

# 管理 VMware vSAN

Update 1

2018 年 10 月 16 日

VMware vSphere 6.7

VMware vSAN 6.7



vmware®

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

VMware 网站还提供了最近的产品更新。

如果您对本文档有任何意见或建议, 请将反馈信息发送至:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

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](http://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](http://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](http://www.vmware.com/cn)

# 目录

## About VMware vSAN 5

### 1 vSAN 简介 6

### 2 配置和管理 vSAN 群集 7

使用 vSphere Client 配置 vSAN 群集 7

使用 vSphere Web Client 配置 vSAN 群集 8

在现有群集上启用 vSAN 10

禁用 vSAN 11

编辑 vSAN 设置 12

查看 vSAN 数据存储 12

### 3 使用 vSAN 策略 14

关于 vSAN 策略 14

主机固定 16

查看 vSAN 存储提供程序 17

关于 vSAN 默认存储策略 17

将默认存储策略分配到 vSAN 数据存储 19

使用 vSphere Client 定义针对 vSAN 的存储策略 19

使用 vSphere Web Client 定义针对 vSAN 的存储策略 21

### 4 扩展和管理 vSAN 群集 23

扩展 vSAN 群集 23

使用维护模式 27

管理 vSAN 群集中的故障域 29

使用 vSAN iSCSI 目标服务 33

将混合 vSAN 群集迁移到全闪存群集 37

关闭 vSAN 群集的电源 38

### 5 vSAN 群集中的设备管理 39

管理磁盘组和设备 39

使用单独的设备 41

### 6 提高 vSAN 群集中的空间效率 49

vSAN 空间效率简介 49

Reclaiming Space with SCSI Unmap 49

使用去重和压缩 50

使用 RAID 5 或 RAID 6 删除编码 54

[RAID 5 或 RAID 6 设计注意事项 55](#)

**7 在 vSAN 群集上使用加密 56**

[vSAN 加密的工作原理 56](#)

[vSAN 加密的设计注意事项 57](#)

[设置 KMS 群集 57](#)

[在新的 vSAN 群集上启用加密 62](#)

[生成新的加密密钥 63](#)

[在现有 vSAN 群集上启用 vSAN 加密 63](#)

[vSAN 加密和核心转储 64](#)

**8 升级 vSAN 群集 68**

[升级 vSAN 之前 68](#)

[升级 vCenter Server 。 70](#)

[升级 ESXi 主机 70](#)

[关于 vSAN 磁盘格式 71](#)

[验证 vSAN 群集升级 77](#)

[使用 RVC 升级命令选项 78](#)

[针对 vSphere Update Manager 的 vSAN 内部版本建议 78](#)

# About VMware vSAN

Administering VMware vSAN describes how to configure and manage a vSAN cluster in a VMware vSphere® environment. In addition, Administering VMware vSAN explains how to manage the local physical storage resources that serve as storage capacity devices in a vSAN cluster, and how to define storage policies for virtual machines deployed to vSAN datastores.

## Intended Audience

This information is for experienced virtualization administrators who are familiar with virtualization technology, day-to-day data center operations, and vSAN concepts.

For more information about vSAN and how to create a vSAN cluster, see the vSAN Planning and Deployment Guide.

For more information about monitoring a vSAN cluster and fixing problems, see the vSAN Monitoring and Troubleshooting Guide.

## vSphere Client and vSphere Web Client

Instructions in this guide reflect the vSphere Client (an HTML5-based GUI). You can also use the instructions to perform the tasks by using the vSphere Web Client (a Flex-based GUI).

Tasks for which the workflow differs significantly between the vSphere Client and the vSphere Web Client have duplicate procedures that provide steps according to the respective client interface. The procedures that relate to the vSphere Web Client, contain vSphere Web Client in the title.

---

**注** In vSphere 6.7 Update 1, almost all of the vSphere Web Client functionality is implemented in the vSphere Client. For an up-to-date list of any remaining unsupported functionality, see [Functionality Updates for the vSphere Client](#).

---

## vSAN 简介

VMware vSAN 是作为 ESXi 管理程序的一部分本机运行的分布式软件层。vSAN 可汇总主机群集的本地或直接连接容量设备，并创建在 vSAN 群集的所有主机之间共享的单个存储池。

虽然 vSAN 支持 HA、vMotion 和 DRS 等需要共享存储的 VMware 功能，但它无需外部共享存储，并且简化了存储配置和虚拟机置备活动。

## 配置和管理 vSAN 群集

可以使用 vSphere Client、esxcli 命令和其他工具配置并管理 vSAN 群集。

本章讨论了以下主题：

- 使用 vSphere Client 配置 vSAN 群集
- 使用 vSphere Web Client 配置 vSAN 群集
- 在现有群集上启用 vSAN
- 禁用 vSAN
- 编辑 vSAN 设置
- 查看 vSAN 数据存储

### 使用 vSphere Client 配置 vSAN 群集

可以在基于 HTML5 的 vSphere Client 中使用“配置 vSAN”向导完成 vSAN 群集的基本配置。

The screenshot displays the 'Configure vSAN' wizard in the vSphere Client. The left sidebar shows a progress list with five steps: 1 Configuration type, 2 Services (highlighted), 3 Claim disks, 4 Create fault domains, and 5 Ready to complete. The main panel is titled 'Services' and contains the following content:

- Select the services to enable.** (with a close button 'X')
- A warning: 'These settings require all disks to be reformatted. Moving large amount of stored data might be slow and temporarily decrease the performance of the cluster.'
- Deduplication and Compression Services:** A toggle switch is turned off, with an information icon (i).
- Encryption:** A toggle switch is turned off, with an information icon (i). Below it is a checkbox 'Erase disks before use' (unchecked) with an information icon (i), and a 'KMS cluster:' dropdown menu.
- Options:** A checkbox 'Allow Reduced Redundancy' (unchecked) with an information icon (i).

At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

#### 前提条件

使用“配置 vSAN”向导完成基本配置之前，创建一个群集并向群集中添加主机。

## 步骤

- 1 导航到 **vSphere Client** 中的现有群集。
- 2 单击**配置**选项卡。
- 3 在“vSAN”下，选择**服务**并单击**配置**按钮。
- 4 选择配置类型，然后单击**下一步**。
  - 单站点群集。一个站点中包含所有主机，具有共享的见证功能。
  - 双主机 vSAN 群集。每个站点包含一台主机，见证主机位于另一个站点上。
  - 延伸群集。两个活动的数据站点，其中每个站点具有偶数个主机和存储设备，一个见证主机在第三个站点上。
- 5 在**服务**页面上，配置 vSAN 服务，然后单击**下一步**。
  - a （可选）在群集上启用**去重和压缩**。
  - b （可选）启用**加密**，然后选择 KMS。
  - c 可以选中**允许精简冗余**复选框以在资源有限的 vSAN 群集上启用加密或去重和压缩。例如，三主机群集的**允许的故障数主要级别**设置为 1 的情况。如果允许减少冗余，执行磁盘重新格式化操作过程中数据可能会处于风险中。
- 6 在**声明磁盘**页面中，选择用于群集的磁盘，并单击**下一步**。  
对于提供存储的每个主机，为缓存层选择一个闪存设备并为容量层选择一个或多个设备。
- 7 基于容错模式，按照向导提示完成群集配置。
  - a 如果选择了**配置双主机 vSAN 群集**，请为群集选择一个见证主机，并为见证主机声明磁盘。
  - b 如果选择了**配置延伸群集**，请定义群集的故障域并选择一个见证主机，然后为见证主机声明磁盘。
  - c 如果选择了**配置故障域**，请定义群集的故障域。  
有关故障域的详细信息，请参见[管理 vSAN 群集中的故障域](#)。  
有关延伸群集的详细信息，请参见《vSAN 规划和部署》中的“延伸群集简介”。
- 8 在**即将完成**页面上，检查配置并单击**完成**。

启用 vSAN 将创建 vSAN 数据存储并注册 vSAN 存储提供程序。vSAN 存储提供程序是内置的软件组件，用于将数据存储的存储功能传递到 vCenter Server。

## 后续步骤

验证是否已创建 vSAN 数据存储。请参见[查看 vSAN 数据存储](#)。

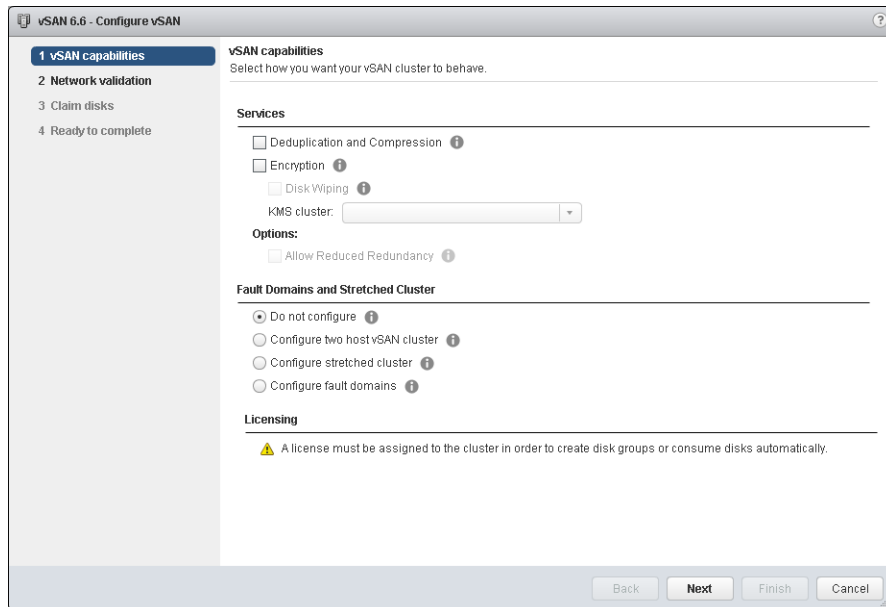
验证是否已注册 vSAN 存储提供程序。请参见[查看 vSAN 存储提供程序](#)。

声明存储设备或创建磁盘组。请参见《管理 VMware vSAN》。

## 使用 vSphere Web Client 配置 vSAN 群集

可以使用“配置 vSAN”向导来完成 vSAN 群集的基本配置。





## 前提条件

使用“配置 vSAN”向导来完成基本配置之前，必须创建群集并将主机添加到群集中。

## 步骤

1 导航到 vSphere Web Client 中的现有群集。

2 单击**配置**选项卡。

3 在"vSAN"下，选择**常规**并单击**配置**按钮。

4 选择 **vSAN 功能**。

a （可选）如果要在群集上启用去重和压缩，请选中**去重和压缩**复选框。

可以选中**允许精简冗余**复选框以在资源有限的 vSAN 群集（如将**允许的故障数主要级别**设置为 1 的三主机群集）上启用去重和压缩。如果允许减少冗余，执行磁盘重新格式化操作过程中数据可能会处于风险中。

b （可选）如果要启用静态数据加密，请选中**加密**复选框，并选择 KMS。

- c 为群集选择容错模式。

选项	描述
不配置	用于单站点 vSAN 群集的默认设置。
双主机 vSAN 群集	为在远程办公室具有两个主机的群集提供容错，此群集在主办办公室具有一个见证主机。将 <b>允许的故障数主要级别</b> 策略设置为 1。
延伸群集	支持两个活动站点，其中每个站点具有偶数个主机和存储设备并在第三个站点上具有一个见证主机。
配置故障域	支持故障域，可用于对可能会一起发生故障的 vSAN 主机进行分组。为每个故障域分配一个或多个主机。

- d 可以选中**允许精简冗余**复选框以在资源有限的 vSAN 群集上启用加密或去重和压缩。例如，三主机群集的**允许的故障数主要级别**设置为 1 的情况。如果允许减少冗余，执行磁盘重新格式化操作过程中数据可能会处于风险中。

- 5 单击**下一步**。

- 6 在**网络验证**页面上，检查 vSAN VMkernel 适配器的设置，并单击**下一步**。

- 7 在**声明磁盘**页面中，选择用于群集的磁盘，并单击**下一步**。

对于提供存储的每个主机，为缓存层选择一个闪存设备并为容量层选择一个或多个设备。

- 8 基于容错模式，按照向导提示完成群集配置。

- a 如果选择了**配置双主机 vSAN 群集**，请为群集选择一个见证主机，并为见证主机声明磁盘。
- b 如果选择了**配置延伸群集**，请定义群集的故障域并选择一个见证主机，然后为见证主机声明磁盘。
- c 如果选择了**配置故障域**，请定义群集的故障域。

有关故障域和延伸群集的详细信息，请参见《管理 VMware vSAN》。

- 9 在**即将完成**页面上，检查配置并单击**完成**。

## 在现有群集上启用 vSAN

可以编辑群集属性以便为现有群集启用 vSAN。

### 前提条件

验证您的环境是否符合所有要求。请参见《管理 VMware vSAN》中的“启用 vSAN 的要求”。

### 步骤

- 1 导航到现有主机群集。

## 2 单击配置选项卡。

选项	描述
<b>vSphere Client</b>	<ul style="list-style-type: none"> <li>a 在“vSAN”下，选择<b>服务</b>。</li> <li>b （可选）在群集上启用去重和压缩。<b>vSAN</b> 将自动升级磁盘格式，这会导致群集中的每个磁盘组执行回滚重新格式化操作。</li> <li>c （可选）在群集上启用加密，然后选择 <b>KMS 服务器</b>。<b>vSAN</b> 将自动升级磁盘格式，这会导致群集中的每个磁盘组执行回滚重新格式化操作。</li> <li>d （可选）选择“允许精简冗余”。如果需要，<b>vSAN</b> 将降低虚拟机的保护级别，同时启用去重和压缩或加密。</li> </ul>
<b>vSphere Web Client</b>	<ul style="list-style-type: none"> <li>a 在“vSAN”下，选择<b>常规</b>。</li> <li>b 在“vSAN 已打开”窗格中，单击<b>编辑</b>按钮。</li> <li>c （可选）如果要在群集上启用去重和压缩，请选中<b>去重和压缩</b>复选框。<b>vSAN</b> 将自动升级磁盘格式，这会导致群集中的每个磁盘组执行回滚重新格式化操作。</li> <li>d （可选）如果要在群集上启用加密，请选中<b>加密</b>复选框，然后选择 <b>KMS 服务器</b>。<b>vSAN</b> 将自动升级磁盘格式，这会导致群集中的每个磁盘组执行回滚重新格式化操作。</li> </ul>

## 3 单击确定或应用以确认您的选择。

### 后续步骤

声明存储设备或创建磁盘组。请参见《管理 VMware vSAN》。

## 禁用 vSAN

可以关闭主机群集的 vSAN。

禁用 vSAN 群集时，位于共享 vSAN 数据存储上的所有虚拟机都将变为无法访问。如果要在 vSAN 处于禁用状态时使用虚拟机，请确保在禁用 vSAN 群集之前，将虚拟机从 vSAN 数据存储迁移到另一数据存储。

### 前提条件

确认主机处于维护模式。

### 步骤

#### 1 导航到 vSAN 群集。

#### 2 单击配置选项卡。

选项	描述
<b>vSphere Client</b>	<ul style="list-style-type: none"> <li>a 在“vSAN”下，选择<b>服务</b>。</li> <li>b 单击<b>关闭 vSAN</b>。</li> <li>c 在“关闭 vSAN”对话框中，确认您的选择。</li> </ul>
<b>vSphere Web Client</b>	<ul style="list-style-type: none"> <li>a 在“vSAN”下，选择<b>常规</b>。</li> <li>b 在“vSAN 已打开”窗格中，单击<b>编辑</b>按钮。</li> <li>c 取消选中 <b>vSAN 打开</b>复选框。</li> </ul>

## 编辑 vSAN 设置

可以编辑 vSAN 群集的设置以更改磁盘声明方法并启用去重和压缩功能。

如果要启用去重和压缩或启用加密，请编辑现有 vSAN 群集的设置。如果启用去重和压缩，或启用加密，群集的磁盘格式会自动升级到最新版本。

### 步骤

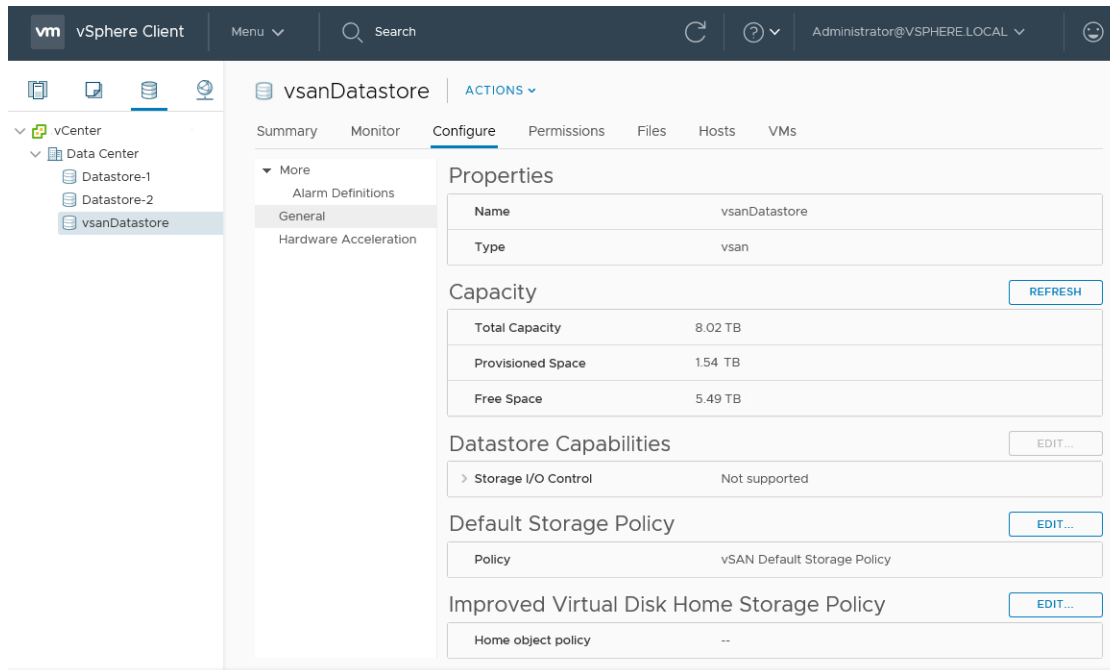
- 1 导航到 vSAN 主机群集。
- 2 单击配置选项卡。

选项	描述
<b>vSphere Client</b>	<ol style="list-style-type: none"> <li>a 在“vSAN”下，选择<b>服务</b>。</li> <li>b 单击要配置的服务对应的<b>编辑</b>按钮。 <ul style="list-style-type: none"> <li>■ 启用或禁用去重和压缩。</li> <li>■ 配置 vSAN 加密。</li> <li>■ 配置 vSAN 性能服务。</li> <li>■ 配置 iSCSI 目标服务。</li> <li>■ 配置高级选项，如对象修复时间、站点读取位置、精简交换设备和大群集支持。</li> </ul> </li> <li>c 修改设置以满足您的要求。</li> </ol>
<b>vSphere Web Client</b>	<ol style="list-style-type: none"> <li>a 在“vSAN”下，选择<b>常规</b>。</li> <li>b 在“vSAN 已打开”窗格中，单击<b>编辑</b>按钮。</li> <li>c （可选）如果要在群集上启用去重和压缩，请选中<b>去重和压缩</b>复选框。vSAN 将自动升级磁盘格式，这会导致群集中的每个磁盘组执行回滚重新格式化操作。</li> <li>d （可选）如果要在群集上启用加密，请选中<b>加密</b>复选框，然后选择 KMS 服务器。vSAN 将自动升级磁盘格式，这会导致群集中的每个磁盘组执行回滚重新格式化操作。</li> </ol>

- 3 单击**确定**或**应用**以确认您的选择。

## 查看 vSAN 数据存储

启用 vSAN 后，将创建一个数据存储。您可以查看 vSAN 数据存储的容量。



### 前提条件

激活 vSAN 并配置磁盘组。

### 步骤

- 1 导航到存储。
- 2 选择 vSAN 数据存储。
- 3 单击配置选项卡。
- 4 查看 vSAN 数据存储容量。

vSAN 数据存储的大小取决于每台 ESXi 主机的容量设备数量以及群集中 ESXi 主机的数量。例如，如果某台主机具有七个 2 TB 的容量设备，群集中包含八台主机，则存储容量约为  $7 \times 2 \text{ TB} \times 8 = 112 \text{ TB}$ 。在使用全闪存配置时，闪存设备将提供容量。对于混合配置，磁盘将计入容量。

部分容量将分配给元数据。

- 对于磁盘格式版本 1.0，每个容量设备会增加约 1 GB。
- 磁盘格式版本 2.0 会增加容量开销，通常每个设备不超过 1-2% 的容量。
- 磁盘格式 3.0 及更高版本会增加容量开销，通常每个设备不超过 1-2% 的容量。如果启用去重和压缩功能以及软件校验和，则每个设备需要约 6.2% 容量的额外开销。

### 后续步骤

为使用 vSAN 数据存储的存储功能的虚拟机创建存储策略。有关信息，请参见 vSphere 存储文档。

## 使用 vSAN 策略

使用 vSAN 时，您可以在策略中定义虚拟机存储要求，例如性能和可用性。vSAN 确保部署到 vSAN 数据存储的每个虚拟机都分配有至少一个存储策略。

分配存储策略后，创建虚拟机时，会将存储策略要求推送到 vSAN 层。虚拟设备分布在 vSAN 数据存储之间，以满足性能和可用性要求。

vSAN 使用存储提供程序向 vCenter Server 提供底层存储的相关信息。该信息可帮助您做出与虚拟机放置有关的正确决定，并帮助监控存储环境。

本章讨论了以下主题：

- [关于 vSAN 策略](#)
- [主机固定](#)
- [查看 vSAN 存储提供程序](#)
- [关于 vSAN 默认存储策略](#)
- [将默认存储策略分配到 vSAN 数据存储](#)
- [使用 vSphere Client 定义针对 vSAN 的存储策略](#)
- [使用 vSphere Web Client 定义针对 vSAN 的存储策略](#)

