



VMware

Enterprise applications

NetApp
February 11, 2026

目录

VMware	1
采用ONTAP的VMware vSphere	1
采用ONTAP的VMware vSphere	1
为什么选择适用于VMware vSphere的ONTAP?	1
统一存储	2
适用于 ONTAP 的虚拟化工具	3
虚拟卷 (VVOL) 和基于存储策略的管理 (SPBM)	5
数据存储库和协议	6
网络配置:	18
虚拟机和数据存储库克隆	20
数据保护	22
服务质量 (QoS)	24
云迁移和备份	29
vSphere 数据加密	29
Active IQ Unified Manager	30
基于存储策略的管理和虚拟卷	31
VMware Storage Distributed Resource Scheduler	33
建议的 ESXi 主机和其他 ONTAP 设置	34
使用工具的虚拟卷(Virtual Volume、ONTAP) 10.	37
概述	37
检查清单	41
将ONTAP 与虚拟卷结合使用	44
在AFF、ASA、ASA R2和FAS系统上部署虚拟卷	49
保护卷	59
故障排除	63
采用ONTAP的VMware Site Recovery Manager	64
使用ONTAP进行VMware实时站点恢复	64
部署最佳实践	66
操作最佳实践	67
复制拓扑	70
使用卷复制时对voISRM/SRM进行故障排除	79
追加信息	79
采用ONTAP的vSphere Metro存储集群	80
采用ONTAP的vSphere Metro存储集群	80
VMware vSphere解决方案概述	83
《VMSC设计和实施准则》	88
计划内和计划外事件的故障恢复能力	97
使用MetroCluster的VMSC的故障情形	98
产品安全性	109

适用于 VMware vSphere 的 ONTAP 工具	109
SnapCenter插件VMware vSphere	111
适用于VMware vSphere的ONTAP工具安全强化指南	113
适用于VMware vSphere 9.13的ONTAP工具安全强化指南	113
验证适用于VMware vSphere 9.13的ONTAP工具安装包的完整性	113
ONTAP工具的端口和协议9.13.	115
适用于VMware vSphere 9.13访问点(用户)的ONTAP工具	116
ONTAP工具9.13相互TLS (基于证书的身份验证)	117
ONTAP工具9.13 HTTPS证书	123
ONTAP工具9.13登录横幅	123
ONTAP工具的非活动超时9.13.	124
每个用户的最大并发请求数(网络安全保护/DOS攻击)适用于VMware vSphere的ONTAP工具9.13	124
ONTAP工具的网络时间协议(NTP)配置9.13.	125
ONTAP工具的密码策略9.13.	125

VMware

采用ONTAP的VMware vSphere

采用ONTAP的VMware vSphere

自2002年引入现代数据中心以来，ONTAP已成为VMware vSphere以及最近的Cloud Foundation环境的主要存储解决方案。它继续推出创新功能、以简化管理并降低成本。

本文档介绍了适用于vSphere的ONTAP解决方案，其中重点介绍了可简化部署、降低风险和简化管理的最新产品信息和最佳实践。



本文档可替代先前发布的技术报告_TR-4597：《适用于ONTAP的VMware vSphere》

最佳实践是指南和兼容性列表等其他文档的补充。它们是根据 NetApp 工程师和客户的实验室测试和丰富的现场经验开发的。它们可能并不是在每个环境中都能使用的唯一受支持的实践，但它们通常是最简单的解决方案，可满足大多数客户的需求。

本文档重点介绍在vSphere 7.0或更高版本上运行的ONTAP (9.x)的最新版本中的功能。有关特定版本的详细信息，请参见 "[互操作性表工具 \(IMT\)](#)" 和 "[VMware 兼容性指南](#)"。

为什么选择适用于VMware vSphere的ONTAP？

客户可以放心地选择ONTAP for vSphere 作为 SAN 和 NAS 存储解决方案。最新的 All SAN 阵列采用了新的简化分解存储架构，为 SAN 存储管理员提供了熟悉的简化体验，同时保留了传统ONTAP系统的大部分集成和功能集。ONTAP系统提供卓越的快照保护和强大的管理工具。通过将功能卸载到专用存储，ONTAP可以最大限度地利用主机资源、降低成本并保持最佳性能。此外，可以使用 Storage vMotion 轻松跨 VMFS、NFS 或vVols迁移工作负载。

使用适用于vSphere的ONTAP的优势

成千上万的客户选择ONTAP作为其vSphere存储解决方案的原因有很多，例如，支持SAN和NAS协议的统一存储系统、使用节省空间的快照的强大数据保护功能以及大量可帮助您管理应用程序数据的工具。使用与虚拟机管理程序不同的存储系统，您可以卸载许多功能，并最大程度地提高对 vSphere 主机系统的投资。这种方法不仅可以确保主机资源专注于应用程序工作负载，还可以避免存储操作对应用程序造成随机性能影响。

ONTAP与 vSphere 结合使用是一种很好的组合，可以让您减少主机硬件和 VMware 软件的费用。您还可以以较低的成本保护您的数据，同时保持始终如一的高性能。由于虚拟化工作负载是移动的，您可以探索使用 Storage vMotion 的不同方法在同一存储系统上跨 VMFS、NFS 或vVols数据存储移动虚拟机。

以下是当今客户重视的关键因素：

- ***统一存储。** *运行ONTAP 的系统在几个重要方面是统一的。最初，这种方法同时涉及 NAS 和 SAN 协议，ONTAP继续成为 SAN 的领先平台，同时又具有 NAS 方面的原有优势。在 vSphere 世界中，这种方法还意味着虚拟桌面基础架构 (VDI) 与虚拟服务器基础架构 (VSI) 的统一系统。运行ONTAP 的系统对于 VSI 而言通常比传统企业阵列更便宜，并且具有高级存储效率功能，可在同一系统中处理 VDI。ONTAP还统一了各种存储介质，从 SSD 到 SATA，并且可以轻松将其扩展到云端。没有必要为了性能而购买一个存储操作系统

，为了归档而购买另一个，为了云而购买另一个。ONTAP将它们全部联系在一起。

- ***全SAN阵列(ASA)**。*最新的ONTAP ASA系统(从A1K、A90、A70、A50、A30和A20开始)基于新的存储架构构建、消除了管理聚合和卷的传统ONTAP存储模式。由于没有文件系统共享、因此不需要卷！连接到HA对的所有存储都被视为通用存储可用性区域(SAZ)、其中LUN和NVMe命名空间配置为"存储单元"(SUS)。最新的ASA系统易于管理、并具有SAN存储管理员熟悉的体验。这种新架构非常适合vSphere环境、因为它可以轻松管理存储资源、并为SAN存储管理员提供简化的体验。ASA架构还支持最新的基于网络结构的NVMe (NVMe-oF)技术、可为vSphere工作负载提供更高的性能和可扩展性。
- ***快照技术**。*ONTAP是第一家提供数据保护快照技术的公司、它仍然是业内最先进的公司。这种节省空间的数据保护方法已扩展为支持VMware vSphere APIS for Array Integration (VAAI)。通过这种集成、您可以利用ONTAP的快照功能执行备份和还原操作、从而减少对生产环境的影响。通过这种方法、您还可以使用快照快速恢复VM、从而减少恢复数据所需的时间和精力。此外、ONTAP的快照技术还与VMware的实时站点恢复(VSR、以前称为站点恢复管理器[SRM])解决方案相集成、为您的虚拟化环境提供全面的数据保护策略。
- **虚拟卷和基于存储策略的管理**。NetApp是VMware在vSphere Virtual Volumes (vVols)开发方面的早期设计合作伙伴、为vVols和VMware vSphere APIs for Storage Awareness (VASA)提供架构输入和早期支持。这种方法不仅为VMFS带来了细粒度的VM存储管理、还支持通过基于存储策略的管理实现存储配置的自动化。这种方法允许存储架构师设计具有不同功能的存储池、以便虚拟机管理员轻松使用。ONTAP在vVol规模方面处于存储行业领先地位、在单个集群中支持数十万个vVols，而企业阵列和小型闪存阵列供应商每个阵列仅支持几千个vVols。NetApp还通过即将推出的功能推动细粒度VM管理的发展。
- ***存储效率**。*尽管NetApp是第一个为生产工作负载提供重复数据删除功能的公司、但这项创新并不是该领域的第一次或最后一次创新。它从快照开始、这是一种节省空间且不会影响性能的数据保护机制、同时结合FlexClone技术、可以立即为生产和备份使用制作虚拟机的读/写副本。NetApp继续提供内联功能、包括重复数据删除、压缩和零块重复数据删除、以从昂贵的SSD中榨取最多的存储空间。ONTAP还增加了使用压缩将较小的I/O操作和文件打包到磁盘块中的功能。这些功能的结合使得客户普遍看到VSI节省高达5:1，VDI节省高达30:1。最新一代ONTAP系统还包括硬件加速压缩和重复数据删除功能、可以进一步提高存储效率并降低成本。这种方法允许您在更少的空间内存储更多数据、从而降低总体存储成本并提高性能。NetApp对其存储效率功能非常有信心、因此提供了一个链接：<https://www.netapp.com/pdf.html?item=/media/79014-ng-937-Efficiency-Guarantee-Customer-Flyer.pdf> [效率保证^]。
- **多租户** ONTAP长期以来一直是多租户领域的领导者、允许您在单个集群上创建多个存储虚拟机(SVM)。这种方法允许您隔离工作负载并为不同的租户提供不同级别的服务、使其成为服务提供商和大型企业的理想选择。最新一代ONTAP系统还包括对租户容量管理的支持。此功能允许您为每个租户设置容量限制、确保没有单个租户可以消耗所有可用资源。这种方法有助于确保所有租户都能获得他们期望的服务级别、同时还能在租户之间提供高级别的安全性和隔离。此外、ONTAP的多租户功能与VMware的vSphere平台集成、使您可以通过以下方式轻松管理和监控虚拟化环境 "[适用于VMware vSphere的ONTAP工具](#)"和 "[数据基础架构洞察力](#)"。
- ***混合云**。*无论用于本地私有云、公共云基础架构还是结合两者优点的混合云、ONTAP解决方案都可以帮助您构建数据结构以简化和优化数据管理。从高性能全闪存系统开始、然后将它们与磁盘或云存储系统结合、以实现数据保护和云计算。从Azure、AWS、IBM或Google Cloud中选择、以优化成本并避免锁定。根据需要利用对OpenStack和容器技术的高级支持。NetApp还为ONTAP提供基于云的备份(SnapMirror Cloud、Cloud Backup Service和Cloud Sync)以及存储分层和归档工具(FabricPool)、以帮助降低运营费用并利用云的广泛覆盖范围。
- **等等**。*利用NetApp AFF A系列阵列的极致性能、在管理成本的同时加快虚拟化基础架构的运行速度。使用横向扩展ONTAP集群享受从维护到升级到完全更换存储系统的无中断运行。利用NetApp加密功能保护空闲数据、无需额外付费。通过精细的服务质量功能确保性能满足业务服务级别要求。它们都是行业领先的企业级数据管理软件ONTAP提供的广泛功能的一部分。

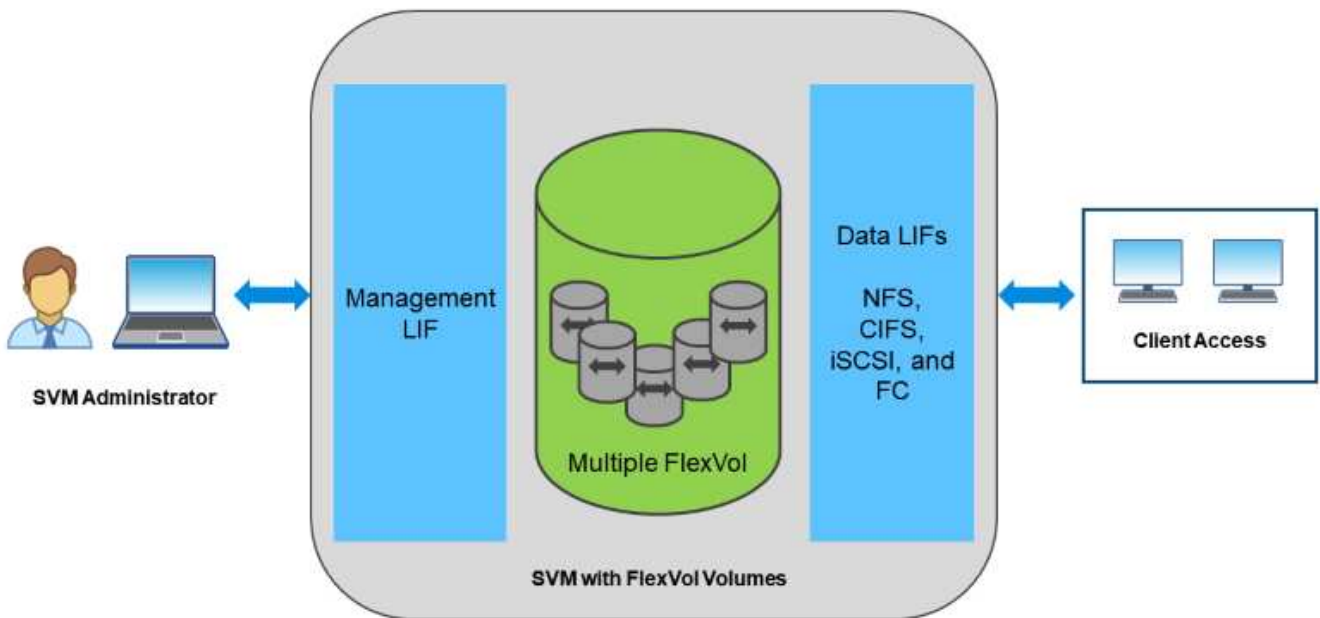
统一存储

ONTAP通过简化的软件定义方法统一存储、实现安全高效的管理、提高性能和无缝可扩展

性。这种方法可增强数据保护并有效利用云资源。

最初，这种统一方法指的是在一个存储系统上同时支持NAS和SAN协议、而ONTAP凭借其在NAS中的原有优势、仍然是SAN的领先平台。ONTAP现在还提供S3对象协议支持。虽然S3不用于数据存储库、但您可以将其用于子系统内应用程序。有关ONTAP中S3协议支持的详细信息，请参见"[S3配置概述](#)"。统一存储一词已发展为一种统一的存储管理方法、包括通过一个界面管理所有存储资源的能力。这包括能够同时管理内部和云存储资源、最新的全SAN阵列(ASA)系统、以及从一个界面管理多个存储系统。

