HP Universal CMDB 和 Configuration Manager

软件版本： 10.10

强化指南

文档发布日期： 2013 年 11 月

软件发布日期： 2013 年 11 月

法律声明

担保

HP 产品和服务的唯一担保已在此类产品和服务随附的明示担保声明中提出。此处的任何内容均不构成额外担保。HP 不会为此处出现的技术或编辑错误或遗漏承担任何责任。

此处所含信息如有更改，恕不另行通知。

受限权利声明

机密计算机软件。必须拥有 HP 授予的有效许可证，方可拥有、使用或复制本软件。按照 FAR 12.211 和 12.212，并根据供应商的标准商业许可的规定，商业计算机软件、计算机软件文档与商品技术数据授权给美国政府使用。

版权声明

商标声明

Adobe® 是 Adobe Systems Incorporated 的商标。

Microsoft® 和 Windows® 是 Microsoft Corporation 在美国的注册商标。

UNIX® 是 The Open Group 的注册商标。

文档更新

此文档的标题页包含以下标识信息：

- 软件版本号，用于指示软件版本。
- 文档发布日期，该日期将在每次更新文档时更改。
- 软件发布日期，用于指示该版本软件的发布日期。

要检查是否有最新的更新，或者验证是否正在使用最新版本的文档，请访问： **http://h20230.www2.hp.com/selfsolve/manuals**

需要注册 HP Passport 才能登录此站点。要注册 HP Passport ID，请访问： **http://h20229.www2.hp.com/passport-registration.html**

或单击“HP Passport”登录页面上的“**New users - please register**”链接。

此外，如果订阅了相应的产品支持服务，则还会收到更新的版本或新版本。有关详细信息，请与您的 HP 销售代表联系。

支持

请访问 HP 软件联机支持网站：**http://www.hp.com/go/hpsoftwaresupport**

此网站提供了联系信息，以及有关 HP 软件提供的产品、服务和支持的详细信息。

HP 软件联机支持提供客户自助解决功能。通过该联机支持，可快速高效地访问用于管理业务的各种交互式技术支持工具。作为尊贵的支持客户，您可以通过该支持网站获得下列支持：

- 搜索感兴趣的知识文档
- 提交并跟踪支持案例和改进请求
- 下载软件修补程序
- 管理支持合同
- 查找 HP 支持联系人
- 查看有关可用服务的信息
- 参与其他软件客户的讨论
- 研究和注册软件培训

大多数提供支持的区域都要求您注册为 HP Passport 用户再登录，很多区域还要求用户提供支持合同。要注册 HP Passport ID，请访问：

http://h20229.www2.hp.com/passport-registration.html

要查找有关访问级别的详细信息，请访问：

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now 可访问 HPSW 解决方案和集成门户网站。此网站将帮助您寻找可满足您业务需求的 HP 产品解决方案，包括 HP 产品之间的集成的完整列表以及 ITIL 流程的列表。此网站的 URL 为 **http://h20230.www2.hp.com/sc/solutions/index.jsp**

目录

第 1 章：强化简介

本章包括：

强化概述

本节介绍了安全的 HP Universal CMDB 应用程序的概念，并讨论了实现安全性所需的计划和体系结构。强烈建议您在阅读后面几节中有关强化的讨论之前，先阅读本节内容。

HP Universal CMDB 旨在成为安全体系结构的一部分，因而可以应对处理可能遇到的安全威胁的挑战。

强化准则可处理实现更安全的 (强化的) HP Universal CMDB 所需的配置。

所提供的强化信息主要适用于 HP Universal CMDB 管理员。管理员应在开始强化过程之前先熟悉强化设置和建议。

强烈建议您对 HP Universal CMDB 使用反向代理，以保证体系结构安全。有关配置反向代理以便用于 HP Universal CMDB 的详细信息，请参阅使用反向代理 (第 36 页)。

如果必须对 HP Universal CMDB 使用另一种类型的安全体系结构，而不是本文档中介绍的体系结构，请联系 HP 软件支持以确定最合适的体系结构。

有关强化 Data Flow Probe 的详细信息，请参阅Data Flow Probe 强化 (第 64 页)。

备注：

- 这些强化过程基于以下假设：仅实施以上章中提供的说明，而不执行其他强化步骤。
- 强化过程集中于某特定分布式体系结构时，并不意味着该结构是最符合组织需求的体系结构。

- 假设将在 HP Universal CMDB 专用计算机上执行以下章中的过程。如果这些计算机用于除 HP Universal CMDB 以外的用途，则可能导致错误的结果。
- 本节中提供的强化信息并不可用来指导您对计算机化系统进行安全风险评估。

强化准备

- 评估一般网络的安全风险/安全状态，并在确定将 HP Universal CMDB 集成到网络中的最佳方式时使用评估结论。
- 深入了解 HP Universal CMDB 技术框架和 HP Universal CMDB 安全功能。
- 查看所有强化准则。
- 启动强化过程之前，先验证 HP Universal CMDB 是否正常工作。
- 在每章中按时间顺序执行强化过程的步骤。例如，如果确定将 HP Universal CMDB 服务器配置为支持 SSL，请阅读启用安全套接字层 (SSL) 通信 (第 16 页)，然后按时间顺序执行所有说明。
- HP Universal CMDB 不支持使用空密码进行基本身份验证。设置基本身份验证连接参数时不要使用空密码。

提示：打印强化过程，并在实施这些过程时进行核对。

在安全体系结构中部署 UCMDB

为了安全部署 HP Universal CMDB 服务器，建议采取以下措施：

- **使用防火墙的 DMZ 体系结构**

  本文档中所指的安全体系结构是一个使用防火墙设备的典型 DMZ 体系结构。此类体系结构的基本理念是建立完整的隔离，避免在 HP Universal CMDB 客户端和 HP Universal CMDB 服务器之间进行直接访问。

- **安全浏览器**

  必须将 Windows 环境中的 Internet Explorer 和 FireFox 配置为安全地处理 Java 脚本、小程序和 cookie。

- **SSL 通信协议**

  安全套接字层协议可确保客户端和服务器之间的连接安全。需要进行 SSL 连接的 URL 使用的是超文本传输协议的安全版本 (HTTPS)。有关详细信息，请参阅启用安全套接字层 (SSL) 通信 (第 16 页)。

- **反向代理体系结构**

  其中一个更安全的推荐解决方案是建议使用反向代理部署 HP Universal CMDB。HP Universal CMDB 完全支持安全的反向代理体系结构。有关详细信息，请参阅使用反向代理 (第 36 页)。

系统访问

Java JMX 访问强化

> **备注：**此处描述的过程也可用于 Data Flow Probe JMX。

为了确保 JMX RMI 端口只有在提供了用户凭据后才可以访问，请执行以下过程：

1. 在服务器上位于 **C:\hp\UCMDB\UCMDBServer\bin** 的 **wrapper.conf** 文件中，请进行以下设置：

   wrapper.java.additional.16=-Dcom.sun.management.jmxremote.authenticate=true

   此设置要求 JMX 提供身份验证。

   - **对于 Data Flow Probe JMX**，请执行以下操作：

     在位于 **C:\hp\UCMDB\DataFlowProbe\bin** 的 **WrapperGateway.conf** 和 **WrapperManager.conf** 文件中，进行以下设置：

     wrapper.java.additional.17=-Dcom.sun.management.jmxremote.authenticate=true

2. 将 **jmxremote.password.template** 文件 (位于：**C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) 重命名为 **jmxremote.password**。

   > **备注：**对于 Data Flow Probe JMX，此文件位于：**C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**。

3. 在 **jmxremote.password**中，为角色 **monitorRole** 和 **controlRole** 添加密码。

   例如：

   monitorRole QED

   controlRole R&D

   将密码 **QED** 分配给 **monitorRole**，然后将密码 **R&D** 分配给 **controlRole**。

> **备注：**由于 **jmxremote.password** 包含明文形式的密码，因此请确保只有拥有者才对该文件具有读写权限。此文件拥有者必须与运行 UCMDB 服务器的用户相同。

4. 在文件 **jmxremote.access** (位于 **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) 中，将访问权限分配给 **monitorRole** 和 **controlRole**。

   例如：

   monitorRole readonly

   controlRole readwrite

   会将只读访问权限分配给 **monitorRole**，并将读写访问权限分配给 **controlRole**。

   > **备注：**对于 Data Flow Probe JMX，此文件位于：**C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**。

5. 按以下方式对文件予以保护：

   - **仅适用于 Windows：**从命令行中运行下列命令，从而对文件予以保护：

     cacls jmxremote.password /P <用户名>:F

     cacls jmxremote.access /P <用户名>:R

     其中，**<用户名>** 是指这两个文件的属性中显示的文件拥有者。打开这两个文件的属性，确保它们正确，且只有一名拥有者。

   - **对于 Solaris 和 Linux 操作系统：**通过运行以下文件设置密码文件的文件权限：

     chmod 600 jmxremote.password

6. **对于服务包的升级、服务器迁移和灾难恢复：**通过运行升级或者迁移安装，将文件 **jmxremote.access** 的所有权 (位于 **C:\hp\UCMDB\UCMDBServer\bin\jre\lib\management**) 更改为操作系统用户。

   > **备注：**
   >
   > - 对于 Data Flow Probe JMX，此文件位于：**C:\hp\UCMDB\DataFlowProbe\bin\jre\lib\management**。
   > - 卸载产品之前，请先编辑 **<UMCDB 安装文件夹>\bin\jre\lib\management\jmxremote.password** 的文件权限，以便您用来登录的用户可对其进行编辑。

更改 JMX 控制台的系统用户名或密码

JMX 控制台针对的是系统用户，即多客户环境中的交叉客户用户。您可以使用任何系统用户名登录 JMX 控制台。默认用户名和密码是 **sysadmin/sysadmin**。

可通过 JMX 控制台或服务器管理工具来更改密码。

要通过 JMX 控制台更改默认的系统用户名或密码，请执行以下操作：

1. 启动 Web 浏览器，并输入以下地址：**http://localhost.<域名>:8080/jmx-console**。
2. 输入 JMX 控制台身份验证凭据。
3. 找到 **UCMDB:service=Authorization Services**，然后单击该链接打开“Operations”页面。
4. 找到 **resetPassword** 操作。
   - 在 **userName** 字段中，输入 **sysadmin**。
   - 在“password”字段中，输入新密码。
5. 单击“Invoke”，保存变更。

要通过服务器管理工具更改默认的系统用户名或密码，请执行以下操作：

1. **对于 Windows：**运行以下文件：**C:\hp\UCMDB\UCMDBServer\tools\server_management.bat。**

   对于 Linux：运行位于下列文件夹的 **server_management.sh**：**/opt/hp/UCMDB/UCMDBServer/tools/**。
2. 使用身份验证凭据登录工具：**sysadmin/sysadmin**。
3. 单击“用户”链接。
4. 选择系统用户，并单击“更改已登录用户的密码”。
5. 输入旧密码和新密码，并单击“确定”。

更改 HP Universal CMDB 服务器服务用户

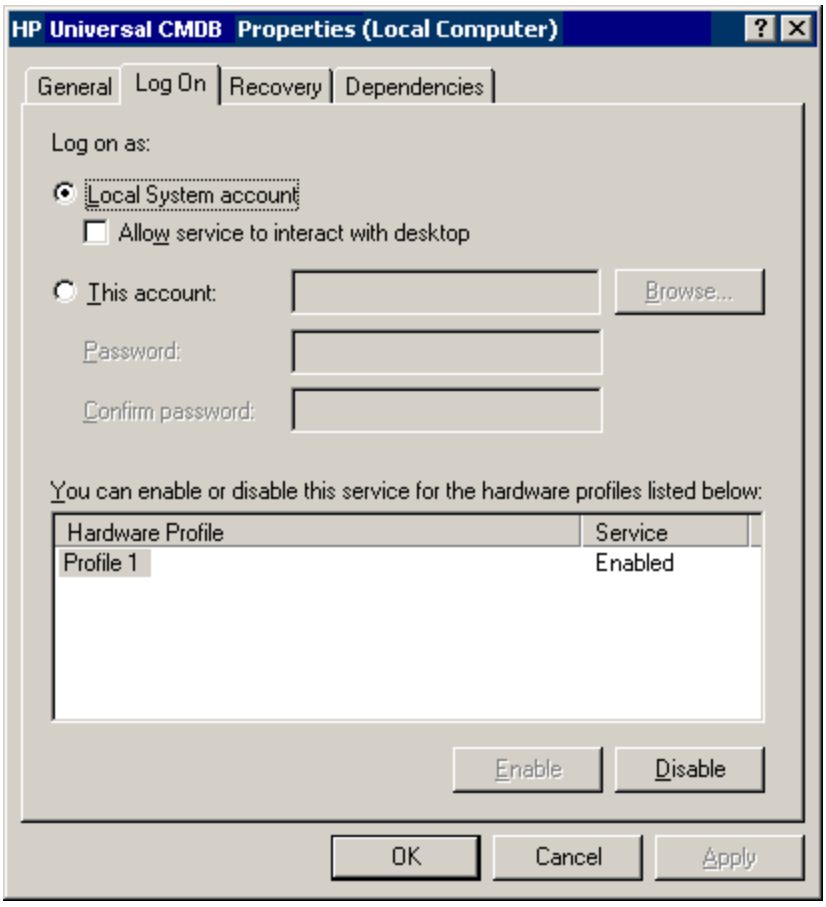
在 Windows 平台上，运行服务器和数据库配置实用程序时，将安装运行所有 HP Universal CMDB 服务和进程的 HP Universal CMDB 服务。默认情况下，此服务以本地系统用户的身份运行。但是，可能需要分配一个其他用户来运行服务 (例如，如果要使用 NTLM 身份验证)。

所分配的用于运行服务的用户必须具有以下权限：

- 足够的数据库权限 (由数据库管理员定义)
- 足够的网络权限
- 本地服务器上的管理员权限

要更改服务用户，请执行以下操作：

1. 通过“开始”菜单 (“开始”>“所有程序”>“HP UCMDB”>“Stop HP Universal CMDB Server”) 或通过停止 HP Universal CMDB 服务器服务，禁用 HP Universal CMDB。有关详细信息，请参阅《HP Universal CMDB 管理指南》中描述如何启动和停止 UCMDB 服务器服务的章节
2. 在 Windows 的“服务”窗口中，双击 **UCMDB_Server**。此时将打开“UCMDB_Server 的属性(本地计算机)”对话框。
3. 单击“登录”选项卡。



4. 选择“此帐户”，然后浏览并从计算机的有效用户列表中选择另一用户。
5. 输入所选用户的 Windows 密码，并确认此密码。

6. 单击“应用”保存设置，然后单击“确定”关闭对话框。

7. 通过“开始”菜单 (“开始”>“所有程序”>“HP UCMDB”>“Start HP Universal CMDB Server”) 或通过启动 HP Universal CMDB 服务器服务，启用 HP Universal CMDB。有关详细信息，请参阅《HP Universal CMDB 管理指南》中描述如何启动和停止 UCMDB 服务器服务的章节。

为 Configuration Manager 加密数据库密码

CM 数据库密码存储在 **<*Configuration Manager 安装目录*>\conf\database.properties** 文件中。如果需要加密密码，默认的加密算法应与 FIPS 140-2 的标准一致。

通过密钥完成加密，密钥可确保对密码进行加密。密钥本身将通过另一个称为主密钥的密钥进行加密。两个密钥都使用相同的算法进行加密。有关加密进程中使用的参数的详细信息，请参阅Configuration Manager 数据库密码加密的参数 (第 13 页)。

警告：如果更改加密算法，则以前加密的所有密码都将无法使用。

要更改数据库密码的加密，请执行以下操作：

1. 打开 **<*Configuration Manager 安装目录*>\conf\database.properties** 文件并编辑以下字段：
   - **engineName。**输入加密算法的名称。
   - **keySize。**输入所选算法的主密钥的大小。
2. 运行 **generate-keys.bat** 脚本，可创建 **<*Configuration Manager 安装目录*>\security\encrypt_repository** 文件并生成加密密钥。
3. 运行 **bin\encrypt-password.bat** 实用程序，以加密密码。设置 **-h** 标记，查看可用选项。
4. 复制密码加密实用程序的结果，并将结果加密粘贴到 **conf\database.properties** 文件。

Configuration Manager 数据库密码加密的参数

下表列出了 **encryption.properties** 文件中用于 CM 数据库密码加密的参数。有关加密数据库密码的详细信息，请参阅为 Configuration Manager 加密数据库密码 (第 13 页)。

参数	描述
cryptoSource	表示实施加密算法的基础结构。可用选项如下： • **lw。**使用 Bouncy Castle 轻型实施措施 (默认选项) • **jce。**Java 加密增强功能 (标准 Java 加密基础结构)

参数	描述
storageType	表示密钥存储的类型。 目前，仅支持**二进制文件**。
binaryFileStorageName	表示文件中存储主密钥的位置。
cipherType	密码类型。目前，仅支持 **symmetricBlockCipher**。
engineName	加密算法的名称。 可用选项如下： • **AES**。美国加密标准。此加密与 FIPS 140-2 兼容。 (默认选项) • **Blowfish** • **DES** • **3DES**。 (FIPS 140-2 兼容) • **空**。无加密
keySize	主密钥的大小。密钥的大小由算法确定： • **AES**。128、192、或者 256 (默认选项为 256) • **Blowfish**。 0-400 • **DES**。 56 • **3DES**。 156
encodingMode	二进制加密结果的 ASCII 编码。 可用选项如下： • **Base64** (默认选项) • **Base64Url** • **Hex**
algorithmModeName	算法模式。目前，仅支持 **CBC**。
algorithmPaddingName	使用的填充算法。 可用选项如下： • **PKCS7Padding** (默认选项) • **PKCS5Padding**

参数	描述
jceProviderName	JCE 加密算法的名称。 **备注：**只有当 crytpSource 为 jce 时才相关。对于 lw，将使用 engineName。

第 2 章：启用安全套接字层 (SSL) 通信

本章包括：

在包含自签名证书的服务器计算机上启用 SSL - UCMDB

以下几节将介绍如何配置 HP Universal CMDB 以支持使用安全套接字层 (SSL) 通道进行通信。

1. **先决条件**

   a. 开始以下过程之前，请先删除位于 **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystor** 中的旧 **server.keystore**。

   b. 将 HP Universal CMDB 密钥库 (JKS 类型) 放在 **C:\hp\UCMDB\UCMDBServer\conf\security** 文件夹中。

2. **生成服务器密钥库**

   a. 创建包含自签名证书和匹配的私钥的密钥库 (JKS 类型)：

      - 在 **C:\hp\UCMDB\UCMDBServer\bin\jre\bin** 中运行以下命令：

        ```
        keytool -genkey -alias hpcert -keystore
        C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore
        ```

        此时将打开控制台对话框。

      - 输入密钥库密码。如果密码已更改，则在 **UCMDB:service=Security Services** 中运行 **changeKeystorePassword** JMX 操作。如果密码尚未更改，则使用默认的 **hppass** 密码。

      - 回答问题“您叫什么名字?”输入 HP Universal CMDB Web 服务器名称。根据组织输入其他参数。

      - 输入密钥密码。密钥密码必须与密钥库密码相同。

        将创建名为 **server.keystore** 的 JKS 密钥库，其中包含名为 **hpcert** 的服务器证书。

   b. 将自签名证书导出到文件：

      在 **C:\hp\UCMDB\UCMDBServer\bin\jre\bin** 中运行以下命令：

      ```
      keytool -export -alias hpcert -keystore
      C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <your
      password> -file hpcert
      ```

3. **将证书放在客户端的信任库中**

   生成 **server.keystore** 并导出服务器证书之后，对于每个需要使用此自签名证书通过 SSL 与 HP Universal CMDB 通信的客户端，将此证书放在客户端的信任库中。

   备注： **server.keystore** 中只能有一个服务器证书。

4. **禁用 HTTP 端口 8080**

   有关详细信息，请参阅启用或禁用 HTTP/HTTPS 端口 (第 29 页)。

   备注： 关闭 HTTP 端口之前，请先检查 HTTPS 通信是否可用。

5. **重新启动服务器**

6. **显示 HP Universal CMDB**

   要验证 UCMDB 服务器是否安全，请在 Web 浏览器中输入以下 URL：**https://<UCMDB 服务器名称或 IP 地址>:8443/ucmdb-ui**。

在包含自签名证书的服务器计算机上启用 SSL - Configuration Manager

本节介绍如何配置 Configuration Manager，以支持使用安全套接字层 (SSL) 通道进行身份验证和加密。

Configuration Manager 使用 Tomcat 7.0.19 作为应用程序服务器。

1. **先决条件** (首次安装时不相关)

   开始以下过程之前，请先删除位于 ***<Configuration Manager 安装目录>*\java\windows\x86_64\lib\security** 文件夹或 ***<Configuration Manager 安装目录>*\java\linux\x86_64\lib\security** 文件夹 (任意相关的文件夹) 中的旧 **tomcat.keystore** 文件 (如有)。

2. **生成服务器密钥库**

   创建包含自签名证书和匹配的私钥的密钥库 (JKS 类型)：

   - 从 ***<Configuration Manager 安装目录>*\java\windows\x86_64\bin** 或 ***<Configuration Manager 安装目录>*\java\linux\x86_64\bin**，运行以下命令：

