vSphere 可用性

VMware vSphere 8.0
VMware ESXi 8.0
vCenter Server 8.0

vmware®

您可以从 VMware 网站下载最新的技术文档：

https://docs.vmware.com/cn/。

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

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

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

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

目录

关于 vSphere 可用性

《vSphere 可用性》介绍提供业务连续性的解决方案，包括如何建立 vSphere® High Availability (HA) 和 vSphere Fault Tolerance。

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

目标读者

此信息专供需要通过 vSphere HA 和 Fault Tolerance 解决方案提供业务连续性的用户使用。本书的目标读者为熟悉虚拟机技术和数据中心操作且具有丰富经验的 Windows 或 Linux 系统管理员。

业务连续性和最小化停机时间

1

无论是计划停机时间还是非计划停机时间，都会带来相当大的成本。但是，用于确保更高级别可用性的解决方案通常都需要较大开销，并且难以实施和管理。

VMware 软件可为重要应用程序提供更高级别的可用性，并且操作更简单，成本更低。使用 vSphere，您可以提高为所有应用程序提供的可用性基准级别，并且以更低成本和更简单的操作来实现更高级别的可用性。使用 vSphere，您可以：

- 独立于硬件、操作系统和应用程序提供高可用性。
- 减少常见维护操作的计划停机时间。
- 在出现故障时提供自动恢复。

vSphere 可以减少计划的停机时间，防止出现非计划停机，并迅速从中断中恢复。

本章讨论了以下主题：

减少计划的停机时间

计划的停机时间通常占数据中心停机时间的 80% 以上。硬件维护、服务器迁移和固件更新均需要将物理服务器停机。为最小化此停机时间的影响，会强制组织延迟维护，直到出现不便且难以调度的停机时间段。

通过 vSphere，组织可以显著减少计划的停机时间。由于 vSphere 环境中的工作负载无需停机或服务中断就可以动态移动到其他物理服务器，所以服务器维护无需应用程序和服务停机就可以执行。通过 vSphere，组织可以执行以下任务：

- 消除常见维护操作的停机时间。
- 消除计划的维护时间段。
- 随时执行维护，无需中断用户和服务。

由于 VMware 环境中的工作负载无需中断服务即可动态移动到不同的物理服务器或基础存储器，所以，通过 vSphere 中的 vSphere vMotion® 和 Storage vMotion 功能，组织可以减少计划的停机时间。管理员可以快速而完整地执行透明的维护操作，无需强制调度不方便的维护时间段。

防止非计划停机时间

在 ESXi 主机为应用程序的运行提供稳定平台时，组织还必须保护自身，避免出现硬件或应用程序故障所导致的非计划停机时间。vSphere 将重要功能构建到数据中心基础架构中，这有助于避免出现非计划停机时间。

这些 vSphere 功能是虚拟基础架构的一部分，因此，对操作系统以及虚拟机中运行的应用程序而言是透明的。这些功能可以进行配置，而且可供物理系统上的所有虚拟机使用，从而降低成本并降低实现高可用性的复杂程度。vSphere 中内置的密钥可用性功能：

- 共享存储器。通过在共享存储器（如光纤通道、iSCSI SAN 或 NAS）上存储虚拟机文件来消除单一故障点。可以使用 SAN 镜像和复制功能将虚拟磁盘的更新副本保留在灾难恢复站点。
- 网络接口绑定。允许单个网卡发生故障。
- 存储多路径。允许存储路径发生故障。

除了这些功能外，vSphere HA 和 Fault Tolerance 功能分别通过提供中断快速恢复和连续可用性来最小化或消除非计划停机时间。

vSphere HA 提供快速中断恢复

vSphere HA 利用配置为集群的多台 ESXi 主机，为虚拟机中运行的应用程序提供快速中断恢复和具有成本效益的高可用性。

vSphere HA 通过以下方式保护应用程序可用性：

- 通过在集群内的其他主机上重新启动虚拟机，防止服务器故障。
- 通过持续监控虚拟机并在检测到故障时对其进行重新设置，防止应用程序故障。
- 通过在仍然有权访问其数据存储的其他主机上重新启动受影响的虚拟机，可防止出现数据存储可访问性故障。
- 如果虚拟机的主机在管理或 vSAN 网络上被隔离，它会通过重新启动这些虚拟机来防止网络隔离。即使网络已分区，仍会提供此保护。

与其他集群解决方案不同，vSphere HA 提供基础架构并使用该基础架构保护所有工作负载：

- 无需在应用程序或虚拟机内安装特殊软件。所有工作负载均受 vSphere HA 保护。配置 vSphere HA 之后，不需要执行操作即可保护新虚拟机。它们会自动受到保护。
- 可以将 vSphere HA 与 vSphere Distributed Resource Scheduler (DRS) 结合使用以防止出现故障，以及在集群内的主机之间提供负载平衡。

与传统的故障切换解决方案相比，vSphere HA 具有多个优势：

最小化设置

设置 vSphere HA 集群之后，集群内的所有虚拟机无需额外配置即可获得故障切换支持。

减少了硬件成本和设置

虚拟机可充当应用程序的移动容器，可在主机之间移动。管理员会避免在多台计算机上进行重复配置。使用 vSphere HA 时，必须拥有足够的资源来对要通过 vSphere HA 保护的主机数进行故障切换。但是，VMware vCenter Server® 系统会自动管理资源并配置集群。

提高了应用程序的可用性

虚拟机内运行的任何应用程序的可用性变得更高。虚拟机可以从硬件故障中恢复，提高了在引导周期内启动的所有应用程序的可用性，而且没有额外的计算需求，即使该应用程序本身不是集群应用程序也一样。通过监控和响应 VMware Tools 检测信号并重新启动未响应的虚拟机，可防止客户机操作系统崩溃。

DRS 和 vMotion 集成

如果主机发生了故障，并且在其他主机上重新启动了虚拟机，则 DRS 会提出迁移建议或迁移虚拟机以平衡资源分配。如果迁移的源主机和/或目标主机发生故障，则 vSphere HA 会帮助从该故障中恢复。

vSphere Fault Tolerance 提供连续可用性

vSphere HA 通过在主机出现故障时重新启动虚拟机来为虚拟机提供基本级别的保护。vSphere Fault Tolerance 可提供更高级别的可用性，允许用户对任何虚拟机进行保护以防止主机发生故障时丢失数据、事务或连接。

Fault Tolerance 通过确保主虚拟机和辅助虚拟机的状态在虚拟机的指令执行的任何时间点均相同来提供连续可用性。

如果运行主虚拟机的主机或运行辅助虚拟机的主机发生故障，则会发生即时且透明的故障切换。正常运行的 ESXi 主机将无缝变成主虚拟机的主机，而不会断开网络连接或中断正在处理的事务。使用透明故障切换，不会有数据损失，并且可以维护网络连接。 在进行透明故障切换之后，将重新生成新的辅助虚拟机，并将重新建立冗余。整个过程是透明且全自动的，并且即使 vCenter Server 不可用，也会发生。

使用 vCenter High Availability 保护 vCenter Server

vCenter High Availability (vCenter HA) 不仅能够在主机和硬件出现故障时提供保护，而且还能够在 vCenter Server 应用程序出现故障时提供保护。使用自动故障切换功能从主动切换到被动，vCenter HA 支持的高可用性可最大限度减少停机时间。

您从 vSphere Client 中配置 vCenter HA。配置向导提供以下选项。

选项	描述
自动	“自动”选项可以将主动节点克隆到被动节点和见证节点，并为您配置这些节点。 如果您的环境满足以下要求，您可以使用此选项。 ■ 成为主动节点的 vCenter Server 要管理其自己的 ESXi 主机及虚拟机。此配置有时称为自我管理 vCenter Server。
手动	“手动”选项更具灵活性。如果您的环境满足硬件和软件要求，便可以使用此选项。 如果您选择此选项，您将负责将主动节点克隆到被动节点和见证节点。您还必须执行一些网络配置。

使用 VMware Service Lifecycle Manager 保护 vCenter Server

VMware Service Lifecycle Manager 可提供 vCenter Server 可用性。

如果 vCenter 服务失败，VMware Service Lifecycle Manager 会重新启动该服务。VMware Service Lifecycle Manager 监控服务的运行状况，并在检测到故障时采取预先配置的修复操作。如果多次尝试修复均失败，服务将不会重新启动。

创建和使用 vSphere HA 集群

2

vSphere HA 集群允许 ESXi 主机集合作为一个组协同工作，这些主机为虚拟机提供的可用性级别比 ESXi 主机单独提供的级别要高。当规划新 vSphere HA 集群的创建和使用时，您选择的选项会影响集群对主机或虚拟机故障的响应方式。

在创建 vSphere HA 集群之前，应清楚 vSphere HA 标识主机故障和隔离以及响应这些情况的方式。还应了解接入控制的工作方式以便可以选择符合故障切换需要的策略。建立集群之后，不但可以通过高级选项自定义其行为，还可以通过执行建议的最佳做法优化其性能。

注 尝试使用 vSphere HA 时可能会获得错误消息。有关与 vSphere HA 相关的错误消息的信息，请参见位于 http://kb.vmware.com/kb/1033634 的 VMware 知识库文章。

本章讨论了以下主题：

- vSphere HA 的工作方式
- vSphere HA 准入控制
- vSphere HA 互操作性
- 创建 vSphere HA 集群
- 配置 vSphere 可用性设置
- 适用于 VMware vSphere® High Availability 集群的最佳做法
- HA VIB 行为的更改

vSphere HA 的工作方式

vSphere HA 可以将虚拟机及其所驻留的主机集中在集群内，从而为虚拟机提供高可用性。集群中的主机均会受到监控，如果发生故障，故障主机上的虚拟机将在备用主机上重新启动。

创建 vSphere HA 集群时，会自动选择一台主机作为首选主机。首选主机可与 vCenter Server 进行通信，并监控所有受保护的虚拟机以及辅助主机的状态。可能会发生不同类型的主机故障，首选主机必须检测并相应地处理故障。首选主机必须能够区分故障主机与网络分区中的主机或已与网络隔离的主机。首选主机使用网络和数据存储检测信号确定故障的类型。


(Sphere HA 集群)

首选主机和辅助主机

在将主机添加到 vSphere HA 集群时，代理将上载到主机，并配置为与集群内的其他代理通信。集群中的每台主机作为首选主机或辅助主机运行。

如果为集群启用了 vSphere HA，则所有活动主机（未处于待机或维护模式的主机或未断开连接的主机）都将参与选择集群的首选主机。挂载最多数量的数据存储的主机在选举中具有优势。每个集群通常只存在一台首选主机，其他所有主机都是辅助主机。如果首选主机出现故障、关机或处于待机模式或者从集群中移除，则会进行新的选举。

集群中的首选主机具有多个职责：

- 监控辅助主机的状况。如果辅助主机发生故障或无法访问，首选主机将确定必须重新启动哪些虚拟机。
- 监控所有受保护虚拟机的电源状况。如果有一台虚拟机出现故障，首选主机可确保重新启动该虚拟机。首选主机还可使用本地放置引擎确定进行重新启动的位置。
- 管理集群主机和受保护的虚拟机列表。
- 充当集群的 vCenter Server 管理界面并报告集群运行状况。

辅助主机主要通过在本地运行虚拟机、监控其运行时状况和向首选主机报告状况更新来对集群提供支持。首选主机也可运行和监控虚拟机。辅助主机和首选主机都可实现虚拟机和应用程序监控功能。

首选主机执行的功能之一是协调受保护虚拟机的重新启动。在 vCenter Server 观察到为响应用户操作，某虚拟机的电源状况由关闭电源变为打开电源之后，该虚拟机会受到首选主机的保护。首选主机会将受保护虚拟机的列表保留在集群的数据存储中。新选的首选主机使用此信息来确定要保护哪些虚拟机。

注 如果断开主机与集群之间的连接，则向该主机注册的虚拟机将不受 vSphere HA 保护。

主机故障类型

VMware vSphere® High Availability 集群的首选主机负责检测辅助主机的故障。根据检测到的故障类型，在主机上运行的虚拟机可能需要进行故障切换。

在 vSphere HA 集群中，检测三种类型的主机故障：

- 故障。主机停止运行。
- 隔离。主机出现网络隔离。
- 分区。主机失去与首选主机的网络连接。

首选主机监控集群中辅助主机的活跃度。此通信通过每秒交换一次网络检测信号来进行。当首选主机停止从辅助主机接收这些检测信号时，它会在声明该主机出现故障之前检查主机活跃度。首选主机执行的活跃度检查用于确定辅助主机是否正在与其中一个数据存储交换检测信号。请参见 数据存储检测信号 。此外，首选主机还检查主机是否对发送至其管理 IP 地址的 ICMP ping 进行响应。

如果首选主机无法直接与辅助主机上的代理通信，则辅助主机不会响应 ICMP ping。如果代理未发出检测信号，则被视为出现故障。会在备用主机上重新启动主机的虚拟机。如果此类辅助主机正在与数据存储交换检测信号，首选主机会认为辅助主机在网络分区上或已与网络隔离。因此，首选主机会继续监控该主机及其虚拟机。请参见 网络分区 。

当主机仍在运行但无法再监视来自管理网络上 vSphere HA 代理的流量时，会发生主机网络隔离。如果主机停止监视此流量，则它会尝试 ping 集群隔离地址。如果此 ping 也失败，主机会声明它已与网络隔离。

首选主机会监控隔离主机上正在运行的虚拟机。如果首选主机观察到虚拟机已关闭电源，且首选主机负责虚拟机，则会重新启动虚拟机。

注 如果您确保网络基础架构具有足够的冗余度且至少有一个网络路径始终可用，则不太可能发生主机网络隔离。

Proactive HA 故障

当主机组件发生故障时，即发生了 Proactive HA 故障，这会导致冗余丢失或非灾难性故障。但是，主机上的虚拟机的功能行为不会受到影响。例如，如果主机出现电源故障，但是其他电源可用，则属于 Proactive HA 故障。

发生 Proactive HA 故障时，可在 vSphere Client 的“vSphere 可用性”部分自动执行修复操作。受影响主机上的虚拟机可以撤出到其他主机，并将该主机置于隔离模式或维护模式。

注 您的集群必须使用 vSphere DRS，以便 Proactive HA 故障监控正常工作。

确定对主机问题的响应

如果主机发生故障而必须重新启动虚拟机，您可使用虚拟机重新启动优先级”设置控制重新启动虚拟机的顺序。您也可使用主机隔离响应设置，配置主机与其他主机失去管理网络连接时 vSphere HA 的响应方式。发生故障后，vSphere HA 重新启动虚拟机时还将考虑其他因素。

以下设置适用于主机发生故障或主机隔离时集群内的所有虚拟机。此外，也可以为特定虚拟机配置异常。请参见自定义单个虚拟机 。

主机隔离响应

主机隔离响应确定当 vSphere HA 集群内的某个主机失去其管理网络连接但仍继续运行时出现的情况。您可以使用隔离响应使 vSphere HA 关闭隔离主机上运行的虚拟机的电源，然后在非隔离主机上将其重新启动。主机隔离响应要求激活“主机监控状态”。如果“主机监控状态”为已停用，则主机隔离响应也将挂起。当主机无法与其他主机上运行的代理通信且无法 ping 其隔离地址时，该主机确定其已被隔离。然后，主机会执行其隔离响应。响应为“关闭虚拟机电源再重新启动虚拟机”或“关闭再重新启动虚拟机”。还可以为各个虚拟机自定义此属性。

注 如果虚拟机的重新启动优先级设置为“已禁用”，则不会做出任何主机隔离响应。

要使用“关闭再重新启动虚拟机”设置，必须在虚拟机的客户机操作系统中安装 VMware Tools。将虚拟机关机的优点在于可以保留其状况。关机操作优于关闭虚拟机电源操作，关闭虚拟机不会将最近的更改刷新到磁盘中，也不会提交事务。在关机完成时，正在关机的虚拟机需要更长时间进行故障切换。未在 300 秒内或在高级选项 `das.isolationshutdowntimeout` 中指定的时间内关机的虚拟机将被关闭电源。

创建 vSphere HA 集群后，可以替代特定虚拟机的“重新启动优先级”和“隔离响应”的默认集群设置。此替代操作对于用于特殊任务的虚拟机很有帮助。例如，可能需要先打开提供基础架构服务（如 DNS 或 DHCP）的虚拟机电源，再打开集群内的其他虚拟机电源。

如果主机已从首选主机隔离或分区，或首选主机无法使用检测信号数据存储与该主机通信，则可能会发生虚拟机“裂脑”情况。在这种情况下，首选主机无法确定该主机处于活动状态，因此声明其已停止运行。然后，首选主机尝试重新启动已隔离或已分区主机上正在运行的虚拟机。如果虚拟机仍在已隔离/已分区主机上运行，且该主机在隔离或分区时失去对虚拟机数据存储的访问权限，则此尝试将成功。然后，便会发生裂脑情况，因为存在两个虚拟机实例。但是，只有一个实例能够读取或写入虚拟机的虚拟磁盘。虚拟机组件保护可用于防止发生此裂脑情况。使用激进设置激活 VMCP 时，它会监控已打开电源的虚拟机的数据存储可访问性，并关闭失去对其数据存储访问权限的虚拟机。

为了从此情况中恢复，ESXi 会针对已丢失磁盘锁的虚拟机生成一个问题（关于主机何时摆脱隔离状态且无法重新获取磁盘锁）。vSphere HA 将自动回答该问题，这就使已丢失磁盘锁的虚拟机实例关闭电源，只留下具有磁盘锁的实例。

虚拟机依赖关系

可以在虚拟机组之间创建依赖关系。要执行此操作，必须首先在 vSphere Client 中创建虚拟机组，方法是转到集群的**配置**选项卡，然后选择**虚拟机/主机组**。创建组之后，可以在组之间创建重新启动依赖关系规则，方法是浏览到**虚拟机/主机规则**，然后在“类型”下拉菜单中，选择**虚拟机到虚拟机**。这些规则可以指定在其他指定虚拟机组就绪之前，不会重新启动某些虚拟机。

重新启动虚拟机要考虑的因素

发生故障后，集群的首选主机会确定一个可打开受影响虚拟机电源的主机，从而尝试重新启动这些虚拟机。选择此类主机时，首选主机会考虑许多因素。

文件可访问性

在可启动虚拟机之前，必须能够从可通过网络与首选主机通信的某个活动集群主机中访问该虚拟机的文件

虚拟机与主机的兼容性

如果存在可访问的主机，则虚拟机必须至少与其中一个主机兼容。为虚拟机设置的兼容性包括任何所需虚拟机-主机关联性规则的影响。例如，如果某个规则仅允许虚拟机在两个主机上运行，则会考虑将其放置在这两个主机上。

资源预留

在可运行虚拟机的主机中，必须至少有一个主机具有足够的未预留容量以满足虚拟机的内存开销及任何资源预留。可采用四种预留类型：CPU、内存、虚拟网卡和虚拟闪存。此外，必须提供足够的网络端口，才能打开虚拟机电源。

主机限制

除了资源预留之外，一个虚拟机只能放置在一个主机上（如果这样做不会违反允许的虚拟机最大数量或正在使用的 vCPU 数量）。

功能限制

如果已设置需要 vSphere HA 强制执行虚拟机-虚拟机反关联性规则的高级选项，则 vSphere HA 不会违反此规则。此外，vSphere HA 不会违反为容错虚拟机配置的任何每主机限制。

如果没有任何主机满足上述注意事项，则首选主机会发布一个事件指出没有足够的资源让 vSphere HA 来启动虚拟机，并会在集群状况发生更改时进行重试。例如，如果虚拟机不可访问，则首选主机会在文件可访问性发生更改后进行重试。

虚拟机和应用程序监控

如果在设置的时间内没有收到单个虚拟机的 VMware Tools 检测信号，虚拟机监控将重新启动该虚拟机。同样，如果没有收到虚拟机正在运行的应用程序的检测信号，应用程序监控也可以重新启动该虚拟机。可以启用这些功能，并配置 vSphere HA 监控无响应时的敏感度。

启用虚拟机监控后，虚拟机监控服务（使用 VMware Tools）将通过检查正在客户机内运行的 VMware Tools 进程的常规检测信号和 I/O 活动来评估集群内的每个虚拟机是否正在运行。如果没有收到检测信号或 I/O 活动，则很有可能是客户机操作系统出现故障，或未分配给 VMware Tools 用来完成任务的时间。在这种情况下，虚拟机监控服务会先确定虚拟机已发生故障，然后决定重新引导虚拟机以还原服务。