### 关于 vSAN 策略

vSAN 存储策略定义对虚拟机的存储要求。这些策略确定如何置备和分配数据存储内的虚拟机存储对象，以保证达到要求的服务级别。

在主机群集上启用 vSAN 后，将创建一个 vSAN 数据存储，并且会为该数据存储分配默认存储策略。

当了解虚拟机的存储要求后，可以创建引用数据存储所播发的功能的存储策略。您可以创建多个策略以捕获不同类型或类别的要求。

将为部署到 vSAN 数据存储的每个虚拟机至少分配一个虚拟机存储策略。您可以在创建或编辑虚拟机时分配存储策略。

---

**注** 如果您未向虚拟机分配存储策略，则 vSAN 将分配默认策略。在默认策略中，允许的故障数主要级别设置为 1，每个对象有一个磁盘带，另外还有一个精简置备的虚拟磁盘。

---

虚拟机交换对象和虚拟机快照内存对象不遵守分配给虚拟机的存储策略。配置这些对象时会将**允许的故障数主要级别**设置为 1。这些对象的可用性可能与所分配策略中具有不同**允许的故障数主要级别**的其他对象有所差异。

**表 3-1. 存储策略规则**

容量	描述
允许的故障数主要级别 (PFTT)	<p>定义虚拟机对象允许的主机和设备故障的数量。如果允许 <math>n</math> 个故障，写入的每条数据存储在 <math>n+1</math> 个位置，如果使用 RAID 5 或 RAID 6，还包括奇偶校验副本。</p> <p>置备虚拟机时，如果未选择存储策略，则 vSAN 将指定此策略作为默认虚拟机存储策略。</p> <p>如果已配置故障域，则需要 <math>2n+1</math> 个故障域，且这些故障域中具有可提供容量的主机。不属于故障域的主机会被视为位于其自己的单主机故障域中。</p> <p>默认值为 1。最大值为 3。</p> <p><b>注</b> 如果不希望 vSAN 保护虚拟机对象的单一镜像副本，则可指定 <b>PFTT = 0</b>。但是，主机在进入维护模式时，可能会出现异常延迟。发生延迟的原因是 vSAN 必须将该对象从主机中撤出才能成功完成维护操作。设置 <b>PFTT = 0</b> 意味着数据不受保护，当 vSAN 群集出现设备故障时可能会丢失数据。</p> <p><b>注</b> 创建存储策略时，如果没有为 <b>PFTT</b> 指定一个值，vSAN 将为虚拟机对象创建一个镜像副本。只允许出现一个故障。但是，如果多个组件出现故障，数据可能会存在风险。</p> <p>在延伸群集中，此规则定义虚拟机对象可允许的站点故障数量。您可以结合使用 <b>PFTT</b> 和 <b>SFTT</b>，以向数据站点内的对象提供本地故障保护。</p> <p>延伸群集的最大值为 1。</p>
允许的故障数辅助级别 (SFTT)	<p>在延伸群集中，此规则定义在达到 <b>PFTT</b> 定义的站点故障数量后对象可允许的额外主机故障数量。如果 <b>PFTT = 1</b> 且 <b>SFTT = 2</b>，且有一个站点不可用，则群集可允许两个额外主机故障。</p> <p>默认值为 1。最大值为 3。</p>
数据局部性	<p>在延伸群集中，仅当<b>允许的故障数主要级别</b>设置为 0 时，该规则才可用。可以将<b>数据局部性</b>规则设置为<b>无</b>、<b>首选</b>或<b>辅助</b>。使用该规则可以将虚拟机对象限制到延伸群集中的某个选定站点或主机。</p> <p>默认值为“无”。</p>
容错方法	<p>指定数据复制方法针对性能还是容量进行优化。如果选择 <b>RAID-1 (镜像) - 性能</b>，vSAN 将使用较多磁盘空间来放置对象的组件，但提供的对象访问性能较高。如果选择 <b>RAID-5/6 (纠删码) - 容量</b>，vSAN 将使用较少磁盘空间，但性能会下降。可以通过以下方式使用 RAID 5：将 <b>RAID-5/6 (擦除编码) - 容量</b> 属性应用于具有四个或更多故障域的群集，并将<b>允许的故障数主要级别</b>设置为 1。可以通过以下方式使用 RAID 6：将 <b>RAID-5/6 (擦除编码) - 容量</b> 属性应用于具有六个或更多故障域的群集，并将<b>允许的故障数主要级别</b>设置为 2。</p> <p>在配置了<b>允许的故障数辅助级别</b>的延伸群集中，该规则仅适用于<b>允许的故障数辅助级别</b>。</p> <p>有关 RAID 5 或 RAID 6 的详细信息，请参见<a href="#">使用 RAID 5 或 RAID 6 删除编码</a>。</p>
每个对象的磁盘带数	<p>虚拟机对象的每个副本在其上进行条带化的容量设备的最低数量。值如果大于 1，则可能产生较好的性能，但也会导致使用较多的系统资源。</p> <p>默认值为 1。最大值为 12。</p> <p>请勿更改默认的条带化值。</p> <p>在混合环境中，磁盘带分散在磁盘中。在全闪存配置中，会在构成容量层的闪存设备中进行条带化。确保您的 vSAN 环境提供了足够的容量设备以容纳请求。</p>

表 3-1. 存储策略规则（续）

容量	描述
闪存读取缓存预留	<p>作为虚拟机对象的读取缓存预留的闪存容量。指定为该虚拟机磁盘 (vmdk) 对象的逻辑大小的百分比。预留的闪存容量无法供其他对象使用。未预留的闪存存在所有对象之间公平共享。仅使用该选项解决特定的性能问题。</p> <p>无需设置预留即可获取缓存。设置读取缓存预留可能会导致在移动虚拟机对象时出现问题，因为该对象始终包含缓存预留设置。</p> <p>只有混合配置才支持“闪存读取缓存预留”存储策略属性。为全闪存群集定义虚拟机存储策略时，不得使用该属性。</p> <p>默认值为 0%。最大值为 100%。</p> <p><b>注</b> 默认情况下，vSAN 将按需为存储对象动态分配读取缓存。此功能是最灵活、最优化的资源利用方式。因此，通常无需更改此参数的默认值 0。</p> <p>如果在解决性能问题时要增加该值，请小心谨慎。在多个虚拟机上过度置备缓存预留可能会导致闪存设备空间浪费在过度预留的缓存上。这些缓存预留无法用来处理在给定时间需要所需空间的工作负载。这种空间浪费和不可用问题可能会导致性能下降。</p>
强制置备	<p>如果该选项设置为<b>是</b>，则即使数据存储不满足存储策略中指定的<b>允许的故障数主要级别、每个对象的磁盘带数和闪存读取缓存预留</b>策略，也会置备该对象。该参数可在引导时以及在出现故障无法再进行标准置备时使用。</p> <p>默认值<b>否</b>对于大多数生产环境都是可接受的。当不满足策略要求时，vSAN 无法置备虚拟机，但是可以成功创建用户定义的存储策略。</p>
对象空间预留	<p>部署虚拟机时必须预留或厚置备的虚拟机磁盘 (vmdk) 对象的逻辑大小百分比。</p> <p>默认值为 0%。最大值为 100%。</p>
禁用对象校验和	<p>如果该选项设置为<b>否</b>，该对象将计算校验和信息来确保其数据的完整性。如果该选项设置为<b>是</b>，该对象不计算校验和信息。</p> <p>vSAN 使用端到端校验和来确保数据的完整性，即确认文件的每个副本都与源文件完全相同。系统会在读取/写入操作期间检查数据的有效性，如果检测到错误，vSAN 将修复数据或报告错误。</p> <p>如果检测到校验和不匹配，vSAN 将使用正确数据覆盖错误数据来自动修复数据。校验和计算和错误更正作为后台操作执行。</p> <p>群集中所有对象的默认设置为<b>否</b>，表示启用校验和。</p>
对象的 IOPS 限制	<p>定义对象（例如 VMDK）的 IOPS 限制。IOPS 使用加权大小计算，表示为 I/O 操作数。如果系统使用的默认基本大小为 32 KB，则 64-KB I/O 表示两个 I/O 操作。</p> <p>计算 IOPS 时，读取和写入同等对待，但不考虑缓存命中率和顺序性。如果磁盘的 IOPS 超过此限制，将限制 I/O 操作。如果<b>对象的 IOPS 限制</b>设置为 0，将不会强制执行 IOPS 限制。</p> <p>vSAN 允许对象在操作的第一秒或一段时间不活动后 IOPS 达到限制速率的两倍。</p>

使用虚拟机存储策略时，必须了解存储功能如何影响 vSAN 群集中存储容量的消耗。有关存储策略设计和大小调整注意事项的详细信息，请参见《管理 VMware vSAN》中的“设计和调整 vSAN 群集的大小”。

## 主机固定

借助 vSAN 主机固定存储策略，您可以在虚拟机的本地主机上存储数据的单个副本。



vSAN 主机固定存储策略可调整 vSAN 的效率和弹性，以适应下一代、无共享应用程序。使用该策略时，vSAN 会保存数据的单个副本并将其存储在运行虚拟机的本地主机上。此策略作为 Big Data（Hadoop、Spark）、NoSQL 和在应用程序层维护数据冗余的其他此类应用程序的部署选项提供。

vSAN 主机固定具有特定的要求和准则，需要 VMware 验证以确保正确部署。vSAN 主机固定策略必须应用于群集中的所有虚拟机，且不能与同一群集上的其他策略相结合。vSAN 加密和去重不能与 vSAN 主机固定策略配合使用。必须禁用 vSphere DRS 和 HA 选项以防止自动移动虚拟机。

对此功能感兴趣的管理员必须联系 VMware，并提交部署意向请求。VMware 在批准支持和生产使用之前将评估请求以确保您的部署满足要求。VMware 不应支持未明确批准的任何部署。有关详细信息，请联系 VMware 代表。

## 查看 vSAN 存储提供程序

启用 vSAN 会自动为 vSAN 群集中的每个主机配置并注册一个存储提供程序。

vSAN 存储提供程序是内置的软件组件，用于将数据存储的功能通知给 vCenter Server。存储功能通常由“键-值”对表示，其中键指的是数据存储提供的某一特定属性。值指的是数据存储可为已置备对象（例如，虚拟机主页命名空间对象或虚拟磁盘）提供的某一数字或范围。您还可以使用标记创建用户定义的存储功能，并在为虚拟机定义存储策略时引用这些标记。有关如何应用标记以及将其与数据存储一起使用的信息，请参见 vSphere 存储文档。

vSAN 存储提供程序会向 vCenter Server 报告一组底层存储功能。此外，它们还将与 vSAN 层进行通信，报告虚拟机的存储要求。有关存储提供程序的详细信息，请参见《vSphere 存储》文档。

vSAN 使用以下 URL 为 vSAN 群集中的每台主机注册单独的存储提供程序：

`http://host_ip:8080/version.xml`

其中，*host\_ip* 是主机的实际 IP。

请确认存储提供程序已注册。

### 步骤

- 1 导航到 vCenter Server。
- 2 依次单击**配置**选项卡和**存储提供程序**。

此时 vSAN 的存储提供程序将显示在列表中。每个主机均有存储提供程序，但只有一个处于活动状态。属于其他主机的存储提供程序处于等待状态。如果存储提供程序当前处于活动状态的主机发生故障，另一主机的存储提供程序将被激活。

---

**注** 无法手动取消注册 vSAN 使用的存储提供程序。要移除或取消注册 vSAN 存储提供程序，请从 vSAN 群集移除相应的主机，然后再重新添加主机。确保至少有一个存储提供程序处于活动状态。

---

## 关于 vSAN 默认存储策略

vSAN 要求已部署到 vSAN 数据存储的虚拟机至少分配有一个存储策略。置备虚拟机时，如果没有向虚拟机明确分配存储策略，将向虚拟机分配 vSAN 默认存储策略。

默认策略包含 vSAN 规则集和一组基本存储功能，通常用于放置已部署到 vSAN 数据存储上的虚拟机。

表 3-2. vSAN 默认存储策略规范

规范	设置
允许的故障数主要级别	1
每个对象的磁盘带数	1
闪存读取缓存预留，或用于读取缓存的闪存容量	0
对象空间预留	0
	<b>注</b> 默认情况下，将对象空间预留设置为零意味着会精简置备虚拟磁盘。
强制置备	否

您可以查看默认虚拟机存储策略的配置设置，方法是导航到**虚拟机存储策略 > vSAN 默认存储策略 > 管理 > 规则集 1: vSAN**。

为获得最佳效果，请考虑创建并使用您自己的虚拟机存储策略，即使该策略的要求与默认存储策略中定义的要求相同。有关创建用户定义的虚拟机存储策略的信息，请参见[使用 vSphere Client 定义针对 vSAN 的存储策略](#)。

将用户定义的存储策略分配给数据存储时，vSAN 会在指定数据存储上应用由用户定义的策略设置。任何时候，您都只能将一个虚拟机存储策略作为默认策略分配给 vSAN 数据存储。

## 特性

以下特性将适用于 vSAN 默认存储策略。

- 如果不分配任何其他 vSAN 策略，当您置备虚拟机时，会将 vSAN 默认存储策略分配给所有虚拟机对象。在“选择存储”页面上，**虚拟机存储策略**文本框将设置为**数据存储默认值**。有关使用存储策略的详细信息，请参见 vSphere 存储文档。

**注** 虚拟机交换对象和虚拟机内存对象收到**强制置备**设置为**是**的 vSAN 默认存储策略。

- vSAN 默认策略仅适用于 vSAN 数据存储。无法将默认存储策略应用于非 vSAN 数据存储，例如 NFS 或 VMFS 数据存储。
- 由于默认虚拟机存储策略与 vCenter Server 中的任何 vSAN 数据存储都兼容，因此您可以将使用默认策略置备的虚拟机对象移动到 vCenter Server 中的任何 vSAN 数据存储中。
- 您可以克隆默认策略，并将其用作模板以创建用户定义的存储策略。
- 如果您具有 **StorageProfile.View** 特权，则可以编辑默认策略。必须至少已启用一个 vSAN 群集且该群集至少包含一个主机。通常情况下，您不需要编辑默认存储策略的设置。
- 无法编辑默认策略的名称和描述或 vSAN 存储提供程序规范。所有其他参数（包括策略规则）均可编辑。
- 无法删除默认策略。
- 当您在虚拟机置备期间分配的策略不包括特定于 vSAN 的规则时，将分配默认存储策略。

## 将默认存储策略分配到 vSAN 数据存储

可以将用户定义的存储策略作为默认策略分配到数据存储，以便重用与您的要求相符的存储策略。

### 前提条件

确认要作为默认策略分配到 vSAN 数据存储的虚拟机存储策略满足 vSAN 群集中虚拟机的要求。

### 步骤

- 1 导航到 vSAN 数据存储。
- 2 单击**配置**。
- 3 在**常规**下，单击默认存储策略的**编辑**按钮，然后选择要作为默认策略分配到 vSAN 数据存储的存储策略。  
可以从与 vSAN 数据存储兼容的存储策略列表中选择策略，例如 vSAN 默认存储策略和定义了 vSAN 规则集的用户定义的存储策略。
- 4 选择策略，然后单击**确定**。

置备新的虚拟机时，如果未明确指定数据存储的存储策略，该存储策略将作为默认策略应用。

### 后续步骤

您可以为虚拟机定义新的存储策略。请参见[使用 vSphere Client 定义针对 vSAN 的存储策略](#)。

## 使用 vSphere Client 定义针对 vSAN 的存储策略

您可以创建一个存储策略，用来定义虚拟机及其虚拟磁盘的存储要求。在此策略中，将引用 vSAN 数据存储

The screenshot shows the 'Create VM Storage Policy' dialog box with the 'vSAN' tab selected. The left sidebar lists five steps: 1 Name and description, 2 Policy structure, 3 vSAN (selected), 4 Storage compatibility, and 5 Review and finish. The main area is titled 'vSAN' and contains three tabs: Availability, Advanced Policy Rules (selected), and Tags. Under 'Advanced Policy Rules', the following settings are visible:

- Number of disk stripes per object: 1
- IOPS limit for object: 0
- Object space reservation: Thin provisioning (Initially reserved storage space for 100 GB VM disk would be 0 B)
- Flash read cache reservation (%): 0 (Reserved cache space for 100GB VM disk would be 0 B)
- Disable object checksum: Off
- Force provisioning: Off

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT.


支持的存储功能。

### 前提条件

- 确认 vSAN 存储提供程序可用。请参见[查看 vSAN 存储提供程序](#)。

- 所需特权：**配置文件驱动的存储.配置文件驱动的存储视图和配置文件驱动的存储.配置文件驱动的存储更新**

### 步骤

- 1 导航到**策略和配置文件**，然后单击**虚拟机存储策略**。
- 2 单击**创建新虚拟机存储策略**图标 ( )。
- 3 在“名称和描述”页面中，选择 **vCenter Server**。
- 4 键入存储策略的名称和描述，然后单击**下一步**。
- 5 在“策略结构”页面中，选择“**vSAN**”存储的“启用”规则，然后单击**下一步**。
- 6 在 **vSAN** 页面中，定义策略规则集。
  - a 在“可用性”选项卡上，定义**站点灾难容错**和**允许的故障数**。  
 可用性选项定义了“允许的故障数主要级别”和“允许的故障数辅助级别”、“数据局部性”以及“容错方法”的规则。
    - **站点灾难容错**定义了用于虚拟机对象的站点容错类型。
    - **允许的故障数**定义了虚拟机对象允许的主机和设备故障数以及数据复制方法。
 例如，如果您选择**双站点镜像**和**2 个故障 - RAID 6 (纠删码)**，vSAN 可配置以下策略规则：
    - 允许的故障数主要级别：1
    - 允许的故障数辅助级别：2
    - 数据局部性：无
    - 容错方法：**RAID-5/6 (纠删码) - 容量**
  - b 在“高级策略规则”选项卡上，定义高级策略规则，例如每个对象的磁盘带数和 **IOPS** 限制。
  - c 在“标记”选项卡上，单击**添加标记规则**，并定义您的标记规则的选项。  
 确保您提供的值位于 **vSAN** 数据存储的存储功能通告的值范围内。
- 7 单击**下一步**。
- 8 在“存储兼容性”页面上，检查与此策略匹配的数据存储列表，然后单击**下一步**。  
 要符合条件，数据存储不需要满足该策略内的所有规则集的要求。该数据存储必须至少满足一个规则集以及此规则集中的所有规则的要求。确认 **vSAN** 数据存储满足存储策略中设置的要求并显示在兼容数据存储的列表中。
- 9 在“检查并完成”页面上，检查策略设置，然后单击**完成**。

新策略将添加到列表中。

### 后续步骤

将此策略分配给虚拟机及其虚拟磁盘。**vSAN** 将根据策略中指定的要求放置虚拟机对象。有关将存储策略应用到虚拟机对象的信息，请参见 **vSphere** 存储文档。

## 使用 vSphere Web Client 定义针对 vSAN 的存储策略

您可以创建一个存储策略，用来定义虚拟机及其虚拟磁盘的存储要求。在此策略中，将引用 vSAN 数据存储

支持的存储功能。

### 前提条件

- 确认 vSAN 存储提供程序可用。请参见[查看 vSAN 存储提供程序](#)。
- 确保已启用虚拟机存储策略。有关存储策略的信息，请参见 [vSphere 存储文档](#)。
- 所需特权：[配置文件驱动的存储](#)、[配置文件驱动的存储视图](#)和[配置文件驱动的存储更新](#)

### 步骤

- 1 从 vSphere Web Client 主页中，单击[策略和配置文件](#)，然后单击[虚拟机存储策略](#)。
- 2 单击[创建新虚拟机存储策略](#)图标 (📁)。
- 3 在“名称和描述”页面中，选择 vCenter Server。
- 4 键入存储策略的名称和描述，然后单击[下一步](#)。
- 5 在“策略结构”页面中，单击[下一步](#)。
- 6 在主机提供的[数据服务常用规则](#)页面上，单击[下一步](#)。
- 7 在“规则集 1”页面中，定义第一个规则集。
  - a 选中[使用存储策略中的规则集](#)复选框。
  - b 从[存储类型](#)下拉菜单中选择 **VSAN**。

在您为 vSAN 数据存储添加规则后，此页面将展开。

- c 从**添加规则**下拉菜单中选择规则。

确保您提供的值位于 vSAN 数据存储的存储功能通告的值范围内。

可以从“存储消耗”模型查看可用的虚拟磁盘大小以及相应的缓存和容量要求，包括应用存储策略时虚拟机可能会占用的预留存储空间。

- d （可选）添加基于标记的功能。

- 8 （可选）单击**添加其他规则集**按钮以添加另一个规则集。

- 9 单击**下一步**。

- 10 在“存储兼容性”页面上，检查与此策略匹配的数据存储列表，然后单击**下一步**。

要符合条件，数据存储不需要满足该策略内的所有规则集的要求。该数据存储必须至少满足一个规则集以及此规则集中的所有规则的要求。确认 vSAN 数据存储满足存储策略中设置的要求并显示在兼容数据存储的列表中。

