

安装和配置指南

vCenter Orchestrator 4.0

ZH_CN-000192-00

vmware[®]

最新的技术文档可以从 VMware 网站下载：

<http://www.vmware.com/cn/support/pubs/>

VMware 网站还提供最近的产品更新信息。

您如果对本文档有任何意见或建议，请把反馈信息提交至：

docfeedback@vmware.com

版权所有 © 2009 VMware, Inc. 保留所有权利。本产品受美国和国际版权及知识产权法的保护。VMware 产品受一项或多项专利保护，有关专利详情，请访问 <http://www.vmware.com/go/patents-cn>。

VMware 是 VMware, Inc. 在美国和/或其他法律辖区的注册商标或商标。此处提到的所有其他商标和名称分别是其各自公司的商标。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

北京办公室
北京市海淀区科学院南路 2 号
融科资讯中心 C 座南 8 层
www.vmware.com/cn

上海办公室
上海市浦东新区浦东南路 999 号
新梅联合广场 23 楼
www.vmware.com/cn

广州办公室
广州市天河北路 233 号
中信广场 7401 室
www.vmware.com/cn

目录

关于本文档	5
1 VMware vCenter Orchestrator 简介	7
Orchestrator 平台的主要功能特征	7
Orchestrator 用户角色和相关任务	8
Orchestrator 架构	9
2 Orchestrator 系统要求	11
Orchestrator 的硬件要求	11
Orchestrator 支持的操作系统	11
支持的目录服务	11
Orchestrator 支持的浏览器	12
Orchestrator 数据库要求	12
3 随 vCenter Server 安装 Orchestrator	13
在 Microsoft Windows 上安装 Orchestrator	13
4 升级 vCenter Server 之后升级 Orchestrator 应用程序	15
5 Orchestrator 数据库设置	17
在 Windows 上启用 Oracle 数据库支持	17
在 Windows 上启用 MySQL 数据库支持	18
MySQL 数据库参数	19
6 配置 Orchestrator	21
启动 Orchestrator 配置服务	21
登录 Orchestrator 配置界面	22
更改默认密码	22
配置网络连接	23
默认配置端口	23
导入 vCenter SSL 证书	24
配置 LDAP 设置	25
生成 LDAP 连接 URL	25
指定浏览凭据	26
定义 LDAP 查询方式	27
设置连接超时	28
密码加密和哈希机制	28
配置数据库连接	29

服务器证书	30
创建自签署服务器证书	30
获取由证书颁发机构签署的服务器证书	30
导出服务器证书	31
更改自签署服务器证书	32
配置默认插件	32
定义默认 SMTP 连接	33
配置 SSH 插件	34
配置 vCenter 4.0 插件	34
Orchestrator 服务器的访问权限	35
导入 vCenter Server 许可证	35
启动 Orchestrator 服务器	36
设置服务超时参数	36
导出 Orchestrator 配置	37
Orchestrator 配置文件	37
导入 Orchestrator 配置	38
配置事件和执行的数目	38
安装应用程序	39
启动已发布的 Web 视图	40
定义服务器日志级别	40
索引	41

关于本文档

《VMware vCenter Orchestrator 4.0 安装和配置指南》提供有关如何安装、升级和配置 VMware® vCenter Orchestrator 的信息和说明。

目标读者

目标读者为熟悉虚拟机技术和数据中心操作的高级 vCenter 管理员和经验丰富的系统管理员。

文档反馈

VMware 欢迎您提出宝贵建议，以便改进我们的文档。如有意见，请将反馈发送到 docfeedback@vmware.com。

技术支持和教育资源

您可以获得以下技术支持资源。有关本文档和其他文档的最新版本，请访问：
<http://www.vmware.com/cn/support/pubs>。

在线支持和电话支持

要通过在线支持提交技术支持请求、查看产品和合同信息以及注册您的产品，请访问 <http://www.vmware.com/cn/support>。

客户只要拥有相应的支持合同，就可以通过电话支持，以最快的速度获得对高优先级问题的答复。请访问
http://www.vmware.com/cn/support/phone_support.html。

支持服务项目

要了解 VMware 支持服务项目如何帮助您满足业务需求，请访问
<http://www.vmware.com/cn/support/services>。

VMware 专业服务

VMware 教育服务课程提供了大量实践操作环境、案例研究示例，以及用作作业参考工具的课程材料。这些课程可以通过现场指导、教室授课的方式学习，也可以通过在线直播的方式学习。关于现场试点项目及实施的最佳实践，VMware 咨询服务可提供多种服务，协助您评估、计划、构建和管理虚拟环境。要了解有关教育课程、认证计划和咨询服务的信息，请访问
<http://www.vmware.com/cn/services>。

VMware vCenter Orchestrator 简介

VMware vCenter Orchestrator 是一个开发和过程自动化平台，提供可扩展的工作流库，用于创建和运行自动化的可配置过程来管理 VMware vCenter 基础架构。

Orchestrator 公开了 vCenter Server API 中的每一步操作，以便您可以将所有这些操作整合到自动化过程中。通过 Orchestrator 的开放式插件架构，您还可以将其与其他管理解决方案集成在一起。

本章讨论了以下主题：

- 第 7 页，“Orchestrator 平台的主要功能特征”
- 第 8 页，“Orchestrator 用户角色和相关任务”
- 第 9 页，“Orchestrator 架构”

Orchestrator 平台的主要功能特征

Orchestrator 由三个截然不同的层组成：一个可提供耦合工具所需常用功能的耦合平台、一个集成了子系统控制功能的插件架构和一个既存过程库。Orchestrator 是一个开放式平台，它不但可以通过添加新插件和库进行扩展，还可以通过一组 API 集成到更大型的 SOAP 架构中。

下面列出了 Orchestrator 的主要功能特征。

持久性	使用生产级外部数据库存储相关信息，如过程、状况和配置信息。
集中式管理	Orchestrator 提供集中过程管理方式。通过基于应用程序服务器的平台（以及完整的版本历史记录），您可以将脚本和与过程相关的基元放在同一位置。采用这种方式，可以防止未实现版本管理和适当变更控制的脚本在您的服务器上传播。
检查点	过程的每一个步骤都将保存在数据库中，这使您可以重新启动服务器而不会丢失状态和相关环境。此功能对于长时间运行的过程特别有用。
版本管理	所有的 Orchestrator 平台对象都具有相关的版本历史记录。通过此功能，您可以在将过程分配到不同的项目阶段或位置时，执行基本的变更管理操作。
脚本引擎	Mozilla Rhino JavaScript 引擎提供一种为 Orchestrator 平台创建新的构建块的方法。该脚本引擎包含基本版本控制、变量类型检查、命名空间管理和异常情况处理等增强功能。它可在以下构建块中使用： <ul style="list-style-type: none">■ 操作■ 工作流■ 策略

- 工作流引擎** 通过工作流引擎，您可以捕获业务过程。它使用下列方法之一来逐步实现自动化：
- 库的构建块
 - 客户提供的构建块
 - 插件
- 用户、调度任务或策略均可启动工作流。
- 策略引擎** 使用策略引擎可以监控并生成事件以应对不断变化的情况。策略可以聚合来自平台或任何插件的事件，因此，您可以处理与任何集成技术有关的不断变化的情况。
- Web 2.0 前端** Web 2.0 前端可以采用多种新方式表现，具备较强的灵活性。它提供一个用户可自定义的组件库来访问 vCO 耦合对象，并且使用 Ajax 技术动态更新内容，而无需重新加载整个页面。
- 安全性** Orchestrator 可提供以下高级安全功能：
- 公共密钥基础设施 (PKI)，可用于签署和加密在服务器之间导入和导出的内容。
 - 数字权限管理 (DRM)，可用于控制导出内容的查看、编辑和重新分配方式。
 - 安全套接字层 (SSL)，可用于加密桌面客户端和服务器之间的通信和通过 HTTPS 访问 Web 前端。
 - 高级访问权限管理，可用于控制对过程和由这些过程操作的对象的操作权限。

Orchestrator 用户角色和相关任务

vCenter Orchestrator 会根据以下这三种全局用户角色的特定职责提供不同的工具和界面：管理员、开发人员和最终用户。

- 管理员** 此角色对所有的 Orchestrator 平台功能都具有完全的访问权限。基本的管理任务包括：
- 安装和配置 Orchestrator
 - 管理 Orchestrator 和应用程序的访问权限
 - 导入和导出软件包
 - 启用和禁用 Web 视图
 - 运行工作流和调度任务
 - 管理导入元素的版本控制
- 开发人员** 此角色的用户拥有访问 Orchestrator 客户端界面的权限并具有以下职责：
- 开发应用程序以扩展 Orchestrator 平台功能
 - 通过自定义现有工作流和创建新的工作流实现过程自动化
 - 使用 Web 2.0 技术自定义这些过程的 Web 前端
- 最终用户** 此角色的用户只拥有访问 Web 前端的权限。他们可以运行和调度工作流和策略。