有时，仍然正常工作的虚拟机或应用程序会停止发送检测信号。为了避免不必要的重置，虚拟机监控服务还监控虚拟机的 I/O 活动。如果在故障时间间隔内未收到任何检测信号，则会检查 I/O 统计间隔（集群级别属性）。I/O 统计间隔确定在前两分钟（120 秒）内是否已发生与虚拟机有关的任何磁盘或网络活动。如果没有，则重置该虚拟机。可以使用高级选项 `das.iostatsinterval` 更改此默认值（120 秒）。

要启用应用程序监控，必须先获取相应的 SDK（或使用可支持 VMware 应用程序监控的应用程序），然后使用它来设置要监控的应用程序的自定义检测信号。完成此操作后，应用程序监控的工作方式将与虚拟机监控的工作方式大致相同。如果在指定时间内没有收到应用程序的检测信号，将重新启动其虚拟机。

您可以配置监控敏感度的级别。高敏感度监控可以更快得出已发生故障的结论。然而，如果受监控的虚拟机或应用程序实际上仍在运行，但由于资源限制等因素导致未收到检测信号，高敏感度监控可能会错误地认为此虚拟机发生了故障。低敏感度监控会延长实际故障和虚拟机重置之间服务中断的时间。请选择一个有效折衷满足需求的选项。

也可以通过选中**自定义**复选框来指定监控敏感度和 I/O 统计间隔的自定义值。

表 2-1. 虚拟机监控设置

设置	故障时间间隔（秒）	重置期
高	30	1 小时
中	60	24 小时
低	120	7 天

检测到故障后，vSphere HA 会重置虚拟机。重置可确保这些服务仍然可用。为了避免因非瞬态错误而反复重置虚拟机，默认情况下，在某个可配置的时间间隔内将对虚拟机仅重置三次。在对虚拟机执行过三次重置后，指定的时间结束之前，vSphere HA 不会在后续故障出现后进一步尝试重置虚拟机。可以使用**每个虚拟机的最大重置次数**自定义设置来配置重置次数。

注　当关闭虚拟机电源然后再次打开虚拟机电源时，或使用 vMotion 将虚拟机迁移到其他主机时，重置统计信息将被清除。这将导致客户机操作系统重新引导，但不同于虚拟机电源状况发生更改的“重新启动”。

虚拟机组件保护

如果激活虚拟机组件保护 (VMCP)，vSphere HA 可以检测到数据存储可访问性故障，并为受影响的虚拟机提供自动恢复。

VMCP 可防止发生数据存储可访问性故障，这些故障可能会影响 vSphere HA 集群中主机上正在运行的虚拟机。当发生数据存储可访问性故障时，受影响的主机无法再访问特定数据存储的存储路径。您可以确定 vSphere HA 将对此类故障作出的响应，从创建事件警报到虚拟机在其他主机上重新启动。

注 使用虚拟机组件保护功能时，ESXi 主机的版本必须为 6.0 或更高版本。

故障类型

存在两种类型的数据存储可访问性故障：

PDL

PDL（永久设备丢失）是在存储设备报告主机无法再访问数据存储时发生的不可恢复的可访问性丢失。如果不关闭虚拟机的电源，此状况将无法恢复。

APD

APD（全部路径异常）表示暂时性或未知的可访问性丢失，或 I/O 处理中的任何其他未识别的延迟。此类型的可访问性问题是可恢复的。

配置 VMCP

在 vSphere Client 中配置虚拟机组件保护。转到**配置**选项卡并单击 **vSphere 可用性**和**编辑**。在**故障和响应**下，可以选择**处于 PDL 状态的数据存储**或**处于 APD 状态的数据存储**。您可选择的存储保护级别以及可用的虚拟机修复操作根据数据库可访问性故障的类型而异。

PDL 故障

在**处于 PDL 状态的数据存储**下，可以选择**发布事件**或**关闭虚拟机电源再重新启动虚拟机**。

APD 故障

响应 APD 事件是更加复杂的，相应地配置是更加精细的。可以选择**发布事件**、**关闭虚拟机电源再重新启动虚拟机 - 保守的重新启动策略**或**关闭虚拟机电源再重新启动虚拟机 - 激进的重新启动策略**

注 如果停用“主机监控”或“虚拟机重新启动优先级”设置，VMCP 将无法执行虚拟机重新启动。但是，仍可监控存储运行状况，且可发布事件。

网络分区

在 vSphere HA 集群发生管理网络故障时，该集群中的部分主机可能无法通过管理网络与其他主机进行通信。一个集群中可能会出现多个分区。

已分区的集群会导致虚拟机保护和集群管理功能降级。请尽快更正已分区的集群。

- 虚拟机保护。vCenter Server 允许虚拟机打开电源，但仅当虚拟机与负责它的首选主机在同一分区中运行时，才能对其进行保护。首选主机必须与 vCenter Server 进行通信。如果首选主机以独占方式锁定虚拟机配置文件所在数据存储上的系统定义的文件，则首选主机将负责该虚拟机。
- 集群管理。vCenter Server 可以与首选主机通信，但只能与一部分辅助主机通信。因此，只有在解决分区之后，配置中影响 vSphere HA 的更改才能生效。此故障可能会导致其中一个分区在旧配置下操作，而另一个分区使用新的设置。

数据存储检测信号

当 VMware vSphere® High Availability 集群中的首选主机无法通过管理网络与辅助主机通信时，首选主机将使用数据存储检测信号来确定辅助主机是否出现故障，是否位于网络分区中，或者是否与网络隔离。如果辅助主机已停止数据存储检测信号，则认为该辅助主机出现故障，并且其虚拟机已在别处重新启动。

VMware vCenter Server® 选择一组首选数据存储集用于检测信号。这种选择会使有权访问检测信号数据存储的主机数最大，也会使数据存储由同一 LUN 或 NFS 服务器支持的可能性最小。

可以使用高级选项 `das.heartbeatdsperhost` 更改 vCenter Server 为每个主机选择的检测信号数据存储的数量。默认值为 2，最大有效值为 5。

vSphere HA 将在用于数据存储检测信号和保留受保护的虚拟机集的每个数据存储的根目录中创建一个目录，目录名称为 `.vSphere-HA`。请勿删除或修改存储在此目录中的文件，因为这可能会对操作产生影响。由于多个集群可能使用一个数据存储，因此将针对每个集群创建该目录的子目录。根用户拥有这些目录和文件，并且只有根用户可以读写这些目录和文件。vSphere HA 使用的磁盘空间取决于多个因素，包括所用的 VMFS 版本以及将数据存储用于信号检测的主机数。使用 vmfs3 时，最大使用量为 2 GB，典型使用量为 3 MB。使用 vmfs5 时，最大使用量和典型使用量均为 3 MB。vSphere HA 使用数据存储增加的开销很小，并且不会对其他数据存储操作的性能产生任何影响。

vSphere HA 会限制配置文件可在单个数据存储中的虚拟机数量。有关更新的限制，请参见最高配置。如果将超过该数量的虚拟机置于数据存储中并打开其电源，则 vSphere HA 只保护该上限数量的虚拟机。

注　vSAN 数据存储无法用于数据存储检测信号。因此，如果集群中的所有主机均无法访问其他共享存储，则无法使用任何检测信号数据存储。但是，如果您拥有的存储可通过独立于 vSAN 网络的备用网络路径访问，则可以将其用于设置检测信号数据存储。

vSphere HA 安全性

多个安全功能增强了 vSphere HA。

选择已打开的防火墙端口

vSphere HA 对代理至代理的通信使用 TCP 和 UDP 端口 8182。防火墙端口将自动打开和关闭，确保仅在需要时打开端口。

使用文件系统权限保护的配置文件

vSphere HA 在本地存储或 ramdisk（如果没有本地数据存储）上存储配置信息。使用文件系统权限保护这些文件，且仅 root 用户可以访问它们。不具有本地存储的主机只有在由 Auto Deploy 管理时才受支持。

详细的日志记录

vSphere HA 放置日志文件的位置取决于主机版本。

- 对于 ESXi 主机，vSphere HA 默认仅写入 syslog，因此，日志放置在 syslog 所配置的放置位置。vSphere HA 日志文件名前置 `fdm`（fdm 代表故障域管理器，vSphere HA 中的一种服务）。
- 对于旧版 ESXi 主机，vSphere HA 写入本地磁盘上的 `/var/log/vmware/fdm` 以及 syslog（如果已配置）。

安全 vSphere HA 登录

vSphere HA 使用 vCenter Server 创建的用户帐户 **vpxuser** 登录到 vSphere HA 代理。此帐户与 vCenter Server 用于管理主机的帐户相同。vCenter Server 为此帐户创建随机密码，并定期更改密码。时间段由 vCenter Server `VirtualCenter.VimPasswordExpirationInDays` 设置进行设置。对主机的根文件夹具有管理特权的用户可登录到代理。

安全通信

vCenter Server 和 vSphere HA 代理之间的所有通信都是通过 SSL 完成的。除选举消息以外（通过 UDP 完成），代理至代理的通信也使用 SSL。选举消息通过 SSL 进行验证，以便恶意代理只能阻止在其上运行代理的主机被选为首选主机。在这种情况下，将发出集群的配置问题，以便用户了解问题。

需要验证主机 SSL 证书

vSphere HA 要求每个主机都具有一个经过验证的 SSL 证书。每个主机在首次引导时都会生成一个自签署证书。然后，可以重新生成或使用机构颁发的证书替换该证书。如果证书被替换，需要重新配置主机上的 vSphere HA。如果主机在其证书更新后断开与 vCenter Server 的连接，且重新启动 ESXi 或 ESX 主机代理，则主机重新连接到 vCenter Server 时将自动重新配置 vSphere HA。如果由于 vCenter Server 主机 SSL 证书验证当前已停用而未断开连接，请验证新证书并在主机上重新配置 vSphere HA。

vSphere HA 准入控制

vSphere HA 使用准入控制确保在主机出现故障时预留足够的资源用于虚拟机恢复。

准入控制对资源使用施加一些限制。任何可能违反这些限制的操作都不会被允许。可能不允许的操作示例如下：

- 打开虚拟机电源

- 迁移虚拟机
- 增加虚拟机的 CPU 或内存预留

vSphere HA 准入控制的基础是集群允许的且仍能保证可故障切换的主机故障数。可通过三种方式来设置主机故障切换容量：

- 集群资源百分比
- 插槽策略
- 专用故障切换主机

注 可以停用 vSphere HA 准入控制。但是，如果禁用 VMware HA 准入控制，将无法保证预期数量的虚拟机能够在故障后重新启动。请勿永久停用准入控制。

无论选择的准入控制选项如何，都会存在虚拟机资源减少阈值。您可以使用此设置指定允许的资源减少百分比，但在激活 vSphere DRS 后才可用。

会针对 CPU 和内存进行资源减少计算。此项计算会考虑虚拟机的预留内存和内存过量分配以便决定是否允许打开电源、执行迁移或更改预留。计算不会考虑虚拟机消耗的实际内存，因为内存预留并不总是与虚拟机的实际内存使用率相关联。如果实际使用率大于预留内存，则故障切换容量会不足，导致故障切换的性能下降。

通过设置性能减少阈值，可以指定配置问题的发生次数。例如：

- 默认值为 100%，不会产生任何警告。
- 如果阈值降至 0%，则集群使用率超过可用容量时，就会生成警告。
- 如果阈值降至 20%，可以允许的性能减少量按如下方式计算：`performance reduction = current utilization * 20%`。当前使用率减去性能减少量的值超过可用容量时，将发出配置通知。

集群资源百分比准入控制

可以将 vSphere HA 配置为通过预留特定百分比的集群 CPU 和内存资源来执行准入控制，用于从主机故障中进行恢复。

使用此准入控制类型，vSphere HA 可确保预留特定百分比的 CPU 和内存资源总量用于进行故障切换。

使用集群资源百分比选项，vSphere HA 可强制执行下列准入控制：

1 计算集群内所有已打开电源虚拟机的总资源要求。

2 计算可用于虚拟机的主机资源总数。

3 计算集群的“当前的 CPU 故障切换容量”和“当前的内存故障切换容量”。

4 确定“当前的 CPU 故障切换容量”或“当前的内存故障切换容量”是否小于对应的“配置的故障切换容量”（由用户提供）。

   如果是，则准入控制不允许执行此操作。

vSphere HA 将使用虚拟机的实际预留。如果虚拟机没有预留（即预留量为 0），则会应用默认设置（0MB 内存和 32MHz CPU）。

注 准入控制的集群资源百分比选项还会检查集群中是否至少有两个启用了 vSphere HA 的主机（不包括正在进入维护模式的主机）。如果只有一个已启用 vSphere HA 的主机，即使可以使用足够的资源百分比，也不允许执行此操作。进行此次额外检查的原因在于如果集群中只有一个主机，则 vSphere HA 无法进行故障切换。

计算当前故障切换容量

已打开电源的虚拟机的总资源要求由两个组件组成，即 CPU 和内存。vSphere HA 将计算这些值。

- CPU 组件值的计算方法是：加总已打开电源虚拟机的 CPU 预留。如果没有为虚拟机指定 CPU 预留，则系统会为其分配一个默认值 32MHz（可以使用 `das.vmcpuminmhz` 高级选项更改此值）。
- 内存组件值的计算方法是：加总每台已打开电源虚拟机的内存预留（以及内存开销）。

计算出主机的 CPU 和内存资源总和，从而得出虚拟机可使用的主机资源总数。这些值包含在主机的根资源池中，而不是主机的总物理资源中。不包括用于虚拟化目的的资源。只有处于连接状态、未进入维护模式而且没有 vSphere HA 错误的主机才列入计算范畴。

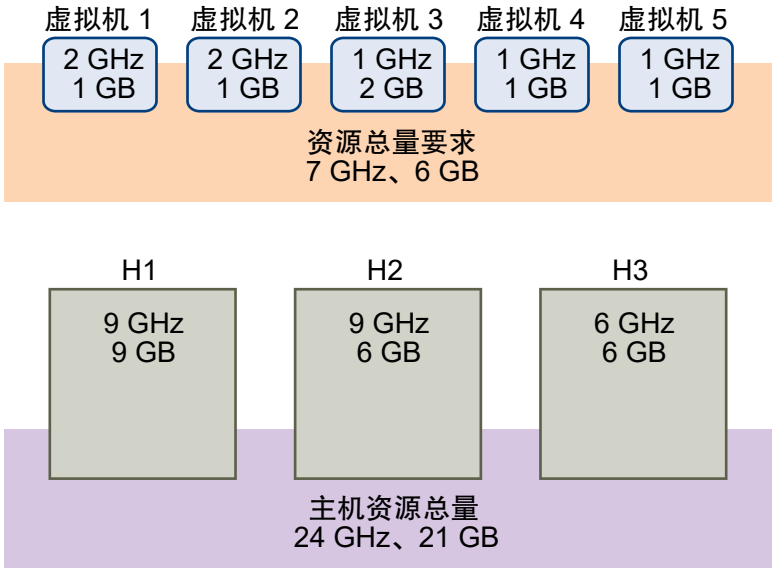
先用主机 CPU 资源总数减去总 CPU 资源要求，然后再用这个结果除以主机 CPU 资源总数，从而计算出“当前的 CPU 故障切换容量”。“当前的内存故障切换容量”的计算方式与之相似。

示例： 使用集群资源百分比进行准入控制

示例中展示了使用此准入控制策略计算和使用“当前故障切换容量”的方式。对集群进行如下假设：

- 集群包括三台主机，每台主机上可用的 CPU 和内存资源数各不相同。第一台主机 (H1) 的可用 CPU 资源和可用内存分别为 9 GHz 和 9 GB，第二台主机 (H2) 为 9 GHz 和 6 GB，而第三台主机 (H3) 则为 6 GHz 和 6 GB。
- 集群内存在五个已打开电源的虚拟机，其 CPU 和内存要求各不相同。VM1 所需的 CPU 资源和内存分别为 2 GHz 和 1 GB，VM2 为 2 GHz 和 1 GB，VM3 为 1 GHz 和 2 GB，VM4 为 1 GHz 和 1 GB，VM5 则为 1 GHz 和 1 GB。
- CPU 和内存的已配置故障切换容量都设置为 25%。

图 2-1. 使用“预留的集群资源的百分比”策略的准入控制示例



已打开电源的虚拟机的总资源要求为 7 GHz CPU 和 6 GB 内存。可用于虚拟机的主机资源总数为 24 GHz CPU 和 21 GB 内存。根据上述情况，“当前的 CPU 故障切换容量”为 70% ((24GHz - 7GHz)/24GHz)。同样，“当前的内存故障切换容量”为 71% ((21GB-6GB)/21GB)。

由于集群的“配置的故障切换容量”设置为 25%，因此仍然可使用 45% 的集群 CPU 资源总数和 46% 的集群内存资源打开其他虚拟机电源。

插槽策略准入控制

使用插槽策略选项，vSphere HA 准入控制允许指定数目的主机出现故障，同时可以确保集群内留有足够的资源来对这些主机上的所有虚拟机进行故障切换。

使用插槽策略时，vSphere HA 通过以下方式执行准入控制：

1 计算插槽大小。

  插槽是内存和 CPU 资源的逻辑表示。默认情况下，会调整插槽的大小来满足集群中任何已打开电源虚拟机的要求。

2 确定集群内每台主机可以拥有的插槽数目。

3 确定集群的当前故障切换容量。

  这是可以发生故障并仍然有足够插槽满足所有已打开电源虚拟机的主机的数目。

4 确定“当前故障切换容量”是否小于“配置的故障切换容量”（由用户提供）。

  如果是，则准入控制不允许执行此操作。

注 您可以从 vSphere Client 中 vSphere HA 设置的准入控制部分设置 CPU 和内存的特定插槽大小。

插槽大小计算


(vSphere HA 插槽大小和准入控制)

插槽大小由两个组件（CPU 和内存）组成。

- vSphere HA 计算 CPU 组件的方法是先获取每台已打开电源虚拟机的 CPU 预留，然后再选择最大值。如果没有为虚拟机指定 CPU 预留，则系统会为其分配一个默认值 32 MHz。可以使用 `das.vmcpuminmhz` 高级选项更改此值。
- vSphere HA 计算内存组件的方法是先获取每台已打开电源虚拟机的内存预留和内存开销，然后再选择最大值。内存预留没有默认值。

如果集群内虚拟机的预留值大小不一致，则会影响插槽大小的计算。为避免出现这种情况，可以使用 `das.slotcpuinmhz` 或 `das.slotmeminmb` 高级选项分别指定插槽大小的 CPU 或内存组件的上限。请参见 vSphere HA 高级选项。

您也可以通过查看需要多个插槽的虚拟机数来确定集群中资源碎片的风险。可以从 vSphere Client 中 vSphere HA 设置的准入控制部分对此进行计算。如果已使用高级选项指定了固定插槽大小或最大插槽大小，则虚拟机可能需要多个插槽。

使用插槽数目计算当前故障切换容量

计算出插槽大小后，vSphere HA 会确定每台主机中可用于虚拟机的 CPU 和内存资源。这些值包含在主机的根资源池中，而不是主机的总物理资源中。可以在 vSphere Client 中主机的**摘要**选项卡上查找 vSphere HA 所用主机的资源数据。如果集群中的所有主机均相同，则可以用集群级别指数除以主机的数量来获取此数据。不包括用于虚拟化目的的资源。只有处于连接状态、未进入维护模式且没有任何 vSphere HA 错误的主机才列入计算范畴。

然后，即可确定每台主机可以支持的最大插槽数目。为确定此数目，请用主机的 CPU 资源数除以插槽大小的 CPU 组件，然后将结果化整。对主机的内存资源数进行同样的计算。然后，比较这两个数字，较小的那个数字即为主机可以支持的插槽数。

