CA Application Performance Management

安全指南

版本 9.5

CA Technologies 产品引用

本文档涉及以下 CA Technologies 产品和功能：

- CA Application Performance Management (CA APM)
- CA Application Performance Management ChangeDetector (CA APM ChangeDetector)
- CA Application Performance Management ErrorDetector (CA APM ErrorDetector)
- CA Application Performance Management for CA Database Performance (CA APM for CA Database Performance)
- CA Application Performance Management for CA SiteMinder® (CA APM for CA SiteMinder®)
- CA Application Performance Management for CA SiteMinder® Application Server Agents (CA APM for CA SiteMinder® ASA)
- CA Application Performance Management for IBM CICS Transaction Gateway (CA APM for IBM CICS Transaction Gateway)
- CA Application Performance Management for IBM WebSphere Application Server (CA APM for IBM WebSphere Application Server)
- CA Application Performance Management for IBM WebSphere Distributed Environments (CA APM for IBM WebSphere Distributed Environments)
- CA Application Performance Management for IBM WebSphere MQ (CA APM for IBM WebSphere MQ)
- CA Application Performance Management for IBM WebSphere Portal (CA APM for IBM WebSphere Portal)
- CA Application Performance Management for IBM WebSphere Process Server (CA APM for IBM WebSphere Process Server)
- CA Application Performance Management for IBM z/OS® (CA APM for IBM z/OS®)
- CA Application Performance Management for Microsoft SharePoint (CA APM for Microsoft SharePoint)
- CA Application Performance Management for Oracle Databases (CA APM for Oracle Databases)
- CA Application Performance Management for Oracle Service Bus (CA APM for Oracle Service Bus)
- CA Application Performance Management for Oracle WebLogic Portal (CA APM for Oracle WebLogic Portal)

- CA Application Performance Management for Oracle WebLogic Server (CA APM for Oracle WebLogic Server)
- CA Application Performance Management for SOA (CA APM for SOA)
- CA Application Performance Management for TIBCO BusinessWorks (CA APM for TIBCO BusinessWorks)
- CA Application Performance Management for TIBCO Enterprise Message Service (CA APM for TIBCO Enterprise Message Service)
- CA Application Performance Management for Web Servers (CA APM for Web Servers)
- CA Application Performance Management for webMethods Broker (CA APM for webMethods Broker)
- CA Application Performance Management for webMethods Integration Server (CA APM for webMethods Integration Server)
- CA Application Performance Management Integration for CA CMDB (CA APM Integration for CA CMDB)
- CA Application Performance Management Integration for CA NSM (CA APM Integration for CA NSM)
- CA Application Performance Management LeakHunter (CA APM LeakHunter)
- CA Application Performance Management Transaction Generator (CA APM TG)
- CA Cross-Enterprise Application Performance Management
- CA Customer Experience Manager (CA CEM)
- CA Embedded Entitlements Manager (CA EEM)
- CA eHealth® Performance Manager (CA eHealth)
- CA Insight™ Database Performance Monitor for DB2 for z/OS®
- CA Introscope®
- CA SiteMinder®
- CA Spectrum® Infrastructure Manager (CA Spectrum)
- CA SYSVIEW® Performance Management (CA SYSVIEW)

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： CA APM 安全概述

本章定义在讨论安全性以及 CA Technologies Application Performance Management (CA APM) 安全选项时所使用的术语。

此部分包含以下主题：

CA APM 安全摘要

CA APM 使用以下安全机制来保护 CA Introscope® 和 CA CEM：

- 针对 Introscope 和 CA CEM 的基于用户和基于组的身份验证和授权访问：
  - 使用 *users.xml* 文件的基于文件的本地安全设置。

    有关详细信息，请参阅“使用本地安全保护 Introscope (p. 29)”和“CA CEM 的本地身份验证和授权 (p. 119)”。
  - LDAP。

    有关详细信息，请参阅使用 LDAP 保护 Introscope (p. 41)。
  - CA EEM。

    有关详细信息，请参阅“使用 CA EEM 保护 Introscope (p. 52)”和“CA CEM 的 CA EEM 身份验证和授权 (p. 111)”。

    注意： CA APM 提供 EEM 8.4 SP4 SDK，并且已使用 EEM 服务器版本 8.4 SP4 及更高版本进行认证。

    另请参阅以下 CA EEM 指南（可随 CA EEM 应用程序一起从 CA Support 站点下载）：

    - *《CA Embedded Entitlements Manager 入门指南》*
    - *《CA Embedded Entitlements Manager 版本说明》*
- 企业管理器安全性：
  - 上级管理器 (MOM) 与收集器之间进行安全身份验证的公钥和私钥。

    有关详细信息，请参阅配置安全身份验证的公钥和私钥 (p. 24)。
  - 保护与企业管理器的连接所需的用户授权。

    有关详细信息，请参阅 Introscope 如何检查安全性 (p. 29)。

- 收集器和 MOM 之间的通信受到干扰。
- 用于保护企业管理器与浏览器之间安全通信的配置属性。

  有关详细信息，请参阅《*CA APM 配置和管理指南*》中的限制仅通过 HTTPS 的企业管理器访问 (p. 132)和“*配置企业管理器 Web 服务器*”。
- 代理与企业管理器之间安全通信的配置属性。

  有关详细信息，请参阅《*CA APM Java 代理实施指南*》或《*CA APM .NET 代理实施指南*》。
- 允许特定用户查看特定 Introscope 域的配置属性。

  有关详细信息，请参阅定义和配置 Introscope 域 (p. 17)以及关于 Introscope 域和安全性 (p. 27)。
- 允许特定用户关闭特定企业管理器的配置属性。

  有关详细信息，请参阅配置企业管理器服务器权限 (p. 39)。
- 允许特定用户查看应用程序分类地图上的特定业务服务和前端的配置属性。

  有关详细信息，请参阅保护应用程序分类地图 (p. 97)。
- 允许特定用户执行动态检测的配置属性。

  有关详细信息，请参阅在 domains.xml 中配置 Introscope 域权限 (p. 36)。
- 允许特定用户执行线程转储的配置属性。

  有关详细信息，请参阅在 domains.xml 中配置 Introscope 域权限 (p. 36)。

- CA CEM 安全：
  - 安装了 TIM 的 Windows 或 Linux 计算机的根密码保护。

    有关详细信息，请参阅《*CA APM 安装和升级指南*》中的主题“*为新 TIM 安装操作系统*”。
  - 用于保护企业管理器与 TIM 之间安全通信的配置属性。

    有关详细信息，请参阅配置通过 HTTPS 的 TIM 通信 (p. 131)。
  - APM 数据库中的 CA CEM 数据经过加密并符合 FIPS 遵从性。有关详细信息，请参阅符合 FIPS 140-2 标准的加密 (p. 129)。
- APM 数据库安全性：
  - APM 数据库的密码保护。

    有关详细信息，请参阅《*CA APM 安装和升级指南*》中的主题“*更改 PostgreSQL 数据库密码*”。

- 保护指向企业管理器的连接。

  有关详细信息，请参阅《*CA APM 安装和升级指南*》中有关在 *tess-db-cfg.xml* 文件中设置加密密码的信息。

- CA Introscope® 和 CA CEM 应用程序监控：
  - 基于业务服务的安全设置需要用户授权。有关详细信息，请参阅默认 CA EEM CEM 访问策略 (p. 114)以及《*CA APM 配置和管理指南*》。

CA APM 安全和权限概述

CA APM 安全（包括身份验证和授权）允许单个用户和用户组（组）（这是指定的用户集，如应用程序管理员、系统管理员或分析人员）安全登录到 Introscope 和 CA CEM 中。权限允许用户和组执行特定的 Introscope 任务。

关于用户身份验证

*身份验证*是安全地识别用户的机制。身份验证向 Introscope 和 CA CEM 提供如下问题的答案：

- 该用户是谁？
- 该用户是否真正代表自己？

身份验证系统依赖于一些独特的已知信息，这些信息只有进行身份验证的个人和身份验证系统知道。为了验证用户的身份，身份验证系统通常会要求用户提供独有的信息。如果身份验证系统可以确认提供的信息是正确的，便认为用户通过了身份验证。

关于用户授权

*授权*是一种机制，系统通过该机制确定已经过身份验证的特定用户对系统控制的安全资源（如应用程序、页面和数据）所应具有的访问权限级别。换句话说，授权是检查用户是否有权对某个资源执行某个操作的过程。

*访问策略*将权限授予特定用户或组，以便对一组给定类型的资源执行操作。

例如，可以将数据库管理系统设计为向特定个人提供从数据库检索信息但不能更改数据库中存储的数据的功能，而向其他个人提供更改数据的功能。授权系统通过提供如下问题的答案来授予这些权限：

- 用户 *X* 是否获得访问资源 *R* 的授权？
- 用户 *X* 是否获得执行操作 *P* 的授权？
- 用户 *X* 是否获得对资源 *R* 执行操作 *P* 的授权？

关于安全领域

安全领域定义负责对用户进行身份验证和/或授权的用户、用户组和访问策略的来源。

可以在 *realms.xml* 文件中为 CA APM 安全配置一个或多个安全领域。Introscope 和 CA CEM 使用在 *realms.xml* 中配置的安全领域来决定如何对用户进行身份验证和授权。用户登录到 Introscope 或者 CA CEM 时，登录到的应用程序会以 realms.xml 中定义的顺序检查每个安全领域。应用程序将检查以查看具有给定 ID 的用户是否存在。如果提供的用户密码与为特定安全领域提供的值匹配，则身份验证成功。如果以下条件之一成立，则身份验证失败：

- 在任何定义的领域中都不存在该名称的用户。
- 在某个领域中存在该用户但密码错误。

有关在 *realms.xml* 中配置领域的信息，请参阅以下主题：

- 在 realms.xml 中配置本地身份验证 (p. 31)
- 在 realms.xml 中配置 LDAP 身份验证 (p. 42)
- 在 realms.xml 中配置 CA EEM 身份验证 (p. 56)

使用以下三个安全领域中的一个或受支持的任意组合来部署 Introscope 安全设置：

- **本地 XML 文件（本地）：**本地安全设置包括本地的身份验证和授权，需要使用企业管理器上存储在 *<EM_Home>/config* 目录中的 XML 文件。
  - 对于本地身份验证，XML 文件用于在每个企业管理器上本地存储用户名和密码信息。默认文件名为 *users.xml*。在运行时，Introscope 将检查本地文件 (*users.xml*) 以对 CA APM 用户进行身份验证。
  - 对于本地授权，Introscope 在每个企业管理器上本地存储两个 XML 文件。Introscope 将 *domains.xml* 用于域权限，将 *server.xml* 用于服务器权限。在运行时，Introscope 将检查本地文件（*domains.xml* 和 *server.xml*）以向 CA APM 用户授权。

Introscope 提供本地安全设置 (p. 29)作为默认安全设置。

重要信息：最好将默认 CA APM 登录从 Workstation、WebView、Web Start Workstation 或 CEM 控制台更改为企业管理器。如果未遵循此最佳实践，并且使用了唯一的 Introscope 本地安全设置，则身份被盗的可能性将增大。因此，CA EEM 是建议使用的安全机制 (p. 15)。

- **轻型目录访问协议 (LDAP)：**一种应用程序协议，用于查询和修改通过 TCP/IP 运行的目录服务。

  如果使用本地 XML 文件进行授权，则只能使用 LDAP 安全领域对 CA APM 用户进行身份验证。有关详细信息，请参阅使用 LDAP 保护 Introscope (p. 41)。

- **CA Embedded Entitlements Manager (CA EEM)：**一种 CA Technologies 应用程序，其他应用程序可借助它共享通用访问策略管理、身份验证和授权服务。

  注意：尽管 CA EEM 安全设置对于 Introscope 是可选的，但出于多种原因，CA Technologies 建议使用 CA EEM 来实现 Introscope 安全。CA EEM 提供了符合行业标准的解决方案、用于管理用户的用户界面以及允许使用细粒度授权权限的集中式存储。如果要保护 Introscope 应用程序分类视图，请部署 CA EEM。

  可以部署 CA EEM 对 CA APM 用户进行身份验证和授权。

  也可以将 CA EEM 配置为使用 LDAP 进行身份验证，使用 CA EEM 进行授权。有关详细信息，请参阅配置使用 LDAP 的 CA EEM 身份验证 (p. 59)。

此表列出了 Introscope 安全领域支持的主要功能。

安全领域支持的功能	CA EEM	LDAP	本地
多个企业管理器共享集中的安全服务器	是	是	否
安全领域始终可用	否	否	是 在企业管理器中运行，因此它始终可用。
支持故障切换	是	是	不适用
与 SiteMinder 集成	是	否	否

安全领域支持的功能	CA EEM	LDAP	本地
支持细粒度权限？ 支持以下细粒度权限类型： ■ 应用程序分类视图权限 ■ 基于业务服务的安全 ■ 灵活的 CA CEM 权限	是	不适用	否
行业标准解决方案	是	是	否
允许进行审核	是	是	否
包括用于管理用户的用户界面	是	是	否
包括用于管理访问策略的用户界面	是	不适用	否

可以使用以下两个安全领域的一个或受支持的任意组合部署 CA CEM 安全：

- **本地 XML 文件（本地）：**本地安全设置包括本地的身份验证和授权，需要使用企业管理器上存储在 *<EM_Home>/config* 目录中的 XML 文件。
  - 对于本地身份验证和授权，XML 文件用于在每个企业管理器上本地存储用户名和密码信息。四个默认 CEM 安全组和属于这些组的用户也将在此处定义。默认文件名为 *users.xml*。授权检查基于为四个默认安全组定义的成员资格。在运行时，本地文件 (*users.xml*) 用于对 CA CEM 用户进行身份验证和授权。

  Introscope 提供本地安全设置作为默认安全设置。
- **CA Embedded Entitlements Manager (CA EEM)：**一种 CA Technologies 应用程序，其他应用程序可借助它来共享通用访问策略管理、身份验证和授权服务。

  注意：出于多种原因，CA Technologies 建议使用 CA EEM 来实现 CA APM 安全。CA EEM 提供了符合行业标准的解决方案、用于管理用户的用户界面以及允许使用细粒度授权权限的集中式存储。
  - 可以部署 CA EEM 对 CA APM 用户进行身份验证和授权。
  - 配置使用 SiteMinder 的 CA EEM 身份验证 (p. 59)和使用 CA EEM 进行授权。
  - 将 CA EEM 配置为仅用于身份验证，将本地 XML 文件配置为用于授权 (p. 95)。

  有关 CA EEM 的详细信息，请参阅使用 CA EEM 保护 Introscope (p. 52)。

CA APM 提供单点登录功能。可以访问 CA CEM 和 Introscope 的用户能够在这两个应用程序之间导航，系统不会再次提示登录。在进行 CA CEM 或 Introscope 用户身份验证时，CA APM 将获得用户的身份以及对用户进行身份验证的领域的名称。Introscope 使用此信息来获得用户所属的组。然后，CA APM 使用以下方法之一对用户进行授权：

- 对于 CA EEM，根据用户访问策略。
- 对于本地安全，根据一个或多个 CA CEM 安全用户组中的成员资格。

在设置 CA APM 安全时，组织必须决定要部署哪个单一的或混合的安全领域。要使 CA APM 用户能访问 Introscope，请部署本地领域或 CA EEM 领域。

注意：CA Technologies 建议部署 CA EEM 身份验证和授权。有关详细信息，请参阅使用 CA EEM 保护 CA APM 的优势 (p. 15)。

使用 CA EEM 保护 CA APM 的优势

CA Technologies 建议部署 CA EEM 以实现 CA APM 安全，因为 CA EEM 提供以下功能：

- 用于管理用户身份和访问策略的通用共享方法
- 集中的 CA APM 安全

  由于 CA EEM 身份验证允许多个企业管理器共享同一个 CA EEM 服务器，因此可以部署集中的 CA APM 安全。
- 有效的访问和授权访问管理
  - 基于业务服务的安全，在其中可以使用访问策略来控制哪些 CA CEM 安全组有权访问业务服务及其关联数据。
  - 应用程序安全设置不能仅限于哪些人能访问什么应用程序。要做到有效，安全策略还必须强制规定每个用户在获得访问权后可以对应用程序中的哪些资源执行特定操作。CA EEM 为各组织提供了一套标准方法，可在其业务应用程序组合中实施灵活和细化的授权策略。
  - 进程内授权会检查授权策略是否安全地缓存在应用程序的 Embedded Entitlements 客户端部分，然后在应用程序内本地评估和执行。这样可以对脱机应用程序实施访问策略。
  - 分离特定于应用程序的策略
    CA EEM 会在中央存储库中隔离特定于应用程序的策略数据，以确保在支持应用程序管理灵活性的同时，将策略和管理控制分开。

- 单一身份存储库

  CA EEM 包含一个存储库，可用作用户身份的单一授权来源。作为替代，该单一来源可以是外部目录，如 Microsoft Active Directory、Novell eDirectory 或 SunONE Directory。

- 企业集成

  可以将 CA EEM 与其他 CA 安全解决方案一起部署，以便在一套复杂的业务应用程序中实现一致的身份和访问管理 (IAM)。这需要 CA EEM 之类的安全工具，这些工具在当前的开发环境中具有可适应、灵活、易管理和可用的特点。

  - CA SiteMinder 集成

    本机集成允许 Embedded Entitlements 客户端应用程序访问 CA SiteMinder 配置使用的用户存储中的用户和组信息，使用 CA SiteMinder 凭据进行身份验证，以及支持通过 CA SiteMinder Web 应用程序进行单点登录。

  - 采用 C#、C++ 和 Java 语言的 SDK

    CA EEM 支持采用 C#、C++ 和 Java 语言的开发环境。C#、C++ 和 Java 参考中对其身份验证、授权、事件管理和管理 API 有全面的介绍。其中包括示例代码和 XML 脚本，以及有关如何将其安全功能嵌入到应用程序的教程。

- 管理 Web 用户界面

  CA EEM 通过提供基于 Web 的单一管理界面，最大限度地减少建立和维护应用程序安全策略、用户存储和审核规则的成本。通过将安全策略管理放到应用程序本身之外，可以随着业务要求的演变保持一致的安全级别，而不用重新开发应用程序代码。

  - 共享的 Web 用户界面

    CA EEM 提供即用型 Web 用户界面，该用户界面可在所有应用程序之间共享，用于管理用户和组以及定义和管理访问策略。或者，也可以使用 CA EEM SDK 将管理用户界面组件嵌入自定义网页中。

  - 管理范围

    可以将管理员权限限制为仅查看或处理特定的应用程序、用户、资源或策略。

  - 权限检查

    可以测试安全策略并查看详细的策略调试信息，以确保在将其投入使用之前可获得所需的结果。

第 2 章： 定义和配置 Introscope 域

本章包含在设置 Introscope 安全之前定义和配置 Introscope 域的有关信息。本章还包含有关为 MOM、收集器和工作站之间的安全身份验证设置公钥和私钥的信息。

此部分包含以下主题：

定义和配置 Introscope 域

Introscope 使用域来划分代理和监控逻辑，以定义哪些 CA APM 用户可以看到什么信息。可以在 *domains.xml* 文件（该文件位于 *<EM_Home>/config* 目录中）中使用 PerlS 正则表达式将 Introscope 代理映射到域。可以使用 *domains.xml* 来定义域，而无需考虑使用的是哪个安全领域。

除了配置域之外，还可以在进行 Introscope 安全设置时配置域权限。对于本地安全设置，将在 *domains.xml* 文件中配置域权限。有关详细信息，请参阅在 domains.xml 中配置 Introscope 域权限 (p. 36)。如果部署 CA EEM 来实现 Introscope 安全，则企业管理器将忽略 *domains.xml* 中的域权限，您应改为在 CA EEM 中配置这些权限。有关详细信息，请参阅创建和删除 CA EEM APM 域资源访问策略 (p. 83)。

域类型

在 Introscope 中有两种类型的域：

- *超级域*－*超级域*是包含系统中所有用户定义的域的超集域。所有代理在*超级域*中均可见，但也可能出现在用户定义的域中。默认的 Introscope 配置仅包含*超级域*。如果未配置任何其他域，则所有代理都将映射到*超级域*。
- 用户定义的域－在 *domains.xml* 文件（该文件位于 *<EM_Home>/config* 目录中）中定义新域。*domains.xml* 文件提供域名到正则表达式的映射。

域的定义规则

在 *domains.xml* 文件中定义域的规则是：

- 定义域时必须遵循有效的 XML 文件规则。
- 域名区分大小写。
- 任何域都必须放在根 XML 域的元素内。
- 在一个*域*或*超级域*中可以有多个代理映射。如果将*域*配置为匹配某个代理，则该代理将映射到该*域*，并且也可从*超级域*看见。

  注意：在启动事务跟踪时，此类代理将附加到“事务踪迹”窗口中的某个用户定义的域上。
- 代理总是映射到分配给它的第一个域。如果没有分配任何域，则代理将映射到*超级域*。如果分配了用户定义的域，则代理将映射到用户定义的域。
- 如果不更改当前的*超级域代理*映射（默认情况下配置为匹配所有代理），则 Introscope 会将所有新定义的域放在 *<SuperDomain>* 标记之前。
- Introscope 将不匹配任何映射（由于 *domains.xml* 文件中的正则表达式有错误，或其他问题）的代理放在*超级域*中。

在群集之内以及跨群集使用相同 domains.xml

在群集内部署 MOM 和收集器以及在群集内和跨群集部署可选 CDV 时，请了解这些重要的 domains.xml 规则。

重要信息！不要在 CA APM 群集内以及 CA APM 群集之间为 MOM、收集器和 CDV 使用不同的 domains.xml 文件。

MOM 可以在群集中为活动代理（正在向群集发送数据的代理）处理不同的域。但是，如果对 MOM 和收集器上的历史代理使用不同的域，会导致 MOM 的历史数据视图中出现不一致。在此类具有混合域的群集中，不会跟踪收集器上的历史代理，因此，历史代理的数据不会显示在通过 MOM 创建的 Workstation 图表中，除非显式装入历史代理。为避免以上情况，CA Technologies 强烈建议在一个群集中的 MOM 以及所有收集器上放置完全相同的 domains.xml 文件。这样，无需装入历史代理以查看 Workstation 上与特定收集器有关的历史数据，实时数据和历史代理数据会一直在 MOM Workstation 中可见。

如果要部署跨群集数据查看器 (CDV)，CDV domains.xml 文件必须包含以下域：

- CDV 连接到的所有收集器的所有域。
- 跨所有群集（包含 CDV 收集数据的收集器）的所有域。

如果某个域存在于收集器 domains.xml 文件中但在 CDV domains.xml 文件中缺失，将发生以下情况：

- CDV 不搜集缺失的收集器域的数据。

CDV Workstation 不显示缺失的收集器域中的数据。

定义代理并将其映射到域

可使用 domains.xml 文件来定义域并将代理映射到域。

请执行以下步骤：

1. 导航到 *<EM_Home>/config* 目录。
2. 打开 *domains.xml* 文件。
3. 使用域的定义规则 (p. 18)和以下属性定义域。

   name

   域的名称

   此属性的规则为：

   - 仅限字母数字字符、下划线 _ 和连字符 -
   - 不允许使用空格

   描述

   域的简短描述

   允许使用除引号之外的任何字符。

   注意：所有 XML 标记都区分大小写。

4. 对所有其他域重复步骤 3。
5. 确保在 domains.xml 的末尾定义超级域映射，以便可以使 domains.xml 在将代理映射到超级域之前先将代理映射到特定域。

   例如，如果将以下超级域映射置于 domains.xml 的开头，则会在处理此 XML 文件其余部分之前将所有代理置于此超级域之下。

   ```
   <SuperDomain>
               <agent mapping="(.*)"/>
               <grant group="Admin" permission="full"/>
   </SuperDomain>
   ```

   通过将该超级域映射置于 domains.xml 的末尾，超级域可以捕获所有不匹配的代理。
6. 保存并关闭 *domains.xml* 文件。
7. 重新启动企业管理器，使其可以加载一个或多个新域。

注意：如果 *domains.xml* 文件中有语法错误或其他错误，企业管理器将不会启动。

新域的 domains.xml 语法

域的语法是：

```
<domain name="Domainname" description="Domain description">
<agent mapping="host\|process\|agentname or matching agents"/>
<grant user="username" permission="permission"/>
</domain>
```

将管理模块与域相关联

在创建新管理模块时，可以选择将要包含它们的域。

通过创建目录（该目录对应于在 *domains.xml* 中定义的域的名称）后将管理模块移动到新目录中，使管理模块与域相关联。

请执行以下步骤：

1. 在 *<EM_Home>/config/modules* 目录中，创建一个与在上一节中创建的域名相对应的目录。

   例如，如果定义了一个名为 PetstoreA　的域，则在此步骤中将创建一个名为 PetstoreA 的目录，如下例所示：

   <EM_Home>/config/modules/PetstoreA

   注意：域目录必须与 *domains.xml* 文件中定义的名称完全匹配（拼写正确，大小写也匹配），否则将不会加载该目录中驻留的任何管理模块。

2. 将所需的管理模块从 *<EM_Home>/config/modules* 目录移到刚创建的新目录中。
3. 重新启动企业管理器，使其可以加载新的域。

将示例管理模块添加到新定义的域中

在定义新域时，它并不包含任何管理模块。如果希望新定义的域显示默认示例显示板，则需要将示例管理模块复制到新定义的域中。

请执行以下步骤：

1. 导航到 *<EM_Home>/config/modules/* 目录。
2. 将 *SampleManagementModule.jar* 文件复制到新定义域中的相应模块目录中。

   例如，如果定义了名为 Petstore A 的域，则将 *SampleManagementModule.jar* 复制到以下目录：

   <EM_Home>/config/modules/PetstoreA
3. 重新启动企业管理器以便加载新的管理模块。

重要信息！复制到新域中的示例管理模块不会以任何方式与原始示例管理模块关联。对原始示例管理模块所做的任何更改都不会影响其他域中的任何示例管理模块副本，反之亦然。

更改代理的域映射

重新将代理映射到不同的域（在删除了某个域或者合并了两个域之后）有以下三种结果：

- 如果不重新分配映射到已删除域的代理，并且该代理仍进行报告，则它将出现在*超级域*下。
- 如果代理有关联的 SNMP 收集，则必须重新发布该 SNMP MIB。
- 将代理移到不同的域时，该代理中的所有关闭信息都将丢失。

删除域

在以下情况下，可能需要删除域：

- 将代理分配给不同的域
- 合并两个域

请执行以下步骤：

1. 关闭企业管理器。
2. 导航到 <EM_Home>/config 目录。
3. 从 domains.xml 文件中删除域。
4. 如有必要，将所有映射的代理重新分配到不同的域。
5. 从 <EM_Home>/config/modules 目录中删除相应的域目录。
6. 重新启动企业管理器。

合并两个域

合并两个域时，需要将所有代理映射信息合并到一个域中，并移动某个域下的所有关联管理模块。

请执行以下步骤：

1. 关闭企业管理器。
2. 打开位于 *<EM_Home>/config* 目录中的 *domains.xml* 文件。
3. 在源域（如域 A）下，复制代理映射 XML 代码信息。
4. 在目标域（如域 B）下，粘贴代理映射 XML 代码信息。
5. 删除源域（如域 A）中的代理映射 XML 代码。
6. 将 *<EM_Home>/config/modules/* 中源域（如域 A）目录内的所有管理模块移到目标域（如域 B）。

   注意：如果目标域目录中存在与要移动的模块同名的任何管理模块，则将需要重命名源域中的管理模块。如果存在两个同名的管理模块，企业管理器将不会启动。
7. 从 *domains.xml* 中删除源域。
8. 重新启动企业管理器。

在不同的 Introscope 安装之间克隆域

如果目标安装域配置与源安装完全相同，则可执行该过程。（即，*domains.xml* 文件中定义的所有域将完全相同的情况。）

请执行以下步骤：

1. 将源安装中的 *<EM_Home>/config/domains.xml* 文件复制到目标安装中的相同目录。
2. 将源安装中的 *<EM_Home>/config/shutoff/MetricShutoffConfiguration.xml*（如果存在）复制到目标安装中的相同目录。
3. 将 *<EM_Home>/config/modules/<domain>* 目录的内容从源安装复制到目标安装。
4. 重新启动企业管理器。

在非克隆安装之间移动域

要在非克隆安装之间移动域时，如果旧安装和新安装之间的域配置有少许变化，则可执行此过程。

请执行以下步骤：

1. 打开位于源安装中的 *<EM_Home>/config* 目录内的 *domains.xml* 文件。
2. 复制域信息。
3. 打开位于目标安装中的 *<EM_Home>/config* 目录内的 *domains.xml* 文件。
4. 将域信息复制到 *domains.xml* 文件中。
5. 在目标安装中，创建新管理模块目录，这些目录对应于源安装中 *<EM_Home>/config/modules* 目录内的那些目录。
6. 复制属于要移动的域的所有管理模块，然后将其粘贴至对应的域目录中。
7. 从源安装中删除域。
8. 重新启动企业管理器。

代理故障转移和用户/域配置

如果使用代理故障转移功能，并且定义了用户和密码，请验证 *domains.xml*、*server.xml* 和 *users.xml* 文件在指定的故障转移企业管理器间是否同步。

有关代理故障切换的详细信息，请参阅《*CA APM Java 代理实施指南*》或《*CA APM .NET 代理实施指南*》中适用于您环境的“*配置代理故障切换*”内容。

配置安全身份验证的公钥和私钥

在群集环境中，MOM、收集器和工作站之间的通信协议使用公钥和私钥进行安全身份验证。

注意：公钥和私钥仅用于在登录时保护密码。要保护所有通信，需要使用 SSL。

关于默认收集器私钥

每个收集器都使用私钥对 MOM 用于连接的密码进行解密。公钥和私钥必须配套。收集器企业管理器的私钥在 *IntroscopeEnterpriseManager.properties* 文件中的 *introscope.enterprisemanager.clustering.privatekey* 属性中定义。

默认值为

```
config/internal/server/EM.private
```

除非为获得额外的安全而希望为收集器生成新公钥和私钥集，否则不需要重新配置私钥。有关重新配置私钥的详细信息，请参阅生成新公钥和私钥集 (p. 25)。有关 *introscope.enterprisemanager.clustering.privatekey* 属性的详细信息，请参阅《*CA APM 配置和管理指南*》。

注意：CA APM 公钥和私钥不会过期。

生成新公钥和私钥集

为了提高 CA APM 环境的安全性，可以为每个收集器生成新公钥和私钥，将公钥放在 MOM 上，并更新 MOM 的“收集器”属性。

请执行以下步骤：

1. 导航到 Introscope 安装目录。
2. 在命令提示符处，键入以下命令：

```
java -classpath
product\enterprisemanager\plugins\com.wily.introscope.em.client14_9.5.0.jar;lib\CLWorkstation.jar;product\enterprisemanager\configuration\org.eclipse.osgi\bundles\24\1\.cp\lib\WilyBouncyCastle.jar
com.wily.util.encryption.KeyGenerator EM.public EM.private
```

3. 如果为收集器生成新密钥，则将公钥复制到 MOM 的 *IntroscopeEnterpriseManager.properties* 文件中的 *introscope.enterprisemanager.clustering.login.em1.publicKey* 属性中指定的位置。

   注意：如果要为 MOM 生成新密钥，则本步骤不适用。

4. 将公钥和私钥复制到位于 *<EM_Home>\config\internal\server* 的企业管理器安装中。

第 3 章： 保护 Introscope

本章包含有关配置身份验证和授权机制的信息，可以部署这些机制以提供 Introscope 安全设置和权限。此外，本章还介绍了应用程序分类地图安全设置和 Introscope SSO。

此部分包含以下主题：

Introscope 安全性和权限概述

Introscope 安全设置（包括身份验证和授权）允许单个用户和用户组（组）（指定的用户集，如应用程序管理员、系统管理员或分析员）安全登录到 Introscope。权限允许用户和组执行特定的 Introscope 任务。

有关 Introscope 安全的背景知识，请参阅《CA APM 安全摘要 (p. 9)》。

关于 Introscope 域和安全性

Introscope 使用域来划分代理和监控逻辑，以定义哪些用户可以看到什么信息。可以在 *domains.xml* 文件中使用 Perl5 正则表达式将代理映射到域。

将代理映射到域之后，可以定义并授予域权限。在授权过程中，Introscope 将执行权限检查。

有关设置 Introscope 域的信息，请参阅定义和配置 Introscope 域 (p. 17)。

关于配置 Introscope 权限

在 Introscope 中，权限决定用户或组可以执行的任务，包括在工作站中配置监控逻辑以及处理企业管理器管理任务。可以为域和企业管理器定义 Introscope 权限。然后，可将用户和组权限授予域和/或企业管理器。

域权限和调查器树

调查器树外观与具有不同域权限的用户或组不同：

- 至少拥有对*超级域*的读取权限的用户或组可以查看调查器树中定义的所有域的内容。
- 拥有多个域的权限的用户或组将看到调查器树中对应的域的域信息。
- 用户或组必须至少拥有一个域的读取权限，否则他们将无法登录工作站或 WebView 以查看调查器树和控制台。

可以使用 *domains.xml* 和 *server.xml* 配置本地授权权限，并可使用 Safex 工具或 CA EEM 用户界面配置 CA EEM 授权权限。有关设置权限的更多信息，请参阅以下主题：

- 在 domains.xml 中配置 Introscope 域权限 (p. 36)
- 配置企业管理器服务器权限 (p. 39)
- 配置 CA EEM 授权 (p. 60)
- 从本地安全设置迁移到 CA EEM 安全设置 (p. 94)

Introscope 的默认安全配置

Introscope 在 *realms.xml* 文件中提供默认安全配置。用于身份验证和授权的本地 XML 文件（位于 *<EM_Home>/config* 目录中）是 Introscope 的默认安全领域。要使用默认安全配置，请参阅使用本地安全设置保护 Introscope (p. 29)。

如果 Introscope 的默认安全配置没有达到要求，则可配置 *realms.xml* 以使用 CA EEM、LDAP 或支持的领域的某个合适组合来进行身份验证和授权。

例如，您可能希望通过以下方式配置 Introscope 安全设置：

- 更改本地安全设置的默认配置设置。有关详细信息，请参阅关于配置本地身份验证 (p. 30)。
- 用 LDAP 服务器身份验证替代本地安全身份验证。有关详细信息，请参阅使用 LDAP 保护 Introscope (p. 41)。
- 用 CA EEM 身份验证和授权替代本地安全设置。有关详细信息，请参阅使用 CA EEM 保护 Introscope (p. 52)。

Introscope 如何检查安全设置

每次安全检查开始时，Introscope 都会确定组织已配置的安全领域。例如，一旦 Introscope 知道您已经使用 SiteMinder 授权实施 CA EEM 身份验证或使用本地授权实施 LDAP 身份验证，则 Introscope 将根据您的安全设置实施内容来执行相应的安全和权限检查。

Introscope 的常规安全和权限检查过程包括以下步骤：

1. 启动身份验证时，检查 *realms.xml* 以确定安全领域并获取一些用户信息。
2. 完成身份验证时，以本地方式从 LDAP 服务器或 CA EEM 服务器的 *users.xml* 文件中获取用户、组和用户-组映射。

   注意：如果已经设置了 CA EEM 与 LDAP 服务器集成，则可使用 LDAP 进行身份验证，使用 CA EEM 进行授权。有关详细信息，请参阅配置使用 LDAP 的 CA EEM 身份验证 (p. 59)。

   注意：如果已经设置了 CA EEM 与 SiteMinder 集成，则可使用 SiteMinder 进行身份验证，使用 CA EEM 进行授权。有关详细信息，请参阅配置使用 CA SiteMinder 的 CA EEM 身份验证 (p. 59)。
3. 开始授权时，在企业管理器上以本地方式获取 *users.xml* 文件中的密码，或者在 CA EEM 中获取密码。
4. 完成授权时，在企业管理器上以本地方式从 *domains.xml* 和 *server.xml* 文件中获取域和企业管理器服务器权限，或者从 CA EEM 中获取域和企业管理器服务器权限。

使用本地安全设置保护 Introscope

现在，您已经了解了 Introscope 安全设置方面的一些背景知识，可以制定您的安全部署计划了。

请执行以下步骤：

1. 如果需要，在 *realms.xml* 中将本地领域配置为安全领域。

   注意：本地领域是 *realms.xml* 中的 Introscope 默认领域。
2. 在 *users.xml* 中设置用户和组以及密码。
3. 在 *domains.xml* 中分配域权限。
4. 在 *server.xml* 中分配企业管理器服务器权限。
5. 根据需要添加、删除、编辑 CA APM 组、用户、域和服务器及其关联的权限，以维护 Introscope 安全。

