HP Universal CMDB Configuration Manager

适用于 Windows 和 Linux 操作系统

软件版本：9.20

部署指南

文档发布日期：2011 年 6 月
软件发布日期：2011 年 6 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 I 部分：安装和配置

第 I 部分

安装和配置

1

概述

本章包括以下内容：

概述

HP Universal CMDB Configuration Manager 是由多个组件组成的软件：

- **HP Universal CMDB Foundation**

  HP Universal CMDB Foundation (UCMDB Foundation) 是企业 IT 组织配置管理数据库 (CMDB)，用于记录、存储和管理业务服务定义以及关联的基础结构关系。

  UCMDB Foundation 可实现数据模型、数据流管理和数据建模功能，并且还提供影响分析、更改跟踪和报告功能以便将 CMDB 数据转换为易于理解、可操作的信息，从而帮助回答关键问题并解决业务问题。

➤ **HP Universal CMDB Configuration Manager**

HP Universal CMDB Configuration Manager (Configuration Manager) 介绍了新的基于策略的拓扑和清单配置管理。此产品专门适用于配置管理器和配置拥有人，它允许这些用户执行除在 UCMDB 中或通过 UCMDB 可用的 CI 数据和拓扑内容以外的分析。Configuration Manager 为配置管理器和拥有人提供了方便设置拓扑和清单配置策略所需的工具，以及自动确定遵守组织标准的级别。

Configuration Manager 已部署为额外的基于 Tomcat 的服务器。它使用功能全面的 UCMDB SDK 与 UCMDB 服务器通信。

➤ **HP Discovery and Dependency Mapping 高级版**

HP Discovery and Dependency Mapping 高级版 (DDMA) 软件具有丰富且持续更新的内容，是 UCMDB 用于获取和维护 IT 基础结构数据的首选方法。

➤ **HP Operations Orchestration**

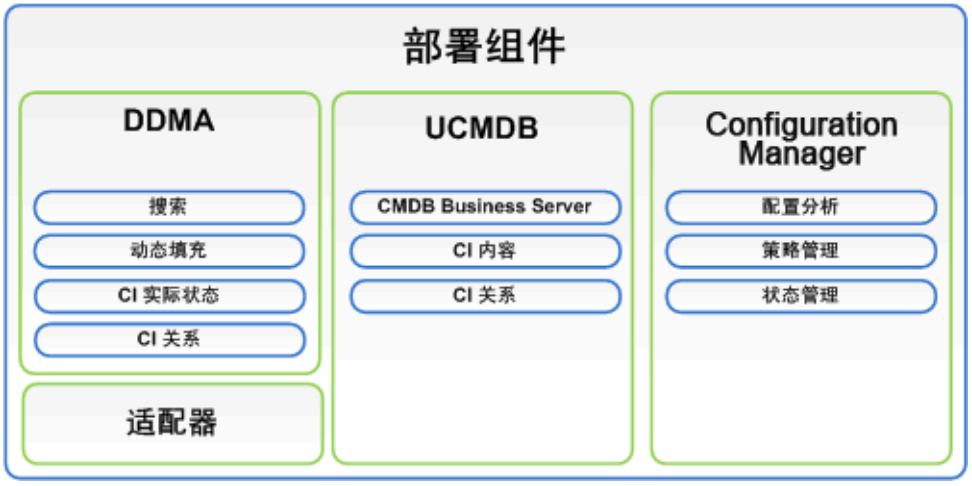
HP Operations Orchestration (OO) 是一个流创作和部署工具。借助 OO Studio 中的直观拖拉功能，即使用户对编程技能一无所知或所知甚少也同样可以设计、创建、共享和自定义流。 OO Studio 通过版本控制功能支持多个作者之间的合作。功能强大的内置调试器允许在多个环境上测试流、加速内容开发并启用流的验证以检查流执行的稳定性和可靠性。

OO Studio 使流的部署易于操作。它支持用户跨多个环境（开发、测试、试运行和生产）比较并改进流。标准过程可以记录下来，并生成结构式文档以便满足使用 Studio 的要求。

➤ **Configuration Manager-OO 集成**

Configuration Manager 提供从 Configuration Manager 框架内部执行 OO 流的功能。有两种执行 OO 流的主要方法：

- **过程集成** – 支持您在包含特定 CI 与特定配置策略的外部服务台请求中打开 RFC。
- **策略修正** – 支持您触发更正配置问题的 OO 流。例如，可以将其他内存分配到虚拟主机计算机。



确认环境

本指南描述了从不同的启动点部署 HP Universal CMDB Configuration Manager 的过程：

对于 Configuration Manager

➤ 如果安装的是 Configuration Manager 版本 9.10

有关升级 Configuration Manager 到最新版本的详细信息，请参阅“升级 Configuration Manager”（第 37 页）。

➤ 如果未安装 Configuration Manager 版本

有关详细信息，请参阅以下任一项：

- ➤ “HP Universal CMDB Configuration Manager 在 Windows 平台上的安装”（第 17 页）
- ➤ “HP Universal CMDB Configuration Manager 在 Linux 平台上的安装”（第 39 页）

对于 UCMDB

➤ 如果安装的 UCMDB 版本低于 9.03

执行以下操作：

- ➤ 升级到 UCMDB 版本 9.03。有关详细信息，请参阅《HP Universal CMDB 部署指南》PDF 文档。您可以从 www.hp.com/go/hpsoftwaresupport 下载此手册。
- ➤ 安装累计更新包 2。您可以从 Configuration Manager 安装媒体中获取，或从 www.hp.com/go/hpsoftwaresupport 下载。

有关配置企业适用性的详细信息，请参阅“配置数据库或用户架构”（第 18 页）。

➤ 如果安装的是 UCMDB 版本 9.03

安装累计更新包 2。您可以从 Configuration Manager 安装媒体中获取，或从 www.hp.com/go/hpsoftwaresupport 下载。

有关配置企业适用性的详细信息，请参阅“配置数据库或用户架构”（第 18 页）。

➤ 如果未安装 UCMDB 的任何版本

请进行下列任一操作：

- ➤ 使用部署管理器（仅适用于 Windows 系统）在安装 Configuration Manager 的同时安装 UCMDB。有关详细信息，请参阅 “HP Universal CMDB Configuration Manager 在 Windows 平台上的安装”（第 17 页）。
- ➤ 按照 “HP Universal CMDB Configuration Manager 在 Linux 平台上的安装”（第 39 页）中的说明，在 Linux 系统上安装 Configuration Manager。

常规信息

此指南还考虑到环境中可能碰到的特殊 UCMDB 部署情况 （例如，高可用性部署），并为这些部署提供部署过程中所需的调整信息。

注意：支持在同一服务器上安装 UCMDB 和 Configuration Manager。出于生产环境中的扩展目的， HP 软件建议您将这些组件分别安装在不同的服务器上。

使用 Configuration Manager 需要使用合并架构模式配置 UCMDB，以及创建新的 UCMDB 状态（授权状态）。这些配置由部署过程在两种安装情况（存在或不存在 UCMDB 的安装，或者是由部署管理器安装的或不是）下自动执行。

重要信息：如果引用现有 UCMDB 安装，并且尚未合并其架构，则合并步骤可能由于数据库的填充量很大（包含超过 5 百万 CI）而花费很长时间（20 到 60 分钟）。

请注意，如果只部署 Configuration Manager （也就是说，使用现有或已升级的 UCMDB 安装程序），UCMDB 服务器必须处于运行状态才能完成 Configuration Manager 的安装。

支持信息

服务器系统要求

CPU	最小 4 核
内存 (RAM)	最少 4 GB
平台	x64
操作系统	Windows （64 位） ➤ Windows 2003 Enterprise SP2 和 R2 SP2 ➤ Windows 2008 Enterprise SP2 和 R2 Linux ➤ Red Hat Enterprise Linux x86 （64 位）
数据库	➤ Microsoft SQL Server 2005 SP2 ； 2005 兼容性模式 80 （全部为企业版） ➤ Microsoft SQL Server 2008 ➤ Oracle 10.2.x、 11.x
Web 服务器	➤ Microsoft IIS 7 ➤ Apache 2

HP Universal CMDB	➤ 具有 CUP 2 的 HP Universal CMDB 版本 9.03（典型 CMDB 安装） 有关系统要求的完整列表，请参考 《HP Universal CMDB 部署指南》 PDF 文档。 **注意：** ➤ 如果 HP Universal CMDB 服务器是与 Configuration Manager 一起部署的，则 Oracle 的企业版和 Oracle 分区选项是必需的。 ➤ 如果之前已经与 Oracle 的标准版本一起部署了 HP Universal CMDB 服务器，并且打算将 Configuration Manager 添加到安装程序中，那么必须首先将标准版本数据库转换为已启用分区选项的企业版本数据库。
LDAP （可选）	➤ Active Directory ➤ SunONE 6.x
建议的最小数据库架构大小（可选）	2 GB

客户端要求

操作系统	➤ Windows XP x86 （32 位） ➤ Windows Vista x86 （32 位和 64 位） ➤ Windows 7 x86 （32 位和 64 位）
浏览器	➤ Microsoft Internet Explorer 7.0、 8.0 ➤ Mozilla Firefox 3.x、 4
Flash Player 浏览器插件	Flash Player 9 或更高版本 **注意：**从以下网址下载 Flash Player：http://www.adobe.com/products/flashplayer/。

屏幕分辨率	➤ 最低 1024x768 ➤ 建议采用 1280x1024
颜色质量	最低 16 位

HP Operations Orchestration（可选）

HP Operations Orchestration	➤ 7.51、9.0

2

HP Universal CMDB Configuration Manager 在 Windows 平台上的安装

重要信息：请确保参阅发行说明了解最新的安装说明。

本章包括以下内容：

预安装设置

本节包括以下内容：

配置数据库或用户架构

注意：此任务在 Configuration Manager 安装过程中自动执行；但是，您还可以选择手动执行此任务。

要使用 Configuration Manager，必须提供数据库架构。 Configuration Manager 和 UCMDB 使用不同的架构。 Configuration Manager 支持 Microsoft SQL Server 和 Oracle 数据库服务器。此任务描述如何为 Configuration Manager 创建架构。如果正在安装 UCMDB，则需要为其设置单独的数据库或用户架构。有关详细信息，请参阅 《HP Universal CMDB 部署指南》 PDF 文档。

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 14 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**：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/zh-cn/library/tcbchxcb(VS.80).aspx。

- 对于 **Oracle**：只授予 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

在 UCMDB 高可用性环境中安装 Configuration Manager

要在 UCMDB 高可用性环境中使用 Configuration Manager，请执行以下步骤：

1 关闭备份 （被动）服务器。在关闭之后等待两分钟。

2 安装 Configuration Manager 版本 9.20。

- **a** 使用负载平衡器主机详细信息。
- **b** 在第三台服务器而非任意 UCMDB 服务器上安装 Configuration Manager。

3 确保 UCMDB 和 Configuration Manager 正常工作。

4 启动备份 （被动）服务器提供高可用性。

注意：HP Universal CMDB Configuration Manager 版本 9.20 本身并不支持高可用性模式。

安装 Configuration Manager

部署管理器可以在不同配置（在安装向导的“产品选择”页面中已选择和已配置）中安装 UCMDB、 Configuration Manager 和 DDMA：

- 安装 UCMDB 的新实例
- 安装 Configuration Manager 的新实例，并将它连接到新的或现有的 UCMDB 实例
- 将 Configuration Manager 的新实例集成到 OO 的现有实例
- 安装 DDMA 的多个实例

注意：

- 部署管理器为您提供了在目标计算机上安装产品、组件和集成的功能。部署管理器不支持卸载产品、修改产品和已安装产品上的修补程序安装，您必须手动执行这些操作。
- 一旦在“产品选择”页面中按下“下一步”按钮，您将无法返回到该页面重新选择部署配置。如果要对部署配置进行更改，则需重新启动部署管理器。

要安装 Configuration Manager，请执行以下操作：

1. 要启动安装，请将 Configuration Manager 安装媒体插入计算机中，然后查找 **setup.exe** 文件。
2. 双击 **setup.exe** 文件运行部署管理器。
3. 在安装期间禁用目标计算机上的 Windows 防火墙。有关防火墙的详细信息，请参阅此过程中的步骤 6。

4 接受最终用户许可协议的条款，并单击“下一步”打开“产品选择”页面。

注意：许可协议的条款适用于部署管理器“产品选择”页面中选定的所有产品。

---

5 在“产品选择”页面上选择部署所需的产品。完成后，单击“下一步”继续到“服务器位置”页面。

“产品选择”页面使您能够选择要安装的产品，并指定部署期间执行的配置选项。

a 选择 HP Universal CMDB Foundation 安装选项。

有两个可用的 UCMDB Foundation 安装选项：

➤ **Connect to an Existing Server** – 选中此选项后，会将 Configuration Manager 或 Discovery and Dependency Mapping 连接并配置到 UCMDB Foundation 服务器的现有实例。