Orchestrator 架构

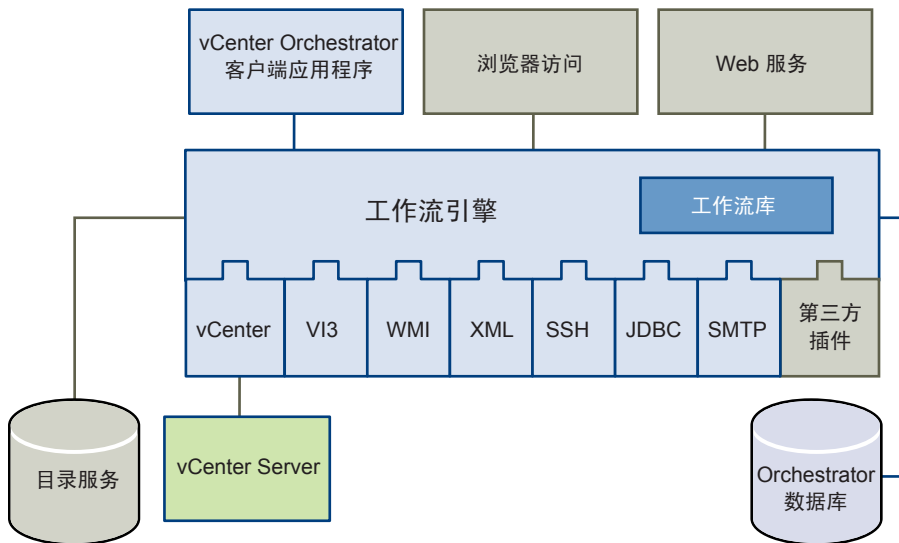
Orchestrator 包含工作流库和工作流引擎，可用于创建和运行自动执行耦合过程的工作流。可以在不同技术对象上运行工作流，Orchestrator 通过一系列插件访问这些技术。

Orchestrator 提供了一组标准插件（包括 VMware vCenter Server 4.0 的插件），使您可以耦合这些插件所在的不同环境中的任务。

此外，Orchestrator 还采用了一个开放式架构，使您可以将外部第三方应用程序插入耦合平台。您可以在由您自己定义的插件技术对象上运行工作流。Orchestrator 可以连接到目录服务服务器以管理用户帐户，此外还可以连接到数据库以存储所运行的工作流的信息。您可以通过 Orchestrator 客户端界面、Web 浏览器或 Web 服务访问 Orchestrator 及其公开的工作流和对象。

图 1-1 显示了 Orchestrator 的架构。

图 1-1 VMware vCenter Orchestrator 的架构



Orchestrator 系统要求

本章介绍安装和配置 VMware vCenter Orchestrator 的技术要求。

本章讨论了以下主题：

- 第 11 页，“Orchestrator 的硬件要求”
- 第 11 页，“Orchestrator 支持的操作系统”
- 第 11 页，“支持的目录服务”
- 第 12 页，“Orchestrator 支持的浏览器”
- 第 12 页，“Orchestrator 数据库要求”

Orchestrator 的硬件要求

安装 Orchestrator 之前，请确保系统符合最低硬件要求。

- 2.0GHz 或 2.0GHz 以上的 Intel 或 AMD x86 处理器。如果数据库也在相同硬件上运行，则对处理器的要求可能会不同。
- 2GB RAM。如果数据库也在相同硬件上运行，则可能需要更多 RAM。
- 10GB 磁盘空间。如果数据库也在相同硬件上运行，则可能需要更多存储空间。
- 可用的静态 IP 地址。

Orchestrator 支持的操作系统

Orchestrator 支持多种操作系统。

- Windows Server 2003 R2，32 位
- Windows Server 2003 R2，64 位
- Windows Server 2008，32 位
- Windows Server 2008，64 位

支持的目录服务

Orchestrator 需要您的基础架构上具有一个有效的 LDAP 服务器。

Orchestrator 支持下列目录服务类型。

- Windows Server 2003 Active Directory
- Windows Server 2008 Active Directory

- Novell eDirectory Server 8.8.3
- Sun Java Directory Server Enterprise Edition (DSEE) Version 6.3

Orchestrator 支持的浏览器

Orchestrator 用户界面需要使用 Web 浏览器。

必须具有以下浏览器之一，才能连接到 Orchestrator。

- Microsoft Internet Explorer 6.0 和 7.0
- Mozilla Firefox 3.0.6 或更高版本
- Safari 3.x (处于实验阶段)

Orchestrator 数据库要求

Orchestrator 要求您具有独立于标准 vCenter 数据库的数据库。

注意 由于 CPU 和内存的使用情况，VMware 建议您在同一个数据中心的同一主机上托管 Orchestrator 数据库和 Orchestrator 服务器。

Orchestrator 支持下列数据库类型：

- Microsoft SQL Server 2005 Enterprise (SP2)
- Microsoft SQL Server 2005 Enterprise (SP2) x64
- Microsoft SQL Server 2005 Enterprise (SP1)
- Microsoft SQL Server 2005 Standard (SP2)
- Microsoft SQL Server 2005 Standard (SP1)
- Microsoft SQL Server 2000 Enterprise (SP4)
- Microsoft SQL Server 2000 Standard (SP4)
- Oracle 10g Enterprise Release 2 (10.2.0.3.0) x64
- Oracle 10g Enterprise Release 2 (10.2.0.3.0) x32

随 vCenter Server 安装 Orchestrator

安装 VMware vCenter Server 时，Orchestrator（客户端和服务端）将作为附加组件在系统上静默安装。要使其可用，必须对其进行配置。

注意 Orchestrator 不支持 IPv6 操作系统。只能使用 IPv4 系统对其进行配置。

如果您已安装 Orchestrator 3.0.1，并且计划随 vCenter Server 安装程序安装 Orchestrator 4.0，则在继续操作之前，请确保 VMware vCenter Orchestrator 配置服务已停止。

有关 vCenter Server 安装的详细说明，请参见《ESX 和 vCenter Server 安装指南》。

在 Microsoft Windows 上安装 Orchestrator

您可以将 Orchestrator 作为独立产品安装到 Windows 服务器中。

前提条件

确保硬件符合 Orchestrator 系统要求。请参见第 11 页，“Orchestrator 的硬件要求”。

步骤

- 1 下载 vCenterOrchestrator.exe 文件。
- 2 双击 .exe 文件，然后单击 **Next**。
安装过程开始。
- 3 选择 **I accept the terms in the License Agreement**，然后单击 **Next**。
- 4 选择安装目录，然后单击 **Next**。
 - 如果安装的是 Orchestrator 独立版本，则默认位置是 C:\Program Files\VMware\Orchestrator。
 - 如果在 64 位 Windows Server 2008 上安装 Orchestrator 的独立版本，则默认位置是 C:\Program Files(x86)\VMware\Orchestrator。
 - 如果是使用 vCenter Server 安装程序安装的 Orchestrator，则默认位置是 C:\Program Files\VMware\Infrastructure\Orchestrator。

要将其安装到其他位置，请单击 **Choose**，然后浏览至新位置。



小心 不能在名称中包含非 ASCII 字符的目录中安装 Orchestrator。如果您是在使用非 ASCII 字符的语言环境中运行 Orchestrator，则必须在默认位置安装 Orchestrator。这是由于存在第三方限制。

- 5 选择安装类型，然后单击 **Next**。

选项	描述
Client	安装 Orchestrator 客户端应用程序，该程序可用于创建和编辑 workflow
Server	安装 Orchestrator 平台
Client-Server	安装 Orchestrator 客户端和服务端

- 6 指定 Orchestrator 快捷方式的位置，然后单击 **Next**。
- 7 单击 **Install** 完成创建过程。
- 8 单击 **Done** 关闭安装程序。

下一步

通过单击 **开始 > 程序 > VMware > vCenter Orchestrator Web Configuration** 登录 Orchestrator 配置界面，然后更改默认密码。

升级 vCenter Server 之后升级 Orchestrator 应用程序

4

如果您将虚拟基础架构从 VMware Infrastructure 3.5 升级到 vCenter Server 4.0，则必须执行相应操作才能继续运行现有的应用程序。

其中一种方法是在 Orchestrator Server 4.0 平台上安装 VMware Infrastructure 3.5 插件，然后导入您的应用程序。VMware Infrastructure 3.5 插件可与 vCenter Server 4.0 插件进行通信，使您可以无需更改即可运行这些应用程序。