关于配置本地身份验证

Introscope 默认使用本地身份验证。如果使用本地身份验证，则 CA APM 用户和密码将存储在 *users.xml* 中。

但是，用户详细信息（如电子邮件和电话号码）并不在本地领域中维护。此外，本地领域无法维护两个名称和密码都相同的用户，但是可以维护两个名称相同但密码不同的用户。如果两个用户的名称相同而密码不同，则本地领域将其视为独立的用户。

有关这些定义用户、组和生成密码的详细信息，请参阅在 users.xml 中配置 CA APM 用户和组 (p. 33)。

本地身份验证更改是动态的：当 CA APM 用户尝试登录时，系统会在用户每次发出身份验证请求时都将密码与 *users.xml* 文件进行比较。

如果您要从以前的 Introscope 安装迁移 Introscope 用户，则在迁移完成之前，不要更改 *users.xml* 文件的名称或位置。

在 realms.xml 中配置本地身份验证

在配置 *realms.xml* 时，请遵循以下规则：

重要信息！如果未满足所有这些规则，企业管理器不会启动。

- *descriptor=* 的值区分大小写。
  - 例如，*descriptor=Local Users and Groups Realm* 不同于 *descriptor=local users and groups realm*。
- 对于本地领域，*descriptor=* 的值必须是 *Local Users and Groups Realm*。
- 在有多个领域的情况下，领域标记中的 *id=* 的值对每个领域必须唯一。例如：

```
<realm descriptor="EEM Realm" id="EEM" active="true">
        <property name="username">
          <value>EiamAdmin</value
        </property>
           <property name="host">
            <value>localhost</value>
        </property>
        <property name="appname">
            <value>APM</value>
        </property>
        <property name="enableAuthorization">
            <value>true</value>
        </property>
        <property name="plainTextPasswords">
            <value>false</value>
        </property>
        <property name="password">
            <value>YhCVozLDYThTJk3icaAaY9/5MhJRqQ1X</value>
        </property>
    </realm>
    <realm descriptor="Local Users and Groups Realm" id="Local Users and
Groups" active="true">
        <property name="usersFile">
            <value>users.xml</value>
        </property>
    </realm>
```

请执行以下步骤：

1. 打开位于 *<EM_Home>/config* 目录中的 *realms.xml* 文件。
2. 确认以下行存在，且为 *realms.xml* 中的第三个条目：

```
<realm active="true" descriptor="Local Users and Groups Realm" id="Local
Users and Groups">
```

3. 对该属性进行相应的设置。

   usersFile

   相对于存储用户的 *<EM_Home>/config* 目录的文件名。默认情况下，此文件名为 *users.xml*。

   注意：该文件还包含组定义。

   注意：有关为安全领域使用多个文件的信息，请参阅关于为安全领域使用多个文件 (p. 32)。

4. 保存对 *realms.xml* 文件所做的更改，然后重新启动企业管理器以应用更改。

启用本地身份验证的 realms.xml 语法

以下是 *realms.xml* 文件中的示例代码。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">
    <realm descriptor="Local Users and Groups Realm" id="Local Users and Groups"
active="true">
        <property name="usersFile">
            <value>users.xml</value>
        </property>
    </realm>
```

关于为安全领域使用多个文件

如果在 *realms.xml* 文件中为所有安全领域仅列出一个文件，则可忽略本主题。

在有些情况下，可以设置多个领域，例如，需要一个默认领域授予用户基本权限，需要另外一个领域授予不同权限的情况。或者，组织可能有两个 LDAP 服务器，您想测试两者的安全性。或者，组织可能一直在使用本地安全设置，而且您希望在移动到 CA EEM 时将其保留在适当位置。

如果在 *realms.xml* 中列出了两个文件作为安全领域，则在身份验证和授权过程中将使用第一个文件。如果您有两个名为 User A 的用户，他们的密码相同，则 *realms.xml* 将使用它在列出的第一个文件中找到的密码。例如，如果已将 *users.xml* 列在 *CEM45.xml* 之前，则 *realms.xml* 将使用 *users.xml* 中的密码执行身份验证。

对于本地领域，不会在 *users.xml* 和 *CEM45.xml* 中维护用户详细信息（如电子邮件和电话号码）。此外，本地领域无法维护名称和密码都相同的两个用户。但是，本地领域可以维护名称相同但密码不同的两个用户。

同样，如果您有两个名为 User A 的用户，他们在 *users.xml* 和 *CEM45.xml* 中属于不同的用户组，则 *realms.xml* 将使用它在列出的第一个文件中找到的用户组。例如，将 *users.xml* 列在 *CEM45.xml* 之前的情况。在 *users.xml* 中，您在“CEM 系统管理员”用户组中有一个名为 Admin 的用户。在 *CEM45.xml,* 中，您在“CEM 分析人员”用户组中有一个名为 Admin 的用户。在这种情况下，*realms.xml* 将使用 *users.xml* 用户组，并向名为 Admin 的用户授予与“CEM 系统管理员”用户组关联的权限。

在 users.xml 中配置 CA APM 用户和组

为每个用户和组定义用户名和密码。

注意：在创建 *admin* 用户时，切记用户和权限区分大小写。如果用户使用 *admin* 或 *Admin* 登录名登录，则会应用该用户角色所适用的权限。

默认的 CA APM 用户配置定义了以下用户：

- *管理员*，无密码
- *来宾*，*Guest* 为密码

请执行以下步骤：

1. 导航到 *<EM_Home>/config* 目录。
2. 打开 *users.xml* 文件。
3. 使用该用户和组命名属性定义用户名。

   注意：所有 XML 标记都区分大小写。

   有关用户和组的示例语法，请参阅用户的 users.xml 语法 (p. 35)和组的 users.xml 语法 (p. 35)。
4. 使用该属性为每个用户或组设置密码。

   注意：所有 XML 标记都区分大小写。

   password

   用户密码。

   以下规则适用于此属性：

   - 除引号之外的任何字符
   - 默认情况下，密码经过加密，不采用明文形式或进行模糊处理（可以选择生成经过编码的密码）。
   - 密码字符可以是合法的 XML 字符。
   - 密码值可以为空。

   最佳实践：遵循您组织的密码策略。

users.xml 文件中用于本地身份验证的密码以加密形式存储。您可以选择使用 MD5Encoder 实用工具生成加密密码，也可以让 Introscope 自动生成密码。Introscope 提供的 MD5 脚本接受纯文本输入，但输出为加密形式。

- 当以下条件适用于您的情况时，请按照步骤 5（手工设置加密密码）中的说明进行操作：
  - 您已经在 *users.xml* 中加密了多个用户。
  - 想更改一个或几个密码。
- 否则，请将所有用户密码改回明文形式。
- 当以下条件适用于您的情况时，请按照步骤 6（设置纯文本密码）中的说明进行操作：
  - 要一次创建或更改多个用户和密码。

5. 手工设置加密密码。
   a. 在 *users.xml* 文件中设置 *plaintextPasswords="false"*。
   b. 运行位于 *<EM_Home>/tools* 目录中的相应脚本。
      - 对于 Windows，运行 *MD5Encoder.bat* <password>
      - 对于 UNIX，运行 *MD5encoder.sh* <password>

      注意：在运行 MD5Encoder.sh 脚本时，请使用反斜杠转义密码中的任何特殊字符。例如，如果您的密码是 *pa$word*，请将反斜杠置于美元符号 ($) 字符之前，以便脚本可以正常运行。正确的命令行是：
      ./MD5Encoder.sh pa\$word
   c. 复制生成的加密密码，并将其粘贴至 users.xml 文件的第二行中。

   例如，

   ```
   <user password="5b5ab9639b79259f54bc39515540aeaf" name="john"/>
   ```

   有关示例语法，请参阅加密密码的 users.xml 语法 (p. 36)。

6. 设置纯文本密码并让 Introscope 自动生成加密密码。

   a. 在 *users.xml* 文件中设置 *plaintextPasswords="true"*。

   重要信息！如果设置了 *plainTextPasswords="true"*，Introscope 将对每个密码进行加密。请将所有密码设置为纯文本，否则 Introscope 会对已经加密的密码进行加密。

   b. 将每个用户的密码设置为纯文本。

   例如，

   ```
   <user password="John Jones Password" name="john"/>
   ```

   企业管理器下次读取 *users.xml* 文件时（在启动时或在对用户进行身份验证时），将执行以下操作：

   - 企业管理器重写 *users.xml*，并对纯文本密码进行加密。
   - 企业管理器将 *plainTextPasswords* 属性重置为 *false*。

7. 对于其他用户或组，重复步骤 3 定义用户名，并重复步骤 4 为每个用户设置密码。

8. 保存并关闭 *users.xml* 文件。

   更改 *users.xml* 文件的内容不需要重新启动企业管理器。

注意：如果 *users.xml* 文件中有任何错误，企业管理器将不会启动。

用户的 users.xml 语法

```
<users>
    <user password="adb831a7fdd83dd1e2a39ce7591dff8" name="Guest"/>
    <user password="" name="Admin"/>
</users>
```

组的 users.xml 语法

```
<groups>
    <group description="Administrator Group" name="Admin">
        <user name="Admin"/>
    </group>
</groups>
```

使用加密密码的 users.xml 语法

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<principals xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
plainTextPasswords="false" version="0.3"
xsi:noNamespaceSchemaLocation="users0.3.xsd">
    <users>
        <user password="adb831a7fdd83dd1e2a39ce7591dff8" name="Guest"/>
        <user password="" name="Admin"/>
    </users>
    <groups>
        <group description="Administrator Group" name="Admin">
            <user name="Admin"/>
        </group>
    </groups>
</principals>
```

在 domains.xml 中配置 CA Introscope® 域权限

当 CA APM 用户或组登录时，会应用权限。如果在 CA APM 用户或组登录之后进行了更改，那么直到下次尝试登录时才会识别这些更改。这意味着，如果在某个会话期间更改了权限，CA Introscope® 不会终止该会话。

CA Introscope® 权限是动态的；只要进行登录尝试，企业管理器就会检查 *domains.xml* 和 *server.xml* 文件。因此，可以在不重新启动企业管理器的情况下更改权限。

系统按照以下顺序授予用户对域的权限：

- 在指定用户的每个域中列出的所有权限。
- 在用户所属的某个组的每个域中列出的所有权限。

另外，当访问域时，还会应用以下规则：

- 在权限方面，对待*超级域*的方式与对待其他任何域一样。
- 授予用户或组的任何超级域访问权限也允许用户或组在所有用户定义的域中使用这些权限。
- 一个用户或组可以对单个域拥有多个权限。
- 一个用户或组可以在多个域中拥有权限。

请执行以下步骤：

1. 使用 XML 编辑程序，打开 *<EM_Home>/config* 目录中的 *domains.xml* 文件。
2. 对于每个域，使用以下属性定义用户或组的权限。

   注意：如果用户或组有多个权限，请为每个用户/权限对使用一行。

   读取

   用户或组可以查看域中的所有代理和业务逻辑。

   该权限包括如下任务：

   - 查看调查器树（将显示域中用户有权访问的代理）
   - 在 Workstation 控制台中查看显示板
   - 在“调查器预览”窗格中查看度量标准和元素数据，包括调查器树中特定资源的默认前 N 个筛选视图
   - 查看任何管理模块、代理或元素设置
   - 查看报警消息
   - 在历史数据查看器中刷新历史数据和进行缩放
   - 更改历史数据查看器的历史日期范围选项
   - 显示/隐藏图表中的度量标准
   - 在数据查看器中向后或向前移动度量标准
   - 更改组和用户首选项（设置主显示板，显示管理模块名称和显示板名称）

   注意：具有读取权限的用户或组可以查看 Workstation 中的所有命令。但他们无权访问的命令会被禁用。

   写入

   具有写入权限的用户或组不仅可以执行需要读取权限的所有操作，而且还可以：

   - 查看域中的所有代理和业务逻辑
   - 创建和编辑显示板
   - 编辑域中的所有监控逻辑

   run_tracer

   用户或组可以为代理启动事务跟踪会话。

   注意：该权限还需要分配读取权限。

historical_agent_control

用户或组可以安装和卸载代理。

注意：该权限还需要分配读取权限。

live_agent_control

用户或组可以关闭针对某个域中的度量标准、资源和代理的报告

注意：该权限还需要分配读取权限。

dynamic_instrumentation

用户或组可以执行动态检测。

有关动态检测的详细信息，请参阅《*CA APM Java 代理实施指南*》或《*CA APM .NET 代理实施指南*》。

thread_dump

用户或组可以查看和使用“线程转储”选项卡。

有关使用和配置线程转储的信息，请参阅《*CA APM Workstation 用户指南*》和《*CA APM Java 代理实施指南*》。

full

用户或组拥有域的所有可能权限。

注意：所有 XML 标记都区分大小写。

3. 对任何其他用户或组，重复步骤 2（对于每个域，定义...）。
4. 保存并关闭 *domains.xml* 文件。

   CA APM 用户登录时，企业管理器会检查 *domains.xml* 文件，以查看用户是否拥有相应的域权限。

注意：如果 *domains.xml* 文件中有语法错误或其他错误，企业管理器将不会启动。

CA APM 用户和组域权限的默认 domains.xml 语法

在默认域配置中：

- 用户或组 *Admin* 在超级域中拥有完全权限。
- 用户或组 *Guest* 在超级域中拥有读取（仅查看）权限。

注意：SAP 用户或组权限略有不同，如下所示：

- 用户或组 *sapsupport* 在超级域中拥有完全权限。
- 用户或组 *Admin* 在超级域中拥有读取（仅查看）权限。
- 用户或组 *sapsupport* 是“CEM 系统管理员”和“管理员”组的成员，因此被授予对 CEM 控制台的访问权限。

以下是域的用户或组权限的配置语法：

```
<grant group="Admin" permission="full"/>
<grant user="Guest" permission="read"/>
```

可选 CA APM 域配置的 domains.xml 语法

以下配置的域权限示例将域权限授予以下用户：

- bsmith，HRApplication 域中的 *full* 权限
- fjones，HRApplication 域中的 *read* 和 *run_tracer* 权限
- jlo，超级域中的 *write* 权限
- pdiddy，超级域中的 *read* 权限
- swonder，*dynamic_instrumentation* 权限
- cstevens，*线程转储*权限

domains.xml 文件与以下示例类似：

```
<?xml version="1.0" encoding="UTF-8"?>
<domains xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="domains0.3.xsd" version="0.3">
   <domain name="HRApplication" description="">
      <agent mapping="(.*)HRAppAgent(.*)" />
<grant user="bsmith" permission="full" />
<grant user="fjones" permission="read" />
<grant user="fjones" permission="run_tracer" />
<grant user="swonder" permission="dynamic_instrumentation" />
<grant user="cstevens" permission="thread_dump" />
   </domain>
  <SuperDomain>
      <agent mapping="(.*)"/>
      <grant user="jlo" permission="write"/>
      <grant user="pdiddy" permission="read"/>
  </SuperDomain>
</domains>
```

在 server.xml 中配置企业管理器服务器权限

这些服务器权限是为与企业管理器的操作相关的活动定义的。

- 关闭企业管理器
- 发布 MIB 文件
- 访问 APM 状态控制台

请执行以下步骤：

1. 使用 XML 编辑程序，打开位于 *<EM_Home>/config* 目录中的 *server.xml* 文件。
2. 使用以下相应的属性，定义每个 CA APM 用户或组的权限。

   注意：所有 XML 标记都区分大小写。

   shutdown

   用户或组可以关闭企业管理器。

   publish_mib

   用户或组可以将 SNMP 收集数据发布到 MIB。

   为了发布 MIB，用户必须创建 SNMP 收集。该任务要求对保存 SNMP 收集的域具有写入访问权限。

   apm_status_console_control

   用户或组可以看到 APM 状态报警图标，使用 APM 状态控制台，然后运行 APM 状态控制台 CLW 命令。

   注意：想在度量标准浏览器树中查看“活动的限定”度量标准信息的用户，必须具有 domains.xml 超级域权限 (p. 36)。

   full

   用户或组拥有所有可能的企业管理器服务器权限。
3. 对于任何其他用户，重复步骤 2（为每个 CA APM 用户定义权限...）。
4. 保存并关闭 *server.xml* 文件。

   注意：如果 *server.xml* 文件中有语法错误或其他错误，企业管理器将不会启动。

服务器权限的 server.xml 语法

以下是配置服务器用户权限的语法：

```
<grant user="username" permission="full">
```

用户或组可以拥有企业管理器的多个权限。要授予多个权限，请为每个用户/权限对或组/权限对使用一行。

默认服务器配置的 server.xml 语法

在默认服务器配置中，Admin 用户或组拥有完全权限。

可选服务器配置的 server.xml 语法

以下示例显示如何将不同权限授予不同的 CA APM 用户：

- bsmith，*shutdown* 权限
- tjones，*publish_mib* 权限
- cstevens，*apm_status_console_control* 权限

server.xml 文件将如以下示例所示：

```
<?xml version="1.0" encoding="UTF-8"?> <server
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="users0.1.xsd" version="0.1">
<grant user="bsmith" permission="shutdown" />
<grant user="tjones" permission="publish_mib" />
<grant user="cstevens" permission="apm_status_console_control" />
</server>
```

使用 LDAP 保护 Introscope

LDAP 仅支持用户身份验证。如果部署 Introscope 安全设置以便企业管理器直接连接 LDAP 服务器进行身份验证，则必须使用本地安全设置进行授权。在这种情况下，使用本地安全设置进行授权意味着：

- 对于 Introscope，必须在 LDAP 服务器上创建用户和组，然后在 domains.xml 文件中分配权限。
- 对于 CA CEM，必须在 LDAP 服务器上创建用户和所有四个默认安全组。例如，在 LDAP 服务器上，创建 cemadmin 用户以及“CEM 系统管理员”安全组。然后将 cemadmin 分配为“CEM 系统管理员”安全组的成员，从而为 cemadmin 提供“CEM 系统管理员”安全组权限。有关四个 CA CEM 默认安全组的信息，请参阅与默认 CA CEM 安全用户组关联的菜单项和权限 (p. 109)。

注意：如果使用 CA EEM 部署 Introscope 安全，并且 CA EEM 服务器与 LDAP 服务器集成，则可配置 CA EEM 服务器让 LDAP 执行身份验证。在这种情况下，企业管理器不会连接到 LDAP 服务器，并且不知道 LDAP 服务器。有关详细信息，请参阅配置使用 LDAP 的 CA EEM 身份验证 (p. 59)。在这种情况下，Introscope 使用 CA EEM 进行授权。

重要信息！如果使用本地安全进行授权，将无法提供应用程序分类视图安全，也无法在 CA CEM 中设置访问策略以控制选项卡和数据可见性。如果要提供应用程序分类视图，并在 CA CEM 中使用访问策略，必须部署 CA EEM 进行授权。

在设置使用本地授权进行 Introscope LDAP 身份验证之前，了解这种类型的安全设置和权限检查很有用。

Introscope LDAP 身份验证支持以下 v3 LDAP 服务器和各种其他服务器：

- IBM Directory Server（版本 5.1）－有关该配置的示例，请参阅 IBM Directory Server 的 realms.xml 语法 (p. 49)。
- Sun ONE Directory Server（版本 5.1）－有关该配置的示例，请参阅 Sun ONE Directory Server 的 realms.xml 语法 (p. 50)。
- MS Active Directory（Windows 2000 和 2003 版本）－有关该配置的示例，请参阅 MS Active Directory 的 realms.xml 语法 (p. 51)。

现在，您已经了解了 Introscope 安全设置方面的一些背景知识，可以制定您的安全部署计划了。

以下是设置和维护 LDAP 安全性的过程：

1. 在 LDAP 服务器上设置 CA APM 用户和组。
2. 在 *realms.xml* 中添加 LDAP 作为安全领域。
3. 设置本地授权。

关于 LDAP 身份验证

LDAP 身份验证信息在*绑定*操作中提供的。其中客户端通过向 LDAP 服务器发送一个包含身份验证信息的*绑定*操作来发起与该服务器的连接。*绑定*操作中提供的身份验证信息取决于客户端选择的身份验证机制。

发送 LDAP 请求但不执行*绑定*的客户端将被视作匿名客户端。即，如果没有为 *bindName* 属性输入任何值，则不会应用任何身份验证机制，并将忽略其他所有身份验证环境属性。仅当要确保忽略可能已设置的其他所有身份验证属性时，可能才需要明确地这样做。无论哪种情况，客户端都将被视为匿名客户端。这意味着，服务器不知道或不关心客户端是谁，并将允许客户端访问（读取和更新）已配置为任何未经身份验证的客户端均可访问的任何数据。

在 realms.xml 中配置 LDAP 身份验证

本主题说明如何将 LDAP 配置为身份验证方法。

注意：可以使用位于 <*企业管理器主目录*>/examples/authentication 目录中的示例 realms.ldap.xml 配置文件以获取帮助。

在配置 realms.xml 时，请遵循以下规则：

重要信息！ 必须满足以下*所有*规则才能启动企业管理器。

- descriptor= 的值区分大小写。
  - 例如，descriptor=LDAP Realm 不同于 descriptor=ldap realm。
- 对于 LDAP 领域，*descriptor=* 的值必须为 LDAP Realm。
- 对于多个领域，领域标记中的 id= 的值对每个领域必须唯一。例如：

```
<realm descriptor="LDAP Realm" id="LDAP" active="true">
```

请执行以下步骤：

1. 打开 <*企业管理器主目录*>/config 目录中的 realms.xml 文件。
2. 要将 LDAP 配置为您的身份验证方法，请设置以下属性。

   使用 LDAP 身份验证时，只要用户 ID 正确，Introscope 用户便可以使用空密码登录 Workstation。LDAP 身份验证不检查是否缺少密码或存在空密码字段，从而允许用户成功登录。无论是登录到 Workstation 客户端还是 WebView，都会发生此 LDAP 身份验证行为。要确保实施该安全设置，请设置 disallowEmptyPassword 属性。

   注意：每个站点上的 LDAP 服务器配置都是独一无二的。先从 LDAP 管理员处获得 LDAP 配置信息，然后才能尝试配置 LDAP 属性。

   url

   远程 LDAP 服务器的 URL。

   非 SSL 连接的默认端口是 389，SSL 连接的默认端口是 636。

   如果使用的是 SSL，请确保 SSL LDAP 端口包括在服务器 URL 中。

   例如，ldap://host:port。

   useSSL

   是否使用 SSL 连接到远程 LDAP 服务器。

   选项是：true、false。

   bindName

   用于绑定到 LDAP 计算机的名称。如果为空白，则使用匿名绑定。

   例如，IntroscopeLDAPUser。

   bindPassword

   用于绑定到 LDAP 计算机的密码。

   此属性是可选的。

   如果 bindName 字段空白（使用匿名绑定），则将忽略 bindPassword 属性。

plainTextPasswords

指示 bindPassword 是纯文本还是经过加密。此属性是可选的。

如果缺少该属性或该属性设置为 True，则企业管理器假定 *bindPassword* 属性是纯文本。

默认情况下，该值设置为 *True*，即假定密码是纯文本。

企业管理器读取 realms.xml 文件并发现该值设置为 *True* 时，企业管理器会执行以下操作：

- 对 bindPassword 属性纯文本密码进行加密
- 使用加密密码重写 realms.xml
- 将 realms.xml plainTextPasswords 属性设置为 *False*

  如果该值设置为 False，则密码是经过加密的。

重要信息！要启动企业管理器，则此属性必须包含在 realms.xml 文件中。

bindAuthentication

在绑定时使用的身份验证类型。

选项是：none、simple 和 DIGEST-MD5。

baseDN

所有用户对象查询的基本可分辨名称 (DN)。

选项是：cn=Users、dc=dev 和 dc=com。

scopeDepth

查询用户对象时的搜索深度。

usernameAttribute

将与 Introscope 用户名匹配的 LDAP 属性的名称。

例如，userPrincipalName。

userObjectQuery

用于查询用户对象的 LDAP 搜索筛选。在执行查询之前，令牌“%u”使用 Introscope 用户名进行填充。

例如 (&(userPrincipalName=%u)(objectclass=user))。

serverCertificate

证书文件的名称。支持的证书类型是 X.509 和 base64 编码类型。

如果未指定，将使用 JVM 提供的默认证书管理机构（请参阅 http://java.sun.com/j2se/1.5/docs/index.html）。

groupNameAttribute

将与 Introscope 用户名匹配的组属性的名称。

例如，*cn*。

groupObjectQuery

用于查询组对象的 LDAP 搜索筛选。在执行查询之前，令牌“%u”使用 Introscope 组名称进行填充。

例如，(&(objectClass=group)(cn={0}))

groupMemberQuery

用于查询组成员的 LDAP 搜索筛选。在执行查询之前，令牌“%u”使用 Introscope 组成员进行填充。

例如，(&(objectClass=group)(member={0}))。

disallowEmptyPassword

要求用户不得以空密码登录。

disableNestedGroupSearch

在 LDAP 身份验证期间，禁用针对该用户所属组中的嵌套组的 LDAP 递归搜索。设置为 true 可以改进 LDAP 身份验证的性能。

此属性是可选的。

选项是：true、false。默认值为 false。

3. 要应用更改，请保存对 realms.xml 文件所做的更改，然后重新启动企业管理器。

注意：在以下情况下升级任务后，请以手工方式更新绝对路径：

- 如果在升级期间重命名了 Introscope 目录。
- 属性文件使用绝对路径来引用 Introscope 目录中的文件。

为了避免发生这种情况，请使用相对路径来引用 Introscope 根目录内的任何文件。

启用 LDAP 身份验证的 realms.xml 语法

以下是用于配置启用 LDAP 的安全领域的示例 *realms.xml* 语法。

```
<?xml version="1.0" encoding="UTF-8"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">

    <realm active="true" descriptor="LDAP Realm" id="LDAP">
        <!-- 为远程 LDAP 服务器设置 URL。-->
        <!-- url 的格式为：ldap://server:port -->
        <property name="url">
            <value>ldap://myActiveDirectoryServer.mydomain.com:389</value>
        </property>
        <!-- 指示是否使用 SSL 连接到远程 LDAP 服务器。-->
        <property name="useSSL">
            <value>false</value>
        </property>
        <!-- 可将 bindName 设置为一个名称或一个空字符串；      -->
        <!-- 或者可将其注释掉。如果指定名称，         -->
        <!-- 则将使用它绑定到 LDAP 服务器。如果未指定   -->
        <!-- 名称（空字符串）或属性本身       -->
        <!-- 已被注释掉，则会发生匿名绑定。-->
        <property name="bindName">
            <value>CN=Automatic Binding
User,OU=Groups,DC=myDomain,DC=com</value>
        </property>
        <!-- 如果进行匿名绑定，则将忽略 bindPassword -->
        <!-- 属性。否则，该属性会         -->
        <!-- 设置绑定到 LDAP 服务器时要使用的密码。-->
        <property name="bindPassword">
            <value>secretPassword</value>
        </property>
        <!-- 如果 bindPassword 是纯文本，则设置为 true -->
        <!-- 如果 plainTextPasswords 设置为 true，企业管理器将覆盖该文件，  -->
        <!-- 对密码进行加密并将 plainTextPasswords 设置为 false -->
        <!-- 该属性是可选属性 -->
        <!-- 默认值为 true -->
        <property name="plainTextPasswords">
            <value>true</value>
        </property>
        <!-- 设置进行绑定时要使用的身份验证类型。-->
        <!-- 有效值：none|simple|Digest-MD5                    -->
        <!-- 请注意，在 Introscope 8.0 中，DIGEST-MD5 支持已替换为 -->
        <!-- Digest-MD5 支持。-->
        <property name="bindAuthentication">
            <value>simple</value>
        </property>
```

```
    <!-- 可将 nameSuffix 设置为一个后缀或空字符串;     -->
    <!-- 或者可将其注释掉。如果定义了后缀,          -->
    <!-- 则在处理 LDAP 查询时会将该值     -->
    <!-- 附加到 Introscope 用户名后面。如果未指定      -->
    <!-- 后缀(空字符串)或属性本身       -->
    <!-- 已被注释掉,则不会向用户名 -->
    <!-- 附加名称后缀。-->
 <!--
    <property name="nameSuffix">
        <value>@dev.com</value>
    </property>
 -->
    <!-- 为所有用户对象查询设置基本 DN。-->
    <property name="baseDN">
        <value>DC=myDomain,DC=com</value>
    </property>
    <!-- 设置查询用户对象时的搜索深度。-->
    <!-- 有效值:onelevel|subtree                          -->
    <property name="scopeDepth">
        <value>subtree</value>
    </property>
    <!-- 设置 LDAP 属性的名称        -->
    <!-- 该名称将与一个 Introscope 用户名匹配。-->
    <property name="usernameAttribute">
        <value>cn</value>
    </property>
    <!-- 设置用来查询用户对象的"LDAP 搜索筛选"。-->
    <!-- 在执行查询之前,令牌"%u"和"{0}"(无引号)将     -->
    <!-- 使用 Introscope 用户名进行填充。-->
    <!-- 必须对查询中的所有 XML 特殊字符进行转义:              -->
    <!--    使用 &amp;amp; 表示与号 &                          -->
    <!--    使用 &amp;lt; 表示左尖括号("小于")字符          -->
    <!--    使用 &amp;gt; 表示右尖括号("大于")字符      -->
    <!--    使用 &amp;quot; 表示引号 "                        -->
    <!--    使用 &amp;apos; 表示撇号 '                        -->
    <property name="userObjectQuery">
        <value>(&(objectClass=organizationalPerson)(cn={0}))</value>
    </property>
    <!-- (可选)设置 LDAP 属性的名称  -->
    <!-- 以用作组名称。-->
<!--
    <property name="groupNameAttribute">
       <value>cn</value>
    </property>
-->
    <!-- (可选)设置搜索筛选以与成员的 LDAP 组匹配。-->
    <!-- 令牌"%u"和"{0}"(无引号)将替换为        -->
    <!-- 成员的可分辨名称。-->
    <!-- 必须对查询中的所有 XML 特殊字符进行转义。请参阅         -->
    <!-- 以上 userObjectQuery 属性的注释。-->
```

```
        <!--
            <property name="groupMemberQuery">

<value>(&(objectClass=groupOfUniqueNames)(uniquemember=%u))</value>
            </property>
        -->
            <!-- 设置用来匹配 LDAP 组名称的搜索筛选。-->
            <!-- 在执行查询之前，令牌“%g”和“{0}”（无引号）        -->
            <!-- 将替换为组名称。-->
            <!-- 必须对查询中的所有 XML 特殊字符进行转义。请参阅          -->
            <!-- 以上 userObjectQuery 属性的注释。-->
        <!--
            <property name="groupObjectQuery">
                <value>(&(objectClass=groupOfUniqueNames)(cn=%g))</value>
            </property>
        -->
            <!-- 在使用 SSL 时，请指定 LDAP 服务器 -->
            <!-- 证书的完整路径名（如果可用）。-->
        <!-- 不必对反斜线进行转义。-->
        <!--
            <property name="serverCertificate">
                <value>C:\path\to\my\cert\cert.cer</value>
            </property>
        -->
            property name="disallowEmptyPassword">
                <value>true</value>
            </property>
    </realm>
</realms>
```

具有不同证书的多个 LDAP 服务器的 realms.xml 语法

可以对 realms.xml 进行配置，以便在多个 LDAP 服务器具有不同的不兼容证书时正确地进行绑定。

在此示例中，一台名为 host1 且对 SSL 使用端口 636 的 LDAP 主机将执行 LDAP 身份验证。主机 1 具有一个证书，该证书在 realms.xml 中称为 host1.pem。您需要再添加一台名为 host2 的主机，该主机也使用端口 636。在 realms.xml 中，主机 2 证书为 host2.pem，它与 host1.pem 证书不兼容。

如果将 serverCertificate 值配置为 host1.pem，则主机 1 可以执行绑定操作，但主机 2 不能执行绑定操作。如果将 serverCertificate 值配置为 host2.pem，则主机 2 可以执行绑定操作，但主机 1 不能执行绑定操作。

要避免此问题，请按此示例所示配置 realms.xml。

```
<property name="url">
<value>ldap://host1.net:636 ldap://host2.net:636</value>
</property>

<property name="serverCertificate">
    <VALUE>CONFIG/host1.PEM</VALUE>
    <VALUE>CONFIG/host2.PEM</VALUE>
</property>
```

在该配置中，主机 1 和主机 2 都可以执行绑定操作。

IBM Directory Server 的 realms.xml 语法

以下 *realms.xml* 示例显示了配置为通过 SSL 与 IBM Directory Server 一起使用的 LDAP 属性。

注意：以下示例代码仅供举例说明之用；每个站点的 LDAP 服务器配置都是唯一的。

```
<?xml version="1.0" encoding="UTF-8"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">
<realm active="true" descriptor="LDAP Realm" id="LDAP">
<property name="url">
<value>ldap://machine01.co.com:123</value>
</property>
<property name="serverCertificate">
<value/>
</property>
<property name="bindPassword">
<value>jon</value>
</property>
<property name="useSSL">
<value>false</value>
</property>
<property name="userObjectQuery">
<value>(&(objectClass=organizationalPerson)(cn={0})) </value>
</property>
<property name="groupNameAttribute">
          <value>cn</value>
       </property>
       <property name="groupObjectQuery">
          <value>(&(objectClass=organizationalUnit)(cn={0}))</value>
       </property>
       <property name="groupMemberQuery">
          <value>(&(objectClass=groupofNames)(member={0}))</value>
       </property>
```

```
<property name="bindAuthentication">
<value>simple</value>
</property>
<property name="bindName">
<value>cn=Jon Doe,ou=Groups,o=unitTest</value>
</property>
<property name="usernameAttribute">
<value>cn</value>
</property>
<property name="scopeDepth">
<value>subtree</value>
</property>
</realm>
</realms>
```

Sun ONE Directory Server 的 realms.xml 语法

以下 *realms.xml* 示例显示了配置为通过 SSL 与 Sun ONE Directory Server 一起使用的 LDAP 属性。

注意：以下示例代码仅供举例说明之用；每个站点的 LDAP 服务器配置都是唯一的。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">
    <realm active="true" id="Introscope LDAP Realm" descriptor="LDAP Realm">
        <property name="bindName">
           <value>uid=User01,ou=Users,dc=co,dc=com</value>
        </property>
        <property name="scopeDepth">
           <value>subtree</value>
        </property>
        <property name="baseDN">
           <value>DC=co,DC=com</value>
        </property>
        <property name="bindPassword">
           <value>jim</value>
        </property>
        <property name="url">
           <value>ldap://123serv01.company.com:389</value>
        </property>
        <property name="usernameAttribute">
           <value>cn</value>
        </property>
        <property name="userObjectQuery">
           <value>(&(objectClass=organizationalPerson)(cn={0}))</value>
        </property>
        <property name="groupNameAttribute">
           <value>cn</value>
        </property>
```

```
        <property name="groupObjectQuery">
           <value>(&(objectClass=group)(cn={0}))</value>
        </property>
        <property name="groupMemberQuery">
           <value>(&(objectClass=group)(member={0}))</value>
        </property>
        <property name="useSSL">
           <value>false</value>
        </property>
        <property name="bindAuthentication">
           <value>simple</value>
        </property>
        <property name="serverCertificate">
           <value/>
        </property>
    </realm>
</realms>
```

MS Active Directory 的 realms.xml 语法

以下 *realms.xml* 示例显示了配置为通过 SSL 与 MS Active Directory 一起使用的 LDAP 属性。

注意：以下示例代码仅供举例说明之用；每个站点的 LDAP 服务器配置都是唯一的。

```
<?xml version="1.0" encoding="UTF-8"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">

<realm active="true" descriptor="LDAP Realm" id="LDAP">
<property name="url">
<value>ldap://123serv01.company.com:389:389</value>
</property>
<property name="serverCertificate">
<value/>
</property>
<property name="bindPassword">
<value>Password4bindPassword</value>
</property>
<property name="useSSL">
<value>false</value>
</property>
<property name="userObjectQuery">
<value>(&(objectClass=organizationalPerson)(cn={0})) </value>
</property>
<property name="baseDN">
<value>DC=ad-dev-02,DC=com</value>
</property>
```