     ```
     keytool -genkey -alias tomcat -keyalg RSA -keystore ..\lib\
     security\tomcat.keystore
     ```

     此时将打开控制台对话框。

   - 输入密钥库密码。如果密码已更改，则在文件中进行手动更改。

   - 回答问题“您叫什么名字?”输入 Configuration Manager Web 服务器名称。根据组织输入其他参数。

   - 输入密钥密码。密钥密码必须与密钥库密码相同。

     将创建名为 **tomcat.keystore** 的 JKS 密钥库，其中包含名为 **hpcert** 的服务器证书。

3. **将证书放在客户端的信任库中**

   将证书添加到计算机上 Internet Explorer 客户端的信任库中 (“工具”>“Internet 选项”>“内容”>“证书”)。如果没有执行此操作，则系统将在您首次尝试使用 Configuration Manager 时提示您执行该操作。

限制：tomcat.keystore 中只能有一个服务器证书。

4. **修改 server.xml 文件**

   打开 **server.xml** 文件，它位于 ***<Configuration Manager 安装目录>*\servers\server-0\conf**。找到以下列代码开头的部分

   ```
   Connector port="8143"
   ```

   该信息显示在注释中。通过删除注释字符并将以下属性添加到 HTTPS 连接器中，激活脚本：

   ```
   keystoreFile="<tomcat.keystore file location>" (请参阅步骤 2)
   keystorePass="<password>"
   ```

   注释掉以下行：

   ```
   <Listener className="org.apache.catalina.core.AprLifecycleListener"
   SSLEngine="on" />
   ```

   备注：请勿阻止 HTTP 连接端口。如果要阻止 HTTP 通信，则可使用防火墙。

5. **重新启动服务器**

   重新启动 Configuration Manager 服务器。

6. **验证服务器安全**

   要验证 Configuration Manager 服务器是否安全，请在 Web 浏览器中输入以下 URL：**https://<Configuration Manager 服务器名称或 IP 地址>:8143/cnc**。

7. 在 Configuration Manger 中，转到“设置”>“应用程序管理”>“邮件设置”，并根据上述值在“Configuration Manager 完整 URL”中更改协议和端口。

8. 在 UCMDB 中，转到“基础结构设置管理器”>“常规设置”，并根据上述值在“Configuration Manager URL”中更改协议和端口。

提示：如果无法建立连接，请尝试使用另一浏览器，或升级至较新版本的浏览器。

在包含来自证书颁发机构的证书的服务器计算机上启用 SSL - UCMDB

要使用由证书颁发机构 (CA) 颁发的证书，密钥库必须是 Java 格式。以下示例介绍了如何格式化 Windows 计算机的密钥库。

1. **先决条件**

   开始以下过程之前，请先删除位于 **C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore** 中的旧 **server.keystore**。

2. **生成服务器密钥库**

   a. 生成 CA 签名的证书，并在 Windows 系统中安装该证书。

   b. 使用 Microsoft 管理控制台 (**mmc.exe**) 将证书导出到 ***.pfx** 文件 (包括私钥) 中。

   输入任何字符串作为 **pfx** 文件的密码。 (将密钥库类型转换成 JAVA 密钥库时，系统将要求您输入此密码。) **.pfx** 文件现在包含公用证书和私钥，并且受密码保护。

   c. 将创建的 **.pfx** 文件复制到以下文件夹：**C:\hp\UCMDB\UCMDBServer\conf\security**。

   d. 打开命令提示符，并将目录更改为 **C:\hp\UCMDB\UCMDBServer\bin\jre\bin**。

   通过运行以下命令，将密钥库类型从 **PKCS12** 更改为 **JAVA** 密钥库：

   ```
   keytool -importkeystore -srckeystore c:\hp\UCMDB\UCMDBServer\conf\securit
   y\<pfx file name> -srcstoretype PKCS12 -destkeystore server.keystore
   ```

   系统将要求您输入源 (**.pfx**) 密钥库密码。此密码是在步骤 b 中创建 **pfx** 文件时所提供的密码。

   e. 输入目标密钥库密码。此密码必须与之前在“安全服务”的 **changeKeystorePassword** JMX 方法中定义的密码相同。如果密码未更改，则使用默认的 **hppass** 密码。

   > **备注：**源密钥库密码必须与目标密钥库密码相同。

   f. 生成证书之后，将禁用 HTTP 端口 8080。有关详细信息，请参阅启用或禁用 HTTP/HTTPS 端口 (第 29 页)。

   g. 如果使用的密码不是 **hppass** 或用于 **.pfx** 文件的密码，则运行

changeKeystorePassword JMX 方法，并确保密钥密码相同。

备注：关闭 HTTP 端口之前，请先检查 HTTPS 通信是否可用。

3. **重新启动服务器**

4. **验证服务器安全**

   要验证 UCMDB 服务器是否安全，请在 Web 浏览器中输入以下 URL：**https://<UCMDB 服务器名称或 IP 地址>:8443/ucmdb-ui**。

警告：**server.keystore** 中只能有一个服务器证书。

在包含来自证书颁发机构的证书的服务器计算机上启用 SSL - Configuration Manager

对于 Configuration Manager，要使用由证书颁发机构 (CA) 颁发的证书，密钥库必须是 Java 格式。以下示例介绍了如何格式化 Windows 计算机的密钥库。

1. **先决条件**

   开始以下过程之前，请先删除位于 ***<Configuration Manager 安装目录>\java\windows\x86_64\lib\security*** 文件夹或 **<Configuration Manager 安装目录>\java\linux\x86_64\lib\security** 文件夹 (任意相关的文件夹) 中的旧 **tomcat.keystore** 文件 (如有)。

2. **生成服务器密钥库**

   a. 生成 CA 签名的证书，并在 Windows 系统中安装该证书。

   b. 使用 Microsoft 管理控制台 (**mmc.exe**) 将证书导出到 ***.pfx** 文件 (包括私钥) 中。

      输入任何字符串作为 **pfx** 文件的密码。 (将密钥库类型转换成 JAVA 密钥库时，系统将要求您输入此密码。)
      .pfx 文件现在包含公用证书和私钥，并且受密码保护。

      将创建的 **.pfx** 文件复制到以下文件夹：***<Configuration Manager 安装目录>\java\lib\security***。

   c. 打开命令提示符，并将目录更改为 ***<Configuration Manager 安装目录>\java\bin***。

      通过运行以下命令，将密钥库类型从 **PKCS12** 更改为 **JAVA** 密钥库：

```
keytool -importkeystore -srckeystore <Configuration Manager 安装目录>\con
f\security\<pfx 文件名> -srcstoretype PKCS12 -destkeystore tomcat.keystor
e
```

系统将要求您输入源 (**.pfx**) 密钥库密码。此密码是在步骤 b 中创建 pfx 文件时所提供的密码。

3. **修改 server.xml 文件**

   打开 **server.xml** 文件，它位于 ***<Configuration Manager 安装目录>*\servers\server-0\conf**。找到以下列代码开头的部分

   ```
   Connector port="8143"
   ```

   该信息显示在注释中。通过删除注释字符并添加以下两行，激活脚本：

   ```
   keystoreFile="../../java/lib/security/tomcat.keystore"
   keystorePass="password" />
   ```

   注释掉以下行：

   ```
   <Listener className="org.apache.catalina.core.AprLifecycleListener"
   SSLEngine="on" />
   ```

   备注：请勿阻止 HTTP 连接端口。如果要阻止 HTTP 通信，则可使用防火墙。

4. **重新启动服务器**

   重新启动 Configuration Manager 服务器。

5. **验证服务器安全**

   要验证 Configuration Manager 服务器是否安全，请在 Web 浏览器中输入以下 URL：**https://<Configuration Manager 服务器名称或 IP 地址>:8143/cnc**。

6. 在 Configuration Manger 中，转到“设置”>“应用程序管理”>“邮件设置”，并根据上述值在“Configuration Manager 完整 URL”中更改协议和端口。

7. 在 UCMDB 中，转到“基础结构设置管理器”>“常规设置”，并根据上述值在“Configuration Manager URL”中更改协议和端口。

限制：tomcat.keystore 中只能有一个服务器证书。

在客户端计算机上启用 SSL - UCMDB

如果 HP Universal CMDB Web 服务器使用的证书是由知名的证书颁发机构 (CA) 颁发的，则您的 Web 浏览器无需任何进一步操作即可验证证书。

如果 Web 浏览器不信任 CA，则应将整个证书信任路径或由 HP Universal CMDB 使用的证书导入到浏览器的信任库中。

以下示例演示了如何将自签名 **hpcert** 证书导入到 Internet Explorer 将使用的 Windows 信任库中。

要将证书导入到 Windows 信任库中，请执行以下操作：

1. 找到 **hpcert** 证书，并将其重命名为 **hpcert.cer**。

   在 Windows 资源管理器中，图标将显示该文件是安全证书。

2. 双击 **hpcert.cer**，打开“Internet Explorer 证书”对话框。

3. 按照说明启用信任，方法是使用证书导入向导安装证书。

备注：将 UCMDB 服务器颁发的证书导入到 Web 浏览器的另一个方法是：登录 UCMDB，并在显示不受信任证书警告时安装证书。

启用含客户端证书的 SSL - Configuration Manager

如果 Configuration Manager Web 服务器使用的证书是由知名的证书颁发机构 (CA) 颁发的，则您的 Web 浏览器无需任何进一步操作即可验证证书。

如果 CA 不受服务器信任库信任，请将 CA 证书导入到服务器信任库中。

以下示例演示了如何将自签名 **hpcert** 证书导入到服务器信任库中 (cacerts)。

要将证书导入到 Server 信任库中，请执行以下操作：

1. 在客户端计算机上，找到 **hpcert** 证书，并将其重命名为 **hpcert.cer**。

2. 将 **hpcert.cer** 复制到服务器计算机上的 ***<Configuration Manager 安装目录>*\java\windows\x86_64bin** 文件夹中。

3. 在服务器计算机上，使用 keytool 实用程序通过以下命令将 CA 证书导入信任库 (cacerts)：

   ```
   <Configuration_Manager 安装目录>\java\bin\keytool.exe -import
   -alias hp -file hpcert.cer -keystore ..\lib\security\cacerts
   ```

4. 如下所示修改 **server.xml** 文件 (位于 ***<Configuration Manager 安装目录>*\servers\server-0\conf** 文件夹)：

   a. 按照修改 server.xml 文件 (第 22 页)中所述进行更改。

   b. 进行更改之后，请将以下属性添加到 HTTPS 连接器：

```
truststoreFile="../../java/lib/security/cacerts"
truststorePass="changeit" />
```

c. 设置 clientAuth="true"。

5. 按照验证服务器安全 (第 22 页)中所述验证服务器的安全性。

在客户端 SDK 上启用 SSL

您可以在客户端 SDK 和服务器 SDK 之间使用 HTTPS 传输：

1. 在客户机的嵌入了客户端 SDK 的产品中，查找传输设置，并确保将其配置为 HTTPS 而不是 HTTP。

2. 将 CA 证书/自签名公用证书下载到客户机，并将其导入到 JRE 上即将连接到服务器的 **cacerts** 信任库中。

   使用以下命令：

   ```
   Keytool -import -alias <CA 名称> -trustcacerts -file <服务器公用证书路径> -k
   eystore <客户端 JRE cacerts 信任库路径 (例如 x:\program files\java\jre\lib\s
   ecurity\cacerts)>
   ```

为 SDK 启用相互证书身份验证

此模式将使用 SSL，并启用 UCMDB 的服务器身份验证和 UCMDB-API 客户端的客户端身份验证。服务器和 UCMDB-API 客户端都会将其证书发送到其他实体，进行身份验证。

备注：在使用相互身份验证的 SDK 上启用 SSL 的以下方法是最安全方法，因而是推荐的通信模式。

1. 在 UCMDB 中强化 UCMDB-API 客户端连接器：

   a. 访问 UCMDB JMX 控制台：启动 Web 浏览器，并输入以下地址：**http://<UCMDB 计算机名称或 IP 地址>:8080/jmx-console**。可能需要使用用户名和密码登录 (默认为 sysadmin/sysadmin)。

   b. 找到 **UCMDB:service=Ports Management Services**，然后单击该链接打开“Operations”页面。

   c. 找到 **PortsDetails** 操作，并单击“Invoke”。请记下用于 HTTPS 的客户端身份验证端口号。默认为 8444，且该端口应该已启用。

   d. 返回到“Operations”页面。

   e. 要将 ucmdb-api 连接器映射到相互身份验证模式，请使用以下参数调用

mapComponentToConnectors 方法：

- **componentName**：ucmdb-api
- **isHTTPSWithClientAuth**：true
- 所有其他标志：false

将显示以下消息：

Operation succeeded.Component ucmdb-api is now mapped to:HTTPS_CLIENT_AUTH ports.

f. 返回到“Operations”页面。

2. 确保运行 UCMDB-API 客户端的 JRE 拥有包含客户端证书的密钥库。
3. 从其密钥库导出 UCMDB-API 客户端证书。
4. 将导出的 UCMDB-API 客户端证书导入到 UCMDB 服务器信任库。
   a. 在 UCMDB 计算机上，将创建的 UCMDB-API 客户端证书文件复制到 UCMDB 上的以下目录：

      C:\HP\UCMDB\UCMDBServer\conf\security

   b. 运行以下命令：

      ```
      C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore
      C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file <导出的
      UCMDB-API 客户端证书> - alias ucmdb-api
      ```

   c. 输入 UCMDB 服务器信任库密码 (默认为 **hppass**)。
   d. 询问 **Trust this certificate?** 时，请按 **y**，然后按 **Enter**。
   e. 确保输出**证书**已添加到密钥库。
5. 从服务器密钥库导出 UCMDB 服务器证书。
   a. 在 UCMDB 计算机上运行以下命令：

      ```
      C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert
      -keystore
      C:\HP\UCMDB\UCMDBServer\conf\security\server.keystore
      -file C:\HP\UCMDB\conf\security\server.cert
      ```

   b. 输入 UCMDB 服务器信任库密码 (默认为 **hppass**)。

c. 验证证书是否在以下目录中创建：

C:\HP\UCMDB\UCMDBServer\conf\security\server.cert

6. 将导出的 UCMDB 证书导入到 UCMDB-API 客户端信任库的 JRE。
7. 重新启动 UCMDB 服务器和 UCMDB-API 客户端。
8. 要从 UCMDB-API 客户端连接到 UCMDB-API 服务器，请使用以下代码：

```
UcmdbServiceProvider provider = UcmdbServiceFactory.getServiceProvider
("https", <SOME_HOST_NAME>, <HTTPS_WITH_CLIENT_AUTH_PORT_NUMBER
(default:8444>));
UcmdbService ucmdbService = provider.connect(provider.createCertificateCrede
ntials(<TheClientKeystore.
e.g:"c:\\client.keystore">, <KeystorePassword>), provider.createClientContext
(<ClientIdentification>));
```

配置 UCMDB 中的 CAC 支持

本节描述了如何在 UCMDB 上配置通用访问卡 (CAC) 支持。

备注：只有在使用 Internet Explorer 8、9 或 10 时，CAC 支持才可用。

1. 按照以下步骤，将 CA 根证书和任意中间证书导入到 UCMDB 服务器信任库中：
   a. 在 UCMDB 计算机上，将这些证书文件复制到 UCMDB 上的以下目录中：

   C:\HP\UCMDB\UCMDBServer\conf\security

   备注：如果您的证书是 Microsoft p7b 格式，则需要将其转换为 PEM 格式。

   b. 对每个证书，运行以下命令：

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore
   C:\HP\UCMDB\UCMDBServer\conf\security\server.truststore -file
   <证书> - alias <证书别名>
   ```

   c. 输入 UCMDB 服务器信任库密码 (默认为 **hppass**)。

   d. 询问 **Trust this certificate?** 时，请按 **y**，然后按 **Enter**。

   e. 确保输出**证书**已添加到密钥库。

2. 通过启动 Web 浏览器并输入以下服务器地址打开 JMX 控制台：http://<UCMDB 服务

器主机名或 IP>:8080/jmx-console。

您可能需要使用用户名和密码登录。

3. 在 UCMDB 下，单击 **UCMDB:service=Ports Management Services** 打开“Operations”页面。
   - (可选) 单击 **ComponentsConfigurations**。执行以下操作：
     - 将 **HTTPSetPort** 设置为 **8444**，然后单击“Invoke”。
     - 单击“Back to MBean”。
   - 单击 **mapComponentToConnectors**。执行以下操作：
     - 在 mapComponentToConnectors 服务中，将 **componentName** 设置为 **ucmdb-ui**。
     - 仅将 **isHTTPSWithClientAuth** 设置为 **true**，然后单击“Invoke”。
     - 单击“Back to MBean”。
     - 在 mapComponentToConnectors 服务中，将 **componentName** 设置为 **root**。
     - 仅将 **isHTTPSWithClientAuth** 设置为 **true**，然后单击“Invoke”。
4. 在 UCMDB 下，单击 **UCMDB:service=Security Services** 打开“Operations”页面。在 **loginWithCAC** 服务中，执行以下操作：
   - 将 **loginWithCAC** 设置为 **true**，然后单击“Invoke”。
   - 单击“Back to MBean”。
   - (可选) 单击 **usernameField** 指定将由 UCMDB 用于提取用户名的证书字段，然后单击“Invoke”。

     备注：如果未指定字段，则默认使用 PRINCIPAL_NAME_FROM_SAN_FIELD。
   - 单击“Back to MBean”。
   - 单击 **pathToCRL** 设置脱机证书吊销列表 (CRL) 的路径，然后单击“Invoke”；当联机 (证书) 列表不可用时将使用吊销列表。

     备注：如果正在使用本地 CRL 且 UCMDB 服务器有正在运行的 Internet 连接，则使用本地 CRL。在以下情况下，任何证书 (即使未调用) 的验证都将失败：

- 已设置 CRL 路径但缺少 CRL 文件
- CRL 已过期
- CRL 具有不正确的签名

如果未设置脱机 CRL 的路径且 UCMDB 服务器无法访问联机 CRL，则包含 CRL 或 OCSP URL 的所有证书都将被拒绝 (因为 URL 无法访问，吊销检查失败)。要授予 UCMDB 服务器 Internet 访问权，请在 **wrapper.conf** 文件中取消注释以下行并提供有效代理和端口：