注意：现有服务器上的 UCMDB 版本必须是具有 CUP 2 的版本 9.03 或更高版本。

➤ **Install New Server** – 选中此选项后，可安装、配置和连接 UCMDB Foundation 服务器的新实例，并将 Configuration Manager 或 DDMA 配置并连接到 UCMDB Foundation 服务器的新实例。

b 选中 **Configuration Manager** 复选框安装并配置 Configuration Manager 的新实例。

如果需要，可选择 **Connect to an Existing HP Operation Orchestration instance**。此选项可通过用 OO 服务器连接详细信息填充 Configuration Manager 来配置 Configuration Manager 和 Operations Orchestration 之间的集成。

c **HP Discovery and Dependency Mapping 高级版。**选中此选项后，可安装并配置 DDMA 的新实例。

Number of DDMA instances 选项使您能够安装多个 DDMA 实例。在输入字段中指定的数字表示连接到单个 UCMDB 服务器实例的 DDMA 实例数。

注意：部署管理器支持相同 DMZ 中多个 DDMA 实例的部署。部署管理器支持每个部署中发现探测的最大实例数为 10。如果需要更多发现探测，请将它们划分为十个一组，在多个部署阶段中进行安装。

---

6 在 “服务器位置” 页面上，为每个选定要部署的产品指定目标部署计算机的远程服务器位置和凭据。完成后，单击 “下一步” 继续到 “连接” 页面。

部署选项

选择目标位置的部署选项。有两个可用选项：

- **Deploy on the local machine** – 如果部署产品的计算机与部署管理器相同，则使用此选项。在这种情况下，远程主机详细信息和凭据的字段为禁用状态。
- **Deploy on the following machine** – 选中此项后，必须提供远程主机地址和操作系统详细信息。提供的用户凭据必须具有远程主机的管理员特权。

注意：提供产品部署的主机名时，请确保仅使用字母 (a-z)、数字 (0-9) 和连字号 （“-”）。

以下是指定远程计算机详细信息时的相关信息：

- **WMI and SMB Protocols** – 用于连接远程计算机。要使部署管理器成功连接远程计算机，必须满足以下先决条件。
  - **WMI Service** – WMI Service 必须正在远程计算机上运行。
  - **Server Service** – 要启用 SMB 协议，Server Service 必须正在远程计算机上运行。
  - **Windows 防火墙** – 远程计算机必须允许远程管理连接。在远程计算机上的命令提示符控制台中执行相关命令：

操作系统	命令
Windows XP Windows Server 2003 Windows Server 2003 R2	netsh firewall set service RemoteAdmin enable
Windows Vista Windows 7 Windows Server 2008 Windows Server 2008 R2	netsh advfirewall firewall set rule group="windows management instrumentation (WMI)" new enable=Yes

测试连接

单击 “测试连接”验证连接凭据和详细信息是否正确，并分析本地和远程系统资源。

如果连接测试失败，则部署管理器将显示有关失败详细信息的错误消息。按“下一步”按钮自动强制测试连接验证。

计算机资源验证将验证以下资源：

- **OS 平台** – 验证操作系统是否通过产品部署认证。
- **磁盘空间** – 验证是否有足够的磁盘空间。
- **内存** – 验证是否有足够的物理内存。
- **端口** – 验证所需端口是否可用。

测试连接执行的资源验证因产品的具体支持情况而异。

注意：如果测试返回 “未知”错误，请验证以下服务是否正在部署主机上运行：

- Server
- Windows Management Instrumentation

在单击 “下一步”之前，确保已关闭用户帐户控制 (UAC)。有关 UAC 的详细信息，请转到 http://technet.microsoft.com/zh-cn/library/cc709691(WS.10).aspx。

7 在 “连接”页面上配置所选产品之间的连接。在 “连接”页面中出现的连接选项反映了为 “产品选择”页面中的部署所选择的组件。完成后，单击 “下一步”继续到 “安装配置”页面。

- UCMDB 与 Configuration Manager 的集成

  当您选择使用 **Connect to an Existing Server** 选项安装 Configuration Manager 时将出现此部分，帮助您配置 Configuration Manager 与 UCMDB 的集成。

注意：为了连接到 UCMDB 的现有实例，该安装必须是具有 CUP 2 的 UCMDB 版本 9.03 或更高版本。

请提供以下 UCMDB 详细信息：

字段	定义
UCMDB Host Name/IP	UCMDB 部署位置地址。 ➤ 如果以高可用性模式配置 UCMDB，则需遵循“在 UCMDB 高可用性环境中安装 Configuration Manager”（第 19 页）中的说明。 ➤ 如果 UCMDB 安装在本地计算机上而 Configuration Manager 安装在远程计算机上，则本地 UCMDB 实例的名称必须是 FQDN 而不能是 localhost。 ➤ 如果 UCMDB 和 Configuration Manager 有不同 DNS 域名，并且要求 LW-SSO 集成，则必须在现有的 UCMDB 主机输入字段中指定 FQDN。
协议	HTTP 或 HTTPS 协议。
UCMDB HTTP(S) 端口	HTTP 或 HTTPS 端口默认值对于 HTTP 是 **8080**，而 HTTPS 则为 **8443**。
Client Certificate File	如果已选择 HTTPS 协议，将出现此字段。必须手动将 UCMDB 客户端证书文件放置在 Configuration Manager 目标主机上，并在相邻输入字段中指定包括文件名的完整文件路径。 如果 UCMDB 使用 HTTPS，那么必须使用密钥交换。在连接测试期间不验证密钥交换。

字段	定义
客户名称	默认 UCMDB 客户名称为 “默认客户”。在 UCMDB 和 Configuration Manager 集成配置期间使用此客户名称值。连接测试不会验证此值。如果提供错误的值，则部署将失败。
JMX 端口	默认值为 **29601**。
UCMDB System User (JMX)	UCMDB (JMX) 系统用户用于激活 JMX 函数，比如创建 Configuration Manager 集成用户和部署 Configuration Manager 包。出厂设置的默认值是 **sysadmin**。
UCMDB System Password	UCMDB 系统用户密码。默认值是 **sysadmin**。

注意：Configuration Manager 配置有内部用户库。如果希望使用外部 LDAP 作为用户库，则必须配置 Configuration Manager。有关详细信息，请参阅 《HP Universal CMDB Configuration Manager 用户指南》中的 “系统设置”。

➤ Configuration Manager 与 OO 的集成

当您选择 “连接到现有 HP Operation Orchestration 实例” 选项时，将出现此部分，使您能够配置 Configuration Manager 与 OO 的集成。

请提供以下 OO 详细信息：

字段	定义
OO Version	有效 OO Version 包括 7.5 和 9.0。
OO Host Name/IP	OO 服务器计算机的主机或 IP 地址。
OO Port Number	默认端口号是 **8443**。
OO 用户名	默认 OO 用户名为 **admin**。用户必须在 OO 中配置为外部。
OO Password	默认 OO Password 是 **admin**。

➤ DDMA 配置

如果您选择 **Discovery and Dependency Mapping Advanced Edition instance** 选项，将出现以下字段，以便您配置 UCMDB 与 DDMA 的连接。

请提供以下 DDMA 详细信息：

字段	定义
Data Flow Probe Identifier	默认值是 DDMA 计算机主机名，并且系统自动填充此字段。您可以更改此值。
Use Default Domain	默认情况下将选中此选项，此选项会影响域名值。如果取消选中此复选框，则可以将默认名称更改为不同的值。
Domain Name	默认值设置为 **DefaultDomain**。**取消选中 Use Default Domain** 复选框可启用此字段。
Initial Heap Size in MB	分配到 DDMA JVM 的初始内存大小。默认值是 256 MB。
Maximum Heap Size in MB	分配到 JVM 的最大内存大小。默认值是 512 MB。

8 为在“安装配置”页面上选定的产品部署设置部署目标目录详细信息。完成后，单击 “下一步”继续到 “数据库配置”页面。

已为每个选定的产品提供默认目录路径。如果在本地计算机上部署，则可以使用 “浏览”选项选择不同的目录路径。如果在远程计算机上安装，则此选项为禁用状态。

注意：安装目录的名称中不得包含空格，并且只能使用英文字母 (a-z)、数字 (0-9) 和连字号 （“-”）。

---

9 在 “数据库配置”页面上配置每个产品的数据库连接和数据库架构。完成后，单击 “下一步”继续到 “端口配置”页面。

您可以配置以下数据库 （架构）：

- UCMDB-CM 架构
- UCMDB 架构
- UCMDB 历史记录架构

字段	定义
Database Host Name/IP	数据库服务器位置地址。
Port	MSSQL 和 Oracle 使用不同的默认端口。默认 Oracle 数据库端口是 1521，而默认 MSSQL 数据库端口是 1433。
SID (Oracle)	Oracle 数据库实例名称。
Admin Username (Oracle)	根据 Oracle 服务器输入 Oracle 管理员用户名。
Admin Password (Oracle)	根据 Oracle 服务器输入 Oracle 管理员密码。

字段	定义
Test Connection	使用提供的凭据测试到目标 DB 主机的连接。
Schema Name (Oracle)	输入架构名称。
Schema Password (Oracle)	输入架构密码。如果创建了新架构，将会出现此字段
Default Tablespace (Oracle)	输入默认表空间名称。
Temporary Tablespace (Oracle)	输入临时表空间名称。
Database Name (MSSQL)	输入 MSSQL 服务器中要使用 / 创建的数据库架构名称。
Database Username (MSSQL)	根据 MSSQL 服务器输入 MSSQL 管理员用户名。
Database Password (MSSQL)	根据 Oracle 服务器输入 MSSQL 管理员密码。

注意：

- 如果 UCMDB 表空间已满，产品部署仍会成功，但产品和组件无法正常工作。
- 在创建新 UCMDB 架构后无法连接到现有 UCMDB 历史记录架构。
- 出于安全考虑，如果已远程安装 UCMDB，则在使用 MSSQL 数据库配置 UCMDB 架构时，不支持使用 NTLM 身份验证。如果 NTLM 身份验证是必需的，请在本地部署 UCMDB。

架构模式

Configuration Manager 需要使用合并架构模式配置 UCMDB，还需要创建新 UCMDB 状态。

如果引用现有 UCMDB 安装，并且尚未合并其架构，则自动合并步骤可能由于数据库已大量填充（包含超过 5 百万 CI）而花费很长时间（20 到 60 分钟）。

注意：此安装过程不支持 Oracle Real Application Cluster (RAC) 和 SQL Server NTLM 连接。如果这些连接是必需的，请首先使用简单数据库连接安装 Configuration Manager，当安装完成后，再更改特定产品配置的连接。要进行上述操作，请根据您的数据库规范修改 **database.properties** 文件。有关详细信息，请参阅 “高级数据库配置 （适用于 Configuration Manager）”（第 31 页）。

数据库配置模式

Configuration Manager 和 UCMDB 必须使用不同的架构。

Configuration Manager 支持用户在 Oracle 或 MSSQL 数据库服务器上配置各个数据库。

配置类型

您既可以连接到现有架构，也可以创建新架构。连接到现有架构将覆盖原有内容。

数据库配置

此步骤由部署管理器自动执行。要手动执行此步骤，请参阅 “配置数据库或用户架构”（第 18 页）。

高级数据库配置 （适用于 Configuration Manager）

必须配置数据库连接，并与标准 URL 连接关联。如果需要高级功能，如 Oracle Real Application Cluster，请先设置标准连接，然后手动编辑 **database.properties** 文件配置高级功能。

Configuration Manager 可以为 Oracle 和 Microsoft SQL Server 数据库使用本机驱动程序。假如这些功能可以使用数据库 URL 配置，则支持所有本机驱动程序功能。此 URL 位于 **database.properties** 文件中。

完成部署管理器向导后，可以执行其他数据库和架构配置。

数据库配置字段

两种可用的数据库类型 – Oracle 和 MSSQL。输入字段因选定的数据库类型而异。

10 在“端口配置”页面上指定 Configuration Manager 连接端口。完成后，单击“下一步”继续到 “用户配置”页面。

Configuration Manager 提供在“端口配置”向导页面上输入字段中出现的出厂默认端口设置。

如果端口号与现有安装发生冲突，则在更改端口号之前请向 IT 管理员咨询。

字段	定义
应用程序 HTTP 端口	8180
JMX HTTP 端口	39900
Tomcat 端口	8005
AJP 端口	8009 （Apache Java 协议）
应用程序 HTTPS 端口	8143
JMX 远程端口	39600

单击 **Revert to Default Values** 按钮可以将端口重置为由部署管理器提供的默认值。

11 在 “用户配置” 页面上创建以下用户：

- 具有管理员权限的 UCMDB-CM 初始登录用户实例。
- UCMDB 中的集成用户 - 根据 Configuration Manager 的需要在 UCMDB 中创建集成用户以支持这两个产品的集成。

