

vCenter Server 安装和设置

VMware vSphere 8.0
vCenter Server 8.0

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

版权所有 © 2018-2022 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

目录

关于 vCenter Server 安装和设置 5

1 vSphere 安装和设置简介 6

- vSphere 安装和设置过程概览 6
- vCenter Server 组件和服务 8
- vCenter ServerAppliance 概览 10
- 了解 vSphere 域和域名 11
- vCenter 增强型链接模式 11
 - vCenter Server Appliance 的 vCenter 增强型链接模式 11
 - 加入 vCenter 增强型链接模式域 12

2 部署 vCenter ServerAppliance 13

- vCenter Server Appliance 的系统要求 14
 - vCenter Server 设备的硬件要求 14
 - vCenter Server 设备的存储要求 15
 - vCenter Server Appliance 的软件要求 15
 - vCenter Server 的所需端口 15
 - vCenter ServerAppliance 的 DNS 要求 16
 - vSphere Client 软件要求 16
- 准备部署 vCenter Server Appliance 17
 - vCenter Server 安装程序的系统要求 17
 - 下载并挂载 vCenter Server 安装程序 18
 - 同步 vSphere 网络连接上的时钟 19
 - 客户端和服务端之间的系统时钟同步 20
- 部署 vCenter Server Appliance 的必备条件 20
- vCenter ServerAppliance 的 GUI 部署 21
 - 部署 vCenter Server Appliance 所需的信息 22
 - 使用 GUI 部署 vCenter Server Appliance 25
 - 第 1 阶段 - 部署 OVA 文件作为 vCenter Server 设备 25
 - 阶段 2 - 设置新部署的 vCenter Server 设备 28
- vCenter Server Appliance 的 CLI 部署 29
 - 为 CLI 部署准备 JSON 配置文件 29
 - vCenter Server Appliance 的 CLI 部署的 JSON 模板 30
 - 部署配置参数 31
 - CLI 部署命令的语法 38
 - 使用 CLI 部署 vCenter Server Appliance 39
 - 使用 CLI 部署多个 vCenter Server Appliance 40

3 vCenter Server 的基于文件的备份和还原 42

基于文件的备份和还原的注意事项和限制 42

调度基于文件的备份 45

使用 vCenter Server 管理界面手动备份 vCenter Server 46

从基于文件的备份还原 vCenter Server 47

第 1 阶段 - 部署新设备 49

第 2 阶段 - 将数据传输到新部署的设备 52

4 部署 vCenter Server Appliance 后 53

使用 vSphere Client 登录到 vCenter Server 53

安装 VMware 增强型身份验证插件 54

将 vCenter Server 重新指向其他域中的另一个 vCenter Server 55

在没有复制合作伙伴的情况下将单个 vCenter Server 节点重新指向另一个现有域 55

在存在复制合作伙伴的情况下将 vCenter Server 节点重新指向另一个现有域 57

将 vCenter Server 节点重新指向新域 59

域重新指向命令的语法 61

了解标记和授权冲突 62

vCenter Server 域重新指向许可证注意事项 65

5 对 vCenter Server 安装或部署进行故障排除 67

收集用于对 vCenter Server 安装和升级进行故障排除的日志 67

手动检索安装日志 67

收集 vCenter Server Appliance 的部署日志文件 68

导出 vCenter Server 支持包以进行故障排除 68

关于 vCenter Server 安装和设置

《vCenter Server 安装和设置》介绍了如何部署 VMware vCenter Server® 设备。

VMware 非常重视包容性。为了在客户、合作伙伴和内部社区中促进这一原则，我们采用包容性语言创建内容。

目标读者

《vCenter Server 安装和设置》适合必须安装和配置 VMware vSphere® 的所有用户。这些主题的目标读者为熟悉虚拟机技术和数据中心操作且具有丰富经验的 Microsoft Windows 或 Linux 系统管理员。

vSphere 安装和设置简介

1

vSphere8.0 提供了各种安装和设置选项。为确保成功部署 vSphere，应了解安装和设置选项以及任务的执行顺序。

vSphere 的两个核心组件是 ESXi 和 vCenter Server。ESXi 是可用于创建和运行虚拟机和虚拟设备的虚拟化平台。vCenter Server 是一种服务，该服务充当连接网络的 ESXi 主机的中心管理员。使用 vCenter Server，您可以池化和管理工作主机的资源。

您需要部署 vCenter ServerAppliance，即已针对运行 vCenter Server 和 vCenter Server 组件而优化的预配置虚拟机。可以在 ESXi 主机或 vCenter Server 实例上部署 vCenter Server Appliance。

有关 ESXi 安装过程的详细信息，请参见《VMware ESXi 安装和设置》。

本章讨论了以下主题：

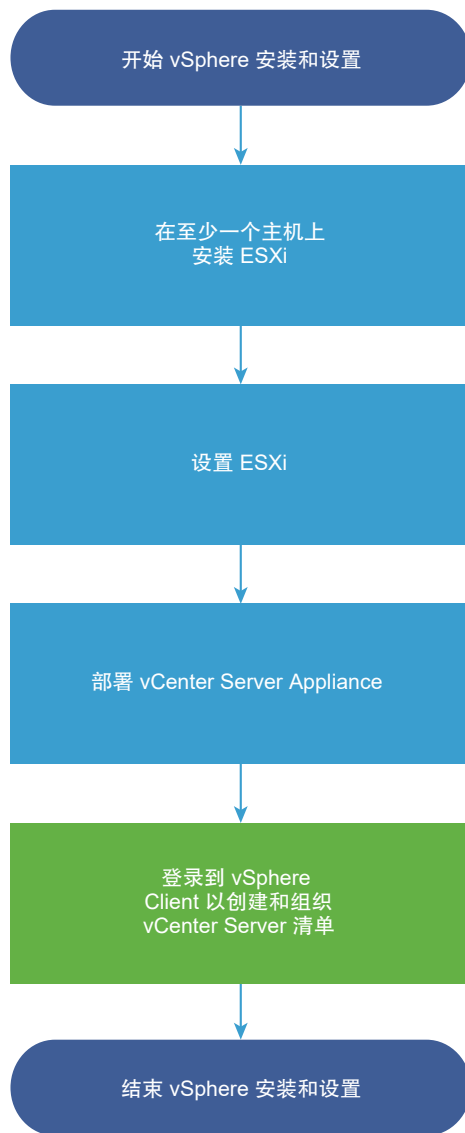
- [vSphere 安装和设置过程概览](#)
- [vCenter Server 组件和服务](#)
- [vCenter ServerAppliance 概览](#)
- [了解 vSphere 域和域名](#)
- [vCenter 增强型链接模式](#)

vSphere 安装和设置过程概览

vSphere 是一个复杂的产品，具有多个要安装和设置的组件。为确保成功部署 vSphere，需要了解所需的任务序列。

安装 vSphere 包含下列任务：

图 1-1. vSphere 安装和设置 workflow



- 1 阅读 vSphere 发行说明。
- 2 安装 ESXi。

注 有关 ESXi 安装过程的详细信息，请参见《VMware ESXi 安装和设置》。

- 3 配置 ESXi 引导和网络设置、直接控制台和其他设置。请参见《VMware ESXi 安装和设置》了解相关信息。
- 4 考虑设置用于远程日志记录的 **syslog** 服务器，以确保具有足够的磁盘存储来存储日志文件。对于本地存储有限的主机，在远程主机上设置日志记录尤为重要。请参见《VMware ESXi 安装和设置》。
- 5 安装 vCenter Server。

可以在 ESXi 主机或 vCenter Server 实例上部署 vCenter Server Appliance。

可以部署或安装多个以增强型链接模式配置连接的 vCenter Server 实例，方法是把这些实例注册到一个通用 Single Sign-On 域。

a 查看 [vCenter Server Appliance](#) 的系统要求中的主题，并验证系统是否满足部署设备的硬件和软件要求。

b 确定要使用的部署方法。

可以使用 GUI 方法以交互方式部署设备。或者，也可以使用 CLI 方法以静默方式部署设备。请参见 [vCenter Server Appliance](#) 的 GUI 部署和 [vCenter Server Appliance](#) 的 CLI 部署。

c 按照部署 [vCenter Server Appliance](#) 所需的信息主题中所述创建包含 GUI 部署所需的信息的工作表，或按照为 [CLI 部署准备 JSON 配置文件](#) 主题中所述创建用于 CLI 部署的 JSON 模板。

d 部署设备。

6 从 vSphere Client 连接到 vCenter Server。请参见第 4 章 [部署 vCenter Server Appliance](#) 后。

7 配置 vCenter Server 实例。请参见《vCenter Server 配置》和《vCenter Server 和主机管理》。

vCenter Server 组件和服务

vCenter Server 为虚拟机和主机的管理、操作、资源置备和性能评估提供了一个集中式平台。

部署 vCenter Server Appliance 时，将在同一系统上部署 vCenter Server、vCenter Server 组件和身份验证服务。

以下组件包含在 vCenter Server Appliance 部署中：

- 身份验证服务包含 vCenter Single Sign-On、License Service、Lookup Service 和 VMware Certificate Authority。
- vCenter Server 服务组包含 vCenter Server、vSphere Client、vSphere Auto Deploy 和 vSphere ESXi Dump Collector。vCenter Server Appliance 还包含 VMware vSphere Lifecycle Manager 扩展服务和 VMware vCenter Lifecycle Manager。

Platform Services Controller 发生了什么情况

从 vSphere 7.0 开始，部署新的 vCenter Server 或升级到 vCenter Server 7.0 需要使用 vCenter Server Appliance，它是针对运行 vCenter Server 而优化的预配置虚拟机。新的 vCenter Server 包含所有 Platform Services Controller 服务，同时保留功能和工作流，包括身份验证、证书管理、标记和许可。不再需要也无法部署和使用外部 Platform Services Controller。所有 Platform Services Controller 服务都已整合到 vCenter Server 中，并且简化了部署和管理。

由于这些服务现在是 vCenter Server 的一部分，因此不再将其描述为 Platform Services Controller 的一部分。在 vSphere 7.0 中，《vSphere 身份验证》出版物替换了《Platform Services Controller 管理》出版物。新出版物包含有关身份验证和证书管理的完整信息。有关从使用现有外部 Platform Services Controller 的 vSphere 6.5 和 6.7 部署迁移到使用 vCenter Server Appliance 的 vSphere 7.0 的信息，请参见《vSphere 升级》文档。

身份验证服务

vCenter Single Sign-On

vCenter Single Sign-On 身份验证服务为 vSphere 软件组件提供了安全身份验证服务。使用 vCenter Single Sign-On，vSphere 组件可通过安全令牌交换机制相互通信，而无需每个组件使用目录服务（如 Active Directory）分别对用户进行身份验证。

vCenter Single Sign-On 可以通过以下操作对用户进行身份验证：

- 外部身份提供程序联合

可以使用联合身份验证为 vCenter Server 配置外部身份提供程序。在此类配置中，将替换 vCenter Server 作为身份提供程序。目前，vSphere 支持将 Active Directory 联合身份验证服务 (AD FS) 作为外部身份提供程序。在此配置中，AD FS 代表 vCenter Server 与身份源进行交互。

- vCenter Server 内置身份提供程序

vCenter Server 包含内置身份提供程序。默认情况下，vCenter Server 使用 vsphere.local 域作为标识源（但可以在安装过程中进行更改）。可以使用 LDAP/S、OpenLDAP/S 和集成 Windows 身份验证 (IWA)，将 vCenter Server 内置身份提供程序配置为使用 Active Directory (AD) 作为其标识源。此类配置允许客户使用其 AD 帐户登录到 vCenter Server。

然后，可以在 vSphere 环境中为经过身份验证的用户分配基于注册的解决方案的权限或角色。

vCenter Server 需要 vCenter Single Sign-On。

vSphere License Service

vSphere License Service 为 Single Sign-On 域内的所有 vCenter Server 系统提供通用的许可证清单和管理功能。

VMware Certificate Authority

默认情况下，VMware Certificate Authority (VMCA) 将使用以 VMCA 作为根证书颁发机构的签名证书置备每个 ESXi 主机。以显式方式将 ESXi 主机添加到 vCenter Server 时进行置备，或在 ESXi 主机安装过程中进行置备。所有 ESXi 证书都存储在本地主机上。

有关所有身份验证服务和功能的信息，请参见《vSphere 身份验证》。

随 vCenter Server 一起安装的服务

安装 vCenter Server 时，将以静默方式安装这些附加组件。这些组件不能单独安装，因为它们没有其自己的安装程序。

PostgreSQL

VMware 分发的用于 vSphere 和 vCloud Hybrid Service 的 PostgreSQL 数据库捆绑版本。

vSphere Client

通过基于 HTML5 的用户界面，可以使用 Web 浏览器连接到 vCenter Server 实例。从 vSphere 7.0 开始，此 vSphere Client 将替代基于 Flex 的 vSphere Web Client。

vSphere ESXi Dump Collector

vCenter Server 支持工具。可以将 ESXi 配置为在系统发生严重故障时将 VMkernel 内存保存到网络服务器而非磁盘。vSphere ESXi Dump Collector 将通过网络收集这些内存转储。

vSphere Auto Deploy

vCenter Server 支持工具，能够使用 ESXi 软件置备大量物理主机。可以指定要部署的映像以及要使用此映像置备的主机。也可以指定应用到主机的主机配置文件，并且为每个主机指定 vCenter Server 位置（文件夹或集群）。

VMware vSphere Lifecycle Manager 扩展

vSphere Lifecycle Manager 可让 VMware vSphere 执行集中式自动修补程序和版本管理，并提供对 VMware ESXi 主机、虚拟机和虚拟设备的支持。VMware vSphere Lifecycle Manager 扩展是 vCenter Server Appliance 的可选服务。

VMware vCenter Lifecycle Manager

vCenter Lifecycle Manager 自动执行虚拟机管理过程，并在适当的时候从服务中移除虚拟机。

vCenter Lifecycle Manager 根据服务器的位置、组织、环境、服务级别或性能级别自动放置服务器。根据一组条件找到解决方案时，会自动部署计算机。

vCenter ServerAppliance 概览

vCenter ServerAppliance 是针对运行 vCenter Server 及关联服务而优化的预配置虚拟机。

vCenter ServerAppliance 软件包包含以下软件：

- Photon OS[®] 3.0
- vSphere 身份验证服务
- PostgreSQL
- VMware vSphere Lifecycle Manager 扩展
- VMware vCenter Lifecycle Manager

vCenter Server 版本 8.0 上部署了虚拟硬件版本 10，此虚拟硬件版本在 ESXi 中支持每个虚拟机具有 64 个虚拟 CPU。

在部署期间，您可以选择适合 vSphere 环境大小的 vCenter ServerAppliance 大小以及满足数据库要求的存储大小。

vCenter Server 使用 VMware vSphere Lifecycle Manager 扩展服务。vSphere 集中式自动修补程序和版本管理不再需要 Windows 上的外部 vSphere Lifecycle Manager 实例。有关 vCenter Server 的信息，请参见 [vCenter Server 组件和服务](#)。

vCenter Server 支持高可用性。有关在 vCenter High Availability 集群中配置 vCenter Server 的信息，请参见《vSphere 可用性》。

vCenter Server 支持基于文件的备份和还原。有关备份和还原的信息，请参见第 3 章 [vCenter Server 的基于文件的备份和还原](#)。

有关 vCenter Server 最高配置的信息，请参见《[VMware 最高配置](#)》。

了解 vSphere 域和域名

每个 vCenter Server 都与一个 vCenter Single Sign-On 域关联。域名默认为 vsphere.local，但可以在部署过程中更改域名。域决定本地身份验证空间。

vCenter Single Sign-On 域

部署 vCenter ServerAppliance 时，系统会提示您创建 vCenter Single Sign-On 域或加入现有域。

域名由 VMware Directory Service (vmdir) 用于所有的轻量目录访问协议 (LDAP) 内部构造。

可以为域指定一个唯一名称。为防止身份验证冲突，请使用未被 OpenLDAP、Microsoft Active Directory 和其他目录服务使用的名称。

指定域名后，可以添加用户和组。您可以添加 Active Directory 或 LDAP 标识源并允许该标识源中的用户和组进行身份验证。也可以将 vCenter Server 实例或其他 VMware 产品（例如，vRealize Operations）添加到该域。

vCenter 增强型链接模式

通过 vCenter 增强型链接模式，您可以登录到任何一个 vCenter Server 实例，并且还可以查看和管理组中所有 vCenter Server 系统的清单。

最多可以在单个 vSphere Single Sign-On 域中加入 15 个具有 vCenter 增强型链接模式的 vCenter ServerAppliance 部署。

可以在部署 vCenter ServerAppliance 期间创建 vCenter 增强型链接模式组。

还可以通过将 vCenter Server 从一个 vSphere 域移至或重新指向另一个现有域来加入 vCenter 增强型链接模式组。有关重新指向 vCenter Server 节点的信息，请参见[将 vCenter Server 重新指向其他域中的另一个 vCenter Server](#)。

vCenter Server Appliance 的 vCenter 增强型链接模式

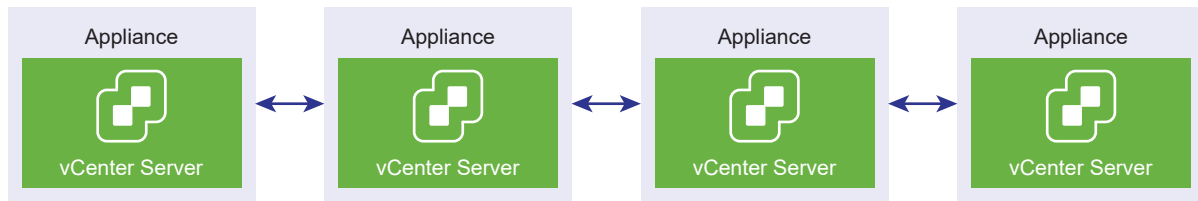
已为 vCenter Server Appliance 部署启用增强型链接模式支持。

可以将 vCenter Server Appliance 部署连接在一起，形成一个域。

其他功能包括：

- 简化的备份和还原过程。有关详细信息，请参见[第 3 章 vCenter Server 的基于文件的备份和还原](#)。
- 简化的 HA 过程，无需负载均衡器。
- 使用增强型链接模式最多可将 15 个 vCenter Server Appliance 部署链接到一起，并在一个清单视图中显示。
- 对于 vCenter High Availability (vCenter HA) 集群，三个节点视为一个逻辑 vCenter Server 节点。有关 vCenter HA 架构概览，请参见《vSphere 可用性》中的“vCenter 架构概览”。一个 vCenter HA 集群需要一个 vCenter Server 标准许可证。

图 1-2. vCenter Server Appliance 部署的增强型链接模式



增强型链接模式和只读复制

如果 vCenter High Availability (vCenter HA) 实例与另一个使用增强型链接模式的 vCenter Server 实例连接，当 vCenter HA 故障切换到被动节点且无法与其他 vCenter Server 节点上的复制合作伙伴通信时，vCenter HA 节点上的副本会进入只读模式。

