# 安装和配置 VMware vRealize Orchestrator

vRealize Orchestrator 7.3

vmware®

您可以从 VMware 网站下载最新的技术文档：

https://docs.vmware.com/cn/。

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

**威睿信息技术（中国）有限公司**
北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

# 目录

# 安装和配置 VMware vRealize Orchestrator

《安装和配置 VMware vRealize Orchestrator》提供了有关安装、升级和配置 VMware® vRealize Orchestrator 的信息和说明。

## 目标读者

本文档提供的信息主要面向熟悉虚拟机技术和数据中心操作且具有丰富经验的高级 vSphere 管理员以及系统管理员。

# VMware vRealize Orchestrator 简介

1

VMware vRealize Orchestrator 是一个开发与自动化处理平台，提供可扩展的工作流库，可让您创建并运行可配置的自动化流程，用于管理 VMware 产品以及其他第三方技术。

vRealize Orchestrator 自动执行 VMware 及第三方应用程序的管理和运行任务，例如服务台、变更管理系统和 IT 资产管理系统。

本章讨论了以下主题：



## Orchestrator 平台的主要功能

Orchestrator 由三个不同层组成：一个编排平台，用来提供编排工具所需的常用功能；一个插件基础架构，用来集成对子系统的控制，以及一个工作流库。Orchestrator 是一个开放式平台，可使用新插件和库进行扩展，并可通过 REST API 集成到规模更大的基础架构中。

下表显示了 Orchestrator 的主要功能。

**持久性**

生产级的数据库会用于存储相关信息，例如进程、工作流状态和配置信息。

**集中管理**

Orchestrator 可让您集中管理各种进程。基于应用程序服务器的平台拥有完整的版本历史记录，可在同一存储位置存储脚本和与进程相关的原语。这样，您就可以避免服务器上出现没有版本控制和适当更改控制的脚本。

**检查点**

工作流的每一步骤都会保存在数据库中，从而防止在服务器必须重启时丢失数据。此功能对于长时间运行的进程特别有用。

**控制中心**

控制中心界面可对运行时操作、工作流监视、统一日志访问和配置以及工作流运行和系统资源之间的相关性进行集中管理，从而提高了 vRealize Orchestrator 实例的管理效率。vRealize Orchestrator 还对日志记录机制进行了优化，采用额外的日志文件来收集 vRealize Orchestrator 引擎吞吐的各性能衡量指标。

### 版本控制

Orchestrator 平台的所有对象都有相关的版本历史记录。版本历史记录对于在向项目阶段或位置分发各种进程时的基本变更管理非常有用。

### 脚本引擎

Mozilla Rhino JavaScript 引擎提供了为 Orchestrator 平台创建构建块的方式。增强后的脚本引擎包含基本版本控制、变量类型检查、名称空间管理和异常处理。该引擎可用于以下构建块：

- 操作
- 工作流
- 策略

### 工作流引擎

工作流引擎可让您自动处理各种业务进程。它使用以下对象在工作流中创建分步式进程自动化处理：

- Orchestrator 提供的工作流和操作
- 客户提供的自定义构建块
- 由插件向 Orchestrator 添加的对象

用户、其他工作流、调度或策略可以启动工作流。

### 策略引擎

您可以使用策略引擎监视并重新生成事件，以此对 Orchestrator 服务器或插件技术中多变的条件作出响应。策略可以汇总来自平台或任何插件的事件，帮助您处理任何集成技术上多变的条件。

### 安全

Orchestrator 提供以下高级安全功能：

- 公钥基础架构 (PKI)，用于对服务器之间导入和导出的内容签名并加密。
- 数字版权管理 (DRM)，用于控制对所导出内容进行查看、编辑和重新分发的方式。
- 安全套接字层 (SSL)，用于在桌面客户端与服务器之间进行加密通信，以及对 Web 前端进行 HTTPS 访问。
- 高级访问权限管理，可对进程以及这些进程所操作的对象进行访问控制。

### 加密

vRealize Orchestrator 使用 FIPS 高级加密标准 (AEC) 和 256 位加密密钥对字符串进行加密。加密密钥随机生成，对群集以外的各种设备来说是唯一的。群集中的所有节点都共享同一加密密钥。

# Orchestrator 用户类型与相关职责

Orchestrator 会根据全局用户角色的具体职责提供不同的工具和界面。在 Orchestrator 中，用户可分为完全权限用户（属于管理员组，即管理员）和有限权限用户（不属于管理员组，即最终用户）。

## 完全权限用户

Orchestrator 管理员和开发人员拥有同样的管理权限，但在职责方面有所区分。

### 管理员

该角色对 Orchestrator 平台的所有功能拥有完全访问权限。基本管理职责包括：

- 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
- 运行工作流和调度任务
- 管理导入元素的版本控制
- 创建新的工作流和插件

### 开发人员

这类用户对 Orchestrator 平台的所有功能拥有完全访问权限。开发人员还可访问 Orchestrator 客户端界面并拥有以下职责：

- 创建应用程序来扩展 Orchestrator 平台功能
- 对现有工作流进行自定义和创建新的工作流和插件，实现流程自动化

## 有限权限用户

### 最终用户

最终用户可以运行并调度管理员或开发人员在 Orchestrator 客户端中为其提供的工作流和策略。

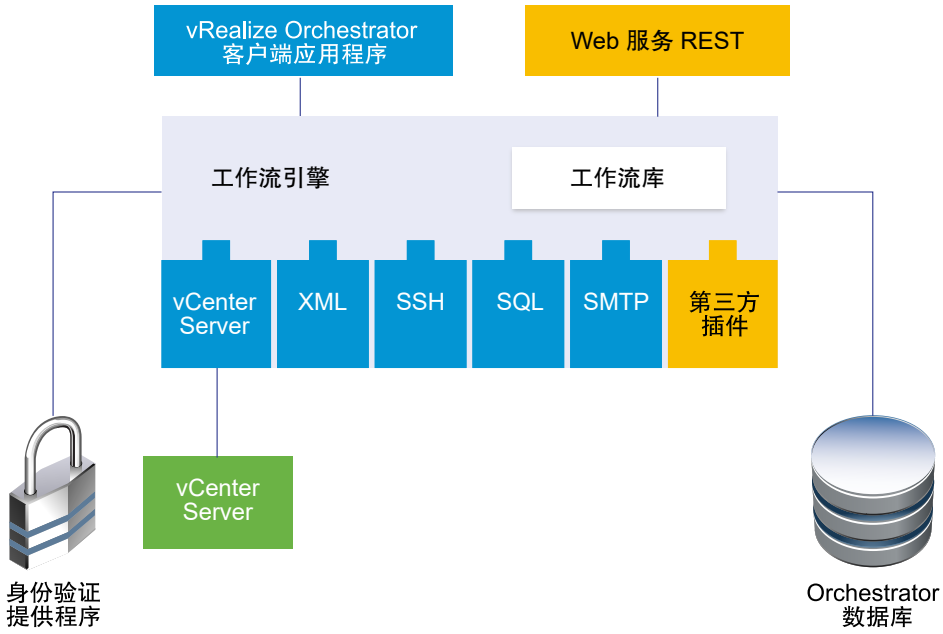
# Orchestrator 架构

Orchestrator 包含一个工作流库和一个工作流引擎，可用于创建并运行相关工作流，实现编排流程自动化。Orchestrator 可通过一系列插件访问各种不同技术对象，您则可以对这些对象运行工作流。

Orchestrator 提供了一组标准插件，包括适用于 vCenter Server 的插件，您可在插件所公开的不同环境中编排各种任务。

Orchestrator 还提供开放式架构，您可将外部第三方应用程序插入到编排平台中。您可以对自定义插件技术的对象运行工作流。Orchestrator 将连接到身份验证提供程序以管理用户帐户，连接到数据库以存储它运行的工作流信息。您可以通过 Orchestrator 客户端界面或通过 Web 服务访问 Orchestrator、Orchestrator 工作流及其公开的对象。

图 1-1. VMware vRealize Orchestrator 架构




# Orchestrator 插件

利用插件，您可以使用 Orchestrator 访问和控制外部技术与应用程序。通过在 Orchestrator 插件中公开外部技术，您可以将对象和功能结合到工作流，用于访问外部技术的对象和函数。

通过插件可以访问的外部技术可能包含虚拟化管理工具、电子邮件系统、数据库、目录服务、远程控制接口等。

Orchestrator 提供了一组标准插件，可用于将上述技术作为 VMware vCenter Server API 和电子邮件功能并入到工作流中。使用插件，您可以自动处理新 IT 服务的交付或调整现有 vRealize Automation 基础架构和应用程序服务的功能。此外，还可以使用 Orchestrator 开放式插件架构，开发用于访问其他应用程序的插件。

VMware 开发的 Orchestrator 插件采用 `.vmoapp` 文件形式分发。有关 VMware 开发和分发的 Orchestrator 插件的详细信息，请参见 http://www.vmware.com/support/pubs/vco_plugins_pubs.html。有关第三方 Orchestrator 插件的详细信息，请参见 https://solutionexchange.vmware.com/store/vco。

# Orchestrator 系统要求

2

您的系统必须满足 Orchestrator 正常工作所需的技术要求。

有关受支持的 vCenter Server、vSphere Web Client、vRealize Automation 和其他 VMware 解决方案版本列表以及兼容的数据库版本列表，请参见 VMware 产品互操作性列表。

本章讨论了以下主题：

- Orchestrator Appliance 硬件要求
- Orchestrator 支持的浏览器
- Orchestrator 数据库要求
- Orchestrator Appliance 中随附的软件
- 国际化支持级别
- Orchestrator 网络端口

## Orchestrator Appliance 硬件要求

Orchestrator Appliance 是一个基于 Linux 的预配置虚拟机。在部署设备前，验证系统是否满足最低硬件要求。

Orchestrator Appliance 具有以下硬件配置：

- 2 个 CPU
- 6 GB 内存
- 17 GB 硬盘

请勿降低默认内存，因为 Orchestrator 服务器至少需要 2 GB 可用内存。

## Orchestrator 支持的浏览器

控制中心需要使用 Web 浏览器。

您必须使用以下任一浏览器连接至控制中心。

- Microsoft Internet Explorer 10 或更高版本

- Mozilla Firefox
- Google Chrome

# Orchestrator 数据库要求

Orchestrator 服务器需要使用数据库。Orchestrator 中预配置了 PostgreSQL 数据库，可用于生产环境。您还可以使用外部数据库，具体视所用的环境而定。

有关各种受支持的数据库版本列表，请参见 VMware 产品互操作性列表。

# Orchestrator Appliance 中随附的软件

Orchestrator Appliance 是一个优化用于 Orchestrator 运行的预配置虚拟机。此设备在分发时已预安装了相关软件。

Orchestrator Appliance 软件包包含以下软件：

- SUSE Linux Enterprise Server 11 Update 3 for VMware，64 位版
- PostgreSQL
- Orchestrator

默认 Orchestrator Appliance 数据配置可用于生产环境。

注 要在生产环境中使用 Orchestrator Appliance，必须将 Orchestrator 服务器配置为通过 vRealize Automation 或 vSphere 进行身份验证。有关配置身份验证提供程序的详细信息，请参见配置独立的 Orchestrator 服务器。

有关配置用于生产环境的数据库的详细信息，请参见设置 Orchestrator 数据库 。

# 国际化支持级别

Orchestrator 控制中心包含西班牙语、法语、德语、繁体中文、简体中文、韩语和日语的区域设置。Orchestrator 客户端支持国际化级别 1。

## Orchestrator 中的非 ASCII 字符支持

尽管 Orchestrator 客户端尚未本地化，但仍可在非英语操作系统上运行并支持非 ASCII 文本。

**表 2-1. Orchestrator GUI 中的非 ASCII 字符支持**

| | 非 ASCII 字符支持 | | | |
|---|---|---|---|---|
| **Orchestrator 项目** | **说明字段** | **名称字段** | **输入和输出参数** | **属性** |
| 操作 | 是 | 否 | 否 | 否 |
| 文件夹 | 是 | 是 | - | - |
| 配置元素 | 是 | 是 | - | 否 |
| 软件包 | 是 | 是 | - | - |

表 2-1. Orchestrator GUI 中的非 ASCII 字符支持 （续）

| | 非 ASCII 字符支持 | | | |
|---|---|---|---|---|
| **Orchestrator 项目** | **说明字段** | **名称字段** | **输入和输出参数** | **属性** |
| 策略 | 是 | 是 | - | - |
| 策略模板 | 是 | 是 | - | - |
| 资源元素 | 是 | 是 | - | - |
| 工作流 | 是 | 是 | 否 | 否 |
| 工作流展示显示组和输入步骤 | 是 | 是 | - | - |

## Oracle 数据库的非 ASCII 字符支持

要采用正确格式将字符存储在 Oracle 数据库中，请先将 NLS_CHARACTER_SET 参数设置为 AL32UTF8，然后再配置 Orchestrator 数据库连接并构建表结构。此设置对于国际化环境至关重要。

# Orchestrator 网络端口

Orchestrator 使用特定端口与其它系统进行通信。这些端口已设置了默认值，且不能更改。

## 默认配置端口

若要提供 Orchestrator 服务，您必须设置默认端口并将防火墙配置为允许入站 TCP 连接。

注 如果使用的是自定义插件，则可能需要其他端口。

表 2-2. VMware vRealize Orchestrator 默认配置端口

| 端口 | 编号 | 协议 | 源 | 目标 | 描述 |
|---|---|---|---|---|---|
| 虚拟设备管理界面 | 5480 | TCP | | | 设备系统设置界面的访问端口。 |
| HTTP 服务器端口 | 8280 | TCP | 最终用户 Web 浏览器 | Orchestrator 服务器 | 发送到 Orchestrator 默认 HTTP Web 端口 8280 的请求会被重定向到默认的 HTTPS Web 端口 8281。 |
| HTTPS 服务器端口 | 8281 | TCP | 最终用户 Web 浏览器 | Orchestrator 服务器 | Web Orchestrator 主页的访问端口。 |
| Web 配置 HTTPS 访问端口 | 8283 | TCP | 最终用户 Web 浏览器 | Orchestrator 配置 | Orchestrator 配置 Web UI 的 SSL 访问端口。 |

