CA Access Control 高级版

升级指南

12.6.01

第三方通知

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

示例脚本和示例 SDK 代码

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

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

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA Access Control 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）
- 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—\ProgramFiles\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。

目录

第 1 章： 关于本指南

本指南提供如何升级 CA Access Control 高级版 服务器和端点组件，以及如何将 PMD 迁移到高级政策环境的信息。

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： 升级服务器和端点组件

此部分包含以下主题：

开始之前

请在开始升级过程之前查看以下主题：

将现有的中央数据库升级到 Microsoft SQL Server 2008

如果在 Microsoft SQL Server 2005 上配置了 CA Access Control 企业管理中央数据库，并且要升级到 Microsoft SQL Server 2008，则需要将企业管理服务器配置为与新服务器配合使用。

请按下列步骤操作：

1. 停止企业管理服务器上所有的 CA Access Control 服务。
2. 停止 JBoss。 完成以下步骤之一：
   - 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。
3. 升级到 Microsoft SQL Server 2008。
4. 从 Microsoft 网站下载 Microsoft SQL Server JDBC Driver 2.0。
5. 将文件提取到企业管理服务器上的临时目录。
6. 完成以下步骤之一：
   - 如果使用的是 JDK 版本 1.5，请查找 sqljdbc.jar 文件。
   - 如果使用的是 JDK 版本 1.6 或更高版本，请查找 sqljdbc4.jar 文件并将其重命名为 sqljdbc.jar。

7. 将文件复制到企业管理服务器上的以下目录：

   JBoss_HOME/server/default/lib

   注意：将覆盖该目录中的现有文件。

8. 启动 Microsoft SQL Server 2008 服务。
9. 启动 JBoss。
10. 启动 CA Access Control 企业管理。

针对企业管理准备 CA Access Control 端点

可以在 CA Access Control 端点上安装企业管理服务器。 端点不包含企业管理服务器需要的所有组件。 您需要先准备端点，然后才可以在端点上安装企业管理服务器。

请按下列步骤操作：

1. 停止端点上的所有 CA Access Control 服务 (Windows) 或后台进程 (UNIX)
2. 在端点上安装企业管理服务器

   安装基于 Web 的应用程序和分发服务器。 此外，安装最新版本的 CA Access Control（如果尚未安装）。

3. 在企业管理服务器上创建 DMS。

   企业管理服务器安装不会在端点上创建 DMS。 使用 dmsmgr 实用程序来创建 DMS。

4. 启动企业管理服务器服务或后台进程。
5. 使用 ADMIN、AUDITOR 和逻辑授权属性创建一个用户帐户。

   在 CA Access Control 企业管理 中定义 DMS 连接设置时，请使用逻辑用户帐户。

6. 在 DMS 上创建主机组。
7. 使用 dmsmgr 实用程序将节点添加到 DMS 中。

8. 使用安装企业管理服务器时指定的管理用户帐户登录到 CA Access Control 企业管理。
9. 在 CA Access Control 企业管理 中，定义 DMS 连接设置。

   指定在端点上创建的 DMS。

   企业管理服务器现已安装并配置为使用您创建的 DMS。

注意：有关 dmsmgr 实用程序的详细信息，请参阅 *《参考指南》*。有关如何使用 selang 创建和配置用户的详细信息，请参阅 *《selang 参考指南》*。

准备升级企业管理服务器

开始将 r12.5.x 企业管理服务器安装升级到 r12.6.1 之前，收集以下信息：

- 消息队列密码

  获取管理用户、reportserver 用户以及 +reportagent 用户密码。
- 数据库连接信息

  获取主机名、端口号、数据库名称、用户名以及密码。
- Java 连接器服务器密码

  获取以前安装 CA Access Control 企业管理 过程中使用的通讯密码。
- （可选）Java 连接器服务器 (JCS) SSL 证书

  仅当使用自定义 SSL 证书时，才需要在升级到 CA Access Control 企业管理 r12.5.x 后导入新的 SSL 证书。

升级后导入 Java 连接器服务器 SSL 证书

由于 CA Access Control r12.5 SP3 中的 Java 连接器服务器 (JCS) SSL 证书发生了更改，因此从 CA Access Control r12.5.x 升级之后，需要导入新的 SSL 证书。

重要说明！ 仅当使用的是自定义 JCS SSL 证书时，才需要完成此过程。如果使用默认 SSL 证书，则不需要执行此过程。

请按下列步骤操作：

1. 停止 JBoss 应用程序服务器。
2. 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/custom/ppm/trusttore/

3. 备份 ssl.keystore 文件。
4. 从先前导航到的目录打开命令提示符窗口。
5. 运行 keytool 实用程序来指定要导入的自定义 SSL keystore，其中 *JAVA_HOME* 表示 JDK 的安装目录。 例如：

   ```
   JAVA_HOME\bin\keytool.exe -import -alias eta_client -file
   c:\custom_certificate.der -keystore ssl.keystore
   ```

   将显示密码提示符。
6. 输入密钥存储密码。 默认密码为 *secret*。

   keytool 显示证书详细信息和指纹。
7. 键入“是”将证书添加到 keystore 中。

   keytool 将添加新的证书。
8. 启动 JBoss 应用程序服务器。

   您已将新的 JCS SSL 证书文件加载到 CA Access Control 企业管理。

如何从 CA Access Control r5.3 升级

由于部署中增加了组件并已发生更改，您无法从 CA Access Control r5.3 升级到 CA Access Control r12.6.1。 先将现有的 CA Access Control r5.3 部署升级到 CA Access Control r8.0Sp1，然后即可升级到 CA Access Control r12.6.1。