```
#wrapper.java.additional.40=-Dhttp.proxyHost=<PROXY_ADDR>
#wrapper.java.additional.41=-Dhttp.proxyPort=<PORT>
#wrapper.java.additional.42=-Dhttps.proxyHost=<PROXY_ADDR>
#wrapper.java.additional.43=-Dhttps.proxyPort=<PORT>
```

- 单击“Back to MBean”。
- (可选) 将 **onlyCACCerts** 设置为 **true**，然后单击“Invoke”。

  将此操作设置为 **true** 可仅接受来自物理 CAC 设备的证书。

现在您应该可以使用 https://<UCMDB 服务器主机名或 IP>.<域名>:8444 登录 UCMDB。

5. 将 UCMDB 配置为使用 LW-SSO 身份验证并重新启动 UCMDB 服务器。

有关 LW-SSO 身份验证的详细信息，请参阅支持使用 LW-SSO 登录 HP Universal CMDB (第 89 页)。

更改服务器密钥库密码

安装服务器之后，HTTPS 端口随即打开，并且密钥库的密码保护强度为弱 (默认为 **hppass**)。如果仅打算使用 SSL，则必须更改密码。

以下过程只介绍了如何更改 **server.keystore** 密码。但是，您应该执行与更改 **server.truststore** 密码相同的过程。

备注：必须执行此过程中的每个步骤。

1. 启动 UCMDB 服务器。
2. 在 JMX 控制台中更改密码：
   a. 启动 Web 浏览器，并输入以下服务器地址：**http://<UCMDB 服务器主机名或 IP>:8080/jmx-console**。

您可能需要使用用户名和密码登录。

b. 在 UCMDB 下，单击 **UCMDB:service=Security Services** 打开“Operations”页面。

c. 找到 **changeKeystorePassword** 操作，并执行该操作。

此字段不得为空，且长度不得少于六个字符。仅在数据库中更改密码。

3. 停止 UCMDB 服务器。

4. 运行命令。

在 **C:\hp\UCMDB\UCMBServer\bin\jre\bin** 中运行以下命令：

a. 更改库密码：

keytool -storepasswd -new <新的密钥库密码> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore -storepass <当前密钥库密码>

b. 以下命令将显示密钥库的内部密钥。第一个参数是别名。为下一条命令保存此参数：

keytool -list -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore

c. 更改密钥密码 (如果库不为空)：

keytool -keypasswd -alias <别名> -keypass <当前密码> -new <新密码> -keystore C:\hp\UCMDB\UCMDBServer\conf\security\server.keystore

d. 输入新密码。

5. 启动 UCMDB 服务器。

6. 对服务器信任库重复以上过程。

启用或禁用 HTTP/HTTPS 端口

您可以从用户界面中或从 JMX 控制台启用或禁用 HTTP 和 HTTPS 端口。

要从用户界面中启用或禁用 HTTP/HTTPS 端口，请执行以下操作：

1. 登录到 HP Universal CMDB。

2. 选择“管理”>“基础结构设置管理器”。

3. 在“按名称筛选”框中输入 **http** 或 **https** 以显示 HTTP 设置。

- **启用 HTTP(S) 连接**。**True**：端口已启用。**False**：端口已禁用。

4. 重新启动服务器以应用变更。

> **警告：**默认情况下，HTTPS 端口处于打开状态；关闭此端口将阻止 **Server_Management.bat** 正常工作。

要从 JMX 控制台启用或禁用 HTTP/HTTPS 端口，请执行以下操作：

1. 启动 Web 浏览器，并输入以下地址：http://localhost.<域名>:8080/jmx-console。
2. 输入 JMX 控制台身份验证凭据。默认凭据为：
   - 登录名 = **sysadmin**
   - 密码 = **sysadmin**
3. 找到 **UCMDB:service=Ports Management Services**，然后单击该链接打开“Operations”页面。
4. 要启用或禁用 HTTP 端口，请找到 **HTTPSetEnable** 操作，然后设置值。
   - **True**：端口已启用。
   - **False**：端口已禁用。
5. 要启用或禁用 HTTPS 端口，请找到 **HTTPSSetEnable** 操作，然后设置值。
   - **True**：端口已启用。
   - **False**：端口已禁用。
6. 要启用或禁用具有客户端身份验证的 HTTPS 端口，请找到 **HTTPSClientAuthSetEnable** 操作，然后设置值。
   - **True**：端口已启用。
   - **False**：端口已禁用。

将 UCMDB Web 组件映射到端口

您可以从 JMX 控制台配置每个 UCMDB 组件到可用端口的映射。

要查看当前组件配置，请执行以下操作：

1. 启动 Web 浏览器，并输入以下地址：**http://localhost.<域名>:8080/jmx-console**。
2. 输入 JMX 控制台身份验证凭据。默认凭据为：

   登录名 = **sysadmin**

密码 = **sysadmin**

3. 找到 **UCMDB:service=Ports Management Services**，然后单击该链接打开“Operations”页面。
4. 找到 **ComponentsConfigurations** 方法，并单击“Invoke”。
5. 对于每个组件，均会显示有效端口和当前映射的端口。

要映射组件，请执行以下操作：

1. 找到 **UCMDB:service=Ports Management Services**，然后单击该链接打开“Operations”页面。
2. 找到 **mapComponentToConnectors** 方法。
3. 在“Value”框中输入组件名称。为每个与选项对应的端口选择 **True** 或 **False**。单击“Invoke”。所选组件将映射到所选端口。通过调用 **serverComponentsNames** 方法，可以查找组件名称。
4. 对每个相关组件重复以上过程。

备注：

- 每个组件必须至少映射到一个端口。如果未将组件映射到任何端口，则默认情况下会将其映射到 HTTP 端口。
- 如果将组件同时映射到 HTTPS 端口和具有客户端身份验证的 HTTPS 端口，则仅会映射客户端身份验证选项 (这种情况下，另一个选项冗余)。
- 如果将 UCMDB UI 组件的 **isHTTPSWithClientAuth** 设置为 **True**，则必须将根组件的该设置也设为 **True**。

您也可以更改分配到每个端口的值。

要设置端口的值，请执行以下操作：

1. 找到 **UCMDB:service=Ports Management Services**，然后单击该链接打开“Operations”页面。
2. 要设置 HTTP 端口的值，请找到 **HTTPSetPort** 方法，并在“Value”框中输入值。单击“Invoke”。
3. 要设置 HTTP 端口的值，请找到 **HTTPSSetPort** 方法，并在“Value” 框中输入值。单击“Invoke”。
4. 要为具有客户端身份验证的 HTTPS 端口设置值，请找到 **HTTPSClientAuthSetPort** 方法，并在“Value”框中输入值。单击“Invoke”。

将 Configuration Manager 配置为与使用 SSL 的 UCMDB 一起使用

可以将 Configuration Manager 配置为与使用安全套接字层 (SSL) 的 UCMDB 一起使用。默认情况下，端口 8443 上的 SSL 连接器在 UCMDB 中已启用。

1. 转到 **<UCMDB 安装目录>\bin\jre\bin** 并运行以下命令：

   ```
   keytool -export -alias hpcert -keystore <UCMDB 服务器目录>
   \conf\security\server.keystore -storepass hppass -file <证书文件>
   ```

2. 将证书文件复制到本地 Configuration Manager 计算机上的临时位置。

3. 执行 Configuration Manager 新安装，或重新配置 Configuration Manager 的现有安装。有关说明，请参阅交互《HP Universal CMDB 部署指南》中的相关章节。

   在 UCMDB 配置屏幕中，将协议设置为 HTTPS，并选择您在步骤 2 中复制的证书文件。

4. 将 **hpcert.cer** 复制到服务器计算机上的 ***<Configuration Manager 安装目录>\java\windows\x86_64\bin*** 文件夹中。

5. 在服务器计算机上，使用 keytool 实用程序通过以下命令将证书导入信任库 (cacerts)：

   ```
   <Configuration Manager 安装目录>\java\bin\keytool.exe -import -alias hp -
   file hpcert.cer -keystore <Configuration Manager 安装目录>\java\windows\x86_
   64\lib\security\cacerts
   ```

6. 将 **hpcert.cer** 复制到服务器计算机上的 ***<Configuration Manager 安装目录>*\java\windows\x86_64\lib\security** 文件夹中。

7. 创建包含自签名证书和匹配的私钥的服务器密钥库 (JKS 类型)。从 ***<Configuration Manager 安装目录>*\java\windows\x86_64\bin** 文件夹中，运行以下命令：

   ```
   keytool –genkey –alias tomcat –keyalg RSA –keystore <Configuration Manager 安
   装目录>\java\windows\x86_64\lib\security\tomcat.keystore
   ```

   a. 输入密钥库密码。

   b. 对于问题 `What is your first and last name?`，请输入 Configuration Manager Web 服务器名称，并根据自己所在的组织输入其他参数。

   c. 输入密钥密码。密钥密码必须与密钥库密码相同。将创建名为 **tomcat.keystore** 的 JKS 密钥库，其中包含名为 **hpcert** 的服务器证书。

8. 按以下步骤修改 **server.xml** 文件：

a. 打开 server.xml 文件，它位于 **<*Configuration Manager 安装目录*>\servers\server-0\conf** 文件夹中。找到以下列代码开头的部分：

```
Connector port="8143"
```

此代码以注释的形式出现。通过删除注释字符激活脚本，然后添加以下行：

```
keystoreFile="<Configuration Manager 安装目录>\java\windows\x86_64\lib\se
curity\tomcat.keystore"
keystorePass="password"
truststoreFile="<Configuration Manager 安装目录>\java\windows\x86_64\lib\
security\cacerts"
truststorePass="changeit" />
```

b. 注释掉以下行：

```
<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEn
gine="on" />
```

9. 重新启动服务器。

要将 Configuration Manager 配置为与使用 SSL 的其他产品 (如负载平衡器) 一起使用，请通过运行以下命令，将产品的安全证书导入到 Configuration Manager 信任库 (默认为 jre 信任库)：

```
<CM JAVA 主目录>\bin\keytool -import -trustcacerts -alias <别名> -keystore
<CM JAVA 主目录>\lib\security\cacerts -storepass changeit -file <证书文件>
```

使 UCMDB KPI 适配器能够与 SSL 一起使用

可以将 UCMDB KPI 适配器信息配置为使用安全套接字层 (SSL) 发送。

1. 导出 Configuration Manager 证书：

```
<CM JAVA 主目录>\bin\keytool -export -alias tomcat -keystore
<CM JAVA 主目录>\lib\security\tomcat.keystore -storepass
<密钥库密码> -file <证书文件名>
```

2. 请按如下所示将从 Configuration Manager 导出的证书导入到 UCMDB 信任库中：

```
<UCMDB 服务器目录>\bin\jre\bin keytool -import -trustcacerts
-alias tomcat -keystore <UCMDB 服务器目录>\bin\jre\lib
\security\cacerts -storepass changeit -file <证书文件>
```

3. 请按如下所示将从 Configuration Manager 导出的证书导入到探测器的信任库中：

a. 打开命令提示并运行以下命令：

```
<DataFlowProbe 目录>\bin\jre\bin\keytool.exe -import -v -keystore
<DataFlowProbe 目录>\conf\security\hpprobeTrustStore.jks -file
<证书文件> -alias tomcat
```

b. 输入密钥库密码：logomania

c. 询问 **Trust this certificate?** 时，请按 **y**，然后按 **Enter**。

将显示以下消息：

Certificate was added to keystore.

有关强化 Data Flow Probe 的其他详细信息，请参阅Data Flow Probe 强化 (第 64 页)

4. 重新启动 UCMDB、Data Flow Probe 和 Configuration Manager。

为 UCMDB Browser 配置 SSL 支持

备注：此处提供的说明与 UCMDB Browser 版本 1.95 相关。如果使用更高的 UCMDB Browser 版本 (另从其他 UCMDB 产品套件中升级而来)，请参阅该版本的《HP Universal CMDB Browser Installation and Configuration Guide》中有关配置 SSL 支持的章节。

在 Tomcat 上安装和配置 SSL 支持，请执行以下操作：

1. 通过执行以下命令之一创建密钥库文件，以存储服务器的私钥和自签名证书：
   - 对于 Windows：**%JAVA_HOME%\bin\keytool -genkey -alias tomcat -keyalg RSA**
   - 对于 Unix：**$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA**

   对于上述两种命令，请均使用密码值 **changeit** (对于打开的控制台对话框中的所有其他字段，可使用任意值)。

2. 从 **$CATALINA_BASE/conf/server.xml** 的条目 **SSL HTTP/1.1 Connector** 中删除注释。其中，**$CATALINA_BASE** 是指 Tomcat 的安装目录。

   备注：有关如何配置 **server.xml** 使用 SSL 的完整说明，请访问 Apache Tomcat 官方站点：http://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html

3. 重新启动 Tomcat 服务器。

要使用 HTTPS 协议连接 UCMDB 服务器，请执行以下操作：

1. 在 **ucmdb_browser_config.xml** 中，将值 **https** 和 UCMDB 服务器的 HTTPS 端口值 (默认情况下为 8443) 分别分配给标记 **<协议>** 和 **<端口>**。

2. 将 UCMDB 服务器公用证书下载到 UCMDB Browser 计算机 (如果在 UCMDB 服务器上使用 SSL，则 UCMDB 管理员可为您提供此证书)，并通过执行以下命令将其导入到 JRE 中要与此服务器相连的 **cacerts** 信任库：

   "%JAVA_HOME%\bin\keytool" -import -alias ucmdb -trustcacerts -file <UCMDB 服务器证书文件> -keystore "%JAVA_HOME%\jre\lib\security\cacerts"

   其中，**<UCMDB 服务器证书文件>** 是指 UCMDB 服务器公用证书文件的完整路径。

3. 重新启动 Tomcat 服务器。

第 3 章：使用反向代理

本节描述了反向代理的安全性问题，以及如何将反向代理用于 HP Universal CMDB 和 Configuration Manager。主要讨论了反向代理在安全性方面的问题，但不包括缓存和负载平衡等其他方面的问题。

本章包括：

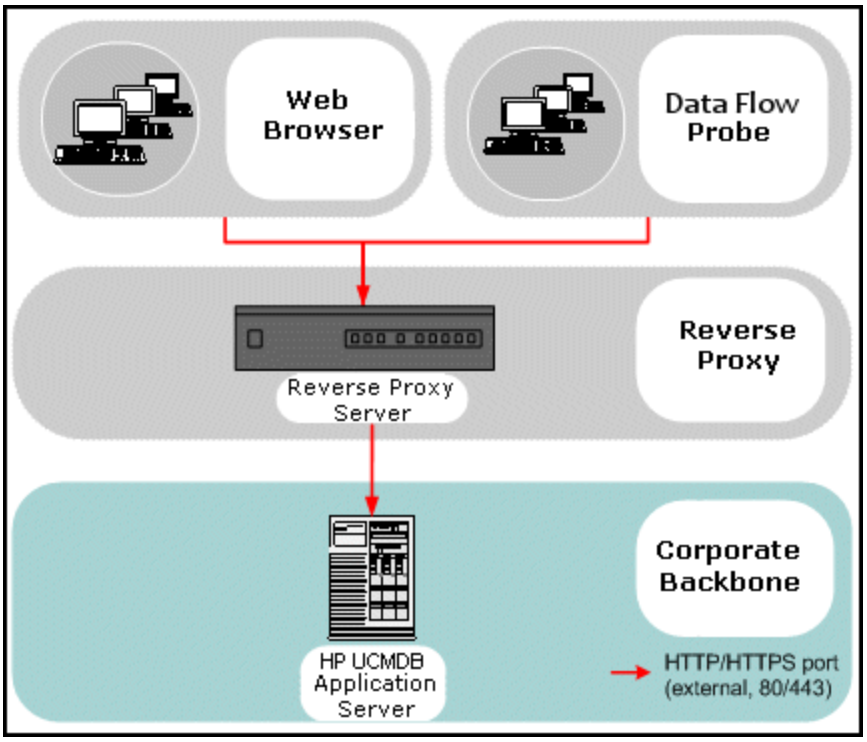
反向代理概述

反向代理是位于客户端计算机和 Web 服务器之间的中间服务器。对于客户端计算机，反向代理显示为标准 Web 服务器，用于为客户端计算机的 HTTP 协议请求提供服务。

客户端计算机使用反向代理的名称 (而不是 Web 服务器的名称) 发送对 Web 内容的普通请求。反向代理会将请求发送到其中一个 Web 服务器。尽管响应是通过反向代理发送回客户端计算机的，但在客户端计算机看来响应是由 Web 服务器发送的。

很有可能会有多个使用不同 URL 的反向代理表示相同的 UCMDB/CM 实例。另外，通过为每台 UCMDB/CM 服务器设置不同的根上下文，单一反向代理服务器也可用来访问多台 UCMDB/CM 服务器。

HP Universal CMDB 和 Configuration Manager 均支持 DMZ 体系结构中的反向代理。反向代理是 Data Flow Probe 和 Web 客户端及 HP Universal CMDB/CM 服务器之间的 HTTP 介体。



备注：

- 不同类型的反向代理需要不同的配置语法。有关 Apache 2.0.x 反向代理配置的示例，请参阅示例：Apache 2.0.x 配置 (第 39 页)。
- 只有使用计划程序创建报告的直接链接时，才需要配置前端 URL 设置。

使用反向代理服务器的安全性方面

反向代理服务器可用作堡垒主机。可以将代理配置为通过外部客户端直接寻址的唯一计算机，从而隐藏其他内部网络部分。通过使用反向代理，可以将应用程序服务器置于内部网络中的单台计算机上。

本节讨论在后端到后端拓扑环境中使用 DMZ 和反向代理。

在此类环境中使用反向代理的主要安全优势如下：

- 不会发生 DMZ 协议转换。传入协议和传出协议相同 (仅标题会产生变更)。
- 只允许对反向代理进行 HTTP 访问，这表示状态包检查防火墙可以更好地保护通信。
- 可以在反向代理上定义一组受限的静态重定向请求。
- 大多数 Web 服务器安全功能在反向代理上均可用 (身份验证方法、加密等)。

- 反向代理可屏蔽真实服务器的 IP 地址以及内部网络的体系结构。
- Web 服务器的唯一可访问客户端为反向代理。
- 此配置支持 NAT 防火墙 (与其他解决方案正好相反)。
- 反向代理只需使用防火墙中的最小开放端口数。
- 与其他 bastion 解决方案相比，反向代理可提供更优良的性能。

配置反向代理

本节介绍如何配置反向代理。从 UCMDB 版本 10.01 开始，UCMDB 不再需要任何配置。在反向代理端，根据反向代理的文档编辑配置文件。有关示例，请参阅示例： Apache 2.0.x 配置 (第 39 页)。

对于在 UCMDB 版本 10.01 之前创建的计划作业，还需按如下所示设置 UCMDB 中的配置：

使用基础结构设置配置反向代理

以下步骤说明如何访问“基础结构设置”以配置反向代理。只有使用计划程序创建报告的直接链接时，才需要此配置。

要配置反向代理，请执行以下操作：

1. 选择“管理”>“基础结构设置管理器”>“常规设置”类别。
2. 更改“前端 URL”设置。输入地址，例如 **https://my_proxy_server:443/**。

备注：进行此更改后，无法通过客户端直接访问 HP Universal CMDB 服务器。要更改反向代理配置，请使用服务器计算机上的 JMX 控制台。有关详细信息，请参阅下文所述的“使用 JMX 控制台配置反向代理”。

使用 JMX 控制台配置反向代理

通过使用 HP Universal CMDB 服务器上的 JMX 控制台，可以更改反向代理配置。只有使用计划程序创建报告的直接链接时，才需要此配置。

要更改反向代理配置，请执行以下操作：

1. 在 HP Universal CMDB 服务器计算机上启动 Web 浏览器，并输入以下地址：

   http://<计算机名称或 IP 地址>.<域名>:8080/jmx-console

   其中 **<计算机名称或 IP 地址>** 是安装了 HP Universal CMDB 的计算机。您可能需要使用用户名和密码登录。

2. 单击“UCMDB-UI”>“UCMDB-UI:name=UI Server frontend settings”链接。

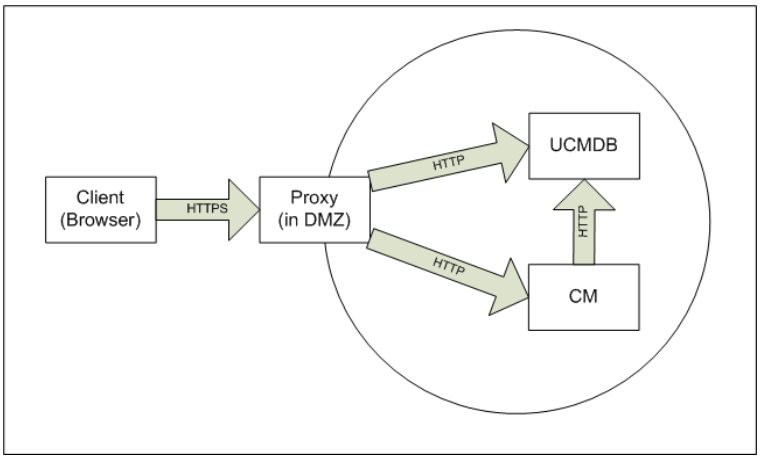
在 **setUseFrontendURLBySettings** 字段中，输入服务器代理 URL，例如，`https://my_proxy_server:443/`。

3. 单击“Invoke”。
4. 要查看此设置的值，请使用 **showFrontendURLInSettings** 方法。

示例：Apache 2.0.x 配置

本节介绍了支持使用 Apache 2.0.x 反向代理的示例配置文件，其中 Data Flow Probe 和应用程序用户均连接到 HP Universal CMDB。

下图演示了 Configuration Manager 和 UCMDB 的反向代理的配置过程。



备注：

- 在此示例中，HP Universal CMDB 计算机的 DNS 名称和端口为 UCMDB_server。
- 在此示例中，HP Configuration Manger 的 DNS 名称和端口为 UCMDB_CM_server。
- 只有熟悉 Apache 管理知识的用户才能进行此更改。

1. 打开 **<Apache 计算机根目录>\Webserver\conf\httpd.conf** 文件。
2. 启用以下模块：
   - **LoadModule proxy_module modules/mod_proxy.so**
   - **LoadModule proxy_http_module modules/mod_proxy_http.so**
3. 将以下行添加到 **httpd.conf** 文件中：

