CA Access Control 高级版

实施指南

12.6

第三方通知

示例脚本和示例 SDK 代码

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

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

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA Access Control 高级版
- CA Access Control
- CA Single Sign-On (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 CA Enterprise Log Manager）
- CA Identity Manager

文档约定

CA Access Control 文档使用以下约定：

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

文档在解释命令语法和用户输入（以等宽字体显示）时还会使用以下特殊约定：

格式	含义
斜体	您必须提供的信息
用方括号括起来 ([])	可选运算符

格式	含义
用大括号括起来 ({})	强制运算符集
用管道符 (|) 分隔的选项。	分隔可选运算符（选择一项）。 例如：下面的示例*既*可以表示用户名，*也*可以表示组名： `{username|groupname}`
…	指明前面的项或项组可以重复
下划线	默认值
前面带空格的行尾反斜杠 (\)	有时，在本指南中，一行无法容纳一个命令。 在这些情况下，行结尾处的空格加上反斜杠 (\) 就表示该命令延续到下一行。 **注意：**请勿复制反斜杠字符，并且请省略换行符。 这些不是实际命令语法的一部分。

示例：命令表示法约定

下面的代码说明了在本指南中使用命令约定的方式：

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

在该示例中：

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

文件位置约定

CA Access Control 文档使用以下文件位置约定：

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

- *ACServerInstallDir*—默认 CA Access Control 企业管理 安装目录。
  - /opt/CA/AccessControlServer
- *DistServerInstallDir*—默认分发服务器安装目录。
  - /opt/CA/DistributionServer
- *JBoss_HOME*—默认 JBoss 安装目录。
  - /opt/jboss-4.2.3.GA

联系技术支持

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

文档更改

从上一版本以来对该文档进行了以下更新：

- 与 CA SiteMinder 集成 (p. 387)－新章节描述执行与 CA SiteMinder 集成的步骤
- 与多个 LDAP 服务器一起使用 (p. 379)－新章节描述如何使用 CA Directory DXlink 实用程序与多个 LDAP 服务器一起使用。

目录

第 9 章： 安装和自定义 UNAB 主机 241

第 1 章： 关于本指南

该指南提供如何计划、安装、自定义 CA Access Control 高级版 各种组件的信息。 这些信息包括 CA Access Control 服务器以及 Windows、Linux 和 CA Access Control 端点管理 组件的端点。 企业管理和报告安装章节仅适用于 CA Access Control 高级版。

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

第 2 章： 规划企业实施

此部分包含以下主题：

规划安全系统

任何安全系统的主要目标都是保护组织的信息资产。 为了有效地实施安全性，您必须知道站点中存在的威胁。 然后，必须确定如何最好地保护站点不受这些威胁侵害。

有两种基本方法可以阻止未经授权使用计算机资源：

- 阻止未经授权的用户访问系统
- 阻止有部分权限的用户访问他们没有访问权限的项目

CA Access Control 提供了同时用这两种方法保护系统的工具。 CA Access Control 还提供了审核工具，通过该工具可以跟踪用户活动，以跟踪对计算机系统的滥用尝试。

确定安全项目的目标后，可以编写安全策略说明并组建一个实施团队。 实施团队应该设置优先级，该优先级可以帮助确定必须确保哪些数据、应用程序和用户的安全。

准备实施计划

定义实施计划时，请反复检查计划的目标是否来自安全策略。 新的安全控制应该分阶段逐步进行，以便为用户提供调整时间。

- 基于安全规划定义具体目标

  定义目标，以帮助您实施安全规划。

- 将一个用户试验组定义为实施 CA Access Control 的原型。

  在保护该试验组外的实体之前，对该组中的所有 CA Access Control 功能进行测试。 对该试验组进行测试可以帮助您了解如何保护组织的其余部分。

- 确定要保护的对象

  CA Access Control 保护试验组中的业务数据、作业和用户

- 定义展开安全控制的方法

  考虑如何在尽量不破坏当前工作模式的前提下逐步采用新的安全控制。 对于各种资源和类，考虑仅审核访问权限，而不限制访问权限的一段时间。 生成的审核记录将显示哪些用户可能需要对这些资源的访问权限。

注意：有关警告模式（仅审核模式）的更多信息，请参阅*《适用于 UNIX 的端点管理指南》*和*《适用于 Windows 的端点管理指南》*。

委托管理

安装 CA Access Control 的管理决策尚不足以充分保证您站点的安全。 为了使安全项目成功，必须主动进行管理。 所谓管理，就必须决定安全策略、安全过程和要分配给安全功能的资源，以及计算机系统用户的责任。 若没有这样的管理人员支持，就会滥用安全过程，使其更像是一种日常管理事务而不是可行的保护方案。 实际上，这种情况会产生错误的安全感，导致严重的安全性暴露。

安全管理员应该与管理人员共同准备一份清楚而有内涵的安全策略说明。 该说明应包括以下内容：

- 涉及全职员工、兼职员工、合同员工和顾问的公司策略--
- 涉及系统外部用户的公司策略
- 系统所有用户的预期行为
- 物理保护注意事项

- 用户部门的安全要求
- 审核要求

生成的安全策略有助于确保 CA Access Control 实施计划既实际又与安装的安全策略一致。

决定如何保护

安装 CA Access Control 之前，确定要使用软件的哪些功能。

CA Access Control 提供下列保护方式

- 本地安全性，使用 CA Access Control 端点管理 实施已经为您所熟悉的安全功能。
- 高级本地安全性，防御更复杂的攻击。 通过 CA Access Control 可以：
  - 限制特权帐户的权限
  - 将特殊权限分配给普通用户，例如：更改特殊用户的用户密码的能力
  - 支持多种文件系统，包括 NTFS、FAT 和 CDFS
  - 跨不同环境（包含 Windows 和 UNIX 系统）集中管理安全策略和审核
- 高级策略管理，可部署您为企业创建的多规则策略（脚本文件）。 使用基于策略的该方式，您可以创建版本控制的策略，在企业的主机组中分配和取消分配策略，直接部署策略和删除部署的策略（取消部署）以及查看部署状态和部署偏差。
- 策略模型数据库 (PMDB)，通过它可以将包含用户、组和访问规则的安全数据库传播给一组订户。 PMDB 定期将收到的所有更新传播给它的订阅者。 该机制减轻了系统管理员的管理负担。
- 特权用户密码管理 (PUPM)，使您能够从中央位置对目标端点上的特权帐户进行基于角色的访问管理。 PUPM 还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。
- UNIX 身份验证代理 (UNAB)，使您能够针对 Active Directory 验证本地 UNIX 用户和组的凭据。 您可以将单个存储库用于所有的用户，使他们能够使用相同的用户名和密码登录所有平台。

教育和培训员工

安全管理员的职责之一是告诉系统用户，要在安装 CA Access Control 时不产生中断需要了解哪些知识。

每个用户需要了解的有关 CA Access Control 的详细信息量取决于您授权该用户使用的功能。 各种类型的系统用户所需的信息示例包括：

- PUPM 用户

  如何签出和签入特权帐户密码，并了解何时请求对特权帐户的访问权限以及何时执行紧急情况。

- 已在 CA Access Control 端点数据库中定义的所有用户
  - 如何通过用户名和密码向系统标识自己以及如何更改密码。 他们还必须了解他们的密码对于系统安全的重要性。
  - 如果要实施密码策略验证，请熟悉密码管理器。
  - 如何使用禁用和启用并发登录的 *secons -d-* 和 *secons -d+* 命令。*并发登录*是由同一用户从多个终端同时 de 登录至系统的多个会话。
  - 熟悉 sesudo 命令，该命令根据预定义的访问规则启用用户替换（进行或不进行密码检查）。

- 技术支持人员

  熟悉迁移注意事项，以及安装或重新安装 CA Access Control 所需的步骤。 维护数据库的用户必须熟悉数据库工具。

- 审核员

  具有 AUDITOR 属性的用户应熟悉审核工具（CA Access Control 端点管理 和 seaudit 实用程序）。

  注意：有关 seaudit 实用程序的详细信息，请参阅*《参考指南》*。

- 编写未经授权的应用程序的编程人员

  编程人员可以在他们的应用程序中使用 CA Access Control* 函数库来请求与安全相关的服务，包括控制对受保护资源的访问（使用 SEOSROUTE_RequestAuth 函数）。- 您的安装可以创建安装定义的资源类。- 如果您的安装在这些类中创建了记录，应用程序可以发出 SEOSROUTE_RequestAuth 命令，以检查用户是否有足够权限完成某操作。 特定用户操作所需的权限级别由应用程序调用 SEOSROUTE_RequestAuth 函数的方式决定。有关

  注意：有关 CA Access Control API 的详细信息，请参阅*《SDK 指南》*。

- 编写已授权应用程序的编程人员

  编写已授权应用程序（使用 SERVER 属性运行的程序）的编程人员可以使用 CA Access Control* 函数库来请求与安全相关的服务，包括：-

  - 用户身份和校验
  - 用户注销服务
  - 用户权限请求

确定实施的大小

在可以开始实施 CA Access Control 之前，您应测量实施的规模并相应地分配资源。 使用以下信息来帮助您确定实施的范围。

建议您为每 3000 个 CA Access Control 端点安装一个分发服务器。

下表描述应为企业管理服务器和报告门户计算机上的各种组件分配的数据库大小：

组件	条件	范围	分配
企业管理服务器	作为用户存储的 Active Directory	针对每 1000 个 Active Directory 帐户	20 MB
CA Access Control	报告快照	针对每 1000 个 CA Access Control 端点	每个快照 5 GB
PUPM	端点类型定义	针对每 1000 个 PUPM 端点	2 MB
PUPM	特权帐户	针对每 1000 个特权帐户	75 MB
PUPM	特权帐户密码操作	针对每 1000 个 PUPM 特权帐户密码操作	250 MB

组件	条件	范围	分配
CA Business Intelligence	CMS 和审核数据库	针对基础安装	300 MB

注意：有关系统要求的详细信息，请参阅*《版本说明》*。

CA Access Control 数据库大小限制

CA Access Control 数据库局限于一百万 (1,000,000) 个对象。 只有在大型环境中使用高级策略管理时，该大小限制才有可能影响您的部署。

如果预计企业中的 CA Access Control 数据库将拥有 100 万个对象，您需要删除不再使用的旧的 DEPLOYMENT 对象。

示例：计算 CA Access Control 数据库中对象的数目

以下示例说明如何计算可以预期在 DMS（中心 CA Access Control 管理数据库）中所具有的对象数目。

在本示例中，我们在 5000 个端点上具有 CA Access Control 的企业部署，其中每个具有 50 个分配的策略。 因此，DMS 包含至少 25 万个对象，如下所示：

```
5000 个端点 X 50 个策略 = 25 万个 DEPLOYMENT 对象
```

如果随着时间的推移，您创建每个策略的四个版本，并且把这些策略分配给 5000 个端点中的每一个，DMS 中对象的数目将到达 100 万个对象限制，如下所示：

```
5000 个端点 X 50 个策略 X 4 个版本 = 100 万个 DEPLOYMENT 对象
```

如何实施 CA Access Control 企业管理

在企业中实施 CA Access Control 企业管理 之前，您应了解要安装哪些组件、以何种顺序安装以及安装在何处。 当实施 CA Access Control 企业管理 的企业部署时，请遵循以下准则：

- 在实施过程中使用“从上到下”的方法。 从安装企业管理服务器开始，安装其他分发服务器，实施企业报告，然后安装 CA Access Control 端点。
- 开始实施之前，确认您使用的计算机满足必要的规范，并且已安装所有必要的软件。

  注意：有关所需硬件和软件规范的详细信息，请参阅 CA 支持上的 CA Access Control 产品页面提供的 CA Access Control 兼容性列表。

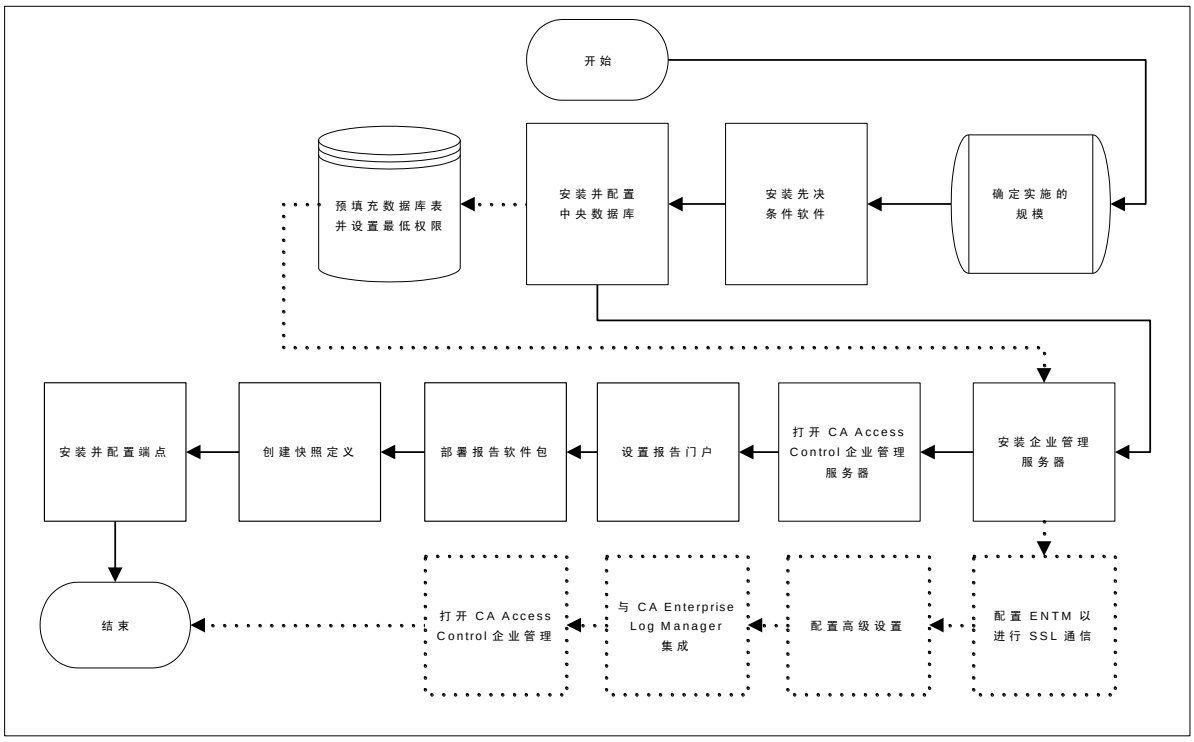
使用以下过程实施 CA Directory：

1. 确定要使用的部署体系结构
2. 安装支持的 RDBMS 作为中央数据库
3. （可选）安装支持的用户存储
4. 安装企业管理服务器
5. 实施企业报告
6. （可选）与 CA User Activity Reporting Module 集成
7. 安装端点

下图说明 CA Access Control 企业管理 的实施过程：

实施企业管理服务器

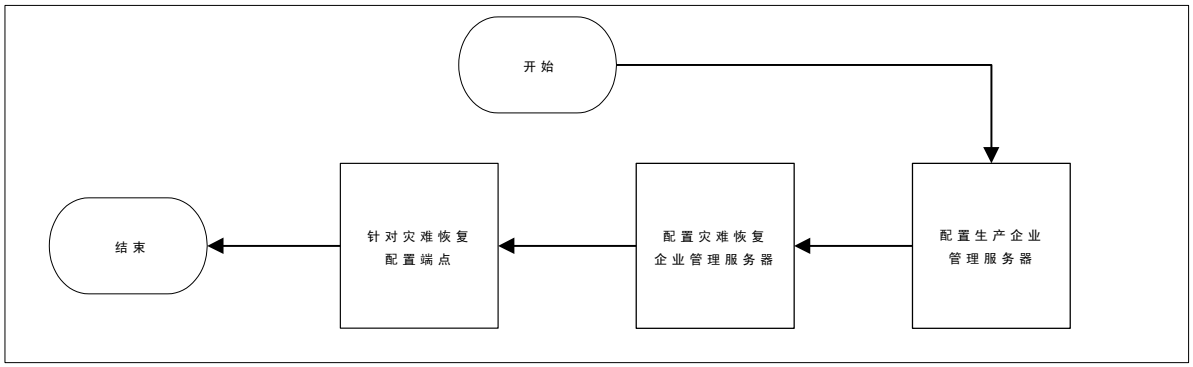
使用该图来帮助您实施企业管理服务器：



注意：虚线表示可选步骤。

为灾难恢复实施 CA Access Control

使用下图来帮助您为灾难恢复实施 CA Access Control：



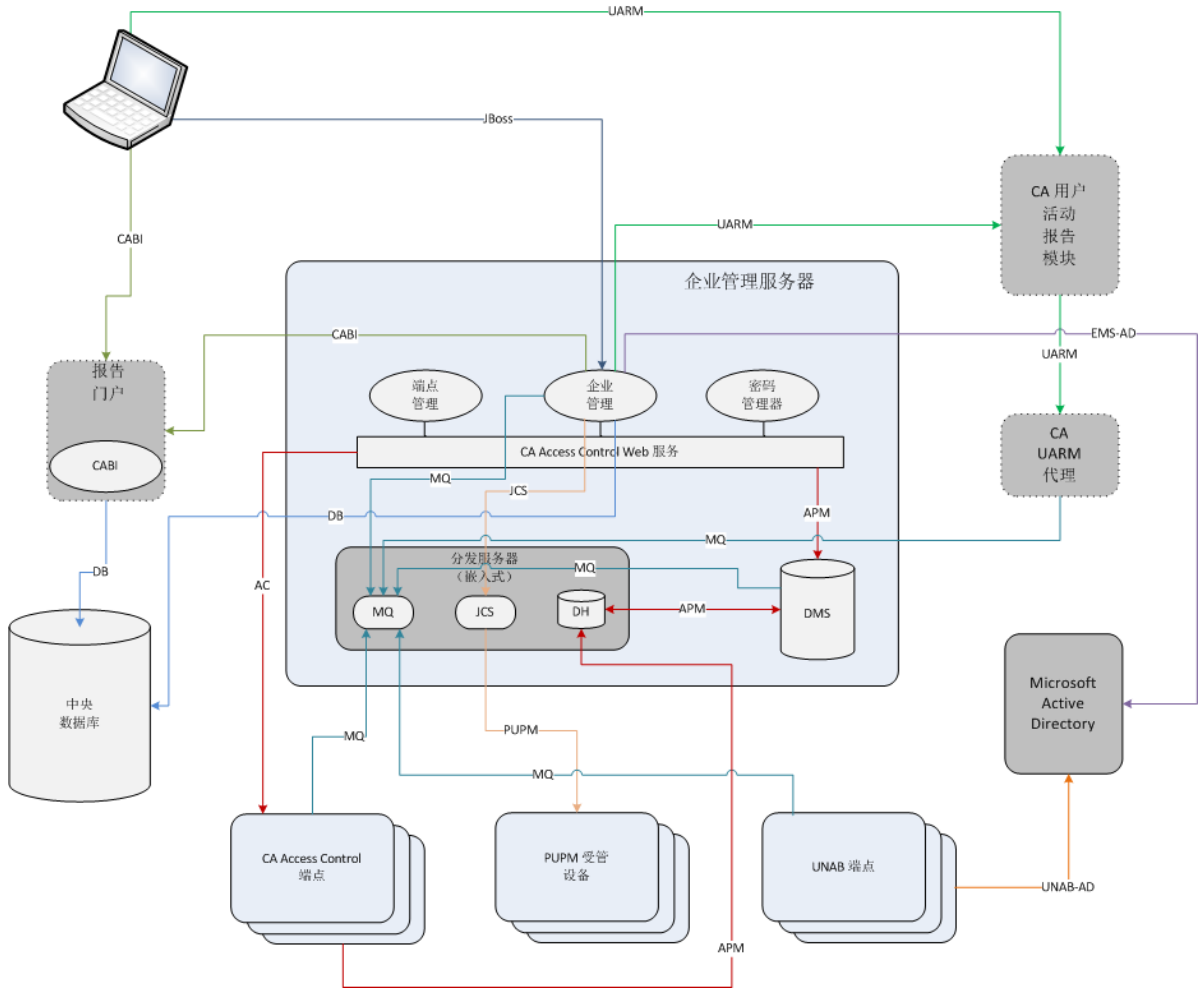
CA Access Control 企业管理 部署体系结构

开始实施 CA Access Control 企业管理 之前，应确定要使用的下列实施体系结构：

- 默认－在默认部署中，在单个服务器上安装 CA Access Control 企业管理 的所有组件。 实施默认体系结构是实施 CA Access Control 企业管理 的最快的方式。 默认实施体系结构不支持高可用性和灾难恢复功能。
- 高可用性－高可用性部署体系结构使您能够为故障转移和冗余实施 CA Access Control 企业管理。 在高可用性实施中，在多台服务器上部署 CA Access Control 企业管理，以便帮助确保在服务器发生故障的情况下，可继续从端点访问数据。
- 灾难恢复－灾难恢复部署体系结构使您能够为灾难恢复实施 CA Access Control 企业管理。 在灾难恢复部署中，在多台服务器上部署 CA Access Control 企业管理 来帮助确保灾难恢复功能。

默认企业部署体系结构

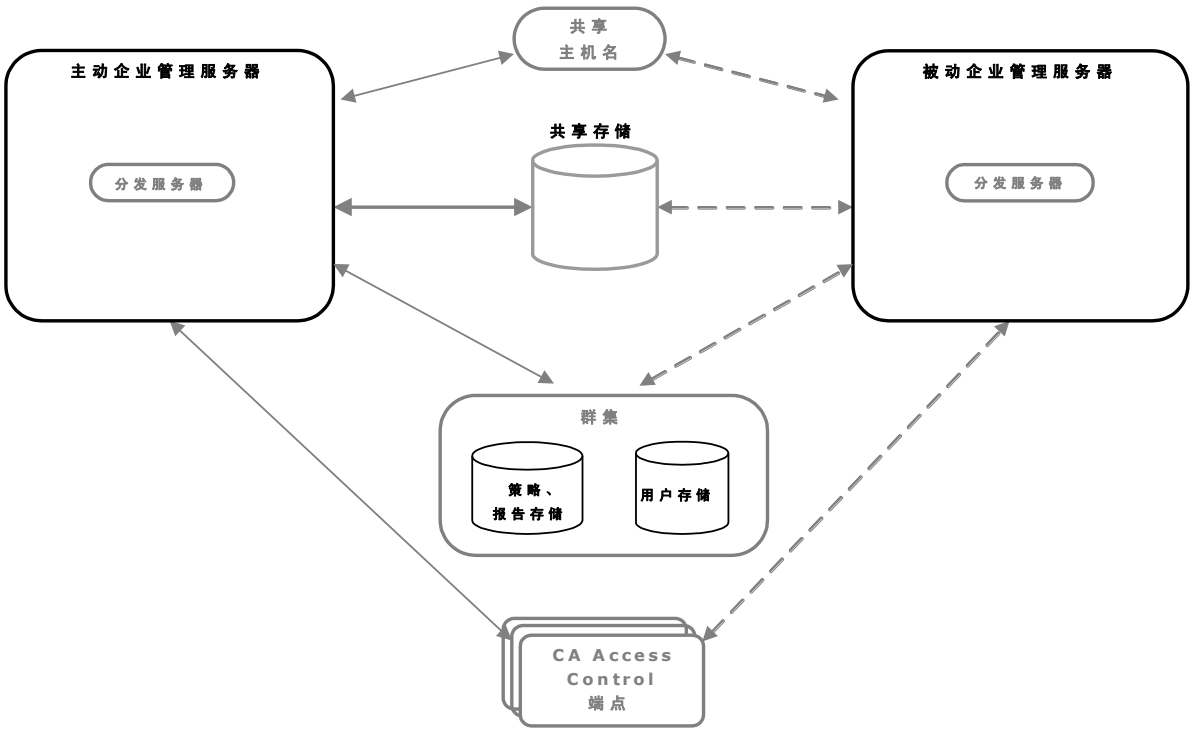
下图显示您在企业中部署 CA Access Control 的方式：



注意：虚线表示可选组件。

高可用性部署体系结构

下图显示高可用性环境中的 CA Access Control 企业管理：

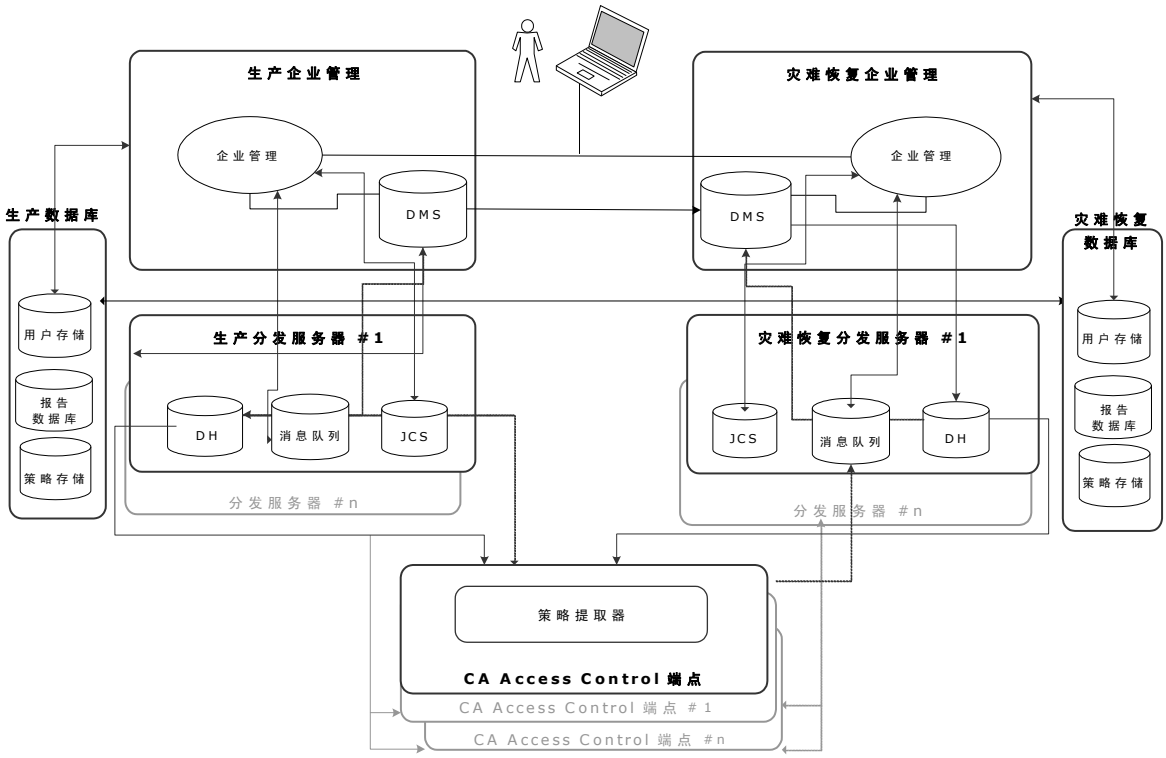


如之前的图中所示，高可用性部署具有以下组件：

- 主企业管理服务器和至少一台备用企业管理服务器
- 策略和报告存储以及用户存储的群集安装
- 主 CA Access Control 企业管理 服务器和备用 CA Access Control 企业管理 服务器都可以访问的共享存储
- 共享主机名
- CA Access Control 端点可以与主企业管理服务器和备用企业管理服务器一起使用

灾难恢复体系结构

下图显示如何在灾难恢复配置中部署 CA Access Control。



CA Access Control 企业管理 的组件

CA Access Control 企业管理 包括或使用以下组件：

企业管理服务器

企业管理服务器是中央管理服务器，包含可用于将策略部署到端点，管理特权帐户，定义资源、访问者和访问级别的组件和工具。 企业管理服务器还包含管理企业管理服务器、端点和其他组件之间的通讯的组件。

安装企业管理服务器时，会静默安装 CA Access Control。 CA Access Control 保护企业管理服务器，并提供支持企业管理服务器中应用程序的核心功能。

分发服务器

分发服务器处理应用程序服务器和端点之间的通讯。 分发服务器包含以下组件：

- 分发主机 (DH)
- 消息队列 (MQ)
- Java 连接器服务器 (JCS)

注意：为进行故障转移，您可以在企业中安装多个分发服务器，或在独立计算机上安装分发服务器组件。 默认情况下在企业管理服务器上安装分发服务器。

分发主机 (DH)

DH 负责将 DMS 上进行的策略部署分发至端点，以及从端点接收部署状态以发送至 DMS。 要完成该任务，DH 将使用两个策略模型数据库：

- **DH Writer**－负责将其从端点接收的数据写入 DMS。

  该 PMDB 的名称是 *DHName*WRITER，其中 *DHName* 是 DH 的名称，默认情况下为 **DH__**。

- **DH Reader**－负责从 DMS 读取数据，以使端点可以检索数据。

  该 PMDB 的名称是 *DHName*，其中 *DHName* 是 DH 的名称，默认情况下为 **DH__**。

默认情况下，DH 与分发服务器安装在同一台计算机上。 不过，您也可以安装多个 DH 节点，以便每个节点管理企业的一部分，从而实现负载平衡。

消息队列

消息队列管理企业管理服务器和其他组件之间的入站和出站消息。 对于每个与企业管理服务器通讯的客户端组件，消息队列都有一个专用队列，这些队列如下：

- 报告队列－接收端点数据库的排定快照。

  报告服务使用快照生成 CA Access Control 报告。

- 审核队列－接收在端点上发生的审核事件。

  您可以配置 CA Enterprise Log Manager 来收集和报告有关审核事件的情况。

- 服务器到端点队列－从 DMS 接收端点收集的数据。

  例如：部署 UNAB 配置策略时，DMS 将配置策略发送到该队列。 然后 UNAB 代理从队列收集策略，并在 UNAB 端点上部署策略。

- 端点到服务器队列－从端点接收 DMS 收集的信息。

  例如：UNAB 端点将检测信号通知发送到该队列。 然后 DMS 从此队列收集检测信号通知，并在其数据库中更新端点状态。

Java 连接器服务器 (JCS)

Java 连接器服务器 (JCS) 与 Java 支持的受管设备（如 Windows 操作系统和 SQL Server）进行通讯，并管理 PUPM 端点上的特权帐户。

基于 Web 的应用程序

使用基于 Web 的应用程序来管理 CA Access Control 的企业安装。 基于 Web 的应用程序安装在应用程序服务器上。 应用程序服务器默认情况下安装在企业管理服务器上。

应用程序服务器包含以下基于 Web 的应用程序：

- CA Access Control 企业管理－允许您管理整个企业的策略以及配置端点。 CA Access Control 企业管理 还包含特权用户密码管理 (PUPM)，让您能够在整个企业中管理特权帐户，并充当特权帐户的密码存储库。
- CA Access Control 端点管理－允许您通过中央管理服务器管理和配置各 CA Access Control 端点。
- CA Access Control 密码管理器－允许您管理 CA Access Control 用户密码。 您可以修改 CA Access Control 用户的密码，或者强制用户在下一次登录时更改自己的密码。

CA Access Control 企业管理

CA Access Control 企业管理 是管理企业的用户界面。 建议您在完成 CA Access Control 企业管理 和 CA Access Control 端点的初始安装之后自行熟悉用户界面。

为了帮助您导航 CA Access Control 企业管理，在选项卡之下对主题特定任务进行分组。 使用这些任务，您可以：

- 查看整个企业的 CA Access Control 的实施
- 配置主机和主机组，并把策略分配给 CA Access Control 和 UNAB 端点
- 签出和签入特权帐户密码
- 配置特权帐户、端点、密码策略和密码使用方
- 显示报告、管理快照定义并捕获快照数据
- 管理用户、组、角色和任务
- 管理系统范围的连接设置
- 查看审核记录

注意：有关在 CA Access Control 企业管理 中完成任务的详细信息，请参阅*联机帮助*。

部署映射服务器 (DMS)

DMS 是高级策略管理的核心。 DMS 用于在每台计算机上保持最新的策略信息（策略版本、脚本）和策略部署状态。 DMS 存储策略版本，您可以在以后根据需要分配、取消分配、部署和取消部署这些策略版本。

DMS 是一个策略模型节点，并将 PMDB 用作其数据存储库。 DMS 从其接收到的来自每个端点（为其配置了 DMS）的通知中收集数据，并存储每个端点的部署信息。

报告门户

报告门户使您能够查看 CA Access Control 报告。

CA Access Control 报告提供每个端点上 CA Access Control 数据库中的数据的相关信息，即您在端点上部署的规则和策略以及规则和策略的偏差。 您在 CA Business Intelligence 或 CA Access Control 企业管理 中查看 CA Access Control 报告。

中央 RDBMS 存储 CA Access Control 报告中所使用的端点数据。

中央 RDBMS

中央 RDBMS 存储以下内容：

- 用于 CA Access Control 报告的端点数据
- 特权帐户密码
- 基于 Web 的应用程序的会话数据
- 基于 Web 的应用程序的用户数据（如果没有将 Active Directory 或 Sun ONE 用作用户存储）

注意：基于 Web 的应用程序是 CA Access Control 企业管理、CA Access Control 端点管理 和 CA Access Control 密码管理器。

端点

CA Access Control 的企业部署具有三种类型的端点：

- CA Access Control 端点－您已经安装 CA Access Control 的端点。

  CA Access Control 端点也可以充当 PUPM 端点。
- UNAB 端点－您已经安装 UNIX 身份验证代理 (UNAB) 的 UNIX 端点。
- PUPM 端点－您使用特权用户密码管理 (PUPM) 来管理的端点。

CA User Activity Reporting Module 组件

您可以将 CA Access Control 审核事件从每个端点以及企业管理服务器发送到 CA User Activity Reporting Module 进行收集和报告。 下列组件支持 CA Access Control 与 CA User Activity Reporting Module 的集成：

- CA User Activity Reporting Module 代理－在分发服务器上收集审核队列的审核事件，并将审核事件发送给 CA User Activity Reporting Module 服务器进行处理。
- CA User Activity Reporting Module 服务器－接收审核事件，并会在存储事件之前应用抑制规则和总结规则。

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。

用户存储

您可以配置 CA Access Control 和 CA Access Control 基于 Web 的应用程序，以使用在 Active Directory 或 Sun One 中定义的组和用户。 这意味着可以将单个数据存储用于所有用户。

注意：基于 Web 的应用程序是 CA Access Control 企业管理、CA Access Control 端点管理 和 CA Access Control 密码管理器。

第 3 章： 安装企业管理服务器

此部分包含以下主题：

环境体系结构

CA Access Control 的企业安装使您能够集中管理策略、特权帐户和 UNAB 端点；查看有关每个端点的策略的信息；以及报告端点的安全状态。 您可以通过基于 Web 的界面或实用程序管理这些功能。

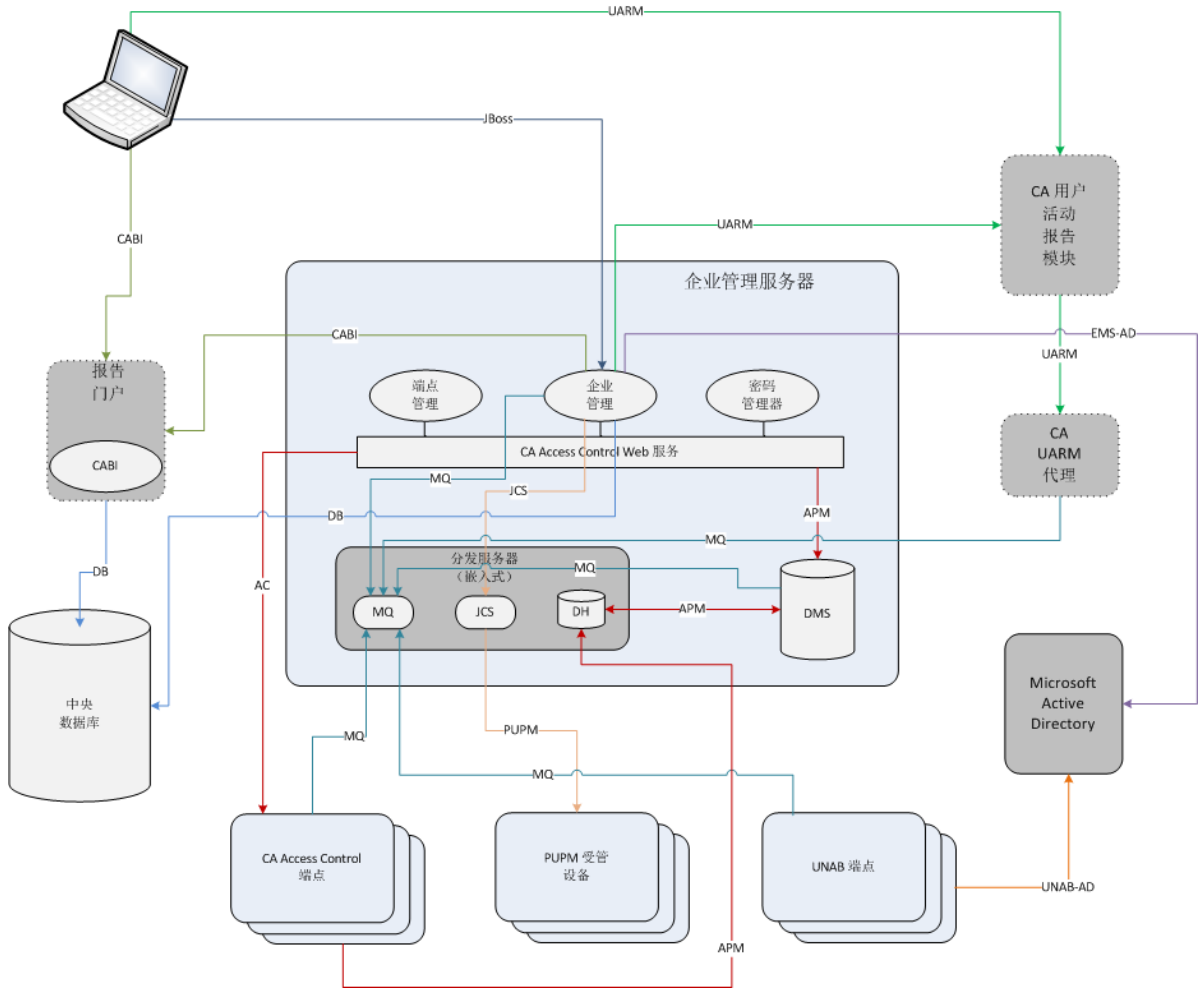
要管理 CA Access Control 的企业安装，请在中心计算机上安装企业管理服务器，并为您的企业配置该服务器。 企业管理服务器包含以下组件：

- 部署映射服务器 (DMS)
- 分发服务器
- 基于 Web 的应用程序

安装企业管理服务器时，将静默安装 CA Access Control。 CA Access Control 保护企业管理服务器，并提供支持企业管理服务器中应用程序的核心功能。

安装企业管理服务器后，安装并配置 CA Access Control 和 UNAB 端点。 如果存在 CA Access Control 端点，请针对高级策略管理和报告功能配置每个端点。

下图显示了企业管理服务器体系结构：



上一图表说明以下内容：

- 企业管理服务器使用以下端口：
  - 要与 CA Access Control 端点通讯－端口 8891（对称加密），端口 5249（SSL 通讯）。
  - 要与 RDBMS 通讯－端口 1433 (MS SQL) 或 1521 (Oracle)。
  - 要与 Active Directory 通讯－端口 389 或 686（加密通讯）。
  - 要与 Java 连接器服务器 (JCS) 通信－20411（加密通讯）。
  - 要与消息队列通信－7243（加密通讯）。

- PUPM 根据端点类型（Windows Agentless、SSH 设备等）与端点进行通讯。
- CA Business Intelligence 使用端口 8080 与企业管理服务器通讯。
- CA User Activity Reporting Module 使用端口 5250 与企业管理服务器通讯（针对加密通讯）。
- UNAB 使用下列端口与 Active Directory 通讯：53、88、123、289、445、464、3268。

如何准备企业管理服务器

在安装企业管理服务器之前，需要准备服务器。 如果您升级 r12.5 或更高版本的 CA Access Control 企业管理 安装，则表示您已准备好企业管理服务器，不需要再次完成这些步骤。

注意：安装企业管理服务器时，安装程序还会安装 CA Access Control 端点管理（如果尚未安装 CA Access Control 端点管理）。 如果您已经安装 CA Access Control 端点管理，则不要重复那些步骤。

要准备企业管理服务器，请执行以下步骤：

1. 为企业管理准备中央数据库 (p. 40)。

   您也可以选择通过使用 RDBMS 本地管理工具手动创建和配置中央数据库来准备数据库。

2. 使用下列方法之一安装必备软件：

   - (Windows) 运行必备软件安装实用程序 (p. 44)。

     CA Access Control 提供安装 Java 开发工具包 (JDK) 和 JBoss 应用程序服务器的实用程序。 如果已经安装该软件，则可以跳过此步骤。

   - 使用现有软件或手动安装必备软件，如下所示：

     注意：您可在 CA Access Control 高级版 第三方组件 DVD 中找到必备的第三方软件。 有关受支持版本的信息，请参阅 *《版本说明》*。

     a. 安装 Java 开发工具包 (JDK) 的受支持版本。

     b. (Linux) 在系统 PATH 中定义 JDK/bin 目录，并将其值设置为安装路径。

        例如：要使用 bash shell 设置 Linux 上的路径，请输入以下命令：

        ```
        export PATH=/usr/jdk/j2sdk.1.6.0_19/bin:$PATH
        ```

        注意：要设置永久路径，请在 shell 启动文件中设置路径。

c. 安装支持的 JBoss 版本。

建议您将 JBoss 作为服务运行。（在 UNIX 上的后台进程）。

注意：如已安装 JBoss，建议在安装 CA Access Control 企业管理 之前运行一次 JBoss，以解决任何尚未解决的端口问题。 CA Access Control 企业管理 安装程序不使用默认 JBoss 端口。 例如：安装程序使用端口号 18080 而非端口号 8080 进行 HTTP 连接。 验证您是否指定企业管理服务器安装期间 JBoss 使用的端口。

d. (Linux) 验证是否安装了 Linux 分发中的 rpmbuild 包。

企业管理服务器需要使用 rpmbuild 包在服务器上安装“高级策略管理”选项。

现在可以在企业管理服务器上安装 CA Access Control 企业管理。

为企业管理准备中央数据库

CA Access Control 企业管理 需要关系数据库管理系统 (RDBMS)。 您必须先设置该系统，然后再安装 CA Access Control 企业管理。

可以通过两个选项将数据库设置为与 CA Access Control 企业管理 一起使用：

- 使用 CA Access Control 提供的部署脚本预填充中央数据库。

  使用该选项可以分开执行数据库准备操作和 CA Access Control 企业管理 安装操作。 数据库管理员可以查看并控制 CA Access Control 需要对数据库做出的更改。

- 允许 CA Access Control 企业管理 在安装期间准备中央数据库。

  使用该选项，CA Access Control 企业管理 安装将在安装过程中填充数据库。

为 CA Access Control 企业管理 准备数据库

1. 如果您没有中央数据库，请安装支持的 RDBMS 作为中央数据库。

   注意：有关受支持的 RDBMS 软件列表，请参阅*《版本说明》*。

2. 为 CA Access Control 企业管理 配置 RDBMS

   确认可从本地和远程客户端访问此数据库。

   - 对于 Oracle，请为中央数据库创建新用户。

     该用户必须具有以下权限和设置：

     - CONNECT（授予以下系统权限：ALTER SESSION、CREATE CLUSTER、CREATE DATABASE LINK、CREATE SEQUENCE、CREATE SESSION、CREATE SYNONYM、CREATE TABLE、CREATE VIEW）
     - RESOURCE（授予以下系统权限：CREATE CLUSTER、CREATE INDEXTYPE、CREATE OPERATOR、CREATE PROCEDURE、CREATE SEQUENCE、CREATE TABLE、CREATE TRIGGER、CREATE TYPE）
     - 托管 CA Access Control 企业管理 服务器的表空间上的无限制配额。

   - 对于 SQL Server：

     - 创建新的*不区分*大小写的数据库。

       数据库必须使用排序顺序 SQL_Latin1_General_CP1_CI_AS。

     - 创建新用户，使新的数据库成为用户的默认数据库，并且向用户分配下列权限：DBCREATOR、SYSADMIN

3. （可选）使用 CA Access Control 提供的部署脚本预填充中央数据库。

   a. 在部署之前自定义部署脚本 (p. 42)。

      部署脚本定义 CA Access Control 企业管理 使用的四个默认用户帐户（superadmin、selfreguser、neteautoadmin、[default user]）。 您可以更改这些默认帐户的名称和密码。

      重要说明！ 仅当计划使用嵌入式用户存储时，才需要自定义脚本。 如果使用 Active Directory，CA Access Control 企业管理 不会将帐户信息存储在中央数据库中。

   b. 部署部署脚本 (p. 43)。

c. 配置用于 CA Access Control 企业管理 安装的数据库用户。

- 对于 Oracle，针对您创建的用户，请保留 CONNECT 和 RESOURCE 角色。
- 对于 SQL Server，请创建新用户，选择您之前创建的数据库作为默认数据库，将用户映射到该数据库，并设置以下权限：CONNECT.SELECT、INSERT、DELETE、UPDATE、EXECUTE。

自定义中央数据库部署脚本

部署脚本定义 CA Access Control 企业管理 使用的四个默认用户帐户（superadmin、selfreguser、neteautoadmin、[default user]）。 您可以更改这些默认帐户的名称和密码。

重要说明！ 仅当计划使用嵌入式用户存储时，才需要自定义脚本。 如果使用 Active Directory，CA Access Control 企业管理 不会将帐户信息存储在中央数据库中。

自定义中央数据库部署脚本

1. 将操作系统相应的 CA Access Control 高级版 服务器组件 DVD 插入光盘驱动器。
2. 将 RDBMS 的部署脚本复制到临时本地文件夹。

   默认情况下，数据库部署脚本位于光盘介质上的以下位置：

   - Oracle：/Scheme/ORACLE/AC125_oracle_script.sql
   - SQL Server：/Scheme/MSSQL/AC125_mssql_script.txt
3. 按如下方式编辑脚本：
   a. 找到 *Table : TBLUSERS* 部分。
   b. 根据需要，将用户定义的每个行编辑为 (INSERT INTO tblusers ...) 以更改帐户名和密码。
4. 保存并关闭脚本。

   现在可以部署自定义脚本了。

示例：自定义 CA Access Control RDBMS 部署脚本

本示例使用 Microsoft SQL Server 和 Oracle 数据库部署脚本所共有的代码片段。 在本示例中，将会自定义脚本，将默认用户帐户超级管理员和密码更改为所选项之一。

如果您使用 RDBMS 作为用户存储，下列片段将设置默认的 CA Access Control 企业管理 超级用户：

```
INSERT INTO tblUsers (ID,loginid, lastname, firstname, password) VALUES
(1,'superadmin', 'Admin','Super', 'test')
```

SQL 命令创建名为 *superadmin*（名字为 *Super*，姓氏为 *Admin*）的用户帐户，密码为 *test*。

在编辑的片段中，将用户帐户名修改为 sysadmin，并向其分配密码 *C0mp!ex*。

```
INSERT INTO tblUsers (ID,loginid, lastname, firstname, password) VALUES
(1,'sysadmin', 'Admin','System', 'C0mp!ex')
```

中央数据库脚本部署示例

完成自定义部署脚本的操作后，可以将此脚本部署到数据库中。 部署脚本将会填充中央数据库，并对其进行准备以完成 CA Access Control 企业管理 安装。 使用本地数据库工具部署脚本。

示例：在 Oracle 数据库 10g 上部署 CA Access Control Oracle 部署脚本

本示例显示如何在 Oracle 数据库 10g 上部署 CA Access Control Oracle 部署。

1. 依次单击“开始”、“所有程序”、“Oracle - *ORACLE_HOME*”、“应用程序开发”、“SQL Plus”。

   此时将打开“Oracle SQL*PLUS”窗口。

2. 使用您之前创建的用户连接到 Oracle 数据库。
3. 在 @ 符号后面输入脚本文件的完整路径名。 例如：

   ```
   @C:\\temp_directory\AC126_oracle_script.sql
   ```

   Oracle 将脚本部署到数据库。

示例：在 SQL Server 2005 上部署 CA Access Control Microsoft SQL Server 部署脚本

本示例显示如何在 SQL Server 2005 上部署 CA Access Control Microsoft SQL Server 部署。

1. 依次单击“开始”、“所有程序”、“Microsoft SQL Server 2005”、“SQL Server Management Studio”。

   此时出现“登录”窗口。

2. 以系统管理员身份登录。

   此时将打开 Microsoft SQL Server Management Studio。

3. 依次单击“文件”、“打开”、“文件”。

   此时将显示“打开文件”对话框。

4. 浏览并选择 CA Access Control Microsoft SQL Server 部署脚本，然后单击“打开”。

5. 从“可用数据库”下拉列表中，选择您之前创建的要在其上部署脚本的数据库。

6. 单击“执行”以部署该脚本。

   Microsoft SQL Server 将脚本部署到数据库。

运行必备软件安装实用程序

在 Windows 上有效

CA Access Control 企业管理 需要有 Java 开发工具包 (JDK) 和 JBoss 应用程序服务器才能运行。 CA Access Control 高级版 第三方组件 DVD 上提供了该第三方必备软件的正确版本。 此外，这些 DVD 上还提供了一个实用程序，它可以按如下所述安装必备软件：

- 将 JDK 和 JBoss 设置为使用适用于 CA Access Control 企业管理 的设置进行安装。
- 以服务的形式安装 JBoss。
- 让您使用预配置的必备软件设置启动 CA Access Control 企业管理 安装。

如果您已安装该软件，则可以跳过此过程。 如果尚未安装该软件，建议您按此过程中的描述，使用提供的实用程序来安装它。

如果已安装 JBoss，建议您在安装 CA Access Control 企业管理 之前，运行一次 JBoss 以解决所有开放端口问题。

运行必备软件安装实用程序

1. 将适用于 Windows 的 CA Access Control 高级版 第三方组件 DVD 插入光盘驱动器中。
2. 导航到光盘驱动器上的 PrereqInstaller 目录，然后运行 **install_PRK.exe**。

   随后将会打开 <InstallAnywhere> 向导。
3. 按照需要完成该向导。

   注意：要配置其他 JBoss 端口号，请在“JBoss 端口设置”页上选择“高级配置”。 如果您指定了一个繁忙的 JBoss 端口，安装程序将提示您指定其他端口号。
4. 查看摘要报告中的详细信息，然后单击“安装”。

   将开始安装必备软件。 这可能需要一些时间。
5. 请执行下列操作之一：
   - 如果要在安装必备软件之后开始 CA Access Control 企业管理 安装过程，请在出现提示时，将适用于您的操作系统的 CA Access Control 高级版 服务器组件 DVD 插入光盘驱动器，然后选择“完成”。 如果显示“产品资源管理器”窗口，请将其关闭。

     随后将会打开 CA Access Control 企业管理 InstallAnywhere 向导。
   - 如果要指定自定义 FIPS 密钥来安装 CA Access Control 企业管理，请在出现提示时单击“完成”，然后单击“结束”以关闭显示的对话框。
   - 如果不希望在安装必备软件后开始 CA Access Control 企业管理安装过程，请在出现提示时单击“完成”，然后单击“结束”以关闭出现的对话框。

     必备软件安装过程现已完成。

如何安装企业管理服务器组件

企业管理服务器组件可让您集中管理 CA Access Control 的企业部署。 安装企业管理服务器组件之后，安装报告服务以及 CA Access Control 和 UNAB 端点。

在开始实施之前，请确认您使用的计算机满足所需的硬件和软件规范。

注意：有关所需硬件和软件规范的详细信息，请参阅 CA 支持上的 CA Access Control 产品页面提供的 CA Access Control 兼容性列表。

要安装企业管理服务器组件，请执行以下操作：

1. 准备企业管理服务器。

   在安装企业管理服务器之前，通过安装和配置必备软件来使计算机做好准备。

   注意：建议在安装企业管理服务器之前，为系统安装最新的软件更新和补丁。

2. 安装 CA Access Control 企业管理。

   已安装所有基于 Web 的应用程序、分发服务器、DMS 和 CA Access Control。

3. （可选）配置 CA Access Control 企业管理 以使用 Sun ONE 目录或 CA Directory 用户存储。

   您可以定义 CA Access Control 企业管理，以使用 Sun ONE 或 CA Directory 用户存储来代替 Active Directory 或嵌入式用户存储。

4. （可选）为 SSL 通讯配置企业管理服务器，如下所述：

   a. 针对 SSL 通讯配置 JBoss。

      默认情况下，安装的 JBoss 不带 SSL 支持。

   b. 修改消息队列服务器 SSL 端口号。

   c. 为 CA Access Control 企业管理 配置 SSL 通讯。

5. （可选）设置高级配置。

   使用 CA Identity Manager 管理控制台可以执行高级配置任务，例如修改中央数据库的属性以生成自定义报告，以及配置 CA Access Control 企业管理，以在发生特定事件时发送电子邮件通知。

6. （可选）更改 CA Access Control Web 服务 URL。

   要提高安全性，您可以更改默认的 CA Access Control Web 服务 URL。

7. （可选）将 Microsoft SQL Server 安全设置修改为 Windows 身份验证模式。

   默认情况下，CA Access Control 企业管理 以 SQL Server 身份验证模式安装。

8. （可选）实施企业报告。

   CA Access Control 企业管理 通过 CA Business Intelligence 公用报告服务器（CA Access Control 报告门户）提供报告功能。

9. （可选）与 CA User Activity Reporting Module 集成

   已安装企业管理服务器。 现在可以安装和配置端点。

更多信息：

如何设置报告服务服务器组件 (p. 97)

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 高级版 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 Access Control 的计算机上安装 CA Access Control 企业管理，请停止 CA Access Control 服务。
3. 将适用于 Windows 的 CA Access Control 高级版 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 高级版 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 高级版 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 高级版 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

定义用于 CA Access Control 企业管理服务器各组件间进行通讯的密码。

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**－定义安装了 Active Directory 的主机的名称。
- **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。

在 Linux 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。

您必须使用控制台安装在 Linux 计算机上安装 CA Access Control 企业管理。

请按下列步骤操作：

1. 如果 JBoss 应用程序服务器正在运行，请将它关闭。
2. 如果在装有 CA Access Control 的计算机上安装 CA Access Control 企业管理，请停止 CA Access Control 服务。

3. 完成以下步骤：

   a. 将操作系统相应的 CA Access Control 高级版 服务器组件 DVD 插入光盘驱动器。

   b. 挂接光盘驱动器。 *不要*指定 noexec 选项。 如果指定 noexec 选项，安装将会失败。

      注意：在 Linux 的某些版本中，操作系统将使用 noexec 选项自动挂接光盘驱动器。

   c. 打开终端窗口，然后将可写临时目录设置为工作目录。

      注意：安装程序会将安装文件解压到工作目录。 如果将工作目录指定到光盘上，安装将会失败，因为安装程序无法将文件解压到光盘。

   d. 执行安装程序，在命令中指定安装程序的完整路径。 例如：如果在 /media 目录中挂接光盘驱动器，请输入以下命令：

      ```
      /media/EnterpriseMgmt/Disk1/InstData/NoVM/install_EntM_r125.bin -i
      console
      ```

      要在安装期间使用自定义的 FIPS 密钥，还必须在命令中指定 FIPS 密钥的完整路径名称（使用格式 -DFIPS_KEY=*path* ）。例如：要使用位于 /tmp/FIPSkey.dat 的自定义 FIPS 密钥进行安装：

      ```
      /media/EnterpriseMgmt/Disk1/InstData/NoVM/install_EntM_r125.bin -i
      console
      -DFIPS_KEY=/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。

   稍后将显示 InstallAnywhere 控制台。

4. 根据需要完成提示。 以下安装输入没有自带说明：

   Java 开发工具包 (JDK)

   定义现有 JDK 的位置。

JBoss 应用程序服务器信息

定义要安装应用程序的 JBoss 实例。

您需要：

- 定义 JBoss 文件夹，该文件夹是安装 JBoss 的顶级目录。

  例如：/opt/jboss-4.2.3.GA

- 定义 JBoss 使用的端口。
- 定义 JBoss 用于安全通讯 (HTTPS) 的端口。
- 定义命名端口号。

注意： CA Access Control 企业管理 安装程序不使用默认的 JBoss 端口，而是将 10000 添加到默认 JBoss 端口号列表中。 例如：安装程序使用端口号 18080 而非端口号 8080 进行 HTTP 连接。 确保指定 JBoss 使用的端口。

通讯密码

定义用于 CA Access Control 企业管理服务器各组件间进行通讯的密码。

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**－定义安装了 Active Directory 的主机的名称。
- **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》*。

5. 查看安装前摘要信息。 如果信息正确，按 Enter。

   CA Access Control 企业管理 已安装。

6. 按 Enter。

   安装程序关闭。

7. 如果需要，请重新启动计算机。

   现在需要为企业配置 CA Access Control 企业管理。

如何配置 CA Access Control 企业管理 以使用 SUN ONE 或 CA Directory

如果将 SUN ONE 或 CA Directory 用作用户存储，请在安装 CA Access Control 企业管理 后配置用户存储目录设置。 使用 CA Identity Manager 管理控制台配置目录和环境设置。

重要说明！ 要将 SUN ONE 目录或 CA Directory 用作用户存储，请在 CA Access Control 企业管理 安装向导的“选择用户存储”屏幕中选择“其他用户存储”选项。

执行以下操作将 CA Access Control 企业管理 配置为使用 SUN ONE 或 CA Directory：

1. 安装该目录。

   注意：针对 SUN ONE，请验证已安装 SUN ONE 目录套件和管理服务。

2. 创建公共用户和系统管理员帐户。

   在创建环境时指定用户凭据。

3. 安装 CA Access Control 企业管理

   安装 CA Access Control 企业管理 时，不要指定用户存储。

4. 使用 CA Identity Manager 管理控制台创建目录。
5. 定义目录连接设置。
6. 使用 CA Identity Manager 管理控制台创建环境。
7. 定义环境设置，以关联到您创建的目录。

更多信息：

为 SUN ONE 用户存储创建目录 (p. 57)
为 SUN ONE 用户存储创建环境 (p. 58)
为 CA Directory 创建目录 (p. 60)
为 CA Directory 创建环境 (p. 61)

为 SUN ONE 用户存储创建目录

目录提供有关 CA Access Control 企业管理 管理的用户目录的信息。 安装 CA Access Control 企业管理 后配置 SUN ONE 目录设置。

为 SUN ONE 用户存储创建目录

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

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

2. 找到 SAM_iPlanet_directory.xml 文件并将该文件复制到临时目录。
3. 按如下所述打开 CA Identity Manager 管理控制台：

   http://*enterprise_host*:*port*/idmmanage

   将打开 CA Identity Manager 管理控制台。
4. 依次选择“目录”、“新建”。

   将打开新建目录窗口。
5. 选择“浏览”，并找到 SAM_iPlanet_directory.xml 文件。 单击“下一步”。
6. 输入以下信息：
   - **名称**－定义目录逻辑名称
   - **说明**－（可选）指定目录的说明
   - **对象连接名称**－指定用户存储的名称
   - **主机**－定义目录主机名或 IP 地址
   - **端口**－定义目录端口号

     示例：389
   - **搜索根**－定义组织搜索根。 目录搜索将从根级别开始
   - **用户 DN**－定义有权登录目录的用户帐户

     示例： cn=Usename, ou=Administration, ou=Corporate, o=Democorp, c=AU
   - **密码**－定义用户帐户密码
   - **确认密码**－输入用户帐户密码以确认密码
   - **安全连接**－指明与目录的连接是安全的
7. 依次单击“下一步”和“完成”。

   新目录已创建。 现在需要创建环境。

为 SUN ONE 用户存储创建环境

对 Windows 有效

为 SUN ONE 目录创建和配置目录设置后，需要创建环境。 环境是用户存储的视图。 在环境中，可以管理用户、组、组织、任务和角色。

注意：在 Windows 启动过程中，JBoss 应用程序服务器服务将自动启动，并且如果不存在环境，将创建一个环境。 我们建议您禁用自动服务启动。 如果环境存在，则在为 SUN ONE 用户存储创建环境之前删除它。

在创建环境之前，必须在 Sun ONE 用户目录中定义系统管理员帐户。

重要说明！ 验证您没有直接在搜索根组织单位 (OU)（位于搜索根下的组织单位）下定义系统管理员帐户。 例如：如果定义的搜索根为 dc=company、dc-com，则按如下所述在用户 OU 下创建系统管理员帐户：uid=Sysmanager、ou=Users、dc=company、dc=com

为 SUN ONE 用户存储创建环境

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

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

   a. 找到以下文件并将它们复制到临时目录：

      ac-RoleDefinitions_Iplanet_EN.xml

      ac-environmentSettings.xml

   b. 删除 ac-environment.properties 文件（如果有）。

2. 打开 CA Identity Manager 管理控制台，选择“环境”，然后选择“新建”。

   此时将显示新建环境屏幕。

3. 输入 **ac_env** 作为环境的名称、提供说明，并输入 **ac** 作为公共 URL 别名，然后单击“下一步”。

   屏幕上将显示可用目录的列表。

4. 选择已定义要与该环境关联的 SUN ONE 目录，然后单击“下一步”。

   a. （可选）选择用作该环境的配给目录的目录，然后单击“下一步”。

   b. （可选）指定用来对匿名连接进行身份验证的用户帐户，然后选择“验证”。

      CA Identity Manager 管理控制台将验证用户帐户。

5. 单击“下一步”继续。

6. 选择“从文件导入角色”，单击“浏览”找到文件 ac-RoleDefinitions_iPlanet_EN.xml，然后单击“下一步”。
7. 指定用户管理员帐户，选择“添加”，然后选择“下一步”。

   将打开摘要屏幕。

   重要说明！ 验证用户管理员帐户是否存在于目录中。
8. 查看摘要然后单击“完成”。

   CA Identity Manager 管理控制台将创建环境。
9. 依次选择“环境”、“ac-env”、“高级设置”，然后单击“导入”。

   将打开“导入设置”窗口。

   a. 浏览并选择要其中保存 ac-environmentSettings.xml 文件的目录，然后单击“完成”。

      CA Identity Manager 管理控制台将创建环境。
10. 选择“继续”，然后选择“启动”。

    将启动环境。
11. 依次选择“环境”、“ac-env”、“高级设置”、“工作流”。

    将打开工作流属性窗口

    a. 选中“已启用”属性旁边的框来启用工作流，然后单击“保存”。

       CA Identity Manager 管理控制台会将更改应用到环境。
12. 依次选择“环境”、“ac-env”、“系统管理员”。

    将打开“系统管理员”窗口。

    a. 指定系统管理员用户帐户，然后选择“验证”。

       CA Identity Manager 管理控制台将显示系统管理员帐户属性。

    b. 依次选择“下一步”、“完成”。

       CA Identity Manager 管理控制台将显示系统管理员配置输出，并指定错误（如果已识别）。

    c. 选择“继续”。
13. 在“状态”字段中，选择“重新启动”。

    CA Identity Manager 管理控制台将重新启动环境。
14. 重新启动 JBoss 应用程序服务器。

    您已将 SUN ONE 目录定义为 CA Access Control 企业管理 的用户存储。 现在可以登录到 CA Access Control 企业管理。

为 CA Directory 创建目录

目录提供有关 CA Access Control 企业管理 管理的用户目录的信息。 安装 CA Access Control 企业管理 后配置 CA Directory 设置。

重要说明！ 如果该目录的 UID 属性不包含值，在创建该目录之前必须编辑 SAM_CA_Directory.xml 文件。 例如：

```
<ImsManagedObjectAttr physicalname="uid" displayname="User ID"
description="User ID" valuetype="String" required="true" multivalued="false"
wellknown="%USER_ID%" maxlength="0" permission="WRITEONCE"/>
```

注意：UID 属性必须有唯一用户定义的数据。 每一个 CA 目录属性曾经被映射到 CA Directory XML 文件的 CA Access Control 企业管理 属性。

为 CA Directory 创建目录

1. 导航到以下目录，其中 JBoss_HOME 表示 JBoss 的安装目录：

   ```
   JBoss_HOME/server/default.deploy/IdentityMinder.ear/user_console.war/META
   -INF/
   ```

2. 将以下文件复制到临时目录。
   a. SAM_CA_Directory.xml
   b. ac-RoleDefinitions_CADir_EN.xml
   c. ac-environmentSettings.xml
3. 删除 ac-environment.properties 文件（如果有）。
4. 启动 JBoss 应用程序服务器。
5. 按如下所述打开 CA Identity Manager 管理控制台：

   ```
   http://enterprise_host:port/idmmanage
   ```

   将打开 CA Identity Manager 管理控制台。
6. 依次选择“目录”、“新建”。

   将打开新建目录窗口。
7. 选择“浏览”，并找到 SAM_CA_Directory.xml 文件。 单击“下一步”。
8. 输入以下详细信息：
   - **名称**－定义目录逻辑名称
   - **说明**－（可选）指定目录的说明
   - **对象连接名称**－指定用户存储的名称
   - **主机**－定义目录主机名或 IP 地址
   - **端口**－定义目录端口号

     示例：389

- **搜索根**－定义组织搜索根。 目录搜索将从根级别开始

  注意：如果您与多域一起使用，让该字段保留为空
- **用户 DN**－定义有权登录目录的用户帐户

  示例： cn=Usename, ou=Administration, ou=Corporate, o=Democorp, c=AU
- **密码**－定义用户帐户密码
- **确认密码**－输入用户帐户密码以确认密码
- **安全连接**－指明与目录的连接是安全的

9. 依次单击“下一步”和“完成”。

   新目录已创建。 现在需要创建环境。

为 CA Directory 创建环境

在 Windows 上有效

为 CA Directory 创建和配置目录设置后，创建环境。 环境是用户存储的视图。 在环境中，可以管理用户、组、组织、任务和角色。

注意：在 Windows 启动过程中，JBoss 应用程序服务器服务将自动启动，并且如果不存在环境，将创建一个环境。 我们建议您禁用自动服务启动。 如果环境存在，则在为 CA Directory 创建环境之前删除它。

在创建环境之前，必须在 CA Directory 中定义系统管理员帐户。

重要说明！ 验证您没有直接在搜索根组织单位 (OU)（位于搜索根下的组织单位）下定义系统管理员帐户。 例如：如果定义的搜索根为 dc=company、dc-com，则按如下所述在用户 OU 下创建系统管理员帐户：uid=Sysmanager、ou=Users、dc=company、dc=com

注意：对于多域支持，定义用户完全 DN

为 CA Directory 创建环境

1. 打开 CA Identity Manager 管理控制台，选择“环境”，然后选择“新建”。

   此时将显示新建环境屏幕。

2. 输入 **ac_env** 作为环境的名称、提供说明，并输入 **ac** 作为公共 URL 别名，然后单击“下一步”。

   屏幕上将显示可用目录的列表。

3. 选择 CA Directory 与该环境关联，然后单击“下一步”。

   a. （可选）选择用作该环境的配给目录的目录，然后单击“下一步”。

   b. （可选）指定用来对匿名连接进行身份验证的用户帐户，然后选择“验证”。

      CA Identity Manager 管理控制台将验证用户帐户。

4. 单击“下一步”继续。

5. 选择“从文件导入角色”，并使用“浏览”找到文件 ac-RoleDefinitions_CADir_EN.xml，然后单击“下一步”。

6. 指定用户管理员帐户，选择“添加”，然后选择“下一步”。

   注意：对于多域支持，请指定用户完全 DN

   将打开摘要屏幕。

   重要说明！ 验证用户管理员帐户是否存在于目录中。

7. 查看摘要然后单击“完成”。

   CA Identity Manager 管理控制台将创建环境

8. 依次选择“环境”、“ac-env”、“高级设置”，然后单击“导入”。

   将打开“导入设置”窗口。

   a. 浏览并选择要其中保存 ac-environmentSettings.xml 文件的目录，然后单击“完成”。

      CA Identity Manager 管理控制台将创建环境。

9. 选择“继续”，然后选择“启动”。

   将启动环境。

10. 依次选择“环境”、“ac-env”、“高级设置”、“工作流”。

    将打开工作流属性窗口

    a. 选中“已启用”属性旁边的框来启用工作流，然后单击“保存”。

       CA Identity Manager 管理控制台会将更改应用到环境。

11. 依次选择“环境”、“ac-env”、“系统管理员”。

    将打开“系统管理员”窗口。

    a. 指定系统管理员用户帐户，然后选择“验证”。

       CA Identity Manager 管理控制台将显示系统管理员帐户属性。

b. 依次选择“下一步”、“完成”。

CA Identity Manager 管理控制台将显示系统管理员配置输出，并指定错误（如果已识别）。

c. 选择“继续”。

12. 在“状态”字段中，选择“重新启动”。

CA Identity Manager 管理控制台将重新启动环境。

13. 重新启动 JBoss 应用程序服务器。

14. 打开命令提示符窗口，并导航到 bin 目录。

15. 运行以下命令来执行 CredentialSender：

```
CredentialsSender cn=root,dc=etasa dc=im,dc=etasa <communication_password>
CA Portal <yes|no>
```

例如：CredentialSecder cn=root,dc=etasa,dc=im,dc=esata *password* 20411 yes

您已定义 CA Access Control 企业管理 使用 CA Directory。 现在可以登录到 CA Access Control 企业管理。

启动 CA Access Control 企业管理

安装 CA Access Control 企业管理 后，您需要启动 CA Access Control 和 Web 应用程序服务器。

请按下列步骤操作：

1. 验证是否已启动 CA Access Control 服务。

CA Access Control 企业管理 要求 CA Access Control 正在运行。

2. 验证是否已启动 JBoss 应用程序服务器服务。 如果未启动 JBoss 应用程序服务器服务，请执行下列操作之一：

- (Windows) 依次单击“启动”、“程序”、“CA”、“Access Control”、“启动任务引擎”。

  注意：任务引擎第一次启动时，可能会花费一些时间进行加载。

- (Windows) 从“服务”面板启动 JBoss 应用程序服务器服务。
- (Linux) 输入 ./JBOSS_DIR/bin/run.sh -b 0.0.0.0

当 JBoss 应用程序服务器服务完成加载时，您可以登录到基于 Web 的 CA Access Control 企业管理 界面。

打开 CA Access Control 企业管理

安装并启动 CA Access Control 企业管理 后，您可以使用 CA Access Control 企业管理 的 URL 从远程计算机启动基于 Web 的界面。

打开 CA Access Control 企业管理

1. 在您的主机中打开 Web 浏览器并输入以下 URL 之一：
   - 要使用非 SSL 连接，请输入以下 URL：

     http://*enterprise_host*:*port*/iam/ac
   - 要使用 SSL 连接，请输入以下 URL：

     https://*enterprise_host*:*HTTPSport*/iam/ac
2. 使用您的凭据登录。

   将显示 CA Access Control 企业管理 主页。

注意：您还可以通过依次单击“开始”、“程序”、“CA”、“Access Control”、“企业管理”从安装了 CA Access Control 端点管理 的 Windows 计算机上打开 CA Access Control 端点管理。

示例：打开 CA Access Control 企业管理

将以下 URL 输入 Web 浏览器中可从网络上的任意计算机打开 CA Access Control 企业管理：

```
http://appserver123:18080/iam/ac
```

该 URL 表明 CA Access Control 企业管理 安装在名为 appserver123 的主机上，并使用默认的 CA Access Control 企业管理 端口 18080。

示例：使用 SSL 打开 CA Access Control 企业管理

将以下 URL 输入 Web 浏览器中，以使用 SSL 从网络上的任一计算机打开 CA Access Control 企业管理：

```
https://appserver123:18443/iam/ac
```

该 URL 表明 CA Access Control 企业管理 安装在名为 appserver123 的主机上，并使用默认的 CA Access Control 企业管理 SSL 端口 18443。

企业管理服务器 SSL 通讯

默认情况下，企业管理服务器组件不使用 SSL 进行通讯。 您可以设置以下组件来使用 SSL 进行通讯：

- JBoss 应用程序服务器

  默认情况下，安装的 JBoss 不带 SSL 支持。

- 消息队列

  您可以修改消息队列默认 SSL 端口，以阻止对常见端口的未经授权访问。

- CA Access Control 企业管理
- （可选）Java 连接器服务器

  只有在使用默认凭据时，才需要在升级到 CA Access Control r12.5 SP3 后导入新的 SSL 凭据。

JBoss 的 SSL 通讯

默认情况下，安装的 JBoss 不带 SSL 支持。 这表示 CA Access Control 企业管理 和 JBoss 之间的所有通讯都未加密。 您可以配置 JBoss，以使用 SSL 进行安全通讯。

注意：有关如何为 JBoss 配置 SSL 的详细信息，请参阅 JBoss 产品文档。

示例：在 Windows 上为 SSL 通讯配置 JBoss

该示例介绍了如何配置 JBoss 应用程序服务器，以便使用 SSL 进行安全通讯。

重要说明！ 该过程描述如何使用 JBoss 版本 4.2.3 和 JDK 版本 1.5.0 配置 JBoss，以使用 SSL 进行安全通讯。

为 SSL 通讯配置 JBoss

1. 如果 JBoss 正在运行，请将其停止。
2. 打开命令提示符窗口，并导航到以下目录：

   JBoss_HOME\server\default\deploy\IdentityMinder.ear\custom\ppm\truststore

3. 输入下面的命令：

   ```
   keytool -genkey -alias entm -keystore ssl.keystore -keyalg RSA
   ```

   -genkey

   指定命令应生成密钥对（公钥和私钥）。

   -alias

   定义用来将条目添加到 keystore 的别名。

   -keystore

   指定要将证书添加到的 keystore。

   -keyalg

   指定要用来生成密钥对的算法。

   将启动 keytool 实用程序。

4. 输入密码 *secret*。

5. 按需要完成提示，并按 Enter 验证已输入的参数。

   证书即可添加到密钥存储。

6. 在以下目录中找到名为 server.xml 的文件，并打开该文件进行编辑：

   JBossInstallDir\server\default\deploy\jboss-web.deployer

7. 在以下部分找到 <Connector Port> 标记：

   ```
   <!-- 定义端口 8443 上的 SSL HTTP/1.1 连接器
          此连接器使用 JSSE 配置，使用 APR 时，
          连接器应使用 OpenSSL 样式配置，
          APR 文档中进行了介绍了该配置 -->
       <!--
       <Connector port="18443" protocol="HTTP/1.1" SSLEnabled="true"
                  maxThreads="150" scheme="https" secure="true"
                  clientAuth="false" sslProtocol="TLS" />
   ```

   注意：连接器端口号对应于在先决条件或 CA Access Control 企业管理 安装过程中指定的 JBoss HTTPS 端口号。

8. 注释掉 <Connector port> 标记上方的 "<!--"。

   现在可以编辑该标记。

9. 将以下属性添加到 <Connector port> 标记：

   ```
   keystoreFile="${jboss.server.home.dir}/conf/ssl.keystore"
   keystorePass="newPassword"
   ```

   keystoreFile

   指定 keystore 文件的完整路径名。

   keystorePass

   指定 keystore 密码。

   <Connector port> 标记现在应按如下所示显示：

   ```
   <Connector port="18443" protocol="HTTP/1.1" SSLEnabled="true"
       maxThreads="150" scheme="https" secure="true"
       clientAuth="false" sslProtocol="TLS"
   keystoreFile="${jboss.server.home.dir}/deploy/IdentityMinder.ear/custom/p
   pm/truststore/ssl.keystore""keystorePass="secret" />
   ```