通过执行以下步骤来升级现有的 CA Access Control r5.3 部署：

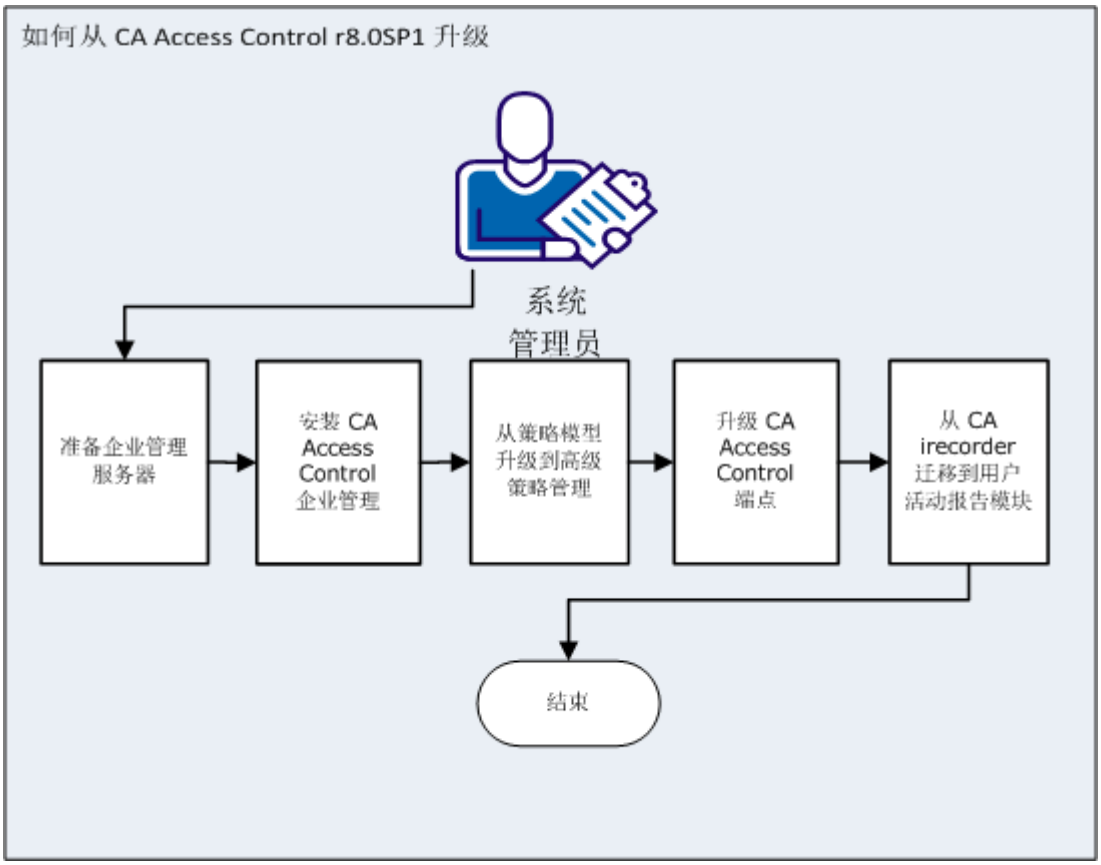
1. 先备份所有 CA Access Control 组件，然后开始升级过程。
2. 升级到 CA Access Control r8.0SP1 (p. 15)
3. 升级到 CA Access Control r12.6.1

第 3 章： 从 CA Access Control r8.0SP1 升级

此方案的目的是说明从 CA Access Control r8.0SP1 升级所要遵循的步骤。本章中的升级过程假定 CA Access Control r8.0SP1 组件安装在独立计算机上。

本节中的信息适用于从事管理 CA Access Control 的系统或 CA Access Control 管理员。

下图说明完成从 CA Access Control r8.0SP1 升级的步骤：



重要说明！ 先备份所有 CA Access Control 组件，然后开始升级过程。

通过执行以下步骤来升级现有的 CA Access Control r8.0SP1 部署：

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。

2. 安装 CA Access Control 企业管理 (p. 18)。
3. 从策略模型环境升级到高级策略管理环境 (p. 57)。
4. 升级 CA Access Control 端点：
   - Windows - 使用产品资源管理器进行安装 (p. 22)
   - UNIX - 使用 install_base 脚本进行安装 (p. 23)

   注意：安装也会升级密码 PMD。
5. （可选）将 iRecorder product 迁移到 CA User Activity Reporting Module。

注意：无法升级策略管理器。 使用 CA Access Control 端点管理 管理端点上的策略。

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)。 在安装 CA Access Control 企业管理 之前，您进行设置。

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。

请按下列步骤操作：

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。

      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。 有关详细信息，请参阅《*实施指南*》。

   b. 部署部署脚本。

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。

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。

请按下列步骤操作：

1. 如果 JBoss 应用程序服务器正在运行，请将其停止。
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\Dis1\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. 根据需要完成向导。 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。

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。

通讯密码

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

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

数据库信息

定义 RDBMS 的连接详细信息：

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

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

安装程序先检查数据库的连接，然后再继续。

用户存储类型

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

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

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

Active Directory 设置

定义 Active Directory 用户存储设置：

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

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

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

安装程序会先检查与 Active Directory 的连接，然后再继续。

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

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

系统用户

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

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

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

管理员密码

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

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

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

6. 选择“是，重新启动我的系统”，然后单击“完成”。

   现在可以为企业配置 CA Access Control 企业管理。

使用产品资源管理器进行安装

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。

请按下列步骤操作：

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”。

   您需要选择安装选项，该选项与正在安装的（32 位、64 位 x64 或 64 位 Itanium）计算机的体系结构相匹配。

   “选择安装语言”窗口将会出现。
5. 选择要安装的 CA Access Control 语言，然后单击“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 CA Access Control 的现有安装，系统会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 时所需要的信息，请参阅安装工作表。

   安装程序将升级 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”。

   系统重新启动之后，您可以检查 CA Access Control 是否已正确安装。

   注意：如果您选择稍后重新启动计算机，会有其他警告出现，提示您安装未完成，直到您重新启动计算机。 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。

使用 install_base 脚本进行安装

您可以使用 install_base 脚本在任何支持的操作系上安装 CA Access Control。 这是一个交互脚本，但您仍可以静默方式运行该脚本。

注意：运行 install_base 脚本之前，请确保您决定要安装哪个功能并查看 install_base 命令，以便了解如何启动此功能的安装。 您也可以首先了解 install_base 脚本的工作原理。