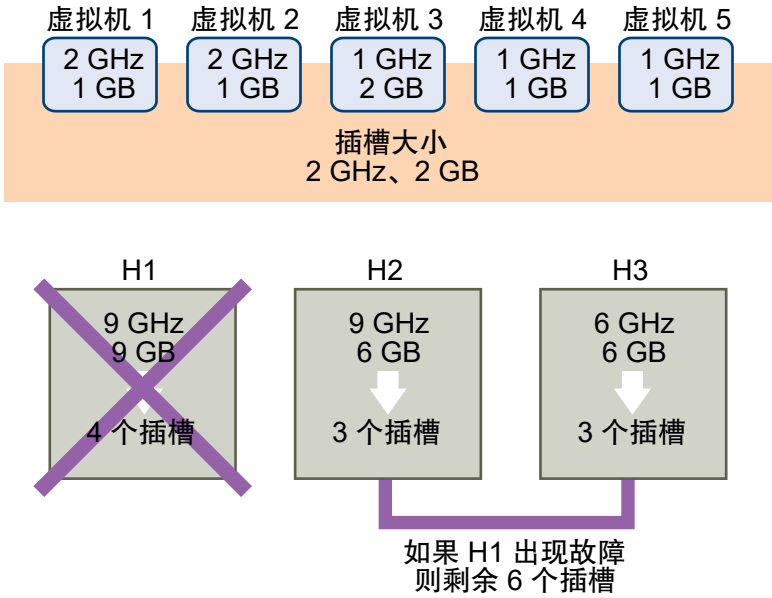
通过确定可以发生故障并仍然有足够插槽满足所有已打开电源虚拟机要求的主机的数目（从最大值开始）来计算当前故障切换容量。

示例： 使用插槽策略的准入控制

示例中展示了使用此准入控制策略计算和使用插槽大小的方式。对集群进行如下假设：

- 集群包括三台主机，每台主机上可用的 CPU 和内存资源数各不相同。第一台主机 (H1) 的可用 CPU 资源和可用内存分别为 9 GHz 和 9 GB，第二台主机 (H2) 为 9 GHz 和 6 GB，而第三台主机 (H3) 则为 6 GHz 和 6 GB。
- 集群内存在五个已打开电源的虚拟机，其 CPU 和内存要求各不相同。VM1 所需的 CPU 资源和内存分别为 2 GHz 和 1 GB，VM2 为 2 GHz 和 1 GB，VM3 为 1 GHz 和 2 GB，VM4 为 1 GHz 和 1 GB，VM5 则为 1 GHz 和 1 GB。
- “集群允许的主机故障数目”设置为 1。

图 2-2. 使用“集群允许的主机故障数目”策略的准入控制示例



1 比较虚拟机的 CPU 和内存要求，然后选择最大值，从而计算出插槽大小。

   最大 CPU 要求（由 VM1 和 VM2 共享）为 2 GHz，而最大内存要求（针对 VM3）为 2 GB。根据上述情况，插槽大小为 2 GHz CPU 和 2 GB 内存。

2 由此可确定每台主机可以支持的最大插槽数目。

   H1 可以支持四个插槽。H2 可以支持三个插槽（取 9GHz/2GHz 和 6GB/2GB 中较小的一个），H3 也可以支持三个插槽。

3 计算出当前故障切换容量。

   最大的主机是 H1，如果它发生故障，集群内还有六个插槽，足够供所有五个已打开电源的虚拟机使用。如果 H1 和 H2 都发生故障，集群内将仅剩下三个插槽，这是不够用的。因此，当前故障切换容量为 1。

集群内可用插槽的数目为 1（H2 和 H3 上的六个插槽减去五个已使用的插槽）。

专用故障切换主机准入控制

在配置 vSphere HA 时可以将特定主机指定为故障切换主机。

借助专用故障切换主机准入控制，在主机发生故障时，vSphere HA 将尝试在任一指定的故障切换主机上重新启动其虚拟机。如果无法重新启动虚拟机（例如，故障切换主机发生故障或者资源不足时），vSphere HA 会尝试在集群内的其他主机上重新启动这些虚拟机。

为了确保故障切换主机上拥有可用的空闲容量，将阻止您打开虚拟机电源或使用 vMotion 将虚拟机迁移到故障切换主机。而且，为了保持负载平衡，DRS 也不会使用故障切换主机。

注 如果使用专用故障切换主机准入控制，并指定多个故障切换主机，则 DRS 不会尝试对故障切换主机上运行的虚拟机实施虚拟机-虚拟机关联性规则。

vSphere HA 互操作性

vSphere HA 可以与其他功能进行交互操作，如 DRS 和 vSAN。

在配置 vSphere HA 之前，应了解其与其他功能或产品进行交互操作的限制。

将 vSphere HA 与 vSAN 配合使用

可以使用 vSAN 作为 vSphere HA 集群的共享存储。如果已激活，vSAN 会将主机上指定的本地可用存储磁盘汇聚到所有主机共享的单个数据存储中。

要将 vSphere HA 与 vSAN 配合使用，必须注意针对这两种功能的互操作性的某些注意事项和限制。

有关 vSAN 的信息，请参见管理 VMware vSAN。

注 可以将 vSphere HA 与 vSAN 延伸集群配合使用。

ESXi 主机要求

仅当满足以下条件时，才能将 vSAN 与 vSphere HA 集群配合使用：

- 集群中所有 ESXi 主机的版本必须全部为 5.5 或更高版本。
- 集群必须最低具有三个 ESXi 主机。

网络连接差异

vSAN 具有自己的网络。如果为同一集群激活 vSAN 和 vSphere HA，HA 代理间流量将流经此存储网络，而非管理网络。仅当停用 vSAN 时，vSphere HA 才使用管理网络。当主机上配置了 vSphere HA 时，vCenter Server 会选择合适的网络。

注 仅当停用 vSphere HA 时，才可以激活 vSAN。

如果您更改了 vSAN 网络配置，vSphere HA 代理将不自动获取新网络设置。要更改 vSAN 网络，必须在 vSphere Client 中执行以下步骤：

1 停用 vSphere HA 集群的主机监控。

2 更改 vSAN 网络。

3 右键单击集群中的所有主机，然后选择**重新配置 vSphere HA**。

4 重新激活 vSphere HA 集群的主机监控。

表 2-2. vSphere HA 网络连接差异显示了使用和不使用 vSAN 时 vSphere HA 网络连接中的差异。

表 2-2. vSphere HA 网络连接差异

	vSAN 已激活	vSAN 已停用
vSphere HA 使用的网络	vSAN 存储网络	管理网络
检测信号数据存储	挂载到 1 个以上主机的任何数据存储，但非 vSAN 数据存储	挂载到 1 个以上主机的任何数据存储
声明已隔离的主机	隔离地址不可 ping，并且 vSAN 存储网络无法访问	隔离地址不可 ping，并且管理网络无法访问

容量预留设置

通过准入控制策略为 vSphere HA 集群预留容量时，必须与确保出现故障时的数据可访问性的相应 vSAN 设置协商此设置。具体来说，vSAN 规则集中的“允许的故障数目”设置不得低于 vSphere HA 准入控制设置预留的容量。

例如，如果 vSAN 规则集仅允许两个故障，则 vSphere HA 准入控制策略预留的容量只能等于一个或两个主机故障。如果您为具有八个主机的集群使用“预留的集群资源的百分比”策略，则预留的容量不得超过集群资源的 25%。在同一集群中，使用“集群允许的主机故障数目”策略时，该设置不得大于两个主机。如果 vSphere HA 预留的容量较少，则故障切换活动可能不可预知。如果预留太多容量，则会过分限制打开虚拟机的电源和集群间 vSphere vMotion 迁移操作。

结合使用 vSphere HA 和 DRS

将 vSphere HA 和 Distributed Resource Scheduler (DRS) 一起使用，可将自动故障切换与负载均衡相结合。这种结合会在 vSphere HA 将虚拟机移至其他主机后生成一个更均衡的集群。

vSphere HA 执行故障切换并在其他主机上重新启动虚拟机时，其首要的优先级是所有虚拟机的立即可用性。虚拟机重新启动后，其上打开虚拟机电源的主机可能会负载过重，而其他主机的负载则相对较轻。vSphere HA 会使用虚拟机的 CPU、内存预留和开销内存来确定主机是否有足够的空闲容量容纳虚拟机。

在结合使用 DRS 和 vSphere HA 并且启用了接入控制的集群内，可能不会从正在进入维护模式的主机上撤出虚拟机。这种行为的出现是由于用于重新启动虚拟机的预留资源出现了故障。必须使用 vMotion 将虚拟机手动迁出主机。

在某些情况下，vSphere HA 可能由于资源限制而无法对虚拟机进行故障切换。这种情况的出现有多种原因。

- 停用了 HA 接入控制，但激活了 Distributed Power Management (DPM)。这会导致 DPM 将虚拟机整合到较少数量的主机上，并将空主机置于待机模式，使得没有足够的已打开电源容量来执行故障切换。
- 虚拟机-主机关联性规则（必需）可能会限制可以容纳某些虚拟机的主机。
- 可能有足够多的聚合资源，但这些资源在多台主机上是资源碎片，因此虚拟机无法使用它们进行故障切换。

在这些情况下，vSphere HA 可使用 DRS 尝试调整集群（例如，通过使主机退出待机模式或者迁移虚拟机以整理集群资源碎片），以便 HA 可以执行故障切换。

如果 DPM 处于手动模式，则可能需要确认主机打开电源建议。同样，如果 DRS 处于手动模式，可能需要确认迁移建议。

如果要使用虚拟机-主机关联性规则，请注意不能违反这些规则。如果执行故障切换违反这样的规则，则 vSphere HA 将不会执行故障切换。

有关 DRS 的详细信息，请参见《vSphere 资源管理》文档。

注 vSphere DRS 是 vSphere 的一项重要功能，要维持在 vSphere 集群内运行的工作负载正常运行，必须使用此功能。从 vSphere 7.0 Update 1 开始，DRS 依赖于 vCLS 虚拟机的可用性。有关详细信息，请参见《vSphere 资源管理》中的“vSphere 集群服务 (vCLS)”。

vSphere HA 和 DRS 关联性规则

如果为集群创建 DRS 关联性规则，可以指定在虚拟机故障切换过程中 vSphere HA 应用此规则的方式。

您可以为以下两种类型的规则指定 vSphere HA 故障切换行为：

- 虚拟机反关联性规则在故障切换操作过程中强制指定的虚拟机保持分离。
- 虚拟机-主机关联性规则在故障切换操作过程中将指定的虚拟机放在特定主机或一组定义主机的成员上。

编辑 DRS 关联性规则时，必须使用 vSphere HA 高级选项强制执行 vSphere HA 的所需故障切换行为。

- **HA 必须在故障切换期间遵守虚拟机反关联性规则** -- 当设置了虚拟机反关联性规则的高级选项时，如果对虚拟机进行故障切换违反规则，则 vSphere HA 不会进行故障切换。而是，vSphere HA 会发出一个事件，报告资源不足，无法执行故障切换。
- **HA 应在故障切换过程中遵守虚拟机-主机关联性规则** -- vSphere HA 尝试将具有此规则的虚拟机放在指定的主机上（如果可能）。

有关更多信息，请参见“vSphere HA 高级选项”。

注 如果在设置规则后不久（默认情况下，在 5 分钟内）发生主机故障，vSphere HA 可以重新启动已停用 DRS 的集群中的虚拟机，以替代虚拟机-主机关联性规则映射。

其他 vSphere HA 互操作性问题

要使用 vSphere HA，必须注意以下其他互操作性问题。

虚拟机组件保护

虚拟机组件保护 (VMCP) 具有以下互操作性问题和限制：

- VMCP 不支持 vSphere Fault Tolerance。如果对使用 Fault Tolerance 的集群启用了 VMCP，受影响的 FT 虚拟机将自动接收停用 VMCP 的替代项。
- VMCP 无法检测或响应 vSAN 数据存储上文件的可访问性问题。如果虚拟机的配置和 VMDK 文件仅位于 vSAN 数据存储上，则它们不受 VMCP 保护。
- VMCP 不会检测或响应位于 Virtual Volumes 数据存储上的文件的可访问性问题。如果虚拟机的配置和 VMDK 文件仅位于 Virtual Volumes 数据存储上，则它们不受 VMCP 保护。

- VMCP 不会防止不可访问的裸设备映射 (RDM)。

IPv6

如果观察到以下注意事项，可以将 vSphere HA 与完全受支持的 IPv6 网络配置一起使用：

- 集群仅包含 ESXi 6.0 或更高版本的主机。
- 必须使用相同的 IP 版本（IPv6 或 IPv4）配置集群中所有主机的管理网络。vSphere HA 集群不能同时包含这两种类型的网络连接配置。
- vSphere HA 使用的网络隔离地址必须与集群用于其管理网络的 IP 版本匹配。
- 不能在 vSphere HA 集群中同时使用 vSAN 和 IPv6。

除了之前的限制外，不支持将以下类型的 IPv6 地址用于 vSphere HA 隔离地址或管理网络：本地链接、ORCHID、具有区域索引的本地链接。此外，不能将环回地址类型用于管理网络。

注 要将现有 IPv4 部署升级到 IPv6，必须先停用 vSphere HA。

创建 vSphere HA 集群

vSphere HA 在 ESXi（或旧版 ESX）主机集群的环境中运行。必须创建集群，然后用主机填充集群，并配置 vSphere HA 设置，才能建立故障切换保护。

创建 vSphere HA 集群时，必须配置许多可决定功能如何运行的设置。在此之前，请确定集群的节点。这些节点是为支持虚拟机而提供资源，并且将由 vSphere HA 用于故障切换保护的 ESXi 主机。然后应当确定如何互相连接这些节点，以及如何将这些节点连接到虚拟机数据所在的共享存储。在建立好网络架构后，可以将主机添加到集群并完成 vSphere HA 配置。

将主机节点添加到集群之前，可以激活和配置 vSphere HA。但是，在将主机添加到集群之前，集群的所有功能并非都能运行，部分集群设置不可用。例如，在出现可以指定为故障切换主机的主机之前，“指定故障切换主机”准入控制策略不可用。

注 对处于（或移入）vSphere HA 集群中的主机上的所有虚拟机停用“虚拟机启动和关机”（自动启动）功能。与 vSphere HA 配合使用时，不支持自动启动。

vSphere HA 对照表

vSphere HA 对照表包含在创建和使用 vSphere HA 集群之前必须了解的要求。

在设置 vSphere HA 集群之前，应查看此列表。有关详细信息，请遵循相应的交叉引用。

- 所有主机必须获得 vSphere HA 许可。
- 集群必须至少包含两个主机。
- 必须为所有主机配置静态 IP 地址。如果使用的是 DHCP，必须确保每台主机的地址在重新引导期间保留。

- 所有主机必须至少有一个共有的管理网络。最佳做法是至少有两个共有的管理网络。您应使用已启用**管理流量**复选框的 VMkernel 网络。这些网络必须能够相互访问，且管理网络上的 vCenter Server 和主机必须能够相互访问。请参见《网络连接的最佳做法》。
- 为了确保任何虚拟机都可以在集群内的任何主机上运行，所有主机都必须可以访问相同的虚拟机网络和数据存储。同样，虚拟机必须位于共享而非本地存储器上，否则在主机出现故障时它们将无法进行故障切换。

  注 vSphere HA 使用数据存储信号检测来区分已分区的主机、已隔离的主机和出现故障的主机。因此，如果环境中有更可靠的数据存储，请将 vSphere HA 配置为优先考虑这些数据存储。

- 为了使虚拟机监控工作，必须安装 VMware Tools。请参见《虚拟机和应用程序监控》。
- vSphere HA 同时支持 IPv4 和 IPv6。有关使用 IPv6 时的注意事项，请参见其他 vSphere HA 互操作性问题 。
- 为使虚拟机组件保护能够正常运行，主机必须已启用全部路径异常 (APD) 超时功能。
- 要使用虚拟机组件保护，集群必须包含 ESXi 6.0 或更高版本的主机。
- 仅可使用包含 ESXi 6.0 或更高版本主机的 vSphere HA 集群来启用 VMCP。包含早期版本主机的集群无法启用 VMCP，且无法将此类主机添加到已启用 VMCP 的集群中。
- 如果您的集群使用虚拟卷数据存储，当启用了 vSphere HA 时，vCenter Server 会在每个数据存储上创建一个配置虚拟卷。vSphere HA 将其使用的文件存储在这些容器中以保护虚拟机。如果您删除这些容器，vSphere HA 将无法正常运行。每个虚拟卷数据存储仅创建一个容器。

在 vSphere Client 中创建 vSphere HA 集群

要为集群启用 vSphere HA，必须先创建空集群。规划集群的资源和网络架构后，可使用 vSphere Client 将主机添加到集群中，并指定集群的 vSphere HA 设置。

启用了 vSphere HA 的集群是 vSphere Fault Tolerance 的必备条件。

前提条件

- 确认所有虚拟机及其配置文件都驻留在共享存储上。
- 验证是否已将主机配置为访问共享存储，以便您可以通过使用集群中的不同主机打开虚拟机电源。
- 确认主机配置为具有虚拟机网络的访问权限。
- 确认正在为 vSphere HA 使用冗余管理网络连接。有关设置网络冗余的信息，请参见网络连接的最佳做法。
- 确认至少已为主机配置两个数据存储，来为 vSphere HA 数据存储检测信号提供冗余。
- 使用具有集群管理员权限的帐户将 vSphere Client 连接到 vCenter Server。

步骤

1 在 vSphere Client 中，浏览到希望集群驻留的数据中心，然后单击**新建集群**。

2 完成**新建集群**向导。

请不要打开 vSphere HA（或 DRS）。

3 单击**确定**关闭向导并创建空集群。

4 根据您的集群资源和网络架构计划，使用 vSphere Client 将主机添加到集群。

5 浏览到集群并启用 vSphere HA。

a 单击**配置**选项卡。

b 选择 **vSphere 可用性**，然后单击**编辑**。

c 选择 **vSphere HA**。

6 在**故障和响应**下，选择**启用主机监控**。

启用主机监控后，集群中的主机可以交换网络检测信号，vSphere HA 可以在检测到故障时采取措施。主机监控是 vSphere Fault Tolerance 恢复进程正常运行所必需的。

7 为**虚拟机监控**选择一项设置。

如果在设置的时间内没有收到单个虚拟机的检测信号，请选择**仅虚拟机监控**以重新启动该虚拟机。也可以选择**虚拟机和应用程序监控**来启用应用程序监控。

8 单击**确定**。

结果

此时即已拥有包含主机的 vSphere HA 集群。

后续步骤

为集群配置相应的 vSphere HA 设置。

- 故障和响应
- 准入控制
- 检测信号数据存储
- 高级选项

请参见配置 vSphere 可用性设置。

配置 vSphere 可用性设置

创建 vSphere HA 集群时或配置现有集群时，必须配置可决定功能如何运行的设置。

在 vSphere Client 中，您可以配置以下 vSphere HA 设置：

故障和响应

在此处提供关于主机故障响应、主机隔离、虚拟机监控和虚拟机组件保护的设置。

准入控制

激活或停用 vSphere HA 集群的准入控制，并选择如何实施的策略。

检测信号数据存储

为 vSphere HA 用于数据存储检测信号的数据存储指定首选项。

高级选项

通过设置高级选项来自定义 vSphere HA 行为。

配置故障响应

利用 vSphere HA 设置的**故障和响应**窗格，可以配置遇到问题时集群的响应方式。

在 vSphere Client 的此部分，可以确定 vSphere HA 集群针对主机故障和隔离做出的特定响应。还可以配置出现永久设备丢失 (PDL) 和全部路径异常 (APD) 状况时的虚拟机组件保护 (VMCP) 操作，并且可以启用虚拟机监控。

可以执行的任务包括：

步骤

1 响应主机故障

您可以针对 vSphere HA 集群中发生的主机故障设置特定响应。

2 响应主机隔离

您可以针对 vSphere HA 集群中发生的主机隔离设置特定响应。

3 配置 VMCP 响应

配置当数据存储遇到 PDL 或 APD 故障时，虚拟机组件保护 (VMCP) 采取的响应。

4 启用虚拟机监控

您可以打开虚拟机和应用程序监控，并设置 vSphere HA 集群的监控敏感度。

响应主机故障

您可以针对 vSphere HA 集群中发生的主机故障设置特定响应。

仅当激活 vSphere HA 后，此页面才可编辑。

步骤

1 在 vSphere Client 中，浏览到 vSphere HA 集群。

2 单击**配置**选项卡。

3 选择 **vSphere 可用性**，然后单击**编辑**。

4 单击**故障和响应**，然后展开**主机故障响应**。

5 选择以下配置选项。

选项	描述
故障响应	如果选择**已禁用**，发生主机故障时，此设置会关闭主机监控，且不会重新启动虚拟机。如果选择**重新启动虚拟机**，发生主机故障时，虚拟机会基于重新启动优先级进行故障切换。
默认虚拟机重新启动优先级	重新启动优先级用于确定主机发生故障时虚拟机的重新启动顺序。优先级较高的虚拟机将首先启动。如果多个主机发生故障，将首先迁移优先级最高的主机上的所有虚拟机，然后迁移优先级第二高的主机上的所有虚拟机，以此类推。
虚拟机重新启动优先级条件	必须选择特定条件以及满足该条件后的延迟，然后才允许 vSphere HA 继续下一个虚拟机重新启动优先级。