完成后，单击 “下一步” 继续到 “安全配置” 页面。

12 在 “安全配置” 页面上激活 UCMDB 和 Configuration Manager 的新实例上的全局 LW-SSO。 LW-SSO 只在 Configuration Manager 或 UCMBD 的新实例上配置，具体根据 “产品选择” 页面中所做的选择而定。完成后，单击 “下一步” 继续到 “摘要” 页面。

LW-SSO 是用于验证不同类型的身份验证和安全令牌 （比如 LW-SSO 和 SAML2）的模块框架。LW-SSO 用于从不同环境中将验证信息桥接并利用到应用程序或安全框架中的应用程序安全上下文中。

LW-SSO 配置根据选择的产品组件而有所不同。

将 Configuration Manager 连接到现有 UCMDB 或 OO 实例时，仅在 Configuration Manager 上配置 LW-SSO。必须从 UCMDB 或 OO 中提取 LW-SSO 字符串，并将该字符串输入 LW-SSO 字符串输入字段中。同时连接到 UCMDB 和 OO 时，验证 UCMDB 和 OO 实例中定义的 LW-SSO 字符串是否匹配。

将 Configuration Manager 的新实例连接到 UCMDB 的现有实例时，使用 FQDN 作为 UCMDB 主机名。

要从 UCMDB 中提取 LW-SSO 字符串，请执行以下操作：

a 打开 UCMDB，并选择 “管理” > “基础结构设置管理器”。

b 在 “名称” 列中，选择并双击 LW-SSO init 字符串字段。

c 从当前值输入字段中复制字符串。

d 将值粘贴到 “安全配置” 页面的 LW-SSO 字符串输入字段中。

将 Configuration Manager 连接到新 UCMDB 实例时，将在 UCMDB 以及 Configuration Manager 上自动配置 LW-SSO。

13 在 “摘要” 页面上检查安装和配置设置。完成后，单击 “下一步” 继续到 “验证” 页面。

“摘要” 页面集中了所有配置详细信息和用户输入。可以根据需要修订摘要的内容，通过单击此页面的 “上一步” 按钮直到达到所需页面，然后调整部署设置来完成修订。根据需要单击 “下一步” 可返回到 “摘要” 页面。

14 部署管理器现在将执行一系列操作验证远程计算机的系统资源是否足够，检查用户输入是否正确，并验证数据库配置设置。这些验证可指明用户定义设置是否遵从已知环境的限制条件。验证过程将自动开始，如果已经返回到部署管理器中以前的页面并且已更改配置，则单击 “运行验证” 开始验证过程。完成后，单击 “部署” 继续到 “部署” 页面。

15 “部署” 页面反映部署过程进行中的状态。部署过程包括产品安装、开始过程以及与其他产品的集成和连接。

一旦成功启动所有产品，则完成部署过程。

单击 “详细信息” 查看部署进度详细信息，这些信息包括部署管理器为每个选定产品的部署采取的步骤。

单击 “取消” 可以适时取消部署，此操作允许当前部署操作完成之后才停止部署。

单击 “中止”（仅在单击 “取消” 之后可用）强制终止当前操作和部署。中止部署可能导致产品处于未决状态。

验证

下表提供由部署管理器执行的验证列表。

验证	错误消息	描述
验证登录凭据	Credentials verification failed	提供的用户凭据错误。
		无法建立连接。
验证操作系统兼容性	Target operating system platform is <Platform> Product <Product Name> supports the following platforms <Platform>	实际目标操作系统与产品的认证操作系统列表不对应。
验证内存	The assigned memory (<Memory> MB) exceeds the available memory (<Memory> MB) on <Target>	目标计算机上没有足够用于所有已分配产品的内存
	<Memory> MB of memory are verified to be available on <Target Machine>	验证成功。
验证磁盘空间	assigned disk space for (<Memory> MB) exceeds available disk space (<Memory> MB) on drive <Target>	在目标计算机上没有足够用于所有已分配产品的磁盘空间。
	<Memory> MB of disk space are verified to be available on drive <Target>	验证成功。
验证是否提供所有强制属性	Missing the target storage device for the product: <Target>	未设置产品的安装目录。

验证	错误消息	描述
验证是否已定义部署计算机	No deployment machine is defined for <Product Name>	产品未配置为可在任意计算机上部署。
验证登录凭据	Credentials verification failed	错误的登录凭据。
验证是否禁用 UAC	The UAC is enabled	已在目标计算机上启用 UAC。
验证可用端口	The required port number <Port> is already in use on <Target>	目标计算机上的所需端口已在使用中。
验证目标存储设备是否存在	The target storage device <Device> does not exist on <Target>	所选目标存储设备不存在于目标计算机上。
验证架构的存在	Schema <Name> does not exist/ already exist	目标计算机上的架构存在 / 不存在。
验证架构权限的存在	Validate <Permissions> schema tables user permissions existence	DB 用户没有足够的权限
验证架构表的存在	Schema Tables <Tables> on the database: <Tables> already exist	数据库上的架构表已经存在。
验证架构表用户权限的存在	The database user does not have the correct permissions	数据库用户没有正确的权限。

验证	错误消息	描述
验证 UCMDB 连接	Connection failed. Connection to UCMDB failed, host: <Host>, username: <User name>, port: <Port>, protocol: <Protocol> due to <Error>	使用给定连接设置测试到 UCMDB 的连接失败。
	Existing UCMDB version must be 9.03 with CUP 2 or later.	现有 UCMDB 版本必须是具有 CUP 2 的 9.03 或更高版本。
验证 DB 连接	The host name/IP address validation failed	指定的数据库主机名/IP 地址不可访问
	The username or password validation failed	指定的用户凭据无效。
	The port validation failed	指定的数据库端口不可访问。
	The SID validation failed	指定的数据库 SID 在 DB 中不存在。
安装验证	The product is already installed	产品已安装在目标主机上

升级 Configuration Manager

在开始之前，升级过程将自动检查并验证以下各项：

- 具有到 UCMDB 服务器的有效连接。
- 已为 UCMDB 安装 CUP 2 修补程序。
- JMX 端口是正确的。

如果上述任何项尚未安装或配置错误，您将看到相应通知您的错误消息。您可以先解决出现的问题，然后执行升级。

- 如果升级因为无法连接到 UCMDB 而失败，请检查 UCMDB 服务器是否已启动并正在运行。
- 如果升级由于未安装修补程序而失败，则按照说明安装 CUP 2，说明可从下面的网址获取：
  http://support.openview.hp.com/selfsolve/document/FID/DOCUMENTUM_UCMDB_00045
- 如果升级由于错误的 UCMDB JMX 端口而失败，则选择正确的 JMX 端口。要执行此操作，请在 **upgrade.properties** 文件中更改 ucmdb.jmx.port 属性，此文件位于 **<Configuration Manager 安装目录 >\utilities\Upgrade** 文件夹中。

要升级，请执行以下步骤：

注意：开始升级过程之前，确保 UCMDB 服务器已启动并且正在运行中。

---

1. 备份您的 Configuration Manager 和 UCMDB 架构。
2. 在 Configuration Manager 安装媒体的 Windows 子文件夹中查找 **setup-win64.msi** 文件。
3. 双击该文件以运行 Configuration Manager 安装向导。
4. 单击 “下一步”打开 “最终用户许可协议”页面。

5 接受许可协议的条款，然后单击 “下一步”打开 “客户信息”页面。

6 输入信息，然后单击 “下一步”打开 “设置类型”页面。

7 选择将要安装 Configuration Manager 的文件夹。确保选择的位置与以前版本所用的位置不同。

默认情况下，Configuration Manager 将安装在如下目录中：**c:\hp\cnc920**。单击 “下一步”接受默认位置，或单击 “浏览”选择不同位置，然后单击 “下一步”。

注意：安装目录的名称中不得包含空格。

---

8 单击 “下一步”确认并开始安装。

在安装向导完成之后，将自动启动 Configuration Manager 安装后向导。

9 单击 “下一步”，直到系统询问您是否执行 Configuration Manager 的新安装或升级。

10 选择 “升级”，并单击 “下一步”。

11 安装完成后，检查 **post_installation.log** 文件 （位于 **<Configuration Manager 安装目录 >/tmp/log** 文件夹中）以确保安装已正确完成。

如果在升级过程中发生错误，将出现帮助您关闭向导的消息。如果发生这种情况，请联系 HP 支持人员。

12 启动 Configuration Manager 服务。

注意：升级之后，必须再次执行 SSL 配置。有关详细信息，请参阅 “强化” （第 84 页）。

3

HP Universal CMDB Configuration Manager 在 Linux 平台上的安装

重要信息：请确保参阅发行说明了解最新的安装说明。

本章包括以下内容：

预安装设置

本节还包括以下内容：

先决条件

- 至少 400MB 的可用磁盘空间
- 推荐运行 X 显示

获取 setup.bin 文件

Linux 安装文件 (**setup.bin**) 可在安装媒体或 ISO 映像 （可从 HP 网站下载）上找到。用以下任一方式访问此文件：

➤ 在 Linux 计算机上装载 DVD：

```
$ mkdir -p /mnt/cdrom
$ mount /dev/cdrom /mnt/cdrom
```

➤ 装载 ISO 映像作为环回块设备：

```
$ mkdir -p /mnt/cdrom
$ mount -o loop cnc-<version>.iso /mnt/cdrom
```

➤ 将 **setup.bin** 文件复制到 Linux 计算机上的临时位置。

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。

如果具有 X 显示，则安装后向导将以 UI 形式出现；如果没有，则向导信息将以控制台模式出现。

注意：此指南中的步骤针对控制台模式进行说明；不过如果使用 UI 向导，也会出现相同的步骤。

要安装 Configuration Manager，请执行以下操作：

1 要在当前位置安装 Configuration Manager，请发出以下命令：

```
chmod 755 setup.bin
$ /path/to/installation/kit/setup.bin
```

2 此时将显示最终用户许可协议 (EULA)，您必须同意此协议。通过重复单击空格键，向下滚动到 EULA 的底部，直到达到 EULA 的末端为止。要同意并继续安装，请键入 **yes**，并按下 **Enter** 键。

HP Universal CMDB Configuration Manager 安装在 **cnc** 子文件夹的当前位置中。

“欢迎使用”页面

```
<============================>
Welcome
<============================>
Welcome to the HP Universal CMDB Configuration Manager
post installation wizard.
Enter [<C>ancel] [Ne<x>t]>
```

按 **Enter** 键继续到下一页。

数据库供应商选择

```
<============================>
Database Connection Configuration
<============================>
-------
Vendor:
-------
  ->1 - Oracle
    2 - Microsoft
Enter index number from 1 to 2 OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

按 **Enter** 键选择 Oracle，或键入 **2**，然后按 **Enter** 键选择 Microsoft。

数据库主机名

```
-------------
Set Hostname:
-------------
        Hostname: = "localhost"
Input the new Hostname: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

键入数据库的主机名，然后按 **Enter** 键。提供的主机名默认值是 **localhost**。

数据库端口

```
---------
Set Port:
---------
        Port: = "1521"
Input the new Port: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

Oracle 的默认端口是 1521，而 Microsoft 的默认端口则是 1433。如果要使用不同的端口号，则在此处键入，然后按 **Enter** 键。

SID/DB 名称

```
-----------
Set SID/DB:
-----------
        SID/DB: = "orcl"
Input the new SID/DB: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

对于 Oracle，此字段指定数据库 SID ；对于 Microsoft，此字段指定数据库名称。键入有效值，然后按 **Enter** 键。

用户 / 架构名称和密码

```
-------------
Set Username:
-------------
Input the Username: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

键入数据库用户名，然后按 **Enter** 键。

```
Input the Password: OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

键入架构密码，然后按 **Enter** 键。

测试数据库连接

```
--------
Set Test
--------
        Test = "Yes"
Choose [<Y>es]/[<N>o] for Test OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

按 **Enter** 键测试数据库连接。

由于此向导会尝试在数据库架构中创建表，因此强烈建议测试您的数据库连接。如果不希望测试连接，则键入 **No**，然后按 **Enter** 键。

数据库连接测试成功完成时，将显示以下消息：

```
success
Enter [<C>ancel] [<B>ack] [Ne<x>t]>
```

按 **Enter** 键继续。如果在连接测试中发生错误，将显示错误消息，并将提示您再次运行测试。请解决连接问题，再次测试并继续安装。

应用程序服务器主机名

```
<============================>
Application Server Configuration
<============================>
Hostname:
----
Set
----
         = "myucmdbcmhost.mydomain"
Input the new  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

主机名的默认值是计算机的实际主机名。如果计划在负载平衡器或反向代理的后面安装，则在此键入外部名称。

自定义应用程序服务器端口

```
-------------------
Select Customize ports
-------------------
        Customize ports = "No"
Choose [<Y>es]/[<N>o] for Customize ports OR [<C>ancel] [<B>ack]
[Ne<x>t]>
```