加入 vCenter 增强型链接模式域

可以在部署 vCenter ServerAppliance 期间将该 vCenter Server Appliance 连接到另一个节点。

注 还可以通过将 vCenter Server 从一个 vSphere 域移至或重新指向另一个现有域来加入 vCenter 增强型链接模式组。有关重新指向 vCenter Server 节点的信息，请参见[将 vCenter Server 重新指向其他域中的另一个 vCenter Server](#)。

例如，假设您要部署两个 vCenter Server Appliance 系统，并使用 vCenter 增强型链接模式连接这两个节点。

如果要使用 UI 安装程序部署 vCenter ServerAppliance 节点：

- 1 对于设备 1，将 vCenter ServerAppliance 部署为 ESXi 主机 1 上的实例。将时间设置与 ESXi 主机 1 同步。
- 2 对于设备 2，将 vCenter ServerAppliance 部署为 ESXi 主机 1 上的实例，并配置时间设置，以便设备 2 与 ESXi 主机 1 同步。在第 2 阶段中，选择加入设备 1 上已部署设备的 vCenter Single Sign-On 服务器。有关具体说明，请参见[阶段 2 - 设置新部署的 vCenter Server 设备](#)。

如果要使用 CLI 部署 vCenter ServerAppliance 节点：

- 1 将设备 1 的 JSON 配置模板 `embedded_vCSA_on_VC.json`（或 `embedded_vCSA_on_ESXi.json`）配置为 ESXi 主机 1 上的实例。有关准备 JSON 配置文件的具体说明，请参见[CLI 部署准备 JSON 配置文件](#)。
- 2 通过运行 `vcasa-cli-installer` 命令部署设备 1。有关说明，请参见[使用 CLI 部署 vCenter Server Appliance](#)。
- 3 将设备 2 的 JSON 配置模板 `embedded_vCSA_replication_on_VC.json`（或 `embedded_vCSA_replication_on_ESXi.json`）配置为 ESXi 主机 1 上的实例。在 `sso` 部分中的 `replication_partner_hostname` 字段中输入第一个嵌入式节点的主机名。
- 4 通过运行 `vcasa-cli-installer` 命令使用 `embedded_vCSA_replication_on_VC.json`（或 `embedded_vCSA_replication_on_ESXi.json`）文件部署设备 2。

部署 vCenter ServerAppliance

2

您可以部署 vCenter ServerAppliance 来管理 vSphere 环境。

您可以在 ESXi 主机 6.7 或更高版本上部署 vCenter Server Appliance，或者通过 vCenter Server 6.7 或更高版本的实例清单在 ESXi 主机或 DRS 集群上部署。

有关 vCenter ServerAppliance 8.0 中所含软件的信息，请参见 [vCenter ServerAppliance 概览](#)。

有关部署 vCenter ServerAppliance 的软件和硬件要求的信息，请参见 [vCenter Server Appliance 的系统要求](#)。

vCenter Server 安装程序包含用于 GUI 和 CLI 部署的可执行文件。

- GUI 部署过程分为两个阶段。第一阶段是部署向导，该向导将在目标 ESXi 主机或 vCenter Server 实例上部署该设备的 OVA 文件。OVA 部署完成后，您应继续执行该过程的第二阶段，以设置并启动新部署设备的服务。
- CLI 部署方法涉及到针对先前准备的 JSON 文件运行 CLI 命令。CLI 安装程序将解析 JSON 文件中的配置参数及其值，并生成 OVF Tool 命令以自动部署和设置该设备。CLI 部署自动依次运行第 1 阶段和第 2 阶段，无需用户交互。

vCenter ServerAppliance 具有以下默认用户名：

用户名	描述
root	使用此用户名可登录设备操作系统和 vCenter Server 管理界面。 在部署虚拟设备时设置密码。
administrator@your_domain_name	使用此用户名可登录 vCenter Single Sign-On。 在创建 vCenter Single Sign-On 域时设置密码。在新的 vCenter Single Sign-On 域中部署 vCenter ServerAppliance 期间，您可以创建 vCenter Single Sign-On 域。 创建 vCenter Single Sign-On 域后，只有 administrator@your_domain_name 用户具有登录到 vCenter Single Sign-On 和 vCenter Server 所需的特权。 administrator@your_domain_name 用户可以执行以下任务： <ul style="list-style-type: none">■ 将在其中定义了其他用户和组的标识源添加到 vCenter Single Sign-On 中。■ 为用户和组提供权限。 有关添加标识源并向用户和组授予权限的信息，请参见《vSphere 身份验证》。

有关升级和修补 vCenter ServerAppliance 的信息，请参见《vSphere 升级》。

有关配置 vCenter Server 的信息，请参见《vCenter Server 配置》。

如果要将 vCenter Server 设置为使用 IPv6 地址版本，请使用设备的完全限定域名 (FQDN) 或主机名。要设置 IPv4 地址，最佳做法是使用设备的 FQDN 或主机名，因为如果 DHCP 分配了 IP 地址，则其可能会更改。

本章讨论了以下主题：

- [vCenter Server Appliance 的系统要求](#)
- [准备部署 vCenter Server Appliance](#)
- [部署 vCenter Server Appliance 的必备条件](#)
- [vCenter Server Appliance 的 GUI 部署](#)
- [vCenter Server Appliance 的 CLI 部署](#)

vCenter Server Appliance 的系统要求

可以在 ESXi 主机 6.7 或更高版本或者 vCenter Server 实例 6.7 或更高版本上部署 vCenter Server Appliance。此外，系统还必须满足软件和硬件要求。

使用完全限定域名时，请确认用于部署设备的客户机和要在其上部署设备的网络使用同一 DNS 服务器。

部署设备之前，请同步 vSphere 网络上的目标服务器以及所有 vCenter Server 实例的时钟。如果时钟未同步，可能会导致身份验证问题，也可能导致安装失败或设备服务无法启动。请参见[同步 vSphere 网络连接上的时钟](#)。

vCenter Server 设备的硬件要求

部署 vCenter Server Appliance 时，可以选择部署适合 vSphere 环境大小的设备。您选择的选项将决定 vCenter Server Appliance 的 CPU 数量和内存大小。

vCenter Server Appliance 的硬件要求取决于 vSphere 清单的大小。

	vCPU 数目	内存
微型环境（最多 10 个主机或 100 个虚拟机）	2	14 GB
小型环境（最多 100 个主机或 1,000 个虚拟机）	4	21 GB
中型环境（最多 400 个主机或 4,000 个虚拟机）	8	30 GB
大型环境（最多 1,000 个主机或 10,000 个虚拟机）	16	39 GB
超大型环境（最多 2,000 个主机或 35,000 个虚拟机）	24	58 GB

注 如果要将包含超过 512 个 LUN 和 2,048 个路径的 ESXi 主机添加到 vCenter Server 清单，必须部署适用于大型或超大型环境的 vCenter Server Appliance。

vCenter Server 设备的存储要求

部署 vCenter Server Appliance 时，部署设备的 ESXi 主机或 DRS 集群必须满足最低存储要求。存储要求不但取决于 vSphere 环境大小和存储大小，还取决于磁盘置备模式。

存储要求对于每个 vSphere 环境大小都不同，并且取决于数据库大小要求。

	默认存储大小	大型存储大小	超大型存储大小
微型环境（最多 10 个主机或 100 个虚拟机）	579 GB	1992 GB	4279 GB
小型环境（最多 100 个主机或 1,000 个虚拟机）	694 GB	2046 GB	4304 GB
中型环境（最多 400 个主机或 4,000 个虚拟机）	908 GB	2140 GB	4468 GB
大型环境（最多 1,000 个主机或 10,000 个虚拟机）	1358 GB	1958 GB	4518 GB
超大型环境（最多 2,000 个主机或 35,000 个虚拟机）	2283 GB	2383 GB	4620 GB

注 存储要求包括 vSphere Lifecycle Manager 在 vCenter Server Appliance 中作为服务运行所需满足的要求。

vCenter Server Appliance 的软件要求

VMware vCenter Server Appliance 可以部署在 ESXi 6.7 主机或更高版本的主机上，也可以部署在 6.7 或更高版本的 vCenter Server 实例上。

可以使用 GUI 或 CLI 安装程序部署 vCenter Server Appliance。应从用于连接到目标服务器的网络客户机运行该安装程序，并在该服务器上部署该设备。可以直接连接到要部署该设备的 ESXi 6.7 主机。还可以连接到 vCenter Server 6.7 实例，以在位于 vCenter Server 清单中的 ESXi 主机或 DRS 集群上部署该设备。

有关网络客户机要求的信息，请参见 [vCenter Server 安装程序](#) 的系统要求。

vCenter Server 的所需端口

vCenter Server 系统必须能将数据发送到每个受管主机，并且能够从每个 vSphere Client 接收数据。要在受管主机间启用迁移和置备活动，源主机和目标主机必须能够通过预确定的 TCP 和 UDP 端口彼此接收数据。

vCenter Server 可通过预定的 TCP 和 UDP 端口进行访问。若要从防火墙外管理网络组件，可能需重新配置防火墙以允许在适当端口的访问。有关 vSphere 中所有受支持端口和协议的列表，请参阅 <https://ports.vmware.com> 中的 VMware Ports and Protocols Tool™。

在安装过程中，如果端口正在使用中或被拒绝列表阻止，vCenter Server 安装程序将显示错误消息。您必须使用另一个端口号才能继续安装。存在一些仅用于进程间通信的内部端口。

VMware 使用指定的端口进行通信。此外，受管主机将在指定的端口上监控来自于 vCenter Server 的数据。如果这些元素中的任意两个之间存在内置防火墙，安装程序将在安装或升级过程中打开这些端口。对于自定义防火墙，必须手动打开所需端口。如果在两台受管主机之间有防火墙，并且您要在源主机或目标主机上执行活动，例如迁移或克隆，则必须配置一种方式，以便受管主机接收数据。

要将 vCenter Server 系统配置为使用不同的端口接收 vSphere Client 数据，请参见《vCenter Server 和主机管理》文档。

vCenter ServerAppliance 的 DNS 要求

与任何网络服务器类似，在部署 vCenter Server Appliance 时，您可以分配固定 IP 地址和可由 DNS 服务器解析的 FQDN，以便客户端能可靠地访问服务。

使用静态 IP 地址部署 vCenter ServerAppliance 时，请确保设备的 IP 地址在系统重新启动后仍然保持不变。

使用静态 IP 地址部署 vCenter ServerAppliance 之前，必须确认该 IP 地址具有有效的内部域名系统 (DNS) 注册。

部署 vCenter ServerAppliance 时，如果安装程序从其 IP 地址中找不到设备的完全限定域名 (FQDN)，则安装支持 vSphere Client 的 Web 服务器组件会失败。反向查询是使用 PTR 记录来实现的。

如果计划使用 FQDN 作为设备系统名称，必须通过添加正向和反向 DNS A 记录来确认 FQDN 可由 DNS 服务器解析。

可以使用 nslookup 命令验证在使用 IP 地址进行查询时，DNS 反向查找服务是否会返回 FQDN，并验证 FQDN 是否可解析。

```
nslookup -nosearch -nodefname FQDN_or_IP_address
```

如果使用 vCenter ServerAppliance 的 DHCP 而不是静态 IP 地址，请验证设备名称是否已在域名服务 (DNS) 中更新。如果可以 ping 设备名称，则该名称已在 DNS 中更新。

确保 ESXi 主机管理接口可以从 vCenter Server 和所有 vSphere Client 实例进行有效的 DNS 解析。确保 vCenter Server 可以从所有 ESXi 主机和 vSphere Client 进行有效的 DNS 解析。

vSphere Client 软件要求

使用 vSphere Client 需要受支持的 Web 浏览器。

VMware 已经过测试，支持以下客户机操作系统和 vSphere Client 的浏览器版本：

受支持的客户机操作系统

- Windows 32 位和 64 位版本
- Mac OS

受支持的浏览器版本

- Google Chrome 89 或更高版本
- Mozilla Firefox 80 或更高版本

- Microsoft Edge 90 或更高版本

注 这些浏览器的更高版本也许可用，但尚未经测试。

准备部署 vCenter Server Appliance

在部署 vCenter Server Appliance 之前，必须下载 vCenter Server 安装程序 ISO 文件并将其挂载到要通过其执行部署的网络虚拟机或物理服务器。

通过其部署设备的计算机必须在满足操作系统要求的 Windows、Linux 或 Mac 操作系统上运行。请参见 [vCenter Server 安装程序的系统要求](#)。

vCenter Server 安装程序的系统要求

可以从受支持版本的 Windows、Linux 或 Mac 操作系统上运行的网络客户机运行 vCenter Server GUI 或 CLI 安装程序。

为确保 GUI 和 CLI 安装程序的最佳性能，请使用满足最低硬件要求的客户机。

表 2-1. GUI 和 CLI 安装程序的系统要求

操作系统	受支持的版本	确保最佳性能的最低硬件配置
Windows	<ul style="list-style-type: none"> ■ Windows 10、11 ■ Windows 2016 x64 位 ■ Windows 2019 x64 位 ■ Windows 2022 x64 位 	4 GB RAM、2 个 2.3 GHz 四核 CPU、32 GB 硬盘、1 个网卡
Linux	<ul style="list-style-type: none"> ■ SUSE 15 ■ Ubuntu 18.04、20.04、21.10 	4 GB RAM、1 个 2.3 GHz 双核 CPU、16 GB 硬盘、1 个网卡 注 CLI 安装程序要求 64 位操作系统。
Mac	<ul style="list-style-type: none"> ■ macOS 10.15、11、12 ■ macOS Catalina、Big Sur 和 Monterey 	8 GB RAM、1 个 2.4 GHz 四核 CPU、150 GB 硬盘、1 个网卡

注 对于在 Mac 10.15 或更高版本上运行的客户机，不支持使用 GUI 同时部署多个设备。必须按顺序部署设备。

注 需要安装 Visual C++ 可再发行库，以在低于 Windows 10 的 Windows 版本上运行 CLI 安装程序。这些库的 Microsoft 安装程序位于 `vcasa-cli-installer/win32/vcredist` 目录中。

注 要使用 GUI 部署 vCenter Server Appliance，分辨率至少必须为 1024x768 才能正常显示。更低的分辨率会截断 UI 元素。

下载并挂载 vCenter Server 安装程序

VMware 发布了 vCenter Server Appliance ISO 映像，其中包含 vCenter Server Appliance 的 GUI 和 CLI 安装程序。

使用包含在 vCenter Server 安装程序中的 GUI 和 CLI 可执行文件，您可以：

- 部署 vCenter Server Appliance。
- 升级 vCenter Server Appliance。
- 将具有外部 Platform Services Controller 的旧版本 vCenter Server 融合到当前版本的 vCenter Server。
- 从基于文件的备份还原 vCenter Server Appliance。

前提条件

- 在 <https://my.vmware.com/web/vmware/> 上创建一个 Customer Connect 帐户。
- 确认客户端计算机满足 vCenter Server 安装程序的系统要求。请参见 [vCenter Server 安装程序的系统要求](#)。

步骤

- 1 登录到 VMware Customer Connect。
- 2 导航到**产品和帐户 > 所有产品**。
- 3 找到 VMware vSphere，然后单击**查看下载组件**。
- 4 从**选择版本**下拉菜单中选择 VMware vSphere 版本。
- 5 选择 VMware vCenter Server 的版本，然后单击**转到下载**。
- 6 下载 vCenter Server Appliance ISO 映像。
- 7 使用 MD5 校验和工具确认 md5sum 正确无误。
- 8 将 ISO 映像挂载到要为其部署、升级、迁移或还原设备的客户机。

注 不支持禁用八个以上目录级别的 ISO 挂载软件，例如，Windows 上的 MagicISO Maker。

对于 Linux OS 和 Mac OS，不支持存档管理器。

对于 Mac OS，您可以使用 DiskImageMounter。

对于 Ubuntu 14.04，您可以使用 Disk Image Mounter。

对于 SUSE 12 OS，您可以使用终端。

```
$ sudo mkdir mount_dir
$ sudo mount -o loop VMware-vCSA-all-version_number-build_number.iso mount_dir
```

重要说明 由于 MacOS Catalina 中的安全更改，您必须修改计算机上的安全设置，直到 vCenter Server 部署完成。如果您尝试在 MacOS Catalina 下运行安装程序而不修改安全设置，vCenter Server 安装程序会报告以下错误：ovftool cannot be opened because the developer cannot be verified。有关更多信息，请参见 [KB 79416](#)。

后续步骤

打开 `readme.txt` 文件并查看有关 vCenter Server Appliance ISO 映像中的其他文件和目录的信息。

同步 vSphere 网络连接上的时钟

验证 vSphere 网络上所有组件的时钟是否均已同步。如果 vSphere 网络中的物理机时钟不同步，则可能无法在网络计算机之间的通信中将时间敏感的 SSL 证书和 SAML 令牌识别为有效。

时钟不同步可能会引起身份验证问题，从而导致安装失败或 vCenter Server `vmware-vpxd` 服务无法启动。

vSphere 中的时间不一致可能会导致首次引导环境中的组件在不同的服务处失败，具体取决于哪段环境时间不准确以及时间何时同步。目标 vCenter Server 的目标 ESXi 主机与 NTP 或 PTP 不同步时，通常会出现问题。同样，如果目标 vCenter Server 迁移到因 DRS 完全自动化而设置为不同时间的 ESXi 主机，也会出现问题。

要避免时间同步问题，请在安装、迁移或升级 vCenter Server 实例之前，确保以下项正确。

- 要部署目标 vCenter Server 的目标 ESXi 主机同步到 NTP 或 PTP。
- 运行源 vCenter Server 的 ESXi 主机同步到 NTP 或 PTP。
- 从 vSphere 6.7 升级或迁移到 vSphere 8.0 时，如果 vCenter Server Appliance 连接到外部 Platform Services Controller，请确保运行外部 Platform Services Controller 的 ESXi 主机同步到 NTP 或 PTP。
- 如果从 vSphere 6.7 升级或迁移到 vSphere 8.0，请确认源 vCenter Server 或 vCenter Server Appliance 以及外部 Platform Services Controller 的时间正确。

验证运行 vCenter Server 的任何 Windows 主机是否与网络时间协议 (Network Time Protocol, NTP) 服务器同步。请参见 VMware 知识库文章，网址为 <https://kb.vmware.com/s/article/1318>。

要将 ESXi 时钟与 NTP 或 PTP 服务器同步，可以使用 VMware Host Client。有关编辑 ESXi 主机时间配置的信息，请参见《vSphere 单台主机管理 - VMware Host Client》文档中的“在 VMware Host Client 中编辑 ESXi 主机的时间配置”主题。