请按下列步骤操作：

1. 如果您已安装 CA Access Control 且正在运行，那么通过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*根*用户身份登录。

   要安装 CA Access Control，您需要具有根权限。

3. 挂接光盘驱动器运行 CA Access Control Endpoint Components for UNIX DVD。

   重要说明！ 如果从光盘驱动器安装在 HP 上，您需要确保可以从 DVD 正常读取文件名。 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. 阅读该许可协议。

   要运行 install_base 脚本，您需要接受最终用户许可协议。 阅读许可协议之后，您可以通过在该文件结尾找到的命令继续安装。 要获得许可文件名和位置，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：安装脚本发现适当的压缩 tar 文件，因此键入用于您的平台的 tar 文件名称为可选。

   现在，CA Access Control 安装已完成；然而，尚未运行。

示例：使用静默安装升级到 CA Access Control r12.6SP1 for UNIX

本示例显示如何将现有的 CA Access Control r8.0SP1 端点升级到 CA Access Control r12.6SP1 for UNIX。 本示例将使用可让您在端点上安装新功能的 parameters 文件来安装 CA Access Control。

1. 查看 install_base 脚本命令。

   使用 install_base 脚本以静默模式安装 CA Access Control r12.6SP1。有关详细信息，请参阅《*实施指南*》。

2. 从 CA Access Control Endpoint Components for UNIX 介质上的 tar 压缩文件中提取 parameters 文件。 该文件位于以下目录：

   ```
   \Unix\Access-Control\
   ```

3. 使用 install_base 脚本安装 CA Access Control。

   使用 -autocfg 命令，并指定使用您自定义的 parameters 文件。

   CA Access Control r12.6SP1 装有您所指定的选项。

示例：parameters 文件

通过 parameters 文件可以选择要添加到端点的软件组件。 如果以本地安装模式安装 CA Access Control，请先自定义文件，然后开始安装。 如果以交互模式安装 CA Access Control，则可以将安装参数提取到某个文件中，然后自定义安装参数。

以下是 parameters 文件中的一个片段：

```
#  Specifies whether you want to configure PUPM Agent
#  Values: "yes", "no"
#  Default: "no"
INSTALL_PUPM="yes"

# Specifies whether  enables KBL audit records management
# Values: yes, no
# Default: no
ENABLE_KBL=yes
```

本示例通过 (INSTALL_PUPM=yes) 指定安装 PUPM 集成， 并通过 (ENABLE_KBL=yes) 启用端点上的键盘日志记录。

示例：安装客户端和服务器软件包和默认功能

以下命令显示出如何启动 install_base 交互式脚本，以便安装客户端和服务器软件包和所有的默认 CA Access Control 功能。 在安装期间，会要求您回答与安装 CA Access Control 的客户端和服务器软件包的相关问题。

```
/dvdrom/Unix/Access-Control/install_base
```

