CA Access Control for Virtual Environments

产品指南

r2.0

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 企业版
- CA Access Control
- CA User Activity Reporting Module
- Identity Manager

文档约定

CA Access Control 文档使用以下约定：

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

文档在解释命令语法和用户输入（以等宽字体显示）时还会使用以下特殊约定：

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

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

示例：命令表示法约定

下面的代码说明了在本指南中使用命令约定的方式：

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

在该示例中：

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

文件位置约定

CA Access Control 文档使用以下文件位置约定：

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

联系技术支持

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

目录

第 1 章： 简介

此部分包含以下主题：

关于本指南

该指南提供如何在 VMware vCenter 环境中计划、部署、配置和管理 CA Access Control for Virtual Environments 的相关信息。

该指南针对在其组织中负责管理和保护基于 VMware 的虚拟化环境的系统、安全以及 VMware 管理员而写。

请您在开始部署和配置所在环境中的 CA Access Control for Virtual Environments 之前查阅该指南。

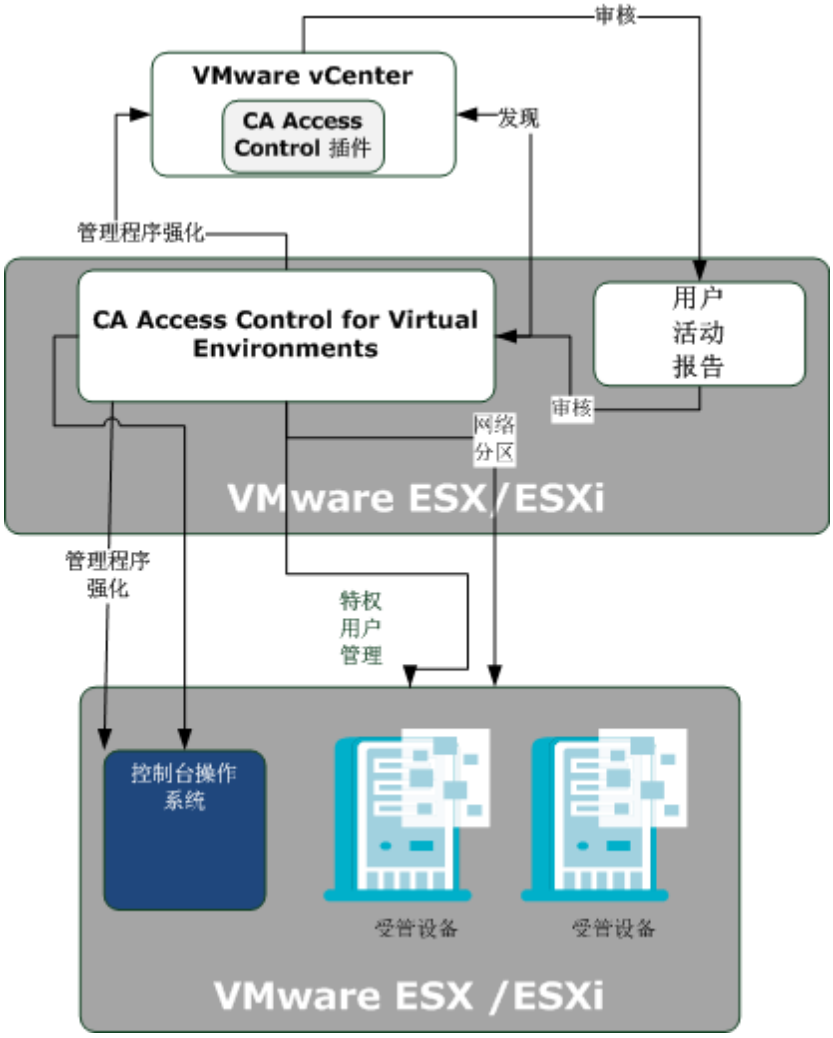
为了简化术语，在本指南中我们将此产品称为 CA Access Control。

关于 CA Access Control for Virtual Environments

CA Access Control for Virtual Environments (CA VE) 是独立的解决方案，保护特权用户访问在您的虚拟环境扩展时可以调节的虚拟环境。 CA Access Control for Virtual Environments 与 VMware vCenter 集成来提供管理接口，通过管理接口，您可以控制受管的设备、安全组、网络区域和策略。 通过使用标记、标记规则和策略，CA Access Control for Virtual Environments 可以帮助您通过自动化大量管理任务来管理虚拟环境。

CA Access Control for Virtual Environments 环境体系结构

下图显示 CA Access Control for Virtual Environments 环境体系结构：

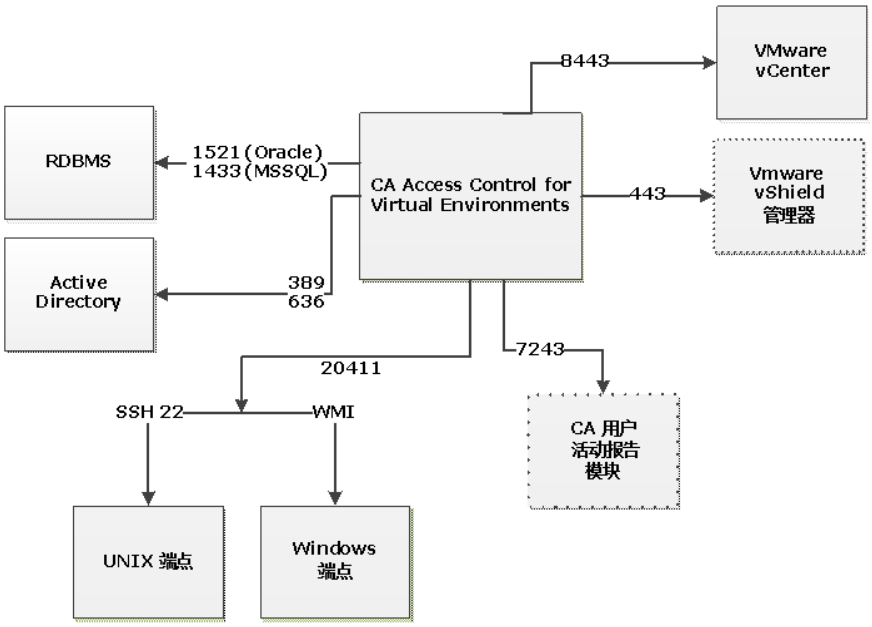


如以前的图表所示，CA Access Control for Virtual Environments 负责以下内容：

- 在虚拟环境的受管设备上的特权用户密码管理
- VMware ESX/ESXi 服务器上的管理程序强化
- 网络分区
- 来自 CA User Activity Reporting Module 报告生成的受管设备的审核事件收集

CA Access Control for Virtual Environments 网络协议和端口

下图显示 CA Access Control for Virtual Environments 使用的网络协议和端口：



注意：虚线表示可选组件

保护的对象是什么？

CA Access Control for Virtual Environments 保护和增强以下实体：

- **管理程序** -- CA Access Control for Virtual Environments 支持几个强化级别。 强化策略可以限制用户登录到 VMware vCenter 服务器，控件远程审核收集、远程管理和 SNMP 陷阱收集。
- **受管设备** -- CA Access Control for Virtual Environments 通过让您部署密码锁定策略来管理特权帐户密码的方法保护受管设备。 您也可以将受管设备分配给网络区域，并通过审核收集策略收集审核记录。