10. 保存并关闭 server.xml 文件。
11. 启动并打开 CA Access Control 企业管理。

    注意：完成该过程后，可以选择以 SSL 或非 SSL 模式连接到 JBoss 和 CA Access Control 企业管理。

更多信息：

配置电子邮件通知设置 (p. 73)

消息队列服务器 SSL 端口号

安装 CA Access Control 企业管理 时，使用默认 SSL 通讯端口号配置消息队列服务器。 您可以在安装 CA Access Control 企业管理 后修改端口号，例如：要阻止对常见端口的未经授权访问。

示例：修改消息队列服务器 SSL 端口号

以下示例说明如何修改默认的消息队列服务器 SSL 端口号。

修改消息队列服务器 SSL 端口号

注意：在修改消息队列服务器设置之前停止所有 CA Access Control 服务或后台进程。

1. 在 CA Access Control 企业管理 服务器中，导航到以下目录：

   ACServer_InstallDir/AccessControlServer/MessageQueue/tibco/ems/bin

2. 打开 routes.conf 文件进行编辑。

3. 找到条目 [PR_DMS_SERVER]，并在 URL 字段修改端口号值。 例如：

   ```
   url = ssl://PR_DMS_SERVER:7777
   ```

4. 打开 tibemsd.conf 文件进行编辑。

5. 找到入口侦听端口，并修改端口号。 例如：

   ```
   listen = ssl://7777
   ```

6. 打开 tibcoems-service.xml 文件进行编辑。

7. 找到 <!-- JMS 提供程序加载程序 --> 部分，并在 java.naming.provider.url 行修改端口号。 例如：

   ```
   java.naming.provider.url=tibjmsnaming://localhost:7777
   ```

8. 打开 factories.conf 文件进行编辑。

9. 找到以下部分：[SSLQueueConnectionFactory]、[SSLTopicConnectionFactory]、[SSLXAQueueConnectionFactory]，并在 URL 字段修改端口号。 例如：

   ```
   [SSLQueueConnectionFactory]
     type                    = queue
     url                     = ssl://7777
     ssl_verify_host         = disabled

   [SSLTopicConnectionFactory]
     type                    = topic
     url                     = ssl://7777
     ssl_verify_host         = disabled

   [SSLXAQueueConnectionFactory]
     type                    = xaqueue
     url                     = ssl://7777
     ssl_verify_host         = disabled
   ```

10. 找到以下条目：org.jboss.naming.NamingAlias，并修改端口号。 例如：

    ```
    tibjmsnaming://localhost:7777
    ```

11. 启动 CA Access Control 服务。

    现已按要求修改消息队列服务器 SSL 端口号。

如何配置 CA Access Control 企业管理 进行 SSL 通讯

默认情况下，安装的 CA Access Control 企业管理 不带 SSL 支持。 因此，CA Access Control 企业管理 和用户目录之间的通讯未加密。 在使用 Active Directory 或 CA Directory 时，可以将 CA Access Control 企业管理 配置为使用 SSL。 要将 CA Access Control 企业管理 配置为使用 SSL，请执行以下操作：

1. 获取 DER、CRT 或 CERT 格式的用户目录证书。
2. 将证书导入 keystore。
3. 将 CA Access Control 企业管理 配置为使用 SSL 通讯。

更多信息：

将用户目录证书添加到 Keystore (p. 69)
配置 CA Access Control 企业管理 进行 SSL 通讯 (p. 70)

将用户目录证书添加到 Keystore

在将 CA Access Control 企业管理 配置为使用 SSL 通讯之前，需要将用户目录证书添加到 Keystore。

注意：有关如何为 Active Directory 或 CA Directory 配置 SSL 的详细信息，请参阅 Active Directory 和 CA Directory 文档。

示例：将 Active Directory 证书添加到 Keystore

重要说明！ 该示例说明如何使用 JBoss 版本 4.2.3 和 JDK 版本 1.5.0 配置 CA Access Control 企业管理，以使用 SSL 进行安全通讯。 在开始该过程之前，必须获取 DER、CER 或 CERT 编码二进制格式的 Active Directory 证书。

1. 如果 JBoss 正在运行，请将其停止。 请执行下列操作之一：
   - 从 JBoss 作业窗口中断 (Ctrl+C) 进程。
   - 从服务面板停止 JBoss 应用程序服务器服务。
2. 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

3. 输入下面的命令：

   keytool -import -keystore ssl.keystore -*alias ad* -file <*activedirecoty.cert*>

   将显示密码提示符。

   -import

   指定实用程序读取证书，并将其存储在 keystore 中。

   -alias

   指定用来将条目添加到 keystore 的别名。

   -file

   指定 Active Directory 证书文件的完整路径名。

4. 输入密码 *secret*。
5. 导航到 JBoss bin 目录。 默认情况下，在以下位置中找到该目录：

   JbossInstallDir/bin

6. 打开 run.bat 文件，并使用受托用户存储数据设置 java_ops 参数。 例如：

   ```
   set JAVA_OPTS=%JAVA_OPTS% -Xms128m -Xmx512m
   -Djavax.net.ssl.trustStore=C:\jboss-4.2.3.GA\server\default\deploy\Identi
   tyMinder.ear\custom\ppm\truststore\ssl.keystore
   ```

7. 保存文件，然后启动 JBoss。

更多信息：

配置 CA Access Control 企业管理 进行 SSL 通讯 (p. 70)

配置 CA Access Control 企业管理 进行 SSL 通讯

在将用户目录证书添加到 keystore 后，可以将 CA Access Control 企业管理 配置为使用 SSL 通讯。

注意：要为 SSL 连接配置 CA Access Control 企业管理，必须启用 CA Identity Manager 管理控制台。 有关 CA Identity Manager 管理控制台的详细信息，请参阅 *CA Identity Manager 管理控制台联机帮助*。

配置 CA Access Control 企业管理 以进行 SSL 通讯

1. 在 CA Identity Manager 管理控制台中，单击“目录”。
2. 单击 ac-dir 目录。

   此时将显示“目录属性”窗口。

3. 在属性窗口的底部，单击“导出”。

4. 出现提示时，保存 XML 文件。
5. 打开 XML 文件进行编辑。
6. 找到 <Provider userdirectory="ac-dir" type="LDAP"> 标记。
7. 将安全参数更改为 True。 例如：

   ```
   <LDAP searchroot="DC=abc,DC=company,DC=com" secure="true">
   ```

8. 找到 <Connection host="COMPUTER.abc.company.com" port=" "> 标记，并将端口号更改为 636。 例如：

   ```
   <Connection host="COMPUTER.abc.company.com" port="636">
   ```

9. 搜索出现的所有 <Container objectclass="top,organizationalUnit" attribute="ou"/> 标记，并在每行的末尾输入 *value* 参数。 例如：

   ```
   <Container objectclass="top,organizationalUnit" attribute="ou" value=""/>
   ```

10. 保存文件。
11. 在 CA Identity Manager 管理控制台中的“目录属性”页面上单击“更新”。

    此时将显示“更新目录”窗口。

12. 键入用来更新 Identity Manager 目录的 XML 文件的路径和文件名，或者浏览到该文件，然后单击“完成”。

    状态信息显示在“目录配置输出”字段中。

13. 单击“继续”，然后重新启动环境。

    CA Access Control 企业管理 现在可以使用 SSL 来与用户目录通讯。

更多信息：

启用 CA Identity Manager 管理控制台 (p. 72)
打开 CA Identity Manager 管理控制台 (p. 73)
将用户目录证书添加到 Keystore (p. 69)

高级配置

可以使用 CA Identity Manager 管理控制台执行高级配置任务，例如：修改报告数据库的属性以生成自定义报告，以及配置 CA Access Control 企业管理 以在发生特定事件时发送电子邮件通知。

使用 CA Identity Manager 管理控制台，可以创建和管理能够控制目录管理和图形展示的环境。

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

更多信息：

启用 CA Identity Manager 管理控制台 (p. 72)
打开 CA Identity Manager 管理控制台 (p. 73)
配置电子邮件通知设置 (p. 73)

启用 CA Identity Manager 管理控制台

首次安装企业管理服务器时，会禁用 CA Identity Manager 管理控制台选项。 要启用 CA Identity Manager 管理控制台，请更改默认设置。

重要说明：只有在安装期间选择使用 Active Directory 或嵌入用户存储时，才能完成以下过程。

启用 CA Identity Manager 管理控制台

1. 如果 JBoss 正在运行，请将其停止。 请执行下列操作之一：
   - 从 JBoss 作业窗口中断 (Ctrl+C) 进程。
   - 从服务面板停止 JBoss 应用程序服务器服务。
2. 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/management_console.war/WEB-INF
   ```
3. 打开可编辑格式的 *web.xml* 文件。
4. 搜索以下部分：

   ```
   AccessFilter
   ```
5. 在 <param-value> 字段中，将值更改为 True。
6. 保存并关闭文件。
7. 启动 JBoss。

   CA Identity Manager 管理控制台现已启用。

打开 CA Identity Manager 管理控制台

CA Identity Manager 管理控制台提供了一个基于 Web 的界面。 启用 CA Identity Manager 管理控制台并启动 CA Access Control 企业管理 之后，可以从网络上的任一计算机打开 CA Identity Manager 管理控制台。

要打开 CA Identity Manager 管理控制台，请在主机上打开 Web 浏览器并输入以下 URL：

`http://enterprise_host:port/idmmanage`

将打开 CA Identity Manager 管理控制台。

示例：打开 CA Identity Manager 管理控制台

将以下 URL 输入 Web 浏览器中可从网络上的任一计算机打开 CA Identity Manager 管理控制台：

`http://appserver123:18080/idmmanage`

在该示例中，CA Identity Manager 管理控制台安装在名为 appserver123 的主机上，并使用默认的 CA Access Control 企业管理 端口 18080。

配置电子邮件通知设置

打开 CA Identity Manager 管理控制台时，表示您已在某个*环境*中操作。环境可控制目录的管理和图形展示。 例如：您可以在环境中设置电子邮件通知选项和定义报告数据库设置。 建议您仅为 PUPM 事件启用电子邮件通知。

注意：有关环境的详细信息，请参阅 *CA Identity Manager 管理控制台联机帮助*（可从控制台访问）。

重要说明！ 对环境所做的更改可能会影响 CA Access Control 企业管理 的稳定性。 要获得帮助，请通过 http://ca.com/worldwide 与技术支持联系。

配置电子邮件通知设置

1. 如果 JBoss 正在运行，请将其停止。 请执行下列操作之一：
   - 如果 JBoss 不是作为服务安装的，请关闭 JBoss 应用程序服务器窗口 (Ctrl+C)。
   - 如果 JBoss 是作为服务安装的，请从“服务”面板停止 JBoss 服务。
2. 打开 mail-service.xml 文件。 默认情况下，该文件位于以下目录中：

   `JBoss_HOME/server/default/deploy`

3. 在文件中找到以下条目：

   ```
   <property name="mail.smtp.host" value="smtp.nosuchhost.nosuchdomain.com"/>
   ```

4. 将 smtp.nosuchhost.nosuchdomain.com 值更改为传出电子邮件服务器主机（SMTP 服务器）的完整 DNS 域名。 例如：

   ```
   myMailServer.myDomain.com
   ```

   注意：企业管理服务器上的主机文件必须将 SMTP 服务器的 IP 地址解析为为该属性指定的完整 DNS 域名。

5. 对于要为其配置电子邮件通知的每个事件，请执行以下操作：

   a. 打开相应的电子邮件模板。 例如：要配置电子邮件通知以便让收件人知道某个特权帐户密码请求已获批准，请打开以下目录中的 CreatePrivilegedAccountExceptionEvent.tmpl 文件：

      ```
      JBoss_HOME/server/default/deploy/IdentityMinder.ear/custom/emailTempl
      ates/default/approved
      ```

      注意：有关电子邮件模板的详细信息，请参阅*《企业管理指南》*。

   b. 将模板主机名和端口由“localhost:8080”更改为企业管理服务器主机名和端口，例如：*computer.com:18080*

   c. 保存并关闭文件。

6. 打开 email.properties 文件。 该文件位于以下目录：

   ```
   JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/
   config/
   ```

7. 指定发件人电子邮件地址，然后保存并关闭该文件，例如：

   ```
   admin.email.address=admin@company.com
   ```

8. 启动 JBoss。

9. 在 CA Identity Manager 管理控制台中，依次单击“环境”（要配置的环境）、“高级设置”、“电子邮件”。

   此时将显示“电子邮件属性”窗口。

10. 为企业配置适用选项，如下所述：

    启用的事件电子邮件

    为 CA Access Control 企业管理 事件启用电子邮件通知，其中包括 PUPM 事件。

    启用的任务电子邮件

    为 CA Access Control 企业管理 任务启用电子邮件通知。

    注意：CA Access Control 企业管理 不会为任务提供电子邮件模板。建议您不要为任务启用电子邮件通知。

    模板目录

    指定 CA Access Control 企业管理 用来创建电子邮件的电子邮件模板。

    注意：电子邮件模板位于以下目录：

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

11. 指定要为其发送电子邮件通知的事件。

    建议您仅指定提供了电子邮件模板的 PUPM 事件。 请执行以下操作：

    a. 选中每个事件旁边的复选框，但以下 PUPM 事件*除外*：

       - BreakGlassCheckOutAccountEvent
       - CheckOutAccountPasswordEvent
       - CreatePrivilegedAccountExceptionEvent

    b. 单击“删除”。

       除三个 PUPM 事件以外的其他所有事件将被删除。 您已将 CA Access Control 企业管理 配置为针对这三个 PUPM 事件发送电子邮件通知。

12. 单击“保存”。

    电子邮件通知属性已保存。

13. 单击“重新启动”。

    CA Identity Manager 管理控制台将重新启动环境并应用您所做的更改。

注意：有关电子邮件通知的详细信息，请参阅 *《企业管理指南》*。

将服务器配置为使用相同的加密密钥

安装多个企业管理服务器时，每个服务器都使用自己的加密密钥，使用加密密钥可以在中央数据库中加密和解密数据。 如果环境使用多个企业管理服务器来将数据写入单个中央数据库或从单个数据库读取数据，则每个服务器必须使用相同的加密密钥。

重要说明！ 仅当在使用 **-DFIPS_KEY** 选项安装辅助企业管理服务器时未指定主企业管理服务器所用的 FIPS 密钥的情况下，才需要完成以下步骤：

将服务器配置为使用相同的加密密钥

1. 如果 JBoss 正在运行，请将其停止。 请执行下列操作之一：
   - 关闭 JBoss 应用程序服务器窗口 (Ctrl+C)。
   - 从“服务”面板停止 JBoss 服务。
2. 将企业管理服务器配置为使用相同的加密密钥。 请执行以下操作：
   a. 从主企业管理服务器复制以下目录中的 FIPSKey.dat 文件：

      JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys

   b. 将 FIPSKey.dat 文件粘贴到每个辅助企业管理服务器的此目录中。

      此时将显示一条消息，通知您存在同名的文件。

   c. 选择使用新文件覆盖现有文件。

      新文件随即被放入该目录。 现在，每个企业管理服务器都使用相同的加密密钥。
3. 使用新的加密密钥更新每个辅助企业管理服务器上的 AES 密码。 请执行以下操作：
   a. 加密明文密码 (p. 455)。
   b. 在每个辅助企业管理服务器上找到以下文件：

      JBoss_HOME/server/default/conf/login-config.xml

      JBoss_HOME/server/default/deploy/properties-service.xml

   c. 用新的加密密码替换文件中的每个 AES 密码。
4. 启动 JBoss。

   现在，主企业管理服务器和辅助企业管理服务器使用相同的加密密钥加密和解密数据。

示例：已加密的 AES 密码

login-config.xml 文件的以下片段显示了已加密的 AES 密码：

```
<application-policy name="imobjectstoredb">
        <authentication>
                <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin"
                flag="required">
                        <module-option name="userName">user1</module-option>
                        <module-option name="password">
                        {AES}:/lxnvWwAEcYhSmOu3YT3ow==</module-option>
                        <module-option name="managedConnectionFactoryName">

        jboss.jca:name=jdbc/objectstore,service=NoTxCM</module-option>
                </login-module>
        </authentication>
</application-policy>
```

更改 CA Access Control Web 服务 URL

使用 CA Access Control Web 服务访问 CA Access Control 企业管理 和 CA Access Control 端点管理。 CA Access Control Web 服务 URL 的格式为 HTTP:*hostname*:*port*;，例如：http://entmserver:5248。 默认情况下，*hostname* 是企业管理服务器的名称。

更改 CA Access Control Web 服务 URL 时，会更改 Web 服务侦听的 IP 地址和端口。 要提高安全性，可以将主机名更改为本地主机，例如：http://127.0.0.1:5248。 使用本地主机有助于限制 Web 服务的暴露，因为它有助于阻止扫描程序从当前本地主机环境的外部检测到 Web 服务。

请按下列步骤操作：

1. 如果 JBoss 和 CA Access Control 服务正在运行，请将其停止。
2. 更改 URL 中的主机名，如下所述：
   - (Windows) 将 WebService 注册表键中的 machineName 注册表值更改为新的主机名。
   - (Linux) 将 seos.ini 文件的 WebService 部分中的 machineName 配置设置值更改为新的主机名。
3. （可选）更改 URL 中的端口号，如下所述：
   - (Windows) 将 WebService 注册表键中的 portNumber 注册表值更改为新的端口号。
   - (Linux) 将 seos.ini 文件的 WebService 部分中的 portNumber 配置设置值更改为端口号。

4. 打开以下文件，其中 *JBoss_home* 是安装 JBoss 的主目录：

   JBoss_home/server/default/conf/webservice.properties

5. 将 webservice.url 属性值更改为新的主机名和端口。 例如：

   webservice.url=http://127.0.0.1:5248

6. 保存并关闭文件。
7. 重新启动 CA Access Control 服务，包括 CA Access Control Web 服务。
8. 重新启动 JBoss。

   CA Access Control Web 服务 URL 已更改。

修改 Microsoft SQL Server 数据库连接设置

在 Microsoft SQL Server 上安装企业管理服务器时，将身份验证模式设置为 SQL Server 身份验证。 您可以在完成安装后修改数据库身份验证模式，以在 Windows 身份验证模式下运行。

当 SQL Server 以 Windows 身份验证模式运行时，企业管理服务器使用 JBoss 服务帐户管理 SQL Server 上的中央数据库。 如果要使用其他 JBoss 服务帐户，请在 SQL Server 数据库实例上更改帐户。

重要说明！ 要将 SQL Server 设置为以 Windows 身份验证模式运行，需要安装 SQL Server JDBC 2.0 驱动程序。

重要说明！ 确认您为 Microsoft SQL Server 中指定的用户分配了 dbowner 数据库角色。

修改 SQL Server 数据库连接设置

1. 将 SQL Server JDBC 2.0 驱动程序文件下载并提取到临时文件夹中（如果尚未执行此操作）。
2. 如果 JBoss 正在运行，请将其停止。 请执行下列操作之一：
   - 关闭 JBoss 应用程序服务器窗口 (Ctrl+C)。
   - 从“服务”面板停止 JBoss 服务。
3. 导航到 JBoss lib 目录。 该目录位于：

   JBossInstallDir/server/default/lib

4. 将文件 sqljdbc.jar 从临时目录复制到 JBoss lib 目录。

   此时将显示一条消息，通知您存在同名的文件。

5. 选择使用新文件覆盖现有文件。

   新文件随即被放入该目录。

6. 导航到 JBoss bin 目录。 默认情况下，该目录位于：

   JBossInstallDir/bin

7. 将文件 sqljdbc_auth.dll 从临时目录复制到 JBoss bin 目录。

   新文件随即被放入该目录。

8. 导航到 JBoss deploy 目录。 默认情况下，该目录位于：

   JBoss-directory/server/default/deploy

9. 打开以下文件：

   - imauditdb-ds.xml
   - imtaskpersistencedb-ds.xml
   - imworkflowdb-ds.xml
   - objectstore-ds.xml
   - reportsnapshot-ds.xml

10. 在每个文件中，找到 <connection-url> 标记，并在 DatabaseName= parameter 后添加以下内容：

    ;integratedSecurity=true

11. 在每个文件中删除 <security-domain> 标记。

12. 保存文件，然后重新启动 JBoss。

    现在，CA Access Control 企业管理 可以在 Windows 身份验证模式下与 SQL Server 配合使用。

示例：修改 JBoss 配置文件以启用 Windows 身份验证模式

该示例说明如何修改其中一个 JBoss 配置文件，以从 SQL 身份验证模式切换到 Windows 身份验证模式。 在该示例中，管理员修改文件 objectstore-ds.xml，并指定连接模式为 Windows 身份验证 (;integratedSecurity=true)。 接着，管理员在该文件中删除 <security-domain> 标记。 之所以删除该标记，是因为它只适用于 SQL 身份验证模式。

管理员修改连接设置后，以下提取内容将显示 objectsstore-ds.xml 文件：

```
<connection-url>jdbc:sqlserver://example.comp.com:1433;
selectMethod=cursor;DatabaseName=ACDB;
integratedSecurity=true</connection-url>
```

在 Windows 上卸载 CA Access Control 企业管理

在 Windows 上有效

要在 Windows 上卸载 CA Access Control 企业管理，必须以拥有 Windows 管理权限的用户（即 Windows 管理员或 Windows Administrators 组成员）身份登录 Windows 系统。

注意：该过程不会卸载必备软件。 如果要卸载必备软件，则必须在卸载 JDK 之前卸载 JBoss。 有关卸载必备软件的详细信息，请参阅产品文档。

在 Windows 上卸载 CA Access Control 企业管理

1. 如果 JBoss 正在运行，请将其停止。
2. 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。
3. 滚动浏览程序列表，然后选择 CA Access Control 企业管理。
4. 单击“更改/删除”。

   此时将显示“卸载 CA Access Control 企业管理”向导。
5. 按照向导说明卸载 CA Access Control 企业管理。

   将完成卸载过程，并从计算机中删除 CA Access Control 企业管理。
6. 单击“完成”关闭向导。

在 Linux 上卸载 CA Access Control 企业管理

如果要从计算机删除 CA Access Control 企业管理，需要使用 CA Access Control 企业管理 提供的卸载程序。

请按下列步骤操作：

1. 执行以下操作之一停止 JBoss：
   - 从 JBoss 作业窗口中断 (Ctrl+C) 进程。
   - 在单独的窗口中键入：

     ```
     ./JBoss_path/bin/shutdown -S
     ```
2. 输入以下命令：

   ```
   "/ACPMInstallDir/Uninstall_EnterpriseManagement/Uninstall_CA_Access_Control_Enterprise_Management"
   ```

   ACPMInstallDir

   定义 CA Access Control 企业管理 的安装目录。默认情况下，此路径为：

   ```
   /opt/CA/AccessControlServer/
   ```

   InstallAnywhere 将加载卸载向导或控制台。
3. 按照提示卸载 CA Access Control 企业管理。

   将完成卸载过程，并从计算机中删除 CA Access Control 企业管理。

从企业管理服务器删除其他组件

要完全卸载 CA Access Control 企业管理，请在运行卸载程序后从计算机卸载其他组件。

为防止丢失业务数据，卸载程序不会删除以下资源：

- CA Access Control 端点管理 筛选器，位于 *JBoss_Dir*/server/default/conf/accesscontrol
- 消息队列数据文件，位于 *ACServerDir*/MessageQueue/tibco/ems/data

从企业管理服务器删除其他组件

1. 删除以下目录：
   - *JBoss_Dir*/server/default/deploy/IdentityMinder.ear
   - *JBoss_Dir*/server/default/deploy/SiteMinderAgent.ear
2. 卸载 CA Access Control。

3. (Windows) 删除以下注册表键：

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\uninstall\CA Access Control Advanced Policy Management Server

4. 按如下方式删除 JCS：

   a. (Windows) 使用“添加或删除程序”对话框卸载 CA Identity Manager－连接器服务器。

   b. 终止 jcs.exe 进程。

   c. 删除 CA Identity Manager－连接器服务器 (Java) 服务。

5. 删除企业管理服务器的安装目录。

   例如：删除 C:\Program Files\CA\AccessControlServer

   现在，所有的 CA Access Control 企业管理 组件都已从计算机中删除。

更多信息：

卸载方法 (p. 172)

如何实施分发服务器

分发服务器处理应用程序服务器和端点之间的通讯。 默认情况下在企业管理服务器上安装分发服务器。 为实现故障转移和高可用性，可以在企业中安装多个分发服务器。

要实施分发服务器，请执行以下操作：

1. 安装分发服务器

   已安装消息队列、Java 连接器服务器 (JCS) 和 DH。

2. 配置分发服务器

   在分发服务器上配置 DH 以使用 DMS。

3. 配置消息路由设置 (p. 85)

   配置消息路由设置，以将所有通讯都转发给企业管理服务器上的消息队列。

   安装并配置分发服务器，以便与企业管理服务器配合使用。

安装分发服务器

在配置 CA Access Control 以便在灾难恢复或高可用性环境中工作时，在独立计算机上安装分发服务器，并配置分发服务器以便在它们之间传播文件。

请按下列步骤操作：

1. 将操作系统相应的 CA Access Control 高级版 服务器组件 DVD 插入光盘驱动器。
2. 完成以下步骤：
   - Windows 系统中：

     如果已启用自动运行，产品资源管理器将自动显示。 请执行以下操作：

     a. 如果不出现产品资源管理器，导航到光盘驱动器目录并且双击 ProductExplorerx86.EXE 文件。

     b. 展开产品资源管理器中的“组件”文件夹，选择 CA Access Control 分发服务器，然后单击“安装”。
   - Linux 系统中：

     a. 挂接光盘驱动器。

     b. 打开终端窗口并导航至光盘驱动器上的以下目录：

     /DistServer/Disk1/InstData/NoVM

     c. 运行以下命令：

     ```
     ./install_DistServer_r125.bin -i console
     ```
3. 根据需要完成向导。 以下安装输入没有自带说明：

   消息队列设置

   定义消息队列服务器管理员的密码。

   限制：最少六 (6) 个字符。

   Java 连接器服务器一配给目录信息

   定义 Java 连接器服务器的密码。

   注意：Java 连接器服务器为 CA Access Control 企业管理 提供特权帐户管理功能。

   CA Access Control 分发服务器安装已完成。

   注意：如果在灾难恢复实施过程中安装分发服务器，则必须完成其他步骤。

更多信息：

设置生产分发服务器 (p. 338)
设置灾难恢复分发服务器 (p. 340)

配置分发服务器

分发服务器包含 DH。 DH 将在 DMS 上创建的策略部署分发到端点，并从端点接收部署状态更新，以发送到 DMS。

配置分发服务器

1. 运行以下命令来配置 DH：

   ```
   dmsmgr -remove -auto
   ```

   ```
   dmsmgr -create -dh name -parent name\
   [-admin user[,user...]] [-desktop host[,host...]]
   ```

   -dh *name*

   使用在本地主机上 *name* 所指定的名称创建 DH。

   -parent *name*

   定义 DH 要将端点通知发送到的生产 DMS。 按照以下格式指定生产 DMS：*DMS_name@hostname*。

   -admin *user*[,*user*...]

   （可选）将内部用户定义为创建的 DH 的管理员。

   -desktop *host*[,*host*...]

   （可选）定义对附带已创建 DH 的计算机具有 TERMINAL 访问权限的计算机列表。

   注意：无论指定与否，运行此实用程序的终端将始终被授予对已创建 DH 的管理权限。

   已创建和配置生产 DH。

2. 运行以下命令：

   sepmd -n *prDMS_name prDH_name*

   prDMS_name

   定义生产 DMS 的名称。

   prDH_name

   定义生产 DH 的名称。 请按以下格式指定名称：*prDH_name@hostname*。

   示例：DH__@prdh.com

   DH 订阅到生产 DMS，并与其同步。

3. 从企业管理服务器运行以下命令：

   sepmd -n DMS_name dh_name

   示例：sepmd –n DMS__ DH__@computer.com

如何配置消息路由设置

在包含企业管理服务器的单个实例和多个分发服务器的环境中运行时，必须配置所有分发服务器上的 MQ 路由设置，以指向企业管理服务器上的 MQ。 这有助于确保 CA Access Control 端点发送的所有消息最终都会路由到企业管理服务器上的单个 MQ。

要将消息从每个分发服务器上的 MQ 路由到企业管理服务器，请执行以下操作：

- 在企业中的每个分发服务器上，执行以下操作：
  - 停止消息队列服务。
  - 修改指向企业管理服务器消息队列的路由。
  - 定义企业管理服务器消息队列的参数。
  - 配置分发服务器消息队列的名称。
  - 指定企业管理服务器消息队列的位置。
  - 启动消息队列服务。

- 在企业管理服务器上，执行以下操作：
  - 停止消息队列服务。
  - 修改指向分发服务器消息队列的路由。
  - 定义分发服务器消息队列的参数。
  - 配置企业管理服务器消息队列的名称。
  - 指定企业管理服务器消息队列的位置。
  - 启动消息队列服务。

注意：有关消息传递的信息，请参阅*《TIBCO 企业消息服务用户指南》*。Tibco 文档作为消息队列的一部分安装在以下位置：*ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc。

修改分发服务器上的消息队列设置

默认情况下，每个分发服务器都配置为与该服务器上运行的消息队列配合使用。 要将消息路由到其他消息队列，必须重新配置消息队列设置。

该过程介绍如何修改分发服务器上的消息队列设置，以便能够与 CA Access Control 企业管理 消息队列通讯。 针对企业中的每个分发服务器完成此过程。

修改分发服务器上的消息队列设置

1. 停止 CA Access Control 消息队列服务。

   重要说明！ 停止 CA Access Control 消息队列服务时，CA DSM r11Common Application Framework 服务也将停止。

2. 在分发服务器上，打开 tibemsd.conf 文件，默认情况下，该文件位于以下目录，其中 *DistServerInstallDir* 是分发服务器的安装目录：

   DistServerInstallDir/ACMQ/tibco/cfgmgmt/ems/data

3. 在 server 参数中输入分发服务器短主机名。
4. 将 routing 参数值更改为已启用。
5. 启动 CA Access Control 消息队列服务。

   已修改分发服务器上的消息队列设置。

注意：有关消息传递的信息，请参阅*《TIBCO 企业消息服务用户指南》*。Tibco 文档作为消息队列的一部分安装在以下位置：*ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc。

示例：tibemsd.conf 文件

该示例显示了在修改名为 DS_Example 的分发服务器的路由设置之后 tibemsd.conf 文件中的某个片段。

```
#######################
# Server Identification Information.
# server:    unique server name
# password:  password used to login into other routed server
#######################
server                  = DS_Example
password                =
#######################
…
#######################
# Routing. Routes configuration is in 'routes.conf'. This enables or
# disables routing functionality for this server.
#######################
routing                 = enabled
#######################
```

修改企业管理服务器上的消息队列设置

以下过程显示如何在企业管理服务器上修改消息队列设置，以便能够与分发服务器进行通讯。

修改企业管理服务器上的消息队列设置

1. 停止 CA Access Control 消息队列服务。

   重要说明！ 停止 CA Access Control 消息队列服务时，CA DSM r11Common Application Framework 服务也将停止。

2. 在企业管理服务器上，打开 tibemsd.conf 文件进行编辑。 该文件位于以下目录，其中 *ACServerInstallDir* 是您企业管理服务器的安装目录：

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

3. 在 server 参数中输入企业管理服务器短主机名（不要以点隔开）。

4. 将 routing 参数值更改为已启用。

5. 启动 CA Access Control 消息队列服务。

   现在已修改了企业管理服务器上的消息队列设置。

注意：有关消息传递的信息，请参阅*《TIBCO 企业消息服务用户指南》*。Tibco 文档作为消息队列的一部分安装在以下位置：*ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc。

示例：tibemsd.conf 文件

此示例显示了为名为 ENTM_Example 的 CA Access Control 企业管理 服务器修改路由设置后 tibemsd.conf 文件中的一个片段：

```
#######################
# Server Identification Information.
# server:    unique server name
# password:  password used to login into other routed server
#######################
server                  = ENTM_Example
password                =
#######################
…
#######################
# Routing. Routes configuration is in 'routes.conf'. This enables or
# disables routing functionality for this server.
#######################
routing                 = enabled
#######################
```

消息队列连接配置

相反，要将消息从分发服务器上的消息队列路由到企业管理服务器，请修改企业中现有的消息队列设置。

示例：在分发服务器上配置消息队列连接设置

该示例显示如何在分发服务器上配置消息队列服务器设置。 通过定义在企业管理服务器上运行的消息队列的参数，可以配置消息队列，以将消息发送到企业管理服务器。

请按下列步骤操作：

1. 在分发服务器上，执行下列操作之一：
   - (Windows 2003 Server) 依次选择“开始”、“程序”、“TIBCO-CA_AC”、“TIBCO EMS 5.1”和“启动 EMS 管理工具”。
   - Linux：
     a. 导航到下列目录，其中 *DistServerInstallDir* 是分发服务器的安装目录：

        DistServerInstallDir/MessageQueue/tibco/ems/5.1/bin

     b. 运行以下命令：

        tibemsadmin

        此时将打开“TIBCO EMS 管理工具”命令提示符窗口。

2. 使用以下两种方法之一连接到消息队列：
   - 输入以下命令，使用 SSL 进行连接：

     ```
     connect ssl://localhost:7243
     ```
   - 输入以下命令，使用 TCP 进行连接：

     ```
     connect tcp://localhost:7222
     ```

   此时将提示您输入登录名称。
3. 输入 **admin**。

   将显示密码提示符。
4. 输入您安装分发服务器时提供的密码。
5. 出现提示时，输入消息队列服务器的新密码。
6. 定义消息队列密码。

   ```
   set server password=
   ```

   示例：set server password=*<C0mp1ex>*
7. 创建名为 ENTM-NAME 的用户，并为其指定密码。

   ```
   create user ENTM-NAME password=acserver_user-passwd
   ```

   示例：create user EMS-SERVER password=*<acserver_user-passwd>*

   重要说明！ 指定您在企业管理服务器的 tibemsd.conf 文件的 server 参数中定义的相同名称。
8. 请执行以下操作：
   a. 输入以下命令：

      ```
      add member ac_server_users ENTM_NAME
      ```

      您创建的用户已添加到 ac_server_users 组中。
   b. 输入以下命令：

      ```
      add member ac_endpoint_users ENTM_NAME
      ```

      您创建的用户已添加到 ac_endpoint_users 组中。
   c. 输入以下命令：

      ```
      add member report_publishers ENTM_NAME
      ```

      您创建的用户已授予了读取消息和将消息发布到 CA Access Control 队列的权限。
9. 重新启动分发服务器。

   系统将应用您所做的更改。

示例：配置企业管理服务器上的消息队列连接设置

该示例显示如何在企业管理服务器上配置消息队列服务器设置。 配置消息队列以将消息发送到分发服务器。

在此示例中，术语 *DS-NAME* 与分发服务器计算机的名称有关，而术语 *ENTM-NAME* 与企业管理服务器的名称有关。 定义消息队列服务器设置时，需要将该名称替换为在 *tibemsd.conf* 文件的 server 标记中定义的服务器实际名称。

请按下列步骤操作：

1. 在企业管理服务器上，执行下列操作之一：
   - (Windows 2003 Server) 依次选择“开始”、“程序”、“TIBCO-CA_AC”、“TIBCO EMS 5.1”和“启动 EMS 管理工具”。
2. 使用以下两种方法之一连接到消息队列：
   - 输入以下命令，使用 SSL 进行连接：

     ```
     connect ssl://localhost:7243
     ```
   - 输入以下命令，使用 TCP 进行连接：

     ```
     connect tcp://localhost:7222
     ```

   此时将提示您输入登录名称。
3. 输入 **admin**。

   将显示密码提示符。
4. 输入您安装企业管理服务器时提供的密码。
5. 定义消息队列密码。

   ```
   set server password=entm_server-passwd
   ```

   示例：set server password=*<ENTM_SERVER_NAME-passwd>*
6. 为每台分发服务器创建名为 DS-NAME 的用户，并为其指定密码。

   ```
   create user DS-NAME password=dist_server_user
   ```

   示例：create user EMS-Server password=*<C0mp1ex>*

   重要说明！ 指定您在企业管理服务器的 tibemsdf.conf 文件的 server 参数中定义的相同名称。

7. 请执行以下操作：

   a. 输入以下命令：

      ```
      add member ac_server_users DS_NAME
      ```

      您创建的用户已添加到 ac_server_users 组中。

   b. 输入以下命令：

      ```
      add member ac_endpoint_users DS_NAME
      ```

      您创建的用户已添加到 ac_endpoint_users 组中。

   c. 输入以下命令。

      ```
      add member report_publishers DS_NAME
      ```

      您创建的用户已授予了读取消息和将消息发布到 CA Access Control 队列的权限。

8. 重新启动分发服务器，使更改生效。

   此时，您已配置了企业管理服务器上的消息队列设置。

注意：有关消息传递的信息，请参阅*《TIBCO 企业消息服务用户指南》*。Tibco 文档作为消息队列的一部分安装在以下位置：*ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc。

配置分发服务器上的消息队列的名称

要将消息从分发服务器转发到企业管理服务器，请配置每个消息路由，以便将消息从分发服务器上的消息队列转发到企业管理服务器上的消息队列。

在此过程中，需要定义分发服务器上的消息队列设置。 修改消息队列设置文件，以在企业管理服务器上提供消息队列设置。

在分发服务器上配置消息队列的名称

1. 在分发服务器上，打开文件 queues.conf。 默认情况下，该文件位于以下目录，其中 *DistServerInstallDir* 是分发服务器的安装目录：

   ```
   DistServerInstallDir/ACMQ/tibco/cfgmgmt/ems/data
   ```

2. 找到名为 queue/snapshots 的队列，并在此队列名称的末尾添加 ENTM-NAME 值，两者中间插入 @ 符号，如下所述：

   ```
   queue/snapshots@ENTM-NAME
   ```

   ENTM-NAME

   定义企业管理服务器的短名称。

   重要说明！ 指定您在企业管理服务器的 tibemsd.conf 文件的 server 参数中定义的相同名称。

3. 找到名为 queue/audit 的队列，并在此队列名称的末尾添加 ENTM-NAME 值，两者中间插入 @ 符号，如下所述：

   queue/audit@*ENTM-NAME*

4. 找到名为 ac_endpoint_to_server 的队列，并在此队列名称的末尾添加 ENTM-NAME 值，两者中间插入 @ 符号，如下所述：

   ac_endpoint_to_server@*ENTM-NAME*

5. 找到名为 ac_server_to_endpoint 的队列，并在此队列名称的末尾添加 ENTM-NAME 值，两者中间插入 @ 符号，如下所述：

   ac_server_to_endpoint@*ENTM-NAME*

6. 保存并关闭文件。

注意：有关消息传递的信息，请参阅*《TIBCO 企业消息服务用户指南》*。Tibco 文档作为消息队列的一部分安装在以下位置：*ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc。

配置企业管理服务器上的消息队列的名称

在此过程中，您定义企业管理服务器上的消息路由设置。 配置企业管理服务器上的消息队列设置以将此消息队列标识为主服务器。

在企业管理服务器上配置消息队列的名称

1. 在企业管理服务器上，打开可编辑格式的 queues.conf 文件。 该文件位于以下目录，其中 *ACServerInstallDir* 是企业管理服务器的安装目录：

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

2. 找到名为 queue/snapshots 的队列，并在队列名称末尾的 secure 词语后面添加 global，如下所述：

   queue/snapshot secure, global

3. 找到名为 queue/audit 的队列，并在队列名称末尾的 secure 词语后面添加 global，如下所示：

   queue/audit secure, global

4. 找到名为 ac_endpoint_to_server 的队列，并在队列名称末尾的 secure 词语后面添加 global，如下所述：

   ac_endpoint_to_server secure, global

5. 找到名为 ac_server_to_endpoint 的队列，并在队列名称末尾的 secure 词语后面添加 global，如下所述：

   ```
   ac_server_to_endpoint secure, global
   ```

6. 保存并关闭文件。

注意：有关消息传递的信息，请参阅*《TIBCO 企业消息服务用户指南》*。Tibco 文档作为消息队列的一部分安装在以下位置：*ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc。

消息路由配置

在分发服务器和企业管理服务器上配置了消息队列设置和消息队列路由设置后，需要在分发服务器和企业管理服务器上设置消息路由。

示例：在分发服务器上设置消息路由

该示例显示如何在分发服务器上设置消息路由设置。 在分发服务器和企业管理服务器之间设置一个路由，将来自 CA Access Control 端点的消息路由到企业管理服务器上的消息队列。 对企业中的每个分发服务器完成此过程。

1. 在分发服务器上，打开文件 routes.conf 进行编辑。 默认情况下，该文件位于以下目录，其中 *DistServerInstallDir* 是分发服务器的安装目录：

   DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

2. 添加以下项：

   ```
   [ENTM-NAME]
   url          = ENTM-URL
   ssl_verify_host = disabled
   ssl_verify_hostname = disabled
   ```

   ENTM-NAME

   定义企业管理服务器的短名称。

   ENTM_URL

   定义企业管理服务器 URL。

3. 保存文件。
4. 重新启动 CA Access Control 消息队列服务。

示例：在企业管理服务器上设置消息路由

该示例显示如何在企业管理服务器上设置消息路由设置。 在企业管理服务器和分发服务器之间设置一个路由，将来自企业管理服务器的消息路由到分发服务器，再由分发服务器路由到端点。

1. 在企业管理服务器上，打开文件 routes.conf。 默认情况下，该文件位于以下目录，其中 *ACServerInstallDir* 是您安装企业管理服务器的目录：

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

2. 添加以下项：

   ```
   [DS-NAME]
   url          = DS-URL
   ssl_verify_host = disabled
   ssl_verify_hostname = disabled
   ```

   DS_NAME

   定义分发服务器的短名称。

   DS_URL

   定义分发服务器 URL。

3. 保存文件。
4. 重新启动 CA Access Control 消息队列服务。

注意：有关消息传递的信息，请参阅*《TIBCO 企业消息服务用户指南》*。Tibco 文档作为消息队列的一部分安装在以下位置：*ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc。

第 4 章： 实施企业报告

此部分包含以下主题：

企业报告功能

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

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

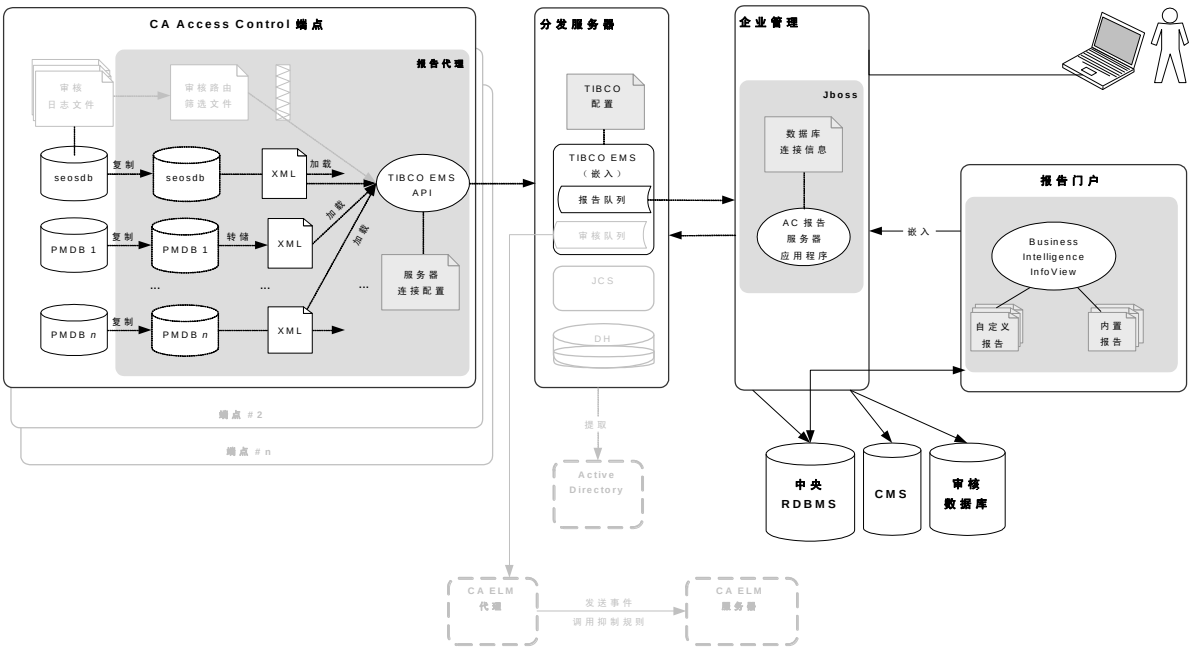
报告服务体系结构

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

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

注意：有关企业报告的详细信息，请参阅*《企业管理指南》*。

下图显示了报告服务组件的体系结构。 该图还显示了组件之间的数据流。



上图说明了以下内容：

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

如何设置报告服务服务器组件

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

注意：报告代理安装和配置是 CA Access Control 和 UNAB 端点安装的一部分，不包含在该过程中。

要设置报告服务服务器组件，请执行以下步骤：

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

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

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

注意：有关生成和查看报告的详细信息，请参阅*《企业管理指南》*。

更多信息：

为报告配置 Windows 端点 (p. 170)
配置 UNIX 端点以进行报告 (p. 224)
配置 UNAB 以进行报告 (p. 291)

如何设置报告门户计算机

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

注意：如果已拥有旧版本的报告门户或 CA Business Intelligence 或 BusinessObjects Enterprise XI 的独立安装，则可以使用现有安装而无需升级。

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

要设置报告门户，请执行以下操作：

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

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

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

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

   注意：默认情况下，Windows 报告门户使用 Microsoft SQL Server 身份验证来验证连接。 如果要使用域用户账户设置进行身份验证，您可以将报告门户配置为在 Windows 身份验证中运行 (p. 107)。

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

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

示例：在 Windows 上安装 CA Business Intelligence

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

注意：安装大约要花费 1 小时才能完成。

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

   将启动 CA Business Intelligence 安装向导。

3. 使用下表完成该安装向导：

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

将开始安装，完成该过程最多将花费一小时。

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

更多信息：

为企业管理准备中央数据库 (p. 40)

为 CA Business Intelligence 安装准备 Linux

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

请按下列步骤操作：

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

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

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

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

   ```
   LANG=en_US.utf8
   ```
4. 以创建的非 root 用户身份登录。

5. 输入以下命令以验证 ORACLE_HOME 和 TNS_ADMIN 环境变量是否已正确设置：

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

如果输出不为空，则表明这些环境变量有效。 例如：

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

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

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

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

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

例如：键入以下命令并在输出中搜索以下路径：

```
echo $LD_LIBRARY_PATH
```

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

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

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

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

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

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

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

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

   TNS Ping 的输出类似于以下示例：

   ```
   TNS Ping Utility for Solaris: Version 10.2.0.1.0 - Production on 07-MAY-2008
   09:17:02
   Copyright (c) 1997, 2005, Oracle.  All rights reserved.
   Used parameter files:
   /opt/oracle/app/oracle/oracle/product/10.2.0/client_1/network/admin/sqlne
   t.ora
   Used TNSNAMES adapter to resolve the alias
   Attempting to contact (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL =
   TCP)(HOST = 172.16.234.75)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME =
   service_name)))
   OK (30 msec)
   ```

   现在，您可在 Linux 上安装 CA Business Intelligence。

报告数据包部署

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

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

在报告门户上部署报告数据包

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

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

请按下列步骤操作：

1. 确认中央数据库、分发服务器和报告门户已设置。

   注意：确认 JAVA_HOME 变量已在报告门户计算机上设置。

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

3. 将 biconfig 目录的内容复制到临时目录。

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

5. 将以下文件从光盘复制到同一临时目录：

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

   RDBMS

   定义用于 CA Access Control 报告的 RDBMS 类型。

   值：Oracle、MSSQL2005

   ***import_biar_config*.xml**

   为您的 RDBMS 定义导入配置文件 (.xml) 的名称。

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

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

   ***AC_BIAR_File*.biar**

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

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

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

<biar-file name>

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

<networklayer>

定义 RDBMS 支持的网络层。

值 (Windows)：

- OLE DB－针对 MS SQL Server 身份验证模式。
- Oracle OCI
- ODBC－针对 Windows 身份验证模式。

<rdms>

定义用于 CA Access Control 报告的 RDBMS 类型。

值 (Oracle OCI)： Oracle 10 或 Oracle 11

值 (ODBC)： 常规 ODBC 数据源

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

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

<username>

定义您在为企业管理准备中央数据库时所创建的 RDBMS 管理用户的用户名。

<password>

定义您在为企业管理准备中央数据库时所创建的 RDBMS 管理用户的密码。

<datasource>

定义以下项之一：

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

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

<server>

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

7. 执行以下操作：

   - 打开命令提示符窗口，然后输入以下命令：

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

     host_name

     定义报告门户主机名。

     user_name

     定义您在安装报告门户时配置的报告门户管理员。

     password

     定义报告门户管理员的密码。

     例如：

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

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

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

     例如：

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

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

示例：Oracle Database 11g 导入配置文件示例

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

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

示例：Microsoft SQL Server 2005 导入配置文件示例

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

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

更多信息：

配置 UNIX 端点以进行报告 (p. 224)
为报告配置 Windows 端点 (p. 170)

报告门户的 Windows 身份验证配置

在 Windows 上有效

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

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

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

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

如何将报告门户配置为在 Windows 身份验证中运行

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

执行以下操作配置 Windows 身份验证的报告门户：

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

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

   指定的该用户用于在将报告门户配置为以 Windows 身份验证模式运行时进行身份验证。
5. 将 ASP.NET Web 服务扩展设置为“已允许”。
6. 安装报告门户 (CA Business Intelligence) (p. 97)。 在安装期间执行以下操作：
   a. 选择以自定义模式安装 CA Business Intelligence。
   b. 指定 Microsoft SQL Server 2005 作为数据库。
   c. 指定 IIS 作为 Web 服务器。

7. 配置 Windows 身份验证的报告门户。

   配置 CA Business Intelligence 服务，以使用 Active Directory 用户账户以 Windows 身份验证模式进行身份验证。

8. 使用 Windows 身份验证为 CA Access Control 报告数据库创建系统 DSN。

   系统 DSN 用来连接到 CA Access Control 报告门户。

9. 在报告门户上部署报告数据包。

配置 Windows 身份验证的报告门户

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

配置 Windows 身份验证的报告门户

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

   将打开中央配置管理器，显示 CA Business Intelligence 服务。

4. 停止所有 CA Business Intelligence 服务。
5. 将服务“登录身份”设置修改为 Active Directory 用户凭据。 对所有 CA Business Intelligence 服务执行该操作。

   重要说明！ 不要更改 WinHTTP Web Proxy Auto-Discovery 和 World Wide Web Publishing 服务的设置。

6. 启动所有 CA Business Intelligence 服务。

   报告门户现已配置为以 Windows 身份验证模式进行身份验证。

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

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

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

1. 右键单击列表中的连接服务器服务并选择“属性”。

   将打开连接服务器服务属性窗口。

2. 在“登录身份”部分，删除“系统帐户”选项中的标记。

   连接设置字段已启用。

3. 输入 Active Directory 用户名、密码，并确认密码。

   示例：域/用户名

   单击“确定”。 服务连接设置已更改。

4. 退出中央配置管理器。

系统 DSN 连接配置示例

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

在以下示例中，为报告门户 CMS 数据库创建系统 DSN：

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

   将打开 ODBC 数据源管理器。

2. 从“系统 DSN”选项卡中选择“创建”。

   将打开“选择新的数据源”窗口。

3. 向下滚动并选择“SQL Server”，然后单击“完成”。

   将打开“创建 SQL Server 的新数据源”向导。

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

   系统 DSN 已创建。

在以 Windows 身份验证模式运行的报告门户上部署报告数据包

在 Windows 上有效

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

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

在报告门户上部署报告数据包

1. 确认中央数据库、分发服务器和报告门户已设置。

   注意：确认 JAVA_HOME 变量已在报告门户计算机上设置。

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

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

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

4. 将 biconfig.zip 的内容提取到临时目录。

5. 将以下文件从光盘复制到同一临时目录：

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

   RDBMS

   定义用于 CA Access Control 报告的 RDBMS 类型。

   值：MSSQL2005。

   ***import_biar_config*.xml**

   为 RDBMS 定义导入配置文件 (.xml) 的名称。

   值：import_biar_config_mssql_2005.xml

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

   ***AC_BIAR_File*.biar**

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

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

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

   重要说明！ 从文件中删除用户名、密码和服务器字段。

   <biar-file name>

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

   <networklayer>

   定义 RDBMS 支持的网络层。

   值： ODBC。

   <rdms>

   定义用于 CA Access Control 报告的 RDBMS 类型。

   值： 通用 ODBC 数据源

   <datasource>

   定义已创建的 DSN

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

7. 打开命令提示符窗口并输入以下命令：

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

   host_name

   定义报告门户主机名。

   user_name

   定义您在安装报告门户时配置的报告门户管理员。

   密码

   定义报告门户管理员的密码。

   例如：

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

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

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

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

为大型部署配置 BusinessObjects

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

为大型部署配置 BusinessObjects

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

      将打开 BusinessObjects 配置管理器。
   b. 右键单击“Crystal 页面服务器”并选择“停止”。
   c. 右键单击“Crystal 页面服务器”并选择“属性”。
   d. 确认以下文本显示在“可执行文件的路径”字段的 *-restart* 之后：

      ```
      -maxDBResultRecords 0
      ```
   e. 重新启动 BusinessObjects 页面服务器。

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

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

   c. 依次单击“编辑”、“新建”、“DWORD 值”。

      将显示 REG_DWORD 类型的新注册表项。
   d. 将该项重命名为 *QPMaxLOVSize*。
   e. 双击该项并将其“数值数据”编辑为 1000。

      已设置新注册表项。
   f. 打开 BusinessObjects 中央管理控制台 (CMC)。
   g. 导航至“服务器”管理区域。
   h. 单击要更改其设置的 Web Intelligence 报告服务器。

      “Web Intelligence 报告服务器”页面将在“属性”选项卡中打开。
   i. 将以下值修改为大于 1000 的值，或根据需要进行修改：
      - 值批次大小列表
      - 用于自定义排序的值列表的最大大小

      单击“应用”提交更改，并重新启动服务器，以使更改立即生效。

配置到 CA Business Intelligence 的连接

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

配置到 CA Business Intelligence 的连接

1. 启用 CA Identity Manager 管理控制台 (p. 72)。
2. 打开 CA Identity Manager 管理控制台 (p. 73)。
3. 单击“环境”、“ac-env”、“高级设置”、“报告”。

   将显示“报告属性”窗口。
4. 输入数据库和业务对象属性。

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

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

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

   CA Business Intelligence 设置已保存。

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

创建快照定义

报告基于从 CA Access Control 和 UNAB 端点收集并存储在中央数据库中的数据快照、CA Access Control 企业管理 中的 PUPM 数据以及用户存储中的数据。

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

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

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

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

注意：默认情况下，您必须具有“系统管理员”角色才能创建快照定义。

创建快照定义

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

4. 填写“配置文件”选项卡中的以下字段：

   快照定义名称

   定义快照定义的名称。

   快照定义说明

   指定描述快照定义的任何其他信息。

   已启用

   指定 CA Access Control 企业管理 启用快照定义。

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

   标识符

   指定用于定义报告快照范围的快照参数 XML 文件。

   默认值：PPM_ALL.xml

   保留最终个数

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

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

5. 单击“重现”选项卡并选择“排定”。

   此时将显示排定选项。

6. 指定快照执行时间和重现模式，然后单击“提交”。

   注意：建议您将此快照排定为运行频率小于来自 CA Access Control 和 UNAB 端点的快照。

   将 CA Access Control 配置为按排定的时间和频率捕获快照。

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

限制报告快照的范围

当 CA Access Control 企业管理 捕获报告快照时，它收集 CA Access Control 和 UNAB 端点的快照数据、CA Access Control 企业管理 的 PUPM 数据，以及用户存储数据。 CA Access Control 企业管理 收集报告数据后，将数据存储在中央数据库中。

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

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

限制报告快照的范围

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

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

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

   您已创建新的快照参数 XML 文件。

3. 以可编辑格式打开新的快照参数 XML 文件。

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

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

6. （可选）限制 Active Directory 快照的范围：

   a. 查看LDAP 查询如何限制报告快照 (p. 123)和LDAP 语法注意事项 (p. 123)主题。

      这些主题中的信息将帮助您按以下步骤定义正确的 LDAP 查询。

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

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

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

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

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

d. 在 <!--PUPM COLLECTORS--> 部分找到以下元素：

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

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

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

您已限制 Active Directory 快照的范围。

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

运行捕获快照任务时，它仅收集快照参数 XML 文件中指定的数据。

示例：将报告快照的范围限制到 CA Access Control 端点

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

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

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

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

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

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

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

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

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

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

快照参数 XML 文件语法－限制报告快照

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

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

每个收集器都具有以下结构：

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

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

每个收集器包含以下元素：

<export>

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

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

<export> 元素只有对象参数。

<where>

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

下表说明 <where> 元素的参数：

参数	说明
attr	表示要用于筛选的属性。

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

<value>

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

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

<exportattr>

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

<exportattr> 元素具有 attr 参数。

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

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

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

LDAP 查询如何限制报告快照中的用户和组数据

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

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

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

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

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

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

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

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

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

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

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

LDAP 语法注意事项

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

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

- AND (&)

  注意：某些限制适用于与号 (&) 字符。
- NOT (!)
- 通配符 (*)

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

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

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

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

示例：与号字符

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

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

在使用 CA Access Control r12.0 安装的报告门户中部署报告数据包

在 Windows 上有效

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

该过程说明如何在使用 CA Access Control r12.0 安装的 CA Business Intelligence 现有安装中部署报告数据包。

请按下列步骤操作：

1. 将适用于您操作系统的 CA Access Control 高级版 Server Components DVD 插入光盘驱动器并导航至 /ReportPackages 目录。
2. 为安装文件创建临时的文件夹：
   - 在 Windows 的 C:\ 驱动器根目录下，创建名为 BO 的文件夹。

     注意：在该文件夹中大约需要 2 GB 内存。
   - 在 Linux 上，创建目录 /work/bo
3. 将以下文件从光盘驱动器复制到同一临时目录：
   - /ReportPackages/*RDBMS/import_biar_config*.xml
   - /ReportPackages/*RDBMS/AC_BIAR_File*.biar

   RDBMS

   定义使用的 RDBMS 类型。

   值：Oracle、MSSQL2005

   ***import_biar_config*.xml**

   为您的 RDBMS 定义导入配置文件 (.xml) 的名称。

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

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

   ***AC_BIAR_File*.biar**

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

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

4. 将针对您平台的 CA Access Control 高级版 r12.0 Server Components DVD 插入光盘驱动器并导航至 /ReportPortal 目录。

   注意：该 DVD 是您与 r12.0 接收的部分介质。

5. 完成以下步骤之一：

   - 在 Windows 上，将 \ReportPortal\BO 目录的内容从 DVD 复制到所创建的 C:\BO 文件夹中。
   - 在 Linux 上，将 /ReportPortal/bo_install.tar.gz 提取到所创建的 /work/bo 文件夹。

6. 将 \ReportPortal\BO 目录的内容从 DVD 复制到所创建的 C:\BO 文件夹中。

7. 打开目标目录并浏览到 *BO_files*/biek-sdk。

8. 按如下所示编辑 biekInstall.properties 文件的副本：

   ```
   BIEK_CONNECT_LAYER=networklayer
   BIEK_CONNECT_DB=rdms
   BIEK_CONNECT_USER=rdbms_adminUserName
   BIEK_CONNECT_PASSWORD=rdbms_adminUserPass
   BIEK_CONNECT_SOURCE=rdbms_Datasource
   BIEK_CONNECT_SERVER=rdbms_hostName
   BIEK_BO_USER=InfoView_adminUserName
   BIEK_BO_PASSWORD=InfoView_adminUserPass
   BIEK_BIAR_FILE=AC_BIAR_File.biar
   ```

   networklayer

   定义 RDBMS 支持的网络层。

   限制：区分大小写。

   rdms

   定义使用的 RDBMS 类型。

   限制：区分大小写。

   rdbms_adminUserName

   定义您创建的 RDBMS 管理用户的用户名。

   rdbms_adminUserPass

   定义您创建的 RDBMS 管理用户的密码。

   rdbms_Datasource

   定义 Oracle 数据库的透明网络底层 (TNS) 的名称。

   rdbms_hostName

   定义 RDBMS 服务器的主机名。

InfoView_adminUserName

定义 InfoView 管理用户的用户名。默认情况下，该用户是*管理员*。

InfoView_adminUserPass

定义 InfoView 管理用户的密码。默认情况下，该用户没有密码（保留为空）。

***AC_BIAR_File*.biar**

定义 CA Access Control 报告文件 (.biar) 的完整路径名。 这是您早些时候复制的文件。

9. 启动批处理文件 *BO_Files*/biek-sdk/importBiarFile.bat。

该文件将 CA Access Control 报告导入 InfoView。 导入可能需要几分钟时间才能完成。

第 5 章： 安装端点管理

此部分包含以下主题：

如何准备端点管理服务器

安装 CA Access Control 端点管理 之前，需对此服务器进行准备。

重要说明！ 如果打算在同一台计算机上安装 CA Access Control 企业管理，您无需执行以下步骤。 安装程序会在安装 CA Access Control 企业管理 的过程中安装 CA Access Control 端点管理。

要准备端点管理服务器，请执行以下操作：

1. 安装受支持的 Java 开发工具包 (JDK)。

   注意：您可在 CA Access Control 高级版 第三方组件 DVD 中找到必备的第三方软件。 有关受支持版本的信息，请参阅 *《版本说明》*。

2. 安装支持的 JBoss 版本。

   建议您将 JBoss 作为服务（UNIX 上的后台进程）运行。

   注意：您可在 CA Access Control 高级版 第三方组件 DVD 中找到必备的第三方软件。 有关受支持版本的信息，请参阅 *《版本说明》*。

3. 安装 CA Access Control。

   注意：按照安装 CA Access Control 端点的说明进行操作。

4. （仅适用于 Windows）重新启动计算机。

5. 停止 CA Access Control 服务 (secons -s)。

   现在该服务器已为安装 CA Access Control 端点管理 做好准备。

在 Windows 上安装 CA Access Control 端点管理

在 Windows 上有效

当您在 Windows 计算机上安装 CA Access Control 端点管理 时，图形安装会使用向导提供支持和引导。

在 Windows 上安装 CA Access Control 端点管理

1. 确认服务器已准备妥当 (p. 129)。
2. 将 CA Access Control 高级版 Server Components for Windows DVD 插入光盘驱动器中。
3. 打开 CA Access Control 产品资源管理器 (ProductExplorerx86.EXE)。

   将显示 CA Access Control 产品浏览器。
4. 展开“组件”文件夹，选择“CA Access Control 端点管理”，然后单击“安装”。

   InstallAnywhere 向导开始加载。
5. 按照需要完成该向导。 以下安装输入需加以说明：

   JBoss 文件夹

   定义 JBoss 应用程序服务器的安装位置。

   如果使用提供的 JBoss 版本，此文件夹将是解压缩 JBoss zip 文件内容的位置。

   Web 服务信息

   定义要安装 CA Access Control Web 服务的*位置*以及此服务要使用的*端口*（默认情况下为 5248）。

   完整的计算机名

   定义应用程序服务器（本地计算机）的名称。 随后访问应用程序时需要在 URL 中使用此名称。

   现在安装已完成。

在 Solaris 或 Linux 上安装 CA Access Control 端点管理

您必须使用控制台安装程序在 Solaris 或 Linux 计算机上安装 CA Access Control 端点管理。

在 Solaris 或 Linux 上安装 CA Access Control 端点管理

1. 确保将服务器准备妥当 (p. 129)。

2. 将 CA Access Control 高级版 Server Components for Solaris 或 CA Access Control 高级版 Server Component for Linux DVD 插入光盘驱动器。
3. 挂接光盘驱动器。
4. 打开终端窗口并导航至光盘驱动器上的 EndPointMgmt 目录。
5. 输入下面的命令：

   ```
   install_EM_r125.bin -i console
   ```

   稍后将显示 InstallAnywhere 控制台。
6. 根据需要完成提示。 以下安装输入需加以说明：

   按数字选择区域设置

   定义代表安装所使用的区域设置的数字。

   注意：要使用任何支持的非英语语言进行安装，需要使用已本地化的操作系统。

   JBoss 文件夹

   定义 JBoss 应用程序服务器的安装位置。

   如果使用提供的 JBoss 版本，此文件夹将是解压缩 JBoss zip 文件内容的位置。

   Web 服务信息

   定义要安装 CA Access Control Web 服务的*位置*以及此服务要使用的*端口*（默认情况下为 5248）。

   完整的计算机名

   定义应用程序服务器（本地计算机）的名称。 随后访问应用程序时需要在 URL 中使用此名称。

   现在安装已完成。

在 Windows 上卸载 CA Access Control 端点管理

请确保使用具有 Windows 管理权限的用户身份（即 Windows 管理员或 Windows Administrators 组成员）登录到 Windows 系统。

在 Windows 上卸载 CA Access Control 端点管理

1. 如果 JBoss 正在运行，请将其停止。
2. 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。
3. 滚动浏览程序列表，然后选择 CA Access Control 端点管理。

4. 单击“更改/删除”。

   此时将显示“卸载 CA Access Control 端点管理”向导。

5. 按照向导的说明卸载 CA Access Control 端点管理。

   卸载完成后，将从您的计算机中删除 CA Access Control 端点管理。

6. 单击“完成”关闭向导。

在 Solaris 或 Linux 上卸载 CA Access Control 端点管理

如果要从计算机中删除 CA Access Control 端点管理，您需要使用 CA Access Control 端点管理 提供的卸载程序。

在 Solaris 或 Linux 上卸载 CA Access Control 端点管理

1. 执行以下操作之一停止 JBoss：

   - 从 JBoss 作业窗口中断 (Ctrl+C) 进程。
   - 在单独的窗口中键入：

     ```
     ./JBoss_path/bin/shutdown -S
     ```

2. 输入下面的命令：

   ```
   "/ACEMInstallDir/Uninstall_EndpointManagement/Uninstall_CA_Access_Control_Endpoint_Management"
   ```

   ACEMInstallDir

   定义 CA Access Control 端点管理 的安装目录。默认情况下，此路径为：

   ```
   /opt/CA/AccessControlServer/EndpointManagement/
   ```

   InstallAnywhere 将加载卸载控制台。

3. 按照提示卸载 CA Access Control 端点管理。

   卸载完成后，将从您的计算机中删除 CA Access Control 端点管理。

启动 CA Access Control 端点管理

安装 CA Access Control 端点管理 后，您需要启动 CA Access Control 和 Web 应用程序服务器。

启动 CA Access Control 端点管理

1. 启动 CA Access Control 服务。

   CA Access Control 端点管理 要求 CA Access Control 正在运行。

2. （仅适用于 Windows）执行下列操作：

   a. 启动以下附加服务，这些服务在您发出 seosd -start 命令时不会加载：

      - CA Access Control Web 服务
      - CA Access Control 消息队列（如果存在）

   b. 通过执行以下操作之一启动 JBoss 应用程序服务器：

      - 依次单击“开始”、“程序”、“CA”、“Access Control”、“启动任务引擎”。

        注意：任务引擎首次启动时可能需要一些时间加载。

      - 在“服务”面板中启动“JBoss 应用程序服务器”服务。

      JBoss 应用程序服务器完成加载后，您将可以登录到 CA Access Control 端点管理 基于 Web 的界面。

3. （仅适用于 UNIX）输入 *./JBoss_HOME*/bin/run.sh -b 0.0.0.0

   注意：JBoss 应用程序服务器首次启动时可能需要一些时间加载。

   JBoss 应用程序服务器完成加载后，您将可以登录到 CA Access Control 端点管理 基于 Web 的界面。

打开 CA Access Control 端点管理

安装并启动 CA Access Control 端点管理 后，您可以使用用于访问 CA Access Control 端点管理 的 URL 从远程计算机打开该基于 Web 的界面。

打开 CA Access Control 端点管理

1. 在您的主机中打开 Web 浏览器并输入以下 URL：

   http://*enterprise_host*:*port*/acem

2. 输入以下信息：

   用户名

   定义有权执行 CA Access Control 管理任务的用户的名称。

   注意：用于登录的用户名应包含计算机名（例如：Windows 上必须包含 *myComputer\Administrator*，UNIX 上必须包含 *root*）。

   密码

   定义 CA Access Control 用户的密码。

   主机名

   定义要在上面执行管理任务的端点的名称。 此端点可以是主机，也可以是 PMDB，用以下格式指定：*PMDB_name@host_name*

   注意：您必须具有从安装了 CA Access Control 端点管理 的计算机上管理端点的权限（使用 TERMINAL 资源）。

   单击“登录”。

   “显示板”选项卡上将打开 CA Access Control 端点管理。

注意：您还可以通过依次单击“开始”、“程序”、“CA”、“Access Control”、“端点管理”从安装了 CA Access Control 端点管理 的 Windows 计算机上打开 CA Access Control 端点管理。

示例：打开 CA Access Control 端点管理

将以下 URL 输入 Web 浏览器中可从网络上的任意计算机打开 CA Access Control 端点管理：

```
http://appserver123:18080/acem
```

该 URL 表明 CA Access Control 端点管理 安装在名为 appserver123 的主机上，并使用默认的 JBoss 端口 18080。

第 6 章： 准备端点实施

此部分包含以下主题：

决定要保护的策略对象

以下各节介绍了在授权对企业应用程序和数据进行访问时，您的安全策略可以使用的一些重要对象。

用户

在 CA Access Control 中，有不同类型的用户。 每一类型的用户都有特定级别的权限和特定的限制。 为组织开发安全策略的一部分任务就是决定哪些特殊权限要授予哪些对象。

CA Access Control 存储关于用户的信息，例如允许用户登录的次数以及对用户执行的审核的类型。 有关用户的信息存储在数据库记录的属性中。

注意：有关用户的详细信息，请参阅 *《端点管理指南》*。

用户类型

CA Access Control 支持以下类型的用户，这些用户用于管理 CA Access Control 数据库中的资源：

常规用户

组织-内部最终用户，即组织中负责业务实施的人员。 可以限制常规用户对同时装有本地操作系统和 CA Access Control 的系统的访问权限。

拥有特殊权限的用户（子管理员）

授予可执行一个或多个特定管理任务的能力的常规用户。 如果授予常规用户执行特定管理功能的权限，就会减轻管理员的工作量。在 CA Access Control 中，这称为任务指派。

管理员

在本地操作系统和 CA Access Control 中具有最高权限的用户。管理员可以添加、删除和更新用户，可以执行几乎所有管理任务。 使用 CA Access Control 可以限制本地超级用户的权限。 可以向无法自动获悉其帐户的特定用户分配管理任务。 这意味着入侵者无法直接搞清楚哪个用户执行管理任务。

组管理员

在一个特定组中可以执行大多数管理功能（例如添加、删除和更新用户）的用户。 在本机 Windows 中，找不到这种类型的拥有有限特定权限的用户。

密码管理员

有权修改其他用户密码的用户。密码管理员无法更改其他用户属性。在本地操作系统中没有此类用户。

组密码管理员

有权修改某个特定组中其他用户密码的用户。 组密码管理员无法更改组中用户的其他用户属性。 在本地操作系统中没有此类用户。

审核员

具有读取审核日志权限的用户。 他们还确定对每次登录和每次访问资源的尝试所做的审核种类。 在本地操作系统中没有此类用户。

组审核员

可以读取与他们的组相关的审核日志的用户。 他们还有权确定在特定组中进行审核的种类。 在本地操作系统中没有此类用户。

操作员

这些用户可以显示（读取）数据库中的所有信息，关闭 CA Access Control，以及使用 secons 实用程序来执行任务（如管理 CA Access Control 跟踪和显示运行时统计信息）。 在本地操作系统中没有此类用户。

注意：有关 secons 实用程序的详细信息，请参阅*《参考指南》*。

组操作员

可以为在其中定义他们的组显示数据库中所有信息的用户。在 在本地操作系统中没有此类用户。

服务器

特殊类型的用户，实际上是一个进程，可以请求对其他用户的权限。

安全策略和用户

准备实施时，您应该决定：

- 向定义的用户授予哪些特殊权限（如果有）
- 向定义的用户授予哪些全局授权属性和组授权属性

  例如：您应该决定将哪些用户定义为系统管理员、密码管理员、组密码管理员、审核员和操作员。

组

组是通常共享相同访问权限的一组用户。 管理员可以将用户添加到组中，从组中删除用户，按组分配或拒绝系统资源的访问权限。 该类型的组在本地操作系统和 CA Access Control 中均存在。

组记录包含有关该组的信息。 存储在组记录中的最重要信息是作为该组成员的用户的列表。

重要说明！ 组记录的授权规则以循环方式应用于该组层级结构中的每个用户。

例如：组 A 有两名成员：用户 X 和组 B。 用户 Y 是组 B 的成员。 更改组 A 的授权规则时，CA Access Control 会将更改的授权规则应用到组 A 层次结构中的所有用户和组，即用户 X、组 B 和用户 Y。

组记录中的信息存储在*属性*中。

在 CA Access Control 中，组管理员可以管理其定义到的特定组的组功能。 组密码管理员可以更改组成员的密码。

安全策略和组

在制定组织的安全策略时，您应该决定：

- 为实现安全管理目标需要创建的组
- 每个组中要加入哪些用户
- 是否定义组管理员和组密码管理员，如果这样，向哪些用户授予这些管理角色

预定义用户组

CA Access Control 中包括用户可加入的预定义组。 _restricted 组即为这样的一个组。 对于 _restricted 组中的用户，所有文件和注册表键都受 CA Access Control 的保护。 如果文件或注册表键没有显式定义访问规则，则将由该类（FILE 或 REGKEY）的 _default 记录授予访问权限。

请慎用 _restricted 组。 _restricted 组中的用户可能没有足够的权限开展工作。 如果您打算向 _restricted 组添加用户，请考虑在开始就使用警告模式。 在警告模式下，审核日志将显示用户工作需要使用哪些文件和注册表键。 检查审核日志后，可以授予适当的权限并关闭警告模式。

资源访问的预定义组

CA Access Control 中其他类型的预定义组定义对于特定资源允许或禁止的访问权限类型。 这些组包括：

- _network

  （仅 Windows）_network 组定义从网络到特定资源的访问权限。 所有用户均被视为该组的成员，因此不必将用户明确添加到该组。

  例如：可以指定只能从网络读取特定资源。 使用 selang 按如下所示定义新的资源：

