vCloud Director 安装、配置和升级指南

2019 年 3 月 28 日

VMware Cloud Director 9.7

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

vCloud Director 安装、配置和升级指南

《vCloud Director 安装、配置和升级指南》提供有关安装和升级 VMware vCloud Director® for Service Providers 软件以及将其配置为与 VMware vSphere®、VMware NSX® for vSphere® 和 VMware NSX-T™ Data Center 配合使用的信息。

目标读者

《vCloud Director 安装、配置和升级指南》供要安装或升级 vCloud Director 软件的用户使用。本指南的目标读者为熟悉 Linux、Windows、IP 网络和 vSphere 且具有丰富经验的系统管理员。

更新信息

本《vCloud Director 安装、配置和升级指南》随产品的每个版本更新或在必要时更新。

下表提供了《vCloud Director 安装、配置和升级指南》的更新历史记录。

修订号	描述
2019 年 6 月 11 日	■ 添加了主题续订 vCloud Director 设备证书。 ■ 添加了章节第 9 章 在高可用性群集配置中使用复制管理器工具套件。
2019 年 5 月 10 日	■ 添加了章节#unique_5。 ■ 添加了主题使用日志文件对 vCloud Director 更新和修补程序进行故障排除。 ■ 添加了主题检查 vCloud Director 更新失败。 ■ 添加了主题安装 vCloud Director 的最新更新失败。
2019 年 4 月 05 日	■ 添加了章节第 12 章 迁移到 vCloud Director 设备。 ■ 添加了主题还原具有高可用性数据库配置的 vCloud Director 设备环境。 ■ 更新了主题设备部署和数据库高可用性配置，改进了工作流中的图形和步骤 2。 ■ 更新了主题检查 vCloud Director 设备中的日志文件，添加了有关包含部署 OVF 参数的文件的信息。
2019 年 3 月 28 日	初始版本。

vCloud Director 安装、配置和升级概述

1

您可以通过在一个或多个 Linux 服务器上安装 vCloud Director 软件或部署 vCloud Director 设备的一个或多个实例来创建 vCloud Director 服务器组。在安装过程中执行初始 vCloud Director 配置，包括建立网络和数据库连接。

适用于 Linux 的 vCloud Director 软件需要外部数据库，而 vCloud Director 设备使用嵌入式 PostgreSQL 数据库。

创建 vCloud Director 服务器组后，将 vCloud Director 安装与 vSphere 资源相集成。对于网络资源，vCloud Director 可以使用 NSX Data Center for vSphere、NSX-T Data Center 或同时使用两者。

升级现有 vCloud Director 安装时，更新 vCloud Director 软件和数据库模式，保留服务器、数据库和 vSphere 之间的现有关系不变。

将 Linux 上的现有 vCloud Director 安装迁移到 vCloud Director 设备时，可以更新 vCloud Director 软件并将数据库迁移到设备中的嵌入式数据库。

本章讨论了以下主题：

vCloud Director 架构

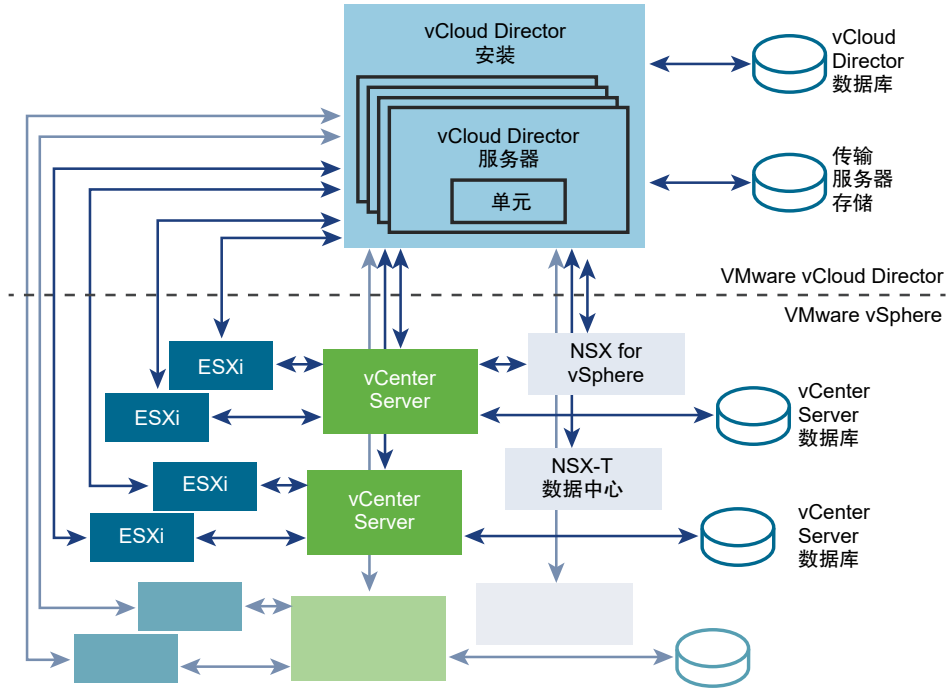
vCloud Director 服务器组由在 Linux 上安装的一个或多个 vCloud Director 服务器或 vCloud Director 设备部署组成。该组中的每台服务器均运行名为 vCloud Director 单元的服务集合。所有单元共享一个 vCloud Director 数据库和传输服务器存储，并连接到 vSphere 和网络资源。

重要事项 不支持在一个服务器组中的 Linux 和 vCloud Director 设备部署中混合安装 vCloud Director。

要确保 vCloud Director 高可用性，必须在服务器组中安装至少两个 vCloud Director 单元。使用第三方负载平衡器时，您可以确保自动进行故障切换而不会出现停机。

您可以将 vCloud Director 安装连接到多个 VMware vCenter Server® 系统及其管理的 VMware ESXi™ 主机。对于网络服务，vCloud Director 可以使用与 vCenter Server 关联的 NSX Data Center for vSphere，也可以将 NSX-T Data Center 注册到 vCloud Director。此外还支持混合 NSX Data Center for vSphere 和 NSX-T Data Center。

图 1-1. vCloud Director 架构图



在 Linux 上安装的 vCloud Director 服务器组使用外部数据库。

由设备部署组成的 vCloud Director 服务器组使用服务器组的第一个成员中的嵌入式数据库。您可以通过将设备的两个实例部署为同一服务器组中的备用单元，来配置 vCloud Director 数据库高可用性。请参见设备部署和数据库高可用性配置。

图 1-2. 包含嵌入式数据库高可用性群集的 vCloud Director 设备

vCloud Director 安装和配置过程会创建单元，将它们连接到共享数据库和传输服务器存储，并创建**系统管理员**帐户。然后，**系统管理员**建立与 vCenter Server 系统、ESXi 主机和 NSX Manager 实例的连接。有关添加 vSphere 和网络资源的信息，请参见《vCloud Director 管理员指南》。

配置计划

vSphere 可为 vCloud Director 提供存储、计算和网络容量。开始安装之前，请考虑您的云所需的 vSphere 和 vCloud Director 容量，并规划可支持它的配置。

配置要求取决于许多因素，其中包括云中的组织数、每个组织中的用户数及其活动级别。以下指导准则可作为大多数配置的起点：

- 为您希望在云中可供访问的每个 vCenter Server 系统分配一个 vCloud Director 单元。
- 确保所有目标 vCloud Director Linux 服务器至少满足《vCloud Director 发行说明》中详细说明的内存和存储的最低要求。
- 如果计划在 Linux 上安装 vCloud Director，请按照准备 vCloud Director 数据库中所述配置 vCloud Director 数据库。

vCloud Director 硬件和软件要求

2

vCloud Director 服务器组中的每台服务器均必须满足特定的硬件和软件要求。此外，受支持的数据库必须能够由组的所有成员访问。每个服务器组都需要访问 vCenter Server 系统、NSX Manager 实例以及一个或多个 ESXi 主机。

与其他 VMware 产品的兼容性

有关 vCloud Director 和其他 VMware 产品之间兼容性的最新信息，请参见 VMware 产品互操作性列表，网址为 http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php。

vSphere 配置要求

要与 vCloud Director 配合使用的 vCenter Server 实例和 ESXi 主机必须满足特定的配置要求。

- 对于供 vCloud Director 使用的任何群集中的所有主机，应能够访问要用作 vCloud Director 外部网络或网络池的 vCenter Server 网络。数据中心的所有主机如果均能访问这些网络，则可简化将新的 vCenter Server 实例添加到 vCloud Director 的任务。
- NSX Data Center for vSphere 支持的隔离网络和网络池需要 vSphere Distributed Switch。
- 与 vCloud Director 配合使用的 vCenter Server 群集必须将 vSphere DRS 自动化级别指定为**全自动**。Storage DRS 如已启用，可以配置为任何自动化级别。
- vCenter Server 实例必须信任其主机。由 vCloud Director 管理的所有群集中的全部主机必须配置为需要经过验证的主机证书。尤其需要注意的是，必须为所有主机确定、比较和选择匹配的指纹。请参见《vCenter Server 和主机管理》文档中的“配置 SSL 设置”。

vSphere 许可要求

vCloud Director Service Provider Bundle 包括必要的 vSphere 许可证。

支持的平台、数据库和浏览器

有关此版本 vCloud Director 支持的服务器平台、浏览器、LDAP 服务器和数据库的信息，请参见《vCloud Director 9.7 发行说明》。

磁盘空间、内存和 CPU 要求

《vCloud Director 9.7 发行说明》中列出了 vCloud Director 单元的物理要求，例如磁盘空间、内存和 CPU。

共享存储

NFS 或 vCloud Director 传输服务的其他共享存储卷。存储卷必须可扩展，并且可供服务器组中的所有服务器访问。

本章讨论了以下主题：

vCloud Director 的网络配置要求

vCloud Director 的安全可靠操作取决于是否具有支持正向和反向查找主机名、网络时间服务和其他服务的安全可靠网络。开始安装 vCloud Director 之前，您的网络必须满足这些要求。

连接 vCloud Director 服务器、数据库服务器、vCenter Server 系统及 NSX 组件的网络必须满足以下多个要求：

IP 地址

每个 vCloud Director 服务器都必须支持两个不同的 SSL 端点。一个端点用于 HTTP 服务，另一个端点用于控制台代理服务。这些端点可以是单独的 IP 地址，也可以是具有两个不同端口的单个 IP 地址。您可以使用 IP 别名或多个网络接口来创建这些地址。请勿使用 Linux `ip addr add` 命令创建第二个地址。

vCloud Director 设备将其 `eth0` IP 地址与自定义端口 8443 用于控制台代理服务。

控制台代理地址

配置为控制台代理端点的 IP 地址不得位于 SSL 终止负载平衡器或反向代理后面。所有控制台代理请求必须直接中继到控制台代理 IP 地址。

对于使用单个 IP 地址的安装，可以从 vCloud Director Web 控制台自定义控制台代理地址。例如，对于 vCloud Director 设备，必须将控制台代理地址自定义为 *vcloud.example.com*:8443。

网络时间服务

您必须使用网络时间服务（如 NTP）将所有 vCloud Director 服务器（其中包括数据库服务器）的时钟同步。被同步服务器的时钟之间最多允许存在 2 秒的偏差。

服务器时区

必须将所有 vCloud Director 服务器（包括数据库服务器）配置为处于同一时区。

主机名解析

安装和配置期间指定的所有主机名均必须由 DNS 通过完全限定域名或非限定主机名的转发和反向查找进行解析。例如，对于名为 *vcloud.example.com* 的主机，必须在 vCloud Director 主机上成功运行以下两个命令：

```
nslookup vcloud
nslookup vcloud.example.com
```

此外，如果主机 *vcloud.example.com* 的 IP 地址为 192.168.1.1，则以下命令必须返回 `vcloud.example.com`：

```
nslookup 192.168.1.1
```

设备需要对 `eth0` IP 地址执行反向 DNS 查找。必须在您的环境中成功执行以下命令：

```
host –W 15 –R 1 –T <eth0–IP–address>
```

网络安全要求

vCloud Director 的安全操作需要拥有一个安全的网络环境。在开始安装 vCloud Director 之前，必须先配置和测试此网络环境。

将所有 vCloud Director 服务器连接到受保护和监控的网络。vCloud Director 网络连接还具有以下几个要求：

- 请勿将 vCloud Director 直接连接到公共 Internet。始终使用防火墙保护 vCloud Director 网络连接。对于入站连接，仅必须打开端口 443 (HTTPS)。如果需要，也可以为入站连接打开端口 22 (SSH) 和 80 (HTTP)。此外，`cell–management–tool` 需要访问单元的 loopback 地址。防火墙必须拒绝来自公共网络的所有其他入站流量，包括发送到 JMX 的请求（端口 8999）。

  表 2-1. 必须支持来自 vCloud Director 主机的入站软件包的端口

端口	协议	注释
111	TCP 和 UDP	由传输服务使用的 NFS portmapper
920	TCP 和 UDP	由传输服务使用的 NFS rpc.statd
61611	TCP	AMQP
61616	TCP	AMQP

- 不要将用于出站连接的端口连接到公共网络。

  表 2-2. 必须支持来自 vCloud Director 主机的出站软件包的端口

端口	协议	注释
25	TCP 和 UDP	SMTP
53	TCP 和 UDP	DNS
111	TCP 和 UDP	由传输服务使用的 NFS portmapper
123	TCP 和 UDP	NTP
389	TCP 和 UDP	LDAP

表 2-2. 必须支持来自 vCloud Director 主机的出站软件包的端口 （续）

端口	协议	注释
443	TCP	使用标准端口的 vCenter、NSX Manager 和 ESXi 连接。如果您为这些服务选择了其他端口，请禁用端口 443 的连接并为所选端口启用这些服务。
514	UDP	可选。启用 syslog。
902	TCP	vCenter 和 ESXi 连接。
903	TCP	vCenter 和 ESXi 连接。
920	TCP 和 UDP	由传输服务使用的 NFS rpc.statd。
1433	TCP	默认的 Microsoft SQL Server 数据库端口。
5672	TCP 和 UDP	可选。任务延期的 AMQP 消息。
61611	TCP	AMQP
61616	TCP	AMQP

- 通过专用网络路由 vCloud Director 服务器与以下服务器之间的流量。
  - vCloud Director 数据库服务器
  - RabbitMQ
  - Cassandra
- 如果可能，通过专用网络路由 vCloud Director 服务器、vSphere 和 NSX 之间的流量。
- 支持提供商网络的虚拟交换机和分布式虚拟交换机必须相互隔离。它们不能共享相同的第 2 层物理网络分段。
- 使用 NFSv4 传输服务存储。最常见的 NFS 版本 NFSv3 不提供传输加密，对于某些配置，这可能会导致正在传输的数据被嗅探或篡改。SANS 白皮书受信任与不受信任环境中的 NFS 安全中介绍了 NFSv3 中固有的威胁。有关配置和保护 vCloud Director 传输服务的其他信息可从 VMware 知识库文章 2086127 获取。

安装 vCloud Director 或部署 vCloud Director 设备之前

3

在 Linux 服务器上安装 vCloud Director 或部署 vCloud Director 设备之前，必须先准备环境。

本章讨论了以下主题：

- 准备 vCloud Director 数据库
- 准备传输服务器存储
- 下载和安装 VMware 公钥
- 为 vCloud Director 安装和配置 NSX Data Center for vSphere
- 为 vCloud Director 安装和配置 NSX-T Data Center

准备 vCloud Director 数据库

vCloud Director 单元使用数据库来存储共享信息。在 Linux 上安装 vCloud Director 之前，必须安装并配置外部 vCloud Director 数据库。vCloud Director 设备使用嵌入式 PostreSQL 数据库。

有关受支持的 vCloud Director 数据库的信息，请参见 VMware 产品互操作性列表。

无论决定使用何种数据库软件，都必须创建单独的专用数据库架构以供 vCloud Director 使用。vCloud Director 无法与其他任何 VMware 产品共享数据库架构。

重要事项 vCloud Director 仅支持通过 SSL 连接到 PostgreSQL 数据库。在无人参与的网络和数据库连接配置期间或创建 vCloud Director 服务器组后，可以在 PostgreSQL 数据库上启用 SSL。请参见 无人参与的配置参考和在外部 PostgreSQL 数据库上执行其他配置。

在 Linux 上为 vCloud Director 配置外部 PostgreSQL 数据库

将 PostgreSQL 数据库与 vCloud Director 一起使用时，PostgreSQL 数据库具有特定的配置要求。在 Linux 上安装 vCloud Director 之前，必须安装和配置数据库实例并创建 vCloud Director 数据库用户帐户。

注 只有 Linux 上的 vCloud Director 才使用外部数据库。vCloud Director 设备使用嵌入式 PostgreSQL 数据库。

前提条件

必须熟悉 PostgreSQL 命令、脚本和操作。

步骤

1 配置数据库服务器。

具有 16 GB 内存、100 GB 存储和 4 个 CPU 的数据库服务器适用于典型的 vCloud Director 服务器组。

2 在数据库服务器上安装受支持的 PostgreSQL 发行版。

- 数据库的 SERVER_ENCODING 值必须为 UTF-8。此值在安装数据库时确定，并始终与数据库服务器操作系统使用的编码相匹配。
- 使用 PostgreSQL initdb 命令将 LC_COLLATE 和 LC_CTYPE 的值设置为 en_US.UTF-8。例如：

```
initdb --locale=en_US.UTF-8
```

3 创建数据库用户。

以下命令将创建用户 vcloud。

```
create user vcloud;
```

4 创建数据库实例，并为其指定一个所有者。

使用类似下述命令将名为 vcloud 的数据库用户指定为数据库所有者。

```
create database vcloud owner vcloud;
```

5 将数据库密码分配给数据库所有者帐户。

以下命令将密码 vcloudpass 分配给数据库所有者 vcloud。

```
alter user vcloud password 'vcloudpass';
```

6 让数据库所有者登录到数据库。

以下命令将 login 选项分配给数据库所有者 vcloud。

```
alter role vcloud with login;
```

后续步骤

创建 vCloud Director 服务器组后，可以将 PostgreSQL 数据库配置为要求从 vCloud Director 单元建立 SSL 连接，并调整某些数据库参数以获得最佳性能。请参见在外部 PostgreSQL 数据库上执行其他配置。

为适用于 Linux 的 vCloud Director 配置外部 Microsoft SQL Server 数据库

将 SQL Server 数据库与 vCloud Director 一起使用时，SQL Server 数据库具有特定的配置要求。在 Linux 上安装 vCloud Director 之前，必须安装和配置数据库实例并创建 vCloud Director 数据库用户帐户。

vCloud Director 数据库性能是影响 vCloud Director 总体性能和可扩展性的重要因素。vCloud Director 使用 SQL Server `tmpdb` 文件存储大型结果集、排序数据以及管理正在并发读取和修改的数据。vCloud Director 遇到高并发负载时，此文件可大幅增长。在具有快速读取和写入性能的专用卷上创建 `tmpdb` 文件是一种好方法。有关 `tmpdb` 文件和 SQL Server 性能的更多信息，请参阅 http://msdn.microsoft.com/en-us/library/ms175527.aspx。

注 只有 Linux 上的 vCloud Director 才使用外部数据库。vCloud Director 设备使用嵌入式 PostgreSQL 数据库。

前提条件

- 必须熟悉 Microsoft SQL Server 命令、脚本和操作。
- 若要配置 Microsoft SQL Server，请使用管理员凭据登录到 SQL Server 主机。可以将 SQL Server 配置为以 LOCAL_SYSTEM 身份运行，或以具有运行 Windows 服务的特权的任何身份运行。
- 有关将 Microsoft SQL Server Always On 可用性组与 vCloud Director 数据库结合使用的信息，请参见 VMware 知识库文章 https://kb.vmware.com/kb/2148767。

步骤

1 配置数据库服务器。

对于大多数 vCloud Director 服务器组来说，配置有 16 GB 内存、100 GB 存储容量以及 4 个 CPU 的数据库服务器便已足够。

2 在 SQL Server 设置期间指定混合模式身份验证。

使用 vCloud Director SQL Server 时，Windows 身份验证不受支持。

3 创建数据库实例。

以下脚本将创建数据库和日志文件以指定正确的排序规则序列。

```
USE [master]
GO
CREATE DATABASE [vcloud] ON PRIMARY
(NAME = N'vcloud', FILENAME = N'C:\vcloud.mdf', SIZE = 100MB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\vcloud.ldf', SIZE = 1MB, FILEGROWTH = 10%)
COLLATE Latin1_General_CS_AS
GO
```

建议采用以下显示的 SIZE 值。可能需要使用更大值。

4 设置事务隔离级别。

以下脚本将数据库隔离级别设置为 READ_COMMITTED_SNAPSHOT。

```
USE [vcloud]
GO
ALTER DATABASE [vcloud] SET SINGLE_USER WITH ROLLBACK IMMEDIATE;
ALTER DATABASE [vcloud] SET ALLOW_SNAPSHOT_ISOLATION ON;
ALTER DATABASE [vcloud] SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;
ALTER DATABASE [vcloud] SET MULTI_USER;
GO
```

有关事务隔离的更多信息，请参阅 http://msdn.microsoft.com/en-us/library/ms173763.aspx。

5 创建 vCloud Director 数据库用户帐户。

以下脚本将创建数据库用户名 `vcloud` 和密码 `vcloudpass`。

```
USE [vcloud]
GO
CREATE LOGIN [vcloud] WITH PASSWORD = 'vcloudpass', DEFAULT_DATABASE =[vcloud],
   DEFAULT_LANGUAGE =[us_english], CHECK_POLICY=OFF
GO
CREATE USER [vcloud] for LOGIN [vcloud]
GO
```

6 将权限分配给 vCloud Director 数据库用户帐户。

以下脚本将 `db_owner` 角色分配给在步骤 5 中创建的数据库用户。

```
USE [vcloud]
GO
sp_addrolemember [db_owner], [vcloud]
GO
```

准备传输服务器存储

要为用于外部发布或订阅的上载、下载和目录项目提供临时存储，必须使 vCloud Director 服务器组中的所有服务器都能够访问 NFS 或其他共享存储卷。

重要事项 vCloud Director 设备仅支持 NFS 类型的共享存储。设备部署过程涉及挂载 NFS 共享的传输服务器存储。

将 NFS 用于传输服务器存储时，您必须配置 vCloud Director 服务器组中的每个 vCloud Director 单元以挂载和使用基于 NFS 的传输服务器存储。您需要特定的用户和组权限来配置每个单元，以挂载基于 NFS 的位置并将其用作传输服务器存储。

服务器组的每个成员会将此卷挂载到同一挂载点，通常为 `/opt/vmware/vcloud-director/data/transfer`。此卷上的空间通过以下两种方式消耗：

- 传输期间，上载和下载均占用此存储。传输完成后，将从存储中移除上载和下载。在 60 分钟内无任何进度的传输将标记为已过期，由系统清理。传输的映像可能会很大，因此，至少分配数百 GB 存储空间以供传输使用是很好的做法。
- 外部发布且启用已发布内容缓存的目录中的目录项会占用此存储。外部发布但未启用缓存的目录中的目录项不会占用此存储。如果允许云中的组织创建外部发布的目录，可以假定数百或甚至数千个目录项需要此卷上的空间。每个目录项的大小大约为一个压缩 OVF 形式的虚拟机大小。

注 传输服务器存储的卷必须具有容量以备将来扩展。

vCloud Director 如何在传输服务器存储位置上使用文件系统权限

对于 vCloud Director 服务器组中的所有 vCloud Director 单元：

- 在标准云运维操作（如将项目上载到目录）中，vCloud Director 单元的守护进程会使用 **vcloud** 组中的 **vcloud** 用户将文件写入到传输服务器存储以及从中读取这些文件。**vcloud** 用户会使用 `umask 0077` 写入文件。当 vCloud Director 安装程序在某个服务器组成员上运行并安装 vCloud Director 软件时，它也会创建 **vcloud** 用户和 **vcloud** 组。
- vCloud Director 日志数据收集器脚本 `vmware-vcd-support` 可在一次操作中从所有 vCloud Director 单元收集日志，并将日志捆绑为一个 `tar.gz` 文件。运行该脚本时，该脚本会使用调用它的用户的用户 ID 将生成的 `tar.gz` 文件写入到传输服务器存储位置中的某个目录中。默认情况下，只有 **root** 用户有权运行该脚本。
- 单元上的 **root** 用户运行脚本，以将 `tar.gz` 文件写入到传输服务器存储位置中的 `vmware-vcd-support` 目录。如果要使用多单元选项一次收集所有单元中的日志，**root** 用户必须具有读取权限才能检索 `tar.gz` 诊断日志包。

配置 NFS 服务器的要求

NFS 服务器配置具有特定要求，以便 vCloud Director 可以将文件写入到基于 NFS 的传输服务器存储位置并从中读取文件。因此，**vcloud** 用户可以执行标准云运维操作，而 **root** 用户则可以执行多单元日志收集。

- NFS 服务器的导出列表必须允许 vCloud Director 服务器组中的每个服务器成员对导出列表中标识的共享位置具有读写访问权限。通过此功能，**vcloud** 用户能够将文件写入到共享位置并从中读取文件。
- NFS 服务器必须允许 vCloud Director 服务器组中每个服务器上的 **root** 系统帐户对共享位置具有读写访问权限。通过此功能，可以使用具有多单元选项的 `vmware-vcd-support` 脚本一次收集所有单元中的日志并存储在单个包中。可以通过在 NFS 导出配置中对此共享位置使用 `no_root_squash` 来满足此要求。

例如，如果 NFS 服务器具有 IP 地址 192.168.120.7，并将名为 vCDspace 的目录作为 vCloud Director 服务器组（位置为 /nfs/vCDspace）的传输空间，则必须确保其所有权和权限为 **root:root** 和 **750**。要允许对名为 vcd-cell1-IP 和 vcd-cell2-IP 的两个单元的共享位置进行读写访问，请使用 no_root_squash 方法。您必须在 /etc/exports 文件中添加一行。

```
192.168.120.7/nfs/vCDspace vCD_Cell1_IP_Address(rw,sync,no_subtree_check,no_root_squash)
vCD_Cell2_IP_Address(rw,sync,no_subtree_check)
```

在导出行中，每个单元 IP 地址与其相邻的左括号之间不能有空格。如果在单元向共享位置写入数据时重新引导 NFS 服务器，则在导出配置中使用 sync 选项可防止在共享位置出现数据损坏。导出文件系统的子目录时，在导出配置中使用 no_subtree_check 选项可提高可靠性。

必须允许 vCloud Director 服务器组中的每个服务器通过检查 NFS 导出的导出列表来挂载 NFS 共享。通过运行 exportfs –a 重新导出所有 NFS 共享以导出挂载。NFS 守护进程 rpcinfo –p localhost 或 service nfs status 必须在服务器上运行。

计划将 vCloud Director 安装升级到更高版本时的注意事项

在升级 vCloud Director 服务器组的过程中，请运行升级版本的安装文件以升级 vCloud Director 服务器组的所有成员。为方便起见，某些组织选择将升级安装文件下载到传输服务器存储位置并从该位置运行文件，因为所有单元都有权访问该位置。由于必须以 **root** 用户身份运行升级安装文件，因此如果要使用传输服务器存储位置运行升级，则必须确保 **root** 用户可以在执行升级时运行升级安装文件。如果无法以 **root** 用户身份运行升级，则必须将文件复制到能够以 **root** 用户身份运行的其他位置，例如，NFS 挂载外部的其他目录。