特权帐户密码管理

CA Access Control for Virtual Environments 在环境的受管设备上发现特权帐户密码，并将密码存储在数据库中。 CA Access Control for Virtual Environments 提供特权帐户和应用程序 ID 密码的安全存储，并基于您定义的策略控制对特权帐户和密码的访问。

网络流量隔离

通过将受管设备分配给*安全组*，CA Access Control for Virtual Environments 控制网络流量和访问。 安全组是对组成员实施安全控制的受管设备的逻辑组。 安全组的每个成员可以与网络区域内的所有其他成员通讯。

CA Access Control for Virtual Environments 与 VMware vShield 管理器集成，以便使用本地防火墙功能实施网络访问规则。

虚拟环境工具和接口增强

CA Access Control for Virtual Environments 增强本地 VMware 虚拟管理工具。 CA Access Control for Virtual Environments 通过增加特权密码管理功能，插入到充实本地环境的 VMware vSphere 客户端中。

而且，CA Access Control for Virtual Environments 与 VMWare vShield 应用程序集成来实施网络访问规则。 VMware vShield 管理器是实施访问控制策略的 vNIC 级别防火墙。

资产标记

资产标记允许您将逻辑标记分配给受管设备和安全组。 在分配标记时，受管设备成为标记适用于的安全组成员。

您可以手动将标记分配给受管设备，并将设备添加到安全组中。 根据您已分配给受管设备的标记，可以定义标记规则和设置规则条件，以便将受管设备与安全组关联。

第 2 章： 准备实施

此部分包含以下主题：

调整您的实施规模

在实施 CA Access Control for Virtual Environments 之前，请确定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。

下表描述 CA Access Control for Virtual Environments 支持的配置：

组件	限制
每台主机的虚拟机	320
每个 vCenter 服务器的主机	3200
每台 vCenter 服务器注册虚拟机	15000
每个数据中心的虚拟机	5000
每个 vCenter 服务器打开的虚拟机	10000

CA Access Control for Virtual Environments 的组件

CA Access Control for Virtual Environments 包括以下软件组件：

CA Access Control 服务器

CA Access Control 服务器作为 CA Access Control for Virtual Environments 部署的一部分安装，并驻留在 VMware ESX/ESXi 服务器上。 CA Access Control 服务器管理以下项目：

- 网络流量管理
- 网络区域管理
- 特权帐户密码管理
- 管理程序强化

CA Access Control 企业管理

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

“企业管理”允许您进行下列操作：

- 查看整个企业的 CA Access Control for Virtual Environments 的实施
- 配置主机和主机组，并将策略分配给安全组和 PUPM 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
- 管理标记和标记规则
- 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*。

CA Access Control 插件

CA Access Control 插件帮助管理虚拟环境。 插件被嵌入到 VMware vCenter 服务器中，通过它您可以从 VMware vSphere 客户端执行以下操作：

- 发现 PUPM 端点和特权密码
- 管理特权帐户密码
- 将标记分配给受管设备
- 显示 CA User Activity Reporting Module 报告

中央 RDBMS

中央 RDBMS 存储以下内容：

- 用于报告的端点数据
- 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 用作用户存储）

用户存储

您可以配置 CA Access Control for Virtual Environments 使用在 Active Directory 或数据库中定义的组和用户。 因此，您可以为所有用户使用单个数据存储。

第 3 章： 实施 CA Access Control for Virtual Environments

此部分包含以下主题：

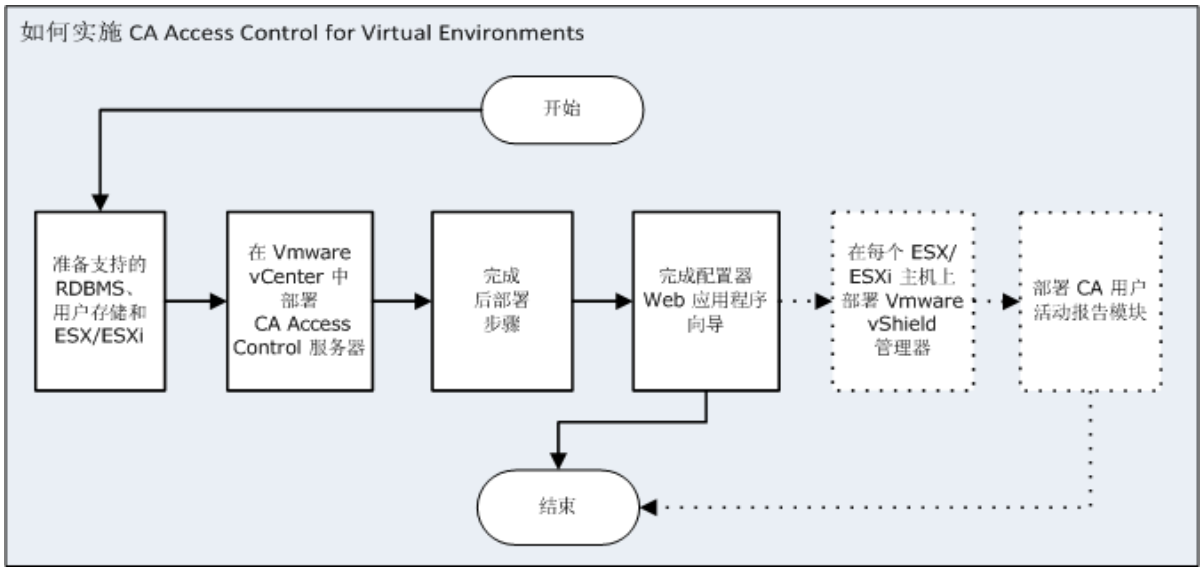
关于 CA Access Control for Virtual Environments 虚拟设备

将 CA Access Control for Virtual Environments 分发为虚拟的设备。 *虚拟设备*是带有预装和预配置的操作系统和应用程序包的虚拟机。

如何实施 CA Access Control for Virtual Environments

通过 CA Access Control for Virtual Environments，您可以管理特权帐户、配置网络分区、管理特权帐户、写入管理程序和审核收集策略，并将标记分配给资产。

下图说明如何实施 CA Access Control for Virtual Environments：



请注意下列事项：

- 有关支持的 RDBMS 和用户存储的信息，请参阅《*版本说明*》。
- 点线表示可选的步骤。

部署 CA Access Control 服务器

部署 CA Access Control for Virtual Environments 虚拟设备，请安装操作系统、CA Access Control 服务器，并在 ESX/ESXi 服务器中创建虚拟机。