  ```
  newres FILE c:\temp\readonly defaccess(none)
  ```

  然后指定允许通过网络进行的访问：

  ```
  authorize FILE c:\temp\readonly gid(_network) access(read)
  ```

  还可以使用 CA Access Control 端点管理 执行该操作。

  现在，从网络访问 c:\temp\readonly 时，用户仅可以从网络读取文件。

- _interactive

  _interactive 组定义允许从特定资源所驻留的计算机上访问该资源的权限。 例如：虽然不允许从网络访问该资源，但是可以从定义文件的计算机授予该文件的“读取”访问权限。

下面的内容非常重要：

- 在 CA Access Control 中，_network 组与 _interactive 组之间没有联系。 这意味着在 _network 组中可以有一个规则定义从网络到特定资源的访问。 _interactive 组中的另一个规则可以定义对相同资源的访问。
- 不必将用户添加到 _network 和 _interactive 组中。
- 这些组可以保护数据库中定义的所有 Windows 资源。

权限属性

授权属性在数据库的用户记录中设置，允许用户执行普通用户不能执行的操作。 两类授权属性是*全局*和*组*。 每个全局权限属性允许用户对数据库中的任何记录执行特定类型的功能。 组权限属性允许用户在一个指定的组中执行特定类型的功能。 以下各节介绍了每个全局授权属性和组授权属性的功能和限制。

全局权限属性

在自己的用户记录中设置了全局权限属性的用户可以对数据库中的任何相关记录执行特殊功能。 全局授权属性包括：

- ADMIN
- AUDITOR
- OPERATOR
- PWMANAGER
- SERVER
- IGN_HOL

注意：有关全局授权属性的更多信息，请参阅*《端点管理指南》*。

组权限属性

在自己的用户记录中具有*组授权属性*的用户可以在指定的组中执行特殊功能。 组授权属性包括：

- GROUP-ADMIN
- GROUP-AUDITOR
- GROUP-OPERATOR
- GROUP-PWMANAGER

注意：有关全局授权属性的详细信息，请参阅*《端点管理指南》*。

使用警告期

除了决定要保护的对象，实施团队还必须考虑如何分阶段进行新的安全控制。 为了尽量不破坏当前工作模式，您应该考虑一个仅监视对资源的访问而不强制访问限制的初始阶段。

可以通过将资源置入警告模式下来监视访问。 为资源或类启用警告模式后，如果用户访问违反了访问限制，CA Access Control 将在审核日志中记录一条警告消息，并授予用户访问该资源的权限。

注意：如果使用警告模式，请考虑增加审核日志的最大大小。 有关警告模式的详细信息，请参阅*《端点管理指南》*。

CA Access Control 后门

首次安装 CA Access Control 时（例如在评估部署中），您可能会在 CA Access Control 数据库中错误地定义规则。 错误定义的规则会阻止用户登录或执行命令。 例如：您可能会错误地定义某个规则来拒绝对系统目录或 Windows 注册表关键部分的访问。

由于很难停止 CA Access Control 并修复这些错误，因此，CA Access Control 上留有一个后门来让您修复这样的问题。 由于后门可能会被恶意利用，因此，在系统设置完成并稳定运行后，CA Access Control 还允许您禁用此后门。

要访问此后门，请在启动计算机时从启动菜单中选择“安全模式”或“带网络连接的安全模式”。 选择其中一个选项后，系统在启动时便不会自动启动 CA Access Control 服务。

要禁用此后门，请在注册表键 HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\AccessControl\ 下定义数据类型为 reg_dword 的注册表值 LockEE，并将其设置为 1。

注意：默认情况下，此注册表值不存在。

下面描述了在 LockEE 设置为 1 时，以下列各模式启动系统时发生的情况：

- 安全模式：仅加载 CA Access Control 引擎和 CA Access Control Watchdog。

  不加载依靠网络服务的 CA Access Control 代理（和任何策略模型）。
- 带网络连接的安全模式：CA Access Control 正常启动。

实施提示

本节提供一些安装 CA Access Control 后要考虑的其他实施信息。

安全类型

可以使用下列方法之一处理站点的安全：

- 禁止未明确允许的内容。 这是理想的方法，但是在实施过程中无法使用。 由于没有规则允许对系统做任何操作，系统会阻止定义访问规则的所有尝试。 这就像钥匙插在点火器上而您被关在车外一样。
- 允许未特别禁止的内容。 该方法的安全性可能较低，但它是实现安全系统的实用方法。

通过 CA Access Control，您可以从第二个方法开始操作，定义完访问规则后，就切换到第一个方法。 默认访问 (defaccess) 和通用访问 (_default) 规则允许您随时定义方法并切换保护策略。

重要说明！ 在切换保护策略时，可能需要将所有用户添加到 _restricted 组中。 在保护策略之间切换时，性能可能会受到较大的影响。

访问者

*访问者*是可以访问资源的实体。 最常见的访问者类型是访问权限应予以分配和检查的用户或组。 当程序访问资源时，该程序的所有者（用户或组）就是访问者。 访问者分为三类：

- 与特定用户 ID 关联的人员
- 作为组成员、拥有访问权限的人员
- 与特定用户 ID 关联的生产进程

最常见的访问者类型是用户，即可以执行登录且为其分配并检查了访问权限的人员。 CA Access Control 的最重要的特点之一是责任性。 每个操作或访问尝试都是代表负责请求的用户执行的。

通过 CA Access Control，您可以定义用户组。 用户通常按项目、部门或分支机构分组。 通过将用户分组到一起，可以明显减少安全管理所需的工作量。

可以通过 CA Access Control 端点管理 或通过 selang 命令定义新用户和组以及修改现有用户和组。

资源

任何安全策略的关键部分是决定必须保护哪些系统资源和定义这些资源要接收的保护类型。

资源类和访问规则

安装后，CA Access Control 立即开始侦听系统事件和检查用户访问资源的权限。 在您设置 CA Access Control 如何限制对系统资源的访问权限以及要限制哪些资源之前，所有权限检查的结果都允许访问。

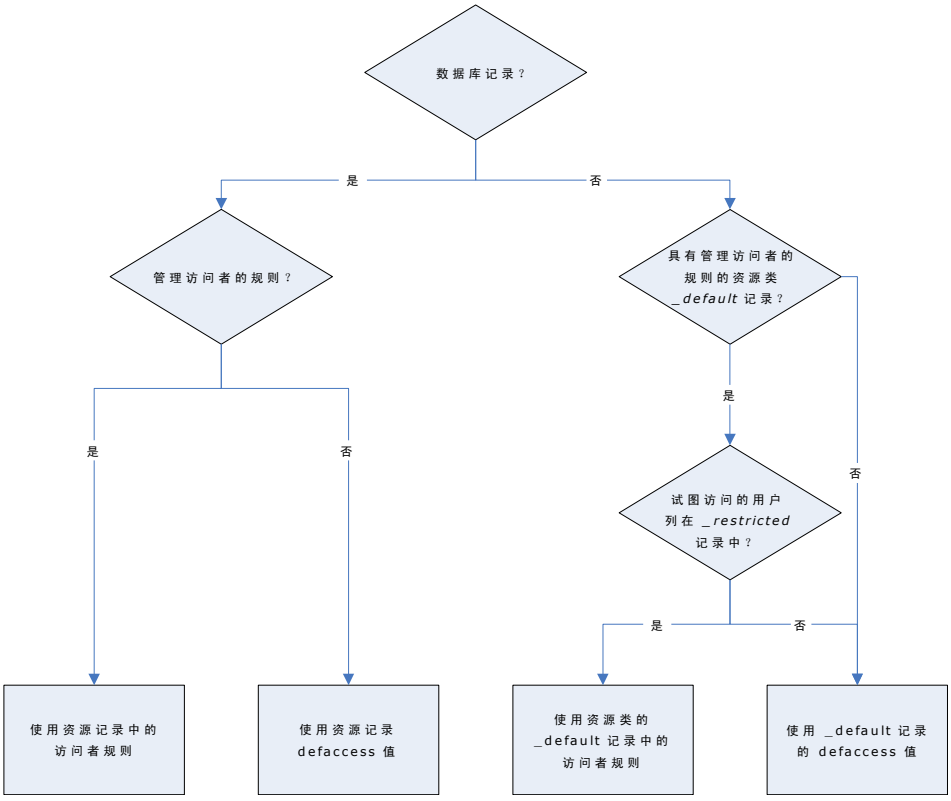
受保护资源的属性存储在资源记录中，资源记录被划分为类。 资源记录中包含的最重要信息是其访问规则。 *访问规则*管理一个或多个访问者使用一个或多个资源的权限。 定义访问规则的一些方法包括：

- Access Control 列表（有权访问资源的访问者及其可以拥有的确切访问权限的特定列表），也称为 ACL
- 拒绝 Access Control 列表（访问权限应被拒绝的访问者的列表），也称为 NACL
- 对资源的默认访问，为 ACL 中未特别列出的访问者指定了访问规则
- 全局访问（类的 _default 记录），指定了对尚未在该类中具有特定资源记录的资源的访问
- 程序 ACL，用于通过特定程序定义特定访问者的访问权限
- 条件 ACL，依赖某些条件进行访问。 例如：在 TCP 记录中，可以定义通过特定访问者对特定远程主机的访问
- Inet ACL，用于定义通过特定端口对传入网络活动的访问

使用 defaccess 和 _default

当请求对某资源进行访问时，将按照下列顺序搜索数据库，以确定应该如何处理该请求，CA Access Control 会使用找到的第一个访问规则。 请注意*默认访问权限* (defaccess) 与 _default 之间的区别。

1. 如果资源在数据库中有记录，且该记录有管理访问者的规则，则 CA Access Control 将使用该规则。
2. 如果有记录但没有管理访问者的规则，则*该记录的*默认访问规则（其 *defaccess 值*）适用于该访问者。
3. 如果*没有*记录，但在资源类中 _default 记录具有管理访问者的规则，则 CA Access Control 将使用该规则。
4. 如果没有记录，且在资源类中 _default 记录也没有管理访问者的规则，则 _default 记录的默认访问规则（其 defaccess 值）适用于该访问者。 对于文件和注册表键，这只适用于 _restricted 用户 (p. 138)。



注意：有关资源类和访问规则的详细信息，请参阅*《selang 参考指南》*。

第 7 章： 安装和自定义 Windows 端点

此部分包含以下主题：

开始之前

安装 CA Access Control 之前，您必须确保满足某些初步要求，并且具有一些必要信息项。

安装方法

您可以使用以下方式从 CA Access Control Endpoint Components for Windows DVD 中安装 CA Access Control for Windows：

- **产品资源管理器**－安装 CA Access Control 最简单的方法是使用产品资源管理器。 产品资源管理器是一个图形安装程序，使您可以在 CA Access Control 的不同体系结构安装之间进行选择和安装运行时 SDK。 产品资源管理器会指导您分步完成安装过程的每个阶段，并提示您输入每个阶段必须提供的信息。
- **命令行**－通过安装程序的命令行界面，您可以：
  - 为运行图形安装程序设置自定义默认值

    您可以将默认值从命令行传递到图形安装程序。 使用该方法可创建批处理文件，该文件通过要使用的预置默认值打开安装程序，但仍可使您为每个安装自定义选项。
  - 执行静默安装

    您可以静默安装 CA Access Control，而不是使用命令行只将默认值传递到图形安装程序。 使用该方法可将安装推入远程计算机。
- **Unicenter Software Delivery**－通过 Unicenter Software Delivery，您可以创建用于分发 CA Access Control 的程序包。

防火墙设置

在 Windows Server 2003 或 Windows Server 2008 上安装 CA Access Control 时，CA Access Control 会打开用于非 SSL TCP 连接的端口 8891 和用于 SSL TCP 连接的端口 5249。 该端口将用作 CA Access Control 代理-客户端连接的默认端口。

注意：有关 CA Access Control 在 Windows 上使用的端口的详细信息，请参阅 *《参考指南》*。

新安装

安装 CA Access Control 的新例程时，请注意以下事项：

- 阅读 *《版本说明》*。

  此文档包含关于所支持平台的信息、已知问题、注意事项以及安装 CA Access Control 之前应阅读的其他重要信息。
- Windows Administrator 或 Administrators 组的成员必须安装 CA Access Control。

- 将 CA Access Control 安装在不同于其他任何产品安装目录的唯一目录中。
- 您必须安装有 Microsoft Internet Explorer 6.x 或 7.x。
- CA Access Control 需要 Microsoft Visual C++ 2005 可再分发程序包完成产品安装。

  如果缺少此程序包，安装程序将首先安装该程序包。
- 使用 CA Technologies 许可

  在某一网络中运行 CA Technologies 软件的每台计算机上，所有 CA Technologies 企业版产品及其选件都需要一个许可文件：CA.OLF。您购买 CA Access Control 产品时会获得许可证书，其中包含成功安装和授予该产品许可所必需的信息。

  要安装企业许可文件，请将 CA.OLF 文件（添加了 CA Access Control 行）复制到 CA_license 目录（例如：C:\Program Files\CA\SharedComponents\CA_LIC）中。

升级和重新安装

升级 CA Access Control 时，请注意以下事项：

- 阅读*《版本说明》*。

  此文档包含有关所支持平台的信息、可升级的 CA Access Control 版本、已知问题、注意事项以及安装 CA Access Control 之前应阅读的其他重要信息。
- 建议您先执行新版本的缩小内部测试，然后再升级产品环境。
- 在升级 CA Access Control 时，您可能需要重新启动计算机以完成安装。 以后的修补程序可能不需要重新引导。

  注意：有关哪些 CA Access Control 版本在升级时需要重新启动的信息，请参阅*《版本说明》*。

- 如果您的环境是使用 PMDB 层级结构设置的，或者您要设置此类环境，建议您：
  - 在层级结构中自下而上（首先是订户）安装或升级每台计算机。

    如果升级后的 PMDB 中有使用早期版本的订户，可能会导致发送错误命令。 由于新 PMDB 包含早期版本的 PMDB 中不存在的类和属性，因此可能会发生这种情况。

    注意：可以同时升级在单台计算机上运行的 PMDB 层级结构。
  - 请*勿*在 PMDB 或策略更新期间进行升级。
  - 备份订户和 PMDB 策略。

  注意：早期版本的 PMDB 可以拥有后期版本的订户，反之则不可。由于后期版本支持早期版本中的命令，因此早期版本的 PMDB 可传播至当前的 CA Access Control 订户。
- 您必须使用与升级前相同的加密密钥。
- 安装程序将自动保存和升级先前安装的注册表设置。 如果重新找到了早期版本的注册表键，则升级过程会将先前的设置复制到新的位置。

  CA Access Control 注册表设置存储在以下位置：

  `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl`
- 升级 CA Access Control 时，默认情况下启用完全审核。

  重要说明！ 由于此功能，根据数据库中的规则，CA Access Control 记录到日志文件中的审核事件的数量可以明显增加。 我们建议您查看审核日志文件大小并备份设置。

  注意：有关完全审核以及如何配置和使用审核日志备份的注册表设置的详细信息，请参阅*《Windows 端点管理指南》*。

与其他产品共存

安装 CA Access Control 时，请考虑 CA Access Control 与计算机上其他程序共存的问题。

CA Access Control 将在与其他程序（例如：CA Antivirus）共存的环境中运行。 这可能导致在 CA Access Control 与在本地计算机上运行的程序出现冲突。 为此目的，在安装 CA Access Control 期间，共存实用程序 (eACoexist.exe) 将运行，以检测本地计算机上可能导致出现冲突的程序。 对于 CA Access Control 支持的每个共存程序，该实用程序将使用插件（二进制模块）。 如果 CA Access Control 检测到受托程序，则 CA Access Control 将通过创建 SPECIALPGM 规则注册该程序。 此 SPECIALPGM 规则可确定该程序的访问权限，并确保当授予权限时 CA Access Control 跳过该程序。

注意：有关 eACoexist 实用程序及受支持插件的详细信息，请参阅*《参考指南》*。

示例：针对 Dr Watson 的受托程序规则

此示例展示了如果共存实用程序在 CA Access Control 所在的同一计算机上发现可能导致出现冲突的程序，它可以为 Dr Watson 应用程序创建的受托程序规则。 在使用默认设置安装了 Windows 2000 Server 的计算机上，这些规则如下所示：

```
editres SPECIALPGM ('C:\WINNT\system32\DRWTSN32.EXE') pgmtype(DCM)
editres PROGRAM ('C:\WINNT\system32\DRWTSN32.EXE') owner(nobody) defacc(x) trust
```

产品资源管理器安装

通过 CA Access Control 产品资源管理器，您可以在 CA Access Control 的不同体系结构安装之间进行选择和安装运行时 SDK。 您还可以查看安装组件的系统要求。

注意：如果已启用自动运行，则将 CA Access Control Endpoint Components for Windows DVD 插入光盘驱动器时将自动显示产品资源管理器。

使用产品资源管理器安装

通过 CA Access Control 产品资源管理器，您可以在 CA Access Control 的不同体系结构安装之间进行选择和安装运行时 SDK。 产品资源管理器使用图形界面安装 CA Access Control 并提供交互反馈。

使用产品资源管理器进行安装

1. 使用具有 Windows 管理权限的用户身份（即 Windows 管理员或 Windows Administrators 组成员）登录到 Windows 系统。
2. 关闭 Windows 系统上正在运行的所有应用程序。
3. 将 CA Access Control Endpoint Components for Windows DVD 插入光盘驱动器中。

   如果已启用自动运行，产品资源管理器将自动显示。 否则，请导航至光盘驱动器目录并双击 PRODUCTEXPLORERX86.EXE 文件。
4. 从产品资源管理器的主菜单中，展开组件文件夹，选择“CA Access Control for Windows”(*my_architecture*)，然后单击“安装”。

   您需要选择与安装所在的计算机的体系结构（32 位、64 位 x64 或 64 位 Itanium）相匹配的安装选项。

   将显示“选择安装语言”窗口。
5. 选择安装 CA Access Control 要使用的语言，并单击“确定”。

   CA Access Control 安装程序开始加载，稍后将显示“简介”屏幕。

   注意：如果安装程序检测到已安装有 CA Access Control，将提示您选择是否要升级 CA Access Control。
6. 按照安装屏幕中的说明进行操作。

   在安装过程中，安装程序将提示您提供信息。 有关安装 CA Access Control 时所需的信息，请参阅“安装工作表” (p. 151)。

   安装程序将安装 CA Access Control。 安装完成后，您需要选择立即重新启动 Windows 还是稍后重新启动。
7. 选择“是，我希望立即重新启动计算机”，然后单击“确定”。

   系统重新引导后，您可以检查 CA Access Control 是否已正确安装 (p. 169)。

   注意：如果您选择稍后重新启动计算机，则系统将显示一条附加的警告信息，提示您重新启动计算机后才能完成安装。 某些 CA Access Control 功能（如登录截获）需要重新启动计算机后才能运行。

安装工作表

安装程序将提示您提供初始 CA Access Control 安装所需的信息。 以下部分说明了需要提供的信息，并提出了建议。

功能选择

通过安装程序的“选择功能”屏幕，您可以定义要安装 CA Access Control 的位置，以及要在该计算机上安装的功能。 提供以下功能：

功能	说明	推荐
任务委托	可使您向普通用户授予执行管理任务所需的权限。 **注意：**默认已选择。	如果要向用户提供子管理权限，请选择该功能。 您也可以配置该安装后功能。
SDK	创建称为 SDK 的子目录。 它包含使用 CA Access Control SDK 和 API 示例所需的库和文件。	如果您要开发受 CA Access Control 保护的内置应用程序，请选择该功能。
堆栈溢出保护 (STOP)	启用 CA Access Control 堆栈溢出保护功能。	选择该功能可保护您的程序不被恶意利用。
大型机密码同步	通过该功能，您可以将用户密码与您的大型机进行同步。	如果您拥有要保持同步的大型机，请选择该功能。
Unicenter 集成	可使您集成 Unicenter NSM 和 CA Access Control 并迁移 Unicenter NSM 数据。 CA Access Control 向 Unicenter NSM 的配置参数所指定的主机或您选择的主机发送审核数据。 **注意：**仅当此计算机安装了 Unicenter NSM 后，此功能才可用。	
高级策略管理客户端	将本地计算机配置为使用高级策略管理。	为希望能够向其部署策略（使用高级策略管理）的每个端点选择该功能。 **注意：**有关高级策略管理的详细信息，请参阅 *《企业管理指南》*。
策略模型订户	将本地计算机配置为从父 PMDB 接收更新。	为希望能够从父 PMDB 进行更新的每个端点选择此功能。 **注意：**有关策略模型服务的详细信息，请参阅 *《适用于 Windows 的端点管理指南》*。

功能	说明	推荐
PUPM 集成	PUPM 集成配置本地计算机以实现特权用户密码管理 (PUPM)，以便您可以发现和管理计算机上的特权帐户和应用程序。	为希望使用 PUPM 管理其特权帐户的每个端点选择此功能。 **注意：**有关 PUPM 的详细信息，请参阅 *《企业管理指南》*。
报告代理	允许您配置计算机，以便将排定的数据库快照发送到分发服务器。 之后您也可以选择将审核记录发送到分发服务器。	如果要将该端点包含在您的企业报告中，请选择该报告代理功能。 如果您想使用 CA Enterprise Log Manager 管理您的企业审核日志，请选择审核传递子功能。

管理员和主机信息

下表说明了需要提供的信息，并提出了建议：

信息	说明	推荐
管理员	可使您定义具有对 CA Access Control 数据库的管理访问权限的用户。	
管理终端	可使您定义管理员可管理 CA Access Control 数据库的计算机。	如果管理员使用 CA Access Control 端点管理管理 CA Access Control，您只需定义安装了 CA Access Control 端点管理 的计算机。 您无需定义管理员打开浏览器的计算机。
DNS 域名	可使您输入 CA Access Control 要添加到主机名的网络域名。	您必须输入至少一个 CA Access Control 添加到主机名的域名。

用户和组

下表说明了需要提供的信息，并提出了建议：

信息	说明	推荐
支持来自主存储的用户和组	允许您使用现有的企业用户存储（主存储）而无需在 CA Access Control 数据库中复制这些用户。	建议您设置 CA Access Control 以支持主存储，即支持企业用户存储。 如果您选择*不*支持企业存储，则需要在 CA Access Control 数据库中复制要保护的访问者。

信息	说明	推荐
导入 Windows 用户和组的数据	如果您要创建要保护的访问者，则它可使您将现有 Windows 用户和组自动创建至数据库。	如果您要导入 Windows 用户和组，请选择以下一个或多个选项： ■ **导入用户**－将您的 Windows 用户导入数据库。 ■ **导入组**－将您的 Windows 组导入数据库。 ■ **将用户与其默认组进行连接**－将导入的用户自动添加到数据库中相应的已导入组。 ■ **更改导入数据的所有者**－将您以外的某个人定义为已导入数据的所有者。默认情况下，这些记录的所有者设置为执行安装的管理员（您）。 ■ **从域导入**－从指定的域导入访问者数据。

Unicenter 集成

下表说明了需要提供的信息，并提出了建议：

信息	说明	推荐
将 CA Access Control 与 Unicenter TNG 集成	可使您将 CA Access Control 设置为向 Unicenter TNG 的配置参数所指定的主机或您选择的主机发送审核数据。	要进行集成，请指定应将审核数据发送至 Unicenter NSM，然后选择 CA Access Control 应将审核数据发送到的主机。
将 CA Access Control 与 Unicenter 日历集成	可使您设置对用户和访问权限与 Unicenter NSM 日历集成的支持。	将 CA Access Control 配置为以大于或小于默认值 10 分钟的频率，从 Unicenter NSM 日历主机服务器中检索更新内容。
迁移 Unicenter 安全数据	可使您将 Unicenter 安全数据迁移至 CA Access Control。	如果您未选择该选项，将不执行从 Unicenter 安全到 CA Access Control 的迁移，CA Access Control 中的用户名将显示为完全限定 (DOMAINNAME\USERNAME)。 如果进行了迁移，用户名将不会限定 (USERNAME)。

组件间通讯加密

下表说明了需要提供的信息，并提出了建议。

屏幕	说明	推荐
SSL 通讯	可使您指定是否将安全套接字层 (SSL) 用于组件间通讯。 您可以同时使用 SSL 和对称密钥加密。	建议您同时使用 SSL（使用公钥）和对称密钥加密。
证书设置	如果选择使用 SSL，您可以指定使用的证书。	建议您使用来自知名的证书颁发机构 (CA) 的证书。
生成证书	可使您创建自行签名证书和密钥对以用作根证书。	您可使用自行签名证书，但并不建议您使用。 如果您使用自行签名证书，则必须允许所有主机都使用该证书。
更改证书设置	可使您更改证书设置。	强烈建议您更改默认证书和密钥对的设置。 您也可以指定密码，以保护服务器证书的私钥。
现有证书	可使您提供已安装证书的信息。	
加密设置	可使您设置加密方法和对称加密的密钥。	强烈建议您更改加密密钥的默认设置。

更多信息：

对称加密 (p. 421)
SSL、身份验证和证书 (p. 425)

策略模型订户设置

下表说明了需要提供的信息，并提出了建议：

信息	说明	推荐
指定父策略模型数据库	允许您定义此数据库所订阅的一个或多个父 PMDB。 本地数据库将不接受来自此列表中未指定的任何 PMDB 的更新。 按以下格式定义父 PMDB：*pmdb@hostname.com*	完成安装后，您需要将此数据库定义为父 PMDB 上的订户。 **注意：**指定 _NO_MASTER_ 作为父 PMDB 可表明本地数据库接受来自任何 PMDB 的更新。

信息	说明	推荐
密码策略模型	允许您定义用于传播密码更改的父密码策略模型。 按以下格式定义密码 PMDB：*pmdb@hostname.com*	完成安装后，您需要将此数据库定义为密码 PMDB 上的订户。

高级策略管理客户端

下表说明了需要提供的信息，并提出了建议：

信息	说明	推荐
指定高级策略管理服务器的主机名	可使您定义安装高级策略管理服务器组件的服务器的名称。	按以下格式定义主机名：*dhName@hostName*。 **注意：**有关高级策略管理和报告的详细信息，请参阅*《企业管理指南》*。

报告代理配置

下表说明了需要提供的信息，并提出了建议：

信息	说明	推荐
选择报告日程	允许您指定报告代理向分发服务器发送数据库快照的时间。	建议您不要排定报告代理在系统资源消耗很大时发送快照。
审核路由配置	可使您指定保留带有时间戳标记的审核日志文件备份。 **注意：**仅在“选择功能”页面上选择安装“审核路由”时，才会显示该选项。	请确保选择保留带有时间戳标记的审核日志文件备份。 此为默认设置，必须使用该设置才能确保报告代理可读取所有审核记录。 当备份审核日志文件达到 50 个时，CA Access Control 会覆盖它们。 如果该数量不合适，您应当编辑 logmgr 注册表子键中的 audit_max_files 标记，使其值符合您企业的要求。

分发服务器配置

下表说明了需要提供的信息，并提出了建议：

信息	说明	推荐
服务器名称	可使您定义安装分发服务器的主机的名称。	您必须为安装分发服务器的主机指定完全限定主机名。
使用安全通讯	可使您指定是否要在分发服务器与报告代理之间以及分发服务器与 PUPM 代理之间使用 SSL 进行通讯。	建议使用 SSL。 如果您不使用 SSL，分发服务器将使用 TCP 与报告代理和 PUPM 代理进行通讯。
服务器端口	可使您定义用于在分发服务器与报告代理之间以及分发服务器与 PUPM 代理之间进行通讯的端口号。	如果使用 SSL 通讯，则默认服务器端口号为 7243。 如果不使用 SSL 通讯，则默认服务器端口号为 7222。
通讯密钥	可使您定义用于验证分发服务器与报告代理之间以及分发服务器与 PUPM 代理之间的通讯的新密钥。	确保安装分发服务器时使用相同的密钥。 **注意：**如果使用 SSL 通讯，必须指定通讯密钥。 如果不使用 SSL 通讯，则可以选择不指定通讯密钥。

命令行安装

您可以使用命令行执行以下操作：

- 将默认值传递给图形安装程序。
- 静默安装 CA Access Control。

为安装程序设置自定义默认值

要使用希望用于公司的默认值来设置 CA Access Control 安装程序，您可以使用命令行。 图形安装程序接受用于确定哪些选项是预先选定的命令行中的输入。

为安装程序设置自定义默认值

1. 以拥有 Windows 管理权限的用户（即 Windows 管理员或 Windows Administrators 组成员）身份登录 Windows 系统。
2. 关闭 Windows 系统上正在运行的所有应用程序。

3. 将 CA Access Control Endpoint Components for Windows DVD 插入光盘驱动器中。

   如果您已启用自动运行，则将显示 CA Access Control 产品资源管理器。

4. 如果显示产品资源管理器，请将其关闭。

5. 打开命令行并导航至光盘驱动器上的以下目录：

   `\architecture`

   体系结构

   定义操作系统的体系结构缩写。

   可以为 **X86**、**X64** 和 **IA64** 中的一个。

6. 输入下面的命令：

   `setup [/s] /v"<insert_params_here>"`

   <insert_params_here> 变量用于指定希望传递到安装程序的安装设置。

   将显示安装程序。 安装程序屏幕将显示您选择要传递的默认选项，并使您可以修改这些选项以安装 CA Access Control。

静默安装

要安装 CA Access Control 而不进行交互反馈，您可以使用命令行静默安装 CA Access Control。

静默安装 CA Access Control

1. 以拥有 Windows 管理权限的用户（即 Windows 管理员或 Windows Administrators 组成员）身份登录 Windows 系统。

2. 关闭 Windows 系统上正在运行的所有应用程序。

3. 将 CA Access Control Endpoint Components for Windows DVD 插入光盘驱动器中。

   如果您已启用自动运行，则将显示 CA Access Control 产品资源管理器。

4. 如果显示产品资源管理器，请将其关闭。

5. 打开命令行并导航至光盘驱动器上的以下目录：

   `\architecture`

   体系结构

   定义操作系统的体系结构缩写。

   可以为 **X86**、**X64** 和 **IA64** 中的一个。

6. 输入下面的命令：

   `setup /s /v"/qn COMMAND=keyword <insert_params_here>"`

   <insert_params_here> 变量用于指定希望传递到安装程序的安装设置。

   注意：要执行静默安装，您必须接受许可协议。 接受许可协议和静默安装 CA Access Control 所需的 *keyword* 可在许可协议底部找到，该许可协议在运行安装程序时会显示。

安装命令－安装 CA Access Control for Windows

使用安装命令，通过预置自定义默认值 (p. 156)来安装 CA Access Control for Windows 或在执行静默安装 (p. 157)时进行安装。

注意：有关命令行语法的详细信息，请参阅 Windows Installer SDK 文档，可从 Microsoft Developer Network Library 中获取该文档。

此命令格式如下：

`setup [/s] [/L] [/v"<insert_params_here>"]`

/s

隐藏安装初始化对话框。

/L

定义 CA Access Control 安装语言。

注意：有关该版本中支持的 CA Access Control 安装语言的详细信息，请参阅 *《版本说明》*。

/v "*<insert_params_here>*"

定义要传递给安装程序的参数。

注意：所有参数均应置于引号 ("") 中。

以下参数将通过 /v 参数传递给安装程序：

/l[*mask*] *log_file*

定义安装日志文件的完整路径和名称。 使用掩码 *v 记录所有可用信息。

/forcerestart

指定安装完成后强制重新启动计算机。

/norestart

指定安装完成后不重新启动计算机。

/qn

指定静默安装，与 */s* 选项联合使用。

重要说明！ 使用 *COMMAND* 参数执行静默安装。

AC_API={1 | 0}

指定是否安装 SDK 库和示例（指定为 1 表示安装）。

默认值：0（不安装）。

ADMIN_USERS_LIST=\"*users*\"

定义对 CA Access Control 数据库具有管理访问权限的用户列表（用空格分隔）。

默认值：用户执行安装。

重要说明！ 不要定义列表中的 NT Authority\System 用户。 定义本地管理用户帐户。

ADV_POLICY_MNGT_CLIENT={1 | 0}

配置用于高级策略管理的本地计算机 (1)。

默认值：1

如果将该选项设置为 1，请指定以下内容：

- **APMS_HOST_NAME=\"***name***\"**

  定义安装高级策略管理组件的服务器的名称。

COMMAND=*keyword*

定义接受许可协议和静默安装 CA Access Control 所需的命令。 实际*关键字*可在许可协议的底部找到，许可协议在运行图形安装程序时显示。

默认值：*无*

DIST_SERVER_NAME=\"*name*\"

定义 PUPM 代理和报告代理与其进行通讯的分发服务器主机的完全限定名（例如：test.company.com）。

默认值：*无*

DIST_SERVER_PORT=\"*port*\"

定义 PUPM 代理和报告代理用于与分发服务器进行通讯的端口号。

默认值：7243

DOMAIN_LIST=\"*domains*\"

定义 CA Access Control 要添加到主机名的网络 DNS 域名列表（用空格分隔）。

默认值：*无*

ENABLE_STOP={1 | 0}

指定是否启用堆栈溢出保护 (STOP) 功能（指定为 1 则表示启用）。

默认值：0（禁用）。

注意：STOP 支持仅适用于 x86 和 x64 安装。

HOSTS_LIST=\"*hosts*\"

定义管理员可从中管理 CA Access Control 数据库的计算机（CA Access Control 终端）列表（用空格分隔）。

默认值：当前计算机。

IMPORT_NT={Y | N}

指定是否支持主（企业）用户存储。 如果指定 N，则支持主用户存储。 如果指定 Y，则不支持主用户存储，您可以指定下列一个或多个选项以将 Windows 用户和组导入 CA Access Control 数据库：

- **IMPORT_USERS={1 | 0}**

  指定是否将 Windows 用户导入数据库。

- **IMPORT_GROUPS={1 | 0}**

  指定是否将 Windows 组导入数据库。

- **IMPORT_CONNECT_USERS={1 | 0}**

  指定是否将导入的用户添加到数据库中相应的已导入组。

- **IMPORT_CHANGE_OWNER={1 | 0}**
  NEW_OWNER_NAME=*name*

  将您以外的其他人指定为已导入数据的所有者。

- **IMPORT_FROM_DOMAIN={1 | 0}**
  IMPORT_DOMAIN_NAME=*name*

  指定是否从定义的域导入访问者数据。

注意：在默认情况下，所有这些选项都未指定（等于值 0）。

INSTALLDIR=\"*location*\"

定义安装 CA Access Control 的位置。

默认值：C:\Program Files\CA\AccessControl\

MAINFRAME_PWD_SYNC={1 | 0}

指定是否安装大型机密码同步功能（指定为 1 表示安装）。

默认值：0（不安装）

NEW_KEY=\"*name*\"

定义用于验证分发服务器与 PUPM 代理和报告代理之间的通讯的 SSL 密钥。

PMDB_CLIENT={1 | 0}

指定是否为本地 CA Access Control 数据库订阅父策略模型数据库。

默认值：0（不发送）

如果指定该选项并将其设置为 1，您还需要指定：

- **PMDB_PARENTS_STR=\"*parents*\"**

  定义本地 CA Access Control 数据库订阅的以逗号分隔的父策略模型数据库列表。 指定 _NO_MASTER_ 作为父 PMDB 可表明本地数据库接受来自任何 PMDB 的更新。

  默认值：*无*

- **PWD_POLICY_NAME=\"*name*\"**

  定义密码策略模型的名称。

  默认值：*无*

PMDB_PARENT={1 | 0}

指定是否创建策略模型父数据库。如果指定该选项并将其设置为 1，您还需要指定：

- **PMDB_NAME=\"*name*\"**

  定义要创建的 PMDB 的名称。

  默认值：pmdb

- **PMDB_SUBSCRIBERS_STR=\"*subs*\"**

  定义 PMDB 使用 PMDB_NAME 选项指定的将更改传播到的订户数据库的列表（用空格分隔）。 基本上，这些数据库是已安装的父 PMDB 的订户数据库。

PUPM_AGENT={1 | 0}

指定是否安装 PUPM 代理（指定为 1 表示安装）。

默认值：0（不安装）

如果指定该选项并将其设置为 1，您还需要指定 DIST_SERVER_NAME、DIST_SERVER_PORT 和 USE_SECURE_COMM。

REPORT_AGENT={1 | 0}

指定是否安装报告代理（指定为 1 表示安装）。

默认值：0（不安装）

如果指定该选项并将其设置为 1，您还需要指定 DIST_SERVER_NAME、DIST_SERVER_PORT、USE_SECURE_COMM 以及以下参数：

- **AUDIT_ROUTING={1 | 0}**

  指定是否安装审核路由功能（指定为 1 表示安装）。

  默认值：0（不安装）

- **REPORT_DAYS_SCHEDULE=***days*

  定义报告代理运行日期的列表（用逗号分隔）。

  值：周日、周一、周二、周三、周四、周五、周六

  默认值：*无*

- **REPORT_TIME_SCHEDULE={***hh*:*mm***}**

  定义报告代理在指定日期开始运行的时间（例如：14:30）。

  限制：*hh* 是 0 到 23 之间的数字，*mm* 是 0 到 59 之间的数字

  默认值：*无*

TASK_DELEGATION={1 | 0}

指定是否启用任务指派功能。

默认值：1（启用）。

UNICENTER_INTEGRATION={1 | 0}

指定是否启用 Unicenter 集成功能（指定为 1 表示启用）。 仅当计算机上安装了 Unicenter NSM 时才能使用该功能。

默认值：0（不启用）

如果指定该选项并将其设置为 1，您还需要指定：

- **SEND_DATA_TO_TNG={1 | 0}**

  指定是否将审核数据发送到 Unicenter NSM（指定为 1 表示发送）。

  默认值：1（发送审核数据）

- **OTHER_TNG_HOST_NAME=\"***name***\"**

  定义要向其发送审核数据的主机。

  默认值：Unicenter NSM 中指定的主机名

- **SUPPORT_TNG_CALENDAR= {1 | 0}**

  指定是否支持 Unicenter NSM 日历（指定为 1 表示支持）。

  默认值：1（支持）

- **TNG_REFRESH_INTERVAL=\"***mm***\"**

  定义刷新间隔（分钟）。 验证您是否还设置了 SUPPORT_TNG_CALENDAR=1。

  默认值：10

- **UNICENTER_MIGRATION={1 | 0}**

  指定是否将 Unicenter Security 数据迁移到 CA Access Control（指定为 1 表示迁移）。

  默认值：1（迁移）

USE_SECURE_COMM={1 | 0}

指定 PUPM 代理和报告代理是否使用安全通讯（指定为 1 表示使用）。

默认值：0（不发送）

如果指定该选项并将其设置为 1，那么您还需要在 NEW_KEY 中指定 SSL 密钥值。

USE_SSL={1 | 0}

指定是否设置 SSL 以进行通讯加密。

默认值：0（不发送）

如果指定该选项并将其设置为 1，那么您还需要指定：

- **CERT_OPTION={1 | 2}**

  指定使用哪个证书选项。

  值：1—生成 CA Access Control 证书；**2**—使用已安装的现有证书。

  默认值：1

- **GENERATE_OPTION={1 | 2}**

  指定如何生成 CA Access Control 证书。 验证您是否还设置了 CERT_OPTION=1。

  值：1—使用默认根证书；**2**—指定根证书。

- **SERVER_PRIV_KEY_PWD=\"***password***\"**

  定义所生成的 CA Access Control 证书的私钥密码。 验证您是否还设置了 CERT_OPTION=1。

- **GEN_ROOT_CERT=\"***file***\"**

  定义根证书文件 (.pem) 的完全限定文件名。 验证您中否设置了 CERT_OPTION=1 和 GENERATE_OPTION=2。

- **GEN_ROOT_PRIVATE=\"***file***\"**

  定义根私钥文件 (.key) 的完全限定文件名。 验证您是否设置了 CERT_OPTION=1 和 GENERATE_OPTION=2。

- **ROOT_PRIV_KEY_PWD=\"***password***\"**

  定义根私钥的密码。 验证您中否设置了 CERT_OPTION=1 和 GENERATE_OPTION=2。

- **EXIST_ROOT_CERT=\"***file***\"**

  定义根证书文件 (.pem) 的完全限定文件名。 验证您是否还设置了 CERT_OPTION=2。

- **EXIST_SERVER_CERT=\"***file***\"**

  定义服务器证书文件 (.pem) 的完全限定文件名。 验证您是否还设置了 CERT_OPTION=2。

- **EXIST_PRIVATE_KEY=\"*file*\"**

  定义服务器私钥文件 (.key) 的完全限定文件名。 验证您是否还设置了 CERT_OPTION=2。

- **EXIST_PRIV_KEY_PWD=\"*password*\"**

  定义服务器私钥的密码。 验证您是否还设置了 CERT_OPTION=2。

USE_SYMT_KEY={1 | 0}

指定是否为通讯设置对称密钥加密。 如果 USE_SSL=0，则该参数设置为 1。

默认值：1

如果指定该选项并将其设置为 1，那么您还需要指定：

- **ENCRYPTION_METHOD={Default | DES | 3DES | 256AES | 192AES | 128AES}**

  指定用于通讯的加密方法。

  默认值：256 AES

- **CHANGE_ENC_KEY={1 | 0}**

  选择是否更改默认的加密密钥（指定为 1 表示是）。

  默认值：1（是）

- **NEW_ENCRYPT_KEY=\"*key*\"**

  在您选择更改默认加密密钥时定义加密密钥。 还要设置 CHANGE_ENC_KEY=1。

示例：使用安装命令设置安装默认值

以下示例设置安装目录、定义 CA Access Control 安装的安装日志文件默认值，然后打开图形安装程序。

```
setup.exe /s /v"INSTALLDIR="C:\Program Files\CA\AccessControl\"
/L*v %SystemRoot%\eACInstall.log"
```

示例：使用安装命令指定加密设置

下列示例使用各种加密设置以静默模式安装 CA Access Control。 在每个示例中，命令还安装 CA Access Control、默认的报告代理和任务指派功能、启用 SSL 和定义安装日志文件的路径和名称：

- 该示例从默认的 CA Access Control 根证书生成服务器证书，并定义服务器私钥的密码：

  ```
  setup.exe /s /v"qn COMMAND=proceed USE_SSL=1 CERT_OPTION=1 GENERATE_OPTION=1
  SERVER_PRIV_KEY_PWD=\"P@ssw0rd\" /l*v C:\AC_silent.log"
  ```

- 该示例从第三方根证书生成服务器证书。 该根私钥受密码保护：

```
setup.exe /s /v"qn COMMAND=proceed USE_SSL=2 CERT_OPTION=1 GENERATE_OPTION=1
GEN_ROOT_CERT=\"C:\Crypto\example.pem\"
GEN_ROOT_PRIVATE=\"C:\Crypto\example.key\" ROOT_PRIV_KEY_PWD=\"P@ssw0rd\"
/l*v C:\AC_silent.log"
```

- 该示例指定 CA Access Control 使用第三方根证书和服务器证书。 服务器私钥受密码保护：

```
setup.exe /s /v"qn COMMAND=proceed USE_SSL=1 CERT_OPTION=2
EXIST_ROOT_CERT=\"C:\Crypto\example.pem\"
EXIST_SERVER_CERT=\"C:\Crypto\server.pem\"
EXIST_PRIVATE_KEY=\"C:\Crypto\server.key\" EXIST_PRIV_KEY_PWD=\"P@ssw0rd\"
/l*v C:\AC_silent.log"
```

更多信息：

通讯加密 (p. 421)

升级 Windows 端点

在您升级端点时，CA Access Control 安装程序会升级 CA Access Control 核心功能以及该端点上已安装的任何功能。 您可以选择在升级 CA Access Control 核心功能之后安装新功能。

注意：可能必须重新启动计算机才能完成升级。 有关升级时哪些 CA Access Control 版本需要重新启动的信息，请参阅*《版本说明》*。

升级端点

1. 使用具有 Windows 管理权限的用户身份（即 Windows 管理员或 Windows Administrators 组成员）登录到 Windows 系统。
2. 关闭 Windows 系统上正在运行的所有应用程序。
3. 将 CA Access Control Endpoint Components for Windows DVD 插入光盘驱动器中。

   如果已启用自动运行，产品资源管理器将自动显示。 否则，请导航至光盘驱动器目录并双击 PRODUCTEXPLORERX86.EXE 文件。
4. 从产品资源管理器的主菜单中，展开“组件”文件夹，选择“CA Access Control for Windows”(*my_architecture*)，然后单击“安装”。

   注意：与计算机的体系结构匹配的安装选项会突出显示，以显示计算机上存在 CA Access Control 的现有安装。

   将出现一个对话框，询问您是否要执行 CA Access Control 的升级。

5. 单击“是”。

   CA Access Control 安装程序开始加载，稍后将显示“简介”屏幕。

6. 按照安装屏幕中的说明进行操作。

   安装程序将升级 CA Access Control。 升级完成后，您需要选择立即重新启动 Windows 还是稍后重新启动。

7. （可选）选择“是”立即重新启动计算机。

   计算机将重新启动并完成升级。

8. （可选）安装其他 CA Access Control 功能，如下所示：

   a. 请依次单击“开始”、“控制面板”、“添加/删除程序”。

   b. 滚动浏览程序列表，然后选择“CA Access Control”并单击“更改”。

      CA Access Control 安装程序开始加载，稍后将显示“程序维护”屏幕。

   c. 选择“修改”并按照安装屏幕上的说明书安装相应功能。

      在安装过程中，安装程序将提示您提供信息。 有关安装这些功能时所需的信息，请参阅安装工作表 (p. 151)。 您可能需要重新启动计算机才能完成安装。

启动和停止 CA Access Control

默认情况下，启动 Windows 时，CA Access Control 服务会自动启动。

停止 CA Access Control

使用 secons 实用程序可停止本地和远程计算机上的 CA Access Control。无需任何特殊的 Windows 权限即可停止 CA Access Control，但是在 CA Access Control 中必须有 ADMIN 或 OPERATOR 属性。

注意：如果 CA Access Control 正在运行，则无法从 Windows 服务管理器中将其停止。 您必须先使用 secons 实用程序停止 CA Access Control，然后才能在 Windows 服务管理器中修改 CA Access Control 服务。

停止 CA Access Control

1. 打开命令提示符窗口，导航到包含 CA Access Control 二进制文件的目录。

   默认情况下，CA Access Control 二进制文件位于 C:\Program Files\CA\AccessControl\\bin。

2. 输入下面的命令：

   `secons -s [hosts | ghosts]`

   -s [*hosts* | *ghosts*]

   在已定义的、以空格分隔的远程主机上关闭 CA Access Control 服务。 如果不指定任何主机，将关闭本地主机上的 CA Access Control。

   您可以输入 ghost 记录的名称来定义一组主机。 如果从远程终端使用此选项，此实用程序会请求进行密码验证。 您还需要具有远程和本地计算机的管理权限，以及对远程主机数据库中的本地计算机的写入权限。

   在您停止本地计算机上的 CA Access Control 时，会出现以下消息：

   `CA Access Control 现已关闭`

   在您停止远程主机上的 CA Access Control 时，CA Access Control 将报告远程主机是否已成功关闭。 即使之前未成功关闭远程主机，系统也会尝试关闭列表中的每个主机。

手动启动 CA Access Control

通常，您通过启动 Windows 来启动 CA Access Control。

如果已停止 CA Access Control，则还可以通过命令提示发布命令来手动重新启动 CA Access Control。

手动启动 CA Access Control

1. 确保以拥有 Windows 管理权限的用户（即 Windows 管理员或 Windows Administrators 组成员）身份登录 Windows 系统。
2. 在命令提示符窗口中，转至包含 CA Access Control 二进制文件的目录（默认情况下为系统目录中的 C:\Program Files\CA\AccessControl\\bin）。
3. 通过输入以下内容启动 CA Access Control：

   ```
   seosd -start
   ```

检查您的安装

如果已成功安装 CA Access Control，则可以发现以下更改：

- 一个新项已添加至 Windows 注册表：

  ```
  HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl
  ```

  当 CA Access Control 正在运行时，CA Access Control 密钥和子密钥受保护，您只能通过 CA Access Control 端点管理 或使用 selang 命令来修改这些密钥。 但是，您不需要使用 CA Access Control 端点管理 或 selang 命令来读取这些密钥和值。
- 重新启动计算机时，将自动启动几项新的 CA Access Control 服务。 这些服务包括始终安装好的 Watchdog、引擎和代理。 根据您在安装过程中选择的选项，可能有其他服务（如任务指派）。 所有 CA Access Control 服务的显示名称均以“CA Access Control”开头。 您可以使用 Windows 服务管理器检查安装了哪些服务，并验证这些服务是否在运行。

显示登录保护屏幕

默认情况下，安装 CA Access Control 后，每次用户以交互方式 (GINA) 登录且 CA Access Control 服务正在运行时，都会显示保护屏幕，通知用户该计算机受 CA Access Control 保护。

初始屏幕将显示四秒钟，然后自动关闭。

要禁用该保护消息，请将 HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\AccessControl\SplashEnable 注册表键的值从 1 更改为 0。

将端点配置为使用高级策略管理

安装高级策略管理服务器组件后，您需要在企业中将每个端点配置为使用高级策略管理。 执行此操作时，需将端点配置为将信息发送到服务器组件并从服务器组件接收信息。

注意：此过程显示了如何配置现有的 CA Access Control 安装来进行高级策略管理。 如果您在端点上安装 CA Access Control 时指定了该信息，则不需要再次配置该端点。

要为高级策略配置端点，请打开一个命令窗口，然后输入以下命令：

```
dmsmgr -config -dhname dhName
```

dhName

定义要与端点配合使用的分发主机 (DH) 名称的列表，以逗号分隔。

示例：DH__@centralhost.org.com

该命令将端点配置为使用高级策略管理，并将其设置为与定义的 DH 配合使用。

注意：有关详细信息，请参阅*《参考指南》*中的 dmsmgr -config 命令。

为报告配置 Windows 端点

安装和配置完 CA Access Control 端点管理 和报告门户之后，您可以通过启用和配置报告代理来配置自己的端点，以将数据发送到分发服务器进行处理。

注意：安装 CA Access Control 时，您可以为报告配置端点。 此步骤说明了如何配置现有端点用于发送报告（如果未在安装时配置该选项）。

为报告配置 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 Access Control。

3. 单击“更改”。

   将显示 CA Access Control 安装向导。

4. 按照向导提示修改 CA Access Control 安装，这样您就可以启用报告代理功能。

注意：启用报告代理之后，您可以修改 CA Access Control 配置设置以更改与性能相关的设置。 有关报告代理配置设置的详细信息，请参阅*《参考指南》*。

为群集环境自定义 CA Access Control

要在群集环境中使用 CA Access Control，必须在群集的每个节点上安装 CA Access Control。 此外还需要为每个节点上的公用资源定义相同的规则集（仲裁磁盘或网络，如果使用网络侦听的话）。

CA Access Control 可以检测出它是否正在群集环境中运行。 如果 CA Access Control 检测出群集拥有自己的网络，而且有仅用于群集内部通讯的单独网络适配器，则将对这些网络适配器禁用网络截获。 对于将集群与企业的其余部分相连的网络接口，网络侦听正常工作。

注意：如果群集将同一网络接口用于群集内部通讯*和*与网络其余部分的通讯，则不会启用该功能。

示例

假设您有两个节点：

- NODE1 有两个 IP 地址：
  - 10.0.0.1 是内部集群网络 IP 地址。
  - 192.168.0.1 是外部网络连接。
- NODE2 也有两个 IP 地址
  - 10.0.0.2 是内部集群网络 IP 地址。
  - 192.168.0.2 是外部网络连接。

  集群本身有一个附加 IP 地址 192.168.0.3。

只要 NODE1 与 NODE2 使用内部集群网络 IP 地址进行通讯，网络侦听就不会阻止它们之间的连接。

如果使用外部网络 IP 地址联系 NODE1 或 NODE2，则网络截获将按照 CA Access Control 规则定义的方式操作。

此外，如果通过群集的 IP 地址 192.168.0.3 联系该群集，则网络截获也会按 CA Access Control 规则定义的方式操作。

卸载方法

您可以使用以下方法从 Windows 端点卸载 CA Access Control：

- 常规卸载－该方法使用图形界面卸载 CA Access Control 并提供交互式反馈。
- 静默卸载－该方法使用命令行卸载 CA Access Control，不提供交互式反馈。

卸载 CA Access Control

确保以拥有 Windows 管理权限的用户（即 Windows 管理员或 Windows Administrators 组成员）身份登录 Windows 系统。

卸载 CA Access Control

1. （可选）关闭 CA Access Control (p. 168)。

   注意：如果未手工执行该操作，安装程序将为您关闭 CA Access Control。

2. 依次选择“开始”、“设置”、“控制面板”。

   将显示 Windows“控制面板”。

3. 双击“添加/删除程序”。-

   将显示“添加/删除”对话框。

4. 从已安装程序的列表中选择“CA Access Control”，然后单击“添加/删除”。

5. 在确认是否要删除 CA Access Control 的消息框中，单击“是”。

6. 卸载完成后，单击“确定”。

7. 重新引导计算机以删除所有的 CA Access Control 组件。

静默卸载 CA Access Control

要卸载 CA Access Control 而不进行交互反馈，您可以使用命令行静默卸载 CA Access Control。 确保以拥有 Windows 管理权限的用户（即 Windows 管理员或 Windows Administrators 组成员）身份登录 Windows 系统。

要静默卸载 CA Access Control r12.5，请输入以下命令：

```
Msiexec.exe /x{822BFADC-E040-4F5C-A00A-B8E558A2D616} /qn insert_params_here
```

<insert_params_here> 变量用于指定希望传递到安装程序的安装设置。例如：以下命令卸载 CA Access Control，并在 c:\ac_uninst.log 中创建一个卸载日志：

```
Msiexec.exe /x{822BFADC-E040-4F5C-A00A-B8E558A2D616} /qn /l*v c:\ac_uninst.log
```

注意：如果未手工执行该操作，安装程序将为您关闭 CA Access Control。

第 8 章： 安装和自定义 UNIX 端点

本章将指导您完成 CA Access Control UNIX 端点的安装过程。 按照本章的说明完成 CA Access Control 的安装后，您的系统将包含一份 CA Access Control 端点软件的副本和一个基础 CA Access Control 数据库。 本章接下来将说明如何启动 CA Access Control 以及如何使用其命令。 以后，您可以通过编辑数据库来定义保护系统的访问规则。

此部分包含以下主题：

开始之前

安装 CA Access Control 之前，您必须确保满足初步要求并且具有所有的必要信息。

操作系统支持和要求

您可以将 CA Access Control 安装在任何一个受支持的 UNIX 操作系统中。

注意：有关详细信息，请参阅*《版本说明》*。

管理终端

您可以使用 CA Access Control 端点管理 和 CA Access Control 企业管理 在一个中心位置管理 CA Access Control 策略，也可以连接至具有 selang 命令行的计算机并在该计算机上直接更新访问规则。

要直接更新计算机的访问规则，您需要在进行管理所使用的终端上拥有写入权限，并对 CA Access Control 数据库中的计算机策略拥有 *admin* 属性。

默认情况下，CA Access Control 安装仅为本地计算机终端设置终端权限。 您可以通过从本地终端禁用此选项，或添加更多可以远程管理的终端来更改终端权限。

要使用用户 *my_user* 向计算机 *my_machine* 添加终端 *my_terminal* 的管理选项，请写入以下 selang 规则：

```
er terminal my_terminal owner(nobody) defaccess(r)
auth terminal my_terminal xuid(my_user) access(all)
```

这些规则允许每个用户登录此终端（常规登录，而非 CA Access Control 管理），并允许企业用户 *my_uid* 登录计算机并使用 CA Access Control 管理工具（selang、CA Access Control 端点管理 等）。

注意：如果管理员使用 CA Access Control 端点管理 管理 CA Access Control，那么您仅需要定义安装 CA Access Control 端点管理 的计算机。您无需定义管理员打开浏览器的计算机。

安装说明

安装 CA Access Control（无论是首次安装还是作为升级的一部分）时，请注意以下方面：

- 阅读*《版本说明》*。

  此文档包含关于所支持平台的信息、已知问题、注意事项以及安装 CA Access Control 之前应阅读的其他重要信息。

- 如果您的环境是使用 PMDB 层级结构设置的，或者您要设置此类环境，建议您：

  - 首先安装或升级部署映射服务器 (DMS) 计算机。

    只有在打算使用基于策略的高级管理，并确保 DMS 注册了每个策略模型节点及其订户时，才需要执行上述操作。

  - 在层级结构中自下而上（首先是订户）安装或升级每台计算机。

    如果升级后的 PMDB 中有使用早期版本的订户，可能会导致发送错误命令。 由于新 PMDB 包含早期版本的 PMDB 中不存在的类和属性，因此可能会发生这种情况。

    注意：可以同时升级在单台计算机上运行的 PMDB 层级结构。

- 请*勿*在 PMDB 或策略更新期间进行升级。
- 备份订户和 PMDB 策略。

注意：早期版本的 PMDB 可以拥有后期版本的订户，反之则不可。由于后期版本支持早期版本中的命令，因此 PMDB 可传播至 CA Access Control r12.0 订户。

- 如果从 r12.0 之前版本进行升级：
  - 应通过 STOP 跳过的程序现在被定义为数据库规则；*stop* 类型的 SPECIALPGM 记录。
  - 应通过 SURROGATE 跳过的程序现在被定义为数据库规则；*surrogate* 类型的 SPECIALPGM 记录。

  注意：升级过程中旧定义（保存在某个文件中）将转换为新数据库规则。 将这些新规则添加到现有 selang 脚本。
- 您可以升级当前的 seos.ini 和 pmd.ini 文件，也可以新建文件。

  无论采用哪种方法，安装脚本都会将旧 seos.ini 文件的副本存储为 seos_ini.back，将每个 pmd.ini 文件的副本存储为 pmd_ini.back（在其各自的策略模型目录中）。
- CA Access Control 在升级过程中将备份以下现有文件：serevu.cfg、audit.cfg、trcfilter.init 和 sereport.cfg。

  如果要保存对上述文件所做的更改，需要使用备份的文件。
- 如果打算升级现有的数据库，建议您：
  - 先备份该数据库。

    使用 dbmgr -b 备份该数据库。
  - 确保没有订户处于*同步*模式。

    使用 sepmd -L 验证订户的状态。
- Unicenter 安全集成和迁移仅适用于 AIX、HP-UX PA-RISC、Solaris SPARC 和 Linux x86 平台。

- Unicenter TNG 和 CA Access Control for UNIX

  如果您安装的 Unicenter TNG 版本早于 Unicenter NSM 3.0，请安装下列 Unicenter TNG 修正以允许 CA Access Control 获取进程信息：

  - 具有 Unicenter TNG 2.4 的 HP-UX 用户，请安装修复程序 QO01182。
  - 具有 Unicenter TNG 2.4 的 Linux 用户，请安装修复程序 PTF LO91335。
  - 具有 Unicenter TNG 2.4 的 Sun 用户，请安装修复程序 QO00890。

  注意：使用运行了 Unicenter NSM 3.0 的 AIX 5.x 的用户，必须与 CA Technologies Unicenter 支持部门联系以获取兼容性修正。 必须首先安装该兼容性修正，然后才能在主机上安装 CA Access Control。

- 如果希望在 Linux s390 上安装 Unicenter 相关选项（install_base 选项：-uni 或 -mfsd），在您安装 CA Access Control 之前，必须安装 korn shell (ksh)。

  CCI Standalone (CCISA) 的安装脚本使用 ksh，而在 Linux 上默认情况下 ksh 不会安装。

- 要在 Linux x86 64 位上安装 CA Access Control 32 位二进制文件，建议您使用 _LINUX_*xxx*.tar.Z 或 CAeAC-*xxxx*-*y*.*y*.*iiii*.i386.rpm 安装程序包。这些安装程序包将 32 位 CA Access Control 二进制文件安装到 Linux x86 64 位系统中。 如果正在升级，那么这些程序包会保持与先前 32 位 CA Access Control 安装的兼容性。 安装 CA Access Control 之前，必须确保已经安装以下操作系统 32 位库。

  ld-linux.so.2、libICE.so.6、libSM.so.6、libX11.so.6、libXext.so.6、libXp.so.6、libXt.so.6、libc.so.6、libcrypt.so.1、libdl.so.2、libgcc_s.so.1、libm.so.6、libncurses.so.5、libnsl.so.1、libpam.so.0、libpthread.so.0、libresolv.so.2、libstdc++.so.5、libaudit.so.0 （仅限 RHEL5 和 OEL 5 及以上）。

  以下列表为所需的相关 RPM 软件包：

  - SLES 10：compat-libstdc++、glibc-32bit、libgcc、ncurses-32bit、pam-32bit、xorg-x11-libs-32bit
  - SLES 9：glibc-32bit、libgcc、libstdc++、ncurses-32bit、pam-32bit、XFree86-libs-32bit
  - RHEL 5 和 OEL 5：audit-libs、compat-libstdc++、glibc、libgcc、libICE、libSM、libXext、libXp、libXt、ncurses、pam
  - RHEL 4 和 OEL 4：compat-libstdc++、glibc、libgcc、ncurses、pam、xorg-x11-deprecated-libs、xorg-x11-libs
  - RHEL 3：glibc、libgcc、libstdc++、ncurses、pam、XFree86-libs

- 要在 Linux x86 64 位上安装 CA Access Control 64 位二进制文件，请使用 _LINUX_X64_*xxx*.tar.Z 或 CAeAC-*xxxx-y.y.iiii*.x86_64.rpm 安装程序包。 如果使用这些安装程序包，则无需安装其他任何 RPM 软件包。

  在将 CA Access Control 64 位二进制文件安装或升级到 Linux x86 64 位系统之前，请注意以下事项：

  - 64 位安装程序包不支持 CA Access Control GUI 实用程序，如 selock 和 selogo。
  - 如果 install_base 脚本可以访问 32 位和 64 位的 tar 文件，那么默认情况下 install_base 脚本将使用 32 位 tar 文件。 要替换此操作，请在运行 install_base 命令时指定所需的 tar 文件。 如果安装 64 位 RPM 软件包，则仅安装 64 位二进制文件和库。 例如：

    ```
    ./install_base_LINUX_X64_125.tar.Z
    ```

  - 被生成并链接到 API 的任何应用程序必须针对 64 位安装进行重新生成。 请使用 LINUX64 目标来生成 64 位 API 示例。 该目标使用 D64BIT 和 -D64BITALL（-m32 已删除）。 需要 -m elf_x86_64 生成库。
  - 如果您使用 install_base 脚本从 32 位安装升级到 64 位 CA Access Control 安装，那么必须在安装之前设置 -force_install 标志。 如果不设置此标志，那么安装将会失败。
  - 要在卸载 CA Access Control 之后完全卸载 cawin，请使用 rpm -e --allmatches 确保卸载进程同时删除 32 位和 64 位版本的 cawin。

- 要在 Linux s390x 64 位上安装 CA Access Control，您必须确定已经安装以下操作系统 32 位库：

  ld.so.1、libcrypt.so.1、libc.so.6、libdl.so.2、libICE.so.6、liblaus.so.1（SLES 8、RHEL 3）、libaudit.so.0（RHEL 4、RHEL 5）、libm.so.6、libnsl.so.1、libpam.so.0、libresolv.so.2、libSM.so.6、libX11.so.6、libXext.so.6、libXp.so.6、libXt.so.6

  以下列表为所需的相关 RPM 软件包：

  - SLES 10：glibc-32bit、pam-32bit、xorg-x11-libs-32bit
  - SLES 9：XFree86-libs-32bit、glibc-32bit、pam-32bit
  - RHEL 5：audit-libs、libXp、glibc、libICE、libSM、libX11、libXext、libXt、pam

  - RHEL 4：audit-libs、glibc、pam、xorg-x11-deprecated-libs、xorg-x11-libs
  - RHEL 3：glibc、laus-libs、pam
- 如果使用 -all 选项在 Linux 和 Linux-IA64 平台上安装 CA Access Control，则不会安装 mfsd。
- 如果您在 Solaris 上安装 CA Access Control，那么请安装 SUNWlibc (Sun Workshop Compilers Bundled libC) 包。
- 在 32 位或 64 位 Linux 计算机中安装 CA Access Control 32 位二进制文件之前，必须确保已经安装 libstdc++.so.5 32 位库。 如果没有安装此库，ReportAgent 后台进程将在安装 CA Access Control 后不启动。
- 在 Linux 上安装 CA Access Control 之前，请在环境中指定主目录。

Linux s390 端点的安装注意事项

如果要使用消息队列功能远程管理 CA Access Control Linux s390 上的 UNAB，并在 Linux IA64 上使用报告功能，请在端点上安装 J2SE 版本 5.0 或更高版本。

消息队列功能允许您将来自 CA Access Control 端点的报告和审核数据分别发送至报告门户和 CA Enterprise Log Manager。 通过远程管理，您可以使用 CA Access Control 企业管理 管理 UNAB 端点。

您可以在端点上安装 CA Access Control 或 UNAB 之前或之后安装 J2SE。 如果在安装 CA Access Control 或 UNAB 之后安装 J2SE，您还必须在端点上配置 Java 位置。

安装程序如何与 Java 进行交互

在 Linux s390、Linux s390x 和 Linux IA64 上有效

要使用消息队列功能远程管理 UNAB Linux s390 端点，并在 Linux IA64 和 Linux s390 上使用报告功能，请在端点上安装受支持的 Java 版本。

在 Linux s390 或 Linux IA64 端点上安装 CA Access Control 或 UNAB 时，安装程序会执行以下操作：

1. 按顺序检查下列位置是否存在有效 Java 环境的路径：
   a. 安装输入内容中的 JAVA_HOME 参数。

      安装输入内容包括 UNAB 安装参数文件、UNIX CA Access Control 安装参数文件、用于本地安装的自定义程序包以及来自交互式 CA Access Control 安装的用户输入内容。

   b. JAVA_HOME 环境变量。

   c. （Linux s390 和 Linux s390x）默认安装路径为：/opt/ibm/java2-s390-50/jre
2. 将 accommon.ini 文件的全局设置中的 java_home 配置设置的值设为下列值之一：
   - 如果安装程序找到有效 Java 环境的路径，会将配置设置的值设为此路径。
   - 如果安装程序未找到有效 Java 环境的路径，会将配置设置的值设为 *ACSharedDir*/JavaStubs。

     默认情况下，*ACSharedDir* 为 /opt/CA/AccessControlShared。

在 Linux s390 和 Linux s390x 端点上配置 Java 位置

在 Linux s390 和 Linux s390x 上有效

要使用消息队列功能并远程管理 UNAB Linux s390 端点，您必须在端点上安装 J2SE 版本 5.0 或更高版本。 如果在安装 CA Access Control 或 UNAB 之后安装 J2SE，您必须执行附加的配置步骤。

在 Linux s390 和 Linux s390x 端点上配置 Java 位置

1. 停止 CA Access Control 和 UNAB（如果它们正在运行）。
2. 将 accommon.ini 文件的全局部分中的 java_home 配置设置的值更改为 Java 安装的路径：

   例如：java_home=/opt/ibm/java2-s390-50/jre
3. 启动 CA Access Control 和 UNAB。

   Java 位置即配置完毕。

本地安装

CA Access Control 提供本地程序包格式，以在支持的操作系统中对 CA Access Control 进行本地安装和管理。 通过本地程序包，您可以使用其中的管理工具来管理 CA Access Control 安装。

本地程序包

CA Access Control 为每个支持的本地安装格式提供本地程序包。 通过这些程序包，您可以使用本地程序包功能来管理 CA Access Control 组件的安装、更新和删除。 本地程序包位于 CA Access Control Endpoint Components for UNIX DVD 的 NativePackages 目录下。

下面列出了这些软件包及其说明：

ca-lic

（仅适用于 Linux）安装 CA Technologies 许可程序，该许可程序是安装所有其他程序包的先决条件。

注意：对于 Linux 仅以 RPM 格式提供。

CAeAC

安装 CA Access Control 核心组件。这是 CA Access Control 主安装程序包，它包括服务器、客户端、文档、TNG 集成、API 和 mfsd 程序包，这些内容以前都是单独打包。

注意：UNAB 软件包也安装 CAWIN 共享组件。

您需要了解程序包的名称才能执行某些本地命令（例如使用 RPM 删除程序包）。 要确定使用程序包文件的程序包的名称，请输入相应的本地程序包命令。 例如：对于 RPM 软件包，请输入：

```
rpm -q -p RPMPackage_filename
```

本地安装的其他注意事项

使用本地程序包安装 CA Access Control 时，请注意以下其他注意事项：

- 要安装 CA Access Control RPM 程序包，您必须拥有许可程序包 ca-lic-01.0080 或更高版本
- 要构建自定义 CA Access Control RPM 本地安装包（customize_eac_rpm），在您的计算机上必须具有 rpmbuild 实用程序。

- 要构建自定义 CA Access Control AIX 本地安装程序包 (customize_eac_bff)，您的计算机中必须安装有 bos.adt.insttools。

  针对 AIX 5.2，bos.adt.insttools 的版本应为 5.2.0.75 或更新。

- AIX 本地软件包与 bos.rte.install 5.2.0.75 一起建立。 因此我们建议您使用 bos.rte.install 5.2.0.75 或更高版本，以与本地程序包一起运行而不发生错误。
- HP-UX 本地软件包在安装过程中使用 Perl。
- Solaris 本地程序包必须位于对组和全局具有读取权限的公共位置，例如：/var/spool/pkg。
- 对于 CA Access Control 程序包，Solaris 本地程序包命令 pkgadd -R 不受支持。

  使用 CA Access Control 程序包自定义脚本修改安装目录 (customize_eac_pkg -i *install_loc*)。

- 要安装本地化版本的 HP-UX 本地程序包，您*必须*在用于自定义程序包的参数文件中设定 LANG 设置的值。

  注意：参数文件中已包含 LANG 设置。 要设定该设置，请删除前面的注释字符 (#) 和空格，然后输入一个值。 您可以使用 locale -a 命令找到操作系统支持的编码值。

如何指定 CA Access Control 使用受密码保护的根证书

在安装 CA Access Control 时，您可以对其进行配置以使用第三方受密码保护的根证书。

在安装 CA Access Control 之后，您可以使用该根证书创建 CA Access Control 服务器证书。 服务器证书用于对 CA Access Control 组件之间的通讯进行加密和验证。

要配置 CA Access Control 以使用第三方受密码保护的根证书，您必须在使用本地程序包安装 CA Access Control 时执行如下所示的一些附加步骤：

1. 在本地程序包安装过程中自定义 params 文件时，在文件中指定以下参数：
   - ENCRYPTION_METHOD_SET=2
   - ROOT_CERT_PATH=*root_cert_path*
   - ROOT_CERT_KEY=*root_key_path*

2. 安装 CA Access Control 之后，执行以下操作：

   a. 按如下所示使用根证书创建 CA Access Control 服务器证书，其中 *ACInstallDir* 是安装 CA Access Control 的目录：

   ```
   ACInstallDir/bin/sechkey -e -sub -in
   /opt/CA/AccessControl/crypto/sub_cert_info -priv root_key_path -capwd
   password [-subpwd password]
   ```

   -priv *root_key_path*

   指定用于保留根证书私钥的文件。

   -ca *password*

   指定根证书私钥的密码。

   -subpwd *password*

   为服务器证书的私钥指定密码。

   b. 如果为服务器密钥指定了密码，验证 CA Access Control 是否可以使用存储的密码打开该密钥：

   ```
   ACInstallDir/bin/sechkey -g -verify
   ```

   c. 将 crypto 部分中的 communication_mode 配置设置值更改为下列值之一：

   all_modes

   如果要同时启用对称和 SSL 加密，请指定此值。 此值允许计算机与所有 CA Access Control 组件进行通讯。

   use_ssl

   指定此值将仅启用 SSL 加密。 此值允许计算机仅与使用 SSL 加密的 CA Access Control 组件进行通讯。

   d. 启动 CA Access Control。

   CA Access Control 将启动并使用 CA Access Control 服务器证书加密和验证通讯。

注意：有关 sechkey 实用程序的详细信息，请参阅 *《参考指南》*。

如何指定 CA Access Control 使用第三方受密码保护的服务器证书

您可以使用第三方受密码保护的服务器证书对 CA Access Control 组件之间的通讯进行加密和验证。

要配置 CA Access Control 以使用第三方受密码保护的服务器证书，您必须在使用本地程序包安装 CA Access Control 时执行如下所示的一些附加步骤：

1. 在本地程序包安装过程中自定义 params 文件时，在文件中指定以下参数：
   - ENCRYPTION_METHOD_SET=2
   - ROOT_CERT_PATH=*root_cert_path*
   - ROOT_CERT_KEY=*root_key_path*
   - PROVIDE_OR_GEN_CERT=2
   - SUBJECT_CERT_PATH=*server_cert_path*
   - SUBJECT_KEY_PATH=*subject_key_path*
2. 安装 CA Access Control 之后，执行以下操作：
   a. 按如下所示将私钥的密码存储在计算机上，其中 *ACInstallDir* 是安装 CA Access Control 的目录：

      ACInstallDir/bin/sechkey -g -subpwd *password*

      -subpwd *password*

      为服务器证书的私钥指定密码。

   b. 验证 CA Access Control 是否可以使用存储的密码打开该密钥：

      ACInstallDir/bin/sechkey -g -verify

   c. 将 crypto 部分中的 communication_mode 配置设置值更改为下列值之一：

      all_modes

      如果要同时启用对称和 SSL 加密，请指定此值。 此值允许计算机与所有 CA Access Control 组件进行通讯。

      use_ssl

      指定此值将仅启用 SSL 加密。 此值允许计算机仅与使用 SSL 加密的 CA Access Control 组件进行通讯。

   d. 启动 CA Access Control。

      CA Access Control 将启动并使用第三方受密码保护的服务器证书加密和验证通讯。

注意：有关 sechkey 实用程序的详细信息，请参阅*《参考指南》*。

RPM 软件包管理器的安装

RPM 软件包管理器 (RPM) 是命令行实用程序，可用于构建、安装、查询、验证、更新和删除各个软件程序包。 该系统设计用于 UNIX 平台。

注意：有关详细信息，请参阅 RPM 软件包管理器网站 http://www.rpm.org 以及有关 RPM 的 UNIX 手册页。

除了常规安装外，您还可以使用 CA Access Control 提供的 RPM 软件包。这样您可以一起管理 CA Access Control 安装和使用 RPM 执行的所有其他软件安装。

从 RPM 数据库中删除现有的 RPM 软件包

如果您已安装了自己创建的 CA Access Control RPM 软件包，则必须将其从 RPM 数据库中删除，以便该数据库反映您安装了哪些程序包。 如果未删除现有程序包并安装了新的程序包，RPM 数据库将显示安装了旧程序包和新程序包，而在您的系统文件中，较新程序包中的文件会覆盖现有文件。 对于要升级程序包的 RPM，其名称必须与当前安装的程序包相同。

注意：删除程序包不会删除任何 CA Access Control 文件，并且本地程序包安装将执行升级。

要从 RPM 数据库中删除程序包，请使用以下命令：