6 单击**确定**。

结果

您的主机故障响应设置将生效。

响应主机隔离

您可以针对 vSphere HA 集群中发生的主机隔离设置特定响应。

仅当激活 vSphere HA 后，此页面才可编辑。

步骤

1 在 vSphere Client 中，浏览到 vSphere HA 集群。

2 单击**配置**选项卡。

3 选择 **vSphere 可用性**，然后单击**编辑**。

4 单击**故障和响应**并展开**针对主机隔离的响应**。

5 要配置主机隔离响应，请选择**已禁用**、**关闭再重新启动虚拟机**或**关闭虚拟机电源并重新启动虚拟机**。

6 单击**确定**。

结果

您的主机隔离响应设置将生效。

配置 VMCP 响应

配置当数据存储遇到 PDL 或 APD 故障时，虚拟机组件保护 (VMCP) 采取的响应。

仅当激活 vSphere HA 后，此页面才可编辑。

步骤

1 在 vSphere Client 中，浏览到 vSphere HA 集群。

2 单击**配置**选项卡。

3 选择 **vSphere 可用性**，然后单击**编辑**。

4 单击**故障和响应**，然后展开**处于 PDL 状态的数据存储**或**处于 APD 状态的数据存储**。

5 如果单击**处于 PDL 状态的数据存储**，则可以将此类问题的 VMCP 故障响应设置为**已禁用**、**发布事件**或**关闭虚拟机电源并重新启动虚拟机**。

6 如果单击**处于 APD 状态的数据存储**，则可以将此类问题的 VMCP 故障响应设置为**禁用**、**发布事件**、**关闭虚拟机电源并重新启动虚拟机 - 保守的重新启动策略**或**关闭虚拟机电源并重新启动虚拟机 - 激进的重新启动策略**。您还可以设置**响应恢复**，即 VMCP 在采取操作之前等待的分钟数。

7 单击**确定**。

结果

您的 VMCP 故障响应的设置将生效。

启用虚拟机监控

您可以打开虚拟机和应用程序监控，并设置 vSphere HA 集群的监控敏感度。

仅当启用 vSphere HA 后，此页面才可编辑。

步骤

1 在 vSphere Client 中，浏览到 vSphere HA 集群。

2 单击**配置**选项卡。

3 选择 **vSphere 可用性**，然后单击**编辑**。

4 单击**故障和响应**，然后展开**虚拟机监控**。

5 选择**虚拟机监控**和**应用程序监控**。

这些设置会分别启用 VMware Tools 检测信号和应用程序检测信号。

6 要设置检测信号监控敏感度，请在**低**和**高**之间移动滑块，或者选择**自定义**以提供自定义设置。

7 单击**确定**。

结果

监控设置将生效。

配置 Proactive HA

您可以配置当提供程序通知 vCenter 其运行状况降级（表示主机出现部分故障）时 Proactive HA 的响应方式。

启用 vSphere DRS 后，才能编辑此页面。

步骤

1 在 vSphere Client 中，浏览到 Proactive HA 集群。

2 单击**配置**选项卡。

3 选择 **vSphere 可用性**，然后单击**编辑**。

4 选择**启用 Proactive HA**。

5 单击 **Proactive HA 故障和响应**。

6 选择以下配置选项。

选项	描述
自动化级别	确定主机隔离或维护模式和虚拟机迁移是建议还是自动执行。 ■ **手动**。vCenter Server 会给出虚拟机的迁移建议。 ■ **自动**。虚拟机将迁移到正常主机，降级主机将进入隔离或维护模式，具体取决于配置的 Proactive HA 自动化级别。
修复	确定对部分降级的主机执行的操作。 ■ **对所有故障应用隔离模式**。在虚拟机性能不受影响的情况下，通过避免使用部分降级的主机来平衡性能和可用性。 ■ **对中等故障应用隔离模式并对严重故障应用维护模式 (混合)**。在虚拟机性能不受影响的情况下，通过避免使用适度降级的主机来平衡性能和可用性。确保虚拟机不在出现严重故障的主机上运行。 ■ **对所有故障应用维护模式**。确保虚拟机不在出现部分故障的主机上运行。 将主机置于隔离模式和维护模式分别需要 `Host.Config.Quarantine` 和 `Host.Config.Maintenance` 特权。

要为该集群启用 Proactive HA 提供程序，请选中相应的复选框。安装了提供程序对应的 vSphere Client 插件时提供程序会显示，并且提供程序会监控集群中的每个主机。要查看或编辑提供程序支持的故障状况，请单击编辑链接。

7 单击**确定**。

配置准入控制

创建集群后，可以配置准入控制，以指定虚拟机违反可用性限制时是否可以启动它们。集群会预留资源，以便在指定数量的主机上对所有正在运行的虚拟机进行故障切换。

“准入控制”页面仅在激活了 vSphere HA 时才会显示。

步骤

1 在 vSphere Client 中，浏览到 vSphere HA 集群。

2 单击**配置**选项卡。

3 选择 **vSphere 可用性**，然后单击**编辑**。

4 单击**准入控制**以显示配置选项。

5 为**集群允许的主机故障数目**选择一个数字。这是集群能够进行恢复或者确保进行故障切换所允许的最大主机故障数。

6 为**主机故障切换容量的定义依据**选择一个选项。

选项	描述
集群资源百分比	指定为了支持故障切换而作为备用容量保留的集群 CPU 和内存资源的百分比。
插槽策略 (已打开电源的虚拟机)	选择可覆盖所有打开电源的虚拟机或为固定大小的插槽大小策略。您还可以计算有多少个虚拟机需要多个插槽。
专用故障切换主机	选择要用于进行故障切换操作的主机。默认故障切换主机没有足够的资源时，仍可在集群内的其他主机上进行故障切换。
已禁用	选择此选项将停用准入控制，并允许在违反可用性限制时打开虚拟机电源。

7 为**虚拟机允许的性能降低**设置百分比。

此设置确定故障期间集群中的虚拟机允许的性能降低百分比。

8 单击**确定**。

结果

准入控制设置将生效。

配置检测信号数据存储

vSphere HA 使用数据存储检测信号区分出现故障的主机和位于网络分区上的主机。利用数据存储检测信号，当发生管理网络分区时，vSphere HA 可以监控主机并继续响应故障。

您可以指定要用于数据存储检测信号的数据存储。

步骤

1 在 vSphere Client 中，浏览到 vSphere HA 集群。

2 单击**配置**选项卡。

3 选择 **vSphere 可用性**，然后单击**编辑**。

4 单击**检测信号数据存储**以显示数据存储检测信号的配置选项。

5 要指示 vSphere HA 如何选择数据存储以及如何处理首选项，请从以下选项中选择：

表 2-3.

数据存储检测信号选项
自动选择可从以下主机访问的数据存储
仅使用指定列表中的数据存储
使用指定列表中的数据存储并根据需要自动补充

6 在“可用检测信号数据存储”窗格中，选择要用于检测信号的数据存储。

列出的数据存储由 vSphere HA 集群中的多个主机共享。选择了某个数据存储后，下方的窗格将显示 vSphere HA 集群中可访问此数据存储的所有主机。

7 单击**确定**。

设置高级选项

要自定义 vSphere HA 行为，请设置高级 vSphere HA 选项。

前提条件

确认您具有集群管理员特权。

注 因为这些选项会影响 vSphere HA 的运行，所以更改时请小心谨慎。

步骤

1 在 vSphere Client 中，浏览到 vSphere HA 集群。

2 单击**配置**选项卡。

3 选择 **vSphere 可用性**，然后单击**编辑**。

4 单击**高级选项**。

5 单击**添加**，然后在文本框中键入高级选项的名称。

您可在“值”列的文本框中设置选项的值。

6 针对要添加的每个新选项重复执行第 5 步，然后单击**确定**。

结果

集群即会使用您已添加或修改的选项。

后续步骤

设置高级 vSphere HA 选项后，它将保持不变，直到您执行以下操作之一：

- 使用 vSphere Client 将其值重置为默认值。
- 从集群中所有主机上的 fdm.cfg 文件中手动编辑或删除此选项。

vSphere HA 高级选项

您可以设置影响 vSphere HA 集群的行为的高级选项。

表 2-4. vSphere HA 高级选项

选项	描述
das.isolationaddress[...]	设置为了确定主机是否与网络隔离而要 ping 的地址。只有当未从集群内的任何其他主机接收到检测信号时才 ping 此地址。如果未指定，则使用管理网络的默认网关。此默认网关必须是可用的可靠地址，以便主机可以确定它是否与网络隔离。可以为集群指定多个隔离地址（最多 10 个）：das.isolationAddressX，其中 X = 0-9。通常每个管理网络应指定一个隔离地址。如果指定的地址太多，则进行隔离检测所需的时间将会较长。
das.usedefaultisolationaddress	默认情况下，vSphere HA 使用控制台网络的默认网关作为隔离地址。此选项指定是否使用此默认设置 (true|false)。
das.isolationshutdowntimeout	关闭虚拟机电源之前，系统等待虚拟机关机的时间段。只有在主机的隔离响应为“关闭虚拟机”时，此选项才适用。默认值为 300 秒。
das.slotmeminmb	定义内存插槽大小的最大限制。如果使用此选项，则插槽大小小于该值，或是小于集群内任何已打开电源虚拟机的最大内存预留以及内存开销。
das.slotcpuinmhz	定义 CPU 插槽大小的最大限制。如果使用此选项，则插槽大小小于该值，或是小于集群内任何已打开电源虚拟机的最大 CPU 预留。
das.vmmemoryminmb	定义在没有指定虚拟机内存预留或者内存预留为零时，分配给虚拟机的默认内存资源值。用于“集群允许的主机故障数目”准入控制策略。如果未指定任何值，则默认值为 0 MB。
das.vmcpuminmhz	定义在没有指定虚拟机 CPU 预留或者内存预留为零时，分配给虚拟机的默认 CPU 资源值。用于“集群允许的主机故障数目”准入控制策略。如果未指定任何值，则默认值为 32 MHz。
das.iostatsinterval	更改虚拟机监控敏感度的默认 I/O 统计间隔。默认值为 120（秒）。可以设置为大于或等于 0 的任何值。设置为 0 将停用该检查。 **注** 建议不要使用小于 50 的值，因为较小的值可能会导致 vSphere HA 意外重置虚拟机。
das.ignoreinsufficienthbdatastore	如果主机不具有足够的 vSphere HA 检测信号数据存储，则停用创建的配置问题。默认值为 false。
das.heartbeatdsperhost	更改所需的检测信号数据存储的数量。有效值范围为 2 至 5，默认值为 2。
das.config.fdm.isolationPolicyDelaySec	在确定主机被隔离后执行隔离策略之前系统等待的秒数。最小值为 30。如果设置的值小于 30，延迟时间将为 30 秒。

表 2-4. vSphere HA 高级选项 （续）

选项	描述
das.respectvmvmantiaffinityrules	确定 vSphere HA 是否强制执行虚拟机间反关联性规则。默认值为“true”，该设置会强制执行规则（即使未激活 vSphere DRS）。在此情况下，如果对虚拟机进行故障切换违反规则，则 vSphere HA 不会进行故障切换，但会发出一个事件，报告资源不足，无法执行故障切换。此选项还可以设置为“false”，该设置不会强制执行规则。 有关反关联性规则的详细信息，请参见《vSphere 资源管理》。
das.maxresets	VMCP 进行重置尝试的最大次数。如果受 APD 状况影响的虚拟机上的重置操作失败，VMCP 将在放弃之前重试此操作许多次
das.maxterminates	VMCP 进行虚拟机终止重试的最大次数。
das.terminateretryintervalsec	如果 VMCP 无法终止虚拟机，这是它重试终止尝试之前系统等待的秒数
das.config.fdm.reportfailoverfailevent	如果设置为 1，则在 vSphere HA 尝试重新启动虚拟机失败时激活详细的每虚拟机事件生成。默认值为 0。在早于 vSphere 6.0 的版本中，会默认生成此事件。
vpxd.das.completemetadataupdateintervalsec	设置虚拟机-主机关联性规则后的时间段（秒），在该时间段内，vSphere HA 可以重新启动已停用 DRS 的集群中的虚拟机以替代此规则。默认值为 300 秒。
das.config.fdm.memReservationMB	默认情况下，vSphere HA 代理运行时的配置内存限制为 250 MB。如果主机用尽可预留的容量，主机可能不允许此预留。您可以使用此高级选项来降低内存限制以避免此问题。仅可指定大于 100（最小值）的整数。相反，为防止在大型集群（包含 6,000 至 8,000 个虚拟机）的主代理选举期间出现问题，应将此限制增加至 325 MB。 **注** 此限制更改后，必须为集群中的所有主机运行重新配置 HA 任务。另外，在将新主机添加到集群或重新引导现有主机时，应对这些主机执行此任务以便更新此内存设置。
das.reregisterrestartdisabledvms	在某个特定虚拟机上停用 vSphere HA 时，此选项确保该虚拟机会在故障后在其他主机上进行注册。这使您能够打开该虚拟机的电源，而无需手动重新注册。 **注** 使用此选项时，vSphere HA 不会打开虚拟机的电源，而是仅注册该虚拟机。
das.respectvmhostsoftaffinityrules	确定 vSphere HA 是否在属于同一虚拟机-主机组的主机上重新启动相应的 VM。如果没有这样的主机可用，或者如果此选项的值设置为“false”，vSphere HA 将在集群中的任何可用主机上重新启动虚拟机。在 vSphere 6.5 或更高版本中，默认值为 true 可能不会在集群的高级 HA 选项中明显地定义此值。如果您要停用该选项，必须在集群的高级 HA 选项中手动将此选项设置为 false。

注 如果更改以下任一高级选项的值，则必须停用 vSphere HA，再重新激活它，更改才会生效。

- `das.isolationaddress[...]`
- `das.usedefaultisolationaddress`
- `das.isolationshutdowntimeout`

自定义单个虚拟机

vSphere HA 集群中的每个虚拟机均分配了“虚拟机重新启动优先级”、“主机隔离响应”、“虚拟机组件保护”和“虚拟机监控”的集群默认设置。可以通过更改这些默认项来指定每个虚拟机的特定行为。如果虚拟机离开该集群，则将丢弃这些设置。

步骤

1. 在 vSphere Client 中，浏览到 vSphere HA 集群。
2. 单击**配置**选项卡。
3. 在“配置”下，选择**虚拟机替代项**，然后单击**添加**。
4. 使用 **+** 按钮选择要将替代项应用到的虚拟机。
5. 单击**确定**。
6. （可选） 您可以更改其他设置，如**自动化级别**、**虚拟机重新启动优先级**、**针对主机隔离的响应**、VMCP 设置、**虚拟机监控**或**虚拟机监控敏感度**设置。

   注 您可先后展开**相关集群设置**和 **vSphere HA**，查看这些设置的集群默认值。
7. 单击**确定**。

结果

现在，对于更改的每项设置，虚拟机的行为将不同于集群默认值。

适用于 VMware vSphere® High Availability 集群的最佳做法

为确保获得最佳 vSphere HA 集群性能，您必须遵循某些最佳做法。本节重点介绍适用于 vSphere HA 集群的一些主要的最佳做法。

您也可以参考《vSphere High Availability 部署最佳做法》出版物了解更多信息。

网络连接的最佳做法

请遵守以下针对主机网卡配置和 vSphere HA 的网络拓扑的最佳做法。最佳做法包括对 ESXi 主机的建议，以及对电缆、交换机、路由器和防火墙的建议。

网络配置和维护

下列网络维护建议可以帮助您避免对由于丢失 vSphere HA 检测信号而发生故障的主机和网络隔离的意外检测。

- 更改集群 ESXi 主机所在网络时，请挂起主机监控功能。更改网络硬件或网络设置会中断 vSphere HA 用于检测主机故障的检测信号，这可能导致不必要的虚拟机故障切换尝试。
- 在 ESXi 主机上更改网络连接配置时（例如，添加端口组或移除 vSwitch），请挂起主机监控。在对网络连接配置进行更改之后，您必须在集群中的所有主机上重新配置 vSphere HA，从而能够重新检查网络信息。然后重新启用主机监控。

注 由于网络是 vSphere HA 的一个重要组件，因此，如果必须执行网络维护，请通知 vSphere HA 管理员。

用于 vSphere HA 通信的网络

要标识哪些网络操作可能会中断 vSphere HA 的运行，必须了解哪些管理网络用于检测信号和其他 vSphere HA 通信。

- 在集群中的旧版 ESX 主机上，vSphere HA 通信通过被指定为服务控制台网络的所有网络进行传输。这些主机没有将 VMkernel 网络用于 vSphere HA 通信。要在 ESX 控制台网络子集中包含 vSphere HA 流量，请使用 `allowedNetworks` 高级选项。
- 在集群中的 ESXi 主机上，默认情况下，vSphere HA 通信通过 VMkernel 网络进行传输。在 ESXi 主机上，如果不使用 vCenter Server 所用的网络与 vSphere HA 主机进行通信，您必须明确启用**管理流量**复选框。

要保留已指定网络上的 vSphere HA 代理流量，请配置主机，以便 vSphere HA 所使用的 vmkNIC 不会与用于其他用途的 vmkNIC 共享子网。如果至少为 vSphere HA 管理流量配置了一个 vmkNIC，则 vSphere HA 代理将使用与给定子网关联的任一 pNIC 发送数据包。因此，要确保网络流量分离，vSphere HA 以及其他功能所使用的 vmkNIC 必须位于不同的子网上。

网络隔离地址

网络隔离地址是要 ping 的 IP 地址，以确定主机是否与网络隔离。只有当主机已停止从集群内的任何其他主机接收检测信号时才 ping 此地址。如果主机可以 ping 其网络隔离地址，则说明该主机并未与网络隔离，并且集群内的其他主机已出现故障或网络分区。但是，如果主机无法 ping 其隔离地址，则可能该主机已与网络隔离，并且不会执行故障切换操作。

默认情况下，网络隔离地址是主机的默认网关。无论已定义多少个管理网络，都只会指定一个默认网关。使用 `das.isolationaddress[...]` 高级选项为其他网络添加隔离地址。请参见 vSphere HA 高级选项。

网络路径冗余

集群节点之间的网络路径冗余对 vSphere HA 可靠性非常重要。单个管理网络会最终成为单一故障点，并且，尽管只有该网络出现故障，仍可能会导致故障切换。如果仅有一个管理网络，那么在网络连接故障期间未保留检测信号数据存储连接时主机和集群之间的任何故障都可能会导致不必要（或错误）的故障切换活动。可能的故障包括网卡故障、网络电缆故障、网络电缆移除和交换机重置。考虑主机可能导致故障的上述原因，然后尝试减少这些问题（通常通过提供网络冗余来实现此目的）。

实现网络冗余的首选方法是在网卡级别使用网卡绑定。如果用两个连接到不同物理交换机的网卡组成一个网卡组，则可以提高管理网络的可靠性。因为通过两个网卡（并且通过单独的交换机）连接的服务器具有两条独立的路径来发送和接收检测信号，所以集群具有更好的弹性。要为管理网络配置网卡组，请在活动或待机配置的 vSwitch 配置中配置 vNIC。推荐的 vNIC 参数设置如下：

- 默认的负载均衡 = 基于源虚拟端口 ID 的路由
- 故障恢复 = 否

在为 vSphere HA 集群中的一个主机添加网卡之后，必须在该主机上重新配置 vSphere HA。

在大多数实现中，网卡绑定可以提供足够的检测信号冗余，但是除此之外，您还可以创建一个连接到单独虚拟交换机的辅助管理网络连接。冗余管理网络连接能够可靠地检测故障并防止出现隔离或分区的情况，因为检测信号可以通过多个网络发送。原始管理网络连接用于网络和管理。辅助管理网络连接创建之后，vSphere HA 会同时通过两种管理网络连接发送检测信号。如果一条路径发生故障，vSphere HA 仍可通过另一条路径发送和接收检测信号。