Storage Virtual Machine (SVM)是ONTAP中的安全多租户单元。它是一种逻辑构造、允许客户端访问运行ONTAP的系统。SVM 可以通过多个数据访问协议通过逻辑接口（ Logical Interface ， LIF ）同时提供数据。SVM 可通过 CIFS 和 NFS 等 NAS 协议提供文件级数据访问，并通过 iSCSI ， FC/FCoE 和 NVMe 等 SAN 协议提供块级数据访问。SVM可以同时分别为SAN和NAS客户端以及S3提供数据。



在 vSphere 环境中，这种方法还可能意味着为虚拟桌面基础架构 (VDI) 和虚拟服务器基础架构 (VSI) 提供一个统一的系统。与传统企业阵列相比、运行ONTAP的系统在VSI方面的成本通常较低、但具有高级存储效率功能、可以在同一系统中处理VDI。ONTAP 还统一了从 SSD 到 SATA 的各种存储介质，并可轻松地将其扩展到云。无需购买一个闪存阵列即可实现高性能、一个SATA阵列可用于归档、而单独的系统则可用于云。ONTAP 将所有这些问题联系在一起。

*注：*有关SVM、统一存储和客户端访问的详细信息、请参见 "[存储虚拟化](#)" 在 ONTAP 9 文档中心。

适用于 **ONTAP** 的虚拟化工具

NetApp提供了多个与传统ONTAP和ASA系统兼容的独立软件工具、可通过集成vSphere来有效管理您的虚拟化环境。

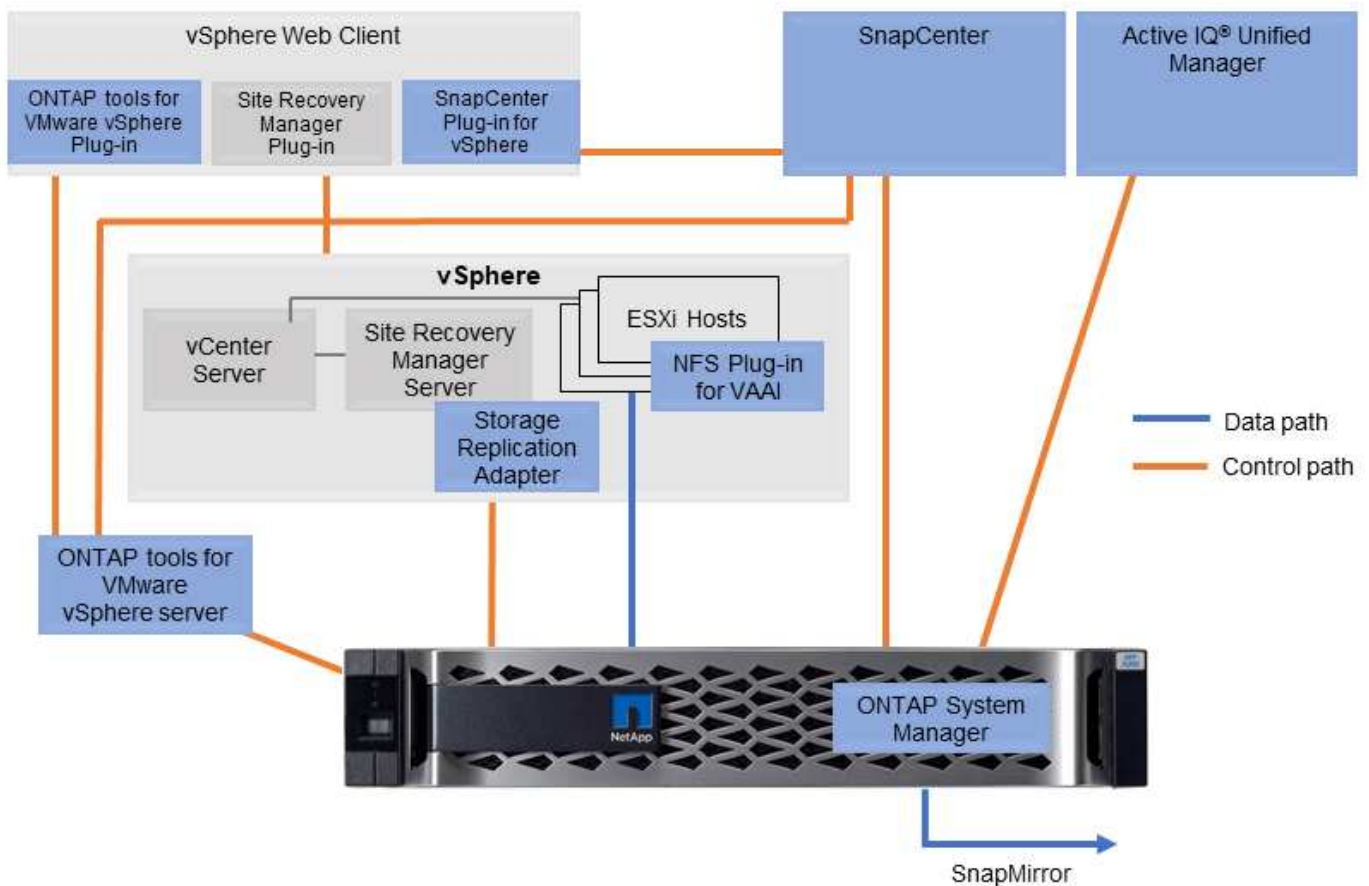
ONTAP One许可证附带了以下工具、无需额外付费。有关这些工具在 vSphere 环境中如何协同工作的说明，请参见图 1。

适用于 VMware vSphere 的 ONTAP 工具

"适用于 VMware vSphere 的 ONTAP 工具"是一组用于将ONTAP存储与vSphere结合使用的工具。无论您使用的是 SAN 还是 NAS，vCenter 插件（以前称为 Virtual Storage Console（VSC））均可简化存储管理和效率功能，提高可用性并降低存储成本和运营开销。它使用最佳实践配置数据存储库，并为 NFS 和块存储环境优化 ESXi 主机设置。为了获得所有这些优势，NetApp建议在将vSphere与运行ONTAP的系统结合使用时、最佳做法是使用这些ONTAP工具。它包括服务器设备、vCenter、VASA Provider和Storage Replication Adapter的用户界面扩展。ONTAP 工具中的几乎所有内容都可以通过简单的REST API实现自动化、而大多数现代自动化工具都可以使用这些API。

- *vCenter UI扩展。*ONTAP工具UI扩展可通过直接在vCenter UI中嵌入易于使用的上下文相关菜单来管理主机和存储、信息性portlet以及本机警报功能来简化工作流、从而简化运营团队和vCenter管理员的工作。
- *适用于ONTAP 的VASA Provider。*适用于ONTAP 的VASA Provider支持VMware vStorage APIs for Storage Awareness (VASA)框架。它作为适用于 VMware vSphere 的 ONTAP 工具的一部分提供，作为一个虚拟设备，易于部署。VASA Provider 可将 vCenter Server 与 ONTAP 连接起来，以帮助配置和监控 VM 存储。它支持 VMware 虚拟卷（VVOL）支持，管理存储功能配置文件和单个 VM VVOL 性能，并提供警报以监控容量和配置文件合规性。
- *存储复制适配器。*SRA 与 VMware Live Site Recovery (VLSR)/Site Recovery Manager (SRM) 一起使用，使用SnapMirror进行基于阵列的复制，管理生产站点和灾难恢复站点之间的数据复制。它可以在发生灾难时自动执行故障转移任务，并可以帮助无中断地测试 DR 副本，以确保对 DR 解决方案的信心。

下图显示了适用于 vSphere 的 ONTAP 工具。



适用于VMware vSphere的SnapCenter插件

这 "适用于VMware vSphere的SnapCenter插件" 是 vCenter Server 的一个插件, 可让您管理虚拟机 (VM) 和数据存储区的备份和还原。它提供了一个单一界面来管理跨多个ONTAP系统的虚拟机和数据存储库的备份、恢复和克隆。SnapCenter支持使用SnapMirror复制到辅助站点以及从辅助站点恢复。最新版本还支持SnapMirror到云 (S3)、防篡改快照、SnapLock和SnapMirror主动同步。适用于 VMware vSphere 的SnapCenter插件可以与SnapCenter应用程序插件集成, 以提供应用程序一致的备份。

适用于 VMware VAAI 的 NFS 插件

[https://mysupport.netapp.com/site/products/all/details/nfsplugin-vmware-vaai/about-tab\["适用于VMware VAAI的NetApp NFS插件"\]](https://mysupport.netapp.com/site/products/all/details/nfsplugin-vmware-vaai/about-tab[)是适用于ESXi主机的插件、允许这些主机对ONTAP上的NFS数据存储库使用VAAI功能。它支持克隆操作的副本卸载、厚虚拟磁盘文件的空间预留以及快照卸载。将副本操作卸载到存储不一定会更快完成、但它会降低网络带宽要求、并减轻CPU周期、缓冲区和队列等主机资源的负载。您可以使用适用于VMware vSphere的ONTAP 工具在ESXi主机或vSphere Lifecycle Manager (如果支持) 上安装此插件。

高级软件选项

NetApp提供以下优质软件产品。它们不包含在ONTAP One 许可证中, 必须单独购买。

- "NetApp Disaster Recovery(DR)"适用于 VMware vSphere。这是一项基于云的服务, 为 VMware 环境提供灾难恢复和备份。它可以与SnapCenter一起使用, 也可以单独使用, 并且支持使用 SAN 或 NAS 进行本地到本地的 DR, 以及使用 NFS 进行本地到云/从云 (如果支持)。
- "数据基础架构洞察力(DII)"。这是一项基于云的服务, 为 VMware 环境提供监控和分析。它支持异构存储环境中的其他存储供应商, 以及多个交换机供应商和其他虚拟机管理程序。DII 提供有关 VMware 环境的性能、容量和健康状况的完整端到端洞察。

虚拟卷 (VVOL) 和基于存储策略的管理 (SPBM)

NetApp于2012年首次宣布、是VMware的早期设计合作伙伴、负责开发VMware vSphere APIS for Storage AWARE/VAWARE(VASA)、这是企业级存储阵列基于存储策略的管理(Storage Policy Based Management、SPBM)的基础。这种方法为VMFS和NFS存储提供了有限的VM粒度存储管理。

作为技术设计合作伙伴、NetApp提供了架构方面的投入、并于2015年宣布支持虚拟卷。现在、这项新技术可通过SPBM实现VM粒度和真正的阵列本机存储配置自动化。

虚拟卷(Virtual Volume、Virtual Volume、Virtual Volume)

vvol是一种革命性的存储架构、支持VM粒度存储管理、不仅可以按VM (包括VM元数据)管理存储、还可以按VMDK管理存储。vvol是软件定义的数据中心(SDDC)战略的一个关键组件、该战略构成了VMware Cloud Foundation (VCF)的基础、可为虚拟化环境提供更高效、可扩展的存储架构。

通过Vvol、VM可以按每个VM使用存储、因为每个VM存储对象都是NetApp ONTAP中的一个唯一实体。对于不再需要卷管理的ASA R2系统、这意味着每个VM存储对象都是阵列上的一个唯一存储单元(SU)、可以独立控制。这样、便可创建可应用于单个VM或VMDK (从而实现独立SUS)的存储策略、从而对性能、可用性和数据保护等存储服务进行精细控制。