注意：因为我们没有指定要安装的软件包，install_base 命令既安装客户端，又安装服务器软件包。

示例：安装对自定义目录启用 STOP 的客户端软件包

以下命令显示如何启动 install_base 交互式脚本，以便将客户端软件包安装到 /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
```

从 CA Access Control r12.0 SP1 升级

本节详细说明 CA Access Control 或系统管理员要升级现有的 CA Access Control r12.0 SP1 部署所遵循的步骤。 本章中的过程假定管理员在不同的计算机上安装 CA Access Control r12.0 SP1 组件。

例如，企业管理服务器安装在一台计算机上，而 DMS、DH 和报告服务器也安装在其他计算机上。

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。

开始之前

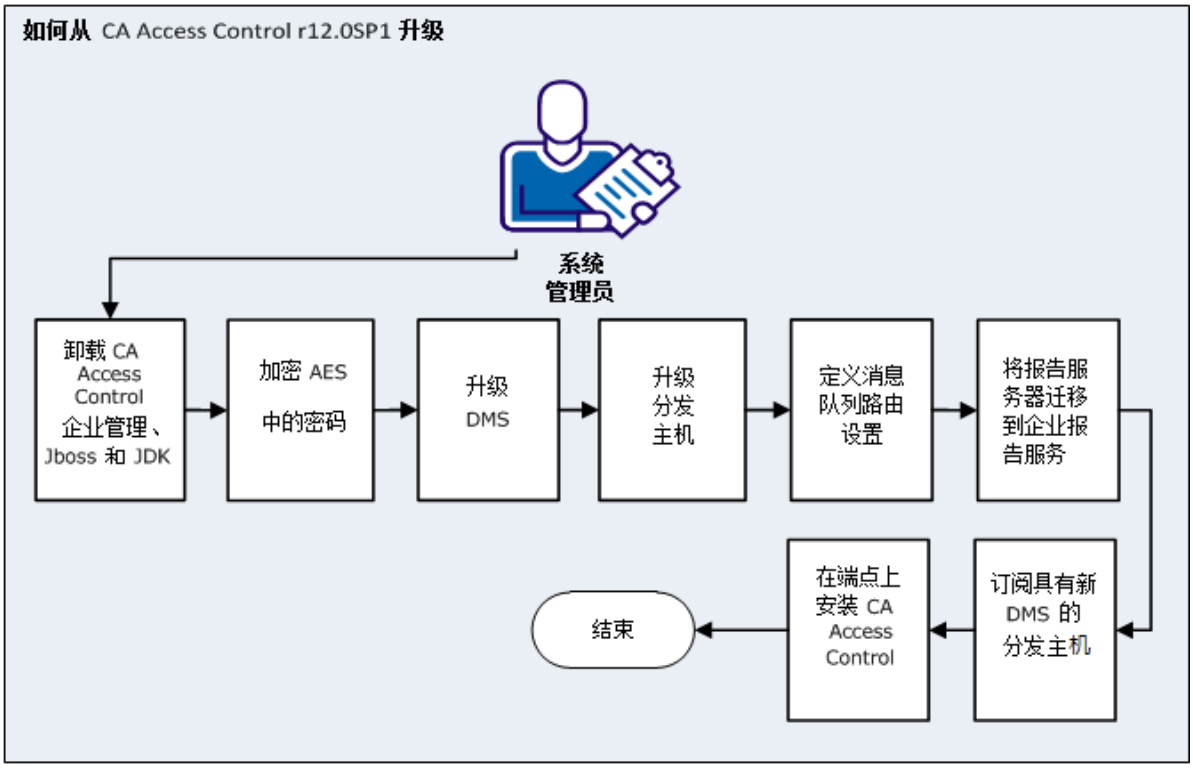
在您开始升级当前的 CA Access Control 安装之前，请考虑以下内容：

- 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：企业管理服务器、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。 您必须先升级企业管理服务器、DMS 和 DH，然后才能启动服务器。
- 在安装企业管理服务器时，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企业管理服务器时，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。

如何从 r12.0 SP1 升级

以下步骤说明如何升级现有的 CA Access Control r12.0 SP1 部署：



1. 升级企业管理服务器。
    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 (p. 30)。
    c. 安装 CA Access Control 企业管理。
2. 使用 AES 加密现有密码 (p. 38)。

    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 (p. 40)。

    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. 升级分发主机 (p. 42)。

    注意：升级您企业中的每个 DH。 如果 DH 与企业管理服务器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 (p. 44)。
6. 将报告服务器迁移到企业报告服务 (p. 55)。
7. 为 DH 订阅新的 DMS (p. 56)。
8. （可选）升级 CA Access Control 端点 (p. 56)。

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后安装步骤。

请按下列步骤操作：

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》*。
2. 卸载现有的 JDK 和 JBoss。

3. 安装先决条件软件 (p. 30)。
4. 安装 CA Access Control 企业管理 (p. 18)。

   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，您必须指定使用嵌入式用户存储。
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 (p. 35)。
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。

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。

请按下列步骤操作：

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. 根据需要完成向导。

   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。
   - 如果您想安装其他企业管理服务器，对于高可用性或灾难恢复，请指定安装 CA Access Control 企业管理 的自定义 FIPS 密钥。 系统提示时，请单击“完成”以关闭出现的对话框。
   - 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。

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

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

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

数据库信息

定义 RDBMS 的连接详细信息：

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

  注意：在准备数据库时已向此用户授予了适当的数据库权限。

- **密码**－定义在准备数据库时创建的用户的 RDBMS 密码。

安装程序先检查数据库的连接，然后再继续。

用户存储类型

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

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

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

Active Directory 设置

定义 Active Directory 用户存储设置：

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

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

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

安装程序会先检查与 Active Directory 的连接，然后再继续。

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

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

系统用户

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

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

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

管理员密码

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

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

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

6. 选择“是，重新启动我的系统”，然后单击“完成”。

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

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。

遵循这些步骤:

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. 输入以下命令更改默认 ssl、keystore 密码：

   keytool -storepasswd -new *password* -keystore ssl.keystore -storepass secret

   -storepasswd

   指定更改 keystore 密码。 密码必须至少为六个字符长。

   -keystore

   指定要添加证书的 keystore 名称。

   -keystore

   指定 keystore 名称。

   -storepass

   定义保护 keystore 所用的密码。
4. 输入以下命令，以便创建企业管理服务器的密钥：

   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。

   -keyalg

   指定要用来生成密钥对的算法。

   将启动 keytool 实用程序。
5. 输入密码 *secret*。
6. 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。

   注意：keystore 和 ket 别名必须使用相同密码。

7. 输入以下命令，以便将 keystore 密码加密到文件：

   ```
   java -cp JBoss_HOME/server/default/lib/jbossx.jar
   org.jboss.security.plugins.FilePassword welcometojboss 13 passowrd
   <kestore_password> keystore.password
   ```

   注意：盐和 IterationCount 是定义加密密码强度的变量。 在此示例中，“welcometojboss”是盐，“13”是重复计数。

8. 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

9. 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
           使用 APR 时，该连接器使用 JSSE 配置，
           连接器应使用 APR 文档中所描述的
           OpenSSL 样式配置 -->
       <!--
       <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。

10. 注释掉 <Connector port> 标记上方的 "<!--"。

    现在可以编辑该标记。

11. 将以下属性添加到 <Connector port> 标记：

    ```
    securityDomain="java:/jaas/encrypt-keystore-password"
    SSLImplementation="org.jboss.net.ssl.JBossImplementation"
    ```

12. 保存并关闭 server.xml 文件。
13. 导航到以下目录找到 jboss-service.xml 文件：

    JBOss_HOME/server/default/deploy/jboss-web.deployer/META-INF

14. 在 <server> 和 </server> 标记之间添加以下 mbean：

```
<mbean code="org.jboss.security.plugins.JaasSecurityDomain"
name="jboss.security:service=PBESecurityDomain">
      <constructor>
         <arg type="java.lang.String"
value="encrypt-keystore-password"></arg>
      </constructor>
      <attribute
name="KeyStoreURL">${jboss.server.home.dir}/deploy/IdentityMinder.ear/cus
tom/ppm/truststore/ssl.keystore</attribute>
      <attribute
name="KeyStorePass">{CLASS}org.jboss.security.plugins.FilePassword:${jbos
s.server.home.dir}/deploy/IdentityMinder.ear/custom/ppm/truststore/keysto
re.password</attribute>
<attribute name="Salt">welcometojboss</attribute>
<attribute name="IterationCount">13</attribute>
 </mbean>
```

    注意：在以上示例中，“welcometojboss”是盐，“13”是重复计数。

15. 保存并且关闭 jboss-service.xml
16. 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。

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。

请按下列步骤操作：

1. 停止所有 CA Access Control 服务。
2. 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’;
```

3. 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。

4. 从连接表中删除 DMS 设置。 运行以下查询：

   ```
   DELETE FROM connection WHERE connection_name='con1';
   ```

5. 启动所有 CA Access Control 服务。

6. 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 (p. 22)。

您现在可配置 CA Access Control 企业管理 以连接到 DMS (p. 41)。

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”。

   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。

   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。

配置到 DMS 的连接

在安装期间，CA Access Control 企业管理 被配置为依靠安装在企业服务器上的部署映射服务器 (DMS) 进行工作。 要创建与其他 DMS 的自定义连接，需要通过配置与自定义 DMS 的连接来针对所用环境进行相应配置。