注 在集群内的服务器之间尽量少配置硬件分段，目的是为了限制单一故障点。此外，跃点过多的路由可能会导致检测信号的网络数据包延迟，并增加潜在的故障点数目。

使用 IPv6 网络配置

只能向 vSphere HA 集群使用的给定网络接口分配一个 IPv6 地址。分配多个 IP 地址会增加集群的首选主机发送的检测信号消息数量，这其实弊大于利。

互操作性的最佳做法

请遵守以下最佳做法，确保 vSphere HA 和其他功能之间的互操作性。

混合集群中的 vSphere HA 和 Storage vMotion 互操作性

在包含 ESXi 5.x 主机和 ESX/ESXi 4.1 或更早版本主机的集群中，以及在广泛使用 Storage vMotion 或激活 Storage DRS 的集群中，请勿部署 vSphere HA。vSphere HA 可通过在某个 ESXi 版本的主机上（不同于出现故障前运行虚拟机的主机版本）重新启动虚拟机来响应主机故障。如果出现故障时 ESXi 5.x 主机正在进行虚拟机 Storage vMotion 操作，且 vSphere HA 在 ESXi 版本 5.0 之前的主机上重新启动虚拟机，则会出现问题。虽然虚拟机可能打开电源，但针对快照操作的任何后续尝试都可能会使 vdisk 状态遭到损坏并导致虚拟机不可用。

将 Auto Deploy 与 vSphere HA 配合使用

可以将 vSphere HA 与 Auto Deploy 配合使用来提高虚拟机的可用性。Auto Deploy 可在打开主机电源时置备这些主机，您还可以将其配置为在引导过程中在主机上安装 vSphere HA 代理。有关详细信息，请参见《vSphere 安装和设置》中的 Auto Deploy 文档。

使用 vSAN 升级集群中的主机

如果要将 vSphere HA 集群中的 ESXi 主机升级到版本 5.5 或更高版本，并且计划使用 vSAN，请按以下过程执行操作。

1 升级所有主机。

2 停用 vSphere HA。

3 激活 vSAN。

4 重新激活 vSphere HA。

集群监控最佳做法

请遵守以下针对监控 vSphere HA 集群状态和有效性的最佳做法。

将警报设置为监控集群更改

当 vSphere HA 或 Fault Tolerance 执行用于维护可用性的操作时（例如，虚拟机故障切换），可能会向您通知此类更改。将 vCenter Server 中的警报配置为在执行这些操作时触发，并向指定的一组管理员发送警示（如电子邮件）。

提供多个默认的 vSphere HA 警报。

- 故障切换资源不足（集群警报）
- 找不到首选主机（集群警报）
- 正在进行故障切换（集群警报）
- 主机 HA 状态（主机警报）
- VM 监控错误（虚拟机警报）
- 虚拟机监控操作（虚拟机警报）
- 故障切换失败（虚拟机警报）

注 默认的警报包括功能名称 vSphere HA。

HA VIB 行为的更改

在 vSphere 7.0 或更高版本中，如果在 Lifecycle Manager (vLCM) 集群上激活 HA，则可能会在某些情况下移除 HA VIB。在以前的版本中，vCenter 不会尝试从 ESXi 主机中移除 HA VIB。

只有在激活了 vSphere HA 的 vLCM 集群上才会出现这种情况。在集群上取消激活 vSphere HA 后，如果执行 vLCM **修复**操作（用户启动的操作或 API 调用），则可能会移除 vSphere HA VIB。

注 这种行为更改无害，因为当再次激活 HA 时，vCenter 会推送所需的 vSphere HA VIB。

为虚拟机提供 Fault Tolerance

3

您可以将 vSphere Fault Tolerance 用于虚拟机，以确保连续性及更高级别的可用性和数据保护。

Fault Tolerance 基于 ESXi 主机平台构建，它通过在单独的主机上运行相同的虚拟机来提供可用性。

要获取 Fault Tolerance 的最佳结果，必须先熟悉其工作原理、如何为集群和虚拟机启用它及其最佳使用方法。

本章讨论了以下主题：

Fault Tolerance 的工作方式

可以为大多数任务关键虚拟机使用 vSphere Fault Tolerance (FT)。FT 通过创建和维护与此类虚拟机相同且可在发生故障切换时随时替换此类虚拟机的其他虚拟机，来确保此类虚拟机的连续可用性。

受保护的虚拟机称为主虚拟机。重复虚拟机，即辅助虚拟机，在其他主机上创建和运行。主虚拟机会持续复制到辅助虚拟机，以便辅助虚拟机可以随时接管工作，从而提供 Fault Tolerant 保护。

主虚拟机和辅助虚拟机会持续监控彼此的状态以确保维护 Fault Tolerance。如果运行主虚拟机的主机出现故障，或者在主虚拟机内存中遇到不可更正的硬件错误（在这种情况下，将立即激活辅助虚拟机替换主虚拟机），则会发生透明故障切换。启动新的辅助虚拟机，并自动重新建立 Fault Tolerance 冗余。如果运行辅助虚拟机的主机发生故障，则该主机也会立即被替换。在任一情况下，用户都不会遭遇服务中断和数据丢失的情况。

容错虚拟机及其辅助副本不允许在相同主机上运行。此限制可确保主机故障不会导致两个虚拟机都丢失。

注 也可以使用虚拟机-主机关联性规则来确定要在其上运行指定虚拟机的主机。如果使用这些规则，应了解对于受这种规则影响的任何主虚拟机，其关联的辅助虚拟机也受这些规则影响。有关关联性规则的更多信息，请参见《vSphere 资源管理》文档。

容错可避免“裂脑”情况的发生，此情况可能会导致虚拟机在从故障中恢复后存在两个活动副本。共享存储上锁定的原子文件用于协调故障切换，以便只有一端可作为主虚拟机继续运行，并由系统自动重新生成新辅助虚拟机。

vSphere Fault Tolerance 可容纳最多具有 8 个 vCPU 的对称多处理器 (SMP) 虚拟机。

Fault Tolerance 用例

几种典型情况可以受益于 vSphere Fault Tolerance 的使用。

Fault Tolerance 可提供比 vSphere HA 更高级别的业务连续性。当调用辅助虚拟机以替换与其对应的主虚拟机时，辅助虚拟机会立即取代主虚拟机的角色，并会保存其整个状况。应用程序已在运行，并且不需要重新输入或重新加载内存中存储的数据。vSphere HA 提供的故障切换将重新启动受故障影响的虚拟机。

更高的连续性级别以及增加的状况信息和数据保护功能可在您要部署容错时提供方案信息。

- 必须始终可用的应用程序，尤其是用户希望在硬件故障期间保持持久客户端连接的应用程序。
- 不能通过任何其他方式实现集群功能的自定义应用程序。
- 可以通过自定义集群解决方案提供高可用性，但这些解决方案太复杂，很难进行配置和维护的情况。

用容错保护虚拟机的另一个关键用例可以描述为按需容错。在这种情况中，虚拟机在正常操作期间受到 vSphere HA 的充分保护。在某些关键期间，您可能希望增强虚拟机的保护。例如，您可能正在运行季末报告，如果发生中断，则可能会延迟关键信息的可用性。使用 vSphere Fault Tolerance，可以在运行此报告之前保护此虚拟机，然后在生成报告之后关闭或挂起 Fault Tolerance。可以在关键时间段使用按需容错保护虚拟机，然后在非关键操作期间将资源置回正常状态。

Fault Tolerance 要求、限制和许可

在使用 vSphere Fault Tolerance (FT) 之前，请考虑适用于此功能的高级别要求、限制和许可。

要求

以下 CPU 和网络要求适用于 FT。

主机中用于容错虚拟机的 CPU 必须与 vSphere vMotion 兼容。此外，还需要 CPU 支持硬件 MMU 虚拟化（Intel EPT 或 AMD RVI）。支持以下 CPU。

- Intel Sandy Bridge 或更高版本。Avoton 不受支持。
- AMD Bulldozer 或更高版本。

请对 FT 使用 10 Gb 日志记录网络并验证网络延迟时间是否非常短。强烈建议使用专用 FT 网络。

限制

在已配置为使用 Fault Tolerance 的集群中，分别强制执行两个限制。

das.maxftvmsperhost

集群中的主机上允许的最大容错虚拟机数量。默认值为 4。未设置每个主机的 FT 虚拟机上限，如果工作负载在 FT 虚拟机中性能良好，可以使用更大的数字。可以通过将该值设置为 **0** 来停用检查。

das.maxftvcpusperhost

主机上所有容错虚拟机的汇总最大 vCPU 数。默认值为 8。未设置每个主机的 FT vCPU 上限，如果工作负载性能良好，可以使用更大的数字。可以通过将该值设置为 **0** 来停用检查。

许可

单个容错虚拟机支持的 vCPU 数量受您针对 vSphere 购买的许可级别限制。Fault Tolerance 支持情况如下：

- vSphere Standard 和 Enterprise。最多可允许 2 个 vCPU
- vSphere Enterprise Plus。最多可允许 8 个 vCPU

注 FT 仅在 vSphere Standard、vSphere Enterprise 和 vSphere Enterprise Plus 版本中受支持。

Fault Tolerance 互操作性

在配置 vSphere Fault Tolerance 之前，必须了解 Fault Tolerance 不能与之交互操作的功能和产品。

Fault Tolerance 不支持的 vSphere 功能

配置集群时，应注意并非所有 vSphere 功能都可与 Fault Tolerance 进行交互操作。

容错虚拟机不支持以下 vSphere 功能。

注 在 vSphere 7.0 Update 2 之前的版本中，FT 不支持 vSphere 虚拟机加密。

- 快照。在虚拟机上启用 Fault Tolerance 前，必须移除或提交快照。此外，不可能对已启用 Fault Tolerance 的虚拟机执行快照。

  注 Fault Tolerance 支持为 vStorage APIs - Data Protection (VADP) 备份而创建的仅磁盘快照。但是，旧版 FT 不支持 VADP。

- Storage vMotion。不能为已启用 Fault Tolerance 的虚拟机调用 Storage vMotion。要迁移存储，应当先暂时关闭 Fault Tolerance，然后再执行 Storage vMotion 操作。在完成迁移之后，可以重新打开 Fault Tolerance。
- 链接克隆。不能在为链接克隆的虚拟机上使用 Fault Tolerance，也不能从启用了 FT 的虚拟机创建链接克隆。
- Virtual Volumes 数据存储。

- 基于存储的策略管理。vSAN 存储支持存储策略。
- I/O 筛选器。
- TPM.
- 启用 VBS 的虚拟机。

不与 Fault Tolerance 兼容的功能和设备

并非所有第三方设备、功能或产品都可与 Fault Tolerance 进行交互操作。

要使虚拟机与 Fault Tolerance 功能兼容，虚拟机不能使用以下功能或设备。

表 3-1. 不与 Fault Tolerance 兼容的功能和设备以及纠正操作

不兼容的功能或设备	纠正操作
物理裸磁盘映射 (RDM)。	使用旧版 FT，可以将具有支持物理 RDM 的虚拟设备的虚拟机重新配置为改用虚拟 RDM。
由物理或远程设备支持的 CD-ROM 或虚拟软盘设备。	移除 CD-ROM 或虚拟软盘设备，或使用共享存储上安装的 ISO 重新配置备用功能。
USB 和声音设备。	从虚拟机移除这些设备。
N_Port ID 虚拟化 (NPIV)。	停用虚拟机的 NPIV 配置。
网卡直通。	Fault Tolerance 不支持此功能，因此必须将其关闭。
热插拔设备。	容错虚拟机的热插拔功能将自动停用。要热插拔设备（添加或移除），必须临时关闭 Fault Tolerance，完成热插拔操作，然后重新启用 Fault Tolerance。 注 使用 Fault Tolerance 时，如果在虚拟机正在运行过程中更改虚拟网卡的设置，该操作即为热插拔操作，因为它要求先拔出网卡，然后重新插入。例如，当正在运行的虚拟机使用虚拟网卡时，如果更改虚拟网卡所连接到的网络，必须首先关闭 FT。
串行或并行端口	从虚拟机移除这些设备。
激活了 3D 功能的视频设备。	Fault Tolerance 不支持启用了 3D 的视频设备。
虚拟机通信接口 (VMCI)	不受 Fault Tolerance 支持。
2TB+ VMDK	2TB+ VMDK 不支持 Fault Tolerance。

将 Fault Tolerance 功能与 DRS 配合使用

可以将 vSphere Fault Tolerance 与 vSphere Distributed Resource Scheduler (DRS) 结合使用。

FT 虚拟机不要求 EVC 支持 DRS。在由 vSphere 6.7 或更高版本 VC 管理的 vSphere 6.5 和 6.0 主机上，可以将 FT 与 DRS 结合使用。

注 vSphere DRS 是 vSphere 的一项重要功能，要维持在 vSphere 集群内运行的工作负载正常运行，必须使用此功能。从 vSphere 7.0 Update 1 开始，DRS 依赖于 vCLS 虚拟机的可用性。有关详细信息，请参见《vSphere 资源管理》中的“vSphere 集群服务 (vCLS)”。

为 Fault Tolerance 准备集群和主机

要为集群启用 vSphere Fault Tolerance，必须满足此功能的必备条件，然后在主机上执行特定的配置步骤。完成这些步骤并创建集群后，还可以检查配置是否符合启用 Fault Tolerance 的要求。

尝试为集群设置 Fault Tolerance 之前，应完成的任务包括：

- 确保您的集群、主机和虚拟机满足 Fault Tolerance 对照表中所述要求。
- 为每台主机配置网络。
- 创建 vSphere HA 集群，添加主机，并检查合规性。

在为集群和主机准备好 Fault Tolerance 之后，便可为虚拟机打开 Fault Tolerance。请参见打开 Fault Tolerance。

Fault Tolerance 对照表

以下对照表包含在使用 vSphere Fault Tolerance 之前需要了解的集群、主机和虚拟机要求。

在设置 Fault Tolerance 之前，应查看此列表。

注 容错虚拟机的故障切换与 vCenter Server 无关，但必须使用 vCenter Server 来设置 Fault Tolerance 集群。

Fault Tolerance 的集群要求

在使用 Fault Tolerance 之前，必须满足以下集群要求。

- 配置了 Fault Tolerance 日志记录和 vMotion 网络。请参见为主机配置网络。
- vSphere HA 集群已创建并启用。请参见创建 vSphere HA 集群。打开容错虚拟机电源或者将主机添加到已支持容错虚拟机的集群之前，必须启用 vSphere HA。

Fault Tolerance 的主机要求

在使用 Fault Tolerance 之前，必须满足以下主机要求。

- 主机必须使用受支持的处理器。
- 主机必须获得 Fault Tolerance 的许可。

- 主机必须已通过 Fault Tolerance 认证。请参见 http://www.vmware.com/resources/compatibility/search.php 并选择**按与容错兼容的集合搜索**，确定主机是否已通过认证。
- 在配置每台主机时，都必须在 BIOS 中启用硬件虚拟化 (HV)。

注 VMware 建议将用于支持 FT 虚拟机的主机的 BIOS 电源管理设置设为“最高性能”或“受操作系统管理的性能”。

要确认集群内的主机是否兼容，从而判断其是否支持 Fault Tolerance，还可以按 创建集群和检查合规性 中所说明的那样运行配置文件合规性检查。

Fault Tolerance 的虚拟机要求

在使用 Fault Tolerance 之前，必须满足以下虚拟机要求。

- 没有不受支持的设备连接到虚拟机。请参见 Fault Tolerance 互操作性。
- 不兼容的功能一定不能与容错虚拟机一起运行。请参见 Fault Tolerance 互操作性。
- 虚拟机文件（VMDK 文件除外）必须存储在共享存储中。可接受的共享存储解决方案包括光纤通道、（硬件和软件）iSCSI、vSAN、NFS 和 NAS。

其他配置建议

在配置 Fault Tolerance 时还应遵循以下准则。

- 如果要使用 NFS 访问共享存储，请使用至少具有 1 千兆位网卡的专用 NAS 硬件，以获取为了使 Fault Tolerance 功能正常工作所需的网络性能。
- 在开启 Fault Tolerance 功能后，容错虚拟机的预留内存设置为虚拟机的内存大小。确保包含容错虚拟机的资源池拥有大于虚拟机内存大小的内存资源。如果资源池中没有额外内存，则可能没有内存可用作开销内存。
- 为确保冗余和最大 Fault Tolerance 保护，集群中应至少有三台主机。如果发生故障切换情况，这可确保有主机可容纳所创建的新辅助虚拟机。

为主机配置网络

在要添加到 vSphere HA 集群的每台主机上，必须配置两个不同的网络交换机（vMotion 和 FT 日志记录），以便主机支持 vSphere Fault Tolerance。

要为主机设置 Fault Tolerance，必须为每个端口组选项（vMotion 和 FT 日志记录）完成此步骤，以确保有足够的带宽可供 Fault Tolerance 日志记录使用。选择一个选项，完成该过程，然后选择另一个端口组选项，再执行一次该过程。

前提条件

需要多个千兆位网络接口卡 (NIC)。对于支持 Fault Tolerance 功能的每台主机，建议最少使用两个物理网卡。例如，您需要一个网卡专门用于 Fault Tolerance 日志记录，另一个则专门用于 vMotion。使用三个或更多网卡来确保可用性。

步骤

1 在 vSphere Client 中，浏览到主机。

2 依次单击**配置**选项卡和**网络**。

3 选择 **VMkernel 适配器**。

4 单击**添加网络**图标。

5 提供相应的连接类型信息。

6 单击**完成**。

结果

在创建 vMotion 和 Fault Tolerance 日志记录虚拟交换机后，可以根据需要创建其他虚拟交换机。将主机添加到集群，并完成打开 Fault Tolerance 所需的所有步骤。

后续步骤

注 如果将网络连接配置为支持 FT，但随后又挂起了 Fault Tolerance 日志记录端口，则已打开电源的容错虚拟机对将保持打开电源状态。如果出现了故障切换情况，那么，当主虚拟机被其辅助虚拟机替换时，将不会启动新的辅助虚拟机，这会导致新的主虚拟机以“不受保护”状态运行。

创建集群和检查合规性

vSphere Fault Tolerance 在 vSphere HA 集群环境中使用。为每台主机配置网络连接后，创建 vSphere HA 集群并向其中添加主机。您可查看集群配置是否正确以及是否符合启用 Fault Tolerance 的要求。

步骤

1 在 vSphere Client 中，浏览到集群。

2 单击**监控**选项卡，然后单击**配置文件合规性**。

3 单击**立即检查合规性**运行合规性测试。

结果

此时将显示合规性测试结果，并显示每台主机是合规还是不合规。

使用 Fault Tolerance

在采取了为集群激活 vSphere Fault Tolerance 所需的全部步骤之后，可以为各个虚拟机打开 Fault Tolerance 功能。

在打开 Fault Tolerance 之前，需要在虚拟机上执行验证检查。

在通过这些检查并为虚拟机打开 vSphere Fault Tolerance 之后，新选项将添加到其上下文菜单的“Fault Tolerance”区域。这包括关闭或停用 Fault Tolerance、迁移辅助虚拟机、测试故障切换和测试辅助虚拟机重新启动的选项。

打开 Fault Tolerance 时的验证检查

如果用于打开 Fault Tolerance 的选项可用，则此任务仍然必须进行验证，并且在未满足某些要求时可能会失败。

在打开 Fault Tolerance 之前，需要在虚拟机上执行多项验证检查。

- 必须在 vCenter Server 设置中激活 SSL 证书检查。
- 主机必须位于 vSphere HA 集群或包含 vSphere HA 和 DRS 的混合集群内。
- 主机必须安装 ESXi 6.x 或更高版本。
- 虚拟机不得有快照。
- 虚拟机不得是模板。
- 对于虚拟机不得停用 vSphere HA。
- 虚拟机不得有激活了 3D 的视频设备。

已启动虚拟机的检查

已对已打开电源的虚拟机（或正在打开电源的虚拟机）执行了多项附加验证检查。

- 容错虚拟机所驻留的主机的 BIOS 必须激活了硬件虚拟化 (HV)。
- 支持主虚拟机的主机必须有支持 Fault Tolerance 的处理器。
- 您的硬件应认证为与 Fault Tolerance 兼容。为了确认这点，请使用 http://www.vmware.com/resources/compatibility/search.php 中的《VMware 兼容性指南》并选择**按与容错兼容的集合搜索**。
- 虚拟机的配置必须有效，以便与 Fault Tolerance 功能配合使用（例如，不得包含任何不受支持的设备）。