- 11 在“即将完成”页面上，检查策略设置，然后单击**完成**。

新策略将添加到列表中。

#### 后续步骤

将此策略分配给虚拟机及其虚拟磁盘。vSAN 将根据策略中指定的要求放置虚拟机对象。有关将存储策略应用到虚拟机对象的信息，请参见 vSphere 存储文档。

## 扩展和管理 vSAN 群集

设置 vSAN 群集后，可以添加主机和容量设备，移除主机和设备，以及管理故障情形。

本章讨论了以下主题：

- 扩展 vSAN 群集
- 使用维护模式
- 管理 vSAN 群集中的故障域
- 使用 vSANiSCSI 目标服务
- 将混合 vSAN 群集迁移到全闪存群集
- 关闭 vSAN 群集的电源

### 扩展 vSAN 群集

可通过添加主机或向现有主机添加设备来扩展现有 vSAN 群集，而不会中断任何正在进行的操作。

使用以下方法之一来扩展 vSAN 群集。

- 将新的 ESXi 主机添加到配置为使用支持的缓存和容量设备的群集。请参见[将主机添加到 vSAN 群集](#)。添加设备或添加带有容量的主机时，vSAN 不会自动向新添加的设备分配数据。要允许 vSAN 向最近添加的设备分配数据，必须通过使用 Ruby vSphere 控制台 (RVC) 手动重新平衡群集。请参见《vSAN 监控和故障排除》中的“手动重新平衡”。
- 使用主机配置文件将现有 ESXi 主机移至 vSAN 群集。请参见[使用主机配置文件配置主机](#)。新的群集成员将添加存储并计算容量。您必须在新添加的主机上手动创建本地容量设备的磁盘组子集。请参见在[vSAN 主机上创建磁盘组](#)。

确认您计划使用的硬件组件、驱动程序、固件和存储 I/O 控制器均经过认证且列在《VMware 兼容性指南》中，网址为 <http://www.vmware.com/resources/compatibility/search.php>。添加容量设备时，请确保设备未格式化且未分区，以便 vSAN 可以识别和声明设备。

- 将新的容量设备添加到作为群集成员的 ESXi 主机。您必须手动将设备添加到主机上的磁盘组。请参见[将设备添加到磁盘组](#)。



## 扩展 vSAN 群集容量和性能

如果 vSAN 群集的存储容量即将耗尽或您注意到群集性能降低，您可以扩展群集的容量和性能。

- 通过向现有磁盘组添加存储设备或添加磁盘组，扩展群集的存储容量。新磁盘组需要闪存设备用于提供缓存。有关将设备添加到磁盘组的信息，请参见[将设备添加到磁盘组](#)。添加容量设备而不增加缓存可能会使缓存与容量比率降低到不受支持的程度。请参见《管理 VMware vSAN》中的“vSAN 中闪存缓存设备的设计注意事项”。
- 通过将至少一个缓存设备（闪存）和一个容量设备（闪存或磁盘）添加到现有存储 I/O 控制器或新主机，提高群集性能。或者，当 vSAN 在 vSAN 群集中完成主动重新平衡后，也可以通过添加一个或多个带有磁盘组的主机以实现相同的性能。

虽然仅计算主机可以存在于 vSAN 群集中并使用群集中其他主机的容量，但添加统一配置的主机可确保高效运行。为获得最佳效果，请添加具有缓存设备和容量设备的主机以扩展群集容量。虽然建议在磁盘组中使用相同或类似的设备，但 vSAN HCL 上列出的任何设备都受支持。尽可能在主机和磁盘组之间均匀分配容量。有关将设备添加到磁盘组的信息，请参见[将设备添加到磁盘组](#)。

扩展群集容量后，请执行手动重新平衡，以在群集中平均分配资源。有关详细信息，请参见《vSAN 监控和故障排除》中的“手动重新平衡”。

## 使用快速入门功能将主机添加到 vSAN 群集

如果通过快速入门功能配置了 vSAN 群集，则可以使用快速入门工作流将主机和存储设备添加到群集。

向 vSAN 群集添加新主机时，可以使用“群集配置”向导完成主机配置。有关快速入门功能的详细信息，请参见《vSAN 规划和部署》中的“使用快速入门功能配置并扩展 vSAN 群集”。

---

**注** 如果群集中的主机运行 vCenter Server，则主机无需置于维护模式，因为可以使用快速入门工作流将它添加到群集。包含 vCenter Server 虚拟机的宿主必须运行 ESXi 6.5 EP2 或更高版本。同一宿主也可以运行 Platform Services Controller。宿主上的所有其他虚拟机必须关闭电源。

---

### 前提条件

快速入门工作流必须可用于 vSAN 群集。

### 步骤

- 1 在 vSphere Client 中，导航到群集。
- 2 单击“配置”选项卡，然后选择**配置 > 快速入门**。
- 3 在“添加主机”卡上，单击**添加**以打开“添加主机”向导。
  - a 在“添加主机”页面上，输入新主机的信息，或单击“现有主机”并选择清单中列出的主机。
  - b 在“主机摘要”页面上，验证主机设置。
  - c 在“即将完成”页面上，单击**完成**。



- 4 在“群集配置”卡上，单击**配置**以打开“群集配置”向导。
  - a （可选）在“vMotion 流量”页面上，输入 vMotion 流量的 IP 地址信息。
  - b 在“存储流量”页面上，输入存储流量的 IP 地址信息。
  - c （可选）在“声明磁盘”页面上，选择每个新主机上的磁盘。
  - d （可选）在“创建故障域”页面上，将新主机移至其相应的故障域。  
有关故障域的详细信息，请参见[管理 vSAN 群集中的故障域](#)。
  - e 在“即将完成”页面上，验证群集设置，然后单击**完成**。

## 将主机添加到 vSAN 群集

您可以将 ESXi 主机添加到正在运行的 vSAN 群集，而不会中断任何正在进行的操作。主机的资源即与群集关联。

### 前提条件

- 确认驱动程序、固件、存储 I/O 控制器等资源是否列在《VMware 兼容性指南》中，网址为 <http://www.vmware.com/resources/compatibility/search.php>。
- VMware 建议在 vSAN 群集中创建统一配置的主机，以保证组件和对象在群集中的各个设备间平均分布。但是，有可能存在群集变得不平衡的情况，尤其是维护期间或因虚拟机部署过多而导致 vSAN 数据存储容量过度分配时。

### 步骤

- 1 导航到 vSAN 群集。
- 2 右键单击该群集并选择**添加主机**。
- 3 输入主机名或 IP 地址，然后单击**下一步**。
- 4 输入与主机关联的用户名和密码，然后单击**下一步**。
- 5 查看摘要信息并单击**下一步**。
- 6 分配许可证密钥，然后单击**下一步**。
- 7 （可选）启用锁定模式，以防止远程用户直接登录到主机。  
可以稍后通过编辑主机设置中的“安全配置文件”来配置该选项。
- 8 查看设置，然后单击**完成**。  
此时主机即会添加到群集。

### 后续步骤

确认 vSAN 磁盘平衡运行状况检查为绿色。如果磁盘平衡运行状况检查发出警告，请在非高峰时间执行手动重新平衡操作。有关详细信息，请参见《vSAN 监控和故障排除》中的“手动重新平衡”。

## 使用主机配置文件配置主机

如果 vSAN 群集中有多个主机，您可以使用现有 vSAN 主机的配置文件来配置 vSAN 群集中的其余主机。

主机配置文件包含有关主机的存储配置、网络配置和其他特性的信息。如果您计划创建含有多个主机（例如 8、16、32 或 64 个主机）的群集，可使用主机配置文件功能。主机配置文件允许您一次向 vSAN 群集添加多个主机。

### 前提条件

- 确认主机处于维护模式。
- 确认硬件组件、驱动程序、固件和存储 I/O 控制器列在《VMware 兼容性指南》中，网址为 <http://www.vmware.com/resources/compatibility/search.php>。

### 步骤

#### 1 创建主机配置文件。

- a 导航到“主机配置文件”视图。
- b 单击**从主机中提取配置文件**图标 (+)。
- c 选择要充当引用主机的主机，然后单击**下一步**。  
所选主机必须是活动主机。
- d 键入新配置文件的名称和描述，然后单击**下一步**。
- e 查看新主机配置文件的摘要信息，然后单击**完成**。

新配置文件将显示在“主机配置文件”列表中。

#### 2 将主机附加到目标主机配置文件。

- a 从“主机配置文件”视图的“配置文件”列表中，选择要应用于 vSAN 主机的主机配置文件。
- b 单击**在主机和群集中附加/分离主机配置文件**图标 (🔗)。
- c 从展开的列表中选择主机，然后单击**附加**将主机添加到配置文件。  
此时主机将添加到“已附加实体”列表。
- d 单击**下一步**。
- e 单击**完成**以完成将主机与配置文件分离的过程。

#### 3 从主机配置文件中分离引用的 vSAN 主机。

当主机配置文件附加到群集时，该群集中的一个或多个主机也会附加到主机配置文件。但是，当主机配置文件与群集分离时，群集中的一个或多个主机与主机配置文件中主机之间的关联仍保持不变。

- a 从“主机配置文件”视图中的“配置文件”列表中，选择要从主机或群集中分离的主机配置文件。
- b 单击**在主机和群集中附加/分离主机配置文件**图标 (🔗)。
- c 从展开的列表中选择主机或群集，然后单击**分离**。

- d 单击**分离全部**从配置文件中分离所有列出的主机和群集。
  - e 单击**下一步**。
  - f 单击**完成**以完成将主机与主机配置文件分离的过程。
- 4 确认 **vSAN** 主机与其附加的主机配置文件的合规性，并确定主机上是否存在与主机配置文件中指定的参数不同的配置参数。
- a 导航到一个主机配置文件。
 

**对象**选项卡将列出所有主机配置文件、附加到该主机配置文件的主机数量，以及上次合规性检查的汇总结果。
  - b 单击**检查主机配置文件合规性**图标 (🔍)。
 

要查看有关合规性检查失败的主机与主机配置文件之间不同参数的特定详细信息，请单击**监控**选项卡并选择“合规性视图”。展开对象层次结构并选择不合规主机。不同的参数将显示在“合规性”窗口中层次结构的下面。

如果合规性检查失败，请使用“修复”操作将主机配置文件设置应用到主机。此操作会将所有主机配置文件受管参数更改为附加到主机的主机配置文件中包含的值。
  - c 要查看有关合规性检查失败的主机与主机配置文件之间不同参数的特定详细信息，请单击**监控**选项卡并选择“合规性视图”。
  - d 展开对象层次结构并选择出现故障的主机。
 

不同的参数将显示在“合规性”窗口中层次结构的下面。
- 5 修复主机以修复合规性错误。
- a 选择**监控**选项卡，然后单击**合规性**。
  - b 右键单击要修复的一个或多个主机，然后选择**所有 vCenter 操作 > 主机配置文件 > 修复**。
 

可以通过自定义主机为主机配置文件策略更新或更改用户输入参数。
  - c 单击**下一步**。
  - d 查看修复主机配置文件所必需的任务，然后单击**完成**。
- 该主机属于 **vSAN** 群集，因此 **vSAN** 群集可以访问其资源。该主机还可以访问 **vSAN** 群集中的所有现有 **vSAN** 存储 I/O 策略。

## 使用维护模式

在关闭、重新引导 **vSAN** 群集中的主机或断开主机连接之前，必须将主机置于维护模式。

使用维护模式时，请注意以下准则：

- 将 **ESXi** 主机置于维护模式时，必须选择数据撤出模式，例如，**确保可从其他主机访问数据**或**将所有数据撤出到其他主机**。
- 如果 **vSAN** 群集的任何成员主机进入维护模式，群集容量将自动减少，因为此时该成员主机不再向群集提供存储。

- 虚拟机的计算资源可能不位于处于维护模式的主机上，而且虚拟机的存储资源可能位于群集中的任何位置。
- **确保数据可访问性**模式比**撤出全部数据**模式更快，因为**确保数据可访问性**仅从主机迁移对运行虚拟机至关重要的组件。处于此模式时，如果遇到故障，虚拟机的可用性将受影响。选择**确保数据可访问性**模式后，在故障期间不会重新保护数据，因此您可能会遇到意外丢失数据的情况。
- 选择**撤出全部数据**模式时，如果资源可用，并且**允许的故障数主要级别**设置为 **1** 或更多，则会在出现故障时自动重新保护数据。处于此模式时，主机中的所有组件都会迁移，并且根据主机上的数据量，迁移可能需要较长时间。使用**撤出全部数据**模式时，即使在计划维护期间，虚拟机也可允许故障。
- 使用三主机群集时，您无法使用**撤出全部数据**将服务器置于维护模式。可以考虑设计一个由四个或更多主机组成的群集，以实现最大可用性。

在将主机置于维护模式之前，必须验证以下内容：

- 如果使用**撤出全部数据**模式，请确认群集具有足够的主机和容量以满足**允许的故障数主要级别**策略要求。
- 确认在其余主机上有足够的闪存容量来处理任何闪存读取缓存预留。要分析每个主机的当前容量使用情况，以及单个主机故障是否可能导致群集运行空间不足和影响群集容量、缓存预留和群集组件，请运行以下 RVC 命令：**vsan.whatif\_host\_failures**。有关 RVC 命令的信息，请参见《RVC 命令参考指南》。
- 确认其他主机上是存在足够的容量设备可以满足条带宽度策略要求（如果选择）。
- 确保其他主机上有足够的可用容量来处理必须从进入维护模式的主机迁移的数据量。

**Enter Maintenance Mode** | 10.26.227.215

This host is in a vSAN cluster. Once the host is put in maintenance mode, it has no access to the vSAN datastore and the state of any virtual machines on that datastore. No virtual machines can be provisioned on this host while in maintenance mode. You must either power off or migrate the virtual machines from the host manually.

☒ Move powered-off and suspended virtual machines to other hosts in the cluster

vSAN data migration

Full data migration  
**Ensure accessibility**  
 No data migration

⚠ No data will be moved. 1 objects will become non-compliant with storage policy. [See detailed report](#)

A rebuild operation will be triggered for any non-compliant objects in 60 minutes unless the host is taken out of Maintenance Mode by then. You can change this timer from the cluster vSAN advanced settings.

Put the selected hosts in maintenance mode?

CANCEL OK

“确认维护模式”对话框提供有关维护活动的指导信息。可以查看每个数据撤出选项的影响。

- 可用于执行操作的容量是否足够。
- 将移动的数据量。
- 将变得不合规的对象数。
- 将变得不可访问的对象数。

## 将 vSAN 群集的成员置于维护模式

在关闭、重新引导 vSAN 群集中的主机或断开主机连接之前，必须将该主机置于维护模式。将主机置于维护模式时，必须选择数据撤出模式，例如**确保可访问性**或**迁移全部数据**。

如果 vSAN 群集的任何成员主机进入维护模式，群集容量将自动减少，因为该成员主机不再向群集提供容量。

此主机提供的任何 vSAN iSCSI 目标将传输到群集中的其他主机，因此 iSCSI 启动器将重定向到新的目标所有者。

### 前提条件

确认您的环境具有您选择的选项所需的功能。

### 步骤

- 1 右键单击主机，然后选择**维护模式 > 进入维护模式**。
- 2 选择数据撤出模式，然后单击**确定**。

选项	描述
确保可访问性	<p>此为默认选项。在关闭主机电源或将主机从群集中移除时，vSAN 将确保此主机上的所有可访问的虚拟机均保持可访问状态。如果要将主机暂时移出群集（例如，为了安装升级）并计划将主机移回群集中，请选择此选项。如果要将主机从群集中永久移除，则此选项不适用。</p> <p>通常，只需撤出部分数据。但是，撤出期间，虚拟机可能不再完全符合虚拟机存储策略。这意味着它可能无权访问其所有副本。如果在主机处于维护模式且<b>允许的故障数主要级别</b>设置为 1 时出现故障，您的群集可能会出现数据丢失的情况。</p> <p><b>注</b> 如果您使用三个主机的群集或配置有三个故障域的 vSAN 群集，这将是唯一可用的撤出模式。</p>
迁移全部数据	<p>群集中存在足够的资源时，vSAN 会将所有数据撤出到群集中的其他主机，维护或修复受影响组件的可用性合规性，并保护数据。如果计划永久迁移主机，请选择此选项。如果从群集中的最后一个主机撤出数据，请确保将虚拟机迁移到其他数据存储，然后将主机置于维护模式。</p> <p>此撤出模式导致出现大量数据传输并消耗大部分时间和资源。所选主机的本地存储上的所有组件都会迁移到群集中的其他位置。主机进入维护模式时，所有虚拟机都有权访问其存储组件，并且仍符合为其分配的存储策略。</p> <p><b>注</b> 如果主机中含有数据的虚拟机对象不可访问且未完全撤出，该主机将无法进入维护模式。</p>
不迁移数据	<p>vSAN 不会将任何数据从该主机中撤出。如果关闭主机电源或将主机从群集中移除，则某些虚拟机可能变得不可访问。</p>

具有三个故障域的群集与三主机群集的限制相同，例如，无法使用**迁移全部数据**模式，出现故障后无法重新保护数据。

### 后续步骤

您可以跟踪群集中数据迁移的进度。请参见《vSAN 监控和故障排除》中的“监控 vSAN 群集中的重新同步任务”。

## 管理 vSAN 群集中的故障域

如果 vSAN 群集跨越多个机架或刀片服务器底盘，则可通过故障域来防止机架或底盘故障。您可以创建故障域并将一台或多台主机添加到每个故障域。

故障域包含一个或多个按其在数据中心的物理位置分组的 vSAN 主机。配置后，故障域可确保 vSAN 允许整个物理机架故障，以及单个主机、容量设备、网络链接或专用于故障域的网络交换机的故障。

群集的**允许的故障数主要级别**策略取决于为虚拟机置备的允许的故障数。如果配置虚拟机时将**允许的故障数主要级别**设置为 1 (PFTT=1)，则 vSAN 可允许一个故障域内出现一个任意类型、任意组件的故障（包括整个机架的故障）。

在机架上配置故障域并置备新虚拟机时，vSAN 将确保多个保护对象（如副本和证明）放置在不同的故障域中。例如，如果虚拟机存储策略的**允许的故障数主要级别**设置为 N (PFTT=n)，则在群集中 vSAN 至少需要  $2*n+1$  个故障域。当使用此策略在包含故障域的群集中置备虚拟机时，将跨不同的机架存储关联虚拟机对象的副本。

至少需要三个故障域才能支持 PFTT=1。为达到最佳效果，请在群集中配置四个或四个以上故障域。具有三个故障域的群集与三主机群集具有相同的限制，例如，在出现故障后无法重新保护数据，也无法使用**迁移全部数据**模式。有关设计和调整故障域大小的信息，请参见《vSAN 规划和部署》中的“设计和调整 vSAN 故障域大小”。

考虑以下情况：有一个包含 16 个主机的 vSAN 群集。主机分散在 4 个机架中，即每个机架 4 个主机。要允许整个机架故障，请为每个机架创建一个故障域。可以配置此类容量的群集，并将**允许的故障数主要级别**设置为 1。如果要将**允许的故障数主要级别**设置为 2，请在群集中配置五个故障域。

当某个机架出现故障时，群集将无法使用所有资源，包括 CPU、机架中的内存。为降低潜在机架故障的影响，请配置较小大小的故障域。增加故障域数将增加在出现机架故障后群集中可用的资源总量。

使用故障域时，请遵循以下最佳做法。

- 在 vSAN 群集中至少配置三个故障域。为获得最佳效果，请配置四个或四个以上故障域。
- 不包括在任何故障域中的主机被视为驻留在自己的单主机故障域中。
- 不需要将每个 vSAN 主机都分配到一个故障域。如果决定使用多个故障域保护 vSAN 环境，请考虑创建相同大小的故障域。
- 当 vSAN 主机移动到另一个群集时，它们将保留其故障域分配。
- 设计故障域时，将在每个故障域中放置统一数量的主机。

有关设计故障域的准则，请参见《vSAN 规划和部署》中的“设计和调整 vSAN 故障域大小”。

- 可以将任意数量的主机添加到故障域。每个故障域必须至少包含一个主机。

## 在 vSAN 群集中创建新的故障域

要确保虚拟机对象在机架故障期间继续顺利运行，可以将主机分到不同的故障域中。

在具有故障域的群集上置备虚拟机时，vSAN 会将保护组件（例如虚拟机对象的证明和副本）分布在不同的故障域中。这样，除单个主机、存储磁盘或网络故障之外，vSAN 环境还能够承受整个机架故障。

### 前提条件

- 选择唯一的故障域名。vSAN 不支持在群集中存在重复的故障域名。
- 确认您的 ESXi 主机版本。故障域中只能包括 6.0 或更高版本的主机。
- 验证 vSAN 主机是否处于联机状态。无法将处于脱机状态或由于硬件配置问题而无法使用的主机分配到故障域中。

**步骤**

- 1 导航到 vSAN 群集。
- 2 单击**配置**选项卡。
- 3 在“vSAN”下，单击**故障域**。
- 4 单击**创建新故障域**图标 (+)。
- 5 输入故障域名称。
- 6 从**显示**下拉菜单中，选择**主机不在故障域中**以查看未分配给故障域的主机的列表，或选择**所有主机**以查看群集中的所有主机。
- 7 选择一个或多个主机添加到故障域中。  
故障域不能为空。必须至少选择一个主机包括到故障域中。
- 8 单击**确定**。  
选定的主机将显示在故障域中。

**将主机移至选定的故障域**

您可以将主机移至 vSAN 群集中选定的故障域。

**步骤**

- 1 导航到 vSAN 群集。
- 2 单击**配置**选项卡。
- 3 在“vSAN”下，单击**故障域**。
- 4 选择故障域，然后单击**将主机移至选定的故障域**图标。
- 5 从页面底部的**显示**下拉菜单中，选择**不在故障域中的主机**以查看可添加至故障域的主机，或选择**所有主机**以查看群集中的所有主机。
- 6 选择要添加至故障域的主机。
- 7 单击**确定**。  
选定的主机将显示在故障域中。

