HP Universal CMDB 9.10 Configuration Manager

适用于 Windows 操作系统

部署指南

文档发布日期：2010 年 11 月
软件发布日期：2010 年 11 月

法律声明

保修

HP 产品与服务的全部保修条款在此类产品和服务附带的保修声明中均已列明。本文中的任何信息均不构成额外的保修条款。 HP 对本文中所包含的技术或编辑错误、遗漏概不负责。

本文所含信息如有更改，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

文档更新

本文档的标题页包含了下列标识信息：

- 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，用于指明该版本软件的发布日期。

若要检查是否有最新更新，或要验证当前使用的文档是否为最新版本，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** （新用户请注册）链接。

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

支持

请访问 HP 软件支持网站：

http://www.hp.com/go/hpsoftwaresupport

该网站提供联系信息以及有关 HP 软件提供的产品、服务和支持的详细信息。

HP 软件在线支持提供客户自助解决功能。该在线支持提供了一种快速有效的方法，使您可以访问业务管理所需的交互技术支持工具。作为我们的尊贵客户，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，很多地方还会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

目录

第 1 章：安装与配置 7
Configuration Manager 概述 8
Configuration Manager 系统要求 8
建议设置准则 10
Configuration Manager 容量限制 10
配置数据库或用户架构 11
安装 Configuration Manager 12
配置高级数据库连接选项 14
数据库配置 - MLU （多语言单位）支持 16
启用轻型单一登录 18
IPv6 支持 20

第 2 章：Configuration Manager 安装后配置向导 21
Configuration Manager 安装后配置概述 22
数据库连接页面 22
应用程序服务器页面 26
Windows 服务配置页面 27
用户凭据页面 28
HP Universal CMDB 连接页面 28
概要页面 30
完成页面 30

第 3 章：配置 LDAP 31
LDAP 概述 31
连接到组织 LDAP 32
配置内部 （共享） LDAP 38
排除 LDAP 故障 39

第 4 章：轻型单一登录身份验证 (LW-SSO) – 一般参考 43
LW-SSO 身份验证概述 43
LW-SSO 安全警告 45

第 5 章：身份管理器身份验证 51
接受身份管理器身份验证 51
使用 Java 连接器将 Configuration Manager 的身份管理功能配置为与 Windows 2003 操作系统上的 IIS6 结合使用的示例 53

第 6 章：登录到 Configuration Manager 59
访问 Configuration Manager 59
如何访问 Configuration Manager 60
访问 Configuration Manager 的 JMX 控制台 61

第 7 章：强化 69
强化 Configuration Manager 69
加密数据库密码 71
使用自签名证书在服务器计算机上启用 SSL 72
使用证书颁发机构颁发的证书在服务器计算机上启用 SSL 74
使用客户端证书启用 SSL 76
仅为身份验证启用 SSL 77
启用客户端证书身份验证 78
加密参数 79

1

安装与配置

本章包括以下内容：

- “Configuration Manager 概述”（第 8 页）
- “Configuration Manager 系统要求”（第 8 页）
- “建议设置准则”（第 10 页）
- “Configuration Manager 容量限制”（第 10 页）
- “配置数据库或用户架构”（第 11 页）
- “安装 Configuration Manager”（第 12 页）
- “配置高级数据库连接选项”（第 14 页）
- “启用轻型单一登录”（第 18 页）
- “IPv6 支持”（第 20 页）

Configuration Manager 概述

HP Universal CMDB Configuration Manager (Configuration Manager) 支持您分析和控制 CMS 中的数据，并提供控制 CMS 基础结构的环境，该环境包含许多数据源并服务于多种产品和应用程序。

在企业网络环境中部署 Configuration Manager 是一个需要资源计划和系统体系结构设计的过程。安装 Configuration Manager 之前，请仔细阅读本节中的信息，包括系统要求。

Configuration Manager 系统要求

服务器系统要求

下表描述了 Configuration Manager 服务器的系统要求：

CPU	Intel Pentium 4，最少 4 核
内存 (RAM)	最少 4 GB
平台	x64
操作系统	支持以下 64 位 Windows 操作系统： ➤ Windows 2003 Enterprise SP2 和 R2 SP2 ➤ Windows 2008 Enterprise SP2 和 R2

数据库	➤ Microsoft SQL Server 2005 SP2 2005 兼容模式 80 （全部为企业版） ➤ Oracle 11.1.x
HP Universal CMDB	➤ HP Universal CMDB 版本 9.03 （典型 CMDB 安装） 有关此版本系统要求的完整列表，请参阅 HP Universal CMDB 文档。

客户端要求

下表描述了用于查看 Configuration Manager 的客户端要求：

浏览器	➤ Microsoft Internet Explorer 7.0 和 8.0 ➤ Mozilla Firefox 3.x
Flash Player 浏览器插件	Flash Player 9 或更高版本
屏幕分辨率	➤ 最低 1024x768 ➤ 建议 1280x1024
颜色质量	最低 16 位

建议设置准则

下表列出了 Configuration Manager 设置选项的准则。

LDAP	支持以下 LDAP 环境： ➤ Active Directory ➤ SunONE 6.x
建议的最小数据库架构大小	2 GB

Configuration Manager 容量限制

下表列出了 Configuration Manager 的容量限制。

建议的最大视图数	100
建议的最大策略数	300
建议的每视图最大组合 CI 数	5000
建议的最大并行用户数	50

配置数据库或用户架构

要使用 Configuration Manager，必须提供数据库架构。Configuration Manager 支持 Microsoft SQL Server 和 Oracle 数据库服务器。此任务描述如何使用安装向导配置 Configuration Manager 数据库或用户架构的连接属性。

注意：有关 Microsoft SQL Server 和 Oracle Server 系统要求的信息，请参阅 “服务器系统要求”（第 8 页）。

要配置数据库，请执行以下操作：

1 分配 Microsoft SQL Server 数据库或 Oracle Server 用户架构。

- 对于 **Microsoft SQL Server 2005**：请激活快照隔离。

  创建数据库之后，立即执行以下命令：

  ```
  alter database <ccm_database_name> set read_committed_snapshot on
  ```

  有关 SQL Server 快照隔离功能的详细信息，请访问 http://msdn.microsoft.com/en-us/library/tcbchxcb(VS.80).aspx。

- 对于 **Oracle**：请仅授予 Oracle 用户 “连接”和 “资源”角色。（如果授予用户 “选择任何表格”特权，将导致架构填充过程失败。）

2 验证配置过程中需要的下列信息：

✔	**必需信息**
	DB 主机名和端口
	DB 用户名和密码
	对于 MS SQL：数据库名称
	对于 Oracle：SID

3 运行 Configuration Manager 安装向导。有关详细信息，请参阅 “安装 Configuration Manager”（第 12 页）。

安装 Configuration Manager

此任务描述如何在服务器上安装 Configuration Manager 以及如何配置数据库连接和 UCMDB 集成。可单击任何向导页面上的“帮助”获取安装帮助。有关向导页面的详细说明，请参阅 “Configuration Manager 安装后配置向导”（第 21 页）。

要安装 Configuration Manager，请执行以下操作：

1 在 Configuration Manager DVD 的根目录中，找到文件：**install.bat**。

2 双击该文件以运行 Configuration Manager 安装向导。

3 单击 “下一步”以打开 “最终用户许可协议”页面。

4 接受许可协议的条款，然后单击 “下一步”以打开 “产品安装”页面。

5 选择要安装的产品 （UCMDB 和 Configuration Manager）并指定安装位置。如果拥有自定义 UCMDB 许可证，则选中相应复选框。单击“下一步”以启动 UCMDB 安装。有关 UCMDB 安装的详细信息，请参阅《HP Universal CMDB 部署指南》 PDF 文档。

6 完成 UCMDB 安装和安装后设置之后，将自动启动“Configuration Manager 安装后配置”向导。

7 在 “欢迎使用”页面上单击 “下一步”以打开 “数据库连接配置”页面。

8 选择数据库类型（Oracle 或 Microsoft SQL Server），然后输入用户名和密码。建议单击 “测试”按钮对连接进行测试。如果连接测试成功，则单击 “下一步”以打开 “应用程序服务器配置”页面。

注意：您可以在完成向导之后配置更多高级数据库连接选项。有关详细信息，请参阅 “配置高级数据库连接选项”（第 14 页）。

---

9 输入主机名，然后单击 “下一步”以打开 “Windows 服务配置”页面。

10 如果要作为 Windows 服务安装 Configuration Manager，请选中相应复选框。单击 “下一步”以打开 “用户凭据”页面。

11 输入管理用户和集成用户的用户名及密码。单击“下一步”以打开“HP UCMDB 连接配置”页面。

12 如果已在此计算机或其他计算机上安装了 UCMDB，请在继续操作之前确保 UCMDB 服务器运行正常。

如果要在其他计算机上安装 UCMDB，请确保选中相应复选框，并输入所需参数。建议单击 “测试”按钮对连接进行测试。如果连接测试成功，则单击 “下一步”以打开 “安装后操作概要”页面。

13 检查 “安装后操作概要”页面中的信息。如果这些信息是正确的，则单击 “下一步”以继续执行安装后配置。

14 在 “完成”页面中单击 “完成”以完成安装后配置。

15 如果不是第一次启动 UCMDB，则需要按照如下操作更改 UCMDB 中的列大小：

a 转到 “管理” > “基础结构设置管理器”。找到 “对象根”设置，并将其更改为 “数据”。退出 UCMDB，并再次登录以使此更改生效。

b 转到 “建模” > “CI 类型管理器”。从树中选择 CI 类型 “数据”，并选择 “属性”选项卡。通过将 “值大小”更改为 900，编辑属性 “用户标签”。

c 返回到 “基础结构设置管理器”，并且将 “对象根”设置更改为它的原始值。退出并再次登录以使此更改生效。

16 如果已在 UCMDB 上运行数据流管理，则可能损坏历史记录数据。要更正此问题，请执行以下步骤：

a 启动 Web 浏览器，并输入以下地址：http://<UCMDB 服务器地址 >.<domain_name>:8080/jmx-console。

输入 JMX 控制台身份验证凭据，默认情况下，这些凭据为：

- 登录名称 = **sysadmin**
- 密码 = **sysadmin**

b 在 **UCMDB** 下选择 “历史记录 DB 服务”。

c 选择 **Fix902EndTimeRecords** 方法。

d 对于实际状态客户，输入客户 ID 值 **1**，然后单击 “调用”。

e 如果操作成功，将显示 “已成功更新历史记录 DB”消息。

f 对于授权状态客户，输入客户 ID 值 **100001**，然后单击 “调用”。

g 如果操作成功，将显示 “已成功更新历史记录 DB”消息。

配置高级数据库连接选项

如果需要更多高级数据库连接属性以支持数据库部署，则可以在安装后向导运行完毕之后配置这些属性。 Configuration Manager 支持所有供应商的 JDBC 驱动程序支持的数据库连接选项，并且可使用数据库连接 URL 进行配置。要配置更多高级连接，请在 **<Configuration Manager 安装目录 >\conf\database.properties** 文件中编辑 **jdbc.url** 属性。