```
ProxyRequests off
<Proxy *>
     Order deny,allow
     Deny from all
```

```
    Allow from all
</Proxy>

ProxyPass /mam http://UCMDB_server/mam
ProxyPassReverse /mam http://UCMDB_server/mam
ProxyPass /mam_images http://UCMDB_server/mam_images
ProxyPassReverse /mam_images http://UCMDB_server/mam_images
ProxyPass /mam-collectors http://UCMDB_server/mam-collectors
ProxyPassReverse /mam-collectors http://UCMDB_server/mam-collectors
ProxyPass /ucmdb http://UCMDB_server/ucmdb
ProxyPassReverse /ucmdb http://UCMDB_server/ucmdb
ProxyPass /site http://UCMDB_server/site
ProxyPassReverse /site http://UCMDB_server/site
ProxyPass /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPass /status http://UCMDB_server/status
ProxyPassReverse /status http://UCMDB_server/status
ProxyPass /jmx-console http://UCMDB_server/jmx-console
ProxyPassReverse /jmx-console http://UCMDB_server/jmx-console
ProxyPass /axis2 http://UCMDB_server/axis2
ProxyPassReverse /axis2 http://UCMDB_server/axis2
ProxyPass /icons http://UCMDB_server/icons
ProxyPassReverse /icons http://UCMDB_server/icons
ProxyPass /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPassReverse /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPass /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPassReverse /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPass /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPass /cm http://UCMDB_Server/cm
ProxyPassReverse /cm http://UCMDB_Server /cm
ProxyPass /cnc http://UCMDB_CM_server/cnc
ProxyPassReverse /cnc http://UCMDB_CM_server/cnc
ProxyPass /docs http://UCMDB_CM_server/docs
ProxyPassReverse /docs http://UCMDB_CM_server/docs
ProxyPass /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
ProxyPassReverse /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
```

4. 保存变更。

通过反向代理或负载平衡器使用相互身份验证连接 Data Flow Probe

若要使用相互身份验证，通过反向代理或加载平衡器连接 Data Flow Probe，请执行以下过程。此过程适用于以下配置：

- 以探测器提供的客户端证书为基础、且反向代理或负载平衡器所需的、探测器与反向代理或加载平衡器之间的相互 SSL 身份验证。
- 反向代理或负载平衡器与 UCMDB 服务器之间的常规 SSL 连接。

备注：以下说明使用 **cKeyStoreFile** 密钥库作为探测器密钥库。这是一个预定义的客户端密钥库，它是 Data Flow Probe 安装的一部分，包含自签名证书。有关详细信息，请参阅服务器和 Data Flow Probe 默认密钥库和信任库 (第 79 页)。

建议您创建一个新的唯一密钥库，其中包含新生成的私钥。有关详细信息，请参阅创建 Data Flow Probe 的密钥库 (第 78 页)。

从证书颁发机构获得证书

获得 CA 根证书，并将其导入以下位置：

- Data Flow Probe 信任库
- Data Flow Probe JVM cacerts
- UCMDB 服务器信任库
- 反向代理信任库

1. 将 CA 根证书导入 Data Flow Probe 信任库。
   a. 将 CA 根证书放到以下目录：<Data Flow Probe 安装目录>\conf\security\<证书文件名>。
   b. 通过运行以下脚本，将 CA 根证书导入 Data Flow 信任库：

      ```
      <Data Flow Probe 安装目录>\bin\jre\bin\keytool.exe -import -trustcacerts
      -alias <您的别名> -file C:\hp\UCMDB\DataFlowProbe\conf\security\<证书文件
      名> -keystore <Data Flow Probe 安装目录>\conf\security\hpprobeTrustStore.
      jks
      ```

      默认密码为：**logomania**。
2. 通过运行以下脚本，将 CA 根证书导入 Data Flow Probe JVM cacerts：

   ```
   <Data Flow Probe 安装目录>\bin\jre\bin\keytool.exe -import -trustcacerts -al
   ias <YourAlias> -file <Data Flow Probe 安装目录>\conf\security\<证书文件名> -
   keystore <Data Flow Probe 安装目录>\bin\jre\lib\security\cacerts
   ```

   默认密码为：**changeit**。
3. 将 CA 根证书导入 UCMDB 信任库。
   a. 将 CA 根证书放到以下目录：<UCMDB 安装目录>\conf\security\<证书文件名>。
   b. 通过运行以下脚本，将 CA 根证书导入 UCMDB 信任库：

```
<UCMDB 安装目录>\bin\jre\bin\keytool.exe -import -trustcacerts -alias <Yo
urAlias> -file <UCMDB 安装目录>\conf\security\<证书文件名> -keystore <UCM
DB 安装目录>\conf\security\sever.truststore
```

默认密码为：**hppass**。

4. 将 CA 根证书导入反向代理信任库。此步骤取决各供应商。

将证书转换为 Java 密钥库

通过运行以下脚本，从证书颁发机构中获得 PFX/PKCS12 格式的 Data Flow Probe 客户端证书 (和私钥)，并将其转换为 Java 密钥库：

```
<Data Flow Probe 安装目录>\bin\jre\bin\keytool.exe -importkeystore -srckeystore
<PFX 密钥库的完整路径> -destkeystore <新目标密钥库的完整路径> -srcstoretype PKCS
12
```

系统将提示您输入源密钥库和目标密钥库的密码。

对于源密钥库密码，请使用导出 PFX 密钥库时使用的相同密码。

Data Flow Probe 密钥库的默认目标密钥库密码为：**logomania**。

备注：如果输入的目标密钥库密码与默认的 Data Flow Probe 密钥库密码 (logomania) 不同，则需要在 **<Data Flow Probe 安装目录>\conf\ssl.properties** 文件 (javax.net.ssl.keyStorePassword) 中以加密形式提供新的密码。有关详细信息，请参阅加密探测器密钥库和信任库密码 (第 78 页)。

将新密码放到以下目录中：**<Data Flow Probe 安装目录>\conf\security**。

警告：请勿覆盖 **hpprobeKeyStore.jks** 文件。

更改 SSL 属性文件，使用新创建的密钥库

将包含 **<Data Flow Probe 安装目录>\conf\ssl.properties** 文件中客户端证书的密钥库设置为 **javax.net.ssl.keyStore**。

如果密钥库的密码不是默认的 Data Flow Probe 密钥库密码 (logomania)，请对 **javax.net.ssl.keyStorePassword** 进行加密后，对其进行更新。有关对密码进行加密的详细信息，请参阅加密探测器密钥库和信任库密码 (第 78 页)。

查看 Data Flow Probe 配置

请按照以下方式编辑 **<Data Flow Probe 安装目录>\conf\DataFlowProbe.properties** 文件：

```
appilog.agent.probe.protocol = HTTPS

serverName = <反向代理服务器地址>

serverPortHttps = <反向代理侦听的、以便将请求重定向至 UCMDB 的 HTTPS 端口>
```

将 UCMDB 配置为使用 SSL

有关详细信息，请参阅启用安全套接字层 (SSL) 通信 (第 16 页)。

如果 UCMDB 服务器证书是由此过程中创建其他证书的相同 CA 创建的，则反向代理或负载平衡器将信任 UCMDB 证书。

通过反向代理配置 UCMDB 的 CAC 支持

本节描述了如何使用反向代理在 UCMDB 上配置通用访问卡 (CAC) 支持。

1. 通过启动 Web 浏览器并输入以下服务器地址打开 JMX 控制台：http://<UCMDB 服务器主机名或 IP>:8080/jmx-console。

   您可能需要使用用户名和密码登录。

2. 在 UCMDB 下，单击 **UCMDB:service=Ports Management Services** 打开“Operations”页面。

   - (可选) 单击 **ComponentsConfigurations**。执行以下操作：
     - 将 **HTTPSetPort** 设置为 **8080**，然后单击“Invoke”。
     - 单击“Back to MBean”。
   - 单击 **mapComponentToConnectors**。执行以下操作：
     - 在 mapComponentToConnectors 服务中，将 **componentName** 设置为 **ucmdb-ui**。
     - 仅将 **isHTTP** 设置为 **true**，然后单击“Invoke”。
     - 单击“Back to MBean”。
     - 在 mapComponentToConnectors 服务中，将 **componentName** 设置为 **root**。
     - 仅将 **isHTTP** 设置为 **true**，然后单击“Invoke”。

3. 在 UCMDB 下，单击 **UCMDB:service=Security Services** 打开“Operations”页面。

   - 将 **loginWithCAC** 设置为 **true**，然后单击“Invoke”。
   - 单击“Back to MBean”。
   - 将 **withReverseProxy** 设置为 **true**，然后单击“Invoke”。

     此设置告知 UCMDB 服务器从 UCMDB_SSL_CLIENT_CERT 标头提取要在 UCMDB 中使用的用户名和用于身份验证的证书。
   - 单击“Back to MBean”。

- (可选)将 **onlyCACCerts** 设置为 **true**，然后单击“Invoke”。

  将此操作设置为 **true** 可仅接受来自物理 CAC 设备的证书。

4. 重新启动 UCMDB 服务器。

示例：Apache 2.4.4 配置

本节描述了 Apache 2.4.4 的示例配置文件 (在 **<Apache 计算机根目录>\Webserver\conf\httpd.conf** 文件中)：

```
LoadModule headers_module modules/mod_headers.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_html_module modules/mod_proxy_html.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule ssl_module modules/mod_ssl.so
ServerName Apache_Server_Name:80
Include conf/extra/httpd-ssl.conf
```

本节描述了使用 SSL 的 Apache 2.4.4 的示例配置文件 (在 **<Apache 计算机根目录>\Webserver\conf\extra\httpd-ssl.conf** 文件中)：

```
Listen 8443<VirtualHost _default_:8443>
ServerName Apache_Server_Name:8443
SSLCACertificateFile "c:/Apache24/conf/ssl.crt"
SSLCARevocationFile "c:/Apache24/conf/ssl.crl"
#SSLCARevocationCheck chain|leaf|none
SSLCARevocationCheck leaf
RequestHeader set UCMDB_SSL_CLIENT_CERT %{SSL_CLIENT_CERT}e


ProxyRequests off
<Proxy *>
     Order deny,allow
     Deny from all
     Allow from all
</Proxy>

ProxyPass /mam http://UCMDB_server/mam
ProxyPassReverse /mam http://UCMDB_server/mam
ProxyPass /mam_images http://UCMDB_server/mam_images
ProxyPassReverse /mam_images http://UCMDB_server/mam_images
ProxyPass /mam-collectors http://UCMDB_server/mam-collectors
ProxyPassReverse /mam-collectors http://UCMDB_server/mam-collectors
ProxyPass /ucmdb http://UCMDB_server/ucmdb
ProxyPassReverse /ucmdb http://UCMDB_server/ucmdb
ProxyPass /site http://UCMDB_server/site
ProxyPassReverse /site http://UCMDB_server/site
ProxyPass /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPassReverse /ucmdb-ui http://UCMDB_server/ucmdb-ui
ProxyPass /status http://UCMDB_server/status
```

```
ProxyPassReverse /status http://UCMDB_server/status
ProxyPass /jmx-console http://UCMDB_server/jmx-console
ProxyPassReverse /jmx-console http://UCMDB_server/jmx-console
ProxyPass /axis2 http://UCMDB_server/axis2
ProxyPassReverse /axis2 http://UCMDB_server/axis2
ProxyPass /icons http://UCMDB_server/icons
ProxyPassReverse /icons http://UCMDB_server/icons
ProxyPass /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPassReverse /ucmdb-api http://UCMDB_server/ucmdb-api
ProxyPass /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPassReverse /ucmdb-docs http://UCMDB_server/ucmdb-docs
ProxyPass /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPassReverse /ucmdb-api/8.0 http://UCMDB_server/ucmdb-api/8.0
ProxyPass /cm http://UCMDB_Server/cm
ProxyPassReverse /cm http://UCMDB_Server /cm
ProxyPass /cnc http://UCMDB_CM_server/cnc
ProxyPassReverse /cnc http://UCMDB_CM_server/cnc
ProxyPass /docs http://UCMDB_CM_server/docs
ProxyPassReverse /docs http://UCMDB_CM_server/docs
ProxyPass /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
ProxyPassReverse /ucmdb-browser http://UCMDB_CM_server/ucmdb-browser
SSLVerifyClient require
SSLVerifyDepth  10
SSLOptions+ExportCertData
```

第 4 章：数据流凭据管理

本章包括：

数据流凭据管理概述

要执行搜寻或运行集成，必须设置凭据才能访问远程系统。凭据在“Data Flow Probe 设置”窗口中配置，并保存在 UCMDB 服务器中。有关详细信息，请参阅《HP Universal CMDB 数据流管理指南》中有关描述 Data Flow Probe 设置的章节。

凭据存储由机密管理器组件进行管理。有关详细信息，请参阅机密管理器 (第 96 页)。

Data Flow Probe 可以使用机密管理器客户端访问凭据。机密管理器客户端位于 Data Flow Probe 上，并与 UCMDB 服务器上的机密管理器服务器通信。机密管理器客户端和机密管理器服务器之间的通信已加密，因此机密管理器客户端连接到机密管理器服务器时需要进行身份验证。

机密管理器服务器上的机密管理器客户端身份验证基于 LW-SSO 组件。在连接到机密管理器服务器之前，机密管理器客户端首先发送 LW-SSO cookie。然后由机密管理器服务器验证 cookie，在成功验证后开始与机密管理器客户端进行通信。有关 LW-SSO 的详细信息，请参阅配置 LW-SSO 设置 (第 50 页)。

机密管理器客户端和机密管理器服务器之间的通信已加密。有关更新加密配置的详细信息，请参阅配置机密管理器通信加密 (第 50 页)。

警告：机密管理器身份验证使用计算机中定义的通用协调时间(UTC)。为了成功进行身份验证，请确保 Data Flow probe 和 UCMDB 服务器的通用协调时间一致。由于 UTC 与时区或者夏令时无关，因此服务器和探测器可以位于不同的时区。

机密管理器客户端维护凭据的本地缓存。可以将机密管理器客户端配置为从机密管理器服务器下载所有凭据，并将这些凭据存储在缓存中。然后从机密管理器服务器不断地自动同步凭据变更。缓存可以是文件系统缓存，也可以是内存中缓存，具体取决于预配置设置。此外，缓存已加密，因此无法从外部进行访问。有关更新缓存设置的详细信息，请参阅在探测器上配置机密管理器客户端的缓存模式 (第 54 页)。有关更新缓存加密的详细信息，请参阅在探测器上配置机密管理器客户端的缓存加密设置 (第 55 页)。

有关疑难解答的详细信息，请参阅更改机密管理器客户端日志文件消息级别 (第 57 页)。

可以将凭据信息从一个 UCMDB 服务器复制到另一个服务器。有关详细信息，请参阅以加密格式导出和导入凭据和范围信息 (第 56 页)。

备注：用于探测器 (在 UCMDB 版本 9.01 或更早版本中) 上凭据存储的 **DomainScopeDocument** (DSD) 不再包含任何凭据敏感信息。该文件现在不仅包含探测器的列表和网络范围信息，还包含每个域的凭据条目列表，其中每个条目只包括凭据 ID 和为此凭据条目定义的网络范围。

本节包括以下主题：

基本安全假设

请注意以下安全假设：

确保 UCMDB 服务器和探测器 JMX 控制台的安全，以便仅启用 UCMDB 系统管理员的访问权 (最好通过 localhost 访问权)。

在单独模式下运行的 Data Flow Probe

Probe Gateway 和 Probe Manager 作为单独的进程运行时，机密管理器客户端组件将成为管理器进程的一部分。缓存后的凭据信息只能供 Probe Manager 使用。要访问 UCMDB 系统上的机密管理器服务器，将由网关进程来处理机密管理器客户端请求，并在此处将请求转发到 UCMDB 系统。

在单独模式下配置探测器时，将自动进行此配置。

保持凭据缓存为最新

在第一次成功连接到机密管理器服务器后，机密管理器客户端将下载所有相关凭据 (在探测器域中配置的所有凭据)。第一次成功通信后，机密管理器客户端将持续与机密管理器服务器进行同步。每隔一分钟执行一次差异同步，在此过程中只同步机密管理器服务器和机密管理器客户端之间的差异。如果在 UCMDB 服务器端上更改了凭据 (如添加了新凭据，或者更新或删除了现有凭据)，则机密管理器客户端将立即收到来自 UCMDB 服务器的通知，并执行其他同步。

将所有探测器与配置变更同步

为了成功进行通信，必须更新机密管理器客户端，包括机密管理器服务器身份验证配置 (LW-SSO init 字符串) 和加密配置 (机密管理器通信加密)。例如，在服务器上更改 init 字符串时，探测器必须知道新的 init 字符串，以便进行身份验证。

UCMDB 服务器将持续监控机密管理器通信加密配置和机密管理器身份验证配置中的变更。每 15 秒进行一次监控；如果发生了变更，则会将更新的配置发送到探测器。该配置将以加密形式传递到探测器，并存储在探测器端的安全存储中。待发送的配置使用对称加密密钥进行加密。默认情况下，将使用相同的默认对称加密密钥安装 UCMDB 服务器和 Data Flow Probe。为了获得最佳安全性，强烈建议在将凭据添加到系统之前更改此密钥。有关详细信息，请参阅生成或更新加密密钥 (第 58 页)。

备注：由于存在 15 秒的监控间隔，因此可能不会用 15 秒内的最新配置来更新探测器端上的机密管理器客户端。

如果选择禁用 UCMDB 服务器和 Data Flow Probe 之间的机密管理器通信和身份验证配置的自动同步，则每次在 UCMDB 服务器端上更新机密管理器通信和身份验证配置时，还应同时用新配置更新所有探测器。有关详细信息，请参阅禁用服务器与探测器之间的机密管理器客户端身份验证和加密设置的自动同步 (第 52 页)。

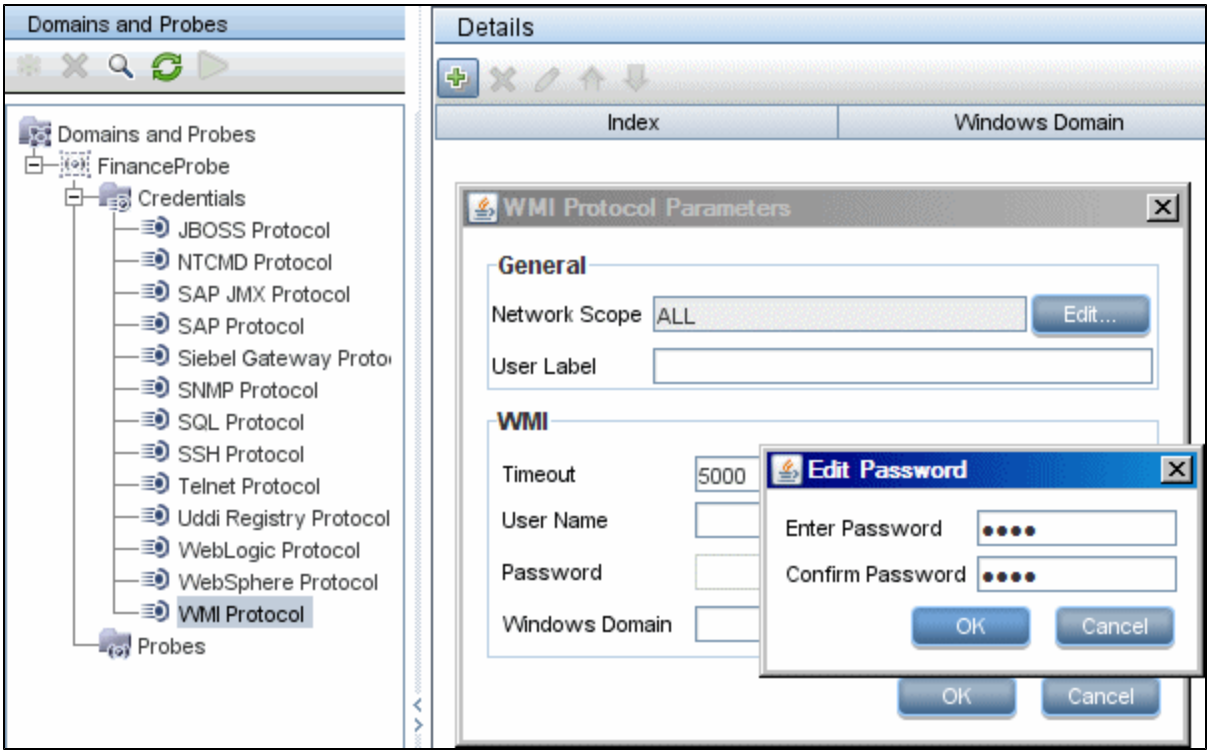
探测器上的安全存储

所有敏感信息 (例如机密管理器通信、身份验证配置和加密密钥) 存储在探测器上的安全存储的 **secured_storage.bin** 文件中，该文件位于 **C:\hp\UCMDB\DataFlowProbe\conf\security**。此安全存储使用在加密过程中依赖 Windows 用户密码的 DPAPI 进行加密。DPAPI 是一种在 Windows 系统上用于保护机密数据 (例如证书和私钥) 的标准方法。探测器应始终以相同的 Windows 用户身份运行，这样即使更改密码，探测器仍可以读取存储在安全存储中的信息。

查看凭据信息

备注：本节描述数据方向为 CMDB 至 HP Universal CMDB 时如何查看凭据信息。

系统不会将密码从 CMDB 发送到应用程序。即不管实际内容如何，HP Universal CMDB 都会在密码字段中显示星号 (*)：



更新凭据

备注：本节描述数据方向为 HP Universal CMDB 至 CMDB 时如何更新凭据。

- 此方向的通信未加密，因此应使用 https\SSL 连接到 UCMDB 服务器，或确保通过受信任网络进行连接。

  尽管通信未加密，但在网络上不会以明文形式发送密码。对密码加密时使用的是默认密钥，因此强烈建议使用 SSL 确保传送过程中的有效保密性。

- 可以使用特殊字符和非英文字符作为密码。

配置机密管理器客户端身份验证和加密设置

此任务描述如何在 UCMDB 服务器上配置机密管理器的身份验证和加密设置，并详细阐述以下步骤：

- 配置 LW-SSO 设置 (第 50 页)
- 配置机密管理器通信加密 (第 50 页)

配置 LW-SSO 设置

此步骤描述如何在 UCMDB 服务器上更改 LW-SSO init 字符串。除非 UCMDB 服务器配置为非自动方式，否则此变更将自动发送到探测器 (以加密字符串的形式)。有关详细信息，请参阅禁用服务器与探测器之间的机密管理器客户端身份验证和加密设置的自动同步 (第 52 页)。

1. 在 UCMDB 服务器上，启动 Web 浏览器，并输入以下地址：**http://localhost:8080/jmx-console**。
2. 单击 **UCMDB-UI:name=LW-SSO Configuration**，打开 JMX MBEAN 视图页面。
3. 找到 **setInitString** 方法。
4. 输入新的 LW-SSO init 字符串。
5. 单击“Invoke”。

配置机密管理器通信加密

此步骤描述如何在 UCMDB 服务器上更改机密管理器通信加密设置。这些设置指定如何对机密管理器客户端和机密管理器服务器之间的通信进行加密。除非 UCMDB 服务器配置为非自动方式，否则此变更将自动发送到探测器 (以加密字符串的形式)。有关详细信息，请参阅禁用服务器与探测器之间的机密管理器客户端身份验证和加密设置的自动同步 (第 52 页)。

1. 在 UCMDB 服务器上，启动 Web 浏览器，并输入以下地址：**http://localhost:8080/jmx-console**。
2. 单击 **UCMDB:service=Security Services**，打开 JMX MBEAN 视图页面。
3. 单击 **CMGetConfiguration** 方法。
4. 单击“Invoke”。

   此时将显示当前机密管理器配置的 XML。
5. 复制显示的 XML 的内容。
6. 返回到“Security Services”JMX MBean 视图页面。
7. 单击 **CMSetConfiguration** 方法。
8. 将复制的 XML 粘贴到“Value”字段中。
9. 更新与传输有关的相关设置并单击“Invoke”。

   示例：