**将主机移出故障域**

根据您的要求，可以将主机移出故障域。

**前提条件**

验证主机是否处于联机状态。无法从故障域中移动脱机或不可用的主机。

**步骤**

- 1 导航到 vSAN 群集。

- 2 单击**配置**选项卡。
- 3 在“vSAN”下，单击**故障域**。

选项	描述
<b>vSphere Client</b>	<ol style="list-style-type: none"> <li>a 展开一个现有故障域以查看其成员主机。</li> <li>b 选择要移动的主机，然后单击<b>将主机移出故障域</b>图标。您还可以单击并将主机拖出故障域。</li> </ol>
<b>vSphere Web Client</b>	<ol style="list-style-type: none"> <li>a 选择要移动的主机，然后单击<b>将主机移出故障域</b>图标。</li> <li>b 单击<b>是</b>。</li> </ol>

选定的主机将不再属于故障域。任何不属于故障域的主机都会被视为位于其自己的单主机故障域中。

#### 后续步骤

可以将主机添加到故障域中。请参见[将主机移至选定的故障域](#)。

## 重命名故障域

可以更改 vSAN 群集中现有故障域的名称。

#### 步骤

- 1 导航到 vSAN 群集。
- 2 单击**配置**选项卡。
- 3 在“vSAN”下，单击**故障域**。

选项	描述
<b>vSphere Client</b>	<ol style="list-style-type: none"> <li>a 选择故障域，然后选择菜单<b>操作 &gt; 重命名</b>。</li> <li>b 输入新的故障域名称。</li> </ol>
<b>vSphere Web Client</b>	<ol style="list-style-type: none"> <li>a 选择故障域，并单击<b>重命名选定的故障域</b>图标。</li> <li>b 输入新的故障域名称。</li> </ol>

- 4 单击**确定**。

新名称将显示在故障域列表中。

## 移除选定的故障域

不再需要故障域时，您可以将其从 vSAN 群集中移除。

#### 步骤

- 1 导航到 vSAN 群集。
- 2 单击**配置**选项卡。



### 3 在“vSAN”下，单击故障域。

选项	描述
<b>vSphere Client</b>	a 选择故障域，然后选择菜单 <b>操作 &gt; 删除</b> 。 b 单击 <b>是</b> 确认。
<b>vSphere Web Client</b>	a 选择要删除的故障域，然后单击 <b>移除选定的故障域</b> 图标 (X)。 b 单击 <b>是</b> 确认。

将移除故障域中的所有主机，并从 vSAN 群集中删除选定的故障域。不属于故障域的每个主机将被视为位于其自己的单主机故障域中。

## 使用 vSAN iSCSI 目标服务

使用 iSCSI 目标服务可使驻留在 vSAN 群集之外的主机和物理工作负载能够访问 vSAN 数据存储。

通过此功能，远程主机上的 iSCSI 启动器可以将块级数据传输到 vSAN 群集中存储设备上的 iSCSI 目标。vSAN 6.7 及更高版本支持 Windows Server 故障切换群集 (WSFC)，因此 WSFC 节点能够访问 vSAN iSCSI 目标。

配置 vSANiSCSI 目标服务后，可以从远程主机发现 vSAN iSCSI 目标。要发现 vSANiSCSI 目标，请使用 vSAN 群集中任何主机的 IP 地址，以及 iSCSI 目标的 TCP 端口。要确保 vSANiSCSI 目标的高可用性，请为 iSCSI 应用程序配置多路径支持。您可以使用两个或更多主机的 IP 地址来配置多路径。

**注** vSANiSCSI 目标服务不支持其他 vSphere 或 ESXi 客户端或启动器、第三方管理程序，或使用裸设备映射 (RDM) 的迁移。

vSANiSCSI 目标服务支持以下 CHAP 身份验证方法：

- CHAP** 在 CHAP 身份验证中，目标需验证启动器，但启动器无需验证目标。
- 双向 CHAP** 在双向 CHAP 身份验证中，提供了供启动器验证目标的额外安全级别。

有关使用 vSANiSCSI 目标服务的详细信息，请参阅 [iSCSI 目标使用指南](#)。

## iSCSI 目标

您可以添加作为逻辑单元号 (LUN) 提供存储块的一个或多个 iSCSI 目标。vSAN 通过唯一 iSCSI 限定名称 (IQN) 标识每个 iSCSI 目标。您可以使用 IQN 向远程 iSCSI 启动器提供 iSCSI 目标，以便启动器可以访问该目标的 LUN。

每个 iSCSI 目标均包含一个或多个 LUN。您可以定义每个 LUN 的大小、向每个 LUN 分配 vSAN 存储策略并在 vSAN 群集上启用 iSCSI 目标服务。您可以配置一个存储策略，将其用作 vSANiSCSI 目标服务的主对象的默认策略。

## iSCSI 启动器组

您可以定义对指定 iSCSI 目标具有访问权限的一组 iSCSI 启动器。iSCSI 启动器组只能访问属于该组成员的启动器。如果未定义 iSCSI 启动器或启动器组，则所有 iSCSI 启动器均可访问每个目标。

使用唯一名称标识每个 iSCSI 启动器组。您可以将一个或多个 iSCSI 启动器添加为该组的成员。使用启动器的 IQN 作为成员启动器名称。

## 启用 iSCSI 目标服务

创建 iSCSI 目标和 LUN 以及定义 iSCSI 启动器组之前，必须先在 vSAN 群集中启用 iSCSI 目标服务。

### 步骤

- 1 导航到 vSAN 群集。
- 2 单击配置选项卡。

选项	描述
vSphere Client	<ol style="list-style-type: none"> <li>a 在 vSAN 下，单击 <b>iSCSI 目标服务</b>。</li> <li>b 单击 <b>启用</b> vSAN iSCSI 目标服务。</li> <li>c 编辑 vSAN iSCSI 目标服务配置。此时您可以选择默认网络、TCP 端口和身份验证方法。您还可以选择 vSAN 存储策略。</li> </ol>
vSphere Web Client	<ol style="list-style-type: none"> <li>a 在“vSAN”下，单击 <b>iSCSI 目标</b>。</li> <li>b 单击 vSAN iSCSI 目标服务 <b>编辑</b> 按钮。</li> <li>c 选中启用 vSAN iSCSI 目标服务复选框。此时您可以选择默认网络、TCP 端口和身份验证方法。您还可以选择 vSAN 存储策略。</li> </ol>

- 3 单击 **确定** 或 **应用**。

### 后续步骤

启用 iSCSI 目标服务后，您可以创建 iSCSI 目标和 LUN，以及定义 iSCSI 启动器组。

## 创建 iSCSI 目标

您可以创建或编辑 iSCSI 目标及其关联的 LUN。

### 前提条件

确认已启用 iSCSI 目标服务。

### 步骤

- 1 导航到 vSAN 群集。

## 2 单击配置选项卡。

选项	描述
<b>vSphere Client</b>	<ol style="list-style-type: none"> <li>在 vSAN 下，单击 <b>iSCSI 目标服务</b>。</li> <li>单击“iSCSI 目标”选项卡。</li> <li>单击<b>添加</b>。将显示<b>新建 iSCSI 目标</b>对话框。如果将“目标 IQN”字段留空，则会自动生成 IQN。</li> <li>输入目标别名。您还可以编辑此目标的网络、TCP 端口和身份验证方法。</li> </ol>
<b>vSphere Web Client</b>	<ol style="list-style-type: none"> <li>在“vSAN”下，单击 <b>iSCSI 目标</b>。</li> <li>在“vSAN iSCSI 目标”部分，单击<b>添加新的 iSCSI 目标</b>图标。此时将显示“新建 iSCSI 目标”对话框。目标 IQN 会自动生成。</li> <li>输入目标别名。您还可以编辑此目标的网络、TCP 端口和身份验证方法。</li> <li>（可选）要为目标定义 LUN，请单击“将第一个 LUN 添加到 iSCSI 目标”复选框，并输入 LUN 的大小。</li> </ol>

## 3 单击确定。

### 后续步骤

定义可以访问此目标的 iSCSI 启动器的列表。

## 向 iSCSI 目标添加 LUN

您可以向 iSCSI 目标添加一个或多个 LUN，也可以编辑现有的 LUN。

### 步骤

- 1 导航到 vSAN 群集。
- 2 单击配置选项卡。

选项	描述
<b>vSphere Client</b>	<ol style="list-style-type: none"> <li>在 vSAN 下，单击 <b>iSCSI 目标服务</b>。</li> <li>单击“iSCSI 目标”选项卡，然后选择一个目标。</li> <li>在“vSAN iSCSI LUN”部分中，单击<b>添加</b>。将显示<b>将 LUN 添加到目标</b>对话框。</li> <li>输入 LUN 的大小。系统将自动分配为 iSCSI 目标服务配置的 vSAN 存储策略。您可向每个 LUN 分配不同的策略。</li> </ol>
<b>vSphere Web Client</b>	<ol style="list-style-type: none"> <li>在“vSAN”下，单击 <b>iSCSI 目标</b>。</li> <li>选择一个目标，并在页面的“目标详细信息”部分选择 <b>LUN</b> 选项卡。</li> <li>单击<b>向目标添加新的 iSCSI LUN</b> 图标。此时将显示“将 LUN 添加到目标”对话框。</li> <li>输入 LUN 的大小。系统将自动分配为 iSCSI 目标服务配置的 vSAN 存储策略。您可向每个 LUN 分配不同的策略。</li> </ol>

## 3 单击添加。

## 创建 iSCSI 启动器组

您可以创建 iSCSI 启动器组，从而为 iSCSI 目标提供访问控制。只有作为启动器组成员的 iSCSI 启动器才能访问 iSCSI 目标。

**步骤**

- 1 导航到 vSAN 群集。
- 2 单击配置选项卡。

选项	描述
<b>vSphere Client</b>	<ol style="list-style-type: none"> <li>a 在 vSAN 下，单击 <b>iSCSI 目标服务</b>。</li> <li>b 单击“启动器组”选项卡，然后单击<b>添加新的 iSCSI 启动器组</b> (+) 图标。将显示<b>新建启动器组</b>对话框。</li> <li>c 输入 iSCSI 启动器组的名称。</li> <li>d （可选）要向启动器组添加成员，请输入每个成员的 IQN。使用以下格式输入成员 IQN：  <i>iqn.YYYY-MM.domain:name</i>  其中： <ul style="list-style-type: none"> <li>■ YYYY = 年份，例如 2016</li> <li>■ MM = 月份，例如 09</li> <li>■ domain = 启动器所在的域</li> <li>■ name = 成员名称（可选）</li> </ul> </li> </ol>
<b>vSphere Web Client</b>	<ol style="list-style-type: none"> <li>a 在“vSAN”下，单击 <b>iSCSI 启动器组</b>。</li> <li>b 在“vSAN iSCSI 启动器组”部分，单击<b>添加新的 iSCSI 启动器组</b>图标。将显示“新建 vSAN iSCSI 启动器组”对话框。</li> <li>c 输入 iSCSI 启动器组的名称。</li> <li>d （可选）要向启动器组添加成员，请输入每个成员的 IQN。使用以下格式输入成员 IQN：  <i>iqn.YYYY-MM.domain:name</i>  其中： <ul style="list-style-type: none"> <li>■ YYYY = 年份，例如 2016</li> <li>■ MM = 月份，例如 09</li> <li>■ domain = 启动器所在的域</li> <li>■ name = 成员名称（可选）</li> </ul> </li> </ol>

- 3 单击**确定或创建**。

**后续步骤**

将成员添加到 iSCSI 启动器组。

**向 iSCSI 启动器组分配目标**

您可以向 iSCSI 启动器组分配 iSCSI 目标。只有作为启动器组成员的启动器才能访问分配的目标。

**前提条件**

确认存在现有的 iSCSI 启动器组。

**步骤**

- 1 导航到 vSAN 群集。

## 2 单击配置选项卡。

选项	描述
<b>vSphere Client</b>	<ol style="list-style-type: none"> <li>在 vSAN 下，单击 <b>iSCSI 目标服务</b>。</li> <li>选择 <b>启动器组</b> 选项卡。</li> <li>在“可访问目标”部分中，单击 <b>为 iSCSI 启动器组添加新的可访问目标 (+)</b> 图标。将显示 <b>添加可访问目标</b> 对话框。</li> <li>从可用目标列表中选择目标。</li> </ol>
<b>vSphere Web Client</b>	<ol style="list-style-type: none"> <li>在“vSAN”下，单击 <b>iSCSI 目标</b>。</li> <li>选择“启动器组”选项卡。</li> <li>在“组详细信息”部分中，选择“可访问目标”选项卡。</li> <li>单击 <b>为 iSCSI 启动器组添加新的可访问目标</b> 图标。将显示“添加可访问目标”对话框。</li> <li>在“筛选器”选项卡中，从可用目标列表中选择目标。“选定对象”选项卡将显示当前选定的目标。</li> </ol>

## 3 单击添加。

## 监控 vSAN iSCSI 目标服务

您可以监控 iSCSI 目标服务，以查看 iSCSI 目标组件的物理放置位置和检查故障组件。也可以监控 iSCSI 目标服务的运行状况。

### 前提条件

确认已启用 vSANiSCSI 目标服务且已创建目标和 LUN。

### 步骤

- ◆ 浏览到 vSAN 群集。


选项	描述
<b>vSphere Client</b>	<ol style="list-style-type: none"> <li>单击 <b>监控</b>，然后选择 <b>虚拟对象</b>。页面上将列出 iSCSI 目标。</li> <li>选择目标，然后单击 <b>查看放置详细信息</b>。“物理放置位置”显示了目标的数据组件的位置。</li> <li>单击 <b>通过主机放置组件</b>，可查看与 iSCSI 数据组件关联的主机。</li> </ol>
<b>vSphere Web Client</b>	<ol style="list-style-type: none"> <li>单击 <b>监控</b> 并选择 <b>vSAN</b>。</li> <li>单击 <b>iSCSI 目标</b>。页面顶部将列出 iSCSI 目标和 LUN。</li> <li>单击目标别名并查看其状态。页面底部的“物理磁盘放置”选项卡将显示目标的数据组件所在的位置。“合规性错误”选项卡将显示故障组件。</li> <li>单击 <b>LUN</b> 并查看其状态。页面底部的“物理磁盘放置”选项卡将显示 LUN 的数据组件所在的位置。“合规性错误”选项卡将显示故障组件。</li> </ol>

## 将混合 vSAN 群集迁移到全闪存群集

您可以将混合 vSAN 群集中的磁盘组迁移到全闪存磁盘组。

vSAN 混合群集将磁盘用于容量层，将闪存设备用于缓存层。您可以更改群集中磁盘组的配置，以便在缓存层和容量层使用闪存设备。

**步骤**

- 1 导航到 vSAN 群集。
- 2 移除群集中各主机的混合磁盘组。
  - a 单击**配置**选项卡。
  - b 在“vSAN”下，单击**磁盘管理**。
  - c 在“磁盘组”下，选择要移除的磁盘组，然后单击**移除磁盘组**图标 ( )。
  - d 选择**迁移全部数据**作为迁移模式，然后单击**是**。
- 3 从主机移除物理 HDD 磁盘。
- 4 将闪存设备添加到主机。  
确认闪存设备上不存在任何分区。
- 5 在每个主机上创建全闪存磁盘组。

## 关闭 vSAN 群集电源

您可以关闭 vSAN 群集电源以执行维护或升级。

**前提条件**

如果 vCenter Server 虚拟机正在 vSAN 群集上运行，请将该虚拟机迁移到第一个主机，或记下当前正在运行该虚拟机的主机。

**步骤**

- 1 关闭在 vSAN 群集上运行的所有虚拟机的电源。  
如果 vCenter Server 在 vSAN 群集上运行，必须最后关闭 vCenter Server 虚拟机的电源。
- 2 将组成群集的 ESXi 主机置于维护模式。
  - 右键单击每个主机，然后选择**维护模式 > 进入维护模式**。
  - 选择**不迁移数据**选项。
- 3 关闭 ESXi 主机的电源。

## vSAN 群集中的设备管理

可以在 vSAN 群集中执行各种设备管理任务。可以创建混合或全闪存磁盘组、允许 vSAN 声明用于容量和缓存的设备、在设备上启用或禁用 LED 指示器、将设备标记为闪存、将远程设备标记为本地设备等。

本章讨论了以下主题：

- [管理磁盘组和设备](#)
- [使用单独的设备](#)

### 管理磁盘组和设备

在群集上启用 vSAN 时，选择磁盘声明模式以将设备整理到组中。

vSAN 6.6 和更高版本在所有场景中使用统一的磁盘声明工作流。它按型号和尺寸或按主机将所有可用的磁盘进行分组。必须选择用于缓存和用于容量的设备。

#### 在主机上创建磁盘组

创建磁盘组时，必须指定要用于 vSAN 数据存储的各个主机和设备。请将缓存和容量设备整理到磁盘组中。

要创建磁盘组，您可以定义磁盘组，并分别选择要包含在磁盘组中的设备。每个磁盘组包含一个闪存缓存设备和一个或多个容量设备。

创建磁盘组时，应考虑闪存缓存与已用容量的比率。该比率与群集的要求和工作负载有关。对于混合群集，请考虑确保闪存缓存与消耗容量的比率至少为 10%（不包括镜像之类的副本）。有关确定全闪存群集缓存比率的指导，请参阅[设计 vSAN 磁盘组 - 全闪存缓存比率更新](#)。

vSAN 群集最初包含未占用字节的单个 vSAN 数据存储。

在各个主机上创建磁盘组并添加缓存和容量设备时，数据存储的大小会根据这些设备的物理容量大小而相应增加。vSAN 使用已添加到群集的主机中可用的本地空容量创建一个分布式 vSAN 数据存储。

如果群集需要多个闪存缓存设备，则必须手动创建多个磁盘组，因为每个磁盘组最多允许一个闪存缓存设备。

**注** 将新的 ESXi 主机添加到 vSAN 群集时，不会自动将该主机中的本地存储添加到 vSAN 数据存储。必须创建磁盘组，并将设备添加到磁盘组中，才能使用新的 ESXi 主机中的新存储。

## 为 vSAN 群集声明磁盘

您可以从主机中选择多个设备，vSAN 会为您创建默认磁盘组。

将更多容量添加到主机或添加具有容量的新主机时，您可以选择新设备以增加 vSAN 数据存储的容量。在全闪存群集中，您可以将要使用的闪存设备标记为容量设备。


vSAN 声明设备后，它将创建 vSAN 共享数据存储。数据存储的总大小反映群集中所有主机的磁盘组中所有容量设备的容量。某些容量开销用于元数据。

## 在 vSAN 主机上创建磁盘组

您可以手动结合使用特定缓存设备和特定容量设备，以便在特定主机上定义磁盘组。

使用此方法，您可以手动选择设备，以便为主机创建磁盘组。您可以为此磁盘组添加一个缓存设备，以及至少一个容量设备。

### 步骤

- 1 导航到 vSAN 群集。
- 2 单击配置选项卡。
- 3 在“vSAN”下，单击磁盘管理。
- 4 选择主机然后单击 创建新磁盘组 图标 ()。
  - 选择用于缓存的闪存设备。
  - 从容量类型下拉菜单选择要使用的容量磁盘类型，具体取决于您要创建的磁盘组类型（混合磁盘组使用 HDD，全闪存磁盘组使用 Flash）。
  - ◆ 选择您要用于容量的设备。
- 5 单击创建或确定以确认您的选择。

新的磁盘组将显示在列表中。

## 为 vSAN 群集声明存储设备

您可以选择一组缓存和容量设备，vSAN 会将其整理到默认磁盘组中。



## 步骤

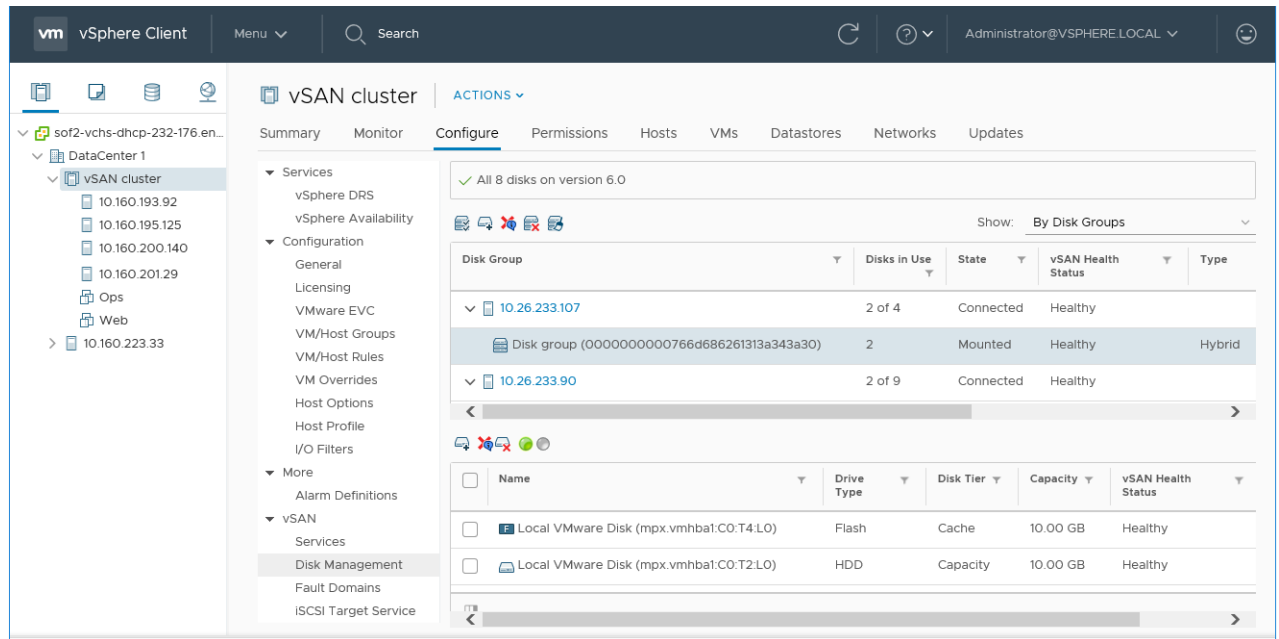
- 1 导航到 vSAN 群集。
- 2 单击配置选项卡。
- 3 在“vSAN”下，单击磁盘管理。
- 4 单击为 vSAN 声明未使用磁盘图标 (🗑️)。
- 5 选择要添加到磁盘组的设备。
  - 对于混合磁盘组，提供存储的每个主机必须提供一个闪存缓存设备和一个或多个 HDD 容量设备。您可以在每个磁盘组中仅添加一个缓存设备。
    - 选择要用作缓存的闪存设备然后单击针对缓存层声明图标 (⚡)。
    - 选择要用作容量的 HDD 设备然后单击针对容量层声明图标 (💿)。
    - 单击确定。
  - 对于全闪存磁盘组，提供存储的每个主机必须提供一个闪存缓存设备和一个或多个闪存容量设备。您可以在每个磁盘组中仅添加一个缓存设备。
    - 选择要用作缓存的闪存设备然后单击针对缓存层声明图标 (⚡)。
    - 选择要用于容量的闪存设备然后单击针对容量层声明图标 (💿)。
    - 单击确定。