辅助虚拟机放置

当为虚拟机打开 Fault Tolerance 这一操作通过验证检查时，将创建辅助虚拟机。辅助虚拟机的放置位置和即时状态取决于在打开 Fault Tolerance 时主虚拟机是已打开电源还是已关闭电源。

如果主虚拟机已打开电源：

- 将复制整个主虚拟机的状况，创建辅助虚拟机，并将其放置在单独的兼容主机上，而且会在通过接入控制时打开电源。
- 虚拟机的 Fault Tolerance 状态显示为**受保护**。

如果主虚拟机已关闭电源：

- 将立即创建辅助虚拟机并在集群的主机中注册（打开该虚拟机电源时，可能会在更合适的主机上重新进行注册）。
- 辅助虚拟机在主虚拟机打开电源之后打开电源。
- 虚拟机的 Fault Tolerance 状态显示为**不受保护、虚拟机未运行**。
- 当尝试在打开 Fault Tolerance 之后打开主虚拟机的电源时，将执行上面列出的附加验证检查。

通过这些检查之后，将打开主虚拟机和辅助虚拟机的电源，并将其分别放置在单独的兼容主机上。虚拟机的 Fault Tolerance 状态标记为**受保护**。

打开 Fault Tolerance

您可以通过 vSphere Client 打开 vSphere Fault Tolerance。

在打开 Fault Tolerance 功能后，vCenter Server 会重置虚拟机的内存限制，并将内存预留值设置为虚拟机的内存大小。当 Fault Tolerance 保持打开状态时，不能更改内存预留、大小、限制、vCPU 数量或份额。也不能添加或移除虚拟机磁盘。在关闭容错功能后，已更改的任何参数均不会恢复到其原始值。

使用具有集群管理员权限的帐户将 vSphere Client 连接到 vCenter Server。

前提条件

如果符合下列任一情况，则用于打开 Fault Tolerance 的选项将不可用并变成灰色：

- 虚拟机所驻留的主机并未获得使用该功能的许可证。
- 虚拟机所驻留的主机处于维护模式或待机模式。
- 虚拟机已断开连接或被孤立（无法访问其 .vmx 文件）。
- 用户没有打开此功能的权限。

步骤

1. 在 vSphere Client 中，浏览到您要为其打开 Fault Tolerance 的虚拟机。
2. 右键单击虚拟机，然后选择 **Fault Tolerance > 关闭 Fault Tolerance**。
3. 单击**是**。
4. 选择用于放置辅助虚拟机配置文件的数据存储。然后，单击**下一步**。
5. 选择要在其中放置辅助虚拟机的主机。然后，单击**下一步**。
6. 检查选择内容，然后单击**完成**。

结果

特定的虚拟机将被指定为主虚拟机，并在另一台主机上建立辅助虚拟机。现在，主虚拟机已启用了容错功能。

注 打开 FT 的过程中会复制虚拟机数据存储和内存。这可能需要几分钟时间，具体取决于复制的数据的大小。复制完成之前，虚拟机状态不会显示为“受保护”。

关闭 Fault Tolerance

关闭 vSphere Fault Tolerance 将删除辅助虚拟机及其配置以及所有历史记录。

如果您不打算重新启动 Fault Tolerance 功能，请使用**关闭 Fault Tolerance** 选项。否则，请使用**挂起 Fault Tolerance** 选项。

注 如果辅助虚拟机所驻留的主机处于维护模式、已断开或不响应，则不能使用**关闭 Fault Tolerance** 选项。在这种情况下，应当挂起 Fault Tolerance，然后再将其恢复。

步骤

1 在 vSphere Client 中，浏览到您要为其关闭 Fault Tolerance 的虚拟机。

2 右键单击虚拟机，然后选择 **Fault Tolerance > 关闭 Fault Tolerance**。

3 单击**是**。

结果

选定虚拟机的 Fault Tolerance 功能将关闭。选定虚拟机的历史记录和辅助虚拟机都将被删除。

注 当辅助虚拟机正在启动时，无法关闭 Fault Tolerance。由于该过程涉及将主虚拟机的完整状态同步到辅助虚拟机，因此所用时间可能会超过预期。

挂起 Fault Tolerance

挂起虚拟机的 vSphere Fault Tolerance 也将挂起 Fault Tolerance 保护，但会保留该虚拟机的辅助虚拟机、配置和所有历史记录。使用该选项可在将来恢复 Fault Tolerance 保护。

步骤

1 在 vSphere Client 中，浏览到要为其挂起 Fault Tolerance 的虚拟机。

2 右键单击虚拟机，然后选择 **Fault Tolerance > 挂起 Fault Tolerance**。

3 单击**是**。

结果

选定虚拟机的 Fault Tolerance 功能将被挂起。所选虚拟机的辅助虚拟机和所有历史记录都将保留，并在恢复该功能时使用。

后续步骤

挂起 Fault Tolerance 后，要恢复功能，请选择**恢复 Fault Tolerance**。

迁移辅助虚拟机

在为主要虚拟机打开 vSphere Fault Tolerance 之后，可以迁移其关联的辅助虚拟机。

步骤

1 在 vSphere Client 中，浏览到您要迁移其辅助虚拟机的主虚拟机。

2 右键单击虚拟机，然后选择 **Fault Tolerance > 迁移辅助虚拟机**。

3 完成“迁移”对话框中的选项，并确认做出的更改。

4 单击**完成**以应用所做的更改。

结果

与选定容错虚拟机关联的辅助虚拟机会迁移到指定的主机中。

测试故障切换

可以通过诱发所选主要虚拟机的故障切换来测试容错保护。

如果已关闭虚拟机电源，则此选项不可用（灰显）。

步骤

1 在 vSphere Client 中，浏览到要对其测试故障切换的主虚拟机。

2 右键单击虚拟机，然后选择 **Fault Tolerance > 测试故障切换**。

3 在任务控制台中查看有关故障切换的详细信息。

结果

此任务通过诱发主要虚拟机故障来确保辅助虚拟机能够替换主要虚拟机。同时会启动一个新的辅助虚拟机，而主要虚拟机将置回受保护状态。

测试重新启动辅助虚拟机

可以通过诱发辅助虚拟机发生故障以测试为所选主要虚拟机提供的容错保护。

如果已关闭虚拟机电源，则此选项不可用（灰显）。

步骤

1 在 vSphere Client 中，浏览到您要对其进行测试的主虚拟机。

2 右键单击虚拟机，然后选择 **Fault Tolerance > 测试重新启动辅助虚拟机**。

3 在任务控制台中查看有关测试的详细信息。

结果

此任务会导致为所选主要虚拟机提供容错保护的辅助虚拟机终止。将启动一个新的辅助虚拟机，而主要虚拟机将置回受保护状态。

升级用于 Fault Tolerance 的主机

请使用以下步骤升级用于 Fault Tolerance 的主机。

前提条件

确认您具有集群管理员特权。

确认拥有多组 ESXi 主机，每组由四台或多台主机组成，这些主机托管已打开电源的容错虚拟机。如果虚拟机已关闭电源，则主虚拟机和辅助虚拟机可以重定位到具有不同内部版本的主机。

注 此升级过程适用于至少包含四个节点的集群。更小的集群也可以遵循此说明，不过不受保护的时间间隔将稍微长一些。

步骤

1 使用 vMotion 从两台主机中迁出容错虚拟机。

2 将这两台已撤出的主机升级到相同的 ESXi 内部版本。

3 在主虚拟机上挂起 Fault Tolerance。

4 使用 vMotion 将已挂起 Fault Tolerance 的主虚拟机移至其中一台已升级的主机上。

5 针对已移动的主虚拟机恢复 Fault Tolerance。

6 要在升级的主机上容纳尽可能多的容错虚拟机对，请重复步骤 1 到步骤 5。

7 使用 vMotion 重新分配容错虚拟机。

结果

集群中的所有 ESXi 主机即已升级。

激活 Fault Tolerance 加密

您可以加密 Fault Tolerance 日志流量。

vSphere Fault Tolerance 会在主虚拟机和辅助虚拟机之间执行频繁检查，以便辅助虚拟机可以从上次成功的检查点快速恢复。检查点包含自上一检查点之后已修改的虚拟机状态。您可以加密 Fault Tolerance 日志流量。

打开 Fault Tolerance 时，FT 加密默认设置为**视情况**，这意味着只有在首选主机和辅助主机均能加密时，才激活加密。如果需要手动更改 FT 加密模式，请执行以下过程。

注 Fault Tolerance 支持 vSphere 7.0 Update 2 及更高版本的 vSphere 虚拟机加密。客户机内和基于阵列的加密不依赖或干扰虚拟机加密。具有多个加密层会使用其他计算资源，这可能会影响虚拟机性能。影响因硬件以及 I/O 的数量和类型而异，但对于大多数工作负载而言，整体性能影响可以忽略不计。去重、压缩和复制等后端存储功能的有效性和兼容性也可能会受到虚拟机加密的影响。

前提条件

FT 加密需要 SMP-FT。不支持对旧版 FT（记录/重放 FT）进行加密。

步骤

1 选择虚拟机，然后选择**编辑设置**。

2 在**虚拟机选项**下，选择**已加密 FT** 下拉菜单。

3 选择以下选项之一：

选项	描述
已禁用	不启用加密 Fault Tolerance 日志记录。
视情况	仅在双方均能加密时，才启用加密。允许 Fault Tolerance 虚拟机移动到不支持加密 Fault Tolerance 日志记录的 ESXi 主机。
必需	选择同时支持加密 FT 日志记录的 Fault Tolerance 首选主机和辅助主机。

注 激活虚拟机加密后，FT 加密模式默认设置为**必需**，且无法修改。

当 FT 加密模式设置为**必需**时：

- 启用 FT 后，将仅列出支持 FT 加密的主机以便放置 FT 辅助主机。
- 只能在支持 FT 加密的主机上进行 FT 故障切换。

4 单击**确定**。

Fault Tolerance 的最佳做法

为确保获得最佳 Fault Tolerance 结果，您应当遵循某些最佳做法。

以下主机和网络配置建议有助于提高集群的稳定性和性能。

主机配置

运行主虚拟机和辅助虚拟机的主机应当按照与处理器大致相同的频率运行，否则辅助虚拟机可能会更频繁地重新启动。不依据工作负载进行调整（例如，为省电而执行功率封顶和强制低频率模式）的平台电源管理功能可能会导致处理器频率大范围浮动。如果辅助虚拟机要定期重新启动，请在运行容错虚拟机的主机上取消激活所有的电源管理模式，或者确保所有主机以相同的电源管理模式运行。

主机网络配置

您可以按照以下准则配置主机的网络，以便在不同流量类型的组合（如 NFS）和不同数目的物理网卡的情况下支持 Fault Tolerance。

- 将每个网卡组分布到两台物理交换机，并确保这两台物理交换机之间的每个 VLAN 的 L2 域连续性。
- 使用确定的绑定策略确保特定流量类型与特定网卡（活动/待机）或网卡集（如源虚拟端口 ID）具有关联性。
- 使用活动/待机策略时，将流量类型配对，以便使两种流量类型共享某个 vmnic 的情况下发生故障切换时所产生的影响最小。
- 使用活动/待机策略时，配置所有活动适配器，以便特定流量类型（如 FT 日志记录）流向相同物理交换机。这样可使网络跃点的数目最少，并降低超额预订交换机到交换机链路的可能性。

注 主虚拟机与辅助虚拟机之间的 FT 日志记录通信是未加密的，且包含客户机网络和存储 I/O 数据以及客户机操作系统的内存内容。此通信可以包含敏感数据，如纯文本格式的密码。为避免这些数据被泄漏，尤其是避免受到“中间人”攻击，请确保此网络是受保护的。例如，可以对 FT 日志记录通信使用专用网络。

同类集群

vSphere Fault Tolerance 可以在主机不一致的集群内使用，但在节点兼容的集群内才能起到最好的效果。构建集群时，所有主机都应具有以下配置：

- 对虚拟机所用数据存储的一般访问权限。
- 相同的虚拟机网络配置。
- 所有主机的相同 BIOS 设置（电源管理和超线程）。

运行**检查合规性**确定不兼容性并进行更正。

性能

要增加主虚拟机和辅助虚拟机之间日志记录通信使用的可用带宽，请使用 10 千兆位网卡，并激活巨型帧。

您可以选择多个网卡用于 FT 日志记录网络。通过选择多个网卡，即使所有网卡都不是专门用于运行 FT，您也可以利用多个网卡的带宽。

在共享存储上存储 ISO 以连续进行访问

将激活了 Fault Tolerance 的虚拟机访问的 ISO 存储在可以供容错虚拟机的两个实例访问的共享存储上。如果使用此配置，虚拟机中的 CD-ROM 会继续正常工作，即使发生了故障切换也是如此。

避免网络分区

当 vSphere HA 集群出现管理网络故障而导致某些主机与 vCenter Server 隔离并且使这些主机彼此隔离时，会出现网络分区。请参见 网络分区 。如果出现分区，则可能降低 Fault Tolerance 保护。

在使用 Fault Tolerance 的已分区 vSphere HA 集群中，主虚拟机（或其辅助虚拟机）可以在由首选主机（不负责管理虚拟机）管理的分区中停止。如果需要故障切换，则仅当主虚拟机位于首选主机（负责管理该主虚拟机）管理的分区中时才重新启动辅助虚拟机。

为确保管理网络尽可能不出现导致网络分区的故障，请遵循网络连接的最佳做法中的建议。

使用 vSAN 数据存储

vSphere Fault Tolerance 可以使用 vSAN 数据存储，但您必须考虑以下限制：

- 主虚拟机和辅助虚拟机均不支持混合使用 vSAN 和其他类型的数据存储。
- FT 不支持 vSAN Metro 集群。

要提高使用 FT 与 vSAN 时的性能和可靠性，建议采用下列条件。

- vSAN 和 FT 应使用单独的网络。
- 将主虚拟机和辅助虚拟机置于单独的 vSAN 故障域中。

旧版 Fault Tolerance

旧版 FT 虚拟机只能存在于版本 6.5 之前的 vSphere 上运行的 ESXi 主机中。

版本 6.5 之前的 ESXi 主机支持基于不同技术的 vSphere Fault Tolerance。如果您正在使用此版本的 Fault Tolerance 并且需要继续使用，建议您保留一个 vCenter 6.0 实例来管理运行这些虚拟机所需的版本 6.5 之前的主机的池。vCenter 6.0 是最后一个完全能够管理由旧版 FT 保护的虚拟机的版本。有关旧版 Fault Tolerance 的更多信息，请参见《vSphere 6.0 可用性》文档。

容错虚拟机故障排除

要保持容错虚拟机的高级别性能和稳定性并最小化故障切换率，应当了解某些故障排除问题。

此处讨论的故障排除主题重点介绍了在虚拟机上使用 vSphere Fault Tolerance 功能时可能遇到的问题。本主题还介绍了解决这些问题的方法。

也可以参见 VMware 知识库文章，网址为 http://kb.vmware.com/kb/1033634，以帮助您排除 Fault Tolerance 故障。该文章包含在尝试使用该功能时可能遇到的错误消息列表，以及如何解决每个错误的建议（如果可用）。

硬件虚拟化未启用

使用 vSphere Fault Tolerance 之前，必须启用硬件虚拟化 (HV)。

问题

尝试打开启用了 Fault Tolerance 的虚拟机的电源时，如果未启用 HV，则可能会显示一条错误消息。

原因

通常情况下，出现此错误的原因是：对于您尝试在其上打开虚拟机电源的 ESXi 服务器，HV 在其上不可用。硬件虚拟化不可用的原因可能是其不受 ESXi 服务器硬件支持或未在 BIOS 中启用。

解决方案

如果 ESXi 服务器硬件支持硬件虚拟化，但当前未启用硬件虚拟化，请在该服务器的 BIOS 中将其启用。各种 BIOS 中启用硬件虚拟化的过程不同。请参见主机的 BIOS 文档以获取有关如何启用硬件虚拟化的详细信息。

如果 ESXi 服务器硬件不支持硬件虚拟化，请切换到使用支持 Fault Tolerance 的处理器的硬件。

无兼容主机可用于辅助虚拟机

如果打开启用了 Fault Tolerance 的虚拟机的电源，但没有为辅助虚拟机提供任何兼容主机，可能会显示一条错误消息。

问题

您可能遇到以下错误消息：

```
辅助虚拟机无法打开电源，因为没有兼容主机可以容纳该虚拟机。
```

原因

这可能是由多种原因造成的，包括集群内没有其他主机、没有其他已启用硬件虚拟化的主机、主机 CPU 不支持硬件 MMU 虚拟化、数据存储不可访问、可用容量不足或主机正处于维护模式中。

解决方案

如果主机数量不足，请向集群内添加更多主机。如果集群内有多台主机，请确保它们支持硬件虚拟化且硬件虚拟化已启用。各种 BIOS 中启用硬件虚拟化的过程不同。请参见主机的 BIOS 文档以获取有关如何启用硬件虚拟化的详细信息。检查主机是否有足够容量，并确认它们未处于维护模式中。

过载主机上的辅助虚拟机降低主虚拟机的性能

如果主虚拟机的执行速度似乎缓慢，即便它所在主机上的负载较轻且有空闲 CPU 时间，也请检查运行辅助虚拟机的主机是否负载较重。

问题

当辅助虚拟机所在的主机负载过重时，辅助虚拟机会影响主虚拟机的性能。

原因

在过载（例如 CPU 资源过载）的主机上运行的辅助虚拟机获取的资源量与主虚拟机获取的资源量可能不同。当出现此情况时，主虚拟机必须减速以使辅助虚拟机跟进，将主虚拟机的执行速度大大降低至辅助虚拟机的较慢速度。

解决方案

如果辅助虚拟机位于过载的主机上，可以将虚拟机移至其他位置而不会导致出现资源争用问题。或者，更具体来说，请执行以下操作：

- 对于 FT 网络争用，请使用 vMotion 技术将辅助虚拟机移至 FT 网络中 FT 虚拟机争用较少的主机上。确认对虚拟机的存储访问质量是非对称的。
- 如果存在存储争用问题，请关闭并重新打开 FT。重新创建辅助虚拟机时，请将其数据存储更改到资源争用较少且潜在性能更佳的位置。
- 要解决 CPU 资源问题，请为主虚拟机设置明确的 CPU 预留（以 MHz 为单位），该预留应足以在所需性能级别上运行负载。此预留对于主虚拟机和辅助虚拟机均适用，能够确保两者均能以指定的速率执行。有关设置此预留的指导，请在启用 Fault Tolerance 前查看虚拟机的性能图表以查看在正常条件下使用的 CPU 资源量。

在 FT 虚拟机中发现网络延迟时间增加

如果您的 FT 网络未以最佳方式配置，FT 虚拟机可能会出现延迟问题。

问题

FT 虚拟机可能会发现数据包延迟时间不断增加（大约增加几毫秒时间）。要求网络数据包延迟或抖动时间非常短的应用程序（例如，某些实时应用程序）可能会发现性能下降。

原因

在一定程度上增加的延迟时间是 Fault Tolerance 的预期开销，但某些因素可能会增加此延迟时间。例如，如果 FT 网络位于延迟时间特别长的链接上，此延迟可能会被传递到应用程序。此外，如果 FT 网络的带宽不足（低于 10 Gbps），可能会出现更长时间的延迟。

解决方案

验证 FT 网络的带宽是否充足（10 Gbps 或更高），并在主虚拟机与辅助虚拟机之间使用短延迟链接。这些预防措施不会避免网络延迟，但可以最大程度地减小潜在影响。

某些主机的 FT 虚拟机过载

如果您的集群主机中 FT 虚拟机分布不平衡，则可能会遇到性能问题。

问题

集群中的某些主机可能 FT 虚拟机过载，其他主机可能包含未使用的资源。

原因

vSphere DRS 不会加载平衡 FT 虚拟机（除非这些虚拟机使用旧的 FT）。此限制可能导致某个集群中出现 FT 虚拟机在主机中不均等分配的状况。

解决方案

使用 vSphere vMotion 手动将 FT 虚拟机在集群中再次平衡。通常，主机上的 FT 虚拟机越少，其性能发挥得越好，因为这样可以减少 FT 网络带宽和 CPU 资源争用。