以下是 Microsoft SQL Server 的更多高级选项的示例：

- **Windows (NTLM) 身份验证。**要应用 Windows 身份验证，请将域属性添加到 database.properties 文件中的 JTDS 连接 URL。指定要进行身份验证的 Windows 域。

  例如：

  ```
  jdbc:jtds:sqlserver://myServer:1433/myDatabase;sendStringParametersAsUnicode=false;domain=myDomain
  ```

- **SSL。**有关使用 SSL 确保 MS SQL Server 连接安全的详细信息，请访问 http://jtds.sourceforge.net/faq.html。

以下是 Oracle 数据库服务器的更多高级选项的示例：

- **Oracle URL。**指定 Oracle 本机驱动程序的 URL 连接。包括有效的 Oracle 服务器名称和 SID。或者，如果要使用 **Oracle RAC**，则需指定 Oracle RAC 配置的详细信息。

  注意：有关配置本机 Oracle JDBC URL 格式的详细信息，请访问 http://www.orafaq.com/wiki/JDBC#Thin_driver。有关配置 Oracle RAC 的 URL 的详细信息，请访问 http://download.oracle.com/docs/cd/B28359_01/java.111/e10788/rac.htm。

- **SSL。**有关使用 SSL 确保 Oracle 连接安全的详细信息，请访问以下链接：
  - http://download.oracle.com/docs/cd/E11882_01/network.112/e10746/asojbdc.htm#ASOAG9604
  - http://download.oracle.com/docs/cd/E11882_01/java.112/e16548/clntsec.htm#insertedID6

数据库配置 - MLU （多语言单位）支持

本节描述支持本地化所需的数据库设置。

Oracle Server 设置

下表列出了 Oracle Server 的必需设置：

选项	支持的设置	建议的设置	注释
字符集	WE8ISO8859P1；UTF8、 AL32UTF8	AL32UTF8	

Microsoft SQL Server 设置

下表列出了 Microsoft SQL Server 的必需设置：

选项	支持的设置	建议的设置	注释
排序规则	不区分大小写。它不支持二进制排序顺序和区分大小写。仅支持包含重音、假名或宽度设置的组合的不区分大小写顺序。	使用“排序规则设置”对话框选择排序规则。请勿选中该二进制复选框。应根据相关数据语言要求选择是否区分重音、假名和宽度。所选语言必须与 Windows 操作系统地区设置语言相同。	限于排序规则区域设置和默认英语定义。
排序规则数据库属性	服务器默认值		

注意：

对于所有语言：“< 语言 >_CI_AS”为最低要求选项。
例如，在日语中，如果要选择 “区分假名”和 “区分宽度”选项，建议选项为：**Japanese_CI_AS_KS_WS** 或 **Japanese_90_CI_AS_KS_WS**。此建议选项表示日语字符是区分重音、假名和宽度的。

- **区分重音 (_AS)。**区分重音和非重音字符。例如， **a** 不等于 **á**。如果不选择此选项，则 Microsoft SQL Server 在排序时会认为字母的重音和非重音版本是相同的。
- **区分假名 (_KS)。**区分两种类型的日语假名字符：平假名和片假名。如果不选择此选项，则 Microsoft SQL Server 在排序时会将平假名和片假名同等视之。
- **区分宽度 (_WS)。**区分同一字符的单字节和双字节表示方法。如果不选择此选项，则 Microsoft SQL Server 在排序时会将同一字符的单字节和双字节表示方式同等视之。

启用轻型单一登录

某些 Configuration Manager 用户也拥有登录到 UCMDB 的权限。为了方便操作，Configuration Manager 提供直接指向 UCMDB 用户界面的链接（选择“管理” > “打开 UCMDB”）。要使用单一登录 （避免需要在登录到 Configuration Manager 后再登录到 UCMDB），必须同时为 Configuration Manager 和 UCMDB 启用 LW-SSO，并确保它们使用相同的 initString。此任务描述如何在 Configuration Manager 和 UCMDB 中启用 LW-SSO。

要启用 LW-SSO，请执行以下操作：

1 打开 Configuration Manager 安装目录中的以下文件：**\servers\server-0\webapps\cnc\WEB-INF\classes\cnclwssofmconf.xml**。

注意：启动 Configuration Manager 之前，此文件不存在。

---

2 定位到以下部分：

```
enableLWSSO enableLWSSOFramework="true"
```

并检查其值是否为 **true**。

3 定位到以下部分：

```
lwssoValidation  id="ID000001">
<domain> </domain>
```

并在 **<domain>** 后输入 Configuration Manager 服务器域。

4 定位到以下部分：

```
<initString="应替换此字符串"></crypto>
```

并将 **"应替换此字符串"** 替换为与 LW-SSO 集成的所有受信任应用程序使用的共享字符串。

5 定位到以下部分：

```
<!--multiDomain>
<trustedHosts>
<DNSDomain> 此值应替换为您的应用程序域 </DNSDomain>
<DNSDomain> 此值应替换为其他应用程序的域 </DNSDomain>
</trustedHosts>
</multiDomain-->
```

删除开头的注释字符，并在 DNSDomain 元素中（替换**此值应替换为您的应用程序域**）输入 Configuration Manager 服务器域。列表应包括步骤 3 （第 18 页）中输入的服务器域。

6 保存更改后的文件，然后重新启动服务器。

7 启动 Web 浏览器，并输入以下地址：http://<UCMDB 服务器地址 >.<domain_name>:8080/jmx-console。

输入 JMX 控制台身份验证凭据，默认情况下，这些凭据为：

- 登录名称 = **sysadmin**
- 密码 = **sysadmin**

8 在 **UCMDB-UI** 下，选择“LW-SSO 配置”以打开“JMX MBEAN 视图”页面。

9 选择 **setEnabledForUI** 方法，将值设置为 **true**，然后单击 “调用”。

10 选择 **setDomain** 方法。输入 UCMDB 服务器的域名，然后单击 “调用”。

11 选择 **setInitString** 方法。输入步骤 4（第 18 页）中为 Configuration Manager 输入的相同 initString，然后单击 “调用”。

12 如果 Configuration Manager 和 UCMDB 位于不同的域中，请选择 **addTrustedDomains** 方法，然后输入 UCMDB 和 Configuration Manager 服务器的域名。单击 “调用”。

13 要查看设置机制中保存的 LW-SSO 配置，请选择 **retrieveConfigurationFromSettings** 方法，然后单击 “调用”。

14 要查看实际加载的 LW-SSO 配置，请选择 **retrieveConfiguration** 方法，然后单击 “调用”。

IPv6 支持

Configuration Manager 仅支持适用于面向客户 URL 的 IPv6 URL。

要使用 IPv6 地址处理 Configuration Manager，请执行以下操作：

1 确保操作系统支持 IPv6。有关详细信息，请参阅相关操作系统文档。

2 打开位于 **<Configuration Manager 安装目录 >** 的 **conf** 目录中的 **client-config.properties** 文件。将 **bsf.server.url** 参数的值更改为两边加了方括号的 IPv6 地址。例如：

```
bsf.server.url=http://[2620:0:a17:e008:d840:5b0f:2040:519c]:8080/bsf
```

2

Configuration Manager 安装后配置向导

本章包括以下内容：

- “Configuration Manager 安装后配置概述”（第 22 页）
- “应用程序服务器页面”（第 26 页）
- “Windows 服务配置页面”（第 27 页）
- “用户凭据页面”（第 28 页）
- “HP Universal CMDB 连接页面”（第 28 页）
- “概要页面”（第 30 页）
- “完成页面”（第 30 页）

Configuration Manager 安装后配置概述

本章将详细介绍 “Configuration Manager 安装后向导” 的各个页面和关联的配置任务。在向导的任何页面中单击 “帮助” 之后就会打开此内容。

数据库连接页面

本节包括以下内容：

- “概述”（第 22 页）
- “参数”（第 23 页）
- “选项”（第 25 页）
- “测试”（第 25 页）

概述

必须设置与标准 URL 连接关联的数据库连接。如果需要更多高级功能，如 Oracle Real Application Cluster，请先设置标准连接，然后手动编辑 **database.properties** 文件以配置高级功能。

Configuration Manager 使用 Oracle 和 Microsoft SQL Server 的本机驱动程序。这表示在一般情况下，所有本机驱动程序的功能都是受支持的，前提是这些功能可使用数据库 URL 进行配置。 URL 位于 **database.properties** 文件中。

注意：完成安装后过程并建立正常的配置之后，请完成高级功能配置。

参数

要设置数据库连接，请定义以下参数：

参数	建议值	描述
供应商	< 用户定义 >	数据库供应商 可能值：**Oracle** 或 **Microsoft** 可使用与 Configuration Manager 相同的安装程序安装 HP Universal CMDB 或单独安装此产品。 如果使用相同安装程序在同一计算机上安装 Configuration Manager 和 UCMDB，则此参数的默认值为已在 UCMDB 安装后向导中选择的数据库供应商。 只有使用相同安装程序安装这两个应用程序时，才会设置默认值。如果使用单独的安装包执行安装，即使 UCMDB 和 Configuration Manager 安装在同一计算机上，默认值也不会出现在安装后向导中。
主机名	< 用户定义 >	数据库服务器的主机名 如果 Configuration Manager 和 UCMDB 安装在同一台计算机上，则此参数的默认值将为 UCMDB 安装后向导中已选中的数据库服务器。 **该值为必填。**