下载和安装 VMware 公钥

安装文件带有数字签名。若要验证签名，必须下载和安装 VMware 公钥。

可以使用 Linux rpm 工具和 VMware 公钥验证 vCloud Director 安装文件的数字签名，或从 vmware.com 下载的任何其他签名文件。如果在计划安装 vCloud Director 的计算机上安装公钥，则会在安装或升级过程中进行验证。在开始安装或升级过程之前，还可以手动验证签名，然后将经过验证的文件应用于所有安装或升级过程。

注 下载站点还发布下载的校验和值。校验和以两种常见形式发布。通过验证校验和可验证下载文件的内容是否与发布文件的内容相同。它不验证数字签名。

步骤

1. 创建目录以存储 VMware 打包公钥。
2. 使用 Web 浏览器从 http://packages.vmware.com/tools/keys 目录下载所有 VMware 打包公钥。
3. 将密钥文件保存到创建的目录。
4. 对于下载的每个密钥，请运行以下命令以导入密钥。

```
# rpm --import /key_path/key_name
```

key_path 是保存密钥的目录。

key_name 是密钥的文件名。

为 vCloud Director 安装和配置 NSX Data Center for vSphere

如果希望 vCloud Director 安装使用来自 NSX Data Center for vSphere 的网络资源，则必须安装和配置 NSX Data Center for vSphere 并将唯一的 NSX Manager 实例与您计划包含在 vCloud Director 安装中的每个 vCenter Server 实例相关联。

NSX Manager 包含在 NSX Data Center for vSphere 下载中。有关 vCloud Director 和其他 VMware 产品之间兼容性的最新信息，请参见 VMware 产品互操作性列表，网址为 http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php。有关网络要求的信息，请参见 vCloud Director 的网络配置要求。

重要事项 此过程仅在对 vCloud Director 执行全新安装时适用。如果要升级 vCloud Director 的现有安装，请参见第 11 章 升级 vCloud Director 并修补 vCloud Director 设备。

前提条件

确认每个 vCenter Server 系统均满足安装 NSX Manager 的必备条件。

步骤

1 执行 NSX Manager 虚拟设备的安装任务。

请参见《NSX 安装指南》。

2 登录到已安装的 NSX Manager 虚拟设备并确认在安装期间指定的设置。

3 将已安装的 NSX Manager 虚拟设备与您打算在计划的 vCloud Director 安装中添加到 vCloud Director 的 vCenter Server 系统相关联。

4 在关联的 NSX Manager 实例中配置 VXLAN 支持。

vCloud Director 将创建 VXLAN 网络池以向提供者 VDC 提供网络资源。如果未在关联的 NSX Manager 中配置 VXLAN 支持，则提供者 VDC 将显示一条网络池错误，您必须创建一个其他类型的网络池，并将其与提供者 VDC 相关联。有关配置 VXLAN 支持的详细信息，请参见《NSX 管理指南》。

5 （可选） 如果您希望系统中的 Edge 网关提供分布式路由，请设置 NSX Controller 群集。

请参见《NSX 管理指南》。

为 vCloud Director 安装和配置 NSX-T Data Center

如果希望 vCloud Director 安装使用来自 NSX-T Data Center 的网络资源，则必须安装 NSX-T Data Center 并至少配置一个 NSX-T Manager 实例。

NSX-T Manager 包含在 NSX-T Data Center 下载中。有关 vCloud Director 和其他 VMware 产品之间兼容性的最新信息，请参见 VMware 产品互操作性列表，网址为 http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php。有关网络要求的信息，请参见 vCloud Director 的网络配置要求。

重要事项 此过程仅在对 vCloud Director 执行全新安装时适用。如果要升级 vCloud Director 的现有安装，请参见第 11 章 升级 vCloud Director 并修补 vCloud Director 设备。

前提条件

您必须熟悉 NSX-T Data Center。

步骤

1. 安装 NSX-T Manager 虚拟设备。

   请参见《NSX-T 安装指南》。

2. 准备要在 NSX-T Data Center 中操作的 ESXi 主机。

   请参见《NSX-T 安装指南》。

3. 根据云要求创建传输节点和传输区域。

   请参见《NSX-T 安装指南》。

4. 配置 Edge 节点和群集。

   请参见《NSX-T 安装指南》。

5. 配置第 0 层和第 1 层路由器。

   请参见《NSX-T 管理指南》。

6. 配置要导入到 vCloud Director 安装中的一个或多个 VLAN 或覆盖逻辑交换机。

   请参见《NSX-T 管理指南》。

后续步骤

安装 vCloud Director 后，您可以将 NSX-T Manager 实例注册到云中。有关注册 NSX-T Manager 实例的信息，请参见《适用于服务提供商的 vCloud API 编程指南》。

在 Linux 上为 vCloud Director 创建和管理 SSL 证书

4

vCloud Director 使用 SSL 来保护客户端和服务器之间的通信。每个 vCloud Director 服务器都必须支持两个不同的 SSL 端点，一个用于 HTTPS 通信，一个用于控制台代理通信。

这两个端点可以采用单独的 IP 地址，也可以采用具有两个不同端口的单个 IP 地址。每个端点都需要具有自己的 SSL 证书。您可以对这两个端点使用相同的证书，例如，使用通配符证书。

本章讨论了以下主题：

在 Linux 上为 vCloud Director 创建 SSL 证书之前

安装适用于 Linux 的 vCloud Director 时，必须为服务器组的每个成员创建两个证书，并将证书导入主机密钥库。

注 只有在 Linux 上安装 vCloud Director 后，才必须为服务器组成员创建证书。vCloud Director 设备在首次引导时创建自签名 SSL 证书。

步骤

1. 以 **root** 身份登录 vCloud Director 服务器。
2. 列出服务器的 IP 地址。

   使用诸如 `ifconfig` 等命令来发现此服务器的 IP 地址。
3. 对于每个 IP 地址，运行以下命令，检索 IP 地址绑定到的完全限定域名 (FQDN)。

   ```
   nslookup ip-address
   ```
4. 记下每个 IP 地址及与其关联的 FQDN。如果为这两个服务使用的不是单个 IP 地址，请确定将哪个 IP 地址用于 HTTPS 服务，哪个 IP 地址用于控制台代理服务。

   创建证书时，必须提供 FQDN；配置网络和数据库连接时，必须提供 IP 地址。记下可访问 IP 地址的任何其他 FQDN，因为如果希望证书包含主体备用名称，必须提供这些 FQDN。

后续步骤

为两个端点创建证书。可以使用由受信任证书颁发机构 (CA) 签名的证书，也可以使用自签名证书。

注 CA 签名证书提供最高级别的信任。

- 有关创建和导入 CA 签名的 SSL 证书的信息，请参见在 Linux 上为 vCloud Director 创建 CA 签名 SSL 证书密钥库。
- 有关创建自签名 SSL 证书的信息，请参见在 Linux 上为 vCloud Director 创建自签名 SSL 证书。
- 有关导入您自己的私钥和 CA 签名证书文件的信息，请参见在 Linux 上使用导入的私钥为 vCloud Director 创建 CA 签名的 SSL 证书密钥库。

在 Linux 上为 vCloud Director 创建自签名 SSL 证书

对于信任问题无关紧要的环境，自签名证书为配置 vCloud Director 的 SSL 提供了一种快捷简便的方式。

每个 vCloud Director 服务器都要求在一个 JCEKS 密钥库文件中有两个 SSL 证书，一个用于 HTTPS 服务，另一个用于控制台代理服务。

使用 `cell-management-tool` 创建自签名 SSL 证书。`cell-management-tool` 实用程序会在运行配置代理之前且运行安装文件之后安装在单元上。请参见在服务器组的第一个成员上安装 vCloud Director。

重要事项 这些示例指定 2048 位密钥大小，但应先评估安装的安全要求，然后再选择适当的密钥大小。根据 NIST 特殊出版物 800-131A，不再支持小于 1024 位的密钥大小。

步骤

1 以 **root** 身份直接或通过 SSH 客户端登录到 vCloud Director 服务器的操作系统。

2 运行以下命令，为 HTTPS 服务和控制台代理服务创建公钥和私钥密钥对。

```
/opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o certificates.ks -w passwd
```

该命令将在 `certificates.ks` 中创建或更新密钥库，密码为 `passwd`。`cell-management-tool` 使用该命令的默认值创建证书。根据环境的 DNS 配置，颁发者 CN 设置为每个服务的 IP 地址或 FQDN。证书使用默认的 2048 位密钥长度，并在创建 1 年后过期。

重要事项 密钥库文件及其存储目录必须可由用户 **vcloud.vcloud** 读取。vCloud Director 安装程序将创建此用户和组。

后续步骤

记下密钥库路径名称。运行配置脚本为 vCloud Director 单元建立网络和数据库连接时，需要使用密钥库路径名称。请参见配置网络和数据库连接。

在 Linux 上为 vCloud Director 创建 CA 签名 SSL 证书密钥库

创建和导入 CA 签名的证书为 SSL 通信提供了最高级别的信任，并有助于保护云计算基础架构中的连接。

每个 vCloud Director 服务器都需要两个 SSL 证书来保护客户端和服务器之间的通信。每个 vCloud Director 服务器都必须支持两个不同的 SSL 端点，一个用于 HTTPS 通信，一个用于控制台代理通信。

这两个端点可以采用单独的 IP 地址，也可以采用具有两个不同端口的单个 IP 地址。每个端点都需要具有自己的 SSL 证书。您可以对这两个端点使用相同的证书，例如，使用通配符证书。

两个端点的证书都必须包含 X.500 标识名和 X.509 主体备用名称扩展。

可以使用由可信证书颁发机构 (CA) 签名的证书，也可以使用自签名证书。

使用 `cell-management-tool` 创建自签名 SSL 证书。在运行配置代理之前和运行安装文件之后，在单元上安装 `cell-management-tool` 实用程序。请参见在服务器组的第一个成员上安装 vCloud Director。

如果您拥有自己的私钥和 CA 签名证书文件，请按照在 Linux 上使用导入的私钥为 vCloud Director 创建 CA 签名的 SSL 证书密钥库中所述的过程操作。

重要事项 这些示例指定 2048 位密钥大小，但应先评估安装的安全要求，然后再选择适当的密钥大小。根据 NIST 特殊出版物 800-131A，不再支持小于 1024 位的密钥大小。

前提条件

- 确认您有权访问具有 Java 版本 8 或更高版本运行时环境的计算机，以便可以使用 `keytool` 命令导入证书。vCloud Director 安装程序会将 `keytool` 副本放在以下位置：`/opt/vmware/vcloud-director/jre/bin/keytool`，但您可以在安装了 Java 运行时环境的任何计算机上执行此过程。使用任何其他源中的 `keytool` 所创建的证书均无法与 vCloud Director 一起使用。以下命令行示例假定 `keytool` 位于用户的路径中。
- 熟悉 `keytool` 命令。
- 有关 `generate-certs` 命令的可用选项的更多详细信息，请参见为 HTTPS 和控制台代理端点生成自签名证书。
- 有关 `certificates` 命令的可用选项的更多详细信息，请参见替换 HTTP 和控制台代理端点的证书。

步骤

1. 以 **root** 身份直接或通过 SSH 客户端登录到 vCloud Director 服务器单元的操作系统。
2. 运行以下命令，为 HTTPS 服务和控制台代理服务创建公钥和私钥密钥对。

```
/opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o certificates.ks -w keystore_password
```

该命令使用指定密码将在 `certificates.ks` 中创建或更新密钥库。将使用命令的默认值创建证书。根据环境的 DNS 配置，颁发者 CN 设置为每个服务的 IP 地址或 FQDN。证书使用默认的 2048 位密钥长度，并在创建 1 年后过期。

重要事项 密钥库文件及其存储目录必须可由用户 **vcloud.vcloud** 读取。vCloud Director 安装程序将创建此用户和组。

3 为 HTTPS 服务和控制台代理服务创建证书签名请求。

重要事项 如果要为 HTTPS 服务和控制台代理服务使用单独 IP 地址，请调整以下命令中的主机名和 IP 地址。

a 在 `http.csr` 文件中创建证书签名请求。

```
keytool –keystore certificates.ks –storetype JCEKS –storepass keystore_password –certreq –
alias http –file http.csr –ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

b 在 `consoleproxy.csr` 文件中创建证书签名请求。

```
keytool –keystore certificates.ks –storetype JCEKS –storepass keystore_password –certreq –
alias consoleproxy –file consoleproxy.csr –ext
"san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

4 将证书签名请求发送给证书颁发机构。

如果您的证书颁发机构要求您指定 Web 服务器类型，则使用 Jakarta Tomcat。

您将获取 CA 签名证书。

5 将签名证书导入到 JCEKS 密钥库。

a 将证书颁发机构的根证书从 `root.cer` 文件导入 `certificates.ks` 密钥库文件。

```
keytool –import –storetype JCEKS –storepass keystore_password –keystore certificates.ks –
alias root –file root_certificate_file
```

b 如果收到的是中间证书，则将其从 `intermediate.cer` 文件导入 `certificates.ks` 密钥库文件。

```
keytool –import –storetype JCEKS –storepass keystore_password –keystore certificates.ks –
alias intermediate –file intermediate_certificate_file
```

c 导入 HTTPS 服务证书。

```
keytool -import -storetype JCEKS -storepass keystore_password -keystore certificates.ks -
alias http -file http_certificate_file
```

d 导入控制台代理服务证书。

```
keytool -import -storetype JCEKS -storepass keystore_password -keystore certificates.ks -
alias consoleproxy -file console_proxy_certificate_file
```

这些命令将使用新获取的 CA 签名版证书覆盖 `certificates.ks` 文件。

6 要检查证书是否已导入 JCEKS 密钥库，请运行以下命令，列出密钥库文件的内容。

```
keytool -storetype JCEKS -storepass keystore_password -keystore certificates.ks -list
```

7 对服务器组中的所有 vCloud Director 服务器重复此过程。

后续步骤

- 如果尚未配置 vCloud Director 实例，请运行 `configure` 脚本将证书密钥库导入 vCloud Director。请参见配置网络和数据库连接。

  注 创建 `certificates.ks` Keystore 文件时使用的是计算机，而不是您生成完全限定域名及其关联 IP 地址的列表的服务器，请立即将 Keystore 文件复制到该服务器。运行配置脚本时，您需要提供密钥库路径名称。

- 如果已安装并配置 vCloud Director 实例，请使用单元管理工具的 `certificates` 命令导入证书密钥库。请参见替换 HTTP 和控制台代理端点的证书。

在 Linux 上使用导入的私钥为 vCloud Director 创建 CA 签名的 SSL 证书密钥库

如果您有自己的私钥和 CA 签名证书文件，则在将密钥库导入到 vCloud Director 环境之前，您必须创建密钥库文件，在其中导入 HTTPS 和控制台代理服务的证书和私钥。

前提条件

- 请参见在 Linux 上为 vCloud Director 创建 SSL 证书之前。
- 确认您有权访问具有 Java 版本 8 或更高版本运行时环境的计算机，以便可以使用 `keytool` 命令导入证书。vCloud Director 安装程序会将 `keytool` 副本放在以下位置：`/opt/vmware/vcloud-director/jre/bin/keytool`，但您可以在安装了 Java 运行时环境的任何计算机上执行此过程。使用任何其他源中的 `keytool` 所创建的证书均无法与 vCloud Director 一起使用。以下命令行示例假定 `keytool` 位于用户的路径中。
- 熟悉 `keytool` 命令。
- 下载并安装 OpenSSL。
- 有关 `certificates` 命令的可用选项的更多详细信息，请参见替换 HTTP 和控制台代理端点的证书。

步骤

1 如果有中间证书，请运行以下命令以将根 CA 签名证书与中间证书合并使用，并创建证书链。

```
cat intermediate-certificate-file-1.cer intermediate-certificate-file-2.cer root-CA-certificate.cer > chain.crt
```

2 使用 OpenSSL 为 HTTPS 和控制台代理服务创建中间 PKCS12 密钥库文件，其中包含私钥、证书链和相应别名，然后为每个密钥库文件指定密码。

a 为 HTTPS 服务创建密钥库文件。

```
openssl pkcs12 -export -in http.crt -inkey http.key -CAfile chain.crt -name http -passout pass:keystore_password -out http.pfx -chain
```

b 为控制台代理服务创建密钥库文件。

```
openssl pkcs12 -export -in consoleproxy.crt -inkey consoleproxy.key -CAfile chain.crt -name consoleproxy -passout pass:keystore_password -out consoleproxy.pfx -chain
```

3 使用 keytool 将 PKCS12 密钥库导入到 JCEKS 密钥库。

a 运行命令以导入 HTTPS 服务的 PKCS12 密钥库。

```
keytool -importkeystore -deststorepass keystore_password -destkeystore certificates.ks -deststoretype JCEKS -srckeystore http.pfx -srcstoretype PKCS12 -srcstorepass keystore_password
```

b 运行命令以导入控制台代理服务的 PKCS12 密钥库。

```
keytool -importkeystore -deststorepass keystore_password -destkeystore certificates.ks -deststoretype JCEKS -srckeystore consoleproxy.pfx -srcstoretype PKCS12 -srcstorepass keystore_password
```

4 要检查证书是否已导入 JCEKS 密钥库，请运行以下命令，列出密钥库文件的内容。

```
keytool -storetype JCEKS -storepass keystore_password -keystore certificates.ks -list
```

5 在环境中的所有 vCloud Director 单元上重复此过程。

后续步骤

- 如果尚未配置 vCloud Director 实例，请运行 configure 脚本将证书密钥库导入 vCloud Director。请参见配置网络和数据库连接。

  注 如果创建 certificates.ks 密钥库文件时使用的是某台计算机，而不是生成完全限定域名及其关联 IP 地址列表的服务器，请将密钥库文件复制到该服务器。运行配置脚本时，您需要提供密钥库路径名称。

- 如果已安装并配置 vCloud Director 实例，请使用单元管理工具的 certificates 命令导入证书密钥库。请参见替换 HTTP 和控制台代理端点的证书。

在 Linux 上安装 vCloud Director

5

可以通过在一个或多个 Linux 服务器上安装 vCloud Director 软件创建 vCloud Director 服务器组。第一个组成员的安装和配置将创建一个响应文件，您应使用该文件配置组的其他成员。

此过程仅适用于新安装。如果要升级现有的 vCloud Director 安装，请参见第 11 章 升级 vCloud Director 并修补 vCloud Director 设备。

重要事项 不支持在一个服务器组中的 Linux 和 vCloud Director 设备部署中混合安装 vCloud Director。

前提条件

- 确认服务器组的目标服务器满足第 2 章 vCloud Director 硬件和软件要求。
- 确认为服务器组的目标服务器的每个端点创建了 SSL 证书。SSL 证书的路径名中的所有目录必须可由任何用户读取。在服务器组的所有成员上使用相同的密钥库路径可简化安装过程，例如 `/tmp/certificates.ks`。请参见在 Linux 上为 vCloud Director 创建 SSL 证书之前。
- 确认已准备好 vCloud Director 服务器组的所有目标服务器都可以访问的 NFS 或其他共享存储卷。请参见准备传输服务器存储。
- 确认已创建组中所有服务器均可访问的 vCloud Director 数据库。请参见准备 vCloud Director 数据库。确认重新引导数据库服务器时数据库服务启动。
- 确认所有 vCloud Director 服务器、数据库服务器、所有 vCenter Server 系统及关联的 NSX Manager 实例可以按照 vCloud Director 的网络配置要求中所述解析环境中的每个主机名。
- 验证所有 vCloud Director 服务器和数据库服务器是否均能按照 vCloud Director 的网络配置要求中所述容差与网络时间服务器同步。
- 如果计划从 LDAP 服务中导入用户或组，请验证每台 vCloud Director 服务器是否均可访问该服务。
- 打开网络安全要求中所示的防火墙端口。在 vCloud Director 和 vCenter Server 系统之间，必须打开端口 443。

步骤

1 在服务器组的第一个成员上安装 vCloud Director

准备好环境并确认必备条件后，可以开始在第一个目标 Linux 服务器上运行 vCloud Director 安装程序以创建 vCloud Director 服务器组。

2 配置网络和数据库连接

在服务器组的第一个成员上安装 vCloud Director 后，必须运行配置脚本，以便为此单元创建网络和数据库连接。脚本将创建一个响应文件，配置服务器组的其他成员时必须使用该文件。

3 在服务器组的其他成员上安装 vCloud Director

您可以随时将服务器添加到 vCloud Director 服务器组中。服务器组中的所有服务器必须使用相同的数据库连接详细信息进行配置，因此必须使用配置服务器组的第一个成员时创建的响应文件。

4 设置 vCloud Director

安装并配置 vCloud Director 服务器组中的所有服务器后，必须设置 vCloud Director 安装。vCloud Director 安装程序会使用许可证密钥、系统管理员帐户和相关信息初始化 vCloud Director 数据库。

后续步骤

可以开始将资源添加到 vCloud Director 安装。要开始使用 vCloud Director，请参见《vCloud Director 管理员指南》。

在服务器组的第一个成员上安装 vCloud Director

准备好环境并确认必备条件后，可以开始在第一个目标 Linux 服务器上运行 vCloud Director 安装程序以创建 vCloud Director 服务器组。

适用于 Linux 的 vCloud Director 作为数字签名的可执行文件分发，名称格式为 `vmware-vcloud-director-distribution-`*v.v.v*`-nnnnnn.bin`，其中 *v.v.v* 表示产品版本，nnnnnn 则为内部版本号。例如：`vmware-vcloud-director-distribution-8.10.0-3698331.bin`。运行此可执行文件可安装或升级 vCloud Director。

vCloud Director 安装程序将验证目标服务器是否满足所有平台必备条件，然后在其上安装 vCloud Director 软件。

前提条件

- 验证您是否拥有目标服务器的超级用户凭据。
- 如果要安装程序验证安装文件的数字签名，则在目标服务器上下载和安装 VMware 公钥。如果已验证安装文件的数字签名，则不需要在安装期间再次验证。请参见下载和安装 VMware 公钥。

步骤

1 以 **root** 身份登录到目标服务器。

2 将安装文件下载到目标服务器。

如果以媒体形式购买软件，请将安装文件复制到所有目标服务器均可访问的位置。

3 验证下载的校验和是否与下载页上发布的校验和相匹配。

MD5 和 SHA1 校验和的值发布在下载页上。使用适当的工具验证已下载安装文件的校验和是否与下载页上显示的校验和相匹配。使用以下形式的 Linux 命令可显示 *installation-file* 的校验和。

```
[root@cell1 /tmp]# md5sum installation-file
```

该命令将返回必须与下载页面上的 MD5 校验和相匹配的安装文件校验和。

4 确保安装文件为可执行文件。

安装文件需要执行权限。要确保安装文件具有此权限，请打开控制台、Shell 或终端窗口，并运行以下 Linux 命令，其中 *installation-file* 是 vCloud Director 安装文件的完整路径名。

```
[root@cell1 /tmp]# chmod u+x installation-file
```