基于存储策略的管理(Storage Policy Based Management、SPBM)

SPBM 提供了一个框架，可用作虚拟化环境可用存储服务与通过策略配置的存储元素之间的抽象层。通过这种方法，存储架构师可以设计具有不同功能的存储池。VM管理员可以轻松使用这些池。然后，管理员可以将虚拟机工作负载要求与所配置的存储池进行匹配。此方法可简化存储管理、并可更高效地利用存储资源。

SPBM是虚拟卷的一个关键组件、可提供一个基于策略的框架来管理存储服务。策略由vSphere管理员使用供应商的VASA Provider (VP)提供的规则和功能来创建。可以为性能、可用性和数据保护等不同存储服务创建策略。可以将策略分配给单个VM或VMDK、从而对存储服务进行精细控制。

NetApp ONTAP和虚拟卷

NetApp ONTAP在虚拟卷扩展领域居于存储行业领先地位，可在一个集群中支持数十万个虚拟卷*。相比之下，企业级阵列供应商和小型闪存阵列供应商支持的每个阵列只能支持数千个的卷。ONTAP为VMware vSphere环境提供了一个可扩展的高效存储解决方案、可通过一组丰富的存储服务(包括重复数据删除、数据压缩、精简配置和数据保护)来支持vvol。SPBM支持与VMware vSphere环境无缝集成。

我们之前提到、VM管理员可以将容量用作存储池。这可以通过使用存储容器来实现、这些存储容器在vSphere中表示为逻辑数据存储库。

存储容器由存储管理员创建、用于对可由VM管理员使用的存储资源进行分组。根据您使用的ONTAP系统类型、创建存储容器的方式可能有所不同。对于传统ONTAP 9集群、系统会为容器分配一个或多个后备FlexVol卷、这些卷共同构成存储池。对于ASA R2系统、整个集群都是存储池。



有关 VMware vSphere 虚拟卷，SPBM 和 ONTAP 的详细信息，请参见 ["TR-4400：采用 ONTAP 的 VMware vSphere 虚拟卷"](#)。

*取决于平台和协议

数据存储库和协议

vSphere数据存储库和协议功能概述

可使用六种协议将VMware vSphere连接到运行ONTAP的系统上的数据存储库：

- FCP
- NVMe/FC
- NVMe/TCP
- iSCSI
- NFS v3
- NFS v4.1

FCP、NVMe/FC、NVMe/TCP和iSCSI是块协议、它们使用vSphere虚拟机文件系统(VMFS)将VM存储在ONTAP FlexVol volume中包含的ONTAP LUN或NVMe命名空间中。NFS 是一种文件协议，无需使用 VMFS 即可将虚拟机放置到数据存储库（即 ONTAP 卷）中。SMB (CIFS)、iSCSI、NVMe/TCP或NFS也可以从子操作系统直接使用到ONTAP。

以下表格展示了 vSphere 支持的使用 ONTAP 的传统数据存储功能。此信息不适用于 vVols 数据存储区，但它通常适用于使用支持的 ONTAP 版本的 vSphere 6.x 及更高版本。您也可以查阅 ["VMware配置最大值工具"](#) 有关特定 vSphere 版本的信息，以确认特定限制。

功能 / 功能	FC	iSCSI	NVMe-oF	NFS
格式。	VMFS 或原始设备映射 (RDM)	VMFS 或 RDM	VMFS	不适用
数据存储库或 LUN 的最大数量	每个 ESXi 主机 1024 个 LUN, 每个 LUN 最多 32 个路径, 每个主机最多 4096 个总路径, 每个数据存储区最多 128 个主机	每个 ESXi 主机 1024 个 LUN, 每个 LUN 最多 32 个路径, 每个主机最多 4096 个总路径, 每个数据存储区最多 128 个主机	每个 ESXi 主机 256 个命名空间, 每个主机每个命名空间最多 32 个路径, 每个主机总共 2048 个路径, 每个数据存储区最多 16 个主机	每个主机256个NFS连接(受nconnect和会话中继的影响)默认NFS。最大卷数为8。使用适用于VMware vSphere 的 ONTAP 工具将其增加到 256。
最大数据存储库大小	64 TB	64 TB	64 TB	使用 FlexGroup 卷时为 300 TB 或更高的 FlexVol 卷
最大数据存储库文件大小	62 TB	62 TB	62 TB	使用ONTAP 9.12.1P2及更高版本时为62 TB
每个 LUN 或文件系统的最佳队列深度	64 – 256	64 – 256	已自动协商	请参见中的 NFS.MaxQueueDepth "建议的 ESXi 主机和其他 ONTAP 设置"。

下表列出了支持的 VMware 存储相关功能。

容量 / 功能	FC	iSCSI	NVMe-oF	NFS
VMotion	是的。	是的。	是的。	是的。
存储 vMotion	是的。	是的。	是的。	是的。
VMware HA	是的。	是的。	是的。	是的。
存储分布式资源计划程序 (Storage Distributed Resource Scheduler , SDRS)	是的。	是的。	是的。	是的。
启用了VMware vStorage APIS for Data Protection (VADP)的备份软件	是的。	是的。	是的。	是的。
虚拟机中的 Microsoft 集群服务 (MSCS) 或故障转移集群	是的。	是 ¹	是 ¹	不支持
容错	是的。	是的。	是的。	是的。
Live Site Recon/Site Recovery Manager	是的。	是的。	否 ²	仅v3 ²

容量 / 功能	FC	iSCSI	NVMe-oF	NFS
精简配置的 VM (虚拟磁盘)	是的。	是的。	是的。	是的。 如果不使用VAAI、则此设置是NFS上所有VM的默认设置。
VMware 原生多路径	是的。	是的。	是的。	NFS v4.1会话中继需要ONTAP 9.14.1及更高版本

下表列出了支持的 ONTAP 存储管理功能。

功能 / 功能	FC	iSCSI	NVMe-oF	NFS
重复数据删除	阵列中的节省量	阵列中的节省量	阵列中的节省量	数据存储库中的节省量
精简配置	数据存储库或 RDM	数据存储库或 RDM	数据存储库	数据存储库
调整数据存储库大小	仅增长	仅增长	仅增长	增长, 自动增长和缩减
适用于 Windows 和 Linux 应用程序的 SnapCenter 插件 (在子系统中)	是的。	是的。	是的。	是的。
使用适用于 VMware vSphere 的 ONTAP 工具监控和主机配置	是的。	是的。	是的。	是的。
使用适用于 VMware vSphere 的 ONTAP 工具进行配置	是的。	是的。	是的。	是的。

下表列出了支持的备份功能。

功能 / 功能	FC	iSCSI	NVMe-oF	NFS
ONTAP Snapshot	是的。	是的。	是的。	是的。
复制的备份支持 SRM	是的。	是的。	否 ²	仅v3 ²
卷 SnapMirror	是的。	是的。	是的。	是的。
VMDK 映像访问	支持SnapCenter和VADP的备份软件	支持SnapCenter和VADP的备份软件	支持SnapCenter和VADP的备份软件	启用了SnapCenter和VADP的备份软件、vSphere Client和vSphere Web Client数据存储库浏览器
vmdk 文件级访问	启用了SnapCenter和VADP的备份软件、仅限Windows	启用了SnapCenter和VADP的备份软件、仅限Windows	启用了SnapCenter和VADP的备份软件、仅限Windows	支持SnapCenter和VADP的备份软件和第三方应用程序
NDMP 粒度	数据存储库	数据存储库	数据存储库	数据存储库或虚拟机

¹ *NetApp 建议*对 Microsoft 群集使用来宾内 iSCSI，而不是在 VMFS 数据存储中使用启用了多写入器的 VMDK。这种方法得到了 Microsoft 和 VMware 的充分支持，通过 ONTAP 提供了极大的灵活性（SnapMirror 到本地或云中的 ONTAP 系统），易于配置和自动化，并且可以使用 SnapCenter 进行保护。vSphere 7 添加了新的群集 VMDK 选项。这与启用了多写入器的 VMDK 不同，后者需要启用了群集 VMDK 支持的 VMFS 6 数据存储。其他限制适用。有关配置指南，请参阅 VMware 的 "[Windows Server 故障转移集群设置](#)" 文档。

²使用 NVMe-oF 和 NFS v4.1 的数据存储库需要 vSphere 复制。SRM 目前不支持对 NFS v4.1 执行基于阵列的复制。适用于 VMware vSphere Storage Replication Adapter (SRA) 的 ONTAP 工具目前不支持使用 NVMe-oF 进行基于阵列的复制。

选择存储协议

运行 ONTAP 的系统支持所有主要的存储协议，因此客户可以根据现有和计划的网络基础设施和员工技能选择最适合其环境的存储协议。从历史上看，NetApp 测试通常显示以相似线速和连接数量运行的协议之间几乎没有差异。但是，NVMe-oF（NVMe/TCP 和 NVMe/FC）在 IOPS 方面显示出显著的增益，延迟减少，并且存储 IO 的主机 CPU 消耗减少了 50% 或更多。另一方面，NFS 提供了最大的灵活性和易管理性，特别是对于大量的虚拟机。所有这些协议都可以使用 ONTAP tools for VMware vSphere 进行使用和管理，该工具提供了一个简单的界面来创建和管理数据存储。

在考虑选择协议时，以下因素可能会很有用：

- *当前操作环境。*虽然 IT 团队通常擅长管理以太网 IP 基础架构，但并非所有 IT 团队都擅长管理 FC SAN 网络结构。但是，如果使用的是不针对存储流量设计的通用 IP 网络，则可能效果不会很好。请考虑您已有的网络基础架构，任何计划内的改进，以及管理这些改进的人员的技能和可用性。
- *易于设置。*除了 FC 网络结构的初始配置（额外的交换机以及 HBA 和固件的布线，分区以及互操作性验证）之外，块协议还需要创建和映射 LUN 以及通过子操作系统进行发现和格式化。创建并导出 NFS 卷后，它们将由 ESXi 主机挂载并准备好使用。NFS 没有特殊的硬件资格认定或固件可供管理。
- *易于管理。*对于 SAN 协议，如果需要更多空间，则需要执行几个步骤，包括扩展 LUN、重新扫描以发现新的大小，然后扩展文件系统。虽然可以增加 LUN，但减小 LUN 的大小则不可能。NFS 允许轻松调整大小，并且可以由存储系统自动调整大小。SAN 通过来宾操作系统 DEALLOCATE/TRIM/UNMAP 命令提供空间回收，允许将已删除文件的空间返回到阵列。这种类型的空间回收对于 NFS 数据存储区是不可能的。
- *存储空间透明度。*在 NFS 环境中，存储利用率通常更容易查看，因为精简配置可以立即实现节省。同样，重复数据删除和克隆节省的空间可立即用于同一数据存储库中的其他虚拟机或其他存储系统卷。NFS 数据存储库中的虚拟机密度通常也会更高，这样可以减少要管理的数据存储库数量，从而节省重复数据删除的空间，并降低管理成本。

数据存储库布局

ONTAP 存储系统可以非常灵活地为 VM 和虚拟磁盘创建数据存储库。虽然在使用 ONTAP 工具为 vSphere 配置数据存储库时会应用许多 ONTAP 最佳实践（在一节中列出"[建议的 ESXi 主机和其他 ONTAP 设置](#)"），但仍需要考虑以下一些准则：

- 使用 ONTAP NFS 数据存储部署 vSphere 可实现高性能、易于管理的实施，提供基于块的存储协议无法获得的 VM 与数据存储比率。这种架构可以使数据存储密度增加十倍，并相应地减少数据存储的数量。虽然较大的数据存储可以提高存储效率并提供运营优势，但请考虑每个节点至少使用四个数据存储（FlexVol 卷）将 VM 存储在单个 ONTAP 控制器上，以从硬件资源中获得最大性能。这种方法还允许您建立具有不同恢复策略的数据存储。根据业务需求，某些数据存储可以比其他数据存储更频繁地备份或复制。对于性能而言，FlexGroup 卷不需要多个数据存储，因为它们通过设计进行扩展。
- *NetApp 建议*对大多数 NFS 数据存储使用 FlexVol 卷。从 ONTAP 9.8 开始，FlexGroup 卷也支持用作数据存储，通常建议用于某些用例。一般不建议使用其他 ONTAP 存储容器，例如 qtree，因为目前 ONTAP tools for VMware vSphere 或 NetApp SnapCenter plugin for VMware vSphere 都不支持这些容器。