此外，要想充分利用 vCenter Server 4.0 的所有功能特性，还可以采用另外一种方法，即重构用旧版本编写的 Orchestrator 应用程序。Orchestrator 4.0 提供了可帮助您将应用程序重构为新版本的工作流。

有关重构应用程序的详细信息，请参见《vCenter Orchestrator 开发指南》。

Orchestrator 数据库设置

Orchestrator 需要使用数据库来存储 workflow、用户、角色和权限等信息。

Orchestrator 服务器完全支持 Oracle 和 Microsoft SQL Server 数据库，并为 MySQL 和 PostgreSQL 提供实验性支持。可以将 MySQL 和 PostgreSQL 用于测试和评估。

数据库的设置方式会影响 Orchestrator 的性能。请在未安装 Orchestrator 的虚拟机上安装数据库。此方法可避免 JVM 和 DB 服务器共享 CPU、RAM 和 IO。

将数据库中的数据库插件与 Orchestrator 使用的插件分别存储在不同的数据库中，这样就可以更好地在升级系统时实现模块化。使用专用数据库实例，您可以在不影响其他产品的情况下执行升级和维护。

数据库的位置很重要，因为 Orchestrator 服务器上几乎每个活动都会触发数据库操作。要避免数据库连接滞后，请连接到最接近 Orchestrator 服务器并且位于具有最高带宽的网络中的数据库服务器。



小心 确保至少有 1GB 的可用磁盘空间

- 在安装数据库的虚拟机上
- 在安装 Orchestrator 服务器的虚拟机上

磁盘存储空间不足可能会导致不希望出现的 Orchestrator 服务器和客户端行为。

本章讨论了以下主题：

- [第 17 页，“在 Windows 上启用 Oracle 数据库支持”](#)
- [第 18 页，“在 Windows 上启用 MySQL 数据库支持”](#)
- [第 19 页，“MySQL 数据库参数”](#)

在 Windows 上启用 Oracle 数据库支持

要使用 Oracle 数据库，必须下载驱动程序，并将其复制到适当位置。Orchestrator 安装程序并不安装 Oracle 数据库的驱动程序。

步骤

- 1 从 [Oracle JDBC 驱动程序网页](#) 下载最新的 Oracle JDBC 驱动程序。
需要下载的是 *Oracle Database 10g Release 2 (10.2.0.4)*、*(10.2.0.3)*、*(10.2.0.2)*、*(10.2.0.1.0)* 驱动程序。
- 2 解压下载的归档文件。
- 3 在解压缩的文件夹中，找到名为 `ojdbc14.jar` 的文件。

- 4 要使驱动程序对 VMware vCenter Orchestrator 服务器和 VMware vCenter Orchestrator 配置界面可用，请将 `ojdbc14.jar` 复制到以下位置：
 - VMware vCenter Orchestrator 配置界面：
C:\Program Files\VMware\Orchestrator\configuration\jetty\lib\ext\
 - VMware vCenter Orchestrator 服务器：
C:\Program Files\VMware\Orchestrator\app-server\server\vmo\lib\
- 5 重新启动 Orchestrator 服务器。
 - a 在桌面上右键单击**我的电脑**，然后选择**管理**。
 - b 在“计算机管理”对话框中，展开**服务和应用程序**，然后选择**服务**。
 - c 在右窗格中，右键单击并选择 **VMware vCenter Orchestrator Server > 重新启动**。
 - d 在右窗格中，右键单击并选择 **VMware vCenter Orchestrator Configuration > 重新启动**。

Oracle JDBC 驱动程序已安装完毕。

在 Windows 上启用 MySQL 数据库支持

要使用 MySQL 数据库，必须下载驱动程序，并将其复制到适当位置。Orchestrator 安装程序并不安装 MySQL 数据库的驱动程序。

步骤

- 1 从 [MySQL 驱动程序网页](#) 下载最新的 MySQL 驱动程序。
需要的下载位于 *MySQL Connector/J - for connecting to MySQL from Java* 标题下。
- 2 解压下载的归档文件。
- 3 在解压缩的文件夹中，找到 `mysql-connector-java-<x.x.x>.jar` 文件，其中 `<x.x.x>` 是当前的次要版本号。
- 4 要使驱动程序对 VMware vCenter Orchestrator 服务器和 VMware vCenter Orchestrator 配置界面可用，请将 `mysql-connector-java-<x.x.x>.jar` 复制到以下位置：
 - VMware vCenter Orchestrator 配置界面：
C:\Program Files\VMware\Orchestrator\configuration\jetty\lib\ext\
 - VMware vCenter Orchestrator 服务器：
C:\Program Files\VMware\Orchestrator\app-server\server\vmo\lib\
- 5 重新启动 Orchestrator 服务器。
 - a 在桌面上右键单击**我的电脑**，然后选择**管理**。
 - b 在“计算机管理”对话框中，展开**服务和应用程序**，然后选择**服务**。
 - c 在右窗格中，右键单击并选择 **VMware vCenter Orchestrator Server > 重新启动**。
 - d 在右窗格中，右键单击并选择 **VMware vCenter Orchestrator Configuration > 重新启动**。

MySQL 数据库驱动程序已安装完毕。

MySQL 数据库参数

使用 MySQL 数据库时，必须将数据库服务器的参数 `max_allowed_packet` 设置为 16M。

步骤

- 1 在 Windows 上，编辑以下文件：C:\Program Files\MySQL\MySQL Server <X.X>\my.ini。
- 2 在 [mysql] 部分中，添加以下行：**`max_allowed_packet = 16M`**。

配置 Orchestrator

VMware vCenter Orchestrator Web Configuration 随 VMware vCenter Server 静默安装。使用此工具，您可以配置与 Orchestrator 引擎相关的组件，如网络、数据库、服务器证书等。正确配置这些组件可确保在 Orchestrator 平台上运行的生命周期管理器或任何其他应用程序正确工作。

本章讨论了以下主题：

- 第 21 页，“启动 Orchestrator 配置服务”
- 第 22 页，“登录 Orchestrator 配置界面”
- 第 22 页，“更改默认密码”
- 第 23 页，“配置网络连接”
- 第 24 页，“导入 vCenter SSL 证书”
- 第 25 页，“配置 LDAP 设置”
- 第 28 页，“密码加密和哈希机制”
- 第 29 页，“配置数据库连接”
- 第 30 页，“服务器证书”
- 第 32 页，“配置默认插件”
- 第 35 页，“Orchestrator 服务器的访问权限”
- 第 35 页，“导入 vCenter Server 许可证”
- 第 36 页，“启动 Orchestrator 服务器”
- 第 37 页，“导出 Orchestrator 配置”
- 第 38 页，“导入 Orchestrator 配置”
- 第 38 页，“配置事件和执行的数目”
- 第 39 页，“安装应用程序”
- 第 40 页，“启动已发布的 Web 视图”
- 第 40 页，“定义服务器日志级别”

启动 Orchestrator 配置服务

VMware vCenter Orchestrator 配置服务的启动类型默认情况下设置为手动。在尝试访问 Orchestrator 配置界面之前以及重新引导之后，都必须手动启动它。

如果使用 GUI 或控制台模式安装 Orchestrator，则 Web 配置服务已启动。

步骤

- 1 选择开始 > 程序 > 管理工具 > 服务。
 - 2 在列表中找到 VMware vCenter Orchestrator Configuration，然后检查其状态。
 - 3 如果状态未设置，请右键单击 **VMware vCenter Orchestrator Configuration**，然后选择**启动**。
- 服务将立即运行，并且可以使用 Orchestrator 配置界面。

下一步

此时即可登录 Orchestrator 配置界面并开始配置 Orchestrator。

登录 Orchestrator 配置界面

要启动配置过程，必须访问 Orchestrator 配置界面。

前提条件

确保 VMware vCenter Orchestrator 配置服务正在运行。

步骤

- 1 要访问 Orchestrator 配置界面，请执行以下操作之一：
 - ◆ 选择开始 > 程序 > VMware > vCenter Orchestrator Web Configuration。
 - ◆ 打开 Web 浏览器窗口，并输入以下 URL：

http://<计算机_DNS_名称_或_IP_地址>:8282.