如果要使用 Configuration Manager 的默认端口，请按 **Enter** 键。如果要使用自定义端口，则键入 **Yes**，然后按 **Enter** 键。默认端口号如下所示：

端口名称	端口号
HTTP	8180
HTTPS	8443
Tomcat 管理	8005
AJP	8009
JMX HTTP	39900
JMX RMI	39600

如果选择自定义端口，对于以上列出的每个端口，系统将要求您输入值。键入新值，然后为每个值按 **Enter** 键：

```
HTTP port:
----
Set
----
         = "8180"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
HTTPS port:
----
Set
----
         = "8443"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
Tomcat port:
----
Set
----
         = "8005"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
AJP port:
----
Set
----
         = "8009"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
JMX HTTP port:
----
Set
----
         = "39900"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
JMX remote port:
----
Set
----
         = "39600"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

初始管理用户

```
<============================>
Users Credentials
<============================>
Initial Administrative User
Admin username:
----
Set
----
Input the  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

初始管理用户将创建为初始登录系统的管理员或超级用户。键入要使用的管理用户名并按 **Enter** 键。

```
Admin password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

键入管理用户的密码，然后按 **Enter** 键。

```
Confirm password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

重新键入管理用户的密码并按 **Enter** 键以进行确认。

集成用户

```
Platform Integration User
Integration username:
----
Set
----
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

选择 UCMDB 集成用户名。此用户将在 UCMDB 中于安装后期间创建。HP 建议使用一个能够清楚表明用于集成用途的用户名 （例如， cm_integration）。键入所选用户名，然后按 **Enter** 键。

```
Integration password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

键入集成用户的密码，然后按 **Enter** 键。

```
Confirm password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

重新键入集成用户的密码并按 **Enter** 键以进行确认。

HP Universal CMDB 服务器主机名

```
<============================>
HP UCMDB Connection Configuration
<============================>
Hostname:
----
Set
----
         = "localhost"
Input the new  OR [<C>ancel] [Back<b>] [Ne<x>t]>
```

键入 UCMDB 服务器的主机名，然后按 **Enter** 键。这可能与默认的 localhost 不同，因此不建议在生产环境中将 UCMDB 和 Configuration Manager 安装在同一台计算机上。

HP Universal CMDB 服务器端口

```
Port:
----
Set
----
         = "8080"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

按 **Enter** 键接受用于 UCMDB 服务器的默认端口号 8080；或键入端口号，然后按 **Enter** 键。

HP Universal CMDB 服务器协议

```
Protocol:
  ->1 - HTTP
    2 - HTTPS
Enter index number from 1 to 2 OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

按 **Enter** 键使用 HTTP，或键入 2 然后按 **Enter** 键使用 HTTPS。

注意：如果选择 HTTPS，则将需要与 UCMDB 交换密钥。有关详细信息，请参阅“强化”（第 84 页）。此步骤使用不安全的自签名证书设置 HTTPS。

HP Universal CMDB 服务器客户

```
Customer:
----
Set
----
         = "Default Client"
Input the new  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

按 **Enter** 键接受 UCMDB 服务器的默认客户名称，或键入客户名称，然后按 **Enter** 键。

HP Universal CMDB 服务器 Sysadmin 凭据

```
Administrative username:
----
Set
----
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

输入 UCMDB 服务器的 sysadmin 用户名。这是可以在 UCMDB 服务器上运行 JMX 方法的用户。这是预先存在的用户，并且不是在安装期间创建的。从您的 UCMDB 服务器管理员那里获取 sysadmin 用户的凭据。

```
Administrative password:
Input the  OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

键入 UCMDB 服务器 sysadmin 用户的密码，然后按 **Enter** 键。

测试 HP Universal CMDB 服务器连接

```
--------
Set Test
--------
        Test = "Yes"
Choose [<Y>es]/[<N>o] for Test OR [<C>ancel] [<B>ack] [Ne<x>t]>
```

按 **Enter** 键测试 UCMDB 服务器连接。由于此向导会尝试部署包，并配置 UCMDB 服务器，因此强烈建议您测试服务器连接。如果不希望测试连接，则键入 **No**，然后按 **Enter** 键。

服务器连接测试成功完成时，将显示以下消息：

```
success
Enter [<C>ancel] [<B>ack] [Ne<x>t]>
```

按 **Enter** 键继续。如果在连接测试中发生错误，将显示错误消息，并将提示您再次运行测试。解决连接问题，再次测试并继续安装。

摘要

在实际执行您作出的所有选择之前，此向导将显示这些选择的摘要：

```
<============================>
Post Installation Actions Summary
<============================>
Post installation actions summary
Users
-----
HP Universal CMDB Configuration Management admin username: admin
HP Universal CMDB Platform integration username: cm_integration

Database
--------
Vendor:Oracle
Host: mydbhost.mydomain
Port: 1521
SID/DB: orcl
Encrypt password? Yes
Create schema objects? Yes

Application Server
------------------
hostname: myucmdbcmhost.mydomain
HTTP: 8180
HTTPS: 8443
Tomcat management: 8005
AJP: 8009
JMX HTTP: 39900
JMX remote: 39600
Debug: 7878

Windows Service
---------------
Create service? No

HP Universal CMDB Platform
-----
URL: http://myucmdb.mydomain:8080
Sysadmin username: sysadmin
Customer: Default Client

Enter [<C>ancel] [Back<b>] [Ne<x>t]>
```

按 **Enter** 键继续进行配置。在进行配置时，将出现进度条。此向导将执行以下任务：

1. 创建数据库表和对象。
2. 使用默认值和初始值填充数据库。
3. 创建初始管理用户。
4. 在 UCMDB 服务器中创建集成用户。
5. 合并 UCMDB 服务器。
6. 在 UCMDB 服务器中创建授权状态。
7. 将 Configuration Manager 包部署到 UCMDB 服务器。

完成配置时，将出现以下消息：

```
<============================>
Finish
<============================>
Post installation configuration has completed.
Enter [Finish<f>]>
```

按 **Enter** 键退出向导。

无提示安装选项

可以使用无提示模式安装 Configuration Manager。这样将只从安装包中提取文件，但不执行任何安装后配置。要以无提示模式运行安装，请执行以下命令：

```
$ /path/to/installation/kit/setup.bin -silent
```

运行 Configuration Manager 应用程序服务器

要运行 Configuration Manager，请执行以下命令：

```
$ cd /path/to/installation/location
$ ./start-server-0.sh
```

可以在 **/etc/init.d** 目录中创建脚本，以便在计算机启动时自动启动 Configuration Manager。

4

登录到 Configuration Manager

本章包括以下内容：

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 浏览器要求以及成功查看 Configuration Manager 的最低要求的详细信息，请参阅 “支持信息”（第 14 页）。

有关安全访问 Configuration Manager 的详细信息，请参阅“强化”（第 84 页）。

有关访问 Configuration Manager 的疑难解答信息，请参阅 “疑难解答”（第 117 页）。

登录到 Configuration Manager

1. 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 >/cnc，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)，而 **< 端口 >** 则表示在安装期间选择的端口。
2. 输入在 Configuration Manager 安装后向导中定义的用户名和密码。
3. 单击 “登录”。登录之后，用户名将显示在屏幕的右上角。
4. （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。

5

其他用例

本章包括以下内容：

在计算机之间转移 Configuration Manager 安装

如果您希望将 Configuration Manager 的安装从一台计算机转移到另一台计算机，同时使数据库架构保持完好并连接到相同 UCMDB 服务器，应当采用此程序。

1. 在 **<Configuration Manager 安装目录 >\cnc\bin** 文件夹中，执行以下命令：edit-server-0.bat。
2. 记录找到的所有参数，包括端口 （例如 JMX 端口）。
3. 停止源计算机上的 Configuration Manager 服务器。（如果源计算机安装于 Windows 系统上，则可以通过停止 Configuration Manager 服务完成此操作）。
4. 在目标计算机上安装 Configuration Manager：
   - 如果是 Windows 系统：运行 **setup-win64.msi** 文件 （位于安装媒体的 **\windows** 文件夹中）。
   - 如果是 Linux 系统：遵循 “安装 Configuration Manager”（第 40 页）中的指示操作。

5 在安装后向导开始后将其取消。

6 将所有文件从源计算机上以前的安装目录复制到目标计算机上的新安装位置中。

7 在目标计算机上，在 **client-config.properties** 和 **resources.properties**（位于 **\conf** 文件夹中）中将主机名更改为目标计算机名称。

注意：如果目标计算机所在的域与源计算机不同，请在 **lwssofmconf.xml** 文件中修改旧域引用。

---

8 在目标计算机上，运行 **bin/create-windows-service.bat** 文件创建 Windows 服务。设置 **-h** 标记可以查看可用选项，并根据需要使用从源计算机服务记录的参数（记录在步骤 2 中）。对于域名参数，请使用 server-0。使用默认值后，命令将如下所示：

c:\HP\cnc920\bin>create-windows-service.bat -j 39900 -n server-0 -r 39600

9 在目标计算机上启动 Configuration Manager 服务器。

在安装之后更改端口号

1 停止 Configuration Manager 服务器。

2 备份 **<Configuration Manager 安装目录>\servers\server-0** 文件夹的内容。

3 删除 **<Configuration Manager 安装目录>\servers\server-0** 文件夹。

4 运行具有 **-h** 标记的 **create-node.bat** 脚本以查看可用选项。将所有需要的端口号传递到实用程序。

5 在目标计算机上，在 **client-config.properties** 和 **resources.properties**（位于 **\conf** 文件夹中）中将端口更改为新 HTTP 端口号。

6 运行 **edit-server-0.bat** 脚本，该脚本位于 **<Configuration Manager 安装目录>\bin** 文件夹中。

7 （对于 Windows 系统）在打开的 HP Universal CMDB Configuration Manager “属性”窗口中，单击 “Java”选项卡，并将 **jmx.http.port** 和 **com.sun.management.jmxremote.port** 设置更改为新端口号。

8 在目标计算机上启动 Configuration Manager 服务。

在系统之间复制系统设置

1 在源计算机上，打开 Configuration Manager。转到 “系统” > “设置”，并单击 “将配置集导出为 zip 文件”按钮。

在导出之前，通过取消选中相关配置项旁边的复选框，可以排除配置的特定部分。

2 将导出配置复制到目标计算机。

3 在目标计算机上，打开 Configuration Manager。转到 “系统” > “设置”，然后单击 “导入配置集”按钮。

备份和还原

您可以备份 Configuration Manager 的安装，以便能够从任何类型的失败中恢复过来，否则将需要重新安装。

备份

备份以下信息：

- Configuration Manager 安装目录中的 **conf** 和 **security** 子文件夹。这可以在系统运行时完成，不需要中断操作。
- 数据库架构

还原 （Windows 系统）

此程序应当在没有安装 Configuration Manager 的新系统上执行。

1. 通过以静默模式运行 **setup-win64.msi** 文件 （位于安装媒体的 **\windows** 文件夹中），可在目标计算机上安装 Configuration Manager，具体如下所示：

   ```
   msiexec /i setup-win64.msi TARGETDIR=path\to\install\dir /passive
   ```

2. 还原 **conf** 和 **security** 目录。使用与备份方式相匹配的方法进行还原。覆盖您在步骤 1 中执行的安装而创建的目录。
3. 还原数据库架构。如果还原到不同的数据库服务器，则必须在 **database.properties** 文件 （位于 **conf** 目录中）中修改 **url** 属性以匹配新数据库服务器名称。
4. 使用 **create-windows-service** 实用程序 （具有 **-h** 标记可查看可用选项）创建 Windows 服务。
5. 启动 Configuration Manager 服务器。

还原 （Linux 系统）

1. 通过运行 **setup.bin** 文件 （位于安装媒体中），在目标计算机上安装 Configuration Manager。有关详细信息，请参阅 “安装 Configuration Manager”（第 40 页），但需在安装后向导的第一个步骤中取消安装。所有文件都会被部署，但系统将取消配置。
2. 还原 **conf** 和 **security** 目录。使用与备份方式相匹配的方法进行还原。覆盖您在步骤 1 中执行的安装而创建的目录。
3. 还原数据库架构。如果还原到不同的数据库服务器，则必须在 **database.properties** 文件 （位于 **conf** 目录中）中修改 **url** 属性以匹配新数据库服务器名称。
4. 启动 Configuration Manager 服务器。

6

高级配置

本章包括以下内容：

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。

注意：在 Linux 系统中执行高级配置时，执行以下操作：

- 更改说明中斜线的方向，使斜线成为正斜线 (/)。
- 在脚本执行中用 **.sh** 替换 **.bat**。

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。HP Universal CMDB 不支持二进制排序顺序和区分大小写。仅支持不区分大小写的排序，以及重音、假名或宽度设置的组合。	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。