## 外部通信端口

您必须将防火墙配置为允许出站连接，以便 Orchestrator 可以与外部服务进行通信。

表 2-3. VMware vRealize Orchestrator 外部通信端口

| 端口 | 编号 | 协议 | 源 | 目标 | 描述 |
| --- | --- | --- | --- | --- | --- |
| SQL Server | 1433 | TCP | Orchestrator 服务器 | Microsoft SQL Server | 与 Microsoft SQL Server 实例（已配置为 Orchestrator 数据库）进行通信的端口。 |
| PostgreSQL | 5432 | TCP | Orchestrator 服务器 | PostgreSQL 服务器 | 与 PostgreSQL Server（已配置为 Orchestrator 数据库）进行通信的端口。 |
| Oracle | 1521 | TCP | Orchestrator 服务器 | Oracle 数据库服务器 | 与 Oracle Database Server（已配置为 Orchestrator 数据库）进行通信的端口。 |
| SMTP 服务器端口 | 25 | TCP | Orchestrator 服务器 | SMTP 服务器 | 用于电子邮件通知的端口。 |
| vCenter ServerAPI 端口 | 443 | TCP | Orchestrator 服务器 | vCenter Server | vCenter ServerAPI 通信端口 - Orchestrator 使用此端口从编排的 vCenter Server 实例中获取虚拟基础架构和虚拟机信息。 |

# 设置 Orchestrator 组件

3

下载并部署 Orchestrator Appliance 时，Orchestrator 服务器已经过预配置。在部署后，服务会自动启动。

若要增加 Orchestrator 设置的可用性和可扩展性，请遵循以下准则：

- 安装并配置数据库，同时配置 Orchestrator 连接到该数据库。
- 安装并配置身份验证提供程序并配置与其结合使用的 Orchestrator。
- 安装和配置负载平衡服务器并将其配置为在两个或多个 Orchestrator 服务器之间分发负载。

本章讨论了以下主题：



## vCenter Server 设置

增加 Orchestrator 设置中的 vCenter Server 实例数会导致 Orchestrator 要管理更多会话。活动会话过多可能会导致 Orchestrator 在出现 10 个以上 vCenter Server 连接时出现超时问题。

有关 vCenter Server 受支持版本的列表，请参见 VMware 产品互操作性列表。

**注** 如果网络拥有足够的带宽和延迟，可以在 Orchestrator 设置中不同的虚拟机上运行多个 vCenter Server 实例。如果使用 LAN 增强 Orchestrator 和 vCenter Server 之间的通信，必须使用 100 MB 网线。

## 身份验证方法

要对用户权限进行身份验证和管理，Orchestrator 需要连接到 vRealize Automation 或 vSphere 服务器实例。

下载并部署 Orchestrator Appliance 时，您必须设置与 vRealize Automation 或 vSphere 的连接。

# 设置 Orchestrator 数据库

Orchestrator 需要使用数据库来存储工作流和操作。

下载并部署 Orchestrator Appliance 时，Orchestrator 服务器已预配置为可与随设备分发的 PostgreSQL 数据库一同使用。默认 Orchestrator Appliance 数据配置可用于生产环境。但是，若要在高负荷的生产环境中使用 Orchestrator，您必须设置单独的数据库，并将 Orchestrator 配置为通过控制中心使用该数据库。

Orchestrator 服务器支持 Oracle、Microsoft SQL Server 和 PostgreSQL 数据库。

用于设置 Orchestrator 数据库的常用工作流包含以下步骤：

1 创建数据库。有关创建数据库的详细信息，请参见数据库提供商的文档。

2 启用数据库的远程连接。

3 配置数据库连接参数。有关详细信息，请参见配置 Orchestrator 数据库连接。

如果您计划设置 Orchestrator 群集，您必须将数据库配置为接受多个连接，以便其接受来自群集中不同 Orchestrator 服务器实例的连接。

数据库设置会影响 Orchestrator 性能。将数据库安装到除 Orchestrator 服务器以外的计算机上，这样可确保 JVM 和数据库服务器不会共享 CPU、RAM 和 I/O。

数据库的位置非常重要，因为 Orchestrator 服务器上几乎每个活动都会触发对数据库的操作。为避免数据库出现连接延迟，请选择距离 Orchestrator 服务器最近的数据库服务器且使用可用带宽最高的网络连接。

根据数据库设置和工作流令牌的处理方式，Orchestrator 数据库大小会有所差异。应为每个 vCenter Server 对象分配约 50 KB 内存空间，为每个工作流运行分配 4 KB 内存空间。

小心 确认要安装 Orchestrator 数据库的计算机上至少拥有 1 GB 可用磁盘空间。

硬盘空间不足可能会导致 Orchestrator 服务器和客户端无法正常工作。

# 安装 Orchestrator

4

Orchestrator 由一个服务器组件和一个客户端组件组成。

Orchestrator 客户端可在 64 位 Windows、Linux 和 Mac 计算机上安装。

若要使用 Orchestrator，您必须先启动 Orchestrator 服务器然后再启动 Orchestrator 客户端。

您可以使用 Orchestrator 控制中心更改默认 Orchestrator 配置设置。

本章讨论了以下主题：



## 下载并部署 Orchestrator Appliance

下载 Orchestrator Appliance 并通过模板部署以进行安装。

**前提条件**

- 验证已安装并运行 vCenter Server。
- 验证要在其上部署设备的主机满足最低硬件要求。有关详细信息，请参见 Orchestrator Appliance 硬件要求。
- 如果系统被隔离，无法访问 Internet，则您必须从 VMware 网站为设备下载 .ova 文件。

**步骤**

1. 以管理员身份登录到 vSphere Web Client。
2. 在 vSphere Web Client 中选择一个清单对象，该对象必须是虚拟机的有效父对象，例如数据中心、文件夹、群集、资源池或主机。
3. 选择**操作 > 部署 OVF 模板**。
4. 输入 .ova 文件的路径或 URL，然后单击**下一步**。
5. 查看 OVF 模板详细信息并单击**下一步**。
6. 接受许可证协议中的条款，然后单击**下一步**。
7. 输入所部署设备的名称和位置，然后单击**下一步**。
8. 选择主机、群集、资源池或 vApp 作为要在其中运行设备的目标，然后单击**下一步**。

9 选择虚拟磁盘和设备存储的保存格式。

| 格式 | 说明 |
| --- | --- |
| **厚置备延迟置零** | 以默认的厚格式创建虚拟磁盘。创建虚拟磁盘时为其分配所需的空间。创建时不会擦除物理设备上保留的任何数据（如有），但是以后从虚拟机首次执行写操作时会按需要将其置零。 |
| **厚置备快速置零** | 支持群集功能，例如 Fault Tolerance。创建虚拟磁盘时为其分配所需的空间。如果物理设备上保留了任何数据，则在创建虚拟磁盘时会将其置零。创建这种格式的磁盘所需的时间可能会比创建其他格式的磁盘长。 |
| **精简置备格式** | 节省硬盘空间。对于精简磁盘，可以根据输入的磁盘大小值置备磁盘所需的数据存储空间。精简磁盘开始时很小，只使用与初始操作所需大小完全相同的存储空间。 |

10 选择想要启用的选项，然后为 root 用户帐户设置初始密码。

初始密码长度不得少于八个字符。

11 （可选） 配置网络设置，然后单击**下一步**。

默认情况下，Orchestrator Appliance 使用 DHCP。您可以更改此设置并在设备的 Web 控制台中指定固定 IP 地址。

12 查看“即将完成”页面，然后单击**完成**。

#### 结果

Orchestrator Appliance 即部署成功。

## 打开 Orchestrator Appliance 电源并打开主页

若要使用 Orchestrator Appliance，您必须首先打开其电源并获取虚拟设备的 IP 地址。

#### 步骤

1 以管理员身份登录 vSphere Web Client。

2 右键单击 Orchestrator Appliance 并选择 **电源 > 打开电源**。

3 在**摘要**选项卡上，查看 Orchestrator Appliance IP 地址。

## 更改 Root 密码

出于安全目的，您可以更改 Orchestrator Appliance 的 root 密码。

#### 前提条件

#### 步骤

1 输入设备用户名和密码。

2 单击**管理**选项卡。

3 在**当前管理员密码**文本框中，输入当前 root 密码。

4 在**新管理员密码**和**重复输入新管理员密码**文本框中输入新密码。

5 单击**变更密码**。

**结果**

您即成功更改了 Orchestrator Appliance 的 root Linux 用户的密码。

## 启用或禁用 vRealize Orchestrator Appliance 上的 SSH 管理员登录

您可以启用或禁用使用 SSH 以 root 用户身份登录 Orchestrator Appliance。

**前提条件**

**步骤**

1 在**管理**选项卡上，选择 **SSH 服务已启用**以启用 Orchestrator SSH 服务。

2 （可选） 单击**管理员 SSH 登录已启用**以允许使用 SSH 以 root 用户身份登录 Orchestrator Appliance。

3 单击**保存设置**。

**结果**

**SSH 状态**会显示为*正在运行*。

## 配置 Orchestrator Appliance 的网络设置

配置 Orchestrator Appliance 的网络设置以指定静态 IP 地址并定义代理设置。

**前提条件**

**步骤**

1 在**网络**选项卡上，单击**地址**。

2 选择设备获取 IP 地址设置的方法。

| 选项 | 描述 |
| --- | --- |
| **DHCP** | 从 DHCP 服务器获取 IP 设置。这是默认设置。 |
| **静态** | 使用静态 IP 设置。输入 IP 地址、网络掩码和网关。 |

您可能需要选择 IPv4 和 IPv6 地址类型，具体取决于网络设置。

3 （可选） 输入必要的网络配置信息。

4 单击**保存设置**。

5 （可选） 设置代理设置并单击**保存设置**。

# 初始配置

5

在开始通过 Orchestrator 将任务自动化和管理系统和应用程序之前，您必须将其配置为使用外部身份验证提供程序并将角色分配给不同的用户。您也可以设置外部数据库，导入 CA 签名证书，安装插件或更改默认日志配置。

本章讨论了以下主题：



## 配置独立的 Orchestrator 服务器

尽管 Orchestrator Appliance 是基于 Linux 的预配置虚拟机，但您必须在访问 Orchestrator 控制中心前按配置向导操作。

### 使用 vRealize Automation 身份验证配置独立的 Orchestrator 服务器。

要准备将要用的 Orchestrator Appliance，必须配置主机设置和身份验证提供程序。您可以配置 Orchestrator 使其通过 vRealize Automation 组件注册表来进行身份验证。

**前提条件**

- 下载并部署 vRealize Orchestrator7.3 Appliance。请参见下载并部署 Orchestrator Appliance。
- 安装和配置 vRealize Automation 并确认 vRealize Automation 服务器是否正在运行。请参见 vRealize Automation 文档。

如果打算创建群集：

- 将负载平衡器设置为在多个 vRealize Orchestrator 实例中分发流量。有关详细信息，请参见 vRealize Orchestrator 负载平衡。
- 设置要用作共享数据库的外部数据库，以便其可以接受来自不同 Orchestrator 实例的连接。

**步骤**

1 访问控制中心以启动配置向导。

   a 导航到 https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter。

   b 以 **root** 用户身份使用您在 OVA 部署期间输入的密码登录。

2 选择**独立 Orchestrator** 部署类型。

   通过选择这种类型，您可以配置单个 Orchestrator 节点或群集的第一个 Orchestrator 节点。

3 单击**更改**以配置可访问控制中心的主机名。

4 配置身份验证提供程序。

   a 在**配置身份验证提供程序**页面中，从**身份验证模式**下拉菜单中选择 **vRealize Automation**。

   b 在**主机地址**文本框中，输入 vRealize Automation 主机地址并单击**连接**。

   c 单击**接受证书**。

   d 在**用户名**和**密码**文本框中，输入在 vRealize Automation 中为 SSO 连接配置的用户帐户的凭据。

   默认情况下，SSO 帐户为**管理员**，默认租户名称为 **vsphere.local**。

   e 在**管理员组**文本框中，输入管理员组的名称并单击**搜索**。

   例如 **vsphere.local\administrators**

   f 在组列表中，双击组的名称以将其选中。

   a 单击**保存更改**。

   此时会显示一条消息，表明您已成功保存并重定向至控制中心主视图。

5 （可选） 将 Orchestrator 节点配置为使用外部共享数据库。有关详细信息，请参见配置数据库连接

6 单击控制中心主页右上角的设置图标，然后单击**注销**。

   从控制中心注销 **root** 帐户。

   注 **root** 帐户将无法再访问控制中心。

7 单击**返回控制中心**。

   您将重定向到 VMware Identity Manager (vIDM) 登录屏幕。

   注 如果您使用负载平衡器服务器，则控制中心仅可通过负载平衡器虚拟服务器地址访问。

8 使用 **vsphere.local** 租户中的**管理员**用户帐户登录控制中心。

在控制中心中，您会看到**基于角色的访问权限管理**菜单选项。

**结果**

您已成功完成控制中心配置。

**后续步骤**

- 确认 **VRA** 是**许可**页面上的已配置许可证提供程序。
- 确认节点已在**验证配置**页面上正确配置。

## 使用 vSphere 身份验证配置独立的 Orchestrator 服务器

您可以使用 vSphere 身份验证模式向 vCenter Single Sign-On 服务器注册 Orchestrator 服务器。vCenter Single Sign-On 身份验证仅适用于 6.0 及更高版本的 vCenter Server。

**前提条件**

- 下载并部署 vRealize Orchestrator7.3 Appliance。请参见下载并部署 Orchestrator Appliance。
- 通过正在运行 vCenter Single Sign-On 服务器安装和配置 vCenter Server。有关信息，请参见 vSphere 文档。

如果打算创建群集：

- 将负载平衡器设置为在多个 vRealize Orchestrator 实例中分发流量。有关详细信息，请参见 vRealize Orchestrator 负载平衡。
- 设置要用作共享数据库的外部数据库，以便其可以接受来自不同 Orchestrator 实例的连接。