要验证添加到全闪存磁盘组的每个设备的角色，请导航至“磁盘管理”页面底部的“磁盘角色”列。该列会显示设备及其在磁盘组中的用途的列表。

vSAN 会声明您选择的设备，并将其整理到支持 vSAN 数据存储的默认磁盘组中。

## 使用单独的设备

可以在 vSAN 群集中执行各种设备管理任务，例如，将设备添加到磁盘组、从磁盘组中移除设备、启用或禁用定位符 LED 以及标记设备。



## 将设备添加到磁盘组

在手动模式下配置 vSAN 以便声明磁盘时，可以将其他本地设备添加到现有磁盘组。

要添加的设备必须与磁盘组中的现有设备类型相同，例如 SSD 或磁盘。

### 步骤

- 1 导航到 vSAN 群集。
- 2 单击配置选项卡。
- 3 在“vSAN”下，单击磁盘管理。
- 4 选择磁盘组，然后单击向选定的磁盘组添加磁盘图标 (📁)。
- 5 选择要添加的设备并单击确定。

如果添加包含残留数据或分区信息的已用设备，则必须先清理设备。有关将分区信息从设备移除的信息，请参见[从设备移除分区](#)。还可以运行 `host_wipe_vsan_disks` RVC 命令将该设备格式化。有关 RVC 命令的详细信息，请参见《RVC 命令参考指南》。

### 后续步骤

确认 vSAN 磁盘平衡运行状况检查为绿色。如果磁盘平衡运行状况检查发出警告，请在非高峰时间执行手动重新平衡操作。有关详细信息，请参见《vSAN 监控和故障排除》中的“手动重新平衡”。

## 从 vSAN 移除磁盘组或设备

可以从磁盘组或整个磁盘组中移除选定的设备。

由于移除不受保护的设备可能会对 vSAN 数据存储和数据存储中的虚拟机造成破坏，请避免移除设备或磁盘组。

通常，在升级设备或更换出现故障的设备时，或者必须移除缓存设备时，会从 vSAN 删除设备或磁盘组。其他 vSphere 存储功能可以使用任何您从 vSAN 群集中移除的闪存设备。

永久删除磁盘组的同时会删除磁盘成员资格以及存储在设备上的数据。

**注** 从磁盘组中移除一个闪存缓存设备或所有容量设备的同时会移除整个磁盘组。

从设备或磁盘组撤出数据可能会导致虚拟机存储策略暂时不合规。

#### 前提条件

- 删除设备或磁盘组时，可以通过选择**迁移全部数据**选项或选择**确保数据可访问性**，将 vSAN 主机置于维护模式。如果从下拉菜单中选择**不迁移数据**，那么撤出期间发生故障时您的数据可能会面临风险。

#### 步骤

- 1 导航到 vSAN 群集。
- 2 单击**配置**选项卡。
- 3 在“vSAN”下，单击**磁盘管理**。
- 4 移除磁盘组或选定的设备。

选项	描述
移除磁盘组	<ol style="list-style-type: none"> <li>在“磁盘组”下，选择要移除的磁盘组，然后单击<b>移除磁盘组</b>图标 ( )。</li> <li>选择数据撤出模式。</li> </ol>
移除选定的设备	<ol style="list-style-type: none"> <li>在“磁盘组”下，选择包含要移除的设备的磁盘组。</li> <li>在“磁盘”下，选择要移除的设备，然后单击<b>从磁盘组中移除选定的磁盘</b>图标 ( )。</li> <li>选择数据撤出模式。</li> </ol>

您可以将撤出的数据移动到同一主机上的其他磁盘或磁盘组。

- 5 单击**是**或**删除**确认。

数据已从选定设备或磁盘组中撤出，无法再用于 vSAN。

## 重新创建磁盘组

在 vSAN 群集中重新创建磁盘组时，请从磁盘组中移除现有磁盘并删除该磁盘组。vSAN 将使用相同的磁盘重新创建磁盘组。

在 vSAN 群集上重新创建磁盘组时，vSAN 管理该过程。vSAN 撤出磁盘组中所有磁盘的数据，移除该磁盘组，并创建具有相同磁盘的磁盘组。

#### 步骤

- 1 在 vSphere Client 中导航到 vSAN 群集。
- 2 单击**配置**选项卡。
- 3 在“vSAN”下，单击**磁盘管理**。

- 4 在“磁盘组”下，选择要重新创建的磁盘组，然后单击**重新创建磁盘组**图标 (🔄)。  
将显示“重新创建磁盘组”对话框。
- 5 选择数据迁移模式，然后单击**重新创建**。

驻留在磁盘上的所有数据都被撤出。磁盘组从群集中移除并重新创建。

## 使用定位符 LED

您可以使用定位符 LED 识别存储设备的位置。

vSAN 可以点亮故障设备上的定位符 LED，从而让您可以轻松识别该设备。当您使用多个热插拔和主机交换方案时，这种方法十分有用。

考虑使用配有直通模式的 I/O 存储控制器，因为如果使用配有 RAID 0 模式的控制器，还需要执行其他步骤才能让控制器识别定位符 LED。

有关将存储控制器配置为 RAID 0 模式的信息，请参见供应商文档。

## 启用和禁用定位符 LED

可以打开或关闭 vSAN 存储设备上的定位符 LED。打开定位符 LED 时，可以确定特定存储设备的位置。

不再需要 vSAN 设备上的可视警示时，可以关闭选定设备上的定位符 LED。

### 前提条件

- 验证您是否已经为启用此功能的存储 I/O 控制器安装了受支持的驱动程序。有关经过 VMware 认证的驱动程序的信息，请参见《VMware 兼容性指南》，网址为 <http://www.vmware.com/resources/compatibility/search.php>。
- 在某些情况下，您可能需要使用第三方实用程序来配置存储 I/O 控制器上的定位符 LED 功能。例如，使用 HP 时，应确认已安装 HP SSA CLI。

有关安装第三方 VIB 的信息，请参见《vSphere 升级》文档。

### 步骤

- 1 导航到 vSAN 群集。
- 2 单击**配置**选项卡。
- 3 在“vSAN”下，单击**磁盘管理**。
- 4 选择一台主机以查看设备列表。
- 5 在页面底部，从列表中选择一个或多个存储设备，并启用或禁用选定设备上的定位符 LED。

选项	操作
开启所选磁盘的定位符 LED 图标	启用所选存储设备上的定位符 LED。您可以通过以下方式启用定位符 LED：在 <b>管理</b> 选项卡中，单击 <b>存储 &gt; 存储设备</b> 。
关闭所选磁盘的定位符 LED 图标	禁用所选存储设备上的定位符 LED。您可以通过以下方式禁用定位符 LED：在 <b>管理</b> 选项卡中，单击 <b>存储 &gt; 存储设备</b> 。

## 将设备标记为闪存

当闪存设备没有被 ESXi 主机自动标识为闪存时，您可以手动将它们标记为本地闪存设备。

如果为闪存设备启用 RAID 0 模式而非直通模式，则闪存设备可能无法被识别。当设备未被识别为本地闪存时，针对 vSAN 提供的设备列表中不包含这些设备，您将无法在 vSAN 群集中使用这些设备。将这些设备标记为本地闪存可使它们对 vSAN 可用。

### 前提条件

- 验证设备是否为您主机的本地设备。
- 确认设备不在使用中。
- 确保访问该设备的虚拟机已关闭电源，且数据存储已卸载。

### 步骤

- 1 导航到 vSAN 群集。
- 2 单击配置选项卡。
- 3 在“vSAN”下，单击磁盘管理。
- 4 选择主机以查看可用设备列表。
- 5 从页面底部的显示下拉菜单中，选择未在使用中。
- 6 从列表中选择一个或多个闪存设备，并单击标记为闪存磁盘图标 (F)。
- 7 单击是，以保存所做的更改。

此时所选设备的驱动器类型显示为“闪存”。

## 将设备标记为 HDD

当本地磁盘没有被 ESXi 主机自动标识为 HDD 设备时，您可以手动将其标记为本地 HDD 设备。


如果已将磁盘标记为闪存设备，则可以通过将设备标记为磁盘更改设备的磁盘类型。

### 前提条件

- 确认磁盘是主机本地磁盘。
- 确认磁盘未使用且为空。
- 确认访问设备的虚拟机已关闭电源。

### 步骤

- 1 导航到 vSAN 群集。
- 2 单击配置选项卡。
- 3 在“vSAN”下，单击磁盘管理。
- 4 选择主机以查看可用磁盘列表。

- 5 从页面底部的**显示**下拉菜单中，选择**未在使用中**。
- 6 从列表中选择一个或多个磁盘并单击**标记为 HDD 磁盘**图标 ( )。
- 7 单击**是**以保存。

所选磁盘的“驱动器类型”显示为 HDD。

## 将设备标记为本地

当主机使用外部 SAS 机箱时，vSAN 可能会将某些设备识别为远程设备，并且可能无法自动声明其为本地设备。

在这些情况下，您可以将设备标记为本地设备。

### 前提条件

确存储设备未共享。

### 步骤

- 1 导航到 vSAN 群集。
- 2 单击**配置**选项卡。
- 3 在“vSAN”下，单击**磁盘管理**。
- 4 选择一台主机以查看设备列表。
- 5 从页面底部的**显示**下拉菜单中，选择**未在使用中**。
- 6 从设备列表中选择一个或多个需要标记为本地设备的远程设备，然后单击**标记为本地**图标。
- 7 单击**是**以保存所做的更改。

## 将设备标记为远程

使用外部 SAS 控制器的主机可以共享设备。您可以手动将这些共享设备标记为远程设备，以便 vSAN 不会在创建磁盘组时声明这些设备。

在 vSAN 中，无法将共享设备添加到磁盘组中。

### 步骤

- 1 导航到 vSAN 群集。
- 2 单击**配置**选项卡。
- 3 在“vSAN”下，单击**磁盘管理**。
- 4 选择一台主机以查看设备列表。
- 5 从页面底部的**显示**下拉菜单中，选择**未在使用中**。
- 6 选择一个或多个需要标记为远程设备的设备，然后单击**标记为远程**图标。
- 7 单击**是**确认。

## 添加容量设备


可以向现有的 vSAN 磁盘组添加容量设备。

无法将共享设备添加到磁盘组。

### 前提条件

确认该设备已格式化且未在使用。

### 步骤

- 1 导航到 vSAN 群集。
- 2 单击**配置**选项卡。
- 3 在“vSAN”下，单击**磁盘管理**。
- 4 选择磁盘组。
- 5 单击页面底部的**向选定的磁盘组添加磁盘**图标 ( )。
- 6 选择要添加到磁盘组的容量设备。
- 7 单击**确定**或**添加**。

该设备即添加到磁盘组。

## 从设备移除分区

可以从设备中移除分区信息，以便 vSAN 能够声明可供使用的设备。


如果已添加包含残留数据或分区信息的设备，必须从设备中移除所有已经存在的分区信息之后才能声明设备以供 vSAN 使用。VMware 建议将干净的设备添加到磁盘组。

从设备中移除分区信息时，vSAN 会从设备中删除包含磁盘格式信息的主分区以及逻辑分区。

### 前提条件

确认 ESXi 未将设备作为引导磁盘、VMFS 数据存储或 vSAN 使用。

### 步骤

- 1 导航到 vSAN 群集。
- 2 单击**配置**选项卡。
- 3 在“vSAN”下，单击**磁盘管理**。
- 4 选择主机以查看可用设备列表。
- 5 从页面底部的**显示**下拉菜单中，选择**不合格**。
- 6 从列表中选择设备，然后单击**清除分区**图标 ( )。

**7** 单击**确定**以确认。

设备已清除干净且不包含任何分区信息。



## 提高 vSAN 群集中的空间效率

借助空间效率技术，可以降低用于存储数据的空间量。这些技术可以减少所需的总存储空间，进而满足您的需求。

本章讨论了以下主题：

- [vSAN 空间效率简介](#)
- [Reclaiming Space with SCSI Unmap](#)
- [使用去重和压缩](#)
- [使用 RAID 5 或 RAID 6 删除编码](#)
- [RAID 5 或 RAID 6 设计注意事项](#)

### vSAN 空间效率简介

借助空间效率技术，可以降低用于存储数据的空间量。这些技术可以降低所需的总存储容量，进而满足您的需求。

vSAN 6.7 Update 1 及更高版本支持 SCSI unmap 命令，该命令可用于回收映射到已删除的 vSAN 对象的存储空间。

可以在 vSAN 群集上启用去重和压缩功能，以消除重复的数据并减少存储数据所需的空间量。

您可以在虚拟机上设置容错方法策略属性以使用 RAID 5 或 RAID 6 删除编码。删除编码可以在使用低于默认 RAID 1 镜像的存储空间时保护您的数据。

可以使用去重和压缩功能、RAID 5 或 RAID 6 删除编码来节省更多的存储空间。与 RAID 1 相比，RAID 5 或 RAID 6 均提供了明确定义的空间节省。去重和压缩功能可节省额外空间。

### Reclaiming Space with SCSI Unmap

vSAN 6.7 Update 1 and later supports SCSI unmap commands that enable you to reclaim storage space that is mapped to a deleted vSAN object.

Deleting or removing files frees space within the file system. This free space is mapped to a storage device until the file system releases or unmaps it. vSAN supports reclamation of free space, which is also called the unmap operation. You can free storage space in the vSAN datastore when you delete or migrate a VM, consolidate a snapshot, and so on.

Reclaiming storage space can provide higher host-to-flash I/O throughput and improve flash endurance.

vSAN also supports the SCSI unmap commands issued directly from a guest operating system to reclaim storage space. vSAN supports offline unmaps as well as inline unmaps. On Linux OS, offline unmaps are performed with the **fstrim(8)** command, and inline unmaps are performed when the **mount -o discard** command is used. On Windows OS, NTFS performs inline unmaps by default.

Unmap capability is disabled by default. To enable unmap on a vSAN cluster, use the following RVC command: **vsan.unmap\_support -enable**

When you enable unmap on a vSAN cluster, you must power off and then power on all VMs. VMs must use virtual hardware version 13 or above to perform unmap operations.

## 使用去重和压缩

vSAN 可以执行块级去重和压缩以节省存储空间。在 vSAN 全闪存群集上启用去重和压缩后，每个磁盘组上的冗余数据都会减少。

去重可以移除冗余数据块，而压缩可以移除每个数据块中的额外冗余数据。两种技术同时使用可以减少存储数据所需的空间量。vSAN 将数据从缓存层移至容量层时，先后会应用去重和压缩。

您可以在群集范围内启用去重和压缩，但需要以磁盘组为单位应用。在 vSAN 群集上启用去重和压缩时，特定磁盘组中的冗余数据会减少为一个副本。

创建新的 vSAN 全闪存群集或编辑现有 vSAN 全闪存群集时，可以启用去重和压缩。有关创建和编辑 vSAN 群集的详细信息，请参见《vSAN 规划和部署》中的“启用 vSAN”。

启用或禁用去重和压缩时，vSAN 会对每个主机上的每个磁盘组执行滚动重新格式化操作。该过程可能需要很长时间，具体取决于 vSAN 数据存储上存储的数据。请勿频繁执行这些操作。如果您计划禁用去重和压缩，必须首先确认有充足的物理容量放置数据。

---

**注** 对于加密虚拟机，去重和压缩可能无效，因为在将主机上的数据写出到存储器之前，虚拟机加密会对这些数据进行加密。使用虚拟机加密时请考虑存储权衡。

---

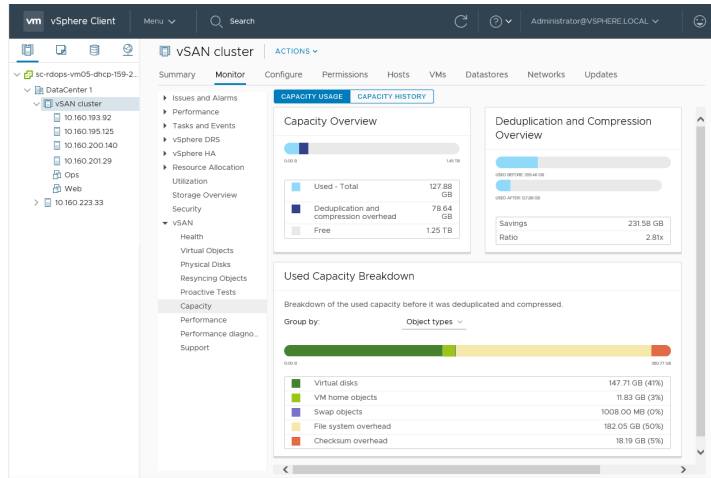
## 如何在启用去重和压缩的群集中管理磁盘

在启用去重和压缩的群集中管理磁盘时，请考虑以下指南。

- 避免以增量方式向磁盘组中添加磁盘。为了有效地去重和压缩，可以考虑添加磁盘组以增加群集存储容量。
- 手动添加磁盘组时，同时添加所有容量磁盘。
- 您无法从磁盘组移除单个磁盘，必须移除整个磁盘组才能进行更改。
- 单个磁盘故障会造成整个磁盘组故障。

## 确认通过去重和压缩所节省的空间

通过去重和压缩所减少的存储量取决于很多因素，包括存储的数据类型以及重复块的数量。较大的磁盘组通常提供更高的去重率。您可以在 vSAN 容量监控中查看“去重和压缩概览”，以检查去重和压缩的结果。



在 vSphere Client 中监控 vSAN 容量时，可以查看“去重和压缩概览”。它显示了有关去重和压缩结果的信息。“之前已使用”空间表示应用去重和压缩之前所需的逻辑空间，而“之后已使用”空间表示应用去重和压缩后所使用的物理空间。“之后已使用”空间还会显示节省的空间量以及去重和压缩率。

去重和压缩率是应用去重和压缩之前存储数据所需的逻辑（“之前已使用”）空间与应用去重和压缩之后所需的物理（“之后已使用”）空间之间的比值。具体来说，此比例是“之前已使用”空间除以“之后已使用”空间。例如，如果“之前已使用”空间是 **3 GB**，而物理“之后已使用”空间是 **1 GB**，则去重和压缩率是 **3 倍**。

在 vSAN 群集上启用去重和压缩后，由于磁盘空间需要回收和重新分配，因此容量更新可能需要几分钟才会反映在容量监控上。

## 去重和压缩设计注意事项

在 vSAN 群集中配置去重和压缩时请考虑以下准则。

- 只有全闪存磁盘组才可以使用去重和压缩。
- 磁盘格式版本 **3.0** 或更高版本支持去重和压缩。
- 必须具有有效的许可证才能在群集上启用去重和压缩。
- 在 vSAN 群集上启用去重和压缩后，所有磁盘组都会通过去重和压缩参与数据缩减。
- vSAN 可以去除每个磁盘组内的重复数据块，但无法跨磁盘组去除重复数据块。
- 去重和压缩所需的容量开销约占原始总容量的 **5%**。
- 策略的对象空间预留必须为 **0%** 或 **100%**。对象空间预留为 **100%** 的策略始终会被接受，但是会降低去重和压缩的效率。

## 在新 vSAN 群集中启用去重和压缩

配置新的 vSAN 全闪存群集时，可以启用去重和压缩。

### 步骤

- 1 导航到一个新的全闪存 vSAN 群集。

## 2 单击配置选项卡。

选项	描述
<b>vSphere Client</b>	<ol style="list-style-type: none"> <li>在“vSAN”下，选择<b>服务</b>并单击<b>配置</b>按钮。</li> <li>在“配置 vSAN”向导的 <b>vSAN 功能</b>页面上，启用“去重和压缩”。</li> <li>（可选）选择<b>允许精简冗余</b>。如果需要，vSAN 会在启用“去重和压缩”的同时降低虚拟机的保护级别。有关更多详细信息，请参见<a href="#">减少 vSAN 群集的虚拟机冗余</a>。</li> </ol>
<b>vSphere Web Client</b>	<ol style="list-style-type: none"> <li>在“vSAN”下，选择<b>常规</b>。</li> <li>单击<b>配置 vSAN</b> 按钮。</li> <li>在群集中配置去重和压缩。 <ol style="list-style-type: none"> <li>在 <b>vSAN 功能</b>页面中，选中“去重和压缩”下的<b>启用</b>复选框。</li> <li>为虚拟机启用精简冗余。请参见<a href="#">减少 vSAN 群集的虚拟机冗余</a>。</li> </ol> </li> <li>在<b>声明磁盘</b>页面中，指定要为 vSAN 群集声明的磁盘。 <ol style="list-style-type: none"> <li>选择要用于容量的闪存设备然后单击<b>针对容量层声明</b>图标 ( )。</li> <li>选择要用作缓存的闪存设备然后单击<b>针对缓存层声明</b>图标 ( )。</li> </ol> </li> </ol>