```
<transport>
      <encryptTransportMode>true</encryptTransportMode>
      <CMEncryptionDecryption>
            <encryptDecryptInitString>radiohead</encryptDecryptInitStrin
            g>
            <cryptoSource>lw</cryptoSource>
            <lwJCEPBECompatibilityMode>true</lwJCEPBECompatibilityMode>
            <cipherType>symmetricBlockCipher</cipherType>
            <engineName>AES</engineName>
            <algorithmModeName>CBC</algorithmModeName>
            <algorithmPaddingName>PKCS7Padding</algorithmPaddingName>
            <keySize>256</keySize>
            <pbeCount>20</pbeCount>
            <pbeDigestAlgorithm>SHA1</pbeDigestAlgorithm>
            <encodingMode>Base64Url</encodingMode>
            <useMacWithCrypto>false</useMacWithCrypto>
            <macType>hmac</macType>
```

```
            <macKeySize>256</macKeySize>
            <macHashName>SHA256</macHashName>
      </CMEncryptionDecryption>
</transport>
```

有关可以更新的值的详细信息，请参阅机密管理器加密设置 (第 62 页)。

在探测器上手动配置机密管理器客户端身份验证和加密设置

此任务包括以下步骤：

- 禁用服务器与探测器之间的机密管理器客户端身份验证和加密设置的自动同步 (第 52 页)
- 在探测器上配置机密管理器客户端身份验证和加密设置 (第 53 页)
- 在探测器上配置机密管理器通信加密 (第 53 页)

禁用服务器与探测器之间的机密管理器客户端身份验证和加密设置的自动同步

默认情况下，UCMDB 服务器配置为向所有探测器自动发送机密管理器/LW-SSO 设置。此信息将作为加密字符串发送到探测器，由探测器在检索后解密信息。可以将 UCMDB 服务器配置为不向所有探测器自动发送机密管理器/LW-SSO 配置文件。在这种情况下，您有责任使用新的机密管理器/LW-SSO 设置手动更新所有探测器。

要禁用机密管理器/LW-SSO 设置的自动同步，请执行以下操作：

1. 在 UCMDB 中，单击“管理”>“基础结构设置管理器”>“常规设置”。
2. 选择“对探测器启用 CM/LW-SSO 配置和 init 字符串的自动同步”。
3. 单击“值”字段，并将 **True** 更改为 **False**。
4. 单击“保存”按钮。
5. 重新启动 UCMDB 服务器。

在探测器上配置机密管理器客户端身份验证和加密设置

只有当 UCMDB 服务器已配置为不会向探测器自动发送 LW-SSO/机密管理器配置和设置时，此步骤才适用。有关详细信息，请参阅禁用服务器与探测器之间的机密管理器客户端身份验证和加密设置的自动同步 (第 52 页)。

1. 在探测器计算机上启动 Web 浏览器，并输入以下地址：**http://localhost:1977**。

   备注：如果 Probe Manager 和 Probe Gateway 作为单独的进程运行，则应当在运行 Probe Manager 的计算机上输入地址，如下所示：**http://localhost:1978**。

2. 单击 **type=CMClient**，打开 JMX MBEAN 视图页面。

3. 找到 **setLWSSOInitString** 方法，并提供为 UCMDB 的 LW-SSO 配置提供的相同 init 字符串。

4. 单击 **setLWSSOInitString** 按钮。

在探测器上配置机密管理器通信加密

只有当 UCMDB 服务器已配置为不会向探测器自动发送 LW-SSO/机密管理器配置和设置时，此步骤才适用。有关详细信息，请参阅禁用服务器与探测器之间的机密管理器客户端身份验证和加密设置的自动同步 (第 52 页)。

1. 在探测器计算机上启动 Web 浏览器，并输入以下地址：**http://localhost:1977**。

   备注：如果 Probe Manager 和 Probe Gateway 作为单独的进程运行，则应当在运行 Probe Manager 的计算机上输入地址，如下所示：**http://localhost:1978**。

2. 单击 **type=CMClient**，打开 JMX MBEAN 视图页面。

3. 更新以下与传输相关的设置：

   备注：必须更新在 UCMDB 服务器上更新的相同设置。要执行此操作，在探测器上更新的某些方法可能需要多个参数。要查看当前探测器配置，请在 JMX MBEAN 视图页面中单击 **displayTransportConfiguration**。有关详细信息，请参阅配置机密管理器通信加密 (第 50 页)。有关可以更新的值的详细信息，请参阅机密管理器加密设置 (第 62 页)。

   a. “setTransportInitString”将更改“encryptDecryptInitString”设置。

   b. “setTransportEncryptionAlgorithm”将根据以下映射更改探测器上的机密管理器设

置：

- **Engine name (引擎名称)** 指的是 <engineName> 条目
- **Key size (密钥大小)** 指的是 <keySize> 条目
- **Algorithm padding name (算法填充名称)** 指的是 <algorithmPaddingName> 条目
- **PBE count (PBE 计数)** 指的是 <pbeCount> 条目
- **PBE digest algorithm (PBE 摘要算法)** 指的是 <pbeDigestAlgorithm> 条目

c. “setTransportEncryptionLibrary”将根据以下映射更改探测器上的机密管理器设置：

- **Encryption Library name (加密库名称)** 指的是 <cryptoSource> 条目
- **Support previous lightweight cryptography versions (支持以前的轻型加密版本)** 指的是 <lwJCEPBECompatibilityMode> 条目

d. “setTransportEncryptionAlgorithm”将根据以下映射更改探测器上的机密管理器设置：

- **Use MAC with cryptography (使用 MAC 加密)** 指的是 <useMacWithCrypto> 条目
- **MAC key size (MAC 密钥大小)** 指的是 <macKeySize> 条目

4. 单击 **reloadTransportConfiguration** 按钮，使这些变更在探测器上生效。

有关不同设置及其可能值的详细信息，请参阅机密管理器加密设置 (第 62 页)。

配置机密管理器客户端缓存

此任务包括以下步骤：

- 在探测器上配置机密管理器客户端的缓存模式 (第 54 页)
- 在探测器上配置机密管理器客户端的缓存加密设置 (第 55 页)

在探测器上配置机密管理器客户端的缓存模式

机密管理器客户端将凭据信息存储在缓存中，当服务器上的信息发生更改时便对其进行更新。缓存可以存储在文件系统上或内存中：

- **存储在文件系统上时**，即使探测器在重新启动后无法连接到服务器，凭据信息仍可用。
- **存储在内存中时**，如果重新启动探测器，则将清除缓存，并从服务器再次检索所有信息。如果服务器不可用，探测器将不包含任何凭据，因此无法运行搜寻或集成。

要更改此设置，请执行以下操作：

1. 在文本编辑器中打开 **DataFlowProbe.properties** 文件。此文件位于 **c:\hp\UCMDB\DataFlowProbe\conf** 文件夹中。
2. 查找以下属性：**com.hp.ucmdb.discovery.common.security.storeCMData=true**
   - 要将信息存储在文件系统上，请保留默认值 (**true**)。
   - 要将信息存储在内存中，请输入 **false**。
3. 保存 **DataFlowProbe.properties** 文件。
4. 重新启动探测器。

在探测器上配置机密管理器客户端的缓存加密设置

此步骤描述如何更改机密管理器客户端的文件系统缓存文件的加密设置。请注意，更改机密管理器客户端的文件系统缓存的加密设置会重新创建文件系统缓存文件。此重新创建过程需要重新启动探测器并与 UCMDB 服务器完全同步。

1. 在探测器计算机上启动 Web 浏览器，并输入以下地址：**http://localhost:1977**。

   备注：如果 Probe Manager 和 Probe Gateway 作为单独的进程运行，则应当在运行 Probe Manager 的计算机上输入地址，如下所示：**http://localhost:1978**。

2. 单击 **type=CMClient**，打开 JMX MBEAN 视图页面。
3. 更新以下与缓存相关的设置：

   备注：在探测器上更新的某些方法可能需要多个参数。要查看当前探测器配置，请在 JMX MBEAN 视图页面中单击 **displayCacheConfiguration**。

   a. “setCacheInitString”将更改文件系统缓存 <encryptDecryptInitString> 设置。

   b. “setCacheEncryptionAlgorithm”将根据以下映射更改文件系统缓存设置：

      - **Engine name (引擎名称)** 指的是 <engineName> 条目
      - **Key size (密钥大小)** 指的是 <keySize> 条目
      - **Algorithm padding name (算法填充名称)** 指的是 <algorithmPaddingName> 条目
      - **PBE count (PBE 计数)** 指的是 <pbeCount> 条目
      - **PBE digest algorithm (PBE 摘要算法)** 指的是 <pbeDigestAlgorithm> 条目

   c. “setCacheEncryptionLibrary”将根据以下映射更改文件系统缓存设置：

- **Encryption Library name (加密库名称)** 指的是 <cryptoSource> 条目
- **Support previous lightweight cryptography versions (支持以前的轻型加密版本)** 指的是 <lwJCEPBECompatibilityMode> 条目

d. “setCacheMacDetails”将根据以下映射更改文件系统缓存设置：

- **Use MAC with cryptography (使用 MAC 加密)** 指的是 <useMacWithCrypto> 条目
- **MAC key size (MAC 密钥大小)** 指的是 <macKeySize> 条目

4. 单击“reloadCacheConfiguration”按钮，使这些变更在探测器上生效。之后将重新启动探测器。

> **备注：**请确保在此操作期间探测器上未运行任何作业。

有关不同设置及其可能值的详细信息，请参阅机密管理器加密设置 (第 62 页)。

以加密格式导出和导入凭据和范围信息

您可以加密格式导出和导入凭据和范围信息，从而将凭据信息从一台 UCMDB 服务器复制到另一台服务器。例如，您可以在系统崩溃后的恢复期间或在升级期间执行此操作。

- **导出凭据信息时，**必须输入您选择的密码。将使用此密码对信息进行加密。
- **导入凭据信息时，**必须使用在导出 DSD 文件时定义的同一个密码。

> **备注：**导出的凭据文档还包含在从中导出文档的系统上定义的范围信息。在导入凭据文档期间，同时也会导入范围信息。

要从 UCMDB 服务器导出凭据信息，请执行以下操作：

1. 在 UCMDB 服务器上，启动 Web 浏览器，并输入以下地址：**http://localhost:8080/jmx-console**。您可能需要使用用户名和密码登录。
2. 单击 **UCMDB:service=DiscoveryManager**，打开 JMX MBEAN 视图页面。
3. 找到 **exportCredentialsAndRangesInformation** 操作。执行以下操作：
   - 输入客户 ID (默认是 1)。
   - 为导出的文件输入名称。
   - 输入密码。

- 如果要使用提供的密码对导出的文件加密，则设置 **isEncrypted=True**；如果不希望对导出的文件加密 (这种情况下将不导出密码和其他敏感信息)，则设置 **isEncrypted=False**。

4. 单击“Invoke”进行导出。

   导出过程成功完成后，文件将保存到此位置：**c:\hp\UCMDB\UCMDBServer\conf\discovery\<客户目录>**。

要从 UCMDB 服务器导入凭据信息，请执行以下操作：

1. 在 UCMDB 服务器上，启动 Web 浏览器，并输入以下地址：**http://localhost:8080/jmx-console**。

   您可能需要使用用户名和密码登录。

2. 单击 **UCMDB:service=DiscoveryManager**，打开 JMX MBEAN 视图页面。

3. 找到 **importCredentialsAndRangesInformation** 操作。

4. 输入客户 ID (默认是 1)。

5. 输入要导入的文件的名称。此文件必须位于 **c:\hp\UCMDB\UCMDBServer\conf\discovery\<客户目录>**中。

6. 输入密码。此密码必须与导出文件时使用的密码相同。

7. 单击“Invoke”，导入凭据。

更改机密管理器客户端日志文件消息级别

探测器提供两个日志文件，其中包含有关机密管理器服务器与机密管理器客户端之间的机密管理器相关通信的信息。这两个文件为：

- 机密管理器客户端日志文件 (第 57 页)
- LW-SSO 日志文件 (第 58 页)

机密管理器客户端日志文件

security.cm.log 文件位于 **c:\hp\UCMDB\DataFlowProbe\runtime\log** 文件夹中。

该日志包含在机密管理器服务器和机密管理器客户端之间交换的信息消息。默认情况下，这些消息的日志级别设置为“信息”。

要将消息的日志级别更改为“调试”级别，请执行以下操作：

1. 在 Data Flow Probe Manager 服务器上，导航到 **c:\hp\UCMDB\DataFlowProbe\conf\log**。

2. 在文本编辑器中打开 **security.properties** 文件。
3. 将行：

   ```
   loglevel.cm=INFO
   ```

   更改为

   ```
   loglevel.cm=DEBUG
   ```

4. 保存该文件。

LW-SSO 日志文件

security.lwsso.log 文件位于 **c:\hp\UCMDB\DataFlowProbe\runtime\log** 文件夹中。

该日志包含与 LW-SSO 相关的信息消息。默认情况下，这些消息的日志级别设置为“信息”。

要将消息的日志级别更改为“调试”级别，请执行以下操作：

1. 在 Data Flow Probe Manager 服务器上，导航到 **c:\hp\UCMDB\DataFlowProbe\conf\log**。
2. 在文本编辑器中打开 security.properties 文件。
3. 将行：

   ```
   loglevel.lwsso=INFO
   ```

   更改为

   ```
   loglevel.lwsso=DEBUG
   ```

4. 保存该文件。

生成或更新加密密钥

您可以生成或更新加密密钥，用于加密或解密在 UCMDB 服务器和 Data Flow Probe 之间交换的机密管理器通信和身份验证配置。在这两种情况下 (生成或更新)，UCMDB 服务器都会根据您提供的参数 (例如，密钥长度、额外 PBE 周期、JCE 提供程序) 创建新的加密密钥，并将其分发到探测器。

运行 **generateEncryptionKey** 方法将得到新生成的加密密钥。此密钥存储在安全存储中，其名称和详细信息未知。如果重新安装现有 Data Flow Probe，或将新探测器连接到 UCMDB 服务器，则新探测器将无法识别此新生成的密钥。在这种情况下，最好使用 **changeEncryptionKey** 方法更改加密密钥。这样，重新安装探测器或安装新探测器时，可以通过在探测器 JMX 控制台上运行 **importEncryptionKey** 方法来导入名称和位置已知的现有密钥。

备注：

- 用于创建密钥(**generateEncryptionKey**)和升级密钥(**changeEncryptionKey**)的方法的不同之处在于 **generateEncryptionKey** 创建新的随机加密密钥，而 **changeEncryptionKey** 则导入您为其提供名称的加密密钥。
- 无论安装了多少个探测器，一个系统上只能存在一个加密密钥。

此任务包括以下步骤：

- 生成新加密密钥 (第 59 页)
- 在 UCMDB 服务器上更新加密密钥 (第 60 页)
- 在探测器上更新加密密钥 (第 61 页)
- 当 Probe Manager 和 Probe Gateway 安装在不同计算机上时手动更改加密密钥 (第 62 页)
- 定义多个 JCE 提供程序 (第 62 页)

生成新加密密钥

您可以生成一个新密钥，供 UCMDB 服务器和 Data Flow Probe 用于加密或解密。UCMDB 服务器将用新生成的密钥替换旧密钥，并在探测器之间分发此密钥。

要通过 JMX 控制台生成新加密密钥，请执行以下操作：

1. 在 UCMDB 服务器上，启动 Web 浏览器，并输入以下地址：**http://localhost:8080/jmx-console**。

   您可能需要使用用户名和密码登录。

2. 单击 **UCMDB:service=DiscoveryManager**，打开 JMX MBEAN 视图页面。

3. 找到“generateEncryptionKey”操作。

   a. 在 **customerId** 参数框中，输入“1” (默认值)。

   b. 对于 **keySize**，指定加密密钥的长度。有效值为 128、192 或 256。

   c. 对于 **usePBE**，指定 **True** 或 **False**：

      - **True**：使用其他 PBE 哈希周期。
      - **False**：不使用其他 PBE 哈希周期。

   d. 对于 **jceVendor**，可以选择使用非默认的 JCE 提供程序。如果该框为空，则使用默认提供程序。

e. 对于 **autoUpdateProbe**，指定 **True**或 **False**：

- **True**：服务器会自动将新密钥分发到探测器。
- **False**：应手动将新密钥置于探测器上。

f. 对于 **exportEncryptionKey**，指定 **True** 或 **False**。

- **True**：除了创建新密码并将其存储在安全存储中以外，服务器还会将新密码导出到文件系统 (**c:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**)。通过此选项，您可以用新密码手动更新探测器。
- **False**：新密码未导出到文件系统。要手动更新探测器，请将 **autoUpdateProbe** 设置为“False”，将 **exportEncryptionKey** 设置为“True”。

> **备注**：请确保探测器已启动并连接到服务器。如果探测器已关闭，则密钥将无法到达探测器。如果在探测器关闭之前更改密钥，则在探测器再次启动后，密钥将重新发送到探测器。但是，如果在探测器关闭之前多次更改了密钥，则必须通过 JMX 控制台手动更改密钥。 (对于 **exportEncryptionKey**，选择 **False**)。

4. 单击“Invoke”，生成加密密钥。

在 UCMDB 服务器上更新加密密钥

使用 **changeEncryptionKey** 方法将自己的加密密钥导入到 UCMDB 服务器，并在所有探测器之间分发该密钥。

要通过 JMX 控制台更新加密密钥，请执行以下操作：

1. 在 UCMDB 服务器上，启动 Web 浏览器，并输入以下地址：**http://localhost:8080/jmx-console**。

   您可能需要使用用户名和密码登录。

2. 单击 **UCMDB:service=DiscoveryManager**，打开 JMX MBEAN 视图页面。

3. 找到 **changeEncryptionKey** 操作。

   a. 在 **customerId** 参数框中，输入 **1** (默认值)。

   b. 对于 **newKeyFileName**，输入新密钥的名称。

   c. 对于 **keySizeInBits**，指定加密密钥的长度。有效值为 128、192 或 256。

   d. 对于 **usePBE**，指定 **True** 或 **False**：

- **True**：使用其他 PBE 哈希周期。
- **False**：不使用其他 PBE 哈希周期。

e. 对于 **jceVendor**，可以选择使用非默认的 JCE 提供程序。如果该框为空，则使用默认提供程序。

f. 对于 **autoUpdateProbe**，指定 **True**或 **False**：

- **True**：服务器会自动将新密钥分发到探测器。
- **False**：应使用探测器 JMX 控制台手动分发新密钥。

> **备注**：请确保探测器已启动并连接到服务器。如果探测器已关闭，则密钥将无法到达探测器。如果在探测器关闭之前更改密钥，则在探测器再次启动后，密钥将重新发送到探测器。但是，如果在探测器关闭之前多次更改了密钥，则必须通过 JMX 控制台手动更改密钥。 (对于 **autoUpdateProbe**，选择 **False**)。

4. 单击“Invoke”，生成和更新加密密钥。

在探测器上更新加密密钥

如果出于安全性考虑，选择不将加密密钥从 UCMDB 服务器自动分发到所有探测器，则应将新加密密钥下载到所有探测器中，并在探测器上运行 **importEncryptionKey** 方法：

1. 将加密密钥文件置于 **C:\hp\UCMDB\DataFlowProbe\conf\security**。
2. 在探测器计算机上启动 Web 浏览器，并输入以下地址：**http://localhost:1977**。

   您可能需要使用用户名和密码登录。

   > **备注**：如果 Probe Manager 和 Probe Gateway 作为单独的进程运行，则应当在运行 Probe Manager 的计算机上输入地址，如下所示：**http://localhost:1978**。

3. 在“探测器”域内，单击 **type=SecurityManagerService**。
4. 找到 **importEncryptionKey** 方法。
5. 输入位于 **C:\hp\UCMDB\DataFlowProbe\conf\security** 中的加密密钥文件的名称。此文件包含要导入的密钥。
6. 单击 **importEncryptionKey** 按钮。
7. 重新启动探测器。

当 Probe Manager 和 Probe Gateway 安装在不同计算机上时手动更改加密密钥

1. 在 Probe Manager 计算机上，启动 Probe Manager 服务 (“开始”>“程序”>“HP UCMDB”>“Probe Manager”)。
2. 使用 Probe Manager JMX 从服务器导入密钥。有关详细信息，请参阅生成新加密密钥 (第 59 页)。
3. 在加密密钥导入成功之后，重新启动 Probe Manager 和 Probe Gateway 服务。

定义多个 JCE 提供程序

通过 JMX 控制台生成加密密钥时，可以使用 **changeEncryptionKey** 和 **generateEncryptionKey** 方法定义多个 JCE 提供程序。

要更改默认 JCE 提供程序，请执行以下操作：

1. 注册 **$JRE_HOME/lib/ext** 中的 JCE 提供程序 jar 文件。
2. 将 jar 文件复制到 $JRE_HOME 文件夹：
   - 对于 UCMDB 服务器：$JRE_HOME 位于：**c:\hp\UCMDB\UCMDBServer\bin\jre**
   - 对于 Data Flow Probe：$JRE_HOME 位于：**c:\hp\UCMDB\DataFlowProbe\bin\jre**
3. 在 **$JRE_HOME\lib\security\java.security** 文件的提供程序列表末尾添加提供程序类。
4. 更新 **local_policy.jar** 和 **US_export_policy.jar** 文件以包括无限制 JCE 策略。可以从 Sun 网站下载这些 jar 文件。
5. 重新启动 UCMDB 服务器和 Data Flow Probe。
6. 针对 **changeEncryptionKey** 或 **generateEncryptionKey** 方法查找 JCE 提供程序字段，并添加 JCE 提供程序的名称。

机密管理器加密设置

下表列出可以使用各种 JMX 方法进行更改的加密设置。这些加密设置适用于机密管理器客户端和机密管理器服务器之间的通信加密，也适用于机密管理器客户端缓存的加密。

机密管理器设置名称	探测器机密管理器设置名称	设置描述	可能值	默认值
cryptoSource	加密库名称	此设置定义要使用的加密库。	lw、jce、windowsDPAPI、lwJCECompatible	lw
lwJCEPBE 兼容性模式	支持以前的轻型加密版本	此设置定义是否支持以前的轻型加密。	true、false	true
engineName	引擎名称	加密机制名称	AES、DES、3DES、Blowfish	AES
keySize	密钥大小	加密密钥长度(以位为单位)	AES - 128、192 或 256； DES - 64； 3DES - 192； Blowfish - 32 和 448 之间的任何数字	256
算法填充名称	算法填充名称	填充标准	PKCS7Padding、PKCS5Padding	PKCS7Padding
pbeCount	PBE 计数	运行哈希操作以根据密码(init 字符串)创建密钥的次数	任何正数	20
pbeDigest 算法	PBE 摘要算法	哈希类型	SHA1、SHA256、MD5	SHA1
useMacWith 加密	使用 MAC 加密	指明是否使用 MAC 加密	true、false	false
macKeySize	MAC 密钥大小	取决于 MAC 算法	256	256

疑难解答和局限性

如果在 UCMDB 服务器上更改默认域名，必须首先确认 Data Flow Probe 不处于运行状态。在应用默认域名之后，必须在 Data Flow Probe 端上执行 **DataFlowProbe\tools\clearProbeData.bat** 脚本。

备注：如果执行 clearProbeData.bat 脚本，将会在探测器启动时在探测器端上导致搜寻循环。

第 5 章：Data Flow Probe 强化

本章包括：

修改 PostgreSQL 数据库加密密码

本节介绍如何对 PostgreSQL 数据库用户的加密密码进行修改。

1. 创建加密形式的密码 (AES，192 位密钥)

   a. 访问 Data Flow Probe JMX 控制台。启动 Web 浏览器，并输入以下地址：**http://<Data Flow Probe 计算机名称或 IP 地址>:1977**。如果在本地运行 Data Flow Probe，则输入 **http://localhost:1977**。

   您可能需要使用用户名和密码登录。

   备注：如果尚未创建用户，则使用默认用户名 sysadmin 和密码 sysadmin 登录。

b. 找到 **Type=MainProbe** 服务，并单击链接打开“Operations”页面。

c. 找到 **getEncryptedDBPassword** 操作。

d. 在“DB Password”字段中，输入要加密的密码。

e. 通过单击 **getEncryptedDBPassword** 按钮调用操作。

调用的结果便是加密密码字符串，例如：