8282 是为 Orchestrator 的 Web UI 配置保留的默认 HTTP 访问端口。如果要通过端口 8283 启用 HTTPS 连接，则必须将 Jetty 配置为使用 SSL。有关详细信息，请参见《Jetty 文档》中的“配置 SSL”部分。

- 2 使用默认凭据登录：
 - 用户名：**vmware**
 - 密码：**vmware**



小心 为避免非法利用管理凭据，请在首次访问配置界面时更改这个不安全的密码。在生产环境中，保留默认密码可能导致严重的安全问题，并且这也是造成数据破坏的常见原因。

有关如何更改默认密码的详细信息，请参见第 22 页，“更改默认密码”。

无法更改 **vmware** 默认用户名。

第一次登录 Orchestrator 配置界面时，您会在 **Information** 选项卡中看到安装路径、Orchestrator 版本和服务状态。左侧所有选项卡的状态指示器均显示红色三角，表明未配置任何组件。

下一步

选择一个选项卡并点击右侧检查器中的链接，输入所需信息，直到所选选项卡上出现绿色圆圈。绿色圆圈表明配置更改正确，并且符合所有相关性。

更改默认密码

VMware 建议您更改默认密码以避免潜在的安全问题。

前提条件

确保 VMware vCenter Orchestrator 配置服务正在运行。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 在 **General** 选项卡上，单击 **Change Password**。
- 3 在 **Current Password** 文本框中，输入 **vmware**。
- 4 在 **New Password** 文本框中，输入新的密码。
- 5 重新输入新密码以进行确认。
- 6 单击 **Apply changes** 保存新密码。

配置网络连接

安装 Orchestrator 时，服务器的 IP 地址会设置为未设置。要进行更改，必须配置 Orchestrator 使用的网络设置。

前提条件

系统管理员必须确保网络提供固定 IP，这可以通过使用正确配置的 DHCP 服务器（使用预留）或通过设置静态 IP 来实现。当 Orchestrator 服务器运行时，它需要此 IP 地址保持不变。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 单击 **Network**。
- 3 从 **IP Address** 下拉菜单中，选择要绑定到 Orchestrator 服务器的网络接口。
Orchestrator 会发现在其上安装此服务器的机器的 IP 地址。
选定接口后，将显示相应的 DNS 名称。如果没有找到网络名称，则会在 **DNS Name** 文本框中显示 IP 地址。
- 4 设置通信端口。
有关默认端口的详细信息，请参见第 23 页，“默认配置端口”。
- 5 单击 **Apply changes**。

下一步

单击 **SSL Certificate** 以在 Orchestrator 中加载 vCenter SSL 证书。

默认配置端口

Orchestrator 使用专用端口与其他系统通信。它嵌入在 JBoss 应用程序服务器中，因此可以获得内置冗余、高可用性、高性能的分布式应用程序服务等优势，并支持复杂的数据库访问。

必须设置的通信端口是 JBoss 使用的标准端口的子集。这些端口使用默认值设置，但您随时都可以更改这些值。在进行更改时，请确保主机上的所有端口均可用，如有必要，请在所需防火墙上打开这些端口。

有关默认端口的列表，请参见表 6-1。

注意 如果正在使用自定义插件，则可能需要其他端口。

表 6-1 VMware vCenter Orchestrator 默认端口

通信端口	端口号	描述
查询端口	8230	与 Orchestrator 服务器通信的主要端口（JNDI 端口）。所有其他端口均通过此端口与 Orchestrator 智能客户端进行通信。它是 Jboss 应用程序服务器基础架构的一部分。
命令端口	8240	用于远程调用的应用程序通信端口（RMI 容器端口）。它是 Jboss 应用程序服务器基础架构的一部分。
消息端口	8250	用于调度事件的 Java 消息端口。它是 Jboss 应用程序服务器基础架构的一部分。
数据端口	8244	用于访问所有 Orchestrator 数据模型（如工作流程和策略）的端口。它是 Jboss 应用程序服务器基础架构的一部分。
HTTP 服务器端口	8280	HTTP 连接器用于连接 Web 前端的端口。
HTTPS 服务器端口	8281	SSL 安全 HTTP 协议用于连接 Web 前端并与 vCenter API 通信的端口。
Web 配置 HTTP 访问端口	8282	Orchestrator Web UI 配置的访问端口。
Web 配置 HTTPS 访问端口	8283	Orchestrator Web UI 配置的 SSL 访问端口。 注意 要启用 HTTPS 连接，请将 Jetty 配置为使用 SSL。有关详细信息，请参见《Jetty 文档》中的“配置 SSL”部分。
LDAP	389	LDAP 身份验证服务器的查询端口。
LDAP（使用 SSL）	636	安全的 LDAP 身份验证服务器的查询端口。
PostgreSQL	5432	Orchestrator 数据库的 PostgreSQL Server。
SQL Server	1433	Orchestrator 数据库的 Microsoft SQL Server。
Oracle	1521	Orchestrator 数据库的 Oracle 数据库。
MySQL	3306	Orchestrator 数据库的 MySQL。
SMTP 服务器端口	25	用于电子邮件通知。

导入 vCenter SSL 证书

Orchestrator 配置界面使用安全连接与 vCenter 进行通信。可以从 URL 或文件导入所需的 SSL 证书。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 单击 **Network**。
- 3 在右窗格中，单击 **SSL Certificate** 选项卡。
- 4 要在 Orchestrator 中加载 vCenter SSL 证书，请执行下列操作之一：

选项	描述
Import from URL	输入 vCenter Server 的 URL： https://<您的_vcenter_server_IP_地址>
Import from file	确保连接到远程服务器，并单击 Browse 以搜索已保存在计算机上的 vCenter Server 证书文件。例如： C:\Documents and Settings\AllUsers\ApplicationData\VMware\VMware VirtualCenter\SSL\rui.crt。 ESX 主机使用位于以下目录中的自我生成的 SSL 证书： /etc/vmware/ssl/rui.crt。

- 5 单击 **Import**。
此时会显示一则消息，表示导入成功。

- 6 对每个 vCenter Server 重复步骤 2 到步骤 5。
- 7 单击 **Start-up Options**。
- 8 在添加新 SSL 证书后，请单击 **Restart the vCO configuration server** 以重新启动 VMware vCenter Orchestrator 配置服务。

此时导入的证书将会显示在已导入的 SSL 证书列表中。在 **Network** 选项卡上，红色三角变为绿色圆圈，表明组件已正确配置。

下一步

每次要指定使用 SSL 连接时，必须返回到 **Network** 选项卡上的 **SSL Certificate** 选项卡，并且导入相应的 vCenter SSL 证书。

配置 LDAP 设置

Orchestrator 需要连接至您的基础架构中的有效 LDAP 服务器。

生成 LDAP 连接 URL

LDAP 服务提供程序使用 URL 地址配置指向目录服务器的连接。要生成 LDAP 连接 URL，必须指定 LDAP 主机、端口和根。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 单击 **LDAP**。
- 3 从 **LDAP client** 下拉菜单中选择正在作为 LDAP 服务器使用的目录服务器类型。

支持的目录服务类型有：**Active Directory**、**eDirectory** 和 **Sun Java** 系统目录服务器。**OpenLDAP** 不受支持，只能用于测试和评估。

注意 如果在对 Orchestrator 对象设置权限（如 workflow 或操作的访问权限）后更改了 LDAP 服务器或类型，则必须重置这些权限。

如果在配置用于捕获和存储用户信息的自定义应用程序后更改了 LDAP 设置，则在针对新的 LDAP 数据库使用在旧的数据库中创建的 LDAP 身份验证记录时，该记录将变得无效。

- 4 （可选）如果使用 **Sun Java** 系统目录服务器，则必须在添加用户、创建组或分配组成员资格时将 **objectClass** 设置为 **groupOfUniqueNames**。对于可以登录 Orchestrator 的每位用户，用户 ID (**uid**) 为必填属性。
使用 **Sun Microsystems** 中的 **Java** 系统目录服务控制中心将 **objectClass** 设置为 **groupOfUniqueNames**。创建新组时，在 **Java** 系统目录服务控制中心选择 **Entry Type > Static Group > groupOfUniqueNames**。
- 5 在 **Primary LDAP host** 文本框中，输入主要 LDAP 服务在其上运行的主机的 IP 地址或 DNS 名称。
这是 Orchestrator 配置界面在其上验证用户凭据的第一台主机。
- 6 （可选）在 **Secondary LDAP host** 文本框中，输入辅助 LDAP 服务在其上运行的主机的 IP 地址或 DNS 名称。
如果主要 LDAP 主机变得不可用，则 Orchestrator 将在辅助主机上验证用户凭据。
- 7 在 **Port** 文本框中，输入 LDAP 服务器的查询端口的值。

注意 Orchestrator 支持 **Active Directory** 分层域结构。可以使用默认端口 **389** 连接到全局目录服务器。

如果没有将域控制器配置为使用全局目录，则必须使用端口 **3268**。

- 8 在 **Root** 文本框中，输入 LDAP 服务的根元素。

如果域名是 `company.org`，则根 LDAP 是 `dc=company,dc=org`。

这是在输入适当凭据之后用于浏览服务目录的节点。对于大型服务目录，在树中指定节点可缩小搜索范围并提高性能。例如，可以指定 `ou=employees,dc=company,dc=org`，这样就不会在整个目录中进行搜索了。它会显示员工组中的所有用户。