注意：在安装期间，CA Access Control 企业管理 使用 *ac_entm_pers* 用户帐户创建与企业管理服务器上 DMS 的默认连接。

配置与 DMS 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 DMS 树。

   此时“创建连接”任务会显示在可用任务列表中。

2. 单击“创建连接”。

   此时出现“创建连接”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

   定义要用于该连接的名称。

   连接类型

   指明所创建连接的类型 (AC)。

   说明

   （可选）定义该连接的说明。

   主机名

   定义 CA Access Control 企业管理 运行所在的 DMS 的名称。

   格式： DMS*Name*@*hostName*

   例如：要使用主机 host1.comp.com 上在安装 CA Access Control 企业管理 时所安装的默认 DMS，请键入：DMS__@host1.comp.com。

用户 ID

定义对 DMS 具有管理权限的用户的名称。

建议您使用您创建的专用代理用户，并且不要使用默认的管理用户来代表已登录用户执行 CA Access Control 企业管理 操作。

注意： DMS 审核记录将显示已定义的代理用户代表已登录至 CA Access Control 企业管理 的用户执行了数据库命令。

密码

定义对 DMS 具有管理权限的用户的密码。

默认连接

指定该连接是否是您登录时 CA Access Control 企业管理 默认使用的连接。

注意： 如果指定默认连接，在建立连接前，需要先注销，然后重新登录。

单击“提交”。

CA Access Control 企业管理 使用您指定的信息来尝试登录 DMS。 如果信息正确，将建立连接，此时您即可使用 CA Access Control 企业管理 来管理 CA Access Control 的企业部署。 如果信息不正确，并且 CA Access Control 企业管理 无法登录到 DMS，将显示错误消息，说明无法建立连接的原因。

升级分发主机 (DH)

成功升级 DMS 之后，您可以升级分发主机 (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，您可以通过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 (p. 43)。

   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. 44)。

   分发服务器现已配置。

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密码（通讯密码）。

   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。

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”。
   - (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/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”。
   - (UNIX) 请执行以下操作：
     a. 导航到下列目录，其中 *ACServerInstallDir* 是企业管理服务器的安装目录：

     ```
     ACServerInstallDir/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。

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。

请按下列步骤操作

1. 在报告服务器计算机上安装分发服务器 (p. 43)。
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. 44)。

   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。

   注意：有关企业报告服务器组件的更多信息，请参阅《*企业管理指南*》。
4. 为 DH 订阅新的 DMS (p. 56)。

为 DH 订阅 DMS

完成升级 CA Access Control 企业管理 组件之后，您无法使用以前的 DMS 继续工作。 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！ 只有在报告服务器计算机上安装分发服务器时，才能完成此步骤。

请按下列步骤操作：

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。

   sepmd -s DH__WRITER DMS__@<entm>
3. 将新的 DMS 添加为分发主机父级。

   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。

   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》*。

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 (p. 22)。

第 4 章： 将 PMD 迁移到高级策略管理环境

此部分包含以下主题：

迁移到高级策略管理环境

从策略模型 (PMD) 环境迁移到高级策略管理环境中时，您可以更改将规则部署到端点的方式：

- 在 PMD 环境中，您在中央数据库 (PMDB) 中定义的常规规则会自动传播到已配置的层级结构中的数据库。
- 在高级策略管理环境中，您可以将策略（规则组）分配到一个或多个主机或主机组。 您还可以取消部署（删除）策略以及查看部署状态和部署偏差。

从 PMD 环境迁移到高级策略管理环境时，可执行以下操作：

- 安装其他组件
- 使用 PMDB 中的规则创建策略
- 升级端点
- 将 PMD 结构扁平化

高级策略管理不支持层级主机组。 如果 PMD 体系结构包含层级 PMDB，必须将 PMD 层级结构扁平化。

注意：高级策略管理不支持使用密码管理命令的策略。 必须使用密码 PMD 同步端点之间的密码以及分发密码管理规则。 不能将密码 PMD 迁移到高级策略管理环境。 相反，您需要将筛选文件应用于密码 PMD，以便其仅将密码规则发送到其订户。

迁移过程的工作原理

通过迁移到高级策略管理环境，您可以部署和取消部署策略，以及查看策略的部署和偏差状态。 虽然您使用 CA Access Control 执行大多数迁移任务，但仍必须自己执行一些任务。 了解迁移过程的工作原理有助于对可能出现的任何问题进行故障排除。

以下过程概述了迁移过程中的各个阶段：

1. 安装企业管理服务器组件。

   高级策略管理环境的设置是企业管理安装过程的一部分。

2. 将 PMD 升级到 CA Access Control r12.5 或更高版本。
3. 将订阅 PMD 的端点迁移到高级策略管理环境。
4. 在 CA Access Control 企业管理 中，将 PMDB 中的规则导出到策略文件。
5. CA Access Control 企业管理 在 DMS 上创建以下项：
   - 主机组（GHNODE 对象），与迁移的 PMDB 相对应
   - 主机（HNODE 对象），与 PMDB 的端点订户相对应
   - POLICY 对象，包含策略文件中的规则
6. 在 CA Access Control 企业管理 中，将主机加入到主机组中。 CA Access Control 将 POLICY 对象分配给主机组，并将 POLICY 对象部署到与 PMDB 的端点订户相对应的主机。
7. 在 CA Access Control 企业管理 中，执行下列操作之一：
   - 如果 PMD 是密码 PMD，将筛选文件应用于 PMD。
   - 如果 PMD 不是密码 PMD，删除 PMD。

注意：也可以使用 policydeploy 实用程序执行迁移任务。

更多信息：

如何迁移到高级策略管理 (p. 61)