**步骤**

1 访问控制中心以启动配置向导。

a 导航到 https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter。

b 以 **root** 用户身份使用您在 OVA 部署期间输入的密码登录。

2 选择**独立 Orchestrator** 部署类型。

通过选择这种类型，您可以配置单个 Orchestrator 节点或群集的第一个 Orchestrator 节点。

3 单击**更改**以配置可访问控制中心的主机名。

4 配置身份验证提供程序。

a 在**配置身份验证提供程序**页面中，从**身份验证模式**下拉菜单中选择 **vSphere**。

b 在**主机地址**文本框中，输入 vSphere 主机地址并单击**连接**。

c 单击**接受证书**。

d 在**用户名**和**密码**文本框中，输入 vCenter Single Sign-On 域本地管理员帐户的凭据。

默认帐户为 **administrator@vsphere.local**。

**注** 已预配置默认租户的名称。

e 在**管理员组**文本框中，输入管理员组的名称并单击**搜索**。

例如 **vsphere.local\Administrators**

f 在组列表中，双击组的名称以将其选中。

a 单击**保存更改**。

此时会显示一条消息，表明您已成功保存并重定向至控制中心主视图。

5 （可选） 将 Orchestrator 节点配置为使用外部共享数据库。有关详细信息，请参见配置数据库连接

6 单击控制中心主页右上角的设置图标，然后单击**注销**。

从控制中心注销 **root** 帐户。

**注** **root** 帐户将无法再访问控制中心。

7 单击**返回控制中心**。

您将重定向到 vCenter Single Sign-On 登录屏幕。

**注** 如果您使用负载平衡器服务器，则控制中心仅可通过负载平衡器虚拟服务器地址访问。

8 使用您在步骤 **4e** 中配置的管理员组成员的帐户（默认情况下为 administrator@vsphere.local）登录到控制中心。

在控制中心中，您会看到**基于角色的访问权限管理**菜单选项。

**结果**

您已成功完成控制中心配置。

**后续步骤**

- 确认 **CIS** 是**许可**页面上的已配置许可证提供程序。
- 确认节点已在**验证配置**页面上正确配置。

# Orchestrator 网络端口

Orchestrator 使用特定端口与其它系统进行通信。这些端口已设置了默认值，且不能更改。

## 默认配置端口

若要提供 Orchestrator 服务，您必须设置默认端口并将防火墙配置为允许入站 TCP 连接。

**注** 如果使用的是自定义插件，则可能需要其他端口。

表 5-1. VMware vRealize Orchestrator 默认配置端口

| 端口 | 编号 | 协议 | 源 | 目标 | 描述 |
| --- | --- | --- | --- | --- | --- |
| 虚拟设备管理界面 | 5480 | TCP | | | 设备系统设置界面的访问端口。 |
| HTTP 服务器端口 | 8280 | TCP | 最终用户 Web 浏览器 | Orchestrator 服务器 | 发送到 Orchestrator 默认 HTTP Web 端口 8280 的请求会被重定向到默认的 HTTPS Web 端口 8281。 |
| HTTPS 服务器端口 | 8281 | TCP | 最终用户 Web 浏览器 | Orchestrator 服务器 | Web Orchestrator 主页的访问端口。 |
| Web 配置 HTTPS 访问端口 | 8283 | TCP | 最终用户 Web 浏览器 | Orchestrator 配置 | Orchestrator 配置 Web UI 的 SSL 访问端口。 |

## 外部通信端口

您必须将防火墙配置为允许出站连接，以便 Orchestrator 可以与外部服务进行通信。

表 5-2. VMware vRealize Orchestrator 外部通信端口

| 端口 | 编号 | 协议 | 源 | 目标 | 描述 |
| --- | --- | --- | --- | --- | --- |
| SQL Server | 1433 | TCP | Orchestrator 服务器 | Microsoft SQL Server | 与 Microsoft SQL Server 实例（已配置为 Orchestrator 数据库）进行通信的端口。 |
| PostgreSQL | 5432 | TCP | Orchestrator 服务器 | PostgreSQL 服务器 | 与 PostgreSQL Server（已配置为 Orchestrator 数据库）进行通信的端口。 |
| Oracle | 1521 | TCP | Orchestrator 服务器 | Oracle 数据库服务器 | 与 Oracle Database Server（已配置为 Orchestrator 数据库）进行通信的端口。 |
| SMTP 服务器端口 | 25 | TCP | Orchestrator 服务器 | SMTP 服务器 | 用于电子邮件通知的端口。 |
| vCenter ServerAPI 端口 | 443 | TCP | Orchestrator 服务器 | vCenter Server | vCenter ServerAPI 通信端口 - Orchestrator 使用此端口从编排的 vCenter Server 实例中获取虚拟基础架构和虚拟机信息。 |

# 配置 Orchestrator 数据库连接

Orchestrator 服务器需要一个数据库用于存储数据。

下载并部署 Orchestrator Appliance 时，Orchestrator 服务器已配置为可与设备中预安装的 PostgreSQL 数据库一同使用。

预配置的 Orchestrator PostgreSQL 数据库可用于生产环境。若要在高负载的生产环境中获得更佳性能，请另外安装关系型数据库管理系统 (RDBMS) 并为 Orchestrator 创建数据库。有关为 Orchestrator 创建数据库的详细信息，请参见设置 Orchestrator 数据库 。若要将 Orchestrator 与外部数据库结合使用，请配置数据库进行远程连接。

# 导入数据库 SSL 证书

如果数据库使用 SSL，您必须将 SSL 证书导入控制中心，并在 Orchestrator 和数据库之间建立安全连接。

### 前提条件

- 配置数据库进行 SSL 访问。请参见数据库文档获取相关说明。
- 获取自签名服务器证书或由 Certificate Authority 签名的证书。
- 明确指定受信任的证书以正确进行 SSL 授权。

### 步骤

1 单击**证书**。

2 在**受信任的证书**选项卡上，单击**导入**。

3 从 URL 或文件加载数据库 SSL 证书。

| 选项 | 操作 |
| --- | --- |
| **从 URL 或代理 URL 导入** | 输入数据库服务器的 URL：<br>`https://your_database_server_IP_address` 或 `your_database_server_IP_address:port` |
| **从文件导入** | 获取数据库 SSL 证书文件并浏览以将其导入。 |

### 结果

导入的证书会显示在受信任 SSL 证书列表中。此时即激活了 Orchestrator 与数据库之间的安全连接。

### 后续步骤

配置数据库连接时，必须在控制中心的**配置数据库**页面中启用 SSL。

# 配置数据库连接

若要建立与 Orchestrator 数据库的连接，必须设置该数据库连接参数。

### 前提条件

- 建立要与 Orchestrator 服务器配合使用的新数据库。请参见设置 Orchestrator 数据库 。
- 如果您采用的是配置为使用动态端口的 SQL Server 数据库，请确认该 SQL Server Browser 服务正在运行。
- 若要在使用 Microsoft SQL Server 数据库时避免发生事务性死锁，您必须启用 `ALLOW_SNAPSHOT_ISOLATION` 和 `READ_COMMITTED_SNAPSHOT` 两个数据库选项。
- 如果您的 Microsoft SQL Server 数据库使用动态端口，请确保 SQL Server Browser 已在运行。
- 若要在使用 Oracle 数据库时避免 `ORA-01450` 错误，请确认您已正确配置了数据库块大小。所需最小值取决于 Oracle 数据库索引所用块的大小。

- 要采用正确格式将字符存储在 Oracle 数据库中，请在为 Orchestrator 配置数据库连接并构建表结构之前，将 NLS_CHARACTER_SET 参数设置为 AL32UTF8。此设置对于国际化环境至关重要。
- 若要将 Orchestrator 配置为通过安全连接与数据库通信，请确保已导入该数据库的 SSL 证书。有关详细信息，请参见导入数据库 SSL 证书。

**步骤**

1 以**管理员**身份登录到控制中心。

2 单击**配置数据库**。

3 从**数据库类型**下拉菜单中，选择想要 Orchestrator 服务器使用的数据库类型。

| 选项 | 描述 |
| --- | --- |
| **Oracle** | 将 Orchestrator 配置为与 Oracle 数据库实例配合工作。 |
| **SQL Server** | 将 Orchestrator 配置为与 Microsoft SQL Server 数据库实例配合工作。 |
| **PostgreSQL** | 将 Orchestrator 配置为与 PostgreSQL 数据库实例配合工作。 |
| **内嵌 DerbyDB** | 将 Orchestrator 配置为与内嵌 DerbyDB 数据库配合工作。<br>注 切勿使用 DerbyDB。 |

4 输入该数据库连接参数，然后单击**保存更改**。

| 选项 | 描述 |
| --- | --- |
| **服务器地址** | 数据库服务器 IP 地址或 DNS 名称。<br>此选项适用于所有数据库。 |
| **端口** | 该数据库服务器端口用于与您自己的数据库进行通信。<br>此选项适用于所有数据库。 |
| **使用 SSL** | 选择**使用 SSL** 以通过 SSL 连接到数据库。若要使用此选项，您必须确保已将数据库 SSL 证书导入 Orchestrator。<br>此选项适用于所有数据库。 |
| **数据库名称** | 数据库的唯一全称。数据库名称在初始化参数文件的 SERVICE_NAMES 参数中指定。<br>此选项仅适用于 SQL Server 和 PostgreSQL 数据库。 |
| **用户名** | Orchestrator 连接和操作所选数据库时所用的用户名。所选名称必须为目标数据库上的有效用户名并具有 **db_owner** 权限。<br>此选项适用于所有数据库。<br>注 预配置的 PostgreSQL 数据库的默认用户名为 **vmware**。 |
| **密码** | 该用户名的密码。<br>此选项适用于所有数据库。<br>注 预配置的 PostgreSQL 数据库的默认密码为 **vmware**。 |
| **实例名称（如有）** | 数据库实例名称，可由数据库初始化参数文件的 INSTANCE_NAME 参数识别。<br>此选项仅适用于 SQL Server 和 Oracle 数据库。 |

| 选项 | 描述 |
| --- | --- |
| **域** | 若要使用 Windows 身份验证，请输入 SQL Server 计算机的域名，例如 *company.org*。<br>若要使用 SQL 身份验证，请将此文本框留空。<br>此选项仅适用于 SQL Server，指定您要使用 Windows 还是 SQL Server 进行身份验证。 |
| **使用 Windows 身份验证模式 (NTLMv2)** | 选中此项以在使用 Windows 身份验证时发送 NTLMv2 响应。<br>此选项仅适用于 SQL Server。 |

如果指定的参数正确，此时会显示一条消息，表示已成功连接到此数据库。

5 更新 Orchestrator 的表结构（如有需要）。

6 单击**保存更改**。

#### 结果

数据库连接即已配置成功。

## 导出 Orchestrator 数据库

创建服务器数据库完整备份的存档。只有当数据库为 PostgreSQL 且在 Linux 上运行时，才能将其导出。

#### 步骤

1 单击**导出数据库**。

2 选择是否要随数据库一起导出工作流令牌和日志事件。

3 单击**导出数据**

#### 结果

控制中心会在安装了 Orchestrator 服务器的计算机上创建 `vco-db-dump-`*`databaseName`*`@`*`hostname`*`.gz` 文件。您可以使用该文件克隆并还原系统。

## 导入 Orchestrator 数据库

在重新安装 Orchestrator 或系统发生故障后，可以导入之前导出的数据库。

#### 前提条件

新的 Orchestrator 数据库必须为空。

#### 步骤

1 单击**导入数据库**。

2 浏览并选择您从上次安装中导出的 `.gz` 文件。

3 单击**导入数据库**

**结果**

此时会显示一条消息，表示数据库已成功导入。新系统即获得了旧系统的数据库。

# 管理证书

证书针对特定服务器颁发，其中包含有关服务器公钥的信息，您可以使用证书对 Orchestrator 中创建的所有元素进行签名，保证其真实可靠。客户端收到来自您服务器的元素（通常为软件包）时，会验证您的身份并决定是否信任您的签名。

**重要事项** 如果 Orchestrator 使用内嵌 Apache Derby 数据库，则您无法更改服务器证书。

- 管理 Orchestrator 证书

  您可以使用“配置”工作流类别中的“SSL Trust Manager”工作流在控制中心的**证书**页面或通过 Orchestrator 客户端来管理 Orchestrator 证书。

## 管理 Orchestrator 证书

您可以使用“配置”工作流类别中的“SSL Trust Manager”工作流在控制中心的**证书**页面或通过 Orchestrator 客户端来管理 Orchestrator 证书。

### 将证书导入 Orchestrator 信任存储区

控制中心使用安全连接与 vCenter Server、关系型数据库管理系统、LDAP、单点登录和其他服务器进行通信。您可以从 URL 或 PEM 编码的文件导入所需 SSL 证书。每次想要对服务器实例使用 SSL 连接时，您必须从**证书**页面上的**受信任证书**选项卡导入相应的证书，并导入相应的 SSL 证书。

您可以从 URL 地址或 PEM 编码的文件将 SSL 证书加载到 Orchestrator 中。

| 选项 | 描述 |
| --- | --- |
| **从 URL 或代理 URL 导入** | 远程服务器的 URL：<br>**https://*your_server_IP_address*** 或 ***your_server_IP_address:port*** |
| **从文件导入** | PEM 编码的证书文件的路径。<br>有关导入 PEM 编码证书文件的详细信息，请参见通过控制中心导入受信任证书。 |

### 生成自签名服务器证书

Orchestrator Appliance 包含一个可根据设备的网络设置自动生成的自签名证书。如果设备的网络设置变更，则必须手动生成新的自签名证书。您可以创建自签名证书以确保通信加密，并为软件包提供签名。但是，收件人无法确定该自签名软件包是由您的服务器颁发还是由假冒您的第三方所颁发。若要证明服务器的身份信息，请使用证书颁发机构签名的证书。

您可以在控制中心的**证书**页面的 **Orchestrator 服务器 SSL 证书**选项卡中生成自签名证书。

| 选项 | 描述 |
| --- | --- |
| **签名算法** | 用来生成数字签名的加密算法。 |
| **公用名** | Orchestrator 服务器的主机名。 |

| 选项 | 描述 |
| --- | --- |
| **组织** | 贵组织的名称。例如 **VMware**。 |
| **组织单位** | 贵组织单位的名称。例如 **R&D**。 |
| **国家/地区代码** | 国家/地区代码缩写。例如 **US**。 |