单一登录 (SSO)

Configuration Manager 和 UCMDB 之间的单一登录使用 HP 的 LWSSO 技术执行。有关详细信息，请参阅 “轻型单一登录身份验证 (LW-SSO) – 一般参考”（第 113 页）。

本节包括以下内容：

启用 Configuration Manager 和 UCMDB 之间的 LW-SSO

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”> “UCMDB Foundation”）。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。此任务应当手动执行，除非已经随同部署管理器安装完成了执行。

要启用 LW-SSO，请执行以下操作：

1. 在 Configuration Manager 安装目录中，编辑 **\conf\lwssofmconf.xml** 文件。
2. 定位到以下部分：

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

   然后验证值是否为 **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-->

注意：仅当 Configuration Manager 和另一个应用程序位于不同域中时，才应当包括第二个 DNSDomain。

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**或**此值应替换为其他应用程序的域**）输入所有服务器域 （如有必要） 。列表应包括步骤 3 （第 70 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”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 71 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”。

在 Operations Orchestration 中配置 LW-SSO

如果在 Configuration Manager 和 Operations Orchestration (OO) 中都启用了 LW-SSO，则允许已经登录到 Configuration Manager 的用户通过 Web 层登录到 Operations Orchestration，而无需提供用户名和密码 （针对系统管理员）。

注意：

- 在以下过程中， <OO_HOME> 表示 Operations Orchestration 主目录。
- LW-SSO 要求用于登录到 Operations Orchestration 和 Configuration Manager 的帐户有相同的帐户名 （但可以有不同的密码）。
- LW-SSO 要求 Operations Orchestration 中的帐户并不是仅供内部使用。

要在 Operations Orchestration 中配置 LW-SSO，请执行以下操作：

1 停止 RSCentral 服务。

2 在 **<OO_HOME>\Central\WEB-INF\applicationContext.xml** 中，启用 LWSSO_SECTION_BEGIN 和 LWSSO_SECTION_END 之间的导入，如下所示：

```
<!--  LWSSO_SECTION_BEGIN-->
       <import resource="CentralLWSSOBeans.xml"/>
<!--  LWSSO_SECTION_END -->
```

3 在 **<OO_HOME>\Central\WEB-INF\web.xml** 中，启用 LWSSO_SECTION_BEGIN 和 LWSSO_SECTION_END 之间的所有筛选器和映射，如下所示：

```
<!-- LWSSO_SECTION_BEGIN  -->

<filter>
        <filter-name>LWSSO</filter-name>
        <filter-
    class>com.iconclude.dharma.commons.util.http.DharmaFilterToBeanProx
    y
        </filter-class>
        <init-param>
            <param-name>targetBean</param-name>
            <param-value>dharma.LWSSOFilter</param-value>
        </init-param>
   ......
   </filter>
<!-- LWSSO_SECTION_END -->

<!-- LWSSO_SECTION_BEGIN-->
   <filter-mapping>
      <filter-name>LWSSO</filter-name><url-pattern>/*</url-pattern>
   </filter-mapping>
<!--LWSSO_SECTION_END -->

<!-- LWSSO_SECTION_BEGIN-->
    <filter-mapping>
          <filter-name>LWSSO2Acegi</filter-name><url-pattern>/*</url-pattern>
    </filter-mapping>
    <filter-mapping>
          <filter-name>dharmaLWSSOGroupsFilter</filter-name><url-
    pattern>/*</url-pattern>
          </filter-mapping>
<!--LWSSO_SECTION_END -->
```

4 在 **<OO_HOME>\Central\conf\lwssofmconf.xml** 中，编辑下面两个参数：

- domain：OO 服务器的域名。
- initString：必须与 OO LW-SSO 配置中的 initString 值相同（最小长度为：12 个字符）。例如， smintegrationlwsso。

  例如：

```
<webui>
<validation>
      <in-ui-lwsso>
       <lwssoValidation id="ID000001">
            <domain>asia.hpqc.net</domain>
            <crypto cipherType="symmetricBlockCipher"
                                    engineName="AES" paddingModeName="CBC"
keySize="256"  encodingMode="Base64Url"
                                    initString=" smintlwsso "></crypto>
       </lwssoValidation>
      </in-ui-lwsso>
</validation>
<creation>
       <lwssoCreationRef id="ID000002">
            <lwssoValidationRef refid="ID000001"/>
            <expirationPeriod>600000</expirationPeriod>
       </lwssoCreationRef>
</creation>
</webui>
```

5 重新启动 RSCentral 服务以使配置生效。

执行身份管理器身份验证

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。

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。

此任务包括以下步骤：

- “先决条件”（第 75 页）
- “配置 HP Universal CMDB Configuration Manager 以接受身份管理器”（第 75 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，并且将端口更改为原始 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，该连接器将用于配置在 Windows 2003 操作系统上运行 IIS6 的情况下 Configuration Manager 所需的身份管理。

要安装 Java 连接器，并将其配置为适用于 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** 下面。

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 installation 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 installation directory>\tomcat
\conf\workers.properties.minimal
# Full path to the uriworkermap.properties file
worker_mount_file==<Configuration Manager installation 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

---

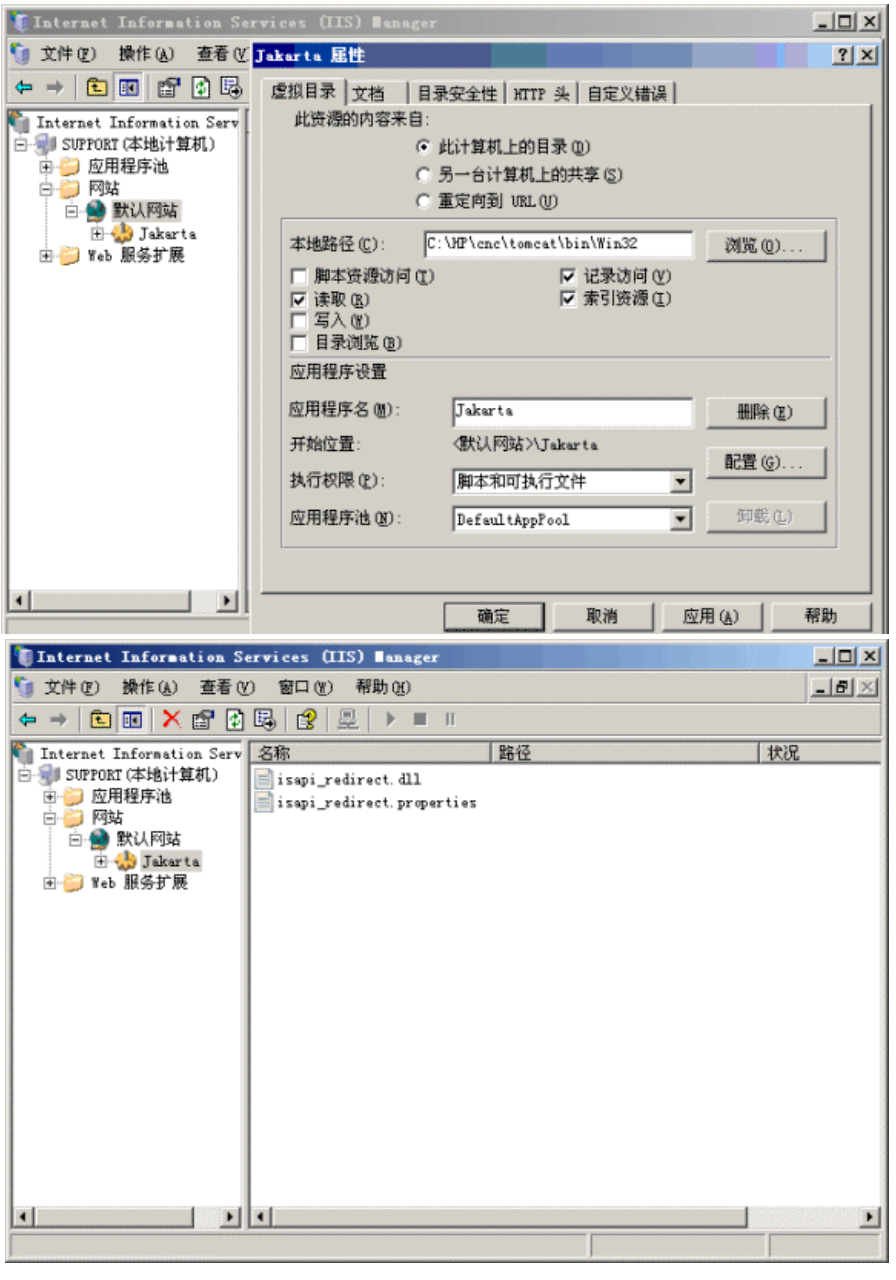
6 在 IIS 配置的相应网站对象中创建虚拟目录。

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：



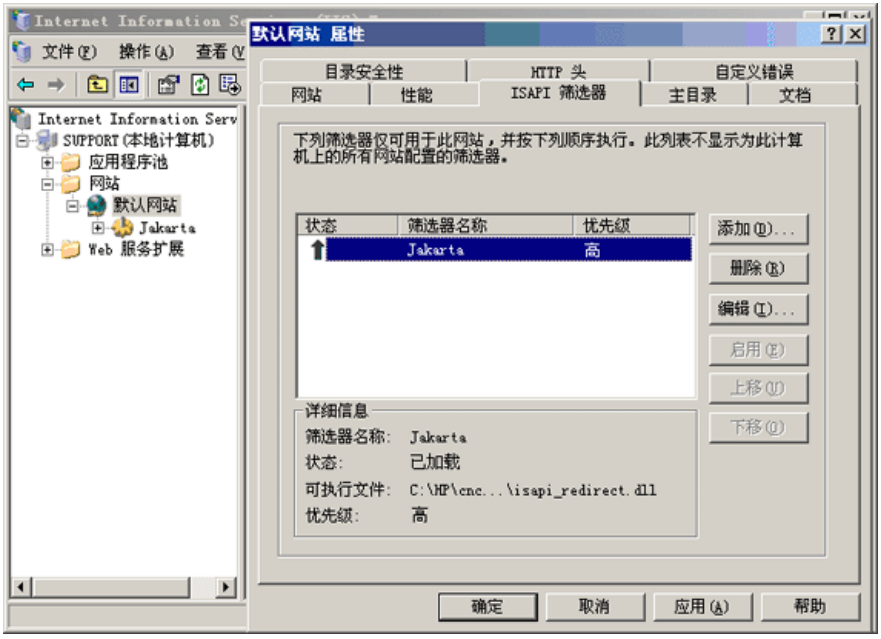
7 添加 **isapi_redirect.dll** 作为 ISAPI 筛选器。

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：



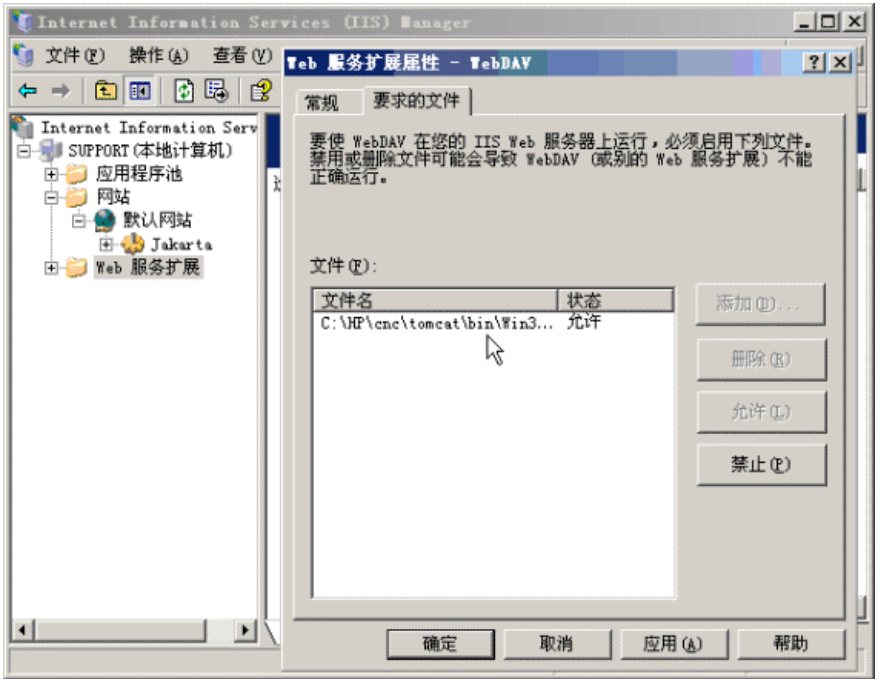
d 单击 “应用”按钮。

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。

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 和 IPv4。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 >/conf** 文件夹中的 **client-config.properties** 文件，然后编辑以下值：