```
<property name="bindAuthentication">
<value>simple</value>
</property>
<property name="bindName">
<value>CN=Jon Doe,cn=Users,DC=ad-dev-02,DC=com</value>
</property>
<property name="usernameAttribute">
<value>cn</value>
</property>
<property name="scopeDepth">
<value>subtree</value>
</property>
</realm>
</realms>
```

使用 CA EEM 保护 Introscope

CA EEM 是一种 CA Technologies 企业级策略服务器，其他应用程序借助它来共享通用的访问策略管理、身份验证和授权服务。它包括支持多个 Embedded Entitlements 客户端应用程序的集中式 Embedded Entitlements Server。

有关更多信息，请参阅 CA EEM 应用程序随附的以下 CA EEM 指南，可从 CA Support 站点 http://www.ca.com/wily/support 下载这些指南：

- *《CA Embedded Entitlements Manager 入门指南》*
- *《CA Embedded Entitlements Manager 编程指南》*
- *《CA Embedded Entitlements Manager 版本说明》*

CA EEM 部署选项

可以使用 CA EEM 通过多种方式设置 Introscope 安全设置：

- 部署 CA EEM 进行身份验证和授权。有关详细信息，请参阅在 realms.xml 中配置 CA EEM 身份验证 (p. 56)和配置 CA EEM 授权 (p. 60)。
- 如果已经设置了 CA EEM 服务器与 LDAP 服务器集成，则可使用 LDAP 进行身份验证，使用 CA EEM 进行授权。有关详细信息，请参阅配置使用 LDAP 的 CA EEM 身份验证 (p. 59)。

- 如果已经设置了 CA EEM 服务器与 LDAP SiteMinder 集成，则可使用 SiteMinder 进行身份验证，使用 CA EEM 进行授权。有关详细信息，请参阅“配置使用 CA SiteMinder 的 CA EEM 身份验证”。
- 部署 CA EEM 仅用于身份验证，使用本地安全设置进行授权。有关详细信息，请参阅将 CA EEM 配置为使用本地授权 (p. 95)。

注意：CA APM 提供 EEM 8.4 SP4 SDK，并且已使用 EEM 服务器版本 8.4 SP4 及更高版本进行认证。

重要信息！如果使用本地安全进行授权，将无法提供应用程序分类视图安全，也无法在 CA CEM 中设置访问策略以控制选项卡和数据可见性。如果要提供应用程序分类视图，并在 CA CEM 中使用访问策略，必须部署 CA EEM 进行授权。

设置和维护 CA EEM 安全性的过程

现在，您已经拥有了一些 Introscope 安全设置的背景知识，可以规划您的 Introscope CA EEM 安全部署了。以下是要执行的高级步骤。

请执行以下步骤：

1. 安装 CA EEM 服务器。请参阅安装 CA EEM (p. 55)。
2. （可选）配置 *IntroscopeEnterpriseManager.properties* 文件以提供 CA EEM 日志消息。请参阅配置 CA EEM 相关消息的日志记录 (p. 55)。
3. 在每个企业管理器上，将 CA EEM 定义为安全领域，并在位于 *<EM_Home>/config* 目录中的 *realms.xml* 文件内设置身份验证和授权属性。请参阅在 realms.xml 中配置 CA EEM 身份验证 (p. 56)。

   注意：如果 CA EEM 服务器与 LDAP 或者 CA SiteMinder Web Access Manager (SiteMinder) 服务器集成，则可以将 CA EEM 配置为使用 LDAP 或 SiteMinder 对用户进行身份验证。
4. （可选）配置 LDAP 进行 CA EEM 身份验证。请参阅配置使用 LDAP 的 CA EEM 身份验证 (p. 59)。
5. （可选）配置 SiteMinder 进行 CA EEM 身份验证。请参阅配置使用 CA SiteMinder 的 CA EEM 身份验证 (p. 59)。
6. （可选，但建议执行）加载在 *<EM_Home>/examples/authentication* 目录中提供的 *eem.register.app.xml* 和 *eem.add.global.identities.xml* 脚本。请参阅配置 CA EEM 授权 (p. 60)。

   注意：CA Technologies 提供了示例脚本，这些脚本可创建具有默认 APM 应用程序用户和组、资源及权限的 APM 应用程序。CA Technologies 建议使用这些脚本执行下面的步骤 7 到步骤 10。有关详细信息，请参阅配置 CA EEM 授权 (p. 60)。

7. 在 CA EEM 中创建一个或多个 APM 应用程序。请参阅在 CA EEM 中注册 APM 应用程序 (p. 65)。
8. 在 CA EEM 中创建 APM 组和用户及其权限。请参阅在 CA EEM 中创建和删除 APM 组 (p. 68)以及在 CA EEM 中创建和删除 APM 用户 (p. 72)。
9. 在 CA EEM 中创建 APM 资源类及其权限。请参阅在 CA EEM 中创建和删除 APM 资源类 (p. 76)。
10. 在 CA EEM 中创建 APM 域、服务器和 APM 应用序程资源及其权限。请参阅创建和删除 CA EEM APM 域资源访问策略 (p. 83)、创建和删除 CA EEM APM 服务器资源访问策略 (p. 86)。创建和删除 CA EEM APM 前端和业务服务资源访问策略 (p. 89)。
11. 重新启动企业管理器。
12. 根据需要，通过执行以下任务添加并维护基于 CA EEM 的安全设置：
    - 配置日志消息以报告 CA EEM 活动和错误。请参阅配置 CA EEM 相关消息的日志记录 (p. 55)。
    - 配置 CA EEM 服务器与 LDAP 或 SiteMinder 集成以进行 CA EEM 身份验证。请参阅配置使用 LDAP 的 CA EEM 身份验证 (p. 59)或配置使用 CA SiteMinder 的 CA EEM 身份验证 (p. 59)。
    - 定义多个领域。例如，使用 CA EEM 领域进行身份验证，使用本地领域进行授权。请参阅将 CA EEM 配置为使用本地授权 (p. 95)。
    - 修改 CA APM 脚本或创建自己的脚本。请参阅配置 CA EEM 授权 (p. 60)。
    - 添加和删除 APM 应用程序。请参阅在 CA EEM 中注册 APM 应用程序 (p. 65)。
    - 添加、编辑和删除 APM 组及其权限。请参阅在 CA EEM 中创建和删除 APM 组 (p. 68)。
    - 添加、编辑和删除 APM 用户及其权限。请参阅在 CA EEM 中创建和删除 APM 用户 (p. 72)。
    - 添加、编辑和删除 APM 资源类及其权限。请参阅在 CA EEM 中创建和删除 APM 资源类 (p. 76)。
    - 添加、编辑和删除 APM 域资源及其权限：
        - 在 CA EEM 中。请参阅创建和删除 CA EEM APM 域资源访问策略 (p. 83)。
        - 对于本地授权，请在 *domains.xml* 文件中更新。请参阅在 domains.xml 中配置 Introscope 域权限 (p. 36)。

- 添加、编辑和删除企业管理器服务器资源及其权限：
  - 在 CA EEM 中。请参阅创建和删除 CA EEM APM 服务器资源访问策略 (p. 86)。
  - 对于本地授权，请在 *server.xml* 文件中更新。配置企业管理器服务器权限 (p. 39)。
- 添加、编辑和删除企业管理器应用程序资源及其权限。请参阅创建并删除 CA EEM APM 前端和业务服务资源访问策略 (p. 89)。

安装 CA EEM

CA EEM 是一个独立的服务器组件，可以安装在与企业管理器相同的计算机上。有关 CA EEM 要求，请参阅《*CA Embedded Entitlements Manager 版本说明*》。

有关安装 CA EEM 的信息，请参阅《*CA APM 安装和升级指南*》。有关其他 CA EEM 安装信息，请参阅以下随 CA EEM 产品安装文件提供的 CA EEM 指南：

- 《*CA Embedded Entitlements Manager 入门指南*》。
- 《*CA Embedded Entitlements Manager 版本说明*》。

重要信息！可以配置 CA EEM 以处理 CA EEM 数据存储和服务器故障切换。有关详细信息，请参阅《*CA Embedded Entitlements Manager 入门指南*》。

CA EEM 服务器提供 Safex 实用工具，可用于将 APM 应用程序、用户和组数据导入 CA EEM。有关详细信息，请参阅配置 CA EEM 授权 (p. 60)。

（可选）配置 CA EEM 相关消息的日志记录

可以更新 IntroscopeEntrerpriseManager.properties 文件以提供详细的 CA EEM 日志消息，该日志消息可以帮助排除 CA EEM 错误。例如，如果用户进行 CA EEM 登录失败，或没有为该用户设置权限等情况。

请执行以下步骤：

1. 导航到 <EM_Home>/config 目录。
2. 打开 IntroscopeEntrerpriseManager.properties 文件。
3. 将以下属性添加到 IntroscopeEntrerpriseManager.properties 文件中：

```
log4j.logger.Manager.EemRealm=DEBUG
log4j.logger.additivity.Manager.EemRealm=false
```

4. 保存并关闭 IntroscopeEntrerpriseManager.properties 文件。

   可以在 <企业管理器主目录>/logs/IntroscopeEnterpriseManager.log 文件的日志消息以及任何调试消息中查看 CA EEM 连接信息。日志消息显示 CA EEM 中企业管理器连接到的应用程序和 CA EEM 服务器的位置。如果已将 CA EEM 服务器配置为使用 SiteMinder 或外部目录（LDAP 领域）来获得用户和组，系统也会对此予以记录。

   例如：

   ```
   8/05/09 04:15:59 PM PDT [INFO] [Manager.EemRealm] EEM realm attached to
   application "APM" in EEM server at <EEM_Machine_Name> using SiteMinder
   ```

在 realms.xml 中配置 CA EEM 身份验证

在 *realms.xml* 文件中将 CA EEM 配置成安全领域时，Introscope 将使用 CA EEM 进行身份验证。

由于每个组织的 CA EEM 服务器配置都独一无二，因此必须先获得 CA EEM 配置信息，然后才能尝试配置 *realms.xml* CA EEM 属性。如果没有安装 CA EEM，请联系您所在组织的 CA EEM 管理员来获得该信息。另外，您还必须确认您要对其进行身份验证的 CA APM 用户拥有 CA EEM 服务器上定义的权限。有关在 CA EEM 服务器上设置 CA APM 用户的信息，请参阅“在 CA EEM 中创建和删除 APM 用户 (p. 72)”。

在配置 *realms.xml* 时，请遵循以下规则：

重要信息！如果未满足所有这些规则，企业管理器不会启动。

- *descriptor=* 的值区分大小写。
  - 例如，*descriptor=EEM Realm* 不同于 *descriptor=eem realm*
- 对于 EEM 领域，*descriptor=* 的值必须为 *EEM Realm*。
- 在有多个领域的情况下，领域标记中的 *id=* 的值对每个领域必须唯一。例如：
  - *<realm descriptor="EEM Realm" id="EEM Server 1" active="true">*
  - *<realm descriptor="EEM Realm" id="EEM Server 2" active="true">*

在有些情况下，可以设置多个领域，例如，需要一个默认领域授予用户基本权限，需要另外一个领域授予不同权限的情况。或者，组织可能有两个 LDAP 服务器，您想测试两者的安全性。或者，组织可能一直在使用本地安全设置，而且您希望在移动到 CA EEM 时将其保留在适当位置。

如果 *realms.xml* 配置不正确，企业管理器会显示错误消息。例如，

```
4/13/10 03:06:32.960 PM PDT [ERROR] [main] [Manager] The EM failed to start.
Invalid realm descriptor in the EEM realm descriptor: eem realm
```

请执行以下步骤：

注意：有关基于名为 *APM* 的应用程序的示例 EEM 领域，请参阅位于 *<EM_Home>/examples/authentication* 目录中的示例 *realms.eem.xml* 配置文件。

1. 打开位于 *<EM_Home>/config* 目录中的 *realms.xml* 文件。
2. 适当设置以下属性。

   注意：通过将 *enableAuthorization* 属性保留为其默认值 *true*，可以使用 CA EEM 服务器进行身份验证和授权。如果该值设置为 *false*，则 CA EEM 仅执行身份验证，而使用本地安全领域进行授权。在有些情况下，您可能会选择使用本地授权，例如，要使用配置为使用 LDAP 或 SiteMinder 进行身份验证的 CA EEM，但将权限保留在本地领域中。

   主机

   CA EEM 服务器的主机名。此属性是可选的。

   appname

   CA EEM 中企业管理器附加到的 APM 应用程序的名称。此属性是必需属性。

   username

   要连接到 CA EEM 服务器的用户名。此属性是可选的。

   CA EEM 默认值为 *EiamAdmin*。

   password

   用于连接到 CA EEM 服务器的密码。此属性是必需属性。

   CA EEM 默认值为 *EiamAdmin*。

   plainTextPasswords

   指示将密码保存为纯文本形式还是加密形式。此属性是必需属性。

   企业管理器读取 *realms.xml* 文件并发现该值设为 *True* 时，它会执行以下操作：

   - 为纯文本密码加密
   - 使用加密密码重写 *realms.xml*
   - 将 *realms.xml plainTextPasswords* 属性设置为 *False*

   如果该值设为 *False*，则假定密码是经过加密的。

重要信息！如果该属性未包含在 *realms.xml* 文件中，则企业管理器不会启动，并显示一条错误消息。

enableAuthorization

启用 CA EEM 作为授权机制。此属性是可选的。

默认情况下，该值设为 *True*，即，使用 CA EEM 进行身份验证和授权。

如果该值设为 *False*，则 CA EEM 仅用于身份验证，而使用本地授权。

3. 保存 *realms.xml* 文件。
4. 重新启动企业管理器以应用 *realms.xml* 更改。

启用 CA EEM 身份验证的 realms.xml 语法示例

以下内容是在 *realms.xml* 中配置启用 CA EEM 的安全领域的语法：

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<realms xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="realms0.1.xsd">
    <realm descriptor="EEM Realm" id="EEM" active="true">
        <!-- 设置 EEM 服务器的主机名 -->
        <!-- 该属性是可选属性 -->
        <!-- 默认值为 localhost -->
            <value>localhost</value>
        </property>
        <!-- 设置要连接到的 EEM 应用程序的名称 -->
        <!-- 该属性是必需属性 -->
        <!--
        <property name="appname">
            <value>MyIntroscopeApp</value>
        </property>
        -->
        <!-- 设置要连接到 EEM 服务器的用户名称 -->
        <!-- 该属性是可选属性 -->
        <!-- 默认值为 EiamAdmin -->
        <property name="username">
            <value>EiamAdmin</value>
        </property>
        <!-- 设置连接到 EEM 服务器的密码 -->
        <!-- 该属性是必需属性 -->
        <property name="password">
            <value>EiamAdmin</value>
        </property>
        <!-- 如果密码是纯文本，则设置为 true -->
        <!-- 如果 plainTextPasswords 设置为 true，企业管理器将覆盖该文件， -->
        <!-- 对密码进行加密并将 plainTextPasswords 设置为 false -->
        <!-- 该属性是必需属性 -->
        <property name="plainTextPasswords">
            <value>true</value>
        </property>
```

```
        <!-- 启用 EEM 服务器中的授权 -->
        <!-- 如果设为 false，EEM 服务器将仅可用来进行身份验证 -->
        <!-- 该属性是可选属性 -->
        <!-- 默认值为 true -->
        <property name="enableAuthorization">
            <value>true</value>
        </property>
    </realm>
</realms>
```

配置使用 LDAP 的 CA EEM 身份验证

如果 CA EEM 服务器与 CA EEM 支持的 LDAP 服务器集成，则可将 CA EEM 配置为使用 LDAP 服务器进行身份验证。在这种情况下，用户和组均来自 LDAP。在将 CA EEM 服务器与 LDAP 服务器集成进行身份验证时，不需要在 Introscope 中执行任何其他配置。有关 Introscope 支持的 LDAP 服务器的信息，请参阅使用 LDAP 保护 Introscope (p. 41)。

注意：无法将 CA EEM 配置为同时与多个外部目录进行集成，例如，同时与 LDAP 和 SiteMinder 集成。

如果配置使用 LDAP 的 CA EEM 身份验证，则需要部署 CA EEM 进行授权。有关详细信息，请参阅配置 CA EEM 授权 (p. 60)。

请执行以下步骤：

1. 设置并配置支持 CA EEM 的 LDAP 服务器，例如，SUNONE LDAP 服务器。
2. 在 LDAP 用户目录中添加用户和组。

   注意：在将 CA EEM 服务器连接到外部用户目录（如 LDAP）时，将无法在 CA EEM 中创建或添加全局用户。
3. 在“CA EEM 配置”选项卡中，配置 CA EEM 以连接到您的 LDAP 或 Active Directory 服务器。

   有关详细信息，请参阅《*CA Embedded Entitlements Manager 入门指南*》和《*CA Embedded Entitlements Manager 编程指南*》中与 LDAP 相关的主题。

配置使用 CA SiteMinder 的 CA EEM 身份验证

SiteMinder 是一个集中的 Web 访问管理系统，支持以下内容：

- 用户身份验证和单点登录
- 身份验证管理

- 基于策略的授权
- 身份联合
- 审核对 Web 应用程序和门户的访问

您可以将 CA EEM 配置为使用 SiteMinder 进行身份验证。在这种情况下，用户和组均来自 SiteMinder。如果 CA EEM 服务器与 SiteMinder 进行了集成以进行身份验证，则不需要在 Introscope 中执行任何其他配置。

如果配置使用 SiteMinder 的 CA EEM 身份验证，您会部署 CA EEM 进行授权。有关详细信息，请参阅配置 CA EEM 授权 (p. 60)。

注意：不能将 CA EEM 配置为同时与多个外部目录进行集成，例如，同时与 SiteMinder 和 LDAP 集成。

请执行以下步骤：

1. 在 SiteMinder 用户目录中添加用户和组。

   注意：在将 CA EEM 服务器连接到外部用户目录（如 SiteMinder）后，将无法在 CA EEM 中创建或添加全局用户。

2. 在“CA EEM 配置”选项卡中，配置 CA EEM 以连接到 SiteMinder。

   注意：有关 CA EEM 与 SiteMinder 集成的详细信息，请参阅以下指南中的相关主题：

   - *《CA Embedded Entitlements Manager 入门指南》*
   - 《*CA Embedded Entitlements Manager 版本说明*》。

   注意：有关部署示例，请参阅知识库文章 TEC534187: CA Wily APM security example: CA SiteMinder for authentication with CA EEM for authorization（CA Wily APM 安全示例：使用 CA SiteMinder 进行身份验证，使用 CA EEM 进行授权）。

配置 CA EEM 授权

如果将 CA EEM 用作授权领域，则必须在 CA EEM 服务器上配置 APM 应用程序以及 APM 用户、组和权限。可以通过以下方法之一实现该操作：

- CA EEM Safex 实用工具

  Safex 是 CA EEM 提供的命令行界面 (CLI) 实用工具。Safex 运行 XML 脚本以在 CA EEM 中注册应用程序并创建用户和组。

  CA APM 提供了一个示例 Safex 脚本，该脚本可创建具有默认的 APM 全局用户、资源和权限的 APM 应用程序。
  也可以使用 Safex 脚本将数据从 CA EEM 导出到 xml 文件。有关详细信息，请参阅《*CA Embedded Entitlements Manager 编程指南*》。

- CA EEM 界面

  有关使用 CA EEM 界面的信息，请参阅《*CA Embedded Entitlements Manager 入门指南*》和《*CA Embedded Entitlements Manager 联机帮助*》。

  有关部署示例，请参阅知识库文章 TEC534188: CA Wily APM security example: Setting up CA Wily APM users, groups, and resources in CA EEM（CA Wily APM 安全性设置示例：在 CA EEM 中设置 CA Wily APM 用户、组和资源）。

访问 CA EEM 界面：

如果您具有访问权限，则可以登录到 CA EEM 以配置 APM 应用程序以及 APM 用户、组和权限。

- 在 CA EEM 中登录到 APM 应用程序。

  a. 在 CA EEM 登录页面上，从“应用程序:”下拉列表中单击 APM 或您注册的应用程序的名称。

  b. 输入登录名和密码。

  APM 应用程序的默认登录名为 *EiamAdmin*。

以非 FIPS 模式配置 APM-CA EEM 集成：

注意：可以使用 EEM 安装位置处的 igateway.conf 文件中的 <FIPSMode>OFF</FIPSMode> 将 FIPS 模式设置为“OFF”，以非 FIPS 模式设置 EEM 服务器。此文件的默认安装位置是 C:\ProgramFiles\CA\SharedComponents\iTechnology。

1. 配置 eiam.config 和 eiam.log4j.config 文件。
   - 在 <EM install>\config 目录中打开 eiam.config 和 eiam.log4j.config 文件。
   - 确认 FIPS 模式已设为 OFF 并显示为 <FIPSMode>OFF</FIPSMode>。默认模式为“OFF”。
2. 将摘要算法设置为下列任一算法：
   - MD5（默认）
   - SHA1
   - SHA256
   - SHA384
   - SHA512

   此时 APM-EEM 集成将配置为非 FIPS 模式。

以 FIPS 模式配置 APM-CA EEM 集成：

注意：可以使用 EEM 安装位置处的 igateway.conf 文件中的 <FIPSMode>ON</FIPSMode> 将 FIPS 模式设置为“ON”，以 FIPS 模式设置 EEM 服务器。此文件的默认安装位置是 C:\Program Files\CA\SharedComponents\iTechnology。

1. 配置 eiam.config 和 eiam.log4j.config 文件。
   - 在 <EM install>\config 目录中打开 eiam.config 和 eiam.log4j.config 文件。
   - 通过将 <FIPSMode>OFF</FIPSMode> 更改为 <FIPSMode>ON</FIPSMode>，将 FIPS 模式设置为 ON。
2. 将摘要算法设置为下列任一算法：
   - SHA1
   - SHA256
   - SHA384
   - SHA512

   此时 APM-EEM 集成将配置为 FIPS 模式。

配置 CA EEM 授权：

重要信息！如果将 CA EEM 用于授权，则企业管理器必须附加到 CA EEM 中的至少一个应用程序。CA EEM 使用应用程序来存储定义权限的访问策略和资源类。

重要信息！在将 CA EEM 服务器连接到外部用户目录（如 LDAP 或 SiteMinder）后，将无法在 CA EEM 中创建或添加全局用户。如果 CA EEM 服务器与 LDAP 或 SiteMinder 服务器集成进行身份验证，则可以在 LDAP 或 SiteMinder 中（而非 CA EEM 中）设置用户和组，或在 LDAP 或 SiteMinder 中更改用户和组 CA EEM 访问策略。

重要信息！*eem.register.app.xml* 脚本不包括设置配置为使用 LDAP 或 SiteMinder 进行身份验证的 CA EEM 的示例代码。

请执行以下步骤：

1. 配置 *realms.xml* 文件进行 CA EEM 授权。
   a. 打开位于 *<EM_Home>/config* 目录中的 *realms.xml* 文件。
   b. 确认 *appname* 属性设置为 CA EEM 中企业管理器将附加到的 APM 应用程序的名称。例如，*APM*。

      使用在步骤 2a 中配置 CA EEM 服务器时所使用的相同应用程序名称。

c. 确认 *enableAuthorization* 属性设置为 *True*。

d. 保存 *realms.xml* 文件。

e. 重新启动企业管理器以应用 *realms.xml* 更改。

2. 创建并运行一个或多个 Safex 脚本，用于加载 APM 应用程序、组、用户、资源类、域和服务器资源。

CA Technologies 在 *<EM_Home>/examples/authentication* 目录中提供了以下 Safex 脚本示例：

eem.register.app.xml

注册默认的 APM 应用程序。

eem.unregister.app.xml

注销默认的 APM 应用程序。

eem.add.global.identities.xml

添加默认的 APM 全局用户。

eem.remove.global.identities.xml

删除默认的 APM 用户。

注意：CA Technologies 建议修改 *eem.register.app.xml* 和 *eem.add.global.identities.xml*，以用作设置 CA EEM 授权部署的基本脚本。运行这些脚本可满足设置 CA EEM 授权所需的要求。

a. 在 Safex 脚本中配置以下 CA EEM 安全元素。

- 应用程序。请参阅在 CA EEM 中注册 APM 应用程序 (p. 65)
- 组。请参阅在 CA EEM 中创建和删除 APM 组 (p. 68)
- 用户。请参阅在 CA EEM 中创建和删除 APM 用户 (p. 72)

注意：CA EEM 不支持空密码，因此每次在 CA EEM 中创建用户时都必须提供密码。

- 资源类。请参阅在 CA EEM 中创建和删除 APM 资源类 (p. 76)
- 域资源权限。请参阅在 CA EEM 中创建和删除 APM 资源类 (p. 76)
- 服务器资源权限。请参阅创建和删除 CA EEM APM 服务器资源访问策略 (p. 86)

b. 可选：如果不使用 *eem.register.app.xml* 文件作为 CA EEM 配置脚本的基础，请使用 CA EEM 界面配置 CA EEM 服务器来满足以下条件：

- 创建两个资源类：*域资源类*和*服务器资源类*。

  资源类必须具有与 Introscope 中可用权限匹配的操作列表。例如，对于服务器权限，Introscope 操作是 *shutdown*、*publish_mib* 和 *full*。有关详细信息，请参阅创建和删除 CA EEM APM 域资源访问策略 (p. 83)以及创建和删除 CA EEM APM 服务器资源访问策略 (p. 86)。

- 创建一组策略。策略定义资源类、一个或多个操作、一个或多个身份以及零个或更多资源。
  - 资源是某个特定资源的名称，例如*超级域*。如果没有指定任何资源，则策略将应用于该资源类的所有实例。*服务器资源类*的策略不应有资源，因为该资源类是孤立的。
  - *Identity* 是组的名称。
- 使用前缀 *ug:* 指定特定于应用程序的用户组，如果适用于您的部署，可以使用 *gug:* 指定全局用户组。

3. 导航到 *<EEM_Server>* 目录，该目录一般位于以下位置：

   ```
   C:\Program Files\CA\SharedComponents\iTechnology
   ```

4. 在命令提示符下，运行以下命令：

   ```
   C:\Program Files\CA\SharedComponents\iTechnology\safex.exe -h hostname -u
   username -p password -f <mySafexScriptname>.xml
   ```

   例如，

   ```
   C:\Program Files\CA\SharedComponents\iTechnology\safex.exe -h hostname -u
   username -p password -f eem.register.app.xml
   ```

   该脚本会运行并加载到您定义的 CA EEM 配置值中。

5. 登录到 CA EEM 并查看 APM 应用程序、组、用户、资源类以及域和服务器资源，还有关联的权限。

   a. 单击“配置”选项卡可查看 APM 应用程序的列表。

   b. 单击“管理身份”选项卡可查看 APM 组和用户。

   c. 单击“管理访问策略”选项卡可查看 APM 资源类以及域和服务器资源。

在 CA EEM 中注册 APM 应用程序

在 CA EEM 中至少注册一个应用程序以用于 Introscope 安全设置。在 CA EEM 中注册应用程序时，会创建一个应用程序实例，用于存储用户详细信息和访问策略。有关使用用户和应用程序的信息，请参阅以下 CA EEM 文档：

- *《CA Embedded Entitlements Manager 入门指南》*
- *《CA Embedded Entitlements Manager 联机帮助》*
- *《CA Embedded Entitlements Manager 编程指南》*

CA APM 提供了默认的 Safex 脚本，用于以名称 *APM* 注册 CA EEM 应用程序。

重要信息！要在 CA EEM 中注册应用程序，请使用 Safex 脚本。不能使用 CA EEM 用户界面注册应用程序。

注意：有关创建名为 *APM* 的应用程序的 Safex 脚本代码，请参阅位于 *<EM_Home>/examples/authentication* 目录中的 *eem.register.app.xml* 示例文件。

以非 FIPS 模式在 CA EEM 中注册 APM 应用程序：

1. 在 *<EEM_Server>* 目录中创建 Safex xml 文件，该目录通常位于 *C:\Program Files\CA\SharedComponents\iTechnology* 目录下。

   例如，

   ```
   C:\Program Files\CA\SharedComponents\iTechnology \Register_APM.xml。
   ```

2. 剪切该代码并将其粘贴到 Safex xml 文件中，然后用您的变量替代引号中的变量。

   ```
   <Safex>
      <!-- 附加为全局用户 -->
      <Attach/>
      <!-- 注册 “APM” 应用程序 -->
      <Register certfile="APM.p12" password="Enter Your Password">
         <ApplicationInstance name="APM" label="APM">
         </ApplicationInstance>
      </Register>
      <Detach/>
   </Safex>
   ```

3. 打开命令提示符并导航到 *<EEM_Server>* 目录，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

4. 要运行 Safex 脚本，请运行以下命令：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f <yourfilename>.xml
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f Register_APM.xml
   ```

5. 在 CA EEM 中查看 APM 应用程序。

   a. 使用脚本中提供的管理员名称和密码登录到 CA EEM。

      例如，用户名：*EiamAdmin*，密码：*<password>*。

      注意：CA EEM 提供 *EiamAdmin* 作为默认全局权限管理员用户名。

   b. 要查看 APM 应用程序的列表，请单击“配置”选项卡。

   c. 要查看或编辑该应用程序的信息，请单击应用程序名称，例如 APM。

以 FIPS 模式在 CA EEM 中注册 APM 应用程序：

重要信息！要在 CA EEM 中注册应用程序，请使用 Safex 脚本。不能使用 CA EEM 用户界面注册应用程序。

注意：有关创建名为 APM 的应用程序的 Safex 脚本代码，请参阅位于 <EM_Home>/examples/authentication 目录中的 eem.register.app.xml 示例文件。

1. 在 <EEM_Server> 目录中创建 Safex xml 文件，该目录通常位于 C:\Program Files\CA\SharedComponents\iTechnology 目录下。

   例如，

   ```
   C:\Program Files\CA\SharedComponents\iTechnology \Register_APM.xml。
   ```

2. 剪切该代码并将其粘贴到 Safex xml 文件中，然后用您的变量替代引号中的变量。

   ```
   <Safex>
   <!-- 附加为全局用户 -->
   <Attach/>
   <!-- 注册“APM”应用程序 -->
   <Register certtype="pem" certfile="APM.pem" keyfile="APM.key">
   <ApplicationInstancxxle name="APM" label="APM">
   </ApplicationInstance>
   </Register>
   <Detach/>
   </Safex>
   ```

3. 打开命令提示符并导航到 <EEM_Server> 目录，该目录通常为 C:\Program Files\CA\SharedComponents\iTechnology。

4. 要运行 Safex 脚本，请运行以下命令：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f <yourfilename>.xml
   -fips
   ```

例如，

```
>safex.exe -h localhost -u EiamAdmin -p <password> -f Register_APM.xml -fips
```

5. 在 CA EEM 中查看 APM 应用程序。
   - 使用脚本中提供的管理员名称和密码登录到 CA EEM。

     例如，用户名：EiamAdmin，密码：<password>。

     注意：CA EEM 使用 EiamAdmin 作为默认全局权限管理员用户名。
   - 要查看 APM 应用程序的列表，请单击“配置”选项卡。
   - 要查看或编辑该应用程序的信息，请单击应用程序名称。例如，APM。

在 CA EEM 中注销 APM 应用程序

在 CA EEM 中注销某个应用程序时，将从 CA EEM 服务器中删除该应用程序以及所有相关的用户和组。

注意：您也可以使用 CA EEM 界面执行这些任务。有关详细信息，请参阅《*CA Embedded Entitlements Manager 入门指南*》、《*CA Embedded Entitlements Manager 联机帮助*》、《*CA Embedded Entitlements Manager 编程指南*》。

请执行以下步骤：

注意：有关注销名为 APM 的应用程序及其用户和组的 Safex 脚本代码，请参阅位于 *<EM_Home>/examples/authentication* 目录中的 *eem.unregister.app.xml* 示例文件。

1. 在 *<EEM_Server>* 目录中创建 Safex XML 文件，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

   例如，*C:\Program Files\CA\SharedComponents\iTechnology\Unregister_APM.xml*。
2. 剪切此代码并将其粘贴到 Safex XML 文件中，然后使用您的变量替代引号中的变量。

```
<Safex>
   <!-- 附加为全局用户 -->
   <Attach/>

   <!-- 取消注册“APM”应用程序 -->
<UnRegister>
     <ApplicationInstance name="APM" label="APM"/>
  </UnRegister>
</Safex>
```

3. 打开命令提示符并导航到 *<EEM_Server>* 目录，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

4. 通过以下命令来运行 Safex 脚本：

```
>safex.exe -h localhost -u EiamAdmin -p <password> -f <yourfilename>.xml
```

例如，

```
>safex.exe -h localhost -u EiamAdmin -p <password> -f Unregister_APM.xml
```

如果要以 FIPS 模式在 CA EEM 中取消注册 APM 应用程序，请运行以下命令以运行 Safex 脚本：

```
>safex.exe -h localhost -u EiamAdmin -p <password> -f <yourfilename>.xml
-fips
```

例如，

```
>safex.exe -h localhost -u EiamAdmin -p <password> -f Unregister_APM.xml
-fips
```

5. 在 CA EEM 中查看 APM 应用程序。

   a. 登录到 CA EEM。

   b. 单击“配置”选项卡可查看 APM 应用程序的列表。

   注销的 APM 应用程序会被删除，不会列出。所有相关的用户和组也会被删除。

在 CA EEM 中创建和删除 APM 组

CA EEM 提供两个用户组级别：

- 特定于应用程序的组，这些组获得特定于允许其访问的应用程序的权限。特定于应用程序的组不会与其他应用程序共享权限。

  注意：默认 CA APM CA EEM 安全是使用特定于应用程序的组部署的。

- 全局用户组，这些组获得所有权限，因为它们可以访问向 CA EEM 注册的所有应用程序。

注意：在将 CA EEM 服务器连接到外部用户目录（如 LDAP 或 SiteMinder）时，将无法在 CA EEM 中创建或添加全局组。如果 CA EEM 服务器与 LDAP 或 SiteMinder 服务器集成进行身份验证，请在 LDAP 或 SiteMinder 中（而非 CA EEM 中）设置组。

CA EEM 支持嵌套组；在嵌套组中，子组从其父组继承权限。因此，不需要为子组分配权限。但是，可以为子组定义额外的权限。

要查看 CEM 控制台，CA APM 用户必须拥有为至少一个 CEM 资源定义的访问策略才能成功授权。CA APM 用户必须在至少一个域中拥有读取权限，才能查看调查器树和控制台。如果 CA APM 用户要查看 CEM 控制台以及调查器树和控制台，则必须同时满足这两个要求。

注意：有关添加默认 APM 用户的 Safex 脚本代码，请参阅位于 *<EM_Home>/examples/authentication* 目录中的 *eem.add.global.identities.xml* 示例文件。

注意：如果已经将 CA EEM 配置为使用 LDAP 或 SiteMinder 进行身份验证，并且已经在 LDAP 或 SiteMinder 服务器上创建了用户和组，则不需要将 APM 组添加到 CA EEM 中。只需要使用 Safex 脚本注册 APM 应用程序。请参阅在 CA EEM 中注册 APM 应用程序 (p. 65)。

注意：您也可以使用 CA EEM 界面执行这些任务。有关详细信息，请参阅《*CA Embedded Entitlements Manager 入门指南*》、《*CA Embedded Entitlements Manager 联机帮助*》、《*CA Embedded Entitlements Manager 编程指南*》。

使用 Safex 实用工具创建 APM 组：

1. 在 *<EEM_Server>* 目录中创建 Safex XML 文件，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

   例如，*C:\Program Files\CA\SharedComponents\iTechnology\Add_Groups.xml*。

2. 剪切该代码并将其粘贴到 Safex xml 文件中，然后使用您的变量替代引号中的变量并配置其他相应的值。

   注意：请使用前缀 *ug:* 指定特定于应用程序的用户组，如果适用于您的部署，可以使用 *gug:* 指定全局用户组。

```
<Safex>
   <!-- 附加为全局用户 -->
   <Attach/>
   <!-- 添加用户组 -->
   <Add>
         <Folder name="/APM" />

         <UserGroup name="Admin" folder="/">
              <Description>Administrator Group</Description>
         </UserGroup>

         <UserGroup name="Guest" folder="/">
              <Description>Guest Group</Description>
         </UserGroup>
      </Add>
      <Detach/>
</Safex>
```

3. 打开命令提示符并导航到 *<EEM_Server>* 目录，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

4. 通过以下命令来运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f <yourfilename>.xml
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f
   eem.add.global.identities.xml
   ```

   如果要为以 FIPS 模式与 CA EEM 集成的 APM 应用程序创建组，请运行以下命令以运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f <yourfilename>.xml
   -fips
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p <password> -f
   eem.add.global.identities.xml -fips
   ```

5. 在 CA EEM 中查看组。

   a. 登录到 CA EEM。

   b. 单击“管理身份”选项卡。

   c. 单击“组”链接。

   d. 在“搜索组”窗口中，选中“显示应用程序组”复选框，然后单击“执行”。

      CA EEM 会在“用户组”窗口中显示 APM 组的列表。

   e. 单击组名称链接可在“用户组”窗口中查看有关该组的更多信息。

使用 Safex 实用工具删除 APM 组：

注意：在删除某个组之前，请先删除该组内的用户。如果有其他组引用要删除的组，请取消引用。

1. 在 *<EEM_Server>* 目录中创建 Safex XML 文件，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