5 运行安装文件。

要运行安装文件，请输入完整路径名，例如：

```
[root@cell1 /tmp]# ./installation-file
```

该文件包括安装脚本和嵌入式 RPM 包。

注 无法从其路径名包含任何嵌入式空格符的目录运行安装文件。

如果未在目标服务器上安装 VMware 公钥，安装程序将显示以下形式的警告：

```
warning:installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

安装程序将执行以下操作。

a 验证主机是否满足所有要求。

b 验证安装文件上的数字签名。

c 创建 `vcloud` 用户和组。

d 解压 vCloud Director RPM 软件包。

e 安装软件。

安装完成时，安装程序会提示您运行配置脚本，此脚本可配置网络和数据库连接。

6 选择是否运行配置脚本。

a 要在交互式模式下运行配置脚本，请输入 **y** 并按 Enter。

b 要稍后在交互式模式或无人参与模式下运行配置脚本，请输入 **n** 并按 Enter。

配置网络和数据库连接

在服务器组的第一个成员上安装 vCloud Director 后，必须运行配置脚本，以便为此单元创建网络和数据库连接。脚本将创建一个响应文件，配置服务器组的其他成员时必须使用该文件。

vCloud Director 服务器组的所有成员均共享数据库连接及其他配置详细信息。在 vCloud Director 服务器组的第一个成员上运行配置脚本时，该脚本会创建一个响应文件，该文件会保留数据库连接信息以供后续服务器安装使用。

您可以在交互模式或无人参与模式下运行配置脚本。对于交互式配置，可运行不带选项的命令，脚本会提示您输入所需的设置信息。对于无人参与配置，可通过使用命令选项提供设置信息。

如果要使用具有两个不同端口（用于 HTTP 服务和控制台代理服务）的单个 IP 地址，必须在无人参与模式下运行配置脚本。

注 单元管理工具包括可用于更改初始配置的网络和数据库连接详细信息的子命令。使用这些子命令进行的更改会写入到全局配置文件和响应文件中。有关使用单元管理工具的信息，请参见《vCloud Director 管理员指南》。

前提条件

- 对于交互式配置，查看 交互式配置参考。
- 对于无人参与配置，查看 无人参与的配置参考。
- 对于无人参与配置，确认环境变量 `VCLOUD_HOME` 的值设置为 vCloud Director 安装目录的完整路径名。此值通常为 `/opt/vmware/vcloud-director`。

步骤

1. 以 root 身份登录 vCloud Director 服务器。
2. 运行 `configure` 命令：
   - 对于交互式模式，运行命令并在出现提示时提供所需的信息。

     ```
     /opt/vmware/vcloud-director/bin/configure
     ```

   - 对于无人参与模式，运行带有相应选项和参数的命令。

     ```
     /opt/vmware/vcloud-director/bin/configure options -unattended
     ```

   脚本验证信息后：

   a 初始化数据库并将其连接到服务器。

   b 显示 vCloud Director 服务启动后可用于连接到 **VMware vCloud Director 设置**向导的 URL。

   c 启动 vCloud Director 单元。
3. （可选） 记下 **VMware vCloud Director 设置**向导 URL，并输入 **y** 以启动 vCloud Director 服务。

   可以决定稍后通过运行 `service vmware-vcd start` 命令启动服务。

结果

您在配置期间提供的数据库连接信息和其他可重用信息均保留在响应文件中，该文件位于此服务器上的 `/opt/vmware/vcloud-director/etc/responses.properties`。此文件包含许多敏感信息。向服务器组添加服务器时，必须重用这些信息。

后续步骤

将响应文件副本保存在一个安全的位置。限制它的访问权限，并确保将其备份到安全位置。备份文件时，避免通过公共网络发送明文。

如果计划将服务器添加到服务器组，请将共享传输存储挂载到 `/opt/vmware/vcloud-director/data/transfer`。

交互式配置参考

在交互模式下运行 `configure` 脚本时，该脚本将提示您输入以下信息。

要接受默认值，请按 Enter。

表 5-1. 交互式网络和数据库配置期间所需的信息

所需信息	描述
HTTP 服务的 IP 地址	默认为第一个可用的 IP 地址。
控制台代理服务的 IP 地址	默认为第一个可用的 IP 地址。 **注** 如果要使用具有两个不同端口（用于 HTTP 服务和控制台代理服务）的单个 IP 地址，必须在无人参与模式下运行配置脚本。
Java 密钥库文件的完整路径	例如，`/opt/keystore/certificates.ks`。
密钥库的密码	请参见在 Linux 上为 vCloud Director 创建 SSL 证书之前。
HTTP SSL 证书的私钥密码	请参见在 Linux 上为 vCloud Director 创建 SSL 证书之前。
控制台代理 SSL 证书的私钥密码	请参见在 Linux 上为 vCloud Director 创建 SSL 证书之前。
启用远程审核日志记录到 syslog 主机	每个 vCloud Director 单元中的服务均会将审核消息记录到 vCloud Director 数据库，并保留 90 天。要将审核消息保留更长时间，可以将 vCloud Director 服务配置为除了将审核消息发送到 vCloud Director 数据库之外，还将其发送到 `syslog` 实用程序。 ■ 要跳过，请按 Enter。 ■ 要启用，请输入 syslog 主机名或 IP 地址。
如果已启用远程审核日志记录，则需要 syslog 主机的 UDP 端口	默认值为 514。
数据库类型	PostgreSQL 或 Microsoft SQL Server。 默认值为 PostgreSQL。
数据库服务器的名称或 IP 地址	运行数据库的服务器。

表 5-1. 交互式网络和数据库配置期间所需的信息 （续）

所需信息	描述
数据库端口	对于 PostgreSQL，默认值为 5432。 对于 Microsoft SQL Server，默认值为 1433。
数据库名称	默认值为 vcloud。
如果数据库类型为 Microsoft SQL Server，则为数据库实例	默认值为默认实例。
数据库用户名	请参见准备 vCloud Director 数据库。
数据库密码	请参见准备 vCloud Director 数据库。
加入或不加入 VMware 客户体验提升计划 (CEIP)	此产品已加入 VMware 客户体验提升计划（“CEIP”）。有关通过 CEIP 收集的数据的详细信息以及 VMware 将其用于何种用途已在“信任与保证中心”中列明，网址为 http://www.vmware.com/trustvmware/ceip.html。您可以随时使用单元管理工具加入或退出此产品的 VMware CEIP。请参见《vCloud Director 管理员指南》中的“单元管理工具参考”。 要加入该计划，请输入 **y**。 如果您不希望加入 VMware CEIP 计划，请输入 **n**。

无人参与的配置参考

在无人参与模式下运行 `configure` 脚本时，可以在命令行以选项和参数形式提供设置信息。

表 5-2. 配置实用程序选项和参数

选项	参数	描述
`--help (-h)`	无	显示配置选项和参数的摘要
`--config-file (-c)`	`global.properties` 文件的路径	运行配置实用程序时提供的信息保存在此文件中。如果忽略此选项，则默认位置为 `/opt/vmware/vcloud-director/etc/global.properties`。
`--console-proxy-ip (-cons)`	IPv4 地址，带有可选端口号	系统会将此地址用于 vCloud Director 控制台代理服务。例如，*10.17.118.159*。
`--console-proxy-port-https`	范围 0-65535 内的整数	用于 vCloud Director 控制台代理服务的端口号。
`--database-ssl`	`true` 或 `false`	如果您使用的是 PostgreSQL 数据库，则可以将该数据库配置为需要从 vCloud Director 发出已正常签名的 SSL 连接。如果 `--database-type` 不是 `postgres`，则将忽略。 如果要将 PostgreSQL 数据库配置为使用自签名或专用证书，请参见在外部 PostgreSQL 数据库上执行其他配置。

表 5-2. 配置实用程序选项和参数 （续）

选项	参数	描述
`--database-host (-dbhost)`	vCloud Director 数据库主机的 IP 地址或完全限定域名	请参见准备 vCloud Director 数据库。
`--database-domain (-dbdomain)`	SQL Server 数据库用户域	如果 `--database-type` 为 `sqlserver`，则为可选。
`--database-instance (-dbinstance)`	SQL Server 数据库实例	如果 `--database-type` 为 `sqlserver`，则使用。
`--database-name (-dbname)`	数据库服务名称	请参见准备 vCloud Director 数据库。
`--database-password (-dbpassword)`	数据库用户的密码。可以为空。	请参见准备 vCloud Director 数据库。
`--database-port (-dbport)`	数据库主机上的数据库服务所使用的端口号	请参见准备 vCloud Director 数据库。
`--database-type (-dbtype)`	数据库类型。可以为： ■ `postgres` ■ `sqlserver`	请参见准备 vCloud Director 数据库。
`--database-user (-dbuser)`	数据库用户的用户名。	请参见准备 vCloud Director 数据库。
`--enable-ceip`	`true` 或 `false`	此产品已加入 VMware 客户体验提升计划（“CEIP”）。有关通过 CEIP 收集的数据的详细信息以及 VMware 将其用于何种用途已在“信任与保证中心”中列明，网址为 http://www.vmware.com/trustvmware/ceip.html。您可以随时使用单元管理工具加入或退出此产品的 VMware CEIP。请参见《vCloud Director 管理员指南》中的“单元管理工具参考”。
`--uuid (-g)`	无	为单元生成新的唯一标识符
`--primary-ip (-ip)`	IPv4 地址，带有可选端口号	系统会将此地址用于 vCloud Director Web 界面服务。例如，*10.17.118.159*。
`--primary-port-http`	范围 0 到 65535 内的整数	用于到 vCloud Director Web 界面服务的 HTTP（不安全）连接的端口号
`--primary-port-https`	范围 0-65535 内的整数	用于到 vCloud Director Web 界面服务的 HTTPS（安全）连接的端口号
`--keystore (-k)`	包含 SSL 证书和专用密钥的 Java 密钥库的路径	必须为完整路径名。例如，`/opt/keystore/certificates.ks`。

表 5-2. 配置实用程序选项和参数 （续）

选项	参数	描述
--syslog-host (-loghost)	Syslog 服务器主机的 IP 地址或完全限定域名	每个 vCloud Director 单元中的服务均会将审核消息记录到 vCloud Director 数据库，并保留 90 天。要将审核消息保留更长时间，可以将 vCloud Director 服务配置为除了将审核消息发送到 vCloud Director 数据库之外，还将其发送到 syslog 实用程序。
--syslog-port (-logport)	范围 0-65535 内的整数	syslog 进程监控指定服务器所使用的端口。默认值为 514（如果未指定）。
--response-file (-r)	响应文件的路径	必须为完整路径名。默认值为 /opt/vmware/vcloud-director/etc/responses.properties（如果未指定）。运行配置时提供的所有信息都会保留在此文件中。 **重要事项** 此文件包含许多敏感信息。向服务器组添加服务器时，必须重用这些信息。将该文件保留在一个安全的位置，并仅在需要时使用。
--unattended-installation (-unattended)	无	指定无人参与安装
--keystore-password (-w)	SSL 证书密钥库密码	SSL 证书密钥库密码。

示例： 具有两个 IP 地址的无人参与配置

以下示例命令针对具有两个不同 IP 地址（用于 HTTP 服务和控制台代理服务）的 vCloud Director 服务器运行无人参与配置。

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./configure -ip 10.17.118.159 -cons 10.17.118.158 \
-dbtype sqlserver -dbhost 10.150.10.78 -dbname mssql-db -dbuser vcloud --enable-ceip true \
-dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret -loghost 10.150.10.10 -unattended
```

示例： 具有单个 IP 地址的无人参与配置

以下示例命令针对具有单个 IP 地址（具有两个端口分别用于 HTTP 服务和控制台代理服务）的 vCloud Director 服务器运行无人参与配置。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./configure -ip 10.17.118.159 --primary-port-https 9000 -cons 10.17.118.159 \
--console-proxy-port-https 9010 -dbtype sqlserver -dbhost 10.150.10.78 -dbname mssql-db \
-dbuser vcloud -dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret \
-loghost 10.150.10.10 --enable-ceip true -unattended
```

保护和重用响应文件

您在第一个 vCloud Director 单元上配置的网络和数据库连接详细信息保存在响应文件中。此文件包含许多敏感信息。向服务器组添加服务器时，必须重用这些信息。您必须将该文件保存在一个安全的位置。

响应文件位于您配置网络和数据库连接的第一台服务器的以下路径中：`/opt/vmware/vcloud-director/etc/responses.properties`。将服务器添加到组时，您必须使用响应文件的副本来提供所有服务器共享的配置参数。

重要事项 单元管理工具包括可用于更改最初指定的网络和数据库连接详细信息的子命令。使用这些工具进行的更改将写入全局配置文件和响应文件，因此必须确保拥有相应的可写入响应文件（位于 `/opt/vmware/vcloud-director/etc/responses.properties`），才能使用这些命令修改该文件。

步骤

1 保护响应文件。

将文件副本保存在一个安全的位置。限制它的访问权限，并确保将其备份到安全位置。备份文件时，请避免通过公共网络发送明文。

2 重用响应文件。

a 将该文件复制到已准备好配置的服务器可访问的位置。

注 必须先在服务器上安装 vCloud Director 软件，才能重用响应文件以对其进行配置。响应文件的路径名中的所有目录必须可由用户 `vcloud.vcloud` 读取，如此例中所示。

```
[root@cell1 /tmp]# ls -l responses.properties
-rw------- 1 vcloud vcloud 418 Jun 8 13:42 responses.properties
```

安装程序将创建此用户和组。

b 通过使用 `-r` 选项并指定响应文件的路径名来运行配置脚本。

以 root 用户身份登录，打开控制台、Shell 或终端窗口，并键入：

```
[root@cell1 /tmp]# /opt/vmware/vcloud-director/bin/configure -r /path-to-response-file
```

后续步骤

在配置其他服务器之后，请删除配置服务器所使用的响应文件副本。

在服务器组的其他成员上安装 vCloud Director

您可以随时将服务器添加到 vCloud Director 服务器组中。服务器组中的所有服务器必须使用相同的数据库连接详细信息进行配置，因此必须使用配置服务器组的第一个成员时创建的响应文件。

重要事项 不支持在一个服务器组中的 Linux 和 vCloud Director 设备部署中混合安装 vCloud Director。

前提条件

- 确认您能够访问配置此服务器组的第一个成员时创建的响应文件。请参见配置网络和数据库连接。
- 确认在 vCloud Director 服务器组的第一个成员上的 `/opt/vmware/vcloud-director/data/transfer` 挂载共享传输存储。

步骤

1 以 **root** 身份登录到目标服务器。

2 将安装文件下载到目标服务器。

如果以媒体形式购买软件，请将安装文件复制到所有目标服务器均可访问的位置。

3 确保安装文件为可执行文件。

安装文件需要执行权限。要确保安装文件具有此权限，请打开控制台、Shell 或终端窗口，并运行以下 Linux 命令，其中 *installation-file* 是 vCloud Director 安装文件的完整路径名。

```
[root@cell1 /tmp]# chmod u+x installation-file
```

4 运行安装文件。

要运行安装文件，请输入完整路径名，例如：

```
[root@cell1 /tmp]# ./installation-file
```

该文件包括安装脚本和嵌入式 RPM 包。

注 无法从其路径名包含任何嵌入式空格符的目录运行安装文件。

如果未在目标服务器上安装 VMware 公钥，安装程序将显示以下形式的警告：

```
warning: installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

安装程序将执行以下操作。

a 验证主机是否满足所有要求。

b 验证安装文件上的数字签名。

c 创建 `vcloud` 用户和组。

d 解压 vCloud Director RPM 软件包。

e 安装软件。

安装完成时，安装程序会提示您运行配置脚本，此脚本可配置网络和数据库连接。

5 输入 **n** 并按 Enter，以拒绝运行配置脚本。

可以稍后通过提供响应文件作为输入来运行配置脚本。

6 将共享传输存储挂载到 `/opt/vmware/vcloud-director/data/transfer`。

服务器组中的所有 vCloud Director 服务器都必须将此卷挂载到同一个挂载点。

7 将响应文件复制到此服务器可访问的位置。

响应文件的路径名中的所有目录必须可由 root 用户读取。

8 运行配置脚本。

a 运行 `configure` 命令并提供响应文件的路径名。

```
/opt/vmware/vcloud-director/bin/configure -r /responses.properties
```

该脚本会将响应文件复制到 `vcloud.vcloud` 可读取的位置，然后使用响应文件作为输入运行配置脚本。

b 出现提示时，提供 HTTP 服务和控制台代理服务的 IP 地址。

c 如果出现提示时配置脚本在响应文件保存的路径名中找不到有效证书，请提供证书的路径名和密码。

该脚本将验证信息，将服务器连接到数据库并启动 vCloud Director 单元。

9 （可选） 输入 **y**，启动 vCloud Director 服务。

可以决定稍后通过运行 `service vmware-vcd start` 命令启动服务。

后续步骤

重复此过程以向此服务器组中添加更多服务器。

vCloud Director 服务在所有服务器上运行时，必须使用许可证密钥、系统管理员帐户和相关信息初始化 vCloud Director 数据库。您可以采用以下方式之一初始化数据库：

- 使用 Web 浏览器，在配置脚本完成时显示的 URL 中打开设置向导。请参见设置 vCloud Director。
- 使用单元管理工具和 `system-setup` 子命令。有关使用单元管理工具的信息，请参见《vCloud Director 管理员指南》。

设置 vCloud Director

安装并配置 vCloud Director 服务器组中的所有服务器后，必须设置 vCloud Director 安装。vCloud Director 安装程序会使用许可证密钥、系统管理员帐户和相关信息初始化 vCloud Director 数据库。

运行 **VMware vCloud Director 设置**向导后才能启动 vCloud Director Web 控制台，该向导收集 Web 控制台启动所需的信息。

除了使用 **VMware vCloud Director 设置**向导配置 vCloud Director 安装，还可以使用单元管理工具的 `system-setup` 子命令。有关单元管理工具的信息，请参见《vCloud Director 管理员指南》。

前提条件

- 确认已在所有服务器上启动 vCloud Director 服务。

- 从 VMware 许可证门户网站中获取 vCloud Director 产品序列号。

步骤

步骤

1 打开 Web 浏览器并转到配置脚本显示的 URL。

要发现 **VMware vCloud Director 设置**向导的 URL，您还可以查找与您在安装第一个服务器时为 HTTP 服务指定的 IP 地址关联的完全限定域名。要连接到向导，请转到 https://*fully-qualified-domain-name*，例如 https://mycloud.example.com。

注 启动向导可能需要几分钟的时间。

2 查看“欢迎使用”页面，然后单击**下一步**。

3 阅读并接受许可协议，然后单击**下一步**。

如果拒绝许可协议，则无法继续进行 vCloud Director 配置。

4 输入您的 vCloud Director 产品序列号，然后单击**下一步**。

5 输入 vCloud Director 系统管理员的用户名、密码和联系信息，然后单击**下一步**。

vCloud Director 系统管理员在整个云中具有超级用户特权。此系统管理员可以创建额外的系统管理员帐户。

6 配置可控制 vCloud Director 与 vSphere 以及 NSX Manager 交互方式的系统设置，然后单击**下一步**。

a 在**系统名称**文本框中，输入要用于此 vCloud Director 安装的 vCenter Server 文件夹的名称。

b 在**安装 ID** 文本框中，设置此 vCloud Director 安装的 ID 以便在为虚拟网卡创建 MAC 地址时使用。

如果打算在多站点部署中跨 vCloud Director 安装创建延伸网络，请考虑为每个 vCloud Director 安装设置一个唯一的安装 ID。

7 在“准备登录”页面上，检查设置，然后单击**完成**。

结果

配置过程完成后，系统会将您重定向到 vCloud Director Web 控制台登录页面。

后续步骤

使用系统管理员的用户名和密码登录到 vCloud Director Web 控制台，然后开始置备您的云。有关将资源添加到 vCloud Director 的信息，请参见《vCloud Director 管理员指南》。

部署 vCloud Director 设备

6

可以通过部署 vCloud Director 设备的一个或多个实例创建 vCloud Director 服务器组。您可以使用 vSphere Client (HTML5)、vSphere Web Client (Flex) 或 VMware OVF Tool 部署 vCloud Director 设备。

重要事项 不支持在一个服务器组中的 Linux 和 vCloud Director 设备部署中混合安装 vCloud Director。

vCloud Director 设备是一个预配置的虚拟机，专门针对运行 vCloud Director 服务进行了优化。

设备分发时采用的名称格式为 `VMware vCloud Director-`*v.v.v.v*`-`*nnnnnn*`_OVF10.ova`，其中 *v.v.v.v* 表示产品版本，*nnnnnn* 则为内部版本号。例如：`VMware vCloud Director-9.7.0.0-9229800_OVA10.ova`。

vCloud Director 设备软件包包含以下软件：

- VMware Photon™ 操作系统
- vCloud Director 服务组
- PostgreSQL 10

主-小型和备用-小型 vCloud Director 设备大小适用于实验室或测试系统。主-大型和备用-大型大小符合生产系统的最低规格要求。根据工作负载，您可能需要添加其他资源。

重要事项 不支持在 vCloud Director 设备上安装任何第三方组件。您只能基于 VMware 产品互操作性列表安装受支持的 VMware 组件。例如，可以安装受支持版本的 VMware vRealize® Operations Manager™ 或 VMware vRealize® Log Insight™ 监控代理。

设备数据库配置

从版本 9.7 开始，vCloud Director 设备包括一个具有高可用性 (HA) 功能的嵌入式 PostgreSQL 数据库。要使用数据库 HA 集群创建设备部署，必须将 vCloud Director 设备的一个实例部署为主单元，并将两个实例部署为备用单元。您可以将服务器组中的 vCloud Director 设备的其他实例部署为 vCD 应用程序单元，这些单元仅在没有嵌入式数据库的情况下运行 vCloud Director 服务组。vCD 应用程序单元连接到主单元中的数据库。请参见设备部署和数据库高可用性配置。

默认情况下，vCloud Director 设备使用 TLS（代替弃用的 SSL）进行数据库连接（包括复制）。此功能在部署后立即处于活动状态，并使用自签名的 PostgreSQL 证书。要使用证书颁发机构 (CA) 的签名证书，请参见替换自签名嵌入式 PostgreSQL 和 vCloud Director 设备管理 UI 证书。

注 vCloud Director 设备不支持外部数据库。

设备网络配置

从版本 9.7 开始，vCloud Director 设备部署了两个网络（`eth0` 和 `eth1`），以便您可以将 HTTP 流量与数据库流量隔离开来。不同的服务侦听一个或两个对应的网络接口。

服务	`eth0` 上的端口	`eth1` 上的端口
SSH	22	22
HTTP	80	不可用
HTTPS	443	不可用
PostgreSQL	不可用	5432
管理 UI	5480	5480
控制台代理	8443	不可用
JMX	8998、8999	不可用
JMS/ActiveMQ	61616	不可用

vCloud Director 设备通过使用 `iptables` 支持用户自定义防火墙规则。要添加自定义 `iptables` 规则，您可以将自己的配置数据添加到 `/etc/systemd/scripts/iptables` 文件的末尾。

本章讨论了以下主题：

- 设备部署和数据库高可用性配置
- 部署 vCloud Director 设备的必备条件
- 使用 vSphere Web Client 或 vSphere Client 部署 vCloud Director 设备
- 使用 VMware OVF Tool 部署 vCloud Director 设备

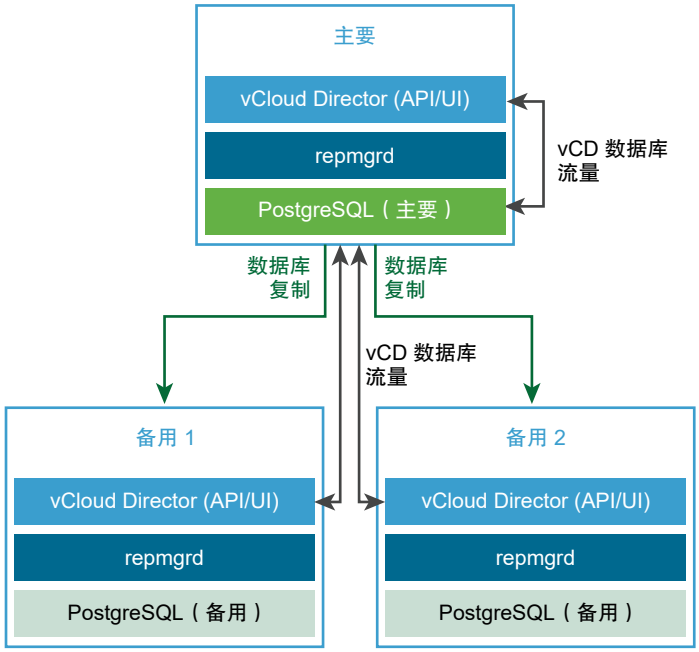
设备部署和数据库高可用性配置

vCloud Director 设备包括一个嵌入式 PostgreSQL 数据库。嵌入式 PostgreSQL 数据库包括复制管理器 (repmgr) 工具套件，可为 PostgreSQL 服务器群集提供高可用性 (HA) 功能。使用为 vCloud Director 数据库提供故障切换功能的数据库 HA 群集，您可以创建设备部署。

您可以将 vCloud Director 设备部署为主单元、备用单元或 vCD 应用程序单元。请参见 使用 vSphere Web Client 或 vSphere Client 部署 vCloud Director 设备、使用 VMware OVF Tool 部署 vCloud Director 设备或使用用于 HTTPS 和控制台代理通信的签名通配符证书部署 vCloud Director 设备。

要为 vCloud Director 数据库配置 HA，创建服务器组时，可以通过部署 vCloud Director 设备的一个主实例和两个备用实例来配置数据库 HA 群集。

图 6-1. vCloud Director 设备数据库 HA 群集



创建具有数据库 HA 的 vCloud Director 设备部署

要创建具有数据库 HA 配置的 vCloud Director 服务器组，请遵循以下工作流：

1 将 vCloud Director 设备部署为主单元。

主单元是 vCloud Director 服务器组中的第一个成员。嵌入式数据库配置为 vCloud Director 数据库。数据库名称是 `vcloud`，数据库用户是 `vcloud`。

2 验证该主单元是否已启动且正在运行。

a 要验证 vCloud Director 服务运行状况，请使用**系统管理员**凭据登录到 vCloud Director Web 控制台，网址为 `https://primary_eth0_ip_address/cloud`。

b 要验证 PostgreSQL 数据库运行状况，请以 **root** 身份登录到设备管理用户界面，网址为 `https://primary_eth1_ip_address:5480`。

主节点必须处于运行状态。

3 将 vCloud Director 设备的两个实例部署为备用单元。

嵌入式数据库是在主数据库的复制模式下配置的。

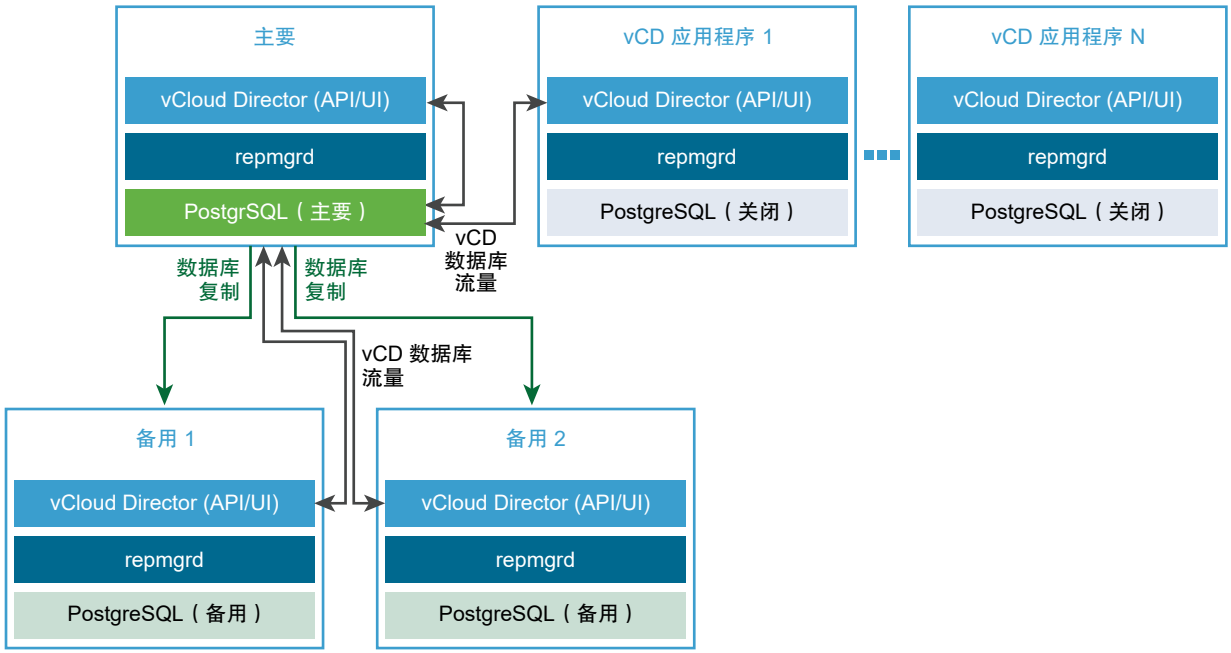
注 在初始备用设备部署之后，复制管理器开始将其数据库与主设备数据库同步。在此期间，vCloud Director 数据库以及 vCloud Director UI 不可用。

4 验证 HA 群集中的所有单元是否都处于运行状态。

请参见查看数据库高可用性群集中单元的状态。

5 （可选）将 vCloud Director 设备的一个或多个实例部署为 vCD 应用程序单元。

不使用嵌入式数据库。vCD 应用程序单元连接到主数据库。



创建不具有数据库 HA 的 vCloud Director 设备部署

要创建不具有数据库 HA 配置的 vCloud Director 服务器，请遵循以下工作流：

1 将 vCloud Director 设备部署为主单元。

主单元是 vCloud Director 服务器组中的第一个成员。嵌入式数据库配置为 vCloud Director 数据库。数据库名称是 `vcloud`，数据库用户是 `vcloud`。

2 验证该主单元是否已启动且正在运行。

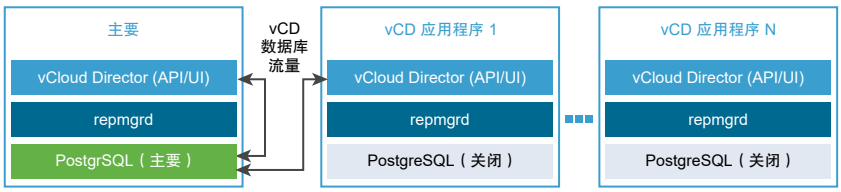
a 要验证 vCloud Director 服务运行状况，请使用**系统管理员**凭据登录到 vCloud Director Web 控制台，网址为 `https://primary_eth0_ip_address/cloud`。

b 要验证 PostgreSQL 数据库运行状况，请以 **root** 身份登录到设备管理用户界面，网址为 `https://primary_eth1_ip_address:5480`。

主节点必须处于运行状态。

3 （可选）将 vCloud Director 设备的一个或多个实例部署为 vCD 应用程序单元。

不使用嵌入式数据库。vCD 应用程序单元连接到主数据库。



部署 vCloud Director 设备的必备条件

要确保 vCloud Director 设备成功部署，在开始部署之前必须执行一些必要的任务和预检查。

- 确认您有权访问 vCloud Director.ova 文件。
- 部署主设备之前，请准备 NFS 共享传输服务存储。请参见准备传输服务器存储。

  注 共享传输服务存储既不能包含 responses.properties 文件，也不能包含 appliance-nodes 目录。

- 安装和配置 RabbitMQ AMQP 代理。

vCloud Director 设备部署方法

- 使用 vSphere Web Client 或 vSphere Client 部署 vCloud Director 设备
- 使用 VMware OVF Tool 部署 vCloud Director 设备
- 使用用于 HTTPS 和控制台代理通信的签名通配符证书部署 vCloud Director 设备

使用 vSphere Web Client 或 vSphere Client 部署 vCloud Director 设备

可以使用 vSphere Web Client (Flex) 或 vSphere Client (HTML5) 将 vCloud Director 设备部署为 OVF 模板。

您必须将 vCloud Director 服务器组的第一个成员部署为主单元。可以将 vCloud Director 服务器组的后续成员部署为备用单元或 vCD 应用程序单元。请参见设备部署和数据库高可用性配置。