## 3 完成群集配置。

## 在现有 vSAN 群集中启用去重和压缩

您可以通过编辑现有全闪存 vSAN 群集中的配置参数来启用去重和压缩。

### 前提条件

创建全闪存 vSAN 群集。

### 步骤

- 1 导航到 vSAN 群集。
- 2 单击**配置**选项卡。

选项	描述
<b>vSphere Client</b>	<ol style="list-style-type: none"> <li>在“vSAN”下，选择<b>服务</b>。</li> <li>单击去重和压缩<b>编辑</b>按钮。</li> <li>启用去重和压缩。</li> <li>（可选）选择<b>允许精简冗余</b>。如果需要，vSAN 会在启用去重和压缩的同时降低虚拟机的保护级别。请参见<a href="#">减少 vSAN 群集的虚拟机冗余</a>。</li> </ol>
<b>vSphere Web Client</b>	<ol style="list-style-type: none"> <li>在“vSAN”下，选择<b>常规</b>。</li> <li>在“vSAN 已打开”窗格中，单击<b>编辑</b>按钮。</li> <li>在群集中配置去重和压缩。 <ol style="list-style-type: none"> <li>将去重和压缩设置为<b>已启用</b>。</li> <li>为虚拟机启用精简冗余。请参见<a href="#">减少 vSAN 群集的虚拟机冗余</a>。</li> </ol> </li> </ol>

## 3 单击应用或确定以保存配置更改。

启用去重和压缩时，vSAN 会更新群集的每个磁盘组的磁盘格式。要完成此更改，vSAN 需要撤出磁盘组中的数据，移除磁盘组并使用支持去重和压缩的新格式重新创建磁盘组。

该启用操作不要求迁移虚拟机或使用 DRS。此操作所需的时间取决于群集中的主机数量和数据量。您可以在**任务与事件**选项卡中监控进度。

## 禁用去重和压缩

您可以在 vSAN 群集中禁用去重和压缩。

在 vSAN 群集中禁用去重和压缩后，群集中已用容量的大小可以扩展（根据去重率）。在禁用去重和压缩前，确认群集有足够的容量处理扩展数据的大小。

### 步骤

- 1 导航到 vSAN 群集。
- 2 单击**配置**选项卡。

选项	描述
<b>vSphere Client</b>	<ol style="list-style-type: none"> <li>a 在“vSAN”下，选择<b>服务</b>。</li> <li>b 单击去重和压缩<b>编辑</b>按钮。</li> <li>c 禁用去重和压缩。</li> <li>d （可选）选择<b>允许精简冗余</b>。如果需要，vSAN 会在启用去重和压缩的同时降低虚拟机的保护级别。请参见<a href="#">减少 vSAN 群集的虚拟机冗余</a>。</li> </ol>
<b>vSphere Web Client</b>	<ol style="list-style-type: none"> <li>a 在“vSAN”下，选择<b>常规</b>。</li> <li>b 在“vSAN 已打开”窗格中，单击<b>编辑</b>按钮。</li> <li>c 禁用去重和压缩。 <ol style="list-style-type: none"> <li>1 将磁盘声明模式设置为<b>手动</b>。</li> <li>2 将去重和压缩设置为<b>已禁用</b>。</li> </ol> </li> </ol>

- 3 单击**应用**或**确定**以保存配置更改。

禁用去重和压缩后，vSAN 会更改群集的每个磁盘组上的磁盘格式。它会撤出磁盘组中的数据，移除磁盘组并使用支持去重和压缩的格式重新创建磁盘组。

此操作所需的时间取决于群集中的主机数量和数据量。您可以在**任务与事件**选项卡中监控进度。

## 减少 vSAN 群集的虚拟机冗余

启用去重和压缩时，在某些情况下，可能需要降低虚拟机的保护级别。

启用去重和压缩需要更改磁盘组的格式。要完成此更改，vSAN 需要撤出磁盘组中的数据，移除磁盘组并使用支持去重和压缩的新格式重新创建磁盘组。

在某些环境中，vSAN 群集可能没有足够的资源用于完全撤出磁盘组。此类部署的示例包括在维持完全保护时没有资源用于撤出副本或见证的三节点群集。或者已部署 RAID-5 对象的四节点群集。在后一种情况下，您没有空间来移动部分 RAID-5 带，因为 RAID-5 对象至少需要四个节点。

您仍可以启用去重和压缩并使用“允许精简冗余”选项。此选项可使虚拟机保持运行，但虚拟机可能无法允许虚拟机存储策略中定义的完全故障级别。因此，在去重和压缩的临时更改格式期间，您的虚拟机可能存在数据丢失的风险。vSAN 在格式转换完成之后会还原完全合规性和冗余。

## 在启用去重和压缩的情况下添加或删除磁盘

在启用去重和压缩的情况下向 vSAN 群集添加磁盘时，应当注意某些事项。

- 可在启用去重和压缩的情况下向磁盘组添加容量磁盘。不过，为了有效地去重和压缩，可以创建新磁盘组以增加群集存储容量，而不是添加容量磁盘。
- 从缓存层移除磁盘时，将移除整个磁盘组。在启用去重和压缩的情况下移除缓存层磁盘会触发数据撤出。
- 去重和压缩在磁盘组级别实现。在启用去重和压缩后不能从群集中移除容量磁盘。必须移除整个磁盘组。
- 如果容量磁盘出现故障，整个磁盘组将变得不可用。要解决此问题，请立即识别并替换故障组件。移除故障磁盘组时，请使用“不迁移数据”选项。

## 使用 RAID 5 或 RAID 6 删除编码

您可以使用 RAID 5 或 RAID 6 删除编码防止数据丢失，提高存储效率。删除编码使用更少的存储容量就可以提供与镜像 (RAID 1) 同一级别的数据保护。

RAID 5 或 RAID 6 纠删码最多支持 vSAN 允许数据存储中的两个容量设备出现故障。您可以在具有四个或更多故障域的全闪存群集上配置 RAID 5。您可以在具有六个或更多故障域的全闪存群集上配置 RAID 5 或 RAID 6。

与 RAID 1 镜像相比，RAID 5 或 RAID 6 删除编码需要较少的额外容量即可保护数据。例如，允许的故障数主要级别为 1 时使用 RAID 1 保护的虚拟机需要两倍的虚拟磁盘大小，但使用 RAID 5 只需要 1.33 倍的虚拟磁盘大小。下表是 RAID 1 与 RAID 5 或 RAID 6 的常规比较。

表 6-1. 在不同 RAID 级别存储和保护数据所需的容量

RAID 配置	允许的故障数主要级别	数据大小	所需容量
RAID 1 (镜像)	1	100 GB	200 GB
具有四个故障域的 RAID 5 或 RAID 6 (删除编码)	1	100 GB	133 GB
RAID 1 (镜像)	2	100 GB	300 GB
具有六个故障域的 RAID 5 或 RAID 6 (删除编码)	2	100 GB	150 GB

RAID 5 或 RAID 6 删除编码是可以应用于虚拟机组件的策略属性。要使用 RAID 5，请将容错方法设置为 **RAID-5/6 (擦除编码) - 容量**，将允许的故障数主要级别设置为 1。要使用 RAID 6，请将容错方法设置为 **RAID-5/6 (擦除编码) - 容量**，将允许的故障数主要级别设置为 2。RAID 5 或 RAID 6 擦除编码不支持将允许的故障数主要级别值设置为 3。

要使用 RAID 1，请将容错方法设置为 **RAID-1 (镜像) - 性能**。RAID 1 镜像要求对存储设备执行较少 I/O 操作，以便提供更好的性能。例如，使用 RAID 1 完成群集重新同步所需的时间更少。

---

**注** 在 vSAN 延伸群集中，**RAID-5/6 (纠删码) - 容量容错方法**仅适用于允许的故障数辅助级别。

---

有关配置策略的更多信息，请参见第 3 章，使用 vSAN 策略。

## RAID 5 或 RAID 6 设计注意事项

在 vSAN 群集中配置 RAID 5 或 RAID 6 纠删码时请考虑以下准则。

- RAID 5 或 RAID 6 删除编码只可用于全闪存磁盘组。
- 要支持 RAID 5 或 RAID 6，需要磁盘格式 3.0 或更高版本。
- 必须拥有有效许可证才能在群集上启用 RAID 5/6。
- 通过在 vSAN 群集上启用去重和压缩功能可以节省额外的空间。

## 在 vSAN 群集上使用加密

可以使用静态数据加密保护 vSAN 群集中的数据。

vSAN 可以执行静态数据加密。在对数据执行所有其他处理（例如，去重）后对数据加密。静态数据加密可保护存储设备上的数据，以防设备从群集中移除的情况。

在 vSAN 群集上使用加密需要做好一些准备工作。设置好环境后，即可在 vSAN 群集上启用加密。

vSAN 加密需要外部密钥管理服务器 (KMS)、vCenter Server 系统和 ESXi 主机。vCenter Server 将从外部 KMS 请求加密密钥。KMS 生成并存储密钥，然后 vCenter Server 从 KMS 获取密钥 ID 并将其分发给 ESXi 主机。

vCenter Server 不会存储 KMS 密钥，只会保留密钥 ID 的列表。

本章讨论了以下主题：

- [vSAN 加密的工作原理](#)
- [vSAN 加密的设计注意事项](#)
- [设置 KMS 群集](#)
- [在新的 vSAN 群集上启用加密](#)
- [生成新的加密密钥](#)
- [在现有 vSAN 群集上启用 vSAN 加密](#)
- [vSAN 加密和核心转储](#)

### vSAN 加密的工作原理

启用加密时，vSAN 会加密 vSAN 数据存储中的所有内容。由于加密了所有文件，因此所有虚拟机及其相应的数据将受到保护。只有具备加密特权的管理员才能执行加密和解密任务。

vSAN 使用加密密钥，如下所示：

- vCenter Server 从 KMS 请求 AES-256 密钥加密密钥 (KEK)。vCenter Server 仅存储 KEK 的 ID，而不存储密钥本身。
- ESXi 主机使用符合行业标准的 AES-256 XTS 模式加密磁盘数据。每个磁盘都有随机生成的不同数据加密密钥 (DEK)。
- 每个 ESXi 主机使用 KEK 加密其 DEK，并将加密的 DEK 存储在磁盘上。主机不会将 KEK 存储在磁盘上。如果主机重新引导，则将从 KMS 请求具有相应 ID 的 KEK。然后，主机可以根据需要解密其 DEK。



- 主机密钥用于加密核心转储，而非数据。同一群集中的所有主机使用相同的主机密钥。收集支持包时，会生成随机密钥以便重新加密核心转储。您可以指定一个用于加密随机密钥的密码。

主机重新引导时，不会挂载其磁盘组，直到收到 KEK。完成此过程可能需要几分钟或更长时间。您可以在 vSAN Health Service 的 **物理磁盘 > 软件状态运行状况** 下监控磁盘组的状态。

## vSAN 加密的设计注意事项

使用 vSAN 加密时，请考虑以下准则。

- 请勿在计划加密的同一 vSAN 数据存储上部署 KMS 服务器。
- 加密会占用大量 CPU。AES-NI 可以大幅提高加密性能。在您的 BIOS 中启用 AES-NI。
- 延伸群集中的见证主机不会参与 vSAN 加密。仅元数据存储见证主机上。
- 建立有关核心转储的策略。核心转储会进行加密，因为它们可能包含敏感信息（例如密钥）。如果要解密核心转储，请谨慎处理其敏感信息。ESXi 核心转储可能包含用于 ESXi 主机及其数据的密钥。
  - 在收集 vm-support 包时，始终应使用密码。通过 vSphere Client 或使用 vm-support 命令生成支持包时，您可以指定密码。  
密码会重新加密使用内部密钥的核心转储，以便使用基于该密码的密钥。您可以在以后使用该密码来解密支持包中可能包含的任何加密核心转储。未加密的核心转储或日志不受影响。
  - 在创建 vm-support 包期间指定的密码不会保留在 vSphere 组件中。您需要负责跟踪支持包的密码。

## 设置 KMS 群集

密钥管理服务 (KMS) 群集提供了可用于加密 vSAN 数据存储的密钥。

在加密 vSAN 数据存储之前，必须先设置 KMS 群集以支持加密。此任务包括将 KMS 添加到 vCenter Server 以及与 KMS 建立信任。vCenter Server 从 KMS 群集置备加密密钥。

KMS 必须支持密钥管理互操作协议 (KMIP) 1.1 标准。

## 将 KMS 添加到 vCenter Server

可以从 vSphere Client 将密钥管理服务 (KMS) 添加到您的 vCenter Server 系统。

vCenter Server 在您添加首个 KMS 实例时创建 KMS 群集。如果在两个或多个 vCenter Server 上配置 KMS 群集，请确保使用相同的 KMS 群集名称。

**注** 请勿在计划加密的 vSAN 群集上部署 KMS 服务器。如果出现故障，vSAN 群集中的主机必须与 KMS 通信。

- 添加 KMS 时，系统会提示您将此群集设置为默认群集。您稍后可以明确更改此默认群集。
- vCenter Server 创建第一个群集后，可以将来自相同供应商的 KMS 实例添加到群集，然后配置所有 KMS 实例以在这些实例之间同步密钥。使用您的 KMS 供应商提供的方法。
- 您可以设置只有一个 KMS 实例的群集。

- 如果您的环境支持来自不同供应商的 KMS 解决方案，则您可以添加多个 KMS 群集。

#### 前提条件

- 确认密钥服务器位于 vSphere 兼容性列表中，且符合 KMIP 1.1。
- 确认您具有所需特权：**Cryptographer.ManageKeyServers**
- 不支持仅使用 IPv6 地址连接到 KMS。
- 不支持通过需要用户名或密码的代理服务器连接到 KMS。

#### 步骤

- 1 登录到 vCenter Server。
- 2 浏览清单列表，然后选择 vCenter Server 实例。
- 3 依次单击**配置**和**密钥管理服务器**。
- 4 单击**添加**，在向导中指定 KMS 信息，然后单击**添加**。

选项	值
<b>KMS 群集</b>	选择 <b>创建新群集</b> 以创建一个新群集。如果存在一个群集，您可以选择该群集。
<b>群集名称</b>	KMS 群集的名称。如果 vCenter Server 实例不可用，您可以使用此名称连接到 KMS。
<b>服务器别名</b>	KMS 的别名。如果 vCenter Server 实例不可用，您可以使用此别名连接到 KMS。
<b>服务器地址</b>	KMS 的 IP 地址或 FQDN。
<b>服务器端口</b>	vCenter Server 连接到 KMS 的端口。
<b>代理地址</b>	连接到 KMS 的可选代理地址。
<b>代理端口</b>	连接到 KMS 的可选代理端口。
<b>用户名</b>	一些 KMS 供应商允许用户通过指定用户名和密码来隔离不同用户或组使用的加密密钥。仅当您的 KMS 支持此功能且您准备使用时指定用户名。
<b>密码</b>	一些 KMS 供应商允许用户通过指定用户名和密码来隔离不同用户或组使用的加密密钥。仅当您的 KMS 支持此功能且您准备使用时指定密码。

## 通过交换证书来建立信任连接

将 KMS 添加到 vCenter Server 系统后，可以建立信任连接。具体过程取决于 KMS 接受的证书和公司策略。

#### 前提条件

添加 KMS 群集。

#### 步骤

- 1 导航到 vCenter Server。
- 2 单击**配置**，然后选择**密钥管理服务器**。
- 3 选择要与之建立信任连接的 KMS 实例。
- 4 单击与 **KMS 建立信任**。

- 5 选择适用于服务器的选项，然后完成各个步骤。

选项	请参见
根 CA 证书	使用“根 CA 证书”选项建立信任连接。
证书	使用“证书”选项建立信任连接。
新建证书签名请求	使用“新建证书签名请求”选项建立信任连接。
上载证书和私有密钥	使用“上载证书和私有密钥”选项建立信任连接。

### 使用“根 CA 证书”选项建立信任连接

某些 KMS 供应商（例如 SafeNet）要求将根 CA 证书上载到 KMS。随后，此 KMS 即会信任根 CA 签名的所有证书。

vSphere 虚拟机加密使用的根 CA 证书为自签名证书，它存储在 vCenter Server 系统上 VMware Endpoint 证书存储 (VECS) 的独立库中。

**注** 仅当要替换现有证书时才生成根 CA 证书。如果执行此操作，根 CA 签名的其他证书将变为无效。可以在此工作流程中生成新的根 CA 证书。

#### 步骤

- 1 导航到 vCenter Server。
- 2 单击**配置**，然后选择**密钥管理服务器**。
- 3 选择要与之建立信任连接的 KMS 实例。
- 4 选择 **根 CA 证书**，然后单击**确定**。

“下载根 CA 证书”对话框将填充 vCenter Server 用于加密的根证书。此证书存储在 VECS 中。

- 5 将证书复制到剪贴板，或将证书作为文件下载。
- 6 按照您的 KMS 供应商的说明，将证书上载到其系统中。

**注** 某些 KMS 供应商（例如 SafeNet）要求 KMS 供应商重新启动 KMS 以发现上载的根证书。

#### 后续步骤

完成证书交换。请参见[完成信任设置](#)。

### 使用“证书”选项建立信任连接

某些 KMS 供应商（例如 Vormetric）要求将 vCenter Server 证书上载到 KMS。上载后，KMS 便会接受来自具有该证书的系统的流量。

vCenter Server 将生成证书以保护与 KMS 的连接。证书存储在 vCenter Server 系统上 VMware Endpoint 证书存储 (VECS) 的独立密钥库中。

#### 步骤

- 1 导航到 vCenter Server。
- 2 单击**配置**，然后选择**密钥管理服务器**。

- 3 选择要与之建立信任连接的 KMS 实例。
- 4 选择**证书**，然后单击**确定**。

“下载证书”对话框将填充 vCenter Server 用于加密的根证书。此证书存储在 VECS 中。

---

**注** 除非您要替换现有证书，否则请勿生成新证书。

---

- 5 将证书复制到剪贴板，或将其作为文件下载。
- 6 按照您的 KMS 供应商的说明，将证书上载到 KMS。

#### 后续步骤

完成信任关系。请参见[完成信任设置](#)。

#### 使用“新建证书签名请求”选项建立信任连接

某些 KMS 供应商（例如 Thales）要求 vCenter Server 生成证书签名请求 (CSR) 并将该 CSR 发送到 KMS。KMS 将签署 CSR 并返回已签名证书。可以将已签名证书上载到 vCenter Server。

使用**新建证书签名请求**选项的过程分为两步。首先，生成 CSR 并将其发送给 KMS 供应商。然后，将从 KMS 供应商收到的已签名证书上载到 vCenter Server。

#### 步骤

- 1 导航到 vCenter Server。
- 2 单击**配置**，然后选择**密钥管理服务器**。
- 3 选择要与之建立信任连接的 KMS 实例。
- 4 选择**新建证书签名请求**，然后单击**确定**。
- 5 在该对话框中，将文本框中的完整证书复制到剪贴板，或将其作为文件下载，然后单击**确定**。  
仅当您要明确生成 CSR 时才使用该对话框中的**生成新的 CSR** 按钮。使用该选项会导致基于旧 CSR 的所有签名证书变得无效。
- 6 按照 KMS 供应商的说明提交 CSR。
- 7 收到来自 KMS 供应商的签名证书时，再次单击**密钥管理服务器**，然后再次选择**新建证书签名请求**。
- 8 将签名证书粘贴到底部文本框中，或单击**上载文件**并上载文件，然后单击**确定**。

#### 后续步骤

完成信任关系。请参见[完成信任设置](#)。

#### 使用“上载证书和私有密钥”选项建立信任连接

某些 KMS 供应商（例如 HyTrust）要求您将 KMS 服务器证书和私有密钥上载到 vCenter Server 系统。

某些 KMS 供应商会针对连接生成证书和私有密钥，并为您提供这些内容。上载这些文件之后，KMS 将信任您的 vCenter Server 实例。

### 前提条件

- 向 KMS 供应商请求证书和私有密钥。这些文件为 PEM 格式的 X509 文件。

### 步骤

- 1 导航到 vCenter Server。
- 2 单击**配置**，然后选择**密钥管理服务器**。
- 3 选择要与之建立信任连接的 KMS 实例。
- 4 选择**上传证书和私有密钥**，然后单击**确定**。
- 5 将从 KMS 供应商收到的证书粘贴到顶部文本框中，或单击**上传文件**上传证书文件。
- 6 将密钥文件粘贴到底部文本框中，或单击**上传文件**上传密钥文件。
- 7 单击**确定**。

### 后续步骤

完成信任关系。请参见[完成信任设置](#)。

## 设置默认 KMS 群集

如果您未将第一个群集设置为默认群集，或者您的环境使用多个群集且您移除了默认群集，则必须设置默认 KMS 群集。

### 前提条件

最佳做法是，验证**密钥管理服务器**选项卡中的“连接状态”是否显示“正常”和一个绿色复选标记。

### 步骤

- 1 导航到 vCenter Server 系统。
- 2 单击**配置**选项卡，然后单击**更多**下面的**密钥管理服务器**。
- 3 选择群集并单击**将 KMS 群集设置为默认值**。  
请勿选择服务器。设置默认值的菜单仅可用于群集。
- 4 单击**是**。  
相应群集名称旁将出现 default 字样。