   例如，*C:\Program Files\CA\SharedComponents\iTechnology\Remove_Group.xml*。

2. 剪切此代码并将其粘贴到 Safex XML 文件中，然后使用您的变量替代引号中的变量并配置其他相应的值。

   注意：请使用前缀 *ug:* 指定特定于应用程序的用户组，如果适用于您的部署，可以使用 *gug:* 指定全局用户组。

```
<Safex>
   <!-- 附加为全局用户 -->
   <Attach/>
<!-- 删除全局用户和组 -->
   <Remove>
            <GlobalUserGroup name="Admin" folder="/"/>
            <GlobalUserGroup name="Guest" folder="/"/>
            <GlobalFolder name="/APM" />
   </Remove>
   <Detach/>
</Safex>
```

3. 打开命令提示符并导航到 *<EEM_Server>* 目录，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

4. 通过以下命令来运行 Safex 脚本：

```
>safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
<yourfilename>.xml
```

   例如，

```
>safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_Group.xml
```

   如果要为以 FIPS 模式与 CA EEM 集成的 APM 应用程序删除组，请运行以下命令以运行 Safex 脚本：

```
>safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
<yourfilename>.xml -fips
```

   例如，

```
>safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_Group.xml -fips
```

5. 在 CA EEM 中查看 APM 组。

   a. 登录到 CA EEM。

   b. 单击“管理身份”选项卡。

   c. 单击“组”链接。

   d. 在“搜索组”窗口中，选中“显示应用程序组”复选框，然后单击“执行”。

   CA EEM 会在“用户组”窗口中显示 APM 组的列表。删除的 APM 组不会列出。

在 CA EEM 中创建和删除 APM 用户

CA EEM 具有两种类型的用户：

- 特定于应用程序的用户，这些用户会获得特定于允许其访问的应用程序的权限。
- 全局用户，其可以访问 CA EEM 中注册的所有应用程序。如果向某个全局用户分配特定于应用程序的用户组的成员资格，则该全局用户将成为特定于应用程序的用户。

使用 CA APM 的 Safex 脚本添加到 CA EEM 中的 APM 全局用户以及特定应用程序的用户，都会设置为 CA EEM 中特定应用程序组的成员。要成功进行 CA EEM 授权，APM 用户不需要成为 CA EEM 中某个组的成员。但是，如果 APM 用户不是 CA EEM 中某个组的成员，则他们必须拥有已定义的访问策略才能编辑任何资源（如域或服务器）。

注意：如果您已将 CA EEM 配置为使用 LDAP 或 SiteMinder 进行身份验证，并且已在 LDAP 或 SiteMinder 服务器上创建了用户和组，则不需要将 APM 用户添加到 CA EEM 中。只需要使用 Safex 脚本注册 APM 应用程序。请参阅在 CA EEM 中注册 APM 应用程序 (p. 65)。

注意：在将 CA EEM 服务器连接到外部用户目录（如 LDAP 或 SiteMinder）时，将无法在 CA EEM 中创建或添加全局用户。但是，您将能够为外部（LDAP 或 SiteMinder）用户目录中的用户添加特定于应用程序的详细信息。如果您的 CA EEM 服务器与 LDAP 或 SiteMinder 服务器进行了集成以进行身份验证，请在 LDAP 或 SiteMinder 中（而非 CA EEM 中）设置用户。

注意：有关添加默认 APM 全局用户的 Safex 脚本代码，请参阅 *eem.add.global.identities.xml* 示例文件。有关将 APM 全局用户添加到 APM 应用程序特定组中的 Safex 脚本代码的信息，请参阅 *eem.register.app.xml* 示例文件。这两个文件都位于 *<EM_Home>/examples/authentication* 目录中。

注意：您也可以使用 CA EEM 界面执行这些任务。有关详细信息，请参阅《*CA Embedded Entitlements Manager 入门指南*》、《*CA Embedded Entitlements Manager 联机帮助*》、《*CA Embedded Entitlements Manager 编程指南*》。

重要信息！ CA EEM 不支持空密码，因此每次在 CA EEM 中创建用户时都必须提供密码。

使用 Safex 实用工具创建 APM 用户：

1. 在 *<EEM_Server>* 目录中创建 Safex XML 文件，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

   例如，*C:\Program Files\CA\SharedComponents\iTechnology\Add_Users.xml*。

2. 剪切该代码并将其粘贴到 Safex xml 文件中，然后使用您的变量替代引号中的变量并配置其他相应的值。

```
<Safex>
   <!-- 附加为全局用户 -->
   <Attach/>

   <!-- 添加全局用户 -->
   <Add>
         <GlobalUser name="admin" folder="/APM">
               <UserName>admin</UserName>
               <DisplayName>Admin</DisplayName>
               <!-- 不允许使用空密码 -->
               <Password>admin</Password>
               <FirstName>APM</FirstName>
               <LastName>Admin</LastName>
               <WorkPhoneNumber>1-888-888-8888</WorkPhoneNumber>
               <EmailAddress>support@yourcompany.com</EmailAddress>
               <GroupMembership>Admin</GroupMembership>
         </GlobalUser>

         <GlobalUser name="guest" folder="/APM">
               <UserName>guest</UserName>
               <DisplayName>Guest</DisplayName>
               <Password>guest12</Password>
               <FirstName>APM</FirstName>
               <LastName>Guest</LastName>
               <WorkPhoneNumber>1-888-888-8888</WorkPhoneNumber>
               <EmailAddress>support@yourcompany.com</EmailAddress>
               <GroupMembership>Guest</GroupMembership>
         </GlobalUser>

   <!-- 将用户添加到组 -->
   <User folder="/APM" name="guest">
   <GroupMembership>Guest</GroupMembership>
   </User>
   <User folder="/APM" name="admin">
   <GroupMembership>Admin</GroupMembership>
   </User>

   </Add>
   <Detach/>
</Safex>
```

3. 打开命令提示符并导航到 *<EEM_Server>* 目录，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。
4. 通过以下命令来运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_Users.xml
   ```

   如果要为以 FIPS 模式与 CA EEM 集成的应用程序创建 APM 用户，请运行以下命令以运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_Users.xml -fips
   ```

5. 在 CA EEM 中查看 APM 用户。
   a. 登录到 CA EEM。
   b. 单击“管理身份”选项卡。
   c. 单击“用户”链接。
   d. 在“搜索用户”窗口中，设置任何属性、运算符或值搜索项，然后单击“执行”。

      CA EEM 将在“用户”窗口中显示 APM 用户的列表。
   e. 单击 APM 用户名链接，以便在“用户详细信息”窗口中查看更多信息。

使用 Safex 实用工具删除 APM 用户：

注意：有关删除默认 APM 全局用户的 Safex 脚本代码，请参阅 *eem.remove.global.identities.xml* 示例文件。有关删除 APM 应用程序（包括特定于应用程序的用户）的 Safex 脚本代码，请参阅 *eem.unregister.app.xml* 示例文件。这两个文件都位于 *<EM_Home>/examples/authentication* 目录中。

1. 在 *<EEM_Server>* 目录中创建 Safex XML 文件，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

   例如，*C:\Program Files\CA\SharedComponents\iTechnology\Remove_User.xml*。

2. 剪切此代码并将其粘贴到 Safex XML 文件中，然后使用您的变量替代引号中的变量并配置其他相应的值。

```
<Safex>
   <!-- 附加为全局用户 -->
   <Attach/>
<!-- 删除全局用户和组 -->
  <Remove>
        <GlobalUser name="admin" folder="/APM"/>
        <GlobalUser name="guest" folder="/APM"/>
        <GlobalFolder name="/APM" />
   </Remove>
   <Detach/>
</Safex>
```

3. 打开命令提示符并导航到 *<EEM_Server>* 目录，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

4. 通过以下命令来运行 Safex 脚本：

```
>safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
<yourfilename>.xml
```

   例如，

```
>safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_User.xml
```

   如果要为以 FIPS 模式与 CA EEM 集成的应用程序删除 APM 用户，请运行以下命令以运行 Safex 脚本：

```
>safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
<yourfilename>.xml -fips
```

   例如，

```
>safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_User.xml -fips
```

5. 在 CA EEM 中查看 APM 用户。

   a. 登录到 CA EEM。

   b. 单击“管理身份”选项卡。

c. 单击“用户”链接。

d. 在“搜索用户”窗口中，设置任何属性、运算符或值搜索项，然后单击“执行”。

CA EEM 将在“用户”窗口中显示 APM 用户的列表。删除的 APM 用户将不会再列出。

在 CA EEM 中创建并删除 APM 资源类

每次注册新应用程序时，可能都需要定义 APM 资源类。Introscope 至少需要域和服务器资源类。如果使用 CA CEM，则必须定义特定于 CA CEM 的资源类。有关 CA CEM CA EEM 安全的详细信息，请参阅 CA CEM 的 CA EEM 身份验证和授权 (p. 111)。

重要信息！ 对于 CA APM 安全设置，必须使用固定的 APM 资源类和权限名称。

对于每个 APM 资源类，必须提供关联的权限（在 CA EEM 中称为*操作*）。

注意： 有关创建具有默认资源类且名为 *APM* 的应用程序的 Safex 脚本代码，请参阅位于 *<EM_Home>/examples/authentication* 目录中的 *eem.register.app.xml* 示例文件。

注意： 您也可以使用 CA EEM 界面执行这些任务。有关详细信息，请参阅《*CA Embedded Entitlements Manager 入门指南*》、《*CA Embedded Entitlements Manager 联机帮助*》、《*CA Embedded Entitlements Manager 编程指南*》。

使用 Safex 实用工具创建 APM 资源类：

1. 在 *<EEM_Server>* 目录中创建 Safex XML 文件，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

   例如，*C:\Program Files\CA\SharedComponents\iTechnology\Add_resource_classes.xml*。

2. 确定域资源类权限。

   读取

   用户或组可以查看域中的所有代理和业务逻辑。

   该权限包括如下任务：

   - 查看调查器树（将显示域中用户有权访问的代理）
   - 在 Workstation 控制台中查看显示板
   - 在“调查器预览”窗格中查看度量标准和元素数据，包括调查器树中特定资源的默认前 N 个筛选视图

- 查看任何管理模块、代理或元素设置
- 查看报警消息
- 在历史数据查看器中刷新历史数据和进行缩放
- 更改历史数据查看器的历史日期范围选项
- 显示/隐藏图表中的度量标准
- 在数据查看器中向后或向前移动度量标准
- 更改组和用户首选项（设置主显示板，显示管理模块名称和显示板名称）

注意：具有读取权限的用户或组可以查看 Workstation 中的所有命令。但他们无权访问的命令会被禁用。

写入

具有写入权限的用户或组不仅可以执行需要读取权限的所有操作，而且还可以：

- 查看域中的所有代理和业务逻辑
- 创建和编辑显示板
- 编辑域中的所有监控逻辑

run_tracer

用户或组可以为代理启动事务跟踪会话。

注意：该权限还需要分配读取权限。

historical_agent_control

用户或组可以安装和卸载代理。

注意：该权限还需要分配读取权限。

live_agent_control

用户或组可以关闭针对某个域中的度量标准、资源和代理的报告

注意：该权限还需要分配读取权限。

dynamic_instrumentation

用户或组可以执行动态检测。

有关动态检测的详细信息，请参阅《*CA APM Java 代理实施指南*》或《*CA APM .NET 代理实施指南*》。

thread_dump

用户或组可以查看和使用“线程转储”选项卡。

有关使用和配置线程转储的信息，请参阅《*CA APM Workstation 用户指南*》和《*CA APM Java 代理实施指南*》。

full

用户或组拥有域的所有可能权限。

有关配置 APM 域的信息，请参阅 Introscope 安全设置和权限概述 (p. 27)。

3. 确定服务器资源类权限。

shutdown

用户或组可以关闭企业管理器。

publish_mib

用户或组可以将 SNMP 收集数据发布到 MIB。

为了发布 MIB，用户必须创建 SNMP 收集。该任务要求对保存 SNMP 收集的域具有写入访问权限。

apm_status_console_control

用户或组可以看到 APM 状态报警图标，使用 APM 状态控制台，然后运行 APM 状态控制台 CLW 命令。

注意：想在度量标准浏览器树中查看“活动的限定”度量标准信息的用户，必须具有 domains.xml 超级域权限 (p. 36)。

full

用户或组拥有所有可能的企业管理器服务器权限。

4. 确定业务服务资源类权限以提供应用程序分类视图安全设置。

写入、读取以及读取敏感数据

Introscope 用户和组可以查看应用程序分类视图上的业务服务。

注意：可以使用任何 CA EEM 权限查看应用程序分类视图上的业务服务。在这种情况下，系统默认提供这三种权限。

注意：如果更改查看业务服务的用户权限，则在用户注销并再次登录到 Workstation 之前，这些更改不会反映在应用程序分类视图中。

5. 确定业务应用程序资源类权限，以便为前端提供应用程序分类视图安全设置。

   写入

   Introscope 用户和组可以在应用程序分类视图上查看前端。

   注意：超级域安全设置将覆盖应用程序分类视图安全设置。有关详细信息，请参阅超级域安全设置将覆盖应用程序分类视图安全设置 (p. 99)。

   注意：CA APM CA EEM 安全设置使用业务应用程序资源类为视图前端提供安全设置。

   注意：可以使用任何 CA EEM 权限在视图上查看前端。在这种情况下，系统默认仅提供写权限。

   注意：如果您更改了用户权限以查看视图前端，则只有当用户注销并再次登录到 Workstation 之后，这些更改才会反映在应用程序分类视图上。

6. 剪切从 <ResourceClass> 开始到 </ResourceClass> 结束的代码并将其粘贴到 Safex XML 文件中，然后用您的变量替代资源类和权限，并配置其他相应的值。

   注意：在 CA EEM 中，权限称为操作。

```
<Safex>
   <!-- 附加为全局用户 -->
   <Attach/>
   <!-- 注册“APM”应用程序  -->
   <Register certfile="APM.p12" password="EiamAdmin">
      <ApplicationInstance name="APM" label="APM">
            <Brand>Introscope</Brand>
            <MajorVersion>1</MajorVersion>
            <MinorVersion>0</MinorVersion>
            <Description>APM Application</Description>
            <ResourceClass>
               <Name>Domain</Name>
               <Action>read</Action>
               <Action>write</Action>
               <Action>run_tracer</Action>
               <Action>historical_agent_control</Action>
               <Action>dynamic_instrumentation</Action>
               <Action>live_agent_control</Action>
               <Action>Thread_Dump</Action>
               <Action>full</Action>
            </ResourceClass>
```

```
                <ResourceClass>
                    <Name>Server</Name>
                    <Action>shutdown</Action>
                    <Action>publish_mib</Action>
                    <Action>apm_status_console_control</Action>
                    <Action>full</Action>
                </ResourceClass>
                <ResourceClass>
                    <Name>Business Service</Name>
                    <Action>write</Action>
                    <Action>read</Action>
                    <Action>read sensitive data</Action>
                </ResourceClass>
                <ResourceClass>
                    <Name>Business Application</Name>
                    <Action>write</Action>
                </ResourceClass>

            </ApplicationInstance>
        </Register>
        <Detach/>
</Safex>
```

注意：设置应用程序分类视图用户权限必须要有*业务服务*和*业务应用程序*资源类。如果没有设置权限，则所有用户都可以看到所有前端。业务应用程序资源类提供查看特定前端所需的权限。

7. 打开命令提示符并导航到 *<EEM_Server>* 目录，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

8. 通过以下命令来运行 Safex 脚本：

```
>safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
<yourfilename>.xml
```

例如，

```
>safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_resource_classes.xml
```

如果要为以 FIPS 模式与 CA EEM 集成的应用程序创建 APM 资源类，请运行以下命令以运行 Safex 脚本：

```
>safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
<yourfilename>.xml -fips
```

例如，

```
>safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_resource_classes.xml
-fips
```

9. 在 CA EEM 中查看 APM 资源类。
   a. 登录到 CA EEM。
   b. 单击“管理访问策略”选项卡。
   c. 单击“策略”链接。

   CA EEM 会列出针对资源类的策略。

使用 Safex 实用工具删除 APM 资源类：

1. 在 *<EEM_Server>* 目录中创建 Safex XML 文件，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

   例如，*C:\Program Files\CA\SharedComponents\iTechnology\Remove_Resource_class.xml*。

2. 剪切此代码并将其粘贴到 Safex XML 文件中，然后使用您的变量替代引号中的变量并配置其他相应的值。

```
<Safex>
   <!-- 附加为全局用户 -->
   <Attach/>

<!-- 删除资源类 -->
      <ApplicationInstance name="APM" label="APM">
      <Remove>
               <ResourceClass>
                  <Name>Business Service</Name>
                  <Action>write</Action>
                  <Action>read</Action>
                  <Action>read sensitive data</Action>
            </ResourceClass>
     </Remove>
   </ApplicationInstance>
   <Detach/>
</Safex>
```

3. 打开命令提示符并导航到 *<EEM_Server>* 目录，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。
4. 通过以下命令来运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_Resource_class.xml
   ```

   如果要为以 FIPS 模式与 CA EEM 集成的应用程序删除 APM 资源类，请运行以下命令以运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_Resource_class.xml
   -fips
   ```

5. 在 CA EEM 中查看 APM 资源类。
   a. 登录到 CA EEM。
   b. 单击“管理访问策略”选项卡。
   c. 单击“策略”链接。

   已删除的资源类不会列出。

关于 CA EEM 访问策略

CA EEM 访问策略反映了授予组对特定资源（如域、服务器、前端和业务服务）执行特定操作的权限。这意味着，为业务服务和前端（在 CA EEM 中称为业务应用程序）提供访问策略的业务安全会影响应用程序分类视图，但不会影响代理。但是，域安全设置会影响代理，却不会影响应用程序分类视图。

将某个全局用户添加到特定于应用程序的用户组中后，该用户将获取授予该组的资源权限。

例如，以下为 CA APM Safex 脚本代码段，可使全局用户 Admin 成为“CEM 系统管理员”应用程序特定用户组的成员：

```
<User folder="/APM" name="cemadmin"><GroupMembership>CEM System
Administrator</GroupMembership><GroupMembership>Admin</GroupMembership>
</User>
```

CA APM Safex 脚本后面为以下代码段，用于设置 CA EEM 应用程序资源访问策略：

```
        <Policy name="Business Application write" folder="/Policies">
        <Description>CEM System Administrator Group and CEM Configuration
Administrator Group have write permission for all Business
Applications.</Description>
        <ResourceClassName>Business Application</ResourceClassName>
        <Action>write</Action>
        <Identity>ug:CEM Configuration Administrator</Identity>
        <Identity>ug:CEM System Administrator</Identity>
       </Policy>
```

策略定义中的这行代码段授予“CEM 系统管理员”用户组访问应用程序资源的权限：

```
ug:CEM System Administrator
```

由于 Admin 是“CEM 系统管理员”用户组的成员，因此 Admin 也有权在应用程序分类视图上查看前端。

前端上的安全适用于分类视图树。这意味着，除非用户有权限，否则就看不到分类视图树中的前端节点。但是，视图安全不适用于度量标准浏览器树（用户可在其中查看所有前端和度量标准）。

创建和删除 CA EEM APM 域资源访问策略

该主题讨论如何在 CA EEM 中保护 CA APM 域。例如，超级域或者已定义的某个域。因此，要提供域安全设置，需要为*超级域*和任何用户定义的域添加 CA EEM 访问策略作为 CA EEM 域资源，这样才能设置域权限。

注意：对于本地安全设置，域权限是在 *domains.xml* 文件中配置的。有关详细信息，请参阅在 domains.xml 中配置 Introscope 域权限 (p. 36)。对于 CA EEM 安全设置，*domains.xml* 中的域权限将被忽略，而改为在 CA EEM 中设置域权限。

注意：有关创建具有域资源默认访问策略且名为 *APM* 的应用程序的 Safex 脚本代码，请参阅位于 *<EM_Home>/examples/authentication* 目录中的 *eem.register.app.xml* 示例文件。

注意：您也可以使用 CA EEM 界面执行这些任务。有关详细信息，请参阅《*CA Embedded Entitlements Manager 入门指南*》、《*CA Embedded Entitlements Manager 联机帮助*》、《*CA Embedded Entitlements Manager 编程指南*》。

使用 Safex 实用工具创建 CA EEM APM 域资源访问策略：

1. 在 *<EEM_Server>* 目录中创建 Safex XML 文件，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

   例如，*C:\Program Files\CA\SharedComponents\iTechnology\Add_domains.xml*。

2. 剪切该代码并将其粘贴到 Safex XML 文件中，然后使用您的变量替代引号中的变量，以及身份、资源类和权限的值。有关域权限，请参阅在 CA EEM 中创建和删除 APM 资源类 (p. 76)中的步骤 2（确定每个资源类允许的权限...）。

   注意：在 CA EEM 中，权限称为操作。

```
<Safex>
   <Attach label="APM"/>
   <!-- 添加策略 -->
   <Add>
        <Policy name="Domain Admin" folder="/Policies">
        <Description>Admin group has full permission for all
domains</Description>
        <Identity>gug:Admin</Identity>
        <Action>full</Action>
        <ResourceClassName>Domain</ResourceClassName>
        <Resource>SuperDomain</Resource>
        </Policy>
     </Add>
     <Detach/>
</Safex>
```

3. 打开命令提示符并导航到 *<EEM_Server>* 目录，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

4. 通过以下命令来运行 Safex 脚本：

```
>safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
<yourfilename>.xml
```

例如，

```
>safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_domains.xml
```

如果要使用 Safex 实用工具为以 FIPS 模式与 CA EEM 集成的应用程序创建 CA EEM APM 域资源访问策略，请运行以下命令以运行 Safex 脚本：

```
>safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
<yourfilename>.xml -fips
```

例如，

```
>safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_domains.xml- fips
```

5. 在 CA EEM 中查看 APM 域。
   a. 登录到 CA EEM。
   b. 单击“管理访问策略”选项卡。
   c. 单击“策略”链接。
   d. 在“搜索策略”窗口中，单击“显示匹配资源的策略”，从“资源类名称”下拉列表中选择“域”，然后单击“执行”。

   CA EEM 在“策略表”窗口中显示 APM 域资源访问策略的列表。

使用 Safex 实用工具删除 CA EEM APM 域资源访问策略：

1. 在 *<EEM_Server>* 目录中创建 Safex XML 文件，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

   例如，*C:\Program Files\CA\SharedComponents\iTechnology\Remove_domain.xml*。

2. 剪切该代码并将其粘贴到 Safex XML 文件中，然后使用您的变量替代引号中的变量，以及身份、资源类和权限的值。有关域权限，请参阅在 CA EEM 中创建和删除 APM 资源类 (p. 76)中的步骤 2（确定每个资源类允许的权限...）。

   注意：在 CA EEM 中，权限称为操作。

```
<Safex>
   <Attach label="APM"/>
   <Remove>
        <Policy name="Domain Guest" folder="/Policies"/>
   </Remove>
   <Detach/>
</Safex>
```

3. 打开命令提示符并导航到 *<EEM_Server>* 目录，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

4. 通过以下命令来运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_domain.xml
   ```

   如果要使用 Safex 实用工具为以 FIPS 模式与 CA EEM 集成的应用程序删除 CA EEM APM 域资源访问策略，请运行以下命令以运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_domain.xml -fips
   ```

5. 在 CA EEM 中查看 APM 域。

   a. 登录到 CA EEM。

   b. 单击“管理访问策略”选项卡。

   c. 单击“策略”链接。

   d. 在“搜索策略”窗口中，单击“显示匹配资源的策略”，从“资源类名称”下拉列表中选择“域”，然后单击“执行”。

   CA EEM 在“策略表”窗口中显示 APM 域资源访问策略的列表。已删除的 APM 域资源访问策略不会列出。

创建和删除 CA EEM APM 服务器资源访问策略

需要添加 CA EEM APM 服务器资源的访问策略才能设置服务器权限。

注意：有关创建具有服务器资源默认访问策略且名为 APM 的应用程序的 Safex 脚本代码，请参阅 *eem.register.app.xml* 示例文件，该文件位于 *<EM_Home>/examples/authentication* 目录中。

注意：您也可以使用 CA EEM 界面执行这些任务。有关详细信息，请参阅《*CA Embedded Entitlements Manager 入门指南*》、《*CA Embedded Entitlements Manager 联机帮助*》、《*CA Embedded Entitlements Manager 编程指南*》。

使用 Safex 实用工具创建 CA EEM APM 服务器资源访问策略：

1. 在 *<EEM_Server>* 目录中创建 Safex XML 文件，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

   例如，*C:\Program Files\CA\SharedComponents\iTechnology\Add_server.xml*。

2. 剪切该代码并将其粘贴到 Safex XML 文件中，然后使用您的变量替代引号中的变量，以及身份、资源类和权限的值。有关服务器权限，请参阅在 CA EEM 中创建并删除 APM 资源类 (p. 76)中的步骤 2（确定每个资源类允许的权限...）

   注意：在 CA EEM 中，权限称为操作。

```
<Safex>
   <Attach label="APM"/>
   <!-- 添加策略 -->

   <Add>
        <Policy name="Server Admin" folder="/Policies">
        <Description>Admin group has full permission for the
server</Description>

        <Identity>gug:Admin</Identity>

        <Action>full</Action>

        <ResourceClassName>Server</ResourceClassName>
        </Policy>
     </Add>

     <Detach/>
</Safex>
```

3. 打开命令提示符并导航到 *<EEM_Server>* 目录，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

4. 通过以下命令来运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_server.xml
   ```

   如果要使用 Safex 实用工具为以 FIPS 模式与 CA EEM 集成的应用程序创建 CA EEM APM 服务器资源访问策略，请运行以下命令以运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_server.xml -fips
   ```

5. 在 CA EEM 中查看 APM 服务器资源。

   a. 登录到 CA EEM。

   b. 单击“管理访问策略”选项卡。

   c. 单击“策略”链接。

   d. 在“搜索策略”窗口中，单击“显示匹配资源的策略”，然后从“资源类名称”下拉列表中选择“服务器”，最后单击“执行”。

      CA EEM 将在“策略表”窗口中显示 APM 服务器资源访问策略的列表。

   e. 单击服务器访问策略名称链接，可在“策略详细信息”窗口中查看有关 APM 服务器资源的详细信息。

使用 Safex 实用工具删除 CA EEM APM 服务器资源访问策略：

1. 在 *<EEM_Server>* 目录中创建 Safex XML 文件，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

   例如，*C:\Program Files\CA\SharedComponents\iTechnology\Remove_server.xml*。

2. 剪切该代码并将其粘贴到 Safex XML 文件中，然后使用您的变量替代引号中的变量，以及身份、资源类和权限的值。有关服务器权限，请参阅在 CA EEM 中创建并删除 APM 资源类 (p. 76)中的步骤 2（确定每个资源类允许的权限...）。

   注意：在 CA EEM 中，权限称为操作。

   ```
   <Safex>
      <Attach label="APM"/>
      <Remove>
           <Policy name="Server Admin" folder="/Policies">
           <Description>Admin group has full permission for the
   server</Description>
   ```

```
            <Identity>gug:Admin</Identity>
            <Action>full</Action>
            <ResourceClassName>Server</ResourceClassName>
            </Policy>
        </Remove>
        <Detach/>
</Safex>
```

3. 打开命令提示符并导航到 *<EEM_Server>* 目录，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

4. 通过以下命令来运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_server.xml
   ```

   如果要使用 Safex 实用工具为以 FIPS 模式与 CA EEM 集成的应用程序删除 CA EEM APM 服务器资源访问策略，请运行以下命令以运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Remove_server.xml -fips
   ```

5. 在 CA EEM 中查看 APM 服务器资源。

   a. 登录到 CA EEM。

   b. 单击“管理访问策略”选项卡。

   c. 单击“策略”链接。

   d. 在“搜索策略”窗口中，单击“显示匹配资源的策略”，然后从“资源类名称”下拉列表中选择“服务器”，最后单击“执行”。

   CA EEM 将在“策略表”窗口中显示 APM 服务器资源访问策略的列表。删除的 APM 服务器资源访问策略将不会再列出。

创建并删除 CA EEM APM 前端和业务服务资源访问策略

需要为前端（在 CA EEM 中称为业务应用程序）和业务服务添加访问策略作为 CA EEM APM 应用程序资源，才能设置应用程序分类地图权限。

注意：您也可以使用 CA EEM 界面执行这些任务。有关详细信息，请参阅《*CA Embedded Entitlements Manager 入门指南*》、《*CA Embedded Entitlements Manager 联机帮助*》、《*CA Embedded Entitlements Manager 编程指南*》。

要使用 Safex 实用工具创建 CA EEM APM 前端或业务服务资源访问策略，请执行以下操作：

1. 在 *<EEM_Server>* 目录中创建 Safex XML 文件，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

   例如，*C:\Program Files\CA\SharedComponents\iTechnolog\Add_application_policy.xml*。

2. 剪切此代码并将其粘贴到 Safex XML 文件中，然后使用您的变量替代引号中的变量以及身份、资源和权限的值。有关应用程序权限，请参阅在 CA EEM 中创建并删除 APM 资源类 (p. 76)中的步骤 2（确定每个资源类允许的权限...）。

   注意：在 CA EEM 中，权限称为操作。

   注意：下面的示例代码将为来宾用户提供权限，使其可以在应用程序分类视图中查看名为 Banking Application 的应用程序。

```
<Safex>
   <Attach label="APM"/>
   <!-- 添加策略 -->

   <Add>
        <Policy name="Business Application Write to a banking application"
folder="/Policies">
        <Description>Guest Group has write permission for a Banking
Application.</Description>

        <ResourceClassName>Business Application</ResourceClassName>

        <Resource>Banking Application</Resource>

        <Action>write</Action>

        <Identity>ug:Guest</Identity>
        </Policy>
     </Add>
     <Detach/>
</Safex>
```

3. 打开命令提示符并导航到 *<EEM_Server>* 目录，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

4. 通过以下命令来运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_application_policy.xml
   ```

   如果要使用 Safex 实用工具为以 FIPS 模式与 CA EEM 集成的应用程序创建 CA EEM APM 前端或业务服务资源访问策略，请运行以下命令以运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f Add_application_policy.xml
   -fips
   ```

5. 在 CA EEM 中查看 APM 应用程序资源策略。

   a. 登录到 CA EEM。

   b. 单击“管理访问策略”选项卡。

   c. 单击“策略”链接。

   d. 在“搜索策略”窗口中，单击“显示匹配资源的策略”，然后从“资源类名称”下拉列表中选择某个应用程序策略名称，最后单击“执行”。

      CA EEM 将在“策略表”窗口中显示 APM 应用程序资源访问策略的列表。

   e. 单击应用程序资源访问策略名称链接，可在“策略详细信息”窗口中查看有关 APM 应用程序资源的详细信息。

要使用 Safex 实用工具删除 CA EEM APM 前端或业务服务资源访问策略，请执行以下操作：

1. 在 *<EEM_Server>* 目录中创建 Safex XML 文件，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

   例如，*C:\Program Files\CA\SharedComponents\iTechnology\Remove_application_policy.xml*。

2. 剪切此代码并将其粘贴到 Safex XML 文件中，然后使用您的变量替代引号中的变量以及身份、资源和权限的值。有关应用程序权限，请参阅在 CA EEM 中创建并删除 APM 资源类 (p. 76)中的步骤 2（确定每个资源类允许的权限...）。

   注意：在 CA EEM 中，权限称为操作。

```
<Safex>
   <Attach label="APM"/>
       <Remove>
        <Policy name="Business Application Write to a banking application"
folder="/Policies">
        <Description>Guest Group has write permission for a Banking
Application.</Description>

        <ResourceClassName>Business Application</ResourceClassName>

        <Resource>Banking Application</Resource>

        <Action>write</Action>

        <Identity>ug:Guest</Identity>
        </Policy>
       </Remove>
     <Detach/>
</Safex>
```

3. 打开命令提示符并导航到 *<EEM_Server>* 目录，该目录通常为 *C:\Program Files\CA\SharedComponents\iTechnology*。