重要事项 不支持在一个服务器组中的 Linux 和 vCloud Director 设备部署中混合安装 vCloud Director。

有关在 vSphere 中部署 OVF 模板的信息，请参见《vSphere 虚拟机管理》。

或者，您可以使用 VMware OVF Tool 部署设备。请参见使用 VMware OVF Tool 部署 vCloud Director 设备。

注 不支持在 vCloud Director 中部署 vCloud Director 设备。

前提条件

请参见部署 vCloud Director 设备的必备条件。

步骤

1 开始 vCloud Director 设备部署

要开始设备部署，可以在 vSphere Web Client (Flex) 或 vSphere Client (HTML5) 中打开部署向导。

2 自定义 vCloud Director 设备并完成部署

要配置 vCloud Director 详细信息，需要自定义设备模板。

后续步骤

- 配置公用控制台代理地址，因为 vCloud Director 设备将其 `eth0` 网卡及自定义端口 8443 用于控制台代理服务。请参见自定义公用端点。
- 要向 vCloud Director 服务器组添加成员，请重复此过程。
- 要输入许可证密钥，请登录到 vCloud Director Web 控制台。
- 要替换设备首次引导期间创建的自签名证书，可以在 Linux 上为 vCloud Director 创建 CA 签名 SSL 证书密钥库。

开始 vCloud Director 设备部署

要开始设备部署，可以在 vSphere Web Client (Flex) 或 vSphere Client (HTML5) 中打开部署向导。

步骤

1. 在 vSphere Web Client 或 vSphere Client 中，右键单击任何清单对象，然后单击**部署 OVF 模板**。
2. 输入 vCloud Director `.ova` 文件的路径，然后单击**下一步**。
3. 输入虚拟机的名称并浏览 vCenter Server 存储库以选择要部署设备的数据中心或文件夹，然后单击**下一步**。
4. 选择要部署设备的 ESXi 主机或群集，然后单击**下一步**。
5. 查看模板详细信息，然后单击**下一步**。
6. 阅读并接受许可协议，然后单击**下一步**。
7. 选择部署类型和大小，然后单击**下一步**。

   主-小型和备用-小型 vCloud Director 设备大小适用于实验室或测试系统。主-大型和备用-大型大小符合生产系统的最低规格要求。根据工作负载，您可能需要添加其他资源。

选项	描述
主-小型	将具有 12 GB RAM 和 2 个 vCPU 的设备部署为 vCloud Director 服务器组中的第一个成员。 主单元中的嵌入式数据库配置为 vCloud Director 数据库。数据库名称是 `vcloud`，数据库用户是 `vcloud`。
主-大型	将具有 24 GB RAM 和 4 个 vCPU 的设备部署为 vCloud Director 服务器组中的第一个成员。 主单元中的嵌入式数据库配置为 vCloud Director 数据库。数据库名称是 `vcloud`，数据库用户是 `vcloud`。
备用-小型	用于在数据库 HA 群集中加入主-小型单元。 将具有 12 GB RAM 和 2 个 vCPU 的设备部署为具有数据库高可用性配置的 vCloud Director 服务器组中的第二个或第三个成员。 备用单元中的嵌入式数据库是在主数据库的复制模式下配置的。

选项	描述
备用-大型	用于在数据库 HA 群集中加入主-大型单元。 将具有 24 GB RAM 和 4 个 vCPU 的设备部署为具有数据库高可用性配置的 vCloud Director 服务器组中的第二个或第三个成员。 备用设备中的嵌入式数据库是在复制模式下与主数据库一同配置的。
vCD 单元应用程序	将具有 8 GB RAM 和 2 个 vCPU 的设备部署为 vCloud Director 服务器组中的后续成员。 不使用 vCD 应用程序单元中的嵌入式数据库。vCD 应用程序单元连接到主数据库。

重要事项 vCloud Director 服务器组中的主单元和备用单元必须具有相同的大小。一个数据库 HA 群集可以由一个主-小型单元和两个备用-小型单元组成，也可以由一个主-大型单元和两个备用-大型单元组成。

部署后，您可以重新配置设备的大小。

8 为虚拟机配置文件和虚拟磁盘选择磁盘格式和数据存储，然后单击**下一步**。

厚格式可提高性能，而精简格式可节约存储空间。

9 从**目标网络**单元的下拉菜单中，为该设备的 `eth1` 和 `eth0` 网卡选择目标网络。

源网络列表的顺序可能相反。确认为每个源网络选择的目标网络正确。

重要事项 两个目标网络必须不同。

10 从 **IP 分配设置**下拉菜单中，选择**静态-手动** IP 分配，然后选择 **IPv4** 协议。

11 单击**下一步**。

您将被重定向到**自定义模板**页面以配置 vCloud Director 详细信息。

自定义 vCloud Director 设备并完成部署

要配置 vCloud Director 详细信息，需要自定义设备模板。

自定义 vCloud Director 设备时，您需要配置设备设置、数据库和网络属性。仅当部署主设备（即服务器组的第一个成员）时，才配置初始系统设置。

注 仅此过程的 步骤 3 可选。您必须完成所有其他步骤才能自定义 vCloud Director 设备。

步骤

1 在 **VCD 设备设置**中，配置设备详细信息。

设置	描述
NTP 服务器	要使用的 NTP 服务器的主机名或 IP 地址。
初始 root 密码	设备的初始 root 密码。必须至少包含八个字符、一个大写字符、一个小写字符、一个数字和一个特殊字符。 **重要事项** 初始 root 密码将成为密钥库密码。群集部署要求所有单元在初始部署期间具有相同的 root 密码。引导过程完成后，您可以更改任何所需单元上的 root 密码。 **注** OVF 部署向导不会根据密码条件验证初始 root 密码。
首次登录时使 Root 密码过期	如果要在首次登录后继续使用初始密码，必须确认初始密码符合 root 密码条件。要在首次登录后继续使用初始 root 密码，请取消选中此选项。
启用 SSH	默认禁用。
用作传输文件位置的 NFS 挂载	请参见准备传输服务器存储。

注 有关更改设备日期、时间或时区的信息，请参见 https://kb.vmware.com/kb/59674。

2 如果要部署服务器组的第一个成员，请在 **VCD 配置 - 仅适用于“主”设备**部分中，输入数据库详细信息，创建**系统管理员**帐户，并配置系统设置。

数据库名称是 `vcloud`，数据库用户是 `vcloud`。

设置	描述
“vcloud”用户的“vcloud”数据库密码	`vcloud` 数据库用户的密码。
管理员用户名	**系统管理员**帐户的用户名。默认值为 `administrator`。
管理员全名	**系统管理员**的全名。默认值为 `vCD Admin`。
管理员用户密码	**系统管理员**帐户的密码。
管理员电子邮件	**系统管理员**的电子邮件地址。
系统名称	要为此 vCloud Director 安装创建的 vCenter Server 文件夹的名称。默认值为 `vcd1`。
安装 ID	为虚拟网卡创建 MAC 地址时要使用的此 vCloud Director 安装的 ID。默认值为 1。 如果打算在多站点部署中跨 vCloud Director 安装创建延伸网络，请考虑为每个 vCloud Director 安装设置一个唯一的安装 ID。

3 （可选） 在**其他网络属性**部分中，如果您的网络拓扑需要，请输入 `eth0` 和 `eth1` 网络接口的静态路由，然后单击**下一步**。

如果要通过非默认网关路由访问主机，则可能需要提供静态路由。例如，管理基础架构只能通过 `eth1` 接口访问，而默认网关位于 `eth0` 上。在大多数情况下，此设置可以保留为空。

静态路由必须位于以逗号分隔的路由规范列表中。路由规范必须由目标网关 IP 地址和可选的无类域间路由 (CIDR) 网络规范组成。例如，
`172.16.100.253 172.16.100.0/19, 172.16.100.253 192.168.100.0/24`。

4 在**网络属性**部分中，输入 `eth0` 和 `eth1` 网卡的网络详细信息，然后单击**下一步**。

注 所有设置都是必需的。

设置	描述
默认网关	设备的默认网关的 IP 地址。
域名	域名，例如，*mydomain.com*。
域搜索路径	设备的域搜索路径以逗号或空格分隔的域名列表。
域名服务器	设备的域名服务器的 IP 地址。
eth0 网络 IP 地址	`eth0` 接口的 IP 地址。
eth0 网络掩码	`eth0` 接口的网络掩码或前缀。
eth1 网络 IP 地址	`eth1` 接口的 IP 地址。
eth1 网络掩码	`eth1` 接口的网络掩码或前缀。

5 在**即将完成**页面上，查看 vCloud Director 设备的配置设置，然后单击**完成**开始部署。

后续步骤

打开新创建的虚拟机的电源。

使用 VMware OVF Tool 部署 vCloud Director 设备

可以使用 VMware OVF Tool 将 vCloud Director 设备部署为 OVF 模板。

您必须将 vCloud Director 服务器组的第一个成员部署为主单元。可以将 vCloud Director 服务器组的后续成员部署为备用单元或 vCD 应用程序单元。请参见设备部署和数据库高可用性配置。

有关安装 OVF Tool 的信息，请参见《VMware OVF Tool 发行说明》文档。

有关使用 OVF Tool 的信息，请参见《OVF Tool 用户指南》。

在运行部署命令之前，请参见部署 vCloud Director 设备的必备条件。

在部署设备后，查看首次引导日志文件中是否存在警告错误消息。请参见检查 vCloud Director 设备中的日志文件。

用于部署 vCloud Director 设备的 ovftool 命令选项和属性

选项	值	描述
`--noSSLVerify`	不可用	跳过 vSphere 连接的 SSL 验证。
`--acceptAllEulas`	不可用	接受所有最终用户许可协议 (EULA)。
`--datastore`	*target_vc_datastore*	用于存储虚拟机配置文件和虚拟磁盘的目标数据存储名称。

选项	值	描述
--allowAllExtraConfig	不可用	将所有额外的配置选项转换为 VMX 格式。
--net:"eth0 Network"	*portgroup_on_vc_for_eth0*	设备 eth0 网络的目标网络。 **重要事项** 必须与 eth1 目标网络不同。
--net:"eth1 Network"	*portgroup_on_vc_for_eth1*	设备 eth1 网络的目标网络。 **重要事项** 必须与 eth0 目标网络不同。
--name	*vm_name_on_vc*	设备的虚拟机名称。
--diskMode	thin 或 thick	虚拟机配置文件和虚拟磁盘的磁盘格式。
--prop:"vami.ip0.VMware_vCloud_Director"	*eth0_ip_address*	eth0 的 IP 地址。用于 UI 和 API 访问。在此地址上，DNS 反向查找确定并设置设备的主机名。
--prop:"vami.ip1.VMware_vCloud_Director"	*eth1_ip_address*	eth1 的 IP 地址。用于访问包括嵌入式 PostreSQL 数据库服务在内的内部服务。
--prop:"vami.DNS.VMware_vCloud_Director"	*dns_ip_address*	设备的域名服务器的 IP 地址。
--prop:"vami.domain.VMware_vCloud_Director"	*domain_name*	DNS 搜索域。在搜索路径中显示为第一个元素。
--prop:"vami.gateway.VMware_vCloud_Director"	*gateway_ip_address*	设备的默认网关的 IP 地址。
--prop:"vami.netmask0.VMware_vCloud_Director"	*netmask*	eth0 接口的网络掩码或前缀。
--prop:"vami.netmask1.VMware_vCloud_Director"	*netmask*	eth1 接口的网络掩码或前缀。
--prop:"vami.searchpath.VMware_vCloud_Director"	*comma_separated_list_of_domain_names*	设备的域搜索路径。 以逗号或空格分隔的域名列表。
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"	true 或 false	启用或禁用对设备的 SSH **root** 访问权限。
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"	true 或 false	确定首次登录后是否继续使用初始密码。
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"	*nfs_ip_address*:*nfs_mount_path*	外部 NFS 服务器的 IP 地址和导出路径。 仅用于主单元。
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"	*ntp_server_ip_address*	时间服务器的 IP 地址。
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"	*vCloud_Director_root_password*	设备的初始 root 密码。必须至少包含八个字符、一个大写字符、一个小写字符、一个数字和一个特殊字符。 **重要事项** 初始 root 密码将成为密钥库密码。集群部署要求所有单元在初始部署期间具有相同的 root 密码。引导过程完成后，您可以更改任何所需单元上的 root 密码。
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"	*db_password*	**vcloud** 用户的数据库密码。 仅用于主单元。
--prop:"vcloudwiz.admin_email.VMware_vCloud_Director"	*vcd_admin_email_address*	**系统管理员**帐户的电子邮件地址。 仅用于主单元。

选项	值	描述
--prop:"vcloudwiz.admin_fname.VMware_vCloud_Director_	*Admin_first_name*	**系统管理员**帐户的名称。 仅用于主单元。
--prop:"vcloudwiz.admin_pwd.VMware_vCloud_Director_	*Admin_password*	**系统管理员**帐户的密码。 仅用于主单元。
--prop:"vcloudwiz.admin_uname.VMware_vCloud_Director_	*Admin_user_name*	**系统管理员**帐户的用户名。 仅用于主单元。
--prop:"vcloudwiz.inst_id.VMware_vCloud_Director_	*Installation_ID*	vCloud Director 安装 ID。 仅用于主单元。
--prop:"vcloudconf.sys_name.VMware_vCloud_Director_	*System_name*	要为此 vCloud Director 安装创建的 vCenter Server 文件夹的名称。
--prop:"vcloudnet.routes0.VMware_vCloud_Director_	*"ip_address1 cidr, ip_address2, ...*	可选。`eth0` 接口的静态路由。必须是以逗号分隔的路由规范列表。路由规范必须由网关 IP 地址和可选的无类域间路由 (CIDR) 网络规范（前缀/位）组成。例如，**`172.16.100.253 172.16.100/19, 172.16.200.253`**。
--prop:"vcloudnet.routes1.VMware_vCloud_Director_	*"ip_address1 cidr, ip_address2, ...*	可选。`eth1` 接口的静态路由。必须是以逗号分隔的路由规范列表。路由规范必须由网关 IP 地址和可选的无类域间路由 (CIDR) 网络规范（前缀/位）组成。例如，**`172.16.100.253 172.16.100/19, 172.16.200.253`**。

选项	值	描述
--deploymentOption	primary-small、primary-large、standby-small、standby-large 或 cell	要部署的设备类型和大小。 主-小型和备用-小型设备大小适用于实验室或测试系统。主-大型和备用-大型大小符合生产系统的最低规格要求。根据工作负载，您可能需要添加其他资源。 ■ primary-small 会将具有 12 GB RAM 和 2 个 vCPU 的设备部署为 vCloud Director 服务器组中的第一个成员。主单元中的嵌入式数据库配置为 vCloud Director 数据库。数据库名称是 vcloud，数据库用户是 vcloud。 ■ primary-large 会将具有 24 GB RAM 和 4 个 vCPU 的设备部署为 vCloud Director 服务器组中的第一个成员。主单元中的嵌入式数据库配置为 vCloud Director 数据库。数据库名称是 vcloud，数据库用户是 vcloud。 ■ standby-small 会将具有 12 GB RAM 和 2 个 vCPU 的设备部署为具有数据库高可用性配置的 vCloud Director 服务器组中的第二个或第三个成员。备用单元中的嵌入式数据库是在主数据库的复制模式下配置的。 ■ standby-large 会将具有 24 GB RAM 和 4 个 vCPU 的设备部署为具有数据库高可用性配置的 vCloud Director 服务器组中的第二个或第三个成员。备用单元中的嵌入式数据库是在主数据库的复制模式下配置的。 ■ cell 会将具有 8 GB RAM 和 2 个 vCPU 的设备部署为 vCloud Director 服务器组中的后续成员。不使用 vCD 应用程序单元中的嵌入式数据库。vCD 应用程序单元连接到主数据库。 **重要事项** vCloud Director 服务器组中的主单元和备用单元必须具有相同的大小。一个数据库 HA 集群可以由一个主-小型单元和两个备用-小型单元组成，也可以由一个主-大型单元和两个备用-大型单元组成。 部署后，您可以重新配置设备的大小。
--powerOn	*path_to_ova*	部署后打开虚拟机电源。

用于部署主 vCloud Director 设备的命令示例

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig  \
```

```
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MyAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.142" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.24" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="44z1Bd1HwIt#" \
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"="XjO52mXAP7n#" \
--prop:"vcloudconf.admin_email.VMware_vCloud_Director"="admin@mycompany.com" \
--prop:"vcloudconf.admin_fname.VMware_vCloud_Director"="vcdadmin" \
--prop:"vcloudconf.admin_pwd.VMware_vCloud_Director"="o@e@vJW26Pnb" \
--prop:"vcloudconf.admin_uname.VMware_vCloud_Director"="administrator" \
--prop:"vcloudconf.inst_id.VMware_vCloud_Director"="59" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MyAppliance" \
--deploymentOption="primary-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_dataceter_name/host/vc_cluster_name
```

用于部署备用 vCloud Director 设备的命令示例

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig  \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MySecondAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.143" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.25" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="44z1Bd1HwIt#" \
```

```
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MySecondAppliance" \
--deploymentOption="standby-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_dataceter_name/host/vc_cluster_name
```

vCloud Director 设备 SSL 证书创建和管理

7

vCloud Director 设备使用 SSL 来保护客户端和服务器之间的通信。每个 vCloud Director 设备都必须支持两个不同的 SSL 端点 - 用于 HTTPS 通信和用于控制台代理通信。

这些端点可以是单独的 IP 地址，也可以是具有两个不同端口的单个 IP 地址。每个端点都需要具有自己的 SSL 证书。您可以对两个端点使用相同的证书（例如，通配符证书）。

本章讨论了以下主题：

- 使用用于 HTTPS 和控制台代理通信的签名通配符证书部署 vCloud Director 设备
- 创建 CA 签名的 SSL 证书并将其导入到 vCloud Director 设备
- 将私钥和 CA 签名的 SSL 证书导入到 vCloud Director 设备
- 替换自签名嵌入式 PostgreSQL 和 vCloud Director 设备管理 UI 证书
- 续订 vCloud Director 设备证书

使用用于 HTTPS 和控制台代理通信的签名通配符证书部署 vCloud Director 设备

可以使用签名通配符证书部署 vCloud Director 设备。可以使用这些证书保护属于证书中所列域名的子域的无限个服务器。

默认情况下，部署 vCloud Director 设备时，vCloud Director 会生成自签名证书，并使用这些证书配置 vCloud Director 单元以进行 HTTPS 和控制台代理通信。

成功部署主设备后，设备配置逻辑会将 `responses.properties` 文件从主设备复制到公用 NFS 共享传输服务存储（位于 `/opt/vmware/vcloud-director/data/transfer`）。为此 vCloud Director 服务器组部署的其他设备将使用此文件自动进行自我配置。`responses.properties` 文件包含 SSL 证书密钥库的路径，而路径中又包含了自动生成的自签名证书 `user.keystore.path`。默认情况下，此路径指向每个设备的本地密钥库文件。

部署主设备后，可以重新配置该设备以使用签名证书。有关创建包含签名证书的密钥库的详细信息，请参见创建 CA 签名的 SSL 证书并将其导入到 vCloud Director 设备。

如果在主 vCloud Director 设备上使用的签名证书是通配符签名证书，则这些证书可以应用于 vCloud Director 服务器组中的所有其他设备，即备用单元和 vCloud Director 应用程序单元。可以使用用于 HTTPS 和控制台代理通信的签名通配符证书部署设备，以便通过签名通配符 SSL 证书配置其他单元。

前提条件

- 确认包含用于 HTTPS 和控制台代理别名的签名通配符 SSL 证书的密钥库在主设备上可用，即 `/opt/vmware/vcloud-director/certificates.ks`。
  - 如果要创建密钥对并导入 CA 签名证书文件，请参见创建 CA 签名的 SSL 证书并将其导入到 vCloud Director 设备。
  - 如果已拥有自己的私钥和 CA 签名证书文件，请参见将私钥和 CA 签名的 SSL 证书导入到 vCloud Director 设备。
- 确认密钥库中密钥的专用密码与密钥库的密码一致。密钥库密码必须与部署所有设备时使用的初始 root 密码一致，例如

  ```
  /opt/vmware/vcloud-director/jre/bin/keytool -keypasswd -alias http_or_consoleproxy -keystore /opt/vmware/vcloud-director/certificates.ks -storetype jceks -storepass root-password
  ```

  。

步骤

1. 将包含完好签名证书的新 `certificates.ks` 文件从主设备复制到传输共享（位于 `/opt/vmware/vcloud-director/data/transfer/`）。
2. 将密钥库文件的所有者和组权限更改为 **vcloud**。

   ```
   chown vcloud.vcloud /opt/vmware/vcloud-director/data/transfer/certificates.ks
   ```
3. 确认密钥库文件的所有者具有读写权限。

   ```
   chmod 0750 /opt/vmware/vcloud-director/data/transfer/certificates.ks
   ```
4. 在主设备上，运行以下命令，将新的签名证书导入到 vCloud Director 实例。

   此命令还会更新传输共享中的 `responses.properties` 文件，从而将 *user.keystore.path* 变量修改为指向传输共享中的密钥库文件。

   ```
   /opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/vcloud-director/data/transfer/certificates.ks --keystore-password root-password
   ```
5. 要使新签名证书生效，请重新启动主设备上的 *vmware-vcd* 服务。

   ```
   service vmware-vcd restart
   ```
6. 使用与密钥库密码一致的初始 root 密码部署备用单元和应用程序单元设备。

结果

使用同一 NFS 共享传输服务存储的所有新部署的设备都配置了主设备所用的同一签名通配符 SSL 证书。

创建 CA 签名的 SSL 证书并将其导入到 vCloud Director 设备

创建和导入证书颁发机构 (CA) 签名的证书为 SSL 通信提供最高级别的信任，并有助于保护云中的连接。

每个 vCloud Director 服务器都需要两个 SSL 证书来保护客户端和服务器之间的通信。每个 vCloud Director 服务器都必须支持两个不同的 SSL 端点 - 用于 HTTPS 和控制台代理通信。

在 vCloud Director 设备中，这两个端点共享同一个 IP 地址或主机名，但使用两个不同的端口 - 443 用于 HTTPS 通信，8443 用于控制台代理通信。每个端点都必须有自己的 SSL 证书。您可以对这两个端点使用相同的证书，例如，使用通配符证书。

两个端点的证书都必须包含 X.500 标识名和 X.509 主体备用名称扩展。

如果您拥有自己的私钥和 CA 签名证书文件，请按照将私钥和 CA 签名的 SSL 证书导入到 vCloud Director 设备中所述的过程操作。

重要事项 部署后，vCloud Director 设备会生成密钥大小为 2048 位的自签名证书。必须先评估安装的安全要求，然后再选择适当的密钥大小。根据 NIST 特殊出版物 800-131A，不再支持小于 1024 位的密钥大小。

在此过程中使用的密钥库密码是 **root** 用户密码，表示为 *root_passwd*。

前提条件

熟悉 `keytool` 命令。您可以使用 `keytool` 将 CA 签名的 SSL 证书导入到 vCloud Director 设备。vCloud Director 将 `keytool` 的副本放在 `/opt/vmware/vcloud-director/jre/bin/keytool` 中。

步骤

1 以 **root** 身份直接或通过 SSH 登录到 vCloud Director 设备控制台。

2 根据您的环境需求，选择以下选项之一。

部署 vCloud Director 设备时，vCloud Director 会自动为 HTTPS 服务和控制台代理服务生成密钥大小为 2048 位的自签名证书。

- 如果您希望证书颁发机构对部署时生成的证书进行签名，请跳至步骤 步骤 5。
- 如果要使用自定义选项（如更大的密钥大小）生成新证书，请继续执行步骤 步骤 3。

3 运行命令以备份现有的 `certificates.ks` 文件。

```
cp /opt/vmware/vcloud-director/certificates.ks /root/certificates.ks.original
```

4 运行以下命令，为 HTTPS 服务和控制台代理服务创建公钥和私钥密钥对。

```
/opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o /opt/vmware/vcloud-director/certificates.ks -w root_passwd
```

该命令会使用您指定的密码在 `certificates.ks` 创建或更新密钥库。将使用命令的默认值创建证书。根据环境的 DNS 配置，颁发者公用名称 (CN) 设置为每个服务的 IP 地址或 FQDN。证书使用默认的 2048 位密钥长度，并在创建 1 年后过期。

重要事项 由于 vCloud Director 设备中的配置限制，必须为证书密钥库使用 `/opt/vmware/vcloud-director/certificates.ks` 位置。

注 您可以使用设备的 **root** 密码作为密钥库密码。

5 为 HTTPS 服务和控制台代理服务创建证书签名请求 (CSR)。

重要事项 vCloud Director 设备对 HTTPS 服务和控制台代理服务共享相同的 IP 地址和主机名。因此，CSR 创建命令必须为主体备用名称 (SAN) 扩展参数使用相同的 DNS 和 IP。

a 在 `http.csr` 文件中创建证书签名请求。

```
keytool -keystore certificates.ks -storetype JCEKS -storepass root_password -certreq -alias
http -file http.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

b 在 `consoleproxy.csr` 文件中创建证书签名请求。

```
keytool -keystore certificates.ks -storetype JCEKS -storepass root_password -certreq -alias
consoleproxy -file consoleproxy.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

6 将证书签名请求发送给证书颁发机构。

如果您的证书颁发机构要求您指定 Web 服务器类型，则使用 Jakarta Tomcat。

您将获取 CA 签名证书。

7 将 CA 签名证书、CA 根证书和任何中间证书复制到 vCloud Director 设备。

8 运行命令以将签名证书导入到 JCEKS 密钥库中。

a 将证书颁发机构的根证书从 `root.cer` 文件导入 `certificates.ks` 密钥库文件。

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-
director/certificates.ks -alias root -file root_certificate_file
```

b 如果收到的是中间证书，则将其从 `intermediate.cer` 文件导入 `certificates.ks` 密钥库文件。

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-
director/certificates.ks -alias intermediate -file intermediate_certificate_file
```

c 导入 HTTPS 服务证书。

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias http -file http_certificate_file
```

d 导入控制台代理服务证书。

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias consoleproxy -file console_proxy_certificate_file
```

这些命令将使用新获取的 CA 签名版证书覆盖 `certificates.ks` 文件。

9 要检查证书是否已导入，请运行以下命令，以列出密钥库文件的内容。

```
keytool -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -list
```

10 运行命令以将证书导入到 vCloud Director 实例中。

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/vcloud-director/certificates.ks --keystore-password root_password
```

11 要使新签名证书生效，请重新启动 vCloud Director 设备上的 `vmware-vcd` 服务。

```
service vmware-vcd restart
```

后续步骤

- 如果使用通配符证书，请参见使用用于 HTTPS 和控制台代理通信的签名通配符证书部署 vCloud Director 设备。
- 如果不使用通配符证书，请在服务器组中的所有 vCloud Director 服务器上重复此过程。
- 有关替换嵌入式 PostgreSQL 数据库和 vCloud Director 设备管理用户界面的证书的详细信息，请参见替换自签名嵌入式 PostgreSQL 和 vCloud Director 设备管理 UI 证书。

将私钥和 CA 签名的 SSL 证书导入到 vCloud Director 设备

如果您有自己的私钥和 CA 签名证书文件，则在将密钥库导入到 vCloud Director 环境之前，您必须创建密钥库文件，在其中导入 HTTPS 和控制台代理服务的证书和私钥。

前提条件

- 熟悉 `keytool` 命令。您可以使用 `keytool` 将 CA 签名的 SSL 证书导入到 vCloud Director 设备。vCloud Director 将 `keytool` 的副本放在 `/opt/vmware/vcloud-director/jre/bin/keytool` 中。
- 将中间证书、根 CA 证书、CA 签名的 HTTPS 服务和控制台代理服务私钥和证书复制到设备中。

步骤

1 以 **root** 身份直接或通过 SSH 登录到 vCloud Director 设备控制台。

2 如果有中间证书，请运行以下命令以将根 CA 签名证书与中间证书合并使用，并创建证书链。