- 对于 FlexVol 卷数据存储库，大小合适的数据存储库大约为 4 TB 到 8 TB。这种大小可以很好地平衡性能，易管理性和数据保护。从小规模入手（例如 4 TB），然后根据需要扩展数据存储库（最大 300 TB）。较小的数据存储库可以更快地从备份中或发生灾难后进行恢复，并可在集群中快速移动。请考虑使用 ONTAP 自动调整大小功能在已用空间发生变化时自动增长和缩减卷。默认情况下、适用于 VMware vSphere 的 ONTAP 工具数据存储库配置向导会对新数据存储库使用自动调整大小。可以使用 System Manager 或命令行对增长和缩减阈值以及大小上限和下限进行其他自定义。
- 或者、也可以为 VMFS 数据存储库配置可通过 FC、iSCSI、NVMe/FC 或 NVMe/TCP 访问的 LUN 或 NVMe 命名空间（在新 ASA 系统中称为存储单元）。VMFS 允许集群中的每个 ESX 服务器同时访问数据存储库。VMFS 数据存储库的大小最多可达 64 TB，并且最多可包含 32 个 2 TB LUN（VMFS 3）或一个 64 TB LUN（VMFS 5）。在 AFF、ASA 和 FAS 系统上、ONTAP 的最大 LUN 大小为 128 TB。NetApp 始终建议对每个数据存储库使用一个大型 LUN、而不是尝试使用块区。与 NFS 一样、请考虑使用多个数据存储库（卷或存储单元）、以最大程度地提高单个 ONTAP 控制器的性能。
- 较旧的子操作系统（OS）需要与存储系统对齐，以获得最佳性能和存储效率。但是，Microsoft 和 Linux 分销商（例如 Red Hat）提供的现代供应商支持的操作系统不再需要进行调整，以便在虚拟环境中将文件系统分区与底层存储系统的块对齐。如果您使用的是可能需要对齐的旧操作系统、请使用“VM 对齐”搜索 NetApp 支持知识库文章、或者向 NetApp 销售人员或合作伙伴联系人申请 TR-3747 副本。
- 避免在子操作系统中使用碎片整理实用程序、因为这不会带来任何性能优势、并会影响存储效率和快照空间使用量。此外，还应考虑在子操作系统中关闭虚拟桌面的搜索索引。
- ONTAP 凭借创新的存储效率功能引领行业发展，帮助您充分利用可用磁盘空间。AFF 系统通过默认实时重复数据删除和数据压缩进一步提高了这种效率。数据会在聚合中的所有卷之间进行重复数据删除，因此您无需再将相似的操作系统和类似应用程序分组到一个数据存储库中，即可最大程度地节省空间。
- 在某些情况下，您甚至可能不需要数据存储库。考虑子系统拥有的文件系统、例如由子系统管理的 NFS、SMB、NVMe/TCP 或 iSCSI 文件系统。有关具体的应用指南，请参见适用于您的应用程序的 NetApp 技术报告。例如、“[基于 ONTAP 的 Oracle 数据库](#)”中有一节介绍虚拟化、并提供了有用的详细信息。
- 一级磁盘（或经过改进的虚拟磁盘）支持独立于运行 vSphere 6.5 及更高版本的 VM 的 vCenter 管理磁盘。虽然它们主要由 API 管理，但对于 VVOL 很有用，尤其是在由 OpenStack 或 Kubernetes 工具管理时。ONTAP 以及适用于 VMware vSphere 的 ONTAP 工具均支持这些功能。

数据存储库和 VM 迁移

将 VM 从另一个存储系统上的现有数据存储库迁移到 ONTAP 时，请记住以下一些实践：

- 使用 Storage vMotion 将虚拟机的批量移动到 ONTAP。这种方法不仅不会对正在运行的 VM 造成中断，而且还可以通过实时重复数据删除和数据压缩等 ONTAP 存储效率功能在数据迁移时对其进行处理。请考虑使用 vCenter 功能从清单列表中选择多个 VM，然后在适当的时间计划迁移（单击操作时使用 Ctrl 键）。
- 虽然您可以仔细规划迁移到适当的目标数据存储，但批量迁移后再根据需要进行组织通常更简单。如果您有特定的数据保护需求，例如不同的 Snapshot 计划，您可能需要使用此方法来指导您迁移到不同的数据存储。此外，一旦 VM 在 NetApp 集群上，存储 vMotion 可以使用 VAAI 卸载在集群上的数据存储之间移动 VM，而无需基于主机的副本。请注意，NFS 不会卸载已开机 VM 的存储 vMotion；但是，VMFS 会。
- 需要更仔细迁移的虚拟机包括使用连接存储的数据库和应用程序。一般情况下、请考虑使用应用程序的工具来管理迁移。对于 Oracle，请考虑使用 RMAN 或 ASM 等 Oracle 工具迁移数据库文件。有关详细信息、请参见“[将 Oracle 数据库迁移到 ONTAP 存储系统](#)”。同样，对于 SQL Server，请考虑使用 SQL Server Management Studio 或 NetApp 工具，例如适用于 SQL Server 的 SnapManager 或 SnapCenter。

适用于 VMware vSphere 的 ONTAP 工具

在使用运行 ONTAP 的系统与 vSphere 时，最重要的最佳实践是安装并使用 ONTAP tools for VMware vSphere 插件（以前称为 Virtual Storage Console）。这个 vCenter 插件简化了存储管理，提高了可用性，并降低了存储成本和运维开销，无论是在 ASA、AFF、FAS 还是 ONTAP Select（在 VMware 或 KVM 虚拟机中运行的

ONTAP 软件定义版本) 上使用 SAN 或 NAS。它采用了为数据存储配置制定的最佳实践, 并针对多路径和 HBA 超时优化了 ESXi 主机设置 (这些内容在附录 B 中有描述)。由于它是一个 vCenter 插件, 所有连接到 vCenter 服务器的 vSphere Web 客户端都可以使用它。

此插件还可帮助您在 vSphere 环境中使用其他 ONTAP 工具。您可以通过此插件安装适用于 VMware VAAI 的 NFS 插件、以便将副本卸载到 ONTAP 以执行 VM 克隆操作、为厚虚拟磁盘文件预留空间以及卸载 ONTAP 快照。



在基于映像的 vSphere 群集上, 仍要将 NFS 插件添加到映像中, 以便在使用 ONTAP tools 安装时不会出现合规性问题。

ONTAP 工具也是适用于 ONTAP 的 VASA Provider 的许多功能的管理界面、支持使用 VVOL 进行基于存储策略的管理。

一般来说, * NetApp 建议 * 在 vCenter 中使用适用于 VMware vSphere 的 ONTAP 工具界面来配置传统数据存储库和 Vvol 数据存储库、以确保遵循最佳实践。

常规网络连接

在运行 ONTAP 的系统中使用 vSphere 时配置网络设置非常简单, 与其他网络配置类似。以下是一些需要考虑的事项:

- 将存储网络流量与其他网络分开。可以通过使用专用 VLAN 或单独的存储交换机来实现单独的网络。如果存储网络共享上行链路等物理路径, 您可能需要 QoS 或其他上行链路端口来确保带宽充足。请勿将主机直接连接到存储; 使用交换机提供冗余路径、并允许 VMware HA 在没有干预的情况下运行。请参见 ["直连网络"](#) 适用于追加信息。
- 如果您的网络需要并支持巨型帧, 则可以使用巨型帧, 尤其是在使用 iSCSI 时。如果使用这些协议, 请确保在存储和 ESXi 主机之间的路径中的所有网络设备, VLAN 等上对其进行相同的配置。否则, 您可能会看到性能或连接问题。此外, 还必须在 ESXi 虚拟交换机, VMkernel 端口以及每个 ONTAP 节点的物理端口或接口组上以相同的方式设置 MTU。
- NetApp 仅建议在 ONTAP 集群中的集群互连端口上禁用网络流量控制。对于用于数据流量的其余网络端口, NetApp 不提供其他最佳实践建议。您应根据需要启用或禁用。有关流量控制的更多背景信息、请参见 ["TR-4182"](#)。
- 当 ESXi 和 ONTAP 存储阵列连接到以太网存储网络时, **PortFast** NetApp 建议将这些系统连接到的以太网端口配置为快速生成树协议 (RSTP) 边缘端口或使用 Cisco 端口快速功能。* NetApp 建议 * 在使用 Cisco PortFast 功能且为 ESXi 服务器或 ONTAP 存储阵列启用了 802.1Q VLAN 中继的环境中启用生成树 PortFast 中继功能。
- * NetApp 建议 * 以下链路聚合最佳实践:
 - 使用支持使用多机箱链路聚合组方法 (例如 Cisco 的 Virtual PortChannel (vPC)) 在两个独立交换机机箱上进行端口链路聚合的交换机。
 - 对连接到 ESXi 的交换机端口禁用 LACP、除非您使用的是配置了 LACP 的 dvSwitches 5.1 或更高版本。
 - 使用 LACP 为具有端口或 IP 哈希动态多模式接口组的 ONTAP 存储系统创建链路聚合。请参见 ["网络管理"](#) 以获得进一步指导。
 - 如果对 vSphere 分布式交换机使用静态链路聚合 (例如 EtherChannel) 和标准 vswitch 或基于 LACP 的链路聚合、请在 ESXi 上使用 IP 哈希绑定策略。如果未使用链路聚合、请改用 "基于源虚拟端口 ID 路由"。

SAN (FC , FCoE , NVMe/FC , iSCSI) , RDM

在 vSphere 中、可以通过四种方式使用块存储设备:

- 使用 VMFS 数据存储库
- 使用原始设备映射 (RDM)
- 作为iSCSI连接的LUN或NVMe/TCP连接的命名空间、由软件启动程序从VM子操作系统访问和控制
- 作为一个卷数据存储库

VMFS 是一种高性能集群文件系统，可提供共享存储池中的数据存储库。可以为VMFS数据存储库配置使用FC、iSCSI、FCoE访问的LUN、或者配置使用NVMe/FC或NVMe/TCP协议访问的NVMe命名区。VMFS允许集群中的每个ESX服务器同时访问存储。从ONTAP 9.12.1P2 (以及ASA系统中的更早版本)开始、最大LUN大小通常为128 TB；因此、可以使用一个LUN来创建大小上限为64 TB的VMFS 5或6数据存储库。



块区是一个vSphere存储概念、您可以将多个LUN "拼接"在一起、以创建一个更大的数据存储库。切勿使用块区来达到所需的数据存储库大小。对于VMFS数据存储库、最佳做法是使用一个LUN。

vSphere内置了对存储设备的多个路径的支持。vSphere可以检测受支持存储系统的存储设备类型、并自动配置多路径堆栈以支持所使用存储系统的功能、无论所使用的协议如何、也无论使用的是ASA、AFF、FAS还是软件定义的ONTAP。

vSphere和ONTAP均支持使用NVMe/FC和NVMe/TCP为光纤通道和iSCSI建立主动/优化和主动/非优化路径、并为NVMe命名空间建立非对称命名空间访问(ANA)。在ONTAP中、AUA或ANA优化的路径遵循直接数据路径、使用托管要访问的LUN或命名空间的节点上的目标端口。默认情况下、vSphere和ONTAP均会启用ALOA/ANA。vSphere中的多路径软件会将ONTAP集群识别为AUA或ANA、并使用适当的本机插件和轮叫负载平衡策略。

在NetApp的ASA系统中、LUN和名称库会通过对称路径提供给ESXi主机。表示所有路径均处于活动状态并已进行优化。vSphere中的多路径软件会将ASA系统识别为对称系统、并使用适当的本机插件和循环负载平衡策略。



有关优化的多路径设置、请参见"[建议的 ESXi 主机和其他 ONTAP 设置](#)"。

ESXi不会发现任何超出其限制的LUN、名称和路径。在较大的 ONTAP 集群中、可以在达到 LUN 限制之前达到路径限制。为了解决此限制、ONTAP 在 8.3 及更高版本中支持选择性 LUN 映射 (SLM)。



有关ESXi中支持的最新限制、请参见"[VMware配置最大值工具](#)"。

SLM 会限制向给定 LUN 公布路径的节点。NetApp最佳实践是、每个SVM的每个节点至少具有两个LIT、并使用SLM限制向托管LUN的节点及其HA配对节点公布的路径。虽然存在其他路径、但默认情况下不会公布这些路径。可以使用 SLM 中的添加和删除报告节点参数修改公布的路径。请注意、在8.3之前的版本中创建的LUN会公布所有路径、需要进行修改、以便仅向托管HA对公布路径。有关SLM的详细信息、请查看的第5.9节 "[TR-4080](#)"。也可以使用先前的端口集方法进一步减少 LUN 的可用路径。端口集有助于减少 igroup 中启动程序可通过的可见路径数。