完成以下步骤：

1. 打开 VMware vSphere 客户端，转到“文件”，“部署 OVF 模板”。

   “部署 OVF 模板”向导将打开。

2. 从“文件”按钮单击“部署”，然后单击“浏览”并找到“CA Access Control for Virtual Environments OVF 模板”。

3. 单击“下一步”。

   “OVF 模板”详细信息屏幕出现。 请执行以下操作：

   a. 查看详细信息并单击“下一步”继续。

      此时会出现“最终用户许可协议”屏幕。

   b. 查看许可协议，选择“接受”，然后单击“下一步”。

      “名称和位置”屏幕出现。

   c. 指定虚拟机名称，并选择您想部署虚拟设备的文件夹。 单击“下一步”。

      “主机/群集”屏幕打开。

      注意：在您开始部署 OVF 模板之前，该屏幕只有在您未选择资源池时才出现。

   d. 选择数据中心来承载虚拟设备。 单击“下一步”。

      “资源池”屏幕打开。

   e. 选择您要将模板部署到的资源池。 单击“下一步”。

      此时会打开“数据存储”屏幕。

   f. 选择将存储虚拟设备的数据存储。 单击“下一步”。

      “网络映射”屏幕打开。

g. 选择要使用的网络。 单击“下一步”。

注意：您可以映射环境中定义的网络所使用的 OVF 模板的网络。

“网络属性”屏幕出现。

h. 填写以下字段：

域名

指定主机名查找的搜索路径。 您可以指定多个搜索路径。

主机名

指定虚拟机的完全限定名称

时区

指定 CA Access Control 服务器所在的时区

默认网关

指定默认网关 IP 地址 如果使用 DHCP，则该字段留为空。

DNS

指定该虚拟机的 DNS 服务器。 如果使用 DHCP，则该字段留为空。

网络 IP 地址

指定虚拟机 IP 地址。 如果使用 DHCP，则该字段留为空。

网络子网掩码

为您选择的网卡指定子网掩码或前缀。如果使用 DHCP，则该字段留为空。

i. 单击“下一步”。

j. 查看部署设置，然后单击“完成”。

VMware vSphere 客户端部署模板，并在您指定的位置添加虚拟机。该过程需要花费几分钟才能完成。 此时会出现消息，表示已成功部署模板。

4. 打开来自 VMware vSphere 客户端的 CA Access Control for Virtual Environments 计算机。

CA Access Control for Virtual Environments 安装过程将开始。 这可能需要几分钟时间才能完成。

5. 转到“控制台”选项卡。
6. 定义根的密码和超级管理员用户帐户。

   请注意下列事项：

   - 在默认情况下，会阻止远程根登录。 您仅可以使用根帐户来登录 CA Access Control for Virtual Environments 计算机控制台。
   - 您可以使用超级管理员用户帐户来远程管理虚拟机。 例如，使用 SSH。
   - 默认情况下，将分配给超级管理员用户与根帐户相同的密码。 运行来自 CA Access Control for Virtual Environments 控制台的 passwd superadminuser 命令，以便更改默认密码。
7. （可选）如果不自动检测，则定义网络设置和主机名。 输入 N 更改设置或输入 Y 接受设置
8. 输入 Y 完成安装。

   最终确定 CA Access Control for Virtual Environments 安装。 该过程需要花费几分钟才能完成。
9. 输入 root 用户帐户密码登录到 CA Access Control for Virtual Environments。

   您已成功部署 CA Access Control for Virtual Environments。 现在您需要完成后部署任务。

后部署任务

部署环境中的 CA Access Control for Virtual Environments 虚拟设备之后，完成以下步骤来配置用户存储和数据库连接信息。

如何准备中央数据库

CA Access Control for Virtual Environments 需要关系数据库管理系统 (RDBMS)。 在配置 CA Access Control for Virtual Environments 之前，您必须准备数据库：

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。

   在安装 RDBMS 之前请注意以下内容：

   - 有关受支持的 RDBMS 软件列表，请参阅《版本说明》。
   - 您不必在 CA Access Control for Virtual Environments 虚拟机上安装中央数据库。 有关 RDBMS 系统要求的信息，请参阅产品文档。

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 SQL Server，请执行下列操作：
     - 创建新的*不区分*大小写的数据库。
     - 将排列顺序设置为 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
   - 对于 Oracle，请执行下列操作：
     - 为中央数据库创建新用户并分配以下权限：

       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）

     - 使用下列查询，在 CA Access Control for Virtual Environments 数据库中授予用户其他权限：

       将 adminiser 数据库触发器授予 <*DB_USER*> ；

     - 设置托管 CA Access Control for Virtual Environments 的表空间上的无限制配额。

配置数据库连接信息

CA Access Control for Virtual Environments 需要关系数据库管理系统 (RDBMS)。

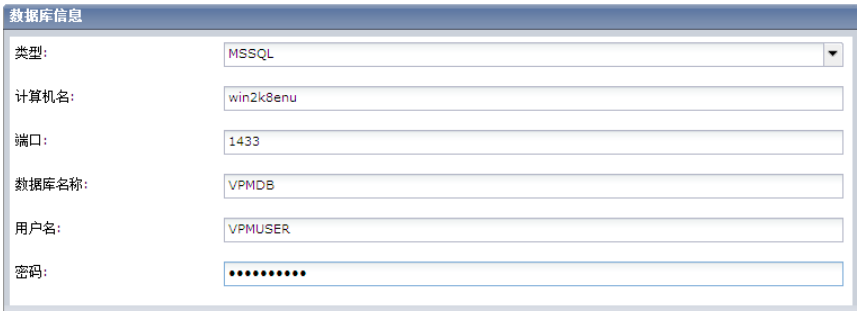
完成以下步骤：

1. 为您的主机打开 Web 浏览器并输入以下 URL：

   `https://enterprise_host:18443/iam/ac`

   示例：https://192.168.1.1:18443/iam/ac

   CA 虚拟设备配置向导出现，显示数据库信息表：



2. 填写以下字段：

   数据库类型－指定支持的 RDBMS。

   计算机名－指定安装 RDBMS 的主机名称。

   端口号－定义 RDBMS 所使用的端口。

   - **Oracle**－1521
   - **SQL**－1433

   数据库名－定义创建的数据库的名称。

   用户名－定义 CA Access Control for Virtual Environments 用来连接到数据库的用户名。 指定在您准备数据库时创建的用户名。

3. 单击“下一步”。

   此时出现“服务器名称配置”屏幕。

4. 定义企业管理服务器的完全限定名。

5. 单击“下一步”。

   安装程序先检查数据库的连接，然后再继续。 现在配置用户存储连接信息。

配置用户存储连接信息

CA Access Control for Virtual Environments 支持 Active Directory 和先前指定为用户存储的数据库。

完成以下步骤：

1. 从“CA 虚拟设备配置”屏幕，选择用户存储类型。

选择以下选项之一：

Active Directory－您指定连接信息详细信息

数据库－将用户信息存储在 RDBMS 中

2. (Active Directory) 完全以下字段：

用户

定义用于管理 CA Access Control for Virtual Environments 的 Active Directory 用户帐户名。

注意：您可以针对此参数定义具有只读权限的用户。

密码

定义用于管理 CA Access Control for Virtual Environments 的 Active Directory 用户帐户的密码。

域名

定义 Active Directory DNS 域名。

使用加密连接

指定使用与 Active Directory 的加密连接

端口

定义默认情况下用于对 Active Directory 进行 LDAP 查询的端口，例如：636。

搜索根

定义搜索根，例如，ou=DomainName，DC=com。

注意：设置搜索根，至少目录树中的一个节点高于定义用户所在的容器。否则，CA Access Control for Virtual Environments 可以在没有显示任何选项卡的情况下启动。

域控制器地址

定义域控制器 IP 地址。

安装程序会先检查与 Active Directory 的连接，然后再继续。

3. （数据库）定义在准备数据库时创建的用户的 RDBMS 密码。
4. 单击“下一步”。

   将打开“系统用户”屏幕。
5. 填写以下字段：

   系统用户

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

   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 for Virtual Environments 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》*。

   密码

   （仅针对数据库）定义*超级管理员*（CA Access Control for Virtual Environments 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 for Virtual Environments。