```
rpm -e --justdb your_ACPackageName
```

自定义 CA Access Control RPM 软件包

在使用本地程序包安装 CA Access Control 之前，您必须自定义 CA Access Control 程序包，以指定您接受许可协议。 在自定义程序包时，您还可以指定自定义安装设置。

自定义程序包的方法是：从程序包中提取安装参数文件，根据需要进行修改，然后将其加载回程序包中。 某些命令由自定义脚本提供，因此您不必修改参数文件。

注意：建议您*不要*手动修改程序包。 您应当按照以下步骤中的说明，使用脚本自定义 CA Access Control 程序包。

您可以在 CA Access Control Endpoint Components for UNIX DVD 的 NativePackages/RPMPackages 目录中找到适用于每个受支持的 Linux 操作系统的 RPM 软件包。

自定义 CA Access Control RPM 软件包

1. 将要自定义的程序包复制到文件系统上的临时位置。

   OS 是操作系统的相应子目录的名称。

   在文件系统上的读取/写入位置上，可以根据需要自定义程序包。

2. 将 customize_eac_rpm 脚本文件和 pre.tar 文件复制到文件系统上的临时位置。

   pre.tar 文件是 tar 压缩文件，包含安装消息和 CA Access Control 许可协议。

   注意：您可以在本地程序包所在的同一位置中找到 customize_eac_rpm 脚本文件和 pre.tar 文件。

3. 显示许可协议：

   ```
   customize_eac_rpm -a [-d pkg_location] pkg_filename
   ```

4. 记录许可协议结尾处方括号中出现的关键字。

   您需要在下一步中指定该关键字。

5. 自定义 CA Access Control 程序包以指定您接受许可协议：

   ```
   customize_eac_rpm -w keyword [-d pkg_location] pkg_filename
   ```

6. （可选）设置安装参数文件的语言：

   ```
   customize_eac_rpm -r -l lang [-d pkg_location] pkg_filename
   ```

7. （可选）从 eTrust Access Control r8 SP1 程序包升级：

   ```
   customize_eac_rpm -u install_prefix [-d pkg_location] pkg_filename
   ```

8. （可选）更改默认的加密文件：

   ```
   customize_eac_rpm -s -c certfile -k keyfile [-d pkg_location] pkg_filename
   ```

9. （可选）获取安装参数文件：

   ```
   customize_eac_rpm -g -f tmp_params [-d pkg_location] pkg_filename
   ```

10. （可选）编辑安装参数文件以适合您的安装要求。

    通过该文件，您可以设置程序包的安装默认值。 例如：激活 POSTEXIT 设置（删除前面的 # 字符）并将其指向要运行的安装后脚本文件。

11. （可选）设置自定义程序包中的安装参数：

    ```
    customize_eac_rpm -s -f tmp_params [-d pkg_location] pkg_filename
    ```

    您现在可以使用程序包通过自定义默认值来安装 CA Access Control。

示例：指定您接受许可协议

要在安装本地程序包时接受许可协议，您需要自定义该程序包。 以下示例显示了如何自定义可在 CA Access Control Endpoint Components for UNIX DVD（挂接到 /mnt/AC_DVD）中找到的 x86 CA Access Control RPM 软件包，以便您接受许可协议：

```
cp /mnt/AC_DVD/NativePackages/RPMPackages/LINUX/CAeAC*i386.rpm /tmp
cp /mnt/AC_DVD/NativePackages/RPMPackages/pre.tar /tmp
chmod 777 /tmp/CAeAC*i386.rpm
/mnt/AC_DVD/NativePackages/RPMPackages/customize_eac_rpm -w keyword -d /tmp
CAeAC*i386.rpm
```

您现在将可以使用 /tmp 目录中的自定义程序包安装 CA Access Control。

更多信息：

customize_eac_rpm 命令—自定义 RPM 软件包 (p. 191)

安装 CA Access Control RPM 软件包

要一起管理 CA Access Control 安装和所有其他软件安装，请安装自定义的 CA Access Control RPM 软件包。

重要说明！ 您必须自定义程序包，以使用可在许可协议中找到的关键字指定自己接受该许可协议。

注意：您使用的实际命令会因多种变量而异，包括您是否首次进行升级或安装，或是否要安装到默认目录。 本主题提供了一些命令示例。

安装 CA Access Control RPM 软件包

1. 使用 rpm 命令安装 ca-lic 程序包。

   将安装许可程序。

2. 自定义 CAeAC 程序包 (p. 186)。

   您必须自定义程序包，以使用可在许可协议中找到的关键字指定自己接受该许可协议。 您也可以自定义程序包以指定自定义安装设置。

   注意：如果您要升级 CA Access Control，则不需要自定义程序包来指定您接受许可协议。

3. 使用 rpm 命令安装 CAeAC 程序包。

   将安装 CA Access Control。

   注意：UNAB 软件包也安装 CAWIN 共享组件。

   重要说明！ 如果要升级现有 CA Access Control 程序包，请先卸载 SEOS syscall，然后再尝试安装新程序包。 否则，该安装会失败。

示例：在 Red Hat Linux 中安装或升级 CA Access Control

以下示例显示了如何在 Red Hat Linux x86 ES 4.0 计算机上安装 CA Access Control 程序包，该程序包位于 CA Access Control Endpoint Components for UNIX DVD 中（挂接到 /mnt/AC_DVD）。 这可以对 CA Access Control 进行全新安装，或者对当前已安装的 CA Access Control RPM 软件包进行升级（无需先删除已安装的程序包）。 要执行此操作，您安装许可程序包，然后自定义 CA Access Control 软件包，接受许可协议并安装如下：

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX
rpm -U ca-lic*i386.rpm ca-cs-cawin*i386.rpm
cp CAeAC*i386.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*i386.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*i386.rpm
rpm -U /tmp/CAeAC*i386.rpm
```

示例：从 eTrust Access Control r8 SP1 程序包安装升级

以下示例将向您展示如何将 eTrust Access Control r8 SP1 程序包（安装在 /opt/CA/eTrustAccessControl）升级为 CA Access Control 程序包，您可以在 Linux s390 SLES 9 计算机上的 CA Access Control Endpoint Components for UNIX DVD（挂接到 /mnt/AC_DVD）上找到该程序包。 要执行此操作，请使用以下命令安装许可程序包、CAWIN 程序包以及自定义的 CA Access Control 程序包（按此顺序）：

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX390
rpm -U ca-lic*rpm ca-cs-cawin*rpm
cp -R CAeAC*s390.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*s390.rpm
../customize_eac_rpm -u /opt/CA  -d /tmp CAeAC*s390.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*s390.rpm
rpm -U /tmp/CAeAC*s390.rpm
```

示例：将 CA Access Control 和必备程序包安装到自定义目录

以下示例显示了如何将默认的 CA Access Control 和必备程序包（位于 CA Access Control Endpoint Components for UNIX DVD（挂接到 /mnt/AC_DVD）中）安装到 Red Hat Linux Itanium IA64 ES 4.0 上的自定义目录中。 要执行此操作，请使用以下命令：

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX_IA64
rpm -U --prefix /usr/CA/shared ca-lic*ia64.rpm
cp -R CAeAC*ia64.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*ia64.rpm
../customize_eac_rpm -u /usr/CA  -d /tmp CAeAC*ia64.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*ia64.rpm
rpm -U --prefix /usr/CA /tmp/CAeAC*ia64.rpm
```

CA Access Control 安装在自定义目录 /usr/CA/AccessControl 中，该路径由您所提供的自定义目录和产品名称 (Access Control) 组成。

注意：仅当未在环境中定义 $CASHCOMP 变量（可在 /etc/profile.CA 中定义）时，许可程序才会安装到指定目录中。 否则，许可程序将安装到 $CASHCOMP。 如果未定义 $CASHCOMP 且未指定 -lic_dir，则许可程序将会安装到 /opt/CA/SharedComponents 目录中。

更多信息：

本地安装的其他注意事项 (p. 182)
自定义 CA Access Control RPM 软件包 (p. 186)
customize_eac_rpm 命令—自定义 RPM 软件包 (p. 191)

customize_eac_rpm 命令－自定义 RPM 软件包

customize_eac_rpm 命令运行 CA Access Control RPM 软件包自定义脚本。

使用此命令时应考虑以下内容：

- 该脚本仅适用于 CA Access Control RPM 软件包。

  注意：该脚本不希望与许可程序包一起使用。

- 要自定义程序包，程序包必须位于您文件系统上的读取/写入目录。

此命令格式如下：

```
customize_eac_rpm -h [-l]
customize_eac_rpm -a [-d pkg_location] pkg_filename
customize_eac_rpm -w keyword [-d pkg_location] pkg_filename
customize_eac_rpm -r [-d pkg_location] [-l lang] pkg_filename
customize_eac_rpm -s [-f tmp_params] | -c certfile | -k keyfile} [-d pkg_location]
pkg_filename
customize_eac_rpm -g [-f tmp_params] [-d pkg_location] pkg_filename
customize_eac_rpm -u install_prefix [-d pkg_location] pkg_filename
customize_eac_rpm -t tmp_dir [-d pkg_location] pkg_filename
```

pkg_filename

定义您要自定义的 CA Access Control 程序包的文件名称。

注意：如果您未指定 -d 选项，则必须定义程序包文件的完整路径名。

-a

显示许可协议。

-c *certfile*

定义根证书文件的完整路径名。

注意：该选项仅适用于 CAeAC 程序包。

-d *pkg_location*

（可选）指定文件系统上程序包所在目录。 如果您未指定程序包所在的目录，则脚本将假设程序包文件的完整路径名为 *pkg_filename*。

-f *tmp_params*

指定要创建的或要从中检索信息的安装参数文件的完整路径和名称。

注意：如果您使用 -g 选项时未指定文件，则安装参数将使用标准输出 (stdout)。

--g

获取安装参数文件并将其置于由 -f 选项指定的文件中。

-h

显示命令用法。 与 -l 选项联合使用时，可显示受支持语言的语言代码。

-k *keyfile*

定义根私钥文件的完整路径名。

注意：该选项仅适用于 CAeAC 程序包。

-l *lang*

将安装参数文件的语言设置为 *lang*。您只能与 -r 选项一起设置语言。

注意：有关可以指定的受支持语言代码的列表，请使用 -h 选项运行 -l。 默认情况下，安装参数文件使用英语。

--r

重置程序包，以使用原始程序包中的默认值。

-s

将指定程序包设置为通过自定义安装参数文件（由 -f 选项指定）的输入。

-t *tmp_dir*

设置安装操作的临时目录。

注意：默认的临时目录是 /tmp。

-u *install_prefix*

为 eTrust Access Control r8 SP1 程序包安装所在的位置定义前缀。 实际安装位置是此前缀加产品名。 r8 SP1 程序包的产品名称中有 eTrust，因此，该程序包安装在 eTrustAccessControl 子目录中。 更新版本将安装在 AccessControl 子目录中。

例如：如果已将 r8 SP1 安装在 /opt/CA/eTrustAccessControl 且正要升级到 r12.0 SP1，则请在使用 rpm 命令安装程序包之前输入以下命令：

```
./customize_eac_rpm -u /opt/CA  -d . CAeAC-1200-0.1106.i386.rpm
```

-w 关键字

定义用于指定您接受许可协议的关键字。 您可以在许可协议的结尾处找到此关键字（在方括号内）。要找到许可协议文件，请使用 -a 选项。

卸载 RPM 程序包

要卸载安装的 CA Access Control RPM 软件包，您需要按照与安装过程相反的顺序来卸载 CA Access Control 程序包。

要卸载 RPM 程序包，请运行以下命令：

```
rpm -e CAeACPackage_name
```

Solaris 本地程序包安装

Solaris 本地程序包以命令行实用程序的形式提供，用于创建、安装、删除各个软件程序包和对其进行报告。

注意：有关 Solaris 本地程序包的详细信息，请参阅 Sun Microsystems 网站和有关 pkgadd、pkgrm、pkginfo 和 pkgchk 的手册页。

除了常规安装外，您还可以使用 CA Access Control 提供的 Solaris 本地程序包。 这样您可以一起管理 CA Access Control 安装和使用 Solaris 本地程序包执行的所有其他软件安装。

重要说明！ 程序包安装后，如果要卸载 CA Access Control，则必须使用 *pkgrm* 命令。 请勿使用 uninstall_AC 脚本。

自定义 Solaris 本地程序包

在使用本地程序包安装 CA Access Control 之前，您必须自定义 CA Access Control 程序包，以指定您接受许可协议。 在自定义程序包时，您还可以指定自定义安装设置。

自定义程序包的方法是：从程序包中提取安装参数文件，根据需要进行修改，然后将其加载回程序包中。 某些命令由自定义脚本提供，因此您不必修改参数文件。

注意：建议您不要手动修改程序包。 您应当按照以下步骤中的说明，使用脚本自定义 CA Access Control 程序包。

您可以在 CA Access Control Endpoint Components for UNIX DVD 的 NativePackages 目录中找到适用于每个受支持的 Solaris 操作系统的 Solaris 本地程序包。

自定义 Solaris 本地程序包

1. 将要自定义的程序包提取到文件系统上的临时位置。

   在文件系统的读取/写入位置上，可以根据需要自定义程序包。

   重要说明！ 当提取程序包时，需验证是否保留了程序包整个目录结构的文件属性，否则 Solaris 本地程序包工具会认为该程序包已损坏。

2. 将 customize_eac_pkg 脚本文件和 pre.tar 文件复制到文件系统上的临时位置。

   pre.tar 文件是 tar 压缩文件，包含安装消息和 CA Access Control 许可协议。

   注意：您可以在本地程序包所在的同一位置中找到 customize_eac_pkg 脚本文件和 pre.tar 文件。

3. 显示许可协议：

   ```
   customize_eac_pkg -a [-d pkg_location] pkg_name
   ```

4. 记录许可协议结尾处方括号中出现的关键字。

   您需要在下一步中指定该关键字。

5. 自定义 CA Access Control 程序包以指定您接受许可协议：

   ```
   customize_eac_pkg -w keyword [-d pkg_location] [pkg_name]
   ```

6. （可选）设置安装参数文件的语言：

   ```
   customize_eac_pkg -r -l lang [-d pkg_location] [pkg_name]
   ```

7. （可选）更改安装目录：

   ```
   customize_eac_pkg -i install_loc [-d pkg_location] [pkg_name]
   ```

8. （可选）更改默认的加密文件：

   ```
   customize_eac_pkg -s -c certfile -k keyfile [-d pkg_location] [pkg_name]
   ```

9. （可选）获取安装参数文件：

   ```
   customize_eac_pkg -g -f tmp_params [-d pkg_location] [pkg_name]
   ```

10. （可选）编辑安装参数文件以适合您的安装要求。

    通过该文件，您可以设置程序包的安装默认值。 例如：激活 POSTEXIT 设置（删除前面的 # 字符）并将其指向要运行的安装后脚本文件。

11. （可选）设置自定义程序包中的安装参数：

    ```
    customize_eac_pkg -s -f tmp_params [-d pkg_location] [pkg_name]
    ```

    您现在可以使用程序包通过自定义默认值来安装 CA Access Control。

示例：指定您接受许可协议

要在安装本地程序包时接受许可协议，您需要自定义该程序包。 以下示例显示了如何自定义可在 CA Access Control Endpoint Components for UNIX DVD（挂接到 /mnt/AC_DVD）中找到的 x86 CA Access Control Solaris 程序包，以便您接受许可协议：

```
cp /mnt/AC_DVD/NativePackages/_SOLARIS_X86_PKG*.tar.Z /tmp
cp /mnt/AC_DVD/NativePackages/pre.tar /tmp
cd /tmp
zcat _SOLARIS_X86_PKG*.tar.Z | tar -xvf -
/mnt/AC_DVD/NativePackages/customize_eac_pkg -w keyword -d /tmp CAeAC
```

您现在将可以使用 /tmp 目录中的自定义程序包安装 CA Access Control。

更多信息：

customize_eac_pkg 命令—自定义 Solaris 本地程序包 (p. 198)

安装 Solaris 本地程序包

要一起管理 CA Access Control 安装和所有其他软件安装，请安装自定义的 CA Access Control Solaris 本地程序包。 通过 CA Access Control Solaris 本地程序包，您可以在 Solaris 中轻松地安装 CA Access Control。

重要说明！ 您必须自定义程序包，以使用可在许可协议中找到的关键字指定自己接受该许可协议。

安装 CA Access Control Solaris 本地程序包

1. （可选）配置 Solaris 本地安装默认值：

   a. 将安装管理文件复制到当前位置：

      ```
      convert_eac_pkg -p
      ```

      将安装管理文件复制当前位置并命名为 *myadmin*。

      可以编辑安装管理文件以更改 pkgadd 安装默认值。 然后您可以使用修改过的文件进行特定安装，如使用 pkgadd -a 选项安装 CA Access Control。 但是，此文件不特定于 CA Access Control。

      重要说明！ 必须执行该步骤将现有的 Solaris 程序包安装从较旧的 CA Access Control 版本升级。

   b. 根据需要编辑安装管理文件 (myadmin)，然后保存该文件。

      现在您可以将已修改的安装设置用于 CA Access Control 本地安装而不会影响其他安装。

   注意：默认情况下，Solaris 本地程序包可能需要用户参与。 有关安装管理文件及其使用方法的详细信息，请参阅有关 pkgadd(1M) 和 admin(4) 的 Solaris 手册页。

2. 自定义 CAeAC 程序包 (p. 193)。

   您必须自定义程序包，以使用可在许可协议中找到的关键字指定自己接受该许可协议。 您也可以自定义程序包以指定自定义安装设置。

3. 安装程序包：

   ```
   pkgadd [-a dir/myadmin] -d pkg_location CAeAC
   ```

   -a *dir*/myadmin

      定义您在步骤 1 中创建的 myadmin 安装管理文件的位置。

      如果未指定此选项，pkgadd 将使用默认的安装管理文件。

   pkg_location

      定义 CA Access Control 程序包 (CAeAC) 所在的目录。

      重要说明！ 程序包必须位于公共位置（即对组和全局而言有读取权限）。 例如：/var/spool/pkg

注意：您可以在 CA Access Control Endpoint Components for UNIX DVD 的 NativePackages 目录中找到 Solaris 本地程序包。

CA Access Control 现已完全安装，但还未启动。

更多信息：

本地安装的其他注意事项 (p. 182)
将 Solaris 本地程序包安装到选定区域 (p. 197)
自定义 Solaris 本地程序包 (p. 193)
customize_eac_pkg 命令－自定义 Solaris 本地程序包 (p. 198)
convert_eac_pkg－配置 Solaris 本地安装 (p. 200)

将 Solaris 本地程序包安装到选定区域

您可以使用 Solaris 本地程序包将 CA Access Control 安装到选定区域。 但是，您也必须将 CA Access Control 安装在全局区域上。

注意：我们建议您使用 Solaris 本地软件包将 CA Access Control 安装到*所有*区域。

将 CA Access Control 安装到选定区域

重要说明！ 请确保您在所有区域中都使用同一 CA Access Control 版本。

1. 从全局区域发布安装 CA Access Control 的命令。

   ```
   pkgadd -G -d pkg_location CAeAC
   ```

   pkg_location

   定义自定义的 CA Access Control 程序包 (CAeAC) 所在的目录。

   重要说明！ 程序包必须位于公共位置（即对组和全局而言有读取权限）。 例如：/var/spool/pkg

   该命令仅将 CA Access Control 安装到全局区域。

2. 在全局区域中，输入 SEOS_load 命令以加载 CA Access Control 内核模块。

   注意：CA Access Control 内核会加载，但是 CA Access Control 不会拦截全局区域中的事件。

3. 在每个要安装 CA Access Control 的非全局区域中：

   a. 将 CAeAC 程序包复制到非全局区域的临时位置。

   b. 从非全局区域发布以下命令：

      ```
      pkgadd -G -d pkg_location CAeAC
      ```

      该命令将 CA Access Control（使用您在上一步骤中复制的程序包）安装到您工作所在的非全局区域。

   现在您可以在内部区域启动 CA Access Control。

注意：必须从所有非全局区域都进行卸载后，才能从全局区域删除 CA Access Control。

customize_eac_pkg 命令 — 自定义 Solaris 本地程序包

customize_eac_pkg 命令运行 CA Access Control Solaris 本地程序包自定义脚本。

使用此命令时应考虑以下内容：

- 该脚本适用于所有可用的 CA Access Control Solaris 本地程序包。
- 要自定义程序包，程序包必须位于您文件系统上的读取/写入目录。
- 要获得本地化的脚本消息，您需要将 pre.tar 文件与脚本文件置于同一目录中。

此命令格式如下：

```
customize_eac_pkg -h [-l]
customize_eac_pkg -a [-d pkg_location] [pkg_name]
customize_eac_pkg -w keyword [-d pkg_location] [pkg_name]
customize_eac_pkg -r [-d pkg_location] [-l lang] [pkg_name]
customize_eac_pkg -i install_loc [-d pkg_location] [pkg_name]
customize_eac_pkg -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
[pkg_name]
customize_eac_pkg -g [-f tmp_params] [-d pkg_location] [pkg_name]
customize_eac_pkg -t tmp_dir [-d pkg_location] [pkg_name]
```

pkg_name

（可选）您要自定义的 CA Access Control 程序包的名称。如果您未指定程序包，脚本将默认使用 CA Access Control 主程序包 (CAeAC)。

-a

显示许可协议。

-c *certfile*

定义根证书文件的完整路径名。

注意：该选项仅适用于 CAeAC 程序包。

-d *pkg_location*

（可选）指定文件系统上程序包所在目录。 如果您未指定程序包所在目录，脚本将默认使用 /var/spool/pkg。

-f *tmp_params*

指定要创建的或要从中检索信息的安装参数文件的完整路径和名称。

注意：如果您使用 -g 选项时未指定文件，则安装参数将使用标准输出 (stdout)。

--g

获取安装参数文件并将其置于由 -f 选项指定的文件中。

-h

显示命令用法。 与 -l 选项联合使用时，可显示受支持语言的语言代码。

-i *install_loc*

将程序包的安装目录设置为 *install_loc*/AccessControl。

-k *keyfile*

定义根私钥文件的完整路径名。

注意：该选项仅适用于 CAeAC 程序包。

-l *lang*

将安装参数文件的语言设置为 *lang*。您只能与 -r 选项一起设置语言。

注意：有关可以指定的受支持语言代码的列表，请使用 -h 选项运行 -l。 默认情况下，安装参数文件使用英语。

--r

重置程序包，以使用原始程序包中的默认值。

-s

将指定程序包设置为通过自定义安装参数文件（由 -f 选项指定）的输入。

-t *tmp_dir*

设置安装操作的临时目录。

注意：默认的临时目录是 /tmp。

-w 关键字

定义用于指定您接受许可协议的关键字。 您可以在许可协议的结尾处找到此关键字（在方括号内）。要找到许可协议文件，请使用 -a 选项。

convert_eac_pkg—配置 Solaris 本地安装

默认的 Solaris pkgadd 行为由安装管理文件确定。 要覆盖默认设置，需要更改安装管理文件（默认情况下为 /var/sadm/install/admin/default）。 例如：CA Access Control 程序包安装 setuid 可执行文件，另外您也可以通过该程序包运行安装后脚本（将作为 *root* 运行）。 默认的 Solaris pkgadd 行为会提示您确认这些操作。

注意：您可以编辑安装管理文件以更改 pkgadd 安装默认值。 然后您可以使用修改过的文件进行特定安装，如使用 pkgadd -a 选项安装 CA Access Control。 但是，此文件不特定于 CA Access Control。

此命令格式如下：

```
convert_eac_pkg -c [-d pkg_location] [pkg_name]

convert_eac_pkg -p [-f file]
```

-c

将旧格式的程序包转换为新格式。

注意：在 CA Access Control r8 SP1 中使用的是旧格式的程序包。 在升级之前，您需要转换这些旧格式的程序包。

您可以为已安装的 CA Access Control 程序包或后台进程包转换信息。 对于后台进程包，请使用 -d 选项指明该程序包的安装位置。

-d *pkg_location*

定义文件系统上程序包所在的目录

pkg_name

定义程序包的名称（默认情况下为 CAeAC）。

-p

准备已命名的自定义程序包配置文件

-f *file*

定义要创建 CA Access Control 安装管理文件的位置。

如果未指定，则该命令将在当前目录中创建名为 *myadmin* 的文件。

示例：将 Solaris 本地安装配置为静默安装

以下过程显示了如何配置 Solaris 本地安装，以使其不提示您确认是安装 setuid 可执行文件还是运行安装后脚本：

1. 将安装管理文件复制到当前位置：

   ```
   convert_eac_pkg -p
   ```

   这样您可以修改 CA Access Control 本地安装的配置设置而不会影响其他安装。

2. 按如下所示编辑程序包配置文件 (myadmin) 中的以下设置：

   ```
   setuid=nocheck
   action=nocheck
   ```

   保存文件。

3. 自定义程序包。

   您至少需要指定您接受许可协议。

4. 运行以下命令静默安装自定义的 CA Access Control 程序包：

   ```
   pkgadd -n -a config_path\myadmin -d pkg_path CAeAC
   ```

示例：升级使用旧格式的 Solaris 本地安装

以下过程显示了如何在升级为新版本之前转换 CA Access Control 本地程序包安装的现有安装。 要执行此操作，请运行以下命令：

```
convert_eac_pkg -c CAeAC
```

HP-UX 本地程序包安装

HP-UX 本地程序包以一系列 GUI 和命令行实用程序的形式提供，用于创建、安装、删除各个软件程序包和对其进行报告。 通过 HP-UX 本地程序包，还可以在远程计算机上安装软件程序包。

注意：有关 HP-UX 本地程序包及 Software Distributor-UX (SD-UX) 的详细信息，请参阅 HP 网站 http://www.hp.com。 您还可以参阅有关 swreg、swinstall、swpackage 和 swverify 的手册页。

除了常规安装外，您还可以使用 CA Access Control 提供的 SD-UX 本地软件包。 这样您可以一起管理 CA Access Control 安装和使用 SD-UX 执行的所有其他软件安装。

重要说明！ 程序包安装后，如果要卸载 CA Access Control，您必须使用 *swremove* 命令。 请勿使用 uninstall_AC 脚本。

自定义 SD-UX 格式程序包

在使用本地程序包安装 CA Access Control 之前，您必须自定义 CA Access Control 程序包，以指定您接受许可协议。 在自定义程序包时，您还可以指定自定义安装设置。

自定义程序包的方法是：从程序包中提取安装参数文件，根据需要进行修改，然后将其加载回程序包中。 某些命令由自定义脚本提供，因此您不必修改参数文件。

注意：建议您不要手动修改程序包。 您应当按照以下步骤中的说明，使用脚本自定义 CA Access Control 程序包。

您可以在 CA Access Control Endpoint Components for UNIX DVD 的 NativePackages 目录中找到适用于每个受支持的 HP-UX 操作系统的 Software Distributor-UX (SD-UX) 格式程序包。

自定义 SD-UX 格式程序包

1. 将要自定义的程序包提取到文件系统上的临时位置。

   在文件系统上的读取/写入位置上，可以根据需要自定义程序包。

   重要说明！ 在提取程序包时，必须确保程序包整个目录结构的文件属性已保留，否则 HP-UX 本地程序包工具会认为该程序包已损坏。

2. 将 customize_eac_depot 脚本文件和 pre.tar 文件复制到文件系统上的临时位置。

   pre.tar 文件是 tar 压缩文件，包含安装消息和 CA Access Control 许可协议。

   注意：您可以在本地程序包所在的同一位置中找到 customize_eac_depot 脚本文件和 pre.tar 文件。

3. 显示许可协议：

   ```
   customize_eac_depot -a [-d pkg_location] pkg_name
   ```

4. 记录许可协议结尾处方括号中出现的关键字。

   您需要在下一步中指定该关键字。

5. 自定义 CA Access Control 程序包以指定您接受许可协议：

   ```
   customize_eac_depot -w keyword [-d pkg_location] [pkg_name]
   ```

6. （可选）设置安装参数文件的语言：

   ```
   customize_eac_depot -r -l lang [-d pkg_location] [pkg_name]
   ```

7. （可选）更改安装目录：

   ```
   customize_eac_depot -i install_loc [-d pkg_location] [pkg_name]
   ```

8. （可选）更改默认的加密文件：

   ```
   customize_eac_depot -s -c certfile -k keyfile [-d pkg_location] [pkg_name]
   ```

9. （可选）获取安装参数文件：

   ```
   customize_eac_depot -g -f tmp_params [-d pkg_location] [pkg_name]
   ```

10. （可选）编辑安装参数文件以适合您的安装要求。

    通过该文件，您可以设置程序包的安装默认值。 例如：激活 POSTEXIT 设置（删除前面的 # 字符）并将其指向要运行的安装后脚本文件。

11. （可选）设置自定义程序包中的安装参数：

    ```
    customize_eac_depot -s -f tmp_params [-d pkg_location] [pkg_name]
    ```

    您现在可以使用程序包通过自定义默认值来安装 CA Access Control。

示例：指定您接受许可协议

要在安装本地程序包时接受许可协议，您需要自定义该程序包。 以下示例显示了如何自定义可在 CA Access Control Endpoint Components for UNIX DVD（挂接到 /mnt/AC_DVD）中找到的 x86 CA Access Control SD-UX 程序包，以便您接受许可协议：

```
cp /mnt/AC_DVD/NativePackages/_HPUX11_PKG_*.tar.Z /tmp
cp /mnt/AC_DVD/NativePackages/pre.tar /tmp
cd /tmp
zcat _HPUX11_PKG_*.tar.Z | tar -xvf -
/mnt/AC_DVD/NativePackages/customize_eac_depot -w keyword -d /tmp CAeAC
```

您现在将可以使用 /tmp 目录中的自定义程序包安装 CA Access Control。

更多信息：

customize_eac_depot 命令—自定义 SD-UX 格式程序包 (p. 204)

安装 HP-UX 本地程序包

要一起管理 CA Access Control 安装和所有其他软件安装，请安装自定义的 CA Access Control SD-UX 格式程序包。 利用 CA Access Control SD-UX 格式程序包，您可以在 HP-UX 中轻松地安装 CA Access Control。

重要说明！ 您必须自定义程序包，以使用可在许可协议中找到的关键字指定自己接受该许可协议。

要安装 CA Access Control HP-UX 本地软件包

1. 以 root 身份登录。

   要注册并安装 HP-UX 本地程序包，您需要与 root 帐户相关联的权限。

2. 自定义 CAeAC 程序包 (p. 202)。

   您必须自定义程序包，以使用可在许可协议中找到的关键字指定自己接受该许可协议。 您也可以自定义程序包以指定自定义安装设置。

3. 使用以下命令注册通过 SD-UX 自定义程序包：

   ```
   swreg -l depot pkg_location
   ```

   pkg_location

   定义 CA Access Control 程序包 (CAeAC) 所在的目录。

4. 使用以下命令安装 CA Access Control 程序包：

   ```
   swinstall -s pkg_location CAeAC
   ```

   SD-UX 开始从 *pkg_location* 目录安装 CAeAC 软件包。

   CA Access Control 现已完全安装，但还未启动。

更多信息：

本地安装的其他注意事项 (p. 182)
自定义 SD-UX 格式程序包 (p. 202)

customize_eac_depot 命令—自定义 SD-UX 格式程序包

customize_eac_depot 命令对 SD-UX 格式程序包运行 CA Access Control 本地程序包自定义脚本。

使用此命令时应考虑以下内容：

- 该脚本适用于所有可用的 CA Access Control Solaris 本地程序包。
- 要自定义程序包，程序包必须位于您文件系统上的读取/写入目录。
- 要获得本地化的脚本消息，您需要将 pre.tar 文件与脚本文件置于同一目录中。

此命令格式如下：

```
customize_eac_depot -h [-l]
customize_eac_depot -a [-d pkg_location] [pkg_name]
customize_eac_depot -w keyword [-d pkg_location] [pkg_name]
customize_eac_depot -r [-l lang] [-d pkg_location] [pkg_name]
customize_eac_depot -i install_loc [-d pkg_location] [pkg_name]
customize_eac_depot -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
[pkg_name]
customize_eac_depot -g [-f tmp_params] [-d pkg_location] [pkg_name]
```

pkg_name

（可选）您要自定义的 CA Access Control 程序包的名称。如果您未指定程序包，脚本将默认使用 CA Access Control 主程序包 (CAeAC)。

-a

显示许可协议。

-c *certfile*

定义根证书文件的完整路径名。

注意：该选项仅适用于 CAeAC 程序包。

-d *pkg_location*

（可选）指定文件系统上程序包所在目录。 如果您未指定程序包所在目录，脚本将默认使用 /var/spool/pkg。

-f *tmp_params*

指定要创建的或要从中检索信息的安装参数文件的完整路径和名称。

注意：如果您使用 -g 选项时未指定文件，则安装参数将使用标准输出 (stdout)。

--g

获取安装参数文件并将其置于由 -f 选项指定的文件中。

-h

显示命令用法。 与 -l 选项联合使用时，可显示受支持语言的语言代码。

-i *install_loc*

将程序包的安装目录设置为 *install_loc*/AccessControl。

-k *keyfile*

定义根私钥文件的完整路径名。

注意：该选项仅适用于 CAeAC 程序包。

-l *lang*

将安装参数文件的语言设置为 *lang*。您只能与 -r 选项一起设置语言。

注意：有关可以指定的受支持语言代码的列表，请使用 -h 选项运行 -l。 默认情况下，安装参数文件使用英语。

--r

重置程序包，以使用原始程序包中的默认值。

-s

将指定程序包设置为通过自定义安装参数文件（由 -f 选项指定）的输入。

-w 关键字

定义用于指定您接受许可协议的关键字。 您可以在许可协议的结尾处找到此关键字（在方括号内）。要找到许可协议文件，请使用 -a 选项。

卸载 HP-UX 程序包

要卸载安装的 CA Access Control HP-UX 程序包，您需要按照与安装过程相反的顺序来卸载 CA Access Control 程序包。

要卸载 CA Access Control 程序包，应卸载 CA Access Control 主程序包：

```
swremove CAeAC
```

AIX 本地程序包安装

AIX 本地程序包以一系列 GUI 和命令行实用程序的形式提供，用于管理各个软件程序包。

除了常规安装外，您还可以使用 CA Access Control 提供的 AIX 本地软件包。 这样您可以一起管理 CA Access Control 安装和使用 AIX installp 执行的所有其他软件安装。

注意：某些 AIX 版本支持多个程序包格式（installp、SysV、RPM），CA Access Control 仅提供 AIX 本地程序包格式 (installp)。

重要说明！ 程序包安装后，如果要卸载 CA Access Control，您必须使用 *installp* 命令。 请勿使用 uninstall_AC 脚本。

自定义 bff 本地程序包文件

在使用本地程序包安装 CA Access Control 之前，您必须自定义 CA Access Control 程序包，以指定您接受许可协议。 在自定义程序包时，您还可以指定自定义安装设置。

自定义程序包的方法是：从程序包中提取安装参数文件，根据需要进行修改，然后将其加载回程序包中。 某些命令由自定义脚本提供，因此您不必修改参数文件。

注意：建议您不要手动修改程序包。 您应当按照以下步骤中的说明，使用脚本自定义 CA Access Control 程序包。

您可以在 CA Access Control Endpoint Components for UNIX DVD 的 NativePackages 目录中找到适用于每个受支持的 AIX 操作系统的 installp 格式本地程序包（bff 文件）。

自定义 bff 本地程序包文件

1. 将要自定义的程序包提取到文件系统上的临时位置。

   在文件系统上的读取/写入位置上，可以根据需要自定义程序包（bff 文件）。

   重要说明！ 该位置需要拥有大于或等于程序包两倍大小的磁盘空间，才能保留临时重新打包的文件。

2. 将 customize_eac_bff 脚本文件和 pre.tar 文件复制到文件系统上的临时位置。

   pre.tar 文件是 tar 压缩文件，包含安装消息和 CA Access Control 许可协议。

   注意：您可以在本地程序包所在的同一位置中找到 customize_eac_bff 脚本文件和 pre.tar 文件。

3. 显示许可协议：

   ```
   customize_eac_bff -a [-d pkg_location] pkg_name
   ```

4. 记录许可协议结尾处方括号中出现的关键字。

   您需要在下一步中指定该关键字。

5. 自定义 CA Access Control 程序包以指定您接受许可协议：

   ```
   customize_eac_bff -w keyword [-d pkg_location] pkg_name
   ```

6. （可选）设置安装参数文件的语言：

   ```
   customize_eac_bff -r -l lang [-d pkg_location] pkg_name
   ```

7. （可选）更改安装目录：

   ```
   customize_eac_bff -i install_loc [-d pkg_location] pkg_name
   ```

8. （可选）更改默认的加密文件：

   ```
   customize_eac_bff -s -c certfile -k keyfile [-d pkg_location] pkg_name
   ```

9. 获取安装参数文件：

   ```
   customize_eac_bff -g -f tmp_params [-d pkg_location] pkg_name
   ```

10. （可选）编辑安装参数文件以适合您的安装要求。

    通过该文件，您可以设置程序包的安装默认值。 例如：激活 POSTEXIT 设置（删除前面的 # 字符）并将其指向要运行的安装后脚本文件。

11. （可选）设置自定义程序包中的安装参数：

    ```
    customize_eac_bff -s -f tmp_params [-d pkg_location] pkg_name
    ```

    您现在可以使用程序包通过自定义默认值来安装 CA Access Control。

更多信息：

customize_eac_bff 命令—自定义 bff 本地程序包文件 (p. 209)

安装 AIX 本地程序包

要一起管理 CA Access Control 安装和所有其他软件安装，请安装自定义的 CA Access Control AIX 本地程序包。 利用 CA Access Control AIX 本地程序包（bff 文件），您可以在 AIX 中轻松地安装 CA Access Control。

重要说明！ 您必须自定义程序包，以使用可在许可协议中找到的关键字指定自己接受该许可协议。

要安装 CA Access Control AIX 本地软件包

1. 以 root 身份登录。

   要注册并安装 AIX 本地程序包，您需要与 root 帐户相关联的权限。

2. 自定义 CAeAC 程序包 (p. 207)。

   您必须自定义程序包，以使用可在许可协议中找到的关键字指定自己接受该许可协议。 您也可以自定义程序包以指定自定义安装设置。

3. （可选）记录要安装的程序包的级别（版本）：

   `installp -l -d pkg_location`

   pkg_location

   定义 CA Access Control 程序包 (CAeAC) 所在的目录。

   对于 *pkg_location* 中的每个程序包，AIX 都均会列出其级别。

   注意：有关 AIX 本地程序包安装选项的详细信息，请参阅有关 installp 的手册页。

4. 使用以下命令安装 CA Access Control 程序包：

   `installp -ac -d pkg_location CAeAC [pkg_level]`

   pkg_level

   定义先前记录的程序包级别号。

   AIX 开始从 *pkg_location* 目录安装 CAeAC 软件包。

   CA Access Control 现已完全安装，但还未启动。

更多信息：

自定义 bff 本地程序包文件 (p. 207)
本地安装的其他注意事项 (p. 182)

customize_eac_bff 命令—自定义 bff 本地程序包文件

customize_eac_bff 命令对 bff 本地程序包文件运行 CA Access Control 本地程序包自定义脚本。

该脚本适用于 AIX 上所有可用的 CA Access Control 本地程序包。 要自定义程序包，程序包必须位于您文件系统上的读取/写入目录。

重要说明！ 提取程序包的位置应具有足够的空间，其大小至少是用于重新打包结果的中间程序包大小的两倍。

注意：要获得本地化的脚本消息，您需要将 pre.tar 文件和脚本文件置于同一目录中。

此命令格式如下：

```
customize_eac_bff -h [-l]
customize_eac_bff -a [-d pkg_location] pkg_name
customize_eac_bff -w keyword [-d pkg_location] pkg_name
customize_eac_bff -r [-d pkg_location] [-l lang] pkg_name
customize_eac_bff -i install_loc [-d pkg_location] pkg_name
customize_eac_bff -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
pkg_name
customize_eac_bff -g [-f tmp_params] [-d pkg_location] pkg_name
```

pkg_name

您要自定义的 CA Access Control 程序包（bff 文件）的名称。

-a

显示许可协议。

-c *certfile*

定义根证书文件的完整路径名。

注意：该选项仅适用于 CAeAC 程序包。

-d *pkg_location*

（可选）指定文件系统上程序包所在目录。 如果您未指定程序包所在目录，脚本将默认使用 /var/spool/pkg。

-f *tmp_params*

指定要创建的或要从中检索信息的安装参数文件的完整路径和名称。

注意：如果您使用 -g 选项时未指定文件，则安装参数将使用标准输出 (stdout)。

--g

获取安装参数文件并将其置于由 -f 选项指定的文件中。

-h

显示命令用法。 与 -l 选项联合使用时，可显示受支持语言的语言代码。

-i *install_loc*

将程序包的安装目录设置为 *install_loc*/AccessControl。

-k *keyfile*

定义根私钥文件的完整路径名。

注意：该选项仅适用于 CAeAC 程序包。

-l *lang*

将安装参数文件的语言设置为 *lang*。您只能与 -r 选项一起设置语言。

注意：有关可以指定的受支持语言代码的列表，请使用 -h 选项运行 -l。 默认情况下，安装参数文件使用英语。

--r

重置程序包，以使用原始程序包中的默认值。

-s

将指定程序包设置为通过自定义安装参数文件（由 -f 选项指定）的输入。

-w 关键字

定义用于指定您接受许可协议的关键字。 您可以在许可协议的结尾处找到此关键字（在方括号内）。要找到许可协议文件，请使用 -a 选项。

卸载 AIX 程序包

要卸载安装的 CA Access Control AIX 程序包，您需要按照与安装过程相反的顺序来卸载 CA Access Control 程序包。

要卸载 CA Access Control 程序包，应卸载 CA Access Control 主程序包：

```
installp -u CAeAC
```

常规脚本安装

CA Access Control 提供 install_base 脚本，用于在 UNIX 上以交互方式或静默方式安装 CA Access Control。

如果使用常规脚本安装（非本地安装），您将需要从 CA Access Control 安装介质获取以下三个文件：

- **install_base**—从 tar 文件安装 CA Access Control 的脚本。
- ***_opSystemVersion_ACVersion*.tar.Z**—包含所有 CA Access Control 文件的压缩 tar 文件。 例如：如果您在 IBM AIX 版本 5 上安装 CA Access Control r12.0，则您的 tar 文件即为 _AIX5_120.tar.Z
- **pre.tar**—包含安装消息以及许可协议的压缩 tar 文件。

  阅读许可协议文件后，您可以通过输入在该文件的结尾找到的命令继续进行安装：

  - 如果您运行的是静默安装（使用 install_base -autocfg），则可以使用 -command 选项和在许可协议文件结尾找到的命令。
  - 如果您使用响应文件 (-autocfg file_name)，则不需要使用 -command 选项。

  要获取许可文件名称和位置，请运行 install_base -h。 即使输入的命令错误，您仍可以获取文件名和位置。

您可以在 CA Access Control Endpoint Components for UNIX DVD 的 /Unix/Access-Control 目录下找到这些文件。

使用 install_base 脚本进行安装

您可以使用 install_base 脚本在任意受支持的操作系统上安装 CA Access Control。 此为交互脚本，但您仍可以以静默方式运行该脚本。

注意：运行 install_base 脚本之前，请确保决定要安装的功能并检查 install_base 命令 (p. 214)，以便了解如何开始安装此功能。 您还可能需要先了解 install_base 脚本的工作原理 (p. 219)。

安装 CA Access Control

1. 如果您已安装 CA Access Control 并且它正在运行，请以管理员身份登录并输入以下命令将其关闭：

   ```
   ACInstallDir/bin/secons -sk
   ACInstallDir/bin/SEOS_load -u
   ```

2. 以 *root* 身份登录。

   要安装 CA Access Control，您需要具有 root 权限。

3. 挂接光盘驱动器运行 CA Access Control Endpoint Components for UNIX DVD。

   重要说明！ 如果您要通过光盘驱动器在 HP 上进行安装，则需要确保从 DVD 中正确读取文件名。 要防止文件名被强制缩短和全部-处于大写格式，请输入 *pfs_mountd &* 和 *pfsd &* 命令，并确保调用以下四个后台进程：pfs_mountd、pfsd.rpc、pfs_mountd.rpc 和 pfsd。 有关详细信息，请参阅有关特定 pfs* 后台进程和命令的手册页。

4. 阅读许可协议。

   要运行 install_base 脚本，您需要接受最终用户许可协议。 阅读许可协议后，可以通过输入在该文件结尾找到的命令继续进行安装。 要获取许可文件名称和位置，请运行 install_base -h。

5. 运行 install_base 脚本。

   install_base 脚本将启动，并根据您的选择提示您回答相应的安装问题。

   注意：安装脚本会找到相应的 tar 压缩文件，因此键入适用于您平台的 tar 文件名是可选操作。

   现在，CA Access Control 安装已完成，但是还尚未运行。

示例：安装客户端和服务器程序包，并启用默认功能

以下命令显示了如何启动 install_base 交互脚本安装客户端和服务器程序包，并启用所有默认 CA Access Control 功能。 在安装过程中，您需要回答与安装 CA Access Control 的客户端和服务器程序包相关的问题。

```
/dvdrom/Unix/Access-Control/install_base
```

注意：由于我们未指定要安装的程序包，因此 install_base 命令会同时安装客户端和服务器程序包。

示例：将客户端程序包安装到自定义目录，并启用 STOP。

以下命令显示了如何启动 install_base 交互脚本将客户端程序包安装到 /opt/CA/AC 目录，并启用“堆栈溢出保护”选项。

```
/dvdrom/Unix/Access-Control/install_base -client -stop  -d /opt/CA/AC
```

install_base 命令—运行安装脚本

install_base 命令运行安装脚本，并安装一个或多个 CA Access Control 程序包且启用一个或多个已选定的安装选项。

此命令格式如下：

```
install_base [tar_file] [packages] [options]
```

tar_file

（可选）定义包含适用于您平台的 CA Access Control 安装文件的 tar 文件的名称。 安装脚本会自动找到相应的 tar 压缩文件，因此键入您的 tar 文件名是可选操作。

packages

（可选）定义您要安装的 CA Access Control 程序包。 如果您未指定任何程序包，则安装脚本会同时安装客户端和服务器程序包，除非您升级 CA Access Control，如果升级 CA Access Control，安装脚本会安装您已经安装的相同程序包。

注意：必须先安装客户端程序包，才能安装任何其他程序包。 不过，您可以指定一起安装客户端程序包与任何其他程序包。

以下是您可以安装的 CA Access Control 程序包：

-所有

安装所有 CA Access Control 程序包。 包括客户端程序包、服务器程序包、API 程序包以及 MFSD 程序包。 还将启用 STOP（-stop 选项）。

--api

安装具有 API 库和示例程序的 API 程序包。

-客户端

安装具有独立计算机所需的核心 CA Access Control 功能的客户端程序包。

-mfsd

安装具有大型机同步后台进程的 MFSD 程序包。

注意：必须先安装服务器程序包，才能安装 MFSD 程序包。

-server

安装服务器程序包，其中包括更多二进制文件和脚本（selogrcd、sepmd、sepmdd、sepmdadm、secrepsw）。 这些项是对客户端程序包的补充。 例如：通过 sepmdd，您可以使用策略模型设置计算机。

--uni

安装 Unicenter 安全集成和迁移程序包，该程序包支持 CA Access Control 与 Unicenter 的 CAUTIL、Workload Management 和 Event Management 组件及 Unicenter EMSec API 集成。

options

（可选）定义您要设置的其他安装选项。

注意：影响 CA Access Control 功能的安装选项（例如：-stop）只能在安装*客户端*程序包时指定。 影响安装过程的安装选项（例如：-verbose）可以在安装任意程序包时指定。

您可以指定以下选项：

-autocfg [*response_file*]

在静默模式（而不是交互模式）下运行安装。 如果指定了响应文件，则安装将使用存储在该文件中的首选项自动响应交互安装过程。 如果未指定响应文件，或者响应文件缺少任何选项，则安装将使用预设的默认值。

创建响应文件：

- 使用 *-savecfg* 选项。
- 编辑安装参数文件（可在 parameters.tar 内找到）

重要说明！ 如果您不指定响应文件，则必须在使用 *-autocfg* 选项时使用 *-command* 选项。

运行静默安装时，请考虑以下事项：

- 您不能更改加密密钥。
- 默认情况下，仅安装客户端和服务器程序包。

  要安装任何其他程序包或功能，必须与在正常安装中一样指定相应的选项。
- 在安装过程中，install_base 命令不在屏幕上显示安装详细信息。

  要在安装过程中在屏幕上查看安装消息，请使用 *-verbose* 选项。
- 由于安全原因，您无法在静默安装中指定用于保护报告代理与分发服务器之间 SSL 通讯安全的共享密钥。 要指定共享密钥，您需要在安装之后配置报告代理用户 (+reportagent)。

-command *keyword*

定义用于指定您接受许可协议的命令。您可以在许可协议的结尾处找到此命令（位于方括号内），并且必须在使用 -autocfg 选项时使用此命令。 要找到许可协议文件，请运行 *install_base -h*

注意：许可协议仅在显示帮助时才会显示。 阅读完帮助后，许可协议会删除。

-d *target_dir*

定义自定义安装目录。 默认安装目录是 /opt/CA/AccessControl/。

重要说明！ 您不能将 CA Access Control 数据库置于挂接的网络文件系统 (NFS) 中。

-dns | -nodns

使用或不使用 DNS 主机创建 Lookaside 数据库。 -nodns 选项指定 CA Access Control 将不在安装期间在任何 DNS 主机上执行 nslookup。

-fips

指定激活仅 FIPS 公钥（非对称）加密。

-force

强制安装忽略处于活动状态的新订户更新（*sepmd -n* 和 *subs <pmdb> newsubs(sub_name)*）并继续进行安装。 默认情况下，安装会停止并要求您先完成新订户更新。

注意：如果使用此选项，新订户更新将失败。

-force_encrypt

强制安装程序接受非默认的加密密钥，而不显示警告。

重要说明！ 升级完成后，您的加密密钥 将设置为默认值。

注意：CA Access Control 还提供 SSL、AES（128 位、192 位和 256 位）、DES 和 3DES 加密选项供您选择。

-force_install

强制新安装覆盖已安装的版本。 当您要覆盖同一版本进行安装时，请使用该选项。

-force_kernel

强制安装继续进行，而不警告您该安装无法卸载旧内核。

注意：您可能需要在安装完成后重新引导计算机。

-g *groupname*

定义 CA Access Control 文件的组所有者名称。 默认值为 0。

--h | -help

显示此命令的帮助。

-ignore_dep

指定安装*不*检查与其他产品的相关性。

-key *encryption_key*

在 升级过程中还原加密 密钥 。

注意：在升级过程中， 您必须使用与 升级之前相同的加密密钥。

-lang *lang*

定义安装 CA Access Control 所使用的语言。 要获得受支持语言和字符集的列表，请在显示帮助时阅读此选项的说明 (install_base -h)。

-lic_dir *license_dir*

如果未安装许可程序，请定义许可程序安装目录。

注意：仅当未在您的工作环境或计算机环境中定义 $CASHCOMP 变量（可在 /etc/profile.CA 中定义）时，许可程序才会安装到指定目录中。 否则，许可程序将安装到 $CASHCOMP。 如果未定义 $CASHCOMP 且未指定 -lic_dir，则许可程序将会安装到 /opt/CA/SharedComponents 目录中。 CAWIN 与许可程序包安装在同一目录中。

--nolink

指定当您将 CA Access Control 安装到默认路径 (/opt/CA/AccessControl/) 时不在 /etc 目录中创建 seos.ini 的链接。

当您将 CA Access Control 安装到非默认目录中时，CA Access Control 会在 /etc 目录中创建 seos.ini 的链接。 这可使 CA Access Control“检测到”安装位置。 如果要安装到默认路径且不想更新 /etc（由于安全要求），请使用此选项。

--nolog

指定不为安装过程保留日志。默认情况下，所有与安装过程相关联的事务均存储到 *ACInstallDir*/AccessControl_install.log（其中，*ACInstallDir* 是 CA Access Control 的安装目录）。

-no_tng_int

指定安装不尝试设置 selogrd 与 Unicenter Event Management 的集成。

如果未指定此选项，安装脚本将检查是否安装了 Unicenter Event Management。如果脚本发现 Unicenter Event Management 似乎已经安装，则该脚本会通过将以下行添加到 selogrd.cfg 来设置 selogrd 与 Unicenter Event Management 的集成：

```
uni hostname
```

-post *program_name*

指定在安装完成后运行某程序。

-pre *program_name*

指定在安装开始前运行某程序。

-rcert *certificate.pem*

指定根证书文件的完整路径名。

注意：当您使用此选项时，脚本会提取 tar 文件，然后将其与您提供的文件一起重新打包来替换默认文件 (def_root.pem)。

-rkey *certificate.key*

指定根密钥文件的完整路径名。

注意：当您使用此选项时，脚本会提取 tar 文件，然后将其与您提供的文件一起重新打包来替换默认文件 (def_root.key)。

-rootprop

指定将根密码的 sepass 更改发送到策略模型。

注意：您可以在安装完成后使用 seos.ini 文件的 AllowRootProp 标记来设置此选项。 有关 seos.ini 初始化文件的详细信息，请参阅 *《参考指南》*。

-savecfg *<response_file>*

将您的响应存储到交互安装中，以供 *-autocfg* 选项稍后使用。

-停止

启用 STOP（堆栈溢出保护）功能。

-system_resolve

指定使用系统函数，这些函数定义系统上的网络缓存回避。

注意：您不能在 IBM AIX 平台上使用此选项。

-v

显示 CA Access Control 程序包的版本。

-verbose

指定在安装过程中在屏幕上显示安装消息。这是交互安装的默认值，如果您要在使用 *-autocfg* 选项后查看这些消息，只需指定此选项即可。

install_base 脚本的工作原理

install_base 脚本执行下列步骤：

1. 询问您是否要更改默认安装目录。
2. 显示您提供的安装选项并要求您确认是否继续进行安装。
3. 将 tar.Z 文件的数据提取到安装位置（默认位置或 *target_dir* 指定的位置）。
4. 不同的平台将产生不同的操作：
   - 对于 Sun Solaris，脚本会将 CA Access Control *syscall* 脚本添加到文件 /etc/name_to_sysnum 中。 原始文件将另存为 /etc/name_to_sysnum.bak。 然后创建文件 /etc/rc2.d/S68SEOS，该文件组成引导序列的一部分。
   - 对于 IBM AIX，脚本将加载 SEOS_syscall 脚本。
5. 分配、初始化并格式化 CA Access Control 数据库，并构建 seos.ini 文件。 数据库文件位于 *ACInstallDir*/seosdb 目录中（其中，*ACInstallDir* 是 CA Access Control 安装目录）。
6. 确定计算机是否为 NIS+
   - 如果是 NIS+，则该脚本会将 [passwd] 部分中的 nis_env 标记设置为 *nisplus*
   - 如果计算机不是 NIS+ 而是 NIS，则该脚本会将标记设置为 *nis*。

     此外，如果 rpc.nisd 正在运行，则该脚本会将 [passwd] 部分中的 NisPlus_server 内标识设置为“是”。

7. 在支持的 32 位平台 Sun Solaris、IBM AIX、HP-UX 以及 Linux 下，该脚本会判断计算机是在 NIS 下运行还是在 DNS 下运行（使用高速缓存）。 如果是，则该脚本将自动创建后备数据库，并将 seos.ini 文件的 [seosd] 部分中的两个标记 under_NIS_server 和 use_lookaside 设置为 yes。

   注意：在其他平台中，该脚本会提示您是否安装后备数据库以及是否安装到目标安装目录。

8. 还会提示您提供以下信息：（可以在安装后随时修改这些设置。）

   - 可以阅读审核文件的审核者组的名称。
   - 是否要立即在 CA Access Control 数据库中添加所有 UNIX 用户、用户组和主机。
   - 是否要为数据库订阅 PMDB；如果是这样，要订阅哪个 PMDB。

     您的答复实际上并不会将数据库订阅到 PMDB，只会使指定的 PMDB 在稍后创建订阅后对此数据库进行更新。

     该问题的两个安全答复包括：

如果需要：	答复方式：
允许为数据库订阅特定的 PMDB	PMDB 名称的格式 *pmd_name@hostname*
防止为数据库订阅任何 PMDB（至少在您进行其他指定之前）	Enter 键。

     第三个答复 _NO_MASTER_ 允许为数据库订阅任何 PMDB。 但是，这可能是一个很危险的答复，因为您会失去对选择 PMDB 的控制。

   - 密码策略模型名称。
   - 哪些用户将成为 CA Access Control 的安全管理员。
   - 您是否希望 CA Access Control 支持企业用户；如果是，您是否要将任何企业用户定义为安全管理员。
   - 如果选择了仅 FIPS 安装，您是否要指定与加密相关的仅 FIPS 选项。
   - 如果未选择仅 FIPS 加密，您是否要替换默认加密方法。

     CA Access Control 提供对称密钥、公钥以及二者的组合作为加密选项供您选择。
   - 如果选择公钥加密，CA Access Control 可使您指定提供主题证书和根证书的方式。

     根据您的选择，CA Access Control 将帮助您设置 SSL。

- 如果选择对称加密，您是否要设置新的加密密钥。

  注意：有关加密的信息，请参阅 *《参考指南》*中的 sechkey。

- 是否要安装基线安全规则。

  基线安全规则使管理员有机会安装包含两组规则的软件包，从而可以更好地保护您的系统、密码和日日志文件。 一组规则将应用于所有平台以保护 CA Access Control 文件。 另一组规则将保护 UNIX 文件，并且专门用于 Sun Solaris、HP-UX、IBM AIX 和 Digital DEC UNIX 平台。 您不能安装一组规则，而不安装另一组规则。 基线安全规则在警告模式下安装，为您提供信息，但不提供实际保护。 这就是我们建议您在熟悉这些规则后立即删除警告模式的原因所在。

- 是否希望能够从远程主机启动 CA Access Control。

- 是否要启用报告代理，如果是，是否要启用 CA Enterprise Log Manager。

  报告代理将排定的数据库快照发送到消息队列。 如果启用报告代理，您必须定义分发服务器的主机名、要使用的端口以及队列名称。 如果启用 CA Enterprise Log Manager，您还可以指定保留带有时间戳的审核日志文件备份。

- 是否要启用 PUPM 代理。

  PUPM 代理会为 PUPM 配置本地计算机，以便您可以从此计算机获得特权帐户密码。 如果启用 PUPM 代理，您必须定义分发服务器的主机名、要使用的端口以及队列名称。

- 是否要设置此端点以进行高级策略管理；如果是，请指定要将计算偏差结果发送到的分发主机 (DH) 名。

  使用格式 *dhName@hostName* 定义 DH 主机名。例如：如果您已在名为 host123.comp.com 的主机上安装了分发服务器，则应使用以下名称：DH__@host123.comp.com

配置 Post-Installation 设置

安装完成后，您需要为您的环境配置 CA Access Control。

配置安装后的设置

1. 将 *ACInstallDir*/bin 目录附加到您的路径

   默认情况下，安装目录为 /opt/CA/AccessControl/

2. 检查 seos.ini (p. 229) 文件标记，确保其设置满足您的要求。

   如有必要，请修改这些设置。

3. 要授予自己对 CA Access Control 手册页的访问权限，请将目录 *ACInstallDir*/man 添加到 MANPATH 中。

   例如：如果正在使用 csh，则为了您当前的会话，请输入以下命令：

   ```
   setenv MANPATH $MANPATH:/opt/CA/AccessControl//man
   ```

   为了将来的会话，请在您的 .login、.profile 或 .cshrc 文件中添加类似的行。

启动 CA Access Control

假设您正在 X Windows 环境中工作，请调用 CA Access Control，并验证它是否已正确地安装在系统上，然后执行下列步骤来启动重要保护：

1. 在 root（超级用户）权限下打开两个窗口。
2. 在每个窗口中，输入以下命令：

   ```
   seload
   ```

   当 seload 命令启动三个 CA Access Control 后台进程（引擎、代理和 Watchdog）时，请稍候。

3. 启动后台进程后，请转至其他窗口并输入以下命令：

   ```
   secons -t+ -tv
   ```

   CA Access Control 将汇集报告操作系统事件的消息文件。 secons -tv 命令也会在屏幕上显示消息。

4. 在第一个窗口中（您在此处提供 seload 命令），输入以下命令：

   ```
   who
   ```

   观察第二个窗口（CA Access Control 正在此处写入跟踪消息），以查看 CA Access Control 是否截获 who 命令的执行情况并报告相关信息。 如果它报告截获 who 命令，则表明 CA Access Control 已正确地安装在您的系统上了。

5. 如果需要，请输入更多命令以查看 CA Access Control 如何响应这些命令。

   数据库尚不包含阻止访问企图的任何规则。 不过，CA Access Control 将监视系统，以便您查看系统在安装和运行 CA Access Control 后的运行方式，以及 CA Access Control 截获的事件。

6. 输入以下命令，关闭 seosd 后台进程：

   ```
   secons -s
   ```

   屏幕上将显示以下消息：

   ```
   CA Access Control 现已关闭!
   ```

将端点配置为使用高级策略管理

安装高级策略管理服务器组件后，您需要在企业中将每个端点配置为使用高级策略管理。 执行此操作时，需将端点配置为将信息发送到服务器组件并从服务器组件接收信息。

注意：此过程显示了如何配置现有的 CA Access Control 安装来进行高级策略管理。 如果您在端点上安装 CA Access Control 时指定了该信息，则不需要再次配置该端点。

要为高级策略配置端点，请打开一个命令窗口，然后输入以下命令：

```
dmsmgr -config -dhname dhName
```

dhName

定义要与端点配合使用的分发主机 (DH) 名称的列表，以逗号分隔。

示例：DH__@centralhost.org.com

该命令将端点配置为使用高级策略管理，并将其设置为与定义的 DH 配合使用。

注意：有关详细信息，请参阅*《参考指南》*中的 dmsmgr -config 命令。

配置 UNIX 端点以进行报告

安装和配置完 CA Access Control 端点管理 和报告门户之后，您可以通过启用和配置报告代理来配置自己的端点，以将数据发送到分发服务器进行处理。

注意：安装 CA Access Control 时，您可以为报告配置端点。 此步骤说明了如何配置现有端点用于发送报告（如果未在安装时配置该选项）。

配置 UNIX 端点以进行报告

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

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

   如果忽略所有配置选项，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。

   此用户应具有 ADMIN 和 AUDITOR 属性，并应具有对本地终端的*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. 为报告代理进程创建 SPECIALPGM。

   SPECIALPGM 会将 root 用户映射至 +reportagent 用户。

注意：启用报告代理之后，您可以修改 CA Access Control 配置设置以更改与性能相关的设置。 有关报告代理配置设置的详细信息，请参阅*《参考指南》*。

示例：配置 UNIX 端点用于报告 selang 使用情况

以下 selang 命令展示了如何创建所需报告代理用户以及为报告代理进程指定特殊安全权限（假定已启用并配置报告代理）：

```
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)
```

自定义 CA Access Control

使用 CA Access Control 实施全面-安全性时，需要定义要强制实施的安全策略。 进行这些定义所花费的时间，取决于您的站点大小和您选择的管理安全性的方式。

例如在大学里，您可能不会将大多数学生定义到 CA Access Control；他们仅根据资源的 _default 设置来获取访问权限。 然而在银行里，您可能会将每个用户都定义到 CA Access Control，并为每种资源设置访问列表，从而允许特定用户访问特定资源。 这样一来，对于相同数量的用户而言，在大学里实施 CA Access Control 就比在银行所用的时间短。

作为安全管理员，您必须定义项目的目标。 必须谨慎做出关于站点策略的决定。 CA Access Control 具有您可以自定义的若干文件，可帮助您实施站点的安全策略。

受托程序

受托程序是只能在未更改的前提下执行的程序。 通常它是 setuid/setgid 程序。 CA Access Control 还允许您将常规程序指定为受托程序。 如果您确定程序未被篡改，请在 PROGRAM 类中注册该程序，CA Access Control 可在该类中保障其完整性。

您可能需要同时使用受信任程序和*程序通路*，以便用户可以仅通过受信任程序执行某些任务。

注意：有关程序路径的详细信息，请参阅*《适用于 UNIX 的端点管理指南》*。

CA Access Control 可以帮助您编写脚本，以便将 setuid 和 setgid 程序的整个集合注册为受托程序。

1. 为了使自己从记住所有 setuid 和 setgid 程序的繁重工作中解脱出来，请使用下面的 seuidpgm 程序。 该程序将扫描您的文件系统、查找所有 setuid 和 setgid 程序，并创建 selang 命令（用于在 PROGRAM 类中注册所有 setuid 和 setgid 程序）的脚本。

   执行以下命令：

   ```
   seuidpgm -q -l -f / > /opt/CA/AccessControl//seuid.txt
   ```

   按照显示的方式运行，seuidpgm 将执行以下操作：

   - 扫描整个文件系统（从根目录 / 开始）。
   - 保持安静模式（-q 选项会隐藏“cannot chdir”消息）。
   - 忽略任何符号链接 (-l)。
   - 在 FILE 和 PROGRAM 类中注册程序 (-f)。
   - 将命令输出到文件 /opt/CA/AccessControl//seuid.txt 中。

   注意：有关 seuidpgm 的完整说明，请参阅 *《参考指南》*。

2. 使用文本编辑器检查 seuid.txt 文件，以确保它包括要信任的所有 setgid/setuid 程序，而不包括其他程序。 如有必要，编辑该文件。

3. 使用 selang 运行编辑的命令文件。 如果 seosd 后台进程未运行，则包括 -l 开关参数。

   ```
   selang [-l] -f /opt/CA/AccessControl//seuid.txt
   ```

   selang 完成可能需要几分钟时间。

4. 重新启动 seosd 后台进程（如果其尚未运行）。 然后检查您的系统是否按预期正常工作，以及是否可以调用 setuid 程序。

5. 将 PROGRAM 类的默认访问权限更改为 NONE 可谓明智之举，这样可以避免在安全管理员不知道的情况下，添加和运行新的不受信任的 setuid 或 setgid 程序。

   输入以下 selang 命令设置此默认的访问权限值：

   ```
   chres PROGRAM _default defaccess(none)
   ```

注意：经验丰富的 CA Access Control 用户将记住此连接中的 UACC 类。该类仍然存在并可用于指定资源的默认访问权限。 然而，为了便于使用，我们建议您使用该类的 _default 记录来指定类的默认访问权限。 _default 规范将覆盖同一类的任何 UACC 规范。

PROGRAM 类中代表您已注册的 setuid、setgid 和常规程序的记录，将存储可执行文件的下列属性。

- 设备-号
- Inode
- 所有者
- 组
- 大小
- 创建日期
- 创建时间
- 上次-修改日期
- 上次-修改时间
- MD5 签名
- SHA1 签名
- 校验和 CRC（循环冗余检查）

您注册的每个程序的最重要的属性，就是该程序是*受托的*。 也就是说，该程序被视为可以运行。 先前列出的任何属性中的更改，都将导致程序失去其受托的状态，之后 CA Access Control 会阻止程序运行。

监控未注册程序的使用

如果您不确定是否已在数据库中成功地注册了所有相应的程序，请使用以下命令寻找未注册的程序：

```
chres PROGRAM _default warning
```

警告属性将 *PROGRAM* 类置于警告模式下，即每次使用未注册的 setuid 或 setgid 程序（而并不防止使用这类程序）时，都将有一条专用审核记录显示为警告。

检查审核日志

您可以在审核日志中手工搜索不受信任的记录，或者设置在某些程序不受信任时要发出的专用通知指令。 该专用通知特别有助于做到：要使用已经变为不受信任的程序的用户，事先不必与您联系；而您则可以在收到“文件已经变为不受信任”的通知后，立即检查该文件。

注意：要设置专用审核通知，请参阅*《端点管理指南》*。

文件保护

为避免执行不受信任的 setuid 和 setgid 命令，请执行以下命令：

注意：CA Access Control 会自动将用户“nobody”包括在数据库中。

```
newres PROGRAM _default defaccess(none) \
owner(nobody) audit(all)
```

CA Access Control 接着就会在允许任何新程序或已更改的程序运行之前，要求获得您的批准，从而防止您遭受后门和特洛伊木马的攻击。

例如：现在假设您已收到新的有用的程序，即 setuid 程序。 您确信它不是特洛伊木马，并且您需要所有的用户都可以执行它。 要将程序注册为受信任的程序，请执行以下命令：

```
newres PROGRAM program-pathname \ defaccess(EXEC)
```

重新托管取消受托的程序

如果程序因其大小、修改日期或任何其他受监控属性发生更改，而不受 CA Access Control 托管，则该程序只能在您*重新托管*它（在数据库中为其注册新的批准）时才能再次运行。 重新托管程序：

```
editres PROGRAM progam_name trust
```

注意：还可以使用 seretrust 实用程序重新托管程序。 有关该实用程序及其选项的详细信息，请参阅*《参考指南》*。

初始化文件

本节介绍 CA Access Control 在初始化时读取的各个文件。 默认情况下，CA Access Control 将初始化文件置于包含文件 seos.ini 的目录中，该目录是 CA Access Control 的安装目录。

seos.ini

seos.ini 文件用于设置全局参数。

注意：有关文件结构和受支持的标记的详细信息，请参阅*《参考指南》*。

seos.ini 文件在安装时就受到保护，不能在 CA Access Control 运行的同时进行更新，但是所有用户始终可以基于读取权限访问该文件。 输入以下命令即可使授权的用户在 CA Access Control 运行的同时更新该文件：

```
newres FILE ACInstallDir/seos.ini owner(authUser) defacc(read)
```

ACInstallDir 是 CA Access Control 的安装目录，默认情况下为 /opt/CA/AccessControl/。

该命令确立以下内容：该文件的默认访问权限为 *READ*，但是，仅该文件的所有者 authUser 可以更新该文件。

注意：使 seos.ini 文件的默认访问权限为读取非常重要，因为许多实用程序都在处理期间访问 seos.ini。 如果它们不能读取该文件，则它们就会失败。

跟踪筛选文件

此可选文件包含一些用于指定筛选掩码的条目，以筛选出任意类型的 CA Access Control 跟踪消息。

跟踪筛选文件指定了要筛选出的跟踪消息（即，不会在跟踪文件中显示的消息）。 每一行都指定一个掩码，用于标识要压缩的一组消息。 例如：以下文件将抑制显示以 WATCHDOG 或 INFO 开头的所有消息，以及以 BYPASS 结尾的所有消息。

```
WATCHDOG*
*BYPASS
INFO*
```

默认情况下，CA Access Control 将使用名为 trcfilter.init 的跟踪筛选文件。 您可以通过编辑 seos.ini 文件的 [seosd] 部分中 trace_filter 标记的值更改跟踪筛选文件的名称和位置。

要筛选跟踪记录，请根据需要编辑该文件。 要在该文件中添加说明（注释行），请在该行的开头加一个分号 (;)。

trcfilter.init 文件不筛选用户跟踪生成的审核记录。 要筛选这些审核记录，请编辑 audit.cfg 文件。

注意：有关详细信息，请参阅 *《参考指南》* 中的 seosd 实用程序。

高级策略管理

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

注意：有关高级策略管理的详细信息，请参阅*《企业管理指南》*。

配置高级策略管理

如果要将您的企业设置为使用基于策略的高级管理，需要在中央位置安装 DMS 和 DH，然后将每个端点配置为使用高级策略管理 (p. 230)。

要在安装后将层级结构配置为使用高级策略管理，请使用 dmsmgr 实用程序。

注意：有关 dmsmgr 实用程序的详细信息，请参阅*《参考指南》*。

为策略偏差计算配置端点

每个端点必须配置为允许策略偏差计算。 通常，在进行安装时执行该操作。 而该过程的目标是在安装后实现此操作。

要为策略偏差计算配置端点，请输入以下 selang 命令：

```
so dms+(DMS@host)
```

DMS@host

为在显示的格式中指定的 DMS 定义名称。

sesu 和 sepass 实用程序

建议您使用 sepass 而不是操作系统的 passwd 命令，使用 sesu 而不是 su 命令。 要实现这一点，需要保存原始系统二进制文件，并将这些文件分别替换为指向 sepass 和 sesu 的符号链接。 完成后，您需要确保可以始终使用这些实用程序。

在大多数操作系统中，即使未加载 CA Access Control，sepass 和 sesu 实用程序也可运行。 但是，在某些操作系统中（例如：AIX），如果未加载 CA Access Control，这些实用程序则无法运行。 对于这些操作系统，CA Access Control 提供包装程序脚本。

sesu 和 sepass 包装程序脚本

可在以下目录中找到 sesu 和 sepass 包装程序脚本：

ACInstallDir/samples/wrappers

该目录包含以下文件：

文件	说明
sesu_wrap.sh	sesu 的包装程序脚本
sepass_wrap.sh	sepass 的包装程序脚本
自述文件	包含这些包装程序的用法和概念信息的文本文件

使用包装程序脚本运行 sesu

在未加载 CA Access Control 则无法运行 sesu 实用程序的操作系统上，使用包装程序脚本即可运行该实用程序。

注意：如果在未加载 CA Access Control 时 sesu 实用程序无法运行，您只需执行该过程。

使用包装程序脚本运行 sesu

1. 在文本编辑器中打开 sesu_wrap.sh 脚本。

   包装程序脚本将显示在文本编辑器中。

2. 如果必要，更改以下两个变量：

   SEOSDIR

   定义 CA Access Control 安装目录。 默认情况下，此项设置为默认的安装目录：

   /opt/CA/AccessControl/

   SYSSU

   定义需要替换的原始 su 系统二进制文件的名称。 默认情况下，此项将设置为：

   /usr/bin/su.orig

3. 替换 su 符号链接以指向 sesu_wrap.sh 包装程序脚本而不是 sesu 实用程序。

   每次运行 su 时，sesu 包装程序脚本都将运行 sesu 实用程序。

使用包装程序脚本运行 sepass

在未加载 CA Access Control 则无法运行 sepass 实用程序的操作系统上，使用包装程序脚本即可运行该实用程序。

注意：如果在未加载 CA Access Control 时 sepass 实用程序无法运行，您只需执行该过程。

使用包装程序脚本运行 sepass

1. 在文本编辑器中打开 sepass_wrap.sh 脚本。

   包装程序脚本将显示在文本编辑器中。

2. 如果必要，更改以下两个变量：

   SEOSDIR

   定义 CA Access Control 安装目录。 默认情况下，此项设置为默认的安装目录：

   ```
   /opt/CA/AccessControl/
   ```

   SYSPASSWD

   定义需要替换的原始 sepass 系统二进制文件的名称。 默认情况下，此项将设置为：

   ```
   /usr/bin/passwd.orig
   ```

3. 替换 passwd 符号链接以指向 sepass_wrap.sh 包装程序脚本而不是 sepass 实用程序。

   每次运行 passwd 时，sepass 包装程序脚本都将运行 sepass 实用程序。

维护模式保护（无人值守模式）

CA Access Control 具有维护模式（也称为静默模式），在 CA Access Control 后台进程关闭以进行维护时提供保护。 在该模式下，CA Access Control 将在这些后台进程关闭时拒绝事件。

CA Access Control 运行时将截获安全敏感事件，并检查是否允许该事件。 在未激活维护模式的情况下，当 CA Access Control 服务关闭时，将允许所有事件。 在活动的维护模式下，当 CA Access Control 后台进程关闭时将拒绝事件，当系统进行维护时停止用户活动。

维护模式可进行调整，默认情况下该模式处于禁用状态。

CA Access Control 安全服务关闭时：

- 如果维护模式处于活动状态，将拒绝所有安全敏感事件（特殊情况和由维护用户执行的事件除外）。
- 如果已禁用维护模式，CA Access Control 将不做干预，执行将转到操作系统。

激活维护模式并且关闭安全机制时，阻止的事件不会记录到审核日志文件中。

要启用维护模式，请遵循下列步骤：

重要说明！ 如果 root 不是维护用户，请确保您具有针对维护用户的打开会话，否则您无法登录。

1. 请确保 CA Access Control 后台进程已关闭。
2. 使用 seini 实用程序 将标记 silent_deny 的值更改为 *yes*。

   该标记 位于 SEOS_syscall 部分。

   ```
   seini -s SEOS_syscall.silent_deny yes
   ```

3. 将标记 silent_admin 的值更改为您希望可在 CA Access Control 后台进程关闭时访问计算机的数字 UNIX UID。

   ```
   seini -s SEOS_syscall.silent_admin <maintenance_UID>
   ```

   注意： *root* 是默认的维护模式用户 (UID 0)。

   重要说明！ 如果维护用户不是 *root*，则必须将 CA Access Control 授权后台进程 setuid 设置为 root 用户，以便可以在维护模式下启动 CA Access Control。 要进行此更改，请输入以下命令：
   chmod 6111 seosd