```
cat intermediate-certificate-file-1.cer intermediate-certificate-file-2.cer root-CA-certificate.cer > chain.crt
```

3 使用 OpenSSL 为 HTTPS 和控制台代理服务创建中间 PKCS12 密钥库文件，其中包含私钥、证书链和相应别名，然后为每个密钥库文件指定密码。

a 为 HTTPS 服务创建密钥库文件。

```
openssl pkcs12 -export -in http.crt -inkey http.key -CAfile chain.crt -name http -passout pass:keystore_password -out http.pfx -chain
```

b 为控制台代理服务创建密钥库文件。

```
openssl pkcs12 -export -in consoleproxy.crt -inkey consoleproxy.key -CAfile chain.crt -name consoleproxy -passout pass:keystore_password -out consoleproxy.pfx -chain
```

4 运行命令以备份现有的 `certificates.ks` 文件。

```
cp /opt/vmware/vcloud-director/certificates.ks /root/certificates.ks.original
```

5 使用 `keytool` 命令将 PKCS12 密钥库导入到 JCEKS 密钥库。

a 导入 HTTPS 服务的 PKCS12 密钥库。

```
keytool -importkeystore -deststorepass keystore_password -destkeystore /opt/vmware/vcloud-director/certificates.ks -deststoretype JCEKS -srckeystore http.pfx -srcstoretype PKCS12 -srcstorepass keystore_password
```

b 导入控制台代理服务的 PKCS12 密钥库。

```
keytool -importkeystore -deststorepass keystore_password -destkeystore /opt/vmware/vcloud-director/certificates.ks -deststoretype JCEKS -srckeystore consoleproxy.pfx -srcstoretype PKCS12 -srcstorepass keystore_password
```

6 验证证书导入是否成功。

```
keytool -storetype JCEKS -storepass keystore_password -keystore /opt/vmware/vcloud-director/certificates.ks -list
```

7 运行命令以将签名证书导入到 vCloud Director 实例中。

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/vcloud-director/certificates.ks --keystore-password keystore_password
```

8 要使 CA 签名的证书生效，请重新启动 vCloud Director 设备上的 `vmware-vcd` 服务。

```
service vmware-vcd restart
```

后续步骤

- 如果使用通配符证书，请参见使用用于 HTTPS 和控制台代理通信的签名通配符证书部署 vCloud Director 设备。
- 如果不使用通配符证书，请在服务器组中的所有 vCloud Director 设备单元上重复此过程。
- 有关替换嵌入式 PostgreSQL 数据库和 vCloud Director 设备管理用户界面的证书的详细信息，请参见替换自签名嵌入式 PostgreSQL 和 vCloud Director 设备管理 UI 证书。

替换自签名嵌入式 PostgreSQL 和 vCloud Director 设备管理 UI 证书

默认情况下，嵌入式 PostgreSQL 数据库和 vCloud Director 设备管理用户界面共享一组自签名 SSL 证书。为了提高安全性，可以将默认的自签名证书替换为证书颁发机构 (CA) 签名的证书。

部署 vCloud Director 设备时，将生成自签名证书，有效期为 365 天。vCloud Director 设备使用两组 SSL 证书。vCloud Director 服务使用一组证书进行 HTTPS 和控制台代理通信。嵌入式 PostgreSQL 数据库和 vCloud Director 设备管理用户界面共享另一组 SSL 证书。

注 替换数据库和设备管理 UI 证书的过程不会影响用于 HTTPS 和控制台代理通信的证书。替换其中一组证书并不意味着必须替换另一组证书。

步骤

1 将位于 `/opt/vmware/appliance/etc/ssl/vcd_ova.csr` 的证书签名请求发送到 CA 以进行签名。

2 如果要替换主数据库的证书，请将所有其他节点置于维护模式，以防数据丢失。

3 将 `/opt/vmware/appliance/etc/ssl/vcd_ova.crt` 中的现有 PEM 格式证书替换为在步骤 1 中从 CA 获取的签名证书。

4 要获取新证书，请重新启动 vpostgres、nginx 和 vcd_ova_ui 服务。

```
systemctl restart nginx.service && systemctl restart vcd_ova_ui.service
```

```
systemctl restart vpostgres.service
```

5 如果要替换主数据库的证书，请将所有其他节点退出维护模式。

结果

下次运行 `appliance-sync` 函数时，新证书将导入到其他 vCloud Director 单元上的 vCloud Director 信任存储区。该操作可能需要长达 60 秒的时间。

续订 vCloud Director 设备证书

部署 vCloud Director 设备时，将生成自签名证书，有效期为 365 天。如果您的环境中存在即将过期或已过期的证书，则可以生成新的自签名证书。必须分别为每个 vCloud Director 单元续订证书。

vCloud Director 设备使用两组 SSL 证书。vCloud Director 服务使用一组证书进行 HTTPS 和控制台代理通信。嵌入式 PostgreSQL 数据库和 vCloud Director 设备管理用户界面共享另一组 SSL 证书。

您可以更改这两组自签名证书。或者，如果使用 CA 签名证书进行 vCloud Director 的 HTTPS 和控制台代理通信，则只能更改嵌入式 PostgreSQL 数据库和设备管理 UI 证书。CA 签名证书包括一个知名公共证书颁发机构的完整信任链。

前提条件

如果要为数据库高可用性群集中的主节点续订证书，请将所有其他节点置于维护模式，以防数据丢失。请参见管理单元。

步骤

1 以 **root** 身份直接或通过 SSH 登录到 vCloud Director 设备的操作系统。

2 要停止 vCloud Director 服务，请运行以下命令。

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u administrator cell --shutdown
```

3 要生成新的自签名证书，请运行以下命令。

```
/opt/vmware/appliance/bin/generate-certificates.sh <root-password>
```

此命令会自动为嵌入式 PostgreSQL 数据库和设备管理 UI 使用新生成的证书。PostgreSQL 和 Nginx 服务器将重新启动。该命令生成新的证书密钥库 `/opt/vmware/vcloud-director/certificates.ks`，其中包含用于进行 vCloud Director 的 HTTPS 和控制台代理通信的新自签名证书，这些证书将在 步骤 4 中使用。

4 如果未使用 CA 签名证书，请运行以下命令，将新生成的自签名证书导入到 vCloud Director。

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/
vcloud-director/certificates.ks --keystore-password <root-password>
```

5 重新启动 vCloud Director 服务。

```
service vmware-vcd start
```

结果

续订的自签名证书将在 vCloud Director 用户界面中可见。

下次运行 `appliance-sync` 函数时，新的 PostgreSQL 证书将导入到其他 vCloud Director 单元上的 vCloud Director 信任存储区。该操作可能需要长达 60 秒的时间。

后续步骤

如有必要，可以使用外部或内部证书颁发机构签名的证书替换自签名证书。

vCloud Director 设备配置

8

可以查看数据库 HA 群集中各单元的状态，可以备份和还原嵌入式数据库，还可以重新配置设备设置。

部署 vCloud Director 设备后，您将无法更改此设备的 `eth0` 和 `eth1` 网络 IP 地址或主机名。如果希望 vCloud Director 设备使用不同的地址或主机名，则必须部署一个新设备。

如果必须对需要关闭数据库高可用性群集的设备进行维护，则必须先关闭主设备，然后再关闭备用设备，以避免出现同步问题。

本章讨论了以下主题：

- 查看数据库高可用性群集中单元的状态
- 从高可用性群集中的主数据库故障中恢复
- vCloud Director 设备的嵌入式数据库备份和还原
- 配置对 vCloud Director 数据库的外部访问
- 启用或禁用对 vCloud Director 设备的 SSH 访问
- 编辑 vCloud Director 设备的 DNS 设置
- 编辑 vCloud Director 设备网络接口的静态路由
- vCloud Director 设备中的配置脚本
- 修改 vCloud Director 设备中的 PostgreSQL 配置

查看数据库高可用性群集中单元的状态

要查看设备数据库高可用性 (HA) 群集中主单元和备用单元的状态，可以登录到数据库 HA 群集中的任何单元的设备管理用户界面。

vCloud Director 设备数据库 HA 群集由一个主单元和两个备用单元组成。请参见设备部署和数据库高可用性配置。

步骤

1 在 Web 浏览器中，转至设备管理用户界面 `https://vcd_ip_address:5480`。

2 以 **root** 用户身份登录。

3 要查看有关数据库 HA 群集中的单元的详细信息，单击 **vCD 数据库可用性**。

属性	描述
名称	单元的 DNS 名称。
角色	可以是主单元或备用单元。 设备数据库 HA 群集由一个主单元和两个备用单元组成。
状态	可以是正在运行、无法访问或失败。 星号 (*) 指示主单元的状态。
沿用	备用单元复制的主单元的名称。

后续步骤

如果备用单元未处于运行状态，请部署新的备用单元。

如果主单元未处于运行状态，则从高可用性群集中的主数据库故障中恢复。

从高可用性群集中的主数据库故障中恢复

如果主单元无法正常运行，要恢复 vCloud Director 数据库，可以将其中一个备用单元提升为新的主单元。之后，必须部署一个新的备用单元。

前提条件

- 主单元处于无法访问或失败状态。
- 两个备用单元处于运行状态。

请参见查看数据库高可用性群集中单元的状态。

步骤

1 以 **root** 用户身份登录到正在运行的备用单元的设备管理用户界面 `https://standby_ip_address:5480`。

2 在要成为新主单元的备用单元的**角色**列中，单击**提升**。

该单元成为处于运行状态的新主单元。另一个备用单元将跟随新提升的主单元。

3 部署新的备用设备。

后续步骤

1 从 vCloud Director 服务器组和 repmgr 高可用性群集中移除出现故障的主设备。请参见删除云单元和取消注册数据库高可用性群集中出现故障的主单元 。

2 如有必要，删除出现故障的主设备。

vCloud Director 设备的嵌入式数据库备份和还原

可以备份 vCloud Director 设备的嵌入式 PostgreSQL 数据库，这有助于在出现故障后还原 vCloud Director 环境。

备份 vCloud Director 设备的嵌入式数据库

如果您的环境中包含具有嵌入式 PostgreSQL 数据库的 vCloud Director 设备部署，则可以从主单元备份 vCloud Director 数据库。生成的 `.tgz` 文件存储在 NFS 共享传输服务存储位置。

步骤

1 以 **root** 身份直接或通过 SSH 登录到主单元。

2 导航到 `/opt/vmware/appliance/bin`。

3 运行 `create-db-backup` 命令。

结果

在 NFS 共享传输服务存储上的 *`vcloudapp.nfs_mount.VMware_vCloud_Director`*`/pgdb-backup/` 目录下，可以看到新创建的 `db-backup-`*`date_time_format`*`.tgz` 文件。该 `.tgz` 文件包含数据库转储文件以及主单元的 `global.properties`、`responses.properties`、`certificates` 和 `proxycertificates` 文件。

还原具有高可用性数据库配置的 vCloud Director 设备环境

如果备份了具有 HA 数据库配置的 vCloud Director 设备环境的嵌入式 PostgreSQL 数据库，则可以部署新的设备群集并在其中还原设备数据库。

要还原具有非 HA 数据库配置的设备部署，请参见还原不具有高可用性数据库配置的 vCloud Director 设备环境。

还原工作流包括三个主要阶段。

- 从传输服务 NFS 共享存储复制嵌入式数据库备份 `.tar` 文件。
- 将数据库还原到嵌入式数据库的主单元和备用单元。
- 部署任何所需的应用程序单元。

必备条件

- 确认您已为嵌入式 PostgreSQL 数据库创建备份 `.tar` 文件。请参见备份 vCloud Director 设备的嵌入式数据库。
- 部署一个主数据库单元和两个备用数据库单元。请参见第 6 章 部署 vCloud Director 设备。
- 如果希望新的设备群集使用以前环境的 NFS 服务器，请在此 NFS 服务器上创建新目录并导出为新共享。无法重用现有挂载点。

过程

1 在主单元和备用单元上，以 **root** 身份登录，然后运行以下命令以停止 vCloud Director 服务。

```
service vmware-vcd stop
```

2 在主单元和备用单元上，将备份 `.tar` 文件复制到 `/tmp` 文件夹。

如果 `/tmp` 文件夹上的可用空间不足，请在其他位置存储 `.tar` 文件。

3 在主单元和备用单元上，解压缩位于 `/tmp` 的备份文件。

```
tar -zxvf db-backup-date_time_format.tgz
```

在 `/tmp` 文件夹中，您会看到提取出来的 `global.properties`、`responses.properties`、`certificates`、`proxycertficates`、`truststore` 以及名为 `vcloud_date_time_format` 的数据库转储文件。

注 `truststore` 文件仅适用于 vCloud Director 9.7.0.1 及更高版本。

4 仅在主单元上，以 **root** 身份登录到控制台并运行以下命令。

a 丢弃 `vcloud` 数据库。

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

b 运行 `pg_restore` 命令。

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/pg_restore -C -d postgres /tmp/
vcloud_date_time_name
```

5 在主单元和备用单元上，保存配置数据文件的副本，进行替换，然后重新配置并启动 vCloud Director 服务。

a 备份属性、证书和信任存储区文件。

`global.properties`、`responses.properties`、`certificates`、`proxycertificates` 和 `truststore` 文件位于 `/opt/vmware/vcloud-director/etc/`。

注 `truststore` 文件仅适用于 vCloud Director 9.7.0.1 及更高版本。

```
cd /opt/vmware/vcloud-director/etc
mkdir -p backup
cp global.properties responses.properties certificates proxycertificates truststore backup
```

b 复制并替换从步骤 3 中提取的备份文件中的属性、证书和信任存储区文件。

```
cd /tmp
cp global.properties responses.properties certificates proxycertificates truststore /opt/
vmware/vcloud-director/etc/.
```

注 truststore 文件仅适用于 vCloud Director 9.7.0.1 及更高版本。

```
cp certificates /optvmware/vcloud-director/.
```

c 备份密钥库文件，即 /opt/vmware/vcloud-director/certificates.ks。

```
cd /opt/vmware/vcloud-director
mkdir -p backup
cp certificates.ks backup
```

d 运行以下命令，重新配置 vCloud Director 服务。

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type postgres
--database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --database-
port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-director/
certificates.ks \
--keystore-password ks_password --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

其中：

- --keystore-password 选项与设备上证书的密钥库密码一致。
- --database-password 选项与在设备部署过程中设置的数据库密码一致。
- --database-host 选项与主数据库设备的 eth1 网络 IP 地址一致。
- --primary-ip 值与还原的设备单元的 eth0 网络 IP 地址一致。这不是主数据库单元的 IP 地址。
- --console-proxy-ip 选项与要还原的设备的 eth0 网络 IP 地址匹配。

有关故障排除信息，请参见迁移或还原到 vCloud Director 设备时，重新配置 vCloud Director 服务失败。

e 运行以下命令，启动 vCloud Director 服务。

```
service vmware-vcd start
```

可以在 /opt/vmware/vcloud-director/logs/cell.log 中监控单元的启动进度。

6 （可选） 部署任何其他应用程序单元。请参见第 6 章 部署 vCloud Director 设备。

7 服务器组的所有单元完成启动过程后，验证 vCloud Director 环境还原是否成功。

   a 使用新服务器组中任何单元的 `eth0` 网络 IP 地址打开 vCloud Director Web Console，即 `https://et0_IP_new_cell/cloud`。

   b 使用现有**系统管理员**凭据登录到 vCloud Director Web Console。

   c 验证您的 vSphere 和云资源在新环境中是否可用。

8 成功验证数据库还原后，使用 vCloud Director Web Console 删除属于旧 vCloud Director 环境的已断开连接单元。

   a 在**管理与监控**选项卡上，单击**云单元**。

   b 右键单击单元名称，并选择**删除**。

还原不具有高可用性数据库配置的 vCloud Director 设备环境

如果备份了具有非 HA 数据库配置的 vCloud Director 设备环境的嵌入式 PostgreSQL 数据库，则可以部署新的设备群集并在其中还原设备数据库。

要还原具有 HA 数据库配置的设备部署，请参见还原具有高可用性数据库配置的 vCloud Director 设备环境。

还原工作流包括三个主要阶段。

- 从传输服务 NFS 共享存储复制嵌入式数据库备份 `.tar` 文件。
- 将数据库还原到嵌入式数据库主单元。
- 部署任何所需的应用程序单元。

必备条件

- 确认您已为嵌入式 PostgreSQL 数据库创建备份 `.tar` 文件。请参见备份 vCloud Director 设备的嵌入式数据库。
- 部署一个主数据库单元。请参见第 6 章 部署 vCloud Director 设备。
- 如果希望新的设备群集使用以前环境的 NFS 服务器，请在此 NFS 服务器上创建新目录并导出为新共享。无法重用现有挂载点。

过程

1 在主单元上，以 **root** 身份登录到控制台，然后运行以下命令以停止 vCloud Director 服务。

```
service vmware-vcd stop
```

2 将备份 `.tar` 文件复制到 `/tmp` 文件夹。

   如果 `/tmp` 文件夹上的可用空间不足，请在其他位置存储 `.tar` 文件。

3 解压缩 `/tmp` 中的备份文件。

```
tar -zxvf db-backup-date_time_format.tgz
```

在 /tmp 文件夹中，您会看到提取出来的 global.properties、responses.properties、certificates、proxycertificates、truststore 以及名为 vcloud_*date_time_format* 的数据库转储文件。

注 truststore 文件仅适用于 vCloud Director 9.7.0.1 及更高版本。

4 运行命令以丢弃数据库并将其还原到新设备。

a 丢弃 vcloud 数据库。

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

b 运行 pg_restore 命令。

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/pg_restore -C -d postgres /tmp/
vcloud_date_time_name
```

5 在主单元上，保存配置数据文件的副本，进行替换，然后重新配置并启动 vCloud Director 服务。

a 备份属性、证书和信任存储区文件。

global.properties、responses.properties、certificates、proxycertificates 和 truststore 文件位于 /opt/vmware/vcloud-director/etc/。

注 truststore 文件仅适用于 vCloud Director 9.7.0.1 及更高版本。

```
cd /opt/vmware/vcloud-director/etc
mkdir -p backup
cp global.properties responses.properties certificates proxycertificates truststore backup
```

b 复制并替换从步骤 3 中提取的备份文件中的属性、证书和信任存储区文件。

```
cd /tmp
cp global.properties responses.properties certificates proxycertificates truststore /opt/
vmware/vcloud-director/etc/.
```

注 truststore 文件仅适用于 vCloud Director 9.7.0.1 及更高版本。

```
cp certificates /optvmware/vcloud-director/.
```

c 备份密钥库文件，即 /opt/vmware/vcloud-director/certificates.ks。

```
cd /opt/vmware/vcloud-director
mkdir -p backup
cp certificates.ks backup
```

d 运行以下命令，重新配置 vCloud Director 服务。

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type postgres
--database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --database-
```

```
port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-director/
certificates.ks \
--keystore-password ks_password --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

其中：

- `--keystore-password` 选项与设备上证书的密钥库密码一致。
- `--database-password` 选项与在设备部署过程中设置的数据库密码一致。
- `--database-host` 选项与主数据库设备的 `eth1` 网络 IP 地址一致。
- `--primary-ip` 值与还原的设备单元的 `eth0` 网络 IP 地址一致。这不是主数据库单元的 IP 地址。
- `--console-proxy-ip` 选项与要还原的设备的 `eth0` 网络 IP 地址匹配。

有关故障排除信息，请参见迁移或还原到 vCloud Director 设备时，重新配置 vCloud Director 服务失败。

e 运行以下命令，启动 vCloud Director 服务。

```
service vmware-vcd start
```

可以在 `/opt/vmware/vcloud-director/logs/cell.log` 中监控单元的启动进度。

6 （可选） 部署任何其他应用程序单元。请参见第 6 章 部署 vCloud Director 设备。

7 服务器组的所有单元完成启动过程后，验证 vCloud Director 环境还原是否成功。

a 使用新服务器组中任何单元的 `eth0` 网络 IP 地址打开 vCloud Director Web Console，即 `https://et0_IP_new_cell/cloud`。

b 使用现有**系统管理员**凭据登录到 vCloud Director Web Console。

c 验证您的 vSphere 和云资源在新环境中是否可用。

8 成功验证数据库还原后，使用 vCloud Director Web Console 删除属于旧 vCloud Director 环境的已断开连接单元。

a 在**管理与监控**选项卡上，单击**云单元**。

b 右键单击单元名称，并选择**删除**。

配置对 vCloud Director 数据库的外部访问

您可以启用从特定外部 IP 地址到主设备中嵌入的 vCloud Director 数据库的访问。

在迁移到 vCloud Director 设备的过程中，或者如果您打算使用第三方数据库备份解决方案，则可能需要启用对嵌入式 vCloud Director 数据库的外部访问。

步骤

1 以 **root** 身份直接或通过 SSH 登录到主单元。

2 导航到数据库目录 /opt/vmware/appliance/etc/pg_hba.d/。

3 创建一个文本文件，其中包含目标外部 IP 地址的条目，类似于：

```
#TYPE  DATABASE  USER    ADDRESS        METHOD
host   vcloud    vcloud  CIDR_notation  md5
```

例如：

```
#TYPE  DATABASE  USER    ADDRESS           METHOD
host   vcloud    vcloud  172.168.100.5/32  md5
host   vcloud    vcloud  172.168.20.5/32   md5
```

您的条目将附加到动态更新的 pg_hba.conf 文件中，该文件控制对 HA 群集中主数据库的访问。

启用或禁用对 vCloud Director 设备的 SSH 访问

在设备部署过程中，您可以保持禁用状态，也可以启用对设备的 SSH 访问。部署后，您可以切换 SSH 访问设置。

SSH 守护进程在设备中运行，供数据库 HA 功能和远程 **root** 登录使用。您可以禁用 **root** 用户的 SSH 访问。数据库 HA 功能的 SSH 访问保持不变。

步骤

1 如果要对 OVF 属性进行临时更改，例如，要进行测试，请在 vCloud Director 中更改此属性。

a 以 **root** 身份直接或通过 SSH 客户端登录到 vCloud Director 设备控制台。

b 运行用于启用或禁用 SSH **root** 访问的脚本。

- 要启用 SSH **root** 访问，请运行 /opt/vmware/appliance/bin/enable_root_login.sh 脚本。
- 要禁用 SSH **root** 访问，请运行 /opt/vmware/appliance/bin/disable_root_login.sh 脚本。

2 如果要对 OVF 属性进行永久更改，请使用 vSphere 用户界面设置 vcloudapp.enable_ssh.VMware_vCloud_Director 属性的值。

注 您必须关闭虚拟机的电源才能在 vSphere 中更改此属性的值。

- 要启用 SSH，请将 vcloudapp.enable_ssh.VMware_vCloud_Director 的值设置为 **True**。
- 要禁用 SSH，请将 vcloudapp.enable_ssh.VMware_vCloud_Director 的值设置为 **False**。

编辑 vCloud Director 设备的 DNS 设置

部署后，可以更改 vCloud Director 设备的一个或多个 DNS 服务器。

重要事项 无法编辑设备的主机名。必须使用所需的主机名部署新设备。

步骤

1 如果要暂时更改 DNS 设置，例如，为了进行测试，请在 vCloud Director 中编辑 DNS 设置。

a 以 **root** 身份直接或通过 SSH 客户端登录到 vCloud Director 设备控制台。

b （可选） 通过运行以下命令验证当前的 DNS 配置：

```
ovfenv --key vami.DNS.VMware_vCloud_Director
```

c 更改一个或多个 DNS 服务器。

要指定多个 DNS 服务器，请将 *DNS_server_IP* 设置为不含空格的逗号分隔列表。

```
ovfenv --key vami.DNS.VMware_vCloud_Director --value DNS_server_IP
```

d 要使更改生效，请重新启动 VAOS 服务。

```
systemctl restart vaos.service
```

2 如果要永久更改 DNS 设置，请使用 vSphere UI 将 `vami.DNS.VMware_vCloud_Director` 属性的值设置为新的 DNS 服务器 IP 地址。

要指定多个 DNS 服务器，请输入逗号分隔的列表（无空格）。

注 您必须关闭虚拟机的电源才能在 vSphere 中更改此属性的值。

编辑 vCloud Director 设备网络接口的静态路由

初始部署 vCloud Director 后，可以更改 `eth0` 和 `eth1` 网络接口的静态路由。

步骤

1 如果要暂时更改静态路由值，例如为了进行测试，请在 vCloud Director 中编辑静态路由。

a 以 **root** 身份直接或通过 SSH 客户端登录到 vCloud Director 设备控制台。

b （可选） 验证当前静态路由配置。

- 对于 `eth0`，运行以下命令。

```
ovfenv --key vcloudnet.routes0.VMware_vCloud_Director
```

- 对于 `eth1`，运行以下命令。

```
ovfenv --key vcloudnet.routes1.VMware_vCloud_Director
```

c 更改静态路由值。

静态路由必须位于以逗号分隔的路由规范列表中。例如，对于“eth0”，您必须运行：

```
ovfenv --key vcloudnet.routes0.VMware_vCloud_Director  --value "172.16.100.253
172.16.96.0/19, 172.16.100.253 192.168.100.0/24"
```

- 对于 eth0，运行以下命令。

  ```
  ovfenv --key vcloudnet.routes0.VMware_vCloud_Director  --value "new_static_routes0"
  ```

- 对于 eth1，运行以下命令。

  ```
  ovfenv --key vcloudnet.routes1.VMware_vCloud_Director  --value "new_static_routes1"
  ```

d 重新启动 vCloud Director 设备上的网络服务。

```
systemctl restart vcd-ova-netconfig.service
```

2 如果要永久更改静态路由值，请使用 vSphere UI 更改 OVF 属性。

静态路由必须位于以逗号分隔的路由规范列表中。

注 您必须关闭虚拟机的电源才能在 vSphere 中更改此属性的值。

- 使用 vSphere 用户界面将 vcloudnet.routes0.VMware_vCloud_Director 属性的值设置为新的路由规范字符串。
- 使用 vSphere 用户界面将 vcloudnet.routes1.VMware_vCloud_Director 属性的值设置为新的路由规范字符串。

vCloud Director 设备中的配置脚本

vCloud Director 设备包含特定的配置脚本。

目录	描述
/opt/vmware/appliance/bin/	设备配置脚本。
/opt/vmware/appliance/etc/	设备配置文件。
/opt/vmware/appliance/etc/pg_hba.d/	可在其中将自定义条目添加到 pg_hba.conf 文件的目录。请参见配置对 vCloud Director 数据库的外部访问。

修改 vCloud Director 设备中的 PostgreSQL 配置

可以使用 PostgreSQL ALTER SYSTEM 命令更改 vCloud Director 设备的 PostgreSQL 配置。

ALTER SYSTEM 命令会将参数设置更改写入 postgresql.auto.conf 文件，该文件在 PostgreSQL 初始化期间优先于 postgresql.conf 文件。一些设置需要重新启动 PostgreSQL 服务，而其他一些设置则进行动态配置，不需要重新启动。不要更改 postgresql.conf 文件，因为重新引导后不会保留这些更改。

步骤

1 以 **root** 身份直接或通过 SSH 客户端登录到主设备的操作系统。

2 将用户更改为 **postgres**。

```
sudo –i –u postgres
```

3 使用 PostgreSQL ALTER SYSTEM 命令更改参数。

```
psql –c "ALTER SYSTEM set parameter='value';"
```