   注意：您可通过此步骤在数据库中创建超级管理员用户。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 for Virtual Environments 时便是以超级管理员身份登录。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》*。
6. 单击“下一步”。

   您已经定义数据库和用户存储连接信息。配置到 VMware vCenter 的连接。

配置到 VMware vCenter 服务器的连接

配置与 VMware vCenter 的连接，以便将 CA Access Control 安全功能与 VMware vCenter 服务器的受管设备集成。

完成以下步骤：

1. 从 CA 虚拟设备配置向导，移到 vCenter 连接配置。

   此时显示以下屏幕：

   填充该对话框中的字段：

   名称

   定义要用于 VMware vCenter 连接的名称。

   说明

   （可选）定义该 VMware vCenter 连接的说明。

   服务器名称

   定义要管理 VMware vCenter 服务器的 DNS 名称

   示例： vcenter.company.com

   用户名

   定义具有 VMware vCenter 服务器管理权限的用户帐户的名称

   密码

   定义具有 VMware vCenter 服务器管理权限的用户帐户的密码

2. 单击“下一步”。

   CA Access Control for Virtual Environments 验证设置并继续到共享秘钥屏幕。

3. 填写以下字段：

   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。 单击“下一步”。

   此时出现“服务器名称配置”屏幕。

4. 定义企业管理服务器的完全限定名。 单击“下一步”。

   将打开摘要屏幕。

5. 查看信息并单击“完成”以完成向导。

   CA Access Control for Virtual Environments 配置数据库和用户存储以便使用。

   CA Access Control for Virtual Environments 使用您指定的信息尝试连接到 VMware vCenter 服务器。 如果信息正确，将设置连接，此时您即可使用 VMware vSphere 客户端来管理 CA Access Control for Virtual Environments 的企业部署。 如果信息不正确，且 CA Access Control for Virtual Environments 无法连接到 VMware vCenter，则会出现错误消息。 消息说明无法建立连接的原因。

如何配置 CA Access Control for Virtual Environments 进行 SSL 通讯

默认情况下，CA Access Control for Virtual Environments 安装有使用自签名证书的 SSL 支持。 要使用不同证书配置 SSL 支持，请配置 CA Access Control for Virtual Environments 在与 Active Directory 一起使用时使用 SSL。

完成以下步骤：

1. 获取 DER、CRT 或 CERT 格式的用户目录证书。
2. 将证书导入 keystore。

更多信息：

将用户目录证书添加到 Keystore (p. 27)

将用户目录证书添加到 Keystore

在将 CA Access Control for Virtual Environments 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！ 该示例介绍了如何配置 CA Access Control for Virtual Environments，以便使用 SSL 进行与 Active Directory 的安全通讯。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. 在 CA Access Control 服务器上，如果 JBoss 正在运行，则停止它。请执行以下操作：
   - 从 JBoss 作业窗口中断 (Ctrl+C) 进程。
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/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。

   您已经将用户存储证书添加到 keystore 中。

第 4 章： 管理 CA Access Control for Virtual Environments

此部分包含以下主题：

打开 CA Access Control for Virtual Environments

一旦安装和启动 CA Access Control 服务器，您就可以为 CA Access Control for Virtual Environments 使用 URL 从远程计算机启动基于 Web 的接口。

遵循这些步骤:

1. 在您的主机中打开 Web 浏览器并输入以下 URL：

   `https://enterprise_host:18443/iam/ac`

2. 使用您在安装 CA Access Control 服务器时指定的凭据登录。

   将显示 CA Access Control for Virtual Environments 主页。

示例：打开 CA Access Control for Virtual Environments

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 for Virtual Environments：

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

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

全局查看

通过 CA Access Control for Virtual Environments 中的“全局查看”，可查看您管理的 CA Access Control for Virtual Environments 的企业实施。

使用“全局查看”，可以执行以下操作：

- 识别受管设备和由 CA Access Control for Virtual Environments 管理的安全组
- 导航 VMware vCenter 层次结构
- 查看有关受管设备和安全组的详细信息。 详细信息包括部署哪些策略、组和受管设备的总数以及每台设备的遵从性状态
- 管理受管设备或安全组
- 管理安全组来分配或删除策略、成员、标记和标记规则。

管理企业实施

使用 CA Access Control 企业管理，可以查看和管理 CA Access Control for Virtual Environments 的企业实施。 企业“全局查看”是 PUPM 端点和受管设备、其逻辑安全性组、部署的策略以及策略标记的快照。

企业部署快照基于您在 VMware vCenter 服务器中配置的受管设备和组层次结构。 对 VMware vCenter 中的层次结构所做的任何更改也会显示在“全局查看”中。

完成以下步骤：

1. 依次转到“全局查看”选项卡、“安全组”、“安全组管理”

   此时出现“安全组管理”页面，显示 VMware vCenter 服务器上的安全组以及由 CA Access Control 服务器定义的逻辑组。

   注意：您可以仅针对 CA Access Control for Virtual Environments 受管设备配置、修改或更改层次结构。

2. （可选）您可以定义其他受管设备、安全组、 标记以及 CA Access Control 服务器中的标记规则。 从“操作”菜单选择以下操作：

   - 创建安全组 (p. 32)
   - 创建标记 (p. 41)
   - 创建标记规则 (p. 41)
   - 查看策略状态

3. 从“安全组”部分中选择一个安全组。

   CA Access Control 企业管理 显示安全组详细信息、分配的策略、组成员和每个成员的遵从性状态。

4. 选择“添加策略”来管理安全组策略。

   以下是可用的策略：

   - 网络区域 (p. 38) — 配置网络隔离策略
   - 审核收集 (p. 47) — 配置 CA User Activity Reporting Module 审核收集策略
   - 管理程序强化 (p. 44) — 配置管理程序强化策略
   - 密码锁定 (p. 35) — 配置特权帐户密码锁定策略

5. （可选）选择“配置”可修改现有策略，或选择“删除”可删除策略。

创建安全组

管理环境中的安全组，以便添加或删除成员，分配或删除标记。

完成以下步骤：

1. 依次转到“全局查看”选项卡、“安全组”、“安全组管理”

   此时出现“安全组管理”页面，显示 VMware vCenter 服务器上的安全组以及 CA Access Control 服务器详细信息。

2. 选择“创建”或“修改”以访问安全组配置

   此时打开“常规”选项卡。

3. 填写以下字段：

   名称

   显示安全组的名称

   说明

   指定安全组的说明。

   所有者

   指定安全组的所有者的名称

   组织单元

   指定安全组的部门单元

4. 选择“受管设备选择”选项卡

   此时打开“主机选择”选项卡。

5. 单击“添加”可将受管设备添加到该组

6. 选择“安全组成员”选项卡

   此时打开“组”选项卡，显示属于该组成员的安全组。

7. 单击“添加”可将安全组添加为该组的成员

8. 选择“标记”选项卡

   此时打开“标记”选项卡，显示分配的标记

9. 单击“添加”将标记分配给计算机组

10. 选择“成员资格(按标记)”选项卡

    此时打开“成员资格(按标记)”选项卡。

11. 单击“AND”将标记添加到成员资格条件中。 单击“添加”将标记添加到条件列表。

    成员资格条件即添加到该列表中。

    注意：您可以在单个成员资格条件中添加最多三 (3) 个标记

12. 单击“提交”