4. 通过以下命令来运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f
   Remove_application_policy.xml
   ```

   如果要使用 Safex 实用工具为以 FIPS 模式与 CA EEM 集成的应用程序删除 CA EEM APM 前端或业务服务资源访问策略，请运行以下命令以运行 Safex 脚本：

   ```
   >safex.exe -h localhost -u EiamAdmin -p <ENTER YOUR PASSWORD> -f
   <yourfilename>.xml -fips
   ```

   例如，

   ```
   >safex.exe -h localhost -u EiamAdmin -p 1234567 -f
   Remove_application_policy.xml -fips
   ```

5. 在 CA EEM 中查看 APM 应用程序资源。

   a. 登录到 CA EEM。

   b. 单击“管理访问策略”选项卡。

   c. 单击“策略”链接。

   d. 在“搜索策略”窗口中，单击“显示匹配资源的策略”，然后从“资源类名称”下拉列表中选择某个应用程序策略名称，最后单击“执行”。

   CA EEM 将在“策略表”窗口中显示 APM 应用程序资源访问策略的列表。已删除的 APM 应用程序访问策略不会列出。

在群集中设置 CA EEM

要在群集中提供 CA EEM 安全设置，请配置 *realms.xml* 文件，使所有企业管理器都附加到 CA EEM 中的同一个应用程序。在将新收集器添加到群集中以增加代理或 TIM 数量时，也要遵循这些说明。

请执行以下步骤：

重要信息！ 如果将 CA EEM 用于授权，则企业管理器必须附加到 CA EEM 中的至少一个应用程序。这是因为 CA EEM 使用应用程序来存储定义权限的访问策略和资源类。

1. 在企业管理器（收集器、MOM 或 CDV）上，配置 *realms.xml* 文件以进行 CA EEM 授权。

   a. 打开位于 *<EM_Home>/config* 目录中的 *realms.xml* 文件。

b. 将 *appname* 属性设置为企业管理器将在 CA EEM 中附加到的应用程序的名称。例如，*APM*。

   这是您在配置 CA EEM 服务器时使用的同一个 APM 应用程序名称。

c. 将 *enableAuthorization* 属性设置为 *True*。

d. 保存 *realms.xml* 文件。

e. 重新启动企业管理器以应用 *realms.xml* 更改

2. 对群集中的每个企业管理器重复上面的步骤 1。

   当群集中的所有企业管理器都附加到 CA EEM 中的同一个应用程序时，就会在整个群集中启用 CA EEM 安全设置。

从本地安全设置迁移到 CA EEM 安全设置

如果您一直在使用本地身份验证和授权运行 Introscope，并希望部署基于 CA EEM 的身份验证和授权，则可通过执行以下操作实现此目的：

- 安装 CA EEM
- 配置 CA EEM 以进行身份验证
- 配置 CA EEM 以进行授权

也可以部署基于 CA EEM 的身份验证和本地授权。有关详细信息，请参阅将 CA EEM 配置为使用本地授权 (p. 95)。

要全面了解 CA EEM 安全设置的部署，请从使用 CA EEM 保护 Introscope (p. 52) 主题的开头开始阅读。

从 LDAP 迁移到 CA EEM 安全性

如果您一直使用 LDAP 身份验证和本地授权来运行 Introscope，但希望部署基于 CA EEM 的身份验证和授权，则可通过执行以下操作实现此目的：

- 安装 CA EEM
- 配置 CA EEM 以进行身份验证
- 配置 CA EEM 以进行授权

要全面了解 CA EEM 安全设置的部署，请从使用 CA EEM 保护 Introscope (p. 52) 主题的开头开始阅读。

将 CA EEM 配置为使用本地授权

如果 CA APM 用户在 EEM 安全领域中进行身份验证，则在默认情况下，CA APM 用户也会在 EEM 领域中进行授权。但是，如果将 *realms.xml* 中的 *enableAuthorization* 标志设置为 *false*，则 CA APM 用户在 CA EEM 中进行身份验证后，会使用本地授权，而不是 CA EEM 授权。在这种情况下，授权访问策略将来自于此 CA APM 用户（CA EEM 安全用户组的成员）的本地领域。在有些情况下，您可能会选择使用本地授权，例如，要使用配置为使用 LDAP 或 SiteMinder 进行身份验证的 CA EEM，但将权限保留在本地领域中。

对于 Introscope，本地领域权限是在 *domains.xml* 和 *server.xml* 文件中定义的。

对于 CA CEM，本地领域访问策略将基于安全用户组成员资格。

要使 CA APM 执行 CA EEM 身份验证，然后再执行本地授权，必须将用户分配给 CA EEM 中的 APM 安全用户组。但是，在这种情况下，不需要在 CA EEM 中创建访问策略。

在这种情况下，使用本地安全设置进行授权意味着：

- *realms.xml* 中的 *enableAuthorization* 标记设置为 *false*。
- 对于 Introscope，您必须在 CA EEM 中创建用户和组，然后在 *domains.xml* 文件中分配权限。
- 对于 CA CEM，您必须在 CA EEM 中创建用户以及全部四个默认安全组。例如，您在 CA EEM 中创建 *cemadmin* 用户以及 *“CEM 系统管理”* 安全组。然后将 *cemadmin* 分配为 *“CEM 系统管理员”* 安全组的成员，从而为 *cemadmin* 提供 *“CEM 系统管理员”* 安全组权限。有关四个 CA CEM 默认安全组的信息，请参阅与默认 CA CEM 安全用户组关联的菜单项和权限 (p. 109)。

请执行以下步骤：

1. 打开位于 *<EM_Home>/config* 目录中的 *realms.xml* 文件。
2. 将 *enableAuthorization* 属性设置为 *false*。

   如果该值设置为 *false*，则 CA EEM 仅执行身份验证，而使用本地安全领域进行授权。有关详细信息，请参阅在 realms.xml 中配置 CA EEM 身份验证 (p. 56)。有关本地授权的信息，请参阅使用本地安全设置保护 Introscope (p. 29)。
3. 保存 *realms.xml* 文件。

4. 配置域权限。请参阅在 domains.xml 中配置 Introscope 域权限 (p. 36)。
5. 配置企业管理器服务器权限。请参阅配置企业管理器服务器权限 (p. 39)。

关于 Introscope 单点登录 (SSO)

单点登录 (SSO) 向用户提供登录一次即可访问多个应用程序的方法，否则，每次访问一个应用程序都需要登录一次。

用户登录到 Introscope 时，如果用户的浏览器接受 Cookie，则将自动进行 SSO。然后，用户可以在 CA APM Web 应用程序之间导航，无需登录到每个应用程序并重新进行身份验证。如果用户的浏览器不接受 Cookie，则将无法进行 SSO，用户必须分别登录到每个 CA APM 应用程序。

以下 Introscope Web 应用程序支持 SSO：

- Web Start 工作站
- WebView
- CEM 控制台

Introscope 工作站（厚客户端）不支持 SSO。

关于 SiteMinder SSO 和 Introscope 安全设置

如果您使用 CA EEM 部署了 Introscope 安全性，并且 CA EEM 服务器已经与 CA SiteMinder 进行了集成以进行身份验证，则 Introscope Web 应用程序可以使用 SiteMinder 的 SSO 功能。有关使用 SiteMinder 进行身份验证的 CA EEM 部署的信息，请参阅配置使用 CA SiteMinder 的 CA EEM 身份验证 (p. 59)。

如果某个 Web 应用程序同时找到了 Introscope 凭据和 SiteMinder SSO 凭据，那么该 Web 应用程序将首先尝试使用 Introscope 凭据进行身份验证。如果身份验证失败，则该 Web 应用程序将尝试使用 SiteMinder 凭据。

有关 SiteMinder SSO 的详细信息，请参阅《*CA APM for CA SiteMinder Web Access Manager 指南*》。

保护应用程序分类视图

如果已使用 CA EEM 部署 Introscope 授权，则可设置用户权限，以便在应用程序分类视图上查看前端和业务服务。通过运行 Safex 脚本或在 CA EEM 中提供针对业务应用程序（前端）和业务服务资源的任何权限（写入、读取或读取敏感数据），也可以设置这些权限。

如果不将 CA EEM 用于安全设置，或者将 CA EEM 部署用于安全设置，但*不*添加特定的前端或业务服务作为关联访问策略中的 CA EEM 业务应用程序和业务服务资源，则用户可以在应用程序分类视图上查看所有业务应用程序和业务服务。有关 CA EEM 业务应用程序和业务服务资源的详细信息，请参阅在 CA EEM 中创建和删除 APM 资源类 (p. 76)。有关使用应用程序分类视图时用户所见内容的信息，请参阅《*CA APM Workstation 用户指南*》。

除了前端和业务服务视图安全设置以外，域安全设置也适用于应用程序分类视图。此外，超级域安全设置将覆盖所有前端和业务服务安全设置。域安全设置可以限制允许用户和组查看的代理数据。有关详细信息，请参阅超级域安全设置将覆盖应用程序分类视图安全设置 (p. 99)。

如果运行 *eem.register.app.xml* 脚本来设置默认的 CA APM 应用程序，则该脚本会提供业务服务和业务应用程序（前端）资源类以及如下所述的操作。有关详细信息，请参阅配置 CA EEM 授权 (p. 60)。

要部署应用程序分类视图安全，请在 CA EEM 中执行以下高级步骤：

1. 定义用户组和用户。

   您可以使用 APM 组 (p. 68)和 APM 用户 (p. 72)示例脚本。

2. 创建基于用户、组和权限（CA EEM 中的操作）的访问策略。

   有关示例脚本，请参阅关于 CA EEM 访问策略 (p. 82)。

3. 将每个访问策略与资源类关联。然后，可以向访问策略添加特定的资源，以进一步限制策略。

4. 向策略添加单个业务服务和业务应用程序，以及业务服务和业务应用程序资源类。

   注意：无需将单个业务服务和业务应用程序定义为其对应业务类的成员。

有关详细信息，请参阅在 CA EEM 中创建和删除 APM 资源类 (p. 76)中的以下步骤：

- 确定业务服务资源类权限以提供应用程序分类视图安全设置。
- 确定业务应用程序资源类权限，以便为前端提供应用程序分类视图安全设置。

注意：对于业务服务和业务应用程序（前端），任何授予的权限都会向用户提供查看应用程序分类视图的访问权限。

注意：如果您更改了用户权限以查看业务服务或业务应用程序，则只有当用户注销并再次登录到 Workstation 之后，这些更改才会反映在应用程序分类视图上。

注意：如果未在在业务服务或业务应用程序策略中指定资源，那么业务服务或业务应用程序策略将适用于业务服务或业务应用程序资源类中的所有资源。

如果添加前端作为 CA EEM 业务应用程序资源，并且不向关联的业务应用程序资源类用户或组提供在应用程序分类视图上查看该前端的权限，则该用户或组将不能查看在分类视图树中列出的前端。这也适用于业务服务，如果用户未获得权限，将不会在树中显示业务服务。但是，如果业务服务调用了用户无权访问的前端，或者是允许用户或组查看的其他前端调用了该前端，则将在视图上显示该前端，但是：

- 显示为已禁用
- 无法选择
- 不显示任何依赖关系或度量标准数据

但是，用户和组可以在度量标准浏览器树中查看有关该前端的单个代理数据。

重要信息！如果用户拥有超级域权限，则允许该用户在应用程序分类视图上查看所有前端和业务服务。有关详细信息，请参阅超级域安全设置将覆盖应用程序分类视图安全设置 (p. 99)。

有关使用 Safex 脚本设置应用程序分类视图权限的说明，请参阅：

- 在 CA EEM 中创建并删除 APM 资源类 (p. 76)。
- 创建和删除 CA EEM APM 前端和业务服务资源访问策略 (p. 89)。

注意：有关启用了应用程序分类视图安全后，Workstation 如何显示业务应用程序和业务服务的信息，请参阅《*CA APM Workstation 用户指南*》。

超级域安全设置将覆盖应用程序分类地图安全设置

除了前端和业务服务视图安全设置以外，域安全设置也适用于应用程序分类视图。域安全设置可以限制允许用户和组查看的代理数据。有关域安全设置的信息，请参阅定义和配置 Introscope 域 (p. 17)以及在 domains.xml 中配置 Introscope 域权限 (p. 36)。

在“分类视图”选项卡上，域安全会限制用户和组在以下列表中看到的代理：

- 应用程序分类地图下方的物理位置列表中的代理列表
- 在任何度量标准显示下的物理位置列表中的代理列表。选择了分类视图树中的某个子节点时，将显示这些代理。例如，运行状况节点或单个度量标准节点。

*超级域*安全设置将覆盖应用程序分类地图安全设置。这意味着，对于在任何领域（本地或 EEM）中被授予*超级域*访问权限的用户，也允许其查看应用程序分类地图上的所有前端和业务服务，即使未授予业务服务和业务应用程序读取权限时也是如此。

例如，假设 Introscope 正在监控三个前端 A、B 和 C。您向名为 Tai 的 Introscope 用户授予权限，只能查看前端 A。Tai 还拥有*超级域*权限，允许查看所有代理。在这种情况下，Tai 可以在应用程序分类地图和“调查器”树中查看这三个前端。

排除 Introscope 安全设置故障

该表提供了一些提示信息，可帮助您解决 Introscope 安全设置中出现的问题。

症状：

运行 Safex 脚本以加载 CA APM 组、用户和资源类时，出现错误消息。

错误消息可能如以下示例所示：

```
"1375 [0x00000458] ERROR PozFactory null - PozFactory::attachPoz - 在主机 localhost 上调用 iPoz::ClientAttach 时出错 1375 [0x00000458] ERROR PozFactory null - PozFactory::attachPoz 错误: 错误签名: 来自主机 [192.168.200.1.ca.com:1331] 的请求中存在不兼容的签名摘录类型。Server is running in [Fips_Mode_On] and request signature digest type is [ITECH_DIGEST_MD5]. FIPS does not support ITECH_DIGEST_MD5 digest type"
```

解决方案：

CA EEM 服务器处于仅 FIPS 模式。

将 CA EEM 服务器设置更改为非 FIPS 模式。

症状：

Introscope 用户登录 Introscope 时，出现错误消息。

Introscope 用户无法登录。

解决方案：

验证是否正确输入了用户名和密码。

症状：

无法确定企业管理器是否已连接到 CA EEM APM 应用程序实例。

您不知道 Introscope 是否已连接到 CA EEM。

解决方案：

查看 <企业管理器主目录>/logs/IntroscopeEnterpriseManager.log 文件中的日志消息。

以下日志消息显示此信息：

- 企业管理器在 CA EEM 中附加到的应用程序
- CA EEM 服务器的位置
- CA EEM 服务器是否正在使用 CA EEM 或外部目录（LDAP 或 SiteMinder）来获取用户和组

例如：

```
8/05/09 04:15:59 PM PDT [INFO] [Manager.EemRealm] EEM realm attached to
application "APM" in EEM server at <EEM_Machine_Name> using SiteMinder
```

症状：

企业管理器与 CA EEM 的交互有问题。

调试 Introscope CA EEM 连接。

解决方案：

设置 CA EEM 调试属性以显示有关 CA EEM 的日志消息。有关详细信息，请参阅配置 CA EEM 相关消息的日志记录 (p. 55)。

Introscope 安全机制

根据您所在组织的安全需求，启用该表中列出的相应 Introscope 安全机制。

提供的安全机制	提供的保护
更改密码并保护密码安全，以便从 Workstation、WebView、Web Start Workstation 或 CEM 控制台登录企业管理器。	CA Technologies 强烈建议您遵循此安全性最佳实践。 有关 Workstation、WebView 和 Web Start 密码的详细信息，请参阅《*CA APM Workstation 用户指南*》。 有关 CEM 控制台密码的详细信息，请参阅管理 CA CEM 密码 (p. 106)。
设置并使用在安装了企业管理器的 Windows 或 Linux 计算机上的文件系统安全设置。	只有获得允许的用户才能访问 *users.xml* 文件来设置 APM 域以实现本地安全设置。
设置并使用收集器与 MOM 之间的加密密钥配置。	只有获得允许的用户才能访问收集器。 有关详细信息，请参阅配置安全身份验证的公钥和私钥 (p. 24)。
更改并保护 APM 数据库密码。	只有允许的用户才能访问 APM 数据库。 有关详细信息，请参阅《*CA APM 安装和升级指南*》。
经过培训的数据库管理员。	维护 APM 数据库的常规运行状况。
通过在 *IntroscopeAgent.profile* 文件中配置 SSL 通信属性，可以实现通过 SSL 进行代理与企业管理器之间的通信。	保护代理和企业管理器之间的通信。 有关详细信息，请参阅《*CA APM Java 代理实施指南*》或《*CA APM .NET 代理实施指南*》。
企业管理器与浏览器之间的 SSL 加密通信。	企业管理器与浏览器之间的安全通信。 有关详细信息，请参阅限制仅通过 HTTPS 的企业管理器访问 (p. 132)。
Introscope 身份验证。	只有获得允许的用户才能登录 Introscope 和 CA APM。
Introscope 授权。	只有允许的用户才能访问 Introscope 域。
应用程序分类地图安全性。	只有获得允许的用户才能在应用程序分类地图上查看特定的业务服务和前端。 有关详细信息，请参阅保护应用程序分类地图 (p. 97)。

第 4 章： 保护 CA CEM

如果要升级 CA CEM，请参阅《*CA APM 安装和升级指南*》中与安全相关的升级主题。

以下列表显示了需要了解的有关 CA CEM 安全的内容：

1. 熟悉 CA CEM 安全 (p. 103)。
2. 了解 CA CEM 用户和安全用户组 (p. 108)。
3. 了解维护 CA CEM 密码 (p. 106)。
4. 如果要部署 CA Embedded Entitlements Manager (CA EEM) 以实现安全设置，请了解以下内容：
   - CA CEM EEM 安全 (p. 111)。
   - 维护必需的 CA CEM 用户和安全用户组 (p. 111)。
   - 资源类 (p. 113)。
   - 资源 (p. 114)。
   - 访问策略 (p. 114)。
5. 如果要部署本地安全设置，请了解以下内容：
   - CA CEM 本地安全 (p. 119)。
   - 维护必需的 CA CEM 用户 (p. 119)。
6. 定义私有参数 (p. 121)。
7. 了解与安全设置有关的 HTTP 响应和请求内容 (p. 123)。
8. （可选）应用 FIPS 140-2 加密 (p. 129)。
9. （可选）配置通过 HTTPS 进行的 TIM 通信 (p. 131)。
10. （可选）将浏览器/企业管理器的通信方式限制为 HTTPS (p. 132)。

CA CEM 安全机制

根据您所在组织的安全需求，启用该表中列出的相应 CA CEM 安全机制。

提供的安全机制	提供的保护
在数据中心内受保护区域中运行 CA CEM，并设置 Introscope 安全。	访问企业管理器计算机，可防止有人未经授权访问企业管理器文件系统。

提供的安全机制	提供的保护
经过培训的数据库管理员。	维护 APM 数据库的常规运行状况。
更改并保护 APM 数据库密码。	只有允许的用户才能访问 APM 数据库。 有关详细信息，请参阅《*CA APM 安装和升级指南*》。
更改每台 TIM 计算机的 Linux 根帐号的默认密码。	TIM 数据安全性。 有关详细信息，请参阅《*CA APM 安装和升级指南*》。
更改密码并保护密码安全，以便从 Workstation、WebView、Web Start Workstation 或 CEM 控制台登录企业管理器。	有关 Workstation、WebView 和 Web Start 密码的详细信息，请参阅《*CA APM Workstation 用户指南*》。 有关 CEM 控制台密码的详细信息，请参阅管理 CA CEM 密码 (p. 106)。
企业管理器和 TIM 之间的 SSL 加密通信。	保护企业管理器和 TIM 之间的通信。 有关详细信息，请参阅配置通过 HTTPS 的 TIM 通信 (p. 131)。
企业管理器与浏览器之间的 SSL 加密通信。	企业管理器与浏览器之间的安全通信。 有关详细信息，请参阅限制仅通过 HTTPS 的企业管理器访问 (p. 132)
符合 FIPS 标准的安全设置。	通过联邦信息处理标准实现更高级别的安全性。 有关详细信息，请参阅符合 FIPS 140-2 的加密 (p. 129)
CA CEM 身份验证。	只有获得允许的用户才能登录 CA CEM。
CA CEM 授权。	使用访问策略来决定特定用户可以看到的以及特定数据用户可以使用的 CEM 控制台选项卡。
“配置 TIM Web 保护”选项。	保护 TIM 网页免受跨站点伪造请求的危害。有关详细信息，请参阅“如何为 TIM 配置 Web 保护”。

注意：如果尚未熟悉 CA APM 安全基础知识，请参阅 CA APM 安全摘要 (p. 9)和 Introscope 如何检查安全 (p. 29)。

在设置 CA APM 安全时，组织必须决定要部署哪个单一的或混合的安全领域。为了使 CA APM 用户能访问 CA CEM，必须部署本地领域、CA EEM 领域或 LDAP 领域。

如何为 TIM 配置 Web 保护

设置“配置 TIM Web 保护”选项以保护 TIM 网页免受跨站点伪造请求的危害。

请执行以下步骤：

1. 访问“TIM 设置”页面。

   有关如何访问“TIM 设置”页面的信息，请参阅《*APM 配置和管理指南*》中的主题“访问 CEM 控制台和设置页面”。

2. 单击“配置 TIM Web 保护”选项。
3. 根据您的应用程序要求，选择以下任一选项来保护相应页面：
   - 用于更改系统状态的页面。
   - 用于显示系统信息的页面。
4. 单击“保存”。

   此时将配置 TIM 保护。

重要信息！为页面启用了“TIM Web 保护”选项后，不能将其添加为书签以供直接访问。

关于 CA CEM 身份验证

如果您的部署使用本地领域对 CA CEM 用户进行身份验证，则 *<企业管理器主目录>/config* 目录文件中的 *users.xml* 文件将向 CA CEM 提供 CA CEM 用户凭据。

注意：如果您曾从 Wily CEM 4.5 升级，并使用了本地安全设置，则您的 Wily CEM 4.5 用户可能会在 *usersCEM45.xml* 文件中。有关详细信息，请参阅《*CA APM 安装和升级指南*》。

如果您的部署在 CA EEM 领域中对 CA APM 用户进行身份验证，则 CA EEM 服务器会向 CA CEM 提供 CA CEM 用户凭据。

注意：如果您的 CA EEM 服务器已配置为与 SiteMinder 配合使用，则可以部署 SiteMinder 来对您的 CA EEM 用户进行身份验证。

管理 CA CEM 密码

CA APM 用户密码在 EEM 领域和本地领域中都经过加密。有关如何在本地安全中加密密码的信息，请参阅“在 users.xml 中配置 CA APM 用户和组 (p. 33)”。

对于本地安全，即用型 CA CEM 提供两个 CA CEM 用户：*admin* 和 *cemadmin*。这两个用户均属于“管理员”和“CEM 系统管理员”CA CEM 安全用户组。有关 *admin* 的默认密码，请参阅《*CA APM 安装和升级指南*》。有关在本地安全中更新 CA CEM 用户密码的信息，请参阅“在 users.xml 中配置 CA APM 用户和组 (p. 33)”。

如果您是 CA EEM 的 CA APM 管理员，则可以更新 CA CEM 用户的密码。CA CEM 用户可以使用 CA EEM 自我管理来更改自己的密码。

要在 CA EEM 中重置 CA CEM 用户密码，请执行以下操作：

如果您是 CA EEM 的 CA APM 管理员，则可以在 CA EEM 中更新 CA CEM 用户的密码。

1. 在 CA EEM 中登录到 APM 应用程序。
   a. 在 CA EEM 登录页面上，从“应用程序:”下拉列表中选择 APM。
   b. 输入登录名和密码。

   APM 应用程序默认登录名为 *EiamAdmin*。
2. 转到“管理身份”选项卡。
3. 在“搜索用户”框中，选择“应用程序用户详细信息”，然后单击“执行”。
4. 单击“用户”框树中的 APM 用户名。
5. 出现用户信息时，在“身份验证”框中执行以下任一操作：
   - 选中“下次登录时更改密码”复选框。
   - 选中“重置密码”复选框，然后输入并确认新密码。向用户通知新密码。
6. 单击“保存”。

   有关详细信息，请参阅《*CA Embedded Entitlements Manager 联机帮助*》。

通过自我管理重置 CA EEM 密码：

CA CEM 用户可以在 CA EEM 中使用以下自我管理过程更改自己的密码。

1. 在 CA EEM 中登录到 APM 应用程序。
   a. 在 CA EEM 登录页面上，从“应用程序:”下拉列表中选择“全局”。
   b. 输入登录名和密码。
2. 转到“主页”选项卡。
3. 在“自我管理”框中，单击“更改密码”链接。

   有关详细信息，请参阅《*CA Embedded Entitlements Manager 联机帮助*》。

关于 CA CEM 授权

如果 CA CEM 用户是本地授权的，则特定用户可以看到的 CEM 控制台选项卡以及用户可以使用的特定数据，均基于每个用户所属的 CA CEM 安全用户组。访问策略会分配给 CA CEM 安全用户组并以这些用户组为基础。

如果您的部署使用本地领域对 CA APM 用户进行授权，则 *users.xml*（如果您曾从 Wily CEM 4.5 升级，则也许是 *usersCEM45.xml*）将允许标准 CA CEM 安全用户组查看 CEM 控制台，如与默认 CA CEM 安全用户组关联的菜单项和权限 (p. 109)中所述。有关详细信息，请参阅本地用户和组以及 CA CEM (p. 119)。

在 CA EEM 中对 CA CEM 用户进行授权时，访问策略确定特定用户可以看到的 CEM 控制台选项卡，以及用户可以使用的特定数据。

如果您的部署在 CA EEM 中对 CA APM 用户进行授权，则可通过运行 *eem.register.app.xml* Safex 脚本来部署默认的 APM 应用程序（建议）或者手工部署，以在 CA EEM 中设置访问策略。

如果通过运行位于 *<企业管理器主目录>/examples/authentication* 目录中的 *eem.register.app.xml* Safex 脚本来设置访问策略，则 CA EEM 将允许标准 CA CEM 用户组查看 CEM 控制台，如与默认 CA CEM 安全用户组关联的菜单项和权限 (p. 109)中所述。

有关详细信息，请参阅 CA CEM 的 CA EEM 身份验证和授权 (p. 111)以及关于 CA EEM 访问策略 (p. 82)。

关于 CA CEM 安全用户组

CA CEM 提供四个默认的安全用户组。如果是从以前版本的 CA CEM 升级，则会熟悉 CA CEM 角色。CA CEM 角色现在称为 CA CEM 安全用户组，以提供统一的 CA APM 安全。

默认的 CA CEM 安全用户组是：

- 管理员－对 Introscope 和 CA CEM 都有访问权限，并且被授予 Introscope 管理员以及 CEM 系统管理员权限。
- CEM 系统管理员－管理所有 CA CEM 系统功能
- CEM 配置管理员－管理常规 CA CEM 配置
- CEM 分析人员－仅能访问 CA CEM 报告和视图
- CEM 突发事件分析人员－可访问 CA CEM 报告和视图，包括有关缺陷的 HTTP 信息

要保护 CA CEM 系统，需要尽可能将分配给管理员组的用户数限制到最少。

有关默认的 CA CEM 安全用户组成员可以查看的 CA CEM 选项卡的信息，请参阅与默认 CA CEM 安全用户组关联的菜单项和权限 (p. 109)。

如果部署的是本地安全，则 CA CEM 将在 *users.xml* 文件中提供这些默认组。

重要信息！如果部署本地授权，则无法将安全用户组添加到默认的 CA CEM 安全用户组中，也无法更改与这些组关联的访问策略。有关详细信息，请参阅本地用户和组以及 CA CEM (p. 119)。

如果部署的是 CA EEM 的安全，则应在 CA EEM 服务器上设置 CA CEM 安全用户组和访问策略。可以通过运行 Safex 脚本或在 CA EEM 中执行此操作。有关详细信息，请参阅在 CA EEM 中创建和删除 APM 组 (p. 68)。如果您愿意，可以添加、修改或删除 CA CEM 安全用户组。

重要信息！如果希望设置访问策略来限制 CA CEM 用户可以查看的内容，则必须部署 CA EEM 授权。

其他 CA CEM 身份验证和授权解决方案

可以配置 LDAP 来进行 CA CEM 身份验证。

有关配置 LDAP 进行 CA APM 身份验证的信息，请参阅“使用 LDAP 保护 Introscope (p. 41)”。

重要信息！如果使用 LDAP 进行身份验证，则必须手工配置 CA APM 用户组。确保 LDAP 组名称与 CA CEM 组名称完全匹配。

也可以将 CA EEM 配置为使用本地安全设置进行 CA CEM 授权。通过将 CA EEM 配置为使用本地领域进行授权，可以执行此操作。有关详细信息，请参阅将 CA EEM 配置为使用本地授权 (p. 95)。

与默认 CA CEM 安全用户组关联的菜单项和权限

该表显示每个默认 CA CEM 安全用户组具有的菜单项以及因此而拥有的权限。

菜单： 特性	CEM 系统管理员	CEM 配置管理员	CEM 分析人员	CEM 突发事件分析人员
系统： 电子邮件设置 Events	是	否	否	否
安全性： 私有参数 FIPS 设置 访问策略（仅限 CA EEM）	是	否	否	否
设置： 域 监视程序 服务 Web 服务器筛选 突发事件设置 HTTPS 设置 插件 Introscope 设置	是	是	否	否

菜单： 特性	CEM 系统管理员	CEM 配置管理员	CEM 分析人员	CEM 突发事件分析人员
管理： 概览 业务应用程序 业务服务 规范 用户组 关联 SLA 记录会话 事务发现	是	是	否	否
工具： 脚本记录器	是	是	否	否
CEM： 服务级别管理 突发事件管理 » 查看注释 性能报告 质量报告 分析图 店腔惆桶	是－所有页面	是－除了无法查看“CEM”>“突发事件管理”>“缺陷详细信息”页面上的“HTTP 信息”部分	是－除了无法查看“CEM”>“突发事件管理”>“缺陷详细信息”页面上的“HTTP 信息”部分	是－所有页面

注意：“CEM”>“突发事件管理”>“缺陷详细信息”页面的“HTTP 信息”部分将显示有关 query 和 post 参数的详细数据以及请求和响应正文。如果选中了“捕获全面缺陷详细信息”复选框（在“设置”>“域”页面上），则 TIM 将收集该信息。

要查看这些详细数据，用户必须是一个组的成员，该组将授予对与该缺陷相关的业务服务的*“读取敏感数据”*访问权限。例如，CEM 突发事件分析人员组便具有该访问权限。

有关详细信息，请参阅保护有关缺陷的 HTTP 请求和响应 (p. 123)。

CA CEM 的 CA EEM 身份验证和授权

如果尚不熟悉 CA EEM，请参阅“使用 CA EEM 保护 Introscope”。

如果部署 CA EEM 以实现 CA CEM 安全，则应在 CA EEM 服务器上完成身份验证和授权。CA EEM 授权基于访问策略，而不是基于安全用户组成员资格。在 CA EEM 中，访问策略包含三个组成部分：资源类、资源和权限（如读取或写入）。有关详细信息，请参阅关于 CA EEM 访问策略 (p. 82)。

注意：在 CA EEM 中，权限称为操作。

以下主题介绍了特定于 CA CEM 的默认资源类、资源和访问策略。CA APM 提供 CA EEM Safex 脚本，该脚本将注册默认 CA APM 应用程序，并创建 CA CEM 全局和应用程序特定的用户、安全用户组、资源类以及资源类的访问策略：

- 在 CA EEM 中管理 CA CEM 用户和组 (p. 111)
- 关于 CA EEM 中的 CA CEM 资源类 (p. 113)
- 关于特定于 Introscope 的资源类 (p. 114)
- 关于 CA EEM 中的 CA CEM 资源 (p. 114)
- 默认 CA EEM CEM 访问策略 (p. 114)
- 关于 CA CEM 默认业务服务访问策略 (p. 117)

在 CA EEM 中管理 CA CEM 用户和组

CA CEM 安全基于 CA EEM 访问策略，后者可应用于特定的用户和特定于应用程序的用户组。

CA Technologies 建议运行 *eem.register.app.xml* 和 *eem.add.global.identities.xml* Safex 脚本来设置提供标准 CA CEM 用户和组的 APM 应用程序。这些 Safex 脚本可创建全局用户，以及全局用户组和特定于 APM 应用程序的用户组。

在 CA EEM 中，CA CEM 用户可以（但不需要）属于四个默认 CA CEM 安全用户组中的任何一个：CEM 系统管理员、CEM 配置管理员、CEM 分析人员或 CEM 突发事件分析人员。CA CEM 用户可以属于您定义的新组（例如，HR 管理组）。有关默认 CA CEM 安全用户组的详细信息，请参阅与默认 CA CEM 安全用户组关联的菜单项和权限 (p. 109)。

可以创建、添加、修改和删除 CA CEM 用户和组。也可以启用和禁用 CA CEM 用户。

重要信息！ 如果 CA APM 用户正在使用 CEM 控制台，并希望查看 Introscope 调查器数据，则他们必须同时包括在一个 APM 安全用户组和一个 CA CEM 安全用户组中。例如，APM 来宾组和 CEM 分析人员组。有关详细信息，请参阅“允许 CA EEM Introscope 用户访问 CEM 控制台 (p. 118)”或“允许本地 Introscope 用户访问 CEM 控制台 (p. 120)”。

添加/修改/删除 CA CEM 用户：

- 使用在 CA EEM 中创建和删除 APM 用户 (p. 72)中所述的方法之一，添加/修改/删除 CA CEM 用户。

添加/修改/删除 CA CEM 安全用户组：

- 可以按照在 CA EEM 中创建和删除 APM 组 (p. 68)中的内容，添加/修改/删除 CA CEM 安全用户组。

启用或禁用 CA CEM 用户：

1. 在 CA EEM 中登录到 APM 应用程序。
   a. 在 CA EEM 登录页面上，从“应用程序:”下拉列表中选择 APM。
   b. 输入登录名和密码。

   CA APM 应用程序默认登录名为 *EiamAdmin*。
2. 转到“管理身份”选项卡。
3. 在“搜索用户”框中，选择“应用程序用户详细信息”，然后单击“执行”。
4. 单击“用户”框树中的 APM 用户名。
5. 出现用户信息时，在“身份验证”框中执行以下任一操作：
   - 单击“启用日期”右边的日历。
   - 单击“禁用日期”右边的日历。
6. 选择一个执行启用或禁用操作的日期和时间，然后单击“确定”。
7. 单击“保存”。

   有关详细信息，请参阅《*CA Embedded Entitlements Manager 联机帮助*》。

关于 CA EEM 中的 CA CEM 资源类

使用 CA EEM 进行 CA CEM 授权时，需要设置访问策略以确定 CA CEM 安全用户组可以查看的 CEM 控制台选项卡。资源类是访问策略的必需组成部分。每个资源类都拥有关联的权限（在 CA EEM 中称为操作）。

此表显示了与默认 CA CEM 资源类关联的操作。

CA CEM 资源类	默认操作
业务应用程序	写入
业务服务	写入 读取 读取敏感数据
突发事件	写入
报告	写入
服务器	写入
系统管理设置	写入
系统安全设置	写入
用户组	写入
Web 服务	允许
访问策略	写入

某个资源类与写入操作关联时，允许访问该资源类的 CA CEM 用户或组可以查看“CEM 控制台”菜单中的关联选项卡。例如，业务应用程序资源类允许 CA CEM 用户查看 CEM 控制台中的“管理”>“业务应用程序”。

业务服务资源类还有另外两个仅与其关联的操作：*读取*和*读取敏感数据*。如果某个 CA CEM 用户具有业务服务的*读取敏感数据*权限，则允许该 CA CEM 用户查看附加到该特定业务服务的缺陷上的 HTTP 头信息。有关详细信息，请参阅《*CA APM 配置和管理指南*》。

业务服务资源类还确定了 CA CEM 用户是否可以访问 TIM 和代理记录（“管理”>“记录会话”）。至少对一个业务服务具有写权限的用户可以访问“记录会话”选项卡。

关于特定于 Introscope 的资源类

除 CA CEM 资源类外，默认 CA APM 应用程序还提供了两个特定于 Introscope 的资源类：

- 域，授予 Introscope 用户查看特定于 Introscope 的域（如超级域）的权限。

  注意：这与“CEM”>“设置”>“域”功能无关。

- 服务器，授予 Introscope 用户启动和停止企业管理器的权限。

请不要编辑或删除这些资源类。

关于 CA EEM 中的 CA CEM 资源

默认 CA APM 应用程序不需要任何 CA CEM 资源。在 CA EEM 中，资源类可以有零个或更多关联的资源。

但是，CA CEM 支持为业务服务资源类创建资源。创建的业务服务资源将特定于您所在的组织。创建业务服务资源时，需要将一个或多个访问策略与每项业务服务关联。也可以在 CA EEM 中编辑 CA CEM 资源。

可以在 CEM 控制台或 CA EEM 中设置业务服务。有关业务服务的默认访问策略的详细信息，请参阅“默认 CA EEM CEM 访问策略 (p. 114)”。有关创建新业务服务的信息，请参阅《*CA APM 事务定义指南*》。

此外，您可能会发现，需要在 CA EEM 中创建具有唯一访问策略的 CA CEM 资源。例如，如果希望将针对业务服务资源的权限限制给某些 CA CEM 用户和安全用户组，您可能会执行此操作。

重要信息！如果要在 CA EEM 中创建新的 CA CEM 资源，则必须使用现有的 CA CEM 资源类以及在 CA EEM 中定义的访问策略。

要定义新资源，需要定义新的访问策略，如默认 CA EEM CEM 访问策略 (p. 114)中所述。

默认 CA EEM CEM 访问策略

在 CA EEM 中，访问策略为特定于应用程序的资源类和资源定义访问规则。

警告：除非您是 Introscope 管理员，否则不要更改或删除在 CA EEM 中看到的域和服务器访问策略。这些策略仅供 Introscope 使用。

在 CA EEM 中，访问策略包含三个组成部分：资源类、资源和操作。

默认 CA CEM 访问策略向标准 CA CEM 安全用户组提供 CEM 控制台菜单和权限。有关详细信息，请参阅与默认 CA CEM 安全用户组关联的菜单项和权限 (p. 109)。

CA Technologies 建议运行位于 *<企业管理器主目录>/examples/authentication* 目录中的 *eem.register.app.xml* Safex 脚本文件。在运行 Safex 脚本以设置 APM 应用程序时，CA Technologies 会向这些 APM 应用程序提供以下 CA CEM 默认访问策略：

CA CEM 访问策略	说明	资源类/操作	授予以下安全用户组
Web 服务－允许	允许 CEM 系统管理员组查看有关 Web 服务的信息	Web 服务/允许	CEM 系统管理员
用户组－写	CEM 系统管理员组和 CEM 系统配置管理员组对可在“管理”>“用户组”选项卡上执行的所有活动拥有写权限	用户组/写	CEM 系统管理员 CEM 配置管理员
系统安全设置	CEM 系统管理员组对“系统安全设置”下的所有资源拥有写权限	系统安全设置/写	CEM 系统管理员
系统配置设置－写	CEM 系统管理员组和 CEM 配置管理员组对“系统配置设置”下的所有资源拥有写权限	系统配置设置/写	CEM 系统管理员 CEM 配置管理员
系统配置设置－捕获全面的缺陷详细信息	CEM 系统管理员组对“捕获全面缺陷详细信息”复选框拥有写权限	系统配置设置/捕获全面缺陷详细信息	CEM 系统管理员
系统管理设置－写	CEM 系统管理员组对“系统管理设置”下的所有资源拥有写权限	系统管理设置/写	CEM 系统管理员

CA CEM 访问策略	说明	资源类/操作	授予以下安全用户组
报告－写	所有 CEM 组对所有报告拥有写权限	报告/写	CEM 系统管理员 CEM 配置管理员 CEM 分析人员 CEM 突发事件分析人员
突发事件－写	所有 CEM 组均对所有突发事件拥有写权限	突发事件/写	CEM 系统管理员 CEM 配置管理员 CEM 分析人员 CEM 突发事件分析人员
业务服务－读取敏感数据	CEM 突发事件分析人员组对所有业务服务拥有读取敏感数据权限	业务服务/读取敏感数据	CEM 突发事件分析人员
业务服务－读取	CEM 分析人员和突发事件分析人员组对所有业务服务拥有读取权限	业务服务/读取	CEM 分析人员/身份 CEM 突发事件分析人员
业务服务－读写	CEM 配置管理员组对所有业务服务拥有读取和写入权限	业务服务/写入 业务服务/读取	CEM 配置管理员
业务服务－所有权限	CEM 系统管理员组对所有业务服务功能拥有所有权限	业务服务/写入 业务服务/读取 业务服务/读取敏感数据	CEM 系统管理员
业务应用程序－写	CEM 系统管理员和 CEM 配置管理员组对所有业务应用程序拥有写权限	业务应用程序/写	CEM 系统管理员 CEM 配置管理员

CA CEM 访问策略	说明	资源类/操作	授予以下安全用户组
访问策略—所有权限	CEM 系统管理员和 CEM 配置管理员组对所有访问策略拥有所有权限	访问策略/写 访问策略/读取	CEM 系统管理员 CEM 配置管理员

关于 CA CEM 默认业务服务访问策略

如果您部署了 CA EEM 进行 CA CEM 授权，则除了可以在 CA EEM 中创建和修改访问策略之外，还可以使用 CEM 控制台的“访问策略”选项卡来添加、修改或删除与业务服务有关的 CA CEM 访问策略。

如果使用 CA CEM 的“访问策略”选项卡来添加或更改 CA CEM 访问策略，那么：

- 需要对 *“访问策略”* 资源类拥有写权限。
- 通过使用 CEM 控制台来管理访问策略，可以仅向 APM 应用程序安全用户组（而不是单个 APM 用户）授予权限和撤消权限。有关详细信息，请参阅《*CA APM 配置和管理指南*》。
- 也可以直接修改访问策略，如在 CA EEM 中更新 CA CEM 访问策略 (p. 117)中所述。
- CA CEM 将访问策略更改直接发送到 CA EEM 以供存储。

如果希望创建或编辑默认业务服务访问策略，或者将这些访问策略关联到新的业务服务，请参阅《*CA APM 事务定义指南*》。

在 CA EEM 中更新 CA CEM 访问策略

可以在 CA EEM 中更改默认 CA CEM 访问策略，以便：

- 允许 CA CEM 用户或安全用户组查看某个 CA CEM 选项卡。
- 限制 CA CEM 用户或安全用户组查看某个选项卡。

请执行以下步骤：

1. 在 CA EEM 中登录到 APM 应用程序。
   a. 在 CA EEM 登录页面上，从“应用程序:”下拉列表中选择 APM。
   b. 输入登录名和密码。

   CA APM 应用程序默认登录名为 *EiamAdmin*。
2. 导航至“管理访问策略”>“访问策略”。
3. 单击访问策略树中的某个访问策略。例如，报告。
4. 在“策略表”部分中，单击访问策略名称链接。例如，报告－写。
5. 在“身份”部分中，添加或更新与策略关联的 CA CEM 用户或安全用户组。

   例如，如果不再希望 CEM 突发事件分析人员组与“报告－写”访问策略关联，请突出显示“[组] CEM 分析人员”，然后单击“选定身份”框右边的垃圾箱图标。
6. 单击“保存”。

在 CA EEM 中添加新的 CA CEM 访问策略

您可以在 CA EEM 中添加新的 CA CEM 访问策略。如果要这样做，则必须使用默认 APM 资源类和权限集。

请执行以下步骤：

- 运行 Safex 脚本以添加与现有资源类相关联的新策略。请参阅创建并删除 CA EEM APM 前端和业务服务资源访问策略 (p. 89)。

允许 CA EEM Introscope 用户访问 CEM 控制台

如果 Introscope 用户希望查看 CEM 控制台，那么，为了使授权成功，该用户必须至少为一个 CA CEM 资源类定义访问策略。要允许 Introscope 用户访问 CEM 控制台，需要为该用户的至少一个 CA CEM 资源类定义访问策略。

请执行以下步骤：

1. 在 CA EEM 中登录到 APM 应用程序。
   a. 在 CA EEM 登录页面上，从“应用程序:”下拉列表中选择 APM。
   b. 输入登录名和密码。

   CA APM 应用程序默认登录名为 *EiamAdmin*。

2. 导航至“管理访问策略”>“访问策略”。
3. 单击访问策略树中的某个访问策略。例如，系统管理设置。
4. 在“策略表”部分中，单击访问策略名称链接。例如，系统管理设置—写。
5. 在“身份”部分中，将 Introscope 用户添加到访问策略中。
6. 单击“保存”。

CA CEM 的本地身份验证和授权

如果要为 CA CEM 部署本地安全，则 CA APM 将使用 *users.xml* 文件进行身份验证和授权。有关本地安全设置的背景知识，请参阅使用本地安全设置保护 Introscope (p. 29)。

注意：如果您曾从 Wily CEM 4.5 升级，并使用了本地安全设置，则您的 Wily CEM 4.5 用户可能会在 *usersCEM45.xml* 文件中。有关详细信息，请参阅 *《CA APM 安装和升级指南》*。

本地用户和组以及 CA CEM

如果要部署本地安全，则 CA CEM 将在 *users.xml* 文件（如果您曾从 Wily CEM 4.5 升级，则可能是 *usersCEM45.xml*）中提供默认安全用户组。

如果本地 CA CEM 用户（即，在 *users.xml* 文件中定义的用户；如果您曾从 Wily CEM 4.5 升级，则可能是在 *usersCEM45.xml* 中定义的用户）想要访问 CEM 控制台，则他们必须是四个标准 CA CEM 安全用户组之一的成员。

警告：如果您部署了本地授权，则不能将安全用户组添加到默认 CA CEM 组或更改与这些组关联的访问策略。CA CEM 本地安全仅基于这些组。任何修改都可能导致 CA CEM 安全部署出现问题。

如果您的部署在 *users.xml*（如果您曾从 Wily CEM 4.5 升级，则可能是 *usersCEM45.xml*）中对 CA CEM 用户授权，则 CA CEM 访问策略是固定的，不能更改。这意味着：

- 不能添加新的访问策略或更改标准 CA CEM 安全用户组的名称。
- 可以将用户添加到 CA CEM 安全用户组中。
- 每个用户必须属于标准 CA CEM 安全用户组之一：CEM 系统管理员、CEM 配置管理员、CEM 分析人员或 CEM 突发事件分析人员。根据用户所在的组，派生该用户的访问策略。有关标准 CA CEM 安全用户组在 CEM 控制台上所看到的内容的信息，请参阅与默认 CA CEM 安全用户组关联的菜单项和权限 (p. 109)。

可以添加、修改和删除 CA CEM 用户。

请执行以下步骤：

- 在 *users.xml* 中添加/修改/删除 CA CEM 用户。有关详细信息，请参阅在 users.xml 中配置 CA APM 用户和组 (p. 33)。

允许本地 Introscope 用户访问 CEM 控制台

如果某个本地 Introscope 用户要查看 CEM 控制台，则该 Introscope 用户必须同时属于一个 APM 安全用户组和一个 CA CEM 安全用户组。例如，APM 来宾组和 CA CEM 分析人员组。

请执行以下步骤：

- 在 *users.xml* 中将 Introscope 用户添加到 CA CEM 用户组。请参阅“在 users.xml 中配置 CA APM 用户和组 (p. 33)”。

例如，将 Tandav Gupta（*users.xml* 中列出的用于 Introscope 身份验证和授权的用户）添加到“CEM 系统管理员”组。

其他 CA CEM 安全任务

除了 CA EEM CEM 和本地安全身份验证和授权设置任务之外，您还可以了解 CA CEM 的“安全性”链接，并执行以下附加的 CA CEM 安全任务：

- CA CEM 中的“安全”链接 (p. 121)
- 设置新业务服务的默认访问策略（请参阅《*CA APM 配置和管理指南*》）。
- 定义私有参数 (p. 121)
- 保护有关缺陷的 HTTP 请求和响应 (p. 123)

- 符合 FIPS 140-2 标准的加密 (p. 129)
- 配置通过 HTTPS 的 TIM 通信 (p. 131)
- 限制仅通过 HTTPS 的企业管理器访问 (p. 132)
- 如果想限制可以查看 CA CEM 报告中业务服务数据的用户，您必须使用 CA EEM 并将 EEM 配置成 CA APM 的唯一安全领域。有关详细信息，请参阅关于安全领域 (p. 12)以及《*CA APM 配置和管理指南*》中有关使用 CA CEM 报告的内容。

CA CEM 安全链接

在“安全”链接上看到的选项卡取决于安装的是 Introscope 还是 CA APM，以及是否正在使用 CA EEM。

例如，不管您的安全解决方案是什么，始终可以隐藏私有参数。但是，仅当使用 CA EEM 进行身份验证和授权时，才能限制对业务服务的访问。该表根据您实施的安全解决方案指明 CEM 控制台中的可见内容。

此 CA CEM 选项卡是否可见？	仅 Introscope 以及 CA EEM	仅 Introscope 且无 CA EEM	CA APM 以及 CA EEM	CA APM 但无 CA EEM
私有参数	是	是	是	是
访问策略	是	否	是	否
FIPS 设置	否	否	是	是

定义私有参数

HTTP 参数是 HTTP 中使用的名称/值对。常见的 HTTP 参数类型有 cookie、query 和 post 参数。有关 CA CEM 中 HTTP 参数的详细信息，请参阅《*CA APM 事务定义指南*》。

CA CEM 在事务记录和识别过程中记录 HTTP 参数。正常情况下，会显示所有已记录的事务的所有 HTTP 参数。

CA CEM 私有参数允许指定必须保持私有的 HTTP 头信息。CA CEM 私有参数值对系统或配置管理员不可见，对任何 CA CEM 用户也不可见。只有最终用户知道这些参数的值。

提示：并非所有私有参数名都是显而易见的（例如，password 和 pin 与 field1 和 field2）。最好在测试事务上复查 HTTP 参数，以确保在查看活动事务之前所有私有参数都得到保护。

将参数指定为私有时，在 TIM 日志中以及 CEM 控制台中会显示该参数值的任何位置，该值都会显示为六个星号。

您可以使用“*”通配符概况化要匹配的模式。允许使用以下通配符字符串：

- abc*－start matching
- *xyz－end matching
- abc*xyz－start and end matching
- *－如果创建只有一个星号的参数名称模式，则*所有*参数都将为私有

例如，您可能需要在“pin”前面添加星号以扩大其通用性，这样，诸如“userpin”或“login_pin”等其他条目也将识别为私有参数。

注意：每个私有参数仅允许使用一个“*”通配符。不能使用正则表达式 (regex)。

默认 CA CEM 私有参数有：

- *access_id
- pass
- *passcode
- pin
- *password
- pw
- *ssn

修改私有参数

按照以下步骤更新现有的 CA CEM 私有参数。

请执行以下步骤：

1. 选择“安全性”>“私有参数”。
2. 单击参数名称，如 *password。星号表示单词 password 前面可以有任意数量的字符。
3. 为 password 集键入其他参数。例如，如果知道单词 password 始终出现在 HTTP 通信中，并且它前面没有任何字符，则可将 *password 参数更改为 password。
4. 单击“保存”保存新的私有参数。

添加私有参数

按照以下步骤创建新的 CA CEM 私有参数。

请执行以下步骤：

1. 选择“安全性”>“私有参数”。
2. 单击“新建”创建新的私有参数。
3. 键入所需的私有参数。
4. 单击“保存”保存新的私有参数。

保护有关缺陷的 HTTP 请求和响应

出现缺陷时，如果您以具有读取敏感数据权限的 CA CEM 用户身份进行登录，则可以看到用户浏览器所发送的确切内容以及生成的确切内容。此外，如果允许，您还可以查看 query 和 post 参数以及 HTTP 请求和响应的正文信息。

默认情况下，属于“CEM 系统管理员”或“CEM 突发事件分析人员”组的 CA CEM 用户拥有读取敏感数据的权限。

查看缺陷信息

“缺陷详细信息”页面提供了有关缺陷的各类信息，包括有关用户、事务和 Web 服务器的信息。以下过程介绍了如何查看为缺陷捕获的特定 HTTP 参数信息。

请执行以下步骤：

1. 选择“突发事件管理”>“缺陷”。
2. 单击要显示的缺陷的日期和时间。

   “HTTP 信息”区域显示特定于出现缺陷时该用户的体验的缺陷信息，包括：

   - 主机、URL 路径、TCP 端口
   - Cookies
   - HTTP 头（cookie 除外）

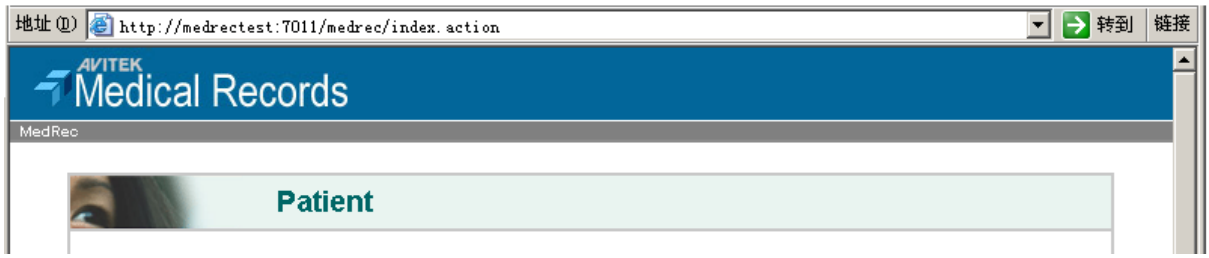
如果允许，还可以在“缺陷详细信息”页面上查看或访问以下 HTTP 信息：

- Query 和 Post 参数
- 响应正文（前 1024 个字节）要更改该值，请参阅更改捕获的响应正文的最大大小 (p. 128)。
- 请求正文（前 1024 个字节）有关详细信息，请参阅关于查看请求正文信息 (p. 124)。

有关使这些 HTTP 信息可见的详细信息，请参阅捕获全面缺陷详细信息 (p. 126)。

3. 要查看出现缺陷时用户正在查看的同一页面，可以将 RequestHeader Referer 内容剪切并粘贴到浏览器中。