4 对要更改的每个配置参数重复步骤 3。

5 如果要更改的某些参数需要重新启动 PostgreSQL 服务，请重新启动 vpostgres 进程。

```
systemctl restart vpostgres
```

6 如果您的环境具有备用节点，请将 `postgresql.auto.conf` 文件复制到备用设备，并在必要时重新启动 PostgreSQL 服务。

   a 将 `postgresql.auto.conf` 从主节点复制到备用节点。

   ```
   scp /var/vmware/vpostgres/current/pgdata/postgresql.auto.conf postgres@<standby-node-address>:/var/vmware/vpostgres/current/pgdata/
   ```

   b 如果复制的 `postgresql.auto.conf` 文件中的某些参数需要重新启动才能生效，请在备用节点上重新启动 vpostgres 进程。

   ```
   systemctl restart vpostgres
   ```

   c 对每个备用节点重复 6.a 和 6.b。

在高可用性群集配置中使用复制管理器工具套件

9

repmgr 开源工具套件是 vCloud Director 设备的嵌入式 PostgreSQL 数据库的一部分。可以使用 repmgr 在 vCloud Director 数据库高可用性群集中配置、监控和控制 PostgreSQL 复制和数据库故障切换。

可以使用 repmgr 命令行界面检查节点或群集的状态和事件，注册或取消注册节点，提升备用节点，交换主节点和备用节点角色，或者遵循新的主节点。

要了解有关 vCloud Director 数据库高可用性配置的更多信息，请参见设备部署和数据库高可用性配置。

要了解有关 repmgr 的更多信息，请访问 repmgr.org。

本章讨论了以下主题：

检查数据库高可用性群集的连接状态

可以使用复制管理器工具套件检查数据库高可用性群集中节点之间的连接。

步骤

1 以 **root** 身份直接或通过 SSH 登录到群集中任何正在运行的单元的操作系统。

2 将用户更改为 **postgres**。

```
sudo –i –u postgres
```

3 检查群集的连接。

- `repmgr cluster matrix` 命令在群集的每个节点上运行 `repmgr cluster show` 命令，并以矩阵的形式显示结果。

```
/opt/vmware/vpostgres/current/bin/repmgr –f /opt/vmware/vpostgres/current/etc/repmgr.conf
cluster matrix
```

在以下示例中，节点 1 和节点 2 处于启动状态，而节点 3 处于关闭状态。每一行对应一台服务器，表示该服务器的出站连接测试结果。

第三行中的三个条目都标有 ? 符号，这是因为节点 3 处于关闭状态，不存在出站连接的相关信息。

```
     Name| Id |  1 |  2  |  3
---------+----+----+----+----
  node 1 |  1 |  * |  * |  x
  node 2 |  2 |  * |  * |  x
  node 3 |  3 |  ? |  ? |  ?
```

- `repmgr cluster crosscheck` 命令交叉检查每个节点组合之间的连接，有助于更好地了解群集连接。

```
/opt/vmware/vpostgres/current/bin/repmgr –f /opt/vmware/vpostgres/current/etc/repmgr.conf
cluster crosscheck
```

在以下示例中，运行 `repmgr cluster crosscheck` 命令的节点将其群集矩阵系统输出与其他节点的输出进行合并，并在节点之间执行交叉检查。在此示例中，所有节点都处于启动状态，但防火墙丢弃源自节点 1 并在节点 3 进行定向的数据包。这是一个非对称网络分区示例，其中，节点 1 无法将数据包发送到节点 3。

```
     Name| Id |  1 |  2  |  3
---------+----+----+----+----
  node 1 |  1 |  * |  * |  x
  node 2 |  2 |  * |  * |  *
  node 3 |  3 |  * |  * |  *
```

后续步骤

要确定数据库高可用性群集中的整体连接状态，请在每个节点上运行这些命令并比较结果。

检查数据库高可用性群集中节点的复制状态

可以使用复制管理器工具套件和 PostgreSQL 交互式终端检查数据库高可用性群集中各个节点的复制状态。

步骤

1 以 **root** 身份直接或通过 SSH 登录到群集中任何正在运行的节点的操作系统。

2 将用户更改为 **postgres**。

```
sudo –i –u postgres
```

3 检查节点的复制状态。

```
/opt/vmware/vpostgres/current/bin/repmgr –f /opt/vmware/vpostgres/current/etc/repmgr.conf node status
```

系统输出提供有关节点、PostgreSQL 版本和复制详细信息的信息。

4 （可选） 有关更多详细信息，请使用 PostgreSQL 交互式终端检查节点的复制状态。

PostgreSQL 交互式终端可以提供有关备用节点的任何已接收日志记录是否落后于主节点所发送日志的信息。

a 连接到 `psql` 终端。

```
/opt/vmware/vpostgres/current/bin/psql
```

b 要展开显示并使查询结果更易于阅读，请运行 `set \x` 命令。

c 根据节点的角色运行复制状态查询。

选项	操作
在主节点上运行查询。	`/opt/vmware/vpostgres/current/bin/psql`
在备用节点上运行查询。	`select * from pg_stat_wal_receiver;`

检查数据库高可用性集群的状态

要对数据库高可用性集群中的问题进行故障排除，必须监控集群中节点和事件的状态。

步骤

1 以 **root** 身份直接或通过 SSH 登录到集群中任何正在运行的单元的操作系统。

2 将用户更改为 **postgres**。

```
sudo –i –u postgres
```

3 检查集群的状态。

上游列显示当前主节点。

```
/opt/vmware/vpostgres/current/bin/repmgr cluster show
```

控制台输出显示集群信息。在以下示例中，集群中的主节点（节点 3）的状态为无法访问。

```
     ID |  Name    | Role    | Status         | Upstream   | Location | Connection string
--------+----------+---------+----------------+------------+----------+-------------------------
 Node 1 | Node name | standby |     running   | Node 3 name| default | host=host IP address
user=repmgr dbname=repmgr
 Node 2 | Node name | standby |     running   | Node 3 name| default | host=host IP address
user=repmgr dbname=repmgr
 Node 3 | Node name | primary | ? unreachable |            | default | host=host IP address
user=repmgr dbname=repmgr
```

在以下系统输出示例中，节点 3 为正常运行集群中的主节点。

```
     ID |  Name     | Role    | Status   | Upstream  | Location| Connection string
--------+-----------+---------+----------+-----------+---------+-----------------------
 Node 1 | Node name | standby |  running | Node3 name| default | host=host IP address user=repmgr
dbname=repmgr
 Node 2 | Node name | standby |  running | Node3 name| default | host=host IP address user=repmgr
dbname=repmgr
 Node 3 | Node name | primary | *running |           | default | host=host IP address user=repmgr
dbname=repmgr
```

4 检查集群事件日志。

```
/opt/vmware/vpostgres/current/bin/repmgr –f /opt/vmware/vpostgres/current/etc/repmgr.conf cluster
event
```

系统输出显示集群中的创建、克隆和注册事件。

后续步骤

如果主节点的状态为无法访问或失败，则必须提升备用节点。

如果备用节点的状态为无法访问或失败，请修复该节点并启动 PostgreSQL 服务（如果该服务未运行）。

检测高可用性群集中恢复联机的前主节点

如果群集中的主节点出现故障，然后在将备用节点提升为新的主节点时恢复联机，则会导致 repmgr 数据不准确。可以使用 `repmgr cluster show` 命令检测违规行为。

示例： 在前主节点上运行 `repmgr cluster show`

在以下示例中，在恢复联机的前主节点上运行 `repmgr cluster show` 命令，会生成以下系统输出。

```
     ID |  Name     | Role    | Status            | Upstream  | Location | Connection string
--------+-----------+---------+-------------------+-----------+----------+-------------------------
 Node 1 | Node1 name| standby |!running as primary|Node 3 name| default  | host=host IP address
user=repmgr dbname=repmgr
 Node 2 | Node2 name| standby |     running       |Node 3 name| default  | host=host IP address
user=repmgr dbname=repmgr
```

```
 Node 3 | Node3 name| primary |   * running       |           | default  | host=host IP address
user=repmgr dbname=repmgr
   WARNING: following issues were detected
  - node 1(ID: Node 1) is registered as standby but running as primary
```

在该示例中，节点 1 是群集中的当前主节点。

运行 `repmgr cluster show` 命令时，备用节点显示 `!running as primary` 状态表示前主节点正在群集中运行。在此情况下，必须关闭并取消注册前主节点。

示例： 在新的主节点上运行 repmgr cluster show

在以下示例中，在新的主节点上运行 `repmgr cluster show` 命令会生成以下系统输出。

```
     ID |  Name    | Role    | Status     | Upstream   | Location | Connection string
--------+----------+---------+------------+------------+----------+-------------------------
 Node 1 |Node1 name| primary |  * running |            | default  | host=host IP address user=repmgr
dbname=repmgr
 Node 2 |Node2 name| standby |    running | Node1 name | default  | host=host IP address user=repmgr
dbname=repmgr
 Node 3 |Node3 name| primary |  ! running |            | default  | host=host IP address user=repmgr
dbname=repmgr
   WARNING: following issues were detected
  - node 3(ID: Node 3) is running but the repmgr node record is inactive
```

在此示例中，repmgr 数据正确。它准确指出节点 1 正在运行，并且是当前主节点。有关节点 3（前主节点）的警告消息表示该节点上的 repmgr 数据不准确。

示例： 提升备用节点后运行 repmgr cluster show，但不在剩余备用节点上运行 standby follow

在以下示例中，可以看到主节点出现故障的群集中每个节点上的 repmgr 数据。已使用 `repmgr standby promote` 命令手动提升备用节点，但未在剩余的备用节点上运行 `repmgr standby follow`。

在新的主节点上运行 `repmgr cluster show` 时，系统输出表示 repmgr 数据正确，但新的主节点（节点 2）后面未跟随任何备用节点。

```
     ID |  Name    | Role    | Status    | Upstream   |Location | Connection string
--------+----------+---------+-----------+------------+---------+-------------------------
 Node 1 |Node1 name| primary | * running |            | default | host=host IP address user=repmgr
dbname=repmgr
 Node 2 |Node2 name| primary | ! running |            | default | host=host IP address user=repmgr
dbname=repmgr
 Node 3 |Node3 name| standby |   running |Node 1 name | default | host=host IP address user=repmgr
dbname=repmgr
   WARNING: following issues were detected
  - node 1(ID: Node 1) is running but the repmgr node record is inactive
```

节点 1（前主节点）和节点 3（前主节点出故障后的备用节点）都提供了不准确的 repmgr 数据。

```
     ID |  Name    | Role    | Status              | Upstream |Location | Connection string
--------+----------+---------+---------------------+----------+---------+-------------------------
 Node 1 |Node1 name| primary |   * running         |          | default | host=host IP address
user=repmgr dbname=repmgr
 Node 2 |Node2 name| standby |! running as primary |Node1 name| default | host=host IP address
user=repmgr dbname=repmgr
 Node 3 |Node3 name| standby |     running         |Node1 name| default | host=host IP address
user=repmgr dbname=repmgr
   WARNING: following issues were detected
  - node 2(ID: Node 2) is registered as standby but running as primary
```

示例： 在备用节点上运行 repmgr cluster show

在当前主节点后的备用节点上运行此命令，会生成 repmgr 数据准确的系统输出，且该数据与当前主节点上的数据相同。

在前主节点后的备用节点上运行此命令，会生成 repmgr 数据不准确的系统输出，且该数据与前主节点上的数据相同。

日志条目

如果出现故障的主节点在将备用节点提升为新的主节点后恢复联机，则 repmgr 数据不准确的所有节点上的 `update-repmgr-data` 文件中将显示以下条目。

```
ERROR: An old primary is running in the repmgr cluster.
ERROR: Manual intervention is required to repair the repmgr cluster.
ERROR: The first step should be to shutdown and unregister the old primary.
```

切换数据库高可用性群集中主单元和备用单元的角色

在计划维护期间，可以使用 repmgr 命令切换数据库高可用性群集中主节点和某个备用节点的角色。

前提条件

- 将属于高可用性群集的所有 vCloud Director 单元置于维护模式。
- 确认群集中的所有节点都正常运行且处于联机状态。

步骤

1. 以 **root** 身份直接或通过 SSH 登录到要提升的备用节点的操作系统。
2. 将用户更改为 **postgres**。

   ```
   sudo –i –u postgres
   ```

3 （可选） 运行具有 `--dry-run` 选项的以下命令，验证是否满足切换的必备条件。

```
/opt/vmware/vpostgres/current/bin/repmgr standby switchover -f /opt/vmware/vpostgres/current/etc/repmgr.conf --siblings-follow --dry-run
```

4 切换主单元和备用单元的角色。

```
/opt/vmware/vpostgres/current/bin/repmgr standby switchover -f /opt/vmware/vpostgres/current/etc/repmgr.conf --siblings-follow
```

结果

控制台输出的最后一行指示备用切换已成功完成。

后续步骤

1 运行 **reconfigure-database** 命令以更新所有 vCloud Director 单元上的数据库 IP 地址。请参见更新 vCloud Director 单元上的数据库 IP 地址。

2 将服务器组中的 vCloud Director 单元重新配置为指向新的主数据库时，请将属于高可用性群集的所有 vCloud Director 单元退出维护模式。

取消注册数据库高可用性群集中出现故障或无法访问的备用节点

可以在群集中某个正在运行的节点上使用 repmgr 取消注册出现故障或无法访问的备用节点。

注 要确保主节点正常运行，至少必须始终有一个备用节点在运行。

前提条件

要取消注册未运行的备用节点，必须提供节点 ID。要查找 IP 地址，请检查群集的状态并找到该节点。在对应的行上，使用“Connection string”列中的主机值确定节点的 IP 地址。请参见检查数据库高可用性集群的状态。

步骤

1 以 **root** 身份直接或通过 SSH 登录到群集中任何正在运行的节点的操作系统。

2 将用户更改为 **postgres**。

```
sudo -i -u postgres
```

3 取消注册出现故障或无法访问的节点。

```
/opt/vmware/vpostgres/current/bin/repmgr standby unregister -f /opt/vmware/vpostgres/current/etc/repmgr.conf --node-id=ID
```

结果

取消注册节点会将节点信息从 repmgr 元数据中移除。

取消注册数据库高可用性群集中出现故障的主单元

如果数据库高可用性群集中的主节点出现故障，并提升了新的主节点，则必须取消注册出现故障的主节点，以将其从群集中移除并避免出现不一致的群集状态数据。

前提条件

- 要取消注册未运行的主节点，必须提供节点 ID。要查找 IP 地址，请检查群集的状态并找到该节点。在对应的行上，使用“Connection string”列中的主机值确定节点的 IP 地址。请参见检查数据库高可用性集群的状态。
- 确认出现故障的主节点处于非活动状态且没有任何跟随的备用节点，并提升了新的主节点。

步骤

1 以 **root** 身份直接或通过 SSH 登录到群集中任何正在运行的节点的操作系统。

2 将用户更改为 **postgres**。

```
sudo -i -u postgres
```

3 （可选） 要验证是否满足取消注册节点的必备条件，请运行具有 `--dry-run` 选项的以下命令。

```
/opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=node ID --dry-run
```

4 取消注册节点。

```
/opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=node ID
```

结果

该操作将从 repmgr 元数据中移除节点。

取消注册数据库高可用性群集中正在运行的备用单元

如果要在其他角色中使用节点，或者要从高可用性群集中移除节点，则必须取消注册该节点。

可以在系统正常运行时运行以下命令。

注 要确保主节点正常运行，至少必须始终有一个备用节点在运行。

前提条件

要取消注册备用节点，必须提供节点 ID。要查找 IP 地址，请检查群集的状态并找到该节点。在对应的行上，使用“Connection string”列中的主机值确定节点的 IP 地址。请参见检查数据库高可用性集群的状态。

步骤

1 以 **root** 身份直接或通过 SSH 登录到群集中任何正在运行的节点的操作系统。

2 将用户更改为 **postgres**。

```
sudo –i –u postgres
```

3 取消注册节点。

```
/opt/vmware/vpostgres/current/bin/repmgr standby unregister ––node–id=node ID –f /opt/vmware/
vpostgres/current/etc/repmgr.conf
```

结果

取消注册节点会将备用节点的记录从 repmgr 工具套件的内部元数据表中移除。

安装 vCloud Director 或部署 vCloud Director 设备之后

10

创建 vCloud Director 服务器组后，可以安装 Microsoft Sysprep 文件和 Cassandra 数据库。如果您使用的是 PostreSQL 数据库，则可以配置 SSL，并调整数据库上的某些参数。

本章讨论了以下主题：

- 在服务器上安装 Microsoft Sysprep 文件
- 自定义公用端点
- 安装和配置 RabbitMQ AMQP 代理
- 安装并配置 Cassandra 数据库以存储历史衡量指标数据
- 在外部 PostgreSQL 数据库上执行其他配置

在服务器上安装 Microsoft Sysprep 文件

如果您的云需要某些旧版 Microsoft 操作系统的客户机自定义支持，则必须在服务器组的每个成员上安装相应的 Microsoft Sysprep 文件。

只有某些较旧的 Microsoft 操作系统才需要 Sysprep 文件。如果您的云不需要支持这些操作系统的客户机自定义，则不需要安装 Sysprep 文件。

要安装 Sysprep 二进制文件，请将其复制到服务器上的特定位置。必须将这些文件复制到服务器组的每个成员。

前提条件

验证您是否有权访问 Windows 2003 和 Windows XP 的 32 位和 64 位 Sysprep 二进制文件。

步骤

1 以 **root** 身份登录到目标服务器。

2 将目录更改为 `$VCLOUD_HOME/guestcustomization/default/windows`。

```
[root@cell1 /]# cd /opt/vmware/vcloud-director/guestcustomization/default/windows
```

3 创建一个名为 `sysprep` 的目录。

```
[root@cell1 /opt/vmware/vcloud-director/guestcustomization/default/windows]# mkdir sysprep
```

4 对于需要 Sysprep 二进制文件的每个客户机操作系统，请创建 `$VCLOUD_HOME/guestcustomization/default/windows/sysprep` 的子目录。

子目录名称特定于客户机操作系统。

表 10-1. Sysprep 文件的子目录分配

客户机操作系统	要在 $VCLOUD_HOME/guestcustomization/default/windows/sysprep 下创建的子目录
Windows 2003（32 位）	svr2003
Windows 2003（64 位）	svr2003-64
Windows XP（32 位）	xp
Windows XP（64 位）	xp-64

例如，要创建一个子目录，用于放置 Windows XP 的 Sysprep 二进制文件，请使用以下 Linux 命令。

```
[root@cell1 /opt/vmware/vcloud-director/guestcustomization/default/windows]# mkdir sysprep/xp
```

5 将 Sysprep 二进制文件复制到服务器组中每个 vCloud Director 服务器上的恰当位置。

6 确保用户 `vcloud.vcloud` 能够读取 Sysprep 文件。

请使用 Linux chown 命令执行此操作。

```
[root@cell1 /]# chown -R vcloud:vcloud $VCLOUD_HOME/guestcustomization
```

结果

如果已将 Sysprep 文件复制到服务器组的所有成员，则可以在您的云中的虚拟机上执行客户机自定义。复制 Sysprep 文件后，不需要重新启动 vCloud Director。

自定义公用端点

为满足负载平衡器或代理要求，可以更改 vCloud Director Web 控制台、vCloud API、租户门户和控制台代理的默认端点 Web 地址。

如果已部署 vCloud Director 设备，则必须配置 vCloud Director 公用控制台代理地址，因为设备会针对控制台代理服务使用具有自定义端口 8443 的单个 IP 地址。请参见步骤 5。

前提条件

只有**系统管理员**可以自定义公用端点。

步骤

1 单击**管理**选项卡，然后在左侧窗格中单击**公用地址**。

2 选择**自定义公用端点**。

取消选中此复选框会将所有端点恢复为其默认值，这些值不会在页面上显示。

3 要自定义 vCloud REST API 和 OpenAPI URL，请编辑 **API** 端点。

a 输入自定义 HTTP 基本 URL。

例如，如果将 HTTP 基本 URL 设置为 **http://vcloud.example.com**，则可以在 `http://vcloud.example.com/api` 上访问 vCloud API，且可以在 `http://vcloud.example.com/cloudapi` 上访问 vCloud OpenAPI。

b 输入自定义 HTTPS REST API 基本 URL，然后单击**浏览**以上载用于为该端点建立信任链的证书。

例如，如果将 HTTPS REST API 基本 URL 设置为 **https://vcloud.example.com**，则可以在 `https://vcloud.example.com/api` 上访问 vCloud API，且可以在 `https://vcloud.example.com/cloudapi` 上访问 vCloud OpenAPI。

证书链必须与服务端点使用的证书相匹配，该证书可以是上载到每个 vCloud Director 单元密钥库且别名为 `http` 的证书，也可以是负载平衡器 VIP 证书（如果使用 SSL 终止）。证书链必须包含端点证书、中间证书以及不含私钥的 `PEM` 格式的根证书。

4 要自定义 vCloud Director 租户门户 URL，请编辑**租户门户**端点。

- 要将 vCloud Director 租户门户配置为使用步骤 步骤 3 中指定的相同端点和证书链，请选择**复制 API URL 设置**。
- 要将 vCloud Director 租户门户配置为使用不同的端点和证书链，请执行以下步骤。

  a 取消选择**复制 API URL 设置**。

  b 输入自定义 HTTP 基本 URL。

  例如，如果将 HTTP 基本 URL 设置为 **http://vcloud.example.com**，则可以在 `http://vcloud.example.com/tenant/`*`org_name`* 上访问租户门户。

  c 输入自定义 HTTPS REST API 基本 URL，然后单击**浏览**以上载用于为该端点建立信任链的证书。

  例如，如果将 HTTPS REST API 基本 URL 设置为 **https://vcloud.example.com**，则可以在 `https://vcloud.example.com/tenant/`*`org_name`* 上访问租户门户。

  证书链必须与服务端点使用的证书相匹配，该证书可以是上载到每个 vCloud Director 单元密钥库且别名为 `http` 的证书，也可以是负载平衡器 VIP 证书（如果使用 SSL 终止）。证书链必须包含端点证书、中间证书以及不含私钥的 `PEM` 格式的根证书。

5 要自定义 vCloud Director Web Console URL 和控制台代理地址，请编辑 **Web 控制台**端点。

a 输入用于 HTTP 连接的自定义 vCloud Director 公用 URL。

该 URL 必须包含 `/cloud`。

例如，如果将 vCloud Director 公用 URL 设置为 **`http://vcloud.example.com/cloud`**，则可以在 `http://vcloud.example.com/cloud` 上访问 vCloud Director Web Console。

b 输入用于 HTTPS 连接的自定义 REST API URL，然后单击**浏览**以上载用于为该端点建立信任链的证书。

该 URL 必须包含 `/cloud`。

例如，如果将基本 URL 设置为 **`https://vcloud.example.com`**，则可以在 `https://vcloud.example.com/cloud` 上访问 vCloud Director Web Console。

证书链必须与服务端点使用的证书相匹配，该证书可以是上载到每个 vCloud Director 单元密钥库且别名为 **`HTTP`** 的证书，也可以是负载平衡器 VIP 证书（如果使用 SSL 终止）。证书链必须包含端点证书、中间证书以及不含私钥的 `PEM` 格式的根证书。

c 输入自定义 vCloud Director 公用控制台代理地址。

此地址为 vCloud Director 服务器或负载平衡器的完全限定域名 (FQDN) 并带有端口号。默认端口为 443。

重要事项 vCloud Director 设备将其 `eth0` 网卡与自定义端口 8443 用于控制台代理服务。

不支持在负载平衡器上对控制台代理连接执行 SSL 终止。控制台代理证书将上载到每个 vCloud Director 单元密钥库且别名为 **`consoleproxy`**。

例如，对于 FQDN 为 `vcloud.example.com` 的 vCloud Director 设备实例，请输入 **`vcloud.example.com:8443`**。

vCloud Director Web 控制台将使用此控制台代理地址在 VM 上打开远程控制台窗口。

6 要保存更改，请单击**应用**。

安装和配置 RabbitMQ AMQP 代理

高级消息队列协议 (Advanced Message Queuing Protocol, AMQP) 是消息队列的开放式标准，支持企业系统进行灵活的消息传输。vCloud Director 使用 RabbitMQ AMQP 代理提供可供扩展服务、对象扩展和通知使用的消息总线。

步骤

1 从 https://www.rabbitmq.com/download.html 下载 RabbitMQ Server。

有关支持的 RabbitMQ 版本列表，请参见《vCloud Director 发行说明》。

2 按照 RabbitMQ 安装说明在支持的主机上安装 RabbitMQ。

RabbitMQ 服务器主机必须使每个 vCloud Director 单元在网络上可到达。

3 在 RabbitMQ 安装期间，记下配置 vCloud Director 以与此 RabbitMQ 安装协同工作所需的值。

- RabbitMQ 服务器主机的完全限定域名，例如 *amqp.example.com*。
- 向 RabbitMQ 进行身份验证的有效用户名和密码。
- 代理监听消息的端口。默认为 `5672`。
- RabbitMQ 虚拟主机。默认为“/”。

后续步骤

默认情况下，vCloud Director AMQP 服务将发送未加密的消息。可以配置 AMQP 服务以使用 SSL 加密这些消息。此外，还可以配置服务，以使用 vCloud Director 单元上 Java Runtime Environment 的默认 JCEKS 信任存储区（通常位于 `$VCLOUD_HOME/jre/lib/security/cacerts`）验证代理证书。

要对 vCloud Director AMQP 服务启用 SSL，请执行以下操作：

1 在 vCloud Director Web 控制台中，单击**管理**选项卡，然后单击**扩展性**。

2 单击**扩展性**，然后单击**设置**选项卡。

3 在 **AMQP 代理设置**部分中，选择**使用 SSL**。

4 选中**接受所有证书**复选框，或者提供以下内容之一：

- SSL 证书路径名
- JCEKS 信任存储路径名和密码

安装并配置 Cassandra 数据库以存储历史衡量指标数据

vCloud Director 可收集衡量指标，该指标提供关于云中虚拟机的虚拟机性能和资源使用量的当前和历史信息。历史衡量指标数据存储在 Cassandra 群集中。

Cassandra 是开源数据库，您可以使用该数据库为可扩展的高性能解决方案提供备用存储，以便收集虚拟机衡量指标等时间序列数据。如果您希望 vCloud Director 支持从虚拟机检索历史衡量指标，则必须安装和配置 Cassandra 群集并使用 `cell-management-tool` 将群集连接到 vCloud Director。检索当前衡量指标不需要可选数据库软件。

前提条件

- 验证 vCloud Director 是否已安装且正在运行，然后配置可选数据库软件。
- 如果尚不熟悉 Cassandra，请查看 http://cassandra.apache.org/ 中提供的材料。
- 请参见《vCloud Director 发行说明》，了解支持用作衡量指标数据库的 Cassandra 版本列表。您可以从 http://cassandra.apache.org/download/ 下载 Cassandra。
- 安装并配置 Cassandra 群集：
  - Cassandra 群集必须至少包含 4 个虚拟机，并且这些虚拟机必须部署在两个或更多主机上。
  - 需要两个 Cassandra 种子节点。

- 启用 Cassandra 客户端到节点加密。请参见 http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureSSLIntro.html。
- 启用 Cassandra 用户身份验证。请参见 http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureConfigNativeAuth.html。
- 在每个 Cassandra 群集上启用 Java Native Access (JNA) 版本 3.2.7 或更高版本。
- Cassandra 节点到节点加密是可选操作。
- 将 SSL 与 Cassandra 一起使用是可选操作。如果您决定不为 Cassandra 启用 SSL，则必须将每个单元 (`$VCLOUD_HOME/etc/global.properties`) 上 `global.properties` 文件中的配置参数 `cassandra.use.ssl` 设置为 `0`。