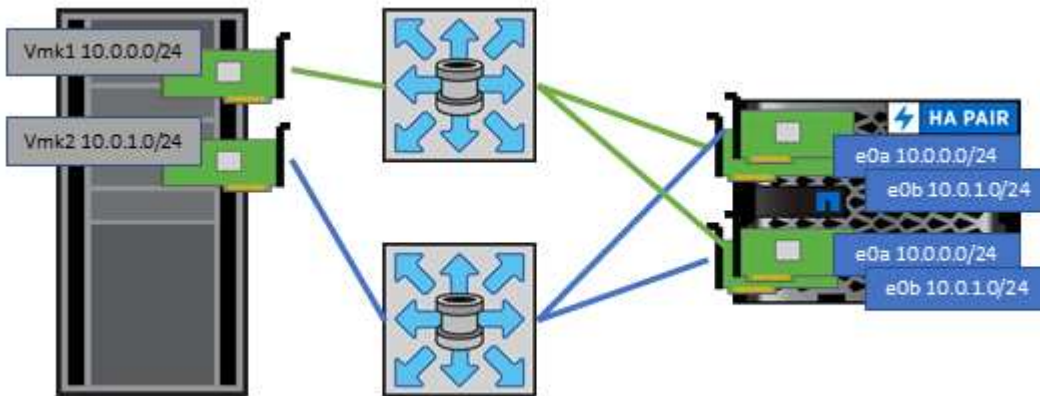
- 默认情况下、SLM 处于启用状态。除非使用端口集、否则不需要进行其他配置。
- 对于在Data ONTAP 8.3之前创建的LUN、请运行命令手动应用SLM `lun mapping remove-reporting-nodes`、以删除LUN报告节点并限制LUN访问权限、使其只能访问拥有LUN的节点及其HA配对节点。

基于SCSI的块协议(iSCSI、FC和FCoE)使用LUN ID、序列号以及唯一名称来访问LUN。FC和FCoE使用全球通用名称(WWNN和WWPN)、而iSCSI则使用iSCSI限定名称(iSCSI限定名称、IQN)根据按端口集和SLM筛选的LUN到igroup的映射来建立路径。基于NVMe的块协议可通过将具有自动生成的命名空间ID的命名空间分配给NVMe子系统并将该子系统映射到主机的NVMe限定名称(NQN)来进行管理。无论FC或TCP如何、NVMe命名空间都使用NQN而不是WWPN或WWNN进行映射。然后、主机将为映射的子系统创建一个软件定义的控制

以访问其命名存储。ONTAP中LUN和名称区的路径对于块协议没有意义、不会显示在协议中的任何位置。因此，只包含 LUN 的卷根本无需在内部挂载，而包含数据存储库中使用的 LUN 的卷则不需要接合路径。

要考虑的其他最佳实践：

- 检查["建议的 ESXi 主机和其他 ONTAP 设置"](#)NetApp与VMware合作建议的设置。
- 确保为 ONTAP 集群中每个节点上的每个 SVM 创建一个逻辑接口（LIF），以最大程度地提高可用性和移动性。ONTAP SAN 最佳实践是，每个节点使用两个物理端口和 LIF，每个网络结构使用一个。ALUA 用于解析路径并识别活动优化（直接）路径与活动非优化路径。ALUA 用于 FC，FCoE 和 iSCSI。
- 对于 iSCSI 网络，如果存在多个虚拟交换机，请在采用 NIC 绑定的不同网络子网上使用多个 VMkernel 网络接口。您还可以使用连接到多个物理交换机的多个物理 NIC 来提供 HA 并提高吞吐量。下图提供了多路径连接的示例。在 ONTAP 中，使用连接到两个或更多交换机的两个或更多链路配置一个单模式接口组以进行故障转移，或者使用 LACP 或其他具有多模式接口组的链路聚合技术来提供 HA 和链路聚合的优势。
- 如果在ESXi中使用质询握手身份验证协议(Challenge-Handshake Authentication Protocol、CHAP)进行目标身份验证、则还必须在ONTAP中使用命令行界面配置此协议 (`vserver iscsi security create`)或使用System Manager (在"Storage">"SVM">"SVM Settings"(SVM设置)>"Protocols"(协议)>"iSCSI"下编辑"Initiator Security"(启动程序安全性)。
- 使用适用于 VMware vSphere 的 ONTAP 工具创建和管理 LUN 和 igroup。此插件会自动确定服务器的 WWPN 并创建适当的 igroup。它还会根据最佳实践配置 LUN 并将其映射到正确的 igroup。
- 请谨慎使用VMM、因为它们更难管理、而且它们还会使用路径、如前文所述、这些路径会受到限制。ONTAP LUN 支持这两者 ["物理和虚拟兼容模式"](#) RDM。
- 有关将 NVMe/FC 与 vSphere 7.0 结合使用的详细信息，请参见此部分 ["《ONTAP NVMe/FC 主机配置指南》"](#) 和 ["TR-4684."](#)下图显示了从 vSphere 主机到 ONTAP LUN 的多路径连接。



NFS

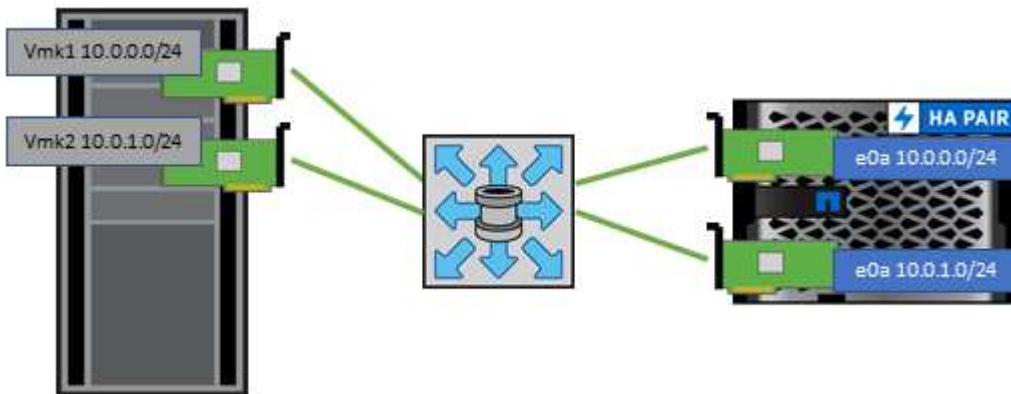
ONTAP是企业级横向扩展NAS阵列、其中包括许多功能。ONTAP支持VMware vSphere从许多ESXi主机并发访问NFS连接的数据存储库、远远超出了对VMFS文件系统施加的限制。将NFS与vSphere结合使用可提供一些易用性和存储效率可见性优势、如一节中所述["数据存储库"](#)。

将 ONTAP NFS 与 vSphere 结合使用时，建议采用以下最佳实践：

- 使用适用于 VMware vSphere 的 ONTAP 工具（最重要的最佳实践）：
 - 使用适用于VMware vSphere的ONTAP工具配置数据存储库、因为它可以简化导出策略的自动管理。

- 使用此插件为VMware集群创建数据存储库时、请选择集群、而不是单个ESX服务器。选择此选项会将数据存储库自动挂载到集群中的所有主机。
 - 使用插件挂载功能将现有数据存储库应用于新服务器。
 - 如果不对 VMware vSphere 使用 ONTAP 工具，请对所有服务器或需要额外访问控制的每个服务器集群使用一个导出策略。
 - 为 ONTAP 集群中每个节点上的每个 SVM 使用一个逻辑接口（LIF）。不再需要以往为每个数据存储库建议的 LIF。虽然直接访问(LIF和同一节点上的数据存储库)是最佳选择、但无需担心间接访问、因为对性能的影响通常很小(微秒)。
 - 如果使用fpolicy、请务必排除.lck文件、因为vSphere会使用这些文件在启动虚拟机时进行锁定。
 - 当前支持的所有VMware vSphere版本均可同时使用NFS v3和v4.1。vSphere 8.0 Update 2 (适用于NFS v3)和Update 3 (适用于NFS v4.1)新增了对nconnect的官方支持。对于NFS v4.1、vSphere仍支持会话中继、Kerberos身份验证和具有完整性的Kerberos身份验证。请务必注意、会话中继需要ONTAP 9.14.1或更高版本。有关nconnect功能及其如何提高性能的详细信息，请访问["NetApp和VMware的NFSv3 nconnect功能"](#)。
- 在vSphere 8中、nconnect的最大值为4、默认值为1。可以通过高级设置按主机提高vSphere中的最大值限制、但通常不需要。
 - 对于需要比单个TCP连接所能提供的性能更高的环境、建议将值设置为4。
 - 请注意、ESXi的NFS连接数限制为256个、每个nconnect连接数均计入此总数。例如、两个nconnect = 4的数据存储库总共会计入八个连接。
 - 在生产环境中实施大规模更改之前、必须测试nconnect对环境的性能影响。
- 值得注意的是、NFSv3和NFSv4.1使用不同的锁定机制。NFSv3使用客户端锁定、而NFSv4.1使用服务器端锁定。虽然ONTAP卷可以通过这两种协议导出、但ESXi只能通过一种协议挂载数据存储库。但是、这并不意味着其他ESXi主机不能通过其他版本挂载同一数据存储库。为了避免出现任何问题、请务必指定挂载时使用的协议版本、以确保所有主机使用相同版本、从而使用相同的锁定模式。请务必避免在主机之间混用NFS版本。如果可能、请使用主机配置文件检查合规性。
 - 由于 NFSv3 和 NFSv4.1 之间不会自动转换数据存储库，因此请创建一个新的 NFSv4.1 数据存储库，并使用 Storage vMotion 将 VM 迁移到新数据存储库。
 - 有关支持所需的特定ESXi修补程序级别、请参见中的NFS v4.1互操作性表说明["NetApp 互操作性表工具"](#)。
 - 如中所述["设置"](#)，如果您不使用适用于Kubernetes的vSphere CSI，则应将newSyncInterval设置为 ["VMware 知识库 386364"](#)
 - NFS导出策略规则用于控制vSphere主机的访问。您可以对多个卷（数据存储库）使用一个策略。对于NFS、ESXi会使用sys (UNIX)安全模式、并需要根挂载选项来执行VM。在 ONTAP 中，此选项称为超级用户，使用超级用户选项时，无需指定匿名用户 ID。请注意、对于和`-allow-suid`使用不同值的导出策略规则`-anon`可能会导致ONTAP工具出现SVM发现问题。IP地址应是一个逗号分隔列表、挂载数据存储库的vmkernel端口地址不含空格。下面是一个策略规则示例：
 - 访问协议：NFS (包括nfs3和nfs4)
 - 客户端匹配主机名、IP地址、网络组或域列表：192.168.42.21、192.168.42.22
 - RO访问规则：任意
 - RW Access Rule：any (RW访问规则：任意)
 - 匿名用户映射到的用户ID：6554

- 超级用户安全类型：any
- 在SETATTR中使用set_id位：true
- 允许创建设备：true
- 如果使用适用于VMware VAAI的NetApp NFS插件、则在创建或修改导出策略规则时、应将该协议设置为nfs。要使VAAI副本卸载正常工作、需要使用NFSv4协议、而将协议指定为`nfs`会自动包括NFS3和NFSv4版本。即使数据存储库类型创建为NFS v3、也需要执行此操作。
- NFS 数据存储库卷是从 SVM 的根卷接合的；因此，ESXi 也必须有权访问根卷，才能导航和挂载数据存储库卷。根卷以及嵌套了数据存储库卷接合的任何其他卷的导出策略必须包含一条或多条适用于ESXi服务器的规则、以便为其授予只读访问权限。下面是根卷的示例策略、该策略也使用VAAI插件：
 - 访问协议：NFS
 - 客户端匹配规范：192.168.42.21、192.168.42.22
 - RO 访问规则：sys
 - RW访问规则：从不(根卷的最佳安全性)
 - 匿名UID
 - 超级用户：sys (使用VAAI的根卷也需要此功能)
- 虽然 ONTAP 提供了一个灵活的卷命名空间结构，可以使用接合在树中排列卷，但这种方法对于 vSphere 来说毫无价值。无论存储的命名空间层次结构如何，它都会在数据存储库的根目录下为每个 VM 创建一个目录。因此，最佳实践是，只需将 vSphere 卷的接合路径挂载到 SVM 的根卷，即适用于 VMware vSphere 的 ONTAP 工具如何配置数据存储库。如果没有嵌套的接合路径，也意味着任何卷都不依赖于根卷以外的任何卷，即使有意使某个卷脱机或销毁该卷，也不会影响指向其他卷的路径。
- 对于 NFS 数据存储库上的 NTFS 分区，块大小为 4k 是可以的。下图显示了从 vSphere 主机到 ONTAP NFS 数据存储库的连接。



下表列出了 NFS 版本和支持的功能。

vSphere 功能	NFSv3	NFSv4.1
VMotion 和 Storage vMotion	是的。	是的。
高可用性	是的。	是的。
容错	是的。	是的。
DRS	是的。	是的。

vSphere 功能	NFSv3	NFSv4.1
主机配置文件	是的。	是的。
存储 DRS	是的。	否
存储 I/O 控制	是的。	否
SRM	是的。	否
虚拟卷	是的。	否
硬件加速 (VAAI)	是的。	是的。
Kerberos 身份验证	否	是 (在 vSphere 6.5 及更高版本中进行了增强, 可支持 AES , krb5i)
多路径支持	否	是(ONTAP 9.14.1)