```
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61
,61
```

2. 停止 Data Flow Probe

“开始”>“所有程序”>“HP UCMDB”>“Stop Data Flow Probe”

3. 运行 set_dbuser_password.cmd 脚本

此脚本位于以下文件夹中：**C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\set_dbuser_password.cmd**

使用新密码作为第一个参数、PostgreSQL 根帐户密码作为第二个参数运行 **set_dbuser_password.cmd** 脚本。

例如：

set_dbuser_password <我的密码><根密码>。

所输入密码的格式必须为未加密形式 (纯文本)。

4. 在 Data Flow Probe 配置文件中更新密码

a. 密码必须在配置文件中加密。要检索密码的加密形式，请使用 **getEncryptedDBPassword** JMX 方法，如步骤 1 中所述。

b. 将加密密码添加到 **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** 文件中的以下属性中。

- **appilog.agent.probe.jdbc.pwd**

例如：

```
appilog.agent.probe.jdbc.user = mamprobe
appilog.agent.probe.jdbc.pwd =
66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,
61,61
```

- **appilog.agent.local.jdbc.pwd**
- **appilog.agent.normalization.jdbc.pwd**

5. 启动 Data Flow Probe

   “开始”>“所有程序”>“HP UCMDB”>“Start Data Flow Probe”

clearProbeData 脚本：用途

要在不更改当前密码的情况下重新创建数据库用户，请在 Windows 上运行 **clearProbeData.bat** 脚本，在 Linux 上运行 **clearProbeData.sh** 脚本。

运行脚本之后：

- 检查以下文件是否存在错误：**C:\hp\UCMDB\DataFlowProbe\runtime\log\probe_setup.log** (Windows)，**/opt/hp/UCMDB/DataFlowProbe/runtime/log/probe_setup.log** (Linux)。
- 删除文件，因为该文件包含数据库密码。

备注：不要运行此脚本，除非 HP 软件支持另有指示。

设置 JMX 控制台加密密码

本节介绍如何对 JMX 用户的密码进行加密。加密密码存储在 DataFlowProbe.properties 文件中。用户必须先登录才能访问 JMX 控制台。

1. **创建加密形式的密码 (AES，192 位密钥)**

   a. 访问 Data Flow Probe JMX 控制台。启动 Web 浏览器，并输入以下地址：**http://<Data Flow Probe 计算机名称或 IP 地址>:1977**。如果在本地运行 Data Flow Probe，则输入 **http://localhost:1977**。

   您可能需要使用用户名和密码登录。

   备注：如果尚未创建用户，则使用默认用户名 sysadmin 和密码 sysadmin 登录。

   b. 找到 **Type=MainProbe** 服务，并单击链接打开“Operations”页面。

   c. 找到 **getEncryptedKeyPassword** 操作。

   d. 在“Key Password”字段中，输入要加密的密码。

   e. 通过单击 **getEncryptedKeyPassword** 按钮调用操作。

调用的结果便是加密密码字符串，例如：

```
85,-9,-61,11,105,-93,-81,118
```

2. **停止 Data Flow Probe**

   “开始”>“所有程序”>“HP UCMDB”>“Stop Data Flow Probe”

3. **添加加密密码**

   将加密密码添加到 **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** 文件中的以下属性中。

   appilog.agent.Probe.JMX.BasicAuth.Pwd

   例如：

   ```
   appilog.agent.Probe.JMX.BasicAuth.User=sysadmin
   appilog.agent.Probe.JMX.BasicAuth.Pwd=12,-35,-37,82,-2,20,57,-40,38,80,-111,-99,-64,-5,35,-122
   ```

   备注：要禁用身份验证，请将这些字段留空。如果执行此操作，则用户可以打开探测器的 JMX 控制台主页，而无需输入身份验证。

4. **启动 Data Flow Probe**

   “开始”>“所有程序”>“HP UCMDB”>“Start Data Flow Probe”

   在 Web 浏览器中测试结果。

设置 UpLoadScanFile 密码

本节介绍如何为离线扫描保存设置 **UpLoadScanFile** 的密码。加密密码存储在 **DataFlowProbe.properties** 文件中。用户必须先登录才能访问 JMX 控制台。

1. **创建加密形式的密码 (AES，192 位密钥)**

   a. 访问 Data Flow Probe JMX 控制台。启动 Web 浏览器，并输入以下地址：**http://<Data Flow Probe 计算机名称或 IP 地址>:1977**。如果在本地运行 Data Flow Probe，则输入 **http://localhost:1977**。

      您可能需要使用用户名和密码登录。

      备注：如果尚未创建用户，则使用默认用户名 sysadmin 和密码 sysadmin 登录。

   b. 找到 **Type=MainProbe** 服务，并单击链接打开“Operations”页面。

c. 找到 **getEncryptedKeyPassword** 操作。

d. 在“Key Password”字段中，输入要加密的密码。

e. 通过单击 **getEncryptedKeyPassword** 按钮调用操作。

调用的结果便是加密密码字符串，例如：

```
85,-9,-61,11,105,-93,-81,118
```

2. **停止 Data Flow Probe**

“开始”>“所有程序”>“HP UCMDB”>“Stop Data Flow Probe”

3. **添加加密密码**

将加密密码添加到 **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** 文件中的以下属性中。

com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd

例如：

```
com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.User=UploadScanFile
com.hp.ucmdb.discovery.Probe.JMX.UploadAuth.Pwd=116,116,21,34,-59,77,-
108,14,127,4,-89,101,-33,-31,116,53
```

4. **启动 Data Flow Probe**

“开始”>“所有程序”>“HP UCMDB”>“Start Data Flow Probe”

在 Web 浏览器中测试结果。

远程访问 PostgreSQL 服务器

本节介绍如何允许/限制从远程计算机访问 PostgreSQL Data Flow Probe 帐户。

备注：

- 默认情况下，限制访问。
- 您无法从远程计算机访问 PostgreSQL 根帐户。

要允许 PostgreSQL 访问，请执行以下操作：

- 在命令提示符窗口中运行以下脚本：

C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\enable_remote_user_access.cmd

要限制 PostgreSQL 访问，请执行以下操作：

- 在命令提示符窗口中运行以下脚本：

  C:\hp\UCMDB\DataFlowProbe\tools\dbscripts\remove_remote_user_access.cmd

在 UCMDB 服务器和 Data Flow Probe 之间启用 SSL

可以为具有证书的 Data Flow Probe 和 UCMDB 服务器设置身份验证。在建立连接之前，将发送每个组件的证书并对其进行身份验证。

备注：在 Data Flow Probe 上启用 SSL 的以下方法是最安全方法，因而是推荐的通信模式。此方法将替换基本身份验证过程。

本节包括以下主题：

概述

UCMDB 在 UCMDB 服务器和 Data Flow Probe 之间支持以下通信模式：

- **服务器身份验证。**此模式使用 SSL，并且探测器会对 UCMDB 服务器证书进行身份验证。有关详细信息，请参阅启用使用服务器 (单向) 身份验证的 SSL (第 70 页)。
- **相互身份验证。**此模式使用 SSL，并启用探测器的服务器身份验证和服务器的客户端身份验证。有关详细信息，请参阅启用相互 (双向) 证书身份验证 (第 72 页)。
- **标准 HTTP。**无 SSL 通信。此为默认模式，并且 UCMDB 中的 Data Flow Probe 组件不需要任何证书。Data Flow Probe 通过标准 HTTP 协议与服务器通信。

备注：使用 SSL 时，搜寻无法使用证书链。因此，如果使用证书链，则应生成自签名证书，以便 Data Flow Probe 能够与 UCMDB 服务器通信。

密钥库和信任库

UCMDB 服务器和 Data Flow Probe 使用密钥库和信任库：

- **密钥库。**包含密钥条目 (证书和匹配的私钥) 的文件。
- **信任库。**包含用于验证远程主机的证书的文件 (例如，使用服务器身份验证时，Data Flow Probe 的信任库需包括 UCMDB 服务器证书)。

相互身份验证限制

Data Flow Probe 密钥库 (如 **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties** 中所定义) 只能包含 1 个密钥条目。

启用使用服务器 (单向) 身份验证的 SSL

此模式使用 SSL，并且探测器会对服务器证书进行身份验证。

此任务包括：

- 先决条件 (第 70 页)
- UCMDB 服务器配置 (第 70 页)
- Data Flow Probe 配置 (第 72 页)
- 重新启动计算机 (第 72 页)

先决条件

1. 验证 UCMDB 和 Data Flow Probe 是否正在运行。

   备注：如果在单独模式下安装探测器，则这些说明与 Probe Gateway 相关。

2. 如果 UCMDB 或 Data Flow Probe 未安装在默认文件夹中，请记录正确的位置，并相应更改命令。

UCMDB 服务器配置

1. **导出 UCMDB 证书**

   a. 打开命令提示并运行以下命令：

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias <keystore alias> -keystore <Keystore file path> -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   其中：

   - **keystore alias** 是指密钥库的给定名称。
   - **Keystore file path** 是指密钥库文件位置的完整路径。

例如，对于现成的服务器密钥库，请使用以下命令：

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert
-keystore C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file
C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
```

b. 输入密钥库密码。例如，现成的密钥库密码为 **hppass**。

c. 验证证书是否在以下目录中创建：**C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **强化 UCMDB 中的 Data Flow Probe 连接器：**

a. 访问 UCMDB JMX 控制台：在 Web 浏览器中输入以下 URL：**http://<ucmdb 计算机名称或 IP 地址>:8080/jmx-console**。您可能需要使用用户名和密码登录。

b. 选择服务：Ports Management Services。

c. 调用 **PortsDetails** 方法，并记下 HTTPS 的端口号。(默认值：8443) 确保“Is Enabled”列中的值为“True”。

d. 返回“Ports Management Services”。

e. 要将 Data Flow Probe 连接器映射到服务器身份验证模式，请使用以下参数调用 **mapComponentToConnectors** 方法：

- **componentName**：mam-collectors
- **isHTTPS**：true
- **所有其他标志**：false

将显示以下消息：

Operation succeeded.Component mam-collectors is now mapped to:HTTPS ports.

f. 返回“Ports Management Services”。

g. 要将机密管理器连接器映射到服务器身份验证模式，请使用以下参数调用 **mapComponentToConnectors** 方法：

- **componentName**：cm
- **isHTTPS**：true
- **所有其他标志**：false

将显示以下消息：

Operation succeeded.Component cm is now mapped to:HTTPS ports.

3. **将 UCMDB 证书复制到每台探测器计算机**

   将 UCMDB 服务器计算机上位于 **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert** 的证书文件复制到每台 Data Flow Probe 计算机上的以下文件夹中： **C:\HP\UCMDB\DataFlowProbe\conf\security**

Data Flow Probe 配置

备注：必须配置每台 Data Flow Probe 计算机。

1. **将在**导出 UCMDB 证书 (第 70 页)**中创建的 server.cert 文件导入到探测器的信任库中。**

   a. 打开命令提示并运行以下命令：

   ```
   C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore C:\HP\UCMDB\DataFlowProbe\conf\security\hpprobeTrustStore.jks -file C:\HP\UCMDB\DataFlowProbe\conf\security\server.cert -alias hpcert
   ```

   b. 输入密钥库密码：logomania

   c. 询问 **Trust this certificate?** 时，请按 **y**，然后按 **Enter**。

   将显示以下消息：

   Certificate was added to keystore.

2. **打开 DataFlowProbe.properties 文件，它位于：C:\HP\UCMDB\DataFlowProbe\conf**

   a. 将 **appilog.agent.probe.protocol** 属性更新为 **HTTPS**。

   b. 将 **serverPortHttps** 属性更新为相关的端口号。 (使用来自UCMDB 服务器配置 (第 70 页)的步骤 2c 中的端口号。)

重新启动计算机

重新启动 UCMDB 服务器和探测器计算机。

启用相互 (双向) 证书身份验证

此模式使用 SSL，并启用探测器的服务器身份验证和服务器的客户端身份验证。服务器和探测器都会将其证书发送到其他实体，进行身份验证。

此任务包括：

先决条件

1. 验证 UCMDB 和 Data Flow Probe 是否正在运行。

   备注：如果在单独模式下安装探测器，则这些说明与 Probe Gateway 相关。

2. 如果 UCMDB 或 Data Flow Probe 未安装在默认文件夹中，请记录正确的位置，并相应更改命令。

初始 UCMDB 服务器配置

1. **导出 UCMDB 证书**

   a. 打开命令提示并运行以下命令：

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias <keystore alias> -keystore <Keystore file path> -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   其中：

   - **keystore alias** 是指密钥库的给定名称。
   - **Keystore file path** 是指密钥库文件位置的完整路径。

   例如，对于现成的服务器密钥库，请使用以下命令：

   ```
   C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -export -alias hpcert -keystore C:\hp\ucmdb\ucmdbserver\conf\security\server.keystore -file C:\HP\UCMDB\UCMDBServer\conf\security\server.cert
   ```

   b. 输入密钥库密码。例如，现成的密钥库密码为 **hppass**。

   c. 验证证书是否在以下目录中创建：**C:\HP\UCMDB\UCMDBServer\conf\security\server.cert**

2. **强化 UCMDB 中的 Data Flow Probe 连接器：**

a. 访问 UCMDB JMX 控制台：在 Web 浏览器中输入以下 URL：**http://<ucmdb 计算机名称或 IP 地址>:8080/jmx-console**。您可能需要使用用户名和密码登录。

b. 选择服务：Ports Management Services。

c. 调用 **PortsDetails** 方法，记下使用客户端身份验证的 HTTPS 的端口号。(默认值：8444) 确保“Is Enabled”列中的值为“True”。

d. 返回“Ports Management Services”。

e. 要将 Data Flow Probe 连接器映射到相互身份验证模式，请使用以下参数调用 **mapComponentToConnectors** 方法：

- **componentName**：mam-collectors
- **isHTTPSWithClientAuth**：true
- **所有其他标志**：false

将显示以下消息：

Operation succeeded.Component mam-collectors is now mapped to:HTTPS_CLIENT_AUTH ports.

f. 返回“Ports Management Services”。

g. 要将机密管理器连接器映射到相互身份验证模式，请使用以下参数调用 **mapComponentToConnectors** 方法：

- **componentName**：cm
- **isHTTPSWithClientAuth**：true
- **所有其他标志**：false

将显示以下消息：

Operation succeeded.Component cm is now mapped to:HTTPS_CLIENT_AUTH ports.

3. **将 UCMDB 证书复制到每台探测器计算机**

将 UCMDB 服务器计算机上位于 **C:\HP\UCMDB\UCMDBServer\conf\security\server.cert** 的证书文件复制到每台 Data Flow Probe 计算机上的以下文件夹中： **C:\HP\UCMDB\DataFlowProbe\conf\security**

Data Flow Probe 配置

备注：必须配置每台 Data Flow Probe 计算机。

1. **将在**导出 UCMDB 证书 (第 73 页)**中创建的 server.cert 文件导入到探测器的信任库中。**

   a. 打开命令提示并运行以下命令：

   ```
   C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -import -v -keystore C:\HP\UCMDB\DataFlowProbe\conf\security\hpprobeTrustStore.jks -file C:\HP\UCMDB\DataFlowProbe\conf\security\server.cert -alias hpcert
   ```

   b. 输入密钥库密码：logomania

   c. 询问 **Trust this certificate?** 时，请按 **y**，然后按 **Enter**。

   将显示以下消息：

   Certificate was added to keystore.

2. **创建新的 client.keystore 文件**

   a. 打开命令提示并运行以下命令：

   ```
   c:\HP\UCMDB\DataFlowProbe\bin\jre\keytool –genkey –alias <ProbeName> -keyalg RSA –sigalg SHA256withRSA –keysize 2048 –keystore c:\HP\UCMDB\DataFlowProbe\conf\security\client.keystore
   ```

   其中，“探测器名称”是指 Data Flow Probe 的唯一别名。

   > **备注：**要确保此别名具有唯一性，请使用定义探测器时为该探测器指定的探测器名称标识符。

   b. 输入至少 6 个字符的密钥库密码，并记下该密码。

   c. 再次输入密码以确认。

   d. 回答以下每个问题之后，按 **Enter** 键：

   您的姓名是什么？[Unknown]:

   您的组织单位名称是什么？[Unknown]:

   您的组织名称是什么?[Unknown]:

   您在哪个城市或位置？[Unknown]:

   您在哪个省/自治区/直辖市?[Unknown]:

   此单位所在的国家/地区代码是多少(两个字母)?[Unknown]:

   e. 当系统询问 **Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown,**

ST=Unknown, C=Unknown correct? 时，请键入 **yes**

f. 回答以下问题之后，按 **Enter** 键：

输入<探测器密钥>的密钥密码(如果该密码与密钥库密码相同，则返回)：

g. 验证该文件在以下文件夹中是否已创建，并确保其文件大小大于 0：**C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore**

3. **导出新的客户端证书**

a. 打开命令提示并运行以下命令：

```
C:\HP\UCMDB\DataFlowProbe\bin\jre\bin\keytool.exe -export -alias <探测器名称> -keystore C:\hp\UCMDB\DataFlowProbe\conf\security\client.keystore -file C:\hp\UCMDB\DataFlowProbe\conf\security\<探测器名称>.cert
```

b. 当系统要求您输入密钥库密码时，请输入密码。(密码是在上述步骤 2b 中确定的。)

将显示以下消息：

证书存储在文件 <C:\hp\UCMDB\DataFlowProbe\conf\security\<探测器名称>.cert> 中

4. **打开 DataFlowProbe.properties 文件，它位于：C:\HP\UCMDB\DataFlowProbe\conf**

a. 将 **appilog.agent.probe.protocol** 属性更新为 **HTTPS**。

b. 将 **serverPortHttps** 属性更新为相关的端口号。(使用来自初始 UCMDB 服务器配置 (第 73 页) 的步骤 2c 中的端口号。)

5. **打开位于以下位置的 ssl.properties 文件：C:\HP\UCMDB\DataFlowProbe\conf\security**

a. 将 **javax.net.ssl.keyStore** 属性更新为 **client.keystore**。

b. 对上述步骤 2b 中输入的密码进行加密：

i. 启动 Data Flow Probe (或确保它已运行)。

ii. 访问探测器 JMX。浏览至：**http://<探测器主机名>:1977**

例如，如果探测器在本地运行，则浏览至：**http://localhost:1977**。

iii. 按“type=MainProbe”链接。

iv. 向下滚动至操作“getEncryptedKeyPassword”。

v. 在“Key Password”字段中输入密码。

vi. 按“getEncryptedKeyPassword”按钮。

c. 复制并粘贴已加密的密码，更新 **javax.net.ssl.keyStorePassword** 属性。

> **备注：**这些数字以逗号分隔。例如： -20,50,34,-40,-50.)