Orchestrator 会生成在您的环境中唯一的服务器证书。有关证书公共密钥的详细信息会显示在 **Orchestrator 服务器 SSL 证书**选项卡上。专用密钥则存储在 Orchestrator 数据库的 `vmo_keystore` 表格中。

## 导入 Orchestrator 服务器 SSL 证书

vRealize Orchestrator 使用 SSL 证书在安全通信期间向客户端和远程服务器表明自己的身份。默认情况下，Orchestrator 包含一个可根据设备的网络设置自动生成的自签名 SSL 证书。您可以导入证书颁发机构签名的 SSL 证书来避免证书信任错误。

您必须导入由证书颁发机构签名且采用 PEM 编码的文件的证书，文件中应包含公共和专用密钥。

## 软件包签名证书

从 Orchestrator 服务器导入的软件包经过数字签名。导入、导出或生成用于软件包签名的新证书。软件包签名证书是一种数字身份标识形式，用来保证加密通信和 Orchestrator 软件包的签名。

Orchestrator Appliance 包含一个可根据设备的网络设置自动生成的软件包签名证书。如果设备的网络设置变更，则必须手动生成新的软件包签名证书。

注 Orchestrator Appliance 包含一个会在 Orchestrator 初始配置期间自动生成的自签名软件包签名证书。您可以更改该软件包签名证书，更改之后，未来导出的所有软件包都会使用新证书签名。

## 通过控制中心导入受信任证书

为了能与其他服务器安全地进行通信，Orchestrator 服务器必须能够验证其身份。为此，您可能需要将远程实体的 SSL 证书导入到 Orchestrator 信任存储区。要信任某个证书，您可以通过建立到特定 URL 的连接或直接将其作为 PEM 编码文件将该证书导入到信任存储区。

### 前提条件

找到您想要通过 SSL 连接的 Orchestrator 服务器的完全限定域名。

### 步骤

1 使用 SSH 以 **root** 用户身份登录 Orchestrator Appliance。

2 运行命令，以检索远程服务器的证书。

```
openssl s_client –connect host_or_dns_name:secure_port
```

a 如果您使用未加密的端口，请在 `openssl` 命令后加上 `starttls` 和所需协议。

```
openssl s_client –connect host_or_dns_name:25 –starttls smtp
```

3 将 -----BEGIN CERTIFICATE-----和 -----END CERTIFICATE----- 标记之间的文本复制到文本编辑器，并将其保存为一个文件。

4

5 转到**证书**页面。

6 在**受信任证书**选项卡上，单击**导入**，然后选择**从 PEM 编码文件导入**选项。

7 定位到证书文件，然后单击**导入**。

**结果**

您即成功将远程服务器证书导入到 Orchestrator 信任存储区。

# 配置 Orchestrator 插件

默认 Orchestrator 插件仅通过工作流进行配置。

如果想要配置任一默认 Orchestrator 插件，需要使用 Orchestrator 客户端相应的工作流。

## 管理 Orchestrator 插件

在控制中心的**管理插件**页面中，可以查看 Orchestrator 所安装全部插件的列表，并可执行基本的管理操作。

### 更改插件日志记录级别

您可以针对特定插件更改日志记录级别，而不用针对 Orchestrator。

### 安装新插件

使用 Orchestrator 插件，Orchestrator 服务器可以与其他软件产品进行集成。Orchestrator Appliance 包含一组预安装的插件，您也可以安装自定义插件。

所有 Orchestrator 插件都通过控制中心进行安装。可用的文件扩展名包括 `.vmoapp` 和 `.dar`。`.vmoapp` 文件可以包含多个不同的 `.dar` 文件，并可作为应用程序进行安装，而 `.dar` 文件则包含与某一个插件相关的所有资源。

### 禁用插件

您可取消选中插件名称旁的**启用**复选框来禁用插件。

此操作不会移除插件文件。有关在 Orchestrator 中卸载插件的更多信息，请参见卸载插件。

# 卸载插件

您可以使用控制中心来禁用插件，但此操作不会将插件文件从 Orchestrator Appliance 文件系统中移除。要移除插件文件，您必须登录 Orchestrator Appliance 并手动移除插件文件。

**步骤**

1 从 Orchestrator Appliance 删除插件。

   a 使用 SSH 以 **root** 用户身份登录 Orchestrator Appliance。

   b 使用文本编辑器打开 `/etc/vco/app-server/plugins/_VSOPluginInstallationVersion.xml` 文件。

   c 删除与想要移除的插件对应的代码行。

   d 导航到 `/var/lib/vco/app-server/plugins` 目录。

   e 删除其中包含想要移除的插件的 `.dar` 存档。

2 重新启动 vRealize Orchestrator 服务。

```
service vco-configurator restart && service vco-server restart
```

3

4 在**管理插件**页面，验证是否已移除插件。

5 通过 Orchestrator 客户端，删除与该插件相关的软件包和文件夹。

   a 登录到 Orchestrator 客户端。

   b 从位于左上角的下拉菜单中选择**设计**。

   c 单击**软件包**视图。

   d 右键单击要删除的软件包，然后选择**删除元素和内容**。

   > **注** 锁定为只读状态的 Orchestrator 元素（例如，标准库中的工作流）不会被删除。

   e 从位于右上角的**工具**菜单中，选择**用户首选项**。

   **首选项**上下文菜单将打开。

   f 在**常规**页面，选中**允许删除非空文件夹**复选框。

   您即可通过单击删除整个文件夹，包括其子文件夹和工作流。

   g 单击**工作流**视图。

   h 删除您想要移除的插件的文件夹。

   i 单击**操作**视图。

   j 删除您想要移除的插件的操作模块。

6 重新启动 vRealize Orchestrator 服务。

**结果**

您即移除了与插件相关的全部自定义工作流、操作、策略、配置、设置和资源。

# Orchestrator 启动选项

首次启动 Orchestrator 可能需要 5 - 10 分钟，因为服务器会在数据库表格中安装 Orchestrator 插件内容。

控制中心的配置更改会触发 Orchestrator 服务器服务自动重新启动。在控制中心的**启动选项**页面中，可以手动启动、停止并重新启动 Orchestrator 服务器服务。

**启动选项**页面会显示 `vco-server` 服务的状态。

| 状态 | 描述 |
| --- | --- |
| 正在运行 | Orchestrator 服务器服务已初始化并正确运行。 |
| 未定义 | Orchestrator 服务器服务正在启动。 |
| 已停止 | Orchestrator 服务器服务未在运行。 |

在群集环境中，单击**启动选项**页面上的**重新启动**按钮将仅重新启动本地节点上的 Orchestrator 服务器服务。

注　要验证您正在访问群集中的哪些 Orchestrator 实例，请导航至控制中心的 **Orchestrator 群集管理**页面，您将看到**本地节点**复选标记。

要重新启动群集中所有节点上的 Orchestrator 服务器服务，您必须通过 SSH 登录到每个节点，并运行 `service vco-server restart` 命令。

# Orchestrator 可用性和可扩展性

若要提高 Orchestrator 服务的可用性，请在包含共享数据库的群集中启动多个 Orchestrator 服务器实例。在配置为作为群集的一部分运行前，vRealize Orchestrator 始终作为单个实例运行。

## Orchestrator 群集

具有相同服务器配置与插件配置的多个 Orchestrator 服务器实例可在同一个群集中运行，并且共享同一个数据库。

所有 Orchestrator 服务器实例可通过交换检测信号互相通信。每个检测信号都是一个时间戳，节点会按特定间隔将这些时间戳写入到群集的共享数据库中。网络问题、数据库服务器未响应或过载都可能导致 Orchestrator 群集节点停止响应。如果活动的 Orchestrator 服务器实例未能在故障切换超时时间段内发送检测信号，则会被认为未响应。故障切换超时时间等于检测信号间隔值乘以故障切换检测信号数量。可以据此来判定不可靠的节点，并可根据可用的资源和生产负载自定义该值。

Orchestrator 节点在丢失与数据库的连接时会进入待机模式，并将此模式一直保持到数据库连接恢复为止。通过从最后未完成的项目（例如可编辑脚本任务或工作流调用）恢复所有中断的工作流，群集中的其他节点将接管活动的作业。

Orchestrator 不提供内置工具用于监控群集状态和发送故障切换通知。您可以使用外部组件（例如负载平衡器）监控群集状态。要检查一个节点是否正在运行，您可以在 https://*your_orchestrator_server_IP_or_DNS_name*:8281/vco/api/healthstatus 使用运行状况 REST API 服务，并在 https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter/docs/ 检查节点的状态以监控控制中心的状态。

# 配置 Orchestrator 群集

要扩展 Orchestrator 服务，并在高可用性模式下使用 Orchestrator，您可以创建两个或多个 Orchestrator 实例群集。

## 使用 vRealize Automation 身份验证配置 Orchestrator 7.3 实例群集

要组成群集，您可以将 Orchestrator 实例配置为将 vRealize Automation 用作身份验证提供程序并将其他 Orchestrator 节点加入其中。

一个 Orchestrator 群集应至少由两个共享同一数据库的 Orchestrator 服务器实例组成。

### 前提条件

- 配置独立的 Orchestrator 服务器节点。请参见使用 vRealize Automation 身份验证配置独立的 Orchestrator 服务器。。
- 对安装有 Orchestrator 服务器实例的虚拟机的时钟进行同步操作。
- 将负载平衡器设置为在多个 vRealize Orchestrator 实例中分发流量。请参见 vRealize Orchestrator 负载平衡。

### 步骤

1 访问将要添加到群集的节点的控制中心以启动配置向导。

   a 导航到 https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter。

   b 以 **root** 用户身份使用您在 OVA 部署期间输入的密码登录。

2 选择**群集 Orchestrator** 部署类型。

   通过选择此类型可以将节点加入到现有的 Orchestrator 群集。

3 在**主机名**文本框中，输入第一个 Orchestrator 服务器实例的主机名或 IP 地址。

   **注** 必须是您要加入群集的 Orchestrator 实例的本地 IP 或主机名。请勿使用负载平衡器地址。

4 在**用户名**和**密码**文本框中，输入第一个 Orchestrator 服务器实例的 root 凭据。

5 单击**加入**。

   Orchestrator 实例节点会克隆其加入的节点的配置。

6 单击控制中心主页右上角的设置图标，然后单击**注销**。

   从控制中心注销 **root** 帐户。您将重定向到 VMware Identity Manager (vIDM) 注销屏幕。

   **注** **root** 帐户将无法再访问控制中心。

7 单击**返回登录页面**。

您将重定向到 VMware Identity Manager (vIDM) 登录屏幕。

注 发送到群集中各个 Orchestrator 节点的请求由负载平衡器服务器管理，因此无法再单独访问控制中心。

8 使用 **vsphere.local** 租户中的**管理员**用户帐户登录控制中心。

#### 结果

您即成功配置了 Orchestrator 实例群集。

#### 后续步骤

确认节点已在**验证配置**页面上正确配置。

## 使用 vSphere 身份验证配置 Orchestrator 7.3 实例的群集

要组成群集，您可以将 Orchestrator 实例配置为将 vCenter Single Sign-On 用作身份验证提供程序并将其他 Orchestrator 节点加入其中。

一个 Orchestrator 群集应至少由两个共享同一数据库的 Orchestrator 服务器实例组成。

#### 前提条件

- 配置独立的 Orchestrator 服务器节点。请参见使用 vSphere 身份验证配置独立的 Orchestrator 服务器。
- 对安装有 Orchestrator 服务器实例的虚拟机的时钟进行同步操作。
- 将负载平衡器设置为在多个 vRealize Orchestrator 实例中分发流量。请参见 vRealize Orchestrator 负载平衡。

#### 步骤

1 访问将要添加到群集的节点的控制中心以启动配置向导。

a 导航到 https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter。

b 以 **root** 用户身份使用您在 OVA 部署期间输入的密码登录。

2 选择**群集 Orchestrator** 部署类型。

通过选择此类型可以将节点加入到现有的 Orchestrator 群集。

3 在**主机名**文本框中，输入第一个 Orchestrator 服务器实例的主机名或 IP 地址。

注 必须是您要加入群集的 Orchestrator 实例的本地 IP 或主机名。请勿使用负载平衡器地址。

4 在**用户名**和**密码**文本框中，输入第一个 Orchestrator 服务器实例的 root 凭据。

5 单击**加入**。

Orchestrator 实例节点会克隆其加入的节点的配置。

6 单击控制中心主页右上角的设置图标，然后单击**注销**。

从控制中心注销 **root** 帐户。您将重定向到 vCenter Single Sign-On 登录屏幕。

注 **root** 帐户将无法再访问控制中心。

注 发送到群集中各个 Orchestrator 节点的请求由负载平衡器服务器管理，因此无法再单独访问控制中心。

7 使用身份验证提供程序的**管理员组**成员的帐户登录控制中心。

管理员默认帐户是 **administrator@vsphere.local**。

#### 结果

您即成功配置了 Orchestrator 实例群集。

#### 后续步骤

确认节点已在**验证配置**页面上正确配置。

## 监控 Orchestrator 群集

在创建群集后，您可以监控群集节点的状态并采取进一步操作以保持各节点同步。

您可以在 **Orchestrator 群集管理**页面的 **Orchestrator 节点设置**选项卡中查看已加入某个群集的 Orchestrator 实例的配置同步状态。

重要事项 控制中心会报告本地节点相对于群集中其他节点的状态。

| 配置同步状态 | 本地节点 | 远程节点 |
| --- | --- | --- |
| 已同步 | 本地节点的配置自上次重新启动后未更改。 | 远程节点的配置与本地节点的配置相同。 |
| 等待重启 | 本地节点配置已更改或是由远程节点复制的。重新启动 Orchestrator 服务器服务以应用挂起配置。 | 远程节点的配置与本地节点已同步，但未应用。重新启动 Orchestrator 服务器服务以应用挂起配置。 |
| 需要同步配置 | 不适用 | 远程节点的活动配置与本地节点的活动配置不同。 |
| 该节点的控制中心不可用 | 不适用 | 远程节点的控制中心服务 (vco-configurator) 已停止或无法访问。同步状态无法检索。 |
| 不可用。缺少本地节点 | 本地节点未包含在群集节点列表中。本地节点的同步状态无法检索。 | 不适用 |