```
RequestHeader    Referer:    http://medrectest:7011/medrec/index.action
```



关于查看请求正文信息

查看请求正文信息可能有助于了解缺陷。POST 请求具有请求正文，但请求正文可能为空。GET 请求没有请求正文。

关于查看请求正文信息，需要了解以下两件事情：

- 只能显示格式正确的 XML/HTML。要查看格式不正确的 XML/HTML，请参阅查看格式不正确的 XML/HTML (p. 124)。
- 默认情况下，对于一个缺陷，可以查看请求正文信息的前 1024 个字节。但是，可以更改该值；请参阅更改显示的请求正文信息的最大大小 (p. 125)。

查看格式不正确的 XML/HTML

如果与缺陷关联的 XML/HTML 的格式不正确，则在单击链接查看 HTTP 请求正文时，显示的请求为空白，或看起来不完整。

有一个解决方法可显示格式不正确的 XML/HTML。

注意：要查看*任何*请求正文信息（格式正确或不正确），必须选中“捕获全面缺陷详细信息”复选框，并且必须具有读取敏感数据的权限。有关详细信息，请参阅捕获全面缺陷详细信息 (p. 126)。

请执行以下步骤：

1. 选择“突发事件管理”>“缺陷”。
2. 单击要显示的缺陷的日期和时间。
3. 右键单击 RequestBody 链接并保存文件。
4. 使用文本编辑器或 HTML 编辑器查看请求正文的完整内容。

更改显示的请求正文信息的最大大小

默认情况下，对于一个缺陷，可以查看请求正文信息的前 1024 个字节。如果允许，可以编辑该值以增加或减少查看的信息。

请执行以下步骤：

1. 访问 TIM 系统设置页面。
   a. 在 CEM 控制台中，选择“设置”>“监视器”。
   b. 单击 TIM 的 IP 地址（最右列）。
   c. 输入用户名和密码。

   系统设置页面的默认用户名为 admin。

   此时将显示“TIM 系统设置”页面。
2. 单击“配置 TIM 设置”。

   此时将显示“TIM 设置”页面。
3. 单击 MaxDefectRequestBodySize。
4. 在“新值”字段中，输入希望能查看的最大大小（以字节为单位）。

   请不要将该值设置为不必要的大值。TIM 和企业管理器都需要花费更多的时间来处理较大的值。
5. 单击“变更”。

   更改将立即生效。无需重新启动 TIM。
6. 如果您有多个 TIM，对每个 TIM 重复上述步骤。

限制缺陷信息的显示

可以使用下列两种方法或其中之一来限制显示的缺陷信息量：

- 选择收集并查看 query 和 post 参数以及请求和响应正文信息（请参阅捕获全面缺陷详细信息 (p. 126)）。

- 设置要隐藏的特定私有参数

  如果参数名称与某个私有参数匹配，则将隐藏 post、query、cookie 和 URL 参数（即，相应的值会替换为“***”）。

  使用私有参数，可以：

  - 通过提供确切的参数名称隐藏特定参数
  - 通过在参数名称模式中使用通配符（“*”）隐藏各种类型的参数
  - 通过为参数名称模式创建带有“*”的私有参数隐藏所有参数，即*所有*参数均为私有参数

  有关详细信息，请参阅定义私有参数 (p. 121)。

捕获全面缺陷详细信息

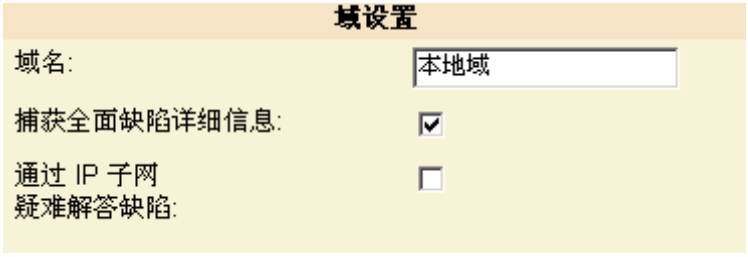
默认情况下，查看 query 和 post 参数以及请求和响应正文信息的功能是被禁用的。如果未选中“捕获全面缺陷详细信息”复选框（在“设置”>“域”页面上），则 TIM 将不会捕获 query 和 post 信息以及请求和响应正文信息。

重要信息！如果有安全忧虑，请不要更改该默认设置，并考虑即使对 CEM 系统管理员也禁用“捕获全面缺陷详细信息”复选框。有关详细信息，请参阅使“捕获全面缺陷详细信息”复选框可用或不可用 (p. 127)。

但是，如果希望可读取敏感数据的用户能够查看缺陷的这一附加信息，请选中“捕获全面缺陷详细信息”复选框。

允许查看 query、post、请求正文和响应正文信息：

1. 选择“设置”>“域”。
2. 选择“捕获全面缺陷详细信息”。



如果页面上未出现“捕获全面缺陷详细信息”复选框，请确保“域”>“监视器”页面上至少列出了一个 TIM。（无需启用 TIM）。

如果“捕获全面缺陷详细信息”复选框不可用，则在允许的情况下，使用以下方法之一更新 CA EEM 或本地权限以使其可用：

- 如果已在 CA EEM 中设置了 CA CEM 用户和访问策略，请参阅“使‘捕获全面缺陷详细信息’复选框可用或不可用 (p. 127)”。
- 如果使用的是本地安全设置，请以“CEM 系统管理员”组的成员身份登录。

3. 单击“保存”。
4. 同步监视器。

注意：如果要执行其他 CA CEM 配置，则可能需要在执行同步之前完成所有配置任务，以便仅必须同步一次监视器。

同步监视器之后，TIM 开始收集缺陷的 query 和 post 信息以及请求和响应正文信息。然后，具有读取敏感数据权限的用户可以查看监视器同步之后捕获的缺陷的这些数据了。

如果以后取消选中该复选框，仍然可以查看选中该复选框时收集的缺陷的信息。

使“捕获全面缺陷详细信息”复选框可用或不可用

默认情况下，属于“CEM 系统管理员”组的所有用户均可选中“捕获全面缺陷详细信息”复选框。这是因为，默认情况下，“CEM 系统管理员”组的所有成员都具有“系统配置设置－捕获全面缺陷详细信息”正文访问策略。

通过将其他用户的组添加到“系统配置设置－捕获全面缺陷详细信息”访问策略中，可以为他们提供访问“捕获全面缺陷详细信息”复选框的权限。

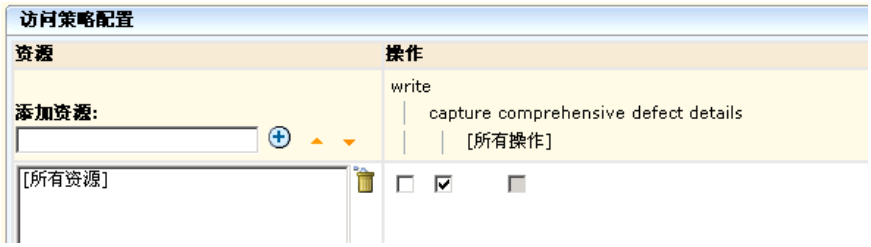
注意：为了使“捕获全面缺陷详细信息”复选框显示在“设置”>“域”页面上，“域”>“监视器”页面上必须至少列出一个 TIM。

请执行以下步骤：

1. 按照在 CA EEM 中更新 CA CEM 访问策略 (p. 117)中的说明，编辑“系统配置设置－捕获全面缺陷详细信息”访问策略。

   添加到“选定身份”中的管理用户或组将能编辑“捕获全面缺陷详细信息”复选框－该复选框允许可读取敏感数据的所有用户查看其他敏感 HTTP 数据（query 和 post 信息以及请求和响应正文信息）。
2. 确保用户或组具有对“系统配置设置”资源类的写入访问权限（这将为用户提供编辑“域”页面的权限）。

3. 保存策略之前，请确保选择了捕获全面缺陷详细信息操作。



重要信息！选中“捕获全面缺陷详细信息”复选框后，CA CEM 用户将可以查看某些潜在的敏感数据。如果您希望提高发生这种情况的难度，可以使该复选框对所有用户都不可用，即使对 CEM 系统管理员（默认情况下具有访问权限）也是如此。

使“捕获全面缺陷详细信息”复选框不可用：

1. 在 CEM 控制台中，确保在“设置”>“域”页面上未选中“捕获全面缺陷详细信息”复选框。
2. 按照在 CA EEM 中更新 CA CEM 访问策略 (p. 117)中的说明，编辑“系统配置设置－捕获全面缺陷详细信息”访问策略。
3. 清除“捕获全面缺陷详细信息”复选框和/或删除“选定身份”列表中的所有条目，并保存捕获全面缺陷详细信息访问策略。

   如果没有为“捕获全面缺陷详细信息”操作选择任何策略，则所有 CA CEM 用户都将无法使 TIM 捕获 query 和 post 信息以及请求和响应正文信息。

更改捕获的响应正文的最大大小

默认情况下，可以捕获响应正文的前 10 KB。如果要增加或减少捕获的响应正文，请按以下过程操作。

请执行以下步骤：

1. 访问 TIM 系统设置页面。
   a. 在 CEM 控制台中，选择“设置”>“监视器”。
   b. 单击 TIM 的 IP 地址（最右列）。
   c. 输入用户名和密码。

   系统设置页面的默认用户名为 admin。

   此时将显示“TIM 系统设置”页面。
2. 单击“配置 TIM 设置”。

   此时将显示“TIM 设置”页面。
3. 单击 MaxDefectResponseBodySize。

4. 在“新值”字段中，输入希望捕获的最大大小（以字节为单位）。

   允许的范围介于 0 和 200000（大约 200 KB）之间。

   请不要将该值设置为不必要的大值。大值需要更多的处理时间和更大的存储空间。

5. 单击“变更”。

   更改将立即生效。无需重新启动 TIM。

6. 如果您有多个 TIM，对每个 TIM 重复上述步骤。

符合 FIPS 140-2 标准的加密

关于 FIPS 140-2

发布的联邦信息处理标准 (FIPS) 140-2 指定了用于软件产品和协议加密的加密库和算法的安全标准。

加密会影响软件安全的以下方面：

- 密码的存储和验证。
- 在产品的组件之间和产品之间发送的所有敏感数据的传递和存储。

关于 CA CEM 和 FIPS 140-2

CA CEM 已经进行了一些修改以增强安全性，从而实现 FIPS 140-2 遵从性：

- 电子邮件服务器的密码是使用符合 FIPS 标准的 128 位 AES 和 SHA 算法进行加密的。
- CA Unicenter Service Desk 的密码是使用符合 FIPS 标准的 128 位 AES 算法进行加密的。
- 您可以采用 128 位加密格式（而不是纯文本格式）将缺陷和用户会话 ID 中包含的 HTTP 信息存储在 APM 数据库中。此 HTTP 信息可能是潜在的敏感数据。

  HTTP 信息可能包含机密数据，如用户名、用户会话 ID、密码、信用卡号以及 Cookie 等。用户会话 ID 可能会被恶意利用以劫持用户会话。

CA CEM 中的 FIPS 104-2 加密功能

下表汇总了 APM 数据库中已经加密（或可以加密）的数据类型。默认情况下，密码是加密的。

该算法是通过 FIPS 认证的 Pure Java 版本 (jsafeFIPS)，来自 RSA Security Inc. Crypto-J 3.5 库。

加密...	在 UI 上查找...	可选？	加密类型	更多信息
SMTP 密码	“系统”>“电子邮件设置”	否	符合 FIPS 标准的 AES	*《CA APM 配置和管理指南》*
包含在缺陷内的 HTTP 信息，包括请求和响应正文	“CEM”>“突发事件管理”>“缺陷”	是	符合 FIPS 标准的 AES	加密缺陷中的 HTTP 信息 (p. 130)
用户会话 ID	仅当与缺陷的全面详细信息一起显示时，才能在 UI 上看到用户会话 ID。	是	符合 FIPS 标准的 AES	加密用户会话 ID (p. 131)

加密缺陷中的 HTTP 信息

默认情况下，与缺陷关联的 HTTP 信息以纯文本格式存储在 APM 数据库中的缺陷元值表中。如果组织已强制使用符合 FIPS 140-2 标准的软件，请按照以下过程对 APM 数据库中存储的 HTTP 信息进行加密。如果已捕获，则会对与缺陷相关联的响应和请求正文进行加密。

即使数据在 APM 数据库中已加密，当该信息在“CEM”>“突发事件管理”>“缺陷详细信息”页面上显示时，也不会进行加密。

HTTP 信息

ResponseHeader	Date:	Mon, 16 Jun 2009 21:12:39 GMT
ResponseHeader	Pragma:	no-cache
ResponseHeader	Server:	WebLogic WebLogic Server 7.0 SP1 Mon Sep 9 2002 206753
ResponseHeader	Content-Language:	en
ResponseHeader	Content-Length:	11191
ResponseHeader	Content-Type:	text/html; charset=ISO-8859-1
ResponseHeader	Expires:	Thu, 01 Jan 1970 00:00:00 GMT
Cookie	JSESSIONID_SAMPLEPORTAL:	lWXHgGLGMR6o96l011iAzdp290Z35D0GMyxsS 614758663

重要信息！ 在选择或取消选择加密时，将删除包括 http 请求和响应正文在内的所有 HTTP 信息（存储在 APM 数据库的缺陷元值表中）。这样可避免在同一数据库表中同时存在纯数据和加密数据。

该表中的数据不是关键数据。默认情况下，会每周将其删除一次。

请执行以下步骤：

1. 选择“安全性”>“FIPS 设置”。
2. 单击“HTTP 缺陷信息”。

   在选择或清除加密时，会收到一条警告，指出将删除 APM 数据库中存储的所有 HTTP 缺陷信息。
3. 单击“保存”。

   将删除以前存储的 HTTP 信息，从现在起，将加密缺陷的 HTTP 信息。

加密用户会话 ID

默认情况下，用户会话 ID 以纯文本格式存储在 APM 数据库中。为了符合 FIPS 140-2 标准，可以选择加密该信息。

如果您的组织要求使用符合 FIPS 140-2 标准的软件，请遵循以下过程来对存储在 APM 数据库中的用户会话 ID 进行加密。

重要信息！在选择或取消选择加密时，将删除所有用户会话 ID（存储在 APM 数据库的用户会话表中）。这样可避免在同一数据库表中同时存在纯数据和加密数据。

这样的删除意味着，在更改 FIPS 设置时，会将所有处于会话中的用户分配给未指定的用户组。因此，CA Technologies 建议在系统上用户通信流量最少时，或者在升级后立即重新启动企业管理器时，更改 FIPS 设置。

请执行以下步骤：

1. 选择“安全性”>“FIPS 设置”。
2. 单击“用户会话 ID”。

   在选择或清除加密时，会收到一条警告，指出将删除所有用户会话 ID。
3. 单击“保存”。

   将删除以前存储的用户会话 ID，从现在起，将加密用户会话 ID。

配置通过 HTTPS 的 TIM 通信

默认情况下，TIM 和运行 TIM 收集服务的企业管理器通过 HTTP 进行通信。但是，为了提高安全性，可以将其配置为改用 SSL over HTTP (HTTPS) 进行通信。

通过将名为 *timTessCommunication.useSsl* 的属性添加到运行 TIM 收集服务的企业管理器上的 *tess-customer.properties* 文件，可完成此操作。

使用 SSL 可能会降低企业管理器与 TIM 之间的通信速度，因此，在应用该配置之前，请考虑此情况。例如，通常情况下，如果企业管理器和 TIM 位于同一防火墙内，则不要应用该配置。

但是，如果 TIM 在管理 VLAN 外部，如在 DMZ（网络隔离区），或可能会通过 WAN（广域网）发送 TIM 数据的非安全环境中，请考虑应用该配置。

请执行以下步骤：

1. 请按照《*CA APM 配置和管理指南*》中的说明修改企业管理器属性默认设置。
2. 打开 *tess-customer.properties* 文件进行编辑时，添加以下行：

   ```
   timTessCommunication.useSsl=1
   ```

   将 *timTessCommunication.useSsl* 属性设置为 1 时，可将企业管理器和 TIM 配置为通过 HTTPS 进行通信。
3. 重新启动企业管理器。

有关详细信息，请参阅《*CA APM 配置和管理指南*》。

限制仅通过 HTTPS 的企业管理器访问

默认情况下，允许在浏览器和企业管理器之间进行 HTTP 通信。通过设置位于 *<EM_Home>\config* 目录中的 *IntroscopeEnterpriseManager.properties* 文件的 *introscope.enterprisemanager.webserver.jetty.configurationFile* 属性，可以配置企业管理器 Web 服务器进行 HTTPS 通信。有关详细信息，请参阅《*CA APM 配置和管理指南*》。

关于 CA APM 事务生成器 (CA APM TG) 安全

CA CEM 可以跟踪和监控 CA APM 事务生成器 (CA APM TG) 执行的综合事务。可以选择专门标识 CA CEM 中的综合事务，并通过创建单独的 CA APM TG 事务用户组，独立于真实事务来单独监控这些事务。

可以将 CA APM TG 事务标识为 CA CEM 中的综合事务，以便能在实际用户受到影响之前，主动解决网站或 Web 应用程序中的问题。通过结合使用 CA APM TG 与 CA CEM 分析，可以确定 Web 应用程序实际用户是否遇到了与模拟用户类似的问题。

如果使用 CA APM TG 来生成综合事务，则可以对控制 CA APM TG 管理服务器访问权限的访问策略进行设置。可以将 CA APM TG 管理服务器配置为使用与 CEM 控制台相同的登录凭据，后者允许管理单个凭据集。CA CEM 用户具有的优势是：针对 CEM 控制台和 CA APM TG 代理配置两者，只需记住一对用户名和密码。

如果使用 CA CEM 的本地安全，并且在“CEM 系统管理员”或“CEM 配置管理员”安全组中定义了用户，则该用户也具有 CA APM TG 管理员权限。

如果使用 CA CEM 的 CA EEM 安全，并且用户被授予对“系统管理设置”或“系统配置设置”访问策略的*写入*权限和*所有操作*权限，则该用户也具有 CA APM TG 管理员权限。

注意：要在 CA EEM 中设置*所有操作*权限，请选中“所有操作”复选框。

有关详细信息，请参阅《*CA APM 事务生成器实施指南*》。

第 5 章： 在 CA CEM 中使用 nCipher

要监控来自受 Thales 提供的 nCipher 硬件安全模块 (HSM) 保护的 Web 服务器的通信，您必须在 CA CEM TIM 中安装 nCipher HSM。

本章包含关于在 TIM 中如何安装和配置 nCipher HSM 的信息。

CA CEM 支持为受 nCipher HSM 保护的 Web 服务器读取 SSL 私钥。

以下显示了关于将 nCipher HSM 与 CA CEM 结合使用您需要了解的内容：

1. 了解 CA CEM 如何支持 nCipher HSM (p. 135)。
2. 在 TIM 上设置 nCipher。 (p. 137)
3. 了解私钥和操作员卡的可用过程。 (p. 146)
4. 了解在密钥或卡发生更改时如何更新私钥和操作员卡。 (p. 151)
5. 排除 nCipher 安装和配置故障。 (p. 151)
6. （可选）了解以前版本的 nCipher 对 CA CEM 的支持。

在 CA CEM 中使用 nCipher

通过在 TIM 中使用 nCipher HSM，可以利用 SSL 私钥获得更高的安全性，并可根据 FIPS 界限内的密钥存储执行操作。HSM 安全界限的 nCipher PCI 行将进行验证，以确保符合 FIPS 140-2 Level 2 和 Level 3 以及通用标准 EAL4+。在使用 nCipher HSM 时，TIM 可以通过使用安全 API 来请求 HTTPS 解密所需的必要信息。

您可以对以下 TIM 使用 nCipher HSM：

- TIM 软件设备
- 多端口监视器上的 TIM

  注意：有关在多端口监视器上部署 TIM 的信息，请参阅《*CA APM 与 CA Infrastructure Management 集成指南*》。

由于 nCipher HSM 直接使用 TIM 软件，因此本章中的说明适用于这两种部署情形。

环境

已针对以下硬件和软件环境认证了 CA CEM 对 nCipher 的支持。

硬件

- CA CEM TIM 设备
- nShield Solo PCI 卡

软件

- CA APM 版本 9.5
- nCipher Software Supplement (nCSS) 版本 11.30

重要信息！ nCipher 支持的版本包括 TIM 和 Web 服务器的必需版本。使用更早的版本可能会产生意外的结果。

测试

这些版本的 CA CEM 和 nCipher 都已在 Sun OS 5.10 上使用 Sun Java System Web Server 7.0 进行了测试。

有关 nCipher 支持的环境，请参阅 nCipher 文档。如果您对 CA CEM 配置有任何疑问，请与 CA Support 联系。

先决条件

要使用该功能，必须：

- 有一个或多个 Web 服务器，其 SSL 私钥受 nCipher 安全全局保护。所有 Web 服务器私钥必须受相同的安全全局保护。
- 在与 TIM 相同的 nCipher 版本上有多个 Web 服务器。
- 有权访问 Web 服务器，包括访问 Web 服务器的以下内容：
  - 安全全局
  - 管理员卡集
  - 操作员卡集
  - 密码短语
- 有权访问 TIM 计算机，并且能够：
  - 将 Thales-nCipher 硬件安全模块 (HSM) 安装在 TIM 计算机中。
  - 按照 nCipher 产品文档中的说明在 TIM 上构建内核驱动程序。

  - 在 TIM 上安装 nCipher Software Supplement，并将其配置为能访问 HSM。
  - 使用 nCipher Software Supplement (nCSS) 11.30。尽管较早的软件版本中可能会有相同的功能，但此文档中对 nCipher 文档的任何引用均特定于《*nShield User Guide for Unix-based OS version 6.3*》。
- 熟悉 CA CEM、TIM 计算机和 CA CEM 文档。
- 熟悉 Thales-nCipher 产品文档，特别是针对 TIM 计算机和 Web 服务器中的 HSM 的用户指南。

设置 CA CEM 以支持 nCipher

以下各节介绍了如何设置 TIM 以读取受 nCipher 硬件安全模块 (HSM) 保护的 SSL 私钥。

要使 TIM 与 nCipher HSM 结合使用，必须遵循下面一系列过程。

1. 在 TIM 中安装 nCipher 硬件 (p. 137)
2. 在 TIM 上安装 nCipher 软件 (p. 138)
3. 生成内核驱动程序 (p. 138)
4. 验证 TIM 上的 nCipher 安装 (p. 139)
5. 在 nCipher 安全全局中登记 TIM HSM (p. 140)
6. 将 Web 服务器的 nCipher 私钥上传至 CA CEM (p. 143)
7. 在 TIM 上配置 nCipher HSM (p. 143)
8. 验证受 nCipher 保护的 Web 通信 (p. 146)

完成所有过程后，便可以使用 TIM 和 nCipher HSM 开始监控 HTTPS 通信了。

在 TIM 中安装 nCipher 硬件

以下是*在* TIM 中安装 nCipher 硬件的基本步骤。有关具体内容，请参考 nCipher 文档。

注意：如果您有多个 TIM 计算机，而且并非全都配备有 nCipher，则应当配置带 nCipher 的 TIM 计算机以监控受 nCipher 保护的 Web 服务器。这有助于更好地平衡负载。

请执行以下步骤：

1. 获取 nShield HSM 硬件：PCI 卡和读卡器。
2. 获取与您的硬件和环境匹配的 nCipher 文档。
3. 获取 TIM 计算机随附的硬件文档。
4. 按照 nCipher 文档中的说明在 TIM 计算机中安装硬件。如有需要，请参考 TIM 计算机的硬件文档。
5. 验证接点是否已完全插入到连接器中。
6. 验证后面板是否已与机箱中的存取槽正确对齐。
7. 继续执行在 TIM 上安装 nCipher 软件 (p. 138)。

在 TIM 上安装 nCipher 软件

以下是*在* TIM 上安装 nCipher 软件的基本步骤。有关具体内容，请参阅 nCipher 文档。

请执行以下步骤：

1. 获取适用于您的硬件和环境的 nCipher 软件。
2. 获取适用于您的软件和环境的 nCipher 文档。

   按照 nCipher 文档中的说明在 TIM 服务器上复制和安装所有 nCipher 软件。具体而言，请参阅 nCipher CD 中的 nShield_Quick_Start_Guide 和 version.txt 文件。version.txt 文档列出了所有软件包名称。

   注意：如果在启动 TIM 之后安装 nCipher 软件，请重新启动 TIM 以建立与 nCipher 硬件的连接。
3. 验证“TIM 系统设置”页面是否包括以下 nCipher 菜单选项：
   - 查看 nCipher 状态
   - 配置 nCipher

   这些菜单选项会在安装了 nCipher 软件后出现。
4. 继续执行生成内核驱动程序 (p. 138)。

构建内核驱动程序

要将 nShield HSM 与 TIM 结合使用，必须构建内核驱动程序。nCipher 为 nCipher PCI 内核驱动程序 (*nfp*) 和 *makefile* 提供源，用于生成作为可加载模块的驱动程序。

下载所需的开发工具（来自 Red Hat 分发版的 RPM）。

此外，还需要相关的实施文档（与您的软件匹配的本文档版本，以及 Thales nCipher 文档），以便在 TIM 计算机上安装和配置 nCipher 软件。

请执行以下步骤：

重要信息！下载与 TIM 上的 Red Hat 版本匹配的 RPM。

1. 从 Thales 获取《*nShield User Guide for Unix-based OS*》和《*nShield Quick Start Guide for Unix-based OS*》文档。
2. 按照 nCipher 文档的说明生成内核驱动程序。
3. 继续执行验证 TIM 上的 nCipher 安装 (p. 139)。

验证 TIM 上的 nCipher 安装

安装了 nCipher 硬件和软件之后，可以使用“TIM nCipher 状态”页面验证新硬件和软件。

验证软件

验证 nCipher 软件是否在 TIM 上正常运行。

请执行以下步骤：

1. 转到“TIM 系统设置”>“查看 nCipher 状态”页面。
2. 复查该页面上的输出。*/opt/nfast/bin/enquiry* 输出的第一部分应显示如下内容：