6. **将探测器证书复制到 UCMDB 计算机**

将 Data Flow Probe 计算机中的文件 **C:\HP\UCMDB\DataFlowProbe\conf\security\client.cert** 复制到位于 **C:\HP\UCMDB\UCMDBServer\conf\security\<探测器名称>.cert** 的 UCMDB 计算机。

更多 UCMDB 服务器配置

1. **将每个探测器证书添加到 UCMDB 的信任库中**

> **备注：**必须针对每个探测器证书完成以下步骤。

a. 打开命令提示并运行以下命令：

```
C:\HP\UCMDB\UCMDBServer\bin\jre\bin\keytool.exe -import -v -keystore C:\hp
\UCMDB\UCMDBServer\conf\security\server.truststore -file C:\hp\UCMDB\UCMDB
Server\conf\security\<探测器名称>.cert -alias <探测器名称>
```

b. 输入密钥库密码。例如，现成的密钥库密码为 **hppass**。

c. 询问 **Trust this certificate?** 时，请按 **y**，然后按 **Enter**。

将显示以下消息：

Certificate was added to keystore

重新启动计算机

重新启动 UCMDB 服务器和探测器计算机。

控制 domainScopeDocument 文件的位置

探测器的文件系统包含 (在默认情况下) 加密密钥和 **domainScopeDocument** 文件。每次启动探测器时，探测器都会从服务器检索 **domainScopeDocument** 文件，并将其存储在文件系统上。为了阻止未经授权的用户获取这些认证，您可以配置探测器，以便将 **domainScopeDocument** 文件存储在探测器的内存中，而不是存储在探测器文件系统上。

要控制 domainScopeDocument 文件的位置，请执行以下操作：

1. 打开 **C:\hp\UCMDB\DataFlowProbe\conf\DataFlowProbe.properties** 并将

   ```
   appilog.collectors.storeDomainScopeDocument=true
   ```

   更改为

   ```
   appilog.collectors.storeDomainScopeDocument=false
   ```

   Probe Gateway 和 Probe Manager 的 serverData 文件夹不再包含 **domainScopeDocument** 文件。

   有关使用 **domainScopeDocument** 文件强化数据流管理的详细信息，请参阅数据流凭据管理 (第 46 页)。

2. 重新启动探测器。

创建 Data Flow Probe 的密钥库

1. 在探测器计算机上运行以下命令：

   ```
   c:\HP\UCMDB\DataFlowProbe\bin\jre\keytool -genkey -alias <探测器名称> -keyalg
   RSA -sigalg SHA256withRSA -keysize 2048 -keystore c:\HP\UCMDB\DataFlowProbe\
   conf\security\client.keystore
   ```

2. 输入新密钥库的密码。

3. 输入要求的信息。

4. 询问 **Is CN=... C=... Correct?** 时，输入 **yes**，并按 **Enter**。

5. 再次按 **Enter** 接受密钥库密码作为密钥密码。

6. 验证 **client.keystore** 是否在以下目录中创建：**C:\HP\UCMDB\DataFlowProbe\conf\security**。

加密探测器密钥库和信任库密码

探测器密钥库和信任库密码以加密的形式存储在 **C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties** 中。以下过程将说明如何加密密码。

1. 启动 Data Flow Probe (或验证它是否已运行)。

2. 访问 Data Flow Probe JMX 控制台：启动 Web 浏览器，并输入以下地址：http://<Data Flow Probe 计算机名称或 IP 地址>:1977。如果在本地运行 Data Flow Probe，请输入 http://localhost:1977。

> **备注：**您可能需要使用用户名和密码登录。如果尚未创建用户，则使用默认用户名 sysadmin 和密码 sysadmin 登录。

3. 找到 **Type=MainProbe** 服务，并单击链接打开“Operations”页面。
4. 找到 **getEncryptedKeyPassword** 操作。
5. 在“Key Password”字段中输入密钥库或信任库密码，然后通过单击 **getEncryptedKeyPassword** 调用该操作。
6. 调用的结果便是加密密码字符串，例如：

   ```
   66,85,54,78,69,117,56,65,99,90,86,117,97,75,50,112,65,53,67,114,112,65,61,61
   ```

7. 将加密密码复制并粘贴到与以下文件中的密钥库或信任库相关的行中：**C:\HP\UCMDB\DataFlowProbe\conf\security\ssl.properties**。

服务器和 Data Flow Probe 默认密钥库和信任库

本节包括以下主题：

- UCMDB 服务器 (第 79 页)
- Data Flow Probe (第 80 页)

UCMDB 服务器

文件位于以下目录中：**C:\HP\UCMDB\UCMDBServer\conf\security**。

实体	文件名/术语	密码/术语	别名
服务器密钥库	server.keystore (sKeyStoreFile)	hppass (sKeyStorePass)	hpcert
服务器信任库	server.truststore (sTrustStoreFile)	hppass (sTrustStorePass)	hpcert (默认受信任条目)
客户端密钥库	client.keystore (cKeyStoreFile)	clientpass (cKeyStorePass)	clientcert

Data Flow Probe

文件位于以下目录中：**C:\HP\UCMDB\DataFlowProbe\conf\security**。

实体	文件名/术语	密码/术语	别名
探测器密钥库	hpprobeKeyStore.jks (pKeyStoreFile)	logomania (pKeyStorePass)	hpprobe
在相互身份验证过程中，Data Flow Probe 使用 **cKeyStoreFile** 密钥库作为默认密钥库。此为客户端密钥库，并在安装 UCMDB 时安装。			
探测器信任库	hpprobeTrustStore.jks (pTrustStoreFile)	logomania (pTrustStorePass)	hpprobe (默认受信任条目)
cKeyStorePass 密码是 **cKeyStoreFile** 的默认密码。			

第 6 章：轻型单一登录 (LW-SSO) 身份验证 - 一般参考

本章包括：

LW-SSO 身份验证概述

LW-SSO 是一种访问控制方法，允许您登录一次便可访问多个软件系统的资源，而不会提示您重新登录。软件系统的配置组内的应用程序信任身份验证，因此从一个应用程序移至另一个应用程序时，无需进一步进行身份验证。

本节的信息适用于 LW-SSO 版本 2.2 和 2.3。

- **LW-SSO 令牌过期**

  LW-SSO 令牌的过期值决定应用程序的会话有效性。因此，其过期值应至少与应用程序会话过期值相同。

- **LW-SSO 令牌过期的建议配置**

  每个使用 LW-SSO 的应用程序均应配置令牌过期。建议值为 60 分钟。对于不需要高级别安全性的应用程序，可以将该值配置为 300 分钟。

- **GMT 时间**

  参与 LW-SSO 集成的所有应用程序都必须使用相同的 GMT 时间，最大时差为 15 分钟。

- **多域功能**

  多域功能需要参与 LW-SSO 集成的所有应用程序都配置 trustedHosts 设置或“protectedDomains”设置，前提是需要这些应用程序与不同 DNS 域中的应用程序集成。此外，这些应用程序还必须在配置的 **lwsso** 元素中添加正确的域。

- **获取 URL SecurityToken 的功能**

要从其他应用程序接收作为 **URL 的 SecurityToken** 发送的信息，主机应用程序应在配置的 **lwsso** 元素中配置正确的域。

LW-SSO 系统要求

应用程序	版本	注释
Java	1.5 和更高版本	
HTTP Servlet API	2.1 和更高版本	
Internet Explorer	6.0 和更高版本	浏览器应启用 HTTP 会话 cookie 和 HTTP 302 重定向功能。
Firefox	2.0 和更高版本	浏览器应启用 HTTP 会话 cookie 和 HTTP 302 重定向功能。
JBoss 身份验证	JBoss 4.0.3 JBoss 4.3.0	
Tomcat 身份验证	Standalone Tomcat 5.0.28 Standalone Tomcat 5.5.20	
Acegi 身份验证	Acegi 0.9.0 Acegi 1.0.4	
Web 服务引擎	Axis 1 - 1.4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	

LW-SSO 安全警告

本节介绍了与 LW-SSO 配置相关的安全警告：

- **LW-SSO 中的机密 InitString 参数。** LW-SSO 将使用对称加密验证并创建 LW-SSO 令牌。配置中的 **initString** 参数可用于初始化密钥。应用程序创建令牌后，使用相同 initString 参数的每个应用程序都会验证该令牌。

  警告：

- 在未设置 **initString** 参数的情况下，无法使用 LW-SSO。
- **initString** 参数是机密信息，在发布、传输和持久保存时应保密。
- **initString** 参数只能在使用 LW-SSO 进行相互集成的应用程序之间共享。
- **initString** 参数的长度至少应为 12 个字符。

- **仅在需要时才启用 LW-SSO。**除非特别需要，否则应禁用 LW-SSO。
- **身份验证安全级别**。使用最弱身份验证框架并发出 LW-SSO 令牌 (受其他集成的应用程序信任) 的应用程序，可确定所有应用程序的身份验证安全级别。

  建议只有使用强大安全的身份验证框架的应用程序才能发出 LW-SSO 令牌。
- **对称加密含义。**LW-SSO 使用对称加密来发出和验证 LW-SSO 令牌。因此，任何使用 LW-SSO 的应用程序均可发出受所有其他应用程序 (共享相同的 initString 参数) 信任的令牌。共享 initString 的应用程序位于不受信任位置或可从不受信任位置对其访问时，可能会出现此潜在风险。
- **用户映射(同步)。**LW-SSO 框架无法确保集成的应用程序之间存在用户映射。因此，集成的应用程序必须监控用户映射。我们建议您在所有集成的应用程序之间共享与 LDAP/AD 相同的用户注册表。

  如果无法映射用户，则可能会导致出现安全漏洞，并对应用程序行为产生负面影响。例如，同一用户名可能会分配到各种应用程序中的不同真实用户。

  此外当用户登录某应用程序 (AppA)，然后访问使用容器或应用程序身份验证的第二个应用程序 (AppB) 时，如果无法映射用户，将强制用户手动登录 AppB 并输入用户名。如果用户输入的用户名与登录 AppA 时所用的用户名不同，则可能出现以下行为：如果用户接着从 AppA 或 AppB 访问第三个应用程序 (AppC)，则他们将分别使用登录 AppA 或 AppB 时所用的用户名来访问 AppC。
- **身份管理器**。为了进行身份验证，必须使用 LW-SSO 配置文件中的 **nonsecureURLs** 设置对身份管理器中的所有未受保护的资源进行配置。
- **LW-SSO 演示模式。**
  - 演示模式应仅用于演示目的。
  - 演示模式应仅在不安全的网络中使用。
  - 演示模式不得在生产中使用。不得使用演示模式与生产模式的任何组合。

疑难解答和局限性

本节介绍使用 LW-SSO 身份验证的已知问题和局限性。

已知问题

本节介绍了 LW-SSO 身份验证的已知问题。

- **安全上下文。**LW-SSO 安全上下文仅支持每个属性名称的一个属性值。

  因此，当 SAML2 令牌针对同一属性名称发送多个值时，LW-SSO 框架只接受一个值。

  同样地，如果 IdM 令牌配置为针对同一属性名称发送多个值，则 LW-SSO 框架只接受一个值。

- **使用 Internet Explorer 7 时的多域注销功能。**在以下情况下，多域注销功能可能会失效：

  - 所用的浏览器是 Internet Explorer 7，并且应用程序将在注销过程中调用三个以上的连续 HTTP 302 重定向动词。

  在这种情况下，Internet Explorer 7 可能会误处理 HTTP 302 重定向响应，并显示“Internet Explorer 无法显示网页”错误页面。

  解决方法是建议减少注销序列中的应用程序重定向命令数 (如果可能)。

局限性

使用 LW-SSO 身份验证时，请注意以下限制：

- **对应用程序的客户端访问。**

  如果在 LW-SSO 配置中定义了域：

  - 应用程序客户端必须访问登录 URL 中包含完全限定域名 (FQDN) (例如 http://myserver.**companydomain**.com/WebApp) 的应用程序。
  - LW-SSO 不支持包含 IP 地址的 URL，例如 http://192.168.12.13/WebApp。
  - LW-SSO 不支持部包含域的 URL，例如 http://myserver/WebApp。

  如果未在 LW-SSO 配置中定义域：客户端可以访问登录 URL 中不包含 FQDN 的应用程序。在这种情况下，专门为不包含任何域信息的单个计算机创建 LW-SSO 会话 cookie。因此，cookie 不会由一个浏览器委托到另一个浏览器，也不会传递到位于相同 DNS 域中的其他计算机。这意味着 LW-SSO 不会在相同的域中工作。

- **LW-SSO 框架集成。**只有提前在 LW-SSO 框架中集成时，应用程序才可以利用和使用 LW-SSO 功能。

- **多域支持。**

- 多域功能基于 HTTP 引用网站。因此，LW-SSO 支持从一个应用程序链接到另一个应用程序，但不支持在浏览器窗口中键入 URL，除非两个应用程序均在相同的域中。
- 不支持使用 **HTTP POST** 的第一个交叉域链接。

  多域功能不支持对第二个应用程序的第一个 **HTTP POST** 请求，仅支持 **HTTP GET** 请求。例如，如果您的应用程序具有到第二个应用程序的 HTTP 链接，则支持 **HTTP GET** 请求，但不支持 **HTTP FORM** 请求。第一个请求之后的所有请求可以是 **HTTP POST** 或 **HTTP GET**。
- LW-SSO 令牌大小：

  LW-SSO 可以从一个域中的某应用程序传输到另一个域中的另一个应用程序的信息大小限制为 15 组/角色/属性 (注意，平均每项长度可能是 15 个字符)。
- 在多域场景中从受保护 (HTTPS) 页面链接到不受保护 (HTTP) 页面：

  从受保护 (HTTPS) 页面链接到不受保护 (HTTP) 页面时，不能正常使用多域功能。这是浏览器限制，因为从受保护资源链接到不受保护资源时，不会发送引用网站标头。有关示例，请参阅：`http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP`
- Internet Explorer 中的第三方 cookie 行为：

  Microsoft Internet Explorer 6 包含支持“隐私首选项平台 (P3P) 项目”的模块，这意味着来自第三方域的 cookie 默认情况下会在 Internet 安全区域中被阻止。会话 cookies 也被认为是 IE 的第三放 cookie，因此会对其进行阻止，从而导致 LW-SSO 停止工作。有关详细信息，请参阅：`http://support.microsoft.com/kb/323752/en-us`。

  要解决此问题，请将启动的应用程序或 DNS 域子集 (如 *.mydomain.com) 添加到计算机上的 Intranet/受信任区域 (在 Microsoft Internet Explorer 中，选择“菜单”>“工具”>“Internet 选项”>“安全”>“本地 Intranet”>“站点”>“高级”)，这样便可接受 cookie。

  警告： LW-SSO 会话 cookie 只是被阻止的第三方应用程序使用的其中一个 cookie。

- **SAML2 令牌**
  - 使用 SAML2 令牌后便不支持注销功能。

    因此，如果使用 SAML2 令牌访问第二个应用程序，则从第一个应用程序注销的用户不会从第二个应用程序注销。
  - **应用程序的会话管理中不会反映 SAML2 令牌的过期。**

    因此，如果使用 SAML2 令牌访问第二个应用程序，则将单独处理每个应用程序的会话管理。

- **JAAS 领域。**不支持 Tomcat 中的 JAAS 领域。
- **使用 Tomcat 目录中的空间。**不支持使用 Tomcat 目录中的空间。

  当 Tomcat 安装路径 (文件夹) 包含空间 (例如 Program Files)，并且 LW-SSO 配置文件位于 **common\classes** Tomcat 文件夹中时，将无法使用 LW-SSO。
- **负载平衡器配置。**部署有 LW-SSO 的负载平衡器必须配置为使用粘性会话。
- **演示模式。**在演示模式下，LW-SSO 支持从一个应用程序链接到另一个应用程序，但不支持在浏览器窗口中键入 URL，因为在此情况下没有 HTTP 引用网站标头。

第 7 章：HP Universal CMDB 登录身份验证

本章包括：

设置身份验证方法

要执行身份验证，您可以使用以下方式工作：

- **针对内部 HP Universal CMDB 服务。**
- **通过轻型目录访问协议 (LDAP)。**您可以使用专用的外部 LDAP 服务器存储身份验证信息，而不用使用内部 HP Universal CMDB 服务。LDAP 服务器必须与所有 HP Universal CMDB 服务器位于相同的子网中。

  有关 LDAP 的详细信息，请参阅《HP Universal CMDB 管理指南》中的“LDAP 映射”一节。

  默认的身份验证方法将使用内部 HP Universal CMDB 服务。如果使用默认方法，则不必对系统进行任何变更。

  这些选项适用于通过 Web 服务以及用户界面执行的登录。

- **通过 LW-SSO。**HP Universal CMDB 配置为使用 LW-SSO。LW-SSO 支持您登录 HP Universal CMDB，并自动访问相同域上运行的其他配置的应用程序，而无需登录这些应用程序。

  启用 LW-SSO 身份验证支持 (默认情况下禁用) 时，必须确保单一登录环境中的其他应用程序已启用 LW-SSO，并使用相同的 initString 参数。

支持使用 LW-SSO 登录 HP Universal CMDB

要对 HP Universal CMDB 启用 LW-SSO，请使用以下过程：

1. 将以下地址输入到 Web 浏览器，以此访问 JMX 控制台：**http://<服务器名称>:8080/jmx-console**，其中 **<服务器名称>** 是安装 HP Universal CMDB 的计算机的名称。
2. 在 **UCMDB-UI** 下，单击 **name=LW-SSO Configuration** 打开“Operations”页面。
3. 使用 **setInitString** 方法设置 init 字符串。
4. 使用 **setDomain** 方法设置安装了 UCMDB 的计算机的域名。
5. 调用 **setEnabledForUI** 方法，并将参数设置为 **True**。
6. **可选**。如果需要使用多域功能，则选择 **addTrustedDomains** 方法，输入域值并单击“Invoke”。
7. **可选。**如果需要使用反向代理，则选择 **updateReverseProxy** 方法，将“Is reverse proxy enabled”参数设置为“True”，为“Reverse proxy full server URL”参数输入 URL，并单击“Invoke”。如果既需直接访问、又需使用反向代理访问 UCMDB，则设置以下其他配置：选择 **setReverseProxyIPs** 方法，为“Reverse proxy ip/s”参数输入 IP 地址，并单击“Invoke”。
8. **可选**。如果需要使用外部身份验证点来访问 UCMDB，则选择 **setValidationPointHandlerEnable** 方法，将“Is validation point handler enabled”参数设置为“True”，为“Authentication point server”参数中的身份验证点输入 URL，并单击“Invoke”。
9. 要在设置机制中保存 LW-SSO 配置时查看该配置，请调用 **retrieveConfigurationFromSettings** 方法。
10. 要查看实际加载的 LW-SSO 配置，请调用 **retrieveConfiguration** 方法。

备注：不可通过用户界面启用 LW-SSO。

设置使用 SSL (安全套接字层) 协议的安全连接

因为登录过程会在 HP Universal CMDB 和 LDAP 服务器之间传递机密信息，所以您可以对内容应用某个安全级别，方法是在 LDAP 服务器上启用 SSL 通信并将 HP Universal CMDB 配置为使用 SSL 进行工作。

HP Universal CMDB 支持使用可信的证书颁发机构 (CA) 颁发的证书的 SSL。

大多数 LDAP 服务器 (包括 Active Directory) 均可为基于 SSL 的连接提供一个安全端口。如果要在 Active Directory 中使用私有 CA，则必须将您的 CA 添加到 JRE 中的可信 CA。

有关将 HP Universal CMDB 平台配置为支持使用 SSL 进行通信的详细信息，请参阅启用安全套接字层 (SSL) 通信 (第 16 页)。

要将 CA 添加到可信 CA，从而为基于 SSL 的连接提供一个安全端口，请执行以下操作：

1. 使用以下步骤从您的 CA 中导出证书，并将其导入到 HP Universal CMDB 使用的 JVM 中：

   a. 在 UCMDB 服务器计算机上访问 **UCMDBServer\bin\JRE\bin** 文件夹。

   b. 运行以下命令：

   ```
   Keytool -import -file <您的证书文件> -keystore C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
   ```