    CA Access Control 企业管理 将更改提交到安全组。

关于标记成员资格标准

要帮助您自动并方便管理受管设备，您可以使用标记成员资格标准。使用标记成员资格标准，您定义安全组，其成员符合所定义的标准规则。 CA Access Control for Virtual Environments 会自动添加标准规则应用于安全组的每个受管设备。

标记成员资格标准使用以下语法：

```
[tag1] AND | OR [tag2] AND | OR [tag3]
```

示例：创建标记成员资格标准

在此示例中，您配置标记成员资格标准，以便分配那些分配为以下标记之一的受管设备：Development、Accounting、Marketing。

```
Development OR Accounting OR Marketing
```

在此示例中，您配置标记成员资格标准，以便自动分配那些仅分配为 Accounts 和 Marketing 标记的受管设备。

```
Accounts AND Marketing
```

查看受管设备状态

通过状态视图，您可以查看与受管设备有关的错误和警告消息。 报警显示您分配给安全组的部署策略的相关信息。

完成以下步骤：

1. 依次选择“全局查看”、“视图”、“状态”

   此时打开“状态”窗口，显示最近的报警。

2. 选择查看全部消息，或仅查看错误和警告消息。
3. 单击“刷新”来刷新报警列表。

特权帐户密码管理

通过特权帐户密码锁定策略，您可以配置统一的策略并将其分配给安全组中所有的特权帐户。

CA Access Control for Virtual Environments 创建端点和帐户的方式

CA Access Control for Virtual Environments 自动创建 PUPM 端点、发现特权帐户并将密码策略分配给帐户密码。

以下过程说明了 CA Access Control for Virtual Environments 配置 PUPM 端点和帐户的方式：

1. 虚拟化管理员将 PUPM 端点添加到安全组。
2. 管理员在 CA Access Control 企业管理 中为安全组中的每个端点类型创建具有管理权限的断开连接的特权帐户。

   CA Access Control for Virtual Environments 使用断开连接的帐户连接到每个端点并发现特权帐户密码。
3. 在 CA Access Control 企业管理 中，管理员配置密码锁定策略并将其分配给安全组。
4. CA Access Control for Virtual Environments 发现端点且自动配置端点连接设置，并尝试配置该端点上的特权帐户。
5. 如果该操作成功，CA Access Control for Virtual Environments 会创建端点特权访问角色，以便使用该端点类型上的特权帐户。

   例如，您第一次在 Windows Agentless 端点上发现特权帐户时，CA Access Control for Virtual Environments 会自动创建 Windows Agentless 连接端点特权访问角色。
6. CA Access Control for Virtual Environments 自动将特权帐户密码策略分配给安全组的每个成员的特权帐户。

配置帐户密码锁定策略

为 CA Access Control for Virtual Environments 管理的每个安全组配置帐户密码锁定策略。 CA Access Control for Virtual Environments 在您添加到该组的每个受管设备上都实施特权密码锁定策略。

重要说明！ 在完成该步骤之前，为您想要 CA Access Control for Virtual Environments 创建和管理的每个端点类型都创建具有管理权限的特权帐户。

完成以下步骤：

1. 依次转到“全局查看”、“安全组”、“安全组管理”。

   此时出现“安全组管理”页面，显示 VMware vCenter 上的安全组以及 CA Access Control 服务器详细信息。

2. 选择安全组。

   CA Access Control 企业管理 显示安全组详细信息和成员。

3. 从“操作”菜单选择“添加帐户密码策略”。

   此时打开“管理密码锁定: *主机名*”窗口。

4. 从下拉菜单中选择操作系统配置文件。 选项：

   - Windows 计算机配置文件
   - Linux 计算机配置文件
   - Solaris 计算机配置文件

   您可以为每个操作系统配置文件配置特殊的密码锁定策略。

5. 填写以下字段：

说明

指定密码锁定策略的说明

操作系统配置文件

显示先前选择的操作系统配置文件

连接帐户

定义 CA Access Control for Virtual Environments 用来连接到每个受管设备的管理员用户帐户。 选择“创建帐户”来创建管理员帐户。

锁定连接帐户

指定连接帐户为已连接的帐户。

受管帐户

定义 CA Access Control for Virtual Environments 在每个受管设备上创建的特权帐户。

密码策略

指定要应用于特权帐户或服务帐户的密码策略。 选择“创建密码策略”来创建密码策略。

签出到期

定义签出帐号到期之前的持续时间（分钟）。

独占帐户

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

签出时更改密码

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

签入时更改密码

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

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

注意：该选项不适用于服务帐户。

登录应用程序

指定要分配给该端点的登录应用程序。

注意：需要先创建一个登录应用程序，之后才能将其分配给端点。 您可以为同一端点分配多个登录应用程序。

6. 单击“提交”。

CA Access Control 企业管理 将特权帐户密码锁定策略提交给该组。

网络隔离

网络隔离是一个过程，安全或虚拟化管理员通过该过程，根据通用标准，定义网络区域中受管设备的组，例如，主机的物理位置或标记。

网络区域中的成员仅可以与该区域内的其他成员进行通信，而无法访问网络上的其他网络区域或主机。 您可以将网络服务分配给安全组，以便让成员能够访问网络。

在 CA Access Control 企业管理 中配置网络区域策略

定义的网络隔离规则指定网络区域并应用于安全组。 应用时，成员仅可以在区域之内通信。 您可以定义安全组并将成员分配给这些组，或使用自动创建的安全组。

注意：请在配置网络区域策略之前定义要使用的网络服务。

完成以下步骤：

1. 依次转到“全局查看”、“安全组”、“安全组管理”。

   此时出现“安全组管理”页面，显示 VMware vCenter 上的安全组以及 CA Access Control 服务器详细信息。

2. 选择安全组。

   CA Access Control 企业管理 显示安全组详细信息和成员。

3. 在“操作”菜单中，选择“添加网络区域策略”。

   此时管理网络规则窗口打开。

4. 完成以下字段：

   说明

   指定网络区域策略的说明。

   服务

   定义网络服务以分配网络区域策略。 单击“添加”搜索要分配的网络服务。

   定向

   定义允许使用的网络服务的网络流量方向。

   选项：入站、出站、双向

5. 单击“提交”。

   CA Access Control 企业管理 提交网络隔离规则。 此时出现一条确认消息，通知您已成功完成任务。

   已成功将网络区域策略应用于安全组。

配置网络服务

为安全组配置网络服务，以便让网络区域中的成员可以访问位于网络区域外部的服务和资源。

完成以下步骤：

1. 在 CA Access Control 企业管理 中，执行如下操作：
   a. 单击“系统”
   b. 单击“网络服务”
   c. 选择“配置网络服务”

   此时打开“配置网络服务: 配置网络搜索”屏幕。
2. （可选）选择现有的网络服务来创建副本，如下：
   a. 选择“创建类型为‘网络服务’的对象”。
   b. 针对搜索选择属性，键入筛选器值，然后单击“搜索”。

      此时显示匹配筛选条件的网络服务的列表。
   c. 选择要用作新网络服务的基础的对象。
3. 单击“确定”。

   此时显示“创建网络服务”任务页面。 如果从现有对象创建了网络服务，则对话框字段中会预先填充来自现有对象的值。
4. 填写以下字段。 以下字段需加以说明：

   网络地址

   定义提供网络服务的服务器的主机名或 IP 地址。

   服务

   定义网络服务属性：

   - 协议－UDP、TCP
   - 端口号
   - 服务
5. 单击“添加”。

   CA Access Control 企业管理 即添加了网络服务。

   注意：您可以为每个安全组定义多个网络服务。
6. 单击“提交”