- 更改 **bsf.server.url** 参数的值，并确保它使用主机名。例如：

  bsf.server.url=http://mycomputer:8080/bsf

- 更改 **bsf.server.services.url** 参数的值，并确保 Configuration Manager URL 是主机名地址。例如：

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

3 打开 Tomcat **servers\server-0\conf\server.xml** 文件，然后编辑以下值：

- 通过将 **address="[::]"** 添加到以下标记，将 IPv6 地址添加到 SHUTDOWN 钩子：

  <Server port="8005" shutdown="SHUTDOWN" **address="[::]"** >

- 复制 HTTP 连接器。为第二个连接器添加 IPv6 [::] 地址。例如：

```
<Connector port="8180" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
<Connector port="8180" protocol="HTTP/1.1" address="[::]"
           connectionTimeout="20000"
           redirectPort="8443" />
```

➤ 复制 AJP 连接器。为第二个连接器添加 IPv6 [::] 地址。例如：

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443"  address="[::]" />
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

4 将环境变量添加到服务器：useIPv6="true":

打开位于 **<Configuration Manager 安装目录>/bin** 文件夹中的 **edit_server-0.bat** 文件。在 Java 选项卡中，将以下属性添加到 Java 选项：-DuseIPv6。

5 重新启动服务器。

LDAP

LDAP 可以在 Configuration Manager 中配置。有关详细信息，请参阅《HP Universal CMDB Configuration Manager 用户指南》中的“系统设置”。

强化

本节包含以下内容：

注意：升级之后，必须再次执行 SSL 配置。有关详细信息，请参阅 “升级 Configuration Manager”（第 37 页）。

强化 Configuration Manager

本节介绍了安全 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，以便满足处理安全威胁的要求。

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。如果希望加密密码，我们的默认加密算法将遵循 FIPS 140-2 标准。

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 87 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. 打开文件 **<Configuration Manager 安装目录 >\conf\encryption.properties**，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大小。
2. 运行 **generate-keys.bat** 脚本，此脚本创建以下目录：**cnc920\security\encrypt_repository**，并生成加密密钥。
3. 运行 **bin\encrypt-password** 实用程序加密密码。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，并将加密结果粘贴到 **conf\database.properties** 文件中。

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 86 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**。
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

参数	描述
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。

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 7.0 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，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

将证书添加到计算机上 Internet Explorer 中客户端的受信任存储中 （“工具” > “Internet 选项” > “内容” > “证书”）。如果未添加，则将在第一次尝试使用 Configuration Manager 时提示您添加证书。

有关使用客户端证书的详细信息，请参阅 “客户端证书”（第 95 页）。

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 **bsf.server.url** 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 >\servers\server-0\conf** 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，并将以下属性添加到 HTTPS 连接器来激活脚本：

keystoreFile="<tomcat.keystore 文件位置 >" （请参阅步骤 2 （第 89 页））
keystorePass="< 密码 >"

取消以下命令行的注释：

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

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**) 将证书导出为 ***.pfx** 文件（包含私钥）。

- 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 installation directory>\conf\security\<pfx file name> -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

打开位于 **<Configuration Manager 安装目录 >\servers\server-0\conf** 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="../../java/lib/security/tomcat.keystore"
keystorePass="password" />

取消以下命令行的注释：

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

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。

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。

例如：java/{os name}/lib。

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**。
2. 将 **hpcert.cer** 复制到服务器计算机的 **<Configuration Manager 安装目录 >\java\bin** 文件夹中。
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：

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

4. 按照下述操作修改 **server.xml** 文件 （位于 **<Configuration Manager 安装目录 >\servers\server-0\conf** 文件夹中）：

   a. 执行步骤 5 （第 90 页）中所述的变更。

   b. 在这些更改之后，将下面的属性添加到 HTTPS 连接器：

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

c 设置 clientAuth="true"。

5 按照步骤 7 （第 90 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。

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 90 页）的 “使用自签名证书在服务器计算机上启用 SSL”（第 88 页）中所述，或直至步骤 5 （第 92 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 91 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 >:8180/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。

1 按照 “使用自签名证书在服务器计算机上启用 SSL”（第 88 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** 指明包含了用户名的证书字段。可用选项包括：

- **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。可用选项包括：

- **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**，并编辑以下属性：

- 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 88 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。

客户端证书

本节包含以下内容：

客户端证书信息

本节描述了客户端证书信息，以及如何从客户端证书取得用户标识符。

➤ 用户标识符

用户标识符是属于用来识别用户身份的客户端证书信息中的独一无二部分。

➤ 基本客户端证书信息

基本客户端证书信息包括以下内容：

证书字段	描述
版本	编码证书的版本。 示例：1 (0x1)
序列号	由证书授权机构分配到每个证书的正整数。 示例：0 (0x0)
签名算法	由证书授权机构用于签名证书的算法的算法标识符。 示例：md5WithRSAEncryption
发行者	已签名并发出证书的实体。 示例：CN=Issuer, C=US, ST=NY, L=New York, O=Work Organization, O=example.com

证书字段	描述
有效性	证书授权机构保证维护有关证书状态信息的时间间隔： ➤ **起始时间**。指定证书有效性期开始的日期。 示例：Nov 25 04:34:49 2009 GMT ➤ **截止时间**。指定证书有效性期结束的日期。 示例：Nov 25 04:34:49 2010 GMT
主题	与主题公钥字段中存储的公钥关联的实体。
Subject Public Key Info	用于承载公钥，并识别出该公钥使用的算法（例如， RSA、 DSA 或 Diffie-Hellman）。

有关详细信息，请参阅 Internet X.509 公钥基础结构证书和证书废止列表 (CRL) 配置文件：

http://tools.ietf.org/html/rfc5280

➤ **“主题”字段**

“主题”字段 （也称为主题区分名称或 SubjectDN）识别与公钥关联的实体。

“主题”字段包含以下相关属性 （还可以包含其他属性）：

主题属性	主题属性描述	示例
CN	常见名称	CN=Bob BobFamily
emailAddress	电子邮件地址	*emailAddress=bob@example.com*
C	国家 / 地区名称	C=US
ST	州或省名称	ST=NY

主题属性	主题属性描述	示例
L	地点名称	L=New York
O	组织名称	O=Work Organization
OU	组织单位名称	OU=Managers

要从主题中检索用户标识符，可以使用整个 SubjectDN 字段或 SubjectDN 属性。

➤ 客户端证书信息扩展

通过为 X.509 v3 证书定义的扩展，可以将其他属性关联到用户或公钥，也可以管理证书授权机构之间的关系。“主题备用名称”字段可以包含用户标识符。

➤ “主题备用名称”字段

通过主题备用名称扩展可以将身份与证书主题绑定。这些身份可以额外添加到证书的主题字段中，也可以替换证书主题字段中的身份。

“主题备用名称”字段可以包含以下身份：

身份	示例
otherName	其他名称：Principal Name= *bobOtherAltName@example.com*
rfc822Name	RFC822 Name =*bobRFC822AltName@example.com*
dNSName	DNS Name=example1.com
x400Address	
directoryName	目录地址： E=*bobDirAltName@example.com*, CN=bob, OU=Gold Ballads, O=Gold Music, C=US
ediPartyName	
uniformResourceIdentifier	URL=http://example.com/

身份	示例
iPAddress	IP Address=192.168.7.1
registeredID	Registered ID=1.2.3.4

要从主题备用名称中检索用户标识符，可以使用上述任一身份。

配置

Configuration Manager 通过 LW-SSO 利用客户端证书的用户标识符。以下属性由客户端证书处理程序用于配置 LW-SSO，以利用用户标识符：

要从客户端证书利用信息， Configuration Manager 应当配置如何检索用户标识符。

应当决定以下项目：

- 应使用的字段：SubjectDN 或主题备用名称？
- 应使用整个字段或仅使用字段的一部分？
- 如果使用输入字段的一部分，则用一个值表示：提供 SubjectDN 的主题属性，或提供主题备用名称的身份。

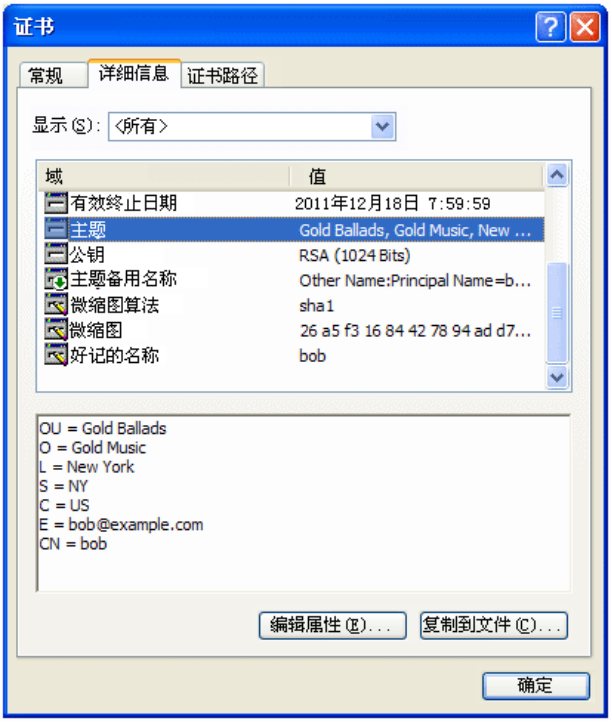
以下属性由客户端证书处理程序用于配置 LW-SSO：

属性名称	描述
enabled	指定是启用还是禁用处理程序。 **重要信息**：强烈建议将此值显式设置为 False ；只有在要求客户端证书验证时，才启用此处理程序。
userIdentifierRetrieveField	此参数表示包含用户标识符的证书字段。选项包括：**SubjectDN** 或 **SubjectAlternativeName**。

属性名称	描述
userIdentifierRetrieveMode	参数 userIdentifierRetrieveMode 表示用户标识符是相关字段的全部内容或是仅为它的一部分。选项包括：**EntireField** 或 **FieldPart**。
userIdentifierRetrieveFieldPart	如果 **userIdentifierRetrieveMode** 的值为 **FieldPart**，则此参数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。 **注意**：**userIdentifierRetrieveMode** 设置为 **FieldPart** 时，此属性不可为空。此外，**userIdentifierRetrievField** 设置为 **SubjectAlternativeName** 时，也不可为空。

示例

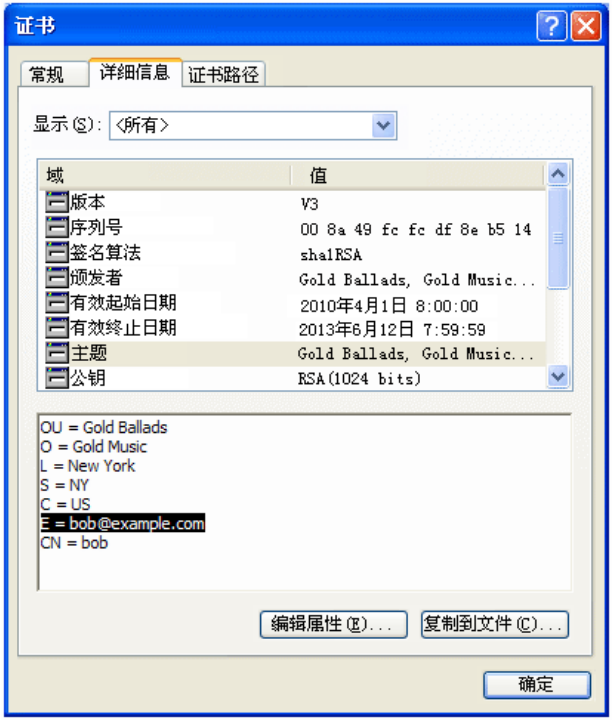
➤ 主题用于保留用户标识符



以下示例显示如何配置处理程序以从整个 SubjectDN 取得用户标识符：

```
<in-clientCertificate userIdentifierRetrieveField="SubjectDN"
userIdentifierRetrieveMode="EntireField" />
```