- 9 (可选) 选中 **Use SSL** 复选框可激活对 Orchestrator 和 LDAP 之间连接的加密认证。

如果您的 LDAP 使用 SSL，则必须首先导入 SSL 证书，然后重新启动 vCO 配置服务器。

注意 SSL 功能不作为 Microsoft Active Directory、eDirectory 和 Sun Java 目录服务器的一部分安装，并且可能需要其他配置。

- 10 (可选) 选中 **Use Global Catalog** 复选框可在 LDAP 客户端是 Active Directory 时允许使用 LDAP 引用。

LDAP 服务器会查询 3268 的端口号变更情况。Orchestrator 会根据 LDAP 引用查找属于 Orchestrator 连接至 Active Directory 树的子域中的用户和组。可以在可从全局目录访问的任何组上添加权限。

示例 6-1 示例值和生成的 LDAP 连接 URL

- LDAP 主机: `DomainController`
- 端口: `389`
- 根: `ou=employees,dc=company,dc=org`

连接 URL: `ldap://DomainController:389/ou=employees,dc=company,dc=org`

下一步

请将凭据分配到 Orchestrator 以确保其能够访问 LDAP 服务器。

有关详细信息，请参见第 26 页，“指定浏览凭据”。

指定浏览凭据

Orchestrator 必须读取 LDAP 结构才能继承其属性。可以指定 Orchestrator 用于连接 LDAP 服务器的凭据。

前提条件

基础架构上必须具备有效的 LDAP 服务，并且已经生成 LDAP 连接 URL。

步骤

- 1 在 Orchestrator 配置界面的 **LDAP** 选项卡中，在 **Username** 文本框中为 LDAP 上具有浏览权限的用户输入有效用户名 (LDAP 字符串)。

可以在 Active Directory 中指定的用户名的可能格式如下：

- 裸用户名格式，例如 `user`。
- 可区分名称格式: `cn=user,ou=employees,dc=company,dc=org`。
对于 OpenLDAP、Sun 和 eDirectory，请使用此格式。
- 规范名称格式: `user@company.org`。
- NetBEUI 格式: `COMPANY\user`。

- 2 在 **Password** 文本框中，为在步骤 1 中输入的用户名输入有效密码。

Orchestrator 将使用这些凭据连接 LDAP 服务器。

下一步

为 Orchestrator 定义 LDAP 容器以便查询用户和组。

定义 LDAP 查询方式

可以定义用户和组的查询信息。

Orchestrator 中具有两个获得认可的全局角色：开发人员和管理员。开发人员角色的用户拥有编辑所有元素的特权。管理员角色的用户的特权不受限制。管理员可以管理权限，或者将管理选定元素组的责任下放给其他任何组或用户。这两个组必须包含在组查找库中。

前提条件

基础架构上必须具有有效的 LDAP 服务。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 单击 **LDAP**。
- 3 定义 **User lookup base**。

这是 Orchestrator 用于搜索潜在用户的 LDAP 容器（顶级域名）。

- a 单击 **Search**，然后输入顶级域名。

搜索 **company** 会返回 **dc=company,dc=org** 和包含搜索项的其他通用名。如果输入 **dc=company,dc=org** 作为搜索项，将找不到结果。

- b 单击所发现分支的 LDAP 连接字符串以将其插入 **User lookup base** 文本框。

如果没有找到匹配结果，请在 LDAP 主页面中检查您的 LDAP 连接字符串。

注意 可以通过端口 389 连接全局目录服务器。它会发出 Orchestrator 遵循的 LDAP 引用以便在子域中找到帐户或组。

- 4 定义 **Group lookup base**。

这是 Orchestrator 用于查询组的 LDAP 容器。

- a 单击 **Search**，然后输入顶级域名。
- b 单击所发现分支的 LDAP 连接字符串以将其插入 **Group lookup base** 文本框。

- 5 定义 **vCO Admin group**。

这是要向其授予 Orchestrator 管理特权的 LDAP 组。

- a 单击 **Search**，然后输入顶级域名。
- b 单击所发现分支的 LDAP 连接字符串以将其插入 **vCO Admin group** 文本框。

重要事项 在 eDirectory 安装中，只有 eDirectory 管理员才能看到拥有管理权限的用户或用户组。如果您使用的是 eDirectory LDAP 服务器，而且是以 vCO 管理组成员身份而非 eDirectory 管理员身份登录 Orchestrator，则可以创建具有管理权限的用户或用户组，但无法看到这些用户使用各自的权利和权限。此问题对于其他 LDAP 服务器不适用。

下一步

单击 **Test Login** 选项卡，然后输入用户凭据以测试他们是否可以访问 Orchestrator 智能客户端。成功登录之后，系统会检查该用户是否属于 Orchestrator 管理员组。

设置连接超时

如果系统超时，可以增加 Orchestrator 客户端和 LDAP 服务器端的超时时长。

如果服务器端超时时长比客户端短，则增加客户端超时时长是无意义的。不建议对依赖于企业 LDAP 服务器的其他进程增加服务器端超时时长。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
 - 2 单击 **LDAP**。
 - 3 在 **Request timeout** 文本框中，输入一个以毫秒为单位的值。
这个值将确定 Orchestrator 服务器将查询发送到服务目录、执行目录搜索和发送回答所用的时长。如果超时时段结束，则修改此值可以检查 Orchestrator 服务器中是否出现超时。
 - 4 （可选）在执行搜索操作之前，对于要执行的所有链接，请选中 **Dereference links** 复选框。
Sun Java 系统目录服务器不支持引用链接。如果要使用引用链接，则必须选中 **Dereference links** 复选框。
 - 5 （可选）要筛选由搜索返回的属性，请选中 **Filter attributes** 复选框。
选中此复选框可加快 LDAP 的搜索速度。但是，随后可能需要使用某些额外 LDAP 属性以达到自动化。
 - 6 （可选）要禁用引用处理，请选中 **Ignore referrals** 复选框。
选中此复选框后，系统将不显示任何引用。
 - 7 在 **Host reachable timeout** 文本框中，输入一个以毫秒为单位的值。
此值将确定用于检查目标主机状态的测试超时时长。
 - 8 单击 **Apply changes**。
- 在 **LDAP** 选项卡上，红色三角变为绿色圆圈，表明组件已正确配置。

下一步

继续执行数据库配置。

密码加密和哈希机制

Orchestrator 以采用 MD5 哈希和 DES 加密机制的 PBE 加密技术对用于连接数据库、LDAP 和 Orchestrator 服务器的存储密码进行编码。

表 6-2 介绍 Orchestrator 使用的密码加密方法和哈希机制。

表 6-2 加密和哈希算法

算法	描述
PBE - 基于密码加密（Java 2 SDK 1.4 的一部分）	通过密码生成加密密钥。PBE 会存储并检查密码的哈希值。有关详细信息，参见 java.sun.com 上的《Java Cryptography 扩展参考指南》。
MD5 - 消息摘要 5 算法	生成 128 位加密消息摘要值，通常以 32 位数的十六进制数表示。
DES - 数据加密标准	将 56 位密钥应用于每个 64 位的数据块中。

配置数据库连接

Orchestrator 需要使用数据库存储 workflow、用户、角色和权限的相关信息。要建立与 Orchestrator 数据库的连接，必须配置数据库连接参数。

前提条件

设置数据库以与 Orchestrator 服务器一起使用。Orchestrator 服务器支持 Oracle 和 SQL Server 数据库。

注意 若要进行测试和评估，可以设置 MySQL 或 PostgreSQL 数据库。

Oracle 和 MySQL 的驱动程序未与 Orchestrator 一起安装。有关启用这些数据库类型的支持的详细信息，请参见第 12 页，“Orchestrator 数据库要求”。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 单击 **Database**。
- 3 从 **Select/Change database type** 下拉菜单中，选择 Orchestrator 服务器使用的数据库类型。
- 4 指定数据库连接参数。

连接参数	描述
Username	Orchestrator 用于连接和运行所选数据库的用户名。所选名称必须是目标数据库上的有效用户，并且必须具有表格创建和删除权限。
Password	Orchestrator 接受的您选定的用户名所带的密码。
Hostname or IP	数据库服务器 IP 地址或 DNS 名称。
Port	用于与数据库之间实现通信的数据库服务器端口。
Database name	数据库独有的完整名称。数据库名称由初始化参数文件中的 SERVICE_NAMES 参数指定。 注意 PostgreSQL JDBC 驱动程序不支持在数据库名称中使用非 ASCII 字符。
Instance name	数据库实例的名称，可以使用数据库初始化参数文件中的 INSTANCE_NAME 参数来标识。
Domain	对于 Windows 身份验证，请输入 Windows 域，例如 company.org 。 对于 SQL 身份验证，请留空此文本框。