   CA Access Control 企业管理 提交任务，并将网络服务分配给安全组。

资产标记

资产标记是一个过程，系统、安全或虚拟化环境管理员通过该过程将标记与受管设备和安全组相关联。 通过分配标记，管理员可以将各个资产作为组进行管理以便自动化策略分发并定义管理范围。

要自动化管理，每个受管设备都会继承您添加到安全组的标记。 您可以基于资产属性（如 IP 地址范围）定义标记规则。 您也可以定义 CA Access Control for Virtual Environments 自动分发给组中所有成员的标记策略。

使用标记管理安全组的方式

使用标记和标记规则可以促进安全组的管理。 基于您定义的标记和标记规则，CA Access Control 企业管理 可自动将受管设备理添加到安全组并将策略应用于受管设备。

完成以下步骤：

1. 在 CA Access Control 企业管理 中创建标记。
2. 然后执行下列操作之 一：
   - 手动将标记分配给受管设备

     受管设备添加到安全组。 将分配给安全组的策略应用于受管设备。
   - 创建标记规则
3. 定义标记规则、将标记与您创建的规则关联并定义规则条件。
4. CA Access Control 企业管理 执行以下操作：
   a. 将规则应用于与标记关联的安全组
   b. 将标记分配给遵守标记规则的每个受管设备
   c. 将遵守标记规则的受管设备添加到安全组中
   d. 将为安全组配置的策略应用于受管设备

   现在您可以管理安全组的受管设备。

   注意：如果您删除标记规则，CA Access Control 企业管理 则从安全组删除受管设备

在 CA Access Control 企业管理 中配置标记

CA Access Control 企业管理 将受管设备（例如，文件夹、数据中心和资源池）映射到主机组。 将标记分配给安全组可简化您的虚拟化环境中的资产管理。 您可以根据分配的标记轻松确定管理范围。

完成以下步骤：

1. 依次转到“全局查看”、“标记”、“创建标记”。

   此时打开“创建标记: 标记搜索”窗口。

2. （可选）按如下方式选择一个现有标记来创建标记作为其副本：

   a. 选择“创建类型为‘标记’的新对象副本”。

   b. 针对搜索选择属性，键入筛选器值，然后单击“搜索”。

      此时显示匹配筛选条件的标记的列表。

   c. 选择要用作新标记基础的对象。

3. 单击“确定”。

   此时显示“创建标记”窗口。

4. 键入标记的名称。

5. 单击“提交”。

   CA Access Control 企业管理 创建标记。 现在您可以将标记分配给受管设备或创建标记规则。

在 CA Access Control 企业管理 中创建标记规则

创建标记规则，根据定义的属性，将受管设备分配到安全组。 当 CA Access Control for Virtual Environments 发现其具有的 IP 地址匹配标记规则的受管设备时，设备已标注并与安全组相关联。

完成以下步骤：

1. 依次转到“全局查看”、“标记”、“创建标记规则”。

   此时打开“创建标记规则: 标记规则搜索”窗口。

2. （可选）按如下方式选择一个现有标记规则来创建标记作为其副本：

   a. 选择“创建类型为‘标记规则’的新对象副本”。

   b. 针对搜索选择属性，键入筛选器值，然后单击“搜索”。

      此时显示匹配筛选条件的标记规则的列表。

   c. 选择要用作新标记基础的对象。

3. 单击“确定”。

   此时显示“创建标记规则”窗口。

4. 填写以下字段：

名称

指定标记规则的名称

说明

指定标记规则的说明

应用的标记

选择要与标记规则相关联的标记

匹配对象类型

显示标记规则应用的对象类型

条件

指定标记规则标准，如下所示：

Name|*IP Address*|*Host*[equal|not equal] *managed_device*

名称

指定受管设备 DNS 名称

IP

指定受管设备 IP 地址

OS 信息

按照 VMware vCenter 中所定义，指定受管设备操作系统

VM 网络

指定受管设备使用的虚拟网络名称

批注

按照 VMware vCenter 中所定义，指定批注键和值。

示例：“Owner=John”

注意：使用通配符 (*) 将标记规则应用于多个受管设备

5. 单击“提交”。

CA Access Control 企业管理 创建标记规则并将其应用于受管设备

将标记分配给 VMware vSphere 客户端的受管设备

您可以将标记分配给从 VMware vSphere 客户端 CA Access Control for Virtual Environments 管理的每个受管设备。

完成以下步骤：

1. 从左边窗格中选择受管设备，然后选择“CA 安全”选项卡。

   此时“CA 安全”选项卡打开，显示摘要内容的选项卡。
2. 单击“添加标记”按钮。
3. 从下拉菜单中选择标记，然后单击“确定”。

   将标记分配给受管设备。

管理程序强化

VMware 管理程序、vSphere 客户端控制台和受管设备易于受到用户的恶意攻击和意外损坏。 强化管理程序和 vSphere 客户端控制台可帮助确保您的 VMware 环境受到保护并能抵御攻击。

CA Access Control for Virtual Environments 帮助系统、安全或 VMware 管理员配置策略。 这些策略会强化 CA Access Control 企业管理 中的管理程序和 VMware vSphere 客户端控制台，并将策略部署到主机组。

注意：有关 VMware 管理程序和 vSphere 客户端控制台强化的更多信息，请参阅 VMware 网站上的*《VMware vSphere Hardening Guide》*（《VMware vSphere 强化指南》）。

管理程序强化策略

在您确定要应用的强化级别之前，请查看以下支持的管理程序强化策略：

- **远程访问** —（仅 ESXi）通过启用锁定模式禁用对 ESXi 服务器的所有远程访问来限制远程访问。 启用后，锁定模式会强制管理员仅从中央位置执行任务，减少了执行未经审核的任务的风险。
- **远程系统日志** — 将事件记录到中央位置会提高管理能力，并让您可以监控中央位置中的所有设备。 而且，将事件保存到中央位置可帮助防止日志篡改。
- **持久性日志** — 将持久性日志配置到数据库可长时间地保留服务器日志。 持久性日志可帮助轻松监控事件并诊断服务器问题。
- **NTP 时间同步** — 错误的时间设置可以让您无法识别和跟踪攻击。 配置 NTP 时间同步可确保所有系统都使用同样的时间源来帮助跟踪和关联攻击。
- **SNMP 配置** —（仅 ESXi）如果 SNMP 代理没有正确配置，攻击者可以将陷阱重定向到恶意主机，并将信息用于恶意用途。
- **直接控制台用户界面**（仅 ESXi）— 直接控制台用户界面 (DCUI) 是 ESXi 管理控制台，让管理员能够执行主机配置和维护任务。 具有本地管理权限的用户可以直接在 DCUI 中执行 VMware vCenter 服务器中未经审核的操作。 禁用 DCUI 可防止用户直接在 ESXi 服务器上执行管理任务。
- **技术支持模式**（仅 ESXi）— 技术支持模式是服务器控制台上或通过 SSH 控制台提供的交互式命令行。 启用后，您可以直接在 ESXi 服务器上执行故障排除和支持的相关任务。 禁用技术支持模式可防止对服务器的未经授权访问。
- **VMSafe 网络 API** — VMSafe 网络 API 为虚拟化环境提供了安全体系结构。 如果您不使用 VMSafe 网络 API，请禁用它。