参数	建议值	描述
端口	< 用户定义 >	数据库侦听器的端口 如果 Configuration Manager 和 UCMDB 安装在同一计算机上，则此参数的默认值将为 UCMDB 安装后向导中已选中的数据库端口。 对于 Oracle，默认值为 **1521**。 对于 Microsoft SQL Server，默认值为 **1433**。 **该值为必填。**
SID/DB	< 用户定义 >	Oracle SID 的名称或 Microsoft SQL Server 数据库的名称 如果 Configuration Manager 和 UCMDB 安装在同一计算机上，则此参数的默认值将为 UCMDB 安装后向导中已选中的数据库 sid/db。 **该值为必填。**
用户名	< 用户定义 >	用于登录数据库的用户名。 **该值为必填。**
密码	< 用户定义 >	用于登录数据库的密码。

选项

还可使用以下选项：

参数	建议值	描述
加密密码	< 用户定义 >	选中此选项可加密 **database.properties** 文件中的密码。出于安全考虑，建议加密存储在文本文件中的密码。
创建架构对象	< 用户定义 >	选中此选项可创建运行 Configuration Manager 所需的架构对象。只有当安装程序使用以前创建的现有架构并用 Configuration Manager 对象填充时，才可以清除此选项。

测试

注意：强烈建议在继续操作之前先测试连接属性。

要测试连接属性，请单击 “测试” 。向导将尝试访问数据库并验证连接。测试结果将显示在 “测试” 按钮右侧。

数据库会生成各种错误消息。这些错误消息无需加以说明，通常与输入不正确的用户名或密码相关。继续操作之前，必须修正错误并得到成功的测试结果。

应用程序服务器页面

本节包括以下内容：

➤ “概述”（第 26 页）

➤ “参数”（第 26 页）

概述

使用下面显示的默认端口号设置 Configuration Manager 应用程序服务器。

参数

要设置 Configuration Manager 应用程序服务器，请定义以下参数：

参数	建议值	描述
主机名	< 用户定义 >	应用程序服务器的外部名称 默认情况下，该值是运行向导 （和 Configuration Manager）的计算机的完全限定主机名。此名称在某些部署中是不同的，如在 Configuration Manager 应用程序服务器前面对 Web 服务器进行的部署。
自定义端口	< 用户定义 >	默认情况下，不会选中此选项。选中此选项后可自定义应用程序服务器的默认端口号。

参数	建议值	描述
HTTP 端口	< 用户定义 >	Configuration Manager 应用程序服务器的 HTTP 端口 默认值为：**8080** 与 HP Universal CMDB 安装在同一计算机上之后的默认值为：**8180**
HTTPS 端口	< 用户定义 >	Configuration Manager 应用程序服务器的 HTTPS 端口 默认值为：**8443** 与 UCMDB 安装在同一计算机上之后的默认值为：**8143**
Tomcat 端口	< 用户定义 >	Configuration Manager 应用程序服务器管理端口 默认值为：**8005**
AJP 端口	< 用户定义 >	Configuration Manager 应用程序服务器 AJP （Apache Java 协议）端口 默认值为：**8009**
JMX HTTP 端口	< 用户定义 >	Configuration Manager 应用程序服务器 JMX HTTP 端口 默认值为：**39900**
JMX 远程端口	< 用户定义 >	Configuration Manager 应用程序服务器 JMX 远程端口 默认值为：**39600**

Windows 服务配置页面

选择是否作为 Windows 服务安装 Configuration Manager。只有安装在 Windows 计算机上后，此选项才可用。

可使用位于 **cnc-home/bin** 目录中的 **create-windows-service.bat** 实用程序手动设置 Windows 服务。

用户凭据页面

本节包括以下内容：

➤ “概述”（第 28 页）

概述

设置以下 Configuration Manager 初始用户：

参数	建议值	描述
管理用户	< 用户定义 >	Configuration Manager 的管理用户，也称为 “超级用户”
集成用户	< 用户定义 >	为实现集成而通过 Configuration Manager 在 HP Universal CMDB 中创建的用户

注意：必须为管理用户和集成用户提供用户名和密码凭据。

HP Universal CMDB 连接页面

本节包括以下内容：

➤ “概述”（第 28 页）
➤ “参数”（第 29 页）
➤ “测试”（第 30 页）

概述

设置与 HP Universal CMDB 的连接为可选操作。

在组合安装中将 Configuration Manager 与 UCMDB 安装在同一计算机上之后，无需在此页面中提供任何信息。

如果未在组合安装中安装 UCMDB 或将 UCMDB 安装在不同计算机上，那么即使在 localhost 上连接 UCMDB 或在安装 Configuration Manager 之前安装了 UCMDB，也必须启动 UCMDB 并提供这些链接属性。

注意：使用 UCMDB 的远程实例执行安装时，必须启动并运行该实例。如果 Configuration Manager 和 UCMDB 安装在同一计算机上，则运行此向导时必须关闭 UCMDB。

参数

要设置 UCMDB 连接，请定义以下参数：

参数	建议值	描述
在不同主机上使用 HP UCMDB	< 用户定义 >	如果 Configuration Manager 和 UCMDB 安装在不同的计算机上，则选中此选项将启用所有其他属性。
主机名	< 用户定义 >	安装了 UCMDB 的主机名
端口	< 用户定义 >	侦听 UCMDB 的端口
协议	< 用户定义 >	HTTP 或 HTTPS
客户	< 用户定义 >	UCMDB 客户
管理用户名	< 用户定义 >	UCMDB sysadmin 用户名
管理密码	< 用户定义 >	UCMDB sysadmin 密码

测试

注意：强烈建议在继续操作之前先测试连接属性。

要测试连接属性，请单击 “测试”。向导将尝试访问 UCMDB 并验证连接。测试结果将显示在 “测试”按钮右侧。

UCMDB 会生成各种错误消息。这些错误消息无需加以说明，通常与输入不正确的用户名或密码相关。继续操作之前，必须修正错误并得到成功的测试结果。

概要页面

将显示在之前的向导页面上所做的全部选择。确认所有选择是否正确，并根据需要进行更改。如果所有选择都是正确的，请单击 “下一步”，即完成向导配置任务。

完成页面

此页面是 Configuration Manager 安装后配置向导的最后一个页面。此时已完成安装后配置任务。单击 “完成”即关闭向导。

注意：虽然已成功完成所有任务，但仍建议您检查位于 **cnc-home/tmp/chp/app.log** 中的日志。

3

配置 LDAP

HP UCMDB Configuration Manager 使用 LDAP 管理用户、角色和权限。本章介绍配置 LDAP 以及排除 LDAP 故障的步骤。

本章包括以下内容：

- “LDAP 概述”（第 31 页）
- “连接到组织 LDAP”（第 32 页）
- “配置内部 （共享） LDAP”（第 38 页）
- “排除 LDAP 故障”（第 39 页）

LDAP 概述

Configuration Manager 配有内部 LDAP 服务器（在用户界面中标识为“共享”），并且还可以连接到组织的 LDAP 服务器。Configuration Manager 使用这些服务器查找用户、组和角色；存储个性化数据；以及验证用户身份。您可以选择上述哪些任务使用组织的 LDAP 服务器，哪些任务使用内部 LDAP 服务器。

典型部署将使用内部 （共享） LDAP 服务器存储角色，而其他任务使用外部 （组织） LDAP 服务器。

选择提供程序

1 以管理员用户身份登录到 **Configuration Manager**。

2 转到“管理”>“服务器管理”>“用户管理”>“用户管理配置”，并按照提供程序的首选项为下列属性选择“共享”或“外部”服务器（“共享”为默认选择）：

- 身份验证提供程序
- 组提供程序
- 个性化提供程序
- 角色提供程序
- 角色关系提供程序

3 保存配置集。

连接到组织 LDAP

HP UCMDB Configuration Manager 最初是用内部（共享）LDAP 配置的。本节描述连接到组织 LDAP 服务器的步骤。

本节包括以下内容：

- “配置 LDAP 连接”（第 33 页）
- “配置组和用户提供程序”（第 33 页）
- “激活配置集”（第 36 页）
- “为用户分配权限”（第 36 页）
- “将身份验证提供程序设置为外部 LDAP”（第 37 页）
- “导入 LDAP 证书”（第 37 页）

配置 LDAP 连接

本节介绍如何将 Configuration Manager 连接到外部 LDAP 服务器。外部 LDAP 服务器即组织 LDAP，它包含组织的用户。

1 以管理员用户身份登录到 **Configuration Manager**。

2 转到“管理”>“服务器管理”>“用户管理”>“用户管理配置”>“外部用户库”，并根据组织 LDAP 的属性更新下列属性：

常规 LDAP 连接

ldapHost：<LDAP 主机名 >

ldapPort：<LDAP 端口号 >

enableSSL：<True/false — 使用 SSL 连接到 LDAP>

useAdministrator：<True/false — 使用用户连接到 LDAP>

ldapAdministrator：<LDAP 用户名 （如果 **useAdministrator=true** 则应进行定义） >

ldapAdministratorPassword：<LDAP 用户密码 （如果 **useAdministrator=true** 则应进行定义） >

3 保存配置集。

配置组和用户提供程序

此步骤将组织 LDAP （外部库）设置为组和用户的提供程序。内部 LDAP （共享库）仍然用于身份验证，但用户和组的检索将从外部 LDAP 进行。此模式用于测试外部 LDAP 配置和分配权限给组织用户。

要设置组和用户提供程序，请执行以下操作：

1 如果尚未到达此页面，请转到“管理”>“服务器管理”>“用户管理”>“用户管理配置”>“外部用户库”。确保使用的配置集草稿与在 “配置 LDAP 连接”（第 33 页）一节保存的配置集草稿相同。