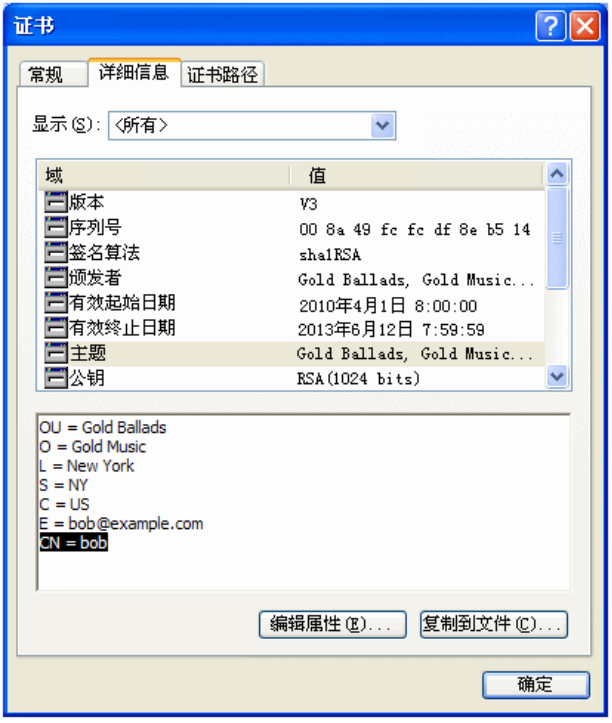
➤ **主题的电子邮件字段用于保留用户标识符**



使用在客户端证书图例中看到的字段名称。以下示例显示如何配置处理程序以从主题的电子邮件字段取得用户标识符：

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

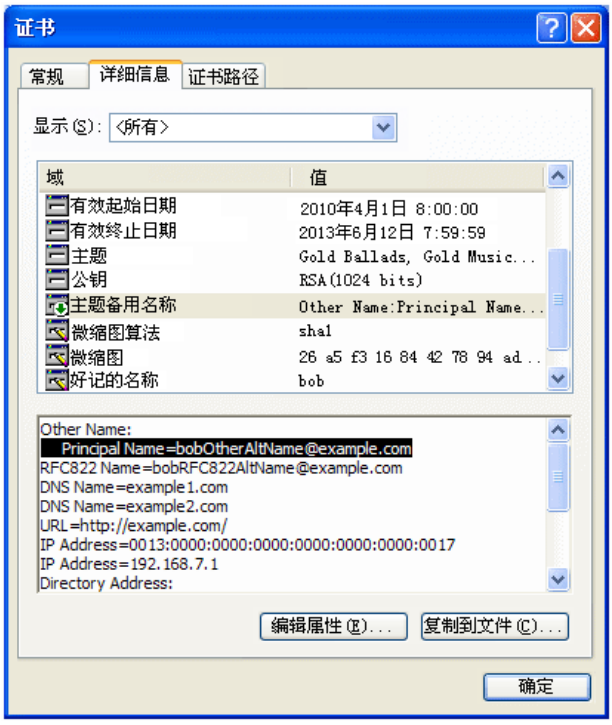
➤ **主题的命令名称字段用于保留用户标识符**



使用在客户端证书图例中看到的字段名称。以下示例显示如何配置处理程序以从主题的自定义名称字段取得用户标识符：

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

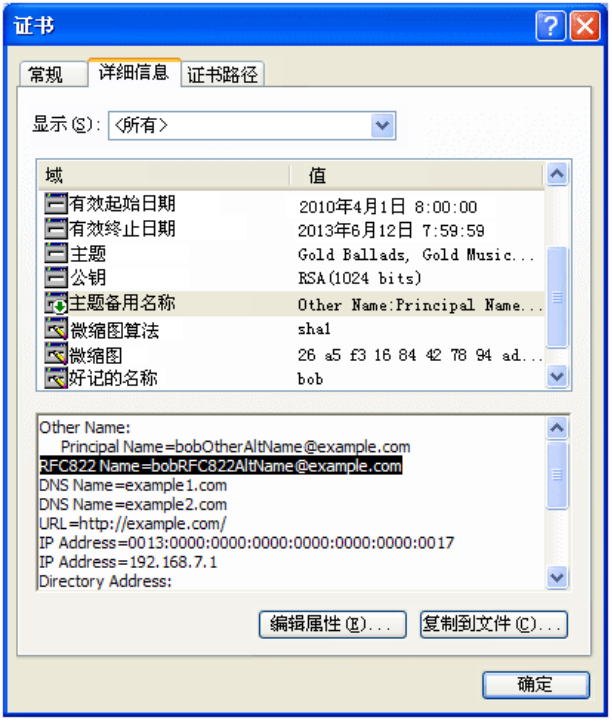
➤ **主题备用名称的 otherName 身份用于保留用户标识符**



使用在客户端证书图例中看到的身份名称。以下示例显示如何配置处理程序以从主题备用名称的 otherName 身份取得用户标识符：

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Principal
Name" />
```

➤ **主题备用名称的 RFC822Name 身份用于保留用户标识符**



使用在客户端证书图例中看到的身份名称。以下示例显示如何配置处理程序以从主题备用名称的 RFC822Name 身份取得用户标识符：

```
<in-clientCertificate userIdentifierRetrieveField="SubjectAlternativeName"
userIdentifierRetrieveMode="FieldPart" userIdentifierRetrieveFieldPart="Principal
Name" />
```

配置 Configuration Manager，以便与使用 SSL 的 UCMDB 结合使用

您可以配置 Configuration Manager，以便与使用安全套接字层 (SSL) 的 UCMDB 结合使用。默认情况下，将启用 UCMDB 中端口 8443 上的 SSL 连接器。

要导出服务器证书并将其导入到客户端信任存储，请执行以下操作

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

```
keytool -export -alias hpcert -keystore <UCMDB server dir>
\conf\security\server.keystore  -storepass hppass -file <certificatefile>
```

2 将证书导入 Configuration Manager 信任存储 （默认 jre 信任存储）：

```
<CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias hpcert -keystore
<CM_JAVA_HOME>\lib\security\cacerts -storepass changeit -file
<certificatefile>
```

3 设置 Configuration Manager 中的 UCMDB 连接属性：

转到“系统”>“设置”>“集成”>“UCMDB Foundation”>“UCMDB Foundation”。将连接策略设置为 **HTTPS**， UCMDB 服务器端口设置为 UCMDB HTTPS 端口，并将 UCMDB 访问 URL 设置为 https://<HostName>:8443。

4 保存并激活配置集。重新启动 Configuration Manager。

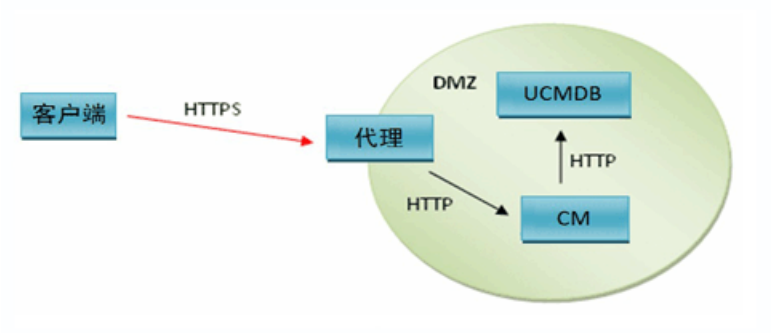
要配置 Configuration Manager，以便与其他使用安全套接字层 (SSL) 的产品（比如负载平衡器）结合使用，请通过运行以下命令将产品的安全证书导入 Configuration Manager 信任存储 （默认 jre 信任存储）：

```
<CM_JAVA_HOME>\bin\keytool -import -trustcacerts -alias <alias> -keystore
<CM_JAVA_HOME>\lib\security\cacerts -storepass changeit -file <certificatefile>
```

反向代理

Configuration Manager 和 UCMDB 位于 DMZ 中时，建议配置系统以结合反向代理服务器使用。配置步骤与用于配置 UCMDB 结合反向代理一起使用的步骤相同。要启用到 Configuration Manager 的访问，需要将路径 **/cnc** 和 **/bsf** 映射到安装 Configuration Manager 的远程服务器的 URL 上。

下面的图片显示了 Configuration Manager 的反向代理配置过程：



例如，如果反向代理是 Apache 服务器，则将下行添加到 **Apache2.2\conf\extra\httpd-ssl.conf** 文件，然后重新启动 Apache 服务器：

```
ProxyPass /cnc http://<CM_HOSTNAME>:<CM_HTTP_PORT>/cnc
ProxyPassReverse /cnc http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/cnc
ProxyPass /bsf http://< CM_HOSTNAME >:<CM_HTTP_PORT>/bsf
ProxyPassReverse /bsf http:// <CM_HOSTNAME>:<CM_HTTP_PORT>/bsf
```

不同类型的反向代理可能需要不同的配置步骤，有关详细信息，请参阅您的代理服务器文档。

要配置 Configuration Manager 的反向代理，请执行以下操作：

更新 **<Configuration Manager 安装目录 >\conf** 文件夹中的 **client-config.properties** 文件，如下所示：

```
bsf.server.url=https://<proxy-server-name>:443/bsf
```

Apache 代理的默认 HTTPS 端口是 443。

第 II 部分

附录

A

容量限制

下表列出了 Configuration Manager 的容量限制。

最大视图数	100
最大策略数	300
每个视图的最大组合 CI 数	5000
最大并发用户数	50
“配置分析”模块中的最大组合 CI 数	1000

B

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 113 页）
- “LW-SSO 安全警告”（第 115 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切换到另一个应用程序时，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。

有关 LW-SSO 的疑难解答信息，请参阅“LW-SSO - 疑难解答和限制”（第 130 页）。

本节包括以下主题：

- “LW-SSO 令牌到期”（第 114 页）
- “建议的 LW-SSO 令牌到期配置”（第 114 页）
- “GMT 时间”（第 114 页）

➤ “多域功能”（第 114 页）

➤ “获取 URL 功能的 SecurityToken”（第 114 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、传输以及保存时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违反安全行为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。

C

疑难解答

本章包括以下内容：

常见疑难解答和限制

限制

在注销 Configuration Manager 然后再次登录前，您不会看到在 UCMDB 中创建的新 CI 类型。

疑难解答

问题。节点 CI 类型的 **name** 属性不符合“更改受监控的”要求，而且未在 CI 授权期间复制为授权状态。如果安装 Configuration Manager 版本 9.20 而没有 UCMDB 的内容包 9，则此现象会发生。

解决办法。请进行下列任一操作：

- 手动设置 **name** 属性，使其符合 UCMDB CI 类型管理器中的“更改受监控的”要求。
- 安装内容包 9。

问题。启动 Configuration Manager 服务时，收到以下错误消息：

> Windows could not start the HP Universal CMDB Configuration Manager on Local Computer. For more information, review the System Manager Event log. If this is a non-Microsoft service, contact the service vendor, and refer to service-specific error code 0.

解决办法。执行以下操作：

1. 转到 **<Configuration Manager 安装目录>\cnc\bin**，执行以下命令：

   edit-server-0.bat

2. 选择“启动”选项卡。在“模式”下拉列表（在底部）中，选择 **jvm** 而不选择 **exe**。
3. 选择“关闭”选项卡。在“类”字段中，将最后一个名称从 **Boostrap** 更改为 **Bootstrap**。
4. 单击“确定”。
5. 运行服务。

部署管理器 - 疑难解答和限制

要对部署管理器进行疑难解答，请打开以前会话的会话日志，您可以在以下目录中找到：

%temp%\HP\ucmdb-dm\Workspace\Sessions

常规重新部署准则

在安装期间，通过单击位于每个部署的组件旁的详细信息按钮，记录下出现在部署管理器“验证”页面上的警告和错误。

一旦在部署期间发现问题并找到了解决方法，请执行以下步骤：

1 卸载部署的产品并重新启动计算机。

2 重新启动部署管理器并重新输入所有配置。

部署失败问题

问题。部署期间的权限错误。

会话日志指明在创建新架构时，存在数据库用户权限问题。

解决办法。要创建新数据库，必须有相关权限。确保在部署中使用的用户凭据具有用于创建表空间和架构的权限。

问题。 UCMDB 中的架构 / 数据库配置失败。

会话日志指明部署管理器未能创建架构或数据库。

解决办法：

注意：在创建新 UCMDB 架构之后，您无法连接到现有 UCMDB 历史记录架构（与数据库服务器类型无关）。

确保 UCMDB 架构和 UCMDB 历史记录架构并未使用以下连接类型：

- UCMDB 架构 - 创建新架构
- UCMDB 历史记录架构 - 连接到现有架构

问题。 UCMDB 中的架构 / 数据库配置失败。

会话日志指明无法创建架构。

解决办法。打开 session.log，并找到以下消息：
SQL error executing statement CREATE USER <schema name>

在部署管理器的 “数据库配置”页面中命名 Oracle 架构时，请确保仅使用字母 (a-z)、数字 (0-9) 和连字号 （“-”）。

问题。由于空间不足，无法创建架构。

解决办法。增加架构或数据库上的可用空间量。使用由 Oracle 和 Microsoft 提供的标准管理接口。

问题。数据库配置失败，错误内容为：
NT AUTHORITY\ANONYMOUS LOGON – Could not connect to database.

选择带有为 UCMDB 数据库配置的 NTLM 身份验证的 MSSQL 服务器时，数据库配置失败会导致部署失败。

解决办法。在 localhost 计算机 （唯一支持 NTLM 身份验证的地方）上部署 UCMDB。

问题。创建新数据库时， Configuration Manager 数据库配置失败。

部署管理器的详细信息面板中可能出现以下错误消息：

Failed to create Oracle schema due to error: ORA-01031: insufficient privileges

或

Failed to create a schema to the database: machineName.
Reason: ORA-01919: role 'RESOURCE' does not exist

解决办法。确保数据库用户有以下角色特权：

- 连接
- 资源

问题。由于目标主机计算机上磁盘空间不足，未能运行部署。

解决办法。登录目标主机计算机，并确保具有成功部署所需的足够磁盘空间：

- UCMDB 需要 1GB 可用空间
- Configuration Manager 需要 1GB 可用空间
- DDMA 需要 1GB 可用空间

注意：除特定产品要求以外，还需要 1GB 可用空间进行临时文件处理。

问题。 Ping UCMDB 实用程序失败。

此实用程序从 Configuration Manager 计算机执行，并验证到现有 UCMDB 实例的连接是否可用。打开 session.log，并找到以下消息：
Failed to test connection due to error: java.net.ConnectException: Connection refused: connect.

解决办法：

- 确保目标 UCMDB 上的端口 8080 没有被 Windows 防火墙阻止。
- 确保 UCMDB 服务器可从 Configuration Manager 计算机访问，且 UCMDB 部署已成功完成并在运行中。

主机计算机连接不可用

问题。 RPC 不可用或未知错误。

按 “测试连接”按钮导致 RPC 不可用错误。

解决办法。如果主机名不正确，请更正；确保 WMI 服务和服务器服务正在运行中，而且 Windows 防火墙没有阻止对 WMI 接口的访问。

禁用 Windows 防火墙或添加防火墙例外可启用远程管理访问。

要执行此操作，请打开 “防火墙”控制面板，并选择 “入站规则”。启用所有文件和打印机、 WMI 规则和端口 8080。

测试连接失败

问题。访问被拒绝。

由于用户名和 / 或密码不正确、无效的 DNS 设置或因为在部署中使用的用户名在目标主机计算机上没有管理凭据，访问被拒绝。

解决办法。确保指定的用户凭据正确，且用户具有目标主机计算机的管理凭据。

无法访问应用程序

问题。成功部署之后 - 无法访问应用程序 （UCMDB 或 Configuration Manager）。

解决办法。确保以下 UCMDB 和 Configuration Manager 服务存在并正在运行。

- **UCMDB_Server** 服务
- **HPUCMDBCMoasisSNAPSHOTserver0** 服务

检查位于会话目录中的部署日志是否存在错误。

LW-SSO 已禁用

问题。成功部署 - 但 LW-SSO 功能被禁用。

解决办法。确保 LW-SSO init 字符串和域在 UCMDB 与 Configuration Manager（如情况允许，则还包括 OO）上是相同的。

通过以下方法检查产品中的 LW-SSO 配置设置：

- Configuration Manager – 打开 **lwssofmconf.xml** 文件并检查域和 init 字符串定义。文件位于 **<Configuration Manager 安装目录>\conf** 文件夹中。
- UCMDB – 打开 UCMDB 并选择“管理器”>“管理”>“基础结构设置管理器”。

如果 Configuration Manager 和 UCMDB 在有不同 DNS 域的主机计算机上驻留，请确保 “信任域”设置中包括这些 DNS 域并在两种产品中均已启用。

要接收其他有关部署的信息，可以在调试模式中启用部署管理器。调试模式提供其他有关部署的信息。

要启用调试模式：

1. 在运行部署管理器之后，打开浏览器窗口，并在地址栏中输入 %temp%。
2. 导航到 **hp\ucmdb-dm** 文件夹。

3 在文本编辑器中打开 **ini** 文件，并将以下属性添加到文件的最后一行：

–Ddebug.mode=true

4 使用 **%temp%\HPmdb-dmmdb-dm.exe** 运行部署管理器。

访问 Configuration Manager - 疑难解答和限制

限制

➤ 一旦更改 Configuration Manager Tomcat 服务器上的时间，则必须重新启动服务器才能更新服务器上的时间。

疑难解答

问题。在更改 “系统” > “设置” 中的配置集后，服务器将不会启动。

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：