步骤

1 使用 `cell-management-tool` 实用程序在 vCloud Director 与 Cassandra 群集中的节点之间配置连接。

在以下示例命令中，*node1-ip*、*node2-ip*、*node3-ip* 和 *node4-ip* 是 Cassandra 群集成员的 IP 地址。使用默认端口 (9042)。衡量指标数据将保留 15 天。

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --configure --create-schema \ --cluster-nodes node1-
ip,node2-ip,node3-ip, node4-ip \ --username admin --password 'P@55w0rd' --ttl 15
```

有关使用单元管理工具的信息，请参见《vCloud Director 管理员指南》。

2 （可选） 如果要升级 vCloud Director 版本 9.1，请使用 `cell-management-tool` 配置衡量指标数据库来存储汇总衡量指标。

运行类似以下示例的命令：

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --add-rollup \ --username admin --password 'P@55w0rd'
```

3 重新启动每个 vCloud Director 单元。

在外部 PostgreSQL 数据库上执行其他配置

创建 vCloud Director 服务器组后，可以将外部 PostgreSQL 数据库配置为需要来自 vCloud Director 单元的 SSL 连接，并调整某些数据库参数以获得最佳性能。

最安全的连接需要良好签名的 SSL 证书，即包括植根于已知公共证书颁发机构的完整信任链。或者，也可以使用自签名 SSL 证书或由私有证书颁发机构签名的 SSL 证书，但必须将该证书导入到 vCloud Director 信任存储区。

要根据系统规范和要求获取最佳性能，可以调整数据库配置文件中的数据库配置和 autovacuum 参数。

步骤

1 在 vCloud Director 和 PostgreSQL 数据库之间配置 SSL 连接。

a 如果对外部 PostgreSQL 数据库使用自签名证书或私有证书，则从每个 vCloud Director 单元运行以下命令，以将数据库证书导入到 vCloud Director 信任存储区。

```
                [root@cell1 /opt/vmware/vcloud-director/bin]#

cell-management-tool import-trusted-certificates --source path_to_self-signed_or_private_cert
```

b 运行以下命令以启用 vCloud Director 和 PostgreSQL 之间的 SSL 连接。

```
                [root@cell1 /opt/vmware/vcloud-director/bin]#
                 cell-management-tool reconfigure-database --database-ssl true
```

可以使用 --private-key-path 选项对服务器组中的所有单元运行以下命令。

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
 cell-management-tool reconfigure-database --database-ssl true --private-key-path
path_to_private_key
```

有关使用单元管理工具的详细信息，请参见《vCloud Director 管理员指南》。

2 根据您的系统规范编辑 `postgresql.conf` 文件中的数据库配置。

例如，对于具有 16 GB 内存的系统，可以使用以下片段。

```
max_connections = 500
# Set effective cache size to 50% of total memory.
effective_cache_size = 8GB
# Set shared buffers to 25% of total memory
shared_buffers = 4GB
```

3 根据您的要求编辑 `postgresql.conf` 文件中的 autovacuum 参数。

对于典型的 vCloud Director 工作负载，可以使用以下片段。

```
autovacuum = on
track_counts = on
autovacuum_max_workers = 3
autovacuum_naptime = 1min
autovacuum_vacuum_cost_limit = 2400
```

系统会为活动设置自定义 `autovacuum_vacuum_scale_factor` 值以及 `activity_parameters` 表。

后续步骤

如果编辑了 `postgresql.conf` 文件，必须重新启动数据库。

升级 vCloud Director 并修补 vCloud Director 设备

11

您可以执行协调升级，将 vCloud Director 手动升级到新版本，或者将修补程序应用到 vCloud Director 设备部署。

如果您的现有 vCloud Director 服务器组包含基于 Linux 的 vCloud Director 安装，则可以使用适用于 Linux 的 vCloud Director 安装程序升级您的环境。或者，也可以将您的环境迁移到 vCloud Director 9.7 设备。请参见第 12 章 迁移到 vCloud Director 设备。

如果您的现有 vCloud Director 服务器组包含 vCloud Director 9.5 设备部署，则只能将您的环境迁移到 vCloud Director 9.7 设备。只能在迁移工作流中使用适用于 Linux 的 vCloud Director 安装程序升级现有环境。请参见第 12 章 迁移到 vCloud Director 设备。

您可以执行 vCloud Director 安装的协调升级或手动升级 vCloud Director 安装。通过协调升级，运行单个命令即可升级服务器组中的所有单元以及数据库。通过手动升级，按顺序升级每个单元和数据库。

从 vCloud Director 9.5 开始：

- 不支持 Oracle 数据库。如果您的现有 vCloud Director 安装使用 Oracle 数据库，请参见使用 Oracle 数据库的 vCloud Director 安装的升级工作流。
- 不支持启用和禁用 ESXi 主机。开始升级之前，必须启用所有 ESXi 主机。可以通过使用 vSphere Web Client 将 ESXi 主机置于维护模式。
- vCloud Director 使用具有增强型 LDAP 支持的 Java。如果使用的是 LDAPS 服务器，为避免 LDAP 登录失败，必须确认具有构造正确的证书。有关信息，请参见《Java 8 版本变更》，网址为 https://www.java.com。

升级 vCloud Director 时，新版本必须与现有安装的以下组件兼容：

- 当前用于 vCloud Director 数据库的数据库软件。

  如果您的现有 vCloud Director 安装使用 Oracle 数据库，请参见使用 Oracle 数据库的 vCloud Director 安装的升级工作流。
- 当前使用的 VMware vSphere ® 版本。
- 当前使用的 VMware NSX® 版本。

有关升级途径和 vCloud Director 与其他 VMware 产品及第三方数据库的兼容性信息，请参阅《VMware 产品互操作性列表》，网址为 http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php。如果打算在 vCloud Director 升级过程中升级 vSphere 或 NSX 组件，则必须在第 13 章 升级或迁移 vCloud Director 之后进行升级。

至少升级一台 vCloud Director 服务器后，可以升级 vCloud Director 数据库。该数据库负责存储有关服务器的运行时状态的信息，包括正在运行的所有 vCloud Director 任务的状态。要确保升级后数据库中的任务信息均有效，必须在开始升级之前确认任何服务器上均没有处于活动状态的任务。

升级过程还将保留以下未存储在 vCloud Director 数据库中的项目：

- 本地和全局属性文件复制到新安装。
- 将用于客户机自定义支持的 Microsoft Sysprep 文件复制到新安装。

升级需要足够长的 vCloud Director 停机时间，以便升级服务器组的所有服务器和数据库。如果使用负载平衡器，可以将其配置为返回一条消息，例如，系统处于脱机状态，无法升级 `(The system is offline for upgrade)`。

使用 Oracle 数据库的 vCloud Director 安装的升级工作流

升级使用 Oracle 数据库的 vCloud Director 安装之前，必须将数据库从 vCloud Director 版本 9.1 迁移到 PostgreSQL。

1 如果当前的 vCloud Director 版本低于 9.1，请升级到版本 9.1。

  有关将 vCloud Director 升级到版本 9.1 的信息，请参见《vCloud Director 安装、配置和升级指南》9.1。

2 当您的 vCloud Director 安装版本为 9.1 时，请将 Oracle 数据库迁移到 PostreSQL 数据库。

  有关迁移到 PostgreSQL 数据库的信息，请参见《vCloud Director 管理员指南》文档中的单元管理工具参考。

3 从版本 9.1 升级 vCloud Director 安装。可以执行 vCloud Director 安装的协调升级，也可以手动升级 vCloud Director 安装。

修补 vCloud Director 设备部署

您可以修补 vCloud Director 设备以改善其功能或提高其安全性。请参见修补 vCloud Director 设备部署。将修补程序应用于每个 vCloud Director 设备并完成数据库升级后，必须重新启动整个服务器组的 vCloud Director 服务才能使其重新联机。

本章讨论了以下主题：

- 执行 vCloud Director 安装的协调升级
- 手动升级 vCloud Director 安装
- 数据库升级实用程序参考
- 修补 vCloud Director 设备部署

执行 vCloud Director 安装的协调升级

您可以通过运行带 `--private-key-path` 选项的 vCloud Director 安装程序来升级服务器组中的所有单元以及共享数据库。

如果 vCloud Director 服务器组包含基于支持的 Linux 操作系统的 vCloud Director 安装，则可以使用适用于 Linux 的 vCloud Director 安装程序升级该服务器组。如果您的 vCloud Director 服务器组包含 vCloud Director 9.5 设备部署，则只能在迁移工作流中使用适用于 Linux 的 vCloud Director 安装程序升级现有环境。请参见第 12 章 迁移到 vCloud Director 设备。

适用于 Linux 的 vCloud Director 作为数字签名的可执行文件分发，名称格式为 `vmware-vcloud-director-distribution-`*v.v.v*`-nnnnnn.bin`，其中 *v.v.v* 表示产品版本，nnnnnn 则为内部版本号。例如：`vmware-vcloud-director-distribution-8.10.0-3698331.bin`。运行此可执行文件可安装或升级 vCloud Director。

运行带 `--private-key-path` 选项的 vCloud Director 安装程序时，您可以添加 `upgrade` 实用程序的其他命令选项，例如 `--maintenance-cell`。有关数据库 `upgrade` 实用程序选项的信息，请参见数据库升级实用程序参考。

前提条件

- 确认 vCloud Director 数据库、vSphere 组件和 NSX 组件与新版本的 vCloud Director 兼容。

  重要事项 如果您的现有 vCloud Director 安装使用 Oracle 数据库，请确认已从 vCloud Director 版本 9.1 迁移到 PostgreSQL 数据库。请参见使用 Oracle 数据库的 vCloud Director 安装的升级工作流。

- 验证您是否拥有目标服务器的超级用户凭据。
- 如果要安装程序验证安装文件的数字签名，则在目标服务器上下载和安装 VMware 公钥。如果已验证安装文件的数字签名，则不需要在安装期间再次验证。请参见下载和安装 VMware 公钥。
- 验证您是否具有有效的许可证密钥来使用要升级到的 vCloud Director 软件版本。
- 确认所有单元都允许超级用户在不输入密码的情况下进行 SSH 连接。要执行验证，可以运行以下 Linux 命令：

  ```
  sudo -u vcloud ssh -i private-key-path root@cell-ip
  ```

  此示例将您的身份设置为 `vcloud`，然后以 root 身份与 *cell-ip* 处的单元建立 SSH 连接，但不提供 root 密码。如果本地单元上 *private-key-path* 中的私钥可由用户 `vcloud.vcloud` 读取，且相应的公钥位于 *cell-ip* 处 root 用户的 `authorized-keys` 文件中，此命令将成功。

  注 `vcloud` 用户、`vcloud` 组和 `vcloud.vcloud` 帐户由 vCloud Director 安装程序创建，用作 vCloud Director 进程运行时所用的身份。`vcloud` 用户没有任何密码。

- 确认所有 ESXi 主机都已启用。从 vCloud Director 9.5 开始，不支持已禁用的 ESXi 主机。
- 确认服务器组中的所有服务器均可访问共享的传输服务器存储。请参见准备传输服务器存储。

- 如果 vCloud Director 安装使用 LDAPS 服务器，为避免升级后 LDAP 登录失败，请确认您具有 Java 8 Update 181 的正确构造证书。有关信息，请参见《Java 8 版本变更》，网址为 https://www.java.com。

步骤

1 以 **root** 身份登录到目标服务器。

2 将安装文件下载到目标服务器。

如果以媒体形式购买软件，请将安装文件复制到所有目标服务器均可访问的位置。

3 验证下载的校验和是否与下载页上发布的校验和相匹配。

MD5 和 SHA1 校验和的值发布在下载页上。使用适当的工具验证已下载安装文件的校验和是否与下载页上显示的校验和相匹配。使用以下形式的 Linux 命令可显示 *installation-file* 的校验和。

```
[root@cell1 /tmp]# md5sum installation-file
```

该命令将返回必须与下载页面上的 MD5 校验和相匹配的安装文件校验和。

4 确保安装文件为可执行文件。

安装文件需要执行权限。要确保安装文件具有此权限，请打开控制台、Shell 或终端窗口，并运行以下 Linux 命令，其中 *installation-file* 是 vCloud Director 安装文件的完整路径名。

```
[root@cell1 /tmp]# chmod u+x installation-file
```

5 在控制台、Shell 或终端窗口中，运行带有 `--private-key-path` 选项和目标单元私钥路径名的安装文件。

您可以添加数据库 `upgrade` 实用程序的其他命令选项。

```
./installation-file --private-key-path /vcloud/.ssh/id_rsa
```

注 无法从其路径名包含任何嵌入式空格符的目录运行安装文件。

安装程序检测到 vCloud Director 的早期版本，会提示您确认升级。

如果安装程序检测到的 vCloud Director 版本高于或等于安装文件中的版本，将显示错误消息并退出。

6 输入 **y** 并按 Enter 确认升级。

结果

安装程序将启动以下多单元升级工作流。

1 确认当前单元主机满足所有要求。

2 解压 vCloud Director RPM 软件包。

3 升级当前单元上的 vCloud Director 软件。

4 升级 vCloud Director 数据库。

5 升级其余每个单元上的 vCloud Director 软件，然后重新启动相应单元上的 vCloud Director 服务。

6 重新启动当前单元上的 vCloud Director 服务。

后续步骤

启动服务器组中所有单元上的 vCloud Director 服务。

您现在可以升级与已连接的 vCenter Server 系统关联的每个 NSX Manager，然后升级 vCenter Server 系统、ESXi 主机和 NSX Edge 。

手动升级 vCloud Director 安装

您可以通过运行不带命令选项的 vCloud Director 安装程序来升级单个单元。重新启动已升级的单元之前，必须先升级数据库模式。升级服务器组中至少一个单元后再升级数据库模式。

如果 vCloud Director 服务器组包含基于支持的 Linux 操作系统的 vCloud Director 安装，则可以使用适用于 Linux 的 vCloud Director 安装程序升级该服务器组。如果您的 vCloud Director 服务器组包含 vCloud Director 9.5 设备部署，则只能在迁移工作流中使用适用于 Linux 的 vCloud Director 安装程序升级现有环境。请参见第 12 章 迁移到 vCloud Director 设备。

对于多单元 vCloud Director 安装，您可以执行 vCloud Director 安装的协调升级，而不是按顺序手动升级每个单元和数据库。

前提条件

- 确认 vCloud Director 数据库、vSphere 组件和 NSX 组件与新版本的 vCloud Director 兼容。

  重要事项 如果您的现有 vCloud Director 安装使用 Oracle 数据库，请确认已从 vCloud Director 版本 9.1 迁移到 PostgreSQL 数据库。请参见使用 Oracle 数据库的 vCloud Director 安装的升级工作流。

- 确认您拥有 vCloud Director 服务器组中服务器的超级用户凭据。
- 如果要安装程序验证安装文件的数字签名，则在目标服务器上下载和安装 VMware 公钥。如果已验证安装文件的数字签名，则不需要在安装期间再次验证。请参见下载和安装 VMware 公钥。
- 验证您是否具有有效的许可证密钥来使用要升级到的 vCloud Director 软件版本。
- 确认所有 ESXi 主机都已启用。从 vCloud Director 9.5 开始，不支持已禁用的 ESXi 主机。

步骤

1 升级 vCloud Director 单元

   vCloud Director 安装程序将验证目标服务器是否符合所有升级必备条件，并升级该服务器中的 vCloud Director 软件。

2 升级 vCloud Director 数据库

   从升级后的 vCloud Director 服务器运行 vCloud Director 数据库升级工具。在升级共享数据库之前，不得重新启动已升级的任何 vCloud Director 服务器。

后续步骤

升级服务器组中的所有 vCloud Director 服务器和数据库后，可以在所有单元上启动 vCloud Director 服务。

您可以升级与已连接的 vCenter Server 系统关联的每个 NSX Manager，之后可以升级 vCenter Server 系统、ESXi 主机和 NSX Edge 。

升级 vCloud Director 单元

vCloud Director 安装程序将验证目标服务器是否符合所有升级必备条件，并升级该服务器中的 vCloud Director 软件。

适用于 Linux 的 vCloud Director 作为数字签名的可执行文件分发，名称格式为 `vmware-vcloud-director-distribution-`*v.v.v*`-`nnnnnn`.bin`，其中 *v.v.v* 表示产品版本，nnnnnn 则为内部版本号。例如：`vmware-vcloud-director-distribution-8.10.0-3698331.bin`。运行此可执行文件可安装或升级 vCloud Director。

对于多单元 vCloud Director 安装，您必须在 vCloud Director 服务器组的每个成员上运行 vCloud Director 安装程序。

步骤

1 以 **root** 身份登录到目标服务器。

2 将安装文件下载到目标服务器。

如果以媒体形式购买软件，请将安装文件复制到所有目标服务器均可访问的位置。

3 验证下载的校验和是否与下载页上发布的校验和相匹配。

MD5 和 SHA1 校验和的值发布在下载页上。使用适当的工具验证已下载安装文件的校验和是否与下载页上显示的校验和相匹配。使用以下形式的 Linux 命令可显示 *installation-file* 的校验和。

```
[root@cell1 /tmp]# md5sum installation-file
```

该命令将返回必须与下载页面上的 MD5 校验和相匹配的安装文件校验和。

4 确保安装文件为可执行文件。

安装文件需要执行权限。要确保安装文件具有此权限，请打开控制台、Shell 或终端窗口，并运行以下 Linux 命令，其中 *installation-file* 是 vCloud Director 安装文件的完整路径名。

```
[root@cell1 /tmp]# chmod u+x installation-file
```

5 运行安装文件。

要运行安装文件，请输入完整路径名，例如：

```
[root@cell1 /tmp]# ./installation-file
```

该文件包括安装脚本和嵌入式 RPM 包。

注 无法从其路径名包含任何嵌入式空格符的目录运行安装文件。

如果安装程序检测到的 vCloud Director 版本高于或等于安装文件中的版本，将显示错误消息并退出。

如果安装程序检测到 vCloud Director 的早期版本，则会提示您确认升级。

6 输入 **y** 并按 Enter 确认升级。

安装程序将启动以下升级工作流。

a 验证主机是否满足所有要求。

b 解压 vCloud Director RPM 软件包。

c 单元上的所有活动 vCloud Director 作业都完成后，停止服务器上的 vCloud Director 服务并升级已安装的 vCloud Director 软件。

如果您未在目标服务器上安装 VMware 公钥，安装程序将显示以下形式的警告：

```
warning: installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

更改目标服务器上的现有 `global.properties` 文件时，安装程序将显示以下形式的警告：

```
warning: /opt/vmware/vcloud-director/etc/global.properties created as /opt/vmware/vcloud-director/etc/global.properties.rpmnew
```

注 如果您先前已更新现有 `global.properties` 文件，您可以从 `global.properties.rpmnew` 中检索这些更改。

7 （可选） 更新日志记录属性。

升级后，新的日志记录属性将写入到文件 `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew` 中。

选项	操作
如果未更改现有日志记录属性	将此文件复制到 `/opt/vmware/vcloud-director/etc/log4j.properties`。
如果已更改日志记录属性	要保留所做更改，请将 `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew` 与现有 `/opt/vmware/vcloud-director/etc/log4j.properties` 文件进行合并。

结果

vCloud Director 升级完成后，安装程序将显示一条消息，其中包含有关旧配置文件位置的信息。然后，安装程序将提示您运行数据库升级工具。

后续步骤

如果尚未升级，可以升级 vCloud Director 数据库。

对服务器组中的每个 vCloud Director 单元重复此过程。

重要事项 升级服务器组中的所有单元和数据库后，才能启动 vCloud Director 服务。

升级 vCloud Director 数据库

从升级后的 vCloud Director 服务器运行 vCloud Director 数据库升级工具。在升级共享数据库之前，不得重新启动已升级的任何 vCloud Director 服务器。

所有正在运行和最新完成的任务信息存储在 vCloud Director 数据库中。由于数据库升级会导致此任务信息失效，因此数据库升级实用程序会在升级过程开始时确认未运行任何任务。

vCloud Director 服务器组中的所有单元共享同一数据库。无论要升级多少单元，只需升级数据库一次。升级数据库后，未升级的 vCloud Director 单元将无法连接到数据库。您必须升级所有单元以便连接到升级后的数据库。

前提条件

- 备份现有数据库。使用数据库软件供应商建议的过程。
- 确认服务器组中的所有 vCloud Director 单元均处于停止状态。在升级过程中，将停止已升级的单元。如果存在尚未升级的 vCloud Director 服务器，您可以使用单元管理工具来静默并关闭其服务。有关如何使用单元管理工具来管理单元的信息，请参见《vCloud Director 管理员指南》。
- 如果安装 vCloud Director 时使用 Oracle 数据库，则将迁移到 PostgeSQL 数据库。有关迁移到 PostgreSQL 数据库的信息，请参见《vCloud Director 管理员指南》中的单元管理工具参考。
- 查看数据库升级实用程序参考。选项和参数非强制。

步骤

1 运行带有或不带选项的数据库 `upgrade` 实用程序。

```
/opt/vmware/vcloud-director/bin/upgrade
```

如果数据库升级实用程序检测到 NSX Manager 版本不兼容，它将显示一条警告消息并取消升级。

2 在提示时，输入 **y** 并按 Enter 确认数据库升级。

3 在提示时，输入 **y** 并按 Enter 确认已备份数据库。

如果使用了 `--backup-completed` 选项，实用程序将跳过此提示。

4 如果实用程序检测到活动单元，请在提示继续时输入 **n** 退出 shell，然后确认没有任何单元正在运行并重试通过步骤 步骤 1 升级。

结果

数据库升级工具将运行，并显示进度消息。升级完成后，系统会提示您在当前服务器上启动 vCloud Director 服务。

后续步骤

输入 **y** 并按 Enter，或者稍后通过运行 `service vmware-vcd start` 命令启动该服务。

您可以启动已升级的 vCloud Director 服务器的服务。

您可以升级服务器组的其余 vCloud Director 成员并启动其服务。请参见升级 vCloud Director 单元。

数据库升级实用程序参考

运行 `upgrade` 实用程序时，可以在命令行以选项和参数形式提供设置信息。

表 11-1. 数据库升级实用程序选项和参数

选项	参数	描述
`--backup-completed`	无	指定您已完成 vCloud Director 备份。包括此选项时，升级实用程序不会提示您备份数据库。
`--ceip-user`	CEIP 服务帐户的用户名。	如果系统组织中已存在使用此用户名的用户，则升级将失败。默认值：`phone-home-system-account`。
`--enable-ceip`	选择一项： ■ true ■ false	指定此安装是否加入 VMware 客户体验改善计划 (CEIP)。默认值为 true（如果未提供），并且不会在当前配置中设置为 false。VMware 客户体验提升计划（“CEIP”）已在“信任与保证中心”（网址为 http://www.vmware.com/trustvmware/ceip.html）提供有关通过 CEIP 收集的数据以及 VMware 将其用于何种用途等其他信息。您可以随时使用单元管理工具加入或退出此产品的 VMware CEIP。请参见《vCloud Director 管理员指南》中的“单元管理工具参考”。
`--installer-path`	vCloud Director 安装文件的完整路径名。用户 vcloud.vcloud 必须能够读取安装文件及其存储目录。	此产品已加入 VMware 客户体验提升计划（“CEIP”）。有关通过 CEIP 收集的数据的详细信息以及 VMware 将其用于何种用途已在“信任与保证中心”中列明，网址为 http://www.vmware.com/trustvmware/ceip.html。您可以随时使用单元管理工具加入或退出此产品的 VMware CEIP。请参见《vCloud Director 管理员指南》中的“单元管理工具参考”。 需要 `--private-key-path` 选项。
`--maintenance-cell`	IP 地址	升级期间，升级实用程序的在维护模式下运行的单元的 IP 地址。此单元在其他单元关闭前进入维护模式，且在升级其他单元时处于维护模式。在其他单元均已升级且至少有一个单元重新启动后，此单元关闭并升级。需要 `--private-key-path` 选项。

表 11-1. 数据库升级实用程序选项和参数 （续）

选项	参数	描述
`--multisite-user`	多站点系统帐户的用户名。	vCloud Director 多站点功能使用此帐户。如果系统组织中已存在使用此用户名的用户，则升级将失败。默认值：`multisite-system-account`。
`--private-key-path`	路径名	单元的专用密钥的完整路径名。使用此选项时，服务器组中的所有单元将正常关闭、升级并在数据库升级后重新启动。请参见执行 vCloud Director 安装的协调升级，了解有关此升级工作流的详细信息。
`--unattended-upgrade`	无	指定无需人工干预的升级

如果使用 `--private-key-path` 选项，所有单元都必须配置为允许超级用户在不输入密码的情况下进行 `ssh` 连接。您可以使用如下所示的 Linux 命令行进行验证。此示例将您的身份设置为 `vcloud`，然后以 `root` 身份建立到 *cell-ip* 单元的 `ssh` 连接，但不提供 root 密码。

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

如果本地单元上 *private-key-path* 中的私钥可由用户 `vcloud.vcloud` 读取，且相应的公钥已添加到 *cell-ip* 处 root 用户的 `authorized-keys` 文件中，此命令将成功。

注 `vcloud` 用户、`vcloud` 组和 `vcloud.vcloud` 帐户由 vCloud Director 安装程序创建，用作 vCloud Director 进程运行时所用的身份。`vcloud` 用户没有任何密码。

修补 vCloud Director 设备部署

可以使用可能与产品功能和安全性改进相关的修补程序更新 vCloud Director 设备。

在 vCloud Director 设备部署修补期间，vCloud Director 服务将停止工作，并且可能会停机一段时间。停机时间取决于修补每个 vCloud Director 设备和运行 vCloud Director 数据库升级脚本所需的时间。vCloud Director 服务器组中的工作单元数会减少，直到停止最后一个 vCloud Director 设备上的 vCloud Director 服务。在 vCloud Director HTTP 端点前面正确配置的负载平衡器应停止将流量路由到停止的单元。

将修补程序应用于每个 vCloud Director 设备并完成数据库升级后，必须重新启动整个服务器组的 vCloud Director 服务才能使其重新联机。

步骤

1 在 Web 浏览器中，登录到 vCloud Director 设备实例的设备管理用户界面以识别主设备，`https://appliance_ip_address:5480`。

记下主设备名称。升级数据库时，必须使用主设备名称。

2 将更新软件包下载到设备。

vCloud Director 作为可执行文件分发，名称格式为 VMware_vCloud_Director_*v.v.v.v*–*nnnnnnnn*_update.tar.gz，其中 *v.v.v.v* 表示产品版本，*nnnnnnnn* 表示内部版本号。例如，VMware_vCloud_Director_9.7.0.4248–13560441_update.tar.gz。

3 创建要在其中提取更新软件包的 local–update–packag 目录。

```
mkdir /tmp/local–update–package
```

4 在新创建的目录中提取更新软件包。

```
tar –zxf VMware_vCloud_Director_v.v.v.v–nnnnnnnn_update.tar.gz \
               –C /tmp/local–update–package
```

5 将 local–update–package 目录设置为更新存储库。

```
vamicli    update ––repo file:///tmp/local–update–package
```

6 检查更新以验证是否正确建立了存储库。

```
vamicli update ––check
```

修补程序版本显示可用更新。

7 运行以下命令，关闭 vCloud Director：

```
/opt/vmware/vcloud–director/bin/cell–management–tool –u <admin username> cell ––shutdown
```