如果指定参数正确，则会显示一则消息，表示已成功连接至数据库。

注意 尽管 Orchestrator 已经与数据库建立了连接，但数据库安装尚未完成。必须安装数据库。

- 5 单击 **Install database** 为 Orchestrator 生成表结构。
- 6 单击 **Apply changes**。

注意 如果您在配置和安装默认插件后更改了 Orchestrator 数据库，则单击 **Troubleshooting** 选项卡，然后通过单击 **Reset current version** 链接强制重新安装插件。此操作将删除用于保存已安装插件版本的 `<安装_目录>\app-server\server\vmoplugins_VSOPluginInstallationVersion.xml` 文件，并强制重新安装插件。

数据库配置更新成功。在 **Database** 选项卡上，红色三角变为绿色圆圈，表明组件已正确配置。

服务器证书

服务器证书是一种数字标识形式，与 HTTPS 结合使用可用于验证 Web 应用程序。该证书针对特定服务器发放，其中包含有关该服务器的公钥信息，您可以使用它对 Orchestrator 中创建的所有元素进行签名并保证其真实性。当客户端从您的服务器接收元素（通常是软件包）时，它们会验证您的标识，并决定是否信任您的签名。

要获得服务器证书，请执行以下任务：

- 1 创建自签署服务器证书。
- 2 生成证书签名请求 (CSR)。
- 3 将 CSR 提交到证书颁发机构 (CA)。
- 4 导入证书签名答复。

创建自签署服务器证书

安装 Orchestrator 时需要创建一个自签署证书。通过创建自签署证书可以确保软件包加密通信并附带签名。但是，接收者无法确保您发送的自签署软件包实际上是由您的服务器发出，而不是由宣称是您的第三方发出的。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 单击 **Server Certificate**。
- 3 单击 **Create a new Certificate Database and server certificate**。
- 4 输入相关信息。
- 5 从下拉菜单中选择一个国家/地区。
- 6 单击 **Create**。

Orchestrator 会生成所在环境中唯一的服务器证书。有关证书的详细信息将显示在 **Server Certificate** 窗口中。

下一步

此时，证书已存储到数据库中。为了实现灾难恢复，您可以通过单击 **Export vCO Certificate Database** 将该证书保存为本地文件。

获取由证书颁发机构签署的服务器证书

为了接收者对您的服务器所创建的软件包具有可接受的信任度，证书通常要由证书颁发机构 (CA) 签署。证书颁发机构可以保证您就是证书的真正持有人，因为他们会用自己的验证令牌来签署您的证书。

前提条件

创建自签署服务器证书，或单击 **Import vCO Certificate Database** 以导入现有服务器证书。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 单击 **Server Certificate**。
- 3 生成证书签名请求 (CSR)。
 - a 单击 **Export Certificate Signing Request**。
 - b 系统提示时，将 **VS0certificate.csr** 文件保存到文件系统中。

- 4 将 CSR 文件发送到证书颁发机构，如 VeriSign 或 Thawte。
操作步骤可能会因 CA 而异，但他们都需要您出示有效的身份证明。
CA 会返回您必须导入的证书签名答复。这是一份精确的实际证书和 CA 签名。
- 5 单击 **Import Certificate Signing Reply**，然后选择由 CA 发送的文件。

Orchestrator 使用服务器证书来：

- 通过将证书公钥附加到每个软件包，在导出之前签署所有软件包。
- 在导入包含由不信任证书签署的元素的软件包时，显示用户提示。

下一步

可以在其他服务器上导入此证书。

导出服务器证书

服务器证书私钥存储在 Orchestrator 数据库的 `vmo_keystore` 表中。如果您丢失或删除了此密钥或将 Orchestrator 服务器绑定到其他数据库，则用此证书签名的导出包内容将变得不可用。为确保在导入时解密这些软件包，必须将此密钥保存到本地文件中。

前提条件

必须已经创建或导入了一个服务器证书。

步骤

- 1 以 `vmware` 身份登录 Orchestrator 配置界面。
- 2 单击 **Server Certificate**。
- 3 单击 **Export certificate database**。
- 4 输入密码以加密导出的密钥库数据库内容。
导入文件时，必须再次输入此密码。
- 5 单击 **Export**。
- 6 系统提示时，请保存 `vmo-server.vmokestore` 文件。

更改自签署服务器证书

如果您想要使用与 Orchestrator 初始配置所用证书不同的服务器证书来对您的软件包签名，则需要导出所有软件包，并重新安装 Orchestrator 服务器。

步骤

- 1 导出所有软件包。
 - a 在 Orchestrator 客户端中单击 **Packages** 视图。
 - b 右键单击要导出的软件包并选择 **Export package**。
 - c 浏览以选择保存软件包的位置，然后单击 **Open**。
 - d 保持 **View content**、**Re-Packeable** 和 **Edit element** 选项处于选中状态。



小心 不要使用当前证书签署软件包。不得加密软件包。删除证书数据库时，私钥将丢失，并且导出的软件包的内容将变得不可用。

- e (可选) 如果不想导出版本历史记录，则取消选中 **Export version history** 复选框。
 - f 单击 **Save**。
- 2 (可选) 导出 Orchestrator 配置。
- 3 卸载 Orchestrator 服务器。
- 4 删除 Orchestrator 数据库或创建备份 (如果希望保留旧数据)。

将 Orchestrator 绑定到其中的数据库不得在 vmo_keystore 表中包含记录。
- 5 重新安装 Orchestrator 服务器。
- 6 (可选) 导入 Orchestrator 配置。
- 7 创建新的自签署证书，或导入一个自签署证书。
- 8 重新导入软件包。
 - a 在 Orchestrator 客户端中单击 **Packages** 视图。
 - b 从下拉菜单中选择 **Import package**。
 - c 浏览以选择要导入的软件包，然后单击 **Open**。
 - d 单击 **Import** 或 **Import and trust provider**。
 - e 单击 **Import checked elements**。

服务器证书更改将在下一次导出软件包时生效。

配置默认插件

要在 Orchestrator 服务器启动时部署默认插件集，系统必须对 LDAP 服务器进行身份验证。可以指定 Orchestrator 与插件一起使用时的管理凭据，还可以在 **Plug-ins** 选项卡上启用和禁用插件。

如果您在配置和安装默认插件后更改了 Orchestrator 数据库，则必须在 **Troubleshooting** 选项卡中单击 **Reset current version** 链接。此操作将删除用于保存已安装插件版本的 `<安装_目录>\app-server\server\vmo\plugins_VSOPluginInstallationVersion.xml` 文件，并强制重新安装插件。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 单击 **Plug-ins**。
- 3 输入 Orchestrator 管理组成员的用户凭据。

Orchestrator 服务器启动时，系统将使用这些凭据设置插件。系统检查已启用的插件并执行任何必要的内部安装，如软件包导入、策略运行、脚本启动，等等。

- 4 (可选) 安装新插件：
 - a 单击 **Browse**。
 - b 选择要安装的文件。
 - c 单击 **Open**。
 - d 单击 **Upload and install**。

可以使用的文件扩展名为 **.vmoapp** 和 **.dar**。**.vmoapp** 文件可包含多个 **.dar** 文件的集合，并且可作为应用程序安装，而 **.dar** 文件则包含与一个插件相关的所有资源。

已安装的插件文件存储在 **<安装_目录>\app-server\server\vmo\plugins** 文件夹中。

注意 如果将 **.dar** 文件直接添加到文件系统，则必须单击 **Reload plug-ins**，才能更新可在 Orchestrator 配置界面使用的插件。

- 5 (可选) 要禁用插件，请取消选中其旁边的复选框。

此操作并不移除插件文件。

- 6 单击 **Apply changes**。

在 **Plug-ins** 选项卡上，红色三角变为绿色圆圈，表明组件已正确配置。首次引导服务器时，它将安装所选插件。

下一步

现在即可配置邮件、SSH 和 vCenter 4.0 插件的设置。

定义默认 SMTP 连接

邮件插件随 Orchestrator 服务器安装，用于发送通知邮件。唯一可供此插件使用的选项是对新邮件消息使用默认值。可以设置默认的电子邮件帐户。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 单击 **Mail**。
- 3 选中 **Define default values** 复选框，并填写必填的文本框。

文本框	描述
SMTP host	输入 SMTP 服务器的 IP 地址或域名。
SMTP port	输入与 SMTP 配置匹配的端口号。 默认 SMTP 端口为 25。
User name	输入有效的电子邮件帐户。 这是 Orchestrator 用于发送电子邮件的电子邮件帐户。