### 将节点从 Orchestrator 群集中移除

Orchestrator 群集管理包括将节点添加到群集和从群集中移除节点。您可以将现有节点从 Orchestrator 群集移除，以替换成新的节点或减少容量。

要从 Orchestrator 群集永久移除某个节点，您必须关闭 Orchestrator 设备的电源并删除托管该节点的虚拟机。有关详细信息，请参见《vSphere 虚拟机管理》文档。此后，您必须编辑负载平衡器配置以删除群集中已不再可用的 Orchestrator 节点的条目。

如果控制中心显示的节点不再属于群集，请访问高级 **Orchestrator 群集管理**页面（地址为：https://*your_orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter/#/control-app/ha?remove-nodes）以删除残留记录。

## 控制中心基于角色的访问权限管理

使用基于角色的访问权限管理，已配置身份验证提供程序的用户或组可以在控制中心中拥有不同的角色。

将 Orchestrator 配置为将 vRealize Automation 或 vSphere 用作身份验证提供程序后，您无法再以 **root** 用户身份登录控制中心。有关详细信息，请参见配置独立的 Orchestrator 服务器。

控制中心提供了三种预定义的角色。**管理员**角色包含**租户管理员**角色的权限。**租户管理员**角色包含**使用者**角色的权限。

| 控制中心角色 | 权限 |
| --- | --- |
| **管理员** | 拥有访问控制中心所有配置菜单的权限。 |
| **租户管理员** | 有权访问：<br>■ **基于角色的访问权限管理**。<br>■ **检查工作流**。有关详细信息，请参见检查工作流。 |
| **使用者** | 拥有访问**检查工作流**的权限。 |

**注** 部分身份验证提供程序角色将被自动映射到控制中心角色。

身份验证是 vSphere 时，来自在身份验证提供程序配置期间选择的**管理员组**的用户可以查看控制中心的所有选项。vSphere 身份提供程序的所有其他用户都可以登录，但它们不能查看控制中心的任何菜单。

当身份验证提供程序是 vRealize Automation 时，vRealize Automation **系统管理员**可以查看控制中心的所有配置选项。vRealize Automation **租户管理员**自动接收**租户管理员**权限，vRealize Automation 身份提供程序的所有其他用户将被映射到**使用者**角色。

### 将用户角色分配给控制中心的用户

要通过 vRealize Automation 或 vSphere 所用的身份提供程序配置在控制中心拥有特定权限的用户和组，您必须将其添加到基于角色的访问权限管理，并为其分配一个或多个预定义角色。

**步骤**

1

2 在**基于角色的访问权限管理**页面中，单击**添加**按钮。

3 在**用户或组**文本框中，输入您要添加的用户或组的名称或部分名称。

4 单击**搜索**。

列表中将显示与搜索条件匹配的条目或与条目列表。

5 单击要添加的用户或组的条目。

6 选择一个或多个可用角色。

注 默认情况下，身份验证提供程序的**管理员组**的成员都具有管理员访问权限。其特权不可见且不能通过控制中心的**基于角色的访问权限管理**页面进行修改。

7 单击**添加**可将角色分配给选定的用户或组。

您会看到拥有控制中心访问权限的用户和组的列表及其角色分配。

# 配置客户体验改善计划

如果选择参加客户体验改善计划 (CEIP)，VMware 会匿名收集某些信息，帮助提高 VMware 产品和服务的质量、可靠性和功能。

## VMware 接收的信息类别

客户体验改善计划 (Customer Experience Improvement Program, CEIP) 将向 VMware 提供让 VMware 可以改善其产品和服务以及修复问题的信息。如果您选择参与 CEIP，VMware 将定期在 CEIP 报告中收集有关您对 VMware 产品和服务的使用的特定类型的技术信息。

要了解 VMware 收集的信息类型以及如何使用此信息，请访问 VMware CEIP 门户，网址为 http://www.vmware.com/trustvmware/ceip.html

## 加入客户体验改善计划

在控制中心内加入客户体验改善计划。

**步骤**

1 以**管理员**身份登录控制中心，然后打开**客户体验改善计划**页面。

2 选择**加入客户体验改善计划**复选框以启用客户体验改善计划 (CEIP) 或取消选中复选框以禁用计划，然后单击**保存**。

3 （可选） 如果想要手动添加代理主机，请取消选中**自动发现代理**。

# 使用 API 服务

6

除了使用控制中心配置 Orchestrator 外，您还可以使用存储在设备中的 Orchestrator REST API、控制中心 REST API 或命令行实用程序来修改 Orchestrator 服务器配置设置。

默认情况下，Orchestrator 软件包中随附配置插件。您可以通过 Orchestrator 工作流库或 Orchestrator REST API 访问配置插件工作流。使用这些工作流，您可以更改 Orchestrator 服务器的受信任证书以及密钥库设置。有关所有可用 Orchestrator REST API 服务调用的信息，请参见《Orchestrator REST API 参考》文档，位于 https://*orchestrator_server_IP_or_DNS_name*:8281/vco/api/docs。

- 使用 REST API 管理 SSL 证书和密钥库

  除了使用控制中心管理 SSL 证书外，您还可以通过运行配置插件中的工作流或使用 REST API 来管理受信任的证书和密钥库。

- 使用控制中心 REST API 自动处理 Orchestrator 配置

  控制中心 REST API 提供了资源的访问权限，可用于配置 Orchestrator 服务器。您可以使用控制中心 REST API 与第三方系统自动处理 Orchestrator 配置。

## 使用 REST API 管理 SSL 证书和密钥库

除了使用控制中心管理 SSL 证书外，您还可以通过运行配置插件中的工作流或使用 REST API 来管理受信任的证书和密钥库。

配置插件包含用于导入和删除 SSL 证书及密钥库的工作流。在 Orchestrator 客户端的工作流视图中，可以导航到**库 > 配置 > SSL Trust Manager** 和**库 > 配置 > 密钥库**访问这些工作流。您还可以使用 Orchestrator REST API 运行这些工作流。

### 使用 REST API 删除 SSL 证书

您可以运行配置插件的“删除受信任证书”工作流或使用 REST API 删除 SSL 证书。

**步骤**

1 在“删除受信任证书”工作流的工作流服务的 URL 发起 GET 请求。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Delete trusted
certificate
```

2 在定义的 URL 发起 GET 请求以检索“删除受信任证书”工作流定义。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd
```

3 在持有“删除受信任证书”工作流执行对象的 URL 发起 POST 请求。

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd/
executions/
```

4 在请求正文中，将想要删除的证书的名称作为“删除受信任证书”工作流的输入参数应用于执行上下文的元素。

## 使用 REST API 导入 SSL 证书

您可以运行配置插件中的工作流或使用 REST API 导入 SSL 证书。

您可以从文件或 URL 导入受信任的证书。有关使用控制中心在 Orchestrator 中导入证书的信息，请参见管理 Orchestrator 证书。

**步骤**

1 在工作流服务的 URL 发起 GET 请求。

| 选项 | 描述 |
| --- | --- |
| **从文件导入受信任证书** | 从文件导入受信任证书。 |
| **从 URL 导入受信任证书** | 从 URL 地址导入受信任证书。 |
| **使用代理服务器从 URL 导入受信任证书** | 使用代理服务器从 URL 地址导入受信任证书。 |
| **从 URL 导入受信任证书及证书别名** | 从 URL 地址导入受信任证书及证书别名。 |

若要从文件导入受信任证书，请发起以下 GET 请求：

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Import
                trusted certificate from a file
```

2 在定义的 URL 发起 GET 请求以检索工作流定义。

若要检索“从文件导入受信任证书”工作流的定义，请发起以下 GET 请求：

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5
```

3 在工作流执行对象所在的 URL 发起 POST 请求。

对于“从文件导入受信任证书”工作流，请发起以下 POST 请求：

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5/
executions
```

4 在请求正文中，提供工作流的输入参数值用于执行上下文元素。

| 参数 | 描述 |
| --- | --- |
| **cer** | 要从其中导入 SSL 证书的 CER 文件。<br>此参数适用于“从文件导入受信任证书”工作流。 |
| **url** | 要从其中导入 SSL 证书的 URL。对于非 HTPS 服务，支持的格式为 *IP_address_or_DNS_name:port*。<br>此参数适用于“从 URL 导入受信任证书”工作流。 |

## 使用 REST API 创建密钥库

您可以运行配置插件的“创建密钥库”工作流或使用 REST API 创建密钥库。

**步骤**

1 在“创建密钥库”工作流的工作流服务的 URL 发起 GET 请求。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Create a keystore
```

2 在定义的 URL 发起 GET 请求以检索“创建密钥库”工作流的定义。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
```

3 在持有“创建密钥库”工作流执行对象的 URL 发起 POST 请求。

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
executions/
```

4 在请求正文中，将想要创建的密钥库的名称作为“创建密钥库”工作流的输入参数应用于执行上下文的元素。

## 使用 REST API 删除密钥库

您可以运行配置插件的“删除密钥库”工作流或使用 REST API 删除密钥库。

**步骤**

1 在“删除密钥库”工作流的工作流服务的 URL 发起 GET 请求。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Delete a keystore
```

2 在定义的 URL 发起 GET 请求以检索“删除密钥库”工作流的定义。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/7a3389eb-1fab-4d77-860b-81b66bb45b86/
```

3 在“删除密钥库”工作流执行对象所在的 URL 发起 POST 请求。

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/7a3389eb-1fab-4d77-860b-81b66bb45b86/
executions/
```

4 在请求正文中，将想要删除的密钥库作为“删除密钥库”工作流的输入参数应用于执行上下文的元素。

## 使用 REST API 添加密钥

您可以运行配置插件的“添加密钥”工作流或使用 REST API 添加密钥。

**步骤**

1 在“添加密钥”工作流的工作流服务的 URL 发起 GET 请求。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows?conditions=name=Add key
```

2 在定义的 URL 发起 GET 请求以检索“添加密钥”工作流的定义。

```
GET https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
```

3 在持有“添加密钥”工作流的执行对象的 URL 发起 POST 请求。