FlexGroup 卷

将ONTAP和FlexGroup卷与VMware vSphere结合使用、可实现简单且可扩展的数据存储库、从而充分利用整个ONTAP集群的全部功能。

ONTAP 9.8以及适用于VMware vSphere的ONTAP工具9.8-9.13和适用于VMware 4.4及更高版本的SnapCenter 插件增加了对vSphere中FlexGroup卷支持的数据存储库的支持。FlexGroup卷可以简化大型数据存储库的创建过程、并自动在ONTAP集群中创建必要的分布式成分卷、以最大程度地提高ONTAP系统的性能。

如果您需要一个具有完整ONTAP集群功能的可扩展vSphere数据存储库、或者如果您的克隆工作负载非常大、可以通过持续保持克隆缓存预热来从FlexGroup克隆机制中受益、请将FlexGroup卷与vSphere结合使用。

副本卸载

除了对vSphere工作负载进行广泛的系统测试之外、ONTAP 9.8还为FlexGroup数据存储库添加了一种新的副本卸载机制。这一新系统使用经过改进的复制引擎在后台成分卷之间复制文件、同时允许访问源和目标。然后、可以使用此成分卷本地缓存根据需要快速例化VM克隆。

要启用FlexGroup优化的副本卸载、请参见 ["如何配置ONTAP FlexGroup卷以允许VAAI副本卸载"](#)

您可能会发现、如果您使用VAAI克隆、但克隆量不足以保持缓存热度、则克隆速度可能不会比基于主机的副本快。如果是这种情况、您可以调整缓存超时以更好地满足您的需求。

请考虑以下情形：

- 您已创建一个包含8个成分卷的新FlexGroup
- 新FlexGroup的缓存超时设置为160分钟

在这种情况下、要完成的前8个克隆将是完整副本、而不是本地文件克隆。在160秒超时时间到期之前对该VM执行任何其他克隆操作都将使用每个成分卷中的文件克隆引擎以循环方式创建几乎即时的副本、这些副本均匀分布在各个成分卷上。

卷收到的每个新克隆作业都会重置超时。如果示例FlexGroup中的成分卷在超时之前未收到克隆请求、则会清除该特定虚拟机的缓存、并且需要重新填充该卷。此外、如果原始克隆的源发生更改(例如、您已更新模板)、则每个成分卷上的本地缓存都将失效、以防止发生任何冲突。如前文所述、缓存可进行调整、并可根据环境需求进行

设置。

有关将FlexGroup卷与VAAI结合使用的详细信息、请参阅此知识库文章：["VAAI：如何对FlexGroup卷使用缓存？"](#)

如果您无法充分利用FlexGroup缓存、但仍需要快速跨卷克隆、请考虑使用虚拟卷。与使用传统数据存储库相比、使用FlexVol进行跨卷克隆的速度要快得多、并且不依赖于缓存。

QoS设置

支持使用ONTAP系统管理器或集群Shell在FlexGroup级别配置QoS、但它不提供VM感知或vCenter集成。

此时、可以在vCenter UI中或使用ONTAP工具通过REST API在数据存储库中的单个虚拟机或所有虚拟机上设置QoS (最大/最小IOPS)。在所有 VM 上设置 QoS 将取代任何单独的每 VM 设置。将来，设置不会扩展到新的或迁移的虚拟机；可以在新虚拟机上设置 QoS ，也可以将 QoS 重新应用于数据存储库中的所有虚拟机。

请注意、VMware vSphere会将NFS数据存储库的所有IO视为每个主机的一个队列、而一个VM上的QoS限制可能会影响该主机的同一数据存储库中其他VM的性能。这与Vvol不同、Vvol可以在迁移到另一个数据存储库时保持其QoS策略设置、并且在受到控制时不会影响其他VM的IO。

指标

ONTAP 9.8还为FlexGroup文件添加了新的基于文件的性能指标(IOPS、吞吐量和延迟)、您可以在适用于VMware vSphere的ONTAP工具信息板和VM报告中查看这些指标。适用于 VMware vSphere 的 ONTAP 工具插件还允许您结合使用最大和 / 或最小 IOPS 来设置服务质量 (QoS) 规则。可以在数据存储库中的所有 VM 之间设置这些值，也可以为特定 VM 单独设置这些值。

最佳实践

- 使用ONTAP工具创建FlexGroup数据存储库、以确保以最佳方式创建FlexGroup、并根据您的vSphere环境配置导出策略。但是、在使用ONTAP工具创建FlexGroup卷之后、您会发现vSphere集群中的所有节点都使用一个IP地址挂载数据存储库。这可能会导致网络端口出现瓶颈。要避免此问题、请卸载此数据存储库、然后使用标准vSphere数据存储库向导使用轮叫DNS名称重新挂载它、以便在SVM上的各个SVM之间平衡负载。重新挂载后、ONTAP工具将再次能够管理数据存储库。如果ONTAP工具不可用、请使用FlexGroup默认值并按照中的准则创建导出策略 ["数据存储库和协议—NFS"](#)。
- 在估算 FlexGroup 数据存储库的规模时，请记住， FlexGroup 由多个较小的 FlexVol 卷组成，这些卷会创建一个较大的命名空间。因此、请将数据存储库的大小至少设置为最大VMDK文件大小的8倍(假设默认为8个成分卷)、外加10-20%的未使用余量、以便灵活地重新平衡。例如、如果您的环境中有6 TB VMDK、请将FlexGroup数据存储库的大小设置为不小于52.8 TB (6x8 + 10%)。
- 从ONTAP 9.14.1开始、VMware和NetApp支持NFSv4.1会话中继。有关特定版本的详细信息、请参见NetApp NFS 4.1互操作性表工具(IMT)说明。从vSphere 8.0U2开始、NFSv3不支持卷的多个物理路径、但支持nconnect。有关nconnect的详细信息，请参见["NetApp和VMware的NFSv3 nConnect功能"](#)。
- 使用适用于 VMware VAAI 的 NFS 插件执行副本卸载。请注意、如前文所述、虽然FlexGroup数据存储库中的克隆功能得到了增强、但在FlexVol和/或FlexGroup卷之间复制VM时、ONTAP与ESXi主机副本相比、不会提供显著的性能优势。因此、在决定使用VAAI或FlexGroup卷时、请考虑克隆工作负载。修改成分卷数量是针对基于FlexGroup的克隆进行优化的一种方法。正如调整前面提到的缓存超时。
- 使用适用于VMware vSphere的ONTAP工具9.8-9.13通过ONTAP指标(信息板和VM报告)监控FlexGroup VM 的性能、并管理各个VM上的QoS。目前无法通过 ONTAP 命令或 API 获得这些指标。
- 适用于VMware vSphere的SnapCenter插件4.4及更高版本支持备份和恢复主存储系统上FlexGroup数据存储库中的VM。4.6号选择控制阀为基于FlexGroup的数据存储库增加了SnapMirror支持。使用基于阵列的快照和复制是保护数据的最有效方式。

网络配置：

在运行ONTAP的系统上使用vSphere时、配置网络设置非常简单、与其他网络配置类似。

需要考虑以下几点：

- 将存储网络流量与其他网络分开。可以通过使用专用 VLAN 或单独的存储交换机来实现单独的网络。如果存储网络共享上行链路等物理路径，您可能需要 QoS 或其他上行链路端口来确保带宽充足。除非您的解决方案指南明确要求、否则请勿将主机直接连接到存储；使用交换机提供冗余路径、并允许VMware HA在没有干预的情况下运行。
- 如果您的网络支持巨型帧、则应使用巨型帧。如果使用这些协议，请确保在存储和 ESXi 主机之间的路径中的所有网络设备，VLAN 等上对其进行相同的配置。否则，您可能会看到性能或连接问题。此外，还必须在 ESXi 虚拟交换机，VMkernel 端口以及每个 ONTAP 节点的物理端口或接口组上以相同的方式设置 MTU 。
- NetApp仅建议在ONTAP集群中的集群互连端口上禁用网络流量控制。对于用于数据流量的其余网络端口的流量控制最佳实践、NetApp不提供任何其他建议。您应根据需要启用或禁用它。有关流量控制的更多背景信息、请参见 "TR-4182"。
- 当 ESXi 和 ONTAP 存储阵列连接到以太网存储网络时，NetApp 建议将这些系统连接到的以太网端口配置为快速生成树协议（RSTP）边缘端口或使用 Cisco PortFast 功能。NetApp 建议在使用 Cisco PortFast 功能且为 ESXi 服务器或 ONTAP 存储阵列启用了 802.1Q VLAN 中继的环境中启用生成树 PortFast 中继功能。
- NetApp 建议采用以下链路聚合最佳实践：
 - 使用支持在两个独立交换机机箱上对端口进行链路聚合的交换机、并采用多机箱链路聚合组方法、例如Cisco的虚拟端口通道(vPC)。
 - 对连接到ESXi的交换机端口禁用LACP、除非您使用的是配置了LACP的dvSwitches 5.1或更高版本。
 - 使用LACP为具有IP哈希的动态多模式接口组的ONTAP 存储系统创建链路聚合。
 - 在ESXi上使用IP哈希绑定策略。

下表汇总了网络配置项，并指出了这些设置的应用位置。

项目	ESXi	交换机	Node	SVM
IP 地址	VMkernel	否	否	是的。
链路聚合	虚拟交换机	是的。	是的。	否 *
VLAN	VMkernel 和 VM 端口组	是的。	是的。	否 *
流量控制	NIC	是的。	是的。	否 *
生成树	否	是的。	否	否
MTU（适用于巨型帧）	虚拟交换机和 VMkernel 端口（9000）	是（设置为最大值）	是（9000）	否 *
故障转移组	否	否	是（创建）	是（选择）

- SVM LIF连接到具有VLAN、MTU和其他设置的端口、接口组或VLAN接口。但是、这些设置不会在SVM级别进行管理。

这些设备具有自己的 IP 地址进行管理，但这些地址不会在 ESXi 存储网络环境中使用。

SAN (FC、NVMe/FC、iSCSI、NVMe/TCP)、RDM

ONTAP使用传统iSCSI和光纤通道协议(Fibre Channel Protocol、FCP)以及高效率和高性能的下一代块协议基于网络结构的NVMe (NVMe-oF)为VMware vSphere提供企业级块存储、并支持NVMe/FC和NVMe/TCP。

有关在vSphere和ONTAP中为VM存储实施块协议的详细最佳实践、请参见["数据存储库和协议—SAN"](#)

NFS

通过 vSphere ， 客户可以使用企业级 NFS 阵列作为 ESXi 集群中的所有节点提供对数据存储库的并发访问。如一节所述["数据存储库"](#)、在vSphere中使用NFS具有一些易用性和存储效率可见性优势。

有关建议的最佳实践、请参见["数据存储库和协议—NFS"](#)

直连网络

存储管理员有时倾向于通过从配置中删除网络交换机来简化其基础架构。在某些情况下、可以支持此功能。但是、需要注意一些限制和注意事项。

iSCSI和NVMe/TCP

使用iSCSI或NVMe/TCP的主机可以直接连接到存储系统并正常运行。原因是路径问题。直接连接到两个不同的存储控制器会导致数据流有两条独立的路径。丢失路径、端口或控制器不会阻止使用另一个路径。

NFS

可以使用直连NFS存储、但有一个重大限制—如果没有大量的脚本编写工作、故障转移将无法正常工作、这是客户的责任。

直连NFS存储的无中断故障转移之所以复杂、是因为本地操作系统上会发生路由。例如、假设主机的IP地址为192.168.1.1/24、并且直接连接到IP地址为192.168.1.50/24的ONTAP控制器。在故障转移期间、该192.168.1.50地址可以故障转移到另一个控制器、并且该地址可供主机使用、但主机如何检测到它的存在？原来的192.168.1.1地址仍然位于不再连接到操作系统的主机NIC上。发往192.168.1.50的流量将继续发送到无法运行的网络端口。

第二个操作系统NIC可配置为192.168.1.2、并且能够与故障转移的192.168.1.50地址通信、但本地路由表默认使用一个*且仅一个*地址与192.168.1.0/24子网通信。sysadmin可以创建一个脚本框架、用于检测失败的网络连接并更改本地路由表或启动和关闭接口。确切的操作步骤取决于所使用的操作系统。

在实践中、NetApp客户确实使用直连NFS、但通常仅适用于故障转移期间IO暂停的工作负载。使用硬挂载时、暂停期间不应出现任何IO错误。IO应冻结、直到服务还原为止、方法是通过故障恢复或手动干预在主机上的NIC之间移动IP地址。

FC直连

不能使用FC协议将主机直接连接到ONTAP存储系统。原因是使用了NPIV。用于向FC网络标识ONTAP FC端口的WWN使用一种称为NPIV的虚拟化类型。连接到ONTAP系统的任何设备都必须能够识别NPIV WWN。目前没有HBA供应商提供可安装在能够支持NPIV目标的主机中的HBA。