2 根据组织 LDAP 的属性更新下列属性：

a **用户搜索**

usersBase：< 用户搜索的基础 DN>

usersScope：< 用户搜索的范围 >

usersFilter：< 用户搜索的筛选器 >

b **用户对象类**（依赖于 LDAP 供应商）

usersObjectClass：< 用户 LDAP 对象类 >

usersUniqueIDAttribute：< 用户唯一 ID LDAP 属性 >

以下属性为可选属性：

usersDisplayNameAttribute：< 用户显示名称 LDAP 属性 >

usersLoginNameAttribute：< 用户登录名称 LDAP 属性 >

usersFirstNameAttribute：< 用户名 LDAP 属性 >

usersLastNameAttribute：< 用户姓 LDAP 属性 >

usersEmailAttribute：< 用户电子邮件 LDAP 属性 >

usersPreferredLanguageAttribute：< 用户首选语言 LDAP 属性 >

usersPreferredLocationAttribute：< 用户首选位置 LDAP 属性 >

usersTimeZoneAttribute：< 用户时区 LDAP 属性 >

usersDateFormatAttribute：< 用户日期格式 LDAP 属性 >

usersNumberFormatAttribute：< 用户数字格式 LDAP 属性 >

usersWorkWeekAttribute：< 用户工作周 LDAP 属性 >

usersTenantIDAttribute：< 用户租户 ID LDAP 属性 >

usersPasswordAttribute：< 用户密码 LDAP 属性 >

c 组搜索

groupsBase：< 组搜索的基础 DN>

groupsScope：< 组搜索的 LDAP 范围 >

groupsFilter：< 组搜索的筛选器 >

rootGroupsBase：< 根组搜索的基础 DN>

rootGroupsScope：< 根组搜索的 LDAP 范围 >

rootGroupsFilter：< 组搜索的筛选器 >

d 组对象类（依赖于 LDAP 供应商）

groupsObjectClass：< 组 LDAP 对象类 >

groupsMembersAttribute：< 组成员 LDAP 属性 >

以下属性为可选属性：

groupsNameAttribute：< 组唯一名称 LDAP 属性 >

groupsDisplayNameAttribute：< 组显示名称 LDAP 属性 >

groupsDescriptionAttribute：< 组描述 LDAP 属性 >

enableDynamicGroups：< 启用动态组 >

dynamicGroupsClass：< 动态组 LDAP 对象类 >

dynamicGroupsMemberAttribute：< 动态组成员 LDAP 属性 >

dynamicGroupsNameAttribute：< 动态组唯一名称 LDAP 属性 >

dynamicGroupsDisplayNameAttribute <动态组显示名称 LDAP 属性>

dynamicGroupsDescriptionAttribute：< 动态组描述 LDAP 属性 >

e 组层次结构（如果您的组织 LDAP 使用组层次结构）

enableNestedGroups：< 启用嵌套组支持 >

maximalAllowedGroupsHierarchyDepth：< 允许的最大组层次结构深度 >

f 高级配置

ldapVersion：<LDAP 版本 >

baseDistinguishNameDelimiter：< 基础 DN 分隔符 >

scopeDelimiter：< 范围分隔符 >

attributeValuesDelimiter：<LDAP 属性值分隔符 >

3 保存配置集草稿。

激活配置集

1 转到“管理”>“服务器管理”>“用户管理”>“用户管理配置”，并更新以下信息：

外部 UUM 源：True

组提供程序：外部

用户提供程序：外部

2 保存配置集，然后将其激活。

3 注销并重新启动 **Configuration Manager** 服务器。

为用户分配权限

此过程将为组织的用户分配**系统管理员**角色。具有**系统管理员**角色的用户将拥有分配相关角色给其余组织用户的权限。

1 以管理员用户身份登录到 **Configuration Manager**。

2 打开 “用户管理”模块 （“管理”>“用户管理”）。

3 确认可以看见组织 LDAP 中的组和用户。

4 转到 “用户管理”>“搜索用户”窗格，并搜索将充当管理员的用户 — 例如：名 = j*，姓 = Smith。

5 为这些用户添加**系统管理员**角色。

将身份验证提供程序设置为外部 LDAP

此过程将外部组织 LDAP 设置为身份验证提供程序，因此组织用户将用于身份验证。

1 转到“管理”>“服务器管理”>“用户管理”>“用户管理配置”，并更新以下信息：

身份验证提供程序：外部

2 保存配置集，然后将其激活。

3 注销并重新启动 **Configuration Manager** 服务器。

4 使用配有**系统管理员**角色的其中一个组织用户进行登录。

导入 LDAP 证书

如果连接到组织 LDAP 需要使用证书，请执行以下步骤：

1 将证书导出至文件。

2 停止 Configuration Manager Windows 服务。

3 运行以下命令：

<Configuration Manager 安装 >\java\windows\x86_64\bin\keytool.exe -import -trustcacerts -alias < 证书别名 > -keystore <Configuration Manager 安装 >\java\windows\x86_64\lib\security\cacerts -storepass changeit -file < 证书文件路径 >

4 启动 Configuration Manager Windows 服务。

配置内部 （共享） LDAP

变更内部 （共享） LDAP 服务器密码 （可选）

出于安全考虑，您可以变更内部 （共享） LDAP 服务器的密码。

1 登录到 **HPUniversal CMDBConfiguration Manager**。

2 打开命令行，并导航到 **<Configuration Manager 安装 >\ldap\serverRoot\bat** 文件夹。

3 执行 **ldappasswordmodify -h localhost -p <LDAP 端口 > -D "cn=Directory Manager" -w <LDAP 管理密码> -c <LDAP 管理密码> -n < 新 LDAP 管理密码>**。

   a 默认 LDAP 管理密码为 **ldapadmin**。

   b 默认端口为 **2389**。

   c 确认命令成功执行后，继续执行以下步骤。

4 在 **UCMDB Configuration Manager** 中，选择“管理”>“服务器管理”>“用户管理”>“用户管理配置”>“共享用户库”。

5 更新 **ldapAdministratorPassword** 属性中的密码。

6 保存配置集，然后将其激活。

7 注销 **UCMDB Configuration Manager**。

8 重新启动 **UCMDB Configuration Manager** 服务器。

配置内部 （共享） LDAP 端口

默认端口 2389 可能已经被另一个应用程序使用。要更改此默认端口，请执行以下步骤。

要配置内部 LDAP 端口，应：

1 打开命令行，并导航到 **<Configuration Manager 安装 >\ldap\serverRoot\bat** 文件夹。

2 执行以下命令：
dsconfig -h localhost -p 2444 -D "cn=directory manager" -w <LDAP 管理密码> --trustAll -X -n set-connection-handler-prop --handler-name "LDAP Connection Handler" --set listen-port:< 新端口 >

默认 <LDAP 管理密码 > 为 **ldapadmin**。

3 确认没有显示错误消息后，才可以继续下列步骤。

4 登录到 HP Universal CMDB Configuration Manager。

5 在 UCMDB Configuration Manager 中，选择 “管理” > “服务器管理” > “用户管理” > “用户管理配置” > “共享用户库”，并更新 **ldapPort** 属性中的端口号。

6 保存配置集，然后将其激活。

7 注销 UCMDB Configuration Manager。

8 重新启动 UCMDB Configuration Manager 服务器。

排除 LDAP 故障

问题：无法建立与 LDAP 服务器的通信。日志中出现通信异常。

解决办法：检查 LDAP 主机、端口和 SSL 模式设置：

a 检查 LDAP 主机和端口的配置是否正确：
选择 “管理” > “服务器管理” > “用户管理” > “用户管理配置” > “外部用户库”，并检查 **ldapHost**、 **ldapPort** 设置。

b 检查 SSL 模式的配置是否正确。与组织的 LDAP 管理员核实 LDAP 连接是否需要管理员用户来执行。选择 “管理” > “服务器管理” > “用户管理” > “用户管理配置” > “外部用户库”，并检查 **enableSSL** 设置。

c 检查是否安装了适当的服务器证书。运行以下命令：

<Configuration Manager 安装>\java\windows\x86_64\bin\keytool.exe -list -trustcacerts [-alias <证书别名>] -keystore <Configuration Manager 安装>\java\windows\x86_64\lib\security\cacerts -storepass changeit

d 与组织的 LDAP 管理员核实 LDAP 连接是否需要管理员来执行。选择 “管理”>“服务器管理”>“用户管理”>“用户管理配置”>“外部用户库”，并检查以下设置：**useAdministrator**、**ldapAdministrator**、**ldapAdministratorPassword**

问题：用户或组的管理屏幕上没有出现组。日志中没有出现异常。

解决办法：检查以下信息：

a 检查用户和组的搜索筛选器是否配置正确：选择 “管理”>“服务器管理”>“用户管理”>“用户管理配置”>“外部用户库”，并修改以下属性：**usersBase**、**usersScope**、**usersFilter**、**groupsBase**、**groupsScope**、**groupsFilter**、**rootGroupsBase**、**rootGroupsScope**、**rootGroupsFilter**

b 打开 LDAP 客户端浏览器，并查看基础 DNS 下的用户。

问题：UI 太慢。

解决办法：通常是因为在 LDAP 中配置了过多的组或用户。按下述操作配置基础 DNS 和筛选器以减少相关子集的组数量：

a 选择 “管理”>“服务器管理”>“用户管理”>“用户管理配置”>“外部用户库”

b 修改以下设置：**usersBase**、**usersScope**、**usersFilter**、**groupsBase**、**groupsScope**、**groupsFilter**、**rootGroupsBase**、**rootGroupsScope**、**rootGroupsFilter**

问题：某些已知用户没有出现在组或用户的管理屏幕上。

解决办法：用户和组的管理屏幕上仅显示属于某些组的用户。为了便于在主屏幕上查看，请将用户放入 LDAP 中的适当组中。

问题：登录时间很长。

解决办法：用户可能属于太多的组。通过更改组搜索筛选器可以优化启动时间，这样便可以减少返回的组数量，如下所述：

a 选择“管理”>“服务器管理”>“用户管理”>“用户管理配置”>“外部用户库”

b 修改 **groupsFilter** 设置。

4

轻型单一登录身份验证 (LW-SSO) – 一般参考

本章包括以下内容：

➤ “LW-SSO 身份验证概述”（第 43 页）

➤ “LW-SSO 安全警告”（第 45 页）

“疑难解答和限制”（第 47 页）

LW-SSO 身份验证概述

LW-SSO 是一种访问控制方法，用户一次登录便可访问多个软件系统的资源，而不会出现再次登录的提示。软件系统的已配置组内的应用程序均信任该身份验证，而且从一个应用程序进入另一个应用程序时，无需再进行身份验证。