文本框	描述
Password	输入与用户名关联的密码。
From name and address	输入显示在由 Orchestrator 发送的所有电子邮件中的发件人信息。

- 单击 **Apply changes**。

配置 SSH 插件

可以设置 SSH 插件以确保实现加密连接。

步骤

- 以 **vmware** 身份登录 Orchestrator 配置界面。
- 单击 **SSH**。
- 单击 **New connection**。
- 在 **Host name** 文本框中，输入要通过 Orchestrator 进行 SSH 访问的主机。

注意 此时不需要用户名和密码，因为 Orchestrator 使用的是当前登录用户的凭据运行 SSH 命令。必须从 LDAP 服务器的目标主机上复制要在 SSH 上工作的帐户。

- 单击 **Apply changes**。
主机将添加到 SSH 连接列表中。
- （可选）在服务器上配置输入路径。
 - 单击 **New root folder**。
 - 输入新路径，然后单击 **Apply changes**。

SSH 主机即会出现在 Orchestrator 智能客户端的 **Inventory** 视图中。

配置 vCenter 4.0 插件

Orchestrator 使用 vCenter Web 服务 API 控制 vCenter。可以将所有参数设为允许 Orchestrator 连接到 vCenter 实例。

前提条件

为定义每个 vCenter 实例导入 SSL 证书。有关详细信息，请参见第 24 页，“[导入 vCenter SSL 证书](#)”。

步骤

- 以 **vmware** 身份登录 Orchestrator 配置界面。
- 单击 **vCenter 4.0**。
- 单击 **New vCenter host**。
- 从 **Available** 下拉菜单中，选择 **Enabled**。
- 在 **Host** 文本框中，输入 vCenter 主机的 IP 地址或 DNS 名称。
- 在 **Port** 文本框中，保留默认值 443。
- （可选）选中 **Secure channel** 复选框以建立与 vCenter 主机的安全连接。
- 在 **Path** 文本框中，使用默认值 **/sdk**。
这是用于连接到 vCenter 实例的 SDK 的位置。

- 9 在 **User name** 和 **Password** 文本框中，输入 Orchestrator 用于建立与 vCenter 连接的凭据。

所选用户必须是在 vCenter Server 上拥有管理特权的有效用户，最好是位于 vCenter 树结构顶部的用户。Orchestrator 使用这些凭据监控 vCenter Web 服务（通常用于运行 Orchestrator 系统工作流）。所有其他请求都将继承触发操作的用户的凭据。

- 10 通过选择下列选项之一，指定在 vCenter 主机上管理用户访问权限的方法：

选项	描述
Share a unique session	输入 vCenter 管理员用户的凭据。
Session per user	如果 vCenter Server 位于 Active Directory 域中，请选择此选项。确保用户拥有执行所需操作必备的权限。 小心 登录的每个用户都会各自创建自己的 vCenter 会话。这将导致更高的流量和更多的查询。

- 11 单击 **Apply changes**。

指向新配置 vCenter 主机的 URL 将添加到已定义主机的列表中。

- 12 对每个 vCenter 实例重复 [步骤 3](#) 到 [步骤 11](#)。

下一步

如果在导入 vCenter SSL 证书后服务器未重新启动，则单击 **Restart the vCO Configuration Server**。

Orchestrator 服务器的访问权限

在 Orchestrator 配置界面中应用的 vCenter Server 许可证的类型可以决定获得的是对 Orchestrator 服务器功能的只读访问还是完全访问权限。

[表 6-3](#) 介绍 Orchestrator 服务器的特权集，具体取决于您的 vCenter Server 许可证版本。

表 6-3 Orchestrator 服务器模式

vCenter 许可证版本	Orchestrator 服务器模式	描述
Standard	Server	您将获得对所有 Orchestrator 元素的完全读写特权。您可以运行并编辑工作流。 注意 根据设计，所有预定义的工作流均锁定为只读状态。必须复制工作流，然后更改自己的工作流副本。
Foundation	Player	您将获得对所有 Orchestrator 元素的只读特权。可以运行工作流，但无法编辑它们。
Essentials	Player	您将获得对所有 Orchestrator 元素的只读特权。可以运行工作流，但无法编辑它们。

导入 vCenter Server 许可证

要完成 Orchestrator 服务器的配置过程，必须导入 vCenter Server 许可证。Orchestrator 随附的插件集不需要许可证。如果要添加需要许可证的插件，则必须导入相应的许可证。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 单击 **Licenses**。

- 3 在 **Serial Number** 文本框中，输入 vCenter Server 许可证密钥。
序列号由五组由连字符分隔的字符串组成，每个字符串包含五个字母数字字符。
- 4 单击 **Apply changes**，并验证许可证是否已安装。
要查看详细信息，请单击导入的许可证名称。
- 5 启动 Orchestrator 服务器。
Orchestrator 服务器已正确配置。

启动 Orchestrator 服务器

可以将 Orchestrator 服务器作为 **Startup Options** 选项卡上的服务安装。执行此操作后，可以从配置界面启动、停止和重新启动服务。此过程是可逆的，因为您始终都可以使用 **Uninstall vCO server from service** 选项。

前提条件

确保所有状态指示器都显示绿色圆圈。如果任一组件配置不正确，都无法启动 Orchestrator 服务器。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 单击 **Startup Options**。
- 3 单击 **Install vCO server as service**。
- 4 单击 **Start service**。

Orchestrator 服务器状态显示为 **Service is starting**。第一次引导可能需要大约 5-10 分钟，因为它要生成数据库表。

此时会显示一则消息，表明服务已成功启动。Orchestrator 服务器状态将显示在每个配置选项卡的底部，其状态如下：

- Running
- Not available
- Stopped

要查看 Orchestrator 服务器状态，请通过单击 **Refresh** 链接更新该页面。

下一步

如果需要，可以保存和导出 Orchestrator 配置文件，以便过后在需要时导入。有关详细信息，请参见 [第 37 页](#)，“导出 Orchestrator 配置”。

设置服务超时参数

如果 Orchestrator 服务器正在高负载运行，例如，如果已经将 Orchestrator 连接到多台正在运行许多虚拟机的 vCenter Server，或如果服务器正在执行交换，则可能会遇到不必要的服务器重新启动。

服务器重新启动是由 Orchestrator 监视程序服务设置的默认超时所致。在某些特定环境中，如果响应时间超过监视程序超时时长，则监视程序可能会错误地检测到 JVM 错误，这会导致服务器重新启动。

如果遇到此行为，可以通过在 Orchestrator 包装配置文件 `wrapper.conf` 中添加或修改超时参数，从而延长监视程序的超时时长。`wrapper.conf` 文件在主机系统中定义 Orchestrator 服务器的包装。

前提条件

您正在将 Orchestrator 服务器作为 Windows 服务运行。

步骤

- 1 导航到包装配置文件 `wrapper.conf`。

在以下位置中查找包装配置文件：<安装_目录>/app-server/bin/wrapper.conf。

- 2 在编辑器中打开 `wrapper.conf` 文件。
- 3 在 `wrapper.conf` 文件中找到 `-wrapper.ping.timeout` 参数，如果它不存在，请将其添加到此文件中。
- 4 增加秒数以便监视程序的 Ping 操作和 JVM 的响应操作能够完成。

默认超时为 30 秒。例如，将超时时长增加到 60 秒，如下所示。

```
-wrapper.ping.timeout=60
```

- 5 通过在 Orchestrator 配置界面中单击 **Startup Options > Restart Service**，重新启动 Orchestrator 服务器。
- 6 如果问题仍然存在，则应增加超时时长。
- 7 如果问题仍然存在，则将超时时长设置为零 (0)。

将超时值设置为零意味着监视程序将永不超时，并且将永不导致 Orchestrator 服务器重新启动。但是，将超时值设置为零也意味着监视程序将无法检测到已挂起的 JVM。

您已经增加了 Orchestrator 监视程序的超时时长。

导出 Orchestrator 配置

Orchestrator 配置提供将系统设置导出到本地文件中的机制。使用此机制，您随时都能取得系统配置的快照，并且将此配置导入到新的 Orchestrator 实例中。

VMware 建议您定期导出并保存配置设置，尤其是在进行修改、执行维护或升级系统时。

步骤

- 1 以 `vmware` 身份登录 Orchestrator 配置界面。
- 2 在 **General** 选项卡上，单击 **Export Configuration**。
- 3 （可选）输入密码保护配置文件。
导入配置时，请使用相同的密码。
- 4 单击 **Export**。
- 5 系统提示时，请单击 **Save**。