```
POST https://{orchestrator_host}:{port}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
executions/
```

4 在请求正文中，将密钥库、密钥别名、PEM 加密的密钥、证书链和密钥密码作为“添加密钥”工作流的输入参数应用于执行上下文的元素。

# 使用控制中心 REST API 自动处理 Orchestrator 配置

控制中心 REST API 提供了资源的访问权限，可用于配置 Orchestrator 服务器。您可以使用控制中心 REST API 与第三方系统自动处理 Orchestrator 配置。

控制中心 REST API 的 root 端点为 https://*orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter/api。有关控制中心 REST API 的所有可用服务调用的信息，请参见《控制中心 REST API 参考》文档，位于 https://*orchestrator_server_IP_or_DNS_name*:8283/vco-controlcenter/docs。

## 命令行实用程序

您可以使用 Orchestrator 命令行实用程序自动处理 Orchestrator 配置。

以 root 身份通过 SSH 登录 Orchestrator Appliance 以访问命令行实用程序。该实用程序位于 `/var/lib/vco/tools/configuration-cli/bin`。若要查看可用配置选项，请运行 `./vro-configure.sh --help`。

# 其他配置选项

7

您可以使用控制中心来更改默认的 Orchestrator 行为。

本章讨论了以下主题：

- 重新配置身份验证
- 导出 Orchestrator 配置
- 导入 Orchestrator 配置
- 配置工作流运行属性
- Orchestrator 日志文件

## 重新配置身份验证

在控制中心的初始配置期间设置身份验证方法后，您可以在任何时候更改身份验证提供程序或已配置的参数。

### 更改身份验证提供程序

要更改身份验证模式或身份验证提供程序连接设置，您必须先注销现有的身份验证提供程序。

#### 前提条件

#### 步骤

1 在**配置身份验证提供程序**页面中，单击主机地址文本框旁边的**注销**按钮以注销正在使用的身份验证提供程序。

2 在**身份服务**部分中，单击**注销**以删除服务器凭据。

#### 结果

您即成功注销身份验证提供程序。

#### 后续步骤

重新配置控制中心的身份验证。有关详细信息，请参见使用 vRealize Automation 身份验证配置独立的 Orchestrator 服务器。或使用 vSphere 身份验证配置独立的 Orchestrator 服务器。

## 更改身份验证参数

将 vRealize Automation 作为控制中心的身份验证提供程序时，您可能要更改 Orchestrator 管理员组的默认租户。使用 vSphere 身份验证时，您可以更改管理员组。

**前提条件**

- 以**管理员**身份登录到控制中心。
- 选择身份验证模式并配置身份验证提供程序的连接设置。

**步骤**

1 更改默认租户。

注 仅当您使用 vRealize Automation 身份验证模式时才可更改默认租户。

a 在控制中心的**配置身份验证提供程序**页面中，单击**默认租户**文本框旁边的**更改**按钮。

b 在文本框中，将现有默认租户名称替换成您想要使用的租户名称。

c 单击**管理员组**文本框旁边的**更改**按钮。

注 如果您未重新配置管理员组，它仍将保留为空且您将无法再访问控制中心。

d 输入管理员组的名称，然后单击**搜索**。

e 在组列表中，双击组的名称以将其选中。

f 单击**保存更改**。

您已从控制中心注销并重定向到 Single Sign-On 登录屏幕。

2 更改管理员组。

a 单击**管理员组**文本框旁边的**更改**按钮。

b 输入管理员组的名称，然后单击**搜索**。

c 在组列表中，双击组的名称以将其选中。

d 单击**保存更改**。

您已从控制中心注销并重定向到 Single Sign-On 登录屏幕。

# 导出 Orchestrator 配置

控制中心可以提供相关机制，将 Orchestrator 配置设置导出到本地文件。您可以使用该机制随时为系统配置创建快照并将此配置导入新的 Orchestrator 实例中。

应定期导出并保存您的配置设置，尤其是在进行修改、执行维护任务或系统升级的情况下。

**重要事项** 确保导出的配置文件安全无忧，因为文件中包含敏感的管理信息。

**步骤**

1 单击**导出/导入配置**。

2 选择要导出的文件类型。

> **注** 如果选择**导出插件配置**且插件配置中包含加密属性，您必须同时选择**导出服务器配置**以便在导入时成功对数据进行解密。

3 （可选） 输入密码以保护配置文件。

在随后导入配置时使用相同的密码。

4 单击**导出**。

**结果**

Orchestrator 会创建一个 `orchestrator-config-export-`*`hostname-dateReference`*`.zip` 文件，该文件随后会下载到您的本地计算机上。您可以使用该文件克隆或还原系统。

**注** 如果选择克隆 Orchestrator 实例，则切勿将数据库设置导入到克隆的 Orchestrator 中，而是必须配置一个与其他外部数据库之间的连接。

# 导入 Orchestrator 配置

在重新安装 Orchestrator 或系统发生故障后，可以还原之前导出的系统配置。

如果采用导入步骤克隆 Orchestrator 配置，则会使 vCenter Server 插件配置失效且无法运行，因为系统会生成一个新的 vCenter Server 插件 ID。

**前提条件**

从控制中心的**启动选项**页面停止 Orchestrator 服务器。

**步骤**

1 单击**导出/导入配置**，并导航到**导入配置**选项卡。

2 浏览并选择您从上次安装中导出的 `.zip` 文件。

3 输入导出配置时使用的密码。

如果导出配置时未使用密码，则不必执行此步骤。

4 单击**导入**。

5 选择要导入的文件类型。

> **重要事项** 导出的文件可能包含先前版本的插件，除非要使用这些插件替代所有新版插件，否则请勿使用“强制导入”插件。版本不兼容可能导致插件停止运行。

6 单击**完成导入**。

此时系统会显示一条消息，表示配置已成功导入。

**结果**

新系统会完全复制旧配置。Orchestrator 服务器服务自动重新启动。

**后续步骤**

# 配置工作流运行属性

默认情况下，每个节点最多可以运行 300 个工作流，在达到活动运行工作流的数量限制时可为 1 万个工作流排队。

如果 Orchestrator 节点需要运行的并发工作流数超过 300，挂起的工作流运行会排队等待。在活动工作流运行完成后，队列中的下一工作流开始运行。如果达到排队工作流的最大数量，则后续工作流运行会失败，直到某个挂起工作流开始运行为止。

在控制中心的**高级选项**页面上，您可以配置工作流运行属性。

| 选项 | 描述 |
| --- | --- |
| **启用安全模式** | 如果启用安全模式，则所有正在运行的工作流将被取消，直到 Orchestrator 节点下次启动时恢复。 |
| **并行运行的工作流数** | 同时运行的 Orchestrator 节点并行工作流数上限。 |
| **队列中正在运行的工作流数上限** | Orchestrator 节点可接受的工作流运行请求数上限（超出此数即会发生节点故障）。 |
| **每个工作流保存的运行数上限** | 群集中每个工作流已完成且可保存为历史记录的工作流运行数上限。一旦超出此数，则最早的工作流运行将被删除。 |
| **日志事件保留天数** | 数据库中群集日志事件的保留天数（超出此天数即会被清除）。 |

# Orchestrator 日志文件

在您提交支持请求时，VMware 技术支持会例行要求您提供诊断信息。这一诊断信息包含了运行产品的主机上的产品特定日志和配置文件。

您可以从控制中心的**导出日志**菜单下载其中包含 Orchestrator 配置文件和日志文件的 ZIP 包。

**表 7-1. Orchestrator 日志文件列表**

| 文件名 | 位置 | 描述 |
| --- | --- | --- |
| `scripting.log` | `/var/log/vco/app-server` | 提供工作流和操作的脚本日志消息。使用 `scripting.log` 文件将工作流运行和操作运行与普通 Orchestrator 操作隔离。此信息也会包含在 `server.log` 文件中。 |
| `server.log` | `/var/log/vco/app-server` | 提供有关 Orchestrator 服务器上所有活动的信息。在您调试 Orchestrator 或 Orchestrator 上运行的任意应用程序时，请分析 `server.log` 文件。 |
| `metrics.log` | `/var/log/vco/app-server` | 包含有关服务器的运行时信息。该信息会以每 5 分钟一次的频率添加到此日志文件。 |
| `localhost_access_log.txt` | `/var/log/vco/app-server` | 服务器的 HTTP 请求日志。 |

表 7-1. Orchestrator 日志文件列表 （续）

| 文件名 | 位置 | 描述 |
| --- | --- | --- |
| localhost_access_log.*date*.txt | /var/log/vco/configuration | 这是控制中心服务的 HTTP 请求日志。 |
| controlcenter.log | /var/log/vco/configuration | 控制中心服务的日志文件。 |

# 日志记录持久性

您能以任何形式的 Orchestrator 脚本（例如工作流、策略或操作）记录信息。此类信息都会具有类型和级别之分。类型可以是持久性和非持久性。级别可以是调试、信息、警告、错误、跟踪和严重。

表 7-2. 创建持久性和非持久性日志

| 日志级别 | 持久性类型 | 非持久性类型 |
| --- | --- | --- |
| 调试 | Server.debug("short text", "long text"); | System.debug("text") |
| 信息 | Server.log("short text", "long text"); | System.log("text"); |
| 警告 | Server.warn("short text", "long text"); | System.warn("text"); |
| 错误 | Server.error("short text", "long text"); | System.error("text"); |

## 持久性日志

持久性日志（服务器日志）会跟踪过往的工作流运行日志并存储在 Orchestrator 数据库中。若要查看服务器日志，您必须选择一个工作流、一个已完成的工作流运行或一项策略，然后在 Orchestrator 客户端中单击**事件**选项卡。

## 非持久性日志

使用非持久性日志（系统日志）创建脚本时，Orchestrator 服务器会就此日志通知所有正在运行的 Orchestrator 应用程序，但此信息不会存储在数据库中。在应用程序重启后，日志信息就会丢失。非持久性日志用于调试用途和实时信息。若要查看系统日志，您必须选择 Orchestrator 客户端中一个已完成的工作流运行，然后在**架构**选项卡上单击**日志**。

# Orchestrator 日志配置

在控制中心的**配置日志**页面上，可以设置服务器日志以及所需脚本日志的日志级别。如果某个日志一天内生成多次，则会很难确定问题原因。

服务器日志以及脚本日志的默认日志级别为信息。更改日志级别会影响服务器输入到日志的所有新消息，以及数据库的活动连接数量。日志记录详细级别按降序递减。

小心　仅在调试问题时将日志级别设置为调试或所有。请勿在生产环境中使用这些设置，因为会严重影响性能。

## 日志轮换设置

若要防止服务器日志文件过大，您可以修改**文件数上限**和**文件大小上限 (MB)** 文本框中的值，设置服务器日志的文件大小和文件数上限。

### Orchestrator 日志文件导出

从控制中心**导出日志**页面，您可以生成故障排除信息的 ZIP 存档，其中包含配置、服务器、包装程序和安装日志文件。

日志信息会存储在名为 `vco-logs-`*`date_hour`*`.zip` 的 ZIP 存档中。

**注** 当群集中有多个 Orchestrator 实例时，ZIP 存档中会包含群集中所有 Orchestrator 实例中的日志。

## 检查工作流

您可以访问控制中心的“检查工作流”页面，快速检查并导出已完成工作流的系统日志和服务器日志。

**重要事项** 日志信息会临时存储。

- 系统日志存储在文件中，最大为 10 MB。日志文件的最大数量为每个节点 5 个。
- 服务器日志在数据库中存储 15 天。

**步骤**

1. 单击**检查工作流**。
2. 单击**完成的工作流**选项卡。
3. （可选） 选择要检查的工作流令牌类型，然后选择日期范围并单击**应用**。
4. （可选） 按名称、ID 或令牌 ID 搜索工作流。
5. 单击要检查的令牌 ID。

   工作流执行日志视图会以全屏方式显示。
6. 检查系统日志和服务器日志。

   **注** 当群集中有多个 Orchestrator 实例时，工作流令牌日志中将仅在启动工作流的 Orchestrator 节点上的控制中心可见。
7. （可选） 单击**导出令牌日志**即可以 `.zip` 文件形式导出工作流令牌日志。

## 筛选 Orchestrator 日志

您可以针对特定工作流运行筛选 Orchestrator 服务器日志，并收集有关工作流运行的诊断数据。

Orchestrator 日志包含许多有用的信息，您可以实时对其监控。如果同时运行同一工作流的多个实例，您可以筛选 Orchestrator 实时日志流中关于每个运行的诊断数据，从而跟踪不同工作流运行。

**注** 当群集中有多个 Orchestrator 实例时，实时日志流将仅显示本地 Orchestrator 节点的日志。

**步骤**

1. 单击**实时日志流**。

2 在搜索栏中，输入搜索参数。

例如，可以按用户名、工作流名称、工作流 ID 或令牌 ID 筛选日志。

3 （可选） 选择**区分大小写**和**筛选器 (grep)** 来进一步筛选结果。

如果选择**筛选器 (grep)**，则实时流仅会显示与搜索参数匹配的行。

**结果**

Orchestrator 实时日志流会根据您的搜索参数进行筛选。

**后续步骤**

某些旧日志无法通过控制中心的**实时日志流**页面进行访问，您可以使用第三方日志分析工具对其进行筛选。

# 配置用例及故障排除

8

您可以将 Orchestrator 服务器配置为与 vCenter Server 设备结合使用，还可以卸载 Orchestrator 中的插件或更改自签名证书。

配置用例旨在提供各种任务流，您可以执行这些任务流来满足 Orchestrator 服务器的具体配置要求，以及查看故障排除主题以了解并解决问题（如有解决办法）。

本章讨论了以下主题：



## 将 Orchestrator 注册为 vCenter Server 扩展

在使用 vCenter Single Sign-On 注册 Orchestrator 服务器并将其配置为与 vCenter Server 结合使用后，您必须将 Orchestrator 注册为 vCenter Server 的扩展。

**步骤**

1 以管理员身份登录到 Orchestrator 客户端。

2 单击**工作流**视图。

3 在工作流层次结构列表中，展开**库 > vCenter > 配置**。

4 右键单击**将 vCenter Orchestrator 注册为 vCenter Server 扩展**工作流并选择**启动工作流**。

5 选择 Orchestrator 要向其注册的 vCenter Server 实例。

6 输入 https://*your_orchestrator_server_IP_or_DNS_name*:8281 或负载平衡器的服务 URL（用于将请求重定向到 Orchestrator 服务器节点）。

7 单击**提交**。

# 取消注册 Orchestrator 身份验证

在控制中心的配置身份验证提供程序页面中将 Orchestrator 取消注册为 Single Sign-On 解决方案。

如果想要重新配置 Orchestrator vCenter Single Sign-On 或 vRealize Automation 身份验证，则必须首先取消注册 Orchestrator 身份验证。

**步骤**

1 单击**配置身份验证提供程序**。

2 单击**取消注册**。

3 （可选） 如果要从身份服务器删除注册数据，请输入您的凭据。

4 单击**身份服务**部分中的**取消注册**。

**结果**

您即成功取消注册 Orchestrator 服务器实例。

# 更改 SSL 证书

默认情况下，Orchestrator 服务器使用自签名的 SSL 证书与 Orchestrator 客户端进行远程通信。您可以更改 SSL 证书，例如因为公司安全策略要求使用本公司的 SSL 证书。

在尝试通过受信任的 SSL Internet 连接使用 Orchestrator 并且在 Web 浏览器中打开控制中心时，如果使用的浏览器是 Mozilla Firefox，您会收到连接不受信任的警告；如果使用的浏览器是 Internet Explorer，则会显示检测到了 Web 站点的安全证书问题。

单击**继续浏览此网站(不推荐)**，即使您之前已在受信任的存储中导入 SSL 证书，仍会在 Web 浏览器的地址栏中看到证书错误红色通知。您可以在 Web 浏览器中使用 Orchestrator，在尝试通过 HTTPS 访问 API 时，第三方系统可能无法正常运行。

在启动 Orchestrator 客户端并尝试通过 SSL 连接到 Orchestrator 服务器时，也有可能会收到证书警告。

您可以安装由商业证书颁发机构 (CA) 签名的证书来解决此问题。若要不再收到 Orchestrator 客户端发出的证书警告，请将 root CA 证书添加到安装了 Orchestrator 客户端的计算机上的 Orchestrator 密钥库。

## 将证书添加到本地存储

在从 CA 接收证书后，您必须将证书添加到本地存储，以便在使用控制中心时不会收到证书警告或错误消息。

此工作流描述了使用 Internet Explorer 将证书添加到本地存储的过程。

1 打开 Internet Explorer 并访问 https://*orchestrator_server_IP_or_DNS_name*:8283/。

2 出现提示时，单击**继续浏览此网站（不推荐）**。

此时会在 Internet Explorer 地址栏的右侧显示证书错误。

3 单击证书错误并选择**查看证书**。

4 单击**安装证书**。

5 在**证书导入向导**的欢迎页面上，单击**下一步**。

6 在**证书存储**窗口中，选择**将所有的证书放入下列存储**。

7 浏览并选择**受信任的根证书颁发机构**。

8 完成向导并重新启动 Internet Explorer。

9 通过 SSL 连接导航到 Orchestrator 服务器。

您不会再收到警告，也不会在地址栏中收到证书错误。

其他应用程序和系统（例如 VMware Service Manager）必须具有通过 SSL 连接访问 Orchestrator REST API 的权限。

## 更改 Orchestrator Appliance 管理站点的证书

Orchestrator Appliance 使用 Light HTTPd 运行自己的管理站点。例如，如果公司安全策略要求您使用其 SSL 证书，则可更改 Orchestrator Appliance 管理站点的 SSL 证书。

**前提条件**

默认情况下，Orchestrator Appliance SSL 证书和私有密钥存储在位于 `/opt/vmware/etc/lighttpd/server.pem` 的 PEM 文件中。若要安装新证书，请确保将新的 SSL 证书和私有密钥从 Java 密钥库中导出到 PEM 文件。

**步骤**

1 找到 `/opt/vmware/etc/lighttpd/lighttpd.conf` 文件并在编辑器中将其打开。

2 找到以下行：