```
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        ...
 mode                 operational
```

3. 如果输出未显示 operational，请参阅 nCipher 文档。

验证硬件

验证 nCipher 硬件是否在 TIM 上正常运行。

请执行以下步骤：

1. 转到“TIM 系统设置”>“查看 nCipher 状态”页面。
2. 复查该页面上的输出。确保 */opt/nfast/bin/enquiry* 输出中至少有一个“Module”（模块）部分；该部分显示如下内容：

```
Module #1:
 enquiry reply flags  none
```

```
enquiry reply level  Six
serial number        ...
mode                 operational
```

3. 如果输出未显示 operational，请参阅 nCipher 文档。
4. 继续执行在 nCipher 安全全局中登记 TIM HSM (p. 140)。

在 nCipher 安全全局中登记 TIM HSM

要使安装在 TIM 计算机中的 HSM 能够访问 Web 服务器私钥，必须在保护 Web 服务器密钥的安全全局环境中对其进行登记。nCipher 安全全局框架包括：

- 硬件安全模块 (HSM)—PCI 硬件卡
- 管理员卡集 (ACS)—用于控制管理和配置访问的智能卡
- 操作员卡集 (OCS)—用于控制访问的智能卡
- SSL 私钥和证书数据

有关 nCipher 安全全局概念的详细信息，请参阅《*nShield User Guide for Unix-based OS*》。

重要信息！在开始登记之前，请验证是否在 Web 服务器和 TIM 上同时运行 nCipher 软件的最低版本。请参阅“软件 (p. 136)”。

登记过程要求具备以下条件：

- TIM 计算机及其 nCipher HSM 的物理访问
- TIM 计算机上的命令行会话，以 root 或 *nfast* 组成员的用户身份运行
- 安全全局的管理员卡集 (ACS) 的法定数目
- 每个操作员卡集具有一个密码短语

重要信息！在开始之前，将 */opt/nfast/kmdata/local* 目录（或 Windows 上的 *%NFAST_KMDATA%\local*）的*副本*备份到 Web 服务器上，包括其所有内容。将备份存储在安全位置。

将安全全局从 Web 服务器复制到 TIM

TIM 需要 Web 服务器的安全全局的副本以开始登记过程。

请执行以下步骤：

1. 将 */opt/nfast/kmdata/local* 目录（或 Windows 上的 *%NFAST_KMDATA%\local*）的内容复制到 Web 服务器上，包括其所有内容。
2. 将 */opt/nfast/kmdata/local* 目录的副本放置在 TIM 计算机上，包括其所有内容。
3. 验证 TIM 上的新目录是否包含安全全局中每个智能卡集的“world”文件、“cards_*”和“card_*”文件，以及受安全全局保护的每个密钥的 key_* 文件。

在安全全局中登记 TIM

需要在 TIM 计算机上使用命令行会话，以便在安全全局中登记 TIM。

请执行以下步骤：

1. 将 nCipher HSM 后面的开关移至“I”位置。
2. 在命令行中运行：

   /opt/nfast/bin/nopclearfail -ca

   -ca 选项指定 *nopclearfail* 命令将对所有可用的 nCipher 模块进行初始化。
3. 注意在执行下一步之前的 ACS 卡及其密码短语的正确数量。
4. 在命令行中运行：

   /opt/nfast/bin/new-world -I

   new-world 实用工具会提示您插入 ACS 卡并键入其密码短语，直到达到法定数目为止。（*-I* 选项表示要将某个模块添加到现有的安全全局中。）

   继续处理卡，直到 *new-world* 完成为止。

   有关 *new-world* 实用工具的详细信息，请参阅 nCipher 文档。
5. 将 nCipher HSM 背后的开关移至“O”位置。
6. 在命令行中运行：

   /opt/nfast/bin/nopclearfail -ca

   完成该过程后，HSM 就可以使用受该安全全局保护的任何私钥了。TIM HSM 已被登记到安全全局中，并且可以访问 Web 服务器私钥。

验证登记

应该验证安全全局和 TIM HSM 是否可用，以及是否能访问 Web 服务器私钥。

请执行以下步骤：

1. 转到“TIM 系统设置”>“查看 nCipher 状态”页面。
2. 复查“TIM 系统设置”>“查看 nCipher 状态”页面上的输出。*/opt/nfast/bin/enquiry* 输出的第一部分应显示运行模式：

```
Server:
 enquiry reply flags  none
 enquiry reply level  Six
 serial number        ...
 mode                 operational
```

3. 如果输出未显示 operational，请参阅 nCipher 文档。
4. 复查“TIM 系统设置”>“查看 nCipher 状态”页面上的输出。确保安全全局和模块在 */opt/nfast/bin/nfkminfo* 输出中显示 Usable（该单词前面没有感叹号）：

```
全局
 generation  2
 state    0x7270000 Initialised Usable Recovery !PINRecovery !ExistingClient
RTC NVRAM !FTO SEEDebug
 n_modules   1
.
.
.
Module #1
 generation 2
 state      0x2 Usable
 flags      0x10000 ShareTarget
 n_slots    2
```

5. 如果输出未显示 Usable，请参阅 nCipher 文档。
6. 通过发布 */opt/nfast/bin/preload ... pause*（*其中 ...* 应替换为用于选择特定受保护密钥的选项），应该可以将任一受保护的密钥加载到 HSM 中（有关详细信息，请参阅 *预加载 — 帮助*）。

   注意：保护密钥的 OCS 可能会使用 NotPersistent 选项。在这种情况下，只要卡仍留在插槽中，应用程序就可以使用预加载的密钥。如果已移除卡，则加载的密钥会失效，任何试图使用预加载密钥的应用程序将不能进行加密操作。必须重新启动应用程序和预加载进程才能重新加载密钥。

7. 继续执行将 Web 服务器的 nCipher 私钥上传至 CA CEM (p. 143)。

将 Web 服务器的 nCipher 私钥上传至 CA CEM

TIM 仅在 *embed* 应用程序类型中接受私钥。如果您的 Web 服务器不是 Apache，则需要在上传密钥之前对其重新定位。

私钥可单独受 HSM 保护，也可受 OCS 保护。OCS 可以使用密码短语进行保护。

nCipher 操作员卡集可包含多张卡（它们可能全都是必需的）。但是，TIM 仅支持一张卡（因为进程在 TIM 中是自动执行的）。如果您的 Web 服务器使用多张卡，则需要将其合并才能用于 TIM。

要将私钥上传至 CA CEM，请执行以下操作：

1. 如果 Web 服务器的私钥不是 *embed* 应用程序类型，则需要将其重新定位。请参阅重新定位 Web 服务器私钥 (p. 147)。
2. 将文件 */tmp/webserver1.pem* 上传至 CA CEM。请参阅《*CA APM 配置和管理指南*》中有关使用 CA CEM 监控安全 Web 应用程序的章节。
3. 如果现有的操作员卡集太小，不足以容纳 TIM 卡，则可以创建一个新集；请参阅创建新的操作员卡集 (p. 149)。
4. 如果 TIM 需要使用多个私钥，则可能需要使用同一操作员卡集来保护密钥。有关详细信息，请参阅合并操作员卡集 (p. 149)。

验证私钥上传：

1. 转到“TIM 系统设置”>“查看 TIM SSL 服务器状态”页面。
2. 验证 Web 服务器的 IP 地址和端口号。
3. 继续执行在 TIM 上配置 nCipher HSM (p. 143)。

在 TIM 上配置 nCipher HSM

现在，可以配置 TIM 以便与 nCipher HSM 和 OCS（可选）结合使用。

配置 TIM

请执行以下步骤：

1. 转到“TIM 系统设置”>“配置 nCipher”页面。
2. 如果需要在 TIM 上启用 nCipher 支持，请单击“启用 nCipher HSM”。

   下次重新启动 TIM 时将启用该项支持。
3. 如果需要在 TIM 上禁用 nCipher 支持，请单击“禁用 nCipher HSM”。

   下次重新启动 TIM 时，它将被禁用。

4. 如果希望每次重新启动 TIM 时都可以使用 nCipher HSM 支持，则必须键入操作员卡集名称，然后单击“保存”。

   有关详细信息，请参阅关于无人值守操作 (p. 145)。

5. 如果操作员卡有密码短语，则可以将其保存，也可以在每次重新启动 TIM 时输入密码短语：

   a. 键入要保存的操作员卡密码短语，然后单击“保存”。

      该密码短语会以加密方式保存，无法使用 TIM Web 页面读取它。可将此方法用于操作员卡有密码短语时的无人值守操作。有关详细信息，请参阅关于无人值守操作 (p. 145)。

   —或—

   b. 键入操作员卡密码短语，然后单击“启动 TIM”（将使用键入的密码短语）

      密码短语不会被保存。

6. 如果需要删除保存的密码短语，请单击“删除保存的密码短语”。

重新启动 TIM 并验证配置

要启用或禁用 nCipher 支持，则需要在保存密码短语之后重新启动 TIM。

请执行以下步骤：

1. 单击“返回 TIM 设置”。
2. 单击“启动或停止 TIM”。
3. 单击“启动 TIM”或“重新启动 TIM”。
4. 验证配置更改。

   页面上将显示状态，如下所示：

```
TIM Control
Stopping old nCipher preload process
Using nCipher HSM
Running background nCipher preload
Operator card set "testocs1" specified
preload log:
-----------------------------------------------
Loading cardsets:
testocs1 on modules 1
Checking modules and reading cards ...
Checking modules and reading cards ...
Loading `testocs1':
Module 1 slot 0: `testocs1' #3
Module 1 slot 0: Enter passphrase: (reading cards)
Module 1 slot 0: Enter passphrase:
```

```
********
Module 1 slot 0:- passphrase supplied - reading card
Module #1 Slot #0: Processing ...
Card reading complete.
Stored Cardset: testocs1 (1ff8...) on module #1
Stored Unsure -- multiple objects on module #1
Loaded embed aee3ef6fefb153f743843a284954828c09328500 key (RSAPrivate) on
modules 1
-----------------------------------------------
The action you requested may take several seconds to complete.
```

注意：可在 */etc/wily/cem/tim/logs/ncipher/preload-log.txt* 中找到相同的 nCipher 日志信息。

5. 验证卡集名称是否正确。
6. 查找以下几行内容：

```
Card reading complete.
Loaded embed < key > (RSAPrivate) on modules < n >
```

7. 继续执行验证受 nCipher 保护的 Web 通信 (p. 146)。

关于无人值守操作

正常情况下，TIM 会在系统启动时自动启动。要在 HSM 上实现此功能，请执行以下操作：

- 用于 TIM 计算机的操作员卡集的法定数目必须为 1。这与 Web 服务器计算机的操作员卡集无关。
- TIM 计算机的操作员卡不能有密码短语，或者必须使用“TIM 系统设置”>“配置 nCipher”页面来保存或输入密码短语。有关如何从操作员卡中删除密码短语的说明，请参阅从操作员卡中删除密码短语 (p. 148)。
- 必须将操作员卡保留在与 TIM 计算机中的 HSM 连接的读卡器中。
- 必须使用“TIM 系统设置”>“配置 nCipher”页面来保存操作员卡集的名称。

重要信息！如果操作员卡中的某个密码短语与保存的密码短语不匹配，或者读卡器中的卡不正确（或没有卡），则将无法自动启动 TIM。（这不在 TIM 日志中，但可在 */etc/wily/cem/tim/logs/ncipher/preload1-log.txt* 和 *preload2-log.txt* 文件中找到。）在这种情况下，可以使用 nCipher 配置页面，并启动 TIM 或保存所需的信息，然后使用“TIM 系统设置”>“启动或停止 TIM”页面来启动 TIM。

验证受 nCipher 保护的 Web 通信

验证使用 nCipher 的 CA CEM 的功能。可以验证 Web 通信。

使用 TIM 事务检查验证 SSL 功能：

注意：请参阅《*CA APM 配置和管理指南*》中有关使用 CA CEM 监控安全 Web 应用程序的信息。请参阅有关*验证使用 SSL 的 CA CEM 的功能*的信息。

使用 TIM SSL 服务器状态验证 SSL 功能：

1. 转到“TIM 系统设置”>“查看 TIM SSL 服务器状态”页面。
2. 如果看到了到无解码故障的 nCipher 服务器的连接，则 TIM 可以使用 nCipher 来监控 Web 服务器通信。

使用 TIM 跟踪验证 SSL 功能：

1. 转到“TIM 系统设置”>“配置 TIM 跟踪选项”页面。
2. 选择启用“跟踪 HTTP 组件”选项。
3. 如果 TIM 日志向加密的服务器显示了所有组件，并且该服务器使用 nCipher，则说明正在进行解密。

使用 nCipher 密钥和操作员卡

本节旨在提供有关如何准备将 Web 服务器私钥与 TIM 结合使用的信息。此处介绍的 Thales-nCipher 实用工具操作应在 Web 服务器上执行。

重要信息！在开始之前，请对 */opt/nfast/kmdata/local*（或 Windows 上的 *%NFAST_KMDATA%\local*）进行备份。这对于 TIM 计算机和 Web 服务器都很重要。

本部分包括以下主题：

重新定位 Web 服务器私钥

注意：本节假定您拥有 nCipher 为 Web 服务器生成的私钥。

nCipher 安全全局可为各种应用程序编程接口 (API)（如 PKCS#11、Java JCE、OpenSSL、Microsoft CAPI（Windows 上）和 nCipher 本机 API）提供密钥。根据生成密钥时所选的应用程序类型，将使用实际的加密密钥材料存储不同的信息，以便简化从该 API 进行的访问。

现有密钥可供其他应用程序使用。该过程称为重新定位。重新定位操作时，会将新密钥 blob 保存到文件系统中，其中包含相同的加密密钥材料，以及特定于新应用程序类型的新访问权限信息。

以下是各种 Web 服务器软件包所使用的不完整 API 列表：

服务器	平台	API	应用程序
Apache	全部	OpenSSL	embed
Sun ONE	全部	PKCS#11	pkcs11
MS IIS	Windows	MS CAPI	mscapi
Tomcat	全部 (Java)	JCE	jce

TIM 计算机需要 *embed* 应用程序类型的密钥。除了 */opt/nfast/kmdata/local* 目录中的加密密钥 blob 之外，embed 密钥也随 *embedsavefile* 文件（该文件将 OpenSSL 指向要使用的特定密钥 blob）一起提供。

要将 Sun ONE Web 服务器密钥从应用程序类型 pkcs11 转换为 embed，请执行以下操作：

- 要将应用程序类型 *pkcs11* 的密钥重新定位到 *embed* 类型，请参考下面的示例。

  在此示例中，名为 *MyOCS* 的 1/N 操作员卡（可保护相应的密钥）位于 HSM 读卡器中。使用 Enter 或 Return 键接受默认值。

```
$ /opt/nfast/bin/generatekey --retarget embed
from-application: Source application? (custom, embed, hwcrhk, pkcs11, simple)
  [default custom] > pkcs11
from-ident: Source key identifier?
(uc66d0f2df3103e32c5703e8de0cfb172a1b35cf82-9051fc31c13c7716a1ac140fdea2eded0
4c0f419)
[default
uc66d0f2df3103e32c5703e8de0cfb172a1b35cf82-9051fc31c13c7716a1ac140fdea2eded04
c0f419]
>
```

```
embedsavefile: Filename to write key to? []
> /tmp/webserver1.pem
plainname: Key name? [] > webserver1
key generation parameters:
 operation         Operation to perform      retarget
 application       Application               embed
 slot              Slot to read cards from   0
 verify            Verify security of key    yes
 from-application  Source application        pkcs11
 from-ident        Source key identifier
uc66d0f2df3103e32c5703e8de0cfb172a1b35cf82-9051fc31c13c7716a1ac140fdea2eded04
c0f419
 embedsavefile     Filename to write key to  /tmp/webserver1.pem
 plainname         Key name                  webserver1

Loading `MyOCS':
 Module 1: 0 cards of 1 read
 Module 1 slot 0: `MyOCS' #1
 Module 1 slot 0:- passphrase supplied - reading card
Card reading complete.

Key successfully retargetted.
Path to key:
/opt/nfast/kmdata/local/key_embed_b4c36e18ff38d2d45a2df425abd9febfaf873da4
```

从操作员卡中删除密码短语

要使用受 OCS 保护的密钥以无人值守方式运行 TIM，一种可能是从位于 TIM 读卡器中的 OCS 卡上删除密码短语。

请执行以下步骤：

- 使用 *cardpp*：

```
$ /opt/nfast/bin/cardpp --change -m 1

Checking/changing passphrase(s):
 Module 1 slot 0: `MyOCS' #1
 Module 1 slot 0: Enter passphrase:                                    [^D:
done]
 Module 1 slot 0:- passphrase supplied - reading card
 Module 1 slot 0: Enter new passphrase: <return>                       [^D:
done]
 Module 1 slot 0:- no passphrase specified - removing passphrase
 Module #1 Slot #0: Processing ...                                     [^D:
done]
 Module 1 slot 0: `MyOCS' #1: Passphrase removed
Insert/change card in module (or change module mode)            [^D: done]
<Control-D>
```

```
Done.
```

注意：可以使用没有密码短语的 OCS 卡运行 TIM；但 Web 服务器软件可能不支持此功能。

创建新的操作员卡集

如果现有操作员卡集 (OCS) 太小，不足以容纳 TIM，则可创建一个新集。

例如，如果现有 Web 服务器具有包含一张卡的卡集，则需要创建一个新卡集（至少包含两张卡），以便也能容纳 TIM 计算机的卡。

注意：应使用 */opt/nfast/kmdata/local* 的本地副本在 TIM 计算机上针对重新定位的密钥执行此操作。

请执行以下步骤：

- 使用 *createocs*：

  ```
  /opt/nfast/bin/createocs -Q 1/n -N name
  ```

  其中 *n* 是卡集的大小，*name* 是为卡集提供的名称。

创建新的操作员卡集后，可以将密钥恢复到新卡集上，如合并操作员卡集 (p. 149)中所述。

合并操作员卡集

如果 TIM 要使用多个密钥，那么用同一操作员卡集 (OCS) 保护它们可能会有优势。如果具有受不同 OCS 保护的多个密钥，*且*这些密钥属于同一安全全局*并*对这些密钥启用了“恢复”，则可以将所有这些密钥恢复到同一 OCS，从而可以通过单个 OCS 加载和访问它们。

请执行以下步骤：

注意：该操作需要访问法定数目的管理员卡集 (ACS) 进行授权。

重要信息！请不要对活动的 Web 服务器密钥执行 *rocs* 操作。请在 TIM 计算机上对副本执行此操作。

注意：如果需要重新定位密钥，请在处理 OCS 之前执行此操作。有关详细信息，请参阅重新定位 Web 服务器私钥 (p. 147)。

1. 要检查密钥是否已启用“恢复”，请使用 *nfkminfo*：

   ```
   $ /opt/nfast/bin/nfkminfo -k embed
   Key listing AppName embed (1 keys):
   ```

```
 AppName embed              Ident 5dce27b0a84b517b0db7b5aa2f09452e27a13d38
$ /opt/nfast/bin/nfkminfo -k embed 5dce27b0a84b517b0db7b5aa2f09452e27a13d38
Key AppName embed Ident 5dce27b0a84b517b0db7b5aa2f09452e27a13d38
 BlobKA length         1052
 BlobPubKA length      444
 BlobRecoveryKA length 1208
 name                  "MyKey"
 hash                  d96ee8282cc7f76ea32df1ce299ab087a206e530
 recovery              Enabled
...
```

2. 将标识符从第一个调用复制到第二个调用。*recovery Enabled* 行显示可以将密钥恢复到新的 OCS。

```
$ /opt/nfast/bin/rocs -i
`rocs' key recovery tool
Useful commands: `help', `help intro', `quit'.
rocs> list cardsets
No. Name                    Keys (recov) Sharing
  1 iWorld1of1              0 (0)        1 of 1; persistent
  2 NonPersistentOCS        9 (9)        1 of 1
rocs> target 1
rocs> list keys
  No. Name                    App        Protected by
    1 MyKey                   caping     module
    2 MyKey                   caping     module
    3 MyKey                   embed      module
    4 Example label           pkcs11     NonPersistentOCS
    ...
rocs> mark 4
rocs> recover

Authorising OCS replacement:
 Module 1: 0 cards of 1 read
 Module 1 slot 0: empty
 Module 1 slot 0: Admin Card #1
... prompt for the ACS passphrase ...
 Module 1 slot 0:- passphrase supplied - reading card
Card reading complete.


Loading `iWorld1of1':
 Module 1: 0 cards of 1 read
 Module 1 slot 0: Admin Card #1
 Module 1 slot 0: empty
 Module 1 slot 0: `iWorld1of1' #1
... prompt for the OCS passphrase ...
 Module 1 slot 0:- passphrase supplied - reading card
Card reading complete.
```

```
rocs> save 4
rocs> quit
```

更新私钥和操作员卡

如果在 Web 服务器上更新了密钥管理数据（例如，创建了新的密钥或卡集），则还需要更新密钥管理数据文件的 TIM 副本。

在获取了 TIM HSM 的新密钥或卡集后，请执行以下步骤。

请执行以下步骤：

1. 在 nCipher 安全全局中登记 TIM HSM (p. 140)。
2. 将 Web 服务器的 nCipher 私钥上传至 CA CEM (p. 143)。
3. 在 TIM 上配置 nCipher HSM (p. 143)。
4. 验证受 nCipher 保护的 Web 通信 (p. 146)。

使用 CA CEM 排除 nCipher 故障

可能需要使用 CA CEM 排除 nCipher 的安装故障。

症状：

安装 nCipher 卡之后 TIM 未启动。或者，TIM 上的 nCipher 安装不工作。

解决方案：

1. 复查“TIM 系统设置”>“查看 nCipher 状态”页面。
2. 请参阅验证 TIM 上的 nCipher 安装 (p. 139)。

症状：

nCipher HSM 未按预期运行。

解决方案：

1. 每次将卡插入插槽时，插入计数就会增加。因此，如果卡未正确插入而随后重新插入，此操作将反映到计数中。
2. 复查“TIM 系统设置”>“查看 TIM SSL 服务器状态”页面。请参阅验证受 nCipher 保护的 Web 通信 (p. 146)。
3. 复查 */etc/wily/cem/tim/logs/ncipher/preload-log.txt* 中的 nCipher 日志信息。请参阅重新启动 TIM 并验证配置 (p. 144)。
4. 复查 TIM 日志。

5. 重新定位密钥 (generatekey) 时，可能会收到一条消息，指示“ERROR: Module #1: LoadBlob (loading private blob) failed: Malformed”。在 nCipher 软件版本不匹配时，可能会发生此情况。请升级您的 Web 服务器以匹配 TIM 上的 nCipher 版本，或者与 Thales 技术支持联系。
6. 如果操作员卡中的某个密码短语与保存的密码短语不匹配，或者读卡器中的卡不正确（或没有卡），则将无法自动启动 TIM。（这不在 TIM 日志中，但可在 */etc/wily/cem/tim/logs/ncipher/preload1-log.txt* 和 *preload2-log.txt* 文件中找到。）在这种情况下，可以使用 nCipher 配置页面，并启动 TIM 或保存所需的信息，然后使用“TIM 系统设置”>“启动或停止 TIM”页面来启动 TIM。
7. 复查 TIM 启动日志。
8. 是否有来自 Web 服务器的 OCS 和操作员卡？如果没有，TIM 可能不会启动。
9. 是否已将安全全局环境的二进制副本从 Web 服务器复制到 TIM？如果没有，则这就是在重新定位期间出现格式错误的 blob 的原因。
10. 确保在运行 new-world 时有 kmdata。
11. 了解在运行 new-world 之前 ACS 卡及其密码短语的数量。
12. 确保将 TIM HSM 设置到 I 位置，并将跳线设置为 OFF 以进行预初始化。
13. 确保将 ncipher HSM 设置到 I 以进行预初始化（在运行 new-world 之前），在运行 new-world 之后设置到 O。
14. 在运行 new-world 之前，不要忘记清除寄存器。

症状：

我安装了 nCipher 卡和软件，但 TIM 不会从 Web 服务器将数据解密，并且在启动时，TIM 日志将显示以下消息：

```
Initializing SSL crypt engine
Sslinterface: "chil" SSL engine initialization failed
```

解决方案：

1. 验证是否已安装 nCipher 捆绑包 Chil SSL：
   a. 登录到 TIM 控制台（使用 PuTTY 或类似的 ssh 客户端）。
   b. 验证以下 nCipher 捆绑包是否存在：
   /opt/nfast/toolkit/hwcrhk/libnfhwcrhk.so
2. 如果 nCipher 捆绑包 Chil SSL 不存在，则从 nCipher CD 进行安装：
   a. 有关详细信息，请参阅 nCipher 安装指南。（在 nCipher 11.30 中，该捆绑包命名为 */<CD>/linux/lib6-3/nfast.hwcrhk/user.tar*。）
   b. 重新启动 TIM。

   TIM 日志应显示 Chil SSL 捆绑包已初始化。

```
Wed Mar 30 02:09:20 2011 19826   Initializing SSL crypt engine
Wed Mar 30 02:09:20 2011 19826   sslinterface: "chil" SSL engine found
Wed Mar 30 02:09:20 2011 19826   sslinterface: "chil" SSL engine
initialized
```

症状：

我希望验证 TIM 是否正在对由具有 nCipher 的 Web 服务器加密的 HTTPS 通信进行解密。

解决方案：

在 TIM 日志中查找跟踪连接并跟踪 HTTPS 组件。

您应该会同时看到连接和 HTTPS 组件。例如，如果 https 服务器在端口 9966 上为 172.16.163.52，则如果启用了连接跟踪，这些组件可能会显示如下：

```
Wed Mar 30 02:34:00 2011 19826   Trace:
[172.16.163.32]:3691->[172.16.163.52]:9966 opened
```

或者如果启用了组件跟踪，可能会显示如下：

```
Wed Mar 30 02:34:00 2011 19826   Trace: Component #18 request:
172.16.163.52/testpage.html client=[172.16.163.32]:3691
server=[172.16.163.52]:9966 at 02:34:00
```

如果 TIM 无法将通信解密，将仅显示以下连接消息：

```
Wed Mar 30 02:34:00 2011 19826   Trace:
[172.16.163.32]:3691->[172.16.163.52]:9966 opened

Wed Mar 30 02:34:00 2011 19826   Trace:
[172.16.163.32]:3691->[172.16.163.52]:9966 closed
```

第 6 章： 在 CA APM 中使用智能卡身份验证

本章包括以下主题：

关于在 CA APM 中使用智能卡

安全环境经常要求使用单一入口点以易于访问管理。如果没有单一入口点，安全管理员必须使用不同的安全级别、要求和用户访问权限来管理几个程序。通过要求使用智能卡来访问所有受控资源，智能卡提供单一入口点。

访问权限是基于用户在 CA APM 中定义的本地安全或 CA EEM 权限授予用户的。

CA APM 为 WebView、Web Start 和 CEM 控制台提供了智能卡身份验证。

本节中的主题向您介绍了智能卡身份验证：

智能卡验证选项

您可以配置智能卡验证以使用以下选项之一：

- *证书吊销列表 (CRL)*

  验证证书是否有效的最常见方式。

  CRL 文件是平面文件，包含吊销的证书序列号。因为证书颁发机构不断增加证书，CRL 文件经常会过期。CRL 文件在预先确定的时间到期，必须重新进行加载。这些文件会占用大量内存，必须将它们放置在本地文件系统上。通常，系统管理员和安全管理员在无权访问 OCSP 服务器或应答器时，会选择该选项。

- *联机证书状态协议 (OCSP)*

  通常，系统管理员和安全管理员在拥有用于设置 OCSP 服务器或应答器的资源和软件时，会选择该选项。OCSP 可以通过使用更少的带宽，更快地进行有效性检查。

  OCSP 可通过提取 CRL 信息并将其存储到数据库中，来消除加载 CRL 文件所需的时间。OCSP 服务器接受验证证书的请求。OCSP 服务器和应答器很少会过期，因为管理员可以随时吊销证书。可以将 OCSP 从产品服务器放到单独的服务器上。

确认证书真实有效之后，将接受智能卡。访问权限是基于定义的授权权限授予 CA APM 的。如果使用 CA EEM 授权，则权限在 *realms.xml* 文件中进行定义。如果使用本地授权，则权限在 *users.xml* 文件中进行定义。

智能卡身份验证组件

基本通信协议（如超文本传输协议 (HTTP)、轻型目录访问协议 (LDAP) 和安全套接字层 (SSL)）用于智能卡身份验证。您必须先对这些概念有一个基本的了解，然后才能为 CA APM 设置智能卡身份验证。

另外，智能卡身份验证使用以下组件：

- 智能卡吊销验证服务 (SCARVES)
- CA Embedded Entitlements Manager (CA EEM)
- CA APM 本地安全

了解 SCARVES

使用 SCARVES 可以验证从智能卡获得的安全证书。验证过程包含使用 OCSP 或 CRL 服务器来验证证书的选项。

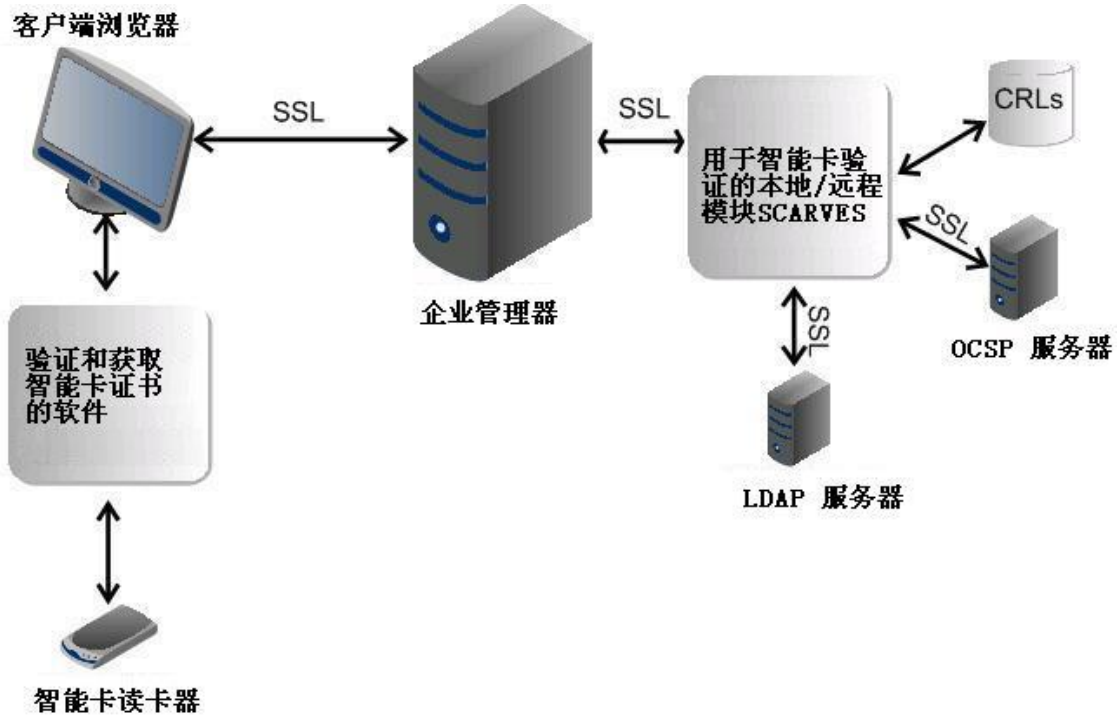
在成功验证证书之后，如果存在用户记录，SCARVES 将通过 LDAP 服务器获得与证书相关联的用户信息。SCARVES 将 LDAP 用户信息检索作为验证过程的一部分。然后，企业管理器将通过使用本地安全或 CA EEM 验证用户角色和访问权限，接收用户信息并继续授权过程。

SCARVES 后台进程是一个处理证书验证处理的进程。从本质上而言，后台进程是正在运行的进程，这些进程充当 OCSP 或者 CRL 服务器的代理。根据配置需求，可以在环境中有一个或多个后台进程。要使用的后台进程数量取决于诸如是否使用 CRL 或 OCSP 服务器等因素。

注意：您可以为独立的企业管理器、收集器或管理器中的管理器 (MOM) 启用智能卡身份验证。如果为 MOM 启用智能卡，应在 MOM 上完成配置，以便将智能卡身份验证应用于整个群集。

CA APM 如何使用智能卡数据进行身份验证

下图说明了 CA APM 如何处理智能卡数据以及使用智能卡数据进行身份验证：



智能卡数据按以下方式进行处理：

1. 在登录到操作系统或桌面时，CA APM 用户将智能卡插入智能卡读卡器。

2. 当用户尝试使用客户端浏览器登录 CA APM 时，会出现一个提示，要求输入个人标识号码 (PIN)。
3. 在用户为智能卡输入正确的 PIN 之后，将打开一个证书选择对话框，其中包含智能卡中的所有证书。用户必须选择正确的证书才能继续进行 Web 身份验证。
4. 在用户选择证书之后，浏览器客户端会使用 SSL 连接将证书发送到企业管理器。
5. 企业管理器接收证书，然后使用 SSL 连接将证书传递给 SCARVES。
6. SCARVES 接收证书并从 OCSP 服务器或 CRL 平面文件请求验证。
7. 如果 OCSP 或 CRL 验证成功，那么 SCARVES 会从 LDAP 服务器检索请求的用户信息。
8. SCARVES 会使用 XML 格式将验证结果和获得的用户信息从 LDAP 返回到企业管理器。
9. 企业管理器基于定义的授权权限向 CA APM 授予访问权限。如果 CA APM 配置为使用 CA EEM 授权，则权限在 *realms.xml* 文件中进行定义。如果使用本地授权，则权限在 *users.xml* 文件中进行定义。

为智能卡身份验证设置 CA APM

按给定的顺序完成以下步骤来为 CA APM 环境启用智能卡身份验证：

1. 验证环境是否已满足必要的要求。有关详细信息，请参阅智能卡身份验证要求 (p. 159)。
2. 解压缩并安装 SCARVES 组件。有关详细信息，请参阅解压缩和安装 SCARVES 组件 (p. 160)。

   注意：您可以为独立的企业管理器、收集器或管理器中的管理器 (MOM) 启用智能卡身份验证。如果为 MOM 启用智能卡，应在 MOM 上完成配置，以便将智能卡身份验证应用于整个群集。
3. 将证书加载到必要的 keystore 中。有关详细信息，请参阅以下主题：
   - 将证书加载到后台进程的证书 keystore 中 (p. 161)
   - 将证书加载到后台进程的信任 keystore 中 (p. 161)
   - 将 SCARVES 证书加载到企业管理器 keystore 中 (p. 161)
4. 加密证书密码。有关详细信息，请参阅为 keystore 加密证书密码 (p. 163)。
5. 如果配置智能卡验证来使用 CRL，请加载 CRL 文件。适用于（可选）加载 CRL 文件 (p. 164)。

6. 配置企业管理器以使用 SCARVES。有关详细信息，请参阅配置企业管理器以使用 SCARVES (p. 164)。
7. 配置 SCARVES 包装器文件。有关详细信息，请参阅配置 SCARVES 包装器 (p. 165)。
8. 配置 SCARVES。有关详细信息，请参阅配置 SCARVES (p. 165)。
9. 启动 SCARVES。有关详细信息，请参阅启动和停止 SCARVES (p. 174)。
10. 验证是否已成功安装和配置智能卡。有关详细信息，请参阅验证智能卡安装 (p. 175)。

智能卡身份验证要求

硬件先决条件：

- 智能卡
- 智能卡读卡器

软件要求：

- CA APM 9.0 或更高版本
- 可验证并获取智能卡证书的软件（如 ActivClient）
- Internet Explorer 6 或 Internet Explorer 7

配置要求：

- 适用于系统中所有智能卡的根安全证书和中间安全证书
- 用于集成现有 LDAP 目录以与智能卡验证一起使用的 LDAP 服务器信息
- 如果计划使用 OCSP 服务器，请收集所有 OCSP 服务器信息：
  - 应答器 URL
  - OCSP 服务器证书
- 如果计划使用 CRL 文件，请为系统中使用的智能卡收集所有 CRL 文件：
  - 所需的 SCARVES 后台进程的数量部分取决于配置智能卡网络解决方案的方式。例如，CRL 文件往往比较大，SCARVES 后台进程在内存中保存所有 CRL 文件。

    一个很好的计算后台进程的起点是每个后台进程的 CRL 文件大小不超过 256 MB。如果发现您所需要的后台进程数量无法由单个服务器进行处理，请考虑购买一台专用 OCSP 服务器。

- 除了计算后台进程的数量之外，请计划并记录以下 SCARVES 后台进程值以便为配置做准备：
  - 每个后台进程的名称
  - 每个后台进程的端口号
  - 每个 CRL 文件的目录名称，如 *<SCARVES_HOME>/crls/<daemon_name>*

在 Windows 上解压缩并安装 SCARVES 组件

解压缩 SCARVES 组件，以便可以配置 SCARVES 并启用智能卡身份验证。

在 Windows 上有效

1. 创建一个用于存储 SCARVES 组件的目录。例如，*<drive>:\SmartCard\scarves*。

   创建的目录将成为智能卡主目录，称为 *<SCARVES_HOME>*。
2. 转到安装企业管理器的顶级目录。例如，*<EM_HOME>*。
3. 转到 *examples\SmartCardAuthentication*，并在适合您环境的 *scarve_0.1* 文件中解压缩内容。有关安装企业管理器的详细信息，请参阅《*CA APM 安装和升级指南*》。

   将创建以下目录：
   - bin
   - conf
   - crls
   - keystores
   - lib
   - logs
4. 从 *<SCARVES_HOME>\bin* 目录中运行 *InstallScarves-NT.bat*。

   成功执行该文件将安装 SCARVES 组件。

在 Unix 和 Linux 上有效

1. 转到 */etc/init.d* 并链接 <*SCARVES_HOME*>/bin/scarves 脚本。
2. 链接以下 *rc?.d* 目录：
   - 在 -s <SCARVES_HOME>/bin/scarves /etc/init.d/scarves 中
   - 在 -s /etc/init.d/scarves /etc/rc3.d/S99scarves 中

- 在 -s /etc/init.d/scarves /etc/rc2.d/K15scarves 中
- /sbin/chkconfig --add scarves

重要信息！这些链接必须是符号链接，因为脚本将使用这些链接来找到配置文件。

加载证书

智能卡通过 SSL 使用一系列证书进行身份验证。必须将证书加载到各种 keystore 中。有关详细信息，请参阅以下主题：

- 将证书加载到后台进程的证书 keystore 中 (p. 161)
- 将证书加载到后台进程的信任 keystore 中 (p. 161)
- 将 SCARVES 证书加载到企业管理器 keystore 中 (p. 161)

将证书加载到后台进程的证书 keystore 中

将服务器证书加载到后台进程验证 keystore 中，以向客户端应用程序提供后台进程详细信息。为了在 SSL 期间与 SCARVES 进行通信时企业管理器可以充当客户端，需要执行该操作。

有关使用证书的各种命令的详细信息，请参阅使用证书的命令 (p. 162)。

将证书加载到后台进程的信任 keystore 中

将证书加载到后台进程信任 keystore，以通过 SSL 与 OCSP 和 LDAP 服务器进行通信。

注意：如果配置 SCARVES 以使用 OCSP，请记下别名。需要别名才能配置 SCARVES。有关详细信息，请参阅（可选）配置 SCARVES 以使用 OCSP (p. 172)。

将证书加载到企业管理器 keystore 中

将 SCARVES 证书加载到企业管理器以与 SCARVES 进行通信。企业管理器使用 SSL 将客户端证书发送给 SCARVES 以及从 SCARVES 发送客户端证书时，会进行验证。有关使用证书的各种命令的详细信息，请参阅使用证书的命令 (p. 162)。

证书命令

使用证书命令可以从 keystore 导入、生成和导出证书。有关详细信息，请参阅以下部分：

- 生成自签名证书 (p. 162)
- 导入证书 (p. 163)
- 导出证书 (p. 163)

生成自签名证书

使用 *-genkey* 命令可以生成自签名安全证书。该命令可以用于为任何 keystore 生成自签名证书。

请执行以下步骤：

1. 以 root 用户身份登录到 CA APM 服务器并访问命令提示符。
2. 导航到 *$JAVA_HOME/bin/keytool* 并使用 *-genkey* 命令运行实用工具。例如：

   ```
   -genkey -keyalg RSA -keystore <SCARVES_HOME>/keystores/daemoncert -alias
   <cert_alias>
   ```

   将启动一个交互式过程，该过程指定您组织的内容，这些内容显示诸如以下信息：

   ```
   输入 keystore 密码：changeit
   重新输入新密码：changeit
   您的姓名是什么？
     [未知]：name.company.com
   您组织单位的名称是什么？
     [未知]：ABC
   您组织的名称是什么？
     [未知]：NOC
   您所在城市或地理位置的名称是什么？
     [未知]：Anytown
   您所在州或省的名称是什么？
     [未知]：Alaska
   该单位的两字母国家/地区代码是什么？
     [未知]：US
   CN=name.company.com、OU=ABC、O=NOC、L=Anytown、
   ST=Alaska、C=US，对吗？
     [否]：是