如何创建和分配策略

在从 PMD 环境迁移到高级策略管理环境时，您使用 CA Access Control 通过 PMDB 中的规则创建策略，并将策略分配给 DMS 上的主机组。

以下过程说明了 CA Access Control 如何创建和分配策略：

1. CA Access Control 将 PMDB 中的规则导出到策略文件。

   注意：您可以指定 CA Access Control 仅导出用于修改特定类中的资源的规则。

2. CA Access Control 将每个创建新资源或访问者的规则更改为修改资源或访问者的规则。 例如：CA Access Control 将所有 newres 规则更改为 editres 规则。

   此步骤可防止在您多次将创建新资源或访问者的规则部署到相同端点时导致的部署错误。

3. CA Access Control 在 DMS 上创建与 PMD 对应的主机组（GHNODE 对象）。

4. 对于 PMDB 中列出的每个端点订户，CA Access Control 会检查 DMS 中是否已创建了对应的主机（HNODE 对象）。

   - 对于 PMDB 中列出的、且在 DMS 中拥有对应主机的每个订户，CA Access Control 会将主机加入到步骤 3 中创建的主机组。
   - 对于 PMDB 中列出的、但在 DMS 中没有对应主机的每个订户，CA Access Control 会创建与端点对应的主机，并将主机加入到步骤 3 中创建的主机组。

   注意：CA Access Control 不会创建与订户 PMDB 对应的主机。

5. CA Access Control 使用导出的策略文件中的规则，在 DMS 中创建 POLICY 对象。

   注意：CA Access Control 不会为 POLICY 对象创建取消部署脚本。

6. CA Access Control 将 POLICY 对象分配给在步骤 3 中创建的主机组。

更多信息：

迁移 PMDB (p. 63)

最初如何将策略发送到迁移端点

在从 PMD 环境迁移到高级策略管理环境时，CA Access Control 会利用 PMDB 中的规则创建策略，并将它们发送到迁移端点。 了解 CA Access Control 最初如何将策略发送到迁移端点可能有助于对迁移过程中出现的任何错误进行故障排除。

以下过程说明了在端点上启动 CA Access Control 后，最初如何将策略发送到迁移端点。

1. CA Access Control 将启动并调用 policyfetcher，此操作会将心跳通知发送到 DMS。
2. DMS 接收检测信号通知并检查 DMS 上是否存在对应主机 (HNODE) 对象。
3. 会出现以下情况之一：
   - 如果 DMS 上存在对应主机，该主机将成为与迁移的 PMD 对应的主机组的一部分：
     a. CA Access Control 关联端点和主机。
     b. CA Access Control 将分配给主机组的策略部署到端点。
   - 如果 DMS 上不存在对应主机：
     a. CA Access Control 创建主机。
     b. 在您创建和分配策略时，CA Access Control 将主机加入与迁移的 PMD 对应的主机组中。
     c. CA Access Control 将分配给主机组的策略部署到端点。
4. CA Access Control 会将策略中列出的每个资源的“更新时间”属性修改为部署策略的时间。

   注意：由于 CA Access Control 已将创建对象的命令更改为修改对象的命令，您应该不会看到策略的任何部署错误。

注意：有关策略和主机组的详细信息，请参阅 *《企业管理指南》*。

CA Access Control 如何将筛选文件应用于密码 PMD

高级策略管理不支持使用密码管理命令的策略。 使用密码 PMD 在各端点之间同步密码以及分发密码管理规则。 在将密码 PMD 迁移到高级策略管理环境时，需要将筛选文件应用于密码 PMD，以便其仅将密码规则部署到其订户。

以下过程说明了 CA Access Control 如何将筛选文件应用于密码 PMD：

1. CA Access Control 创建名为 filter.flt 的文本文件并在其中添加以下行：

```
#-------------------------------------------------------------------------
------
# access    env     class   objects properties              pass/nopass
#-------------------------------------------------------------------------
------
  *         *       USER    *       OLD_PASSWD;CLR_PASSWD   PASS
  *         *       *       *       *                       NOPASS
#-------------------------------------------------------------------------
------
```

2. CA Access Control 将 filter.flt 保存在密码 PMD 目录中。
3. CA Access Control 将 filter.flt 的完整路径添加到下列位置中的 filter 配置设置中：
   - UNIX) pmd.ini 文件的 [pmd] 部分
   - (Windows) 以下注册表键：

     HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\AccessControl\Pmd*PMDB_Name*

如何迁移到高级策略管理

通过迁移到高级策略管理环境，您可以部署和取消部署策略，以及查看策略的部署和偏差状态。

注意：高级策略管理不支持使用密码管理命令的策略。 必须使用密码 PMD 同步端点之间的密码以及分发密码管理规则。 不能将密码 PMD 迁移到高级策略管理环境。

在开始迁移过程之前，验证：

- 所有订户都可用
- 订户已经从 PMDB 接收到所有更新
- 没有订户与 PMDB 同步

重要说明！ 强烈建议在开始迁移过程之前备份 PMDB。

要从 PMD 环境迁移到高级策略管理环境，请执行以下操作：

1. 安装企业管理服务器组件。

   高级策略管理环境的设置是企业管理安装过程的一部分。
2. 将 PMD 主机升级到 CA Access Control r12.5 或更高版本。
3. 迁移端点 (p. 62)。
4. 迁移 PMDB (p. 63)。

更多信息：

迁移过程的工作原理 (p. 58)

迁移端点

迁移端点是从 PMD 环境迁移到高级策略管理环境这一过程的第三步。在之前的步骤中，您已经：

- 安装了企业管理服务器组件
- 将 PMD 主机升级到了 CA Access Control r12.5 或更高版本

在此步骤中，请迁移订阅迁移的 PMDB 的端点。

迁移端点

1. 将端点升级到 CA Access Control r12.0 或更高版本。
2. 在端点上运行以下命令以配置高级策略管理客户端组件：

   ```
   dmsmgr -config -endpoint
   dmsmgr -config -dh dh_name@host_name
   ```

   端点升级到高级策略管理环境。

迁移 PMDB

在迁移 PMDB 之前，建议您先了解在整个迁移过程的每个阶段中必须执行的步骤。 迁移 PMDB 只是将 CA Access Control 的企业部署迁移到高级策略管理环境这一过程中的一个步骤。