4. 使用 seload 命令启动 CA Access Control 后台进程。

   注意： 如果维护模式用户不是 root，请使用 seosd 命令启动 CA Access Control 后台进程。

Solaris 10 区域实施

Solaris 10 提供虚拟操作系统服务，虚拟操作系统服务就像称为*区域*的不同 Solaris 例程。 所有 Solaris 10 系统均包含主区域，称为*全局区域*。 非全局区域伴随全局区域运行，您可以从全局区域对其进行配置、监控和控制。

您可以使用 CA Access Control 保护环境中的每个区域（或选中的区域）。这使您可以为每个区域定义不同的规则和策略，因此可以为每个区域定义不同的访问限制。

在 Solaris 10 区域上安装 CA Access Control 与常规安装完全相同，您可以使用以下任一方法完成该操作：

- 使用 Solaris 本地程序包安装 CA Access Control

  CA Access Control 设计为使用 Solaris 本地程序包工具（pkgadd 和 pkgrm）进行安装和卸载。

  如果您使用 Solaris 本地程序包安装进行安装，则可以：

  - 在所有区域上安装 CA Access Control (p. 193)。

    在 Solaris 10 上安装 CA Access Control 的最简单和建议的方法是在全局区域上安装，*或*在*所有*区域（包括非活动区域和以后创建的任何区域）上安装。

  - 在选中区域安装 CA Access Control (p. 197)。

    虽然我们不建议这样做，但您也可以使用 Solaris 本地程序包工具在选中区域上安装 CA Access Control。 但是，要使 CA Access Control 在任何非全局区域运行，您必须也在全局区域中安装 CA Access Control。

  如果您使用 Solaris 本地程序包进行了安装，则可使用该本地程序包从所有区域卸载 CA Access Control。

- 使用 install_base 脚本在每个区域安装 CA Access Control (p. 212)。

  install_base 脚本在您执行该脚本所在的区域内安装 CA Access Control。

  要使 CA Access Control 在任何非全局区域运行，您必须也在全局区域中安装 CA Access Control。

  如果您使用 install_base 脚本安装了 CA Access Control，可以从各个非全局区域将其卸载。 但是，CA Access Control 内核只能从全局区域卸载，*并且*仅在 CA Access Control 已在所有区域停止后才能卸载。

  重要说明！ 如果您先使用 install_base 从全局区域卸载 CA Access Control，再从所有区域卸载 CA Access Control，则用户可能被锁定在区域中。 建议您使用 Solaris 本地程序包在 Solaris 区域上安装和卸载 CA Access Control。

区域保护

CA Access Control 保护 Solaris 10 区域的方式与保护任何计算机的方式相同。 每个区域均独立于任何其他区域受到保护，您在 CA Access Control 中定义的每个规则仅应用于在该区域中工作的用户。 在全局区域中应用的规则，甚至应用于非全局区域中可见资源的规则，仅应用于从全局区域访问这些资源的用户。

注意：请确保根据需要在非全局区域和全局区域中保护非全局区域资源。

示例：全局区域规则和非全局区域规则

在以下示例中，我们将定义保护非全局区域 (myZone1) 文件的规则。 所有系统文件始终从全局区域中可见。

我们要保护的文件为 /myZone1/root/bin/kill（从全局区域的路径）。 为保护该文件，我们定义以下 CA Access Control 规则：

- 在全局区域中：

```
nu admin_pers owner(nobody)
nr FILE /myZone1/root/bin/kill defaccess(none) owner(nobody)
authorize FILE /myZone1/root/bin/kill uid(admin_pers) access(all)
```

- 在 myZone1（非全局区域）中：

```
nu admin_pers owner(nobody)
nr FILE /bin/kill defaccess(none) owner(nobody)
authorize FILE /bin/kill uid(admin_pers) access(all)
```

通过在全局区域和非全局区域中使用这些规则，我们定义了用户 (admin_pers)、将文件定义为要保护的资源并授权用户访问该文件。 如果没有在这两个区域均执行该操作，则资源会面临风险。

新区域设置

如果您使用 Solaris 本地程序包在所有区域安装 CA Access Control，CA Access Control 也会在初始安装后自动安装在您创建的所有区域上。 但是，CA Access Control 安装后过程脚本需要从非全局区域运行，因此对于新区域，这些脚本只能在新区域配置完成后运行。 特别是，您必须运行“zlogin -C *zonename*”命令（该命令完成名称服务、root 密码等的配置）。

重要说明！ 如果您未运行“zlogin -C *zonename*”命令，或者您很快引导并登录至新区域，则由于安装后脚本未运行，CA Access Control 安装将不完整。

注意：有关正确设置新区域的详细信息，请参阅 Oracle Documentation 网站上 Oracle 的*《系统管理指南：Solaris Containers－资源管理和 Solaris Zones》*。

在 Solaris 标记区域中安装

Solaris 限制意味着 pkgadd 不支持 Solaris 10 全局区域中安装的应用程序传播到标记区域中。 同样，CA Access Control 必须使用 ioctl 而不是 syscall 与内核模块通讯。

在 Solaris 标记区域中安装

1. 使用 pkgadd 在 Solaris 全局区域安装 CA Access Control。
2. 使用 pkgadd 在 Solaris 标记区域安装 CA Access Control。

   注意：当您在全局区域中安装时，安装参数文件也允许您自动执行此操作。
3. 在标记区域，请验证 seos.ini 项 SEOS_use_ioctl 是否设置为 1，如果没有，请将其修正。

   此操作确认将 CA Access Control 配置为使用 ioctl。
4. 在全局区域，请验证 seos.ini 项 SEOS_use_ioctl 是否设置为 1。

   此操作确认将 CA Access Control 配置为使用 ioctl。

   安装完成，现在可以启动标记区域中的 CA Access Control。

   重要说明！ 如果 SEOS_use_ioctl 设置为 0，则需要将 CA Access Control 修改为使用 ioctl 在所有区域中进行通讯。 完成此更改之后，重新启动所有区域，安装即完成。

使用 ioctl 进行通讯

如果要将 CA Access Control 安装在 Solaris 标记区域，则必须使用 ioctl，而不是 syscall，与内核模块通讯。

将 CA Access Control 修改为使用 ioctl 进行通讯

1. 在全局区域及所有非全局区域中停止 CA Access Control。

   使用 secons -sk 停止上一区域禁用事件拦截并准备内核模块进行卸载。

2. 在全局区域 (SEOS_load -u) 中卸载 CA Access Control 内核模块。

   注意：SEOS_load -u 命令确保在卸载 CA Access Control 之前， 没有在任何非全局区域中运行。

3. 在安装了 CA Access Control（全局、非全局和标记区域）的每个区域中，seos.ini 项 SEOS_use_ioctl = 1（默认情况下，该项设置为 0）。

4. 在全局区域中加载内核模块 (SEOS_load)。

   这将安装 pseudo 设备让 CA Access Control 通过 ioctl 与其内核模块通讯，并标识要求重新启动的区域，由此他们可以利用 ioctl。

5. 重新启动标识为需要重新启动，安装了 CA Access Control 的每个非全局区域和标记区域。

在区域中启动和停止 CA Access Control

通常，在 Solaris 10 区域中启动和停止 CA Access Control 的方式与您平时在任何 Solaris 计算机上启动和停止 CA Access Control 的方法相同。

以下例外适用于在区域中启动 CA Access Control：

- 您只能从全局区域加载 CA Access Control 内核模块 (SEOS_load)。
- 您必须先在全局区域中加载 CA Access Control 内核模块，然后在任何非全局区域中启动 CA Access Control。

  CA Access Control 内核模块在全局区域中加载后，您可以在任何非全局区域以任意顺序启动和停止 CA Access Control。

以下例外适用于在区域中停止 CA Access Control：

- 当一个或多个区域启用了维护模式 (p. 232)时，您无法卸载 CA Access Control 内核模块。
- 您可以通过在每个区域中发出 *secons -s* 命令，在所有区域中以任意顺序停止 CA Access Control。

- 您可以通过将所有区域添加到 GHOST 记录，然后从全局区域发出 secons -s *ghost_name* 命令的方式，在所有区域同时停止 CA Access Control。

  这非常有用，例如：当您想在所有区域升级 CA Access Control 时。

- 您应使用 *secons -sk* 停止最后一个区域以禁用事件拦截，并准备 CA Access Control 内核模块以进行卸载。
- 您只能从全局区域卸载 CA Access Control 内核模块 (SEOS_load -u)。

  注意：SEOS_load -u 命令确保在卸载 CA Access Control 之前， 没有在任何非全局区域中运行。

在非全局区域中启动 CA Access Control

您可以通过通常使用的方式从任何非全局区域启动 CA Access Control，但是必须先在全局区域中加载 CA Access Control 内核模块。

在非全局区域中启动 CA Access Control

1. 在全局区域中，输入 SEOS_load 命令以加载 CA Access Control 内核模块。

   CA Access Control 内核会加载，您现在可以在任何区域启动 CA Access Control。

   注意：CA Access Control 内核会加载，但是 CA Access Control 不会拦截全局区域中的事件。

2. 在非全局区域中，输入 seload 命令以在该区域启动 CA Access Control。

   非全局区域受 CA Access Control 的保护。

   注意：您也可以在非全局区域中远程启动 CA Access Control。 有关详细信息，请参阅 *《参考指南》* 中的 seload 命令。

zlogin 实用程序保护

使用 zlogin 实用程序，管理员可以输入一个区域。 您应为该实用程序添加 LOGINAPPL 资源，以控制可以登录至任何非全局区域的用户。

CA Access Control 附带预定义的 LOGINAPPL 资源，以保护 zlogin 实用程序。

自动启动 CA Access Control

测试 CA Access Control 并试验其功能后，您即可实施 CA Access Control 保护。

要安排 seosd 后台进程在引导时自动启动，以便可以立即保护您的资源，请使用 *ACInstallDir*/samples/system.init/*sub-dir* 目录，其中 *sub-dir* 是用于您操作系统的目录。 每个子目录都包含自述文件，其中包含在各个操作系统上执行该任务的说明。

使用服务管理工具管理 CA Access Control

在 Solaris 10 上有效

您可以使用 Solaris 服务管理工具 (SMF) 实用程序管理 CA Access Control 后台进程。 使用 SMF 实用程序，您可以控制授权后台进程 (seosd)，该程序用于管理 watchdog 后台进程 (seoswd) 和 seagent 后台进程。 您使用的是特定于 SMF 的命令，而不是 seload 和 secons 命令。

注意：您可以在 Solaris 10 上安装 CA Access Control 之后立即使用服务管理工具实用程序管理 CA Access Control。

注意：有关 seload 和 secons 命令的详细信息，请参阅 *《参考指南》*。

SMF 命令格式如下：

```
#svcadm enable daemon

#svcadm disable daemon

#svcadm restart daemon

#svcadm refresh daemon

#svcs daemon

#svcs -l daemon

#svcadm clear daemon
```

示例：启动 seosd 后台进程

以下示例显示了如何启动 seosd 后台进程：

```
#svcadm enable seosd
```

注意：此命令相当于使用 seload 命令。

示例：停止 seosd 后台进程

以下示例显示了如何停止 seosd 后台进程：

```
#svcadm disable seosd
```

注意：此命令相当于使用 secons -sk 命令。

示例：重新启动 seosd 后台进程

以下示例显示了如何重新启动 seosd 后台进程：

```
#svcadm restart seosd
```

示例：重新加载 seosd 配置

此示例显示了如何重新加载 seosd 后台进程配置：

```
#svcadm refresh seosd
```

注意：此命令相当于使用 secons -rl 命令。

示例：显示 seosd 后台进程的状态

以下示例显示了如何列出 seosd 后台进程的状态：

```
#svcs -l seosd
```

示例：清除 seosd 后台进程的维护状态

以下示例显示了如何清除 seosd 后台进程的维护服务状态：

```
#svcadm clear seosd
```

第 9 章： 安装和自定义 UNAB 主机

此部分包含以下主题：

UNAB 主机

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

将 UNIX 帐户与 Active Directory 相集成可强制实施严格的身份验证和密码策略，将基本的 UNIX 用户和组属性传输到 Active Directory。 这样，您便可以在管理 Windows 用户和组的相同位置管理 UNIX 用户和组。

注意： UNAB 不会在安装时替换任何现有的 PAM 模块。 UNAB PAM 将插入到现有的 PAM 堆栈中。

如何实施 UNAB

在开始实施 UNAB 之前，建议您复查下列步骤，以在您的企业中自定义、安装和配置 UNAB。

1. 验证 UNIX 计算机名是否能够解析 (p. 253)。
2. 检查系统遵从性 (p. 250)。

   uxpreinstall 实用程序会验证系统是否与 UNAB 要求兼容。
3. 自定义 UNAB 安装程序包 (p. 254)。

   注意： 您不需要为每个计划安装 UNAB 的 UNIX 主机自定义 UNAB 安装程序包。 只需为每个操作系统自定义一次安装程序包，并使用它在企业中安装 UNAB。

4. 配置 UNAB 以与 CA Access Control 企业管理 配合使用 (p. 258)。

   使用 CA Access Control 企业管理 服务器用户界面管理 UNAB 端点。

5. 在 UNIX 主机上安装 UNAB 程序包。

   注意：有关系统要求和操作系统支持的详细信息，请参阅 *《版本说明》*。

6. 将 UNIX 主机注册到 Active Directory (p. 289)。

7. 启动 UNAB (p. 292)。

   此步骤将启动 UNAB 后台进程 (uxauthd)。

8. 在 CA Access Control 企业管理 中创建登录授权策略并将策略分配给 UNAB 端点。

   登录策略定义了被允许或拒绝访问 UNIX 主机的企业用户和组。

   注意：有关登录策略的详细信息，请参阅 *《企业管理指南》*。

9. 在 UNIX 主机上激活 UNAB (p. 292)。

   激活 UNAB 将允许企业用户登录到 UNIX 主机。

10. （可选）在完全集成模式下实施 UNAB (p. 293)。

    在完全集成模式下，UNAB 使用 Active Directory 来验证和授权用户。

开始之前

安装 UNAB 之前，请确保已满足初步要求并具有必要的信息。 建议您复查实施 UNAB 所需完成的步骤，并执行初步验证。

安装模式

UNAB 支持两种安装模式：

- **完全集成**－在完全集成模式下，UNIX 主机依赖 Active Directory 服务器对用户进行身份验证和授权。
- **部分集成**－在部分集成模式下，UNIX 主机仅依赖 Active Directory 服务器进行身份验证，而使用基于 UNIX 的用户存储进行授权。 如果要维护 UNIX 用户存储，请使用部分集成模式。

Active Directory 站点支持

在安装 UNAB 之前，您应当了解 UNAB 如何实施 Active Directory 站点支持。 Active Directory 站点支持有助于优化网络流量、提高连接速度和缩短响应时间。

在将 UNAB 端点注册到 Active Directory 时，默认情况下 uxconsole 实用程序会执行以下操作：

- 发现最接近端点物理位置的 Active Directory 站点。
- 将该 Active Directory 站点的名称写入 uxauth.ini 文件的 ad 部分的 ad_site 配置设置。

注册后，UNAB 端点仅会与已发现的 Active Directory 站点中的域控制器 (DC) 进行通讯。 如果端点无法与此站点中的 DC 通讯，UNAB 端点的状态将更改为脱机。

建议您不要更改默认行为。 但是，在自定义 UNAB 安装程序包时，您可以指定与 UNAB 端点通讯的 DC 列表，以及 UNAB 端点忽略的 DC 列表（分别为 lookup_dc_list 和 ignore_dc_list 参数）。 您在这些列表中指定的 DC 将以下列方式与 Active Directory 站点支持进行交互：

- lookup_dc_list－UNAB 端点将与此配置设置中列出的 DC 进行通讯，而不会与 Active Directory 站点支持或 DNS 查询所发现的 DC 进行通讯。
- ignore_dc_list－UNAB 端点将与*未*在此配置设置中列出的、由 Active Directory 站点支持或 DNS 查询发现的任何 DC 进行通讯。

注意：安装后，您可以使用 uxconsole -register 实用程序手动设置与 UNAB 端点进行通讯的 Active Directory 站点。 有关 uxconsole 实用程序的详细信息，请参阅 *《参考指南》*。

64 位 Linux 主机的安装注意事项

在 Linux 64 位计算机上安装 UNAB 之前，您必须确保安装了下列操作系统 32 位库：

ld-linux.so.2、libICE.so.6、libcrypt.so.1、libdl.so.2、libgcc_s.so.1、libm.so.6、libnsl.so.1、libpam.so.0、libpthread.so.0、libresolv.so.2、libstdc++.so.5（以及内核 v2.6 上的 libstdc++.so.6）、libaudit.so.0（仅限 RHEL5 和 OEL 5）。

以下列表为所需的相关 RPM 软件包：

- SLES 10：compat-libstdc++、glibc-32bit、libgcc、pam-32bit
- SLES 9：glibc-32bit、libgcc、libstdc++、pam-32bit
- RHEL 5 和 OEL 5：audit-libs、compat-libstdc++、glibc、libgcc、pam
- RHEL 4 和 OEL 4：compat-libstdc++、glibc、libgcc、pam
- RHEL 3：glibc、libgcc、libstdc++、pam

在 Linux s390x 64 位计算机上安装 UNAB 之前，您必须确保安装了下列操作系统 32 位库：

ld.so.1、libcrypt.so.1、libc.so.6、libdl.so.2、liblaus.so.1 (RHEL 3)、libaudit.so.0（RHEL 4、RHEL 5）、libm.so.6、libnsl.so.1、libpam.so.0、libresolv.so.2

以下列表为所需的相关 RPM 软件包：

- SLES 10：compat-libstdc++、glibc-32bit、pam-32bit
- SLES 9： glibc-32bit、libstdc++、pam-32bit
- RHEL 5：audit-libs、compat-libstdc++、glibc、pam
- RHEL 4：audit-libs、compat-libstdc++、glibc、pam
- RHEL 3：glibc、laus-libs、libstdc++、pam

Linux s390 端点的安装注意事项

如果要使用消息队列功能远程管理 CA Access Control Linux s390 上的 UNAB，并在 Linux IA64 上使用报告功能，请在端点上安装 J2SE 版本 5.0 或更高版本。

消息队列功能允许您将来自 CA Access Control 端点的报告和审核数据分别发送至报告门户和 CA Enterprise Log Manager。 通过远程管理，您可以使用 CA Access Control 企业管理 管理 UNAB 端点。

您可以在端点上安装 CA Access Control 或 UNAB 之前或之后安装 J2SE。 如果在安装 CA Access Control 或 UNAB 之后安装 J2SE，您还必须在端点上配置 Java 位置。

安装程序如何与 Java 进行交互

在 Linux s390、Linux s390x 和 Linux IA64 上有效

要使用消息队列功能远程管理 UNAB Linux s390 端点，并在 Linux IA64 和 Linux s390 上使用报告功能，请在端点上安装受支持的 Java 版本。

在 Linux s390 或 Linux IA64 端点上安装 CA Access Control 或 UNAB 时，安装程序会执行以下操作：

1. 按顺序检查下列位置是否存在有效 Java 环境的路径：
   a. 安装输入内容中的 JAVA_HOME 参数。

      安装输入内容包括 UNAB 安装参数文件、UNIX CA Access Control 安装参数文件、用于本地安装的自定义程序包以及来自交互式 CA Access Control 安装的用户输入内容。

   b. JAVA_HOME 环境变量。

   c. （Linux s390 和 Linux s390x）默认安装路径为：/opt/ibm/java2-s390-50/jre
2. 将 accommon.ini 文件的全局设置中的 java_home 配置设置的值设为下列值之一：
   - 如果安装程序找到有效 Java 环境的路径，会将配置设置的值设为此路径。
   - 如果安装程序未找到有效 Java 环境的路径，会将配置设置的值设为 *ACSharedDir*/JavaStubs。

     默认情况下，*ACSharedDir* 为 /opt/CA/AccessControlShared。

在 Linux s390 和 Linux s390x 端点上配置 Java 位置

在 Linux s390 和 Linux s390x 上有效

要使用消息队列功能并远程管理 UNAB Linux s390 端点，您必须在端点上安装 J2SE 版本 5.0 或更高版本。 如果在安装 CA Access Control 或 UNAB 之后安装 J2SE，您必须执行附加的配置步骤。

在 Linux s390 和 Linux s390x 端点上配置 Java 位置

1. 停止 CA Access Control 和 UNAB（如果它们正在运行）。
2. 将 accommon.ini 文件的全局部分中的 java_home 配置设置的值更改为 Java 安装的路径：

   例如：java_home=/opt/ibm/java2-s390-50/jre
3. 启动 CA Access Control 和 UNAB。

   Java 位置即配置完毕。

在 Linux IA64 端点上配置 Java 位置

在 Linux IA64 上有效

要在 CA Access Control Linux IA 64 端点上使用消息队列功能和报告功能，请在端点上安装 J2SE 版本 6.0 或更高版本。 如果在安装 CA Access Control 之后安装 J2SE，您需要执行附加的配置步骤。

在 Linux IA64 端点上配置 Java 位置

1. 停止 CA Access Control（如果其正在运行）。
2. 将 accommon.ini 文件的全局部分中的 java_home 配置设置的值更改为 Java 安装的路径：

   例如：java_home=/usr/share/java016.0/jre
3. 启动 CA Access Control。

   Java 位置即配置完毕。

Kerberos 和 SSO 注意事项

您可以在启用了 Kerberos 的端点上安装和注册 UNAB，以利用 Kerberos 单点登录 (SSO) 服务进行一次身份验证，然后使用相同的用户凭据登录到多个端点。 如果未配置，请通过安装和配置 Kerberized 网络服务和应用程序在端点上启用 SSO 功能。

因为系统间的配置不同，强烈建议您先执行以下操作，然后再在端点上启用 Kerberos 和 SSO：

- 阅读系统手册页以及计划用于 SSO 的本机应用程序服务二进制文件的版本特定选项，特别是以下内容：
  - sshd(1M)
  - telnetd
  - in.telnetd
  - inetd
  - pam.conf
  - inetd.sec
- 验证支持 Kerberos 的网络应用程序版本的 PATH 变量。 例如：在大多数的 Linux 系统上，Kerberos 工具位于 /usr/Kerberos 目录下。
- 确认下列支持 Kerberos 的应用程序配置如下：
  - SSH－支持凭据指派，例如：将 GSSAPIDelegateCredentials 标记设置为 yes
  - SSHD－支持并启用 GSSAPIAuthentication 标记
  - Telnet－在 Solaris 上，PAM 堆栈已配置，并且 Kerberos 配置和 keytab 文件可用。 创建符号链接或环境变量 KRB5_CONFIG 和 KRB5_KTNAME 可以使 keytab 文件可用
  - rlogin－安装支持 Kerberos 的应用程序版本。

注意：有关更多特定于系统的 Kerberos 和 SSO 配置，请参阅您的系统文档。

示例：在 Solaris 上配置 Kerberos

以下示例显示了在 Solaris 上配置 Kerberos 所需的配置。 在此示例中，您安装和配置 Solaris 程序包以启用 Kerberos。

重要说明！ 您可能需要安装和配置附加程序包才能配置要用于 Kerberos 的系统。

- 安装 SUNWcry 程序包以启用强加密
- 在 Solaris 10 上，SSH 不支持 GSSAPIDelegateCredentials
- 启用 svc:/network/shell:kshell、svc:/network/login:klogin、svc:/network/telnet:default 以使用 rsh、rlogin 和 telnet 服务
- 修改 /etc/pam.conf 文件以处理 Kerberos 身份验证。

下面是 /etc/pam.conf 文件的一个片段，显示了为 rlogin、rsh 和 telnet 启用 Kerberos 身份验证而添加的小节：

```
# Kerberized rlogin service
#
krlogin auth required           pam_unix_cred.so.1
krlogin auth required           pam_krb5.so.1
#
# rsh service (explicit because of pam_rhost_auth,
# and pam_unix_auth for meaningful pam_setcred)
#
rsh     auth sufficient         pam_rhosts_auth.so.1
rsh     auth required           pam_unix_cred.so.1
#
# Kerberized rsh service
#
krsh    auth required           pam_unix_cred.so.1
krsh    auth required           pam_krb5.so.1
#
# Kerberized telnet service
#
ktelnet auth required           pam_unix_cred.so.1
ktelnet auth required           pam_krb5.so.1
```

UNAB 注册在启用了 Kerberos 的环境中的工作原理

当您在 Active Directory 中注册主机时，UNAB 会在与本地 Kerberos 相同的位置创建用户票单。 用户可以简单明了地继续使用 kerberized 应用程序，无需手动获得 Ticket Granting Ticket (TGT)。

启用了 Kerberos 的主机中的 UNAB 注册过程如下所示：

1. 您运行 uxconsole -register 命令并指定 -sso 参数，以在 Active Directory 中注册 UNAB。

   -sso 参数强制 uxconsole 使用主机 Kerberos 文件，而不是 uxauth.ini 文件。

2. uxconsole 确认 UNAB 可以使用主机 Kerberos 文件进行配置。 将发生以下情况之一：

   a. uxconsole 识别文件包含注册 UNAB 所需的域信息。

   b. uxconsole 识别文件不包含注册所需的信息。

3. 如果文件不包含此信息，UNAB 会创建原始文件的备份，并将 kerberos_configuration 标记设置为 internal。

   注意：如果您使用 uxconsole -deregister 命令从 Active Directory 中删除 UNAB，Kerberos 配置文件不会被修改，备份文件也不会被删除。

4. 如果文件包含必需的信息，uxconsole 会将 kerberos_configuration 标记设置为 standard。

5. uxconsole 继续进行注册过程。

   注意：有关 uxconsole -register 命令和 seos.ini kerberos_configuration 标记的详细信息，请参阅*《参考指南》*。

重要说明！ 如果主机上的 Kerberos 文件不包含注册 UNAB 所需的信息，注册将失败。

为 SSO 启用 UNAB 主机

您可以为 SSO 配置 UNAB 主机，以便登录到 UNAB 主机的 Active Directory 用户可以使用自己的用户名登录到另一个 UNAB 主机。 在启用了 SSO 的模式下，UNAB 会将生成的密钥保留在 UNIX 存储库中。 启用了 Kerberos 的应用程序会在用户登录到另一台主机时使用此密钥对用户进行身份验证。

重要说明！ 确认其 UNAB 启用了 SSO 模式的每个主机都启用了 Kerberos。 在开始此步骤之前，请使用 uxpreinstall 实用程序检查系统遵从性。

为 SSO 启用 UNAB 主机

1. 以 root 身份登录到 UNIX 主机。
2. 在 SSO 模式下将 UNAB 注册到 Active Directory。 运行以下命令：

   ```
   ./uxconsole -register -d<active_directory_domain> -sso
   ```

   注意：在 SSO 模式下注册 UNAB 之前，您不需要取消注册 UNAB。
3. 激活 UNAB，以便用户能够登录到 UNIX 主机。 运行以下命令：

   ```
   ./uxconsole -activate
   ```
4. 确认使用 -status -detail 参数将 Kerberos 模式设置为 Standard。 例如：

   ```
   ./uxconsole -status -detail | grep Kerberos

       Kerberos configuration - standard
   ```

   您已经为 SSO 配置了 UNAB 主机。

检查系统遵从性

uxpreinstall 实用程序会验证 UNIX 计算机是否符合 UNAB 系统要求。 在您启动和激活 UNAB 之前，强烈建议您使用 uxpreinstall 检查系统遵从性，并解决实用程序识别的任何错误或冲突。 解决这些错误有助于防止出现 UNAB 操作问题。

重要说明！ uxpreinstall 实用程序会通知您真实或潜在的问题，但不会更正这些问题。 您不能使用该实用程序配置操作系统或 UNAB。

您可以在安装 UNAB 之前或之后使用 uxpreinstall。 uxpreinstall 不会修改端点或 UNAB 安装，但会诊断可能的问题并针对这些问题建议解决方案。 uxpreinstall 识别的任何问题都是关于端点的问题，而非 uxpreinstall 的问题。

注意：要在安装 UNAB 之前运行 uxpreinstall，请从安装了 UNAB 的另一个端点复制实用程序。 有关 uxpreinstall 实用程序的详细信息，请参阅*《参考指南》*。

检查系统遵从性

1. 使用超级用户身份登录到 UNIX 计算机。
2. 使用详细级别 0 运行 uxpreinstall。

   uxpreinstall 将运行并显示所执行的检查以及识别的任何错误或冲突的摘要。
3. 如果 uxpreinstall 识别出任何错误或冲突，请使用详细级别 2 或更高级别再次运行 uxpreinstall。

   uxpreinstall 将显示关于所识别的错误和冲突的详细信息。
4. 解决错误和冲突。
5. 重复步骤 2-4，直到 uxpreinstall 识别不出任何错误或冲突。

   当 uxpreinstall 的输出不显示任何错误或冲突时，计算机即符合 UNAB 的要求。 您现在可以启动和激活 UNAB。

示例：运行 uxpreinstall 实用程序

此示例以管理员用户凭据使用详细级别 3 对 Active Directory 域 domain.com 运行 uxpreinstall 实用程序。

```
./uxpreinstall -a administrator -w admin -d domain.com -v 3
```

使用 Uxconsole 和 Microsoft 实用程序排除 Active Directory 问题故障

实施过程中，您可遇到 Active Directory 的各种问题，如注册和激活问题。 uxpreinstall 实用程序可帮助您收集、识别和评估所有有价值因素。要增强排除 Active Directory 故障的能力，您可以使用 Microsoft 的 dcdiag（域控制器诊断）和 netdiag （网络诊断）实用程序

重要说明！ 如果正在使用 Windows Server 2003，您可以在支持工具软件绑定中找到 dcdiag.exe 和 netdiag.exe 实用程序。 有关详细信息，请参阅 Microsoft 知识库文章：KB247811、KB265706、KB321708。

使用以下过程可排除 Active Directory 问题：

1. 使用详细级别 0 运行 uxpreinstall。

   uxpreinstall 将运行并显示所执行的检查以及识别的任何错误或冲突的摘要。

2. 如果 uxpreinstall 识别出任何错误或冲突，请使用详细级别 2 或更高级别再次运行 uxpreinstall。

   uxpreinstall 将显示关于所识别的错误和冲突的详细信息。

   注意：我们建议您在使用 -l （系统记录器检查）和 -k （单一登录预备检查）参数时，由于大量输出，要小心谨慎。

3. 要记录 uxpreinstall 输出，请运行 uxpreinstall -f。
4. 要记录 Microsoft dcdiag 实用程序输出，请运行 dcdiag /f。

   注意：netdiag 实用程序自动创建以下日志文件：NetDiag.log。

5. 查看日志文件失败，错误消息；或警告。 如果存在，使用更高详细级别运行 uxpreinstall 和 dcdiag 实用程序。
6. 重新查看日志文件，找到未成功完成的操作和警告消息。

   由于用户首选项，可将错误记录为警告，并不作为错误消息。

7. 运行 dcdiag /test:DNS /v /e 排除域控制器参数故障。
8. 查看输出，从日志文件的末开始。
9. 继续排除故障，直到您解决所有警告和错误消息。

示例：使用 dsquery 查询用户和组

以下示例向您显示如何使用 dsquery 实用程序为用户和组查询：

```
dsquery user -name user1
dsquery group -name grp1
dsquery * "CN=Users,DC=example,DC=com" -scope base -attr *
```

示例：使用 dnscmd 实用程序检索 DNS 设置

以下示例向您显示如何使用 dnscmd 检索 DNS 设置：

```
dnscmd /enumzones
dnscmd /zoneprint <zonename>
```

示例：使用 dsquery 实用程序发现 Active Directory 站点

以下示例向您显示如何使用 dsquery 实用程序发现 Active Directory 站点：

```
dsquery subnet –name 192.168.*
dsquery site -o dn
dsquery subnet -o rdn -site <mysite>
nltest /DSGETSITECOV
```

验证 UNIX 计算机名是否能够正确解析。

要使 UNAB 正常运行，UNIX 计算机和 Active Directory 计算机必须将 UNIX 计算机的 IP 地址解析为相同的计算机名，包括域名。

要验证 UNIX 计算机名是否能正确解析，请运行 uxpreinstall 实用程序。

示例：使用 uxpreinstall 实用程序验证 UNIX 计算机名是否能够正确解析

此示例展示：对于在 Windows、Active Directory 服务器和 UNIX 计算机上都名为 computer.caom 的计算机，在 Linux 上使用详细级别 3 运行 uxpreinstall 的结果：

```
正在域 <DOMAIN.COM> 中查找 Active Directory 服务
正在 DNS 中查找“_ldap._tcp.DOMAIN.COM.”记录 ...
computer.com:389 [100:0] (_ldap)
computer.com:389 [100:0] (_ldap)
找到 LDAP 服务:
   computer:389
正在对 <computer.com> 执行名称解析
正在运行命令“host computer.com” ...
   DNS 服务器回复:
      computer.com 的地址为 192.168.1.1
名称 <computer.com> 已解析为 IP 地址 <1192.168.1.1>
```

示例：使用 nslookup 命令验证 UNIX 计算机名是否正确解析

此示例展示，对于在 Windows、Active Directory 服务器和 UNIX 计算机上都名为 acctdept 的计算机，在 Linux 上发出转发 nslookup 解析命令的结果：

```
# nslookup acctdept
服务器:         172.24.789.0
地址:        172.24.789.0#53

名称:   acctdept.parallel.com
地址: 172.24.123.110
```

UNAB 安装参数文件－自定义 UNAB 安装

UNAB 参数文件包含可以根据要求进行自定义的安装参数。

此文件格式如下：

AUDIT_BK

指定是否要保留审核文件的带有时间戳的备份。

注意：如果要将审核数据发送到分发服务器，请将该值设置为 yes。如果将此值设置为 yes，CA Access Control 会在审核文档达到 audit_size 配置设置所指定的大小限制时备份该文件，并为文件添加时间戳记。 这样可以确保所有审核数据对于报告代理均可用。

限制：yes、no

默认值：no

COMPUTERS_CONTAINER

定义注册了 UNIX 计算机的 Active Directory 中的容器名称。

默认值：cn=Computers

DIST_SRV_HOST

指定分发服务器主机名。

限制：任何有效的主机名。

默认值：无

DIST_SRV_PORT

指定分发服务器端口号。

限制：SSL：7243，TCP：7222

默认值：7243

DIST_SRV_PROTOCOL

指定分发服务器通讯协议。

限制：：tcp、ssl

默认值：ssl

ENABLE_ELM

指定报告代理是否将端点审核数据发送到分发服务器。 这将允许您与 CA Enterprise Log Manager 集成。

注意：如果将该值设置为 yes，请设置 CA Access Control 来保留审核备份 (AUDIT_BK=yes)。

限制：yes、no

默认值：no

GROUP_CONTAINER

定义包含 UNIX 组定义的 Active Directory 容器的名称。

IGNORE_DC_LIST

指定在建立 LDAP 连接时，UNAB 忽略哪些 Active Directory 域控制器。

注意：您可以指定来自当前域和受信任域的域控制器。

限制：none，以逗号分隔的列表

默认值：none

IGNORE_DOMAIN_LIST

指定在查询用户和组时，UNAB 忽略哪些 Active Directory 域。

限制：none，UNAB 查询当前域和所有受信任域；all，UNAB 仅查询当前的域；以逗号分隔的要忽略的域的列表

默认值：none

IGNORE_USER_CONTAINER

指定搜索 Active Directory 时要忽略的用户容器。

容器由其可分辨名称 (DN) 定义，以分号分隔。 如果容器的 DN 不包含域名，它将应用于所有查询的域。

限制：以分号分隔的容器 DN 的列表，none

默认值：none

IGNORE_GROUP_CONTAINER

指定搜索 Active Directory 时要忽略的组容器。

容器由其可分辨名称 (DN) 定义，以分号分隔。 如果容器的 DN 不包含域名，它将应用于所有查询的域。

限制：以分号分隔的容器 DN 的列表，none

默认值：none

INTEGRATION_MODE

指定 UNAB 集成模式。

限制：1，部分集成；2，完全集成

默认值：2

JAVA_HOME

(Linux s390) 指定已安装的 Java 环境的完整路径名（取决于 Java 版本和操作系统）。

只有当 Java 环境未安装在默认位置中时才需要指定此参数。 如果 Java 环境安装在默认位置，安装程序会设置此参数的值。

LANG

指定安装语言。

LIC_CMD

指定接受许可的命令。

LOCAL_POLICY

指定登录策略用法选项。

限制：yes，使用 UNAB 策略和本地登录文件；no，仅使用 UNAB 登录策略。

默认值：no

LOOKUP_DC_LIST

指定要与其建立 LDAP 连接的 Active Directory 域控制器 (DC)。

注意：您可以指定来自当前域和受信任域的 DC。 如果要指定要使用的 DC，UNAB 会从 Active Directory 检索 DC 的列表。 如果您不指定要使用的 DC，UNAB 会发现最接近端点实际位置的 Active Directory 站点，并与所发现站点中的 DC 进行通讯。

限制：none，以逗号分隔的列表。

默认值：none

NTP_SRV

定义网络时间协议 (NTP) 服务器的名称或 IP 地址。

REPORT_SHARED_SECRET

指定报告代理用于验证分发服务器身份的共享密钥。

限制：任何有效的字符串。

默认值：无

注意：您必须指定在安装分发服务器时定义的相同共享密钥。

REPORT_SRV_QNAME

指定将快照发送到的队列的名称。

限制：表示队列名称的字符串。

默认值：queue/snapshots

REPORT_SRV_SCHEDULE

定义报告代理何时生成报告并将它们发送到分发服务器。

此标记使用以下格式：time@day[,day2] [...]

默认值：00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

SSO

指定 UNAB 是否支持基于 Kerberos 的单点登录 (SSO)

限制：yes、no

默认值：no

TIME_SYNCH

指定 UNAB 是否将系统时间与 NTP（网络时间协议）服务器同步。

注意：如果将此值设置为 yes，您必须为 NTP_SRV 标记指定值。 如果将此值设置为 no，UNAB 会将 /etc/ntp.conf 中定义的 UNIX 机制用于系统时间。

限制：yes、no

默认值：no

USER CONTAINER

定义包含 UNIX 用户定义的 Active Directory 容器名称。

UXACT_ADMINISTRATOR

定义 Active Directory 管理员的用户名。

UXACT_ADMIN_PASSWORD

定义 Active Directory 管理员的帐户密码。

UXACT_DOMAIN

定义 UNIX 计算机所属的域。

UXACT_RUN

指定是否在安装期间执行 uxconsole -register 命令。

限制： yes、no

默认值： no

注意： uxconsole -register 命令将 UNIX 计算机注册在 Active Directory 服务器的“计算机”容器下。

UXACT_RUN_AGENT

指定是否在安装过程结束时启动 UNAB 后台进程。

限制： yes、no

默认值： yes

UXACT_SERVER

输入 Active Directory 服务器的名称。

UXACT_VERB_LEVEL

定义详细级别。

限制： 0-7

使用 CA Access Control 企业管理 管理 UNAB

您可以使用 CA Access Control 企业管理 管理 UNAB 端点。 这样，您将可以通过“全局查看”查看 UNAB 端点，创建和分配登录和配置策略，以及解决在迁移过程中发现的冲突。 为了使用 CA Access Control 企业管理 管理 UNAB 端点，请将 UNAB 注册到 CA Access Control 企业管理。 自定义 UNAB 安装程序包以修改程序包参数。

注意： 在安装 UNAB 之前请完成此步骤。

使用 CA Access Control 企业管理 管理 UNAB

1. 将安装参数从 UNAB 程序包提取到临时文件。
2. 在文本编辑器中打开临时文件。
3. 为企业修改以下参数：

   DISTRIBUTION_SRV_HOST

   指定分发服务器主机名。

   限制： 任何有效的主机名。

   默认值： 无

DISTRIBUTION_SRV_PROTOCOL

指定分发服务器通讯协议。

限制：：tcp、ssl

默认值：ssl

DISTRIBUTION_SRV_PORT

指定分发服务器端口号。

限制：ssl：7243，tcp：7222

默认值：7243

4. 设置自定义程序包中的安装参数。
5. 使用自定义程序包安装 UNAB。

   UNAB 将使用自定义设置进行安装。
6. 使用 acuxchkey 实用程序设置在将企业管理服务器安装到 UNAB 主机过程中指定的消息队列密码。 例如：

   ```
   acuxchkey -t pwd "password"
   ```

   完成安装并在 UNAB 主机上设置了消息队列密码后，便可以使用 CA Access Control 企业管理 来管理 UNAB 端点。

   注意：有关 seaudit 实用程序的详细信息，请参阅 *《参考指南》*。

与 CA Access Control 的集成

如果您打算在同一端点上安装 UNAB 和 CA Access Control，可以利用一些 UNAB 功能在 CA Access Control 中显示特定于 UNAB 的信息。 例如：您可以在审核记录中显示企业用户名而不是 UNIX 帐户名称。 seos.ini 配置文件包含要将 UNAB 与 CA Access Control 集成时启用的标记。

重要说明！ 在将 UNAB 与 CA Access Control 集成前，请确认端点上安装了 CA Access Control 版本 r12.5 或更高版本。

[seosd] 部分的下列标记控制 UNAB 与 CA Access Control 的集成：

use_unab_db

指定 seosd 使用 UNAB 数据库解析用户和组名称。 此标记使 CA Access Control 可以检测 UNAB 中的更改，如新用户登录。

use_mapped_user_name

指定 seosd 是否在审核记录中使用用户企业名称。启用时，seaudit 实用程序将显示企业用户名，而不是 UNIX 帐户名称。

[OS_User] 部分的下列标记控制 UNAB 与 CA Access Control 的集成：

nonunix_unabgroup_enabled

指定 CA Access Control 是否支持 UNAB 数据中的非 UNIX 用户组。 启用时，CA Access Control 将支持来自非 UNIX 组的用户。

osuser_enabled

指定是否启用企业用户和组。

[seos] 部分的下列标记控制 UNAB 与 CA Access Control 的集成：

auth_login

确定登录授权方法。 此标记使密码检查可以验证用户的身份，例如：sesudo、sesu 和 sepass。

pam_enabled

指定本地主机是否允许使用 PAM 在 LDAP 数据库中进行身份验证和密码更改。

[passwd] 部分的下列标记控制 UNAB 与 CA Access Control 的集成：

nis_env

指定本地主机是 NIS 客户端还是 NIS+ 客户端。

change_pam

指定本地主机是否使用 PAM 在 LDAP 数据库中进行密码验证和更改。使用此标记可以使 sepass 与外部 pam 存储配合使用，例如：UNAB。

[pam_seos] 部分的下列标记控制 UNAB 与 CA Access Control 的集成：

PamPassUserInfo

指定 pam_seos 是否将用户信息发送到 seosd。

pam_login_events_enabled

指定 pam_seos 是否将登录事件发送到 seosd。

pam_surrogate_events_enabled

指定 pam_seos 是否将代理事件发送到 seosd。

注意：有关 seos.ini 标记的详细信息，请参阅 *《参考指南》*。

与 RSA SecurID 的集成

如果您的组织使用 RSA SecurID 对用户进行身份验证，您可以使用 RSA SecurID 的功能对登录 UNAB 端点的用户进行身份验证。 您可以在安装有 RSA SecurID 客户端的主机上安装 UNAB，并在 Active Directory 中管理用户登录策略。

如果 UNAB 运行在安装有 RSA SecurID 的主机上，它将不会在登录时对用户进行身份验证。 UNAB 会检测到用户身份验证是由第三方程序完成的。 随后，UNAB 便可以管理端点上的用户活动，例如：实施本地和企业安全策略并生成审核消息。

UNAB 如何与 RSA SecurID 集成

UNAB 利用 PAM 堆栈功能来与 RSA SecurID 集成。 PAM 堆栈功能允许您设置在登录过程中使用哪个身份验证程序进行用户身份验证以及身份验证发生的顺序。

以下过程说明了 UNAB 与 RSA SecurID 的集成：

1. 在安装有 RSA SecurID 客户端的端点上安装 UNAB。
2. 按照您希望的用户身份验证顺序配置 PAM 堆栈。 例如：将 PAM 堆栈配置为调用 RSA SecurID 对用户通行码和 PIN 码进行身份验证，如果不成功，则使用 UNAB 对用户的 Active Directory 凭据进行身份验证。
3. 当用户尝试登录到 UNAB 主机时，会发生以下情况：

   使用 RSA SecurID 身份验证和 UNAB 身份验证：

   a. RSA SecurID 提示用户输入通行码和 PIN 码。
   b. 用户输入通行码和 PIN 码。
   c. RSA SecurID 尝试对用户通行码和 PIN 码进行身份验证。 随后出现下列情况：
      - RSA SecurID 验证用户通行码和 PIN 码有效并允许用户登录。此时，身份验证过程结束，用户帐户管理过程开始。
      - RSA SecurId 拒绝用户通行码或 PIN 码。
      - UNAB 提示用户输入 Active Directory 用户帐户或本地帐户凭据。
      - UNAB 尝试对用户凭据进行身份验证，如果通过验证，身份验证过程将结束，用户帐户管理过程将开始。

示例：在 Red Hat Advanced Server 5.3 中使用 RSA SecurID 身份验证

来自 /etc/pam.d/system-auth 文件的以下片段指示 Red Hat Linux Advanced Server 5.3 的用户身份验证仅使用 RSA SecurID 完成：

```
auth required pam_securid.so
```

示例：在 Red Hat Linux Advanced Server 5.3 中使用 RSA SecurID、本地 UNIX 和 UNAB 身份验证

来自 /etc/pam.d/system-auth 文件的以下片段指示 Red Hat Linux Advanced Server 5.3 的用户身份验证使用 RSA SecurID、本地 UNIX 和 UNAB 完成：

```
auth sufficient   pam_securid.so
auth sufficient   pam_unix.so
auth sufficient   pam_uxauth.so
```

在此示例中，/etc/pam.d/system-auth 文件配置为调用 RSA SecurID (pam_securid.so) 模块尝试对用户凭据进行身份验证。 如果不成功，本地的 UNIX PAM 模块 (pam_unix.so) 会尝试对用户凭据进行身份验证。 如果还不成功，UNAB PAM 堆栈模块 (pam_uxauth.so) 会尝试对用户凭据进行身份验证。 在此示例中，当 UNAB PAM 模块尝试对用户凭据进行身份验证时，UNAB 不会提示用户输入密码。 本地 UNIX PAM 模块会为 UNAB PAM 堆栈模块提供密码。

注意：身份验证过程可以任何一个 PAM 堆栈模块结束。

示例：在 Red Hat Advanced Server 5.3 中使用 UNAB 身份验证和 RSA SecurID 身份验证

来自 /etc/pam.d/system-auth 文件的以下片段指示 Red Hat Linux Advanced Server 5.3 的用户身份验证使用 UNAB 身份验证和 RSA SecurID 身份验证完成：

```
auth optional     pam_unix.so
auth sufficient   pam_uxauth.so
auth sufficient   pam_securid.so
```

在此示例中，/etc/pam.d/system-auth 文件配置为首先使用 UNAB PAM 堆栈 (pam_uxauthd.so) 尝试对用户 Active Directory 凭据进行身份验证，然后使用 RSA SecurID PAM 堆栈 (pam_securid.so) 对用户通行码进行身份验证。 本地 UNIX PAM 堆栈模块 (pam_unix.so) 设置为可选。 这表明本地 UNIX PAM 堆栈不会对用户进行身份验证，而是会提示用户输入密码，然后将密码转发给 PAM 堆栈。

注意：在此示例中，身份验证过程可以 RSA SecurID 或以 UNAB 结束（不使用本地 UNIX 身份验证）。

RPM 软件包管理器的安装

RPM 软件包管理器 (RPM) 是一个命令行实用程序，使用它可以构建、安装、查询、验证、更新和删除各个软件程序包。 此程序用于 Linux 平台。

注意：有关详细信息，请参阅 RPM 软件包管理器网站 http://www.rpm.org 以及有关 RPM 的 UNIX 手册页。

您可以使用 CA Access Control 为 UNAB 提供的 RPM 软件包，以使用 RPM 管理您的 UNAB 安装和所有其他软件安装。

安装 UNAB RPM 软件包

要使用 Active Directory 用户帐户登录到 UNIX 计算机，您需要在要访问的每个 UNIX 计算机上安装 UNAB。 您可以使用 UNAB RPM 软件包在 Linux 计算机上安装 UNAB。

安装 UNAB RPM 软件包

1. 以 root 身份登录到 Linux 计算机。
2. 从 CA Access Control Endpoint Components for UNIX DVD 的 /UNAB 目录下将适用于服务器平台的压缩 tar 文件复制到文件系统上的临时位置。

   在文件系统上的读取/写入位置上，可以根据需要自定义程序包。 tar 压缩文件中包含 UNAB 程序包和安装文件。
3. 导航到临时目录，解压缩并提取 tar 压缩文件中的内容。 例如：以下命令解压缩名为 _LINUX_Ux_PKG_125.tar.Z 的文件并从中提取内容：

   ```
   gunzip _LINUX_Ux_PKG_125.tar.Z
   tar xvf _LINUX_Ux_PKG_125.tar
   ```
4. 使用 rpm 命令安装 ca-lic 程序包。 ca-lic 是 CA Technologies 许可程序，是安装所有其他程序包的先决条件。 例如：

   ```
   rpm -U ca-lic-0.0080-04.i386.rpm
   ```

   将安装 ca-lic 程序包。
5. 自定义 UNAB 程序包 (p. 264)。

   您必须自定义程序包，以使用可在许可协议中找到的关键字指定自己接受该许可协议。 您也可以自定义程序包以指定自定义安装设置。

6. 使用 rpm 命令安装 UNAB 程序包。 例如：

   ```
   rpm -U uxauth-125-3.0.1517.i386.rpm
   ```

   安装过程将开始。

   系统会显示一条消息，通知您安装过程已成功完成。

   注意：UNAB 软件包也安装 CAWIN 共享组件。

7. 有关安装过程的详细信息，请查看安装日志文件 uxauth_install.log。

   您可以在以下默认位置的 UNAB 安装目录中找到该日志文件：

   ```
   /opt/CA/uxauth
   ```

8. 验证安装是否已成功完成 (p. 267)。

自定义 UNAB RPM 软件包

在可以安装 UNAB 之前，您必须自定义 RPM 软件包以指定您接受许可协议。 在自定义程序包时，您还可以指定自定义安装设置。

建议您不要手动修改程序包。 而应该按照说明使用 customize_uxauth_rpm 脚本。 要构建自定义 UNAB rpm 安装程序包，您的计算机上必须安装 rpmbuild 实用程序。

自定义 UNAB 程序包

1. 如果您尚未完成此任务，请执行以下操作：

   a. 从 CA Access Control Endpoint Components for UNIX DVD 的 /UNAB 目录下将适用于服务器平台的压缩 tar 文件复制到文件系统上的临时位置。

      在文件系统上的读取/写入位置上，可以根据需要自定义程序包。

   b. 导航到临时目录，解压缩并提取 tar 压缩文件中的内容。

      tar 压缩文件中包含 UNAB 安装文件。

2. 输入以下命令从安装程序包中提取 uxpreinstall 实用程序：

   ```
   customize_uxauth_rpm -e uxpreinstall -f tmp_params [-d pkg_location] pkg_filename
   ```

   在安装 UNAB 之前，请使用 uxpreinstall 实用程序检查系统遵从性。

3. （可选）输入以下命令设置安装参数文件的语言：

   ```
   customize_uxauth_rpm -r -l lang [-d pkg_location] pkg_filename
   ```

4. 输入以下命令显示许可协议：

   ```
   customize_uxauth_rpm -a [-d pkg_location] pkg_filename
   ```

5. 记录许可协议结尾处方括号中出现的关键字。

   您需要在下一步中指定该关键字。

6. 输入下面的命令：

   ```
   customize_uxauth_rpm -w keyword [-d pkg_location] pkg_filename
   ```

   此命令将指定您接受该许可协议。

7. 输入以下命令获得安装参数文件：

   ```
   customize_uxauth_rpm -g -f tmp_params [-d pkg_location] pkg_filename
   ```

8. 编辑安装参数文件以适合安装要求 (p. 254)。

   通过该文件，您可以设置程序包的安装默认值。

9. 输入下面的命令：

   ```
   customize_uxauth_rpm -s -f tmp_params [-d pkg_location] pkg_filename
   ```

   此命令将设置自定义程序包中的安装参数。

   现在您将可以使用程序包以自定义的默认值安装 UNAB。

示例：自定义 UNAB RPM 软件包

以下示例显示了如何自定义位于 /unab_tmp 目录的名为 uxauth-125-3.0.1517.i386.rpm 的 UNAB RPM 软件包。

- 下面的示例显示许可协议和关键字：

  ```
  ./customize_uxauth_rpm -a /unab_tmp/uxauth-125-3.0.1517.i386.rpm
  ```

- 下面的示例接受许可协议。 示例中的关键字是 agreement：

  ```
  ./customize_uxauth_rpm -w agreement /unab_tmp/uxauth-125-3.0.1517.i386.rpm
  ```

- 下面的示例获取安装参数文件，并将其放置在同一目录的 parameters.txt 文件中：

  ```
  ./customize_uxauth_rpm -g -f parameters.txt
  /unab_tmp/uxauth-125-3.0.1517.i386.rpm
  ```

- 下面的示例在 parameters.txt 文件中的参数中设置安装参数：

  ```
  ./customize_uxauth_rpm -s -f parameters.txt
  /unab_tmp/uxauth-125-3.0.1517.i386.rpm
  ```

customize_uxauth_rpm 命令－自定义 UNAB RPM 软件包

customize_uxauth_rpm 命令运行 UNAB RPM 软件包自定义脚本。

注意：要自定义程序包，程序包必须位于您文件系统上的读取/写入目录。

此命令格式如下：

```
customize_uxauth_rpm -h [-l]
customize_uxauth_rpm -a [-d pkg_location] pkg_filename
customize_uxauth_rpm -w keyword [-d pkg_location] pkg_filename
customize_uxauth_rpm -r [-d pkg_location] [-l lang] pkg_filename
customize_uxauth_rpm -s -f tmp_params [-d pkg_location] pkg_filename
customize_uxauth_rpm -g [-f tmp_params] [-d pkg_location] pkg_filename
customize_uxauth_rpm -e uxpreinstall [-f tmp_params] [-d pkgdir] [pgn_name]
customize_uxauth_rpm -t tmp_dir [-d pkg_location] pkg_filename
```

pkg_filename

定义要自定义的 UNAB 程序包的文件名称。

注意：如果您未指定 -d 选项，则必须定义程序包文件的完整路径名。

-a

显示许可协议。

-e uxpreinstall

指定从安装程序包中抽取 uxpreinstall 实用程序。

-w 关键字

定义用于指定您接受许可协议的关键字。 您可以在许可协议的结尾处找到此关键字（在方括号内）。要找到许可协议文件，请使用 -a 选项。

-d *pkg_location*

（可选）指定文件系统上程序包所在目录。 如果您未指定程序包所在的目录，脚本将假定程序包文件的完整路径名包含在 *pkg_filename* 中。

-f *tmp_params*

指定要创建的或要从中检索信息的安装参数文件的完整路径和名称。

注意：如果您使用 -g 选项时未指定文件，则安装参数将使用标准输出 (stdout)。

--g

获取安装参数文件并将其置于由 -f 选项指定的文件中。

-h

显示命令用法。 与 -l 选项联合使用时，可显示受支持语言的语言代码。

-l *lang*

将安装参数文件的语言设置为 *lang*。您只能与 -r 选项一起设置语言。

注意：要获得可以指定的受支持语言代码的列表，请运行 customize_uxauth_rpm -l -h。 默认情况下，安装参数文件使用英语。

--r

重置程序包，以使用原始程序包中的默认值。

-s

将指定程序包设置为通过自定义安装参数文件（由 -f 选项指定）的输入。

-t *tmp_dir*

设置安装操作的临时目录。

注意：默认的临时目录是 /tmp。

验证安装是否已成功完成

在完成安装 UNAB 后，您应当验证安装是否已成功完成。

要验证安装是否已成功完成，请输入以下命令：

```
rpm -q unab_package_name
```

unab_package_name

定义 UNAB 本地程序包的名称。

如果您成功安装了 UNAB，会显示一条消息，通知您该程序包已安装。

示例：验证安装是否已成功完成

以下示例验证名为 uxauth 的 UNAB 本地程序包的安装是否已成功完成：

```
rpm -q uxauth
```

升级 UNAB RPM 软件包

如果已安装了 UNAB 的某个现有版本并想安装新版本，您可以升级 UNAB 的现有版本，而无需删除已安装的版本。 您可以使用 UNAB RPM 软件包在 Linux 计算机升级 UNAB。

注意：您不需要手动升级 ca-lic。

升级 UNAB RPM 软件包

1. 以 root 身份登录到 Linux 计算机。
2. 从 CA Access Control Endpoint Components for UNIX DVD 的 /UNAB 目录下将适用于服务器平台的压缩 tar 文件复制到文件系统上的临时位置。

   tar 压缩文件中包含安装和升级文件。
3. 导航到临时目录，解压缩并提取压缩文件中的内容。 例如：以下命令解压缩名为 _LINUX_Ux_PKG_125.tar.Z 的文件：

   ```
   unzip _LINUX_Ux_PKG_125.tar.Z
   tar xvf _LINUX_Ux_PKG_125.tar
   ```

   压缩程序包中包含 UNAB 的安装和升级文件。
4. 使用 rpm 命令升级 UNAB。 例如：

   ```
   rpm -U uxauth-125-3.0.1517.i386.rpm --verbose
   ```

   升级过程将开始。

   系统会显示一条消息，通知您升级过程已成功完成。

卸载 UNAB RPM 软件包

要卸载 UNAB，您需要从安装 RPM 软件包的 UNIX 计算机中删除该程序包。

要卸载 UNAB，请以 root 身份登录并输入以下命令：

```
rpm -e unab_package_name
```

unab_package_name

定义 UNAB 本地程序包的名称。

卸载过程将开始。

系统会显示一条消息，通知您该过程已成功完成。

Solaris 本地程序包安装

Solaris 本地程序包以命令行实用程序的形式提供，用于创建、安装、删除各个软件程序包和对其进行报告。

注意：有关 Solaris 本地程序包的详细信息，请参阅 Sun Microsystems 网站和有关 pkgadd、pkgrm、pkginfo 和 pkgchk 的手册页。

重要说明！ 程序包安装后，如果要卸载 UNAB，您必须使用 *pkgrm* 命令。

自定义 UNAB Solaris 本地程序包

在使用 Solaris 本地程序包安装 UNAB 之前，请自定义安装程序包并接受许可协议。 在自定义程序包时，您还可以指定自定义安装设置。

按照此过程中的步骤自定义任何 UNAB 程序包。 建议您不要手动修改程序包， 而应该按照说明使用 customize_uxauth_pkg 脚本。

自定义 Solaris 本地程序包

1. 从 CA Access Control Endpoint Components for UNIX DVD 的 /UNAB 目录中将要自定义的程序包提取到文件系统中的临时位置。

   在文件系统上的读取/写入位置上，可以根据需要自定义程序包。

   重要说明！ 在提取程序包时，必须验证是否保留了程序包整个目录结构的文件属性，否则 Solaris 本地程序包工具会认为该程序包已损坏。

2. （可选）将 customize_uxauth_pkg 脚本文件和 pre.tar 文件复制到文件系统上的临时位置。

   将 pre.tar 文件与脚本文件放置在同一目录中，以接收所有语言的脚本消息。 pre.tar 文件是 tar 压缩文件，其中包含安装消息和 UNAB 许可协议。

   注意：您可以在提取程序包的位置同时找到 customize_uxauth_pkg 脚本文件和 pre.tar 文件。

3. 输入以下命令从安装程序包中提取 uxpreinstall 实用程序：

   ```
   customize_uxauth_pkg -e uxpreinstall -f tmp_params [-d pkg_location]
   [pkg_name]
   ```

   在安装 UNAB 之前，请使用 uxpreinstall 检查系统遵从性。

4. （可选）输入以下命令：

   `customize_uxauth_pkg -r -l lang [-d pkg_location] [pkg_name]`

   将设置安装参数文件的语言。

5. 输入下面的命令：

   `customize_uxauth_pkg -a [-d pkg_location] pkg_name`

   此命令将显示许可协议。

6. 记录许可协议结尾处方括号中出现的关键字。

   您需要在下一步中指定该关键字。

7. 输入下面的命令：

   `customize_uxauth_pkg -w keyword [-d pkg_location] [pkg_name]`

   此命令将指定您接受该许可协议。

8. （可选）输入以下命令：

   `customize_uxauth_pkg -i install_loc [-d pkg_location] [pkg_name]`

   此命令将更改安装目录。

9. 输入以下命令获得安装参数文件：

   `customize_uxauth_pkg -g -f tmp_params [-d pkg_location] [pkg_name]`

10. 编辑安装参数文件以适合安装要求。 (p. 254)

    通过该文件，您可以设置程序包的安装默认值。

11. 输入以下命令设置自定义程序包中的安装参数：

    `customize_uxauth_pkg -s -f tmp_params [-d pkg_location] [pkg_name]`

    现在您将可以使用程序包以自定义的默认值安装 UNAB。

customize_uxauth_pkg 命令—自定义 Solaris 本地程序包

customize_uxauth_pkg 命令运行 UNAB Solaris 本地程序包自定义脚本。

使用此命令时应考虑以下内容：

- 该脚本适用于所有可用的 UNAB Solaris 本地程序包。
- 要自定义程序包，程序包必须位于您文件系统上的读取/写入目录。
- 要获得本地化的脚本消息，您需要将 pre.tar 文件与脚本文件置于同一目录中。

此命令格式如下：

```
customize_uxauth_pkg -h [-l]
customize_uxauth_pkg -a [-d pkg_location] [pkg_name]
customize_uxauth_pkg -w command [-d pkg_location] [pkg_name]
customize_uxauth_pkg -r [-d pkg_location] [-l lang] [pkg_name]
customize_uxauth_pkg -i install_loc [-d pkg_location] [pkg_name]
customize_uxauth_pkg -s -f tmp_params [-d pkg_location] [pkg_name]
customize_uxauth_pkg -g [-f tmp_params] [-d pkg_location] [pkg_name]
customize_uxauth_pkg -e uxpreinstall [-f tmp_params] [-d pkg_location] [pkg_name]
customize_uxauth_pkg -t tmp_dir [-d pkg_location] [pkg_name]
```

pkg_name

（可选）要自定义的 UNAB 程序包的名称。 如果不指定程序包，脚本将默认使用 UNAB 主程序包 (uxauth)。

-a

显示许可协议。

-e uxpreinstall

指定从安装程序包中抽取 uxpreinstall 实用程序。

-w 关键字

定义用于指定您接受许可协议的关键字。 您可以在许可协议的结尾处找到此关键字（在方括号内）。要找到许可协议文件，请使用 -a 选项。

-l *lang*

将安装参数文件的语言设置为 *lang*。您只能与 -r 选项一起设置语言。

注意：有关可以指定的受支持语言代码的列表，请使用 -h 选项运行 -l。 默认情况下，安装参数文件使用英语。

-d *pkg_location*

（可选）指定文件系统上程序包所在目录。 如果您未指定程序包所在目录，脚本将默认使用 /var/spool/pkg。

-f *tmp_params*

指定要创建的或要从中检索信息的安装参数文件的完整路径和名称。

注意：如果您使用 -g 选项时未指定文件，则安装参数将使用标准输出 (stdout)。

--g

获取安装参数文件并将其置于由 -f 选项指定的文件中。

-h

显示命令用法。 与 -l 选项联合使用时，可显示受支持语言的语言代码。

-i *install_loc*

将程序包的安装目录设置为 *install_loc*/uxauth。

--r

重置程序包，以使用原始程序包中的默认值。

-s

将指定程序包设置为通过自定义安装参数文件（由 -f 选项指定）的输入。

-t *tmp_dir*

设置安装操作的临时目录。

注意：默认的临时目录是 /tmp。

安装 UNAB Solaris 本地程序包

利用 UNAB Solaris 本地程序包，您可以在 Solaris 中轻松地安装 UNAB。

注意：以下过程使用默认设置安装 UNAB。 在安装 UNAB 程序包之前，您可以自定义该程序包。

安装 UNAB Solaris 本地程序包

1. （可选）配置 Solaris 本地安装默认值：
   a. 输入下面的命令：

      ```
      convert_uxauth_pkg -p
      ```

      将安装管理文件复制当前位置并命名为 *myadmin*。

      可以编辑安装管理文件以更改 pkgadd 安装默认值。 然后，您可以使用修改过的文件进行特定安装，如使用 pkgadd -a 选项安装 UNAB。 但是，此文件并不特定于 UNAB。

   b. 根据需要编辑安装管理文件 (myadmin)，然后保存该文件。

      现在您将可以使用修改过的安装设置进行 UNAB 本地安装，而不会影响其他安装。

   注意：默认情况下，Solaris 本地程序包可能需要用户参与。 有关安装管理文件及其使用方法的详细信息，请参阅有关 pkgadd(1M) 和 admin(4) 的 Solaris 手册页。

2. 输入下面的命令：

   pkgadd [-a *dir*/myadmin] -d *pkg_location* uxauth

   -a *dir*/myadmin

   定义您在步骤 1 中创建的 myadmin 安装管理文件的位置。

   如果未指定此选项，pkgadd 将使用默认的安装管理文件。

   pkg_location

   定义 UNAB 程序包 (uxauth) 所在的目录。

   重要说明！ 程序包必须位于公共位置（即对组和全局而言有读取权限）。 例如：/var/spool/pkg

   注意：您可以在 CA Access Control Endpoint Components for UNIX DVD 的 UNAB 目录中找到 Solaris 本地程序包。

   至此，UNAB 便已完全安装，但尚未启动。

将 UNAB Solaris 本地程序包安装到选定区域

您可以使用 Solaris 本地程序包将 UNAB 安装到选定区域。 但是，您也必须将 UNAB 安装到全局区域。

注意：建议您使用 Solaris 本地程序包将 UNAB 安装到*所有*区域。

将 UNAB 安装到选定区域

重要说明！ 请确保您在所有区域中都使用同一 UNAB 版本。

1. 在全局区域中，输入以下命令：

   pkgadd -G -d *pkg_location* uxauth

   pkg_location

   定义 UNAB 程序包 (uxauth) 所在的目录。

   重要说明！ 程序包必须位于公共位置（即对组和全局而言有读取权限）。 例如：/var/spool/pkg

   此命令仅将 UNAB 安装到全局区域。

2. 在每个要安装 UNAB 的非全局区域中，执行以下操作：

   a. 将 uxauth 程序包复制到非全局区域的临时位置。

   b. 在非全局区域中输入以下命令：

      pkgadd -G -d *pkg_location* uxauth

      此命令将 UNAB（使用您在步骤 1 中复制的程序包）安装到您当前操作所在的非全局区域。

   现在您将可以在内部区域启动 UNAB。

注意：您必须将 UNAB 从所有非全局区域中卸载后，才能将其从全局区域中删除。

在 Solaris 上升级 UNAB

利用 UNAB Solaris 本地程序包，您可以将 Solaris 上的现有 UNAB 版本升级到更新的 UNAB 版本。

在 Solaris 上升级 UNAB

1. 停止所有 UNAB 后台进程。
2. （可选）配置 Solaris 本地安装默认值：
   a. 输入下面的命令：

      ```
      convert_uxauth_pkg -p
      ```

      将安装管理文件复制当前位置并命名为 *myadmin*。

      可以编辑安装管理文件以更改 pkgadd 安装默认值。 然后，您可以使用修改过的文件进行特定安装，如使用 pkgadd -a 选项安装 UNAB。 但是，此文件并不特定于 UNAB。

   b. 根据需要编辑安装管理文件 (myadmin)，然后保存该文件。

      现在您将可以使用修改过的安装设置进行 UNAB 本地安装，而不会影响其他安装。

   注意：默认情况下，Solaris 本地程序包可能需要用户参与。 有关安装管理文件及其使用方法的详细信息，请参阅有关 pkgadd(1M) 和 admin(4) 的 Solaris 手册页。
3. 输入下面的命令：

   ```
   pkgadd [-a dir/myadmin] -v -d . UNAB
   ```

   -a *dir*/myadmin

   定义您在步骤 1 中创建的 myadmin 安装管理文件的位置。

   如果未指定此选项，pkgadd 将使用默认的安装管理文件。

   UNAB

   定义 UNAB 本地程序包的名称。

   注意：如果之前版本的 UNAB 的安装目录不是默认目录，请运行以下命令指定 UNAB 目录的完整路径：

   ```
   ./customize_eac_pkg -i previous-path -d ./ CAeAC
   ```

   -i *Previous-path*

   定义现有 UNAB 目录的完整路径。

   注意：请确认完整路径名的结尾不包含斜线字符 (/)。

   至此，UNAB 的新版本便已安装，但尚未启动。

卸载 UNAB Solaris 本地程序包

要卸载安装的 UNAB Solaris 程序包，请卸载 UNAB 程序包。

要卸载 UNAB 主程序包，请输入以下命令：

pkgrm *unab_package_name*

unab_package_name

定义 UNAB 本地程序包的名称。

UNAB 将从计算机中删除。

HP-UX 本地程序包安装

HP-UX 本地程序包以一系列 GUI 和命令行实用程序的形式提供，用于创建、安装、删除各个软件程序包和对其进行报告。 通过 HP-UX 本地程序包，还可以在远程计算机上安装软件程序包。

注意：有关 HP-UX 本地程序包及 Software Distributor-UX (SD-UX) 的详细信息，请参阅 HP 网站 http://www.hp.com。 您还可以参阅有关 swreg、swinstall、swpackage 和 swverify 的手册页。

重要说明！ 程序包安装后，如果要卸载 UNAB，您必须使用 *swremove* 命令。

自定义 UNAB SD-UX 格式程序包

在使用本地程序包安装 UNAB 之前，您必须自定义 UNAB 程序包并接受许可协议。 在自定义程序包时，您还可以指定自定义安装设置。

建议您不要手动修改程序包。 您应当按照以下步骤中的说明，使用脚本自定义 UNAB 程序包。

您可以在 CA Access Control Endpoint Components for UNIX DVD 的 UNAB 目录中找到适用于每个受支持的 HP-UX 操作系统的 Software Distributor-UX (SD-UX) 格式程序包。

自定义 SD-UX 格式程序包

1. 将要自定义的程序包提取到文件系统上的临时位置。

   在文件系统上的读取/写入位置上，可以根据需要自定义程序包。

   重要说明！ 在提取程序包时，必须确保程序包整个目录结构的文件属性已保留，否则 HP-UX 本地程序包工具会认为该程序包已损坏。

2. 将 customize_uxauth_depot 脚本文件和 pre.tar 文件复制到文件系统上的临时位置。

   pre.tar 文件是 tar 压缩文件，其中包含安装消息和 UNAB 许可协议。

   注意：您可以在以下目录中找到 customize_uxauth_depot 脚本文件和 pre.tar 文件：

   ```
   /uxauth/FILESET/opt/CA/uxauth/lbin
   ```

3. 输入以下命令从安装程序包中提取 uxpreinstall 实用程序：

   ```
   customize_exauth_depot -e uxpreinstall -f tmp_params [-d pkg_location] [pkg_name]
   ```

   在安装 UNAB 之前，请使用 uxpreinstall 检查系统遵从性。

4. 输入下面的命令：

   ```
   customize_uxauth_depot -a [-d pkg_location] [pkg_name]
   ```

   此命令将显示许可协议。

5. 记录许可协议结尾处方括号中出现的关键字。

   您需要在下一步中指定该关键字。

6. 输入下面的命令：

   ```
   customize_uxauth_depot -w keyword [-d pkg_location] [pkg_name]
   ```

   此命令将指定您接受该许可协议。

7. （可选）输入以下命令：

   ```
   customize_uxauth_depot -r -l lang [-d pkg_location] [pkg_name]
   ```

   此命令将设置安装参数文件的语言

8. （可选）输入以下命令：

   ```
   customize_uxauth_depot -i install_loc [-d pkg_location] [pkg_name]
   ```

   此命令将更改安装目录。

9. （可选）输入以下命令获得安装参数文件：

   ```
   customize_uxauth_depot -g -f tmp_params [-d pkg_location] [pkg_name]
   ```

10. （可选）编辑安装参数文件以适合您的安装要求 (p. 254)。

    通过该文件，您可以设置程序包的安装默认值。

11. （可选）输入以下命令：

    ```
    customize_uxauth_depot -s -f tmp_params [-d pkg_location] [pkg_name]
    ```

    此命令将设置自定义程序包中的安装参数。

    现在您将可以使用程序包以自定义的默认值安装 UNAB。

示例：指定您接受许可协议

要在安装本地程序包时接受许可协议，您需要自定义该程序包。 以下示例显示了如何自定义 x86 UNAB SD-UX 程序包以接受许可协议（您可以在程序包文件所提取到的目录中找到该程序包）：

```
cp /mnt/AC_DVD/UNAB/_HPUX11_Ux_PKG_1*.tar.Z /tmp
cd /tmp
zcat _HPUX11_Ux_PKG_1*.tar.Z | tar -xvf -
/uxauth/FILESET/opt/CA/uxauth/lbin/customize_eac_depot -w keyword -d /tmp uxauth
```

您现在将可以使用 /tmp 目录中的自定义程序包安装 UNAB。

更多信息：

customize_eac_depot 命令－自定义 SD-UX 格式程序包 (p. 204)

customize_uxauth_depot 命令－自定义 SD-UX 格式程序包

customize_uxauth_depot 命令对 SD-UX 格式程序包运行 UNAB 本地程序包自定义脚本。

使用此命令时应考虑以下内容：

- 该脚本适用于所有可用的 UNAB HP-UX 本地程序包。
- 要自定义程序包，程序包必须位于您文件系统上的读取/写入目录。
- 要获得本地化的脚本消息，您需要将 pre.tar 文件与脚本文件置于同一目录中。

此命令格式如下：

```
customize_uxauth_depot -h [-l]
customize_uxauth_depot -a [-d pkg_location] [pkg_name]
customize_uxauth_depot -w keyword [-d pkg_location] [pkg_name]
customize_uxauth_depot -r [-l lang] [-d pkg_location] [pkg_name]
customize_uxauth_depot -i install_loc [-d pkg_location] [pkg_name]
customize_uxauth_depot -s -f tmp_params [-d pkg_location] [pkg_name]
customize_uxauth_depot -e uxpreinstall [-f tmp_params] [-d pkg_location]
[pkg_name]
customize_uxauth_depot -g [-f tmp_params] [-d pkg_location] [pkg_name]
```

pkg_name

（可选）要自定义的 UNAB 程序包的名称。 如果不指定程序包，脚本将默认使用 UNAB 主程序包 (uxauth)。

-a

显示许可协议。

-e uxpreinstall

指定从安装程序包中抽取 uxpreinstall 实用程序。

-d *pkg_location*

（可选）指定文件系统上程序包所在目录。 如果您未指定程序包所在目录，脚本将默认使用 /var/spool/pkg。

-f *tmp_params*

指定要创建的或要从中检索信息的安装参数文件的完整路径和名称。

注意：如果您使用 -g 选项时未指定文件，则安装参数将使用标准输出 (stdout)。

--g

获取安装参数文件并将其置于由 -f 选项指定的文件中。

-h

显示命令用法。 与 -l 选项联合使用时，可显示受支持语言的语言代码。

-i *install_loc*

将程序包的安装目录设置为 *install_loc*/uxauth。

-l *lang*

将安装参数文件的语言设置为 *lang*。您只能与 -r 选项一起设置语言。

注意：有关可以指定的受支持语言代码的列表，请使用 -h 选项运行 -l。 默认情况下，安装参数文件使用英语。

--r

重置程序包，以使用原始程序包中的默认值。

-s

将指定程序包设置为通过自定义安装参数文件（由 -f 选项指定）的输入。

-w 关键字

定义用于指定您接受许可协议的关键字。 您可以在许可协议的结尾处找到此关键字（在方括号内）。要找到许可协议文件，请使用 -a 选项。

安装 UNAB HP-UX 本地程序包

要一起管理 UNAB 安装和所有其他软件安装，请安装自定义的 UNAB SD-UX 格式程序包。 利用 UNAB SD-UX 格式程序包，您可以在 HP-UX 中轻松地安装 UNAB。