本节中的信息适用于 LW-SSO 版本 2.2 和 2.3。

本节包括以下主题：

➤ “LW-SSO 令牌到期”（第 44 页）

➤ “建议的 LW-SSO 令牌到期配置”（第 44 页）

➤ “GMT 时间”（第 44 页）

➤ “多域功能”（第 44 页）

➤ “获取 URL 功能的 SecurityToken”（第 44 页）

LW-SSO 令牌到期

LW-SSO 令牌的到期值可确定应用程序会话的有效性。因此，此到期值至少应等于应用程序会话到期值。

建议的 LW-SSO 令牌到期配置

每个使用 LW-SSO 的应用程序都应当配置令牌到期。建议值为 60 分钟。对于不需要高级别安全性的应用程序，可将到期值配置为 300 分钟。

GMT 时间

所有参与 LW-SSO 集成的应用程序都必须使用相同的 GMT 时间，并且最大差值为 15 分钟。

多域功能

如果必须与不同 DNS 域中的应用程序集成，则多域功能要求所有参与 LW-SSO 集成的应用程序都配置 trustedHosts 设置 （或 **protectedDomains** 设置） 。此外，它们还必须在配置的 **lwsso** 元素中添加正确的域。

获取 URL 功能的 SecurityToken

要接收来自其他应用程序且作为 **URL 的 SecurityToken** 发送的信息，主机应用程序应当在配置的 **lwsso** 元素中配置正确的域。

LW-SSO 安全警告

本节描述与 LW-SSO 配置相关的安全警告：

➤ **LW-SSO 中的机密 InitString 参数。** LW-SSO 使用 “对称加密”验证并创建 LW-SSO 令牌。配置中的 **initString** 参数用于初始化密钥。当某个应用程序创建令牌后，每个使用相同 initString 参数的应用程序都将验证该令牌。

警告：

➤ 在未设置 **initString** 参数的情况下，无法使用 LW-SSO。

➤ **initString** 参数属于机密信息，并且在进行发布、传输以及保持持久性方面也应作为机密信息处理。

➤ 只能在使用 LW-SSO 互相集成的应用程序之间共享 **initString** 参数。

➤ **initString** 参数的最小长度应为 12 个字符。

➤ **仅在需要时启用 LW-SSO。**除非明确指定使用，否则应禁用 LW-SSO。

➤ **身份验证安全级别。**使用最弱的身份验证框架并且发布受其他集成应用程序信任的 LW-SSO 令牌的应用程序将确定所有应用程序的身份验证安全级别。

建议只允许使用了较强且安全的身份验证框架的应用程序发布 LW-SSO 令牌。

- **对称加密的含义。** LW-SSO 使用对称加密发布和验证 LW-SSO 令牌。因此，任何使用 LW-SSO 的应用程序都可以发布受到共享 **initString** 参数的所有其他应用程序信任的令牌。而潜在的风险与以下两种情况有关：共享 initString 的应用程序驻留在不受信任的位置，或者可从不受信任的位置访问该应用程序。

- **用户映射 （同步）。** LW-SSO 框架无法确保集成应用程序之间的用户映射。因此，集成的应用程序必须监控用户映射。建议在所有集成的应用程序中共享同一个用户注册表 （作为 LDAP/AD）。

  用户映射失败可能会导致安全违反以及应用程序行为不正常。例如，相同的用户名可能会分配给各种应用程序中的不同真实用户。

  此外，如果用户登录到某个应用程序 (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)，则用户映射失败之后将强制用户手动登录到 AppB 并输入用户名。如果用户输入的用户名与之前登录到 AppA 时使用的用户名不同，将出现以下情况：如果用户随后从 AppA 或 AppB 访问第三个应用程序 (AppC)，则登录到 AppA 或 AppB 时分别使用的用户名将用来访问 AppC。

- **身份管理器**。用于身份验证，“身份管理器”中所有不受保护的资源都必须在 LW-SSO 配置文件中使用 **nonsecureURLs** 设置进行配置。

疑难解答和限制

已知问题

本节描述 LW-SSO 身份验证的已知问题。

➤ **安全上下文。** LW-SSO 安全上下文对于每个属性名称仅支持一个属性值。

因此，当 SAML2 令牌为同一个属性名称发送多个值时， LW-SSO 框架将只接受一个值。

同样，即使 IdM 令牌配置为向同一属性名称发送多个值，LW-SSO 框架也只接受一个值。

➤ **使用 Internet Explorer 7 时的多域注销功能**。在下列情况下，多域注销功能有可能失败：

➤ 使用的浏览器是 Internet Explorer 7，应用程序将在注销过程中调用三个以上连续的 HTTP 302 重定向谓词。

在这种情况下， Internet Explorer 7 可能会错误地处理 HTTP 302 重定向响应，并转而显示 “Internet Explorer 无法显示网页”错误页面。

如有可能，建议按注销顺序减少应用程序重定向命令作为应对方案。

限制

使用 LW-SSO 身份验证时，请注意以下限制：

➤ **客户端对应用程序的访问**。

如果在 LW-SSO 配置中定义域：

➤ 应用程序客户端必须在登录 URL 中使用完全限定域名 (FQDN) 访问应用程序，例如， http://myserver.**companydomain**.com/WebApp。

➤ LW-SSO 无法支持使用 IP 地址的 URL，例如，http://192.168.12.13/WebApp。

- LW-SSO 无法支持不包含域的 URL，例如， http://myserver/WebApp。

如果未在 LW-SSO 配置中定义域：客户端可通过不包含 FQDN 的登录 URL 访问应用程序。在这种情况下，将专门为不包含域信息的单个计算机创建 LW-SSO 会话 cookie。因此，不会通过浏览器将此 cookie 委托给其他 cookie，也不会将其传送到位于同一 DNS 域中的其他计算机上。这意味着 LW-SSO 在相同的域中不起作用。

- **LW-SSO 框架集成。**只有事先在 LW-SSO 框架中集成之后，应用程序才能利用和使用 LW-SSO 功能。
- **多域支持**。
  - 由于多域功能基于 HTTP 引用网站，因此，LW-SSO 支持应用程序之间的链接，不支持在浏览器窗口中键入 URL，除非两个应用程序在同一个域中。
  - 第一个使用 **HTTP POST** 的跨域链接不受支持。

    多域功能不支持发送给第二个应用程序的第一个 **HTTP POST** 请求（仅支持 **HTTP GET** 请求）。例如，如果应用程序具有指向第二个应用程序的 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 可以从某个域的某个应用程序传送到其他域的其他应用程序的信息大小限于 15 组 / 角色 / 属性（请注意，每项的平均长度可以为 15 个字符）。

- 在多域情形下从受保护 (HTTPS) 页面链接不受保护 (HTTP) 页面：

  从受保护 (HTTPS) 页面链接不受保护 (HTTP) 页面时，多域功能无法正常工作。这是浏览器的限制问题：其中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，请访问：
  http://support.microsoft.com/support/kb/articles/Q178/0/66.ASP

- **SAML2 令牌。**
  - 如果使用 SAML2 令牌，则注销功能不受支持。

    因此，如果使用 SAML2 令牌访问第二个应用程序，则在第一个应用程序注销的用户无法从第二个应用程序注销。

  - SAML2 令牌的到期时间不会反映在应用程序的会话管理中。

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

- **JAAS 领域。**不支持 Tomcat 中的 JAAS 领域。
- **在 Tomcat 目录中使用空格。**不支持在 Tomcat 目录中使用空格。

  如果 Tomcat 安装路径 （文件夹）中包含空格 （例如， Program Files），而且 LW-SSO 配置文件位于 **common\classes** Tomcat 文件夹中，则无法使用 LW-SSO。

- **负载平衡器配置。**使用 LW-SSO 部署的负载平衡器必须配置为使用粘性会话。

5

身份管理器身份验证

本章包括以下内容：

- “接受身份管理器身份验证”（第 51 页）
- “使用 Java 连接器将 Configuration Manager 的身份管理功能配置为与 Windows 2003 操作系统上的 IIS6 结合使用的示例”（第 53 页）

接受身份管理器身份验证

如果使用身份管理器并且打算添加 HP Universal CMDB Configuration Manager，则必须执行此任务。

此任务描述如何配置 HP Universal CMDB Configuration Manager 以接受身份管理器身份验证。

此任务包括以下步骤：

- “先决条件”（第 51 页）
- “配置 HP Universal CMDB Configuration Manager 以接受身份管理器”（第 52 页）

先决条件

Configuration Manager Tomcat 服务器应通过 Tomcat Java (AJP13) 连接器连接到由身份管理器保护的 Web 服务器 （IIS 或 Apache）。

有关使用 Tomcat Java (AJP13) 连接器的说明，请参阅 Tomcat Java (AJP13) 文档。

配置 HP Universal CMDB Configuration Manager 以接受身份管理器

要使用 IIS6 配置 Tomcat Java (AJP13)，请执行以下操作：

1 将身份管理器配置为发送包含用户名并请求标头名称的个性化标头 / 回调。

2 打开 **<Configuration Manager 安装目录>\conf\lwssofmconf.xml** 文件，并定位到以 **in-ui-identity-management** 开头的部分。

例如：

```
<in-ui-identity-management enabled="false">
    <identity-management>
     <userNameHeaderName>sm-user</userNameHeaderName>
    </identity-management>
</in-ui-identity-management>
```

a 通过删除注释字符激活该功能。

b 将 **enabled="false"** 替换为 **enabled="true"**。

c 将 **sm-user** 替换为步骤 1 中请求的标头名称。

3 打开 **<Configuration Manager 安装目录>\conf\client-config.properties** 文件，并编辑以下属性：

a 将 **bsf.server.url** 更改为身份管理器 URL，并将端口更改为身份管理器端口：

bsf.server.url=http://<身份管理器 URL>:<身份管理器端口>/bsf

b 将 **bsf.server.services.url** 更改为 HTTP 协议，并将端口更改为原始 Configuration Manager 端口：

bsf.server.services.url=http://<Configuration Manager URL>:<Configuration Manager 端口 >/bsf

使用 Java 连接器将 Configuration Manager 的身份管理功能配置为与 Windows 2003 操作系统上的 IIS6 结合使用的示例

此示例任务描述如何安装和配置 Java 连接器，以用它将身份管理配置为将 Configuration Manager 与运行于 Windows 2003 操作系统上的 IIS6 结合使用。

要安装 Java 连接器，并将其配置为使用 Windows 2003 上的 IIS6，请执行以下操作：

1 从 Apache 网站下载最新版本的 Java 连接器 （例如， **djk-1.2.21**）。

   a 单击 **http://www.apache.org/dist/tomcat/tomcat-connectors/jk/binaries/win64/**。

   b 选择最新版本。

   c 从 **amd64** 目录下载 **isapi_redirect.dll** 文件。

2 将此文件存储在 **<Configuration Manager 安装目录>\tomcat\bin\win32** 下。

3 在包含 isapi_redirect.dll 的相同目录中创建名为 **isapi_redirect.properties** 的新文本文件。

   此文件的内容为：

   # Configuration file for the Jakarta ISAPI Redirector

   # The path to the ISAPI Redirector Extension, relative to the website

   # This must be in a virtual directory with execute privileges

   extension_uri=/jakarta/isapi_redirect.dll

   # Full path to the log file for the ISAPI Redirector

   log_file=<Configuration Manager Install Directory>\servers\server-0\logs\isapi.log

   # Log level (debug, info, warn, error or trace)

   log_level=info

   # Full path to the workers.properties file

worker_file==<Configuration Manager Install Directory>\tomcat\conf\workers.properties.minimal

Full path to the uriworkermap.properties file

worker_mount_file==<Configuration Manager Install Directory>\tomcat\conf\uriworkermap.properties

4 在 **<Configuration Manager 安装目录>\tomcat\conf** 中创建名为 **workers.properties.minimal** 的新文本文件。

此文件的内容为：

workers.properties.minimal -

#

This file provides minimal jk configuration

properties needed to

connect to Tomcat.