迁移 PMDB 是从 PMD 环境迁移到高级策略管理环境这一过程的最后一步。 在之前的步骤中，您已经：

- 安装了企业管理服务器
- 将 PMD 主机升级到了 CA Access Control r12.5 或更高版本
- 迁移了端点（将端点升级到了 CA Access Control r12.0 或更高版本，并配置了高级策略管理客户端组件）

在此步骤中，使用 CA Access Control 企业管理 从 PMDB 中的规则创建策略，为迁移的 PMDB 创建主机组，并将与 PMDB 订户相对应的主机加入到该主机组。 还可以选择将新策略分配给该主机组。

重要说明！ 每次单击“下一步”按钮时，CA Access Control 企业管理 都会完成 DMS 或 PMDB 中的某个操作。 撤消这些操作的结果可能很困难。

迁移 PMDB

1. 在 CA Access Control 企业管理 中，单击“策略管理”选项卡，单击“策略”子选项卡，展开策略树，然后单击“PMDB 迁移”。

   将显示“PMDB 主机登录”页面。

2. 键入有权访问 PMDB 的用户名和密码以及要迁移的 PMDB 的名称，然后单击“登录”。

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

   此时，“PMDB 迁移过程”页面将显示在“常规”任务阶段中。

3. 填写以下字段，然后单击“下一步”。

   名称

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

   说明

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

策略类

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

导出依存类

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

将显示“策略脚本”任务阶段。

4. 检查导出的规则，并根据需要进行修改，然后单击“下一步”。

CA Access Control 企业管理 将从这些规则创建策略。 将显示“主机组”任务阶段。

5. 按如下方式填写该对话框，然后单击“下一步”：

主机组

指定要添加主机的主机组的名称。 可以指定现有主机组，或创建新的主机组。

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

分配策略

（可选）指定将策略分配给主机组。

分配的主机

指定要添加到主机组的主机。

注意：默认情况下，此表包含您有权访问的迁移 PMDB 的所有订户。 您可以在“分配的主机”列表中添加和删除主机；但是，如果您无权访问某主机，则无法将该主机添加到主机组中。

CA Access Control 企业管理 会将这些主机添加到主机组中，如果已指定，还会将策略分配给主机组。 “PMD 选项”任务阶段随即出现。

6. 选择要应用到迁移 PMDB 的以下任何选项：

取消订阅在第 3 步（“主机组”步骤)中指定的主机

指定从迁移的 PMDB 取消订阅在前一个任务阶段中选择的端点。

取消订阅所有 PMDB 订户

指定取消订阅迁移的 PMDB 的所有订户。

删除 PMD

指定删除迁移的 PMDB。

重要说明！ 如果您使用 PMDB 来传播用户密码命令，请不要删除它。

添加 PMD 筛选文件

指定将筛选文件添加到迁移的 PMDB 中，以便 PMDB 只将用户密码命令传播到其订户。 如果您选择该选项，迁移的 PMDB 会成为密码 PMDB。

7. 单击“下一步”。

CA Access Control 将执行您指定的操作。 将显示“迁移操作摘要”任务阶段，迁移过程随即完成。

更多信息：

如何创建和分配策略 (p. 59)

类依存关系

从 PMDB 导出指定类的规则时，可以选择还同时导出依存类的规则。 如果指定 CA Access Control 应该导出依存类，CA Access Control 将导出以下内容：

- 如果您导出修改特定类中资源的规则，并且该类具有相应的资源组，则 CA Access Control 还会导出修改该资源组中资源的规则。

  例如：如果指定导出 FILE 类规则，CA Access Control 将导出修改 FILE 和 GFILE 类中资源的规则。

- 如果您导出修改特定资源组中资源的规则，则 CA Access Control 还会导出修改资源组的成员资源的规则。

  例如：如果指定导出 GFILE 类规则，CA Access Control 将导出修改 GFILE 和 FILE 类中资源的规则。

- 如果您导出修改特定类中资源的规则，并且该类具有 PACL，则 CA Access Control 还会导出修改 PROGRAM 类中资源的规则。

- 如果您导出修改特定类中资源的规则，并且该类具有 CALACL，则 CA Access Control 还会导出修改 CALENDAR 类中资源的规则。
- 如果您导出修改特定类中资源的规则，并且该类中的其中一个资源是 CONTAINER 资源组的成员，则 CA Access Control 会导出修改 CONTAINER 类中资源的规则，并导出修改作为每个 CONTAINER 资源组成员的资源的规则。

  例如：如果指定导出 CONTAINER 类规则，并且 CONTAINER 对象包含 FILE 对象，CA Access Control 将导出修改 CONTAINER 和 FILE 类中资源的规则。

DMS 中显示重复的 HNODE

症状：

在将 PMD 迁移到高级策略管理环境后，DMS 中创建了两个代表同一端点的 HNODE。

解决方案：

端点的完全限定主机名在 DMS 与端点上有所不同。 要修复此问题，请删除 DMS 中的其中一个 HNODE 对象。

注意：有关 HNODE 对象和 DMS 的详细信息，请参阅*《企业管理指南》*。

迁移层级 PMDB

高级策略管理不支持层级主机组。 如果您的 PMD 体系结构包含层级 PMDB，必须在迁移过程中扁平化 PMD 层级结构。

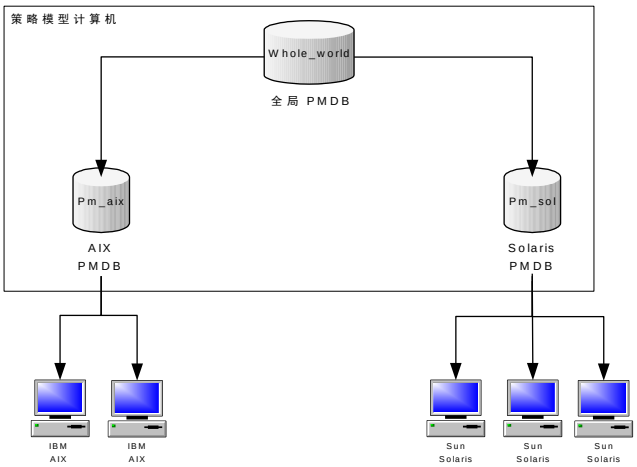
扁平化 PMD 层级结构时，您分别迁移每个 PMDB。 在迁移过程中，CA Access Control 会为层级环境中的每个 PMDB 创建主机组，并将每个端点添加到与所订阅到的 PMDB 对应的所有主机组。