要了解如何更改 vCenter Server 的时间同步设置，请参见《vCenter Server 配置》文档中的“配置系统时区和时间同步设置”主题。

要了解如何使用 vSphere Client 编辑主机的时间配置，请参见《vCenter Server 和主机管理》文档中的“编辑主机的时间配置设置”主题。

客户端和服务端之间的系统时钟同步

要与 vCenter Server（服务器）建立安全 TLS 连接，在其中运行 CLI 安装程序（客户端）的系统的系统时钟和服务器的系统时钟之间的时间差不得超过可接受限制（容错）。

有关每个部署方案的特定值，请参见表 2-2. 客户端时钟容错。

注 客户端时钟值仅适用于 vCenter Server 6.7 及更高版本。

表 2-2. 客户端时钟容错

部署方案	时钟容错	连接说明
将一个 vCenter Server 与另一个 vCenter Server 链接	部署第二个 vCenter Server 时，客户端和第一个 vCenter Server 之间的时钟容错不得超过 10 分钟。	
安装 vCenter Server Appliance（配合使用容器 vCenter Server 与 *. _on_vc.json 模板）。	客户端和容器 vCenter Server 之间的最大时钟容错为 8 小时 20 分钟。	

部署 vCenter Server Appliance 的必备条件

要确保 vCenter Server Appliance 成功部署，运行安装程序之前必须执行一些必要的任务和预检查。

常规必备条件

- 下载并挂载 vCenter Server 安装程序。

目标系统必备条件

- 验证系统是否满足最低软件和硬件要求。请参见 vCenter Server Appliance 的系统要求。
- 如果要在 ESXi 主机上部署设备，请确认 ESXi 主机不处于锁定模式或维护模式并且不属于全自动 DRS 集群的一部分。
- 如果要在含有 vCenter Server 实例清单的 DRS 集群上部署设备，请确认该集群至少包含一个不处于锁定模式或维护模式的 ESXi 主机。
- 如果计划将 NTP 服务器用于时间同步，请确认 NTP 服务器正在运行，并且 NTP 服务器与要部署设备的目标服务器之间的时间同步。
- 如果要在使用 vSAN ESA 加密的 vSAN ESA 集群上部署设备，必须先启用 vSAN ESA 加密，然后再安装 vCenter Server。vSAN Express Storage Architecture 是下一代架构，旨在充分利用高性能存储设备，从而提高性能和效率。您可以通过 vSAN SDK 或 vSAN API 启用 vSAN ESA 加密。

vCenter 增强型链接模式必备条件

在增强型链接模式部署中部署新的 vCenter Server 时，请为环境中的现有 vCenter Server 节点创建基于映像的备份。可以将该备份用作部署过程中出现故障时的预防措施。

如果部署失败，请删除新部署的 vCenter Server Appliance，然后从其相应的基于映像的备份还原 vCenter Server 节点。必须从基于映像的备份还原环境中的所有节点。如果未执行此操作，可能会导致复制合作伙伴与还原的节点不同步。

- 要了解有关创建 vCenter 增强型链接模式部署的更多信息，请参见 [vCenter 增强型链接模式](#)。
- 要了解基于映像的备份，请参见[#unique_33](#)。

网络必备条件

如果计划在设备的网络设置中分配静态 IP 地址和 FQDN 作为系统名称，请确认已为此 IP 地址配置了正向和反向 DNS 记录。

vCenter ServerAppliance 的 GUI 部署

可以使用 GUI 安装程序以交互方式部署 vCenter ServerAppliance。

执行 GUI 部署时，应将 vCenter Server 安装程序下载到网络客户机，从该客户机运行部署向导，并提供部署和设置设备所需的输入。

GUI 部署过程包括两个阶段。

图 2-1. 第 1 阶段 - OVA 部署



第一阶段将引导您完成部署向导，以选择部署类型和设备设置。此阶段将使用所提供的部署类型和设备设置在目标服务器上完成 OVF 文件的部署。

作为使用 GUI 安装程序执行部署的第一阶段的替代方法，您也可以使用 vSphere Client 部署 vCenter Server Appliance 的 OVA 文件。OVA 部署完成后，您必须登录到新部署的设备的 vCenter Server 管理界面，以继续执行部署过程的第二阶段。有关使用 vSphere Client 部署 OVA 文件的信息，请参见《vSphere 虚拟机管理》《vSphere 虚拟机管理》中的“部署 OVF 或 OVA 模板”。

图 2-2. 第 2 阶段 - 设备设置



第二阶段将引导您完成设置向导，以配置设备时间同步和 vCenter Single Sign-On。此阶段将完成初始设置并启动新部署设备的服务。

作为使用 GUI 安装程序执行部署的第二阶段的替代方法，您也可以登录到新部署的设备的 vCenter Server 管理界面：https://FQDN_or_IP_address:5480。

部署 vCenter Server Appliance 所需的信息

使用 GUI 方法部署 vCenter Server Appliance 时，向导会提示您输入部署信息和设置信息。最佳做法是将您输入的值记录下来，以便在将来重新安装此产品时使用。

可以使用此工作表记录部署 vCenter Server Appliance 所需的信息。

表 2-3. GUI 部署过程的第 1 阶段所需的信息

所需信息	默认	条目
要在其上面部署设备的目标服务器的 FQDN 或 IP 地址。 目标服务器可以是 ESXi 主机或 vCenter Server 实例。	-	
目标服务器的 HTTPS 端口	443	
对目标服务器具有管理特权的用户名 ■ 如果目标服务器是 ESXi 主机，请使用 root。 ■ 如果目标服务器是 vCenter Server 实例，请使用 <code>user_name@your_domain_name</code> ，例如 <code>administrator@vsphere.local</code> 。	-	
对目标服务器具有管理特权的用户的密码	-	
vCenter Server 清单中要在其上面部署设备的数据中心。 目标服务器必须是 vCenter Server 实例。 (可选) 可以提供数据中心文件夹。	-	
数据中心清单中要在其上面部署设备的 ESXi 主机或 DRS 集群	-	
设备的虚拟机名称 ■ 不得包含百分号 (%)、反斜杠 (\) 或正斜杠 (/) ■ 长度不得超过 80 个字符	vCenter Server	
设备操作系统的 root 用户的密码 ■ 必须仅包含不含空格的低位 ASCII 字符。 ■ 长度至少必须为 8 个字符，但不能超过 20 个字符 ■ 必须至少包含一个大写字母 ■ 必须至少包含一个小写字母 ■ 必须至少包含一个数字 ■ 必须至少包含一个特殊字符，例如美元符号 (\$)、井号 (#)、@ 符号 (@)、句点 (.) 或感叹号 (!)	-	

表 2-3. GUI 部署过程的第 1 阶段所需的信息（续）

所需信息	默认	条目
适用于 vSphere 环境的 vCenter Server Appliance 部署大小。有关您可以选择的部署大小的信息，请参见 vCenter Server 设备的硬件要求 。您选择的选项将决定 vCenter Server Appliance 的 CPU 数量和内存大小。	微型	
适用于 vSphere 环境的 vCenter Server Appliance 存储大小。所需存储不仅取决于 vSphere 环境的大小，还取决于磁盘置备模式。请参见 vCenter Server 设备的存储要求 。 如果需要更大的卷用于 SEAT 数据（统计信息、事件、警报和任务），请增加默认存储大小。	默认	
要在其中存储设备的配置文件和虚拟磁盘的数据存储的名称 注 安装程序将显示一系列可从目标服务器访问的数据存储。	-	
启用或禁用精简磁盘模式	已禁用	
要将设备连接到的网络的名称 注 安装程序将根据目标服务器的网络设置显示网络下拉菜单。如果将设备直接部署在 ESXi 主机上，则非临时分布式虚拟端口组将不受支持，且不会显示在下拉菜单中。 该网络必须可以从执行部署的客户机访问。	-	
设备地址的 IP 版本 可以是 IPv4 或 IPv6。	IPv4	
设备地址的 IP 分配 可以是静态或 DHCP。	静态	
FQDN 适用于静态 IP 分配 vCenter Server 使用 FQDN 或 IP 地址作为系统名称。	-	
IP 地址	-	
对于 IPv4 网络，可以使用子网掩码或网络前缀。子网掩码采用点分隔十进制记数法（例如 255.255.255.0）。IPv4 网络前缀是介于 0 到 32 之间的整数。 对于 IPv6 网络，必须使用网络前缀。IPv6 网络前缀是介于 0 到 128 之间的整数。	-	
默认网关	-	

表 2-3. GUI 部署过程的第 1 阶段所需的信息（续）

所需信息	默认	条目
用逗号分隔的 DNS 服务器	-	
系统名称 (FQDN)	-	
仅当您将 DHCP 与 IPv4 结合使用并且您的环境中具有动态 DNS (DDNS) 服务器时。		

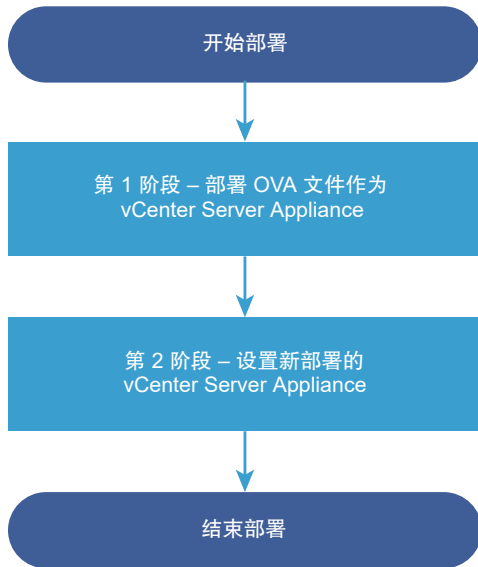
表 2-4. GUI 部署过程的第 2 阶段所需的信息

所需信息	默认	条目
时间同步设置 您可以将设备的时间与 ESXi 主机的时间同步，或者与一个或多个 NTP 服务器同步。 如果要使用多个 NTP 服务器，您必须以逗号分隔列表的格式提供这些 NTP 服务器的 IP 地址或 FQDN。	与 NTP 服务器同步时间	
启用或禁用 SSH 访问 注 vCenter Server High Availability 要求可对设备进行远程 SSH 访问。	已禁用	
新的 vCenter Single Sign-On 域的名称 例如，vsphere.local。	-	
管理员帐户的密码， <code>administrator@your_domain_name</code> <ul style="list-style-type: none"> ■ 长度至少必须为 8 个字符，但不能超过 20 个字符 ■ 必须至少包含一个大写字母 ■ 必须至少包含一个小写字母 ■ 必须至少包含一个数字 ■ 必须至少包含一个特殊字符，例如与号 (&)、井号 (#) 和百分号 (%) 	-	
vCenter Single Sign On 域管理员用户的密码	-	
加入或不加入 VMware 客户体验提升计划 (CEIP) 有关 CEIP 的信息，请参见《vCenter Server 和主机管理》中的“配置客户体验提升计划”一节。	加入 CEIP	

使用 GUI 部署 vCenter Server Appliance

可以使用 GUI 安装程序以交互方式部署 vCenter Server Appliance。必须从位于要部署设备的网络中的 Windows、Linux 或 Mac 计算机执行 GUI 部署。

图 2-3. vCenter Server 设备的部署 workflow



前提条件

- 请参见部署 vCenter Server Appliance 的必备条件。
- 请参见部署 vCenter Server Appliance 所需的信息。

步骤

1 第 1 阶段 – 部署 OVA 文件作为 vCenter Server 设备

在部署过程的第 1 阶段，您应部署包含在 vCenter Server 安装程序中的 OVA 文件作为 vCenter Server 设备。

2 阶段 2 – 设置新部署的 vCenter Server 设备

OVA 部署完成后，您应继续执行部署过程的第 2 阶段，以设置并启动新部署的 vCenter Server 设备的服务。

第 1 阶段 – 部署 OVA 文件作为 vCenter Server 设备

在部署过程的第 1 阶段，您应部署包含在 vCenter Server 安装程序中的 OVA 文件作为 vCenter Server 设备。

步骤

- 1 在 vCenter Server 安装程序中，导航到 `vcasa-ui-installer` 目录，转至所用操作系统的子目录，然后运行安装程序可执行文件。
 - 对于 Windows 操作系统，转至 `win32` 子目录，并运行 `installer.exe` 文件。

- 对于 Linux 操作系统，转至 `lin64` 子目录，并运行 `installer` 文件。
 - 对于 Mac 操作系统，转至 `mac` 子目录，并运行 `Installer.app` 文件。
- 2 在主页中，单击**安装**以启动部署向导。
 - 3 查看“简介”页面，以了解部署过程，然后单击**下一步**。
 - 4 阅读并接受许可协议，然后单击**下一步**。
 - 5 连接到要部署 vCenter Server Appliance 的目标服务器。

选项	步骤
可以连接到要部署该设备的 ESXi 主机。	<ol style="list-style-type: none"> 1 输入 ESXi 主机的 FQDN 或 IP 地址。 2 输入 ESXi 主机的 HTTPS 端口。 3 输入对 ESXi 主机具有管理特权的用户的用户名和密码，例如 <code>root</code> 用户。 4 单击下一步。 5 确认证书警告显示安装在目标 ESXi 主机上的 SSL 证书的 SHA1 指纹，然后单击接受证书指纹。
可以连接到 vCenter Server 实例，并浏览清单以选择要部署该设备的 ESXi 主机或 DRS 集群。	<ol style="list-style-type: none"> 1 输入 vCenter Server 实例的 FQDN 或 IP 地址。 2 输入 vCenter Server 实例的 HTTPS 端口。 3 输入对 vCenter Server 实例具有 vCenter Single Sign-On 管理特权的用户的用户名和密码，例如 <code>administrator@your_domain_name</code> 用户。 4 单击下一步。 5 确认证书警告显示安装在目标 vCenter Server 实例上的 SSL 证书的 SHA1 指纹，然后单击接受证书指纹。 6 选择包含要部署设备的 ESXi 主机或 DRS 集群的数据中心或数据中心文件夹，然后单击下一步。 <p>注 所选择的数据中心或数据中心文件夹必须至少包含一个未处于锁定或维护模式的 ESXi 主机。</p> <ol style="list-style-type: none"> 7 选择要部署设备的 ESXi 主机或 DRS 集群，然后单击下一步。

- 6 在“设置设备虚拟机”页面上，输入 vCenter Server 设备的名称，设置 `root` 用户的密码，然后单击**下一步**。

设备名称不得包含百分号 (%)、反斜杠 (\) 或正斜杠 (/)，并且长度不得超过 80 个字符。

密码必须只包含没有空格的小写 ASCII 字符，至少八个字符，由数字、大小写字母和特殊字符（例如，感叹号 (!)、井号 (#)、@ 符号 (@) 或括号 (())）组成。

- 7 为 vSphere 清单选择 vCenter Server Appliance 的部署大小。

有关您可以选择的部署大小的信息，请参见 [vCenter Server 设备的硬件要求](#)。您选择的选项将决定 vCenter Server Appliance 的 CPU 数量和内存大小。

- 8 选择 vCenter Server Appliance 的存储大小，然后单击**下一步**。

所需存储不仅取决于 vSphere 环境的大小，还取决于磁盘置备模式。请参见 [vCenter Server 设备的存储要求](#)。

9 为将存储所有虚拟机配置文件和虚拟磁盘的 vCenter Server 设备选择存储位置。

选项	操作
安装在可从目标主机访问的现有数据存储上	从兼容数据存储列表选择一个数据存储。
安装在包含目标主机的新 vSAN 集群上	指定创建新 vSAN 集群或 vSAN Express Storage Architecture (vSAN ESA) 集群以存储 vCenter Server 设备所需的详细信息。
安装在现有 vSAN 数据存储上并声明更多磁盘	指定在 vSAN 数据存储上创建集群所需的详细信息。仅当您的环境中包含 vSAN 数据存储时，才会显示此选项。

要启用精简置备，请选择**启用精简磁盘模式**。NFS 数据存储默认为精简置备。

10 （可选）如果选择 vSAN 作为存储位置，则必须声明用于存储的磁盘。

- 对于 vSAN，请为缓存层和容量层单独声明磁盘。
- 对于 vSAN ESA，请从兼容磁盘列表中声明磁盘。

11 在“配置网络设置”页面上，设定网络设置。

设备的 IP 地址或 FQDN 将用作系统名称。建议使用 FQDN。但是，如果要使用 IP 地址，请使用设备的静态 IP 地址分配，因为 DHCP 分配的 IP 地址可能会更改。

选项	操作
网络	<p>选择要将设备连接到的网络。</p> <p>下拉菜单中显示的网络取决于目标服务器的网络设置。如果将设备直接部署在 ESXi 主机上，则非临时分布式虚拟端口组将不受支持，且不会显示在下拉菜单中。</p>
IP 版本	<p>选择设备 IP 地址的版本。</p> <p>您可以选择 IPv4 或 IPv6。</p>
IP 分配	<p>选择如何分配设备的 IP 地址。</p> <ul style="list-style-type: none"> ■ 静态 <p>向导将提示您输入 IP 地址和网络设置。</p> ■ DHCP <p>DHCP 服务器用于分配 IP 地址。只有当环境中有 DHCP 服务器时，才可选择此选项。</p> <p>如果环境中已启用 DDNS，可以输入设备的首选完全限定域名（FQDN）。</p>
常见端口	<p>您可以自定义 HTTP 和 HTTPS 端口（可选）。</p> <p>如果要指定自定义 HTTP 端口号和 HTTPS 端口号，请确保不使用已由 vCenter Server 使用的端口号，或默认 HTTP 端口 (80) 和 HTTPS 端口 (443)。</p>

12 在“即将完成第 1 阶段”页面上，检查 vCenter Server 设备的部署设置，然后单击**完成**开始 OVA 部署过程。

13 等待 OVA 部署完成，然后单击**继续**以继续执行部署过程的第 2 阶段，设置并启动新部署的设备的服

注 如果通过单击**关闭**退出向导，必须登录到 vCenter Server 管理界面以设置并启动服务。

结果

新部署的 vCenter Server 设备正在目标服务器上运行，但服务尚未启动。

阶段 2 – 设置新部署的 vCenter Server 设备

OVA 部署完成后，您应继续执行部署过程的第 2 阶段，以设置并启动新部署的 vCenter Server 设备的服务。

步骤

- 1 查看部署过程第 2 阶段的简介，然后单击**下一步**。
- 2 配置设备中的时间设置，对设备启用远程 SSH 访问（可选），然后单击**下一步**。

选项	描述
与 ESXi 主机同步时间	启用周期性时间同步，VMware Tools 会将客户机操作系统的时间设置为与 ESXi 主机的时间相同。
与 NTP 服务器同步时间	使用网络时间协议服务器来同步时间。如果选择此选项，必须以逗号分隔的格式输入 NTP 服务器的名称或 IP 地址。