在 CA Access Control 企业管理 中配置管理程序强化策略

管理程序强化策略可帮助您限制对管理程序的用户访问、配置远程系统日志、时间同步并配置 SNMP 代理设置。

注意：您必须分配系统管理员角色才能管理虚拟机访问权限。

重要说明！ 在完成该步骤之前，确认您是否配置了到 VMware vCenter 服务器的连接。 此外，是否为应用强化策略的每个管理程序创建了 PUPM 端点。

完成以下步骤：

1. 依次转到“全局查看”、“安全组”、“安全组管理”。

   此时出现“安全组管理”页面，显示 VMware vCenter 服务器上的安全组以及 CA Access Control 服务器详细信息。

2. 选择安全组。

   CA Access Control 企业管理 显示安全组详细信息和成员。

   重要说明！ 确认您选择的安全组有至少一个 ESX 服务器作为该组的成员。

3. 在“操作”菜单中，选择“添加管理程序强化策略”。

   此时打开“管理安全组管理程序强化*主机组名称*”页面。

4. 填写以下字段：

   注释

   指定强化策略的说明。

   锁定

   指定阻止对管理程序的远程访问。

   直接控制台 UI

   指定禁用本地管理控制。

   技术支持模式

   指定禁用技术支持模式。

   技术支持模式超时

   指定在其后禁用技术支持模式的时间间隔（以秒为单位）。

   本地数据存储路径

   （仅 ESXi）指定系统日志记录消息的数据存储的完整路径。

   示例： [storage1]/var/log/messages

   远程系统日志主机

   定义远程系统日志主机名。

   远程端口

   定义远程系统日志主机端口号。

   NTP Server

   指定 NTP（网络时间协议）服务器名称。

已启用

指定启用 SNMP 配置。

SNMP 端口

定义 SNMP 侦听端口号。

只读社区

指定具有只读访问权限的社区名称。

示例：snmp-server community public RO

陷阱目标

定义 SNMP 陷阱目标主机名、端口和社区。

格式：*target_hostname@port/community*

示例：SNMP_host@55222/comm

VMSafe 网络 API

指定以禁用使用 VMSafe 网络 API。

管理程序管理员

定义管理程序管理员帐户的名称。 CA Access Control for Virtual Environments 使用该帐户连接到管理程序。

5. 单击“提交”。

CA Access Control 企业管理 将强化策略部署到该组。

审核收集

通过 CA User Activity Reporting Module，您可以对 IT 活动进行收集、正常化、汇总和报告，还可在可能发生遵从性违规时生成报警。

通过 CA User Activity Reporting Module 审核收集策略，您可以根据分配给该组的审核收集配置文件为每个虚拟机组分配策略。

注意：有关 CA Access Control for Virtual Environments 和 CA User Activity Reporting Module 的详细信息，请参阅*《企业管理指南》*。

在 CA Access Control 企业管理 中配置审核收集策略

为 CA Access Control for Virtual Environments 管理的每个安全组都配置审核收集策略。 CA Access Control for Virtual Environments 在您添加到该组的每台虚拟机上都实施审核收集策略。

完成以下步骤：

1. 依次转到“全局查看”、“安全组”、“安全组管理”

   此时出现“安全组管理”页面，显示 VMware vCenter 上的计算机组以及和 CA Access Control 服务器详细信息

2. 从“安全组”部分中选择一个组

   CA Access Control 企业管理 显示组详细信息和成员。

3. 从“操作”菜单中选择“添加审核收集策略”

   此时打开“管理安全组审核收集: *安全组名称*”窗口。

4. 填写以下字段：

   说明

   指定审核收集策略的说明。

   已启用

   选择启用受管设备中的事件收集。

   操作系统配置文件

   选择想要应用审核收集策略的操作系统配置文件。

   审核收集配置文件

   指定您在 CA User Activity Reporting Module 中定义的审核收集配置文件。

   配置文件说明

   指定来自审核收集配置文件的说明。

   身份验证帐户

   定义用于连接到 CA User Activity Reporting Module 的用户帐户。

   注意：根据您选择的审核收集配置文件来启用或禁用该字段。

5. 选择“提交”

   CA Access Control 企业管理 创建审核收集策略并将策略分配给安全组。 现在，CA User Activity Reporting Module 可以直接从受管设备收集审核事件。

在 VMware vSphere 客户端中查看 CA User Activity Reporting Module 报告

如果 CA User Activity Reporting Module 已配置为从受管设备收集审核记录，那么您可以查看来自 VMware vSphere 客户端的 CA User Activity Reporting Module 报告。

完成以下步骤：

1. 从左边窗格中选择受管设备，然后选择“CA 安全”选项卡。

   此时“CA 安全”选项卡打开，显示摘要内容的选项卡。

2. 选择“用户活动报告模块”选项卡。
3. 从下拉菜单中选择报告。

   报告即会显示。

特权帐户密码发现

特权帐户密码发现是过程，通过该过程 CA Access Control for Virtual Environments 发现、存储并管理特权帐户和应用程序 ID 密码。 一旦发现，您可以使用 CA Access Control for Virtual Environments 控制基于您定义的策略的特权帐户和密码。

在 VMware vSphere 客户端中手动发现特权帐户密码

要控制对特权帐户密码的访问，请首先识别受管设备上的特权帐户，然后将特权帐户密码存储在 CA Access Control for Virtual Environments 中。

完成以下步骤：

1. 从左边窗格中选择受管设备，然后选择“CA 安全”选项卡。

   此时“CA 安全”选项卡打开，显示摘要内容的选项卡。

2. 如果要禁用 PUPM 以启动帐户发现向导，请从“服务”字段，选择“配置”。

   帐户发现和跳跃向导将启动。

3. 填写对话框中的以下字段：

   名称

   识别您配置的受管设备的名称。

   说明

   指定端点的说明。

   端点类型

   定义端点类型。

   注意：在您选择终端类型时，其他的对话框将打开。 使用该对话框提供管理该类型端点上的特权帐户所需的凭据。您选择的端点类型会影响您必须提供的连接信息。

4. 选择“验证”。

   CA Access Control for Virtual Environments 尝试验证端点连接设置。

5. 单击“下一步”。

6. 针对搜索选择属性，键入筛选器值，然后单击“搜索”。

   此时将显示匹配筛选条件的特权帐户的列表。

7. 选择要管理的特权帐户并单击“下一步”。

   “锁定属性”屏幕将打开。

8. 填充该对话框中的字段。 以下字段需加以说明：

   断开系统

   指定帐户是否起源于断开的系统。

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

   密码策略

指定要应用于特权帐户或服务帐户的密码策略。

签出到期

定义签出帐号到期之前的持续时间（分钟）。

独占帐户

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

签出时更改密码

指定是否要 PUPM 在每次签出时更改特权帐户的密码。

签入时更改密码

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

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

9. 单击“下一步”。

   将打开“摘要”屏幕。

10. 查看详细信息，然后单击“完成”。

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

更多信息：

Windows Agentless 连接信息 (p. 51)
SSH 设备连接信息 (p. 52)
VMware ESX/ESXi 连接信息 (p. 53)