重要说明！ 您必须自定义程序包，以使用可在许可协议中找到的关键字指定自己接受该许可协议。

安装 UNAB HP-UX 本地程序包

1. 以 root 身份登录。

   要注册并安装 HP-UX 本地程序包，您需要与 root 帐户相关联的权限。

2. 自定义 UNAB 程序包 (p. 276)。

   您必须自定义程序包，以使用可在许可协议中找到的关键字指定自己接受该许可协议。 您也可以自定义程序包以指定自定义安装设置。

3. 使用以下命令注册通过 SD-UX 自定义程序包：

   ```
   swreg -l depot pkg_location
   ```

   pkg_location

   定义 UNAB 程序包所在的目录。

4. 使用以下命令安装 UNAB 程序包：

   ```
   swinstall -s pkg_location uxauth
   ```

   SD-UX 开始从 *pkg_location* 目录安装该程序包。

   至此，UNAB 便已完全安装，但尚未启动。

更多信息：

本地安装的其他注意事项 (p. 182)
自定义 SD-UX 格式程序包 (p. 202)

卸载 HP-UX 程序包

要卸载安装的 UNAB HP-UX 程序包，您需要按照与安装过程相反的顺序来卸载 UNAB 程序包。

要卸载 CA Access Control 程序包，应卸载 UNAB 主程序包：

```
swremove unab_package_name
```

unab_package_name

定义 UNAB 本地程序包的名称。

AIX 本地程序包安装

AIX 本地程序包作为一套 GUI 和命令行实用程序提供，通过他们，您可以管理个人软件程序包。

注意：虽然某些 AIX 版本支持多种程序包格式（installp、SysV、RPM），但 UNAB 仅提供 AIX 本地程序包格式 (installp)。

重要说明！

- 程序包安装后，如果要卸载 UNAB，您必须使用 *installp* 命令。
- UNAB 使用可插入身份验证模块 (PAM) 验证用户，而不使用 AIX 可加载身份验证模块 (LAM)。 在安装 UNAB 之前，请配置 AIX 系统以启用 PAM。
- 要防止应用程序失败，请确认用户 ID 和主要组 ID 不来源于其他用户存储。 例如，如果用户 ID 来自 /etc/passwd，且主要组来自 Active Directory。

AIX 上的可插入身份验证模块 (PAM)

默认情况下，AIX 使用可加载身份验证模块 (LAM) 对用户进行身份验证。 要使 UNAB 可以验证访问系统的用户的身份，您必须将 AIX 配置为使用 PAM。 在自定义和安装 UNAB 之前，需将 AIX 系统配置为使用 PAM。

注意：您可以在 AIX 版本 5.3 及更高版本上启用 PAM。

示例：将 AIX 配置为使用 PAM

以下示例显示了如何将 AIX 版本 5.3 及更高版本配置为使用 PAM，以便 UNAB 可以用于身份验证。

1. 创建 PAM 配置文件。

   AIX 不提供默认的 /etc/pam.conf 文件。

2. 打开 pam.conf 文件，包括基本模块堆栈，然后保存该文件。 例如：

```
#
# Authentication
#
ftp     auth    required        /usr/lib/security/pam_aix
imap    auth    required        /usr/lib/security/pam_aix
login   auth    required        /usr/lib/security/pam_aix
rexec   auth    required        /usr/lib/security/pam_aix
rlogin  auth    required        /usr/lib/security/pam_aix
snapp   auth    required        /usr/lib/security/pam_aix
su      auth    required        /usr/lib/security/pam_aix
telnet  auth    required        /usr/lib/security/pam_aix
OTHER   auth    required        /usr/lib/security/pam_aix
#
# Account Management
#
ftp     account required        /usr/lib/security/pam_aix
login   account required        /usr/lib/security/pam_aix
rexec   account required        /usr/lib/security/pam_aix
rlogin  account required        /usr/lib/security/pam_aix
rsh     account required        /usr/lib/security/pam_aix
su      account required        /usr/lib/security/pam_aix
telnet  account required        /usr/lib/security/pam_aix
OTHER   account required        /usr/lib/security/pam_aix
#
# Password Management
#
login   password  required      /usr/lib/security/pam_aix
rlogin  password  required      /usr/lib/security/pam_aix
su      password  required      /usr/lib/security/pam_aix
telnet  password  required      /usr/lib/security/pam_aix
OTHER   password  required      /usr/lib/security/pam_aix
#
# Session Management
#
ftp     session required        /usr/lib/security/pam_aix
imap    session required        /usr/lib/security/pam_aix
login   session required        /usr/lib/security/pam_aix
rexec   session required        /usr/lib/security/pam_aix
rlogin  session required        /usr/lib/security/pam_aix
rsh     session required        /usr/lib/security/pam_aix
snapp   session required        /usr/lib/security/pam_aix
su      session required        /usr/lib/security/pam_aix
telnet  session required        /usr/lib/security/pam_aix
```

```
OTHER   session required        /usr/lib/security/pam_aix
```

3. 导航到 /lib/security 并打开 methods.cfg 文件进行编辑。
4. 通过添加以下行启用 PAM 身份验证，然后保存该文件：

```
PAM:
        program = /usr/lib/security/PAM
PAMfiles:
        options = auth=PAM,db=BUILTIN
```

5. 导航到 /etc/security 并打开 login.cfg 文件进行编辑。
6. 将身份验证类型配置为 PAM，然后保存该文件：auth_type = PAM_AUTH

   例如：

```
chsec -f /etc/security/login.cfg -s usw -a auth_type=PAM_AUTH
```

7. 导航到 /etc/ssh/ 并打开 sshd_config 文件进行编辑。
8. 通过添加以下参数启用 SSH PAM 身份验证，然后保存该文件：

```
UsePAM yes
```

   注意：请验证您是否使用了支持 PAM 的 OpenSSH 版本（版本 3.9p1 及更高版本）。 使用以下命令验证版本：

```
lslpp -i openssh.base.server
```

9. 导航到 /etc 并打开 pam.conf 文件进行编辑。
10. 通过添加以下行添加 SSH PAM 身份验证，然后保存该文件：

```
sshd    auth            required        /usr/lib/security/pam_aix
OTHER   auth            required        /usr/lib/security/pam_aix
sshd    account         required        /usr/lib/security/pam_aix
OTHER   account         required        /usr/lib/security/pam_aix
sshd    password        required        /usr/lib/security/pam_aix
OTHER   password        required        /usr/lib/security/pam_aix
sshd    session         required        /usr/lib/security/pam_aix
OTHER   session         required        /usr/lib/security/pam_aix
```

11. 重新启动计算机。

    AIX 将配置为使用 PAM 进行身份验证。 您现在将可以自定义 AIX 本地程序包并安装 UNAB。

自定义 bff 本地程序包文件

在使用本地程序包安装 UNAB 之前，需自定义 UNAB 程序包以指定您接受许可协议。 在自定义程序包时，您还可以指定自定义安装设置。

建议您不要手动修改程序包。 您应当按照以下步骤中的说明，使用脚本自定义 UNAB 程序包。

您可以在 CA Access Control Endpoint Components for UNIX DVD 的 UNAB 目录中找到适用于每个受支持的 AIX 操作系统的 installp 格式本地程序包（bff 文件）。

重要说明！ 在安装 UNAB 之前，请验证您是否已将 AIX 配置为使用 PAM 进行身份验证。

自定义 bff 本地程序包文件

1. 将要自定义的程序包提取到文件系统上的临时位置。

   在文件系统上的读取/写入位置上，可以根据需要自定义程序包（bff 文件）。

   重要说明！ 该位置需要拥有大于或等于程序包两倍大小的磁盘空间，才能保留临时重新打包的文件。

2. 将 customize_uxauth_bff 脚本文件和 pre.tar 文件复制到文件系统上的临时位置。

   pre.tar 文件是 tar 压缩文件，其中包含安装消息和 UNAB 许可协议。

   注意：您可以在本地程序包所在的同一位置中找到 customize_uxauth_bff 脚本文件和 pre.tar 文件。

3. 输入以下命令从安装程序包中提取 uxpreinstall 实用程序：

   `customize_uxauth_bff -e uxpreinstall -f tmp_params [-d pkg_location] pkg_name`

   在安装 UNAB 之前，请使用 uxpreinstall 检查系统遵从性。

4. 输入下面的命令：

   `customize_uxauth_bff -a [-d pkg_location] pkg_name`

   此命令将显示许可协议。

5. 记录许可协议结尾处方括号中出现的关键字。

   您需要在下一步中指定该关键字。

6. 输入下面的命令：

   `customize_uxauth_bff -w keyword [-d pkg_location] pkg_name`

   此命令将指定您接受该许可协议。

7. （可选）输入以下命令：

   ```
   customize_uxauth_bff -r -l lang [-d pkg_location] pkg_name
   ```

   此命令将设置安装参数文件的语言：

8. （可选）输入以下命令：

   ```
   customize_uxauth_bff -i install_loc [-d pkg_location] pkg_name
   ```

   此命令将更改安装目录。

9. 输入以下命令获得安装参数文件：

   ```
   customize_uxauth_bff -g -f tmp_params [-d pkg_location] pkg_name
   ```

10. （可选）编辑安装参数文件以适合您的安装要求 (p. 254)。

    通过该文件，您可以设置程序包的安装默认值。

11. （可选）输入以下命令设置自定义程序包中的安装参数：

    ```
    customize_uxauth_bff -s -f tmp_params [-d pkg_location] pkg_name
    ```

    现在您将可以使用程序包以自定义的默认值安装 UNAB。

customize_uxauth_bff 命令－自定义 bff 本地程序包文件 (UNAB)

customize_uxauth_bff 命令对 bff 本地程序包文件运行 <uxauth> 本地程序包自定义脚本。

该脚本适用于 AIX 上所有可用的 <uxauth> 本地程序包。 要自定义程序包，程序包必须位于您文件系统上的读取/写入目录。

重要说明！ 提取程序包的位置应具有足够的空间，其大小至少是用于重新打包结果的中间程序包大小的两倍。

注意：要获得本地化的脚本消息，您需要将 pre.tar 文件和脚本文件置于同一目录中。

此命令格式如下：

```
customize_uxauth_bff -h [-l]
customize_uxauth_bff -a [-d pkg_location] pkg_name
customize_uxauth_bff -w keyword [-d pkg_location] pkg_name
customize_uxauth_bff -r [-d pkg_location] [-l lang] pkg_name
customize_uxauth_bff -i install_loc [-d pkg_location] pkg_name
customize_uxauth_bff -s -f tmp_params [-d pkg_location] pkg_name
customize_uxauth_bff -e uxpreinstall [-f tmp_params] [-d pkg_location]
pkg_filename
customize_uxauth_bff -g [-f tmp_params] [-d pkg_location] pkg_name
```

pkg_name

您要自定义的 UNAB 程序包（bff 文件）的名称。

-a

显示许可协议。

-e uxpreinstall

指定从安装程序包中抽取 uxpreinstall 实用程序。

-c *certfile*

定义根证书文件的完整路径名。

注意：该选项仅适用于 CAeAC 程序包。

-d *pkg_location*

（可选）指定文件系统上程序包所在目录。 如果您未指定程序包所在目录，脚本将默认使用 /var/spool/pkg。

-f *tmp_params*

指定要创建的或要从中检索信息的安装参数文件的完整路径和名称。

注意：如果您使用 -g 选项时未指定文件，则安装参数将使用标准输出 (stdout)。

--g

获取安装参数文件并将其置于由 -f 选项指定的文件中。

-h

显示命令用法。 与 -l 选项联合使用时，可显示受支持语言的语言代码。

-i *install_loc*

将程序包的安装目录设置为 *install_loc*/uxauth。

-l *lang*

将安装参数文件的语言设置为 *lang*。您只能与 -r 选项一起设置语言。

注意：有关可以指定的受支持语言代码的列表，请使用 -h 选项运行 -l。 默认情况下，安装参数文件使用英语。

--r

重置程序包，以使用原始程序包中的默认值。

-s

将指定程序包设置为通过自定义安装参数文件（由 -f 选项指定）的输入。

-w 关键字

定义用于指定您接受许可协议的关键字。 您可以在许可协议的结尾处找到此关键字（在方括号内）。要找到许可协议文件，请使用 -a 选项。

安装 UNAB AIX 本地程序包

要一起管理 UNAB 安装和所有其他软件安装，请安装自定义的 UNAB AIX 本地程序包。 利用 UNAB AIX 本地程序包（bff 文件），您可以在 AIX 中轻松地安装 UNAB。

重要说明！ 您必须自定义程序包，以使用可在许可协议中找到的关键字指定自己接受该许可协议。 如果要通过 CA Access Control 企业管理 管理 UNAB 端点，您必须在安装 UNAB *之前*将 UNAB 端点注册到 CA Access Control 企业管理。

安装 UNAB AIX 本地程序包

1. 以 root 身份登录。

   要注册并安装 AIX 本地程序包，您需要与 root 帐户相关联的权限。

2. 自定义 UNAB 程序包 (p. 284)。

   您必须自定义程序包，以使用可在许可协议中找到的关键字指定自己接受该许可协议。 您也可以自定义程序包以指定自定义安装设置。

3. （可选）记录要安装的程序包的级别（版本）：

   ```
   installp -l -d pkg_location
   ```

   pkg_location

   定义 UNAB 程序包 (uxauth) 所在的目录。

   对于 *pkg_location* 中的每个程序包，AIX 都均会列出其级别。

   注意：有关 AIX 本地程序包安装选项的详细信息，请参阅有关 installp 的手册页。

4. 使用以下命令安装 UNAB 程序包：

   ```
   installp -ac -d pkg_location uxauth[pkg_level]
   ```

   pkg_level

   定义先前记录的程序包级别号。

   AIX 开始从 *pkg_location* 目录安装 UNAB 程序包。

   至此，UNAB 便已完全安装，但尚未启动。

更多信息：

本地安装的其他注意事项 (p. 182)

卸载 AIX 程序包

要卸载安装的 UNAB AIX 程序包，您需要按照与安装过程相反的顺序来卸载 UNAB 程序包。

要卸载 UNAB 程序包，应卸载 UNAB 主程序包：

```
installp -u unab_package_name
```

unab_package_name

定义 UNAB 本地程序包的名称。

安装后任务

下列主题说明了为配置 UNAB 端点和激活 UNAB 所需要执行的安装后任务。

在 Active Directory 中注册 UNIX 主机

要允许在 Active Directory 中定义的用户登录到 UNIX 计算机，需在 Active Directory 服务器上注册每个安装了 UNAB 的 UNIX 计算机。

注意：您可以配置 UNAB 安装参数文件，以指定在 UNAB 安装期间，安装过程将在 Active Directory 上注册 UNIX 端点。

在 Active Directory 中注册 UNIX 主机

1. 验证 UNIX 主机的时间是否与 Active Directory 服务器同步。
2. 使用超级用户身份登录到 UNIX 计算机。

   注意：您必须先激活 UNAB，Active Directory 用户才能登录到 UNIX 计算机。
3. 如果您使用 Microsoft Services for UNIX (SFU)，请在 uxauth.ini 文件的 map 部分指定属性名称。

   如果在 uxauth.ini 文件中未指定属性名称，则仅在 SFU 中定义的用户将无法登录到 UNAB 主机。

   注意：有关 uxauth.ini 文件的详细信息，请参阅*《参考指南》*。
4. 导航到 UNAB bin 目录。 默认情况下，该目录为：

   ```
   /opt/CA/uxauth/bin
   ```
5. 运行 uxconsole -register 实用程序。

   UNAB 在 Active Directory 中注册 UNIX 计算机并启动 uxauthd 后台进程。

   注意：有关 uxconsole -register 的详细信息，请参阅*《参考指南》*。

示例：在 Active Directory 中注册 UNIX 主机

此示例展示了如何在 Active Directory 中注册 UNIX 计算机。 您键入用户名 (-a administrator) 和密码 (-w admin)，定义 Active Directory 主机名 (-d Active_Directory_Host)，设置详细级别 (-v 3)，指定 UNAB 代理在安装结束时不运行 (-n)，以及在 Active Directory 中定义容器的名称 (-o OU=COMPUTERS)。 必须存在容器才能在 Active Directory 中注册 UNIX 计算机：

```
./uxconsole -register -a administrator -w admin -d Active_Directory_Host -v 3 -n
-o OU=COMPUTERS
```

示例：为 Active Directory 用户指派注册 UNIX 主机的权限

如果您在运行 uxconsole -register 命令时不想指定管理员用户名和密码，可以指定具有在 Active Directory 中注册 UNIX 主机的指派特权的用户的用户名和密码。 以下示例显示了如何为 Active Directory 用户指派在 Active Directory 注册 UNIX 主机的权限。

1. 在 Active Directory 计算机上，依次单击“开始”、“程序”、“管理工具”、“Active Directory 用户和计算机”。

   将打开“Active Directory 用户和计算机”管理控制台。

2. 右键单击“计算机”文件夹并选择“指派控制”。

   将打开指派控制向导。

3. 单击“下一步”。

   将启动该向导。

4. 按照下表完成安装向导，然后单击“完成”：

信息	操作
用户和组	指定要向其指派控制的用户。 选择“添加”并搜索要指派控制的用户。
指派任务	定义要向选定用户或组指派的任务。 选择“创建指派的自定义任务”
Active Directory 对象类型	定义指派任务的范围。 请执行以下操作： ■ 选择“此文件夹、此文件夹中的现有对象以及此文件夹中的新对象的创建”。 ■ 选择“从列表中创建计算机对象的权限”。
权限	定义要指派给用户的权限。 选择“特定子对象的创建/指派”。

向导将关闭。您已经为用户指派了在 Active Directory 中创建计算机对象的权限。 用户现在具有足够的权限，可以在 Active Directory 中注册 UNIX 主机。

配置 UNAB

uxauth.ini 文件指定了 UNAB 在启动和运行时期间所采取的操作。 uxauth.ini 文件包含一组默认值，您可以更改这些值以满足自己的具体情况。

配置 UNAB

1. 登录到正在运行 UNAB 的 UNIX 主机。
2. 打开 uxauth.ini 文件，默认情况下，该文件位于以下目录：

   `/opt/CA/uxauth`
3. 查看设置并根据需要进行更改。

注意：有关 uxauth.ini 配置设置的详细信息，请参阅 *《参考指南》*。

注意：您可以使用 CA Access Control 企业管理 配置 uxauth.ini 文件。

配置 UNAB 以进行报告

安装和配置完 UNAB 之后，您可以启用和配置报告代理，以将数据发送到分发服务器进行处理。 如果在安装 UNAB 时未配置报告代理设置，请在启用报告代理时进行配置。

注意：此过程说明了如何配置现有的 UNAB 端点以发送报告。 如果在同一计算机上安装了 CA Access Control 和 UNAB，则只需要配置报告代理设置一次。

要配置 UNAB 以实现报告功能，请运行 *ACSharedDir*/lbin/report_agent.sh：

```
report_agent config {-server hostname [-proto {ssl|tcp}] [-port port_number]
[-rqueue queue_name] -schedule <time@day> [,day2][...] > [-audit] | [-silent] ]
```

如果您忽略任何配置选项，脚本会为该选项设置默认值。

注意：有关 report_agent.sh 脚本和报告代理配置设置的详细信息，请参阅 *《参考指南》*。

启动 UNAB

要使 Active Directory 的用户登录到 UNIX 计算机，需要启动 UNAB。

启动 UNAB

1. 使用超级用户身份登录到 UNIX 计算机。
2. 找到 UNAB lbin 目录。
3. 输入下面的命令：

   ```
   ./uxauthd.sh start
   ```

   UNAB 后台进程将启动。

激活 UNAB

在 Active Directory 中注册 UNIX 主机后，您需要激活 UNAB。 激活是 UNAB 实施过程中的最后一步。 激活 UNAB 之后，它将根据 Active Directory 密码对用户进行身份验证。

激活 UNAB

1. 使用超级用户身份登录到 UNIX 计算机。
2. 导航到 UNAB bin 目录。 默认情况下，该目录为：

   ```
   /opt/CA/uxauth/bin
   ```

3. 运行以下命令：

   ```
   ./uxconsole -activate
   ```

   -activate

   指定已为 Active Directory 用户激活登录

   UNAB 将被激活。

注意：通过激活 UNAB，拥有 Active Directory 帐户的本地用户可以继续登录到 UNIX 主机。

注意：有关 uxconsole 实用程序的详细信息，请参阅 *《参考指南》*。

示例：激活之后登录到 UNAB

以下示例显示了在以部分模式安装 UNAB 并注册之后如何使用 Active Directory 帐户登录到 UNIX 计算机。

1. 打开终端窗口。
2. 连接到 UNIX 主机：

   ```
   telnet computer.com
   ```

   您将连接到 UNIX 计算机，UNIX shell 将打开。
3. 输入 Active Directory 帐户的用户名和密码。

   如果成功，将显示一条消息，通知您上次登录的详细信息。

如何实施完全集成模式

在完全集成模式下，UNAB 端点依赖于 Active Directory 服务器对用户进行身份验证和授权。

在完全集成模式下实施 UNAB

1. 实施 UNAB。

   此步骤在 UNIX 端点上安装并激活 UNAB。
2. 安装用于管理 Active Directory 用户的 UNIX 属性的工具。

   因为 Active Directory 用户和计算机并不公开 UNIX 属性，您必须安装其他工具才能查看和修改这些属性。 例如：您可以使用 CA Access Control UNIX 属性插件、Microsoft Identity Management for UNIX、ADSI Edit 或简单的 LDAP 客户端来查看和修改 UNIX 属性。
3. 将 UNAB 端点上的用户和组的属性迁移到 Active Directory。 请执行下列操作之一：

   - 使用 UNAB 迁移工具将 UNAB 端点的用户和组的属性复制到 Active Directory。
   - 使用第 2 步中安装的工具在 Active Directory 上手动配置 UNAB 端点用户和组的属性。

   此步骤允许您使用 Active Directory 控制对端点的访问。 至此，UNAB 已在完全集成模式下实施。
4. （可选）为 Active Directory 上的 UNIX 管理员指派管理 UNAB 用户和组权限的权限。
5. 根据需要，使用第 2 步中安装的工具升级 Active Directory 的 UNIX 属性。

   例如：管理员使用该工具更新用户的默认登录 shell。

UNAB 与 Active Directory 的交互

在完全集成模式下，以下 UNIX 用户和组属性存储在 Active Directory 上：

- UID
- GID
- 主目录
- 登录 shell
- GECOS

UNAB 使用 Windows 2003 R2 架构存储这些属性。 通常，UNAB 会读取这些属性，但不写入这些属性。 只有当您使用 uxconsole -migrate 实用程序将 UNIX 用户和组迁移到 Active Directory 时，UNAB 才会写入 Active Directory 属性。

UNAB 不会扩展 Active Directory 架构。

安装 CA Access Control UNIX 属性插件

CA Access Control UNIX 属性插件允许您管理 Active Directory 上的 UNAB 用户的 UNIX 属性。 该插件不安装 NIS 服务器。 可以用于管理 UNAB 用户的 UNIX 属性的其他工具包括 Microsoft Identity Management for UNIX、ADSI Edit 或简单的 LDAP 客户端。

默认情况下，插件使用 Active Directory 2003 R2 架构读取和写入 Active Directory 数据。 如果 R2 架构不存在，您可以配置该插件使用不同的属性。

您必须在用户用来管理 Active Directory 的服务器上安装该插件，但不需要在 Active Directory 域控制器 (DC) 上安装该插件。

安装 CA Access Control UNIX 属性插件

1. 将 CA Access Control Endpoint Components for UNIX DVD 插入服务器的光盘驱动器中。
2. 浏览至以下目录：

   ```
   ADTools\UnixADTabExt
   ```

3. 选择适合正在使用的操作系统的目录。
4. 双击 setup.exe 文件。

   将打开 CA Access Control UNIX 属性插件安装向导。
5. 按照说明安装 CA Access Control UNIX 属性插件。

   CA Access Control UNIX 属性插件将安装在 Active Directory 主机上。
6. （可选）配置插件使用的 Active Directory 属性。

   如果 Active Directory 架构不是 Windows 2003 R2，请完成此步骤。

配置插件使用的属性

CA Access Control UNIX 属性插件使用 Active Directory 2003 R2 架构读取和写入 Active Directory 数据。 如果您的 Active Directory 服务器不使用 2003 R2 架构，您可以将插件配置为使用不同架构的属性。

如果将插件配置为使用不同架构的属性，您还必须将 UNAB 端点配置为使用相同的属性。 您可以使用 uxauth.ini 文件的 map 部分配置 UNAB 端点使用的属性。

要配置插件使用的属性，需更改以下注册表项的值。 这些项位于以下注册表键中：

```
HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\uxauth
```

项	默认值	插件的字段名称
user_uid_attr_name	uidNumber	UID
user_loginshell_attr_name	loginShell	登录 Shell
user_homedir_attr_name	unixHomeDirectory	主目录
user_gecos_attr_name	gecos	GECOS
user_gid_attr_name	gidNumber	主要组名称/GID
group_gid_attr_name	gidNumber	GID（组 ID）

注意：有关 uxauth.ini 文件的详细信息，请参阅*《参考指南》*。

卸载 CA Access Control UNIX 属性插件

CA Access Control UNIX 属性插件允许您管理 Active Directory 上的用户和组的 UNIX 属性。

卸载 CA Access Control UNIX 属性插件

1. 请依次单击“开始”、“控制面板”、“添加/删除程序”。

   此时将显示“添加或删除程序”对话框。

   注意：在 Windows Server 2008 上，依次单击“开始”、“控制面板”、“程序和功能”。

2. 滚动浏览程序列表，然后选择 CA Access Control UNIX 属性管理单元。

3. 根据您使用的操作系统，单击“更改\删除”或“卸载”。

   卸载进程会从系统中删除 CA Access Control UNIX 属性插件。

4. 删除以下注册表键：

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\uxauth

5. 从计算机中删除 ACUnixAttributesShellExt.dll 文件。

   CA Access Control UNIX 属性插件即已卸载。

示例：卸载 ACUnixAttributesShellExt.dll

以下示例从目录 C:\WINDOWS\system32 中卸载 CA Access Control UNIX 属性插件：

```
regsvr32 /u %WINDIR%\system32\ACUnixAttributesShellExt.dll
```

用户和组迁移

通过将管理任务合并为单一的管理应用程序，将用户从 UNIX 主机迁移到 Active Directory 简化了 UNIX 主机上的用户和组管理。 在将 UNIX 用户迁移到 Active Directory 之后，您可以控制对 UNIX 主机的访问，并且不再需要维护每个 UNIX 主机上的密码或 shadow 文件。

在将用户和组从 UNIX 主机迁移到 Active Directory（完全集成模式）之后，Active Directory 将执行用户的身份验证和授权。

更多信息：

迁移的工作原理 (p. 297)
将 UNIX 用户和组迁移到 Active Directory (p. 298)

迁移的工作原理

在 UNIX 主机上启动迁移进程时，UNAB 将执行以下任务：

1. 检索本地用户和 NIS/NIS+ 用户的列表。

   针对列表中的每个用户名检查 Active Directory，并对每个用户执行以下操作之一：

   - 如果用户存在于 Active Directory 中，且用户 UNIX 属性与 UNIX 主机中显示的属性相同，则迁移该用户帐户。
   - 如果用户存在于 Active Directory 中，但缺少某些用户 UNIX 属性，则 UNAB 不会迁移该用户，并会记录缺少的属性。
   - 如果用户存在于 Active Directory 中，但用户没有任何 UNIX 属性，则 UNAB 将迁移该用户并添加缺少的属性。
   - 如果用户不存在于 Active Directory 中，则 UNAB 不会在 Active Directory 中创建该用户帐户。

2. 检索本地组和 NIS/NIS+ 组的列表。

   针对组名称检查 Active Directory，并对每个组执行以下操作之一：

   - 如果组存在于 Active Directory 中，且组的 UNIX 属性与 UNIX 主机中的属性相同，则迁移该组。
   - 如果组存在于 Active Directory 中，但组的 ID 与 UNIX 主机上的 ID 不同，则 UNAB 不会将该组（包括其成员）迁移到 Active Directory。
   - 如果组存在于 Active Directory 中且组 ID 相同，但缺少某些 UNIX 属性，则 UNAB 会将该组迁移到 Active Directory 并补全缺少的属性。
   - 如果组不存在于 Active Directory 中，则 UNAB 将创建组并将这些组迁移到 Active Directory 中。

注意：如果在 Active Directory 中存在名称相同的用户或组，则不能迁移用户或组。 例如：如果您尝试迁移名为 g1 的组，但是在 Active Directory 中存在名为 g1 的用户，则 UNAB 无法迁移该组。

注意：如果选择将 root 用户迁移到 Active Directory，root 帐户将在本地和登录 Active Directory 时进行身份验证。 因此，身份验证过程的时间会很长。

将 UNIX 用户和组迁移到 Active Directory

您可以将用户从本地 UNIX 主机迁移到 Active Directory，以便从单个位置管理对主机的访问。

将 UNIX 用户和组迁移到 Active Directory

1. 以 root 用户身份登录到 UNIX 计算机。
2. 导航到 UNAB 安装 bin 目录，默认情况下为：

   ```
   /opt/CA/uxauth/bin
   ```

3. 运行 -uxconsole -migrate 实用程序。

   uxconsole 程序将 UNIX 用户和组迁移到 Active Directory。 此时将显示一条消息，通知您该操作已成功完成。

注意：有关解决迁移冲突的详细信息，请参阅*《企业管理指南》*。 有关 uxconsole 实用程序的详细信息，请参阅*《参考指南》*。

为 UNIX 管理员指派管理 UNIX 用户和组属性的权限

要使 UNIX 管理员管理 Active Directory 的 UNIX 用户和组属性，您可以将具体的管理权限指派给 UNIX 管理员。 通过指派管理权限，UNIX 管理员可以在将 UNIX 用户和组迁移到 Active Directory 后继续管理它们的属性。

在指派管理权限之前，请验证您是否安装了用于管理 Active Directory 用户的 UNIX 属性的工具。 建议您将管理权限指派给组，而不是单个用户。

示例：为 UNIX 管理员指派管理 UNIX 用户和组属性的权限

以下示例显示了如何向 UNIX 管理员组指派管理 Active Directory 中的 UNIX 用户和组的权限。

1. 在 Active Directory 计算机上，依次单击“开始”、“程序”、“管理工具”、“Active Directory 用户和计算机”。

   将打开“Active Directory 用户和计算机”管理控制台。

2. 右键单击“组织单元 (OU)”，然后选择“属性”。

   将打开“组织单元”属性窗口。

3. 选择“安全”选项卡。

   注意：如果未看到“安全”选项卡，请核实“视图”选项卡下的“高级功能”选项是否已突出显示。

4. 单击“高级”，然后单击“添加”按钮。

   将打开“选择用户、计算机或组”窗口。

5. 输入要指派管理权限的组或用户的名称。 单击“确定”。

   将打开“权限条目”窗口。

6. 单击“属性”选项卡。

   您可以在此窗口中为组或用户分配权限。

7. 在“应用到”菜单中，选择“组对象”。
8. 在“允许”列中选择“读取 gidNumber”和“写入 gidNumber”选项。
9. 单击“确定”。

   您已经将对 UNIX 组属性的管理指派给 UNIX 管理员组。

10. 重复步骤 1-6 指派对 UNIX 用户的管理权限。
11. 在“应用到”菜单中，选择“用户对象”。
12. 在“允许”列中选择以下属性：
    - 读取 Gecos
    - 写入 Gecos
    - 读取 gidNumber
    - 写入 gidNumber
    - 读取 uid
    - 写入 uid
    - 读取 uidNumber
    - 写入 uidNumber
    - 读取 unixHomeDirectory
    - 写入 unixHomeDirectory
    - 读取 loginShell
    - 写入 LoginShell
13. 单击“确定”。

    您已经将对 UNIX 用户属性的管理指派给 UNIX 管理员组。

配置 Active Directory 用户的 UNIX 属性

此过程介绍了如何使用 CA Access Control UNIX 属性插件管理 Active Directory 上的 UNIX 用户的属性。 您可以使用其他工具管理 Active Directory 上的 UNIX 属性，例如：Microsoft Identity Management for UNIX、ADSI Edit 或简单的 LDAP 客户端。

注意：在定义用户帐户属性时，您不需要指定该用户可以登录到的计算机。 这些设置不适用于 UNIX 主机。

配置 Active Directory 用户的 UNIX 属性

1. 依次选择“开始”、“程序”、“管理工具”、“Active Directory 用户和计算机”。

   将打开“Active Directory 用户和计算机”窗口。

2. 双击一个用户帐户。

   此时将显示该用户帐户的属性。

3. 单击“CA Access Control UNIX 属性”选项卡。

   此时将显示“CA Access Control UNIX 属性”选项卡。

4. 填写以下字段：

   启用 UNIX 属性

   指定用户帐户是否启用 UNIX 属性。 您必须选中此复选框以启用该用户的 UNIX 属性。

   UID

   定义 UNIX 计算机上的用户 ID 号。 单击“生成”查找下一个可用的 UID。

   主目录

   定义 UNIX 计算机上的用户主目录。

   示例：/home/user

   重要说明！ 请验证在配置用户主目录之前，主目录的母目录存在。

   登录 Shell

   定义用户帐户登录 shell

   示例：/bin/sh

   GECOS

   指定用户的 GECOS 信息。

主要组名称/GID

定义用户所属的主要组名称或 GID。

示例：UNIXUsers

重要说明！ 在定义用户帐户时，必须分配有效的组名称/GID。

5. 单击“确定”。

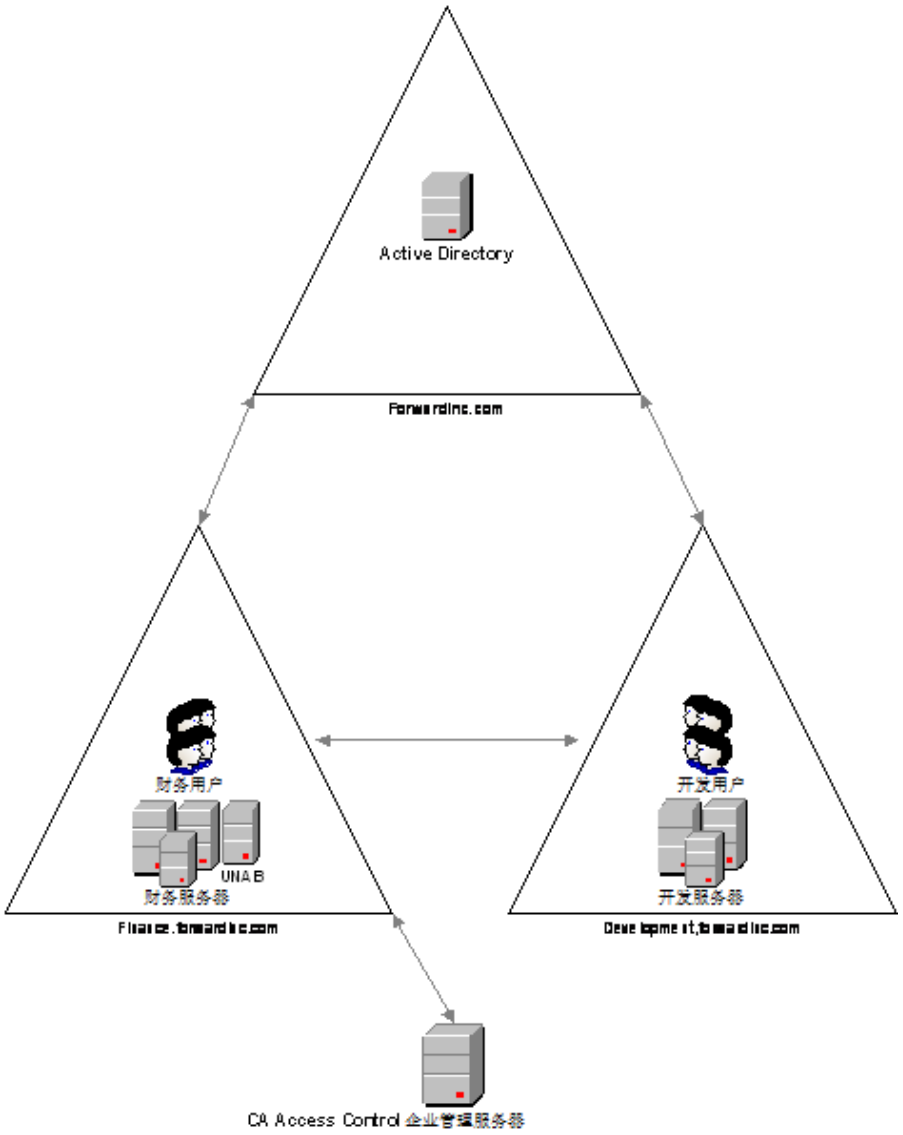
用户 UNIX 属性即已配置。

在受信任域环境中实施 UNAB

在安装 UNAB 时，您需要指定注册 UNAB 的域的参数。 在安装、注册和激活 UNAB 之后，需要将用户和组迁移到该域。

如果指定的域已与其他域建立了信任关系，则这些域中的用户可以访问 UNAB 所属域中的计算机。

此图表显示了在受信任域环境中实施 UNAB 的过程：



在上面的图表中，UNAB 安装在一个与其他域建立了信任连接的域中。在此环境中，受信任域中的用户可以访问其他域，尽管这些用户不是其他域的成员。

在受信任域环境中安装 UNAB 之前，需考虑以下事项：

- UNAB 登录策略基于用户名控制对域中计算机的访问。 如果多个用户具有相同的用户名且在多个域中进行定义，UNAB 将无法辨别用户的原始域并授予对该域的访问权限。
- 您可以仅为 UNAB 所属的域生成报告。 您无法为受信任域生成报告。
- 您可以将用户迁移到在 UNAB 所属的域中定义的 Active Directory。

建议您保留唯一的用户和组名称，以防止受信任域中未经授权的用户的访问。

第 10 章： 安装高可用性部署

此部分包含以下主题：

高可用性

CA Access Control 企业管理使用镜像站点来提供高可用性部署。 *镜像*站点是具有完整、实时信息镜像功能的完全冗余设施，从各技术方面讲，等同于主站点。 数据同时在主站点和镜像站点上进行处理和存储。

镜像站点采用主动-被动部署以实现故障转移。 *主动-被动*部署包括两个或更多个数据中心，其中一个主动地处理请求，其他数据中心已准备好在主动数据中心出现故障时为请求提供服务。 所选的群集解决方案软件负责控制主动和被动服务器，并在出现故障时在它们之间进行切换。

在主动-被动部署中，主动服务器称为主服务器，被动服务器称为辅助服务器。

高可用部署的优点和限制

高可用性部署可帮助确保当一个或多个组件或服务器出现故障时，CA Access Control 企业管理 组件能够继续为请求提供服务。 如果端点无法连接到主环境，它们可以在还原主环境之前连接到辅助服务器。

高可用性部署具有以下优点：

- 防止在主企业管理服务器出现故障时丢失特权帐户、DMS 数据源文件和端点定义。
- 帮助确保无中断使用。

在规划高可用性部署时，请考虑以下限制：

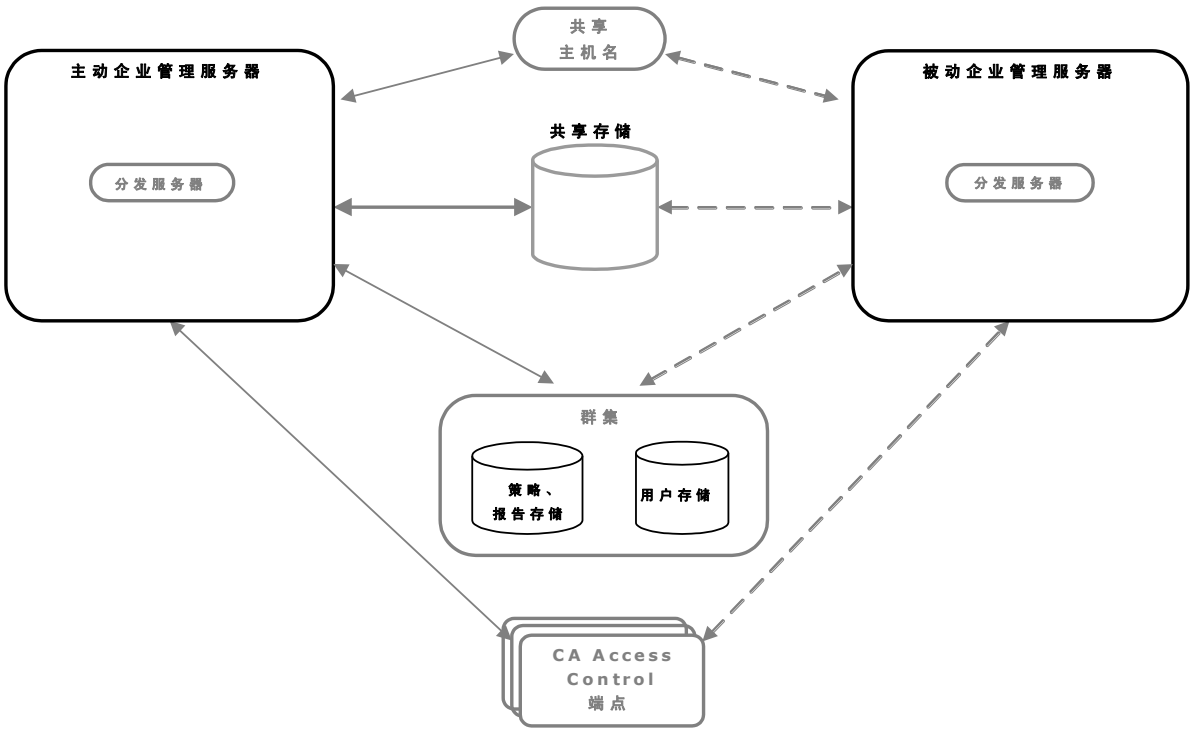
- 企业管理服务器在发生故障时不支持会话连续性。 如果主动服务器无法响应，用户会话将会终止。 已登录的用户必须重新登录。
- 仅支持一台主动 DMS。
- 安装主企业管理服务器和辅助企业管理服务器时，使用相同的通讯密码。
- 主服务器和辅助服务器上的 Java 连接器服务器 (JCS) 必须使用相同的名称。

注意：建议您使用由群集软件解决方案控制的虚拟 DNS 名称，以便出现故障时在服务器之间实现无缝转换。

例如：如果在打开某个用户会话时主企业管理服务器出现故障，用户可以键入辅助企业管理服务器的 URL 或者通过虚拟 DNS 或负载平衡器来使用相同的 URL 继续工作。

高可用性部署体系结构

下图显示高可用性环境中的 CA Access Control 企业管理：



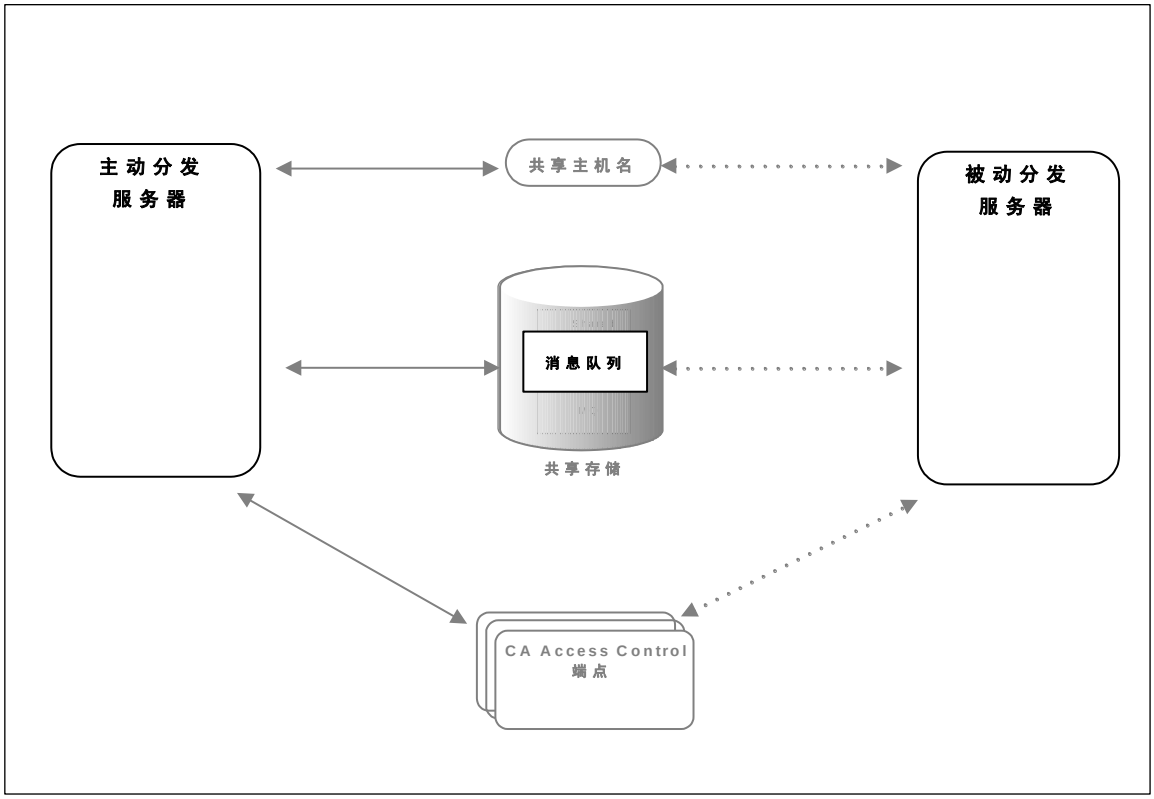
如之前的图中所示，高可用性部署具有以下组件：

- 主企业管理服务器和至少一台备用企业管理服务器
- 策略和报告存储以及用户存储的群集安装
- 主 CA Access Control 企业管理 服务器和备用 CA Access Control 企业管理 服务器都可以访问的共享存储
- 共享主机名
- CA Access Control 端点可以与主企业管理服务器和备用企业管理服务器一起使用

高可用性环境体系结构中的分发服务器

您可以部署额外的分发服务器来实现高可用性，从而在分发服务器出现故障时防止丢失从端点收集的审核事件。

下图显示了在高可用性环境中主分发服务器和辅助分发服务器的实施：



如前一个图中所示，分发服务器的高可用性实施基于：

- 一台主分发服务器和至少一台辅助分发服务器。
- 主分发服务器和辅助分发服务器可以访问的、用于保存消息队列数据文件的共享存储。

  可以将消息队列数据文件放置在共享存储器上，以确保在分发服务器出现故障时不会丢失从端点收集的审核事件消息。
- 共享主机名。
- CA Access Control 端点能够配合主分发服务器和辅助分发服务器。

高可用性环境的组件

要在高可用性环境中部署 CA Access Control，需要满足以下条件。

- 主服务器：
  - 企业管理服务器
- 辅助服务器：
  - 企业管理服务器
- 用户存储库
- 策略和报告数据库
- 共享存储解决方案：
  - 群集软件
  - 共享存储

共享存储

建议使用共享存储设备来实施共享存储解决方案。 主动服务器和被动服务器必须均可访问该共享存储。 确认所用的共享存储解决方案满足以下条件：

- 写入顺序－共享存储解决方案必须按缓冲区中的同样顺序将数据块写入共享存储。
- 同步写入持久性－从同步写入调用返回后，存储解决方案保证所有数据已写入持久性存储。

以下是基于软件的共享存储解决方案的示例：

- 双端口 SCSI 设备
- 存储区域网络 (SAN)

双端口 SCSI 和 SAN 解决方案符合写入顺序和同步写入持久性要求。

群集软件

群集软件使整个网络中的多台服务器可以在计算机群集中共同工作，以提供应用程序高可用性。

重要说明！ 在本章中描述的步骤仅适用于 Microsoft 群集软件和 Active Directory。

在高可用性部署中，群集软件执行以下任务：

- 监视主企业管理服务器和辅助企业管理服务器的状态
- 确认一次只有一个实例（主服务器或辅助服务器）处于活动状态
- 管理企业管理服务器上的 CA Access Control 服务
- 管理将端点指向主动服务器的共享主机名

如果出现故障会发生什么？

在高可用性部署中，群集解决方案软件按照固定时间间隔查询主服务器的可用性。 如果在预定义时间段内主服务器无响应，群集解决方案软件和 CA Access Control 会执行以下操作：

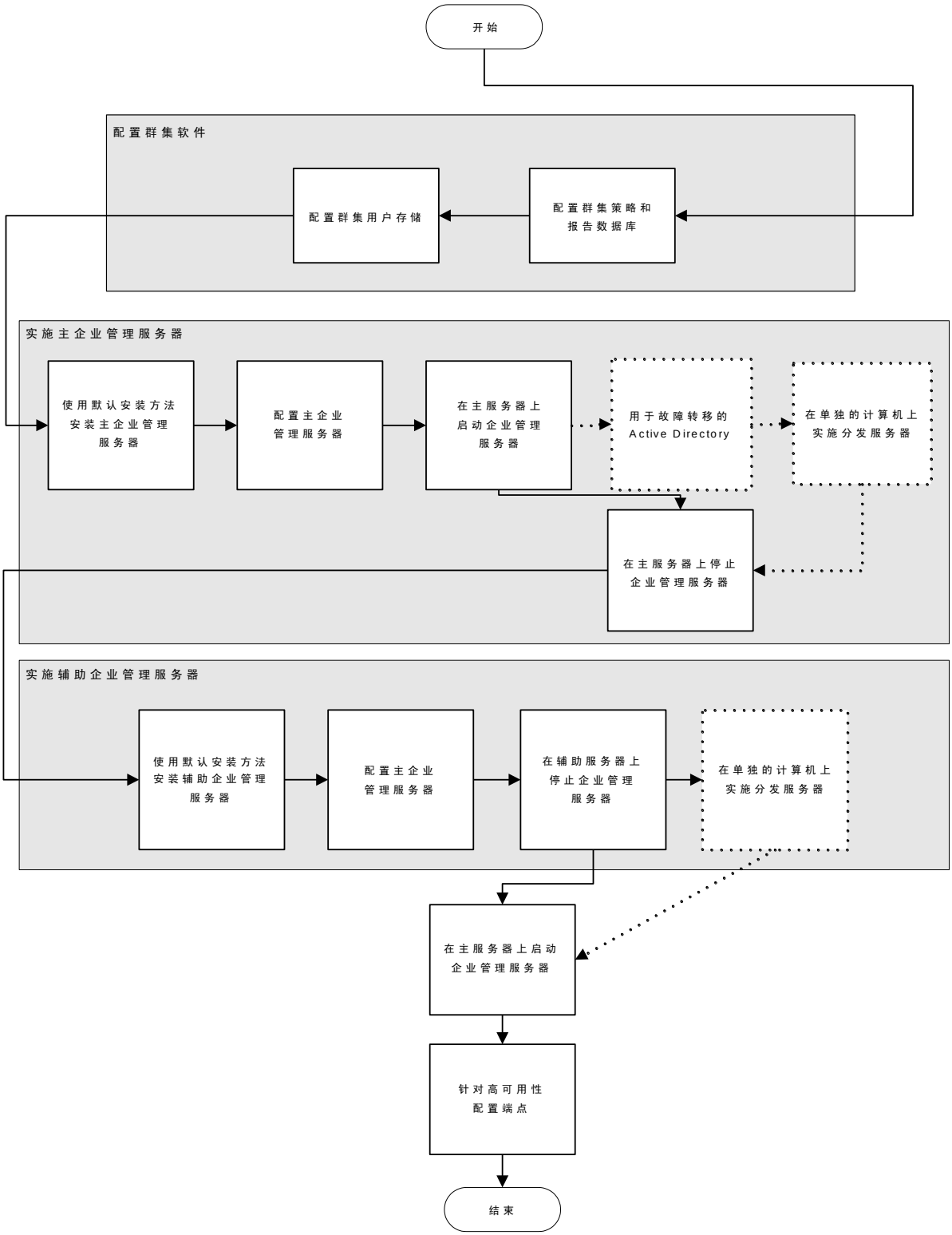
1. 群集解决方案软件停止在主服务器上运行的所有企业管理服务器服务。
2. 群集解决方案软件会启动辅助服务器上的所有企业管理服务器服务。
3. CA Access Control 端点尝试连接到辅助服务器并继续工作。
4. 在群集软件解决方案停止主服务器上的企业管理服务器服务时，登录到该应用程序的任何用户都会被注销。 为了继续使用该应用程序，用户必须再次登录到 CA Access Control 企业管理。

如何配置 CA Access Control 企业管理 for High Availability

要正确配置高可用性部署，必须按正确顺序设置主企业管理服务器和辅助企业管理服务器。

下图显示了在高可用性环境中实施多个企业管理服务器时需要执行的步骤。

注意：配置 Active Directory 进行故障转移以及在独立计算机上实施分发服务器为可选步骤。


开始
配置群集软件
配置群集用户存储
配置群集策略和报告数据库
实施主企业管理服务器
使用默认安装方法安装主企业管理服务器
配置主企业管理服务器
在主服务器上启动企业管理服务器
用于故障转移的 Active Directory
在单独的计算机上实施分发服务器
在主服务器上停止企业管理服务器
实施辅助企业管理服务器
使用默认安装方法安装辅助企业管理服务器
配置主企业管理服务器
在辅助服务器上停止企业管理服务器
在单独的计算机上实施分发服务器
在主服务器上启动企业管理服务器
针对高可用性配置端点
结束

更多信息：

在 Windows 上安装 CA Access Control 企业管理 (p. 47)
如何安装企业管理服务器组件 (p. 45)
如何设置报告服务服务器组件 (p. 97)

配置主企业管理服务器

主企业管理服务器是中央管理服务器，并包含一些组件和工具，用于将策略部署到端点、管理特权帐户以及定义资源、访问者和访问级别。

请按下列步骤操作：

1. 在主服务器上安装 CA Access Control 企业管理（如果尚未安装）。

   已安装所有基于 Web 的应用程序、分发服务器、DMS 和 CA Access Control。
2. 停止所有 CA Access Control 服务。
3. 修改服务以手动启动，而非自动。
4. 将 DMS 和 DH 复制到共享存储，如下所述：
   a. 找到 DMS 目录并将它复制到共享存储。 此目录位于以下位置：

      `ACServerInstallDir/APMS/AccessControl/data/DMS__`

      ACServerInstallDir

      定义企业管理服务器的安装目录的名称。
   b. 找到 DH 目录并将它复制到共享存储。 此目录位于以下位置：

      `ACServerInstallDir/APMS/AccessControl/Data/DH__`
   c. 找到 DH__WRITER 目录并将它复制到共享存储。 默认情况下，此目录位于以下位置：

      `ACServerInstallDir/APMS/AccessControl/Data/DH__WRITER`
   d. 将 _pmd directory_ 注册表项配置设置指定为 DMS 及 DH 复制到的共享存储目录的完整路径名。 例如：Z:\PMD。

   主服务器配置为使用共享存储中的 DMS 和 DH。

5. 将消息队列配置为使用共享存储，如下所述：
   a. 将消息队列数据存储文件夹复制到共享存储。 这些文件位于以下目录中：

      ```
      ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data
      ```

   b. 打开 tibemsd.conf 文件进行编辑。 默认情况下，此文件位于以下目录中：

      ```
      EACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data
      ```

   c. 将 store 标记值设置为指向数据存储文件复制到的共享存储中目录。 例如：Z:\PMD\DATASTORE
   d. 保存并关闭文件。
   e. 打开 queues.conf 文件进行编辑。
   f. 附加一个逗号，并在每个队列定义行末尾添加 failsafe 一词，然后保存并关闭该文件。
6. 主要企业管理服务器恢复操作时，创建批处理文件来启动全部 CA Access Control 服务，如下所示：

   ```
   seosd -start
   net start acrptmq
   net start "CA Access Control Web Service"
   net start im_jcs
   net start JBAS50SVC
   ```

7. 主要企业管理服务器失败时，创建批处理文件来停止全部 CA Access Control 服务，如下所示：

   ```
   secons -s

   net stop acrptmq
   net stop "CA Access Control Web Service"
   net stop im_jcs
   net stop JBAS50SVC
   ```

8. 配置群集软件在失败时运行脚本。
9. 启动所有 CA Access Control 服务

示例：编辑 queues.conf 文件

以下示例是来自 queues.conf 文件的片段，说明了如何修正文件以将消息队列配置为使用共享存储。

```
queue/snapshots secure,failsafe
queue/audit secure,failsafe
ac_endpoint_to_server secure,failsafe
ac_server_to_endpoint secure,failsafe
```

更多信息：

在 Windows 上安装 CA Access Control 企业管理 (p. 47)

配置辅助企业管理服务器

当主服务器出现故障时，辅助企业管理服务器将处理端点请求。

请按下列步骤操作：

1. 如有必要，将 FIPS 密钥从主企业管理服务器复制到临时目录。 该文件位于以下目录：

   ```
   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/config/com/netegrity/config/keys
   ```

   JBOSS_HOME

   定义安装 JBoss 的目录名称。

2. 从命令提示符窗口在辅助服务器上安装企业管理服务器并指定 e -DFIPS_KEY=<*full_pathname_to_key*> 选项。

   重要说明！ 在运行辅助企业管理服务器安装程序时，指定 **--DFIPS_KEY** 选项。 先将 FIPS 密钥从主企业管理服务器复制到辅助企业管理服务器，然后开始安装过程。

   已安装所有基于 Web 的应用程序、分发服务器、DMS 和 CA Access Control。

3. 停止所有 CA Access Control 服务。

4. 修改服务以手动启动，而非自动。

5. 将 *_pmd directory_* 注册表项配置设置指定为 DMS 及 DH 复制到的共享存储目录的完整路径名。 例如：Z:\PMD。

   辅助服务器配置为使用共享存储中的 DMS 和 DH。

6. 将消息队列配置为使用共享存储。 请执行以下操作：

   a. 打开 tibemsd.conf 文件进行编辑。 默认情况下，此文件位于以下目录中：

      ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

      ACServerInstallDir

      定义企业管理服务器的安装目录的名称。

   b. 将 *store* 标记值设置为指向数据存储文件复制到的共享存储中目录，例如：Z:\PMD。

   c. 保存并关闭文件。

   d. 打开 queues.conf 文件进行编辑。

   e. 附加一个逗号，并在每个队列定义行末尾添加 **failsafe** 一词，然后保存并关闭该文件。

7. 确认 CA Access Control 服务未在运行。

8. 配置 DMS 以授权辅助企业管理服务器，如下所示：

   a. 在主要企业管理服务器上，启动 JCS、JBoss 应用程序服务器、CA Access Control 和消息队列服务。

   b. 打开 selang 命令提示符窗口并输入以下命令：

      ```
      host DMS__@
      ```

      消息出现，通知您连接到本地主机。

   c. 输入以下命令，以便显示授权的终端列表：

      ```
      sr TERMINAL *
      ```

      CA Access Control 显示授权终端的详细信息。

   d. 输入以下命令，以便将辅助企业管理服务器添加到授权的终端表中：

      ```
      newres TERMINAL
      <secondary_enterprise_management_server_full_DN> audit (f)
      owner(nobody)defacc(r)
      authorize TERMINAL
      <ssecondary_enterprise_management_server_full_DN>
      uid(+reportagent) access(write)
      authorize TERMINAL
      <ssecondary_enterprise_management_server_full_DN>
      uid(DOMAIN\Administrator) access(write,read)
      authorize TERMINAL
      <secondary_enterprise_management_server_full_DN>
      uid(an_entm_pers) access(write,read)
      ```

9. 主要企业管理服务器失败时，创建批处理文件来启动全部 CA Access Control 服务，如下所示：

```
seosd -start
net start acrptmq
net start "CA Access Control Web Service"
net start im_jcs
net start JBAS50SVC
```

10. 主要企业管理服务器恢复操作时，创建批处理文件来停止全部 CA Access Control 服务，如下所示：

```
secons -s
net stop acrptmq
net stop "CA Access Control Web Service"
net stop im_jcs
net stop JBAS50SVC
```

11. 配置 Microsoft 群集软件在失败时运行脚本。

    已配置辅助企业管理服务器。

更多信息：

在 Windows 上安装 CA Access Control 企业管理 (p. 47)

针对故障转移配置 Active Directory

如果使用 Active Directory 作为用户存储，则可将企业管理服务器配置为与多个域控制器配合使用。 当主域控制器出现故障时，另一个域控制器将接管工作并继续为客户端请求提供服务。

请按下列步骤操作：

1. 启用 CA Identity Manager 管理控制台 (p. 72)。

   使用 CA Identity Manager 管理控制台配置环境中的域控制器列表。

2. 打开 CA Identity Manager 管理控制台 (p. 73)。

3. 单击“目录”，然后单击 ac-dir 环境。

   此时将显示“目录属性”窗口。

4. 单击“导出”，然后保存 XML 文件。

5. 打开 XML 文件进行编辑。 找到 <Connection host= *host_name*> 标记。 例如：

   ```
   <Connection host="primaryDir.com" port="389">
   ```

6. 在行尾添加字符串 **failover**，在空格分隔列表中指定域控制器的主机名和端口号，然后保存文件。 例如：

   ```
   <Connection host="ADserver1" port="389"
   failover="ADserver2:389"/>
   ```

7. 在管理控制台中单击“更新”。

   随后将打开“更新目录”窗口。

8. 输入编辑的 XML 文件的完整路径名，或浏览到该文件，然后单击“完成”。

   状态信息显示在“目录配置输出”字段中。

9. 单击“继续”，然后重新启动环境。

   现在，企业管理服务器即可与主域控制器和辅助域控制器配合使用。

使用本地 DMS 配置 CA Access Control 企业管理

使用 localhost（而不是完全限定域名）配置企业管理服务器上的 DMS，以连接到 DMS。

使用本地 DMS 配置 CA Access Control 企业管理

1. 登录 CA Access Control 企业管理，然后依次选择“系统”、“DMS”、“修改连接”。

   此时将显示“修改连接: 搜索连接”窗口。

2. 搜索默认的 DMS 连接，然后单击“选择”。

   随后将打开“修改连接: *ConnectionName*”窗口。

3. 将主机名改成 LocalHost，如下所述：

   ```
   DMS__@localhost
   ```

4. 单击“提交”。

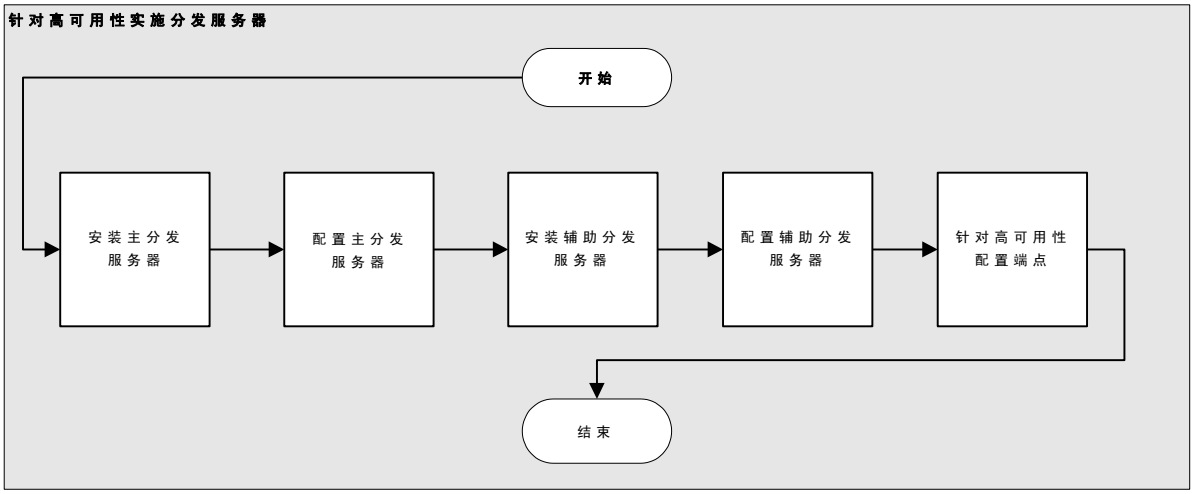
   现在，主分发主机和辅助分发主机可以共享 DMS 计算机。

如何针对高可用性配置分发服务器

要在高可用性环境中正确配置多个分发服务器，请按正确顺序设置主分发服务器和辅助分发服务器。

下图显示了设置多个分发服务器，以便与企业管理服务器配合使用时需要执行的步骤。

重要说明！ 仅当您要将 CA Access Control 企业管理 与 CA Enterprise Log Manager 集成时，才需要完成以下步骤。 针对高可用性配置分发服务器可以避免丢失故障分发服务器收集的且没有发送给企业管理服务器和 CA Enterprise Log Manager 的所有事件。



更多信息：

安装分发服务器 (p. 337)

配置主分发服务器

分发服务器处理应用程序服务器和端点之间的通讯。

如果仅安装独立的分发服务器，则应该完成此过程。

请按下列步骤操作：

1. 在“服务”窗口中，停止 JCS、CA Access Control 和消息队列服务器服务。
2. 修改服务以手动启动，而非自动。
3. 在共享存储上创建 PMD 目录。
4. 将分发主机配置为使用共享存储，如下所述：
   a. 将 DH 目录复制到共享存储。 此目录位于以下位置：

      DistServerInstallDir/APMS/AccessControl/Data/DH__

      DistServerInstallDir

      定义分发服务器的安装目录的名称。

   b. 将 DH__WRITER 目录复制到共享存储。 此目录位于以下位置：

      DistServerInstallDir/APMS/AccessControl/Data/DH__WRITER

   c. 将 DMS__ 目录复制到共享存储。 此目录位于以下位置：

      DistServerInstallDir/APMS/AccessControl/Data/DMS__

   d. 将 *ComputerAssociates**AccessControl**PMD* 下的 *_pmd_directory_* 注册表项配置设置指定为 DMS 及 DH 复制到的共享存储目录的完整路径名。 例如：Z:\PMD。

   主服务器配置为使用共享存储中的 DMS 和 DH。

5. 将消息队列配置为使用共享存储，如下所述：
   a. 在共享存储上创建目录。 例如：Z\MessageQueue
   b. 将消息队列数据存储文件复制到共享存储。 这些文件位于以下目录中：

      DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

   c. 打开 tibemsd.conf 文件进行编辑。 此文件位于以下目录：

      DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

   d. 将 *store* 标记值设置为指向数据存储文件复制到的共享存储中目录。 例如：F:\MessageQueue。
   e. 保存并关闭文件。
   f. 打开 queues.conf 文件进行编辑。
   g. 附加一个逗号，并在每个队列定义行末尾添加 **failsafe** 一词，然后保存该文件。
6. 启动 CA Access Control 服务。

示例：编辑 queues.conf 文件

queues.conf 文件中的以下片段显示了如何修改文件，以便将消息队列配置为使用共享存储。

```
queue/snapshots secure,failsafe
queue/audit secure,failsafe
ac_endpoint_to_server secure,failsafe
ac_server_to_endpoint secure,failsafe
```

配置辅助分发服务器

当主动分发服务器在预定义时间间隔内无法响应时，辅助分发服务器将处理应用程序服务器和端点之间的通讯。

请按下列步骤操作：

1. 停止 JCS、CA Access Control 和消息队列服务器服务。
2. 修改服务以手动启动，而非自动。
3. 将 *\ComputerAssociates\AccessControl\PMD* 下的 *_pmd_directory_* 注册表项配置设置指定为 DMS 及 DH 复制到的共享存储目录的完整路径名。 例如：Z:\PMD。

   辅助分发服务器现在可以访问共享存储中的 DMS 和 DH 文件。 已将分发主机配置为使用共享存储。

4. 将消息队列配置为使用共享存储，如下所述：
   a. 打开 tibemsd.conf 文件进行编辑。 此文件位于以下目录：

      DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

      DistServerInstallDir

      定义分发服务器的安装目录的名称。

   b. 将“*store*”标记值设置为指向数据存储文件复制到的共享存储中目录，例如：Z:\Datastore。
   c. 保存并关闭文件。
   d. 打开 queues.conf 文件进行编辑。
   e. 附加一个逗号，并在每个队列定义行末尾添加 **failsafe** 一词，然后保存该文件。
5. 确认辅助服务器上的 CA Access Control 服务已停止。

针对高可用性配置端点

在安装并配置主企业管理服务器和辅助企业管理服务器之后，将 CA Access Control 端点设置为可在高可用性环境中工作。

针对高可用性配置端点

1. 使用端点上启用的高级策略管理客户端功能安装 CA Access Control。

   CA Access Control 端点已安装。
2. 在端点上打开命令提示符窗口，然后输入以下命令：

   `dmsmgr -config -dhname names`

   该命令可将端口配置为能够处理分发主机的逗号分隔列表。

   注意：有关 dmsmgr 实用程序的详细信息，请参阅*《参考指南》*。
3. 设置 *Distribution_Server* 配置设置，以列出分发服务器（以逗号分隔）：

   `ssl://ds1.sample.com:7243, ssl://ds2.sample.com:7243`
4. 保存设置。

   现已配置端点可与其通讯的分发主机和分发服务器的列表。 现在，端点能够在高可用性环境中工作。

示例：配置分发服务器列表

以下示例显示如何针对高可用性配置分发服务器列表。

在安装端点的过程中，您需要输入与端点进行通讯的分发服务器的参数。 默认情况下，它是企业管理服务器。 为实现高可用性，可以将端口配置为在主分发服务器出现故障时使用辅助分发服务器。

1. 输入主分发服务器和辅助分发服务器的名称：

   ```
   dmsmgr -config -dhname DH__@node1.computer.com,DH__@node2.computer.com
   ```

   此时将显示一条消息，要求您确认操作。

2. 指定主分发服务器和辅助分发服务器的 URL 的列表。

   - UNIX：修改 accommon.ini 文件的 [communication] 部分中的 Distribution_Server 参数。
   - Windows：修改 Windows 注册表的 Distribution_Sever 值。 该参数在下列位置：

     ```
     HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\通讯
     ```

更多信息：

安装和自定义 Windows 端点 (p. 145)
安装和自定义 UNIX 端点 (p. 175)

针对高可用性的 Oracle RAC 配置

如果您使用 Oracle 作为策略和报告数据库，则可使用 Oracle RAC 配置 Oracle 以实现高可用性。Oracle Real Applications Cluster (RAC) 是基于共享磁盘体系结构的群集数据库，该体系结构为 Oracle 数据库提供了高可用性。

示例：使用 Oracle RAC 配置 CA Access Control 企业管理 for High Availability

以下示例说明如何将 CA Access Control 企业管理 配置为使用 Oracle RAC，以实现高可用性。

1. 为企业管理准备 Oracle 数据库。

   在 Oracle RAC 服务器上创建用户帐户，并分配安装 CA Access Control 企业管理 的用户特权。

2. 实施 CA Access Control 企业管理 for High Availability。

   安装并配置主企业管理服务器和辅助企业管理服务器。

   注意：在“主机名”字段中指定 Oracle RAC 的逻辑名称，在“服务名称”字段中指定共享服务名称。

3. 确认可以正确解析 Oracle RAC 主机名。

   将主机 IP 地址映射到 Oracle RAC 的逻辑名称。 例如：

   ```
   11.11.111.11  Node1MachineName
   11.11.111.12  Node2MachineName
   11.11.111.11  Node1LogicalMachineName
   11.11.111.12  Node2LogicalMachineName
   ```

4. 修改主企业管理服务器和辅助企业管理服务器设置，以使用 Oracle RAC。 请执行以下操作：

   a. 停止 JBoss 应用程序服务器。

   b. 导航到以下路径，其中 JBoss_HOME 表示 JBoss 的安装目录：

      ```
      JBoss_HOME/server/default/deploy
      ```

5. 打开以下文件进行编辑：

   ```
   imauditdb-ds.xml
   imtaskpersistencedb-ds.xml
   imworkflowdb-ds.xml
   objectstore-ds.xml
   reportsnapshot-ds.xml
   ```

6. 在每个文件中，找到 <connection-url> 标记，然后按如下所述指定主机名和服务名称：

   ```
   <connection-url>jdbc:oracle:thin:@(DESCRIPTION=(LOAD_BALANCE=off)(FAILOVER=on)(ADDRESS_LIST=(ADDRESS=(protocol=tcp)(host=Node1LogicalMachineName)(port=1521))(ADDRESS=(protocol=tcp)(host=Node2LogicalMachineName)()(port=1521)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=SharedService)))</connection-url>
   ```

7. 在每个文件中添加以下行：

   ```
   <check-valid-connection-sql>select 1 from dual</check-valid-connection-sql>
   ```

8. 保存并关闭文件。

9. 启动 JBoss 应用程序服务器。

现已配置主企业管理服务器和辅助企业管理服务器。

第 11 章： 安装灾难恢复部署

此部分包含以下主题：

灾难恢复概述

在子系统崩溃或其他灾难性故障发生之后，可利用灾难恢复还原系统。

灾难恢复的目标是还原尽可能多的数据，并且限制在备份和还原阶段期间所需的资源。

更多信息：

灾难恢复

在出现灾难性的系统故障时，灾难恢复部署可更方便地还原企业管理服务器。 如果 CA Access Control 和 PUPM 端点无法连接到生产环境，他们将连接到灾难恢复环境，直到还原生产环境。

灾难恢复部署有以下优点：

- 灾难恢复 DMS 的数据库是生产 DMS 数据库的复制品。 这意味着如果生产 DMS 数据库损坏，您具有策略的副本。
- 端点可以连接到生产或灾难恢复环境。 如果生产环境关闭，端点将数据发送到灾难恢复环境，因此，如果发生灾难性的系统故障，有关策略状态和偏差的信息不会丢失。
- 从灾难恢复之后，无需重新订阅每个端点。