#

Defining a worker named ajp13w and of type ajp13

Note that the name and the type do not have to

match.

worker.list=ajp13w

worker.ajp13w.type=ajp13

worker.ajp13w.host=localhost

worker.ajp13w.port=8009

#END

5 在 **<Configuration Manager 安装目录>\tomcat\conf** 中创建名为 **uriworkermap.properties** 的新文本文件。

此文件的内容为：

uriworkermap.properties - IIS

#

This file provides sample mappings for example:

```
# ajp13w worker defined in workermap.properties.minimal
# The general syntax for this file is:
# [URL]=[Worker name]

/cnc=ajp13w
/cnc/*=ajp13w
/bsf=ajp13w
/bsf/*=ajp13w
#END
```

重要信息：请注意， Configuration Manager 必须具有两个规则。新语法允许将这两个规则合并为一个，例如：

/cnc|/*=ajp13w

---

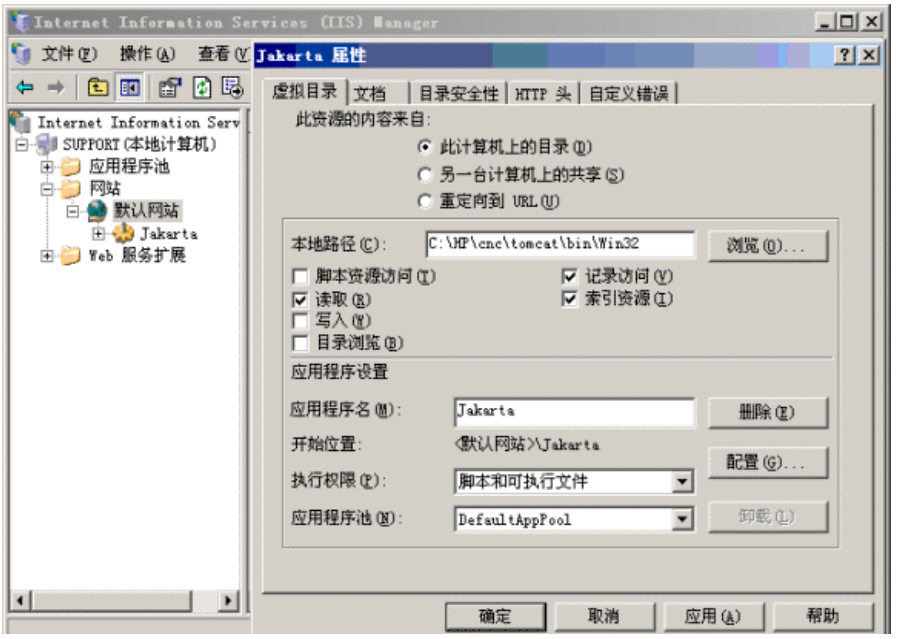
6 在 IIS 配置的相应网站对象中创建虚拟目录。

a 在 Windows“开始”菜单中，打开**设置 \ 控制面板 \ 管理工具 \Internet 信息服务 (IIS) 管理器**。

b 在右窗格中，右键单击 **< 本地计算机名称 >\ 网站 \< 用户网站名称 >**，然后选择**新建 \ 虚拟目录**。

c 将目录别名命名为 **Jakarta**，并将本地路径设置为包含 isapi_redirect.dll 的目录。

管理器的窗口类似于下图：



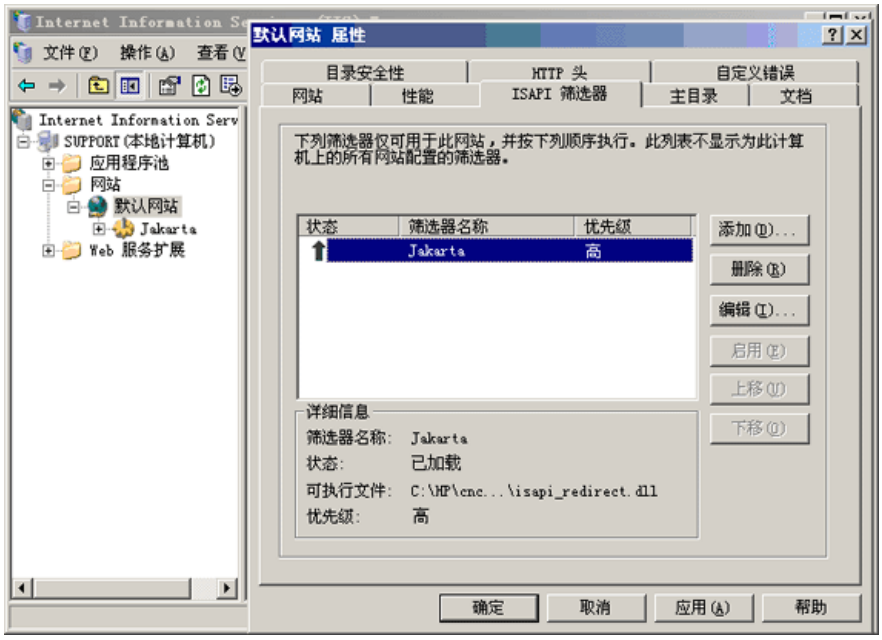
7 添加 **isapi_redirect.dll** 作为 ISAPI 筛选器。

a 右键单击 < **用户网站名称** >，并选择 “属性”。

b 选择 “ISAPI 筛选器”选项卡，然后单击 “添加 ...”按钮。

c 选择 **Jakarta** 作为筛选器名称，并浏览到 **isapi_redirect.dll**。筛选器已添加，但仍处于非活动状态。

配置窗口类似于下图：



d 单击 “应用”按钮。

8 定义并允许新 Web 服务扩展。

a 右键单击 < **本地计算机名称** >**Web 服务扩展**条目，然后选择“添加新 Web 服务扩展 ...”菜单项。

b 将新 Web 服务扩展命名为 **Jakarta**，并浏览到 **isapi_redirect.dll** 文件。

注意：单击 “确定”按钮之前，请选中 “设置扩展状态为允许”复选框。

9 重新启动 IIS Web 服务器，并通过 Web 服务访问应用程序。

6

登录到 Configuration Manager

本章包括以下内容：

➤ “访问 Configuration Manager”（第 59 页）

➤ “如何访问 Configuration Manager”（第 60 页）

➤ “访问 Configuration Manager 的 JMX 控制台”（第 61 页）

“疑难解答和限制”（第 61 页）

访问 Configuration Manager

在与 Configuration Manager 服务器之间具有网络连接（Intranet 或 Internet）的计算机上，可使用受支持的 Web 浏览器访问 Configuration Manager。授予用户的访问级别取决于用户的权限。有关授予用户权限的详细信息，请参阅 《HP Universal CMDB Configuration Manager 用户指南》中的 “用户管理”。

有关 Web 浏览器要求的详细信息以及成功查看 Configuration Manager 的最低要求，请参阅 “Configuration Manager 系统要求”（第 8 页）。

有关安全访问 Configuration Manager 的详细信息，请参阅“强化”（第 69 页）。

如何访问 Configuration Manager

在 Web 浏览器中，输入 Configuration Manager 服务器的 URL，例如，**http://< 服务器名称或 IP 地址 >.< 域名 >:< 端口 >**，其中 **< 服务器名称或 IP 地址 >.< 域名 >** 表示 Configuration Manager 服务器的完全限定域名 (FQDN)，**< 端口 >** 表示在安装期间选择的端口。

登录到 Configuration Manager

1. 输入在 Configuration Manager 安装后向导中定义的用户名和密码。
2. 单击 “登录”。登录之后，用户名将显示在屏幕的右上角。
3. （建议）连接到组织 LDAP 服务器并将管理角色分配给 LDAP 用户以便 Configuration Manager 管理员能够访问系统。有关在 Configuration Manager 系统中为用户分配角色的详细信息，请参阅《HP Universal CMDB Configuration Manager 用户指南》中的 “用户管理”。

注销

建议您在完成会话之后从该网站中注销以防未经授权的进入。

要注销，请执行以下操作：

单击页面顶部的 “注销”。

注意：默认的会话过期时间为 30 分钟。

访问 Configuration Manager 的 JMX 控制台

为了进行故障排除或修改某些配置，可能需要访问 JMX 控制台。

要访问 JMX 控制台，请执行以下操作：

1. 打开位于 http://< 服务器名称或 IP 地址 >:< 端口 >/cnc/jmx-console 的 JMX 控制台。端口是指在安装 Configuration Manager 的过程中配置的端口。
2. 输入默认用户凭据。它们与登录到 Configuration Manager 所用的用户凭据相同。