- 3 创建一个新的 vCenter Single Sign-On 域或加入现有域。

选项	描述
创建新的 Single Sign-On 域	<p>创建新的 vCenter Single Sign-On 域。</p> <ol style="list-style-type: none"> 输入域名称，例如 vsphere.local。 <p>注 确保域名不包含任何大写字母。</p> <ol style="list-style-type: none"> 设置 vCenter Single Sign-On 管理员帐户的密码。 <p>这是用户 <code>administrator@your_domain_name</code> 的密码。</p> <ol style="list-style-type: none"> 确认管理员密码，然后单击下一步。
加入现有的 vCenter Single Sign-On 域	<p>将新的 vCenter Single Sign-On 服务器加入现有的 vCenter Single Sign-On 域中。您必须提供要将新 vCenter Single Sign-On 服务器加入到其中的 vCenter Single Sign-On 服务器的相关信息。</p> <ol style="list-style-type: none"> 输入要加入的 vCenter Single Sign-On 服务器的完全限定域名 (FQDN) 或 IP 地址。 输入用来与 vCenter Single Sign-On 服务器通信的 HTTPS 端口。 输入您要加入的 vCenter Single Sign-On 的域名，例如 vsphere.local。 输入 vCenter Single Sign-On 管理员帐户的密码。 单击下一步。

选择加入现有 vCenter Single Sign-On 域时，可以启用增强的链接模式功能。基础架构数据随加入的 vCenter Single Sign-On 服务器一起复制。

- 4 查看 VMware 客户体验提升计划 (CEIP) 页面，然后选择是否希望加入该计划。
- 有关 CEIP 的信息，请参见《vCenter Server 和主机管理》中的“配置客户体验提升计划”一节。
- 5 在“即将完成”页面上，查看 vCenter Server 设备的配置设置，单击**完成**，然后单击**确定**完成部署过程的第 2 个阶段并设置设备。

6 （可选）完成初始设置后，在浏览器中输入 URL https://vcenter_server_appliance_fqdn/ui 以转到 vSphere Client，并登录到 vCenter Server Appliance 中的 vCenter Server 实例，或单击 https://vcenter_server_appliance_fqdn:443 转到 vCenter Server Appliance 的“入门”页面。

7 单击**关闭**退出向导。

您将重定向到 vCenter Server Appliance 的“入门”页面。

后续步骤

您可以为 vCenter Server Appliance 配置高可用性。有关提供 vCenter Server Appliance 高可用性的信息，请参见《vSphere 可用性》。

vCenter Server Appliance 的 CLI 部署

可以使用 CLI 安装程序以静默方式在 ESXi 主机或 vCenter Server 实例上部署 vCenter Server Appliance。

CLI 部署过程包括将 vCenter Server 安装程序下载到要从中执行部署的网络虚拟机或物理服务器、准备包含部署信息的 JSON 配置文件以及运行部署命令。

此外，还可以观看有关如何使用 CLI 安装程序安装 vCenter Server Appliance 的视频。



(vCenter Server 命令行安装)

为 CLI 部署准备 JSON 配置文件

运行 CLI 安装程序部署 vCenter Server Appliance 前，必须准备包含部署规范的配置参数及其值的 JSON 文件。

vCenter Server 安装程序包含所有部署选项的 JSON 模板。有关模板的信息，请参见 [vCenter Server Appliance 的 CLI 部署的 JSON 模板](#)。

通过将值设置为适用于您的规范的 JSON 模板中的配置参数，您可以使用最少配置部署设备。可以编辑预设值、移除配置参数，并为自定义配置添加配置参数。

有关配置参数及其描述的完整列表，请导航到操作系统的安装程序子目录并运行 `vcasa-deploy install --template-help` 命令，或者参见 [部署配置参数](#)。

前提条件

- 您必须熟悉 JSON 语法。
- [下载并挂载 vCenter Server 安装程序](#)。

步骤

- 1 在 vCenter Server 安装程序中，导航到 `vcasa-cli-installer` 目录，然后打开 `templates` 子文件夹。

- 2 将 install 子文件夹中的部署模板复制到工作区。

重要说明 指向 JSON 配置文件的路径必须仅包含 ASCII 字符。扩展 ASCII 字符和非 ASCII 字符不受支持。

- 3 在文本编辑器中打开适用于您的规范的模板文件。

为确保 JSON 配置文件的语法正确无误，请使用 JSON 编辑器。

- 4 为必需的配置参数填充值，也可以输入其他参数及其值。

例如，如果要对设备的网络使用 IPv4 DHCP 分配，请在模板的 network 子部分中将 mode 参数的值更改为 dhcp，并移除用于静态分配的默认配置参数。

```
"network": {
  "ip_family": "ipv4",
  "mode": "dhcp"
},
```

重要说明 String 值（包括密码）必须仅包含 ASCII 字符。扩展 ASCII 字符和非 ASCII 字符不受支持。

要设置包含反斜杠 (\) 或引号 (") 字符的值，必须在该字符之前附加反斜杠 (\) 字符。例

如，"password": "my\"password" 可设置密码 my"password，"image": "G:\\vcsa\\VMware-vCenter-Server-Appliance-8.0.0.XXXX-YYYYYYY_OVF10.ova" 可设置路径 G:\vcsa\VMware-vCenter-Server-Appliance-8.0.0.XXXX-YYYYYYY_OVF10.ova。

Boolean 值必须仅包含小写字母，也就是说，值可以是 true 或 false。例

如，"ssh_enable": false。

-
- 5 （可选）使用所选 JSON 编辑器验证 JSON 文件。

- 6 以 UTF-8 格式保存并关闭文件。

后续步骤

您可以根据部署规范的需要创建并保存其他模板。

vCenter Server Appliance 的 CLI 部署的 JSON 模板

vCenter Server 安装程序包含 JSON 模板，这些模板具有所有部署选项的最低配置参数。这些模板位于 vcsa-cli-installer/templates/install 目录中。

每个部署选项都有一个模板用于在 ESXi 主机上部署设备，还有一个模板用于在 vCenter Server 实例上部署设备。

表 2-5. vCenter Server 安装程序中包含的部署 JSON 模板

模板	描述
embedded_vCSA_on_ESXi.json	包含在 ESXi 主机上部署 vCenter Server Appliance 所需的最低配置参数。
vCSA_with_cluster_on_ESXi.json	包含在 ESXi 主机上部署 vCenter Server Appliance 以及单节点 vSAN 和 vLCM 管理的集群所需的最低配置参数。
embedded_vCSA_on_VC.json	包含在 vCenter Server 实例上部署 vCenter Server Appliance 所需的最低配置参数。
embedded_vCSA_replication_on_ESXi.json	包含在 ESXi 主机上部署作为另一个嵌入式 vCenter Server 的复制合作伙伴的 vCenter Server Appliance 所需的最低配置参数。
embedded_vCSA_replication_on_VC.json	包含在 vCenter Server 实例上部署另一个 vCenter Server Appliance 的 vCenter Server Appliance 复制合作伙伴所需的最低配置参数。

部署配置参数

为 CLI 部署准备 JSON 配置文件时，必须设置参数和值，以便为 vCenter Server Appliance 部署提供输入数据。

JSON 部署文件中的配置参数的部分和子部分

用于 CLI 升级的 JSON 配置文件中的配置参数按部分和子部分进行组织。

表 2-6. JSON 部署文件中的配置参数的部分和子部分

部分	子部分	描述
new_vcsa - 描述要部署的设备	esxi	<p>仅当要直接在 ESXi 主机上部署设备时才应使用。</p> <p>包含描述目标 ESXi 主机的配置参数。</p> <p>根据是否希望在部署过程中配置 vSAN 或 vLCM 管理的集群，请参见相关部分，了解有关配置参数的详细信息。</p> <ul style="list-style-type: none"> ■ 表 2-7. 带有 vSAN 和 vLCM 管理的集群的部署的 new_vcsa 部分的 esxi 子部分中的配置参数 ■ 表 2-8. 不带 vSAN 或 vLCM 管理的集群的部署的 new_vcsa 部分的 esxi 子部分中的配置参数 <p>注 您必须填充 esxi 或 vc 子部分。</p>
	vc	<p>仅当要在 vCenter Server 实例清单上部署设备时才应使用。</p> <p>包含描述目标 ESXi 主机或 vCenter Server 清单的 DRS 集群的配置参数。请参见表 2-9. new_vcsa 部分的 vc 子部分中的配置参数。</p> <p>注 您必须填充 vc 或 esxi 子部分。</p>
	appliance	包含描述设备的配置参数。请参见表 2-10. new_vcsa 部分的 appliance 子部分中的配置参数。
	network	包含描述设备网络设置的配置参数。请参见表 2-11. new_vcsa 部分的 network 子部分中的配置参数。
	os	包含描述设备操作系统设置的配置参数。请参见表 2-12. new_vcsa 部分的 os 子部分中的配置参数。

表 2-6. JSON 部署文件中的配置参数的部分和子部分（续）

部分	子部分	描述
	sso	包含描述设备 vCenter Single Sign-On 设置的配置参数。请参见表 2-13. <code>new_vc</code> 部分的 <code>sso</code> 子部分中的配置参数。
	ovftool_arguments	用于将任意参数及其值添加到安装程序所生成的 OVF Tool 命令的可选子部分。 重要说明 vCenter Server 安装程序不会验证 <code>ovftool_arguments</code> 子部分中的配置参数。如果设置了 OVF Tool 无法识别的参数，部署可能会失败。
ceip- 描述是否加入 VMware 客户体验提升计划 (Customer Experience Improvement Program, CEIP)	settings	仅包含 <code>ceip_enabled</code> 配置参数，用来设置是否加入 VMware 客户体验提升计划 (CEIP)。请参见表 2-14. <code>ceip</code> 部分的 <code>settings</code> 子部分中的配置参数。 注 如果设置为 <code>true</code> ，则必须使用 <code>--acknowledge-ceip</code> 参数运行 CLI 部署命令。 有关 CEIP 的信息，请参见《vCenter Server 和主机管理》中的“配置客户体验提升计划”一节。

重要说明 String 值（包括密码）必须仅包含 ASCII 字符。扩展 ASCII 字符和非 ASCII 字符不受支持。

要设置包含反斜杠 (\) 或引号 (") 字符的值，必须在该字符之前附加反斜杠 (\) 字符。例如，`"password":"my\"password"` 可设置密码 `my"password`。同样，`"image":"G:\\vc\sa\VMware-vCenter-Server-Appliance-8.0.0.XXXX-YYYYYYY_OVF10.ova"` 可设置路径 `G:\vc\sa\VMware-vCenter-Server-Appliance-8.0.0.XXXX-YYYYYYY_OVF10.ova`。

Boolean 值必须仅包含小写字母。其必须为 `true` 或 `false`。例如，`"ssh_enable":false`。

new_vc 部分中的配置参数

表 2-7. 带有 vSAN 和 vLCM 管理的集群的部署的 `new_vc` 部分的 `esxi` 子部分中的配置参数

名称	类型	描述
hostname	string	要在上面部署设备的目标 ESXi 主机的 IP 地址或 FQDN。
username	string	对目标 ESXi 主机具有管理特权的用户名，例如 <code>root</code> 。
password	string	对目标 ESXi 主机具有管理特权的用户的密码。
deployment_network	string	要将设备连接到的网络的名称。 注 该网络必须可从目标 ESXi 主机进行访问。 如果目标 ESXi 主机仅具有一个网络，则忽略此参数。
datacenter	string	要创建的特定数据中心。
cluster	string	vSAN 或 vLCM 管理的集群的名称。
compression_only	布尔	将此值设置为 <code>true</code> 可在 vSAN 集群上启用压缩。如果此参数设置为 <code>true</code> ，则 <code>deduplication_and_compression</code> 参数必须设置为 <code>false</code> 。
deduplication_and_compression	布尔	将此值设置为 <code>true</code> 可在 vSAN 集群上启用压缩和去重。如果此参数设置为 <code>true</code> ，则 <code>compression_only</code> 参数必须设置为 <code>false</code> 。
cache_disk		要用于缓存的磁盘的 UUID 或规范名称的列表。仅指定 SSD。

表 2-7. 带有 vSAN 和 vLCM 管理的集群的部署的 new_vcsc 部分的 esxi 子部分中的配置参数（续）

名称	类型	描述
capacity_disk		要用于存储的磁盘的 UUID 或规范名称的列表。指定 SSD 或 HDD。
enable_vlcm	布尔	设置为 true 可创建 vLCM 管理的集群。
enable_vsan_esa	布尔	设置为 true 以创建启用了 vSAN ESA 的 vSAN 集群。vSAN Express Storage Architecture 是下一代架构，旨在充分利用高性能存储设备，从而提高性能和效率。
single_tier	数组	要添加到 vSAN 存储池的磁盘的 UUID 或规范名称列表。仅当将 enable_vsan_esa 设置为 true 时才需要。
vsan_hcl_database_path	String	本地 vSAN HCL 数据库路径。如果位于此位置的 vSAN HCL 数据库过期，安装程序将下载最新版本并用其替换旧版本。仅当将 enable_vsan_esa 设置为 true 时才需要。
datastore	string	要在其中存储设备的配置文件和虚拟磁盘的数据存储的名称。 注 该数据存储必须可从 ESXi 主机进行访问。 如果使用的是精简磁盘模式，则数据存储大小至少应为 25 GB。
port	integer	目标 ESXi 主机的 HTTPS 反向代理端口。 默认端口为 443。仅当目标 ESXi 主机使用自定义 HTTPS 反向代理端口时才应使用。

表 2-8. 不带 vSAN 或 vLCM 管理的集群的部署的 new_vcsc 部分的 esxi 子部分中的配置参数

名称	类型	描述
hostname	string	要在上面部署设备的目标 ESXi 主机的 IP 地址或 FQDN。
username	string	对目标 ESXi 主机具有管理特权的用户名，例如 root。
password	string	对目标 ESXi 主机具有管理特权的用户的密码。
deployment_network	string	要将设备连接到的网络的名称。 注 该网络必须可从目标 ESXi 主机进行访问。 如果目标 ESXi 主机仅具有一个网络，则忽略此参数。
datastore	string	要在其中存储设备的配置文件和虚拟磁盘的数据存储的名称。 注 该数据存储必须可从 ESXi 主机进行访问。 如果使用的是精简磁盘模式，则数据存储大小至少应为 25 GB。
port	integer	目标 ESXi 主机的 HTTPS 反向代理端口。 默认端口为 443。仅当目标 ESXi 主机使用自定义 HTTPS 反向代理端口时才应使用。

表 2-9. new_vcsc 部分的 vc 子部分中的配置参数

名称	类型	描述
hostname	string	要在上面部署设备的目标 vCenter Server 实例的 IP 地址或 FQDN。
username	string	目标 vCenter Server 实例上的 vCenter Single Sign-On 管理员用户名，例如 administrator@vsphere.local。

表 2-9. new_vcsa 部分的 vc 子部分中的配置参数（续）

名称	类型	描述
password	string	目标 vCenter Server 实例上的 vCenter Single Sign-On 管理员用户的密码。
deployment_network	string	<p>要将设备连接到的网络的名称。</p> <p>注 必须可从要在其中部署设备的目标 ESXi 主机或 DRS 集群访问该网络。</p> <p>如果目标 ESXi 主机或 DRS 集群只有一个网络，则忽略此参数。</p>
datacenter	array	<p>包含要在其中部署设备的目标 ESXi 主机或 DRS 集群的 vCenter Server 数据中心。如果数据中心位于文件夹或文件夹结构中，则将值指定为逗号分隔的字符串列表。例如，</p> <pre>["parent_folder", "child_folder", "datacenter_name"]</pre> <p>注 值区分大小写。</p>
datastore	string	<p>要在其中存储设备的配置文件和虚拟磁盘的数据存储的名称。</p> <p>注 该数据存储必须可从目标 ESXi 主机或 DRS 集群进行访问。</p> <p>该数据存储必须具有至少 25 GB 的可用空间。</p>
port	integer	<p>目标 vCenter Server 实例的 HTTPS 反向代理端口。</p> <p>默认端口为 443。仅当目标 vCenter Server 实例使用自定义 HTTPS 反向代理端口时才应使用。</p>
target	array	<p>要在其中部署设备的目标 ESXi 主机或 DRS 集群。</p> <p>重要说明 必须提供 vCenter Server 清单中显示的名称。例如，如果目标 ESXi 主机的名称是 vCenter Server 清单中的一个 IP 地址，则不能提供 FQDN。</p> <p>如果目标 ESXi 主机或 DRS 集群位于文件夹或文件夹结构中，则将值指定为逗号分隔的字符串列表。例如，</p> <pre>["parent_folder", "child_folder", "esxi-host.domain.com"]</pre> <p>如果目标 ESXi 主机是集群的一部分，请将路径指定为逗号分隔的字符串列表。例如，</p> <pre>["cluster_name", "esxi-host.domain.com"]</pre> <p>注 值区分大小写。</p>
vm_folder	string	可选。部署设备的虚拟机文件夹的名称。

表 2-10. new_vcsa 部分的 appliance 子部分中的配置参数

名称	类型	描述
thin_disk_mode	Boolean	设置为 true 可部署具有精简虚拟磁盘的设备。
deployment_option	string	<p>设备的大小。</p> <ul style="list-style-type: none"> ■ 如果要为具有默认存储大小的最多 10 个主机和 100 个虚拟机部署 vCenter Server Appliance，请设置为 tiny。 部署具有 2 个 CPU、12 GB 内存和 315 GB 存储的设备。 ■ 如果要为具有大型存储大小的最多 10 个主机和 100 个虚拟机部署 vCenter Server Appliance，请设置为 tiny-lstorage。 部署具有 2 个 CPU、12 GB 内存和 1390 GB 存储的设备。 ■ 如果要为具有超大型存储大小的最多 10 个主机和 100 个虚拟机部署 vCenter Server Appliance，请设置为 tiny-xlstorage。 部署具有 2 个 CPU、12 GB 内存和 3145 GB 存储的设备。 ■ 如果要为具有默认存储大小的最多 100 个主机和 1,000 个虚拟机部署 vCenter Server Appliance，请设置为 small。 部署具有 4 个 CPU、19 GB 内存和 380 GB 存储的设备。 ■ 如果要为具有大型存储大小的最多 100 个主机和 1,000 个虚拟机部署 vCenter Server Appliance，请设置为 small-lstorage。 部署具有 4 个 CPU、19 GB 内存和 1435 GB 存储的设备。 ■ 如果要为具有超大型存储大小的最多 100 个主机和 1,000 个虚拟机部署 vCenter Server Appliance，请设置为 small-xlstorage。 部署具有 4 个 CPU、19 GB 内存和 3195 GB 存储的设备。 ■ 如果要为具有默认存储大小的最多 400 个主机和 4,000 个虚拟机部署 vCenter Server Appliance，请设置为 medium。 部署具有 8 个 CPU、28 GB 内存和 600 GB 存储的设备。 ■ 如果要为具有大型存储大小的最多 400 个主机和 4,000 个虚拟机部署 vCenter Server Appliance，请设置为 medium-lstorage。 部署具有 8 个 CPU、28 GB 内存和 1600 GB 存储的设备。 ■ 如果要为具有超大型存储大小的最多 400 个主机和 4,000 个虚拟机部署 vCenter Server Appliance，请设置为 medium-xlstorage。 部署具有 8 个 CPU、28 GB 内存和 3360 GB 存储的设备。 ■ 如果要为具有默认存储大小的最多 1,000 个主机和 10,000 个虚拟机部署 vCenter Server Appliance，请设置为 large。 部署具有 16 个 CPU、37 GB 内存和 965 GB 存储的设备。 ■ 如果要为最多 1,000 个主机和 10,000 个虚拟机（具有大型存储大小）部署 vCenter Server，则设置为 large-lstorage。 部署具有 16 个 CPU、37 GB 内存和 1665 GB 存储的设备。 ■ 如果要为具有超大型存储大小的最多 1,000 个主机和 10,000 个虚拟机部署 vCenter Server Appliance，请设置为 large-xlstorage。 部署具有 16 个 CPU、37 GB 内存和 3425 GB 存储的设备。 ■ 如果要为具有默认存储大小的最多 2,000 个主机和 35,000 个虚拟机部署 vCenter Server Appliance，请设置为 xlarge。 部署具有 24 个 CPU、56 GB 内存和 1705 GB 存储的设备。