Windows Agentless 连接信息

Windows Agentless 端点类型允许您管理特权 Windows 帐户。

注意：如果您在本地计算机上配置域用户，CA Access Control for Virtual Environments 无法更改该域用户的密码。 该限制是由于 Windows 行为引起的。

当您创建该类型的端点时，请提供以下信息：

用户名

定义该端点的管理用户的名称。CA Access Control 企业管理 使用该帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。

密码

定义该端点的管理用户的密码。

主机

定义该端点的主机名。

示例：myhost-ac-1

主机域

指定该主机所属的域的名称。

注意：只使用前缀指定主机域名。 例如：如果完整域名是 company.com，您只输入前缀 company。

是 Active Directory

指定用户帐户是否是 Active Directory 帐户。

用户域

指定用户所属的域的名称。

注意：只使用前缀指定用户域名。 例如：如果完整域名是 company.com，您只输入前缀 company。

重要说明！ 如果想使用 PUPM 自动登录登录端点，则验证是否指定了主机域名。 如果端点是工作组的成员，请指定主机名，而不是工作组名称。

注意：有关需要配置 Windows Agentless 端点的他步骤详细信息， 请参阅《*企业管理指南*》。

SSH 设备连接信息

SSH 设备类型允许您管理特权 UNIX 帐户。

重要说明！ 在您配置 PUPM SSH 端点之前，先在端点上禁用隧道明文密码，然后再配置端点设置。

当您创建此类设备时，请提供以下信息，以使 CA Access Control 企业管理 可以连接到设备：

用户名

定义该端点的管理用户的名称。CA Access Control 企业管理 使用该帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。如果您指定操作管理员帐户，PUPM 会使用该帐户在端点上执行管理任务。

密码

定义该端点的管理用户的密码。

主机

定义该端点的主机名。

操作管理员用户登录

（可选）定义端点的操作管理员用户的名称。PUPM 使用该帐户在端点上执行管理任务，例如，发现和更改特权帐户的密码。 如果您不指定操作管理员用户，PUPM 会使用用户登录帐户在端点上执行管理任务。

如果为使用检查点防火墙的 SSH 端点指定操作管理员用户，则请指定专家用户。 但是，您无法使用 PUPM 更改端点上的专家帐户的密码。该限制意味着，专家帐户必须是 PUPM 中的断开帐户。

操作管理员密码

（可选）定义操作管理员用户的密码。

配置文件

指定 SSH 设备 XML 配置文件的名称。 您可以根据需要自定义 XML 文件。

注意：如果您不指定该字段的值，CA Access Control 企业管理 将使用 ssh_connector_conf.xml 文件。

注意：有关需要配置 SSH 设备端点的他步骤详细信息， 请参阅《*企业管理指南*》。

VMware ESX/ESXi 连接信息

VMware ESX/ESXi 端点类型允许您管理特权 VMware ESX/ESXi 帐户。

当您创建此类端点时，请提供以下信息，以使 CA Access Control for Virtual Environments 可以连接到端点：

用户名

定义该端点的管理用户的名称。CA Access Control 企业管理 使用该帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。

注意：如果您指定“高级”选项，PUPM 不使用“用户登录”帐户来执行管理任务。 相反，PUPM 使用指定的特权帐户在端点上执行管理任务。

密码

定义该端点的管理用户的密码。

主机

定义该端点的主机名。

高级

指定是否要使用特权管理帐户在端点上执行管理任务，例如：连接到端点、发现帐户和更改密码。 例如：您可以指定一个可以在多个端点上执行管理任务的特权域帐户。

如果指定该选项，PUPM 不使用“用户登录”帐户来执行管理任务。

从 VMware vSphere 客户端签出特权帐户密码

可以签出特权帐户密码，以登录该帐户所属的受管设备。 签出特权帐户时，可以选择来显示密码、将密码复制到剪贴板或登录受管设备。

完成以下步骤：

1. 从 VMware vSphere 客户窗口的左窗格中选择受管设备，然后选择“CA 安全”选项卡。

   此时“CA 安全”选项卡打开，显示摘要内容的选项卡。

2. 导航到“特权帐户管理”选项卡。

   此时打开“特权帐户管理”选项卡，显示可供您签出的可用帐户。

3. 选择要签出的帐户及受管设备，然后从“操作”菜单中选择以下选项之一：

   - 选择“签出”以签出密码
   - 选择“自动登录”以登录到受管设备
   - 选择“显示密码”以显示密码

   VMware vSphere 客户端根据您选择的选项处理任务并继续。

   如果您已选择登录到受管设备，那么受管设备上的窗口将打开并登录。

   注意：第一次登录到受管设备时，系统会在可以连接到受管设备之前向您确认操作。

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

从 VMware vSphere 客户端签入特权帐户密码

从受管设备注销后，应签入特权帐户密码。 在您签入特权帐户密码之后， CA Access Control for Virtual Environments 可以根据配置选项的设置更改密码。

完成以下步骤：

1. 从 VMware vSphere 客户窗口的左窗格中选择受管设备，然后选择“CA 安全”选项卡。

   此时“CA 安全”选项卡打开，显示摘要内容的选项卡。

2. 导航到“特权帐户管理”选项卡。

   此时打开“特权帐户管理”选项卡，显示可供您签入的可用帐户。

3. 选择要签入的帐户密码，并从菜单中选择“签入”。

   CA Access Control for Virtual Environments 签入帐户。

在紧急情况处理期间会发生什么事情

用户在需要立即访问其无权管理的帐户时，会执行紧急情况签出。

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

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

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

注意：只有具有紧急情况特权访问角色的用户才可以执行紧急情况处理。

CA Access Control 企业管理 的紧急情况

使用紧急情况任务可以*立即*访问您没有特权访问权限的端点。

注意：如果不需要立即访问端点，那么您可以请求访问特权帐户。 然后等待管理员批准该请求。

完成以下步骤：

1. 在 CA Access Control 企业管理，依次单击“主页”、“我的帐户”、“我的特权帐户”。

   此时出现“我的帐户”页面，其中显示可供您签出的帐户。

2. 在“选择帐户”字段中，选择“高级”。

   此时出现高级搜索选项。

3. 选择包括紧急情况帐户，并选择“搜索”。

   此时将显示匹配筛选条件的特权帐户的精简列表。

4. 从“操作”菜单中选择要签出的特权帐户。

5. 填写理由，然后单击“签出”。

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

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

VMware vSphere 客户端的紧急情况

使用紧急情况任务可以*立即*访问您没有特权访问权限的端点。

完成以下步骤：

1. 从“主机信息”屏幕中选择“特权帐户管理”。

   此时打开“特权帐户管理”选项卡，显示可供您处理紧急情况的特权帐户。

2. 选择要签出的特权帐户，然后单击“紧急情况”。
3. 填写理由，然后单击“签出”。

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

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

在 CA Access Control 企业管理 中签入紧急情况特权帐户密码

从受管端点注销后，应签入紧急情况特权帐户密码。

完成以下步骤：

1. 依次单击“主页”、“我的帐户”、“我的特权帐户”。

   此时出现“我的帐户”页面，其中显示可供您签入的帐户。

2. 在“选择帐户”字段中，选择“高级”。

   此时出现高级搜索选项。

3. 选择包括紧急情况帐户，并选择“搜索”。

   此时将显示匹配筛选条件的特权帐户的精简列表。

4. 选择要签入的帐户，并从“操作”菜单中单击“签入”。

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