疑难解答和限制

问题：变更 “服务器管理”中的配置集后，服务器无法启动。

解决办法：还原为以前的配置集。请按以下步骤操作：

1. 运行下面的命令查找上次激活的配置集的 ID：

   <HP Universal CMDB Configuration Manager>\bin\export-cs.bat < 数据库属性 > --history

   其中， < **数据库属性** > 可通过指向 <**Configuration Manager 安装目录** >**conf\database.properties** 文件的位置或指定各个数据库属性来指定。例如：

   cd <HP Universal CMDB Configuration Manager>\bin export-cs.bat -p ..\conf\database.properties --history

2. 运行下面的命令以导出上一个配置集：

   <HP Universal CMDB Configuration Manager>\bin\export-cs.bat < 数据库属性 > < 配置集 ID> < 转储文件名 >

其中，< **配置集 ID**> 是上一步中的配置集 ID，< **转储文件名** > 是用于存储配置集的临时文件的名称。例如，要将 ID 为 **491520** 的配置集导出到 **mydump.zip** 文件，请输入以下命令：

```
cd <HP Universal CMDB Configuration 安装主页 >\bin export-cs.bat -p
..\conf\database.properties -i 491520 -f mydump.zip
```

3 停止 HP Universal CMDB Configuration Manager 服务。

4 运行以下命令以导入并激活上一个配置集：

```
<HP Universal CMDB Configuration Manager>\bin\import-cs.bat < 数据库
属性 > < 转储文件名 > --activate
```

问题：UCMDB 连接出现错误。

解决办法：可能是下列一种原因造成：

- UCMDB 服务器已停止。待 UCMDB 完全启动（验证 UCMDB 服务器状态是否为 “启动”）后，重新启动 Configuration Manager。
- UCMDB 服务器已启动但 Configuration Manager 连接凭据或 URL 错误。启动 Configuration Manager。转到 “服务器管理”，更改 UCMDB 的连接设置，并保存新的配置集。激活该配置集并重新启动服务器。

问题：LDAP 连接设置错误。

解决办法：还原为以前的配置集。设置正确的 LDAP 连接设置，并激活新的配置集。

问题：Configuration Manager 中未检测到 UCMDB 类模型的变更。

解决办法：重新启动 Configuration Manager 服务器。

问题：Configuration Manager 日志中包含 “UCMDB 执行超时时间已到” 错误。

解决办法：当 UCMDB 数据库过载时，就会出现此问题。要更正此错误，请按下述步骤增加连接超时时间：

1 在 **UCMDBServer\conf** 文件夹中创建文件 jdbc.properties。

2 输入文本：QueryTimeout=< 秒数 >。

3 重新启动 UCMDB 服务器。

问题：Configuration Manager 不允许您添加要管理的视图。

解决办法：添加要管理的视图时，会在 UCMDB 中创建一个新的 TQL。如果达到活动 TQL 的最大限量，则无法添加视图。要增加 UCMDB 中活动 TQL 的限量，可通过在基础结构设置管理器中更改下列设置实现：

- 服务器中活动 TQL 的最大数量
- 客户活动 TQL 的最大数量

问题：HTTPS 服务器证书无效。

解决办法：可能是下列一种原因造成：

- 已过了证书的验证日期。需要获取新证书。
- 证书上的证书颁发机构不是受信任的机构。将证书颁发机构添加到受信任的根证书颁发机构列表。

问题：从 Configuration Manager 登录页面登录后，会出现登录错误或拒绝访问页面。

解决办法：可能是下列一种原因造成：

- 可能未在身份验证提供程序（外部 / 共享 LDAP）中定义用户名。在身份验证提供程序系统中添加用户。
- 已定义用户，但不具有 Configuration Manager 的登录权限。授予用户登录权限。最佳解决办法是将登录权限分配给所有 Configuration Manager 用户的根组。
- 这些解决办法还适用于 IDM 系统登录失败的情况。

问题：由于输入的数据库凭据不正确，Configuration Manager 服务器无法启动。

解决办法：如果对数据库凭据进行了更改，但服务器仍然无法启动，则凭据可能是错误的。（**注意：**安装后向导不会自动测试输入的凭据。必须单击向导中的“测试”按钮。）需要重新加密数据库密码并在配置文件中输入新凭据。请按以下步骤操作：

1 从命令行运行以下命令，以加密更新的数据库密码：

<Configuration Manager (CnC) 安装文件夹 >\bin\encrypt-password.bat – p < 密码 >

此操作将返回加密后的密码。

2 将加密后的密码（包括 {ENCRYPTED} 前缀）复制到 **<CnC 安装文件夹 >\conf\database.properties** 中的 **db.password** 参数中。

问题：如果 DNS 配置不正确，则可能需要使用服务器 IP 地址登录。输入 IP 地址之后，发生第二次 DNS 错误。

解决办法：再次用 IP 地址替换计算机名称。例如：

如果登录时使用的 IP 地址为 http://16.55.245.240:8180/cnc/

并且获取显示 DNS 错误并包含计算机名称的地址，如：
http://my.example.com:8180/bsf/secure/authenicationPointURL.jsp...

则将此地址替换为
http://10.0.0.1:8180/bsf/secure/authenicationPointURL.jsp...

并在浏览器中再次启动应用程序。

问题：无法启动 Configuration Manager Tomcat 服务器。

解决办法：请尝试下列一项操作：

- 运行安装后向导并替换 Configuration Manager 服务器端口。
- 中止占用 Configuration Manager 端口的其他进程。
- 在 Configuration Manager 配置文件中手动更改端口，方法是编辑文件：**<CnC 安装文件夹>\servers\server-0\conf\server.xml** 并更新相关端口：
  - HTTP (8080)：第 69 行
  - HTTPS (8443)：第 71 和 90 行

问题：在 Configuration Manager 日志中发现内存不足的错误。

解决办法：根据需要增加 Java 最大内存量。

要在 Configuration Manager 服务中更改内存大小，请执行以下操作：

1. 转到 **<CnC 安装文件夹>\cnc\bin** 目录，并执行命令：edit-server-0.bat。
2. 选择 **Java** 选项卡。
3. 更新 “初始内存池”和 “最大内存池”参数。

要在批处理文件中更改内存大小，请执行以下操作：

1. 转到 **<CnC 安装文件夹>\cnc** 目录，并打开要编辑的 **start-server-0.bat** 文件
2. 定位到以 **SET JAVA_OPTS=-Dcnc.home** 开头的行。

3 找到 **-Xms** 和 **-Xmx** 命令，并按照以下要求进行更改：

-Xms< 初始内存池大小 > -Xmx< 最大内存池大小 >

例如：要将初始内存池设置为 100MB，最大内存池设置为 800 MB，请输入：

-Xms100m -Xmx800m

问题：单击 “完成”之后，安装后向导需要运行很长时间。

解决办法：对于没有预先配置为合并模式的 UCMDB 系统，可能需要较长时间执行合并架构的操作 （取决于数据量）。请等待 15 分钟。如果发现没有任何进展，则中止安装后向导，并重新启动进程。

问题：UCMDB 中 CI 的变更未反映在 Configuration Manager 中。

解决办法：Configuration Manager 运行脱机异步分析过程。该过程可能尚未处理 UCMDB 中最新的变更。要解决此问题，请尝试以下一项操作：

- 等待几分钟时间。两次分析过程执行之间的默认时间间隔为 10 分钟。该时间间隔可在 “服务器管理”模块中配置。
- 执行 JMX 调用以便对相关视图运行脱机分析计算。
- 转到 “策略管理”。单击 “重新计算策略分析”按钮。这将为所有视图调用脱机分析过程 （可能需要一些时间）。还可能需要对某个策略进行人工变更并进行保存。

问题：单击 “管理” > “打开 UCMDB”时，出现 UCMDB 登录页面。

解决办法：如果希望不再次登录而访问 UCMDB，则需要启用单一登录。有关详细信息，请参阅 “启用轻型单一登录”（第 18 页）。另外，请确保 UCMDB 用户管理系统中定义了登录的 Configuration Manager 用户。

问题：在安装后向导中将 UCMDB 连接配置为 IPv6 地址之后，无法使用菜单项“管理” > “打开 UCMDB”。

解决办法：请按以下步骤操作：

1. 转到“管理”>“服务器管理”>“Configuration Manager”>“UCMDB 连接”。
2. 将方括号添加到 UCMDB 访问 URL 中的 IP 地址。该 URL 应当像这样：http://[x:x:x:x:x:x:x:x]:8080/。
3. 保存并激活配置集。
4. 重新启动 Configuration Manager。

以下限制适用于使用 Configuration Manager 的情况：

- 一旦更改了 Configuration Manager Tomcat 服务器上的时间，就必须重新启动服务器以便更新服务器上的时间。

7

强化

本章包括以下内容：

- “强化 Configuration Manager”（第 69 页）
- “加密数据库密码”（第 71 页）
- “使用自签名证书在服务器计算机上启用 SSL”（第 72 页）
- “使用证书颁发机构颁发的证书在服务器计算机上启用 SSL”（第 74 页）
- “使用客户端证书启用 SSL”（第 76 页）
- “仅为身份验证启用 SSL”（第 77 页）
- “启用客户端证书身份验证”（第 78 页）
- “加密参数”（第 79 页）

强化 Configuration Manager

本节介绍安全 Configuration Manager 应用程序的概念，并讨论实现安全所需的计划和体系结构。强烈建议您在继续后续各节的强化讨论前先阅读本节内容。

Configuration Manager 的设计思路是可将其作为安全体系结构的一部分，因此能够应对处理它可能面临的安全威胁的挑战。

强化准则规定了执行更安全 （强化） Configuration Manager 所需的配置。

提供的强化信息主要面向 Configuration Manager 管理员，便于他们在开始强化过程之前熟悉强化设置和建议。

下面是建议您在强化系统时要做的准备工作：

- 评估常规网络的安全风险 / 安全状态，并在决定以最佳方式将 Configuration Manager 集成到网络时利用所得出的结论。
- 提高对 Configuration Manager 技术框架和 Configuration Manager 安全功能的了解。
- 审核所有强化准则。
- 开始强化过程之前先验证 Configuration Manager 是否完全正常工作。
- 遵照各节中以时间顺序排列的强化过程步骤。