8 从主设备中，备份 vCloud Director 设备的嵌入式数据库。

注 如果要从 vCloud Director 9.7.0.1 升级到更高版本，请手动备份位于 /opt/vmware/vcloud–director/etc/truststore 的信任存储区文件。

```
/opt/vmware/appliance/bin/create–db–backup
```

9 应用可用修补程序。

```
vamicli update ––install latest
```

10 在每个设备上重复 步骤 2 至 步骤 7 和 步骤 9。

11 从任何设备中，运行 vCloud Director 数据库升级脚本。

```
/opt/vmware/vcloud–director/bin/upgrade
```

12 启动每个设备上的 vCloud Director 服务。

```
service vmware–vcd start
```

迁移到 vCloud Director 设备

12

从版本 9.7 开始，vCloud Director 设备包括一个具有高可用性功能的嵌入式 PostgreSQL 数据库。可以将早期版本的现有 vCloud Director 环境迁移到包含 vCloud Director 9.7 设备部署的 vCloud Director 环境。

可以迁移包含基于 Linux 或 vCloud Director 设备部署的 vCloud Director 安装的 vCloud Director 环境。可以迁移使用外部 Microsoft SQL 数据库或外部 PostgreSQL 数据库的 vCloud Director 环境。

如果您的 vCloud Director 环境使用外部 Oracle 数据库，则在迁移到 vCloud Director 设备之前，必须将数据库从 vCloud Director 版本 9.1 迁移到 PostgreSQL。有关升级具有 Oracle 数据库的 vCloud Director 安装的工作流的信息，请参见第 11 章 升级 vCloud Director 并修补 vCloud Director 设备。

本章讨论了以下主题：

将具有外部 Microsoft SQL 数据库的 vCloud Director 迁移到 vCloud Director 设备

如果早期版本的当前 vCloud Director 环境使用外部 Microsoft SQL 数据库，则可以迁移到包含 vCloud Director 9.7 设备部署的新 vCloud Director 环境。您当前的 vCloud Director 环境可以包含基于 Linux 或 vCloud Director 设备部署的 vCloud Director 安装。新的 vCloud Director 环境可以在高可用性模式下使用设备的嵌入式 PostgreSQL 数据库。

迁移工作流包括四个主要阶段。

- 通过部署 vCloud Director 9.7 设备的一个或多个实例创建新的 vCloud Director 服务器组
- 升级现有的 vCloud Director 环境
- 将外部数据库迁移到嵌入式数据库
- 复制共享传输服务数据和证书数据。

过程

1 将当前 vCloud Director 环境升级到版本 9.7，然后升级源数据库模式。

请参见第 11 章 升级 vCloud Director 并修补 vCloud Director 设备。

2 确认迁移源 vCloud Director 重新启动成功。

3 如果希望新的 vCloud Director 环境使用现有环境的 IP 地址，请将现有单元的 IP 地址更改为临时 IP 地址。

4 如果希望新的 vCloud Director 环境使用现有环境的 NFS 服务器，请在此 NFS 服务器上创建新目录并导出为新的共享 NFS 挂载点。

   无法重用现有的挂载点，因为旧 NFS 中用户的用户 ID 和组 ID (UID/GID) 可能与新 NFS 中的用户 ID 和组 ID 不匹配。

5 通过部署 vCloud Director 9.7 设备的一个或多个实例创建新的服务器组。

   - 如果要使用数据库高可用性功能，请部署一个主单元和两个备用单元以及（可选）一个或多个 vCD 应用程序单元。
   - 如果将现有单元的 IP 地址更改为临时 IP 地址，则可以对新单元使用原始 IP 地址。
   - 如果在现有 NFS 服务器上导出新路径，则可以对新环境使用这个新的共享挂载点。

   请参见第 6 章 部署 vCloud Director 设备。

6 在每个现有单元以及每个新部署的单元上，运行以下命令，停止 vCloud Director 服务。

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

7 选择要用作迁移源的现有单元之一。

   迁移源必须有权访问新部署的主单元的 `eth1` 网络 IP 地址。

8 在新的主单元上，启用从迁移源访问嵌入式数据库。

   请参见配置对 vCloud Director 数据库的外部访问。

9 在迁移源上，运行单元管理工具以将外部数据库迁移到新主单元中嵌入的数据库。

   嵌入式数据库使用设备的 `eth1` 网络 IP 地址。

```
/opt/vmware/vcloud-director/bin/cell-management-tool dbmigrate -dbhost eth1_IP_new_primary \
-dbport 5432 -dbuser vcloud -dbname vcloud -dbpassword database_password_new_primary
```

   有关使用单元管理工具的信息，请参见《vCloud Director 管理员指南》。

10 在每个新部署的单元上，备份并替换配置数据，然后重新配置并启动 vCloud Director 服务。

   a 备份属性和证书文件，然后从迁移源复制并替换这些文件。

      `global.properties`、`responses.properties`、`certificates` 和 `proxycertificates` 文件位于 `/opt/vmware/vcloud-director/etc/`。

      重要事项 如果要迁移到 vCloud Director 版本 9.7.0.1 或更高版本，还必须从迁移源备份、复制和替换 `truststore` 文件以及其他文件。

   b 备份密钥库文件，即 `/opt/vmware/vcloud-director/certificates.ks`。

      请勿从迁移源复制并替换密钥库文件。

c 运行以下命令，重新配置 vCloud Director 服务。

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type postgres
--database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --database-
port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-director/
certificates.ks \
--keystore-password root_password_new_primary --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

其中：

- `--keystore-password` 值与此设备的初始 **root** 密码一致。
- `--database-password` 值与在设备部署过程中设置的数据库密码一致。
- `--database-host` 值与主设备的 `eth1` 网络 IP 地址一致。
- `--keystore` 值是在步骤 10.b 中备份的 `certificates.ks` 文件的路径。
- `--primary-ip` 值与设备的 `eth0` 网络 IP 地址一致。
- `--console-proxy-ip` 值与设备的 `eth0` 网络 IP 地址一致。

有关故障排除信息，请参见迁移或还原到 vCloud Director 设备时，重新配置 vCloud Director 服务失败。

d 运行以下命令，启动 vCloud Director 服务。

```
service vmware-vcd start
```

可以在 `/opt/vmware/vcloud-director/logs/cell.log` 中监控单元的启动进度。

11 新服务器组的所有单元完成启动过程后，验证 vCloud Director 环境的迁移是否成功。

a 使用新服务器组中任何单元的 `eth0` 网络 IP 地址打开 vCloud Director Web Console，即 `https://`*`et0_IP_new_cell`*`/cloud`。

b 使用现有**系统管理员**凭据登录到 vCloud Director Web Console。

c 验证您的 vSphere 和云资源在新环境中是否可用。

12 成功验证 vCloud Director 迁移后，使用 vCloud Director Web Console 删除属于旧 vCloud Director 环境的断开连接单元。

a 在**管理与监控**选项卡上，单击**云单元**。

b 右键单击单元名称，并选择**删除**。

可以部署 vCloud Director 设备以将成员添加到迁移环境的服务器组中。

后续步骤

新迁移的 vCloud Director 设备环境使用自签名证书。要使用旧环境的正确签名证书，请在新环境的每个单元上，执行以下步骤：

1 将密钥库文件从旧单元复制到 `/opt/vmware/vcloud-director/data/transfer/certificates.ks` 并替换。

2 运行单元管理工具命令以替换证书。

确保 `vcloud.vcloud` 是此文件的所有者。

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/
vcloud-director/data/transfer/certificates.ks \
--keystore-password ks_password_old_vCD
```

3 重新启动 vCloud Director 服务。

```
service vmware-vcd restart
```

如果向此服务器组添加新成员，则会使用这些完好签名证书部署新的设备单元。

将具有外部 PostgreSQL 数据库的 vCloud Director 迁移到 vCloud Director 设备

如果早期版本的当前 vCloud Director 环境使用外部 PostgreSQL 数据库，则可以迁移到包含 vCloud Director 9.7 设备部署的新 vCloud Director 环境。您当前的 vCloud Director 环境可以包含基于 Linux 或 vCloud Director 设备部署的 vCloud Director 安装。新的 vCloud Director 环境可以在高可用性模式下使用设备的嵌入式 PostgreSQL 数据库。

迁移工作流包括四个主要阶段。

- 升级现有的 vCloud Director 环境
- 通过部署 vCloud Director 9.7 设备的一个或多个实例创建新的 vCloud Director 服务器组
- 将外部数据库迁移到嵌入式数据库
- 复制共享传输服务数据和证书数据。

过程

1 如果当前外部 PostgreSQL 数据库的版本为 9.x，请将外部 PostgreSQL 数据库升级到版本 10。

2 将当前的 vCloud Director 环境升级到版本 9.7。

请参见第 11 章 升级 vCloud Director 并修补 vCloud Director 设备。

3 确认迁移源 vCloud Director 重新启动成功。

4 在已升级的 vCloud Director 环境的每个单元上，运行以下命令，停止 vCloud Director 服务。

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

5 在外部 PostgreSQL 数据库上，备份当前数据库。

```
sudo -u postgres path_to_pg_dump -Fc db_name > /tmp/db_dump_name
```

如果 /tmp 文件夹上的可用空间不足，请使用其他位置存储转储文件。

6 如果数据库所有者和数据库名称不同于 vcloud，请记下用户名和数据库名称。

在步骤 13 中，您必须在新环境中创建此用户并重命名数据库。

7 如果需要新的 vCloud Director 环境使用现有环境的 IP 地址，则必须将属性和证书文件复制到外部 PostgreSQL 数据库上的某个位置，然后关闭单元的电源。

a 将位于 /opt/vmware/vcloud-director/etc/ 中的 global.properties、responses.properties、certificates 和 proxycertificates 文件复制到外部 PostgreSQL 数据库上的 /tmp 或任何首选位置。

b 关闭现有环境中单元的电源。

8 如果希望新的 vCloud Director 环境使用现有环境的 NFS 服务器，请在此 NFS 服务器上创建新目录并导出为新的共享 NFS 挂载点。

无法重用现有的挂载点，因为旧 NFS 中用户的用户 ID 和组 ID (UID/GID) 可能与新 NFS 中的用户 ID 和组 ID 不匹配。

9 通过部署 vCloud Director 9.7 设备的一个或多个实例创建新的服务器组。

- 如果要使用数据库高可用性功能，请部署一个主单元和两个备用单元以及（可选）一个或多个 vCD 应用程序单元。
- 如果已关闭现有环境中单元的电源，则可以使用新单元的原始 IP 地址。
- 如果在现有 NFS 服务器上导出新路径，则可以对新环境使用这个新的共享挂载点。

请参见第 6 章 部署 vCloud Director 设备。

10 在每个新部署的单元上，运行以下命令，停止 vCloud Director 服务。

```
service vmware-vcd stop
```

11 将外部 PostgreSQL 数据库上 /tmp 文件夹中的转储文件复制到新环境主单元上的 /tmp 文件夹。

请参见步骤 5。

12 更改转储文件的权限。

```
chmod a+r /tmp/db_dump_name
```

13 以 **root** 身份登录到新部署的主单元的控制台，然后将 vCloud Director 数据库从外部数据库传输到嵌入式数据库。

a 将用户切换为 postgres，连接到 psql 数据库终端，然后运行以下语句以丢弃 vcloud 数据库。

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

b 如果现有外部数据库的数据库所有者不同于 vcloud，请使用在步骤 6 中记录的名称创建一个用户。

```
sudo –i –u postgres /opt/vmware/vpostgres/current/bin/psql –c 'CREATE USER
<db_owner_external_pg>;'
```

c 运行 pg_restore 命令。

```
sudo –u postgres /opt/vmware/vpostgres/current/bin/pg_restore –C –d postgres /tmp/db_dump_name
```

d 如果现有外部数据库的数据库名称不同于 vcloud，请使用在步骤 6 中记录的名称将数据库名称更改为 vcloud。

```
sudo –i –u postgres /opt/vmware/vpostgres/current/bin/psql –c 'ALTER DATABASE
<db_name_external_pg> RENAME TO vcloud;'
```

e 如果现有 vCloud Director 环境的数据库所有者不同于 vcloud，请将数据库所有者更改为 vcloud，然后将表重新分配给 vcloud。

```
sudo –i –u postgres /opt/vmware/vpostgres/current/bin/psql –c 'ALTER DATABASE vcloud OWNER TO
vcloud;'
```

```
sudo –i –u postgres /opt/vmware/vpostgres/current/bin/psql –d vcloud –c 'REASSIGN OWNED BY
<db_owner_external_pg> TO vcloud;'
```

14 在每个新部署的单元上，备份并替换配置数据，然后重新配置并启动 vCloud Director 服务。

a 备份属性和证书文件，然后从迁移源的外部 PostgreSQL 数据库上的位置（在步骤 7a 中将文件复制到的位置）复制并替换这些文件。

global.properties、responses.properties、certificates 和 proxycertificates 文件位于 /opt/vmware/vcloud-director/etc/。

重要事项 如果要迁移到 vCloud Director 版本 9.7.0.1 或更高版本，还必须从迁移源备份、复制和替换 truststore 文件以及其他文件。

b 备份密钥库文件，即 /opt/vmware/vcloud-director/certificates.ks。

请勿从迁移源复制并替换密钥库文件。

c 运行以下命令，重新配置 vCloud Director 服务。

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type postgres
--database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --database-
port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-director/
certificates.ks \
--keystore-password root_password_new_primary --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

其中：

- `--keystore-password` 值与此设备的初始 **root** 密码一致。
- `--database-password` 值与在设备部署过程中设置的数据库密码一致。
- `--database-host` 值与主设备的 `eth1` 网络 IP 地址一致。
- `--primary-ip` 值与设备的 `eth0` 网络 IP 地址一致。
- `--console-proxy-ip` 值与设备的 `eth0` 网络 IP 地址一致。
- `--console-proxy-port` 值与设备控制台代理端口 8443 一致。

有关故障排除信息，请参见迁移或还原到 vCloud Director 设备时，重新配置 vCloud Director 服务失败。

d 运行以下命令，启动 vCloud Director 服务。

```
service vmware-vcd start
```

可以在 `/opt/vmware/vcloud-director/logs/cell.log` 中监控单元的启动进度。

15 新服务器组的所有单元完成启动过程后，验证 vCloud Director 环境的迁移是否成功。

a 使用新服务器组中任何单元的 `eth0` 网络 IP 地址打开 vCloud Director Web Console，即 `https://`*`et0_IP_new_cell`*`/cloud`。

b 使用现有**系统管理员**凭据登录到 vCloud Director Web Console。

c 验证您的 vSphere 和云资源在新环境中是否可用。

16 成功验证 vCloud Director 迁移后，使用 vCloud Director Web Console 删除属于旧 vCloud Director 环境的断开连接单元。

a 在**管理与监控**选项卡上，单击**云单元**。

b 右键单击单元名称，并选择**删除**。

可以部署 vCloud Director 设备以将成员添加到迁移环境的服务器组中。

后续步骤

新迁移的 vCloud Director 设备环境使用自签名证书。要使用旧环境的正确签名证书，请在新环境的每个单元上，执行以下步骤：

1 将密钥库文件从旧单元复制到 `/opt/vmware/vcloud-director/data/transfer/certificates.ks` 并替换。

2 运行单元管理工具命令以替换证书。

确保 `vcloud.vcloud` 是此文件的所有者。

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/
vcloud-director/data/transfer/certificates.ks \
--keystore-password ks_password_old_vCD
```

3 重新启动 vCloud Director 服务。

```
service vmware-vcd restart
```

如果向此服务器组添加新成员，则会使用这些完好签名证书部署新的设备单元。

升级或迁移 vCloud Director 之后

13

升级或迁移所有 vCloud Director 服务器及共享数据库后，可以升级为云提供网络服务的 NSX Manager 实例。然后，可以升级注册到 vCloud Director 安装的 ESXi 主机和 vCenter Server 实例。

重要事项 从版本 9.7 开始，vCloud Director 仅支持高级 Edge 网关。必须将任何旧版非高级 Edge 网关转换为高级网关。请参见 https://kb.vmware.com/kb/66767。

本章讨论了以下主题：

升级与已连接的 vCenter Server 系统关联的每个 NSX Manager

升级注册到 vCloud Director 的 vCenter Server 和 ESXi 主机之前，必须升级与该 vCenter Server 关联的每个 NSX Manager。

升级 NSX Manager 会中断对 NSX 管理功能的访问，但不会中断网络服务。可以在 vCloud Director 升级前或升级后升级 NSX Manager，而无论是否正在运行任何 vCloud Director 单元。

有关升级 NSX 的信息，请参见 NSX for vSphere 文档，网址为 https://docs.vmware.com。

步骤

1 升级与注册到 vCloud Director 安装的每个 vCenter Server 关联的 NSX Manager。

2 升级所有 NSX Manager 后，可以升级注册的 vCenter Server 系统和 ESXi 主机。

升级 vCenter Server 系统、ESXi 主机和 NSX Edge

升级 vCloud Director 和 NSX Manager 后，您必须升级已注册到 vCloud Director 的 vCenter Server 系统和 ESXi 主机。升级所有已连接 vCenter Server 系统和 ESXi 主机后，您可以升级 NSX Edge。

前提条件

确认已升级与连接到云的 vCenter Server 系统相关联的每个 NSX Manager。请参见升级与已连接的 vCenter Server 系统关联的每个 NSX Manager。

步骤

1 禁用 vCenter Server 实例。

a 在 vCloud Director Web 控制台中，单击**管理与监控**选项卡，并在左侧窗格中单击 **vCenter**。

b 右键单击目标 vCenter Server 名称，然后单击**禁用**。

c 单击**是**。

2 升级 vCenter Server 系统。

有关信息，请参见《vCenter Server 升级》。

3 验证所有的 vCloud Director 公用 URL 和证书链。

a 在 vCloud Director Web 控制台中，单击**管理**选项卡，然后在左侧窗格中单击**公用地址**。

b 确认所有公用地址。

4 刷新 vCloud Director 中的 vCenter Server 注册。

a 在 vCloud Director Web 控制台中，单击**管理与监控**选项卡，并在左侧窗格中单击 **vCenter**。

b 右键单击目标 vCenter Server 名称，然后单击**刷新**。

c 单击**是**。

5 升级已升级的 vCenter Server 系统支持的每个 ESXi 主机。

请参见《VMware ESXi 升级》。

重要事项 若要确保有足够升级的主机容量以在云中支持虚拟机，请小批量升级主机。执行此操作时，主机代理可以及时完成升级并允许虚拟机迁移到已升级的主机中。

a 使用 vCenter Server 系统将主机置于维护模式，并允许该主机上的所有虚拟机迁移到其他主机。

b 升级主机。

c 使用 vCenter Server 系统重新连接主机。

d 使用 vCenter Server 系统将主机退出维护模式。

6 （可选） 升级与已升级的 vCenter Server 系统关联的 NSX Manager 所管理的 NSX Edge。

升级后的 NSX Edge 改进了性能和集成。您可以使用 NSX Manager 或 vCloud Director 来升级 NSX Edge。

- 有关使用 NSX Manager 升级 NSX Edge 的信息，请参见 NSX for vSphere 文档，网址为 https://docs.vmware.com。
- 要使用 vCloud Director 升级 NSX Edge，必须在 Edge 支持的 vCloud Director 网络对象上执行操作：
  - 使用 vCloud Director Web 控制台或 vCloud API 重置 Edge 网关服务的网络时，会相应地自动升级 Edge 网关。
  - 重新部署 Edge 网关将升级关联的 NSX Edge 设备。

- 重置 vApp 环境中的 vApp 网络将升级与该网络关联的 NSX Edge 设备。要使用 vCloud Director Web 控制台在 vApp 的上下文中重置 vApp 网络，请导航到该 vApp 的**网络**选项卡，显示其网络连接详细信息，右键单击 vApp 网络并选择**重置网络**。

有关如何重新部署 Edge 网关和重置 vApp 网络的详细信息，请参见 vCloud Director Web 控制台联机帮助或《vCloud API 编程指南》。

后续步骤

对注册到 vCloud Director 安装的其他 vCenter Server 系统重复此过程。

此版本中的新权限

vCloud Director 9.7 中引入了新权限，您可能希望将其添加到已发布给租户的任何现有全局角色中。

权限	描述	默认角色
SDDC: 查看 SDDC	可用于查看已发布到组织的所有 SDDC。 **系统管理员**可以查看所有 SDDC。	**系统管理员**和**组织管理员**
SDDC: 管理 SDDC	可用于添加、移除和编辑 SDDC。	**系统管理员**
SDDC: 管理 SDDC 代理	可用于添加、移除、启用和禁用 SDDC 代理。	**系统管理员**
服务应用程序: 查看服务应用程序	可用于查看已注册服务应用程序的列表。 用于 VMC 帐户。	**系统管理员**
服务应用程序: 注册 VMC SDDC	可用于创建、查看、编辑和移除服务应用程序。 用于 VMC 帐户。	**系统管理员**
服务应用程序: 管理服务应用程序	可用于注册服务应用程序。 用于 VMC 帐户。	**系统管理员**
Edge 群集: 查看 Edge 群集	可用于查看 Edge 群集的列表以及检索单个 Edge 群集。	**系统管理员**和**组织管理员**
Edge 群集: 管理 Edge 群集	可用于创建、编辑和移除 Edge 群集。	**系统管理员**和**组织管理员**
vApp: 编辑 VM 计算策略	允许用户更改虚拟机的计算策略。	**系统管理员**、**组织管理员**、**目录作者**和 **vApp 作者**
网关: 导入 Edge 网关	可用于将第 1 层路由器导入为 Edge 网关。	**系统管理员**和**组织管理员**

有关管理权限和角色的信息，请参见《vCloud Director 服务提供商管理门户指南》。

vCloud Director 设备故障排除

14

如果 vCloud Director 设备部署失败或设备运行不正常，则可以检查设备日志文件以确定问题的原因。

VMware 技术支持通常会在处理支持请求时要求提供诊断信息。您可以使用 `vmware-vcd-support` 脚本收集主机日志信息和 vCloud Director 日志。有关收集 vCloud Director 的诊断信息的详细信息，请参见 https://kb.vmware.com/s/article/1026312。运行 `vmware-vcd-support` 脚本时，日志可能包含有关已取消配置或已替换单元（状态为 `FAIL`）的信息。请参见 https://kb.vmware.com/s/article/71349。

本章讨论了以下主题：

检查 vCloud Director 设备中的日志文件

部署 vCloud Director 设备后，可以检查首次引导日志和数据库日志中是否有错误和警告。

步骤

1. 以 **root** 身份直接或通过 SSH 登录到 vCloud Director 设备控制台。
2. 导航到 `/opt/vmware/var/log`。
3. 检查日志文件。
   - `firstboot` 文件包含与设备首次引导相关的日志记录信息。
   - `/opt/vmware/var/log/vcd/` 目录包含与复制管理器 (repmgr) 工具套件设置和重新配置以及设备同步相关的日志。
   - `/opt/vmware/var/log/vcd/pg/` 目录包含与嵌入式设备数据库备份相关的日志。
   - `/opt/vmware/etc/vami/ovfEnv.xml` 文件包含部署 OVF 参数。

设备部署后 vCloud Director 单元无法启动

您成功部署了 vCloud Director 设备，但 vCloud Director 服务可能无法启动。

问题

`vmware-vcd` 服务在设备部署后处于非活动状态。

原因

如果部署了主单元，由于预填充的 NFS 共享传输服务存储，vCloud Director 服务可能无法启动。部署主设备之前，共享传输服务存储不得包含 `responses.properties` 文件或 `appliance-nodes` 目录。

如果部署了备用或 vCD 应用程序单元，则 vCloud Director 服务可能会由于 NFS 共享传输存储中缺少 `responses.properties` 文件而无法启动。部署备用或 vCD 应用程序设备之前，共享传输服务存储必须包含 `responses.properties` 文件。

解决方案

1. 以 **root** 身份直接或通过 SSH 登录到 vCloud Director 设备控制台。
2. 检查 `/opt/vmware/var/log/vcd/setupvcd.log` 中是否有关于 NFS 存储的错误消息。
3. 针对设备类型准备 NFS 存储。
4. 重新部署单元。

迁移或还原到 vCloud Director 设备时，重新配置 vCloud Director 服务失败

迁移或还原到 vCloud Director 设备时，运行 `configure` 命令可能会失败。

问题

将 vCloud Director 迁移或还原到新 vCloud Director 设备环境的过程中，需要运行 `configure` 命令以在每个新单元中重新配置 vCloud Director 服务。`configure` 命令可能会失败，并显示以下错误消息“`sun.security.validator.ValidatorException: PKIX 路径验证失败: java.security.cert.CertPathValidatorException: 签名检查失败 (sun.security.validator.ValidatorException: PKIX path validation failed: java.security.cert.CertPathValidatorException: signature check failed)`”。

解决方案

1. 在目标单元上，运行以下命令。

```
sed -i '/vcd_ova.crt/ s/$/ --force /' /opt/vmware/appliance/bin/appliance-sync.sh
```

2. 等待 1 分钟，然后重新运行 `configure` 命令。

使用日志文件对 vCloud Director 更新和修补程序进行故障排除

将修补程序应用于 vCloud Director 设备时，可以检查日志文件中是否存在错误和警告。

问题

如果 `vamicli` 命令返回错误，则可以使用日志文件进行故障排除。

解决方案

1 以 **root** 身份直接或通过 SSH 登录到 vCloud Director 设备控制台。

2 导航到相应的日志文件。

- 如果 `vamicli update --check` 失败，则导航到 `/opt/vmware/var/log/vami/vami.log`。
- 如果 `vamicli update --install latest` 失败，则导航到 `/opt/vmware/var/log/vami/updatecli.log`。

3 检查日志文件。

检查 vCloud Director 更新失败

检查 vCloud Director 设备的更新时，运行 `vamicli update --check` 命令可能会失败。

问题

将修补程序应用于 vCloud Director 设备的过程中，您需要运行 `vamicli update --check` 命令检查可用更新。`vamicli update --check` 命令可能会失败并显示错误消息：失败：下载清单时出错。请联系您的供应商 (`Failure: Error downloading manifest. Please contact your vendor`)。

原因

更新存储库目录的路径不正确。

解决方案

1 使用正确的路径运行 `vamicli` 命令。

```
vamicli update --repo file:/root/local-update-repo
```

2 再次运行命令以检查更新。

```
vamicli update --check
```

安装 vCloud Director 的最新更新失败

将最新更新安装到 vCloud Director 设备时，运行 `vamicli update --install latest` 命令可能会失败。

问题

将修补程序应用于 vCloud Director 设备的过程中，您需要运行 `vamicli update --install latest` 命令以应用最新的可用修补程序。`vamicli update --install latest` 命令可能会失败并显示错误消息：失败：运行软件包安装时出错 (Failure: Error while running package installation)

原因

NFS 服务器无法访问时，会出现该错误。

解决方案

1 验证挂载到 `/opt/vmware/vcloud-director/data/transfer` 的 NFS 服务器是否可访问。

2 再次运行以下命令以应用可用修补程序。

```
vamicli update --install latest
```

卸载 vCloud Director 软件

15

使用 Linux rpm 命令可从单个服务器中卸载 vCloud Director 软件。

步骤

1 以 **root** 身份登录到目标服务器。

2 卸载传输服务存储，通常挂载于以下位置：/opt/vmware/vcloud-director/data/transfer。

3 打开控制台、Shell 或终端窗口，并运行 Linux rpm 命令。

```
rpm -e vmware-phonehome vmware-vcloud-director vmware-vcloud-director-rhel
```

如果安装了依赖 vmware-vcloud-director 软件包的其他软件包，系统将提示您在卸载 vCloud Director 前先卸载这些软件包。