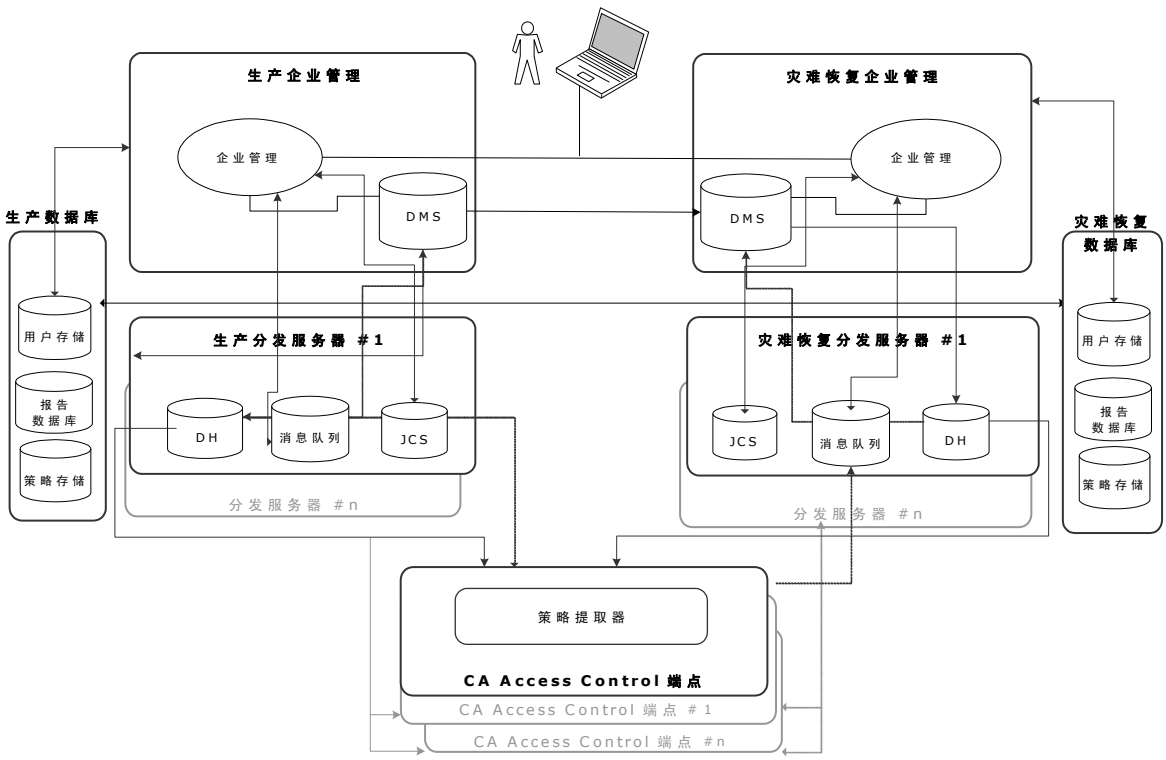
在灾难恢复过程中，不会备份或还原以下 CA Access Control 组件。 单独备份这些组件：

- 密码策略模型
- PMDB
- RDBMS
- CA Access Control 端点管理
- CA Access Control 企业管理
- 端点上的数据
- CA Access Control 审核文件
- CA Access Control 端点
- 报告
- 消息队列
- CA Business Intelligence

注意：备份 DMS 时，保存了 DMS 审核文件。

灾难恢复体系结构

下图显示如何在灾难恢复配置中部署 CA Access Control。



用于灾难恢复的组件

您需要以下组件在灾难恢复配置中部署 CA Access Control：

- 对于生产环境：
  - 企业管理服务器的一次安装
  - 中央数据库 (RDBMS)
  - 分发服务器的一次或多次安装。
- 对于灾难恢复环境：
  - 企业管理服务器的一次安装
  - 中央数据库 (RDBMS)
  - 分发服务器的一次或多次安装。

在计划灾难恢复部署时，考虑以下几点：

- 只能从保存在相同平台、操作系统和 CA Access Control 版本上的备份文件还原 DMS。 例如：无法从使用 CA Access Control r12.0 SP1 的 DMS 的备份文件还原使用 CA Access Control r12.5 的 DMS。
- 您可以在 RDBMS 上设置群集或其他故障转移解决方案。
- 您应在生产和灾难恢复服务器之间同步 RDBMS 中的数据。
- 您应在生产和灾难恢复服务器之间同步消息队列数据存储。

端点上的灾难恢复部署如何工作

灾难恢复部署创建生产分发服务器数据库的复制品，帮助确保从端点发送的数据不会在系统故障中丢失，并且轻松地实现在灾难之后还原生产环境。

以下过程描述端点上的灾难恢复部署如何工作：

1. 配置要与生产和灾难恢复分发服务器的列表一起使用的端点。

2. 在指定的时间，端点尝试连接到生产环境中的分发服务器。

   a. 端点尝试连接到其列表中的第一个生产分发服务器。 如果它未连接，则以指定的次数尝试连接到该分发服务器。 会出现以下情况之一：

      - 端点连接到生产分发服务器。 该过程在此步骤完成。
      - 端点无法连接到生产分发服务器。 该过程转至步骤 b。

      注意：端点尝试连接到分发服务器的次数以及要连接的分发服务器在通讯部分中的 Distribution_Server 配置设置和 policyfetcher 部分中的 max_dh_command_retry 配置设置中定义。

   b. 端点尝试连接到其列表中的第二个生产分发服务器，然后连接到第三个，依此类推（如果必要，以定义的相同次数）。 会出现以下情况之一：

      - 端点连接到生产分发服务器。 该过程在此步骤完成。
      - 端点无法连接到任何生产分发服务器，循环结束。 该过程转至步骤 3。

3. 端点以指定的循环次数重复步骤 2。 会出现以下情况之一：

   - 端点连接到生产分发服务器。 该过程在此步骤完成。
   - 端点未连接到生产分发服务器。 该过程转至下一步。

     注意：端点尝试连接到分发服务器的次数以及要连接的分发服务器在通讯部分中的 Distribution_Server 配置设置和 policyfetcher 部分中的 max_dh_command_retry 配置设置中定义。

4. 端点尝试连接到其列表中的第一个灾难恢复分发服务器。 如果它未连接到该分发服务器，则尝试连接到其列表中的第二个灾难恢复分发服务器，然后连接到第三个，依此类推，直到端点与灾难恢复分发服务器连接。

   注意：如果端点无法连接到生产或灾难恢复分发服务器，它不会将检测信号发送到 DMS。 要确定端点处于联机状态还是脱机状态，请检查上次向 DMS 发送检测信号通知的时间。

5. 当它连接到灾难恢复分发服务器之后，端点继续尝试连接到生产分发服务器。 会出现以下情况之一：

   - 端点连接到生产分发服务器，然后返回到生产环境。
   - 端点未连接生产分发服务器。 端点保留在灾难恢复环境中，重复步骤 4。

   注意：有关 policyfetcher 和通讯部分的详细信息，请参阅*《参考指南》*。

如何安装灾难恢复部署

为了确认已正确地彼此订购灾难恢复组件，按以下过程中指定的顺序设置生产和灾难恢复组件。

在出现灾难性的系统故障时，灾难恢复配置可可更方便地还原企业管理服务器组件。 您可能需要单独备份其他 CA Access Control 组件，例如中央数据库 (RDBMS)。

重要说明！：您不能从使用其他操作环境或 CA Access Control 版本的备份文件还原 DMS。 确认生产和灾难恢复环境部署在相同平台、操作系统和 CA Access Control 版本上。

注意：该过程假设您在独立主机上安装了 DMS 和 DH。

以下过程说明了如何安装灾难恢复部署：

1. 设置生产企业管理服务器 (p. 331)
2. 设置灾难恢复企业管理服务器 (p. 333)
3. 配置生产和灾难恢复服务器之间的数据库复制
4. 配置 DMS 订阅 (p. 335)
5. 同步消息队列服务器数据文件 (p. 350)
6. 设置端点 (p. 336)。

注意：建议您通过群集或允许站点之间的数据同步的任何其他方法来安装 RDBMS。

设置生产 CA Access Control 企业管理

生产企业管理服务器包含 DMS。 DMS 存储有关策略版本、策略脚本和每个端点的策略部署状态的最新信息。 使用生产 DMS 来部署和管理您的企业策略。

因为生产 DH 和灾难恢复 DMS 订阅生产 DMS，所以在设置任何其它灾难恢复组件之前设置生产 DMS。 这帮助确保在稍后的安装过程中正确地配置订阅。

设置生产企业管理服务器

1. 实施企业管理服务器 (p. 47)。

   安装所有基于 Web 的应用程序、分发服务器、DMS 以及 CA Access Control。

2. （可选）实施分发服务器 (p. 337)。

   安装消息队列和 Java 连接器服务器。

3. （可选）如果要从企业管理服务器中删除本地 DH，并使用分发服务器上的 DH，以维护管理和分发服务器之间的分隔，在生产企业管理服务器上运行以下命令：

   `dmsmgr -remove -dh name`

   -dh *name*

   使用在本地主机上 *name* 所指定的名称删除 DH。

   示例： *dmsmgr -remove -dh DH*

   以上示例从主机中删除名为 DH 的 DH。

   创建了无订户的生产 DMS。

4. 将消息队列配置为以故障安全模式工作。 请执行以下操作：

   a. 导航到下列目录，其中 *ACServerInstallDir* 是安装企业管理服务器的目录：

      ACServerInstallDir`/MessageQueue/tibco/cfgmgmt/ems/data`

   b. 打开 queues.conf 文件进行编辑。

   c. 在每个队列定义行的结尾添加“**failsafe**”，然后保存并关闭文件。

5. 使用本地 DMS 配置 CA Access Control 企业管理。 (p. 319)

   您已经安装并配置了生产企业管理服务器。 现在可以配置灾难恢复企业管理服务器。

示例：编辑 queues.conf 文件

以下示例是来自 queues.conf 文件的片段，说明了如何修正文件以将消息队列配置为使用共享存储。

```
queue/snapshots secure,failsafe
queue/audit secure,failsafe
ac_endpoint_to_server secure,failsafe
ac_server_to_endpoint secure,failsafe
```

设置灾难恢复 CA Access Control 企业管理

灾难恢复企业管理服务器部署和管理出现灾难性的系统故障时的企业策略。 因为灾难恢复企业管理服务器是生产企业管理服务器的订户，其数据库包含与生产企业管理服务器相同的策略版本、策略脚本和端点部署状态信息。

注意：在您设置灾难恢复企业管理服务器之前配置生产企业管理服务器。

设置灾难恢复企业管理服务器

1. 将 FIPSKey.dat 文件从生产企业管理服务器复制到灾难恢复服务器。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/config/com/netegrity/config/keys
   ```

2. 在灾难恢复服务器上实施企业管理服务器 (p. 47)。

   安装所有基于 Web 的应用程序、分发服务器、DMS 以及 CA Access Control。

   重要说明！ 指定在您启动安装过程时，从生产企业管理服务器中复制的 FIPSKey.dat 文件。 例如：

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

3. （可选）实施灾难恢复分发服务器 (p. 340)。

   安装消息队列和 Java 连接器服务器。

4. （可选）如果您要删除本地 DH，并使用分发服务器上的 DH，以维护管理和分发服务器之间的分隔，在灾难恢复企业管理服务器上运行以下命令：

   ```
   dmsmgr -remove -dh name
   ```

   -dh *name*

   使用在本地主机上 *name* 所指定的名称删除 DH。

   示例：*dmsmgr -remove -dh DH*

   创建了无订户的灾难恢复 DMS。

5. 将消息队列配置为以故障安全模式工作。 请执行以下操作：
   a. 导航到下列目录，其中 *ACServerInstallDir* 是安装企业管理服务器的目录：

      ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

   b. 打开 queues.conf 文件进行编辑。
   c. 在每个队列定义行的结尾添加“**failsafe**”，然后保存并关闭文件。
6. 使用本地 DMS 配置 CA Access Control 企业管理。 (p. 319)

您已经安装并配置了灾难恢复企业管理服务器。

示例：编辑 queues.conf 文件

以下示例是来自 queues.conf 文件的片段，说明了如何修正文件以将消息队列配置为使用共享存储。

```
queue/snapshots secure,failsafe
queue/audit secure,failsafe
ac_endpoint_to_server secure,failsafe
ac_server_to_endpoint secure,failsafe
```

配置 DMS 订阅

灾难恢复企业管理服务器是生产企业管理服务器的订户。 因此，其数据库包含与生产企业管理服务器相同的策略版本、策略脚本和端点部署状态信息。

将灾难恢复企业管理服务器的数据库配置为生产企业管理服务器的订户来同步这两个数据库。

配置 DMS 订阅

1. 移至灾难恢复企业管理服务器。
2. 将生产企业管理服务器定义为灾难恢复企业管理服务器的父项。 运行以下命令：

   ```
   env pmd
   subs drpmd_name parentpmd(<pr_dms_pmdname>@pr_host)
   ```

   drpmd_name

   定义灾难恢复 PMDB 的名称。
3. 移至生产企业管理服务器：
4. 运行以下命令：

   ```
   sepmd -ul dms_name
   ```

   prDMS_name

   定义生产 DMS 的名称。

   drDMS_name

   定义灾难恢复 DMS 的名称。 按照以下格式指定灾难恢复 DMS：*drDMS_name@hostname*。

灾难恢复企业管理服务器订阅到生产企业管理服务器，并与其同步。

设置端点

在生产和灾难恢复环境中安装企业管理服务器后，需要在企业中配置每个端点，以便与生产和灾难恢复服务器组件一起使用。 执行此操作时，需将端点配置为将信息发送到服务器组件并从服务器组件接收信息。

注意：在安装过程中，提供高级策略管理服务器组件的主机名。 按下列格式输入生产 DH 的名称：*prDH_name@hostname*[, *prDH_name@hostname*..]

设置端点

1. 在端点主机上安装 CA Access Control 端点功能，并启用高级策略管理客户端组件。

   CA Access Control 端点功能安装在主机上，并且端点订阅生产 DH。

2. 在端点上打开 selang 命令窗口。

3. 输入下面的命令：

   `so dh_dr+(drDH_name[, drDH_name...])`

   drDH_name

   定义灾难恢复 DH 的名称。格式：*drDH_name@hostname*。

   端点订阅到灾难恢复 DH。

4. 指定生产和灾难恢复分发服务器 URL 的列表。

   - UNIX：修改 accommon.ini 文件的 [communication] 部分中的 Distribution_Server 参数。
   - Windows：修改 Windows 注册表的 Distribution_Sever 值。 该参数在下列位置：

     `HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\common\communication`

   注意：有关 Distribution_Server 值的详细信息，请参阅*《参考指南》*。

   注意：您也可以通过创建包含所述 selang 命令的策略并且把它部署到端点，来将端点订阅到灾难恢复 DH。 有关创建和部署策略的详细信息，请参阅 *《企业管理指南》*。

安装灾难恢复部署的其他信息

下列主题说明了安装灾难恢复部署所需执行的其他配置步骤。

安装分发服务器

在配置 CA Access Control 以便在灾难恢复或高可用性环境中工作时，在独立计算机上安装分发服务器，并配置分发服务器以便在它们之间传播文件。

安装分发服务器

1. 将操作系统相应的 CA Access Control 高级版 服务器组件 DVD 插入光盘驱动器。
2. 请执行以下操作之一：
   - 在 Windows 上：

     如果已启用自动运行，产品资源管理器将自动显示。 请执行以下操作：

     a. 如果不出现产品资源管理器，导航到光盘驱动器目录并且双击 ProductExplorerx86.EXE 文件。

     b. 展开产品资源管理器中的“组件”文件夹，选择 CA Access Control 分发服务器，然后单击“安装”。

     将启动 InstallAnywhere 安装程序。
   - 在 UNIX 上：

     a. 挂接光盘驱动器。

     b. 打开终端窗口并导航至光盘驱动器上的以下目录：

     /DistServer/Disk1/InstData/NoVM

     c. 运行以下命令：

     ```
     ./install_DistServer_r125.bin -i console
     ```

     将启动 InstallAnywhere 安装程序。

3. 按照需要完成该向导。 以下安装输入需加以说明：

消息队列设置

定义消息队列服务器管理员的密码。

限制：最少六 (6) 个字符。

Java 连接器服务器－配给目录信息

定义 Java 连接器服务器的密码。

注意：Java 连接器服务器为 CA Access Control 企业管理 提供特权帐户管理功能。

CA Access Control 分发服务器安装已完成。

注意：如果在灾难恢复实施过程中安装分发服务器，则必须完成其他步骤。

更多信息：

设置生产分发服务器 (p. 338)
设置灾难恢复分发服务器 (p. 340)

设置生产分发服务器

生产分发服务器包含 DH。 DH 将生产 DMS 上创建的策略部署分发至端点，并且从端点接收部署状态更新以发送给生产 DMS。

因为生产 DH 和灾难恢复 DMS 订阅生产 DMS，所以在设置任何其它灾难恢复组件之前设置生产 DMS。 这帮助确保在稍后的安装过程中正确地配置订阅。

设置生产分发服务器

1. 在生产分发服务器计算机上安装分发服务器 (p. 337)。
2. 在生产分发服务器上运行以下命令来配置 DH：

   ```
   dmsmgr -remove -auto
   ```

   ```
   dmsmgr -create -dh name -parent name\
   [-admin user[,user...]] [-desktop host[,host...]]
   ```

   -dh *name*

   使用在本地主机上 *name* 所指定的名称创建 DH。

   -parent *name*

   定义 DH 要将端点通知发送到的生产 DMS。 按照以下格式指定生产 DMS：*DMS_name@hostname*。

   -admin *user*[,*user*...]

   （可选）将内部用户定义为创建的 DH 的管理员。

   -desktop *host*[,*host*...]

   （可选）定义对附带已创建 DH 的计算机具有 TERMINAL 访问权限的计算机列表。

   注意：无论指定与否，运行此实用程序的终端将始终被授予对已创建 DH 的管理权限。

   已创建和配置生产 DH。

3. 运行以下命令：

   ```
   sepmd -n prDMS_name prDH_name
   ```

   prDMS_name

   定义生产 DMS 的名称。

   prDH_name

   定义生产 DH 的名称。 请按以下格式指定名称：*prDH_name@hostname*。

   示例：DH__@prdh.com

   DH 订阅到生产 DMS，并与其同步。

4. 设置分发服务器和生产 DMS 之间的消息队列路由 (p. 85)。
5. 为每个生产分发服务器重复步骤 1-4。

设置灾难恢复分发服务器

因为灾难恢复分发服务器是生产分发服务器的订户，其数据库包含与生产分发服务器相同的策略版本、策略脚本和端点部署状态信息。

注意：必须在设置灾难恢复分发服务器之前设置生产分发服务器。

设置灾难恢复分发服务器

1. 在灾难恢复分发服务器计算机上安装分发服务器 (p. 337)。
2. 在灾难恢复分发服务器上运行以下命令来配置 DH：

   ```
   dmsmgr -remove -auto
   ```

   ```
   dmsmgr -create -dh name -parent name\
   [-admin user[,user...]] [-admin user[,user...]]
   ```

   -dh *name*

   使用在本地主机上 *name* 所指定的名称创建 DH。

   -parent *name*

   定义 DH 要将端点通知发送到的灾难恢复 DMS。 按照以下格式指定灾难恢复 DMS：*drDMS_name@hostname*。

   -admin *user* [*,user...*]

   （可选）将内部用户定义为创建的 DH 的管理员。

   -desktop *host*[*,host...*]

   （可选）定义对附带已创建 DH 的计算机具有 TERMINAL 访问权限的计算机列表。

   注意：无论指定与否，运行此实用程序的终端将始终被授予对已创建 DH 的管理权限。

   已创建和配置灾难恢复 DH。

3. 在灾难恢复分发服务器上运行以下命令：

   ```
   sepmd -n drDMS_name drDH_name
   ```

   drDMS_name

   定义灾难恢复 DMS 的名称。

   drDH_name

   定义灾难恢复 DH 的名称。 请按以下格式指定名称：*drDH_name@hostname*。

   示例：DH__@drdh.com

   DH 订阅到灾难恢复 DMS，并与其同步。

4. 设置分发服务器和灾难恢复 DMS 之间的消息队列路由 (p. 85)。
5. 为每个灾难恢复分发服务器重复步骤 1-4。

灾难恢复过程

灾难恢复过程有两个阶段：备份和还原。 在备份阶段中，DMS 数据库中的数据复制到另一个目录中。 在还原阶段中，dmsgmr 实用程序使用备份 DMS 文件来还原现有的 DMS，或创建 DMS。

注意：灾难恢复配置有助于在遭遇灾难性系统故障时更轻松地还原高级策略管理组件。 您可能需要单独备份其他 CA Access Control 组件。

更多信息：

可还原的数据 (p. 341)
何时还原 DMS (p. 342)
何时还原 DH (p. 342)
如何还原 DMS (p. 342)
如何还原 DH (p. 343)

可还原的数据

还原 DMS 时，dmsmgr 使用来自其他 DMS 的备份文件来创建新的 DMS。 还原 DH 时，dmsmgr 会将 DMS 备份文件的数据复制到 DH Reader 目录。 这两种情况还原相同的数据。

您还原的数据是 DMS 数据库中数据的副本，包括：

- 有关企业策略、版本和分配的信息
- 有关部署和策略状态、部署偏差和部署层级结构的信息
- 主机和主机组定义
- 配置设置
- updates.dat 文件
- 注册表项
- DMS 审核文件

注意：您无需还原 DH__Writer，因为它具有临时数据库。

何时还原 DMS

还原 DMS 时，dmsmgr 使用来自其他 DMS 的备份文件来创建新的 DMS。 以下方案说明还原生产 DMS 的时间：

- 发生灾难性的生产系统故障时。
- 生产 DMS 数据库损坏时。
- 需要在另一主机上设置新的生产 DMS 时。

以下方案说明还原灾难恢复 DMS 的时间：

- 灾难恢复 DMS 与生产 DMS 不同步时。
- 灾难恢复 DMS 数据库损坏时。
- 需要在另一主机上设置新的灾难恢复 DMS 时。

注意：可以在现有的 DMS 上还原 DMS，或还原到不存在 DMS 的新目录中。

何时还原 DH

还原 DH 时，dmsmgr 会将 DMS 备份文件的数据复制到 DH Reader 目录。 以下方案说明了还原 DH 的时间：

- 发生灾难性的生产系统故障时。
- DH 数据库损坏时。
- DH 与其 DMS 不同步时。
- 需要在另一主机上设置新的 DH 时。

注意：您无需还原 DH Writer，因为它是一个临时数据库。 在还原 DH 之前，请检查 DH Writer 是否存在于现有 DH 文件结构中。

如何还原 DMS

了解 dmsmgr 实用程序如何还原 DMS 可帮助您诊断在还原过程中可能发生的任何问题。

以下过程说明了 dmsmgr 如何还原 DMS：

1. dmsmgr 删除现有的 DMS。
2. dmsmgr 将备份 DMS 文件从您指定的位置复制到 DMS 目录。
3. dmsmgr 删除 DMS 的所有订户。

4. 会出现以下情况之一：
   - 如果还原生产 DMS，dmsmgr 将灾难恢复 DMS 作为第一个订户添加到生产 DMS，偏移值等于存储在备份文件中的最后的全局偏移。
   - 如果还原灾难恢复 DMS，dmsmgr 将灾难恢复 DMS 重新订阅到生产 DMS，偏移值等于存储在备份文件中的最后的全局偏移。
5. dmsmgr 为 DMS 订阅每个 DH。 每个 DH 偏移值为 0，并且未处于同步状态。

   注意：DH 不同步时，无法接收来自 DMS 的更新。 要解除 DH 的不同步状态，请还原 DH。

如何还原 DH

了解 dmsmgr 实用程序如何还原 DH 可帮助您诊断在还原过程中可能发生的任何问题。

以下过程说明了 dmsmgr 如何还原 DH：

1. dmsmgr 删除现有的 DH。
2. dmsmgr 将备份 DH 文件从您指定的位置复制到 DH 目录。
3. dmsmgr 为 DMS 订阅 DH，偏移值等于存储在备份文件中的上次全局偏移。
4. dmsmgr 在 DH 上清除未同步的标志。

偏移值

updates.dat 文件存储 DMS 部署的每个命令。 创建新的订户时，策略模型将 updates.dat 文件中的命令发送到订户。 每个命令都有递增的数字下标，称为*偏移值*。

当您将订户添加到 DMS 时，可以指定偏移：

- **0**－策略模型将所有命令发送到订户。
- **最后一个偏移**－策略模型不将任何命令发送到订户。
- **0 和最后一个偏移之间的整数 X**－策略模型将 X 和最后一个偏移之间的所有命令发送到订户。

不同步的订户

*不同步的订户*是上次截断 updates.dat 文件以来尚未接收任何更新的订户。 标记不同步的订户可使 CA Access Control 忽略该订户，不会将命令发送给该订户。

不同步的订户不会从其父 DMS 或策略模型接收任何更新。 要清除不同步的标志并允许订户接收更新，您必须将订户重新订阅到其父项。

如果父 DMS 或策略模型的每个订户都未同步，则父项实际上没有订户。

如何从灾难中恢复

如果生产系统发生故障，则端点会在灾难恢复环境中工作。 从灾难中恢复时，操作将从灾难恢复环境移回还原的生产环境。

以下过程说明了如何从灾难中恢复：

1. 停止生产企业管理服务器和生产分发服务器上的 CA Access Control。
2. 停止所有在灾难恢复 DMS 中的管理工作，即停止 CA Access Control 企业管理 和 policydeploy 实用程序。
3. （可选）自动截短 updates.dat 文件。
4. 备份灾难恢复 DMS。 您可以使用以下方法之一备份 DMS：
   - 本地备份 (p. 345)
   - 远程备份 (p. 346)
5. 还原生产数据库 (RDBMS)。
6. 从灾难恢复 DMS 备份文件还原生产 DMS (p. 348)。
7. 在生产 DMS 上启动 CA Access Control。
8. 备份生产 DMS。您可以使用下列方法之一备份 DMS：
   - 本地备份 (p. 345)
   - 远程备份 (p. 346)
9. 从生产 DMS 备份文件还原每个生产 DH (p. 347)。
10. 在每台生产分发服务器上启动 CA Access Control。
11. 将所有管理工作移动到生产 DMS，即在生产 CA Access Control 企业管理 上启动 CA Access Control 企业管理 和 policydeploy 实用程序。

12. （可选）如果灾难恢复 DMS 与生产 DMS 不同步，请完成以下步骤：
    a. 从生产 DMS 备份文件还原灾难恢复 DMS (p. 349)。
    b. 备份灾难恢复 DMS。可以使用下列方法之一备份 DMS：
        - sepmd 使用程序 (p. 345)
        - selang 命令 (p. 346)
    c. 从灾难恢复 DMS 备份文件还原所有灾难恢复 DH (p. 347)。

使用 sepmd 备份 DMS

备份 DMS 来保存部署到端点的策略副本以及企业管理服务器从端点接收的报告快照的副本。

备份 DMS 时，数据将从 DMS 数据库复制到指定的目录。

sepmd 实用程序仅在本地主机上备份 DMS。 您应将备份的 DMS 文件存储至一个安全的位置，最好是受 CA Access Control 访问规则保护的位置。 建议您在备份 DMS 之前自动截短 updates.dat 文件。

注意：您还可以使用 selang 命令在本地或远程主机上备份 DMS。

使用 sepmd 备份 DMS

1. 使用以下命令锁定 DMS：

   ```
   sepmd -bl dms_name
   ```

   DMS 将锁定，并且无法向其订户发送任何命令。

2. 使用以下命令备份 DMS 数据库：

   ```
   sepmd -bd dms_name [destination_directory]
   ```

   dms_name

   定义在本地主机上备份的 DMS 的名称。

   destination_directory

   定义 DMS 备份到的目录。

   默认值：(UNIX) *ACInstallDir*/data/policies_backup/dmsName

   默认值：(Windows) *ACInstallDir*\data\policies_backup\dmsName

   DMS 数据库将备份到目标目录。

3. 使用以下命令解锁 DMS：

   ```
   sepmd -ul dms_name
   ```

   DMS 将解锁，并且将向其订户发送命令。

使用 selang 备份 DMS

备份 DMS，将数据从 DMS 数据库复制到指定的目录。

您可以使用 selang 命令在本地或远程主机上备份 DMS。 您应将备份的 DMS 文件存储至一个安全的位置，最好是受 CA Access Control 访问规则保护的位置。 建议您在备份 DMS 之前自动截短 updates.dat 文件。

注意：您还可以使用 sepmd 实用程序在本地主机上备份 DMS。

使用 selang 备份 DMS

1. （可选）如果要使用 selang 从远程主机连接 DMS，请使用以下命令连接 DMS 主机：

   ```
   host dms_host_name
   ```

2. 使用以下命令移至 PMD 环境：

   ```
   env pmd
   ```

3. 使用以下命令锁定 DMS：

   ```
   pmd dms_name lock
   ```

   DMS 将锁定，并且无法向其订户发送任何命令。

4. 使用以下命令备份 DMS 数据库：

   ```
   backuppmd dms_name [destination(destination_directory)]
   ```

   dms_name

   定义在本地主机上备份的 DMS 的名称。

   destination*(destination_directory)*

   定义 DMS 备份到的目录。

   默认值：(UNIX) *ACInstallDir*/data/policies_backup/dmsName

   默认值：(Windows) *ACInstallDir*\data\policies_backup\dmsName

   DMS 数据库将备份到目标目录。

5. 使用以下命令解锁 DMS：

   ```
   pmd dms_name unlock
   ```

   DMS 将解锁，并且将向其订户发送命令。

还原 DH

还原 DH，以使用 dmsmgr 实用程序将数据从 DMS 备份文件复制到 DH_Reader 目录。您无需还原 DH Writer，因为它具有临时数据库。 在还原 DH 之前，请检查 DH Writer 是否存在于现有 DH 文件结构中。

注意：如果 DH Writer 在现有 DH 文件结构中不存在，或者您要设置新的 DH，请在还原 DH 之前使用 dmsmgr -create 功能创建新的 DH。

注意：您必须具有对操作系统的完全管理权限，才可以使用 dmsmgr 实用程序。

要还原 DH，请在 DH 主机上运行以下命令：

```
dmsmgr -restore -dh name -source path -parent name\
[-admin user[,user...]] [-xadmin user[,user...]] [-desktop host[, host...]]
```

-admin *user*[,*user*...]

(UNIX) 将内部用户定义为还原的 DMS 或 DH 的管理员。

-desktop *host*[, *host*...]

（可选）定义对附带已还原 DH 的计算机具有 TERMINAL 访问权限的计算机列表。

注意：无论指定与否，运行此实用程序的终端将始终被授予对已还原 DH 的管理权限。

-dh *name*

定义在本地主机上还原的 DH 的名称。

-parent *name*

定义还原的 DH 将订阅到的父 DMS 的名称。 按照以下格式指定父 DMS：*DMS_name@hostname*。

-source *path*

定义包含要还原的备份文件的目录。

-xadmin *user*[,*user*...]

(UNIX) 将企业用户定义为还原的 DMS 或 DH 的管理员。

DH 将还原，且订阅到 DMS。

还原生产 DMS

还原生产 DMS 时，dmsmgr 会将数据从灾难恢复 DMS 备份文件复制到生产 DMS 目录。

注意：您必须具有对操作系统的完全管理权限，才可以使用 dmsmgr 实用程序。

要还原生产 DMS，请在生产 DMS 主机上输入以下命令：

```
dmsmgr -restore -dms name -source path -replica name\
[-subscriber dhname[,dhname...]] [-admin user[,user...]]\
[-xadmin user[,user...]]
```

-admin *user*[,*user*...]

(UNIX) 将内部用户定义为还原的 DMS 或 DH 的管理员。

-dms *name*

定义在本地主机上还原的 DMS 的名称。

-replica *name*

定义订阅到生产 DMS 的灾难恢复 DMS 的名称。按照以下格式指定灾难恢复 DMS：*DMS_name@hostname*。

-subscriber *dh_name*[, *dh_name*...]

（可选）定义还原的 DMS 要将策略更新发送到的 DH 的列表（以逗号分隔）。 指定以下格式的 DH：*DH_name@hostname*。

-source *path*

定义包含要还原的备份文件的目录。

-xadmin *user*[,*user*...]

(UNIX) 将企业用户定义为还原的 DMS 或 DH 的管理员。

生产 DMS 将还原。

注意：还原生产 DMS 后，您必须备份生产 DMS，并从备份文件还原生产 DH。 这可确保生产 DMS 和生产 DH 同步。

还原灾难恢复 DMS

还原灾难恢复 DMS 时，dmsmgr 会将数据从备份文件复制到灾难恢复 DMS 目录。

注意：您必须具有对操作系统的完全管理权限，才可以使用 dmsmgr 实用程序。

要还原灾难恢复 DMS，请在灾难恢复 DMS 主机上输入以下命令：

```
dmsmgr -restore -dms name -source path -parent name\
[-subscriber dhname[,dhname...]] [-admin user[,user...]]\
[-xadmin user[,user...]]
```

-admin *user*[,*user*...]

(UNIX) 将内部用户定义为还原的 DMS 或 DH 的管理员。

-dms *name*

定义在本地主机上还原的 DMS 的名称。

-parent *name*

定义还原的灾难恢复 DMS 将订阅到的生产 DMS 的名称。按照以下格式指定生产 DMS：*DMS_name@hostname*。

-source *path*

定义包含要还原的备份文件的目录。

-subscriber *dh_name*[, *dh_name*...]

（可选）定义还原的 DMS 要将策略更新发送到的 DH 的列表（以逗号分隔）。 指定以下格式的 DH：*DH_name@hostname*。

-xadmin *user*[,*user*...]

(UNIX) 将企业用户定义为还原的 DMS 或 DH 的管理员。

灾难恢复 DMS 将还原，并且将订阅到生产 DMS。

注意：还原灾难恢复 DMS 后，必须备份灾难恢复 DMS，并从备份文件还原灾难恢复 DH。 这可确保灾难恢复 DMS 和灾难恢复 DH 同步。

备份消息队列服务器数据文件

备份消息队列服务器数据文件，将数据从生产消息队列服务器复制到灾难恢复消息队列服务器。

要备份消息队列服务器数据文件，请将消息队列服务器数据文件从生产分发服务器复制到灾难恢复分发服务器。 默认情况下，数据文件位于以下目录，其中 *ACServerInstallDir* 是消息队列服务器的安装目录：

ACServerInstallDir/MessageQueue/tibco/ems/bin/datastore

还原消息队列服务器数据文件

还原消息队列服务器数据文件，将数据从灾难恢复消息队列服务器复制到生产消息队列服务器。

要还原消息队列服务器数据文件，请将消息队列服务器数据文件从灾难恢复分发服务器复制到生产分发服务器。 默认情况下，数据文件位于以下目录，其中 *ACServerInstallDir* 是消息队列服务器的安装目录：

ACServerInstallDir/MessageQueue/tibco/ems/bin/datastore

如何同步消息队列服务器数据文件

当您在灾难恢复环境中工作时，使生产和灾难恢复消息队列服务器同步至关重要。 同步服务器有助于确保生产和灾难恢复消息队列服务器上的数据更新，同时，如果生产服务器无法正常工作，灾难恢复服务器可以继续为数据服务且不造成中断。

注意：同步解决方案基于第三方复制工具。 验证存储解决方案按与数据缓冲区中相同的顺序将数据块写入共享存储。 验证从同步写入调用返回时，存储解决方案是否能够确保所有数据已写入持久性存储。

要使消息队列服务器的数据文件同步，请执行以下操作：

1. 在生产分发服务器上，设置消息队列服务器和安装在企业管理服务器上的所有消息队列服务器之间的消息路由设置。
2. 设置灾难恢复分发服务器和灾难恢复企业管理服务器上的消息队列服务器之间的消息路由设置。

3. 在企业管理服务器上修改灾难恢复服务器和生产消息队列服务器上的 queues.conf 文件，并添加 fail-safe 行。

   例如：

   ```
   queue/snapshots secure,failsafe
   queue/audit secure, failsafe
   ac_endpoint_to_server secure, failsafe
   ac_server_to_endpoint secure,failsafe
   ```

   默认情况下，该文件位于以下目录，其中 *ACServerInstallDir* 是企业管理服务器的安装目录：

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

4. 使用第三方复制工具，将企业管理服务器上的生产消息队列服务器 EMS 数据文件复制到灾难恢复企业管理服务器上的消息队列服务器。

   默认情况下，消息队列服务器 EMS 数据文件位于以下目录，其中 *ACServerInstallDir* 是企业管理服务器的安装目录：

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data/datastore

   您已经配置了消息队列服务器 EMS 数据文件同步设置。

第 12 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。

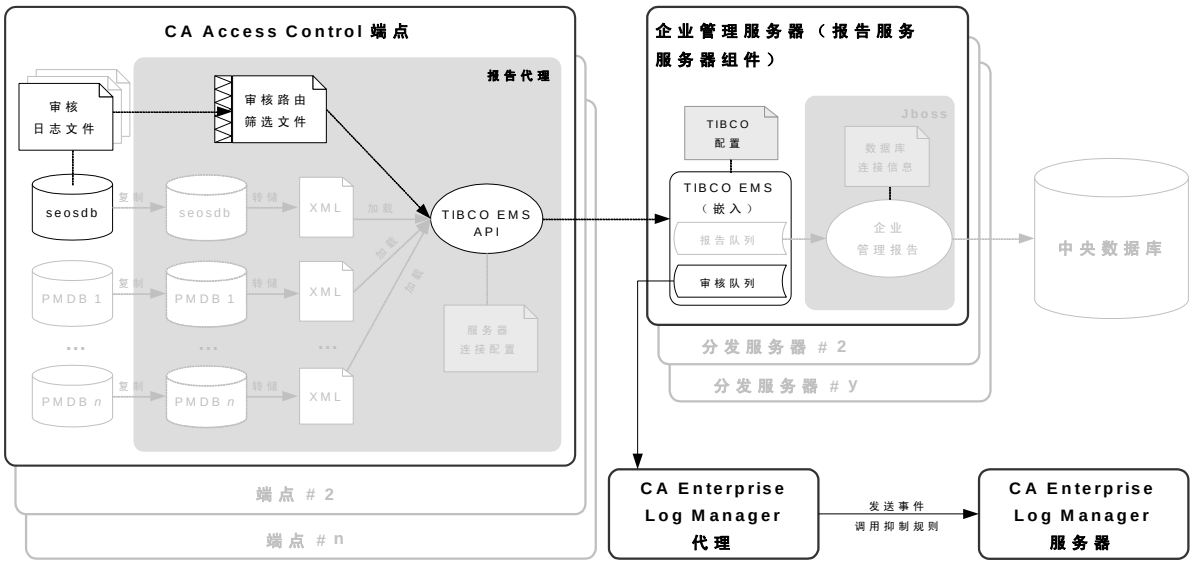
CA User Activity Reporting Module 集成体系结构

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

您可以配置 CA Access Control，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 Access Control 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 Access Control 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。

更多信息：

报告服务体系结构 (p. 95)

CA Enterprise Log Manager 集成组件

CA Enterprise Log Manager 集成使用以下 CA Access Control 组件。 这些组件是 CA Access Control 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 Access Control 或 UNAB 端点上运行，并将信息发送到驻留在分发服务器上的已配置消息队列中的队列。 对于 CA Enterprise Log Manager 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 Access Control 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。

CA Enterprise Log Manager 集成还使用以下 CA Enterprise Log Manager 组件：

- *CA Enterprise Log Manager 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 CA Enterprise Log Manager 服务器进行处理。 对于 CA Access Control 审核数据，代理将部署 CA Access Control 连接器。
- *CA Access Control 连接器*是适用于 CA Access Control 审核事件源的即取即用的 CA Enterprise Log Manager 集成。 连接器允许从 CA Access Control 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 Enterprise Log Manager 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。

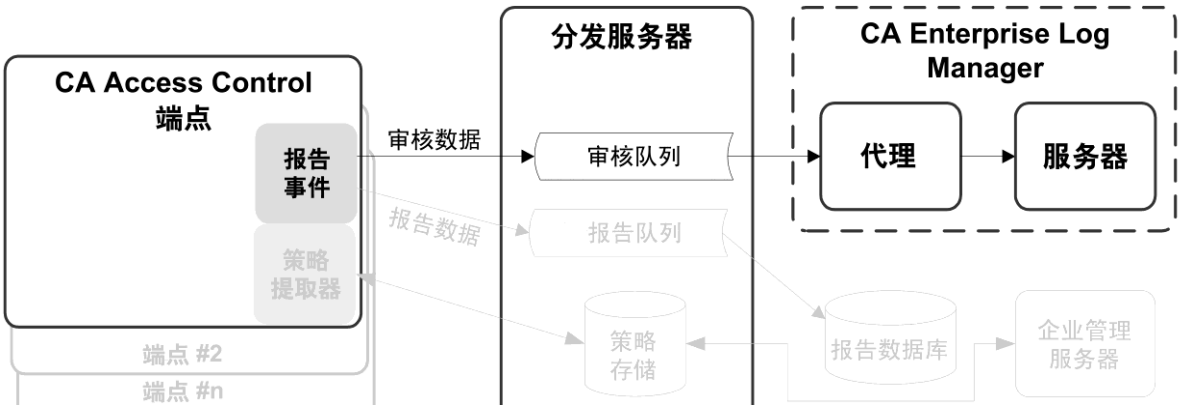
注意：有关 CA Enterprise Log Manager 组件的详细信息，请参阅 CA Enterprise Log Manager 文档。

更多信息：

报告服务体系结构 (p. 95)

审核数据如何从 CA Access Control 流向 CA Enterprise Log Manager

要了解 CA Access Control 如何与 CA Enterprise Log Manager 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 与 CA Enterprise Log Manager 之间的审核数据流。 下图说明了 CA Access Control 如何将审核事件传递给分发服务器上的消息队列，CA Enterprise Log Manager 代理的 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 Enterprise Log Manager 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 CA Enterprise Log Manager 代理部署的 CA Enterprise Log Manager 连接器与审核队列连接，并从该队列调用事件（消息）。
3. CA Enterprise Log Manager 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 CA Enterprise Log Manager 服务器。
4. CA Enterprise Log Manager 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 Enterprise Log Manager 工作原理的详细信息，请参阅 CA Enterprise Log Manager 文档。

如何为 CA Access Control 设置 CA Enterprise Log Manager

要使用 CA Enterprise Log Manager 创建包含来自所有 CA Access Control 端点的审核数据的报告，请首先实施企业报告。 您必须在与 CA Enterprise Log Manager 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 Access Control 设置 CA Enterprise Log Manager。

要为 CA Access Control 安装 CA Enterprise Log Manager，请执行以下步骤：

1. 安装 CA Enterprise Log Manager 服务器。

   注意：有关详细信息，请参阅 *《CA Enterprise Log Manager 实施指南》*。

2. 在分发服务器上或其附近安装 CA Enterprise Log Manager 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 CA Enterprise Log Manager 服务器。

   注意：安装 CA Enterprise Log Manager 代理之前请验证操作系统是否支持 CA Enterprise Log Manager 代理。 有关安装该代理的详细信息，请参阅 *《CA Enterprise Log Manager 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 CA Enterprise Log Manager 代理并与 CA Enterprise Log Manager 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 Access Control 事件源（分发服务器上的审核队列）。

   注意：下列主题说明了 CA Access Control 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 *《CA Enterprise Log Manager 管理指南》*和*联机帮助*。

5. 创建从 CA Access Control 企业管理 到 CA Enterprise Log Manager 的连接。

6. （可选）配置审核收集器。

7. 为审核收集配置 CA Access Control 端点。

更多信息：

企业报告功能 (p. 95)
如何设置报告服务服务器组件 (p. 97)

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。

为 CA Enterprise Log Manager 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 Access Control 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 CA Enterprise Log Manager 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 Access Control。

3. 单击“更改”。

   将显示 CA Access Control 安装向导。

   按照向导提示修改 CA Access Control 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 Access Control 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. 360)。 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 Access Control 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 Access Control 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. 360)。 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 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 (p. 72)。
2. 导出 CA Enterprise Log Manager 受信任证书并添加到密钥存储 (p. 366)。
3. 配置到 CA Enterprise Log Manager 的连接 (p. 367)。
4. （可选）配置审核收集器 (p. 369)。

   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 Enterprise Log Manager 受信任证书添加到密钥存储

CA Enterprise Log Manager 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 Enterprise Log Manager 源，从而验证数据的可靠性。

要查看 CA Access Control 企业管理 中的 CA Enterprise Log Manager 报告，首先要导出证书，然后再将其添加到密钥存储。

将 CA Enterprise Log Manager 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 CA Enterprise Log Manager 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 CA Enterprise Log Manager 的连接

CA Access Control 企业管理 可通过与 CA Enterprise Log Manager 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 Enterprise Log Manager 的连接。

配置到 CA Enterprise Log Manager 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 CA Enterprise Log Manager 连接”任务会显示在可用任务列表中。
2. 单击“管理 CA Enterprise Log Manager 连接”。

   将显示“管理 CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 主机的名称。

   示例： host1.comp.com

   端口号

   定义 CA Enterprise Log Manager 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 CA Enterprise Log Manager 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 CA Enterprise Log Manager 连接设置。

示例：获得 CA Enterprise Log Manager 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 Enterprise Log Manager 连接设置时需要提供的 CA Enterprise Log Manager 证书信息。

1. 使用以下格式在 Web 浏览器中输入 CA Enterprise Log Manager 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 Enterprise Log Manager 的有效用户名和密码。
3. 选择“注册”选项以在 CA Enterprise Log Manager 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 13 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. 373)。

   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 (p. 45)。
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。

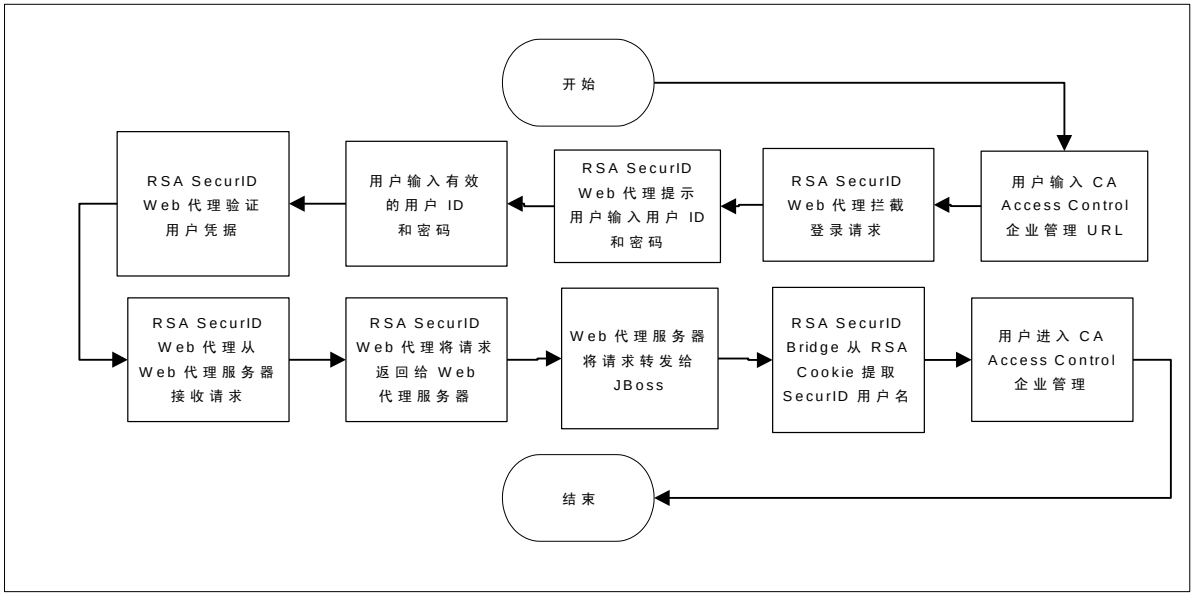
每当用户尝试登录到 CA Access Control 企业管理 时，RSA SecurID 会提示用户输入有效 RSA SecurID 凭据而不是 CA Access Control 企业管理 用户帐户详细信息。 如果通过身份验证，RSA SecurID 会将用户登录到 CA Access Control 企业管理。

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 14 章： 与多个 LDAP 服务器一起使用

此部分包含以下主题：

简介

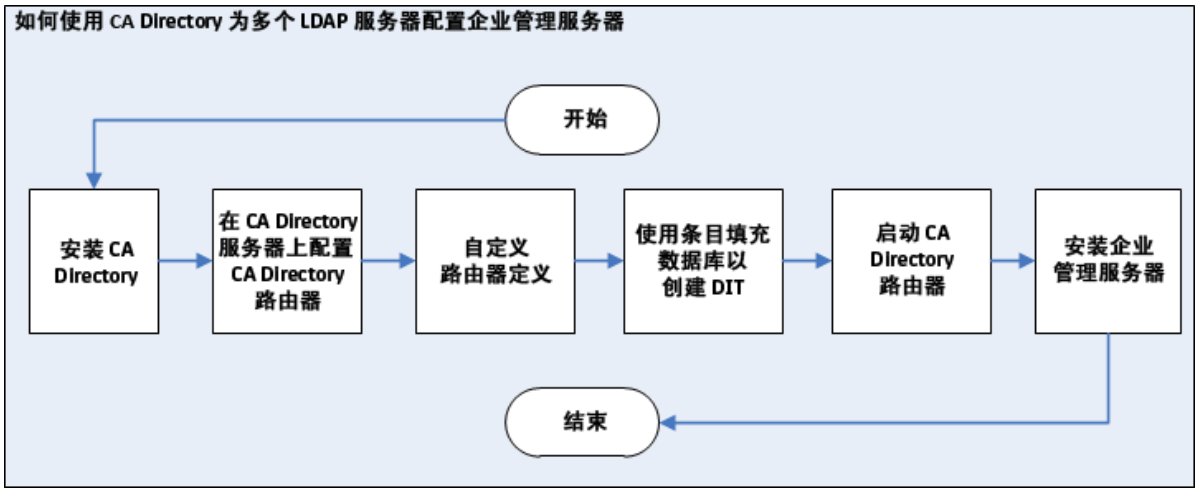
此章中该信息描述系统或数据库管理员如何将 CA Access Control 企业管理 配置为使用 CA Directory 与多个 LDAP 服务器一起使用。 通过与多个 LDAP 服务器一起使用，管理员可以将多个 LDAP 用户存储集成到单个企业范围的用户存储。

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，该实用程序可以在多个 LDAP 目录服务器上搜索。

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. 381)
3. 自定义 CA Directory 路由器定义 (p. 383)
4. 为数据库填充实体，创建 DIT (p. 386)
5. 启动 CA Directory
6. 安装企业管理服务器，以 Active Directory 作为用户存储 (p. 45)

   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－CA Directory 主机名
   - 端口号－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－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 Access Control 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 15 章： 与 CA SiteMinder 集成

此部分包含以下主题：

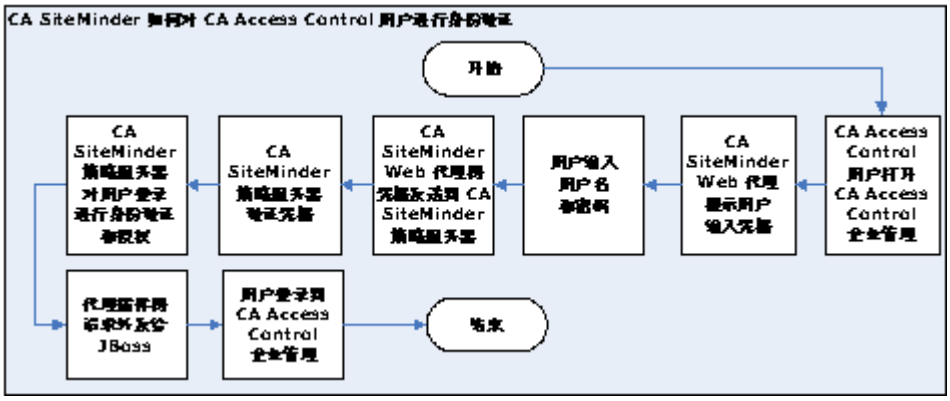
简介

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 Access Control 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 Access Control 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。

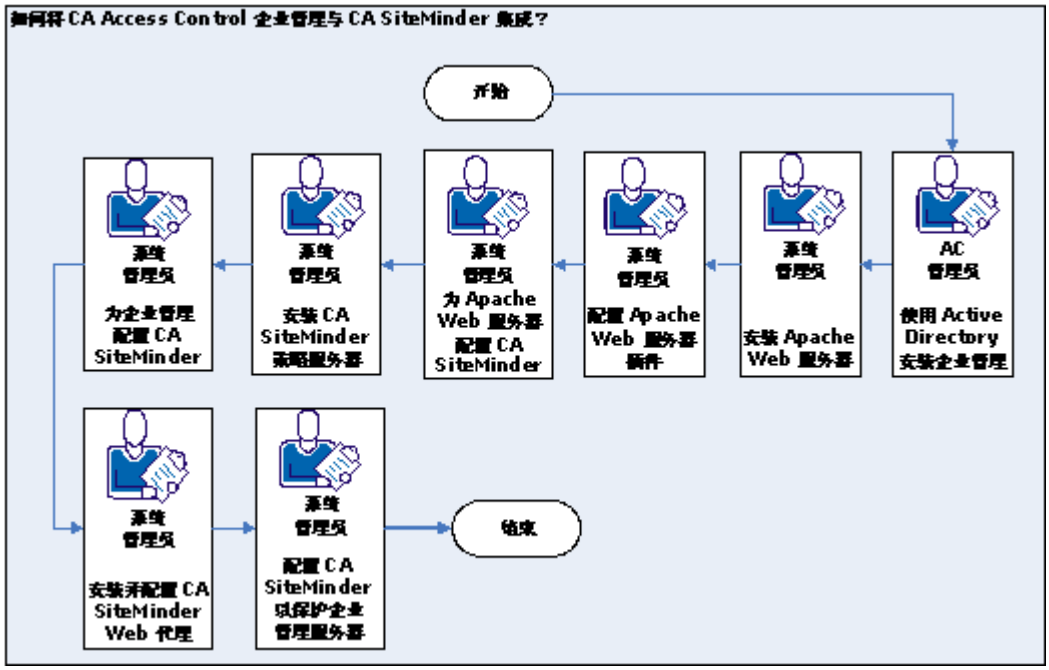
下图说明 CA SiteMinder 验证和授权 CA Access Control 用户登录到 CA Access Control 企业管理 的方式：



如何与 CA SiteMinder 集成

将 CA Access Control 企业管理 与 CA SiteMinder 集成可促进 CA SiteMinder 高级用户验证和授权功能。

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：



以下过程说明如何与 CA SiteMinder 集成：

1. 安装企业管理服务器 (p. 47)

   安装所有基于 Web 的应用程序、分发服务器、DMS 以及 CA Access Control。

   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。

2. 配置企业管理服务器上的 Apache Web 服务器 (p. 389)
3. 安装 CA SiteMinder 策略服务器
4. 为企业管理服务器配置 CA SiteMinder (p. 393)
5. 配置 CA SiteMinder Web 代理 (p. 394)
6. 配置 CA SiteMinder 以保护企业管理服务器 (p. 395)
7. 配置企业管理服务器以使用 CA SiteMinder 验证用户 (p. 397)

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。

示例：在企业管理服务器上配置 Apahce Web 服务器代理插件

在该示例中，您已在 Windows 2008 服务器上安装了企业管理服务器。 您也需要在启用 SSL 支持的企业管理服务器上安装 Apache Web 服务器版本 2.2.19。 您现在需要配置 Apache Web 服务器代理插件。 请执行以下操作：

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. 编辑 httpd.conf 文件，以便启用代理模块并包括代理配置：
   a. 取消注释以下行：

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

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

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

您已在企业管理服务器上配置了 Apache Web 服务器代理插件。

示例：为 Apache Web Server 配置 CA SiteMinder

在该示例中，在企业管理服务器上配置 Apache Web 服务器代理插件之后，现在您需要为 Apache Web 服务器配置 CA SiteMinder。

1. 使用 CA SiteMinder 管理员接口执行以下操作：
   a. 依次进入“开始”、“所有程序”、“CA”、“CA SiteMinder”、“CA SiteMinder 管理 UI”。

      CA SiteMinder 管理用户界面打开，提示用户输入用户名和密码。

   b. 登录到 CA SiteMinder 管理 UI。
   c. 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”。
   d. 选择“DefaultHostSettings 对象”，然后单击“确定”。
   e. 填写以下字段：
      - **名称**－webservernode-HCO
      - **说明**－Web 服务器主机配置
   f. 移到配置值框，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

   g. 单击“提交”。

   您已配置主机配置对象。
2. 选择“基础架构”、“代理”、“代理”、“创建代理”、“创建代理类型的新对象”。
3. 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**－清除

   您已配置 Web 代理对象。

4. 选择“代理配置”、“创建代理配置”、“创建代理类型配置的对象副本”。
5. 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 并删除名称值中的 # 字符。
   e. 如下设置值：
      - **LogoffUri**－/iam/logout.jsp

   注意：有关代理参数的更多信息，请参阅《CA *Site*Minder *代理配置指南*》。
6. 单击“提交”。

   您已创建代理配置对象。

示例：为企业管理服务器配置 CA SiteMinder

在该示例中，您为企业管理服务器配置 CA SiteMinder。

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
   - **说明**－ENTM 主机配置
7. 移到配置值框，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。 下一步您安装并配置 CA SiteMinder Web 代理。

示例：配置 CA SiteMinder Web 代理

在该示例中，系统管理员 Steve 在企业管理服务器上安装了 CA SiteMinder Web 代理。 Steve 使用他先前定义的主机和代理对象配置，现在为 Apache Web 服务器配置 Web 代理。

1. 请执行以下操作：
   a. 导航到以下目录，其中 *APACHE_HOME* 是您安装 Apache Web 服务器的目录：

      APACHE_HOME/conf

   b. 编辑 WebAgent.conf 文件来启用 Web 代理，如下所示：

      EnableWebAgent="YES"

   c. 保存并关闭文件：
2. 重新启动 Apache Web 服务器

   您已配置 CA SiteMinder Web 代理。

示例：配置 CA SiteMinder 以保护企业管理服务器

在该示例中，您配置 CA SiteMinder，以便在会话中保护企业管理服务器日志。 您需要配置 CA SiteMinder 保护身份验证方案和域策略的用户存储。

1. 请执行以下操作：
   a. 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 Steve 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. 选择“领域”，创建领域并完成以下字段：
    - **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”两次。
13. 选择“策略”，在“常规”选项卡中创建并完成以下字段：
    - **名称**－ac-policy
14. 移到“用户”选项卡并选择“添加全部”

15. 移到“规则”选项卡，单击“添加规则”，选择 ac 规则，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。

示例：配置企业管理服务器以使用 CA SiteMinder 验证用户

在该示例中，您针对 CA SiteMinder 集成配置企业管理服务器。

1. 在企业管理服务器主机上，执行以下操作：
   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.FrameworkLoginFilter</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. 运行位于下列目录的密码工具：

```
/CA/AccessControlServer/IAMSuite/AccessControl/tools/PasswordTool
```

例如：

pwdTools -FIPS -p <clear_*text_password*> -k JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/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==</config-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/Passwordtool/pwdtools.bat -FIPS -p <your_shared_secret> -k JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/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==</config-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\IdentityMinder.ear\library;%SystemRoot%\SYSTEM32;%SystemRoot%;%SystemRoot%\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。

第 16 章： 从 CA Access Control r12.0 SP1 升级

此部分包含以下主题：

从 CA Access Control r12.0 SP1 升级

本章详细描述升级现有 CA Access Control r12.0 SP1 部署的步骤。 本章中的升级过程假定您在不同的计算机上安装 CA Access Control r12.0 SP1 组件。

例如：CA Access Control 企业管理 安装在一台计算机上，DMS、DH 和报告服务器安装在不同的计算机上。

本章中介绍的升级过程将说明如何分别升级每个组件。

注意：您只能从 CA Access Control 企业管理 r12.0 SP1 升级。

在您开始前

在您开始升级当前的 CA Access Control 安装之前，请考虑以下内容：

- 建议您在开始升级过程之前备份 CA Access Control 组件。 建议在开始升级过程之前备份系统文件，包括所有数据库。
- CA Access Control 企业管理 安装以下组件：CA Access Control 企业管理、CA Access Control、分发服务器、企业报告服务。
- 升级之后，以前的 DMS 将不可用。 您必须升级 CA Access Control 企业管理、DMS 和 DH，然后才能启动服务器。
- 安装 CA Access Control 企业管理 时，请指定使用嵌入式用户存储。

  重要说明！ 在嵌入式用户存储上安装 CA Access Control 企业管理 时，您不能使用 UNAB 报告和登录授权策略。 要生成 UNAB 报告并配置登录授权策略，您必须安装 Active Directory。 如果您选择安装 Active Directory，那么现有用户和角色的所有记录将会丢失。

如何从 r12.0 SP1 升级

在您开始升级之前，我们建议您查看需要完成升级现有 CA Access Control r12.0 SP1 部署的步骤：

1. 升级 CA Access Control 企业管理。
    a. 卸载 CA Access Control 企业管理 r12.0 SP1、JBoss 和 JDK
    b. 使用先决条件安装程序安装 JDK 1.5.0 和 JBoss 4.2.3。
    c. 安装 CA Access Control 企业管理
2. 使用 AES 加密现有密码。

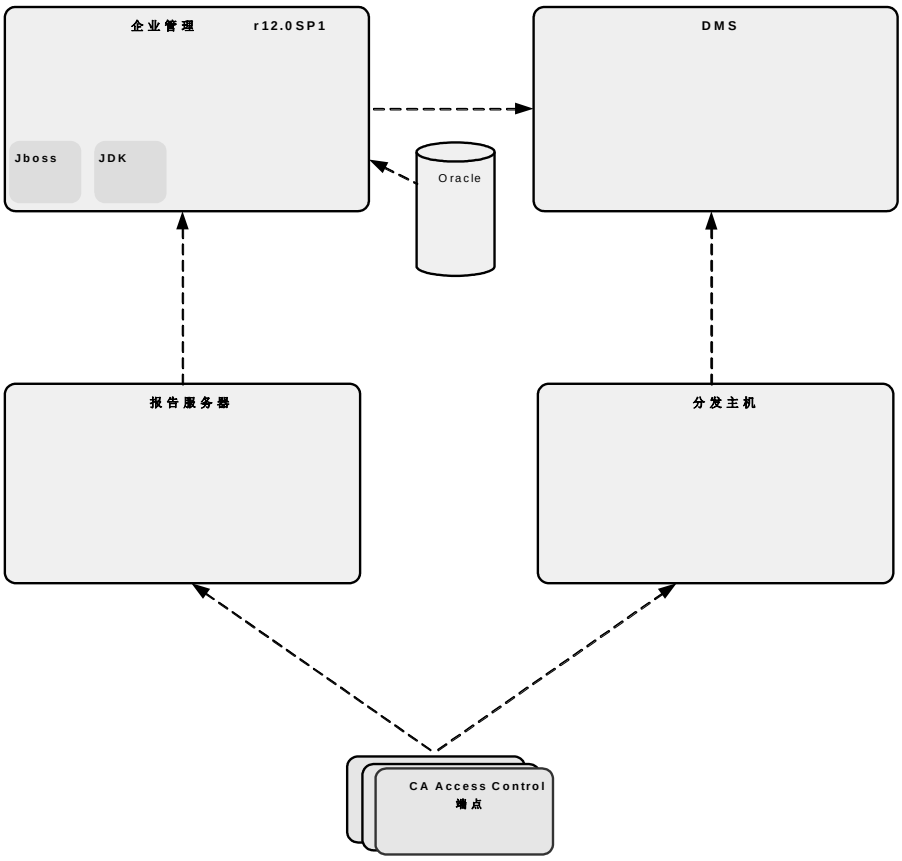
    在 CA Access Control 企业管理 r12.5 SP1 中，加密方法已从 RC2 更改为 AES。
3. 升级 DMS 计算机。

    注意：如果 DMS 与 CA Access Control 企业管理 安装在同一计算机上，您不需要完成该步骤。
4. 升级 DH 计算机。

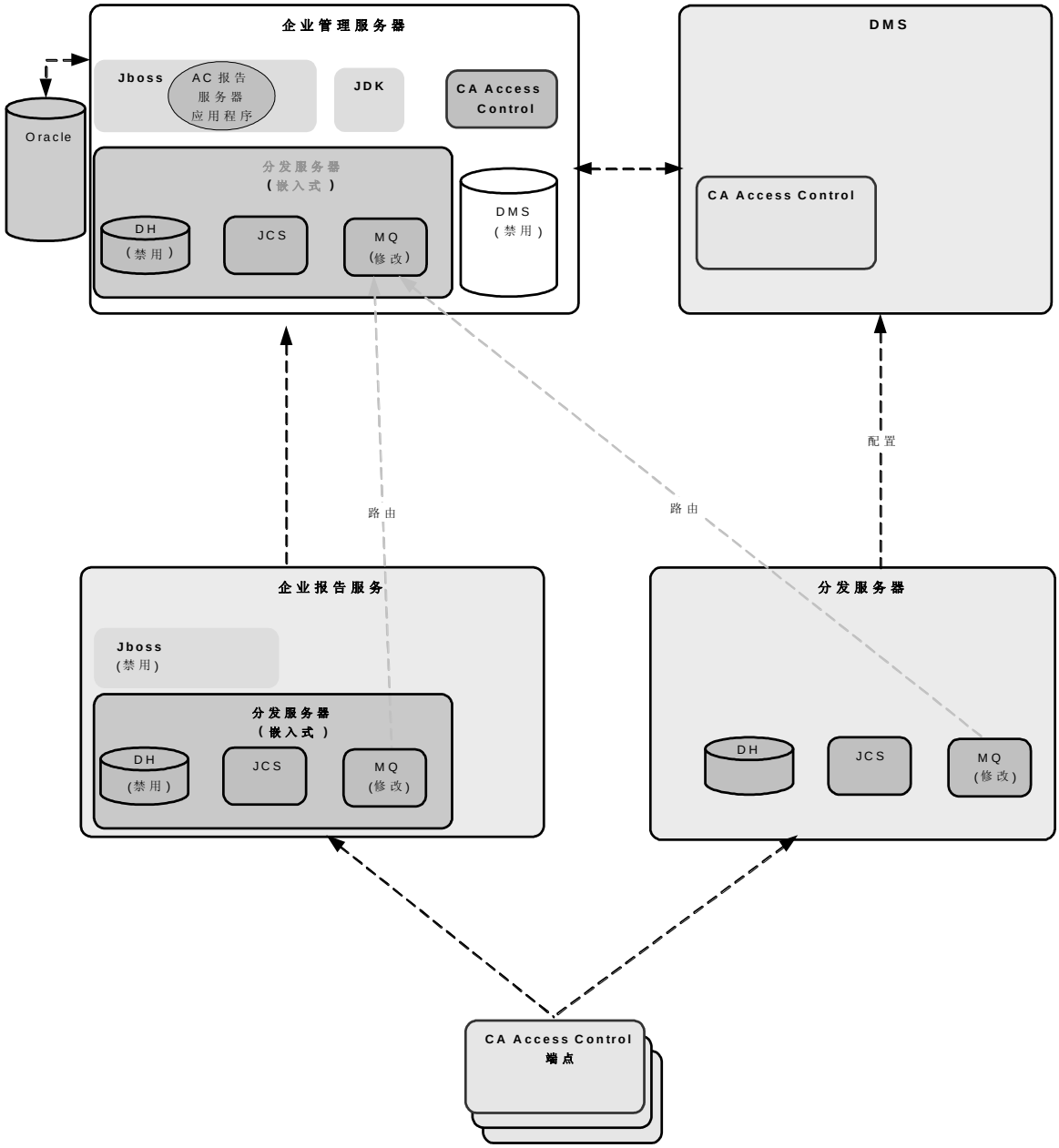
    注意：必须升级您企业中的每个 DH。 如果 DH 与 CA Access Control 企业管理 安装在同一计算机上，您不需要完成该步骤。
5. 定义消息队列 (MQ) 路由设置。
6. 将报告服务器迁移到企业报告服务。
7. 为 DH 订阅新的 DMS。
8. （可选）在端点上安装 CA Access Control。

CA Access Control 升级过程

下图显示升级之前 CA Access Control r12.0 SP1 部署体系结构的示例：



下图显示升级之后， CA Access Control 部署的示例：


企业管理服务器
Jboss
AC 报告
服务器
应用程序
JDK
CA Access
Control
Oracle
分发服务器
(嵌入式)
DH
(禁用)
JCS
MQ
(修改)
DMS
(禁用)
DMS
CA Access Control
配置
路由
路由
企业报告服务
Jboss
(禁用)
分发服务器
(嵌入式)
DH
(禁用)
JCS
MQ
(修改)
分发服务器
DH
JCS
MQ
(修改)
CA Access Control
端点

升级企业管理服务器

该过程介绍在升级企业管理服务器时要遵循的步骤以及需要执行的安装后步骤。

升级企业管理服务器

1. 卸载 CA Access Control 企业管理 r12.0 SP1。

   注意：有关卸载 CA Access Control 企业管理 r12.0 SP1 的信息，请参阅该版本的 *《实施指南》*。

   重要说明！ 在 Solaris 上，搜索并删除 /var/.CA_IAM_FW.registry.xml 和 /var/.com.zerog.registry.xml 隐藏文件（如果存在）。

2. 卸载现有的 JDK 和 JBoss。

3. 安装先决条件软件。

4. 安装 CA Access Control 企业管理。

   CA Access Control 企业管理 还安装以下组件：

   - 企业管理服务器
   - CA Access Control
   - 企业报告服务
   - 分发服务器

   重要说明！ 在安装 CA Access Control 企业管理 时，您必须指定嵌入式用户存储。

5. 如果报告数据库架构与 CA Access Control 企业管理 上的架构不同，请通过运行提供的脚本来更新数据库架构。

6. （可选）为 JBoss 配置安全通讯。

7. 在 CA Access Control 企业管理 上禁用 DMS 和 DH。 运行以下命令：

   ```
   dmsmgr -remove -auto
   ```

   重要说明！ 仅当 DMS 与 CA Access Control 企业管理 分别安装在不同计算机上时完成该步骤。

   注意：升级之后，现有的 DMS 将不再可用。 在安装新的企业管理服务器之后升级 DMS。 有关 dmsmgr 实用程序的详细信息，请参阅 *《参考指南》*。

   新的 CA Access Control 企业管理 服务器已安装。 在启动 CA Access Control 企业管理 之前，您必须立即升级 DMS 和分发主机。

使用 AES 加密方法加密密码

在 CA Access Control r12.0 SP1 中，密码是使用 RC2 加密方法加密的。 在 CA Access Control r12.5 SP1 中，密码加密方法已更改为 AES。 因此，使用 RC2 加密方法加密的密码在 CA Access Control 的更新版本中将不起作用。 要解决该问题，请在从 CA Access Control r12.0 SP1 升级之后使用 AES 加密现有密码。

使用 AES 加密方法加密密码

1. 如果尚未安装 CA Access Control 企业管理，请安装。
2. 停止所有 CA Access Control 服务。
3. 请执行以下操作：
   a. 以拥有读写访问权限的用户身份连接到企业管理服务器数据库。
   b. 运行以下查询以删除 CA Access Control 企业管理 用于连接用户存储的密码：

      ```
      update IM_DIR_CONNECTION set password=null where
      connection_name='java:/userstore';
      ```
4. 使用 pwdtools 实用程序加密数据库中的所有密码。

   对于 tlbusers 表中的每个条目，使用生成的加密密码更改密码。
5. 从连接表中删除 DMS 设置。 运行以下查询：

   ```
   DELETE FROM connection WHERE connection_name='con1';
   ```

   将从数据库中删除 DMS 连接设置。
6. 启动 CA Access Control 企业管理。
7. 配置 CA Access Control 企业管理 中的 DMS 连接设置。

   注意：有关 DMS 连接设置的详细信息，请参阅*联机帮助*。

示例：使用 pwdtools 实用程序加密密码

该示例介绍如何使用 pwdtools 实用程序以 AES 加密模式加密用户密码以及在企业管理服务器数据库中设置加密密码。

1. 打开 pwdtool.bat 进行编辑。 该文件位于以下目录，其中 *ACServerInstallDir* 是安装企业管理服务器的目录：

   ACServerInstallDir/IAM_Suite/Access_Control/tools/PasswordTool/

2. 在“::SET JAVA_HOME=<请在此处输入有效的 java 主目录>”标记处输入 JAVA_HOME 路径。 例如：

   ```
   SET JAVA_HOME=C:\jdk1.5.0
   ```

3. 从命令行窗口运行以下命令，其中 *password* 是明文密码，*JBOSS_Home* 是安装 JBoss 的目录：

   ```
   pwdtools -FIPS -p <"password"> -k
   JBOSS_HOME\server\default\deploy\IdentityMinder.ear\config\com\netegrity\
   config\keys\FIPSkey.dat
   ```

   将显示加密密码。 将该密码复制到剪贴板。

4. 以对数据库拥有读写访问权限的用户身份连接到企业管理服务器。

5. 运行以下查询，其中 *encrypted password* 是您先前复制到剪贴板的加密密码，*username* 是用户帐户名称：

   ```
   update tblusers set password = '<encrypted password>' where
   loginid='<username>';
   ```

   您已使用加密密码设置帐户密码。

升级 DMS

在安装新的 CA Access Control 企业管理 服务器之后，您必须升级现有 DMS。 在升级之前，无需删除 DMS 的现有安装。

重要说明！ 仅当 DMS 与 CA Access Control 企业管理 分别安装在不同计算机上时完成该步骤。

要升级 DMS，请在 DMS 计算机上安装 CA Access Control。

您现在可配置 CA Access Control 企业管理 以连接到 DMS。

升级分发主机 (DH)

成功升级 DMS 之后，您必须升级分发主机 (DH)。 您可以通过在运行分发主机的每台计算机上安装分发服务器来升级 DH。 安装分发服务器之后，您必须配置消息队列路由设置来建立路由，用于在分发服务器和 CA Access Control 企业管理 之间发送和接收消息。

重要说明！ 仅当 DH 与 CA Access Control 企业管理 分别安装在不同计算机上时完成该步骤。

升级分发主机

1. 在 DH 计算机上安装分发服务器。

   分发服务器会安装 Java 连接器服务器 (JCS)、DH 和消息队列。

2. 在分发服务器和 CA Access Control 企业管理 之间定义消息队列路由设置 (p. 410)。

   分发服务器现已配置。

为 DH 订阅 DMS

在创建新的 DH 时，您必须将其订阅到 DMS。

如果您从 r12.0 SP1 升级，则在升级完 CA Access Control 企业管理 组件后，您将无法继续使用以前的 DMS。 您必须配置升级的 DH 以使用新的 DMS，才能启动 CA Access Control 企业管理。

重要说明！ 如果从 r12.0 SP1 升级，仅当在报告服务器计算机上安装分发服务器时完成该步骤。

将 DH 订阅到 DMS

1. 在分发服务器上打开命令提示符窗口。
2. 为新的 DMS 订阅分发主机。

   示例： sepmd -s *DH__WRITER DMS__@<entm>*
3. 将新的 DMS 添加为分发主机父级。

   示例： sepmd -s *DMS__ DH__@<host_name>*
4. 在企业管理服务器上，打开命令提示符窗口并创建新的订户。

   示例： sepmd -n *DH__@<host_name>*

   注意： 有关 sepmd 实用程序的详细信息，请参阅 *《参考指南》*。

将报告服务器迁移到企业报告服务

企业报告服务将报告服务器功能绑定到一个企业范围的报告服务中。由于更改了体系结构，报告服务器现在是 CA Access Control 企业管理 的一部分，不再是单个组件。 您可以通过在报告服务器上安装分发服务器并重新配置消息队列设置，来迁移报告服务器。

注意：通过执行该迁移过程，可允许现有端点继续使用报告服务器计算机上的消息队列。 完成该过程之后，您不需要在端点上重新配置 ReportAgent 设置。

重要说明！ 仅当报告服务器与 CA Access Control 企业管理 分别安装在不同计算机上时完成该步骤。

将报告服务器迁移到企业报告服务

1. 在报告服务器计算机上安装分发服务器。
2. 禁用 JBoss 服务。
3. 在分发服务器和 CA Access Control 企业管理 之间定义消息队列路由设置 (p. 410)。

   企业报告服务（包括报告服务器）已安装。 您现在可以配置企业报告服务器组件。
4. 为 DH 订阅新的 DMS (p. 408)。

升级 CA Access Control 端点

在升级 CA Access Control 企业管理、DMS、分发主机和报告服务器之后，您现在可以升级现有 CA Access Control r12.0 SP1 端点。

要升级 CA Access Control 端点，请在端点上安装 CA Access Control。

如何配置消息路由设置

在包括 CA Access Control 企业管理 单个实例和多个分发服务器的环境中工作时，您必须将所有分发服务器上的 MQ 路由设置配置为指向 CA Access Control 企业管理 上的 MQ。 这有助于确保 CA Access Control 端点发送的所有消息最终都会路由到位于 CA Access Control 企业管理 服务器上的单个 MQ。

要将消息从每个分发服务器上的 MQ 路由到 CA Access Control 企业管理 服务器，请执行以下操作：

- 在企业中的每个分发服务器上，执行以下操作：
  - 停止消息队列服务。
  - 修改到 CA Access Control 企业管理 消息队列的路由。
  - 定义 CA Access Control 企业管理 消息队列的参数。
  - 配置分发服务器消息队列的名称。
  - 指定 CA Access Control 企业管理 消息队列的位置。
  - 启动消息队列服务。
- 在 CA Access Control 企业管理 上，请执行下列操作：
  - 停止消息队列服务。
  - 修改指向分发服务器消息队列的路由。
  - 定义分发服务器消息队列的参数
  - 配置 CA Access Control 企业管理 消息队列的名称。
  - 指定 CA Access Control 企业管理 消息队列的位置
  - 启动消息队列服务。

注意：有关消息传递的信息，请参阅 *《TIBCO 企业消息服务器用户指南》*。

更多信息：

修改分发服务器上的消息队列设置 (p. 411)
修改 CA Access Control 企业管理 上的消息队列设置 (p. 412)
消息队列连接配置 (p. 412)
配置分发服务器上的消息队列的名称 (p. 416)
配置 CA Access Control 企业管理 计算机上消息队列的名称 (p. 417)
消息路由配置 (p. 417)

修改分发服务器上的消息队列设置

默认情况下，每个分发服务器都配置为与该服务器上运行的消息队列配合使用。 要将消息路由到其他消息队列，必须重新配置消息队列设置。

该过程介绍如何修改分发服务器上的消息队列设置，以便能够与 CA Access Control 企业管理 消息队列通讯。 针对企业中的每个分发服务器完成此过程。

修改分发服务器上的消息队列设置

1. 停止 CA Access Control 消息队列服务。
2. 在分发服务器上，打开 tibemsd.conf 文件，默认情况下，该文件位于以下目录，其中 *DistServerInstallDir* 是分发服务器的安装目录：

   DistServerInstallDir/ACMQ/tibco/ems/bin
3. 在 server 参数中输入分发服务器短主机名。
4. 将 routing 参数值更改为已启用。
5. 启动 CA Access Control 消息队列服务。

   已修改分发服务器上的消息队列设置。

注意：有关消息传递的信息，请参阅 *《TIBCO 企业消息服务器用户指南》*。

示例：tibemsd.conf 文件

该示例显示了在修改名为 DS_Example 的分发服务器的路由设置之后 tibemsd.conf 文件中的某个片段。