## 完成信任设置

除非**添加服务器**对话框提示您信任 KMS，否则您在完成证书交换后必须以显式方式建立信任。

您可以完成信任设置，即：通过信任 KMS 或上传 KMS 证书使 vCenter Server 信任 KMS。您有两个选项：

- 通过使用**刷新 KMS 证书**选项以显式方式信任证书。

- 通过使用**上载 KMS 证书**选项，可以将 KMS 叶证书或 KMS CA 证书上载到 vCenter Server。

**注** 如果上载根 CA 证书或中间 CA 证书，则 vCenter Server 将信任 CA 签发的所有证书。出于强安全性，请上载叶证书或 KMS 供应商控制的中间 CA 证书。

#### 步骤

- 1 导航到 vCenter Server。
- 2 单击**配置**，然后选择**密钥管理服务器**。
- 3 选择要与之建立信任连接的 KMS 实例。
- 4 要建立信任关系，请刷新或上载 KMS 证书。

选项	操作
刷新 KMS 证书	<ol style="list-style-type: none"> <li>a 单击<b>所有操作</b>，然后选择<b>刷新 KMS 证书</b>。</li> <li>b 在显示的对话框中，单击<b>信任</b>。</li> </ol>
上载 KMS 证书	<ol style="list-style-type: none"> <li>a 单击<b>所有操作</b>，然后选择<b>上载 KMS 证书</b>。</li> <li>b 在显示的对话框中，单击<b>上载文件</b>，上载证书文件，然后单击<b>确定</b>。</li> </ol>

## 在新的 vSAN 群集上启用加密

配置新的 vSAN 群集时，可以启用加密。

#### 前提条件

- 所需特权：
  - 主机.清单.编辑群集
  - 密码员.管理加密策略
  - 密码员.管理 KMS
  - 密码员.管理密钥
- 您必须设置 KMS 群集并在 vCenter Server 和 KMS 之间建立信任连接。

#### 步骤

- 1 导航到现有群集。
- 2 单击**配置**选项卡。
- 3 在“vSAN”下，选择**常规**，并单击“加密”的**编辑**按钮。
- 4 在 **vSAN 服务**对话框中，启用**加密**，然后选择 KMS 群集。

**注** 确保已取消选中**使用前清除磁盘**复选框，除非您要在加密时擦除存储设备上的现有数据。

- 5 完成群集配置。

已在 vSAN 群集上启用静态数据加密。vSAN 将加密添加到 vSAN 数据存储的所有数据。

## 生成新的加密密钥

如果密钥到期或信誉受到损害，可以生成新的加密密钥。

为 vSAN 群集生成新的加密密钥时，以下选项可用。

- 如果您生成新的 KEK，vSAN 群集中的所有主机将收到来自 KMS 的新的 KEK。已使用新的 KEK 重新加密每个主机的 DEK。
- 如果您选择使用新的密钥重新加密所有数据，将生成新的 KEK 和新的 DEK。需要执行回滚磁盘重新格式化操作才能重新加密数据。

### 前提条件

- 所需特权：
  - 主机.清单.编辑群集
  - 密码员.管理密钥
- 您必须设置 KMS 群集并在 vCenter Server 和 KMS 之间建立信任连接。

### 步骤

- 1 导航到 vSAN 主机群集。
- 2 单击配置选项卡。
- 3 在“vSAN”下，选择服务。
- 4 单击生成新的加密密钥。
- 5 要生成新的 KEK，请单击应用。将使用新 KEK 重新加密 DEK。
  - 要生成新的 KEK 和新的 DEK，并重新加密 vSAN 群集中的所有数据，请选中以下复选框：**同时使用新的密钥重新加密存储器上的所有数据。**
  - 如果 vSAN 群集的资源有限，请选中**允许精简冗余**复选框。如果允许减少冗余，执行磁盘重新格式化操作过程中数据可能会处于风险中。

## 在现有 vSAN 群集上启用 vSAN 加密

您可以通过编辑现有 vSAN 群集中的配置参数来启用加密。

### 前提条件

- 所需特权：
  - 主机.清单.编辑群集
  - 密码员.管理加密策略
  - 密码员.管理 KMS
  - 密码员.管理密钥

- 您必须设置 KMS 群集并在 vCenter Server 和 KMS 之间建立信任连接。
- 群集的磁盘声明模式必须设置为手动。

#### 步骤

- 1 导航到 vSAN 主机群集。
- 2 单击配置选项卡。
- 3 在“vSAN”下，选择服务。
- 4 单击“加密”的编辑按钮。
- 5 在“vSAN 服务”对话框中，启用加密，然后选择 KMS 群集。
- 6 （可选）如果群集中的存储设备包含敏感数据，请选中使用前清除磁盘。

此设置将引导 vSAN 在加密时擦除存储设备上的现有数据。此选项会增加处理每个磁盘的时间，因此请勿选择该选项，除非磁盘上存在不需要的数据。

- 7 单击应用。

vSAN 加密 vSAN 数据存储中的所有数据时，将对所有磁盘组执行回滚重新格式化操作。

## vSAN 加密和核心转储

如果您的 vSAN 群集使用加密，且 ESXi 主机发生错误，则将对生成的核心转储进行加密以保护客户数据。还会对 vm-support 软件包中包含的核心转储进行加密。

---

**注** 核心转储可能包含敏感信息。处理核心转储时，请遵循您组织的数据安全和隐私权政策。

---

## ESXi 主机上的核心转储

当 ESXi 主机崩溃时，会生成加密核心转储，然后主机重新引导。核心转储将使用 ESXi 密钥缓存中的主机密钥进行加密。后续操作取决于若干因素。

- 在大多数情况下，重新引导后 vCenter Server 将从 KMS 检索主机密钥并尝试将该密钥推送到 ESXi 主机。如果此操作成功，您可以生成 vm-support 软件包，并对核心转储进行解密或重新加密。
- 如果 vCenter Server 无法连接到 ESXi 主机，您也许可以从 KMS 检索密钥。
- 如果主机使用自定义密钥，且该密钥不同于 vCenter Server 推送到主机的密钥，您将无法处理核心转储。请避免使用自定义密钥。

## 核心转储和 vm-support 软件包

当您遇到严重错误而联系 VMware 技术支持时，您的支持代表通常会要求您生成 vm-support 软件包。该软件包包含日志文件和其他信息，包括核心转储。如果支持代表无法通过查看日志文件和其他信息解决问题，您可以解密核心转储以提供相关信息。请遵循您组织的安全和隐私权政策，以保护主机密钥等敏感信息。



## vCenter Server 系统上的核心转储

vCenter Server 系统上的核心转储未加密。vCenter Server 已包含可能的敏感信息。请至少确保运行 vCenter Server 的 Windows 系统或 vCenter Server Appliance 受保护。您还可以考虑关闭 vCenter Server 系统的核心转储。日志文件中的其他信息可以帮助确定问题所在。

## 收集加密 vSAN 群集中 ESXi 主机的 vm-support 软件包

如果在 vSAN 群集上启用了加密，将对 vm-support 软件包中的任何核心转储进行加密。您可以收集该软件包，如果随后希望解密核心转储，则可以指定一个密码。

vm-support 软件包中包含日志文件、核心转储文件等。

### 前提条件

通知您的支持代表，已在 vSAN 群集中启用加密。支持代表可能会要求您解密核心转储以提取相关信息。

**注** 核心转储可以包含敏感信息。请遵循您组织的安全和隐私权政策，以保护主机密钥等敏感信息。

### 步骤

- 1 使用基于 Flex 的 vSphere Web Client 登录到 vCenter Server。
- 2 单击**主机和群集**，然后右键单击 ESXi 主机。
- 3 选择**导出系统日志**。
- 4 在对话框中，选择**已加密核心转储的密码**，然后指定并确认密码。
- 5 其他选项保留默认值，或者根据 VMware 技术支持要求进行更改，然后单击**完成**。
- 6 指定该文件的位置。
- 7 如果支持代表要求您解密 vm-support 软件包中的核心转储，请登录任一 ESXi 主机，然后按照以下步骤操作。
  - a 登录 ESXi 并连接到 vm-support 软件包所在的目录。  
文件名采用 **esx.date\_and\_time.tgz** 模式。
  - b 确保该目录具有足够的空间来存储该软件包、未压缩的软件包和重新压缩的软件包，或者移动该软件包。
  - c 将该软件包解压缩到本地目录中。

```
vm-support -x *.tgz .
```

生成的文件层次结构可能包含 ESXi 主机的核心转储文件（通常位于 `/var/core` 中），并且可能包含虚拟机的多个核心转储文件。

- d 单独解密每个加密核心转储文件。

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdump decryptedZdump
```

*vm-support-incident-key-file* 是位于该目录顶层的事件密钥文件。

*encryptedZdump* 是加密核心转储文件的名称。

*decryptedZdump* 是该命令生成的文件名。请确保该名称类似于 *encryptedZdump* 名称。

- e 提供在创建 **vm-support** 软件包时指定的密码。
- f 移除加密核心转储，然后重新压缩该软件包。