表 2-10. new_vcsa 部分的 appliance 子部分中的配置参数（续）

名称	类型	描述
		<ul style="list-style-type: none"> ■ 如果要为具有大型存储大小的最多 2,000 个主机和 35,000 个虚拟机部署 vCenter Server Appliance，请设置为 <code>xlarge-1storage</code>。 部署具有 24 个 CPU、56 GB 内存和 1805 GB 存储的设备。 ■ 如果要为具有超大型存储大小的最多 2,000 个主机和 35,000 个虚拟机部署 vCenter Server Appliance，请设置为 <code>xlarge-x1storage</code>。 部署具有 24 个 CPU、56 GB 内存和 3565 GB 存储的设备。
<code>image</code>	<code>string</code>	可选。vCenter Server Appliance 安装软件包的本地文件路径或 URL。 默认情况下，安装程序使用包含于 ISO 文件中的安装包，该文件位于 <code>vcsa</code> 文件夹中。
<code>name</code>	<code>string</code>	设备的虚拟机名称。 必须仅包含除百分号 (%)、反斜杠 (\) 或正斜杠 (/) 以外的 ASCII 字符，并且长度不能超过 80 个字符。
<code>ovftool_path</code>	<code>string</code>	可选。指向 OVF Tool 可执行文件的本地文件路径。 默认情况下，安装程序使用包含于 ISO 文件中的 OVF Tool 实例，该文件位于 <code>vcsa/ovftool</code> 文件夹中。

表 2-11. new_vcsa 部分的 network 子部分中的配置参数

名称	类型	描述
<code>ip_family</code>	<code>string</code>	设备的网络 IP 版本。 请设置为 <code>ipv4</code> 或 <code>ipv6</code> 。
<code>mode</code>	<code>string</code>	设备的网络 IP 分配。 请设置为 <code>static</code> 或 <code>dhcp</code> 。
<code>ip</code>	<code>string</code>	设备的 IP 地址。 仅当使用静态分配（也就是将 <code>mode</code> 参数设置为 <code>static</code> ）时才需要。 必须设置与网络 IP 版本对应的 IPv4 或 IPv6 地址，也就是设置为 <code>ip.family</code> 参数的值。 IPv4 地址必须符合 RFC 790 准则。 IPv6 地址必须符合 RFC 2373 准则。
<code>dns_servers</code>	<code>string</code> 或 <code>array</code>	<p>一个或多个 DNS 服务器的 IP 地址。</p> <p>要设置多个 DNS 服务器，请使用逗号分隔的字符串列表或作为单个字符串的逗号分隔列表来提供路径。例如，</p> <pre>["x.y.z.a", "x.y.z.b"]</pre> <p>或</p> <pre>"x.y.z.a, x.y.z.b"</pre> <p>当 <code>mode</code> 参数设置为 <code>static</code> 时为可选。当 <code>mode</code> 设置为 <code>DHCP</code> 时不受支持。</p>

表 2-11. new_vcsa 部分的 network 子部分中的配置参数（续）

名称	类型	描述
prefix	string	<p>网络前缀长度。</p> <p>仅当 mode 参数设置为 static 时才应使用。当 mode 参数设置为 dhcp 时移除。</p> <p>网络前缀长度是在子网掩码中设置的位数。例如，如果子网掩码为 255.255.255.0，则二进制版本的前缀长度中有 24 位，因此网络前缀长度为 24。</p> <p>对于 IPv4 版本，值必须介于 0 到 32 之间。</p> <p>对于 IPv6 版本，值必须介于 0 到 128 之间。</p>
gateway	string	<p>默认网关的 IP 地址。</p> <p>对于 IPv6 版本，值可以是 default。</p>
ports	string	<p>可选。vCenter Server Appliance 用于直接 HTTP 连接的端口号。默认情况下，端口 80 会将请求重定向到 HTTPS 端口 443。您可以自定义 vCenter Server HTTP 端口和 HTTPS 端口。如果要指定自定义 HTTP 端口号和 HTTPS 端口号，请确保不使用已由 vCenter Server 使用的端口，或默认 HTTP 端口 (80) 和 HTTPS 端口 (443)。</p> <p>用于指定自定义端口的选项为："rhttpproxy.ext.port1":"port_number"（用于 HTTP 端口）和 "rhttpproxy.ext.port2":"port_number"（用于 HTTPS 端口）。</p> <p>以下示例将端口 81 和 444 分别指定为 HTTP 端口和 HTTPS 端口：</p> <pre>ports: {"rhttpproxy.ext.port1":"81", "rhttpproxy.ext.port2":"444"}</pre> <p>有关 vCenter Server 使用的端口的详细信息，请参见 vCenter Server 的所需端口。</p>
system_name	string	<p>主网络标识。</p> <p>可以是 IP 地址或 FQDN，首选是 FQDN。</p> <p>部署后将无法更改此参数的值。</p> <p>FQDN 和用点分隔的十进制数字必须符合 RFC 1123 准则。</p>

表 2-12. new_vcsa 部分的 os 子部分中的配置参数

名称	类型	描述
password	string	<p>设备操作系统的 root 用户的密码。</p> <p>该密码必须包含 8 到 20 个字符，至少一个大写字母、一个小写字母、一个数字和一个特殊字符，例如美元符号 (\$)、井号 (#)、@ 符号 (@)、句点 (.) 或感叹号 (!)。所有字符必须是没有空格的小写 ASCII 字符。</p>
ntp_servers	string 或 array	<p>可选。一个或多个要进行时间同步的 NTP 服务器的主机名或 IP 地址。</p> <p>要设置多个 NTP 服务器，请使用逗号分隔的字符串列表或作为单个字符串的逗号分隔列表来提供路径。例如，</p> <pre>["x.y.z.a", "x.y.z.b"]</pre> <p>或</p> <pre>"x.y.z.a, x.y.z.b"</pre>

表 2-12. new_vcsa 部分的 os 子部分中的配置参数（续）

名称	类型	描述
ssh_enable	Boolean	<p>设置为 true 可在设备上启用 SSH 管理员登录。</p> <p>注 vCenter Server Appliance 高可用性需要对设备进行远程 SSH 访问。</p>
time_tools_sync	Boolean	<p>可选。设置为 true 可使用 VMware Tools 时间同步部署设备。VMware Tools 会将设备的时间与 ESxi 主机的时间同步。</p> <p>如果设置 NTP 服务器进行时间同步，也就是说，如果设置 ntp.servers 参数，则忽略此参数。</p>

表 2-13. new_vcsa 部分的 sso 子部分中的配置参数

名称	类型	描述
password	string	<p>vCenter Single Sign-On 管理员用户 administrator@your_domain_name 的密码。</p> <p>如果要部署 vCenter Server Appliance 部署为新 vCenter Single Sign-On 域中的第一个实例，则必须为 vCenter Single Sign-On 管理员用户设置密码。</p> <p>该密码必须包含 8 到 20 个字符，至少一个大写字母、一个小写字母、一个数字和一个特殊字符，例如美元符号 (\$)、井号 (#)、@ 符号 (@)、句点 (.) 或感叹号 (!)。所有字符必须是 ASCII 字符。</p>
domain_name	string	<p>vCenter Single Sign-On 域名，例如 vsphere.local。</p> <p>如果要部署 vCenter Server Appliance 部署为新 vCenter Single Sign-On 域中的第一个实例，则必须为新 vCenter Single Sign-On 域设置名称。</p>
replication_partner_hostname	string	<p>合作伙伴 vCenter Server 的系统名称。</p> <p>仅当在现有的 vCenter Single Sign-On 域中部署复制合作伙伴时才需要。</p>
sso_port	integer	<p>合作伙伴 vCenter Server 的 HTTPS 反向代理端口。</p> <p>默认端口为 443。仅当合作伙伴使用自定义 HTTPS 反向代理端口时才使用。</p>

ceip 部分中的配置参数

表 2-14. ceip 部分的 settings 子部分中的配置参数

名称	类型	描述
ceip_enabled	Boolean	设置为 true 可加入此设备的 CEIP。

CLI 部署命令的语法

可以使用命令实参来设置部署命令的执行形参。

可以向 CLI 部署命令添加用空格分隔的参数列表。

```
vcsa-deploy install path_to_the_json_filelist_of_arguments
```

参数	描述
--accept-eula	接受最终用户许可协议。 此参数对执行部署命令是必需的。
--acknowledge-ceip	确认您要加入 VMware 客户体验改善计划 (CEIP)。 在 JSON 部署模板中将 ceip.enabled 参数设置为 true 时，此参数是必需的。
-v, --verbose	将调试信息添加到控制台输出。
-t, --terse	隐藏控制台输出。仅显示警告消息和错误消息。
--log-dir <i>LOG_DIR</i>	设置日志文件和其他输出文件的位置。
--skip-ovftool-verification	对 JSON 文件中的配置参数执行基本验证并部署设备。不对 OVF Tool 参数执行验证。
--no-esx-ssl-verify	跳过 ESXi 连接的 SSL 验证。 重要说明 请避免使用此选项，因为此选项可能会导致在部署期间或部署后出现问题，因为未验证目标 ESXi 主机的标识。
--no-ssl-certificate-verification	跳过所有服务器连接的安全证书验证。
--operation-id <i>OPERATION_ID</i>	提供用于跟踪安装活动的操作 ID。
--pause-on-warnings	暂停并等待对警告进行确认。
--verify-template-only	对 JSON 文件中的配置参数执行基本模板验证。不部署设备。
--precheck-only	仅执行基本模板验证和 OVF Tool 参数验证。不部署设备。
--sso-ssl-thumbprint <i>SSL-SHA1-THUMBPRINT</i>	根据提供的 SHA1 指纹验证服务器证书。
-h, --help	显示 vcsa-deploy install 命令的帮助消息。
--template-help	显示有关 JSON 部署文件中的配置参数用法的帮助消息。

执行完成后，您可以获取命令的退出代码。

退出代码	描述
0	命令已成功运行
1	运行时错误
2	验证错误
3	模板错误

使用 CLI 部署 vCenter Server Appliance

可以使用 CLI 安装程序以无需人工干预的方式部署 vCenter Server Appliance。必须从位于要部署设备的网络中的 Windows、Linux 或 Mac 计算机执行 CLI 部署。

前提条件

- 请参见部署 vCenter Server Appliance 的必备条件。

- 为 CLI 部署准备 JSON 配置文件。
- 请查看 CLI 部署命令的语法。
- 确认用来登录客户机的用户名、vCenter Server 安装程序的路径、JSON 配置文件的路径和 JSON 配置文件中的字符串值仅包含 ASCII 字符。扩展 ASCII 字符和非 ASCII 字符不受支持。
- 需要安装 Visual C++ 可再发行库版本 14.0 或更高版本才能在低于 Windows 10 的 Windows 版本上运行此实用程序。这些库的 Microsoft 安装程序位于 `vcsa\ovftool\win32\vcredist` 目录中。

步骤

- 1 导航到操作系统的 `vcsa-cli-installer` 子目录。
 - 如果在 Windows 操作系统中运行部署，则导航到 `vcsa-cli-installer\win32` 目录。
 - 如果在 Linux 操作系统中运行部署，则导航到 `vcsa-cli-installer/lin64` 目录。
 - 如果在 Mac 操作系统中运行部署，则导航到 `vcsa-cli-installer/mac` 目录。
- 2 （可选）在没有部署设备的情况下运行部署前检查，确认已正确准备部署模板。

```
vcsa-deploy install --precheck-only path_to_the_json_file
```

- 3 运行部署命令。

```
vcsa-deploy install --accept-eula --acknowledge-ceip optional_arguments
path_to_the_json_file
```

可以使用 *optional_arguments* 输入用空格分隔的实参，以设置部署命令的其他执行形参。例如，您可以设置安装程序所生成的日志文件和其他输出文件的位置。

```
vcsa-deploy install --accept-eula --acknowledge-ceip --log-dir=path_to_the_location
path_to_the_json_file
```

使用 CLI 部署多个 vCenter Server Appliance

可以使用 CLI 安装程序同时（以批量模式）部署 vCenter Server Appliance 的多个实例。

要同时部署多个实例，请为部署中的所有 vCenter Server 实例创建 JSON 模板。CLI 安装程序会使用这些 JSON 模板评估部署的拓扑并确定顺序。因此，部署中彼此依赖的所有 vCenter Server 实例的 JSON 模板必须使用静态 IP 地址。

重要说明 每个设备的 JSON 模板必须使用静态 IP 地址来解析部署中该设备依赖的其他设备的网络地址。

要执行批量部署，请将定义部署的 JSON 模板放在单个目录中。调用 CLI 安装程序时，它会使用 JSON 模板中定义的拓扑来部署现有部署。

步骤

- 1 在您的工作区中，创建用于存放批量部署的 JSON 文件的文件夹。例如，`MyWorkspace/BatchDeploy`。

- 2 准备每个 JSON 配置文件，并将文件复制到批量部署文件夹。有关配置 JSON 文件的说明，请参见[为 CLI 部署准备 JSON 配置文件](#)。
- 3 导航到操作系统的 `vcsa-cli-installer` 子目录。
 - 如果在 Windows 操作系统中运行部署，则导航到 `vcsa-cli-installer\win32` 目录。
 - 如果在 Linux 操作系统中运行部署，则导航到 `vcsa-cli-installer/lin64` 目录。
 - 如果在 Mac 操作系统中运行部署，则导航到 `vcsa-cli-installer/mac` 目录。
- 4 （可选） 在没有部署设备的情况下运行部署前检查，确认已正确准备部署模板。例如：

```
vcsa-deploy install --precheck-only MyWorkspace/BatchDeploy
```

- 5 运行部署命令。例如，

```
vcsa-deploy install --accept-eula --acknowledge-ceip optional_arguments MyWorkspace/  
BatchDeploy
```

可以使用 *optional_arguments* 输入用空格分隔的实参，以设置部署命令的其他执行形参。

例如，您可以设置安装程序所生成的日志文件和其他输出文件的位置。

```
vcsa-deploy install --accept-eula --acknowledge-ceip --log-dir=path_to_the_location  
MyWorkspace/BatchDeploy
```

vCenter Server 的基于文件的备份和还原

3

vCenter Server 支持基于文件的备份和还原机制，这有助于在出现故障后恢复环境。

您可以使用 vCenter Server 界面创建 vCenter Server 的基于文件的备份。创建备份后，可以使用设备的 GUI 安装程序进行还原。

可使用 vCenter Server 界面执行 vCenter Server 核心配置、清单和所选历史数据的基于文件的备份。已备份的数据通过 FTP、FTPS、HTTP、HTTPS、SFTP、NFS 或 SMB 流式传输到远程系统。备份不会存储在 vCenter Server 上。

您只能对之前使用 vCenter Server 界面备份的 vCenter Server 执行基于文件的还原。可以使用 vCenter Server Appliance 的 GUI 安装程序执行此类还原操作。该过程包括部署新的 vCenter Server Appliance，以及将数据从基于文件的备份复制到新设备。

重要说明 如果备份 vCenter Server 高可用性集群，备份操作将仅备份主要的 vCenter Server 实例。在还原 vCenter Server 高可用性集群之前，必须关闭主动节点、被动节点和见证节点的电源。还原操作将以非 vCenter Server 高可用性模式还原 vCenter Server。还原操作成功完成后，必须重新构建集群。

本章讨论了以下主题：

- 基于文件的备份和还原的注意事项和限制
- 调度基于文件的备份
- 使用 vCenter Server 管理界面手动备份 vCenter Server
- 从基于文件的备份还原 vCenter Server

基于文件的备份和还原的注意事项和限制

当您备份或还原 vCenter Server 环境时，请考虑以下注意事项和限制。

协议

以下注意事项适用于基于文件的备份和还原协议：

- FTP 和 HTTP 不是安全协议
- 备份服务器必须支持每个 vCenter Server 至少同时具有 10 个连接
- 必须具有写入权限以执行上载操作，且必须具有读取权限以执行下载操作

- FTPS 仅支持显式模式
- 如果使用 HTTP 或 HTTPS，则必须在备份 Web 服务器上启用 WebDAV
- 只能使用 FTP、FTPS、HTTP 或 HTTPS 通过 HTTP 代理服务器传输数据
- 可以在 vCenter Server 基于文件的备份和还原中使用 IPv4 和 IPv6 URL。不支持在备份服务器和 vCenter Server 之间使用混合模式的 IP 版本。

配置

还原后，以下配置将恢复到执行备份时的状态。

- 虚拟机资源设置
- 资源池层次结构和设置
- 集群-主机成员资格
- DRS 配置和规则

Storage DRS

如果配置发生更改，则还原后以下内容可能会更改。

- 数据存储集群配置
- 数据存储集群成员资格
- 数据存储 I/O 资源管理 (Storage I/O Control) 设置
- 数据存储-数据中心成员资格
- 主机-数据存储成员资格

分布式电源管理

如果在备份后将主机置于待机模式，则还原备份时 vCenter Server 可能会强制主机退出待机模式。

分布式虚拟交换机

如果您使用的是分布式虚拟交换机，建议在还原到备份之前单独导出分布式虚拟交换机配置。您可以在还原后导入该配置。如果忽略此注意事项，您可能会丢失在备份之后对分布式虚拟交换机所做的更改。有关详细步骤，请参见位于 <http://kb.vmware.com/kb/2034602> 的 VMware 知识库文章。

内容库

如果在备份后删除库或项目，则无法在还原后访问或使用这些库或项目。只能删除此类库或项目。系统将显示一条警告消息，通知您存储备份中缺少文件或文件夹。

如果在备份后创建新项目或项目文件，在还原操作后，Content Library Service 中没有新项目或文件的记录。系统将显示一条警告，通知您在存储备份中发现了额外的文件夹或文件。