重要信息：

- 强化过程假定您仅执行这些章节中提供的说明，而不会实施别的地方记述的其他强化步骤。
- 当强化过程着眼于特定分布式体系结构时，并不表示这是适合您组织需要的最佳体系结构。
- 我们假定后续各节所述步骤将在专用于 Configuration Manager 的计算机上执行。将这类计算机用于 Configuration Manager 以外的目的可能会导致结果出现问题。
- 本节中提供的强化信息不可作为评估计算机化系统的安全风险的指导。

加密数据库密码

数据库密码存储在 **<Configuration Manager 安装目录>\conf\database.properties** 文件中。如果要对密码进行加密，则默认加密算法符合 FIPS 140-2 标准。要加密数据库密码，请在 Configuration Manager 安装后向导的“数据库配置”页面中选中 “加密密码”复选框。

加密是通过对密码进行加密的密钥完成的。此密钥自身会由另一个称为主密钥的密钥加密。两个密钥使用相同的算法进行加密。有关加密过程中使用的参数的详细信息，请参阅 “加密参数”（第 79 页）。

警告：如果更改加密算法，则所有以前加密的密码将不再可用。

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\encryption.properties** 文件，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大小。
2. 运行 **generate-keys.bat** 脚本，此脚本创建以下目录：**cnc\security\encrypt_repository** 并生成加密密钥。
3. 重新运行安装后向导。

使用自签名证书在服务器计算机上启用 SSL

以下各节说明如何配置 Configuration Manager，以便使用安全套接字层 (SSL) 通道支持身份验证和加密。

Configuration Manager 使用 Tomcat 6.0 作为应用程序服务器。

注意：所有目录和文件位置取决于特定平台、操作系统和安装首选项。

---

1 先决条件

开始下述过程之前，先删除位于 **<Configuration Manager 安装目录 >\java\lib\security\tomcat.keystore** 中的旧 **tomcat.keystore** 文件。

2 生成服务器密钥库

使用自签名证书和匹配的私钥创建密钥库 （JKS 类型）：

➤ 从 **<Configuration Manager 安装目录 >** 中 Java 安装程序的 bin 目录中，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。如果密码发生变更，请在文件中手动更改。

➤ 回答问题**您的姓名？**输入 Configuration Manager Web 服务器名称。按照组织要求输入其他参数。

➤ 输入密钥密码。密钥密码必须与密钥库密码相同。

名称为 **tomcat.keystore** 的 JKS 密钥库即创建完成，服务器证书名为 **hpcert**。

3 将证书放置于客户端的受信任存储中

生成 **tomcat.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与 Configuration Manager 通过 SSL 通信的客户端，请将此证书置于客户端的受信任存储中。

限制：在 **tomcat.keystore** 中只能有一个服务器证书。

---

4 验证客户端配置设置

打开位于 **<Configuration Manager 安装目录 >** 的 **conf** 目录中的 **client-config.properties** 文件。将协议设置为 **https**，端口设置为 **8443**。

5 修改 server.xml 文件

打开位于 **<Configuration Manager 安装目录 >** 的 **conf** 目录中的 **server.xml** 文件。定位到开头为

Connector port="8443"

的部分 （出现在注释中）。通过删除注释字符激活脚本，并添加以下两行：

keystoreFile="<tomcat.keystore 文件位置 >"（请参阅步骤 2 （第 72 页））

keystorePass="< 密码 >"

6 重新启动服务器

7 验证服务器安全性

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 >:8443/cnc**。

提示：如果未能建立连接，请尝试使用其他浏览器或将当前浏览器升级到新版本。

使用证书颁发机构颁发的证书在服务器计算机上启用 SSL

要使用由证书颁发机构 (CA) 发放的证书，密钥库必须是 Java 格式。下面的例子说明了如何针对 Windows 计算机格式化密钥库。

1 先决条件

开始下述过程之前，先删除位于 **<Configuration Manager 安装目录 >\java\lib\security\tomcat.keystore** 中的旧 **tomcat.keystore** 文件。

2 生成服务器密钥库

a 生成 CA 签名的证书，并安装在 Windows 上。

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

➤ 为 **pfx** 文件输入作为密码的任意字符串。（将密钥库类型转变为 JAVA 密钥库时会要求您提供此密码。）
.pfx 文件现在包含公用证书和私钥，并受密码保护。

c 将创建的 **.pfx** 文件复制到下面的文件夹：**<Configuration Manager 安装目录 >\java\lib\security**。

d 打开命令提示符，并将目录更改为 **<Configuration Manager 安装目录 >\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 <Configuration Manager 安装目录 >\conf\
security\<pfx 文件名 > -srcstoretype PKCS12 -destkeystore tomcat.keystore
```

要求提供源 (**.pfx**) 密钥库密码。该密码应为在步骤 b 中创建 pfx 文件时提供的密码。

3 验证客户端配置设置

打开下面的文件：**<Configuration Manager 安装目录 >\cnc\conf\client-config.properties**，并验证 **bsf.server.url** 属性是否设置为 **https**，以及端口是否为 **8443**。

4 修改 server.xml 文件

打开下面的文件：**<Configuration Manager 安装目录 >\conf\server.xml**。定位到开头为

Connector port="8443"

的部分 （出现在注释中）。通过删除注释字符激活脚本，并添加以下两行：

keystoreFile="../../java/lib/security/tomcat.keystore"

keystorePass="password" />

5 重新启动服务器

6 验证服务器安全性

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 >:8443/cnc**。

限制：在 **tomcat.keystore** 中只能有一个服务器证书。

使用客户端证书启用 SSL

如果 Configuration Manager Web 服务器使用的证书由知名证书颁发机构 (CA) 颁发，则您的 Web 浏览器很可能无需其他操作就能够验证证书。

如果 CA 不受服务器信任存储信任，请将 CA 证书导入到服务器信任存储中。

下面的例子演示了如何将自签名 **hpcert** 证书导入到服务器信任存储 (cacerts) 中。

要将证书导入到服务器信任存储，请执行以下操作：

1. 在客户端计算机上，定位 **hpcert** 证书并重命名为 **hpcert.cer**。

   在 Windows 资源管理器中，图标显示该文件为安全证书。

2. 双击 **hpcert.cer** 以打开 “Internet Explorer 证书”对话框，然后导入文件。

3. 在服务器计算机上，用下面的命令使用密钥工具将 CA 证书导入到信任存储 (cacerts) 中：

   ```
   keytool.exe -import -alias hp -file hp.cer -keystore ..\lib\security\cacerts
   ```

4 按照下述操作修改 server.xml 文件：

a 执行步骤 5 （第 73 页）中所述的变更。

b 执行变更后立即添加下列行：

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

c 设置 clientAuth="true"。

5 按照步骤 7 （第 74 页）中所述验证服务器安全性。

仅为身份验证启用 SSL

此任务描述如何配置 Configuration Manager 以仅支持身份验证。这是使用 Configuration Manager 所需的最低安全级别。

要为身份验证启用 SSL，请执行以下操作：

1 为了在服务器计算机上启用 SSL，请执行以下任一过程，如直至步骤 6 （第 74 页）的“使用自签名证书在服务器计算机上启用 SSL”（第 72 页）中所述，或直至步骤 5 （第 76 页）的 “使用证书颁发机构颁发的证书在服务器计算机上启用 SSL”（第 74 页）中所述。

2 在 Web 浏览器中输入以下 URL：**http://<Configuration Manager 服务器名称或 IP 地址 >:8080/cnc**。

启用客户端证书身份验证

此任务描述如何设置 Configuration Manager 以接受客户端证书身份验证。

要启用客户端证书身份验证，请执行以下操作：

1 按照“使用自签名证书在服务器计算机上启用 SSL”（第 72 页）中所述执行在服务器计算机上启用 SSL 的过程。

2 打开下面的文件：**<Configuration Manager 安装目录 >\conf\lwssofmconf.xml**。定位到以 in-client certificate 开头的部分。例如：

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="e" />
```

通过删除注释字符激活客户端证书功能。

3 按照下述过程从证书中提取用户名：

a 参数 **userIdentifierRetrieveField** 指明哪个证书字段包含用户名。选项包括：

- **SubjectDN**
- **SubjectAlternativeName**

b 参数 **userIdentifierRetrieveMode** 指明用户名是包含相关字段的整个内容还是只包含其中一部分。选项包括：

- **EntireField**
- **FieldPart**

c 如果 **userIdentifierRetrieveMode** 的值为 **FieldPart**，则参数 **userIdentifierRetrieveFieldPart** 指明用户名中所用的相关字段部分。该值为基于证书中定义的图例的代码字母。

4 打开下面的文件：**<Configuration Manager 安装目录>\conf\client-config.properties**，并编辑下列属性：

- 更改 **bsf.server.url** 以使用 HTTPS 协议，并将 HTTPS 端口更改为“使用自签名证书在服务器计算机上启用 SSL”（第 72 页）中所述的端口。
- 更改 **bsf.server.services.url** 以使用 HTTP 协议，并将端口更改为原始 HTTP 端口。

加密参数

下表列出了 **encryption.properties** 文件中用于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 “加密数据库密码”（第 71 页）。

参数	描述
cryptoSource	指明实现加密算法的基础结构。可用选项包括： ➤ **lw**。使用 Bouncy Castle 轻型实现方式（默认选项） ➤ **jce**。Java 加密增强 （标准 Java 加密基础结构）
storageType	指明密钥存储的类型。 目前仅支持**二进制文件**。
binaryFileStorageName	指明文件中存储主密钥的位置。
cipherType	密码的类型。目前仅支持 **symmetricBlockCipher**。

参数	描述
engineName	加密算法的名称。 可用选项包括： ➤ **AES。**美国加密标准。此加密算法符合 FIPS 140-2 标准。（默认选项） ➤ **Blowfish** ➤ **DES** ➤ **3DES。**（符合 FIPS140-2 标准） ➤ **Null。**无加密
keySize	主密钥的大小。大小由算法确定： ➤ **AES。**128、192 或 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。 可用选项包括： ➤ **Base64**（默认选项） ➤ **Base64Url** ➤ **十六进制**
algorithmModeName	算法的模式。目前仅支持 **CBC**。
algorithmPaddingName	使用的填充算法。 可用选项包括： ➤ **PKCS7Padding**（默认选项） ➤ **PKCS5Padding**
jceProviderName	JCE 加密算法的名称。 **注意：**仅当 crytpSource 为 **jce** 时才相关。对于 **lw**，使用的是 engineName。