```
vm-support --reconstruct
```

- 8 移除任何包含保密信息的文件。

## 解密或重新加密已加密核心转储

您可以使用 **crypto-util** CLI 解密或重新加密 ESXi 主机上的已加密核心转储。

您可以自行解密并检查 **vm-support** 软件包中的核心转储。核心转储可能包含敏感信息。请遵循您组织的安全和隐私权政策，以保护主机密钥等敏感信息。

有关重新加密核心转储的详细信息以及 **crypto-util** 的其他功能，请参见命令行帮助。

**注** **crypto-util** 面向高级用户。

### 前提条件

用于加密核心转储的 ESXi 主机密钥必须在生成核心转储的 ESXi 主机上可用。

### 步骤

- 1 直接登录到发生核心转储的 ESXi 主机。  
如果 ESXi 主机处于锁定模式，或者如果 SSH 访问已禁用，您可能需要先启用访问。
- 2 确定核心转储是否已加密。

选项	描述
监控程序核心转储	<code>crypto-util envelope describe vmmcores.ve</code>
zdump 文件	<code>crypto-util envelope describe --offset 4096 zdumpFile</code>

### 3 根据相应的类型解密核心转储。

选项	描述
监控程序核心转储	<code>crypto-util envelope extract vmmcores.ve vmmcores</code>
zdump 文件	<code>crypto-util envelope extract --offset 4096 zdumpEncrypted zdumpUnencrypted</code>

# 升级 vSAN 群集

升级 vSAN 的过程分为多个阶段，必须按照此处介绍的顺序执行每个阶段的升级步骤。

在尝试升级之前，请确保您清楚地了解完整的升级过程，以确保顺畅、无中断地升级。如果不熟悉常规的 vSphere 升级步骤，应先查看《vSphere 升级》文档。

---

**注** 如果不按照此处介绍的顺序执行升级任务，将会导致数据丢失和群集故障。

---

vSAN 群集升级任务按以下顺序进行。

- 1 升级 vCenter Server。请参见《vSphere 升级》文档。
- 2 升级 ESXi 主机。请参见[升级 ESXi 主机](#)。有关迁移和准备 ESXi 主机进行升级的信息，请参见《vSphere 升级》文档。
- 3 升级 vSAN 磁盘格式。升级磁盘格式是可选操作，但是为获得最佳效果，请升级对象以使用最新版本。磁盘格式会向 vSAN 的完整功能集公开您的环境。请参见[使用 RVC 升级 vSAN 磁盘格式](#)。

本章讨论了以下主题：

- [升级 vSAN 之前](#)
- [升级 vCenter Server。](#)
- [升级 ESXi 主机](#)
- [关于 vSAN 磁盘格式](#)
- [验证 vSAN 群集升级](#)
- [使用 RVC 升级命令选项](#)
- [针对 vSphere Update Manager 的 vSAN 内部版本建议](#)

## 升级 vSAN 之前

计划和设计升级以免升级失败。尝试升级 vSAN 之前，确认您的环境满足 vSphere 硬件和软件要求。

## 升级必备条件

注意可能会延迟整个升级过程的各个方面。有关准则和最佳做法，请参见《vSphere 升级》文档。

将群集升级到 vSAN 6.7.1 之前，请查看主要要求。

表 8-1. 升级必备条件

升级必备条件	描述
软件、硬件、驱动程序、固件和存储 I/O 控制器	确认 vSAN 6.7.1 支持您计划使用的软件和硬件组件、驱动程序、固件和存储 I/O 控制器。受支持的项目在《VMware 兼容性指南》网站上已列出，网址为 <a href="http://www.vmware.com/resources/compatibility/search.php">http://www.vmware.com/resources/compatibility/search.php</a> 。
vSAN 版本	确认使用的是最新版本的 vSAN。不能从测试版升级到 vSAN 6.7.1。从测试版升级时，必须全新部署 vSAN。
磁盘空间	确认有足够的可用空间来完成软件版本升级。vCenter Server 安装所需的磁盘存储量取决于您的 vCenter Server 配置。有关升级 vSphere 所需的磁盘空间的准则，请参见《vSphere 升级》文档。
vSAN 磁盘格式	<p>确认您有足够的容量可用于升级磁盘格式。如果可用空间小于最大磁盘组的已用容量，而具有可用空间的磁盘组不是正在转换的磁盘组，则必须选择<b>允许精简冗余</b>作为数据迁移选项。</p> <p>例如，群集中最大的磁盘组具有 10 TB 的物理容量，但仅消耗了 5 TB。那么，群集中的其他磁盘组（正在迁移的磁盘组除外）上需要有另外 5 TB 空闲容量。升级 vSAN 磁盘格式时，请确认主机不处于维护模式。当 vSAN 群集的任何成员主机进入维护模式后，群集容量将自动减少。该成员主机不再向群集提供存储，并且该主机上的容量不可用于数据。有关各种撤出模式的信息，请参见<a href="#">将 vSAN 群集的成员置于维护模式</a>。</p>
vSAN 主机	<p>确认已将 vSAN 主机置于维护模式并选择了<b>确保数据可访问性</b>或<b>撤出所有数据</b>选项。</p> <p>可以使用 vSphere Update Manager 自动操作和测试升级过程。但是，使用 vSphere Update Manager 升级 vSAN 时，默认撤出模式为<b>确保数据可访问性</b>。使用<b>确保数据可访问性</b>模式时，您的数据不受保护，如果在升级 vSAN 时出现故障，可能会意外丢失数据。但是，<b>确保数据可访问性</b>模式的速度比<b>撤出全部数据</b>模式快，因为您无需将所有数据移至群集中的其他主机。有关各种撤出模式的信息，请参见<a href="#">将 vSAN 群集的成员置于维护模式</a>。</p>
虚拟机	确认您已备份虚拟机。

## 建议

部署 ESXi 主机与 vSAN 一起使用时，请考虑以下建议：

- 如果为 ESXi 主机配置的内存容量为 512 GB 或更少，则使用 SATADOM、SD、USB 或硬盘设备作为安装介质。
- 如果为 ESXi 主机配置的内存容量大于 512 GB，则使用单独的磁盘或闪存设备作为安装介质。如果使用单独的设备，请确认 vSAN 未声明该设备。
- 从 SATADOM 设备引导 vSAN 主机后，必须使用单层单元 (SLC) 设备，并且引导设备的大小至少必须为 16 GB。
- 为确保硬件符合 vSAN 的要求，请参阅《vSAN 规划和部署》中的“vSAN 硬件要求”。

在 vSAN 6.5 及更高版本中，可以调整 vSAN 群集中 ESXi 主机的引导大小要求。有关详细信息，请参见 VMware 知识库文章，网址为 <http://kb.vmware.com/kb/2147881>。

## 升级双主机群集或延伸群集中的见证主机

双主机群集或延伸群集中的见证主机位于 vSAN 群集外部，但由同一个 vCenter Server 管理。升级见证主机时，可以使用与升级 vSAN 数据主机相同的过程。

所有数据主机均升级并退出维护模式后再升级见证主机。

使用 vSphere Update Manager 并行升级主机可能会导致并行升级见证主机与某个数据主机。要避免升级问题，请配置 vSphere Update Manager，以便其不会并行升级见证主机与数据主机。

## 升级 vCenter Server。

vSAN 升级的首个要执行的任务是常规的 vSphere 升级，包括升级 vCenter Server 和 ESXi 主机。

VMware 支持在 64 位系统上从 vCenter Server 4.x、vCenter Server 5.0.x、vCenter Server 5.1.x 和 vCenter Server 5.5 到 vCenter Server 6.0 和更高版本的就地升级。vCenter Server 升级包括数据库架构升级和 vCenter Server 升级。您可以使用其他计算机升级到 vCenter Server，而不是进行就地升级。有关详细说明和各种升级选项，请参见 vSphere 升级文档。

## 升级 ESXi 主机

升级 vCenter Server 后，vSAN 群集升级的下一任务是升级 ESXi 主机以使用当前版本。

如果 vSAN 群集中具有多个主机，并且使用 vSphere Update Manager 升级这些主机，则默认撤出模式为**确保数据可访问性**。使用此模式时，如果在升级 vSAN 时遇到故障，可能会丢失数据。有关在撤出模式下运行的信息，请参见[将 vSAN 群集的成员置于维护模式](#)

有关使用 vSphere Update Manager 的信息，请参见文档网站，网址为：

[https://www.vmware.com/support/pubs/vum\\_pubs.html](https://www.vmware.com/support/pubs/vum_pubs.html)。

尝试升级 ESXi 主机之前，查看《vSphere 升级》文档中所述的最佳做法。VMware 提供了多个 ESXi 升级选项。选择最适用于您要升级的主机类型的升级选项。有关各个升级选项的更多信息，请参见《vSphere 升级》文档。

### 前提条件

- 确认您拥有足够的磁盘空间来升级 ESXi 主机。有关磁盘空间要求的准则，请参见《vSphere 升级》文档。
- 确认使用的是最新版本的 ESXi。您可以从 VMware 产品下载网站下载最新的 ESXi 安装程序，网址为：<https://my.vmware.com/web/vmware/downloads>。
- 确认使用的是最新版本的 vCenter Server。
- 验证网络配置、Storage I/O 控制器、存储设备和备份软件的兼容性。
- 确认您已备份虚拟机。
- 使用 Distributed Resource Scheduler (DRS) 防止虚拟机在升级过程中停机。确认每个虚拟机的自动化级别都已设置为**全自动**模式，以便在主机进入维护模式后，帮助 DRS 迁移虚拟机。或者，也可以关闭所有虚拟机的电源或执行手动迁移。

## 步骤

- 1 将要升级的主机置于维护模式。

升级途径必须从 vSAN 群集中的 ESXi 5.5 或更高版本的主机开始。

- a 右键单击主机，然后选择**维护模式 > 进入维护模式**。
- b 根据您的要求，选择**确保数据可访问性**或**撤出全部数据**撤出模式，并等待主机进入维护模式。

如果使用 vSphere Update Manager 升级主机，或者使用三主机群集，则可用的默认撤出模式为**确保数据可访问性**。此模式比比**撤出全部数据**模式快。但是，**确保数据可访问性**模式不会完全保护您的数据。在故障期间，您的数据可能有风险，并且您可能会遇到停机和意外丢失数据。

- 2 将软件上载到 ESXi 主机的数据存储，并验证数据存储内目录中的文件是否可用。例如，您可以将软件上载到 `/vmfs/volumes/<datastore>/VMware-ESXi-6.0.0-1921158-depot.zip`。

- 3 运行 `esxcli` 命令 `install -d /vmfs/volumes/53b536fd-34123144-8531-00505682e44d/depot/VMware-ESXi-6.0.0-1921158-depot.zip --no-sig-check`。使用 `esxcli` 软件 VIB 运行此命令。

成功安装 ESXi 主机后，会看到以下消息：

更新已成功完成，但需要重新引导系统以使更改生效 (The update completed successfully, but the system needs to be rebooted for the changes to be effective)。

- 4 手动重新启动 ESXi 主机。
  - a 导航到清单中的 ESXi 主机。
  - b 右键单击该主机，选择**电源 > 重新引导**，并单击**是**确认，然后等待主机重新启动。
  - c 右键单击该主机，选择**连接 > 断开连接**，然后选择**连接 > 连接**以重新连接到主机。

要升级群集中的其他主机，请为每个主机重复该步骤。

如果 vSAN 群集中具有多个主机，则可以使用 vSphere Update Manager 升级剩余主机。

- 5 退出维护模式。

## 后续步骤

- 1 (可选) 升级 vSAN 磁盘格式。请参见[使用 RVC 升级 vSAN 磁盘格式](#)。
- 2 验证主机许可证。大多数情况下，必须重新应用主机许可证。有关应用主机许可证的更多信息，请参见《vCenter Server 和主机管理》文档。
- 3 (可选) 通过使用 vSphere Client 或 vSphere Update Manager 升级主机上的虚拟机。

## 关于 vSAN 磁盘格式

磁盘格式升级是可选操作。如果您使用以前版本的磁盘格式，您的 vSAN 群集也会继续顺利运行。

为获得最佳效果，请升级对象以使用最新的磁盘格式。最新的磁盘格式提供了 vSAN 的完整功能集。

磁盘格式升级所耗用时间因磁盘组大小而异，因为一次只升级一个磁盘组。升级每个磁盘组时，每个设备的所有数据都将撤出且磁盘组也将从 vSAN 群集中移除。然后，将该磁盘组添加回使用新磁盘格式的 vSAN。

**注** 升级磁盘格式后，无法回滚主机上的软件，也无法将某些旧主机添加到群集。

启动磁盘格式升级后，vSAN 会执行多个操作，可以在“重新同步组件”页面中监控这些操作。下表汇总了磁盘格式升级期间发生的各个过程。

**表 8-2. 升级进度**

完成百分比	描述
0%-5%	群集检查。检查群集组件，为升级做好准备。此过程需要几分钟。 vSAN 确认不存在任何可阻止升级完成的未解决问题。 <ul style="list-style-type: none"> <li>■ 所有主机均已连接。</li> <li>■ 所有主机的软件版本均正确无误。</li> <li>■ 所有磁盘均正常运行。</li> <li>■ 所有对象均可访问。</li> </ul>
5%-10%	磁盘组升级。vSAN 将执行首次磁盘升级，但不会迁移任何数据。此过程需要几分钟。
10%-15%	对象重新对齐。vSAN 将修改所有对象的布局，确保对象正确对齐。此过程对于具有少量快照的小型系统而言可能只需要几分钟。但对于具有大量快照、大量碎片写入内容和大量未对齐对象的大型系统而言可能需要数小时或甚至数天。
15% - 95%	磁盘组移除和重新格式化。每个磁盘组都将经历从群集中移除、重新格式化、添加回群集三个步骤。此过程所需的时间因分配的兆字节数和系统负载而异。达到或接近其 I/O 容量的系统传输较缓慢。
95% - 100%	最终对象版本升级。将对象转换为新磁盘格式以及重新同步已完成。此过程所需的时间因已用空间量和是否选择 <b>允许精简冗余</b> 选项而异。

升级过程中，可以通过“重新同步组件”页面监控升级过程。请参见《vSAN 监控和故障排除》中的“监控 vSAN 群集中的重新同步任务”。您还可以使用 RVC 命令 (`vsan.upgrade_status <cluster>`) 来监控升级。按 **Ctrl+C** 之前，请使用可选的 `-r <seconds>` 标记定期刷新升级状态。每次刷新之间允许的最小秒数为 60 秒。

可以在状态栏的“近期任务”窗格中监控其他升级任务，例如，设备移除和升级。

升级磁盘格式时，请注意以下事项：

- 如果升级包含三个主机的群集，并希望执行完全撤出，对于**允许的故障数主要级别**大于 0（零）的对象，撤出将失败。三主机群集无法只使用两个主机的资源重新保护完全撤出的磁盘组。例如，当**允许的故障数主要级别**设置为 1 时，vSAN 需要三个保护组件（两个镜像、一个见证），其中每个保护组件位于不同的主机上。

对于三主机群集，必须选择**确保数据可访问性**撤出模式。如果处于此模式，任何硬件故障都可能会导致数据丢失。

此外，还必须确保有足够的可用空间。该空间必须等于最大磁盘组的逻辑耗用容量。该容量必须由正在迁移的磁盘组之外的磁盘组提供。



- 升级三主机群集或升级资源有限的群集时，允许虚拟机在精简冗余模式下运行。运行 **RVC** 命令选项：**vsan.ondisk\_upgrade --allow-reduced-redundancy**。
- 使用**--allow-reduced-redundancy** 命令选项意味着某些虚拟机在迁移期间可能不允许出现故障。允许的故障数减少还可能导致数据丢失。**vSAN** 在升级完成之后会还原完全合规性和冗余。升级期间，虚拟机的合规性状态及其冗余临时处于不合规状态。完成升级以及所有重新构建任务之后，虚拟机将恢复合规状态。
- 在升级过程中，请勿移除任何主机或断开主机连接，也不要将主机置于维护模式。这些操作可能会导致升级失败。

有关 **RVC** 命令和命令选项的信息，请参见《**RVC** 命令参考指南》。

## 使用 vSphere Client 升级 vSAN 磁盘格式

完成 vSAN 主机升级后，可以执行磁盘格式升级。

The screenshot shows the vSphere Client interface for a vSAN cluster. The left sidebar contains a navigation tree with categories like Services, Configuration, and vSAN. The main panel is titled 'vSAN cluster' and has tabs for Summary, Monitor, Configure, Permissions, Hosts, VMs, Datastores, and Networks. The 'Configure' tab is active, showing a warning about disks on older versions and buttons for 'UPGRADE' and 'PRE-CHECK UPGRADE'. Below this is a table of disk groups with columns for Disk Group, Disks in Use, State, and vSAN Health Status. The table shows two disk groups, each with 3 disks in use, all in a 'Mounted' state with 'Healthy' status. At the bottom, there is a section for disk management with a table of local VMware disks, showing their names, drive types (Flash), and disk tiers (Cache, Capacit).

**注** 如果在现有 vSAN 群集上启用加密或启用去重和压缩，磁盘格式会自动升级到最新版本。不需要此步骤。这样可以避免再次重新格式化磁盘组。请参见[编辑 vSAN 设置](#)。

### 前提条件

- 确认使用的是更新版本的 **vCenter Server**。
- 确认使用的是最新版本的 **ESXi** 主机。
- 确认磁盘处于正常运行状态。导航到“磁盘管理”页面以验证对象状态。
- 确认您计划使用的硬件和软件已经过认证且列在《**VMware** 兼容性指南》中，网址为 <http://www.vmware.com/resources/compatibility/search.php>。

- 确认有足够的可用空间来执行磁盘格式升级。通过运行 RVC 命令 (`vsan.whatif_host_failures`)，确定是否有足够的容量来完成升级，或在升级期间遇到故障时执行组件重新构建操作。
- 确认主机未处于维护模式。升级磁盘格式时，请勿将主机置于维护模式。如果 vSAN 群集的任何成员主机进入维护模式，该成员主机不再向群集提供容量。群集容量将减少，并且群集升级可能会失败。
- 确认 vSAN 群集中当前不存在任何正在进行的组件重新构建任务。有关 vSAN 重新同步的信息，请参见 vSphere 监控和性能。

#### 步骤

- 1 导航到 vSAN 群集。
- 2 单击配置选项卡。
- 3 在“vSAN”下，选择磁盘管理。
- 4 （可选）单击预检查升级。

升级预检查会分析群集以揭露可能阻止成功升级的任何问题。检查的某些项目包括主机状态、磁盘状态、网络状态和对象状态。升级问题将显示在磁盘预检查状态文本框中。

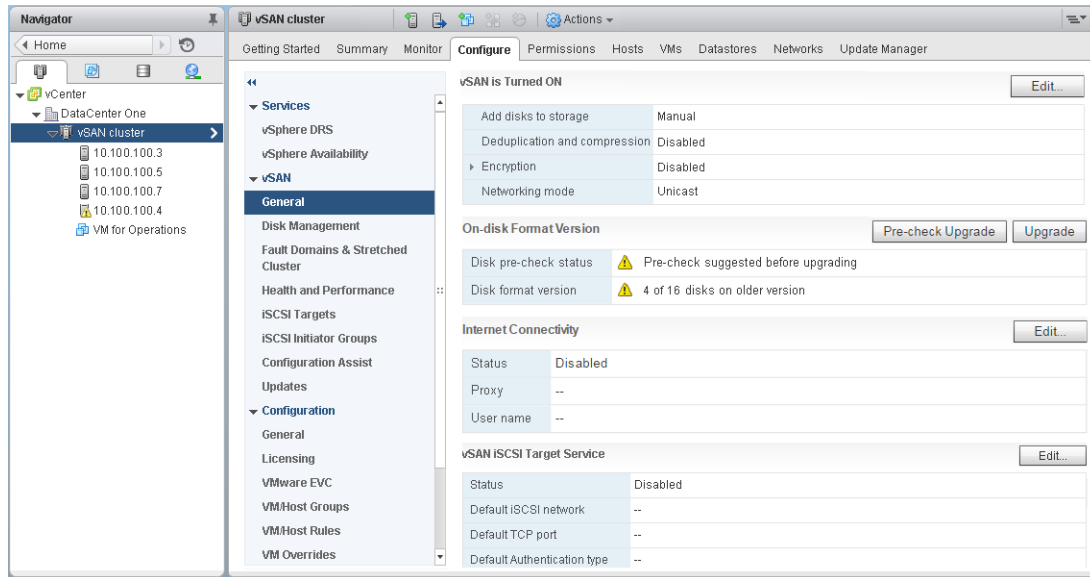
- 5 单击升级。
- 6 在“升级”对话框中单击是，以执行磁盘格式升级。

vSAN 将对群集中的每个磁盘组执行滚动重新引导。“磁盘格式版本”列显示了群集中存储设备的磁盘格式版本。

如果升级期间出现故障，可以查看“重新同步对象”页面。等待所有重新同步操作完成，然后再次运行升级。此外，还可以使用运行状况服务来检查群集运行状况。解决运行状况检查指出的所有问题后，可以再次运行升级。

## 使用 vSphere Web Client 升级 vSAN 磁盘格式

完成 vSAN 主机升级后，可以执行磁盘格式升级。



**注** 如果在现有 vSAN 群集上启用加密或启用去重和压缩，磁盘格式会自动升级到最新版本。不需要此步骤。这样可以避免再次重新格式化磁盘组。请参见[编辑 vSAN 设置](#)。

### 前提条件

- 确认使用的是更新版本的 vCenter Server。
- 确认使用的是最新版本的 ESXi 主机。
- 确认磁盘处于正常运行状态。导航到 vSphere Web Client 中的“磁盘管理”页面以验证对象状态。
- 确认您计划使用的硬件和软件已经过认证且列在《VMware 兼容性指南》中，网址为 <http://www.vmware.com/resources/compatibility/search.php>。
- 确认有足够的可用空间来执行磁盘格式升级。通过运行 RVC 命令 (`vsan.whatif_host_failures`)，确定是否有足够的容量来完成升级，或在升级期间遇到故障时执行组件重新构建操作。
- 确认主机未处于维护模式。升级磁盘格式时，请勿将主机置于维护模式。如果 vSAN 群集的任何成员主机进入维护模式，该成员主机不再向群集提供容量。群集容量将减少，并且群集升级可能会失败。
- 确认 vSAN 群集中当前不存在任何正在进行的组件重新构建任务。请参见《vSAN 监控和故障排除》中的“监控 vSAN 群集中的重新同步任务”。

### 步骤

- 1 在 vSphere Web Client 中，导航到 vSAN 群集。
- 2 单击配置选项卡。
- 3 在“vSAN”下，选择常规。

#### 4 （可选）在**磁盘格式版本**下，单击**预检查升级**。

升级预检查会分析群集以揭露可能阻止成功升级的任何问题。检查的某些项目包括主机状态、磁盘状态、网络状态和对象状态。升级问题将显示在**磁盘预检查状态**文本框中。

#### 5 在**磁盘格式版本**下，单击**升级**。

#### 6 在“升级”对话框中单击**是**以执行磁盘格式升级。

vSAN 将对群集中的每个磁盘组执行滚动重新引导。“磁盘格式版本”列显示了群集中存储设备的磁盘格式版本。**版本过期的磁盘**列指示了使用新格式的设备数。如果升级成功，**版本过期的磁盘**将为 0（零）。

如果升级期间出现故障，您可以查看 vSphere Web Client 中的“正在重新同步组件”页面。等待所有重新同步操作完成，然后再次运行升级。此外，还可以使用运行状况服务来检查群集运行状况。解决运行状况检查指出的所有问题后，可以再次运行升级。

## 使用 RVC 升级 vSAN 磁盘格式

完成 vSAN 主机升级之后，可以使用 Ruby vSphere 控制台 (RVC) 继续升级磁盘格式。

### 前提条件

- 确认使用的是更新版本的 vCenter Server。
- 确认 vSAN 群集中运行的 ESXi 主机的版本为 6.5 或更高版本。
- 通过“磁盘管理”页面，确认磁盘处于正常运行状态。还可以通过运行 RVC 命令 (`vsan.disk_stats`) 确认磁盘状态。
- 确认您计划使用的硬件和软件已经过认证且列在《VMware 兼容性指南》中，网址为 <http://www.vmware.com/resources/compatibility/search.php>。
- 确认有足够的可用空间来执行磁盘格式升级。通过运行 RVC 命令 (`vsan.whatif_host_failures`)，可以确定是否有足够的容量来完成升级，或在升级期间遇到故障时，成功执行组件重新构建操作。
- 确认已安装 PuTTY 或类似的 SSH 客户端以访问 RVC。

有关下载 RVC 工具以及使用 RVC 命令的详细信息，请参见《RVC 命令参考指南》。

- 确认主机未处于维护模式。升级磁盘格式时，请勿将主机置于维护模式。如果 vSAN 群集中的任何成员主机进入维护模式，群集中的可用资源容量将减少，因为此时该成员主机不再向群集提供容量。群集升级可能会失败。
- 通过运行 RVC 命令 (`vsan.resync_dashboard`)，确认 vSAN 群集中当前不存在任何正在进行的组件重新构建任务。

### 步骤

#### 1 使用 RVC 登录到 vCenter Server。

- 2 运行以下 RVC 命令，查看磁盘状态: `vsan.disks_stats /< vCenter IP address or hostname>/<data center name>/computers/<cluster name>`

例如: `vsan.disks_stats /192.168.0.1/BetaDC/computers/VSANCluster`

该命令可列出 vSAN 群集中所有设备和主机的名称。该命令还会显示当前磁盘格式及其健康状况。您还可以在**磁盘管理**页面中的**健康状况**列检查设备的当前健康状况。例如，对于具有故障设备的主机或磁盘组，设备状态在**健康状况**列中显示为“不正常”。

- 3 运行以下 RVC 命令: `vsan.ondisk_upgrade <path to vsan cluster>`

例如: `vsan.ondisk_upgrade /192.168.0.1/BetaDC/computers/VSANCluster`

- 4 监控 RVC 中的进度。

RVC 一次升级一个磁盘组。

成功升级磁盘格式后，将显示以下消息。

磁盘格式升级阶段已完成 (Done with disk format upgrade phase)

有 n 个 v1 对象需要升级，对象升级进度: n 个已升级，剩于 0 个 (There are n v1 objects that require upgrade  
Object upgrade progress: n upgraded, 0 left)

对象升级已完成: n 个已升级 (Object upgrade completed: n upgraded)

VSAN 升级已完成 (Done VSAN upgrade)

- 5 运行以下 RVC 命令，验证对象版本是否已升级到新磁盘格式: `vsan.obj_status_report`

## 验证 vSAN 磁盘格式升级

完成磁盘格式升级后，必须验证 vSAN 群集是否使用新磁盘格式。

### 步骤

- 1 导航到 vSAN 群集。
- 2 单击**配置**选项卡。
- 3 在“vSAN”下，单击**磁盘管理**。

页面顶部将显示当前磁盘格式版本。

## 验证 vSAN 群集升级

需验证您使用的是 vSphere 最新版本并且 vSAN 可用后，才能完成 vSAN 群集升级。

### 步骤

- 1 导航到 vSAN 群集。

## 2 单击配置选项卡，验证是否已列出 vSAN。

您也可以导航到您的 ESXi 主机然后选择**摘要 > 配置**，验证您使用的是最新版本的 ESXi 主机。

## 使用 RVC 升级命令选项

`vsan.ondisk_upgrade` 命令提供了可用于控制和管理 vSAN 群集升级的各个命令选项。例如，当可用空间较少时，可以使用“允许精简冗余”来执行升级。

运行 `vsan.ondisk_upgrade --help` 命令以显示 RVC 命令选项列表。

可将这些命令选项与 `vsan.ondisk_upgrade` 命令配合使用。

**表 8-3. 升级命令选项**

选项	描述
<code>--hosts_and_clusters</code>	用来指定群集中所有主机系统或群集计算资源的路径。
<code>--ignore-objects, -i</code>	用于跳过 vSAN 对象升级。您也可以使用此命令选项以避免升级对象版本。当您使用此命令选项时，对象继续使用当前磁盘格式版本。
<code>--allow-reduced-redundancy, -a</code>	使用此选项，在磁盘升级期间不必考虑可用空间必须等于一个磁盘组的要求。在使用此选项的情况下，虚拟机在升级过程中会在冗余较少的模式下运行，这意味着某些虚拟机可能暂时不能允许出现故障，这可能会导致数据丢失。vSAN 在升级完成之后会还原完全合规性和冗余。
<code>--force, -f</code>	用于强制继续操作，并自动回答所有需确认的问题。
<code>--help, -h</code>	用于显示帮助选项。

有关使用 RVC 命令的信息，请参见《RVC 命令参考指南》。

## 针对 vSphere Update Manager 的 vSAN 内部版本建议

vSAN 会生成用于 vSphere Update Manager 的系统基准和基准组。可以使用这些建议基准更新 vSAN 群集中主机的软件、修补程序和扩展。

vSAN 6.6.1 和更高版本为 vSAN 群集生成自动化内部版本建议。vSAN 将《VMware 兼容性指南》和 vSAN 版本目录中的信息与有关已安装 ESXi 版本的信息组合在一起。这些建议更新提供了最佳可用版本以确保硬件处于受支持状态。

vSAN 6.7.1 及更高版本的系统基准也可以包含设备驱动程序和固件更新。这些更新支持针对您的群集建议的 ESXi 软件。

## vSAN 系统基准

通过用于 Update Manager 的 vSAN 系统基准提供 vSAN 内部版本建议。这些系统基准由 vSAN 管理。它们是只读的，无法进行自定义。

vSAN 为每个 vSAN 群集生成一个基准组。vSAN 系统基准在“基准和组”选项卡的**基准**窗格中列出。可以继续创建和修复您自己的基准。

vSAN 系统基准可以包含认证供应商提供的自定义 ISO 映像。如果 vSAN 群集中的主机具有 OEM 特定的自定义 ISO，则 vSAN 建议的系统基准可以包括来自同一供应商的自定义 ISO。Update Manager 无法为 vSAN 不支持的自定义 ISO 生成建议。如果运行的自定义软件映像覆盖了主机映像配置文件中的供应商名称，则 Update Manager 无法建议系统基准。

Update Manager 自动扫描每个 vSAN 群集以针对基准组检查合规性。要升级群集，必须通过 Update Manager 手动修复系统基准。可以在单个主机上或者整个群集上修复 vSAN 系统基准。

## vSAN 版本目录

vSAN 版本目录维护有关可用版本、版本优先顺序以及每个版本所需的关键修补程序的信息。vSAN 版本目录托管在 VMware Cloud 上。

vSAN 需要 Internet 连接以访问版本目录。无需加入客户体验改进计划 (CEIP)，vSAN 也可以访问版本目录。

如果您没有 Internet 连接，则可以将 vSAN 版本目录直接上载到 vCenter Server。在 vSphere Client 中，单击 **配置 > vSAN > 更新**，然后单击“版本目录”部分中的 **从文件上载**。可以下载最新的 vSAN [版本目录](#)。

使用 Update Manager，可以导入针对您的 vSAN 群集建议的存储控制器固件和驱动程序。某些存储控制器供应商提供了软件管理工具，vSAN 可使用该工具更新控制器驱动程序和固件。如果 ESXi 主机上尚未安装该管理工具，您可以下载此工具。

## 使用 vSAN 内部版本建议

Update Manager 会根据《VMware 兼容性指南》中硬件兼容性列表 (HCL) 中的信息检查已安装 ESXi 的版本。它基于当前的 vSAN 版本目录确定每个 vSAN 群集的正确升级路径。vSAN 还包括其系统基准中建议版本所需的驱动程序和修补程序更新。

vSAN 内部版本建议可确保每个 vSAN 群集都保持当前或更佳的硬件兼容性状态。如果 vSAN 群集中的硬件未包含在 HCL 上，则 vSAN 建议升级到最新版本，因为它不会比当前状态差。

---

**注** 对 vSAN 群集中的主机执行修复预检查时，Update Manager 使用 vSAN 运行状况服务。vSAN 运行状况服务在运行 ESXi 6.0 Update 1 或更低版本的主机上不可用。Update Manager 升级运行 ESXi 6.0 Update 1 或更低版本的主机时，vSAN 群集中最后一个主机的升级可能会失败。如果修复因 vSAN 运行状况问题而失败，您仍可以完成升级。使用 vSAN 运行状况服务解决主机上的运行状况问题，然后将该主机退出维护模式以完成升级 workflow。

---

以下示例说明了 vSAN 内部版本建议背后的逻辑。

- |             |   |
|-------------|---|
| <b>示例 1</b> | vSAN 群集运行 6.0 Update 2，并且其硬件包含在 6.0 Update 2 HCL 中。HCL 列出了 6.0 Update 3 及更低版本支持但 6.5 及更高版本不支持的硬件。vSAN 建议升级到 6.0 Update 3，包括版本所需的关键修补程序。 |
| <b>示例 2</b> | vSAN 群集运行 6.0 Update 2，并且其硬件包含在 6.0 Update 2 HCL 中。版本 6.5 Update 1 的 HCL 也支持该硬件。vSAN 建议升级到版本 6.5 Update 1。                              |
| <b>示例 3</b> | vSAN 群集运行 6.0 Update 2，但其硬件不在该版本的 HCL 上。vSAN 建议升级到 6.5 Update 1，即使硬件不在 6.5 Update 1 的 HCL 上也是如此。vSAN 建议进行升级，因为新状态不会比当前状态差。              |

建议引擎定期运行（每天一次），或者在发生以下事件时运行。

- 群集成员资格发生改变。例如，添加或移除主机时。
- vSAN 管理服务重新启动。
- 用户通过 vSphere Client 或 RVC 登录到 My VMware (my.vmware.com)。
- 更新了《VMware 兼容性指南》或 vSAN 版本目录。

vSAN 内部版本建议运行状况检查会显示为 vSAN 群集建议的当前内部版本。它还会警告您有关该功能的任何问题。

## 系统要求

必须手动将 Update Manager 安装在 Windows vCenter Server 上。

vSAN 需要 Internet 访问以更新版本元数据，检查《VMware 兼容性指南》，以及从 My VMware 下载 ISO 映像。

vSAN 需要有效的 My VMware (my.vmware.com) 凭据以下载 ISO 映像进行升级。对于运行 6.0 Update 1 及更低版本的主机，必须使用 RVC 输入 My VMware 凭据。对于运行更高版本软件的主机，可以从 ESX 内部版本建议运行状况检查进行登录。

要通过 RVC 输入 My VMware 凭据，请运行以下命令：`vsan.login_iso_depot -u <username> -p <password>`