如果在备份后创建新库，在还原后，Content Library Service 中没有新库的记录。库内容存在于存储备份中，但系统不显示警告。您必须手动清理新库。

虚拟机生命周期操作

- 从在 vCenter Server 实例中执行正在进行的重新定位操作过程中获得的备份还原 vCenter Server

还原 vCenter Server 后，虚拟机的 vCenter Server 视图与虚拟机的 ESXi 视图可能不同步。如果在 vCenter Server 上执行正在进行的操作过程中进行备份，也会产生此类状况。如果还原 vCenter Server 后虚拟机消失，您可以参考以下几种情况。

- 缺少的虚拟机位于目标 ESXi 主机中，并且已向目标 ESXi 主机注册，但它是孤立的，或者不在 vCenter Server 清单中。您必须手动将虚拟机添加到 vCenter Server 清单中。
- 缺少的虚拟机位于目标 ESXi 主机中，但未向目标 ESXi 主机注册，并且不在 vCenter Server 清单中。必须手动将虚拟机注册到 ESXi 主机，并将虚拟机重新添加到 vCenter Server 清单中。
- 缺少的虚拟机位于目标 ESXi 主机中，但未向目标 ESXi 主机注册。在 vCenter Server 实例中，缺少的虚拟机标记为孤立。必须从 vCenter Server 清单中移除虚拟机，然后重新添加。

- 从具有过期链接克隆虚拟机布局的备份还原 vCenter Server。

如果在备份后创建链接克隆虚拟机并从旧备份还原 vCenter Server，那么还原后，vCenter Server 不会识别新的链接克隆虚拟机，直至 vCenter Server 发现新的链接克隆虚拟机。如果在发现新的链接克隆虚拟机之前移除所有现有虚拟机，则移除现有虚拟机操作会因缺少磁盘而损坏新的链接克隆。为了避免这种情况，必须等待 vCenter Server 发现所有链接克隆虚拟机，才能移除虚拟机。

- 从虚拟机注册期间执行的备份还原 vCenter Server。

如果在备份期间注册虚拟机并从旧备份还原 vCenter Server，则在还原后，虚拟机在 vCenter Server 实例中被标记为孤立。您必须手动将虚拟机添加到 vCenter Server 清单中。

vSphere High Availability

从备份还原 vCenter Server 可能导致其回滚到早期版本的 vSphere HA 集群状态（主机列表、集群配置、虚拟机保护状态），而集群中的主机为最新版本的集群状态。需要确保在还原和备份操作期间 vSphere HA 集群状态保持不变。否则，可能出现以下问题。

- 如果备份后且还原 vCenter Server 之前，在 vSphere HA 集群中添加、移除主机，则虚拟机可能会故障切换到 HA 集群中非 vCenter Server 管理的主机。
- 新虚拟机的保护状态不会在 vSphere HA 集群中主机的 vSphere HA 代理中更新。因此，虚拟机不会受到保护或处于未保护状态。
- 新集群配置状态不会在 vSphere HA 集群中主机的 vSphere HA 代理中更新。

vCenter High Availability

还原 vCenter Server 需要重新配置 vCenter HA。

基于存储策略的管理

从备份还原 vCenter Server 会导致出现以下与存储策略、存储提供程序和虚拟机相关的不一致。

- 备份后注册的存储提供程序会丢失。
- 备份后取消注册的存储提供程序重新出现，并且可能显示不同的提供程序状态。

- 备份后对存储策略执行的更改（如创建、删除或更新）会丢失。
- 备份后对存储策略组件执行的更改（如创建、删除或更新）会丢失。
- 备份后对数据存储执行的默认策略配置更改会丢失。
- 虚拟机及其磁盘的存储策略关联以及它们的策略合规性可能发生更改。

虚拟存储区域网络

从备份还原 vCenter Server 可能会导致 vSAN 出现不一致。有关如何检查 vSAN 运行状况的信息，请参见《《管理 VMware vSAN》》。

修补

从备份还原 vCenter Server 可能导致缺少安全修补程序。在还原完成后，必须再次应用修补程序。有关修补 vCenter Server 的信息，请参见《《vSphere 升级》》。

调度基于文件的备份

您可以为 vSphere 6.7 及更高版本调度基于文件的备份。您可以设置用于执行定期备份的调度。

可以使用有关备份位置、重复周期和保留的信息来设置备份的调度。

一次只能设置一个调度。

前提条件

- 必须确保 FTP、FTPS、HTTP、HTTPS、SFTP、NFS 或 SMB 服务器启动并正在运行，而且具有足够的磁盘空间用于存储备份。

步骤

- 1 在 Web 浏览器中，转至 vCenter Server 管理界面，<https://appliance-IP-address-or-FQDN:5480>。
- 2 以 root 用户身份登录。
- 3 在 vCenter Server 管理界面中，单击**备份**。
- 4 单击**配置**以设置备份调度。
- 5 输入备份位置详细信息。

选项	描述
备份位置	<p>输入备份位置，包括要用于连接到备份服务器的协议、端口、服务器地址和用于存储备份文件的备份文件夹。</p> <p>使用以下协议之一：FTP、FTPS、HTTP、HTTPS、SFTP、NFS 或 SMB。</p> <p>对于 FTP、FTPS、HTTP 或 HTTPS，路径对于为服务配置的主目录而言是相对的。</p>
备份服务器凭据	输入对备份服务器具有 写入 特权的用户的用户名和密码。

6 设置备份的调度重复周期和时间。

可以将重复周期设置为每日或每周，或者也可以将调度自定义为在一周中特定的一天或多天运行。可以将备份指定为在一天中的特定时间运行。默认时间为 11:59pm。

7 （可选） 如果要对备份文件进行加密，请输入加密密码。

如果您选择加密备份数据，则必须对还原过程使用加密密码。

8 选择保留所有备份，或者输入要保留的备份数量。

保留信息指定了要为给定 vCenter Server 保留的备份数量。

9 （可选） 选择统计信息、事件和任务以从数据库备份其他历史数据。**10 单击创建。**

备份调度信息会填充到“备份”页面。

结果

已完成的和正在进行的备份会在“活动”下列出。

后续步骤

通过从“立即备份”对话框上的备份调度中选择使用备份调度中的备份位置和用户名，可以使用现有调度信息执行立即备份。

使用 vCenter Server 管理界面手动备份 vCenter Server

您可以使用 vCenter Server 管理界面备份 vCenter Server 实例。可以选择是否在备份文件中包括历史数据，如统计信息、事件和任务。

注 vCenter High Availability 集群的备份操作仅备份主动节点。

前提条件

- 必须确保 FTP、FTPS、HTTP、HTTPS、SFTP、NFS 或 SMB 服务器启动并正在运行，而且具有足够的磁盘空间用于存储备份。

步骤

- 1 在 Web 浏览器中，转至 vCenter Server 管理界面，<https://appliance-IP-address-or-FQDN:5480>。
- 2 以 root 用户身份登录。
- 3 在 vCenter Server 管理界面中，单击**备份**。
“活动”下的表将显示已创建的最新版本 vCenter Server 备份。
- 4 单击**立即备份**。
将打开**备份设备**向导。
- 5 （可选） 选择**使用备份调度中的备份位置和用户名**可使用已调度备份中的信息。

6 输入备份位置详细信息。

选项	描述
备份位置	<p>输入备份位置，包括要用于连接到备份服务器的协议、端口、服务器地址和用于存储备份文件的备份文件夹。</p> <p>使用以下协议之一：FTP、FTPS、HTTP、HTTPS、SFTP、NFS 或 SMB。</p> <p>对于 FTP、FTPS、HTTP 或 HTTPS，路径对于为服务配置的主目录而言是相对的。</p>
备份服务器凭据	<p>输入对备份服务器具有写入特权的用户的用户名和密码。</p> <p>注 用户名和密码应仅包含 ASCII 字符。</p>

7 （可选）如果要对备份文件进行加密，请输入加密密码。

如果您选择加密备份数据，则必须对还原过程使用加密密码。

8 （可选）选择统计信息、事件和任务以从数据库备份其他历史数据。

9 （可选）在描述文本框中，输入备份的描述。

10 单击开始以开始备份过程。

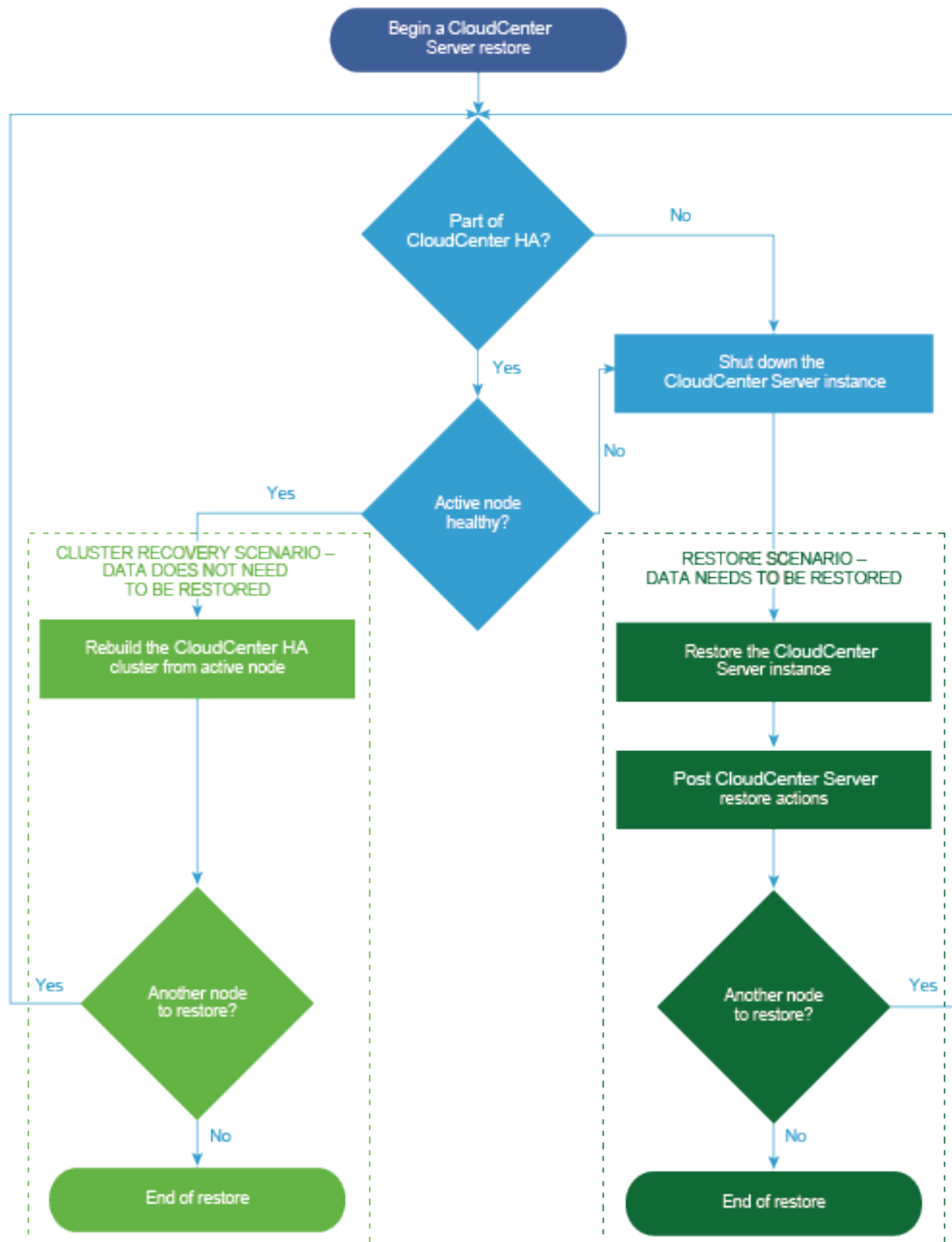
结果

已完成的和正在进行的备份会在“活动”下列出。

从基于文件的备份还原 vCenter Server

您可以使用 vCenter Server Appliance GUI 安装程序将 vCenter Server 还原到 ESXi 主机或 vCenter Server 实例。还原过程分为两个阶段。第一阶段是部署新的 vCenter Server Appliance。第二阶段是使用基于文件的备份中存储的数据填充新部署的 vCenter Server Appliance。

图 3-1. vCenter Server 还原 workflow



前提条件

- 验证系统是否满足最低软件和硬件要求。请参见。
- 如果 vCenter Server 实例是 vCenter 高可用性集群的一部分，则在还原 vCenter Server 之前必须关闭集群的主动节点、被动节点和见证节点。

步骤

1 第 1 阶段 - 部署新设备

在还原过程的第 1 阶段中，您将部署 OVA 文件，它包括在 vCenter Server GUI 安装程序中。

2 第 2 阶段 - 将数据传输到新部署的设备

OVA 部署完成后，您将重定向到还原过程的第 2 阶段，在这个阶段中，数据将从备份位置复制到新部署的 vCenter Server Appliance。

第 1 阶段 - 部署新设备

在还原过程的第 1 阶段中，您将部署 OVA 文件，它包括在 vCenter Server GUI 安装程序中。

作为使用 GUI 安装程序执行还原第一阶段的替代方法，也可以使用 vSphere Client 部署新 vCenter Server Appliance 的 OVA 文件。OVA 部署完成后，必须登录到新部署设备的 vCenter Server 管理界面，才能继续执行还原过程的第二阶段。有关使用 vSphere Client 部署 OVA 文件的信息，请参见《vSphere 虚拟机管理》《vSphere 虚拟机管理》中的“部署 OVF 或 OVA 模板”。

前提条件

- 下载并挂载 vCenter Server 安装程序。请参见[下载并挂载 vCenter Server 安装程序](#)。

注 如果要从应用了 vCenter Server 产品修补程序的产品中还原备份，则必须下载该特定修补程序的完整 ISO。请参见[下载 VMware vSphere](#)。

- 如果计划在 ESXi 主机上还原 vCenter Server，请确认目标 ESXi 主机未处于锁定模式或维护模式，或者不属于全自动 DRS 集群。
- 如果计划还原 vCenter Server 清单 DRS 集群上的 vCenter Server，请确认该集群包含至少一个未处于锁定模式或维护模式的 ESXi 主机。
- 如果计划为设备分配静态 IP 地址，请确认已为此 IP 地址配置了正向和反向 DNS 记录。
- 如果您尝试还原仍在运行的 vCenter Server 实例，则在开始还原操作之前关闭已备份的 vCenter Server。

步骤

- 1 在 vCenter Server 安装程序中，导航到 vcsa-ui-installer 目录，转至所用操作系统的子目录，然后运行安装程序可执行文件。
 - 对于 Windows 操作系统，转至 win32 子目录，并运行 installer.exe 文件。
 - 对于 Linux 操作系统，转至 lin64 子目录，并运行 installer 文件。
 - 对于 Mac 操作系统，转至 mac 子目录，并运行 Installer.app 文件。

- 2 在主页中，单击**还原**。
- 3 查看“简介”页面以了解还原过程，然后单击**下一步**。
- 4 阅读并接受许可协议，然后单击**下一步**。
- 5 在“输入备份详细信息”页面上，输入您要还原的备份文件的详细信息，然后单击**下一步**。

选项	描述
备份位置	<p>输入服务器地址和存储备份文件的备份文件夹。也可以输入备份服务器的 IP 地址或主机名，并浏览备份文件夹的位置。指定要用于从备份服务器检索备份的协议。可以选择 FTP、FTPS、HTTP、HTTPS、SFTP、NFS 或 SMB。例如，</p> <pre>ftp://<server_IP_address>/tmp/vCenter/hostname_vcenter.com/<backup_filename></pre>
用户名	输入备份服务器上具有 读取 特权的用户的用户名。
密码	输入备份服务器上具有 读取 特权的用户的密码。

- 6 查看备份信息，然后单击**下一步**。
- 7 连接到 ESXi 主机或者要部署 vCenter Server Appliance 用于还原操作的 vCenter Server。

选项	步骤
可以连接要部署用于还原操作的设备的 ESXi 主机。	<ol style="list-style-type: none"> 1 输入 ESXi 主机的 FQDN 或 IP 地址。 2 输入 ESXi 主机的 HTTPS 端口。 3 输入对 ESXi 主机具有管理特权的用户的用户名和密码，例如 root 用户。 4 单击下一步。 5 确认证书警告显示安装在目标 ESXi 主机上的 SSL 证书的 SHA1 指纹，然后单击接受证书指纹。
可以连接到 vCenter Server 实例并浏览清单，以选择要部署用于还原操作的设备的 ESXi 主机或 DRS 集群。	<ol style="list-style-type: none"> 1 输入 vCenter Server 实例的 FQDN 或 IP 地址。 2 输入 vCenter Server 实例的 HTTPS 端口。 3 输入对 vCenter Server 实例具有 vCenter Single Sign-On 管理特权的用户的用户名和密码，例如 administrator@your_domain_name 用户。 4 单击下一步。 5 确认证书警告显示安装在目标 vCenter Server 实例上的 SSL 证书的 SHA1 指纹，然后单击接受证书指纹。 6 选择包含要部署设备的 ESXi 主机或 DRS 集群的数据中心或数据中心文件夹，然后单击下一步。 <p>注 所选择的数据中心或数据中心文件夹必须至少包含一个未处于锁定或维护模式的 ESXi 主机。</p> <ol style="list-style-type: none"> 7 选择要部署设备的 ESXi 主机或 DRS 集群，然后单击下一步。

- 8 接受证书警告。
- 9 输入 vCenter Server Appliance 的名称，设置 root 用户的密码，然后单击**下一步**。

10 根据 vSphere 清单大小，选择新 vCenter Server Appliance 的部署大小。

部署大小选项	描述
微型	部署具有 2 个 vCPU 和 14 GB 内存的设备。 适用于最多包含 10 个主机或 100 个虚拟机的环境。
小型	部署具有 4 个 CPU 和 21 GB 内存的设备。 适用于最多包含 100 个主机或 1,000 个虚拟机的环境。
中等	部署具有 8 个 CPU 和 30 GB 内存的设备。 适用于最多包含 400 个主机或 4,000 个虚拟机的环境。
大型	部署具有 16 个 CPU 和 39 GB 内存的设备。 适用于最多包含 1,000 个主机或 10,000 个虚拟机的环境。
超大型	部署具有 24 个 CPU 和 58 GB 内存的设备。 适用于最多包含 2,500 个主机或 45,000 个虚拟机的环境。

11 选择新的 vCenter Server Appliance 的存储大小，然后单击下一步。

重要说明 必须考虑要还原的设备的存储大小。

存储大小选项	微型部署大小的描述	小型部署大小的描述	中型部署大小的描述	大型部署大小的描述	超大型部署大小的描述
默认	部署具有 579 GB 存储的设备。	部署具有 694 GB 存储的设备。	部署具有 908 GB 存储的设备。	部署具有 1358 GB 存储的设备。	部署具有 2283 GB 存储的设备。
大型	部署具有 2019 GB 存储的设备。	部署具有 2044 GB 存储的设备。	部署具有 2208 GB 存储的设备。	部署具有 2258 GB 存储的设备。	部署具有 2383 GB 存储的设备。
超大型	部署具有 4279 GB 存储的设备。	部署具有 4304 GB 存储的设备。	部署具有 4468 GB 存储的设备。	部署具有 4518 GB 存储的设备。	部署具有 4643 GB 存储的设备。