```
#### SSL engine
ssl.engine = "enable"
ssl.pemfile = "/opt/vmware/etc/lighttpd/server.pem"
```

3 更改 `ssl.pemfile` 属性以指向包含新 SSL 证书和私有密钥的 PEM 文件。

4 保存 `lighttpd.conf` 文件。

5 运行以下命令来重新启动 light-httpd 服务器。

```
service vami-lighttp restart
```

**结果**

您即成功更改了 Orchestrator Appliance 管理站点的证书。

# 取消正在运行的工作流

如果 Orchestrator 服务器已停止，请取消工作流，否则相关操作可能会失败。

**前提条件**

从控制中心的**启动选项**页面停止 Orchestrator 服务器。

**步骤**

1 单击**故障排除**。

2 取消正在运行的工作流。

| 选项 | 描述 |
| --- | --- |
| **取消所有工作流运行** | 输入工作流 ID，取消该工作流的所有令牌。如果服务器未停止，则可能不会取消工作流令牌。 |
| **按 ID 取消工作流运行** | 输入想要取消的所有令牌 ID，使用逗号进行分隔。如果服务器未停止，则可能不会取消工作流令牌。 |
| **取消所有令牌** | 取消服务器上正在运行的所有工作流。您必须停止服务器才能使用该选项。 |

**结果**

在下一次服务器启动时，工作流会设置为已取消状态。

**后续步骤**

从控制中心的**检查工作流**页面中验证工作流是否已被取消。

# 启用 Orchestrator 服务器调试

您可以调试模式启动 Orchestrator 服务器来调试在开发插件时遇到的问题。

**步骤**

1 单击 **Orchestrator 调试**。

2 单击**启用调试**。

3 （可选） 输入端口（须与默认端口不同）。

4 （可选） 单击**挂起**。

选择该选项，您必须先附加调试器，然后再启动 Orchestrator 服务器。

5 单击**保存**。

6 打开控制中心的启动选项页面，然后单击**重新启动**。

**结果**

Orchestrator 在启动时就会挂起，直到您将远程 Java 调试器附加到定义的端口为止。

# 备份 Orchestrator 配置和元素

您可以为 Orchestrator 配置创建快照并将此配置导入新的 Orchestrator 实例以备份 Orchestrator 配置。您也可以备份已修改的 Orchestrator 元素。

如果在编辑完标准的工作流、操作、策略或配置元素后再导入包含相同元素但 Orchestrator 版本号更高的软件包，那么之前对元素所做的更改会丢失。若要使已修改和自定义的元素在升级后继续可用，必须先将其导出到软件包，然后再开始相关步骤。

每个 Orchestrator 服务器实例都有唯一的证书，并且每个 vCenter Server 插件实例都有唯一的 ID。证书和唯一的 ID 定义了 Orchestrator 服务器和 vCenter Server 插件的身份。如果未备份 Orchestrator 元素或未导出 Orchestrator 配置进行备份，请确保更改这些身份标识要素。

### 前提条件

部署和配置新的 Orchestrator 服务器实例。请参见配置独立的 Orchestrator 服务器。

### 步骤

1. 单击**导出/导入配置**。
2. 选择要导出的文件类型。
3. （可选） 输入密码以保护配置文件。

   使用您导入该配置时的相同密码。
4. 登录 Orchestrator 客户端应用程序。
5. 创建一个软件包，其中包含您已创建或编辑的所有 Orchestrator 元素。
   a. 单击**软件包**视图。
   b. 单击软件包列表标题栏中的菜单按钮，选择**添加软件包**。
   c. 输入新软件包的名称并单击**确定**。

      软件包名称的语法为 *domain.your_company.folder.package_name*。

      例如：`com.vmware.myfolder.mypackage`。
   d. 右键单击该软件包并选择**编辑**。
   e. 在**常规**选项卡上，添加软件包的说明。
   f. 在**工作流**选项卡上，将工作流添加到软件包。
   g. （可选） 将策略模板、操作、配置元素、资源元素和插件添加到软件包。
6. 导出软件包。
   a. 右键单击要导出的软件包，然后选择**导出软件包**。
   b. 浏览并选择要保存软件包的位置，然后单击**打开**。
   c. （可选） 使用相应的证书为软件包签名。
   d. （可选） 为导出的软件包添加相关限制。

e （可选） 若要对导出软件包的内容应用某种限制，请根据需要取消选中相关选项。

| 选项 | 描述 |
| --- | --- |
| **导出版本历史记录** | 不会导出该软件包的版本历史记录。 |
| **导出配置设置的值** | 不会导出该软件包中配置元素的属性值。 |
| **导出全局标记** | 不会导出该软件包中的全局标记。 |

f 单击**保存**。

**7** 将已导出的软件包导入到新 Orchestrator 实例。

a 登录新 Orchestrator 实例的 Orchestrator 客户端应用程序。

b 从 Orchestrator 客户端的下拉菜单中，选择**管理**。

c 单击**软件包**视图。

d 在左侧窗格中单击右键，然后选择**导入软件包**。

e 浏览到要导入的软件包并将其选中，然后单击**打开**。

此时系统会显示有关导出实例的证书信息。

f 查看软件包导入详细信息并选择**导入**或**导入并信任提供者**。

此时会显示导入软件包视图。如果导入的软件包元素的版本高于服务器上的版本，则系统会选择相应元素进行导入。

g 取消选中不想导入的元素。

例如，取消选择已存在较高版本的自定义元素。

h （可选） 如果不想导入软件包中配置元素的属性值，请取消选中**导入配置设置的值**。

i 从下拉菜单中，选择是否要导入软件包中的标记。

| 选项 | 描述 |
| --- | --- |
| **导入标记但保留现有值** | 导入软件包中的标记但不覆盖现有标记值。 |
| **导入标记并覆盖现有值** | 导入软件包中的标记并且覆盖现有值。 |
| **不导入标记** | 不导入软件包中的标记。 |

j 单击**导入选择的元素**。

# 备份和还原 vRealize Orchestrator

您可以使用 vSphere Data Protection 对包含 vRealize Orchestrator 实例的虚拟机 (VM) 进行备份和还原。

vSphere Data Protection 是一款基于磁盘的 VMware 备份和还原解决方案，专为 vSphere 环境设计。vSphere Data Protection 与 vCenter Server 完全集成。使用 vSphere Data Protection 可以中管理各备份作业并将备份文件存储在具有重复数据删除功能的目标存储位置。在部署并配置 vSphere Data Protection 后，您可以使用 vSphere Web Client 接口访问 vSphere Data Protection 并选择、调度、配置和管理虚拟机的备份和还原。备份期间，vSphere Data Protection 会为虚拟机创建静默快照。每次备份都会自动执行重复数据删除功能。

有关如何部署和配置 vSphere Data Protection 的信息，请参见《vSphere Data Protection 管理》文档。

## 备份 vRealize Orchestrator

您可以将 vRealize Orchestrator 实例备份为虚拟机。

您可以先导出数据库，然后再进行完整的虚拟机备份。有关如何导出数据库的信息，请参见导出 Orchestrator 数据库。如果 vRealize Orchestrator 和外部数据库位于不同虚拟机上，必须单独备份数据库。

**注** 为确保单个产品中虚拟机的所有组件都能一起备份，请在单一 vCenter Server 文件夹中存储 vRealize Orchestrator 环境的虚拟机，并为该文件夹创建备份策略作业。

### 前提条件

- 确认 vSphere Data Protection 设备已部署并配置。有关如何部署和配置 vSphere Data Protection 的信息，请参见《vSphere Data Protection 管理》文档。
- 使用 vSphere Web Client 登录到在环境中承担管理职能的 vCenter Server 实例。以在 vSphere Data Protection 配置期间使用的具有管理员权限的用户身份登录。

### 步骤

1. 在 vSphere Web Client 主页中，单击 **vSphere Data Protection**。
2. 从 **VDP 设备**下拉菜单中选择 vSphere Data Protection 设备，然后单击**连接**。
3. 在**开始使用**选项卡上，单击**创建备份作业**。
4. 单击**客户机映像**以备份 vRealize Orchestrator 实例，然后单击**下一步**。
5. 选择**完整映像**以备份整台虚拟机，然后单击**下一步**。
6. 展开**虚拟机**树并选中 vRealize Orchestrator 虚拟机的复选框。
7. 按照提示设置备份计划、保留策略以及备份作业的名称。

   有关如何备份和还原虚拟机的更多信息，请参见《vSphere Data Protection 管理》文档。

   您的备份作业会显示在**备份**选项卡上的备份作业列表中。

8 （可选） 打开**备份**选项卡，选择您的备份作业并单击**立即备份**以备份 vRealize Orchestrator。

> **注** 或者，也可以等待备份根据您设置的计划自动启动。

备份操作会显示在**近期任务**页面上。

**结果**

虚拟机的映像会显示在**还原**选项卡中的备份列表中。

**后续步骤**

在**还原**选项卡上，确认虚拟机的映像位于备份列表中。

## 还原 vRealize Orchestrator 实例

您可以将自己的 vRealize Orchestrator 实例还原到原始位置或同一 vCenter Server 上的不同位置。

如果 vRealize Orchestrator 和外部数据库在不同虚拟机上运行，必须首先还原数据库，然后再还原 vRealize Orchestrator 虚拟机。

**前提条件**

- 确认 vSphere Data Protection 设备已部署并配置。有关如何部署和配置 vSphere Data Protection 的信息，请参见《vSphere Data Protection 管理》文档。
- 备份 vRealize Orchestrator 实例。请参见备份 vRealize Orchestrator。
- 使用 vSphere Web Client 登录到在环境中承担管理职能的 vCenter Server 实例。以在 vSphere Data Protection 配置期间使用的具有管理员权限的用户身份登录。

**步骤**

1 在 vSphere Web Client 主页中，单击 **vSphere Data Protection**。

2 从 **VDP 设备**下拉菜单中选择 vSphere Data Protection 设备，然后单击**连接**。

3 打开**还原**选项卡。

4 在备份作业列表中，选择要还原的 vRealize Orchestrator 备份。

> **注** 如果有多台虚拟机，必须同时将其还原以保持同步状态。

5 若要将 vRealize Orchestrator 实例还原到同一 vCenter Server 上，请单击**还原**图标并按照提示来设置在 vCenter Server 上用来还原 vRealize Orchestrator 的位置。

请勿选择**打开电源**，因为该设备必须是最后一个开机的组件。有关如何备份和还原虚拟机的信息，请参见《vSphere Data Protection 管理》文档。

此时会显示一条消息，表明还原流程已成功启动。

6 （可选） 打开数据库主机电源（如为外部）并还原负载平衡器配置。

7 打开 vRealize Orchestrator Appliance 电源。

**结果**

已还原的 vRealize Orchestrator 虚拟机会显示在 vCenter Server 清单中。

**后续步骤**

在控制中心内打开 vRealize Orchestrator 验证配置**页面，确认**已正确配置。

# 使用 Site Recovery Manager 对 Orchestrator 进行灾难恢复

您必须配置 Site Recovery Manager 为 vRealize Orchestrator 提供保护。完成 Site Recovery Manager 的常规配置任务以完善该保护。

## 准备环境

在开始配置 Site Recovery Manager 前，必须确保满足以下必备条件。

- 验证 vSphere 5.5 已安装在受保护的恢复站点上。
- 验证您使用的是 Site Recovery Manager 5.8。
- 验证已配置 vRealize Orchestrator。

## 为 vSphere Replication 配置虚拟机

您必须为 vSphere Replication 配置虚拟机或基于阵列的复制以便使用 Site Recovery Manager。

若要在所需虚拟机上启用 vSphere Replication，请执行以下步骤。

**步骤**

1. 在 vSphere Web Client 中，选择要在其中启动 vSphere Replication 的虚拟机并单击**操作 > 所有 vSphere Replication 操作 > 配置复制**。
2. 在**复制类型**窗口中，选择**复制到 vCenter Server**，然后单击**下一步**。
3. 在**目标站点**窗口中，为恢复站点选择 vCenter 并单击**下一步**。
4. 在**复制服务器**窗口中，选择 vSphere Replication 服务器并单击**下一步**。
5. 在**目标位置**窗口中，单击**编辑**并选择目标数据存储（用于存储复制的文件），然后单击**下一步**。
6. 在**复制选项**窗口中，保留默认设置并单击**下一步**。
7. 在**恢复设置**窗口中，为**恢复点对象 (RPO)** 和**时间实例中的点**输入时间，然后单击**下一步**。
8. 在**即将完成**窗口中，验证设置并单击**完成**。
9. 在所有要启用 vSphere Replication 的虚拟机上重复这些步骤。

## 创建保护组

创建保护组可以使 Site Recovery Manager 保护虚拟机。

创建保护组时，请等待以确保操作按预期完成。请确保 Site Recovery Manager 创建了保护组并且成功保护了组中的虚拟机。

**前提条件**

确认已执行以下任一任务：

- 已将虚拟机放入配置了基于阵列的复制的数据存储中
- 已在虚拟机上配置了 vSphere Replication
- 已执行了上述部分或全部操作

**步骤**

1 在 vSphere Web Client 中，选择**站点恢复** > **保护组**。

2 在**对象**选项卡上，单击图标以创建保护组。

3 在保护组类型页面上，选择受保护站点、选择复制类型并单击**下一步**。

| 选项 | 操作 |
| --- | --- |
| **基于阵列的复制组** | 选择**基于阵列的复制 (ABR)** 并选择阵列对。 |
| **vSphere Replication 保护组** | 选择 **vSphere Replication**。 |

4 选择要添加到保护组的数据存储组或虚拟机。

| 选项 | 操作 |
| --- | --- |
| **基于阵列的复制保护组** | 选择数据存储组并单击**下一步**。 |
| **vSphere Replication 保护组** | 选择列表中的虚拟机，然后单击**下一步**。 |

创建 vSphere Replication 保护组时，列表中只会显示针对 vSphere Replication 配置并且不属于保护组的虚拟机。

5 查看设置，然后单击**完成**。

您可以在**对象**选项卡的**保护组**下，监控保护组的创建进度。

**结果**

- 如果 Site Recovery Manager 将清单映射成功应用到受保护的虚拟机，则保护组的保护状态为良好。
- 如果 Site Recovery Manager 成功保护与存储策略相关的所有虚拟机，则保护组的保护状态为良好。

## 创建恢复计划

创建恢复计划，以建立 Site Recovery Manager 恢复虚拟机的方式。

**步骤**

1 在 vSphere Web Client 中，选择**站点恢复** > **恢复计划**。

2 在**对象**选项卡上，单击图标以创建恢复计划。

3 输入计划的名称和说明，然后选择文件夹并单击**下一步**。

4 选择恢复站点并单击**下一步**。

5 从菜单中选择组类型。

| 选项 | 描述 |
| --- | --- |
| **虚拟机保护组** | 选择此选项以创建包含基于阵列的复制和 vSphere Replication 保护组的恢复计划。 |
| **存储策略保护组** | 选择此选项以创建包含存储策略保护组的恢复计划。 |

默认值为**虚拟机保护组**。

注 如果使用延伸存储，请为组类型选择**存储策略保护组**。

6 为要恢复的计划选择一个或多个保护组，然后单击**下一步**。

7 单击**测试网络**值，选择测试恢复期间要使用的网络，然后单击**下一步**。

默认选项为自动创建隔离网络。

8 查看摘要信息，然后单击**完成**创建恢复计划。

## 将恢复计划整理到文件夹中

您可以创建文件夹以整理恢复计划。

如果有许多恢复计划，将其整理到文件夹中会很有用。您可以将恢复计划放置在文件夹中并为不同用户或组指定不同的文件夹许可，从而限制恢复计划的访问权限。

**步骤**

1 在 vSphere Web Client 的主页视图中，单击**站点恢复**。

2 展开**清单树**并单击**恢复计划**。

3 选择**相关对象**选项卡并单击**文件夹**。

4 单击**创建文件夹**图标，输入要创建的文件夹的名称，然后单击**确定**。

5 将新的或现有恢复计划添加到文件夹。

| 选项 | 描述 |
| --- | --- |
| **创建新的恢复计划** | 右键单击文件夹并选择**创建恢复计划**。 |
| **添加现有恢复计划** | 将清单树中的恢复计划拖放到文件夹内。 |

6 （可选） 若要重命名或删除文件夹，请右键单击文件夹并选择**重命名文件夹**或**删除文件夹**。

您仅可以删除空的文件夹。

## 编辑恢复计划

可以编辑恢复计划以更改此恢复计划创建时指定的属性。可从受保护站点或恢复站点编辑恢复计划。

**步骤**

1 在 vSphere Web Client 中，选择**站点恢复** > **恢复计划**。

2 右键单击某个恢复计划，然后选择**编辑计划**。

您还可以在**监控**选项卡的**恢复步骤**视图内单击**编辑恢复计划**图标，从而编辑恢复计划。

3 （可选） 在**恢复计划**的文本框中更改计划的名称或说明，然后单击**下一步**。

4 在“恢复站点”页面上，单击**下一步**。

您不能更改恢复站点。

5 （可选） 选择或取消选择一个或多个保护组，从而将其添加到计划或从计划中移除，然后单击**下一步**。

6 （可选） 单击测试网络以选择恢复站点上的其他测试网络，然后单击**下一步**。

7 查看摘要信息，然后单击**完成**将指定更改应用于恢复计划。

您可以在“近期任务”视图中监控计划的更新。

# 设置系统属性

9

您可以设置系统属性来更改默认的 Orchestrator 行为。

本章讨论了以下主题：



## 禁用非管理员的 Orchestrator 客户端访问权限

您可以配置 Orchestrator 服务器拒绝所有非 Orchestrator 管理员组成员的 Orchestrator 客户端访问权限。

默认情况下，所有已被授予执行权限的用户都可以连接到 Orchestrator 客户端。但是，您可以设置 Orchestrator 配置系统属性，将 Orchestrator 客户端的访问权限限制为 Orchestrator 管理员。

**重要事项** 如果未配置该属性或属性设置为 false，则 Orchestrator 会允许所有用户访问 Orchestrator 客户端。

**步骤**

1 单击**系统属性**。

2 单击**添加**图标 (+)。

3 在**键**文本框中，输入 **com.vmware.o11n.smart-client-disabled**。

4 在**值**文本框中，输入 **true**。

5 （可选） 在**描述**文本框中，输入**禁用 Orchestrator 客户端连接**。

6 单击**添加**。

7 单击弹出菜单中的**保存更改**。

此时显示一条消息，表示您已保存成功。

**结果**

您即禁用了所有非 Orchestrator 管理员组用户的 Orchestrator 客户端访问权限。

# 设置工作流和操作对服务器文件系统的访问权限

在 Orchestrator 中，工作流和操作对特定文件系统目录的访问受限。您可以修改 `js-io-rights.conf` Orchestrator 配置文件将访问权限延伸到服务器文件系统的其他部分。

## js-io-rights.conf 文件中允许 Orchestrator 系统写入权限的规则

`js-io-rights.conf` 文件包含的规则允许对服务器文件系统中已定义目录拥有写入权限。

### js-io-rights.conf 文件的必需内容

`js-io-rights.conf` 文件的每一行都必须包含以下信息。

- 加号 (`+`) 或减号 (`-`)，表示允许或拒绝权限
- 读取 (`r`)、写入 (`w`) 和执行 (`x`) 权限级别
- 应用这些权限时的路径

### js-io-rights.conf 文件的默认内容

Orchestrator Appliance 中 `js-io-rights.conf` 配置文件的默认内容如下：