```
#######################
# Server Identification Information.
# server:    unique server name
# password:  password used to login into other routed server
#######################
server                  = DS_Example
password                =
#######################
...
#######################
# Routing. Routes configuration is in 'routes.conf'. This enables or
# disables routing functionality for this server.
#######################
routing                 = enabled
#######################
```

修改 CA Access Control 企业管理 上的消息队列设置

该程序向您显示如何修改 CA Access Control 企业管理 上的消息队列设置，以便启用与分发服务器的通信。

修改 CA Access Control 企业管理 上的消息队列设置

1. 停止 CA Access Control 消息队列服务。
2. 在 CA Access Control 企业管理 上，打开 tibemsd.conf 文件进行编辑。 默认情况下，该文件位于以下目录，其中 *DistServerInstallDir* 是您安装分发服务器的目录：

   DistServerInstallDir/ACMQ/tibco/ems/bin
3. 在“server”参数中输入 CA Access Control 企业管理 服务器短主机名（不要以点隔开）。
4. 将 routing 参数值更改为已启用。
5. 启动 CA Access Control 消息队列服务。

   已修改 CA Access Control 企业管理上的消息队列设置。

注意：有关消息传递的信息，请参阅 *《TIBCO 企业消息服务器用户指南》*。

示例：tibemsd.conf 文件

此示例显示了为名为 ENTM_Example 的 CA Access Control 企业管理 服务器修改路由设置后 tibemsd.conf 文件中的一个片段：

```
#####################
# Server Identification Information.
# server:    unique server name
# password:  password used to login into other routed server
#####################
server                  = ENTM_Example
password                =
#####################
...
#####################
# Routing. Routes configuration is in 'routes.conf'. This enables or
# disables routing functionality for this server.
#####################
routing                 = enabled
#####################
```

消息队列连接配置

相反，要将消息从分发服务器上的消息队列路由到企业管理服务器，请修改企业中现有的消息队列设置。

示例：在分发服务器上配置消息队列连接设置

该示例显示如何在分发服务器上配置消息队列服务器设置。 通过定义在企业管理服务器上运行的消息队列的参数，可以配置消息队列，以将消息发送到企业管理服务器。

在分发服务器上配置消息队列连接设置

1. 在分发服务器上，执行下列操作之一：
   - (Windows 2003 Server) 依次选择“开始”、“程序”、“TIBCO”、“TIBCO EMS 4.4.1”和“启动 EMS 管理工具”。
   - (UNIX) 请执行以下操作：
     a. 导航到下列目录，其中 *DistServerInstallDir* 是分发服务器的安装目录：

        DistServerInstallDir/MessageQueue/tibco/ems/bin

     b. 运行以下命令：

        tibemsadmin

        此时将打开“TIBCO EMS 管理工具”命令提示符窗口。
2. 使用以下两种方法之一连接到消息队列：
   - 输入以下命令，使用 SSL 进行连接：

     connect ssl://localhost:7243
   - 输入以下命令，使用 TCP 进行连接：

     connect tcp://localhost:7222

   此时将提示您输入登录名称。
3. 输入 **admin**。

   将显示密码提示符。
4. 输入您安装分发服务器时提供的密码。
5. 出现提示时，输入消息队列服务器的新密码。
6. 定义消息队列密码。

   set server password=

   示例：set server password=*<C0mp1ex>*
7. 创建名为 ENTM-NAME 的用户，并为其指定密码。

   create user ENTM-NAME password=*acserver_user-passwd*

   示例：create user EMS-SERVER password=*<acserver_user-passwd>*

   重要说明！ 指定您在企业管理服务器的 tibemsdf.conf 文件的 server 参数中定义的相同名称。

8. 请执行以下操作：
   a. 输入以下命令：

      ```
      add member ac_server_users ENTM_NAME
      ```

      您创建的用户已添加到 ac_server_users 组中。
   b. 输入以下命令：

      ```
      add member ac_endpoint_users ENTM_NAME
      ```

      您创建的用户已添加到 ac_endpoint_users 组中。
   c. 输入以下命令：

      ```
      add member report_publishers ENTM_NAME
      ```

      您创建的用户已授予了读取消息和将消息发布到 CA Access Control 队列的权限。
9. 重新启动分发服务器。

   系统将应用您所做的更改。

示例：配置 CA Access Control 企业管理 上的消息队列连接设置

该示例显示如何在企业管理服务器上配置消息队列服务器设置。 配置消息队列以将消息发送到分发服务器。

在此示例中，术语 *DS-NAME* 与分发服务器计算机的名称有关，而术语 *ENTM-NAME* 与企业管理服务器的名称有关。 定义消息队列服务器设置时，需要将该名称替换为在 *tibemsd.conf* 文件的 server 标记中定义的服务器实际名称。

配置 CA Access Control 企业管理 上的消息队列连接设置

1. 在 CA Access Control 企业管理 计算机上，执行下列操作之一：
   - (Windows 2003 Server) 依次选择“开始”、“程序”、“TIBCO”、“TIBCO EMS 4.4.1”和“启动 EMS 管理工具”。
   - (UNIX) 请执行以下操作：
     a. 导航到下列目录，其中 *ACServerInstallDir* 是安装 CA Access Control 企业管理 的目录：

        ```
        ACServerInstallDir/MessageQueue/tibco/ems/bin
        ```
     b. 运行以下命令：

        ```
        tibemsadmin
        ```

        此时将打开“TIBCO EMS 管理工具”命令提示符窗口。

2. 使用以下两种方法之一连接到消息队列：
   - 输入以下命令，使用 SSL 进行连接：

     ```
     connect ssl://localhost:7243
     ```
   - 输入以下命令，使用 TCP 进行连接：

     ```
     connect tcp://localhost:7222
     ```

   此时将提示您输入登录名称。
3. 输入 **admin**。

   将显示密码提示符。
4. 输入您安装企业管理服务器时提供的密码。
5. 定义消息队列密码。

   ```
   set server password=entm_server-passwd
   ```

   示例：set server password=*<ENTM_SERVER_NAME-passwd>*
6. 为每台分发服务器创建名为 DS-NAME 的用户，并为其指定密码。

   ```
   create user DS-NAME password=dist_server_user
   ```

   示例：create user EMS-Server password=*<C0mp1ex>*

   重要说明！ 指定您在企业管理服务器的 tibemsdf.conf 文件的 server 参数中定义的相同名称。
7. 请执行以下操作：
   a. 输入以下命令：

      ```
      add member ac_server_users DS_NAME
      ```

      您创建的用户已添加到 ac_server_users 组中。
   b. 输入以下命令：

      ```
      add member ac_endpoint_users DS_NAME
      ```

      您创建的用户已添加到 ac_endpoint_users 组中。
   c. 输入以下命令。

      ```
      add member report_publishers DS_NAME
      ```

      您创建的用户已授予了读取消息和将消息发布到 CA Access Control 队列的权限。
8. 重新启动分发服务器，使更改生效。

   已配置 CA Access Control 企业管理上的消息队列连接设置。

   注意：有关消息传递的信息，请参阅*《TIBCO 企业消息服务器用户指南》*。

配置分发服务器上的消息队列的名称

要将消息从分发服务器转发到 CA Access Control 企业管理，请配置每个信息路由，以便将消息从分发服务器上的消息队列转发到 CA Access Control 企业管理 上的消息队列。

在此过程中，需要定义分发服务器上的消息队列设置。 修改消息队列设置文件，以在 CA Access Control 企业管理 上提供消息队列的设置。

在分发服务器上配置消息队列的名称

1. 在分发服务器上，打开文件 queues.conf。 默认情况下，该文件位于以下目录，其中 *DistServerInstallDir* 是分发服务器的安装目录：

   DistServerInstallDir/ACMQ/tibco/ems/bin

2. 找到名为 queue/snapshots 的队列，并在此队列名称的末尾添加 ENTM-NAME 值，两者中间插入 @ 符号，如下所述：

   queue/snapshots@*ENTM-NAME*

   ENTM-NAME

   定义 CA Access Control 企业管理 计算机的短名称。

   重要说明！ 指定您在 CA Access Control 企业管理 上的 tibemsd.conf 文件的“server”参数中定义的相同名称。

3. 找到名为 queue/audit 的队列，并在此队列名称的末尾添加 ENTM-NAME 值，两者中间插入 @ 符号，如下所述：

   queue/audit@*ENTM-NAME*

4. 找到名为 ac_endpoint_to_server 的队列，并在此队列名称的末尾添加 ENTM-NAME 值，两者中间插入 @ 符号，如下所述：

   ac_endpoint_to_server@*ENTM-NAME*

5. 找到名为 ac_server_to_endpoint 的队列，并在此队列名称的末尾添加 ENTM-NAME 值，两者中间插入 @ 符号，如下所述：

   ac_server_to_endpoint@*ENTM-NAME*

6. 保存并关闭文件。

注意：有关消息传递的信息，请参阅 *《TIBCO 企业消息服务器用户指南》*。

配置 CA Access Control 企业管理 计算机上消息队列的名称

在此过程中，您定义 CA Access Control 企业管理 上的消息路由设置。 您配置 CA Access Control 企业管理 上的消息队列设置，以便将该消息队列识别为主服务器。

配置 CA Access Control 企业管理 计算机上消息队列的名称

1. 在 CA Access Control 企业管理 上，在可编辑的表单中打开文件 queues.conf。 默认情况下，该文件位于以下目录，其中 *ACServerInstallDir* 是安装 CA Access Control 企业管理 的目录：

   ACServerInstallDir/MessageQueue/tibco/ems/bin

2. 找到名为 queue/snapshots 的队列，并在队列名称末尾的 secure 词语后面添加 global，如下所述：

   ```
   queue/snapshot secure, global
   ```

3. 找到名为 queue/audit 的队列，并在队列名称末尾的 secure 词语后面添加 global，如下所示：

   ```
   queue/audit secure, global
   ```

4. 找到名为 ac_endpoint_to_server 的队列，并在队列名称末尾的 secure 词语后面添加 global，如下所述：

   ```
   ac_endpoint_to_server secure, global
   ```

5. 找到名为 ac_server_to_endpoint 的队列，并在队列名称末尾的 secure 词语后面添加 global，如下所述：

   ```
   ac_server_to_endpoint secure, global
   ```

6. 保存并关闭文件。

注意：有关消息传递的信息，请参阅 *《TIBCO 企业消息服务器用户指南》*。

消息路由配置

在配置消息队列设置，并配置分发服务器和 CA Access Control 企业管理 上的消息队列路由设置之后，您在分发服务器和 CA Access Control 企业管理 上设置消息路由。

示例：在分发服务器上设置消息路由

该示例显示如何在分发服务器上设置消息路由设置。 在分发服务器和 CA Access Control 企业管理 之间设置一个路由，将来自 CA Access Control 端点的消息路由到 CA Access Control 企业管理 上的消息队列。 对企业中的每个分发服务器完成此过程。

1. 在分发服务器上，打开文件 routes.conf 进行编辑。 默认情况下，该文件位于以下目录，其中 *DistServerInstallDir* 是分发服务器的安装目录：

   DistServerInstallDir/MessageQueue/tibco/ems/bin

2. 添加以下项：

   ```
   [ENTM-NAME]
   url          = ENTM-URL
   ssl_verify_host = disabled
   ssl_verify_hostname = disabled
   ```

   ENTM-NAME

   定义 CA Access Control 企业管理 计算机的短名称。

   ENTM_URL

   定义 CA Access Control 企业管理 URL。

3. 保存文件。
4. 重新启动 CA Access Control 消息队列服务。

示例：在 CA Access Control 企业管理 上设置消息路由

该示例向您显示如何在 CA Access Control 企业管理 上设置消息路由设置。 在 CA Access Control 企业管理 和分发服务器之间设置一个路由，将消息从 CA Access Control 企业管理 发送到分发服务器，并从该位置发送到端点。

1. 在 CA Access Control 企业管理 上，打开文件 routes.conf。 默认情况下，该文件位于以下目录，其中 *ACServerInstallDir* 是安装 CA Access Control 企业管理 的目录：

   ACServerInstallDir/MessageQueue/tibco/ems/bin

2. 添加以下项：

   ```
   [DS-NAME]
   url          = DS-URL
   ssl_verify_host = disabled
   ssl_verify_hostname = disabled
   ```

   DS_NAME

   定义分发服务器的短名称。

   DS_URL

   定义分发服务器 URL。

3. 保存文件。
4. 重新启动 CA Access Control 消息队列服务。

注意：有关消息传递的信息，请参阅 *《TIBCO 企业消息服务器用户指南》*。

附录 A： 更改通讯加密方法

此部分包含以下主题：

通讯加密

您可以使用以下方法加密 CA Access Control 组件之间的通讯和 CA Access Control 客户端/服务器通讯：

- 对称加密
- SSL

注意：在 Windows 上，当更改加密模式（例如：更改为仅 FIPS 模式）后，如果需要从密码 PMDB 传播密码，必须重新启动 CA Access Control 服务。

对称加密

CA Access Control 使用加密库来实施对称（标准）加密。 您可以使用以下方法加密 CA Access Control 组件之间的通讯：

- 默认（专有）加密
- AES128
- AES192
- AES256
- DES
- 3DES

注意：名为 default 的加密方法不是默认的 CA Access Control 加密方法。默认加密方法为 AES256。

安装 CA Access Control 时，安装程序将加密库存储在以下目录中，其中 *ACInstallDir* 是 CA Access Control 的安装目录：

- (Windows) *ACInstallDir*\bin
- (UNIX) *ACInstallDir*/lib

在 Windows 上，CA Access Control 将进行对称加密的加密库的完整路径存储在以下配置设置中：

```
HKEY_LOCAL_MACHINE\Software\ComputerAssociates\AccessControl\Encryption Package
```

使用 sechkey 实用程序更改对称加密密钥和对称加密方法。

更多信息：

更改对称加密密钥 (p. 423)
更改对称加密方法 (p. 424)

sechkey 配置对称加密的过程

对称加密密钥长达 55 个字符。 sechkey 可自动截短较长的密钥并加长较短的密钥。

使用 sechkey 更改加密密钥时，sechkey 会一次性更改 CA Access Control 数据库内所有程序中的密钥。 sechkey 更改对称密钥或对称加密方法时，会先解密然后再加密以下项：

- 安装在计算机上的任何策略模型的加密记录
- CA Access Control 数据库中的所有加密密码，包括 CA Access Control 消息队列密码和用户密码（如果 CA Access Control 使用双向密码）
- 服务器私钥（如果密钥不受密码保护）
- 服务器私钥的密码（如果密钥是受密码保护）

此外，每当使用 CA Access Control API 创建可与 CA Access Control 通讯的程序时，新程序的通讯也会使用相同的密钥进行加密。

更改对称加密密钥

对称加密密钥保护 CA Access Control 组件之间的通讯。 使用 sechkey 实用程序可更改对称加密密钥。 可以在交互或非交互模式下使用 sechkey。

在更改对称加密密钥之前，请注意以下限制：

- 密码长度必须为 1 到 55 个字符
- 密码不得包含高 ASCII 字符
- 密码不得包含双引号 (")

必须具有 ADMIN 属性才能使用 sechkey。

重要说明！ 为避免通讯问题，请在所有运行 CA Access Control 组件的计算机上使用相同的加密密钥。

更改对称加密密钥

1. 停止 CA Access Control。

   如果您正在更改 CA Access Control 企业管理服务器上的加密设置，请同时停止 CA Access Control Web 服务。

2. 在交互模式下运行 sechkey 实用程序：

   ```
   sechkey
   ```

   实用程序会提示您输入现有密钥和新密钥，并更改对称加密密钥。

3. 启动 CA Access Control。

   如果您正在更改 CA Access Control 企业管理服务器上的加密设置，请同时启动 CA Access Control Web 服务。

   CA Access Control 使用新的加密密钥启动并加密通讯。

示例：在非交互模式下更改对称加密密钥

下列示例将默认的 CA Access Control 对称密钥更改为值为 newkey 的新密钥：

```
sechkey -d newkey
```

注意：有关 sechkey 实用程序的详细信息，请参阅 *《参考指南》*。

更改对称加密方法

对称加密保护 CA Access Control 组件之间的通讯并由加密库实施。 使用 sechkey 实用程序可更改加密库和对称加密方法。

必须具有 ADMIN 属性才能使用 sechkey。

注意：当 CA Access Control 以仅 FIPS 模式运行时，将无法更改对称加密方法。 crypto 部分中 fips_only 配置标记的值为 1 时，CA Access Control 以仅 FIPS 模式运行。 此项限制可防止您将加密方法更改为不遵从 FIPS 的方法。

重要说明！ 为避免通讯问题，请在所有运行 CA Access Control 组件的计算机上使用相同的加密方法。

更改对称加密方法

1. 停止 CA Access Control。

   如果您正在更改 CA Access Control 企业管理服务器上的加密设置，请同时停止 CA Access Control Web 服务。

2. 使用 sechkey 实用程序更改对称加密方法。

3. 启动 CA Access Control。

   如果您正在更改 CA Access Control 企业管理服务器上的加密设置，请同时启动 CA Access Control Web 服务。

   CA Access Control 使用新的加密方法启动并加密通讯。

示例：将对称加密方法更改为 3DES

以下命令可将对称加密方法更改为 3DES：

```
sechkey -m -sym tripledes
```

注意：有关 sechkey 实用程序的详细信息，请参阅*《参考指南》*。

企业部署中的多种对称加密方法

端点可以与使用不同加密方法的其他 CA Access Control 组件进行通讯。crypto 部分中的 encryption_methods 配置设置指定端点接受的对称加密方法。

默认情况下，配置设置按顺序列出以下加密方法：

- AES256
- AES192
- AES128
- DES
- 3DES

当 CA Access Control 代理解密从其他组件传入的通讯时，会依次尝试使用列表中的每种方法，直到解密成功。 代理使用相同的加密方法来加密传到该组件的传出通讯。

同样地，当 CA Access Control Web 服务尝试连接到端点时，也会尝试依次使用列表中的每种方法，直到成功与端点通讯。

通过多种加密方法可以轻松升级企业 CA Access Control 部署。 例如：使用 DES 加密可以实现 r12.5 部署。 可以分阶段执行升级到 r12.5 SP4 的过程，并将已升级组件的加密方法更改为 AES256。 将企业管理服务器升级到 r12.5 SP4；该服务器现在默认使用 AES256 加密。 但是，因为 r12.5 SP4 服务器还可以与使用 DES 加密的 CA Access Control 组件通讯，所以企业管理服务器可以继续管理 r12.5 端点。

SSL、身份验证和证书

安全套接字层 (SSL)（包括 TLS）提供计算机程序之间的通讯。 SSL 帮助确保通讯具有以下属性：

- 通讯中的参与者已通过身份验证，也就是说，通讯的参与者是自身声明的程序或用户。
- 数据安全加密，并且只有参与者可以读取。

参与者通过使用 X.509 证书验证彼此身份。 X.509 证书是电子文档，该文档通过公钥链接证书所有者的地址。 该证书不可伪造。

SSL 在客户端/服务器模型上运行并使用 PKI（公钥基础结构）。 客户端从服务器接收 X509 证书后，将检查该证书是否有效。 如果该证书有效，客户端将知道该服务器是自身声明的程序或用户，因此该服务器将会通过身份验证。 同样，如果客户端使用证书的公钥加密数据，则只有该服务器可解密数据，因此数据是安全的。 反之，服务器以相同方式使用从客户端接收的 X.509 证书。

证书包含的内容

程序发送 X.509 证书以证明其身份绑定至公钥。 这样，其他程序加密消息就知道只有证书的主题能够对其解密。

X.509 证书的内容如下所示：

- **证书数据**－最重要的证书数据字段为：
  - 证书主题的公共标识符（例如：Web 地址）
  - 证书的有效期（开始和结束日期）
- **颁发证书的证书颁发机构 (CA) 的名称**－证书读取器可以确定，如果签名有效，CA 将会验证公钥是否与主题关联。 这表示如果证书读取器信任 CA，则这些读取器可以相信使用公钥加密的数据只能由主题读取。
- **主题的公钥**－证书读取器使用公钥来加密要发送到证书主题的数据。
- **数字签名**－数字签名是证书（使用 CA 的私钥加密）中所有其他数据的哈希封装。 （请注意发送者使用公钥加密数据的加密情况的对比。）任何具有 CA 公钥访问权限的人都可以读取签名，并检查签名是否与证书中的其他数据匹配。 如果证书中的任何文字被更改，则签名将不再与证书文字匹配。

主题的私钥与证书相关联，但保持独立和安全。 主题使用私钥对程序使用公钥加密的消息进行解密。

证书证明的内容

读取器可通过使用证书颁发机构 (CA) 的公钥来验证证书签名。 如果解密的签名与证书的其余部分匹配，并且读取器信任 CA，则表示读取器将知道以下内容为真：

- 如果读取器使用公钥加密数据，则只有私钥的所有者能够解密和读取该数据。
- 证书私钥的所有者是在证书中提供的主题。

为确认证书有效，读取器需要信任 CA，还需要访问 CA 的公钥。 在大多数情况下，CA 是知名的公司，并且程序（及所有最常用的 Web 浏览器）具有 CA 公钥的副本，因此读取器无需在线检查 CA 是否真正验证了证书。

如果发布程序也是所有者，证书为自行签名，则信任发布程序很可能有问题。

要检查发送证书的程序是否是证书所有者，读取器需要使用一些其他方法。 通常，读取器将检查其用于查找证书发送者的地址是否与证书中的地址相同。

根证书和服务器证书

根证书（或 CA 证书）是经由证书颁发机构 (CA) 验证并受信任的 X.509 证书。 可以使用该受信任的证书创建其他名为“服务器证书”或“主题证书”的 X.509 证书。 每个服务器证书均由根证书的私钥签名。 如果读取器信任根证书，则知道可以信任从此根证书创建的任何服务器证书。

根证书生成并验证服务器证书。 您可以在 CA Access Control 中使用以下类型的根证书：

- 默认的 CA Access Control 根证书
- 第三方根证书，包括受密码保护的证书

服务器证书对 CA Access Control 客户端/服务器通讯以及 CA Access Control 组件之间的通讯进行加密和身份验证。 您可以在 CA Access Control 中使用以下类型的服务器证书：

- 默认的 CA Access Control 服务器证书
- 第三方服务器证书，包括受密码保护的证书
- 从第三方根证书创建的 CA Access Control 服务器证书

启用 SSL 加密

安装 CA Access Control 时配置加密设置。 安装后，可以使用 sechkey 实用程序更改 SSL 加密。 可能还需要更改配置设置的值。

重要说明！ 为避免通讯问题，请在所有运行 CA Access Control 组件的计算机上使用相同的加密方法。

启用 SSL 加密

1. 停止 CA Access Control。

   如果要更改 CA Access Control 企业管理 服务器上的加密设置，还需要停止 CA Access Control Web 服务。

2. 将 crypto 部分中的 communication_mode 配置设置值更改为下列值之一：

   all_modes

   如果要同时启用对称和 SSL 加密，请指定此值。 此值允许计算机与所有 CA Access Control 组件进行通讯。

   注意：如果指定此值，CA Access Control 会在每次尝试与其他 CA Access Control 组件进行通讯时使用 SSL 加密。 如果 SSL 失败，则将使用对称加密。 此值可以让您将 CA Access Control 部署从对称加密环境迁移到 SSL 加密环境。

   use_ssl

   指定此值将仅启用 SSL 加密。 此值允许计算机仅与使用 SSL 加密的 CA Access Control 组件进行通讯。

   注意：(Windows) 如果正在使用采用 CA Access Control SDK 的第三方程序，加密区位于安装期间定义的 CA Access Control SDK 注册表路径。

3. （建议）配置 SSL 通讯，以执行下列操作之一：

   - 使用第三方根证书和服务器证书 (p. 429)。
   - 使用从第三方根证书生成的服务器证书 (p. 430)。

   注意：如果未进一步配置 SSL 加密，则可以使用默认的 CA Access Control X.509 证书来对 CA Access Control 组件之间的通讯进行加密和身份验证。 但是，我们建议更改默认证书。

4. 启动 CA Access Control：
   - 如果要更改 CA Access Control 企业管理 服务器上的加密设置，还需要启动 CA Access Control Web 服务。
   - 如果正在使用第三方程序（该程序使用了 CA Access Control SDK），请重新启动使用 CA Access Control SDK 的进程。

   SSL 加密已启用。

使用第三方根证书和服务器证书

如果使用 SSL 加密，则可以使用第三方根证书和服务器证书来对 CA Access Control 组件之间的通讯进行加密和身份验证。

需要提供以下文件才能使用第三方根证书和服务器证书：

- **root.pem**－根证书
- **server.pem**－服务器证书
- **server.key**－服务器证书的私钥

  如果使用受密码保护的 OU 服务器证书，则还需要服务器证书的私钥密码。

注意：由于已创建服务器证书，因此不需要根证书的私钥。

使用第三方根证书和服务器证书

1. 确认 CA Access Control 服务已停止并且 SSL 已启用。
2. 替换根证书。 请执行下列操作之一：
   - 将新的根证书复制到 crypto 部分中 ca_certificate 配置设置指定的位置。
   - 编辑 crypto 部分中 ca_certificate 配置设置的值，以指定新根证书的完整路径。

     注意：如果在新目录中安装根证书，请编写 CA Access Control FILE 规则以保护新目录。
3. 替换服务器证书。 请执行下列操作之一：
   - 将新的服务器证书复制到 crypto 部分中 subject_certificate 配置设置指定的位置。
   - 编辑 crypto 部分中 subject_certificate 配置设置的值，以指定新服务器证书的完整路径。

     注意：如果在新目录中安装服务器证书，请写入 CA Access Control FILE 规则以保护新目录。

4. 替换服务器密钥。 请执行下列操作之一：
   - 将新的服务器密钥复制到 crypto 部分中 private_key 配置设置指定的位置。
   - 编辑 crypto 部分中 private_key 配置设置的值，以指定新服务器密钥的完整路径。

     注意：如果在新目录中安装服务器密钥，请编写 CA Access Control FILE 规则以保护新目录。
5. 如果使用受密码保护的 OU 证书，请执行以下操作：
   a. 确认 crypto 部分中 fips_only 配置设置的值为 0。

      注意：如果 CA Access Control 在仅限 FIPS 模式下运行，则不能使用受密码保护的证书。

   b. 按如下方法在计算机上存储服务器证书私钥的密码：

      ```
      sechkey -g -subpwd private_key_password
      ```

      注意：必须配置 ADMIN 属性才能使用 sechkey。

   c. 验证 CA Access Control 是否可以使用已存储的密码来打开私钥：

      ```
      sechkey -g -verify
      ```

      如果 CA Access Control 无法打开密钥，则重复步骤 b 并指定正确的密码。

   注意：有关 sechkey 实用程序的详细信息，请参阅*《参考指南》*。
6. 启动 CA Access Control：
   - 如果要更改 CA Access Control 企业管理 服务器上的加密设置，还需要启动 CA Access Control Web 服务。
   - 如果正在使用第三方程序（该程序使用了 CA Access Control SDK），请重新启动使用 CA Access Control SDK 的进程。

   SSL 加密已启用。

使用从第三方根证书生成的服务器证书

如果使用 SSL 加密，可以从第三方根证书创建服务器证书。 使用这些证书来对 CA Access Control 组件之间的通讯进行加密和身份验证。

您可以创建受密码保护的服务器证书，这样，CA Access Control 将使用指定的密码保护服务器证书的私钥。

需要提供下列文件才能从第三方根证书创建服务器证书：

- **root.pem**－根证书
- **root.key**－根证书的私钥

使用从第三方根证书生成的服务器证书

1. 确认 CA Access Control 服务已停止并且 SSL 已启用。
2. 如果使用受密码保护的 OU 证书，请确认 crypto 部分中 fips_only 配置设置的值为 0。

   注意：如果 CA Access Control 在仅限 FIPS 模式下运行，则不能使用受密码保护的证书。
3. 删除以下目录中*除* sub_cert_info 以外的其他所有文件，其中 *ACInstallDir* 是 CA Access Control 的安装目录：

   ACInstallDir/data/crypto

   重要说明！ 不要删除 sub_cert_info 文件。

   将删除默认服务器证书和服务器证书的默认密钥。
4. 替换根证书。 请执行下列操作之一：
   - 将新的根证书复制到 crypto 部分中 ca_certificate 配置设置指定的位置。
   - 编辑 crypto 部分中 ca_certificate 配置设置的值，以指定新根证书的完整路径。

     注意：如果在新目录中安装根证书，请编写 CA Access Control FILE 规则以保护该目录。
5. 使用 sechkey 实用程序生成服务器证书。

   注意：有关 sechkey 实用程序的详细信息，请参阅*《参考指南》*。 必须具有 ADMIN 属性才能使用 sechkey。 如果正在使用第三方程序（该程序使用 CA Access Control SDK），请在运行 sechkey 时将 -s 选项附加到 sechkey 命令。
6. （可选）删除根证书的私钥。

   如果不想从根证书创建其他服务器证书，则可以删除根证书的私钥。
7. 启动 CA Access Control：
   - 如果要更改 CA Access Control 企业管理 服务器上的加密设置，还需要启动 CA Access Control Web 服务。
   - 如果正在使用第三方程序（该程序使用了 CA Access Control SDK），请重新启动使用 CA Access Control SDK 的进程。

   SSL 加密已启用。

示例：使用 sechkey 创建服务器证书

该示例从第三方根证书创建服务器证书。 该示例使用默认的 CA Access Control 证书信息文件。 根证书的私钥名为 custom_root.key，位于 /opt/CA/AccessControl/data/crypto 下：

```
sechkey -e -sub -in "/opt/CA/AccessControl/data/crypto/sub_cert_info" -priv
/opt/CA/AccessControl/data/crypto/custom_root.key
```

受密码保护的服务器证书

您可以将 CA Access Control 配置为使用受密码保护的服务器证书，这样，CA Access Control 将使用指定的密码来保护服务器证书的私钥。 CA Access Control 将密码存储在 *ACInstallDir*/Data/crypto 目录下的 crypto.dat 文件中，其中 *ACInstallDir* 是 CA Access Control 的安装目录： crypto.dat 文件为隐藏、加密、只读文件，且受 CA Access Control 保护。 如果 CA Access Control 已停止，则只有超级用户可以访问密码。

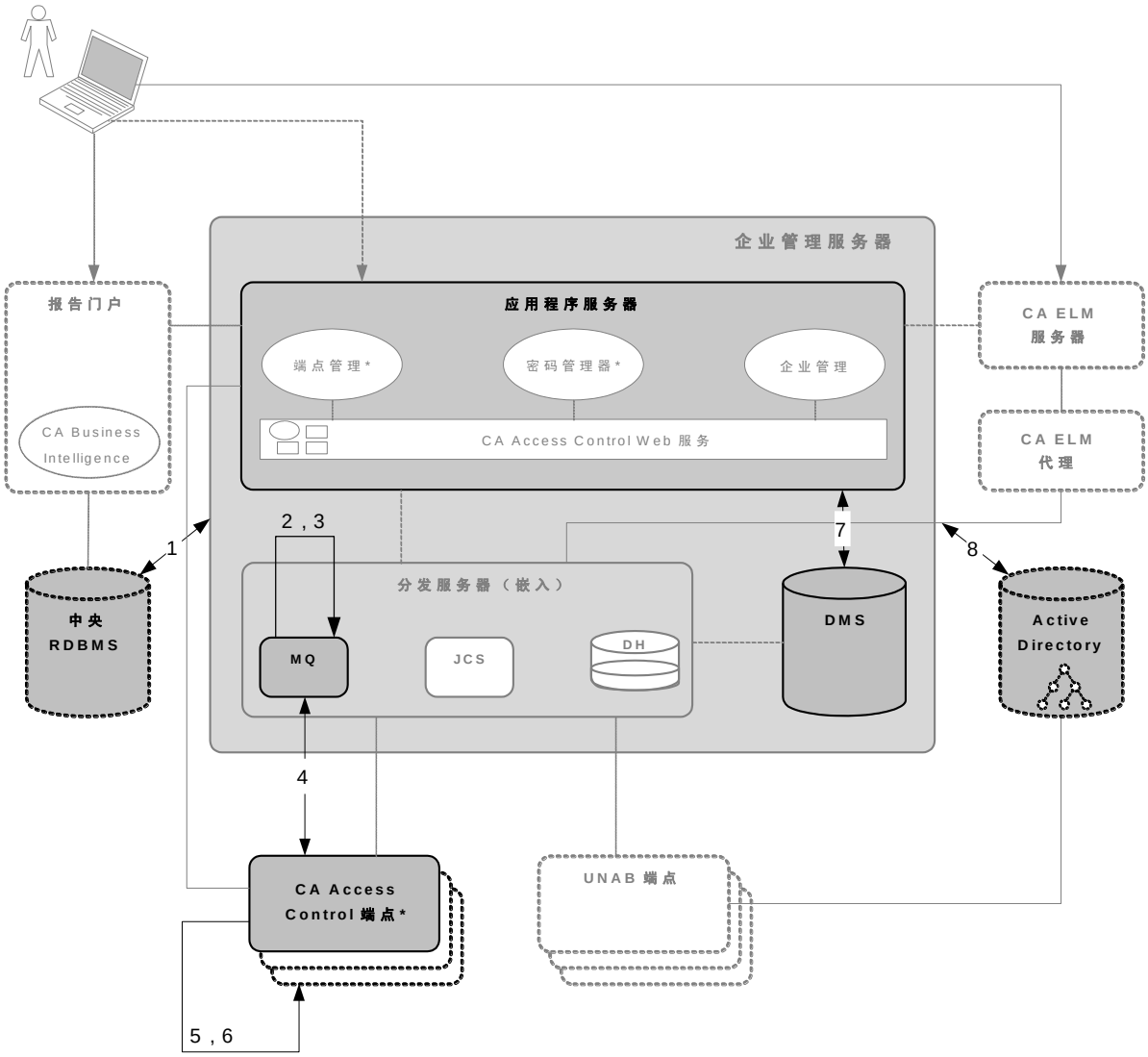
如果创建受密码保护的服务器证书，sechkey 不会对证书进行加密。 如果创建不受密码保护的服务器证书，sechkey 将使用 AES256 和 CA Access Control 加密密钥对证书进行加密。

附录 B： 更改 CA Access Control 服务帐户设置

此部分包含以下主题：

CA Access Control 服务帐户与 CA Access Control 组件的交互方式

下图显示了服务帐户如何与各种 CA Access Control 组件进行交互。



图中的编号对应于以下服务帐户：

1. RDBMS_service_user

   该帐户验证企业管理服务器和 RDMBS 之间的通讯。

   注意：该帐户的名称不是 RDBMS_service_user。 该帐户的名称是在创建用户以便为 CA Access Control 企业管理 准备数据库时指定的。

2. guest

   该帐户是 JNDI 连接帐户，可用来查找消息队列服务器中的消息队列。

   注意：您可以在安装后更改 JNDI 连接帐户。

3. reportserver

   该帐户允许 DMS 和 CA Access Control 企业管理 登录到消息队列。

4. +reportagent

   该帐户允许端点登录到消息队列。

5. +policyfetcher

   该帐户在端点上执行 policyfetcher 后台进程或服务。

6. +devcalc

   该帐户在端点上执行策略偏差计算。

7. ac_entm_pers

   该帐户对企业管理服务器和 DMS 之间的通讯进行身份验证。

8. ADS_LDAP_bind_user

   该帐户允许 CA Access Control 企业管理 针对 Active Directory 执行 LDAP 查询。

   注意：该帐户的名称不是 ADS_LDAP_bind_user。 该帐户的名称是在安装 CA Access Control 企业管理 时在 Active Directory 设置向导页面中指定的用户 DN。

服务帐户密码

大多数情况下，在安装 CA Access Control 企业管理 时需要为 CA Access Control 服务帐户设置密码。 但是，在安装后，您可能需要更改这些帐户的密码。 例如：可能每年都需要更改密码，以符合组织的安全或密码策略。

如果服务帐户与 CA Access Control 组件交互，则必须在每个组件上更改帐户的密码。 如果仅在一个组件上更改密码，服务帐户将无法登录到其他组件。

更改 RDBMS_service_user 密码

RDBMS_service_user 帐户对企业管理服务器和 RDBMS 之间的通讯进行身份验证。 该帐户的名称不是 RDBMS_service_user。 该帐户是在为 CA Access Control 企业管理 准备数据库时创建的，并在安装 CA Access Control 企业管理 时需要随其他数据库信息一起提供帐户名称和密码。

您可能需要定期更改 RDBMS_service_user 密码，以符合组织的安全和密码策略。 必须同时更改企业管理服务器和 RDBMS 上的密码。

在更改该帐户的密码时，请注意以下事项：

- 该帐户的默认密码是在创建用户时指定的密码。
- 密码具有以下限制：
  - 长度必须是 1-50 个字符
  - 不能包含高 ASCII 字符
  - 不能包含双引号 (")
  - 必须符合 RDBMS 密码规则
- 密码存储在以下 XML 文件中，其中 *JBoss_home* 是 JBoss 的安装目录：

  JBoss_home/server/default/conf/login-config.xml

更改 RDBMS_service_user 密码

1. 使用数据库工具更改密码。

   注意：有关如何更改密码的详细信息，请参阅 MS SQL 或 Oracle 文档。

2. 在企业管理服务器中更改密码：
   a. 停止 JBoss 应用程序服务器。
   b. 加密明文密码 (p. 455)。
   c. 在 login-config.xml 文件中更改密码 (p. 458)。
   d. 重新启动 JBoss 应用程序服务器。
   e. 确认可以登录到 CA Access Control 企业管理。

      JBoss 已成功启动，且已在企业管理服务器中更改密码。

   所有位置中的 RDBMS_service_user 密码已更改。

示例：在 login-config.xml 文件中更改密码

login-config.xml 文件的该片段显示了已更改的 RDMBS_service_user 密码的一个实例。 用户名为 caidb01。 密码为 }>8:Jt^+%INK&i^v 并已加密：

```
<application-policy name="imobjectstoredb">
        <authentication>
                <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin"
                flag="required">
                        <module-option
name="userName">caidb01</module-option>
                        <module-option name="password">
                        {AES}:}>8:Jt^+%INK&i^v==</module-option>
                        <module-option name="managedConnectionFactoryName">

        jboss.jca:name=jdbc/objectstore,service=NoTxCM</module-option>
                </login-module>
        </authentication>
</application-policy>
```

更改 reportserver 密码

CA Access Control 企业管理 和 DMS 使用 reportserver 帐户连接到消息队列。

CA Access Control 企业管理 使用 reportserver 帐户执行以下操作：

- 将报告数据发送到 CA Enterprise Log Manager
- 发送 UNAB 远程迁移命令
- 向 PUPM 端点上的 PUPM 代理提供特权帐户密码
- 从 CA Access Control 端点接收报告数据

DMS 使用 reportserver 帐户执行以下操作：

- 将 UNAB 策略发送到 UNAB 端点
- 接收从 UNAB 端点发送的策略部署状态信息

您可能需要定期更改 reportserver 密码，以符合组织的安全和密码策略。 必须在分发服务器、企业管理服务器和 DMS 上更改密码。

在更改 reportserver 密码之前，请注意以下事项：

- 该帐户的默认密码是在安装 CA Access Control 企业管理 时指定的通讯密码。
- 密码具有以下限制：
  - 长度必须是 1-240 个字符
  - 不能包含高 ASCII 字符
  - 不能包含双引号 (")
- 密码存储在消息队列和以下 XML 文件中，其中 *JBoss_home* 是 JBoss 的安装目录：
  - *JBoss_home*/server/default/deploy/properties-service.xml
  - *JBoss_home*/server/default/conf/login-config.xml

重要说明！ 如果企业中有多个分发服务器，应首先更改企业管理服务器上安装的分发服务器的密码，然后再更改企业中其他分发服务器的密码。

更改 reportserver 密码

1. 在分发服务器上，为 reportserver 服务器设置消息队列密码 (p. 454)。

   已在分发服务器上更改 reportserver 密码。
2. 在企业管理服务器上更改密码，如下所述：
   a. 停止 JBoss 应用程序服务器。
   b. 加密明文密码 (p. 455)。
   c. 在 properties-service.xml 文件中更改密码 (p. 457)
   d. 在 login-config.xml 文件中更改密码 (p. 458)。
   e. 重新启动 JBoss 应用程序服务器。
   f. 确认可以登录到 CA Access Control 企业管理。

      JBoss 已成功启动，且企业管理服务器上的密码已更改。
3. 使用 sechkey 更改 DMS 上的 reportserver 密码 (p. 453)。

   reportserver 密码在所有位置中已更改。

示例：为 reportserver 用户设置消息队列密码

该 Tibco EMS 管理工具命令可为 reportserver 用户设置消息队列密码。密码为“secret”，必须采用明文形式，并包含在双引号中：

```
ssl://localhost:7243> set password reportserver "secret"
Password of user 'reportserver' has been modified
ssl://localhost:7243>
```

示例：在 properties-service.xml 文件中更改密码

properties-service.xml 文件的该片段显示了已更改的 reportserver 密码。密码为 }>8:Jt^+%INK&i^v 并已加密：

```
<attribute name="Properties">
      SamMDB.mdb-user=reportserver
      <!-- 编码的 tibco 密码 -->
      SamMDB.mdb-passwd={AES}:}>8:Jt^+%INK&i^v==
</attribute>
```

示例：在 login-config.xml 文件中更改密码

login-config.xml 文件的该片段显示了已更改的 reportserver 密码。 密码为 }>8:Jt^+%INK&i^v 并已加密：

```
<application-policy name="JmsXATibcoRealm">
       <authentication>
          <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
             <module-option name="userName">reportserver</module-option>
           <module-option
name="password">{AES}:}>8:Jt^+%INK&i^v==</module-option>
                <module-option name="managedConnectionFactoryName">
                jboss.jca:service=TxCM,name=TibcoJmsXA</module-option>
          </login-module>
       </authentication>
</application-policy>
```

示例：使用 sechkey 更改 DMS 上的消息队列密码

该命令可更改 DMS 上的消息队列密码。 密码为“secret”，必须采用明文形式，并包含在双引号中：

```
sechkey -t -server -pwd "secret"
```

更改 +reportagent 密码

+reportagent 帐户允许端点登录到消息队列。 在每个端点上，UNAB 代理、PUPM 代理和报告代理使用该帐户与消息队列通讯。

您可能需要定期更改 +reportagent 密码，以符合组织的安全和密码策略。 同时更改消息队列和端点上的密码。

在更改 +reportagent 密码之前，请注意以下事项：

- 默认密码是在安装 CA Access Control 企业管理 时指定的通讯密码。
- 密码具有以下限制：
  - 长度必须是 1-240 个字符
  - 不能包含高 ASCII 字符
  - 不能包含双引号 (")
- 密码存储在消息队列和端点上的 CA Access Control 数据库 (seosdb) 中。

重要说明！ 如果企业中有多个分发服务器，应首先更改企业管理服务器上安装的分发服务器的密码，然后再更改企业中其他分发服务器的密码。 消息队列是分发服务器的一部分。

更改 +reportagent 密码

1. 在分发服务器上，为 +reportagent 用户设置消息队列密码 (p. 454)。

   在消息队列上更改 +reportagent 密码。

2. 使用 sechkey 更改密码 (p. 453)，ReportAgent 使用该密码连接到端点上的消息队列。

   已更改的 +reportagent 密码已传播到端点。

   注意：您还可以使用 selang 更改端点上的 +reportagent 密码。 但是，无法使用策略传播 selang 命令，因为无法使用高级策略管理设置用户密码。

示例：为 +reportagent 用户设置消息队列密码

该 Tibco EMS 管理工具命令可为 +reportagent 用户设置消息队列密码。密码为“secret”，必须采用明文形式，并包含在双引号中：

```
ssl://localhost:7243> set password +reportagent "secret"
Password of user '+reportagent' has been modified
ssl://localhost:7243>
```

示例：使用 sechkey 更改端点上的消息队列密码

该命令将 +reportagent 用户的消息队列密码传播到分发服务器订阅的端点。 密码为“secret”，必须采用明文形式，并包含在双引号中：

```
sechkey -t -pwd "secret"
```

更改 +policyfetcher 密码

+policyfetcher 帐户执行 policyfetcher 后台进程或服务，该后台进程或服务可以查找 DH 上的部署任务、将策略更新应用到本地 CA Access Control 数据库 (seosdb)，以及以固定的时间间隔将检测信号发送到 DH。 CA Access Control 使用 SPECIALPGM 规则将 +policyfetcher 定义为系统用户。 +policyfetcher 在 Windows 中以 NT AUTHORITY\SYSTEM 用户身份运行。

您可能需要定期更改 +policyfetcher 密码，以符合组织的安全和密码策略。

在更改 +policyfetcher 密码之前，请注意以下事项：

- 该帐户没有默认密码。 在安装期间，CA Access Control 不会为 +policyfetcher 设置密码。
- 密码具有以下限制：
  - 长度必须是 1-240 个字符
  - 不能包含高 ASCII 字符
  - 不能包含双引号 (")
- 密码存储在 seosdb（本地 CA Access Control 数据库）中。

重要说明！ 为了防止此用户登录到 CA Access Control 数据库，建议您不要为此用户设置密码。

要更改 +policyfetcher 密码，请使用 selang (p. 452)。

示例：更改 +policyfetcher 密码

该命令可为 +policyfetcher 用户更改密码。 密码为“secret”，必须采用明文形式，并包含在双引号中：

```
AC> cu +policyfetcher password("secret") grace- nonative
(localhost)
已成功更新 USER +policyfetcher
```

更改 +devcalc 密码

+devcalc 执行策略偏差计算，该计算将会评估（策略部署后）部署到端点上的预期访问规则和已成功部署到同一端点上的实际规则之间的差别。 CA Access Control 使用 SPECIALPGM 规则将 +devcalc 定义为系统用户。 +devcalc 在 Windows 中以 NT Authority\System 用户身份运行。

您可能需要定期更改 +devcalc 密码，以符合组织的安全和密码策略。

在更改 +devcalc 密码之前，请注意以下事项：

- 该帐户没有默认密码。 在安装期间，CA Access Control 不会为 +devcalc 设置密码。
- 密码具有以下限制：
  - 长度必须是 1-240 个字符
  - 不能包含高 ASCII 字符
  - 不能包含双引号 (")
- 密码存储在 seosdb（本地 CA Access Control 数据库）中。

重要说明！ 为了防止此用户登录到 CA Access Control 数据库，建议您不要为此用户设置密码。

要更改 +devcalc 密码，请使用 selang (p. 452)。

示例：更改 +devcalc 密码

该命令可更改 +devcalc 用户的密码。 密码为“secret”，必须采用明文形式，并包含在双引号中：

```
AC> cu +devcalc password("secret") grace- nonative
(localhost)
已成功更新 USER +devcalc
```

更改 ac_entm_pers 密码

ac_entm_pers 帐户对 DMS 和企业管理服务器之间的通讯进行身份验证。

您可能需要定期更改 ac_entm_pers 密码，以符合组织的安全和密码策略。 必须同时更改 RDBMS 和 DMS 上的密码。

在更改 ac_entm_pers 密码之前，请注意以下事项：

- 默认密码是在安装期间由 CA Access Control 随机生成的密码。
- 密码具有以下限制：
  - 长度必须是 1-48 个字符
  - 不能包含双引号 (")
  - 不能包含高 ASCII 字符
- 密码存储在 RDBMS 和 DMS 中。

更改 ac_entm_pers 密码

1. 使用 selang 更改 DMS 中的 ac_entm_pers 密码 (p. 452)。
2. 在 CA Access Control 企业管理 中，配置与 DMS 之间的连接并指定新密码。

   所有位置中的 ac_entm_pers 密码已更改。

   注意：有关配置与 DMS 之间的连接的详细信息，请参阅 *CA Access Control 企业管理 联机帮助*。

示例：使用 selang 更改 ac_entm_pers 密码

此命令可以连接到 DMS 并更改 ac_entm_pers 用户的密码。 密码为“secret”，必须采用明文形式，并包含在双引号中：

```
AC> host DMS__@example.com
(DMS__@example.com)
已成功连接
AC> cu ac_entm_pers password("secret") grace- nonative
(localhost)
已成功更新 USER ac_entm_pers
```

更改 ADS_LDAP_bind_user 密码

ADS_LDAP_bind_user 帐户允许 CA Access Control 企业管理 针对 Active Directory 执行 LDAP 查询。 该帐户的名称不是 ADS_LDAP_bind_user。 该帐户的名称是在安装 CA Access Control 企业管理 时在 Active Directory 设置向导页面中指定的用户 DN。

您可能需要定期更改 ADS_LDAP_bind_user 密码，以符合组织的安全和密码策略。 必须同时更改 Active Directory 和 RDBMS 上的密码。

在更改 ADS_LDAP_bind_user 密码之前，请注意以下事项：

- 默认密码是您在安装 CA Access Control 企业管理 时在 Active Directory 设置向导页面中指定的密码。
- 密码具有以下限制：
  - 长度必须是 7-120 个字符
  - 不能包含高 ASCII 字符
  - 不得包含冒号 (:)
  - 必须遵守 Active Directory 密码规则
- 密码存储在 Active Directory 和 DMS 中

更改 ADS_LDAP_bind_user 密码

1. 使用 Active Directory 工具更改 Active Directory 中的密码。

   注意：有关如何更改密码的详细信息，请参阅 Active Directory 文档。

2. 在 CA Identity Manager 管理控制台中更改用户目录密码 (p. 460)。

   所有位置中的 ADS_LDAP_bind_user 密码已更改。

更改 JNDI 连接帐户

JNDI 连接帐户的名称为 guest，可以在消息队列服务器中查找消息队列。 默认情况下，该帐户没有密码。

您可以更改 JNDI 在消息队列服务器中查找消息队列所用的帐户。 该帐户的名称存储在消息队列和以下 XML 文件中，其中 *JBoss_home* 是 JBoss 的安装目录：

JBoss_home/server/default/deploy/jms/tibco-jms-ds.xml

更改 JNDI 连接帐户

1. 创建消息队列用户。
2. 按如下所述更改 JNDI 连接帐户：
   a. 停止 JBoss 应用程序服务器。
   b. 将 tibco-jms-ds.xml 文件中的帐户名替换为您创建的消息队列用户的名称。
   c. 重新启动 JBoss 应用程序服务器。
   d. 确认您可以登录到 CA Access Control 企业管理。

      此时，JBoss 已成功启动，并且 JNDI 连接帐户已更改。

创建消息队列用户

更改 JNDI 连接帐户时需要创建消息队列用户。

创建消息队列用户

1. 导航到以下目录，其中 *DistServer* 是分发服务器的安装目录：

   DistServer/MessageQueue/tibco/ems/5.1/bin
2. (UNIX) 输入以下命令：

   tibemsadmin

   此时将启动 Tibco EMS 管理工具。
3. (Windows) 输入以下命令：

   tibemsadmin.exe

   此时将启动 Tibco EMS 管理工具。
4. 使用以下命令之一连接到当前环境：
   - 如果分发服务器在端口 7222（默认端口）上侦听报告代理，请使用以下命令：

     connect
   - 如果分发服务器在端口 7243 上侦听处于 SSL 模式的报告代理，请使用以下命令：

     connect SSL://7243
5. 输入用户名和密码。

   注意：默认用户名是 admin，密码是您安装 CA Access Control 企业管理 时指定的通讯密码。

   此时您已连接到消息队列。

6. 输入下面的命令：

   ```
   create user username
   ```

   用户名称

   指定新消息队列用户的名称。

   新用户即已创建。

示例：创建消息队列用户

以下 Tibco EMS 管理工具命令可以创建名为 example 的消息队列用户：

```
> connect SSL://7243
登录名 (admin): admin
密码:
已连接到: ssl://localhost:7243
ssl://localhost:7243> 创建用户 example
已创建用户 example
ssl://localhost:7243>
```

更改 tibco-jms-ds.xml 文件中的帐户

更改 JNDI 连接帐户时需要更改 tibco-jms-ds.xml 文件中的帐户。

更改 tibco-jms-ds.xml 文件中的帐户

1. 停止 JBoss 应用程序服务器（如果尚未停止）。
2. 导航到以下目录，其中 *JBoss_home* 是 JBoss 的安装目录：

   ```
   JBoss_home/server/default/deploy/jms
   ```

3. 在基于文本的编辑器中打开 tibco-jms-ds.xml 文件。
4. 更改以下参数末尾的帐户名：

   ```
   java.naming.security.principal=
   ```

5. 保存并关闭文件。

示例：更改 tibco-jms-ds.xml 文件中的帐户名

以下 Tibco-jms-ds.xml 文件片段显示了已更改的 JNDI 连接帐户。 该帐户的名称为 example：

```
<!-- JMS 提供程序加载程序 -->
        <mbean code="org.jboss.jms.jndi.JMSProviderLoader"
        name=":service=JMSProviderLoader,name=TibjmsProvider">
                <attribute name="ProviderName">TIBCOJMSProvider</attribute>
                <attribute name="ProviderAdapterClass">
                org.jboss.jms.jndi.JNDIProviderAdapter</attribute>
                <attribute
name="FactoryRef">SSLXAQueueConnectionFactory</attribute>
                <attribute
name="QueueFactoryRef">SSLXAQueueConnectionFactory</attribute>
                <attribute
name="TopicFactoryRef">SSLXATopicConnectionFactory</attribute>
                <attribute name="Properties">
                        java.naming.security.principal=example

        java.naming.factory.initial=com.tibco.tibjms.naming.TibjmsInitialCont
extFactory

        java.naming.provider.url=tibjmsnaming://localhost:7243
                        java.naming.factory.url.pkgs=com.tibco.tibjms.naming
                        com.tibco.tibjms.naming.security_protocol=ssl
                        com.tibco.tibjms.naming.ssl_enable_verify_host=false

                </attribute>
        </mbean>
```

更改消息队列通讯设置

您可以更改以下消息队列通讯设置：

- 消息队列管理员的密码
- 消息队列服务器证书
- 消息队列 SSL keystore 的密码
- 端点连接到消息队列所用的密码

  注意：端点使用 +reportagent 服务帐户连接到消息队列。
- CA Access Control 企业管理 和 DMS 连接到消息队列所用的密码

  注意：CA Access Control 企业管理 和 DMS 使用 reportserver 服务帐户连接到消息队列。

更多信息：

更改 +reportagent 密码 (p. 440)
更改 reportserver 密码 (p. 437)

更改消息队列管理员密码

消息队列管理员帐户名为 *admin*，使用它可以在消息队列中执行管理任务。

您可能需要定期更改 admin 密码，以符合组织的安全和密码策略。

在更改消息队列管理员密码之前，请注意以下事项：

- 该帐户的默认密码是在安装 CA Access Control 企业管理 时指定的通讯密码。
- 密码具有以下限制：
  - 长度必须是 1-240 个字符
  - 不能包含高 ASCII 字符
  - 不能包含双引号 (")
- 密码存储在消息队列中。

重要说明！ 如果企业中有多个分发服务器，应首先更改企业管理服务器上安装的分发服务器的密码，然后再更改企业中其他分发服务器的密码。 消息队列是分发服务器的一部分。

要更改消息队列管理员密码，请为 Admin 用户设置消息队列密码 (p. 454)。

示例：为 admin 用户设置消息队列密码

以下 Tibco EMS 管理工具命令可为 admin 用户设置消息队列密码： 密码为“secret”，必须采用明文形式，并包含在双引号中：

```
ssl://localhost:7243> set password admin "secret"
用户“admin” 的密码已修改
ssl://localhost:7243>
```

更改消息队列服务器证书

消息队列使用服务器证书在消息队列及其客户端之间进行 SSL 通讯。 消息队列客户端是 CA Access Control 端点和 CA Access Control 企业管理。

更改消息队列服务器证书

1. 停止 CA Access Control 消息队列。
2. 创建 X.509 服务器证书。

   建议您创建 .p12 格式的证书。
3. 导航到以下目录，其中 *DistServer* 是分发服务器的安装目录：

   DistServer/MessageQueue/tibco/bin/ems
4. 输入下面的命令：

   tibemsadmin -mangle *password*

   密码

   指定服务器证书的密码。

   服务器证书的密码已加密。
5. 在基于文本的编辑器中打开 tibemsd.conf 文件。 该文件位于以下目录：

   DistServer/MessageQueue/tibco/bin/ems
6. 更改下列参数的值：

   ssl_server_identity

   指定服务器证书的完整路径。

   ssl_server_key

   指定服务器证书密钥的完整路径。

   注意：如果使用 .p12 格式的证书，请将该参数留空。

   ssl_password

   指定服务器证书的已加密密码。
7. 保存并关闭文件。

   消息队列服务器证书已更改。
8. 重新启动 CA Access Control 消息队列。

示例：tibemsd.conf 文件

以下是 .p12 服务器证书的 tibemds.conf 文件中的消息队列服务器参数的示例。 密码是 }>8:Jt^+%INK&i^v 并已加密，ssl_server_key 参数没有值：

```
ssl_server_identity     = "C:\Program
Files\CA\AccessControlServer\MessageQueue\conf\keystore.p12"
ssl_server_key          =
ssl_password            = }>8:Jt^+%INK&i^v
```

更改消息队列 SSL Keystore 的密码

消息队列 SSL keystore 存储消息队列为 SSL 通讯使用的服务器证书。 更改消息队列 SSL keystore 的密码时，将会更新用于签署服务器证书的公钥/私钥对。

您可能需要定期更改消息队列 SSL keystore 的密码，以符合组织的安全和密码策略。

在更改消息队列 SSL keystore 的密码之前，请注意以下事项：

- 默认密码是在安装 CA Access Control 企业管理 时指定的通讯密码。
- 密码具有以下限制：
  - 长度必须是 6-50 个字符
  - 不能包含高 ASCII 字符
  - 不能包含双引号 (")
- 密码存储在以下文件中，其中 *ACServer* 是 CA Access Control 企业管理 的安装目录：

  ACServer/MessageQueue/conf/keystore.p12

重要说明！ 如果企业中有多个分发服务器，应首先更改企业管理服务器上安装的分发服务器的密码，然后再更改企业中其他分发服务器的密码。 消息队列是分发服务器的一部分。

更改消息队列 SSL keystore 的密码

1. 停止 CA Access Control 消息队列服务。
2. 打开命令提示符窗口并导航到以下目录，其中 *JDK* 是 Java 开发工具包的安装目录：

   JDK/bin

3. 运行以下命令：

   keytool -genkey -keyalg RSA -keysize 1024 -keystore "keystore.p12" -storetype PKCS12 -dname "cn=acmq" -alias acmq -storepass "*password*" -keypass "*password*"

   -genkey

   指定命令创建密钥对（公钥和私钥）。

   -keyalg RSA

   指定使用 RSA 算法生成密钥对。

   -keysize 1024

   指定生成的密钥大小为 1024 位。

   -storetype PKCS12

   指定生成的密钥格式为 PKCS12 文件格式。

   -dname "cn=acmq"

   指定生成的证书的 X.500 可分辨名称为 acmq。该名称在证书的颁发者和主题字段中使用。

   -alias acmq

   指定更新名称为 acmq 的 keystore 条目。

   -storepass "*password*"

   指定用于保护消息队列 SSL keystore 的密码。 该密码必须与您为 -keypass 参数指定的密码相同。

   -keypass "*password*"

   指定用于保护新密钥对中私钥的密码。 该密码必须与您为 -storepass 参数指定的密码相同。

   keytool 实用程序将会更改消息队列 SSL keystore 的密码。

4. 导航到以下目录，其中 *DistServer* 是分发服务器的安装目录：

   DistServer/MessageQueue/tibco/bin/ems

5. 运行以下命令：

   tibemsadmin -mangle *password*

   将为 SSL keystore 的密码加密。

密码更改过程

以下过程说明更改 CA Access Control 密码的不同方式。

使用 selang 更改密码

您可以使用 selang 更改下列服务帐户的密码：

- +policyfetcher
- +devcalc
- ac_entm_pers

您可能需要定期更改这些帐户的密码，以符合组织的安全和密码策略。

使用 selang 更改密码时，请注意以下事项：

- 必须在密码两侧加上双引号。
- 不能使用高级策略管理来传播密码更改命令。

注意：您可能需要使用多种方法更改与服务帐户交互的所有组件上的密码。

要使用 selang 更改密码，请运行以下命令：

```
cu user password("password") grace- nonative
```

user

指定要更改其密码的用户名。

password

指定新的密码。

注意：如果将密码剪切并粘贴到命令中，请确认密码不包含回车或换行。

示例：更改 +policyfetcher 密码

该命令可为 +policyfetcher 用户更改密码。 密码为“secret”，必须采用明文形式，并包含在双引号中：

```
AC> cu +policyfetcher password("secret") grace- nonative
(localhost)
已成功更新 USER +policyfetcher
```

更多信息：

更改 +policyfetcher 密码 (p. 441)
更改 +devcalc 密码 (p. 442)
更改 ac_entm_pers 密码 (p. 443)

使用 sechkey 更改消息队列密码

您可以使用 sechkey 更改下列服务帐户的密码：

- reportserver
- +reportagent

您可能需要定期更改这些帐户的密码，以符合组织的安全和密码策略。在使用 sechkey 更改密码时，必须在密码两侧加上双引号。

注意：您可能需要使用多种方法更改与服务帐户交互的所有组件上的密码。

要使用 sechkey 更改消息队列密码，请在分发服务器上运行以下命令：

```
{sechkey | acuxchkey} -t [-server] -pwd "password"
```

sechkey

指定此项可以更改 CA Access Control 端点上的密码。

acuxchkey

指定此项可以更改 UNAB 端点上的密码。

-server

指定此项可以更改 DMS 上的密码。

注意：此参数仅与 sechkey 参数一起使用时才有效。

密码

指定新的密码。

注意：如果将密码剪切并粘贴到命令中，请确认密码不包含回车或换行。

示例：更改 UNAB 端点上的消息队列密码

以下命令将消息队列密码传播到与分发服务器通讯的所有 UNAB 端点。密码为“secret”，必须采用明文形式，并包含在双引号中：

```
acuxchkey -t -pwd "secret"
```

示例：更改 DMS 上的消息队列密码

该命令可更改 DMS 上的消息队列密码。 密码为“secret”，必须采用明文形式，并包含在双引号中：

```
sechkey -t -server -pwd "secret"
```

更多信息：

更改 reportserver 密码 (p. 437)
更改 +reportagent 密码 (p. 440)

设置消息队列密码

设置消息队列密码以更改下列服务帐户的密码：

- reportserver
- +reportagent

您可能需要定期更改这些帐户的密码，以符合组织的安全和密码策略。在设置消息队列密码时，您必须在密码两侧加上双引号。

注意：您可能需要使用多种方法更改与服务帐户交互的所有组件上的密码。

设置消息队列密码

1. 导航到以下目录，其中 *DistServer* 是分发服务器的安装目录：

   DistServer/MessageQueue/tibco/ems/5.1/bin

2. (UNIX) 输入以下命令：

   ```
   tibemsadmin
   ```

   此时将启动 Tibco EMS 管理工具。

3. (Windows) 输入以下命令：

   ```
   tibemsadmin.exe
   ```

   此时将启动 Tibco EMS 管理工具。

4. 使用以下命令之一连接到当前环境：

   - 如果分发服务器在端口 7222（默认端口）上侦听报告代理，请使用以下命令：

     ```
     connect
     ```

   - 如果分发服务器在端口 7243 上侦听处于 SSL 模式的报告代理，请使用以下命令：

     ```
     connect SSL://7243
     ```

5. 输入用户名和密码。

   注意：默认用户名是 admin，密码是您安装 CA Access Control 企业管理 时指定的通讯密码。

   此时您已连接到消息队列。

6. 运行以下命令：

   set password *user* "*password*"

   user

   指定要更改其密码的用户名。

   "***password***"

   指定新的密码。

   用户密码已在消息队列上更改。

   注意：如果将密码剪切并粘贴到命令中，请确认密码不包含回车或换行。

示例：为 reportserver 用户设置消息队列密码

该 Tibco EMS 管理工具命令可为 reportserver 用户设置消息队列密码。密码为“secret”，必须采用明文形式，并包含在双引号中：

```
> connect SSL://7243
登录名 (admin): admin
密码:
已连接到: ssl://localhost:7243
ssl://localhost:7243> set password reportserver "secret"
用户 “reportserver” 的密码已修改
ssl://localhost:7243>
```

更多信息：

更改 reportserver 密码 (p. 437)
更改 +reportagent 密码 (p. 440)

加密明文密码

加密下列服务帐户的明文密码：

- RDBMS_service_user
- reportserver

之所以对密码加密，是因为这些密码存储在 JBoss 目录中的明文 XML 文件内。 使用 pwdtools 实用程序可加密明文密码。

为避免意外选择加密密码中的换行符，建议将加密密码（实用程序的输出）定向到文本文件。 否则，如果加密密码的长度超过一行，可能会发生换行。

在使用 pwdtools 加密明文密码时，您必须在密码两侧加上双引号。

加密明文密码

1. 打开命令提示符窗口。
2. 导航到下列目录，其中 *ACServerInstallDir* 是 CA Access Control 企业管理 的安装目录：

   ACServerInstallDir/IAM Suite/Access Control/tools/PasswordTool
3. 运行以下命令：

   pwdtools -FIPS -p "*password*" -*k* [*filename*]

   密码

   指定明文密码。

   filename

   指定 pwdtools 将加密密码输出到的文件的名称。

   pwdtools 将会加密密码。

示例：加密明文密码

以下命令可以加密明文密码，并将加密的密码定向到文件 pw.txt。 明文密码是 "secret"，必须在其两侧加上双引号：

```
C:\Program Files\CA\AccessControlServer\IAM Suite\Access
Control\tools\PasswordTool>
pwdtools.bat -FIPS -p "secret" -key
C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\config\com\netegri
ty\config\keys\FIPSkey.dat"
```

更多信息：

更改 RDBMS service user 密码 (p. 436)
更改 reportserver 密码 (p. 437)

更改 properties-service.xml 文件中的密码

更改 properties-service.xml 文件中的密码可以更改 reportserver 帐户的密码。 您可能需要定期更改该帐户的密码，以符合组织的安全和密码策略。

注意：您可能需要使用多种方法更改与服务帐户交互的所有组件上的密码。

更改 properties-service.xml 文件中的密码

1. 停止 JBoss 应用程序服务器。
2. 导航到以下目录，其中 *JBoss_home* 是 JBoss 的安装目录：

   JBoss_home/server/default/deploy
3. 在基于文本的编辑器中打开 properties-service.xml 文件。
4. 更改 SamMDB.mdb-passwd 参数中的密码。
5. 保存并关闭文件。

示例：在 properties-service.xml 文件中更改密码

properties-service.xml 文件的该片段显示了已更改的 reportserver 密码。密码为 }>8:Jt^+%INK&i^v 并已加密：

```
<attribute name="Properties">
      SamMDB.mdb-user=reportserver
      <!-- 编码的 tibco 密码 -->
      SamMDB.mdb-passwd={AES}:}>8:Jt^+%INK&i^v==
</attribute>
```

更多信息：

更改 reportserver 密码 (p. 437)

更改 login-config.xml 文件中的密码

在更改下列服务帐户的密码时，将会更改 login-config.xml 文件中的密码：

- RDBMS_service_user
- reportserver

您可能需要定期更改这些帐户的密码，以符合组织的安全和密码策略。

注意：您可能需要使用多种方法更改与服务帐户交互的所有组件上的密码。 如果密码是明文密码，请先使用 pwdtools 实用程序加密该密码，然后再更改 login-config.xml 文件中的密码。

更改 login-config.xml 文件中的密码

1. 停止 JBoss 应用程序服务器。
2. 导航到以下目录，其中 *JBoss_home* 是 JBoss 的安装目录：

   JBoss_home/server/default/conf
3. 在基于文本的编辑器中打开 login-config.xml 文件。
4. 更改 RDBMS_service_user 密码：
   a. 在该文件中找到 RDBMS_service_user 帐户名称的每个实例。

      该文件中有六个实例。 在创建用户以便为 CA Access Control 企业管理 准备数据库时，需要为该帐户命名。

   b. 更改紧接在每个名称实例后面的参数中的密码。

      参数括在 <module-option name="password"> 和 </module-option> 标记内。

   RDBMS_service_user 密码已更改。
5. 更改 reportserver 密码：
   a. 在文件中找到以下参数：

      ```
      <module-option name="userName">reportserver</module-option>
      ```
   b. 更改紧接在该参数后面的参数中的密码。

      参数括在 <module-option name="password"> 和 </module-option> 标记内。

   reportserver 密码已更改。
6. 保存并关闭文件。

示例：更改 login-config.xml 文件中的 RDBMS_service_user 密码

login-config.xml 文件的该片段显示了已更改的 RDMBS_service_user 密码的一个实例。 用户名为 caidb01。 密码为 }>8:Jt^+%INK&i^v 并已加密：

```
<application-policy name="imobjectstoredb">
        <authentication>
                <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin"
                flag="required">
                        <module-option
name="userName">caidb01</module-option>
                        <module-option
name="password">{AES}:}>8:Jt^+%INK&i^v==</module-option>
                        <module-option name="managedConnectionFactoryName">

        jboss.jca:name=jdbc/objectstore,service=NoTxCM</module-option>
                </login-module>
        </authentication>
</application-policy>
```

示例：更改 login-config.xml 文件中的 reportserver 密码

login-config.xml 文件的该片段显示了已更改的 reportserver 密码。 密码为 }>8:Jt^+%INK&i^v 并已加密：

```
<application-policy name="JmsXATibcoRealm">
       <authentication>
          <login-module
code="com.netegrity.jboss.datasource.PasswordEncryptedLogin" flag="required">
             <module-option name="userName">reportserver</module-option>
            <module-option
name="password">{AES}:}>8:Jt^+%INK&i^v==</module-option>
                <module-option name="managedConnectionFactoryName">
                jboss.jca:service=TxCM,name=TibcoJmsXA</module-option>
          </login-module>
       </authentication>
    </application-policy>
```

更多信息：

更改 RDBMS_service_user 密码 (p. 436)
更改 reportserver 密码 (p. 437)

更改 CA Identity Manager 管理控制台中的用户目录密码

更改 ADS_LDAP_bind_user 密码时，会更改 CA Identity Manager 管理控制台中的用户目录密码。 您可能需要定期更改该帐户的密码，以符合组织的安全和密码策略。

注意：您可能需要使用多种方法更改与服务帐户交互的所有组件上的密码。

更改 CA Identity Manager 管理控制台中的用户目录密码

1. 加密明文密码 (p. 455)。
2. 打开 CA Identity Manager 管理控制台 (p. 73)。
3. 单击“目录”。

   此时将显示“目录”页面。
4. 单击 ac-dir。

   此时将显示“目录属性”页面。
5. 单击“导出”。

   已导出 ac-dir.xml 文件。
6. 在基于文本的编辑器中打开导出的文件。
7. 找到以下参数：

   ```
   <Credentials user=
   ```
8. 在 <credentials> 参数后面的以下字段中输入加密密码：

   ```
   {PBES}=
   ```
9. 保存并关闭文件。
10. 在 CA Identity Manager 管理控制台中的“目录属性”页面上单击“更新”。

    此时将显示“更新目录”窗口。
11. 键入已编辑的 XML 文件的路径和文件名，或浏览到该文件，然后单击“完成”。

    状态信息显示在“目录配置输出”字段中。
12. 单击“继续”，然后重新启动环境。

    已更改 CA Identity Manager 管理控制台中的用户目录密码。

示例：更改用户目录密码

导出的 ac-dir.xml 文件中的该片段显示了更改的用户目录密码。 用户命名为 Administrator。 密码为 }>8:Jt^+%INK&i^v 并已加密：

```
<Credentials user="CN=Administrator,cn=Users,DC=unixauthdemo,DC=co,DC=il">
{PBES}:}>8:Jt^+%INK&i^v==</Credentials>
```

更多信息：

启用 CA Identity Manager 管理控制台 (p. 72)
打开 CA Identity Manager 管理控制台 (p. 73)
更改 ADS_LDAP_bind_user 密码 (p. 444)