- 从可用数据存储列表中，选择将存储所有虚拟机配置文件和虚拟磁盘的位置，也可以通过选择**启用精简磁盘模式**启用精简置备。
- 在“配置网络设置”页面上，查看从 vCenter Server 的备份文件填充的设置。
- （可选）编辑网络配置，使其与还原 vCenter Server 的当前网络环境一致。
- 在“即将完成第 1 阶段”页面上，查看已还原的 vCenter Server Appliance 的部署设置，然后单击**完成**开始 OVA 部署过程。
- 等待 OVA 部署完成，然后单击**继续**以继续执行还原过程的第 2 阶段，将数据传输到新部署的设备。

注 如果通过单击**关闭**退出向导，必须登录到 vCenter Server 管理界面以传输数据。

结果

新部署的 vCenter Server Appliance 在目标服务器上运行，但未从备份位置复制数据。

第 2 阶段 - 将数据传输到新部署的设备

OVA 部署完成后，您将重定向到还原过程的第 2 阶段，在这个阶段中，数据将从备份位置复制到新部署的 vCenter Server Appliance。

步骤

- 1 查看还原过程第 2 阶段的简介，然后单击**下一步**。
- 2 查看备份详细信息，然后单击**下一步**。
- 3 如果要为 vCenter Server Appliance 还原支持增强型链接模式的节点，系统会要求您提供 Single Sign-On 凭据。输入 Single Sign-On 用户名和密码，然后单击**验证并恢复**。
- 4 在“即将完成”页面上，查看详细信息，单击**完成**，然后单击**确定**完成还原过程的第 2 阶段。

还原过程将重新启动 vCenter Server Management Service。在重新启动期间不能访问 vCenter Server Management API。

重要说明 如果 vCenter Server Appliance 虚拟机的还原操作失败，则必须关闭部分还原的虚拟机的电源并将其删除。然后，可以尝试重新还原虚拟机。

- 5 （可选）还原过程结束后，单击 https://vcenter_server_appliance_fqdn/ui 转至 vSphere Client 并登录到 vCenter Server 实例，或者单击 https://vcenter_server_appliance_fqdn:443 转到 vCenter Server 的“入门”页面。
- 6 单击**关闭**退出向导。
您将重定向到 vCenter Server 的“入门”页面。
- 7 如果已备份的 vCenter 节点是 vCenter 高可用性集群的一部分，则在还原操作成功完成后需要重新配置它。

有关如何执行备份和还原操作的信息，请参见《vSphere 可用性》。

后续步骤

成功完成还原操作后，如果所有存储和服务器全部受损（即所有物理硬件或硬件中的数据全部丢失），请按照 VMware 知识库文章 (<http://kb.vmware.com/kb/76585>) 中的说明进行操作，以便将系统恢复到备份时的还原前状态。

部署 vCenter Server Appliance 后

4

部署 vCenter Server Appliance 后，请先考虑以下安装后选项，然后再添加供 vCenter Server 管理的清单。

如果计划将 Windows 11 作为客户机操作系统安装在虚拟机上，则必须配置密钥提供程序。安装 Windows 11 需要可信平台模块 (TPM) 2.0。将 Windows 11 作为客户机操作系统安装在虚拟机上时，可以使用虚拟可信平台模块 (vTPM)，而不使用物理 TPM。vTPM 是物理 TPM 2.0 芯片的基于软件的表现形式。vTPM 依赖虚拟机加密来保护重要的 TPM 数据，因此要求配置密钥提供程序。有关 vSphere 支持的密钥提供程序的信息，请参见《vSphere 安全性》文档中的“虚拟机加密”一章。最简单的方法是配置 VMware vSphere® Native Key Provider™。所有 vSphere 版本均包含 vSphere Native Key Provider，它不需要外部密钥服务器。有关配置 vSphere Native Key Provider 的信息，请参见《vSphere 安全性》文档中的“配置和管理 vSphere Native Key Provider”一章。与所有安全解决方案一样，请考虑系统设计、实施注意事项和使用 vSphere Native Key Provider 的利弊。

有关配置 vSphere Authentication Proxy 服务的信息，请参见《vSphere 安全性》。

有关升级 vCenter Server 的信息，请参见《vCenter Server 升级》。

本章讨论了以下主题：

- 使用 vSphere Client 登录到 vCenter Server
- 安装 VMware 增强型身份验证插件
- 将 vCenter Server 重新指向其他域中的另一个 vCenter Server

使用 vSphere Client 登录到 vCenter Server

可以使用 vSphere Client 登录到 vCenter Server 并管理 vSphere 清单。

vSphere Client 将在 vCenter Server Appliance 部署过程中自动安装。这样可保证 vSphere Client 始终指向同一 vCenter Single Sign-On 实例。

步骤

- 1 打开 Web 浏览器，然后输入 vCenter Server 实例的 URL：

`https://vcenter_server_ip_address_or_fqdn`

或者，也可以打开 Web 浏览器，然后输入 vSphere Client 的 URL：

`https://vcenter_server_ip_address_or_fqdn/ui`。

- 如果显示有关潜在安全风险的警告消息，请选择继续访问该网站。

浏览器	操作
Microsoft Edge	<ol style="list-style-type: none"> 单击详细信息。 在显示的其他消息下，单击继续转到网页。
Mozilla Firefox	<ol style="list-style-type: none"> 单击高级。 在显示的其他消息下，单击接受风险并继续。
Google Chrome	<ol style="list-style-type: none"> 单击高级。 在显示的其他消息下，单击继续访问 <i>vcenter_server_ip_address_or_fqdn</i>。

- 在 vSphere 欢迎使用页面上，选择**启动 vSphere Client (HTML5)**。
- 如果再次显示有关潜在安全风险的警告消息，请重复步骤 2。
- 输入在 vCenter Server 上具有权限的用户的凭据，然后单击**登录**。

结果

vSphere Client 将连接到指定用户具有权限的所有 vCenter Server 系统，且您可以查看和管理 vSphere 清单。

安装 VMware 增强型身份验证插件

VMware 增强型身份验证插件提供了集成 Windows 身份验证和基于 Windows 的智能卡功能。

在 vSphere 6.5 版本中，VMware 增强型身份验证插件代替了 vSphere 6.0 及早期版本中的客户端集成插件。增强型身份验证插件提供了集成 Windows 身份验证和基于 Windows 的智能卡功能。只有这两项功能是从以前的客户端集成插件沿用而来的。在 vSphere 6.0 或更低版本中，如果已在系统上安装客户端集成插件，则增强型身份验证插件可以无缝运行。安装两个插件时，不会出现任何冲突。

仅安装一次插件就可以启用插件提供的所有功能。

注 启用 Active Directory 联合身份验证服务时，增强型身份验证插件仅适用于 vCenter Server 为身份提供程序的配置（基于 LDAP 的 Active Directory、集成 Windows 身份验证和 OpenLDAP 配置）。

步骤

- 打开 Web 浏览器，然后键入 vSphere Client 的 URL。
- 在 vSphere Client 登录页面底部，单击**下载增强型身份验证插件**。
- 如果浏览器通过发出证书错误或运行弹出窗口阻止功能阻止安装，请按照浏览器的“帮助”说明解决问题。
- 将插件保存在计算机中，然后运行可执行程序。
- 完成 VMware 增强型身份验证插件和随后运行的 VMware 插件服务安装向导中的步骤。
- 安装完成后，刷新浏览器。

- 7 在“外部协议请求”对话框中，单击**启动应用程序**以运行增强型身份验证插件。

登录页面将不再显示下载插件的链接。

将 vCenter Server 重新指向其他域中的另一个 vCenter Server

可以将 vCenter Server 从一个 vSphere 域移至另一个 vSphere 域。诸如标记和许可等服务将保留并迁移到新的域。

支持以下用例：

- 可以在存在或不存在复制的情况下，将 vCenter Server 从一个现有域迁移到另一个现有域。迁移的 vCenter Server 将从其当前的 Single Sign-on 域中移出，并作为通过增强型链接模式连接的另一个 vCenter Server 加入另一个现有域。
 - 有关在没有复制合作伙伴的情况下将单个嵌入式节点从一个域重新指向另一个现有域的说明，请参见[在没有复制合作伙伴的情况下将单个 vCenter Server 节点重新指向另一个现有域](#)。
 - 有关在使用复制的情况下将嵌入式节点从一个域重新指向另一个现有域的说明，请参见[在存在复制合作伙伴的情况下将 vCenter Server 节点重新指向另一个现有域](#)。
- 可以将 vCenter Server 从现有域迁移到新创建的域（其中迁移的 vCenter Server 是第一个实例）。有关此类重新指向的说明，请参见[将 vCenter Server 节点重新指向新域](#)。在这种情况下，无复制合作伙伴。

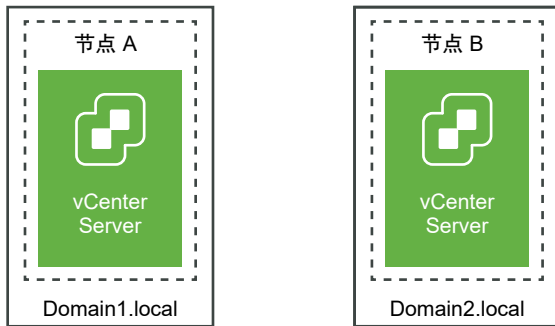
在没有复制合作伙伴的情况下将单个 vCenter Server 节点重新指向另一个现有域

可以在没有复制合作伙伴的情况下将单个 vCenter Server 从一个 Single Sign-on 域重新指向另一个现有 Single Sign-On 域。每个 Single Sign-on 域都包含单个 vCenter Server。

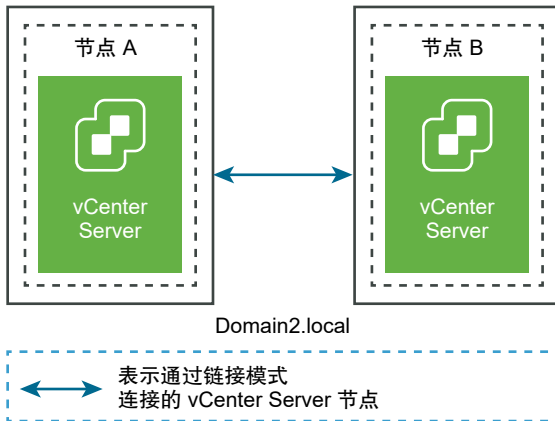
有关将单个 vCenter Server 从一个域重新指向另一个现有域的示例，请参见图 4-1. [将单个 vCenter Server 从一个域重新指向另一个现有域](#)。这是创建增强型链接模式节点的诸多方法之一。在这种情况下，不存在复制。

图 4-1. 将单个 vCenter Server 从一个域重新指向另一个现有域

在重新指向之前



在重新指向之后



前提条件

- 仅 vCenter Server 6.7 Update 1 及更高版本支持重新指向。
- 您必须重新指向相同版本的 vCenter Server。
- 为确保不发生数据丢失，请先对每个节点进行基于文件的备份，然后再继续对 vCenter Server 执行重新指向。

步骤

- 1 在开始重新指向过程之前，请确保两个 vCenter Server 节点均已打开电源。
- 2 （可选）运行预检查模式命令。预检查模式将从 vCenter Server 提取标记数据（标记和类别）和授权数据（角色和特权）。预检查不会迁移任何数据，但会检查源和目标 vCenter Server 之间发生的冲突。例如，使用以下 CLI 运行预检查：

```
cmsso-util domain-repoint -m pre-check --src-emb-admin Administrator --replication-partner-fqdn FQDN_of_destination_node --replication-partner-admin PSC_Admin_of_destination_node --dest-domain-name destination_PSC_domain
```

注 如果复制合作伙伴不存在（重新指向新创建的域），则不需要预检查。

有关 `cmsso-util domain-repoint` 命令的参数定义，请参见[域重新指向命令的语法](#)。

预检查将冲突写入 `/storage/domain-data` 目录。

- 3 （可选）查看冲突，然后针对所有冲突应用解决方法或针对每个冲突应用单独的解决方法。

冲突解决方法包括：

- 复制：在目标域中创建数据副本。
- 跳过：跳过将数据复制到目标域。
- Merge：合并冲突但不创建副本。

注 标记和授权冲突的默认解决方法模式为“复制”，除非在预检查期间生成的冲突文件中被替代。

- 4 运行 `execute` 命令。在执行模式下，在预检查模式期间生成的数据将读取并导入到目标节点。然后将 vCenter Server 重新指向目标域。例如，在没有复制合作伙伴的情况下重新指向时，请运行带以下选项的 `execute` 命令：

```
cmsso-util domain-repoint -m execute --src-emb-admin Administrator --replication-partner-fqdn FQDN_of_destination_node --replication-partner-admin PSC_Admin_of_destination_node --dest-domain-name destination_PSC_domain
```

有关 `cmsso-util domain-repoint` 命令的参数定义，请参见[域重新指向命令的语法](#)。

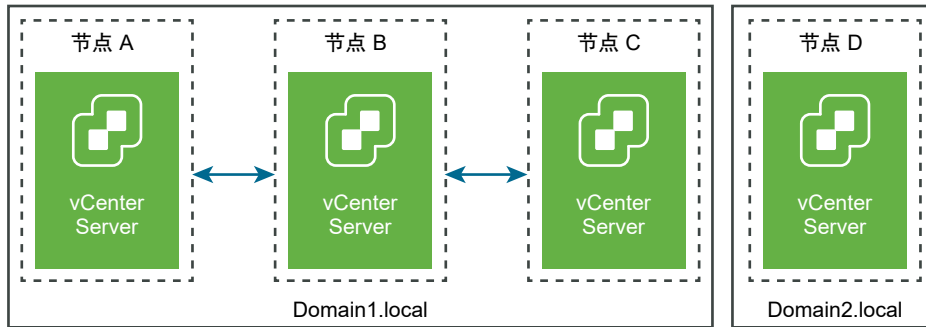
在存在复制合作伙伴的情况下将 vCenter Server 节点重新指向另一个现有域

可以在使用复制合作伙伴的情况下将 vCenter Server 从一个 Single Sign-on 域重新指向另一个现有域。

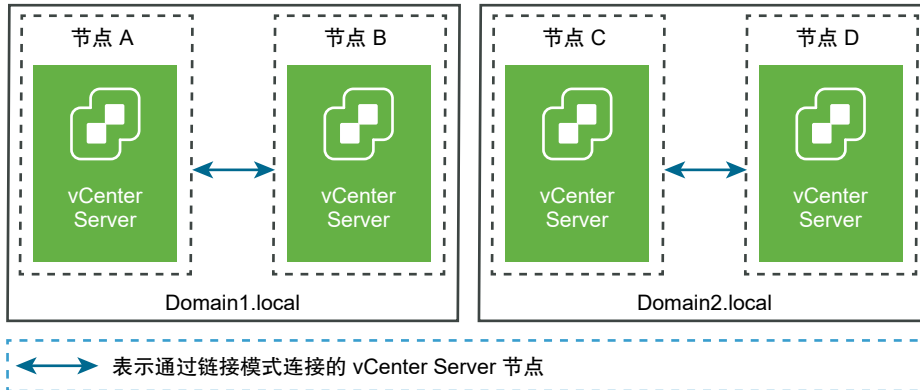
有关重新指向现有域的示例，请参见[图 4-2. 将 vCenter Server 从一个域重新指向另一个现有域](#)。在这种情况下，存在复制。

图 4-2. 将 vCenter Server 从一个域重新指向另一个现有域

在重新指向之前



在重新指向之后



前提条件

- 仅 vCenter Server 6.7 Update 1 及更高版本支持重新指向。
- 您必须重新指向相同版本的 vCenter Server。
- 为确保不发生数据丢失，请先对每个节点进行基于文件的备份，然后再继续对 vCenter Server 执行重新指向。

步骤

- 1 关闭要重新指向（移动到其他域）的节点（例如，节点 C）。
- 2 取消配置要重新指向的 vCenter Server 节点。例如，要取消配置节点 C，请登录到节点 B（在原始域上），然后运行以下命令：

```
cmsso-util unregister --node-pnid Node_C_FQDN --username
Node_B_sso_administrator@sso_domain.com --passwd Node_B_sso_adminuser_password
```

取消注册节点 C 后，重新启动服务。对节点 C 的引用将从节点 B 以及与原始域中的节点 C 链接的任何其他节点中删除。

- 3 打开节点 C 的电源以开始重新指向过程。

- 4 （可选）运行预检查模式命令。预检查模式将从 vCenter Server 提取标记数据（标记和类别）和授权数据（角色和特权）。预检查不会迁移任何数据，但会检查源和目标 vCenter Server 之间发生的冲突。例如，使用以下 CLI 运行预检查：

```
cmsso-util domain-repoint -m pre-check --src-emb-admin Administrator --replication-partner-fqdn FQDN_of_destination_node --replication-partner-admin PSC_Admin_of_destination_node --dest-domain-name destination_PSC_domain
```

注 如果复制合作伙伴不存在（重新指向新创建的域），则不需要预检查。

有关 `cmsso-util domain-repoint` 命令的参数定义，请参见[域重新指向命令的语法](#)。

预检查将冲突写入 `/storage/domain-data` 目录。

- 5 （可选）检查冲突，然后针对所有冲突应用解决方法或针对每个冲突应用单独的解决方法。

冲突解决方法包括：

- 复制：在目标域中创建数据副本。
- 跳过：跳过将数据复制到目标域。
- Merge：合并冲突但不创建副本。

注 标记和授权冲突的默认解决方法模式为“复制”，除非在预检查期间生成的冲突文件中被替代。

- 6 运行执行命令。在执行模式下，在预检查模式期间生成的数据将读取并导入到目标节点。然后将 vCenter Server 重新指向目标域。例如，使用以下 CLI 运行 `execute` 命令：

```
cmsso-util domain-repoint -m execute --src-emb-admin Administrator --replication-partner-fqdn FQDN_of_destination_node --replication-partner-admin destination_node_PSC_Admin_user_name --dest-domain-name destination_PSC_domain
```