```
<Configuration Manager 安装目录 >\bin\export-cs.bat < 数据库属性 > --history
```

其中，< **数据库属性** > 可以通过指向 <**Configuration Manager 安装目录** >**conf\database.properties** 文件或指定每个数据库属性来进行指定。例如：

```
cd <Configuration Manager 安装目录 >\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：

```
<Configuration Manager 安装目录 >\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** 的配置集导出为 **mydump.zip** 文件，请输入以下命令：

```
cd <Configuration Manager 安装目录 >\bin export-cs.bat -p
..\conf\database.properties -i 491520 -f mydump.zip
```

3 停止 Configuration Manager 服务。

4 运行以下命令以导入并激活上一个配置集：

```
<Configuration Manager 安装目录 >\bin\import-cs.bat
< 数据库属性 > -i < 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 “系统” > “设置” > “集成” > “UCMDB Foundation” > “UCMDB Foundation”，更改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 输入以下文本：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，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 安装目录 >\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 **<Configuration Manager 安装目录 >\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：

如果登录所用的 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...

将其替换为：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：**<Configuration Manager 安装文件夹 >\servers\server-0\conf\server.xml** 并更新相关端口：
  - HTTP (8180)：第 69 行
  - HTTPS (8443)：第 71、 90 行

问题。接收到 “内存不足”消息。

解决办法。执行以下更改服务器启动参数的操作：

1 运行以下批处理文件：

<Configuration Manager 安装目录 >/bin/edit-server-0.bat

2 更改以下设置：

-Dapplication.ms=< 初始内存池大小 >
-Dapplication.mx=< 最大内存池大小 >

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。它可以在 “系统” > “设置” 中进行配置。
- 执行 JMX 调用以便对相关视图运行脱机分析计算。
- 转到 “管理” > “策略” > “配置策略”。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” > “UCMDB Foundation” 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 “单一登录 (SSO)”（第 70 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” > “UCMDB Foundation”。

解决办法。请按以下步骤操作：

1 转到“系统”>“设置”>“集成”>“UCMDB Foundation”>“UCMDB Foundation”。

2 将方括号添加到 UCMDB 访问 URL 中的 IP 地址。 URL 的格式应为：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。

LW-SSO - 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。

疑难解答

问题：在登录后没有创建 LW-SSO cookie。

- **可能原因**：在配置的 LW-SSO 元素中没有正确定义非空域。
- **可能的解决办法**：确保在配置的 LW-SSO 元素中定义的域等于应用程序的域。
- **可能原因**：作为参数传递到 enableSSO 函数的非空域不正确。
- **可能的解决办法**：确保作为参数传递到 enableSSO 函数的域等于应用程序的域。
- **可能原因**：在 LW-SSO 配置中定义域时，您没有在登录 URL 中使用完全限定域名 (FQDN) 访问应用程序 （例如：http://192.168.12.13/WebApp）。
- **可能的解决办法**：确保在登录 URL 中使用完全限定域名 (FQDN) 访问应用程序（例如：http://myserver.companydomain.com/WebApp）。

问题：LW-SSO 未能创建 AutoCookieCreation 功能的 cookie。

- **可能原因**：在配置的 LW-SSO 元素中的域没有正确进行定义。
- **可能的解决办法**：确保在配置的 LW-SSO 元素中定义的域等于应用程序的域。

问题：LW-SSO 令牌未经验证。

- **可能原因**：两个应用程序在配置的加密元素 （或其他加密参数）中有不同的 initString 参数。
- **可能的解决办法**：在这两个应用程序（除 LW-SSO 创建元素中的所有其他加密参数以外）中使用相同的 initString。
- **可能原因**：两个应用程序之间的 GMT 时间差异大于 15 分钟。

- **可能的解决办法**：确保所有参与 LW-SSO 集成的应用程序均设置为相同的 GMT 时间，并且最大差值为 15 分钟。
- **可能原因**：在配置的 LW-SSO 元素中有域为空，且您访问了其他具有相同 DNS 域的计算机上的第二个应用程序。
- **可能的解决办法**：确保在配置的 LW-SSO 元素中定义的域等于应用程序的域。
- **可能原因**：在配置的 LW-SSO 元素中有域未定义，且您访问了其他具有相同 DNS 域的计算机上的第二个应用程序。
- **可能的解决办法**：将域添加到 LW-SSO 元素并确保定义的域与应用程序的域等同。

问题：LW-SSO 未能在多域环境中验证 LW-SSO 令牌

- **可能原因**：在某个应用程序的配置中的域在 LW-SSO 元素中未正确定义。
- **可能的解决办法**：在应用程序的配置的 LW-SSO 元素中定义的域必须与实际使用的应用程序域相同。
- **可能原因**：在某个应用程序的配置中，未在 trustedHosts 设置 （或 protectedDomains 设置）中正确定义域。
- **可能的解决办法**：确保所有应用程序配置的 trustedHosts 设置 （或 protectedDomains 设置）中的域均正确定义。
- **可能原因**：使用 Internet Explorer 6.x、7.x 或 8.x 时， LW-SSO 会话 cookie 被阻止或拒绝。
- **可能的解决办法**：在计算机上，将所有 LW-SSO 服务器添加到 Internet Explorer 安全区域中的“Intranet”/“信任”区域（“工具”>“Internet 选项”>“安全”>“本地 Intranet”>“站点”>“高级”）。这将允许接受所有 cookie。

- **可能原因：**部分应用程序在配置的加密元素 （或其他加密参数）中有不同 initString 参数。
- **可能的解决办法：**在所有应用程序（除 LW-SSO 创建元素中的所有其他加密参数以外）中使用相同的 initString。
- **可能原因：**某些应用程序的 GMT 时间差异大于 15 分钟。
- **可能的解决办法：**确保所有参与 LW-SSO 集成的应用程序均设置为相同的 GMT 时间，并且最大差值为 15 分钟。
- **可能原因：**多域链接从受保护的 (HTTPS) 资源链接到不受保护的 (HTTP) 资源。
- **可能的解决办法：**从一个域链接或跨越到另一个域时，请确保第一个链接 / 跨越请求是从一个受保护的资源 (HTTPS) 到另一个受保护的资源 (HTTPS)。

IPv6 支持 - 疑难解答和限制

限制

- URL 不能包含 IP 地址。
- 操作系统必须支持 IPv6 和 IPv4。如果不支持或未关闭 IPv4 地址，则您将无法登录到 Configuration Manager 服务器。
- 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。

疑难解答

问题。在安装期间配置 IPv6 地址的 UCMDB 连接后，“管理”>“UCMDB Foundation”菜单选项无法正常使用。

解决办法。执行以下操作：

1. 转到“系统”>“设置”>“集成”>“UCMDB Foundation”>“UCMDB Foundation”。
2. 将方括号添加到 UCMDB 访问 URL 字段中的 IP 地址。 URL 的格式应为：http://[x:x:x:x:x:x:x:x]:8080/ucmdb-ui/。
3. 保存并激活配置集。
4. 重新启动 Configuration Manager。

身份验证 - 疑难解答和限制

本节说明已知的身份验证问题。

问题：在重定向到身份验证点后进行应用程序的身份验证时，收到错误 500。

- **可能原因：**Configuration Manager WAR 和 BSF WAR 在配置的加密元素中有不同的 initString 参数 （或其他加密参数）。

- **可能的解决办法：**在这两个应用程序（除 LW-SSO 创建元素中的所有其他加密参数以外）中使用相同的 initString。

问题：在重定向到身份验证点后进行应用程序的身份验证时，无法看到登录表单。

解决办法：使用 Internet Explorer 版本 6.0、7.0 或 8.0 浏览器时，Configuration Manager 身份验证会话 cookie 被阻止或拒绝。在计算机上，将 Configuration Manager 服务器添加到 Internet Explorer 安全区域中的“Intranet/ 信任”区域（“工具”>“Internet 选项”>“安全”>“本地 Intranet”>“站点”>“高级”）。这将允许接受所有 cookie。

问题：在身份验证之后，接收到错误 403。

- **可能原因：**在应用程序配置的 LW-SSO 元素中未正确定义域。
- **可能的解决办法：**确保在应用程序配置的 LW-SSO 元素中定义的域等于应用程序的域。
- **可能原因:**在 LW-SSO 配置中定义域时，您没有在登录 URL 中使用完全限定域名 (FQDN) 访问应用程序 （例如：http://192.168.12.13/WebApp）。
- **可能的解决办法：**确保在登录 URL 中使用完全限定域名 (FQDN) 访问应用程序 （例如：http://myserver.companydomain.com/WebApp）。

问题：在身份验证之后，将显示“获取 Acegi 用户详细信息”页面。

解决办法：使用 Internet Explorer 版本 6.0、7.0 或 8.0 浏览器时，Configuration Manager 身份验证会话 cookie 被阻止或拒绝。在计算机上，将 Configuration Manager 服务器添加到 Internet Explorer 安全区域中的“Intranet/ 信任”区域（“工具”>“Internet 选项”>“安全”>“本地 Intranet”>“站点”>“高级”）。这将允许接受所有 cookie。