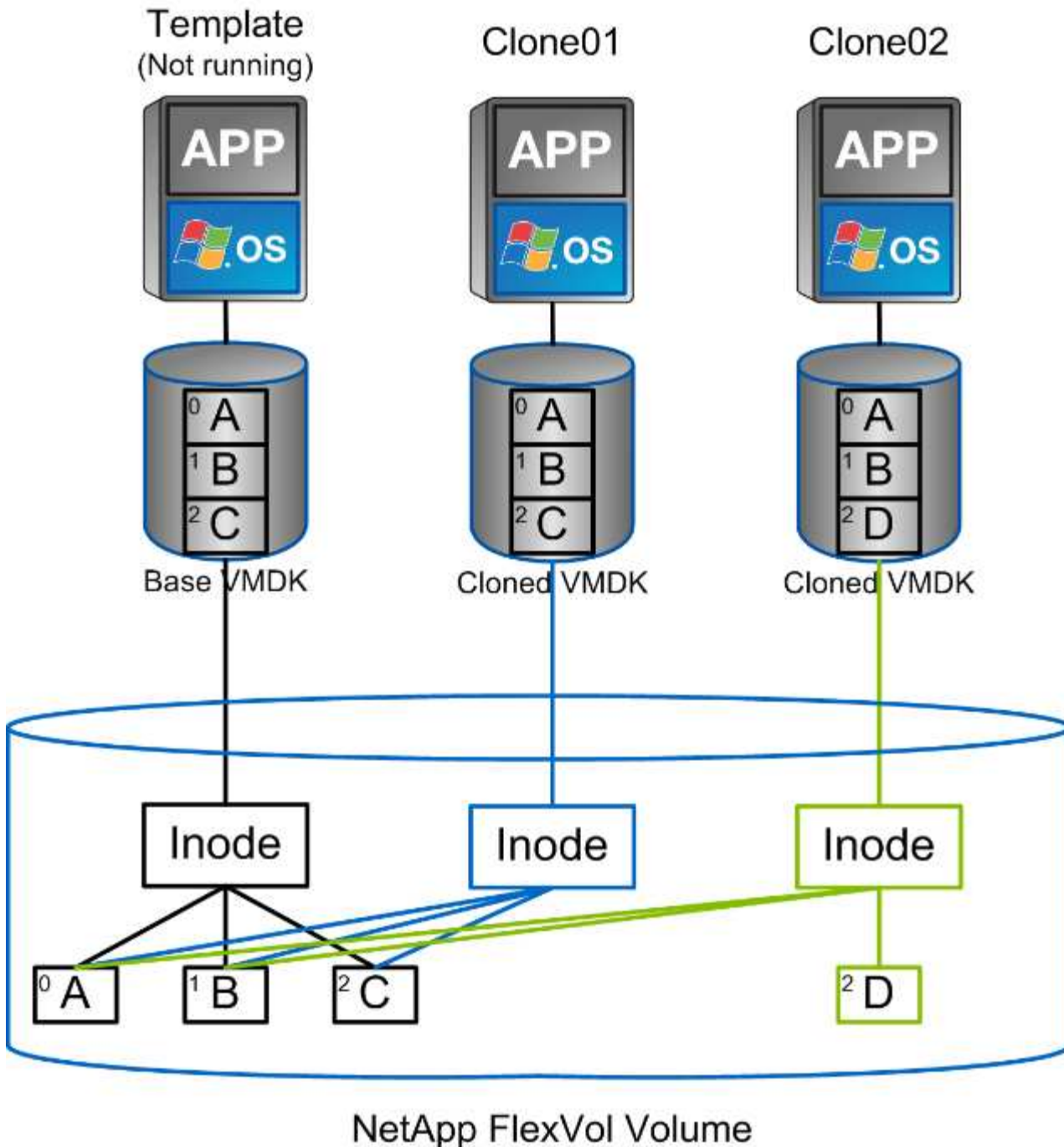
虚拟机和数据存储库克隆

通过克隆存储对象，您可以快速创建副本以供将来使用，例如配置其他 VM ， 备份 / 恢复操作等。

在 vSphere 中，您可以克隆虚拟机，虚拟磁盘， VVol 或数据存储库。克隆后，通常可以通过自动化过程进一步自定义对象。vSphere 既支持完整副本克隆，也支持链接克隆，在这些克隆中，它可以独立于原始对象跟踪更改。

链接克隆非常有助于节省空间，但它们会增加 vSphere 为虚拟机处理的 I/O 量，从而影响该虚拟机的性能，甚至整个主机的性能。因此、NetApp 客户经常使用基于存储系统的克隆来充分利用这两种环境：高效利用存储和提高性能。

下图显示了 ONTAP 克隆。



克隆可以通过多种机制卸载到运行ONTAP的系统、通常是在虚拟机、VVOL或 数据存储库级别。其中包括：

- 使用 NetApp vSphere APIs for Storage Awareness (VASA) Provider 的 VVOL 。 ONTAP克隆用于支持由vCenter管理的VVOL快照、这些快照可节省空间、并且创建和删除这些快照时的I/O影响极小。此外，还可以使用 vCenter 克隆 VM ，这些 VM 也会卸载到 ONTAP ，无论是在单个数据存储库 / 卷中还是在数据存储库 / 卷之间。
- 使用 vSphere API 阵列集成 (VAAI) 进行 vSphere 克隆和迁移。在SAN和NAS环境中、可以将VM克隆操作卸载到ONTAP (NetApp提供了一个ESXi插件来为NFS启用VAAI)。vSphere仅会卸载NAS数据存储库中冷(已关闭) VM上的操作、而热VM上的操作(克隆和Storage vMotion)也会卸载到SAN上。ONTAP根据源和目标使用最高效的方法。此功能也可供使用 "Omnissa地平线景观"。
- SRA (与VMware Live Site Recon/Site Recovery Manager结合使用)。此处，克隆用于无中断测试灾难恢复副本的恢复情况。

- 使用 SnapCenter 等 NetApp 工具进行备份和恢复。VM克隆用于验证备份操作以及挂载VM备份、以便可以还原各个文件。

VMware，NetApp 和第三方工具可以调用 ONTAP 卸载克隆。卸载到 ONTAP 的克隆具有多个优势。在大多数情况下，它们节省空间，只需要存储即可更改对象；读取和写入它们不会产生额外的性能影响，在某些情况下，通过在高速缓存中共享块来提高性能。它们还会从 ESXi 服务器卸载 CPU 周期和网络 I/O。使用 FlexVol volume 的传统数据存储库中的副本卸载在获得 FlexClone 许可(包含在 ONTAP One 许可证中)的情况下可以快速而高效、但 FlexVol 卷之间的副本速度可能会较慢。如果您将 VM 模板维护为克隆源，请考虑将其放置在数据存储库卷中（使用文件夹或内容库对其进行组织），以实现节省空间的快速克隆。

您也可以直接在 ONTAP 中克隆卷或 LUN 以克隆数据存储库。使用 NFS 数据存储库时，FlexClone 技术可以克隆整个卷，并且可以从 ONTAP 导出克隆并由 ESXi 作为另一个数据存储库挂载该克隆。对于 VMFS 数据存储库，ONTAP 可以克隆卷或整个卷中的 LUN，包括其中的一个或多个 LUN。包含 VMFS 的 LUN 必须映射到 ESXi 启动程序组（igroup），然后由 ESXi 重新签名，才能挂载并用作常规数据存储库。对于某些临时使用情形，可以挂载克隆的 VMFS 而无需重新签名。克隆数据存储库后，可以注册，重新配置和自定义数据存储库中的 VM，就像它们是单独克隆的 VM 一样。

在某些情况下，可以使用其他许可功能来增强克隆功能，例如用于备份的 SnapRestore 或 FlexClone。这些许可证通常包含在许可证包中，无需额外付费。要执行 vVol 克隆操作以及支持 vVol 的受管快照(从虚拟机管理程序卸载到 ONTAP)、需要 FlexClone 许可证。在数据存储库 / 卷中使用 FlexClone 许可证还可以改进某些基于 VAAI 的克隆（创建节省空间的即时副本，而不是块副本）。此外，SRA 还会使用它来测试灾难恢复副本的恢复，并使用 SnapCenter 来执行克隆操作，以及浏览备份副本以还原单个文件。

数据保护

备份和快速恢复虚拟机(VM)是使用适用于 vSphere 的 ONTAP 的主要优势。可以通过适用于 VMware vSphere 的 SnapCenter 插件在 vCenter 中轻松管理此功能。许多客户通过 SnapCenter 增强了第三方备份解决方案、以利用 ONTAP 的快照技术、因为它提供了使用 ONTAP 恢复 VM 的最快、最直接的方式。拥有 ONTAP One 许可证的客户可以免费获得 SnapCenter、也可以获得其他许可证包。

此外，适用于 VMware 的 SnapCenter 插件可以与 ["NetApp Backup and Recovery"](#)，为大多数 ONTAP 系统提供有效的 3-2-1 备份解决方案。请注意，如果使用具有高级服务的虚拟机备份和恢复，可能会收取一些费用，例如用于额外备份存储的对象存储。本节概述了可用于保护虚拟机和数据存储的各种选项。

NetApp ONTAP 卷快照

使用快照快速创建虚拟机或数据存储库的副本而不影响性能、然后使用 SnapMirror 将其发送到二级系统、以实现长期异地数据保护。这种方法只存储更改后的信息，从而最大限度地减少存储空间和网络带宽。

快照是 ONTAP 的一项重要功能、可用于创建数据的时间点副本。它们节省空间、并且可以快速创建、因此非常适合保护虚拟机和数据存储库。快照可用于各种用途、包括备份、恢复和测试。这些快照与 VMware (一致性)快照不同、适用于长期保护。由于性能和其他影响、建议仅在短期内使用 VMware vCenter 管理的快照。"[Snapshot 限制](#)"有关详细信息、请参见。

快照是在卷级别创建的、可用于保护该卷中的所有虚拟机和数据存储库。这意味着、您可以创建整个数据存储库的快照、其中包括该数据存储库中的所有虚拟机。

对于 NFS 数据存储库、您可以通过浏览 Snapshot 目录轻松查看快照中的 VM 文件。这样、您就可以快速从快照访问和还原文件、而无需使用特定的备份解决方案。

对于 VMFS 数据存储库、您可以根据所需的快照创建数据存储库的 FlexClone。这样、您就可以根据快照创建新

的数据存储库、此数据存储库可用于测试或开发目的。FlexClone仅会为创建快照后所做的更改占用空间、从而可以节省空间来创建数据存储库副本。创建FlexClone后、您可以像常规数据存储库一样、将LUN或命名空间映射到ESXi主机。这样、您不仅可以还原特定的VM文件、还可以根据生产数据快速创建测试或开发环境、而不会影响生产环境的性能。

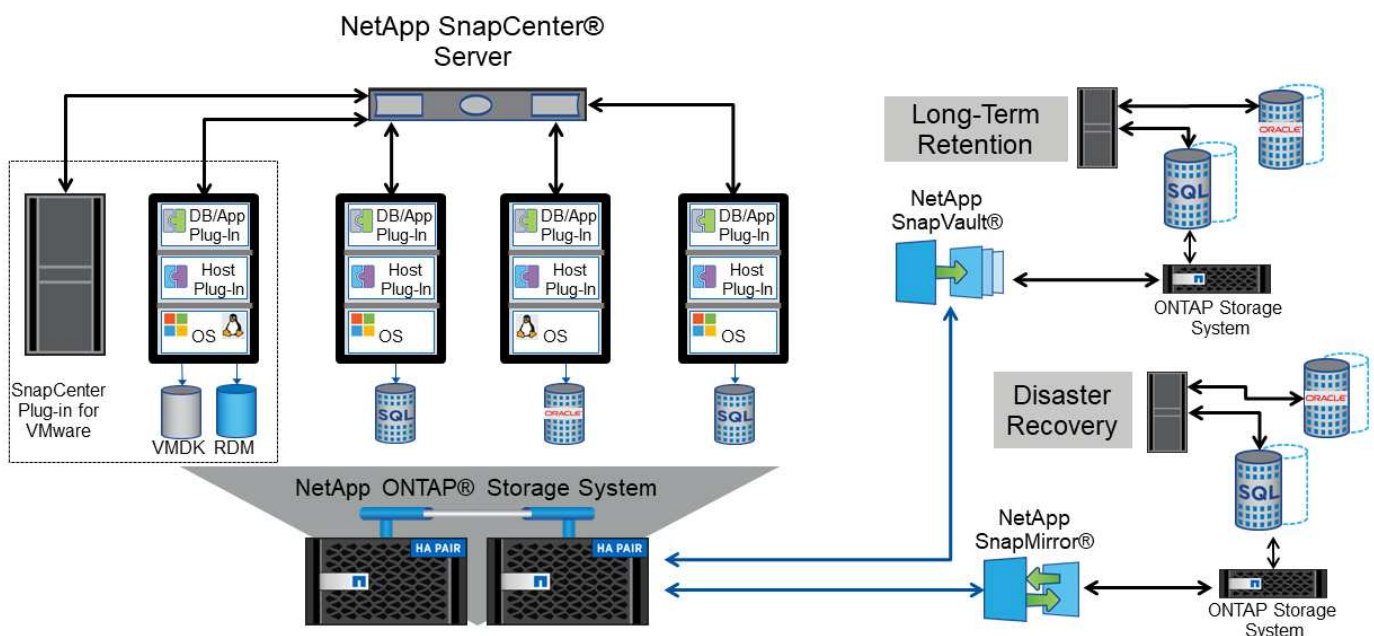
有关快照的更多信息，请参阅ONTAP文档。以下链接提供了更多详细信息：["ONTAP本地Snapshot副本"](#)
["ONTAP SnapMirror复制工作流程"](#)