无法访问 FT 元数据数据存储

访问 Fault Tolerance 元数据数据存储对于 FT 虚拟机的正常运行至关重要。无法访问会导致出现各种问题。

问题

由此产生的问题如下：

- FT 意外终止。
- 如果主虚拟机和辅助虚拟机均无法访问元数据数据存储，则虚拟机可能会意外终止。通常，当主虚拟机和辅助虚拟机均无法访问 FT 元数据数据存储时，也会发生无关联故障并导致 FT 终止。然后，vSphere HA 会尝试在可访问元数据数据存储的主机上重新启动主虚拟机。
- vCenter Server 可能会停止将虚拟机识别为 FT 虚拟机。识别失败会导致某些操作不受支持，如在虚拟机上执行快照操作，而且会导致有问题的行为出现。

原因

无法访问 Fault Tolerance 元数据数据存储会导致先前列表中出现不良结果。

解决方案

规划 FT 部署时，请将元数据数据存储置于高可用性存储中。FT 运行时，如果发现主虚拟机或辅助虚拟机无法访问元数据数据存储，请立即解决存储问题，以免访问失败导致先前问题出现。如果 vCenter Server 停止将虚拟机识别为 FT 虚拟机，请勿在虚拟机上执行不支持的操作。恢复访问元数据数据存储。FT 虚拟机的访问恢复且刷新时间间隔结束后，将可识别虚拟机。

为打开电源的虚拟机打开 vSphere FT 失败

如果尝试为打开电源的虚拟机打开 vSphere Fault Tolerance，则该操作可能会失败。

问题

为打开电源的虚拟机选择**打开 Fault Tolerance** 时，该操作失败并会显示未知错误 (Unknown error) 消息。

原因

如果运行虚拟机的主机没有足够的内存资源来提供容错保护，此操作可能失败。vSphere Fault Tolerance 会自动尝试为虚拟机分配主机上的全部内存预留。容错虚拟机需要开销内存，且开销内存有时可扩展到 1 到 2 GB。如果运行打开电源的虚拟机的主机没有足够的内存资源来容纳全部预留以及内存开销，则尝试打开 Fault Tolerance 的操作将失败。随后，将返回未知错误 (Unknown error) 消息。

解决方案

选择以下解决方案之一：

- 释放主机上的内存资源来容纳虚拟机的内存预留以及增加的开销。
- 将该虚拟机移到具有足够的可用内存资源的主机，然后重试。

vSphere DRS 未放置或撤出 FT 虚拟机

如果当前已停用 vSphere DRS (EVC)，则已启用 Enhanced vMotion Compatibility 的集群中的 FT 虚拟机无法正常运行。

问题

由于 EVC 是 DRS 与 FT 虚拟机搭配使用的必备条件，如果已停用 EVC（即使随后重新启用），则 DRS 不会放置或撤出这些虚拟机。

原因

如果已在 DRS 集群上停用了 EVC，则可能会添加在 FT 虚拟机上停用 DRS 的虚拟机替代项。即使随后重新启用 EVC，也不会取消此替代项。

解决方案

如果 DRS 未放置或撤出集群中的 FT 虚拟机，请检查虚拟机是否存在禁用 DRS 的虚拟机替代项。如果找到替代项，请移除将停用 DRS. 的替代项。

注 有关如何编辑或删除虚拟机替代项的详细信息，请参见《vSphere 资源管理》。

Fault Tolerant 虚拟机故障切换

即使主虚拟机或辅助虚拟机的 ESXi 主机未崩溃，主虚拟机或辅助虚拟机也可进行故障切换。在这种情况下，虚拟机执行不会中断，但会临时失去冗余。要避免此类故障切换，请了解可能会出现此类故障切换的一些情况，并采取措施进行避免。

与存储器有关的部分硬件故障

当存储器访问缓慢或无法访问某台主机时，可能出现此问题。此问题发生时，VMkernel 日志中将列出许多存储器错误。要解决此问题，必须解决与存储器有关的问题。

与网络有关的部分硬件故障

如果日志记录网卡不能正常工作或通过该网卡与其他主机的连接断开，将触发容错虚拟机进行故障切换，从而重新建立冗余。要避免此问题，请将每个独立网卡专门用于 vMotion 和容错日志记录通信，并仅在虚拟机活动较少时执行 vMotion 迁移。

日志记录网卡网络上的带宽不足

如果主机上有过多的容错虚拟机，则会发生此问题。要解决此问题，请将容错虚拟机对分布到更多的不同主机上。

请对 FT 使用 10 Gb 日志记录网络并验证网络滞后时间是否非常短。

由虚拟机活动级别引起的 vMotion 故障

如果通过 vMotion 迁移容错虚拟机失败，则虚拟机可能需要进行故障切换。此问题通常在虚拟机过于活跃（因而无法在对其造成最小损坏的情况下完成迁移）时发生。要避免此问题，请只在虚拟机活动较少时执行 vMotion 迁移。

VMFS 卷上活动过多可能会导致虚拟机故障切换

在单一 VMFS 卷上执行大量文件系统锁定操作、虚拟机启动/关闭或 vMotion 迁移时，可能会触发容错虚拟机进行故障切换。可能发生此现象的症状为在 VMkernel 日志中收到许多有关 SCSI 预留的警告。要解决此问题，请减少文件系统操作的数量，或确保容错虚拟机位于 VMFS 卷上，而且该卷上没有大量定期启动/关闭或使用 vMotion 进行迁移的其他虚拟机。

文件系统空间不足导致无法启动辅助虚拟机

请检查 /(root) 或 /vmfs/*datasource* 文件系统中是否有可用空间。这些文件系统可能会因多种原因而变得空间已满，空间不足会导致您无法启动新辅助虚拟机。

vCenter High Availability

4

vCenter High Availability (vCenter HA) 可防止 vCenter Server 发生主机和硬件故障。修补 vCenter Server 时，解决方案的主动-被动架构还有助于显著缩短停机时间。

进行某些网络配置之后，请创建一个包含主动节点、被动节点和见证节点的三节点集群。可使用不同配置路径。所选路径取决于现有配置。

步骤

1 规划 vCenter HA 部署

配置 vCenter HA 之前，必须考虑几种要素。包含使用不同版本 vSphere 组件的部署需要考虑的要素不同于仅包含 vSphere 8.0 组件的部署。灰场部署还必须要认真考虑资源和软件要求以及网络连接设置。

2 配置网络

无论您选择哪种部署选项和清单层次结构，都必须先设置网络，然后才能开始配置。要设置 vCenter HA 网络的基础，请将端口组添加到每个 ESXi 主机。

3 使用 vSphere Client 配置 vCenter HA

使用 vSphere Client 时，**设置 vCenter HA** 向导会在 vCenter Server 上创建和配置第二个网络适配器，克隆主动节点，并配置 vCenter HA 网络。

4 管理 vCenter HA 配置

配置 vCenter HA 集群之后，您可以执行管理任务。这些任务包括证书替换、SSH 密钥替换和 SNMP 设置。您还可以编辑集群配置，以停用或激活 vCenter HA、进入维护模式以及移除集群配置。

5 vCenter HA 环境故障排除

如果出现问题，您可以对环境进行故障排除。需要执行的任务取决于故障症状。有关其他故障排除信息，请参见 VMware 知识库系统。

6 修补 vCenter High Availability 环境

可以使用 vCenter Servershell 中提供的 **`software-packages`** 实用程序修补 vCenter High Availability 集群中的 vCenter Server。

规划 vCenter HA 部署

配置 vCenter HA 之前，必须考虑几种要素。包含使用不同版本 vSphere 组件的部署需要考虑的要素不同于仅包含 vSphere 8.0 组件的部署。灰场部署还必须要认真考虑资源和软件要求以及网络连接设置。

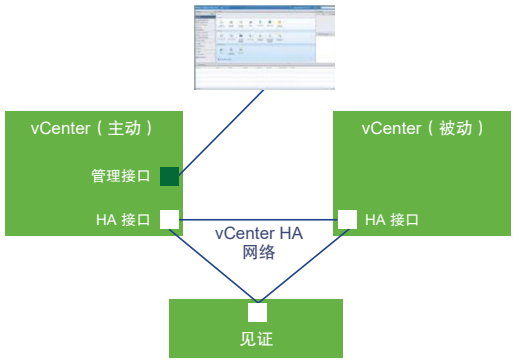
vCenter 架构概览

一个 vCenter HA 集群由三个 vCenter Server 实例组成。第一个实例初始用作主动节点，该节点被克隆两次，分别克隆为被动节点和见证节点。三个节点一起可提供主动-被动故障切换解决方案。

在不同的 ESXi 实例上部署单独的节点可防止出现硬件故障。向 DRS 集群中添加三个 ESXi 主机可为您的环境提供进一步保护。

vCenter HA 配置完成后，只有主动节点具有活动管理界面（公共 IP）。三个节点通过称为 vCenter HA 网络的专用网络通信，该网络是在配置过程中设置的。主动节点会不断将数据复制到被动节点。

图 4-1. vCenter 三节点集群



所有这三个节点是运行此功能所必需的。比较节点责任。

表 4-1. vCenter HA 节点

节点	描述
活动	■ 运行主动 vCenter Server 实例 ■ 为管理界面使用公共 IP 地址 ■ 使用 vCenter HA 网络将数据复制到被动节点。 ■ 使用 vCenter HA 网络与见证节点通信。
被动	■ 最初是主动节点的克隆 ■ 通过 vCenter HA 网络不断从主动节点接收更新，并与主动节点保持同步状态 ■ 在发生故障时自动接管主动节点的角色
见证	■ 主动节点的轻量克隆 ■ 提供仲裁来防止发生裂脑情况

vCenter HA 硬件和软件要求

设置 vCenter HA 之前，请确保内存、CPU 和数据存储资源充足，并确保所使用的 vCenter Server 和 ESXi 版本支持 vCenter HA。

您的环境必须满足以下要求。

表 4-2. vCenter HA 要求

组件	要求
ESXi	■ 需要 ESXi 6.0 或更高版本。 ■ 强烈建议至少使用三个 ESXi 主机。可以在不同主机上运行单独的 vCenter HA 节点以获得更加完善的保护。
管理 vCenter Server（如果使用）	您的环境可以包括管理 vCenter Server 系统，也可以设置 vCenter Server 来管理在其上运行的 ESXi 主机（自行管理的 vCenter Server） ■ 需要 vCenter Server 6.0 或更高版本。
vCenter Server	■ 需要 vCenter Server 6.5 或更高版本。 ■ 需要部署“小型”规模（4 CPU 和 16GB RAM）或稍大一些的规模，以满足 RTO。不要在生产环境中使用“微型”规模。 ■ vCenter HA 受支持，并已通过测试，可用于 VMFS、NFS 和 vSAN 数据存储。 ■ 确保主动节点具有充足的磁盘空间，可用于收集和存储所有三个节点的支持包。请参见收集 vCenter HA 节点的支持包。
网络连接	■ 主动节点、被动节点和见证节点之间的 vCenter HA 网络延迟时间必须小于 10 毫秒。 ■ vCenter HA 网络与管理网络必须位于不同的子网。
vCenter HA 所需的许可	■ vCenter HA 需要一个 vCenter Server 许可证。 ■ vCenter HA 需要 Standard 许可证。

vSphere Client 中的配置工作流概述

可以在 vSphere Client 中使用**设置 vCenter HA** 向导配置被动节点和见证节点。**设置 vCenter HA** 向导会在 vCenter HA 配置过程中自动创建被动节点和见证节点。使用手动选项，您需手动克隆主动节点，才能创建被动节点和见证节点。

在 vSphere Client 中执行自动配置

必须满足以下要求才能执行自动配置。

- 将成为主动节点的 vCenter Server 管理自己的 ESXi 主机及虚拟机。此配置有时称为自我管理 vCenter Server。

如果您满足上述要求，则可执行如下自动工作流。

1 用户部署第一个 vCenter Server，它将成为主动节点。

2 用户在每个 ESXi 主机上为 vCenter HA 通信添加另一个网络（端口组）。

3 用户开始进行 vCenter HA 配置，并为每个克隆提供 IP 地址、目标 ESXi 主机或集群和数据存储。

4 系统将克隆主动节点，并使用完全相同的设置（包括相同的主机名）创建被动节点。

5 系统再次克隆主动节点，并创建更轻型的见证节点。

6 系统设置 vCenter HA 网络，在此网络中，三个节点将通过交换检测信号和其他信息等方式进行通信。

在 vSphere Client 中执行手动配置

如果需要更好地控制部署，可以执行手动配置。使用此选项后，您需自己在 vCenter HA 设置过程中克隆主动节点。如果选择此选项并稍后移除 vCenter HA 配置，则需删除自己创建的节点。

对于手动选项，工作流如下所示。

1 用户部署第一个 vCenter Server，它将成为主动节点。

2 用户在每个 ESXi 主机上为 vCenter HA 通信添加另一个网络（端口组）。

3 如果主动管理 vCenter Server 的凭据未知，用户必须将第二个网络适配器（网卡）添加到主动节点。

4 用户使用 vSphere Client 登录到 vCenter Server（主动节点）。

5 用户开始进行 vCenter HA 配置，选中手动配置对应的复选框，并为被动节点和见证节点提供 IP 地址和子网信息。（可选）用户可替代故障切换管理的 IP 地址。

6 用户登录到管理 vCenter Server 并创建两个 vCenter Server 克隆（主动节点）。

7 系统设置 vCenter HA 网络，在此网络中，三个节点将交换检测信号和复制信息。

8 vCenter Server 受 vCenter HA 保护。

有关详细信息，请参见使用 vSphere Client 配置 vCenter HA。

配置网络

无论您选择哪种部署选项和清单层次结构，都必须先设置网络，然后才能开始配置。要设置 vCenter HA 网络的基础，请将端口组添加到每个 ESXi 主机。

完成配置后，vCenter HA 集群拥有两个网络，第一个虚拟网卡上的管理网络和第二个虚拟网卡上的 vCenter HA 网络。

管理网络

管理网络可处理客户端请求（公共 IP）。管理网络 IP 地址必须为静态地址。

vCenter HA 网络

vCenter HA 网络可连接到主动节点、被动节点和见证节点，并复制服务器状态。它还可监控检测信号。

- 主动节点、被动节点和见证节点的 vCenter HA 网络 IP 地址必须为静态地址。
- vCenter HA 网络与管理网络必须位于不同的子网。三个节点可以位于同一子网，也可以位于不同子网。
- 主动节点、被动节点和见证节点之间的网络延迟必须少于 10 毫秒。
- 您不得为集群网络添加默认的网关条目。

前提条件

- 稍后成为主动节点的 vCenter Server 已部署。
- 您可访问并有特权修改该 vCenter Server 以及它在其上运行的 ESXi 主机。
- 在网络设置期间，管理网络需要静态 IP 地址。管理和集群网络地址必须为 IPv4 或 IPv6。它们不能是混合模式的 IP 地址。

步骤

1 登录到管理 vCenter Server 并找到运行主动节点的 ESXi 主机。

2 将一个端口组添加到 ESXi 主机。

此端口组可以位于现有虚拟交换机，您也可以为加强网络隔离而创建新的虚拟交换机。它必须不同于管理网络。

3 如果您的环境包括建议的三个 ESXi 主机，请将该端口组添加到每个主机上。

使用 vSphere Client 配置 vCenter HA

使用 vSphere Client 时，**设置 vCenter HA** 向导会在 vCenter Server 上创建和配置第二个网络适配器，克隆主动节点，并配置 vCenter HA 网络。

前提条件

- 部署您要用作初始主动节点的 vCenter Server。
  - vCenter Server 必须具有静态 IP 地址。
  - 必须在 vCenter Server 上激活 SSH。
- 确认您的环境满足以下要求。
  - 将成为主动节点的 vCenter Server 管理自己的 ESXi 主机及虚拟机。此配置有时称为自我管理 vCenter Server。
- 为 vCenter HA 网络设置基础架构。请参见配置网络。
- 确定要用于两个 vCenter Server 节点的静态 IP 地址，这两个节点将分别成为被动节点和见证节点。

注 要在主动节点上使用 NSX-T 分段，必须使用**编辑虚拟机设置**创建 NIC2/eth1，以添加第二个具有 NSX-T 分段的网卡。您不需要为被动节点或见证节点指定任何资源，因为在为包含具有 IP 地址的 NIC1/eth0 和 NIC2/eth1 的被动节点和见证节点添加必要的客户机自定义规范后，必须使用**克隆虚拟机**创建克隆。在 vCenter Server 中为 eth1 配置 VCHA IP 地址时，将自动填充主动节点上的 eth1。

步骤

1 通过 vSphere Client 登录到主动节点。

2 在清单中选择 vCenter Server 对象，然后选择**配置**选项卡。

3 选择设置下的 **vCenter HA**。

4 单击**设置 vCenter HA** 按钮以启动设置向导。

- 如果 vCenter Server 是自我管理，则会显示**资源设置**页面。继续到步骤 7。
- 如果您的 vCenter Server 由同一 SSO 域中的其他 vCenter Server 管理，请转到步骤 7。
- 如果您的 vCenter Server 由不同 SSO 域中的其他 vCenter Server 管理，则输入该管理 vCenter Server 的位置和凭据详细信息。

5 单击**管理 vCenter Server 凭据**。指定管理 vCenter Server FQDN 或 IP 地址、Single Sign-On 用户名和密码，然后单击**下一步**。

如果没有 Single Sign-On 管理员凭据，请选择第二个项目符号，然后单击**下一步**。

6 您可能会看到显示**证书警告**。查看 SHA1 指纹，然后选择**是**以继续。

7 在**资源设置**部分中，首先从下拉菜单中为主动节点选择 vCenter HA 网络。

注 在创建 NIC2/eth1 后，网络选择器不再可见。

8 如果要自动创建被动节点和见证节点的克隆，请单击相应的复选框。

注 如果不选中该复选框，则必须在单击**完成**后，手动创建被动节点和见证节点的克隆。

9 对于被动节点，单击**编辑**。

a 指定唯一名称和目标位置。

b 为此操作选择目标计算资源。

c 选择要存储配置和磁盘文件的数据存储。

d 选择虚拟机管理（网卡 0）网络和 vCenter HA（网卡 1）网络。

如果选择内容出现问题，则会显示错误或兼容性警告。

e 检查选择内容，然后单击**完成**。

10 对于见证节点，单击**编辑**。

a 指定唯一名称和目标位置。

b 为此操作选择目标计算资源。

c 选择要存储配置和磁盘文件的数据存储。

d 选择 vCenter HA（网卡 1）网络。

如果选择内容出现问题，则会显示错误或兼容性警告。

e 检查选择内容，然后单击**完成**。

11 单击**下一步**。

12 在 **IP 设置**部分中，从下拉菜单中选择 IP 版本。

13 输入主动节点、被动节点及见证节点的 IPv4 地址（网卡 1）和子网掩码或前缀长度信息。

可以为被动节点编辑管理网络设置。自定义这些设置是可选的。默认情况下，将应用主动节点的管理网络设置。

14 单击**完成**。

结果

将创建被动节点和见证节点。完成**设置 vCenter HA** 时，vCenter Server 具有高可用性保护。激活 vCenter HA 后，可以单击**编辑**，进入维护模式，启用或禁用 vCenter HA。有移除 vCenter HA 或启动 vCenter HA 故障切换的单独按钮。

后续步骤

请参见管理 vCenter HA 配置，查看集群管理任务列表。

有关使用 vCenter HA 时 vSphere Client 中的增强功能的简要概述，请参见：

(在 vSphere Client 中使用 vCenter HA 的增强功能)

管理 vCenter HA 配置

配置 vCenter HA 集群之后，您可以执行管理任务。这些任务包括证书替换、SSH 密钥替换和 SNMP 设置。您还可以编辑集群配置，以停用或激活 vCenter HA、进入维护模式以及移除集群配置。

- 设置 SNMP 陷阱

  您可以设置简单网络管理协议 (Simple Network Management Protocol, SNMP) 陷阱以接收 vCenter HA 集群的 SNMP 通知。

- 设置环境以使用自定义证书

  每个节点上的计算机 SSL 证书用于集群管理通信和复制流量加密。若要使用自定义证书，必须移除 vCenter HA 配置、删除被动节点和见证节点、使用自定义证书置备主动节点并重新配置集群。

- 管理 vCenter HA SSH 密钥

  vCenter HA 在主动节点、被动节点和见证节点之间使用 SSH 密钥进行无密码身份验证。身份验证用于检测信号交换，以及文件和数据复制。要替换 vCenter HA 集群节点中的 SSH 密钥，请停用该集群，在主动节点上生成新的 SSH 密钥，将密钥传输到被动节点，然后启用该集群。