```
-rwx /
+rwx /var/run/vco
-rwx /etc/vco/app-server/security/
+rx /etc/vco
+rx /var/log/vco/
```

默认 `js-io-rights.conf` 配置文件中的前两行允许以下访问权限：

**`-rwx /`**

拒绝对文件系统的所有访问权限。

**`+rwx /var/run/vco`**

`/var/run/vco` 目录中允许读取、写入和执行访问权限。

### js-io-rights.conf 文件中的规则

Orchestrator 会按各访问权限在 `js-io-rights.conf` 文件中的显示顺序对其进行解析。每一行都可以覆盖上一行。

**重要事项** 您可以在 `js-io-rights.conf` 文件中设置 `+rwx /` 来允许访问文件系统的所有部分。但是，这么做会面临较高的安全风险。

## 设置工作流和操作对服务器文件系统的访问权限

若要更改工作流和 Orchestrator API 对服务器文件系统内具体区域的访问权限，请修改 `js-io-rights.conf` 配置文件。`js-io-rights.conf` 文件会在工作流试图访问 Orchestrator 服务器文件系统时创建。

**步骤**

1. 以 **root** 用户身份登录 Orchestrator Appliance Linux 控制台。
2. 导航到 `/etc/vco/app-server`。
3. 在文本编辑器中打开 `js-io-rights.conf` 配置文件。
4. 将必要的命令行添加到 `js-io-rights.conf` 文件以允许或拒绝访问文件系统的相关区域。

   例如：以下命令行拒绝了 */path_to_folder*/noexec 目录中的执行权限：

   ```
   -x /path_to_folder/noexec
   ```

   */path_to_folder*/noexec 保留了执行权限，但 */path_to_folder/noexec/bar*/noexec/bar 未保留。两个目录都仍然可进行读写操作。

**结果**

您即修改了工作流和 Orchestrator API 对文件系统的访问权限。

## 设置工作流和操作对操作系统命令的访问权限

Orchestrator API 提供了脚本类 (Command)，可在 Orchestrator 服务器主机操作系统中运行命令。为防止对 Orchestrator 服务器主机未经授权的访问，默认情况下，Orchestrator 应用程序没有 Command 类的运行权限。如果 Orchestrator 应用程序需要在主机操作系统上运行命令，您可以激活 Command 脚本类。

您可以设置 Orchestrator 配置系统属性，授予 Command 类的使用权限。

**步骤**

1. 单击**系统属性**。
2. 单击**添加**图标 (+)。
3. 在**键**文本框中，输入 **com.vmware.js.allow-local-process**。
4. 在**值**文本框中，输入 **true**。

5 在**说明**文本框中，输入系统属性的说明。

6 单击**添加**。

7 单击弹出菜单中的**保存更改**。

此时显示一条消息，表示您已保存成功。

**结果**

您即向 Orchestrator 应用程序授权权限可在 Orchestrator 服务器主机操作系统上运行本地命令。

注 将 `com.vmware.js.allow-local-process` 系统属性设置为 `true`，您可以允许 `Command` 脚本类在文件系统任意位置中进行写入。此属性会覆盖您在 `js-io-rights.conf` 文件中针对 `Command` 脚本类设置的任何文件系统访问权限。在 `js-io-rights.conf` 文件中设置的文件系统访问权限仍会适用于 `Command` 以外的所有脚本类。

# 将 JavaScript 访问权限设置为 Java 类

默认情况下，Orchestrator 会将 JavaScript 的访问权限限制为一组 Java 类。如果想要 JavaScript 访问范围更广的 Java 类，您必须设置 Orchestrator 系统属性来允许相关访问权限。

允许 JavaScript 引擎全权访问 Java 虚拟机 (JVM) 会带来潜在的安全问题。有缺陷或恶意的脚本可能有权访问运行 Orchestrator 服务器的用户所能够访问的全部系统组件。因此，Orchestrator JavaScript 引擎在默认情况下仅能访问 `java.util.*` 软件包中的类。

如果需要 JavaScript 访问除 `java.util.*` 软件包以外的类，您可在配置文件中列出允许 JavaScript 访问的 Java 软件包。随后，将 `com.vmware.scripting.rhino-class-shutter-file` 系统属性设置为指向该文件。

**步骤**

1 创建一个文本配置文件以存储要允许 JavaScript 访问的 Java 软件包列表。

例如，若要允许 JavaScript 访问 `java.net` 软件包中的所有类和 `java.lang.Object` 类，您可在文件中添加以下内容。

```
java.net.*
java.lang.Object
```

2 使用适当的名称将配置文件保存到适当的位置。

3 单击**系统属性**。

4 单击**添加**图标 (+)。

5 在**键**文本框中，输入 **`com.vmware.scripting.rhino-class-shutter-file`**。

6 在**值**文本框中，输入配置文件的路径。

7 在**说明**文本框中，输入系统属性的说明。

8 单击**添加**。

9 在弹出菜单中单击**保存更改**。

此时系统会显示一条消息，提示您已保存成功。

**结果**

JavaScript 引擎即有权访问指定的 JavaScript 类。

# 设置自定义超时属性

vCenter Server 过载后，会花费更多时间（相比默认的 20000 毫秒）向 Orchestrator 服务器返回响应。为防止出现此类情况，您必须修改 Orchestrator 配置文件以增加默认超时时间段。

如果默认超时时间段在完成特定操作前过期，则 Orchestrator 服务器日志会包含错误。

```
Operation 'getPropertyContent' total time : '5742228' for 1823 calls, mean time : '3149.0', min time : '0', max time : '32313' Timeout, unable to get property 'info' com.vmware.vmo.plugin.vi4.model.TimeoutException
```

**步骤**

1 单击**系统属性**。

2 单击**添加**图标 (+)。

3 在**键**文本框中，输入 **com.vmware.vmo.plugin.vi4.waitUpdatesTimeout**。

4 在**值**文本框中，输入新的超时时间段（单位：毫秒）。

5 （可选） 在**描述**文本框中，输入系统属性的描述。

6 单击**添加**。

7 单击弹出菜单中的**保存更改**。

此时显示一条消息，表示您已保存成功。

**结果**

您设置的值会替换现有的 20000 秒默认超时设置。

# 后续操作

10

在安装并配置 vRealize Orchestrator 后，您可以使用 Orchestrator 自动处理与虚拟环境管理相关的频繁性重复操作。

- 登录 Orchestrator 客户端，在 vCenter Server 清单对象或 Orchestrator 通过其插件访问的其他对象上运行并调度工作流。请参见《使用 VMware vRealize Orchestrator 客户端》。
- 复制并修改标准 Orchestrator 工作流并自行编写操作和工作流以在 vCenter Server 中自动处理相关操作。
- 开发相关插件和 Web 服务以拓展 Orchestrator 平台。
- 使用 vSphere Web Client 在 vSphere 清单对象上运行工作流。

本章讨论了以下主题：



## 从 Orchestrator Appliance Web 控制台登录 Orchestrator 客户端

若要执行常规管理任务或编辑和创建工作流，您必须登录 Orchestrator 客户端界面。

Orchestrator 客户端界面专为具有管理权限且希望开发工作流、操作和其他自定义元素的开发人员而设计。

**重要事项** 确保 Orchestrator Appliance 的时钟与 Orchestrator 客户端计算机的时钟保持同步。

**前提条件**

- 在您要用于运行 Orchestrator 客户端的工作站上安装 64 位 Java。

  **注** 不支持 32 位 Java

**步骤**

1 单击**启动 Orchestrator 客户端**。

2 在**主机名**文本框中输入 Orchestrator Appliance 的 IP 地址或域名。

默认情况下会显示 Orchestrator Appliance 的 IP 地址。

3 使用 Orchestrator 客户端用户名和密码登录。

如果您采用 vRealize Automation 身份验证、vCenter Single Sign-On 或其他目录服务进行身份验证，请输入相应的凭据以登录 Orchestrator 客户端。

4 在**安全警告**窗口中，选择一个选项以处理证书警告。

Orchestrator 客户端使用 SSL 证书与 Orchestrator 服务器进行通信。可信 CA 在安装期间不签署证书。每次连接到 Orchestrator 服务器时，您都会收到证书警告。

| 选项 | 描述 |
| --- | --- |
| **忽略** | 使用当前的 SSL 证书继续。<br>重新连接到同一 Orchestrator 服务器或者尝试将工作流与远程 Orchestrator 服务器同步时，会再次显示警告消息。 |
| **取消** | 关闭该窗口并停止登录过程。 |
| **安装此证书，且不再显示该服务器的任何安全警告。** | 选中该复选框并单击**忽略**，以安装证书并停止接收安全警告。 |

您可以使用由 CA 签名的证书更改默认 SSL 证书。有关更改 SSL 证书的详细信息，请参见《安装和配置 VMware vRealize Orchestrator》。

**后续步骤**

您可以在系统上导入软件包、启动工作流或设置根访问权限。