可以使用 `vmo_config_dateReference.vmoconfig` 文件来克隆或还原系统。

下一步

有关导出的配置设置列表，请参见第 37 页，“Orchestrator 配置文件”。

Orchestrator 配置文件

导出系统配置时，将在本地创建 `vmo_config_dateReference.vmoconfig` 文件。它包含所有 Orchestrator 配置文件。

注意 导出期间创建的部分配置文件为空文件。例如，服务器文件为空，因为 Orchestrator 服务器的启动选项对每个安装 Orchestrator 服务器的计算机来说是唯一的。必须重新配置这些空文件，即使之前已导入了有效的配置。

表 6-4 包含一个配置导出期间未保存的设置列表。

表 6-4 配置导出期间未保存的设置

文件	描述
证书	证书不导出。大多数证书存储在 Orchestrator 数据库中。但是，vCenter Server 证书不存储在该数据库中。必须将其单独存储，或在导入 Orchestrator 配置时将其再次导入。
许可证	许可证不导出。许可证存储在 Orchestrator 数据库中。
服务器	服务器配置。

表 6-5 包含一个配置导出期间已保存的设置列表。

表 6-5 配置导出期间已保存的设置

文件	描述
常规	所记录的已完成事件和工作流的最大数目，以及 Web 视图开发和配置。
网络	由 Orchestrator 服务器的不同元素使用的 IP 绑定地址和 TCP 端口。
数据库	数据库配置。
ldap	LDAP 服务器配置。
日志	日志设置信息。
插件	已禁用插件和帐户名列表。
故障排除	调试信息。
邮件插件	SMTP 主机、SMTP 端口、用户名、密码、发件人名称和发件人地址。
vCenter 4.0 插件	vCenter 4.0 插件配置。

导入 Orchestrator 配置

发生系统故障或重新安装 Orchestrator 时，可以还原之前导出的系统配置。

步骤

- 1 在新服务器上安装新的 Orchestrator 实例。
- 2 以 vmware 身份登录 Orchestrator 配置界面。
- 3 在 **General** 选项卡上，单击 **Import Configuration**。
- 4 （可选）输入导出时所使用的保护密码（如果有）。
- 5 浏览以选择从之前安装中导出的 .vmoconfig 文件。
- 6 单击 **Import**。

此时会显示一则消息，表示配置已成功导入。新系统已完成对旧配置的复制。

配置事件和执行的数目

可以定义存储在数据库中的最大事件数和最大工作流执行数。

每个事件对应于一种工作流或策略状态更改，并且存储在数据库中。达到为工作流或策略事件设置的最大数目时，数据库会删除最旧的事件以存储新事件。

每次运行一个 workflows 时，即会在数据库中创建一个 workflow 令牌。此令牌包含与运行此 workflow 相关的所有参数。例如，如果运行 workflow 测试三次，则会创建三个 workflow 令牌。这三个令牌将显示在 Orchestrator 客户端中的测试 workflow 上方。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 在 **General** 选项卡上，单击 **Advanced Configuration**。
- 3 填写 **Max number of events** 文本框。
要跟踪基础架构中的每个更改，请输入 **0**（零等于无限）。这意味着服务器永不翻转，但它可能会变得不可用。数据库管理员必须定期清理服务器并归档事件。
- 4 填写 **Max number of executions** 文本框。
在达到执行的最大数目后，将会启动翻转过程。如果不希望启动翻转过程，则在此文本框中输入 **0**。如果输入 **0**，则数据库将继续扩展。
- 5（可选）要设置默认登录凭据，请填写 **Web auto-login user name and password** 文本框。
通过此功能，可以生成 URL，以便运行、回答、调度或监控 workflow，而不必输入凭据。请对这些文本框使用默认操作员凭据。
- 6 填写 **Web view directory** 文本框。
从其中加载开发 Web 视图的根文件夹。每个 Web 视图的文件都必须位于单独的子文件夹中，并且此子文件夹的名称必须与客户端中定义的 URL 文件夹的名称相同。
- 7（可选）要将服务器置于 Web 视图开发模式下，请选中 **Web view development enable** 复选框。
在此模式下，Web 视图中的所有元素都将从指定的 Web 视图目录加载，而不再从 Web 视图内容自身加载。
- 8 单击 **Apply changes**。

安装应用程序

应用程序是一组插件和软件包。由于 Orchestrator 安装只包含几个预定义插件，因此必须经常安装应用程序以扩展基本功能。

前提条件

获取包含应用程序的 **.vmoapp** 文件。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 在 **General** 选项卡上，单击 **Install Application**。
- 3 浏览以选择 **.vmoapp** 文件进行安装。
- 4 单击 **Install**。

下一步

每次安装应用程序时，系统都会对服务器配置进行验证。在大多数情况下，必须执行其他配置步骤。

启动已发布的 Web 视图

可以使用 Web 视图生成用户前端。Web 视图可以是显示基本信息的简单页面，也可以是复杂的 Web 2.0 应用程序。Orchestrator 提供一个名为 WebOperator 的演示 Web 视图，您可以使用它来查看 Web 视图的工作方式。可以通过 Orchestrator 配置界面访问 Web 视图。

前提条件

确保 Orchestrator 服务器已启动。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 在 **General** 选项卡上，单击 **Web views**。

此时将显示指向已发布 Web 视图的链接。单击这些链接即可在新的浏览器窗口中打开 Web 视图。

定义服务器日志级别

在 Orchestrator 配置界面中，可以设置需要的服务器日志级别。

步骤

- 1 以 **vmware** 身份登录 Orchestrator 配置界面。
- 2 单击 **Log**。
- 3 从 **Log level** 下拉菜单中选择一个选项。

选项	描述
FATAL	仅将重要错误条目写入日志文件。
ERROR	错误和更高级别条目均写入日志文件。
WARN	警告和更高级别条目均写入日志文件。
DEBUG	调试信息和更高级别条目均写入日志文件。
INFO	信息和更高级别条目均写入日志文件。
ALL	不筛选事件。所有事件均写入日志文件。
OFF	不向日志文件中写入任何条目，也不进行日志更新。

注意 日志会显示所选级别和更高级别的消息。如果选择 **INFO** 级别，则所有 **INFO** 消息和更高级别（**INFO**、**DEBUG**、**WARN**、**ERROR** 和 **FATAL**）的消息均写入日志文件。

- 4 单击 **Apply changes**。
- 5 （可选）单击 **Generate log report** 链接以导出日志文件。

此操作将创建所有日志的 ZIP 归档文件。

无需重新启动服务器，新的服务器日志级别将在一分钟内应用。日志存储在 `<安装目录>\app-server\server\vmo\log` 下。

索引

A

安全性 7

B

版本管理 7

C

策略引擎 7

插件

安装应用程序 39

SSH 插件 34

vCenter 插件 34

邮件插件 33

超时 28

持久性 7

重构 15

D

登录 22

DES 28

F

非 ASCII 字符 13, 29

服务

启动 21, 36

VMware vCenter Orchestrator 配置 21

VMware vCenter Orchestrator Server 36

服务器, 超时参数 36

服务器日志

导出 40

日志级别 40

服务器证书

CA 签署 30

导出 30, 31

移除 32

自签署 30

G

工作流引擎 7

H

哈希 28

I

IPv4 13

IPv6 13

J

加密 28

检查点 7

脚本引擎 7

L

LDAP

查询方式 27

连接 URL 25

浏览凭据 26

M

MD5 28

密码 22

默认端口

查询端口 23

HTTP 端口 23

HTTPS 端口 23

LDAP 端口 23

命令端口 23

Oracle 端口 23

PostgreSQL 端口 23

数据端口 23

SMTP 端口 23

SQL Server 端口 23

Web 配置 HTTP 访问端口 23

Web 配置 HTTPS 访问端口 23

消息端口 23

MySQL

安装 MySQL 驱动程序 18

参数 19

O

Oracle, 安装 Oracle 驱动程序 17

Orchestrator 架构 9

P

PBE 28

配置

导出配置设置 37

导入配置设置 38

LDAP 设置 27

默认插件 32

配置文件 37

数据库连接 29

网络连接 23

Q

取消链接引用 28

S

筛选属性 28

升级 15

事件 38

数据库

安装 17

服务器大小 17

连接参数 29

MySQL 17

Oracle 17

PostgreSQL 17

设置 17

SQL Server 17

SMTP 连接 33

SSL 证书 24

随 vCenter Server 安装 Orchestrator

vCenter Server 安装程序 13

Windows 独立安装程序 13

W

Web 视图

启动 Web 视图 40

显示 Web 视图 40

X

系统要求

操作系统 11

目录服务 11

硬件 11

支持的浏览器 12

支持的数据库 12

许可证

导入 vCenter Server 许可证 35

Orchestrator 服务器访问权限 35

Y

用户角色 8

Z

证书数据库 31, 32

支持的数据库, Oracle, SQL Server 12

执行 38