypeProperties>
      <UserLogin>user1</UserLogin>
      <URL>URL Value</URL>
      <Host>Endpoint_Host_Address</Host>
      <Password>User_Password</Password>
   </EndpointTypeProperties>
   <AdministrativeAdvanced>false</AdministrativeAdvanced>

</Endpoint>
```

Name

指定端点名称。

EndpointType

指定端点类型。

UserLogin

为端点指定用户登录。

URL

指定端点的 URL 值。

Host

指定端点主机地址。

Password

指定在 UserLogin 标记中指定的端点用户的密码。

AdministrativeAdvanced

指定端点是否针对高级管理启用。

注意：*EndpointTypeProperties* 标记是动态的，且由为 *EndpointType* 标记指定的输入确定。有关如何获取动态端点类型属性的属性架构的说明，请参阅“获取端点类型” (p. 108)主题。

更新端点

要更新端点，请将 HTTP PUT 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints
```

host_name

指定主机名称。

以下示例显示更新端点的 HTTP 正文内容：

```
<Endpoint>
    <Name>endpoint_name</Name>
    <EndpointType>Endpoint_type</EndpointType>
    <EndpointTypeProperties>
        <UserLogin>user1</UserLogin>
        <URL>URL Value</URL>
        <Host>Endpoint_Host_Address</Host>
        <Password>User_Password</Password>
    </EndpointTypeProperties>
<AdministrativeAdvanced>false</AdministrativeAdvanced>
</Endpoint>
```

Name

指定端点名称。

EndpointType

指定端点类型。

UserLogin

为端点指定用户登录。

URL

指定端点的 URL 值。

Host

指定端点主机地址。

Password

指定在 UserLogin 标记中指定的端点用户的密码。

AdministrativeAdvanced

指定端点是否针对高级管理启用。

删除端点

要删除端点，请将 HTTP DELETE 请求发送到以下 URL：

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>`

host_name

指定主机名称。

endpoint_name

指定端点名称。

获取端点

要检索所有端点，请将 HTTP GET 请求发送到以下 URL：

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>`

host_name

指定主机名称。

endpoint_name

指定端点名称。

获取端点

使用获取端点命令检索所有端点。

要检索所有端点，请将 HTTP GET 请求发送到以下 URL：

`https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints`

host_name

指定主机名称。

获取端点类型

使用获取端点类型命令检索所有端点类型。

要检索所有端点类型，请将 HTTP GET 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoint-types
```

EndpointTypeProperties 标记是动态的，且由为 EndpointType 标记指定的输入确定。使用以下 URL 获取属性架构：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoint-types/<host_name>/properties-schema
```

host_name

指定主机名称。

创建帐户请求

要创建帐户请求，请将 HTTP POST 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequests
```

host_name

指定主机名称。

endpoint_name

指定端点名称。

account_name

指定帐户名称。

以下示例显示创建帐户请求的 HTTP 正文内容：

```
<AccountRequest>
    <StartTime>Start_Time</StartTime>
    <ValidUntilTime>Valid_Until_Time</ValidUntilTime>
    <User>
        <Name>user1</Name>
    </User>
    <Approver>
    <User>
        <Name>superadmin</Name>
    </User>
    </Approver>
    <Justification>user1 requests</Justification>

</AccountRequest>
```

StartTime

请求人用户可以执行共享帐户请求任务的开始时间。

采用以下格式输入日期：

```
yyyy-mm-ddThh:mm:sec
```

ValidUntilTime

指定用户可以执行共享帐户请求任务的有效时间。

采用以下格式输入日期：

```
yyyy-mm-ddThh:mm:sec
```

Name

指定请求人的用户名。

<Approver><User>Name

指定批准人的用户名。

Justification

指定理由注释。

删除帐户请求

要删除帐户请求，请将 HTTP DELETE 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequest/<account_request_name>
```

host_name

指定主机名称。

endpoint_name

指定端点名称。

account_name

指定帐户名称。

account_request_name

指定帐户请求名称。

获取请求的帐户密码

要检索用户可以请求的所有帐户密码，请将 HTTP GET 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts?to-request=true
```

host_name

指定主机名称。

endpoint_name

指定端点名称。

获取帐户请求

要检索特定帐户请求，例如：*exc-113*，将 HTTP GET 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequests/exc-113
```

要检索有权访问特权帐户 (account_name) 的所有帐户请求，将 HTTP GET 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints/<endpoint_name>/accounts/<account_name>/accountrequests
```

要在整个环境中检索所有帐户请求，请将 HTTP GET 请求发送到以下 URL：

```
https://<host_name>:18443/iam/api/1.0/restapi/environments/ac/endpoints?display=accountrequests
```

host_name

指定主机名称。

endpoint_name

指定端点名称。

account_name

指定帐户名称。