   例如：

   ```
   Keytool -import -file c:\ca2ss_ie.cer -keystore C:\hp\UCMDB\UCMDBServer\bin\JRE\lib\security\cacerts
   ```

2. 选择“管理”>“基础结构设置管理器”>“LDAP 常规”类别。

   备注：还可以使用 JMX 控制台来配置这些设置。有关详细信息，请参阅如何使用 JMX 控制台启用和定义 LDAP 身份验证方法 (第 92 页)。

3. 查找“LDAP 服务器 URL”，并输入值，格式为：

   ```
   ldaps://<ldapHost>[:<port>]/[<baseDN>][??scope]
   ```

   例如：

   ```
   ldaps://my.ldap.server:389/ou=People,o=myOrg.com??sub
   ```

   请注意 **ldaps** 中的 **s**。

4. 单击“保存”保存新值，或单击“恢复默认值”将条目替换为默认值 (空白 URL)。

使用 JMX 控制台测试 LDAP 连接

本节介绍了使用 JMX 控制台测试 LDAP 身份验证配置的方法。

1. 启动 Web 浏览器，并输入以下地址：**http://<服务器名称>:8080/jmx-console**，其中 **<服务器名称>** 是安装 HP Universal CMDB 的计算机的名称。

   您可能需要使用用户名和密码登录。

2. 在 **UCMDB** 下，单击 **UCMDB:service=LDAP Services**，打开“Operations”页面。

3. 找到 **testLDAPConnection**。

4. 在参数 **customer id** 的“Value”框中，输入客户 ID。
5. 单击“Invoke”。

   JMX MBEAN 操作结果页面将指示 LDAP 连接是否成功。如果连接成功，则该页面还会显示 LDAP 根组。

如何启用和定义 LDAP 身份验证方法

您可以启用并定义 HP Universal CMDB 系统的 LDAP 身份验证方法。

备注：

- 还可以使用 JMX 控制台配置 LDAP 身份验证设置。有关详细信息，请参阅如何使用 JMX 控制台启用和定义 LDAP 身份验证方法 (第 92 页)。
- 有关 LDAP 身份验证设置的示例，请参阅LDAP 身份验证设置 - 示例 (第 93 页)。

要在 UCMDB 用户界面中启用和定义 LDAP 身份验证方法，请执行以下操作：

1. 选择“管理”>“基础结构设置管理器”>“LDAP 常规”类别。
2. 选择“LDAP 服务器 URL”，并输入 LDAP URL 值，格式为：

   ```
   ldap://<ldapHost>[:<port>]/[<baseDN>][??scope]
   ```

   例如：

   ```
   ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub
   ```

3. 选择“LDAP 组定义”类别，查找“组的基础 DN”，并输入常规组的可分辨名称。
4. 查找“根组基础 DN”，并输入根组的可分辨名称。
5. 选择“LDAP 常规”类别，查找“启用用户权限同步”，并验证是否已将值设置为“True”。
6. 选择“LDAP 常规身份验证”类别，查找“具有搜索权限的用户的密码”，并填写密码。
7. 选择“适用于类和属性的 LDAP 选项”类别，查找“组类对象”，并填写对象类名称 (Microsoft Active Directory 的 **group** 和 Oracle 目录服务器的 **groupOfUniqueNames**)。
8. 查找“组成员属性”，并填写属性名称 (Microsoft Active Directory 的 **member** 和 Oracle 目录服务器的 **uniqueMember**)。
9. 查找“用户对象类”，并填写对象类名称 (Microsoft Active Directory 的 **user** 和 Oracle 目

录服务器的 **inetOrgPerson**）。

10. 查找“UUID 属性”，为目录服务器中的用户填写唯一标识属性。务必选择目录服务器中的唯一属性。例如，使用 SunOne/Oracle 目录服务器时，UID 属性不是唯一属性。在这种情况下，请使用电子邮件地址属性或可分辨名称。使用非唯一属性作为 UCMDB 中的唯一标识属性时，可能会导致登录过程中出现不一致的行为。

11. 保存新值。要将条目替换为默认值，请单击“恢复默认值”。

12. 如果将“LDAP 常规”下的基础结构设置“使用 LDAP 进行身份验证时是否要求区分大小写”设置为“True”，则身份验证将区分大小写。

    警告：更改此基础结构的设置值时，UCMDB 管理员必须手动删除所有外部用户。

13. 将 LDAP 用户组映射到 UCMDB 用户组。有关详细信息，请参阅HP Universal CMDB 登录身份验证 (第 88 页)。

14. 如果需要为没有组映射的 LDAP 组中的用户定义一组默认权限，请选择“LDAP 常规”类别，查找“自动分配的用户组”，并输入组名称。

15. **重要信息：**如果正在高可用性环境中配置 LDAP，则必须重新启动群集才能使变更生效。

备注：每位 LDAP 用户都将名字、姓氏和电子邮件地址保存在本地库中。如果 LDAP 服务器中存储的上述任一参数值不同于本地库中的值，则每次登录时，LDAP 服务器值将覆盖本地值。

如何使用 JMX 控制台启用和定义 LDAP 身份验证方法

此任务描述如何使用 JMX 控制台配置 LDAP 身份验证设置。

备注：

- 在高可用性环境中，请确保登录到编写器服务器的 JMX 控制台。
- 还可以在 UCMDB 中配置 LDAP 身份验证设置。有关详细信息，请参阅如何启用和定义 LDAP 身份验证方法 (第 91 页)。
- 有关 LDAP 身份验证设置的示例，请参阅LDAP 身份验证设置 - 示例 (第 93 页)。

要配置 LDAP 身份验证设置，请执行以下操作：

1. 启动 Web 浏览器，并输入以下地址：**http://<服务器名称>:8080/jmx-console**，其中 **<服务器名称>** 是安装 HP Universal CMDB 的计算机的名称。

   您可能需要使用用户名和密码登录。

2. 在 **UCMDB** 下，单击 **UCMDB:service=LDAP Services** 打开“Operations”页面。

3. 要查看当前 LDAP 身份验证设置，请找到 **getLDAPSettings** 方法。单击“Invoke”。此时将显示一张表，其中列出所有 LDAP 设置及其值。

4. 要更改 LDAP 身份验证设置的值，请找到 **configureLDAP** 方法。输入相关设置的值，并单击“Invoke”。JMX MBEAN 操作结果页面将指示 LDAP 身份验证设置是否已成功更新。

   备注：如果未输入设置的值，则该设置将保留其当前值。

5. 配置 LDAP 设置之后，您可以验证 LDAP 用户凭据：

   a. 找到 **verifyLDAPCredentials** 方法。

   b. 输入客户 ID、用户名和密码。

   c. 单击“Invoke”。

      JMX MBEAN 操作结果页面将指示用户是否通过 LDAP 身份验证。

6. **重要信息：**如果正在高可用性环境中配置 LDAP，则必须重新启动群集才能使变更生效。

备注：每位 LDAP 用户都将名字、姓氏和电子邮件地址保存在本地库中。如果 LDAP 服务器中存储的上述任一参数值不同于本地库中的值，则每次登录时，LDAP 服务器值将覆盖本地值。

LDAP 身份验证设置 - 示例

下表包含为 LDAP 身份验证设置值的示例：

设置	值
用户对象类	user
LDAP 身份验证时是否要求区分大小写	false
组成员属性	member
可分辨名称 (DN) 解析	true

设置	值
根组筛选器	(objectCategory=group)
LDAP 连接字符串	ldap://myldap.example.com:389/OU=Users,OU=Dept,OU=US,DC=example,DC=com??sub
LDAP 搜索用户	CN=John Doe,OU=Users,OU=Dept,OU=US,DC=example,DC=com
组类对象	group
使用自下而上算法查找父组	true
UUID 属性	sAMAccountName
组名称属性	cn
组的基础筛选器	(objectclass=group)
用户筛选器	(&(sAMAccountName=*)(objectclass=user))
搜索重试次数计数	3
组显示名属性	cn
根组范围	sub
用户显示名属性	cn
组搜索范围	sub
启用 LDAP 身份验证	false
启用 LDAP 同步	true
根组	OU=Users,OU=Security Groups,DC=example,DC=com
组的基础	OU=AMRND,OU=Security Groups,DC=example,DC=com
默认组	AdminsGroup
组描述属性	description

在分布式环境中检索当前 LW-SSO 配置

在分布式环境 (例如 BSM 部署) 中嵌入 UCMDB 后，请执行以下过程，以在处理计算机上检索当前 LW-SSO 配置。

要检索当前 LW-SSO 配置，请执行以下操作：

1. 启动 Web 浏览器，并输入以下地址：`http://localhost.<域名>:8080/jmx-console`

   可能要求您输入用户名和密码。

2. 找到 **UCMDB:service=Security Services**，然后单击该链接打开“Operations”页面。

3. 找到 **retrieveLWSSOConfiguration** 操作。

4. 单击“Invoke”，检索配置。

第 8 章：机密管理器

本章包括：

机密管理器概述

机密管理器框架可解决为 HP Universal CMDB 及其他 HP 软件产品管理和分发敏感数据的问题。

机密管理器包含两个主要组件：客户端和服务器。这两个组件负责以安全的方式传输数据。

- 机密管理器客户端是应用程序用来访问敏感数据的库。
- 机密管理器服务器将从机密管理器客户端或第三方客户端接收请求，并执行所需的任务。机密管理器服务器主要负责以安全的方式保存数据。

机密管理器将对传输凭据、客户端缓存凭据、持久性凭据和内存中的凭据进行加密。它不仅使用对称加密在机密管理器客户端和机密管理器服务器之间通过共享秘密传输凭据。还可以根据配置将各种秘密用于缓存、持久性和传输加密。

有关管理 Data Flow Probe 上凭据加密的详细准则，请参阅数据流凭据管理 (第 46 页)。

安全注意事项

- 可以对安全算法使用以下密钥大小：128 位、192 位和 256 位。密钥越小，算法运行速度越快，但安全性会较低。在大多数情况下，128 位大小的密钥足够安全。
- 要使系统更加安全，请使用 MAC：将 **useMacWithCrypto** 设置为 **true**。有关详细信息，请参阅加密属性 (第 98 页)。
- 要充分利用强大的客户安全提供程序，您可以使用 JCE 模式。

配置 HP Universal CMDB 服务器

使用 HP Universal CMDB 时，应当使用以下 JMX 方法配置加密的秘密和加密属性：

1. 在 HP Universal CMDB 服务器计算机上，启动 Web 浏览器，并输入服务器地址：**http://<UCMDB 服务器主机名或 IP>:8080/jmx-console**。

   您可能需要使用用户名和密码登录。

2. 在 UCMDB 下，单击 **UCMDB:service=Security Services** 打开“Operations”页面。

3. 要检索当前配置，请找到 **CMGetConfiguration** 操作。

   单击“Invoke”显示机密管理器的服务器配置 XML 文件。

4. 要对配置进行更改，请将在以前步骤中调用的 XML 复制到文本编辑器。根据加密属性 (第 98 页)中的表进行更改。

   找到 **CMSetConfiguration** 操作。将已更新的配置复制到“Value”框中，并单击“Invoke”。此时新配置将写入 UCMDB 服务器。

5. 要将用户添加到机密管理器进行授权和复制，请找到 **CMAddUser** 操作。此步骤还适用于复制过程。在复制过程中，从服务器应通过特许用户与主服务器通信。

   - **username**。用户名。
   - **customer**。默认为 ALL_CUSTOMERS。
   - **resource**。资源名称。默认为 ROOT_FOLDER。
   - **permission**。在 ALL_PERMISSIONS、CREATE、READ、UPDATE 和 DELETE 之间选择。默认为 ALL_PERMISSIONS。

   单击“Invoke”。

6. 如有必要，请重新启动 HP Universal CMDB。

   在大多数情况下，无须重新启动服务器。但在更改以下资源之一后，则可能需要重新启动服务器：

   - 存储类型
   - 数据库表名称或列名称
   - 数据库连接的创建者
   - 数据库的连接属性 (即 URL、用户、密码、驱动程序类名称)
   - 数据库类型

备注：

- UCMDB 服务器及其客户端有相同的传输加密属性，这一点很重要。如果在 UCMDB 服务器上更改了这些属性，则必须在所有客户端上也进行相应更改。(这与 Data Flow Probe 无关，因为它在与 UCMDB 服务器相同的进程上运行，即不需要传输加密配置。)
- 默认情况下未配置机密管理器复制，但可在需要时对其进行配置。
- 如果启用了机密管理器复制，且主服务器的传输 **initString** 或任何其他加密属性发生更改，则所有从服务器必须采用同样的更改。

定义

存储加密属性。此配置可定义服务器保存和加密数据的方式 (在数据库或文件中，必须加密或解密数据的加密属性等)、凭据的安全存储方式、加密处理方式和根据的配置。

传输加密属性。传输配置可定义服务器和客户端加密两者之间传输的方式、使用的配置、凭据的安全传输方式、加密处理方式和根据的配置。在服务器和客户端中必须使用相同的传输加密和解密的加密属性。

复制和复制加密属性。由机密管理器安全保存的数据在多个服务器之间安全地复制。复制和复制加密属性则可定义这些数据在从服务器和主服务器之间传输的方式。

备注：

- 包含机密管理器服务器配置的数据库表名为：**CM_CONFIGURATION。**
- 机密管理器服务器的默认配置文件位于 app-infra.jar 中，名为 **defaultCMServerConfig.xml**。

加密属性

下表对加密属性进行说明。有关使用以下参数的详细信息，请参阅配置 HP Universal CMDB 服务器 (第 96 页)。

参数	描述	建议值
encryptTransportMode	加密传输的数据： true false	true
encryptDecrypt InitString	加密的密码	超过 8 个字符

参数	描述	建议值
cryptoSource	要使用的加密实现库： • lw • jce • windowsDPAPI • lwJCECompatible	lw
lwJCEPBE CompatibilityMode	支持以前版本的轻型加密： • true • false	true
cipherType	机密管理器使用的密码类型。机密管理器仅支持一个值： **symmetricBlockCipher**	symmetric BlockCipher
engineName	• AES • Blowfish • DES • 3DES • 空 (未加密)	AES
algorithmModeName	块加密算法的模式： • CBC	CBC
algorithmPaddingName	填充标准： • PKCS7Padding • PKCS5Padding	PKCS7Padding
keySize	取决于算法 (**engineName** 支持的算法)	256
pbeCount	运行哈希操作以根据 **encryptDecryptInitString** 创建密钥的次数。 任何正数。	1000

参数	描述	建议值
pbeDigestAlgorithm	哈希类型： • SHA1 • SHA256 • MD5	SHA256
encodingMode	加密对象的 ASCII 表示： • Base64 • Base64Url	Base64Url
useMacWithCrypto	定义加密是否使用 MAC： • true • false	false
macType	消息身份验证代码 (MAC) 的类型： • hmac	hmac
macKeySize SHA256	取决于 MAC 算法	256
macHashName	哈希 MAC 算法： • SHA256	SHA256

第 9 章：高可用性强化

本章包括：

群集身份验证

要启用群集身份验证，请执行以下操作：

1. 在 UCMDB 中，转到“管理”>“基础结构设置管理器”。
2. 找到设置“加入高可用性群集时启用身份验证”并将其设置为“true”。
3. 提供 JKS 格式的单个服务器身份验证密钥库 (证书 + 私钥和公钥)。此密钥库将放置在所有服务器上，并在连接高可用性群集时用于身份验证。

   将密钥库放在以下位置：**<UCMDB 安装文件夹>\conf\security**，并将其命名为 **cluster.authentication.keystore**。

   > **备注：**UCMDB 附带此现成的预定义密钥库。此密钥库对于所有全新 UCMDB 安装都相同，因此并不安全。如果希望身份验证加入请求安全，则删除此文件并创建一个新文件。

4. 按照以下步骤生成群集身份验证密钥库：
   a. 在 C:\hp\UCMDB\UCMDBServer\bin\jre\bin 中运行以下命令：

      ```
      keytool -genkey -alias hpcert –keystore <UCMDB 安装文件夹>\conf\security\
      cluster.authentication.keystore -keyalg RSA
      ```

      将打开控制台对话框并要求输入新密钥库密码。

   b. 默认密码为 **hppass**。如果要使用其他密码，则通过运行以下 JMX 方法更新服务器：**UCMDB:service=High Availability Services:changeClusterAuthenticationKeystorePassword**

   c. 在控制台对话框中，对问题“您叫什么名字?”输入群集名称。

   d. 根据组织的详细信息输入其他参数。

   e. 输入密钥密码。密钥密码必须与密钥库密码相同。

在 **<UCMDB 安装文件夹>\conf\security\cluster.authentication.keystore** 中将创建一个 JKS 密钥库

5. 使用此新密钥库替换群集中所有服务器的旧 **<UCMDB 安装文件夹>\conf\security\cluster.authentication.keystore**。

6. 重新启动群集中的所有服务器。

群集消息加密

使用群集消息加密对群集中的所有消息进行加密。

要启用群集消息加密，请执行以下操作：

1. 在 UCMDB 中，转到“管理”>“基础结构设置管理器”。

2. 找到设置“启用高可用性群集通信加密”并将其设置为“true”。

3. 为所有服务器上的对称加密提供一个密钥。该密钥应放置在以下位置的 JCEKS 类型的密钥库中：**<UCMDB 安装文件夹>\conf\security\cluster.encryption.keystore**。

   备注：UCMDB 附带此现成的预定义密钥库。此密钥库对于所有全新 UCMDB 安装都相同，因此并不安全。如果希望安全加密群集消息，请删除此文件，然后按照以下步骤创建一个新文件。

4. 从 **<UCMDB 安装文件夹>\bin\jre\bin** 运行以下命令：

   Keytool –genseckey –alias hpcert –keystore <UCMDB 安装文件夹>\conf\security\cluster.encryption.keystore –storetype JCEKS

5. 系统会询问新密钥库密码。默认密码为“hppass”。如果要使用其他密码，则需要通过运行以下 JMX 方法更新服务器：

   UCMDB:service=High Availability Services:changeClusterEncryptionKeystorePassword

6. 使用此新密钥库替换群集中所有服务器的旧 **<UCMDB 安装文件夹>\conf\security\cluster.encryption.keystore**。

7. 重新启动服务器。

疑难解答

服务器每次启动时都会向群集发送测试消息验证是否已成功连接到该群集。如果连接有问题，则消息会失败，此时服务器将停止以避免整个群集卡住。

下面是一些错误群集加密配置示例：

- 在一个节点上禁用了加密，而其他节点已启用加密。
- cluster.encryption.keystore 错误或缺失
- 密钥库中的密钥错误或缺失

如果服务器因配置问题卡住，则错误消息为：

```
2012-09-11 17:48:23,584 [Thread-14] FATAL - #### Server failed to connect proper
ly to the cluster and its service is stopped!Please fix the problem and start it
again ####

2012-09-11 17:48:23,586 [Thread-14] FATAL -       Potential problems can be:wron
g security configuration (wrong or missing cluster.encryption.keystore, wrong ke
y, disabled encryption in a cluster with enabled encryption)
```

更改 key.bin 中的密钥

在包含几个服务器的高可用性环境中，按照以下步骤更改 **key.bin** 中的**键**：

1. 转到 JMX 中的编写器计算机。可选择群集中的任何计算机，然后单击每个页面顶部的“编写器”链接。
2. 在控制台的 UCMDB 部分，单击 **UCMDB:service=Discovery Manager**。
3. 通过以下任一方式更改密钥：
   - 单击 **changeEncryptionKey** (此操作导入现有加密密钥)
   - 单击 **generateEncryptionKey** (此操作生成随机加密密钥)
4. 在编写器计算机上，转到文件系统并在以下路径找到 **key.bin**：**C:\hp\UCMDB\UCMDBServer\conf\discovery\key.bin**
5. 将 **key.bin** 从编写器计算机上的该位置复制到群集中其他每个计算机的以下文件夹中：**C:\hp\UCMDB\UCMDBServer\conf\discovery\customer_1**，然后重命名目标文件 (例如，**key_new.bin**)。
6. 对其他每个服务器 (读取器) 执行以下操作：
   a. 将读取器切换为编写器 (可从高可用性 JMX 中执行该操作) 并等待变更生效。
   b. 连接到当前编写器的 JMX，并单击 **UCMDB:service=Discovery Manager**。
   c. 单击并调用 **changeEncryptionKey**，使用步骤 3 中输入的相同详细信息 (对于 **newKeyFileName**，请使用步骤 5 中指定的新名称)。
   d. 验证是否已获取以下消息：**Key was created successfully**。

我们感谢您提出宝贵的意见！

如果对本文档有任何意见，可以通过电子邮件与文档团队联系。如果在此系统上配置了电子邮件客户端，请单击以上链接，此时将打开一个电子邮件窗口，主题行中为以下信息：

强化指南 (Universal CMDB 和 Configuration Manager 10.10) 反馈

只需在电子邮件中添加反馈并单击“发送”即可。

如果没有可用的电子邮件客户端，请将以上信息复制到 Web 邮件客户端的新邮件中，然后将您的反馈发送至 SW-Doc@hp.com。