有关 `cmsso-util domain-repoint` 命令的参数定义，请参见[域重新指向命令的语法](#)。

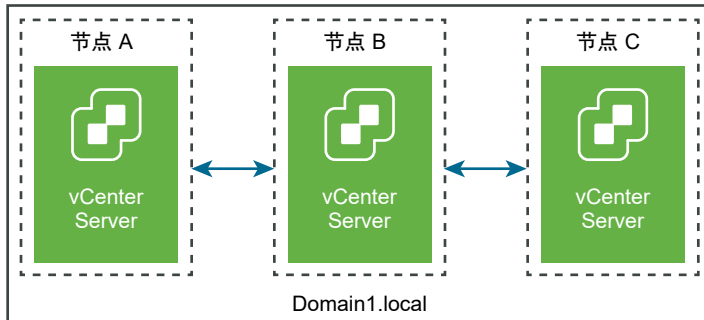
将 vCenter Server 节点重新指向新域

可以将 vCenter Server 从现有域重新指向新创建的域。

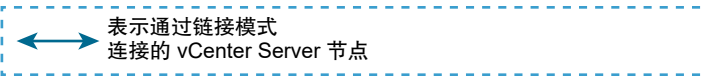
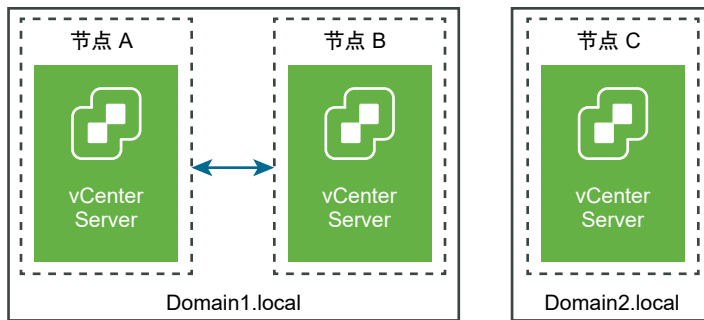
有关重新指向新域的示例，请参见[图 4-3. 将 vCenter Server 从一个域重新指向新域](#)。在这种情况下，无复制合作伙伴。

图 4-3. 将 vCenter Server 从一个域重新指向新域

在重新指向之前



在重新指向之后



前提条件

- 仅 vCenter Server 6.7 Update 1 及更高版本支持重新指向。
- 您必须重新指向相同版本的 vCenter Server。
- 为确保不发生数据丢失，请先对每个节点进行基于文件的备份，然后再继续对 vCenter Server 执行重新指向。

步骤

- 1 关闭要重新指向（移动到其他域）的节点（例如，节点 C）。
- 2 取消配置要重新指向的 vCenter Server 节点。例如，要取消配置节点 C，请登录到节点 B（在原始域上），然后运行以下命令：

```
cmsso-util unregister --node-pnid Node_C_FQDN --username
Node_B_sso_administrator@sso_domain.com --passwd Node_B_sso_adminuser_password
```

取消注册节点 C 后，重新启动服务。对节点 C 的引用将从节点 B 以及与原始域中的节点 C 链接的任何其他节点中删除。

- 3 打开节点 C 的电源以开始重新指向过程。

- 4 运行执行命令。在执行模式下，在预检查模式期间生成的数据将读取并导入到目标节点。然后将 vCenter Server 重新指向目标域。例如，在没有复制合作伙伴的情况下重新指向（重新指向新域）时，请运行带以下选项的执行命令：

```
cmsso-util domain-repoint -m execute --src-emb-admin Administrator --dest-domain-name destination_PSC_domain
```

有关 `cmsso-util domain-repoint` 命令的参数定义，请参见[域重新指向命令的语法](#)。

域重新指向命令的语法

可以使用命令实参来设置域重新指向命令的执行形参。

`cmsso-util domain-repoint CLI` 将 vCenter Server 从一个域重新指向另一个域。

可以向 CLI 重新指向命令添加用空格分隔的参数列表。

使用以下命令可将 vCenter Server 重新指向另一个 vCenter Server 节点：

```
cmsso-util domain-repoint -m execute --src-emb-admin Administrator --replication-partner-fqdn FQDN_of_destination_node --replication-partner-admin destination_node_PSC_Admin_user_name --dest-domain-name destination_PSC_domain
```

参数	描述
<code>-m, --mode</code>	<i>mode</i> 可以是 <code>pre-check</code> 或 <code>execute</code> 。 <code>pre-check</code> 参数在预检查模式下运行命令。 <code>execute</code> 参数在执行模式下运行命令。
<code>-spa, --src-psc-admin</code>	源 vCenter Server 的 SSO 管理员用户名。不要附加 <code>@domain</code> 。
<code>-dpf, --dest-psc-fqdn</code>	要重新指向的 vCenter Server 的 FQDN。
<code>-dpa, --dest-psc-admin</code>	目标 vCenter Server 的 SSO 管理员用户名。不要附加 <code>@domain</code> 。
<code>-ddn, --dest-domain-name</code>	目标 vCenter Server 的 SSO 域名。
<code>-dpr, --dest-psc-rhttps</code>	（可选）目标 vCenter Server 的 HTTPS 端口。如果未设置，将使用默认端口 443。
<code>-dvf, --dest-vc-fqdn</code>	指向目标 vCenter Server 的 vCenter Server 的 FQDN。将使用 vCenter Server 在预检查模式下检查组件数据冲突。如果未提供，则会跳过冲突检查，并为导入过程中发现的任何冲突应用默认解决方法 (COPY)。 注 仅当目标域没有 vCenter Server 时，此参数才是可选的。如果目标域中存在 vCenter Server，则此参数是必需的。
<code>-sea, --src-emb-admin</code>	具有嵌入式 vCenter Server 部署的 vCenter Server 的管理员。请勿将 <code>@domain</code> 附加到管理员 ID。
<code>-rpf, --replication-partner-fqdn</code>	（可选）vCenter Server 复制到的复制合作伙伴节点的 FQDN。

参数	描述
<code>-rpr, --replication-partner-rhttps</code>	(可选) 复制节点的 HTTPS 端口。如果未设置，默认值为 443。
<code>-rpa, --replication-partner-admin</code>	(可选) 复制合作伙伴 vCenter Server 的 SSO 管理员用户名。
<code>-dvr, --dest-vc-rhttps</code>	(可选) 指向目标 vCenter Server 的 vCenter Server 的 HTTPS 端口。如果未设置，将使用默认端口 443。
<code>--ignore-snapshot</code>	(可选) 忽略快照警告。
<code>--no-check-certs</code>	(可选) 忽略证书验证。
<code>--debug</code>	(可选) 检索命令执行详细信息。
<code>-h, --help</code>	(可选) 显示 cmsso-util domain repoint 命令的帮助消息。

了解标记和授权冲突

在预检查模式下运行域重新指向命令时，将导出并检查来自 vCenter Server 的数据，而且会将冲突写入到文件中。

以下数据会导出到 `/storage/domain-data/` 或 `ProgramData/VMWare/vCenterServerdata/domain-data` 文件夹：

- `All_Privileges.json`
- `All_Roles.json`
- `All_TagCategories.json`
- `All_Tags.json`

这些文件包含来自运行该命令的 vCenter Server 的所有数据（授权和标记）。

如果使用 `-dvf` 或 `--dest-vc-fqdn` 选项提供辅助 vCenter Server，则任何冲突也会导出到同一个文件夹：

- `Conflicts_Roles.json`
- `Conflicts_TagCategories.json`
- `Conflicts_Tags.json`

以下是示例冲突文件：

```
<---- Sample Conflict file code block ---->
{
  "global" : {
    "resolution" : "MERGE|SKIP|COPY",
    "description" : "Default resolution option used to resolve Role Conflicts is COPY. The
conflicts list describes the differences between Role entities on source and target vCenter
Server. If
the source information represents an empty JSON array, it simply means that all the entity
```

```

attributes from source and target are identical. If the source lists few entries, it means
that only these entity attributes are missing from the target. If the target lists few
entries,
it means that only these entity attributes are missing from the source. Though a global
resolution
can be set, it can also be overridden at each conflict level by providing individual
resolution
mode."
    },
    "conflicts-count" : 1,
    "conflicts-list" : {
        "NoCryptoAdmin" : {
            "source" : {
                "privileges" : "[]"
            },
            "target" : {
                "privileges" : "[Group-1.SamplePriv-1, Group-1.SamplePriv-4, Group-2.SamplePriv-10,
Group-2.SamplePriv-3, Group-2.SamplePriv-7, Group-3.SamplePriv-2, Group-3.SamplePriv-9]"
            },
            "resolution" : ""
        }
    }
}
<----- End of code block ---->

```

以下是示例冲突文件的几个部分：

- `description`.提供有关如何阅读和理解相应冲突文件的详细信息。
- `source` 和 `target`。JSON 对象，仅列出源和目标 vCenter Server 对象之间的差异。
- `resolution`.用户需提供有效的解决方法。有效的解决方法为 MERGE、COPY 和 SKIP。

要指定用于处理冲突的解决方法，可在 `"global": "resolution" = "MERGE|SKIP|COPY"` 部分中为所有冲突提供默认解决方法选项。如果没有为 `resolution` 提供有效的全局解决方法类型或没有对其进行任何编辑，系统将使用 `COPY` 作为默认解决方法选项。

还可以通过在每个冲突级别编辑 `resolution` 属性为每个冲突提供有效的解决方法选项，该解决方法选项将替代全局解决方法选项。

表 4-1. 冲突类型中列出了冲突类型。

表 4-1. 冲突类型

冲突	用于比较类别对象的属性	冲突类型	有冲突的属性	冲突解决方法选项
角色冲突	<ul style="list-style-type: none"> ■ name: 类别的名称。 ■ privilegeId: 角色的特权列表。 	导入角色时，如果目标 vCenter Server 中存在具有相同名称但具有不同特权的角色时，将发生 RoleName 冲突。	对于 RoleName 冲突类型，有冲突的属性可以是 Privileges。	<ul style="list-style-type: none"> ■ COPY.将在目标 vCenter Server 中创建有冲突角色的副本，并将 --copy 附加到角色名称。将使用新的角色 ID 创建具有相同特权 ID 集的新角色。新的角色 ID 会更新到 VPX_ACCESS 表中。新的角色 ID 同时适用于角色名称冲突和角色 ID 冲突。 <p>注</p> <p>用于解决角色冲突的默认解决方法选项是 COPY。</p> <ul style="list-style-type: none"> ■ MERGE. 将按以下顺序解决 MERGE 选项： <ul style="list-style-type: none"> a 如果源 vCenter Server 中的角色与目标 vCenter Server 中的角色具有相同的名称和特权列表，但角色 ID 不同，则会使用目标 vCenter Server 中的角色 ID 并将其更新到 VPX_ACCESS 表中。 b 如果源 vCenter Server 中的角色与目标 vCenter Server 中的角色具有相同的名称，但特权列表不同，则会合并两个角色的特权列表。 ■ SKIP.不执行任何操作。将跳过特定角色。
标记类别冲突： 类别名称在 vCenter Server 中必须是唯一的。	<ul style="list-style-type: none"> ■ name: 类别的名称。 ■ cardinality: 类别的基数，可以是 Single 或 Multiple。 ■ associableEntityType: 可与该类别的标记相关联的 vCenter Server 对象的列表。值 All 表示所有 vCenter Server 对象。 	导入标记类别时，只会出现一种冲突类型，即 CategoryName 冲突。此冲突指示目标 vCenter Server 中存在具有相同名称但具有不同属性（cardinality 或 associableEntityType）的类别。	对于 CategoryName 冲突类型，有冲突的属性可以是以下一种或两种类型：Cardinality 或 AssociableTypes。	<ul style="list-style-type: none"> ■ COPY.将在目标 vCenter Server 中创建有冲突类别的副本，并将 --copy 附加到类别名称。将创建具有与源 vCenter Server 中相同的属性名称的新类别。该类别下存在的所有标记会导入到新创建的 CategoryCopy 下。 <p>注</p> <p>用于解决 CategoryName 冲突的默认解决方法选项是 COPY。</p>

表 4-1. 冲突类型（续）

冲突	用于比较类别对象的属性	冲突类型	有冲突的属性	冲突解决方法选项
				<ul style="list-style-type: none"> ■ MERGE.有冲突的属性将与 SSO 中已存在的类别合并。将按如下所示合并属性： <ul style="list-style-type: none"> a Description.将使用已存在的描述。 b Cardinality.不能缩小基数。如果存在基数冲突，基数会设置为 multiple。基数不能缩小为 single。 c AssociableTypes.如果 <code>associableEntityType</code> 值为 null，则会将其设置为 null。否则会合并 Objects 类型。 ■ SKIP.不执行任何操作。所有标记会导入到存在的类别下。
标记冲突：tag 对象始终属于 category 对象。标记名称在类别中必须是唯一的。	<ul style="list-style-type: none"> ■ name ■ description 	导入标记时，只会出现一种冲突类型，即 TagName 冲突。此冲突指示目标 vCenter Server 中的相同类别下存在具有相同名称但具有不同属性的标记。	对于 TagName 冲突类型，有冲突的属性可以是 Description。	<ul style="list-style-type: none"> ■ COPY.将在目标 vCenter Server 中创建有冲突标记的副本，并将 --copy 附加到标记名称。采用新创建的标记的 MoRef（内部标记 ID）并根据需要更新标记关联。 <p>注</p> <p>用于解决 CategoryName 冲突的默认解决方法选项是 COPY。</p> <ul style="list-style-type: none"> ■ MERGE.保留现有描述。采用 MoRef（内部标记 ID）并根据需要更新一个或多个标记关联。 ■ SKIP.不执行任何操作。不会创建该标记。清理任何标记关联。

vCenter Server 域重新指向许可证注意事项

域重新指向会将许可证密钥复制到新域。复制许可证密钥可确保重新指向后保留所有资产的有效许可。

vCenter Server 将基于域跟踪许可证使用情况。如果某个密钥在多个域中使用，必须确保该密钥的使用量总和不超过其容量。要简化许可证管理工作，请移除复制到另一个域的每个许可证，然后为资产分配新的许可证。

请考虑以下两种情况：

- 重新指向后，原始域中不再使用（即，分配给资产）的许可证密钥。

- 在多个域中使用（即，分配给资产）的许可证密钥。

未在域中使用的许可证密钥

如果在完成重新指向后，某个许可证密钥显示在多个域中，但未在其中的某些域中使用，则可从不使用该许可证密钥的任何域中移除它。有关如何在 vCenter Server 中移除许可证的说明，请参见《vCenter Server 和主机管理》中的“移除许可证”。

在多个域中使用的许可证密钥

如果在完成重新指向后，某个许可证密钥在多个域中使用（即，分配给资产），那么要从一个域以外的所有其他域移除该许可证密钥，首先必须为将从中移除许可证密钥的域中的每个资产分配一个不同的许可证密钥。两种常见方法：

- 如果您有具有足够未使用容量的其他许可证密钥可用，则可以使用这些其他密钥代替要移除的许可证密钥。请参见《vCenter Server 和主机管理》中的“将许可证分配给多个资产”，以在 vCenter Server 中分配许可证。
- 您可能会将在多个域中使用的许可证密钥拆分为单独的许可证密钥，并为每个域分配一个。要拆分许可证密钥，请参见 VMware 知识库文章，网址为 <http://kb.vmware.com/kb/2006972>。要确定要在原始许可证密钥拆分成的每个许可证密钥中包含的容量，请参见《vCenter Server 和主机管理》中的“查看许可信息”，以查看 vCenter Server 中每个域的许可证密钥使用情况。

然后，可将生成的每个许可证密钥添加到一个不同的域，并在 vCenter Server 中分配给先前使用原始许可证密钥许可的资产。请参见《vCenter Server 和主机管理》中的“创建新许可证”创建许可证，并参见《vCenter Server 和主机管理》中的“将许可证分配给多个资产”将许可证分配给多个资产。

在将不同许可证分配给所有资产后，可使用 vCenter Server 从所有域中移除不再有效的原始许可证密钥。请参见《vCenter Server 和主机管理》中的“移除许可证”。

对 vCenter Server 安装或部署进行故障排除

5

vCenter Server 部署故障排除主题针对您在 vCenter Server Appliance 部署过程中可能遇到的问题提供了解决方案。

本章讨论了以下主题：

- 收集用于对 vCenter Server 安装和升级进行故障排除的日志

收集用于对 vCenter Server 安装和升级进行故障排除的日志

可以收集 vCenter Server 的安装或升级日志文件。如果安装或升级失败，查看这些日志文件可帮助确定失败的原因。

也可以收集 vCenter Server 的部署日志文件。

- 手动检索安装日志
可以手动检索安装日志文件以进行检查。
- 收集 vCenter Server Appliance 的部署日志文件
如果 vCenter Server Appliance 部署失败，您可以检索日志文件并检查这些文件以了解失败的原因。
- 导出 vCenter Server 支持包以进行故障排除
您可以使用 DCUI 主屏幕上显示的 URL 来导出设备中 vCenter Server 实例的支持包以进行故障排除。

手动检索安装日志

可以手动检索安装日志文件以进行检查。

步骤

- 1 导航到安装日志文件位置。
 - %PROGRAMDATA%\VMware\vCenterServer\logs 目录，通常为
C:\ProgramData\VMware\vCenterServer\logs
 - %TEMP% 目录，通常为 C:\Users\username\AppData\Local\Temp
%TEMP% 目录中的文件包括 vc-install.txt、vminst.log、pkgmgr.log、pkgmgr-comp-
msi.log 和 vim-vcs-msi.log。

- 2 在文本编辑器中打开安装日志文件以进行检查。

收集 vCenter Server Appliance 的部署日志文件

如果 vCenter Server Appliance 部署失败，您可以检索日志文件并检查这些文件以了解失败的原因。

日志文件的完整路径将显示在 vCenter Server Appliance 部署向导中。

如果首次引导失败，则可以在 Windows 主机上下载支持包并检查日志文件以确定失败的首次引导脚本。请参见[导出 vCenter Server 支持包以进行故障排除](#)。

步骤

- 1 在用于部署 vCenter Server Appliance 的 Windows 计算机上，导航到日志文件文件夹。
如果以管理员身份登录，默认情况下为
C:\Users\Administrator\AppData\Local\VMware\CIP\vcsaInstaller 文件夹。
- 2 在文本编辑器中打开安装日志文件以进行检查。

导出 vCenter Server 支持包以进行故障排除

您可以使用 DCUI 主屏幕上显示的 URL 来导出设备中 vCenter Server 实例的支持包以进行故障排除。

您也可以通过运行 `vc-support.sh` 脚本，从 vCenter Server Appliance Bash shell 收集支持包。

支持包将以 `.tgz` 格式导出。

步骤

- 1 登录到要下载包的 Windows 主机。
- 2 打开 Web 浏览器，然后输入 DCUI 中显示的支持包的 URL。
`https://appliance-fully-qualified-domain-name:443/appliance/support-bundle`
- 3 输入 root 用户的用户名和密码。
- 4 单击 **Enter**。

支持包将在 Windows 计算机上下载为 `.tgz` 文件。

- 5 （可选）要确定哪个 `firstboot` 脚本失败，请检查 `firstbootStatus.json` 文件。

如果在 vCenter Server Appliance Bash shell 中运行 `vc-support.sh` 脚本，要检查 `firstbootStatus.json` 文件，请运行

```
cat /var/log/firstboot/firstbootStatus.json
```