- 启动 vCenter HA 故障切换

  您可以手动启动故障切换，并使被动节点成为主动节点。

- 编辑 vCenter HA 集群配置

  编辑 vCenter HA 集群配置时，可以停用或激活集群、将集群置于维护模式或移除集群。

- 执行备份和恢复操作

  为了提高安全性，您可以备份 vCenter HA 集群中的主动节点。然后您可以在出现灾难性故障时还原该节点。

- 移除 vCenter HA 配置

  您可以从 vSphere Client 中移除 vCenter HA 配置。

- 重新引导所有 vCenter HA 节点

  如果需要先关闭再重新引导集群中的所有节点，您必须按特定的关闭顺序以防止被动节点承担主动节点的角色。

- 更改服务器环境

  部署 vCenter Server 时，您需要选择环境。对于 vCenter HA，生产环境支持“小型”、“中型”、“大型”和“超大型”这几种配置。如果您需要更多空间并且想要更改环境，您必须先删除被动节点虚拟机，然后才能更改配置。

- 收集 vCenter HA 节点的支持包

  从 vCenter HA 集群的所有节点收集支持包有助于进行故障排除。

设置 SNMP 陷阱

您可以设置简单网络管理协议 (Simple Network Management Protocol, SNMP) 陷阱以接收 vCenter HA 集群的 SNMP 通知。

陷阱默认为 SNMP 版本 1。

为主动节点和被动节点设置 SNMP 陷阱。通过在 snmpd 配置中添加一个目标项告知代理发送相关陷阱的位置。

步骤

1 使用虚拟机控制台或 SSH 登录到主动节点。

2 运行 `vicfg-snmp` 命令，例如：

```
vicfg-snmp -t 10.160.1.1@1166/public
```

在此示例中，`10.160.1.1` 为客户端侦听地址，`1166` 为客户端侦听端口，`public` 为社区字符串。

3 通过运行以下命令激活 SNMP 代理 (snmpd)。

```
vicfg-snmp -e
```

后续步骤

以下命令可能也会非常有用。

- 要查看命令的完整帮助，请运行 **`vicfg-snmp -h`**。
- 要停用 SNMP 代理，请运行 **`vicfg-snmp -D`**。
- 要显示 SNMP 代理的配置，请运行 **`vicfg-snmp -s`**。
- 要将配置重置为默认值，请运行 **`vicfg-snmp -r`**。

设置环境以使用自定义证书

每个节点上的计算机 SSL 证书用于集群管理通信和复制流量加密。若要使用自定义证书，必须移除 vCenter HA 配置、删除被动节点和见证节点、使用自定义证书置备主动节点并重新配置集群。

如果可以，请先替换将成为主动节点的 vCenter Server 中的证书，然后再克隆该节点。

步骤

1 编辑集群配置并选择**移除**。

2 删除被动节点和见证节点。

3 在当前作为独立 vCenter Server 的主动节点上，将计算机 SSL 证书替换为自定义证书。

4 重新配置集群。

管理 vCenter HA SSH 密钥

vCenter HA 在主动节点、被动节点和见证节点之间使用 SSH 密钥进行无密码身份验证。身份验证用于检测信号交换，以及文件和数据复制。要替换 vCenter HA 集群节点中的 SSH 密钥，请停用该集群，在主动节点上生成新的 SSH 密钥，将密钥传输到被动节点，然后启用该集群。

步骤

1 编辑集群，然后将模式更改为**禁用**。

2 使用虚拟机控制台或 SSH 登录到主动节点。

3 激活 Bash Shell。

```
bash
```

4 运行以下命令在主动节点上生成 SSH 密钥。

```
/usr/lib/vmware-vcha/scripts/resetSshKeys.py
```

5 使用 SCP 将密钥复制到被动节点和见证节点。

```
scp /vcha/.ssh/*
```

6 编辑集群配置，将 vCenter HA 集群设置为**启用**。

启动 vCenter HA 故障切换

您可以手动启动故障切换，并使被动节点成为主动节点。

vCenter HA 集群支持两种故障切换。

自动故障切换

被动节点在主动节点发生故障时尝试接管主动节点的角色。

手动故障切换

用户可以使用“启动故障切换”操作强制被动节点接管主动节点的角色。

启动手动故障切换以进行故障排除和测试。

步骤

1 使用 vSphere Client 登录到主动节点 vCenter Server，然后针对需要启动故障切换的 vCenter Server 单击**配置**。

2 在**设置**下，选择 **vCenter HA** 并单击**启动故障切换**。

3 单击**是**启动故障切换。

此时将打开一个对话框，其中提供了强制进行故障切换而不执行同步的选项。在大多数情况下，最好执行同步。

4 进行故障切换之后，您可以在 vSphere Client 中验证被动节点是否具有主动节点的角色。

编辑 vCenter HA 集群配置

编辑 vCenter HA 集群配置时，可以停用或激活集群、将集群置于维护模式或移除集群。

vCenter Server 的运行模式可控制 vCenter HA 集群中的故障切换能力和状态复制。

vCenter HA 可以在下列模式之一中运行。

表 4-3. vCenter HA 集群运行模式

模式	自动故障切换	手动故障切换	复制	
已启用	是	是	是	此默认运行模式通过执行自动故障切换，可防止 vCenter Server 出现硬件和软件故障。
维护	否	是	是	用于一些维护任务。对于其他任务，必须停用 vCenter HA。
已禁用	否	否	否	如果被动节点或见证节点丢失或正从故障中恢复，可以取消激活 vCenter HA 配置。主动节点作为独立 vCenter Server 继续运行。

注 如果集群在“维护”或“已禁用”模式下运行，即使被动节点和见证节点已丢失或不可访问，主动节点仍可继续处理客户端请求。

前提条件

验证 vCenter HA 集群是否已部署并包含主动、被动和见证节点。

步骤

1 使用 vSphere Client 登录到主动节点 vCenter Server，然后单击**配置**。

2 在**设置**下，选择 **vCenter HA**，然后单击**编辑**。

3 选择其中一个选项。

选项	结果
启用 vCenter HA	激活主动节点和被动节点之间的复制。如果集群处于正常状态，将从被动节点进行自动故障切换以保护主动节点。
维护模式	在维护模式下，主动节点与被动节点之间仍会进行复制。但是，将停用自动故障切换。
禁用 vCenter HA	停用复制和故障切换。保留集群的配置。稍后可以再次激活 vCenter HA。
移除 vCenter HA 集群	移除集群。不再提供复制和故障切换。主动节点作为独立 vCenter Server 继续运行。有关详细信息，请参见移除 vCenter HA 配置。

4 单击确定。

执行备份和恢复操作

为了提高安全性，您可以备份 vCenter HA 集群中的主动节点。然后您可以在出现灾难性故障时还原该节点。

注 在还原主动节点之前先移除集群配置。如果在您还原主动节点时被动节点仍在运行或者其他集群配置仍存在，则结果不可预知。

前提条件

确认 vCenter HA 与备份和还原解决方案的互操作性。其中一种解决方案是基于 vCenter Server 文件的还原。

步骤

1 备份主动节点。

请勿备份被动节点和见证节点。

2 在还原集群之前，请关闭所有 vCenter HA 节点的电源并将它们删除。

3 还原主动节点。

主动节点将还原为独立的 vCenter Server。

4 重新配置 vCenter HA。

移除 vCenter HA 配置

您可以从 vSphere Client 中移除 vCenter HA 配置。

步骤

1 登录主动节点 vCenter Server 并单击**配置**。

2 在**设置**下，选择 **vCenter HA** 并单击**移除 VCHA**。

- 从主动节点、被动节点和见证节点中移除 vCenter HA 集群的配置。
- 您可以选择删除被动节点和见证节点。

- 主动节点继续作为独立的 vCenter Server 运行。
- 无法在新的 vCenter HA 配置中重用被动节点和见证节点。
- 如果执行了手动配置，或者无法发现被动节点和见证节点，您必须明确删除这些节点。
- 即使第二个虚拟 NIC 是由配置过程添加的，移除过程也不会移除该虚拟 NIC。

重新引导所有 vCenter HA 节点

如果需要先关闭再重新引导集群中的所有节点，您必须按特定的关闭顺序以防止被动节点承担主动节点的角色。

步骤

1 按以下顺序关闭节点。
   - 被动节点
   - 主动节点
   - 见证节点

2 重新启动每个节点。

   可以按任何顺序重新启动节点。

3 验证是否所有节点均成功加入集群，并验证先前的主动节点是否恢复该角色。

更改服务器环境

部署 vCenter Server 时，您需要选择环境。对于 vCenter HA，生产环境支持“小型”、“中型”、“大型”和“超大型”这几种配置。如果您需要更多空间并且想要更改环境，您必须先删除被动节点虚拟机，然后才能更改配置。

步骤

1 使用 vSphere Client 登录主动节点，编辑集群配置，并选择**禁用**。

2 删除被动节点虚拟机。

3 更改主动节点的 vCenter Server 配置，例如从小型环境更改为中型环境。

4 重新配置 vCenter HA。

收集 vCenter HA 节点的支持包

从 vCenter HA 集群的所有节点收集支持包有助于进行故障排除。

从 vCenter HA 集群中的主动节点收集支持包时，系统将执行如下操作。

- 从主动节点本身收集支持包信息。
- 从被动和见证节点收集支持包，并将其放置在主动节点支持包上的 `commands` 目录中。

注 从被动和见证节点收集支持包是最佳操作方式，在节点可访问时才可行。

vCenter HA 环境故障排除

如果出现问题，您可以对环境进行故障排除。需要执行的任务取决于故障症状。有关其他故障排除信息，请参见 VMware 知识库系统。

- vCenter HA 克隆操作在部署过程中失败

  如果 vCenter HA 配置过程未成功创建克隆，您必须解决该克隆错误。

- 重新部署被动或见证节点

  如果被动或见证节点发生故障，并且 vCenter HA 集群是使用自动克隆方法配置的，则可以在 **vCenter HA 设置**页面中对其进行重新部署。

- vCenter HA 部署失败并显示错误

  部署失败的原因可能是配置问题，尤其是网络设置问题。

- 已降级 vCenter HA 集群的故障排除

  要让 vCenter HA 集群正常运行，每个主动、被动和见证节点都必须完全正常运行，并且可通过 vCenter HA 集群网络进行访问。如果任何节点出现故障，集群将被视为处于已降级状态。

- 从隔离的 vCenter HA 节点中恢复

  如果 vCenter HA 集群中的所有节点均无法相互通信，主动节点将停止处理客户端请求。

- 解决故障切换故障

  如果被动节点在故障切换期间未成为主动节点，您可以强制被动节点在故障切换期间成为主动节点。

- VMware vCenter® HA 警报和事件

  如果 vCenter HA 集群处于已降级状态，则警报和事件显示错误。

vCenter HA 克隆操作在部署过程中失败

如果 vCenter HA 配置过程未成功创建克隆，您必须解决该克隆错误。

问题

克隆操作失败。

注 将 VCHA 部署的被动或见证虚拟机克隆到与源主动节点相同的 NFS 3.1 数据存储会失败。您必须使用 NFS4 或将被动和见证虚拟机克隆到与主动虚拟机不同的数据存储。

原因

查找克隆异常。它可能指示以下问题之一。

- 您有一个已启用 DRS 的集群，但是没有三个主机。
- 主机或数据库连接丢失。
- 磁盘空间不足。
- 其他**克隆虚拟机**错误

解决方案

1 解决造成这个问题的错误。

2 移除集群并重新启动配置。

重新部署被动或见证节点

如果被动或见证节点发生故障，并且 vCenter HA 集群是使用自动克隆方法配置的，则可以在 **vCenter HA 设置**页面中对其进行重新部署。

步骤

1 通过 vSphere Client 登录到主动节点。

2 在清单中选择 vCenter Server 对象，然后选择**配置**选项卡。

3 选择**设置**下的 **vCenter HA**。

4 单击节点旁边的**重新部署**按钮以启动“重新部署”向导。

5
- 如果您的 vCenter Server 由同一 SSO 域中的其他 vCenter Server 管理，请转到步骤 6。
- 如果您的 vCenter Server 由不同 SSO 域中的其他 vCenter Server 管理，则输入该管理 vCenter Server 的位置和凭据详细信息。输入**管理 vCenter Server FQDN 或 IP 地址**和 **Single Sign-On** 凭据。

6 指定唯一名称和目标位置。

7 为此操作选择目标计算资源。

8 选择要存储配置和磁盘文件的数据存储。

9 配置虚拟机网络。
- 如果将重新部署被动节点，请选择虚拟机管理（网卡 0）和 vCenter HA（网卡 1）网络。
- 如果将重新部署见证节点，请选择 vCenter HA（网卡 1）网络。

如果选择内容出现问题，则会显示错误或兼容性警告。

10 查看您的选择，然后单击**完成**以重新部署节点。

vCenter HA 部署失败并显示错误

部署失败的原因可能是配置问题，尤其是网络设置问题。

问题

开始 vCenter HA 集群配置，但配置失败并显示错误。错误可能会显示问题的原因，例如，您可能会看到 SSH 连接失败消息。

解决方案

如果部署失败，请按照以下步骤解决网络问题。

1 确认可从主动节点访问被动节点和见证节点。

2 确认节点之间的路由设置正确。

3 检查网络延迟。

已降级 vCenter HA 集群的故障排除

要让 vCenter HA 集群正常运行，每个主动、被动和见证节点都必须完全正常运行，并且可通过 vCenter HA 集群网络进行访问。如果任何节点出现故障，集群将被视为处于已降级状态。

问题

集群处于已降级状态时，不会进行故障切换。有关集群处于已降级状态时故障情形的信息，请参见解决故障切换故障。

原因

集群处于已降级状态有很多原因。

某个节点出现故障

- 如果主动节点出现故障，则会自动从主动节点故障切换到被动节点。故障切换之后，被动节点将成为主动节点。

  此时，集群处于已降级状态，因为原来的主动节点不可用。

  出现故障的节点在修复或恢复联机后成为新的被动节点，而集群在主动节点和被动节点同步后恢复到正常状态。

- 如果被动节点发生故障，主动节点继续正常运行，但是无法进行故障切换且集群处于已降级状态。

  如果被动节点已修复或恢复联机，它会自动重新加入集群，主动节点和被动节点同步后，集群状态恢复正常。

- 如果见证节点发生故障，主动节点继续正常运行，主动节点和被动节点之间的复制也会继续，但无法进行故障切换。

  如果见证节点已修复或恢复联机，它会自动重新加入集群且集群状态恢复正常。

数据库复制失败

当主动节点与被动节点之间的复制失败时，集群将被视为已降级。主动节点继续与被动节点同步。如果同步成功，集群恢复到正常状态。此状态可能是由于网络带宽问题或其他资源短缺所致。

配置文件复制问题

如果主动节点和被动节点之间未正确复制配置文件，集群则处于已降级状态。主动节点继续尝试与被动节点同步。此状态可能是由于网络带宽问题或其他资源短缺所致。

解决方案

如何进行恢复取决于已降级集群状态的起因。如果集群处于已降级状态，事件、警报和 SNMP 陷阱将显示错误。

如果某个节点关闭，请检查是否发生硬件故障或网络隔离。检查发生故障的节点是否已打开电源。

如果复制失败，请检查 vCenter HA 网络的带宽是否充足，并确保网络延迟不超过 10 ms。

从隔离的 vCenter HA 节点中恢复

如果 vCenter HA 集群中的所有节点均无法相互通信，主动节点将停止处理客户端请求。

问题

节点隔离为网络连接问题。

解决方案

1 尝试解决连接问题。如果连接可以还原，隔离的节点会自动重新加入集群，并且主动节点会开始处理客户端请求。

2 如果无法解决连接问题，您必须直接登录到主动节点的控制台。

   a 关闭被动节点和见证节点虚拟机的电源并删除这些虚拟机。

   b 使用 SSH 或通过虚拟机控制台登录主动节点。

   c 要启用 Bash shell，请在 `appliancesh` 提示符下输入 **`shell`**。

   d 运行以下命令移除 vCenter HA 配置。

```
vcha-destroy -f
```

   e 重新引导主动节点。

   主动节点现在为独立的 vCenter Server。

   f 再次执行 vCenter HA 集群配置。

解决故障切换故障

如果被动节点在故障切换期间未成为主动节点，您可以强制被动节点在故障切换期间成为主动节点。

问题

在尝试承担主动节点的角色时，被动节点发生故障。

原因

vCenter HA 故障切换可能会因为以下原因而无法成功。

- 当被动节点尝试承担主动节点的角色时，见证节点不可用。
- 节点之间存在服务器状态同步问题。

解决方案

可以按如下所示从此问题恢复。

1 如果主动节点从故障中恢复，它会再次成为主动节点。

2 如果见证节点从故障中恢复，请遵循以下步骤。

a 通过虚拟机控制台登录到被动节点。

b 要启用 Bash shell，请在 `appliancesh` 提示符下输入 **`shell`**。

c 运行下列命令。

```
vcha-reset-primary
```

d 重新引导被动节点。

3 如果主动节点和见证节点均无法恢复，可以强制被动节点成为独立 vCenter Server。

a 删除主动节点虚拟机和见证节点虚拟机。

b 通过虚拟机控制台登录到被动节点。

c 要启用 Bash shell，请在 `appliancesh` 提示符下输入 **`shell`**。

d 运行下列命令。

```
vcha-destroy
```

e 重新引导被动节点。

VMware vCenter® HA 警报和事件

如果 vCenter HA 集群处于已降级状态，则警报和事件显示错误。

问题

表 4-4. 以下事件会在 vpxd 中引发 VCHA 运行状况警报：

事件名称	事件描述	事件类型	类别
vCenter HA 集群状态当前为正常	vCenter HA 集群状态当前为正常	com.vmware.vcha.cluster.state.healthy	信息
vCenter HA 集群状态当前为已降级	vCenter HA 集群状态当前为已降级	com.vmware.vcha.cluster.state.degraded	警告
vCenter HA 集群状态当前为已隔离	vCenter HA 集群状态当前为已隔离	com.vmware.vcha.cluster.state.isolated	错误
vCenter HA 集群已销毁	vCenter HA 集群已销毁	com.vmware.vcha.cluster.state.destroyed	信息

表 4-5. 以下事件会在 vpxd 中引发 PSC HA 运行状况警报：

事件名称	事件描述	事件类型	类别
PSC HA 状态当前为正常	PSC HA 状态当前为正常	com.vmware.vcha.psc.ha.health.healthy	信息
PSC HA 状态当前为已降级	PSC HA 状态当前为已降级	com.vmware.vcha.psc.ha.health.degraded	信息
在销毁 vCenter HA 集群后 PSC HA 不受监控	PSC HA 状态为不受监控	com.vmware.vcha.psc.ha.health.unknown	信息

表 4-6. 集群状态相关的事件

事件名称	事件描述	事件类型	类别
节点 {nodeName} 重新加入了集群	有一个节点重新加入了集群	com.vmware.vcha.node.joined	信息
节点 {nodeName} 退出了集群	有一个节点退出了集群	com.vmware.vcha.node.left	警告
故障切换成功	故障切换成功	com.vmware.vcha.failover.succeeded	信息
当集群处于禁用模式时，无法继续进行故障切换	当集群处于禁用模式时，无法继续进行故障切换	com.vmware.vcha.failover.failed.disabled.mode	警告
当集群并未连接所有三个节点时，无法继续进行故障切换	当集群并未连接所有三个节点时，无法继续进行故障切换	com.vmware.vcha.failover.failed.node.lost	警告
当被动节点上的 vPostgres 尚未准备好接管时，无法继续进行故障切换	当被动节点尚未准备好接管时，无法继续进行故障切换	com.vmware.vcha.failover.failed.passive.not.ready	警告
vCenter HA 集群模式已更改为 {clusterMode}	vCenter HA 集群模式已更改	com.vmware.vcha.cluster.mode.changed	信息

表 4-7. 数据库复制相关的事件

事件名称	事件描述	事件类型	类别
数据库复制模式已更改为 {newState}	数据库复制状态已更改为：同步、异步或未复制	com.vmware.vcha.DB.replication.state.changed	信息

表 4-8. 文件复制相关的事件

事件名称	事件描述	事件类型	类别
设备 {fileProviderType} 处于 {state} 状态	设备文件复制状态已更改	com.vmware.vcha.file.replication.state.changed	信息

修补 vCenter High Availability 环境

可以使用 vCenter Servershell 中提供的 **`software-packages`** 实用程序修补 vCenter High Availability 集群中的 vCenter Server。

有关详细信息，请参见 vSphere 升级中的修补 vCenter High Availability 环境。