   为 <newcert> 输入密钥密码
           （如果与 keystore 密码相同，则为 RETURN）：
   ```

导入证书

使用 *-importcert* 命令导入证书。该命令可以用于将证书导入到任何 keystore 中。

请执行以下步骤：

1. 以 root 用户身份登录到 CA APM 服务器并访问命令提示符。
2. 导航到 *$JAVA_HOME/bin/keytool* 并使用 *-importcert* 命令运行实用工具。例如：

```
keytool -importcert -keystore <SCARVES_HOME>/keystores/daemoncert -alias
cert_alias -file cert_file
```

导出证书

使用 *-exportcert* 命令导出证书。该命令可以用于从任何 keystore 中导出证书。

请执行以下步骤：

1. 以 root 用户身份登录到 CA APM 服务器并访问命令提示符。
2. 导航到 *$JAVA_HOME/bin/keytool* 并使用 *-exportcert* 命令运行实用工具。例如：

```
keytool -exportcert -keystore <SCARVES_HOME>/keystores/daemoncert -alias
cert_alias -file cert_file
```

为 keystore 加密证书密码

Keystore 仅储存加密的证书密码。加密的密码可保护证书。加密算法为高级加密标准 (AES)。该算法在不使用明文的情况下，在服务和后台进程代码中嵌入密钥。加密的密码采用 Base64 编码，因此它可以产生一个可打印的字符串。

请执行以下步骤：

1. 转到 *<SCARVES_HOME>/lib* 并打开 *scarve_client.jar* 文件。

   该文件会为 keystore 获得要求加密的密码。

2. 运行以下命令：

   ```
   java -cp scarve_client.jar com.ca.scarve.common.xml.cond e p
   <password_that_requires_encryption>
   ```

   加密的密码可以在 *SCARVESconfig.xml* 文件中使用。

（可选）加载 CRL 文件

如果配置 SCARVES 以启用 CRL，还必须加载 CRL 文件。

请执行以下步骤：

- 将 CRL 文件复制到 *<SCARVES_HOME>/crls/<DAEMON_NAME>* 目录。

  注意：如果配置 SCARVES 以使用 CRL，请记下 CRL 位置。需要 CRL 位置才能配置 SCARVES。有关详细信息，请参阅（可选）配置 SCARVES 以使用 CRL (p. 171)。

配置企业管理器以使用 SCARVES

必须配置企业管理器才能启用智能卡身份验证。

请执行以下步骤：

1. 转到 *<EM_HOME>\config*，打开 *IntroscopeEnterpriseManager.properties* 文件，然后设置以下属性：
   - *introscope.enterprisemanager.scauth.SCARVES.hostname=<scarves_machine_name>*
   - *introscope.enterprisemanager.scauth.SCARVES.port=9998*
   - *introscope.enterprisemanager.webserver.scauth.keystore=/internal/daemoncert*
   - *introscope.enterprisemanager.webserver.scauth.keypass=password*
   - *introscope.enterprisemanager.webserver.scauth.enable=true*
2. 转到 *<EM_HOME>\config*，打开 *em-jetty-config.xml* 文件，然后设置以下属性：
   - *needclientauth= true*
3. 转到 *<EM_HOME>\config*，打开 *IntroscopeEnterpriseManager.properties* 文件，然后执行以下步骤：
   a. 对属性 *introscope.enterprisemanager.webserver.jetty.configurationFile=em-jetty-config.xml* 取消注释
   b. 将 *needclientauth* 属性设置为 *true*。

4. 转到 *<EM_HOME>\config*，打开 *introscopewebview.properties* 文件，然后执行以下步骤：
   a. 对属性 *introscope.webview.jetty.configurationFile=webview-jetty-config.xml* 取消注释
   b. 将 *needclientauth* 属性设置为 *true*。
5. 重新启动企业管理器。

配置 SCARVES 包装器

SCARVES 包装器是配置文件，该文件提供启动运行 SCARVES 的 Java 程序所需的必要信息。

请执行以下步骤：

1. 转到 *<SCARVES_HOME>/conf* 和 *wrapper.conf* 文件。
2. 设置以下属性：
   - wrapper.java.command=java
   - wrapper.app.parameter.2=../conf/SCARVESconfig.xml
3. 保存该文件。

配置 SCARVES

在提取智能卡组件之后，请更新模板配置文件。您可以将 *SCARVESconfigtemplate.xml* 文件用作一个模板来定义诸如 keystore 位置、每个 SCARVES 后台进程的说明以及 SCARVES 使用 OCSP 还是 CRL 等详细信息。

重要信息！ 必须将 *SCARVESconfigtemplate.xml* 模板另存为 *SCARVESconfig.xml* 才能成功应用 SCARVES 配置设置。

常规 XML 格式如下所示：

```
<?xml version="1.0" encoding="UTF-8"?>
<SmartCardService>
    ... Service Parameters ...
    ... One or more Daemon descriptions ...
</SmartCardService>
```

请执行以下步骤：

1. 转到 *<SCARVES_HOME>/conf* 并打开 *SCARVESconfigtemplate.xml*。

2. 使用 XML 编辑工具来设置常规 SCARVES 设置：
   - 配置 SCARVES 服务参数 (p. 166)
   - 配置 SCARVES 后台进程 (p. 167)
   - 配置 SCARVES 以使用 LDAP (p. 169)

   还指定一个智能卡验证协议：
   - （可选）配置 SCARVES 以使用 OCSP (p. 172)
   - （可选）配置 SCARVES 以使用 CRL (p. 171)

   注意：只能为您的环境启用一个协议。
3. 将文件另存为 *SCARVESconfig.xml*。
4. 启动 SCARVES 服务。有关详细信息，请参阅启动和停止 SCARVES (p. 174)。

配置 SCARVES 服务参数

SCARVES 服务参数指定 keystore 位置和密码详细信息。

常规 XML 格式如下所示：

```
<SmartCardService>
    <trust-keystore>filename of keystore</trust-keystore>
    <trust-keystore-pass>encrypted password of keystore</trust-keystore-pass>
    <jvm-arg>-mx1024m</jvm-arg> <!-- optional, param for all Daemon JVMs -->
    ... One or more Daemon descriptions ...
</SmartCardService>
```

可以配置以下参数：

<trust-keystore>

为所有后台进程指定信任 keystore。该文件必须包含所有根证书和中间证书才能接受所有智能卡。该参数使用以下参数传递到所有后台进程：

-Djavax.net.ssl.trustStore=filename JVM

注意：所有后台进程使用相同的信任 keystore。

<trust-keystore-pass>

为信任 keystore 指定密码。该密码必须在 XML 文件中进行加密。该密码是使用以下参数以明文形式传递给所有后台进程的：

```
-Djavax.net.ssl.trustStorePassword=password
```

<debug>

设置调试日志记录的级别。以下是可用的值：

- 0－指定无任何调试。此值是默认值。
- 1－指定调试的最低级别详细信息。
- 2－指定调试的标准中等级别详细信息。
- 3－指定调试的最高级别详细信息。

<jvm-arg>

为所有后台进程 JVM 指定该参数。该参数用于调整可用内存量。

有关应用配置设置的详细信息，请参阅配置 SCARVES (p. 165)。

配置 SCARVES 后台进程

SCARVES 后台进程参数指定使用 CRL 还是 OCSP 和 LDAP 详细信息。虽然 CRL 和 OCSP 可以同时存在，但是只能启用其中一个，因此必须注释掉一个。

常规 XML 格式如下所示：

```
<SmartCardService>
    ... Service Parameters ...
    <Daemon name="name" port="port number">
        <keystore>...filename of keystore...</keystore>
        <keystore-pass>...encrypted password of keystore...</keystore-pass>
        <jvm-arg>-mx1024m</jvm-arg> <!-- optional, param for this Daemon JVM -->
        ... Protocol Description...
        ... LDAP Description...
    </Daemon>
    ... more Daemon descriptions ...
</SmartCardService>
```

可以配置以下参数：

name

为每个后台进程名称指定一个唯一的名称。该名称用于内部跟踪，并以日志文件中相应的错误和调试代码为前缀。

port

指定后台进程侦听的 TCP 端口。

<keystore>

指定 keystore 文件，该文件包含后台进程用于进行 SSL 通信的证书。

<keystore-pass>

为 keystore 指定密码。该密码必须在 XML 文件中进行加密。

<jvm-arg>

为所有后台进程 JVM 指定该参数。该参数调整对于该部分中指定的*每个*后台进程可用的内存量。它不同于基本 SCARVES 服务参数部分中的 <jvm-arg> 标记，因为不会将它发送给*所有*后台进程。

有关应用配置设置的详细信息，请参阅配置 SCARVES (p. 165)。

配置 SCARVES 以使用 LDAP

如果后台进程使用 LDAP，则必须定义参数以便为此身份验证方法指定详细信息。

常规 XML 格式如下所示：

```
<SmartCardService>
    ... Service Parameters ...
    <Daemon ...parameters...>
        ... More daemon parameters...
        ... Protocol Description...
        CA LDAP Server for z/OS
            <ldap-enabled>true</ldap-enabled>
            <ldap-hostname>renge01-winvm</ldap-hostname>
            <ldap-port>24132</ldap-port>
            <ldap-ssl>false</ldap-ssl>
            <ldap-user-dn>uid=GGantt,ou=people,dc=ca,dc=com</ldap-user-dn>

<ldap-user-pass>05V2irWBg8O39H6ANGic241UWooJuIbJiHE+ZqKPvUY=</ldap-user-pass>
            <ldap-base-dn>ou=people,dc=ca,dc=com</ldap-base-dn>
            <cert-uniqueid-field>subject</cert-uniqueid-field>
            <cert-uniqueid-regex>CN=\w*\.\w*\.(\d+),</cert-uniqueid-regex>

<ldap-uniqueid-search-field>facsimileTelephoneNumber</ldap-uniqueid-search-fi
eld>
            <ldap-cache-lifetime>300</ldap-cache-lifetime>
        </ldap>
    </Daemon>
    ... more Daemon descriptions ...
</SmartCardService>
<ldap-enabled>
```

可以配置以下参数：

<ldap-enabled>

指定要启用还是禁用 LDAP。以下是可用的值：

- *True* 会为后台进程启用 LDAP。
- *False* 会为后台进程禁用 LDAP。将该值设置为 False 将允许配置文件使用 CA LDAP Server for z/OS 部分来存储未使用过的设置。

<ldap-hostname>

指定 LDAP 服务器的主机名。

<ldap-port>

指定 LDAP 服务器的端口。

<ldap-ssl>

如果该值设置为 *True*，请指定 LDAP 服务器使用 SSL。如果启用该功能，请确认 LDAP 服务器证书处于信任 keystore 中。

<ldap-user-dn>

指定后台进程用于登录到 LDAP 服务器的可分辨名称。服务器必须向该可分辨名称授予搜索权限。

<ldap-user-pass>

指定后台进程用于登录到 LDAP 服务器的密码。该密码必须在 XML 文件中进行加密。

<ldap-base-dn>

指定基础可分辨名称，该名称作为 LDAP 搜索的起点。要搜索的所有可分辨名称必须显示在基础可分辨名称之下。

<cert-uniqueid-field>

指定证书字段，该字段包含电子数据交换个人标识符 (EDIPI) 或其他唯一标识。有效值包括 *subject*、*subuid*、*an_other* 和 *an_rfc822*。

<cert-uniqueid-regex>

指定正则表达式，该表达式详细说明了如何从给定的字段提取唯一标识。

<ldap-uniqueid-search-field>

指定包含 EDIPI 或其他唯一标识的 LDAP 输入字段。

<ldap-cache-lifetime>

指定缓存的 LDAP 查找有效的最长时间（以秒为单位）。

如果默认值设置为 *零*，则不会缓存 LDAP 查找。

请不要将该值设置得太高，因为如果更改 LDAP 条目，缓存的条目会返回不正确的值，直到缓存超时为止。

加密

指定必须对存储在 XML 文件中的密码进行加密。加密算法为高级加密标准 (AES)，它在不使用明文的情况下，在服务和后台进程代码中嵌入密钥。加密的密码采用 Base64 编码，以生成可在 XML 文件中存储的可打印字符串。

有关应用配置设置的详细信息，请参阅配置 SCARVES (p. 165)。

（可选）配置 SCARVES 以使用 CRL

CRL 参数指定文件存储详细信息。一次只能配置一个 CRL。

重要信息！ 如果配置 *SCARVESconfig.xml* 以使用 CRL，必须将 *<ocsp-enabled>* 参数的 OCSP 值设置为 *False*，以便在单一后台进程中无错启动 SCARVES。

常规 XML 格式如下所示：

```
<SmartCardService>
    ... Service Parameters ...
    <Daemon ...parameters...>
        ... More daemon parameters...
        <crl>
            <crl-enabled>true</crl-enabled>
            <crl-dp>false</crl-dp>
            <crl-url>...URL containing CRL files...</crl-url>
            <crl-dir>...dirname containing CRL files...</crl-dir>
            <crl-poll-int>30</crl-poll-int>
        </crl>
        ... LDAP Description...
    </Daemon>
    ... more Daemon descriptions ...
</SmartCardService>
```

可以配置以下参数：

<crl-enabled>

通过将该值设置为 *True*，指定后台进程使用 CRL 文件。将该值设置为 *False* 将允许后台进程使用 OCSP。

<crl-dp>

指定从其下载 CRL 文件的分发点。

<crl-url>

指定包含 CRL 文件的 URL。

<crl-dir>

指定包含 CRL 文件的目录名称。

<crl-poll-int>

指定在 CRL 目录或 CRL URL 中扫描新的或更改的 CRL 文件的频率（以秒为单位）。已缓存扫描的证书。如果未指定该参数，则默认时间间隔为 60 秒。

有关应用配置设置的详细信息，请参阅配置 SCARVES (p. 165)。

（可选）配置 SCARVES 以使用 OCSP

OCSP 参数指定使用 OCSP 进行智能卡验证所需的详细信息。如果使用该协议，则需要在配置文件中注释掉 CRL 协议选项。

重要信息！ 如果配置 *SCARVESconfig.xml* 以使用 OCSP，则必须将 *<crl-enabled>* 参数的 CRL 值设置为 *False*，以便在单一后台进程中无错启动 SCARVES。

常规 XML 格式如下所示：

```
<SmartCardService>
    ... Service Parameters ...
    <Daemon ...parameters...>
        ... More daemon parameters...
        <ocsp>
            <ocsp-enabled>true</ocsp-enabled>
            <ocsp-aia>false</ocsp-aia>
            <ocsp-cert-alias>ocsp_qacle3</ocsp-cert-alias>
            <ocsp-url>http://qacle3:3501/responder</ocsp-url>
        </ocsp>
        ... LDAP Description...
    </Daemon>
    ... more Daemon descriptions ...
</SmartCardService>
```

可以配置以下参数：

<ocsp-enabled>

如果将该值设置为 *True*，将指定后台进程使用 OCSP。

<ocsp-aia>

如果在实施智能卡身份验证时将该值设置为 *True*，将指定授权信息访问 (AIA)。

<ocsp-cert-alias>

指定 OCSP 应答器用来签署响应的证书的别名。如果启用该功能，请确认 OCSP 服务器证书处于信任 keystore 中。

<ocsp-url>

指定 OCSP 应答器的 URL。

有关应用配置设置的详细信息，请参阅配置 SCARVES (p. 165)。

示例 SCARVES 配置文件

以下代码示例代表 *SCARVESconfig.xml* 配置文件的一部分。它定义了两个后台进程来使用一个 CRL 服务器和一个 LDAP 服务器验证智能卡。

虽然可以在两个选项同时存在的情况下配置 XML，但必须仅为 OCSP 或 CRL 启用配置属性。

```
<?xml version="1.0" encoding="UTF-8"?>

<SmartCardService>
<trust-keystore>../keystores/daemontrust</trust-keystore>
<trust-keystore-pass>YEDZLwyEVTnCfzS+rYTfC41UWooJuIbJiHE+ZqKPvUY=</trust-keys
tore-pass>
<debug>0</debug>

<jvm-arg>-mx1024m</jvm-arg>

<Daemon name="daemon-crl-1" port="9999">
   <keystore>../keystores/daemoncert</keystore>

<keystore-pass>YEDZLwyEVTnCfzS+rYTfC41UWooJuIbJiHE+ZqKPvUY=</keystore-pass>

   <crl>
    <crl-enabled>true</crl-enabled>
    <crl-dp>false</crl-dp>
    <crl-url />
    <crl-dir>../crls/daemon-crl</crl-dir>
    <crl-poll-int>600</crl-poll-int>
   </crl>
  <ldap>
    <ldap-enabled>true</ldap-enabled>
    <ldap-hostname>host1</ldap-hostname>
    <ldap-port>24000</ldap-port>
    <ldap-ssl>false</ldap-ssl>
    <ldap-base-dn>ou=people,dc=abc,dc=com</ldap-base-dn>
    <ldap-user-dn>uid=JDoe,ou=people,dc=abc,dc=com</ldap-user-dn>

<ldap-user-pass>05V2irWZg8O39L6ANGic241UWiOJuIbJiHE+ZqKPvUY=</ldap-user-pass>
    <cert-uniqueid-field>subject</cert-uniqueid-field>
    <cert-uniqueid-regex>CN=\w*\.\w*\.(\d+),</cert-uniqueid-regex>

<ldap-uniqueid-search-field>facsimileTelephoneNumber</ldap-uniqueid-search-fi
eld>
  </ldap>
</Daemon>
```

```
<Daemon name="daemon-ocsp-1" port="9998">
  <keystore>../keystores/daemoncert</keystore>
  <keystore-pass>YEDZLwyEVTnCfzS+rYTfC41UWooJuIbJiHE+ZqKPvUY=</keystore-pass>

  <ocsp>
    <ocsp-enabled>true</ocsp-enabled>
    <ocsp-aia>false</ocsp-aia>

    <ocsp-cert-alias>ocsp_qacle3</ocsp-cert-alias>

    <ocsp-url>http://qacle3:3501/responder</ocsp-url>
  </ocsp>
  <ldap>
    <ldap-enabled>true</ldap-enabled>
    <ldap-hostname>host1</ldap-hostname>
    <ldap-port>24001</ldap-port>
    <ldap-ssl>false</ldap-ssl>
    <ldap-base-dn>ou=people,dc=abc,dc=com</ldap-base-dn>
    <ldap-user-dn>uid=JDoe,ou=people,dc=abc,dc=com</ldap-user-dn>

<ldap-user-pass>O5V2irWBg8O39H6ANGic377UWooJuIbJiHE+ZqKPvUY=</ldap-user-pass>
    <cert-uniqueid-field>subject</cert-uniqueid-field>
    <cert-uniqueid-regex>CN=\w*\.\w*\.(\d+),</cert-uniqueid-regex>

<ldap-uniqueid-search-field>facsimileTelephoneNumber</ldap-uniqueid-search-fi
eld>
    <ldap-cache-lifetime>300</ldap-cache-lifetime>
  </ldap>
</Daemon>

</SmartCardService>
```

启动和停止 SCARVES

SCARVES 是一个 Java 程序，该程序通过读取 *SCARVESconfig.xml* 配置文件来控制后台进程，并为指定的每个端口启动一个后台进程程序。如果出现以下任一情况，SCARVES 会停止一个后台进程，并启动一个新的后台进程：

- 某个后台进程崩溃
- 某个后台进程无法对通信做出响应
- 某个后台进程无法对某个 XML ping 做出响应

请执行以下步骤：

- 以 root 用户身份登录到 CA APM 服务器并访问命令提示符。

  在 Windows 上有效

  - 运行启动批处理以启动 SCARVES：
    `<SCARVES_HOME>\bin\StartSCARVES-NT.bat`
  - 运行停止批处理以停止 SCARVES：
    `<SCARVES_HOME>\bin\StopSCARVES-NT.bat`

  在 Linux 上有效

  - 运行启动脚本以启动 SCARVES：
    `/etc/init.d/SCARVES start`
  - 运行停止脚本以停止 SCARVES：
    `/etc/init.d/SCARVES stop`
  - 运行重新启动脚本以重新启动 SCARVES：
    `/etc/init.d/SCARVES restart`

  在 Unix 上有效

  - 输入 start 命令以启动 SCARVES：
    `<SCARVES_HOME>/bin/scarves start`
  - 输入 stop 命令以停止 SCARVES：
    `<SCARVES_HOME>/bin/scarves stop`
  - 运行 status 命令以获取 SCARVES 状态：
    `<SCARVES_HOME>/bin/scarves status`

验证智能卡安装

在设置完智能卡身份验证之后，请验证身份验证方法是否已成功安装并启用。

请执行以下步骤：

1. 在为智能卡身份验证设置 CA APM 之后，请启动 WebView、Web Start 或 CEM 控制台。

   将显示一个页面，提示您输入用户标识和个人标识号码 (PIN)。

2. 输入 PIN。
3. 确认已经在位于 *<SCARVES_HOME>\log* 目录的日志文件中记录一条初始化消息。

对 CA APM 智能卡身份验证进行故障排除

故障排除信息可以帮助您解决在智能卡身份验证中出现的问题和错误消息。

以下部分提供了帮助：

SCARVES 无法启动

在 Windows、UNIX 和 Linux 上有效

症状：

当我尝试使用智能卡身份验证进行身份验证时，SCARVES 无法启动，并出现以下错误消息：

```
[ERROR] [btpool0-2] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: 从给定证书获取用户时出错。
java.net.ConnectException: 连接被拒绝：连接
```

解决方案：

当 SCARVES 无法启动某条错误消息返回时，可以进行故障排除来解决该问题。

对 SCARVES 启动问题进行故障排除

1. 打开位于 *<SCARVES_HOME>\logs* 中的 *scarve.log* 文件。
2. 如果记录了*在 DEBUG 模式下配置*错误消息，则 SCARVES 不会正确启动。可以通过执行以下操作进行故障排除：
   - 验证在 *wrapper.conf* 文件中提供的 JVM 参数是否有效。例如：
     `wrapper.java.command=C:/Progra~1/Java/jdk1.6.0_20/bin/java`
   - 检查是否在 *scarve.log* 文件中记录了端口绑定错误。如果存在此错误，请通过输入以下命令检查后台进程端口号的可用性：
     `netstat -ao | find <port-no>`

     如果该端口号已被占用，请分配一个新的端口号，因为后台进程必须有一个唯一的端口号。
   - 验证是否已正确设置 *SCARVESconfigtemplate.xml* 中的属性集的格式。
   - 验证位于 *<SCARVES_HOME>/keystores* 中的 keystore 文件是否可用。
3. 如果未记录*在 DEBUG 模式下配置*错误消息，请重新安装 SCARVES。

   注意：如果卸载并重新安装，会保留 *config* 和 *keystores* 子目录中的文件。
4. 重新启动 SCARVES。

   可以使用智能卡进行身份验证。

OCSP 验证失败

在 Windows、UNIX 和 Linux 上有效

症状：

当使用我的 Web 浏览器选择某个有效证书时，OCSP 验证失败，并出现以下错误消息：

```
[ERROR] [btpool0-0] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: 与 OCSP 服务器联系时出现问题
```

解决方案：

验证是否可以通过重新启动 OCSP 服务器访问 OCSP 服务器。

重新启动 OCSP：

1. 从 *services.msc* 重新启动 OCSP 服务器。
2. 打开浏览器并选择有效证书。

   OCSP 验证成功。

CRL 验证失败

在 Windows、UNIX 和 Linux 上有效

症状：

尝试为某个配置 CRL 的环境使用智能卡进行身份验证失败。

解决方案：

如果在使用 CRL 进行验证时遇到问题，可以进行故障排除来解决该问题。

对 SCARVES 启动问题进行故障排除

1. 打开位于 *<SCARVES_HOME>\logs* 中的 *scarve.log* 文件。
2. 如果存在 CRL 到期日期详细信息，则 CRL 文件已过期。

   注意：CRL 文件每周到期一次。
3. 下载最新的 CRL 文件。

   CRL 验证成功。

OCSP 服务器未响应

在 Windows、UNIX 和 Linux 上有效

症状：

当我尝试使用 OCSP 选项进行智能卡身份验证时，OCSP 服务器失败，并出现以下消息：

```
[ERROR] [btpool0-0] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException:
```

解决方案：

出现该消息是因为 OCSP 服务器无法启动，可以进行故障排除来解决该问题。

对 OCSP 服务器进行故障排除：

- 确认应答器没有因从 *services.msc* 重新启动 OCSP 服务器而卡住。
- 验证 SCARVES 和 OCSP 之间的时间和日期是否相同。如果不相同，将显示错误消息。

LDAP 服务器未响应

在 Windows、UNIX 和 Linux 上有效

症状：

当我尝试使用智能卡身份验证时，LDAP 服务器无法启动，并出现以下消息：

```
[ERROR] [btpool0-2] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: LDAP 服务器未响应
```

解决方案：

如果 LDAP 服务器无法启动，则无法访问在 *SCARVESconfig.xml* 文件中指定的 LDAP 实例。

对 LDAP 服务器进行故障排除：

- 验证是否已使用适当的值设置 LDAP 配置。
- 验证 LDAP 服务器是否可用。
- 验证 LDAP 服务器是否已启动并运行

收到 CRL 错误

在 Windows、UNIX 和 Linux 上有效

症状：

当我尝试使用 CRL 选项进行智能卡身份验证时，位于 *<SCARVES_HOME>/logs* 目录中的 *scarve.log* 文件中将出现以下错误消息：
`[ERROR] [btpool0-12] [Manager.SCAuth] com.wily.introscope.spec.server.user.SCException:` 证书已过期，或被吊销，或无法进行验证。

注意：未在企业管理器日志文件中记录无效 CRL 文件的详细信息。

解决方案：

如果在某个配置为使用 CRL 的环境中无法使用智能卡成功地进行身份验证，请对该问题进行故障排除。

对 CRL 进行故障排除：

- 确认 *SCARVESconfig.xml* 文件指定的文件夹在 *<SCARVES_HOME>/crls* 目录中存在。如果不存在，请执行以下操作：
  1. 转到 *<SCARVES_HOME>/conf* 并打开 *SCARVESconfig.xml* 。
  2. 复制指定的 <daemon-name> 的名称。
  3. 转到 *<SCARVES_HOME>/crls* 目录，并使用相同的 <daemon-name> 创建文件夹。
  4. 将 CRL 文件复制到该目录并重新启动 SCARVES。
- 验证为 CRL 后台进程提供的绝对路径是否正确。
  1. 转到 *<SCARVES_HOME>/conf* 并打开 *SCARVESconfig.xml* 。
  2. 验证为 CRL 位置提供的路径是否正确。
  3. 这样可验证 SCARVES 是否能够跟踪包含 CRL 文件的 CRL 文件夹。

收到用户不在 LDAP 中的错误

在 Windows、UNIX 和 Linux 上有效

症状：

当我尝试使用智能卡身份验证时，在 *<EM_HOME>/logs/IntroscopeEnterpriseManager.log* 文件中出现以下错误消息：

收到用户不在 LDAP 中的错误

解决方案：

未使用 LDAP 的用户目录中的用户详细信息定义 LDAP 时，会发生这种情况。可以通过添加一个 LDAP 用户目录来解决该问题。

添加 LDAP 用户目录：

1. 转到 <SCARVES_HOME>/conf 并打开 *SCARVESconfig.xml* 。
2. 定义以下属性：

   facismilenumber

   输入所使用证书的 EDIPI 号。

   uid

   使用存在于企业管理器和用户登录凭据中的用户名输入属性。
3. 重新启动 SCARVES。

收到连接被拒绝的错误

在 Windows、UNIX 和 Linux 上有效

症状：

当我尝试使用智能卡身份验证时，出现以下错误消息：

```
[ERROR] [btpool0-2] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: 从给定证书获取用户时出错。
java.net.ConnectException: 连接被拒绝：连接
```

未启动定义的 scarves 实例，或无法访问定义的 scarves 实例时，会记录该企业管理器错误。

解决方案：

- 转到 *<SCARVES_HOME>/conf*，打开 *SCARVESconfig.xml*，并验证 SCARVES 主机名是否正确。

收到 LDAP 未配置的错误

在 Windows、UNIX 和 Linux 上有效

症状：

当我尝试使用智能卡身份验证时，在企业管理器日志文件中出现以下错误消息：

```
[ERROR] [btpool0-0] [Manager.SCAuth]
com.wily.introscope.spec.server.user.SCException: 未配置 LDAP
```

未启动定义的 scarves 实例，或无法访问定义的 scarves 实例时，会记录该企业管理器错误。

解决方案：

- 转到 *<SCARVES_HOME>/conf*，打开 *SCARVESconfig.xml*，并验证该文件中的 LDAP 内容是否存在且准确。

在企业管理器中发生握手例外

在 Windows、UNIX 和 Linux 上有效

症状：

当我尝试使用智能卡身份验证时，出现握手例外。

解决方案：

发生握手例外时，可以进行故障排除来解决该问题。

对握手例外进行故障排除：

1. 转到 *<SCARVES_HOME>/conf* 并打开 *SCARVESconfigtemplate.xml*。
2. 验证在 *SCARVESconfigtemplate.xml* 中定义的 keystore 属性是否准确。
3. 验证是否已将有效自签名证书从 SCARVES 导入到在属性文件中定义的 keystore 中。
4. 验证 *<EM_HOME>\config* 中的 keystore 的属性是否准确，且自签名证书是否位于 *<SCARVES_HOME>/keystores/daemoncert* 目录中。如果自签名证书不存在，请将证书导出到企业管理器 keystore 中。

有关证书的详细信息，请参阅：

加载证书 (p. 161)
证书命令 (p. 162)