迁移层级 PMDB

1. 迁移主 PMDB。
2. 迁移每个订户 PMDB。

示例：迁移层级 PMDB

下图展示了具有层级 PMDB 的 PMD 环境示例。



在此示例中，名为 pm_aix 和 pm_solaris 的 PMDB 是名为 whole_world 的 PMDB 的订户。 所有 IBM AIX 端点均为 pm_aix 的订户。 所有 Sun Solaris 端点均为 pm_sol 的订户。 实际上，所有端点均为 whole_world 的订户。

在将此 PMD 环境迁移到高级策略管理环境时，请执行以下操作：

1. 迁移 whole_world PMDB。

   CA Access Control 将创建 whole_world 主机组。 所有端点均为此主机组的成员。

2. 迁移订户 PMDB：

   - 迁移 pm_aix PMDB。

     CA Access Control 将创建 pm_aix 主机组。 IBM AIX 端点是该主机组的成员。

   - 迁移 pm_sol PMDB。

     CA Access Control 将创建 pm_sol 主机组。 Sun Solaris 端点是此主机组的成员。

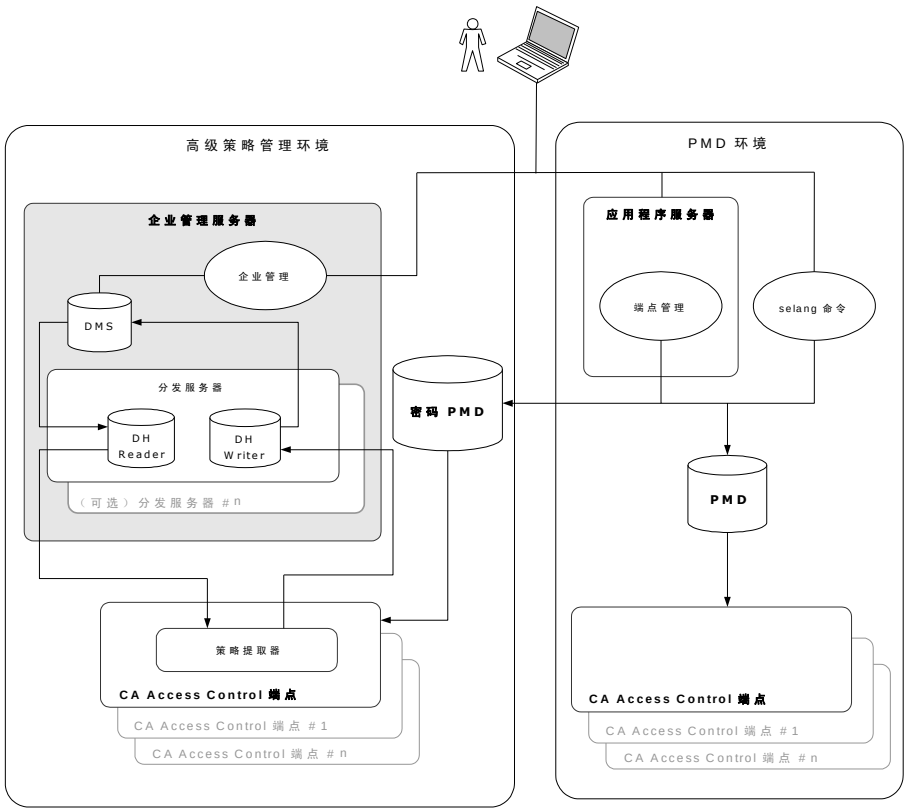
注意：在 PMD 环境中，如果将筛选文件应用到 pm_aix PMDB，该筛选文件可能会阻止从 whole_world PMDB 部署的规则到达 IBM AIX 端点。 在高级策略管理环境中，IBM AIX 端点是 whole_world 主机组的成员。 所有部署到 whole_world 主机组的规则将部署到所有端点而不会经过筛选。 在高级策略管理环境中部署规则时，您应当注意这一更改的行为。

混合策略管理环境

混合策略管理环境是一种 CA Access Control 部署，其中某些端点订阅了 PMD 而某些端点是在高级策略管理环境中定义的。

以下图表展示了混合策略管理环境中的 CA Access Control 部署示例。

注意：尽管端点未显示在图表中，但端点可以订阅 PMD 也可以在高级策略管理环境中定义。 例如：您可以将策略部署到高级策略管理环境中的端点，也可以将 selang 规则从 PMD 传播到同一端点。



更新混合策略管理环境中的端点

更新混合策略管理环境中的端点时，您需要在每个环境中分别更新端点。

注意：端点无法接受对后期 CA Access Control 版本中引入的类进行修改的规则。 例如：即使您从 r12.5 PMD 或 DMS 部署规则，r8 端点也只能接受更改 r8 功能的规则。

更新混合策略管理环境中的端点

1. 使用要部署到端点的 selang 部署命令创建脚本文件。

2. 在 CA Access Control 企业管理 中，执行以下操作：
   a. 在 DMS 上存储策略版本。
   b. 将已存储的策略版本分配到您要更新的主机组。

   CA Access Control 会将策略部署到主机组中的端点。
3. 使用脚本文件中的 selang 命令更新 PMDB。

   PMDB 会将命令传播到其端点。

注意：有关如何存储和分配策略版本的详细信息，请参阅*《企业管理指南》*。有关如何更新 PMDB 的详细信息，请参阅适用于您的操作系统的*《端点管理指南》*。