适用于VMware vSphere的SnapCenter插件

使用 SnapCenter，您可以创建可应用于多个作业的备份策略。这些策略可以定义计划，保留，复制和其他功能。它们仍然允许选择虚拟机一致的快照、从而利用虚拟机管理程序在创建VMware快照之前将I/O置于静修状态的功能。但是，由于VMware快照对性能的影响，通常不建议使用这些快照，除非您需要暂停子文件系统。而是使用快照进行常规保护、并使用SnapCenter应用程序插件等应用程序工具来保护SQL Server或Oracle等事务处理数据。

这些插件提供了扩展功能，可在物理和虚拟环境中保护数据库。在vSphere中、您可以使用它们来保护SQL Server或Oracle数据库、其中数据存储存储在RDM LUN、Vvol或NVMe/TCP命名空间和直接连接到子操作系统的iSCSI LUN上、或者VMFS或NFS数据存储库上的VMDK文件上。这些插件允许指定不同类型的数据库备份、支持联机或脱机备份、并保护数据库文件和日志文件。除了备份和恢复之外、这些插件还支持出于开发或测试目的的克隆数据库。

下图显示了 SnapCenter 部署的一个示例。



有关规模估算信息，请参见 ["适用于VMware vSphere的SnapCenter插件规模估算指南"](#)

适用于采用VMware Live Site Recovery的VMware vSphere的ONTAP工具

适用于VMware vSphere的ONTAP工具(OT4VS)是一款免费插件、可在VMware vSphere和NetApp ONTAP之间实现无缝集成。您可以通过它直接从vSphere Web Client管理ONTAP存储、从而更轻松地执行配置存储、管理复制和监控性能等任务。

要改进灾难恢复功能、请考虑使用适用于VMware vSphere的ONTAP工具中的适用于ONTAP的NetApp SRA以

及VMware Live Site Recovery (以前称为Site Recovery Manager)。此工具不仅支持使用SnapMirror将数据存储库复制到灾难恢复站点、还支持通过克隆复制的数据存储库在灾难恢复环境中进行无中断测试。此外、借助内置的自动化功能、还可以简化从灾难中恢复以及在解决中断后重新保护生产环境的过程。

NetApp Disaster Recovery

灾难恢复 (DR) 是一种基于云的服务，可在发生灾难时提供保护您的数据和应用程序的全面解决方案。它提供了一系列功能，包括自动故障转移和故障恢复、多个时间点恢复点、应用程序一致的灾难恢复以及对本地和基于云的ONTAP系统的支持。NetApp Disaster Recovery旨在与ONTAP和您的 VMware vSphere 环境无缝协作，提供统一的灾难恢复解决方案。

NetApp MetroCluster和SnapMirror处于活动同步状态的vSphere Metro Storage Cluster (VMSC)

最后、要获得最高级别的数据保护、请考虑使用NetApp MetroCluster的VMware vSphere Metro Storage Cluster (VMSC)配置。VMSC是一款经VMware认证且受NetApp支持的解决方案、它使用同步复制、可提供与高可用性集群相同的优势、但分布在不同的站点上以防止站点灾难。NetApp SnapMirror Active Sync (采用ASA和AFF)以及MetroCluster (采用AFF)为同步复制提供了经济高效的配置，可从任何单个存储组件故障中透明恢复，并可在SnapMirror活动同步时透明恢复，或在发生站点灾难时使用MetroCluster进行单命令恢复。中详细介绍了VMSC。"[TR-4128](#)"

服务质量 (QoS)

在控制服务级别、管理未知工作负载或在部署之前测试应用程序以确保它们不会影响生产环境中的其他工作负载时、吞吐量限制非常有用。它们还可用于在确定抢占资源的工作负载后对其进行限制。

ONTAP QoS策略支持

运行ONTAP的系统可以使用存储服务质量(QoS)功能来限制不同存储对象(例如文件、LUN、卷或整个SVM)的吞吐量(以MBps和/或每秒I/O数(IOPS)为单位)。

此外，还支持基于 IOPS 的最低服务级别，以便为 ONTAP 9.2 中的 SAN 对象和 ONTAP 9.3 中的 NAS 对象提供稳定一致的性能。

可以使用 MBps 和 / 或 IOPS 设置对象的 QoS 最大吞吐量限制。如果同时使用这两者，则 ONTAP 会强制实施达到的第一个限制。一个工作负载可以包含多个对象，一个 QoS 策略可以应用于一个或多个工作负载。将一个策略应用于多个工作负载时，这些工作负载将共享此策略的总限制。不支持嵌套对象（例如，卷中的文件不能各自具有自己的策略）。QoS 最小值只能以 IOPS 为单位进行设置。

目前，以下工具可用于管理 ONTAP QoS 策略并将其应用于对象：

- ONTAP 命令行界面
- ONTAP 系统管理器
- OnCommand Workflow Automation
- Active IQ Unified Manager
- 适用于 ONTAP 的 NetApp PowerShell 工具包
- 适用于 VMware vSphere VASA Provider 的 ONTAP 工具

要为 LUN（包括 VMFS 和 RDM）分配 QoS 策略，可以从适用于 VMware vSphere 的 ONTAP 工具主页上的存储系统菜单获取 ONTAP SVM（显示为 Vserver），LUN 路径和序列号。选择存储系统(SVM)、然后选择相

关对象> SAN。使用 ONTAP 工具之一指定 QoS 时，请使用此方法。

请参见 ["性能监控和管理概述"](#) 有关详细信息 ...

非卷NFS数据存储库

ONTAP QoS策略可应用于整个数据存储库或其中的各个VMDK文件。但是、请务必了解、传统(非Vvol) NFS数据存储库上的所有VM都会共享给定主机的一个通用I/O队列。如果任何虚拟机受到ONTAP QoS策略的控制、则实际上会导致该主机上该数据存储库的所有I/O都受到控制。

- 示例： *
 - *对于主机ESXi -01作为传统NFS数据存储库挂载的卷、您需要在vm1.vmdk上配置QoS限制。
 - *同一主机(ESXi -01)正在使用vm2.vmdk、并且位于同一个卷上。
 - *如果vm1.vmdk受到节流、则vm2.vmdk也会显示为已节流、因为它与vm1.vmdk共享同一个IO队列。



这不适用于此类卷。

从vSphere 6.5开始、您可以利用具有存储I/O控制(SIIOC) v2的基于存储策略的管理(Storage Policy-Based Management、SPBM)来管理非Vvol数据存储库的文件粒度限制。

有关使用SIC和SPBM策略管理性能的详细信息、请参见以下链接。

["SPBM基于主机的规则：SIIOC v2"](#)
["使用vSphere管理存储I/O资源"](#)

要将 QoS 策略分配给 NFS 上的 VMDK ， 请注意以下准则：

- 必须将此策略应用于 `vmname-flat.vmdk` 包含实际虚拟磁盘映像、而不是 `vmname.vmdk` (虚拟磁盘描述符文件)或 `vmname.vmx` (VM描述符文件)。
- 不要将策略应用于其他虚拟机文件、例如虚拟交换文件 (`vmname.vswp`) 。
- 在使用vSphere Web Client查找文件路径("数据存储库">"文件")时、请注意、它会合并的信息 - `flat.vmdk` 和 `.vmdk` 只需显示一个名为的文件 `.vmdk` 但的大小 - `flat.vmdk`。添加 `-flat` 以获取正确的路径。

在使用适用于 VMware vSphere 9.8 及更高版本的 ONTAP 工具时， FlexGroup 数据存储库可提供增强的 QoS 功能。您可以轻松地在数据存储库中的所有 VM 或特定 VM 上设置 QoS 。有关详细信息，请参见本报告的 FlexGroup 一节。请注意、上述传统NFS数据存储库的QoS限制仍然适用。

VMFS数据存储库

使用ONTAP LUN、可以将QoS策略应用于包含LUN或单个LUN的FlexVol卷、但不能应用于单个VMDK文件、因为ONTAP无法识别VMFS文件系统。

数据存储库

使用基于存储策略的管理和Vvol、可以轻松地在各个VM或VMDK上设置最小和/或最大QoS、而不会影响任何其他VM或VMDK。

在为VVOV容器创建存储功能配置文件时、请在性能功能下指定一个最大和/或最小IOPS值、然后使用虚拟机的存储策略引用此SCP。在创建虚拟机时使用此策略或将此策略应用于现有虚拟机。



vvol需要使用适用于VMware vSphere的ONTAP工具、该工具可用作适用于ONTAP的VASA Provider。请参见["采用ONTAP的VMware vSphere虚拟卷\(Vvol\)"](#)、了解有关此类卷的最佳实践。

ONTAP QoS 和 VMware SIOC

ONTAP服务质量(QoS)和VMware vSphere存储I/O控制(SIO)是两项相辅相成的技术、vSphere和存储管理员可以结合使用这些技术来管理运行ONTAP的系统上托管的vSphere VM的性能。每个工具都有自己的优势，如下表所示。由于VMware vCenter 和 ONTAP 的作用域不同，因此某些对象可以由一个系统查看和管理，而不能由另一个系统查看和管理。

属性	ONTAP QoS	VMware SIOC
处于活动状态时	策略始终处于活动状态	存在争用时处于活动状态（数据存储库延迟超过阈值）
单位类型	IOPS ， MBps	IOPS ， 共享
vCenter 或应用程序范围	多个 vCenter 环境，其他虚拟机管理程序和应用程序	单个 vCenter 服务器
是否在虚拟机上设置 QoS ？	仅限 NFS 上的 VMDK	NFS 或 VMFS 上的 VMDK
是否为 LUN 设置 QoS （ RDM ） ？	是的。	否
是否为 LUN （ VMFS ） 设置 QoS ？	是的。	是(数据存储库可能会受到控制)
是否为卷 （ NFS 数据存储库） 设置 QoS ？	是的。	是(数据存储库可能会受到控制)
是否在 SVM （租户） 上设置 QoS ？	是的。	否
基于策略的方法？	是；可以由策略中的所有工作负载共享，也可以将其全部应用于策略中的每个工作负载。	是，在 vSphere 6.5 及更高版本中。
需要许可证	随 ONTAP 提供	Enterprise Plus

VMware Storage Distributed Resource Scheduler

VMware Storage Distributed Resource Scheduler （ SDRS ） 是一项 vSphere 功能，可根据当前 I/O 延迟和空间使用情况将 VM 放置在存储上。然后，它会在数据存储库集群（也称为 Pod ） 中的数据存储库之间无中断地移动虚拟机或 VMDK ， 从而选择最佳数据存储库，以便将虚拟机或 VMDK 放置在数据存储库集群中。数据存储库集群是一组相似的数据存储库、从vSphere管理员的角度来看、这些数据存储库会聚合到一个使用单元中。

在将SDRS与适用于VMware vSphere的ONTAP工具结合使用时、您必须先使用此插件创建数据存储库、使用vCenter创建数据存储库集群、然后再将此数据存储库添加到其中。创建数据存储库集群后，可以直接从详细信息页面上的配置向导将其他数据存储库添加到数据存储库集群中。

有关 SDRS 的其他 ONTAP 最佳实践包括：

- 集群中的所有数据存储库都应使用相同类型的存储（例如 SAS ， SATA 或 SSD ）， 可以是所有 VMFS 或 NFS 数据存储库，并且具有相同的复制和保护设置。
- 请考虑在默认（手动）模式下使用 SDRS 。通过此方法，您可以查看建议并决定是否应用这些建议。请注意 VMDK 迁移的以下影响：

- 在数据存储库之间移动 VMDK 时，通过 ONTAP 克隆或重复数据删除节省的任何空间都将丢失。您可以重新运行重复数据删除以重新获得这些节省。
- 在SDRS移动VMDK后、NetApp建议在源数据存储库中重新创建快照、因为空间会被移动的VM锁定。
- 在同一聚合上的数据存储库之间移动 VMDK 没有什么优势， SDRS 无法查看可能共享该聚合的其他工作负载。

基于存储策略的管理和虚拟卷

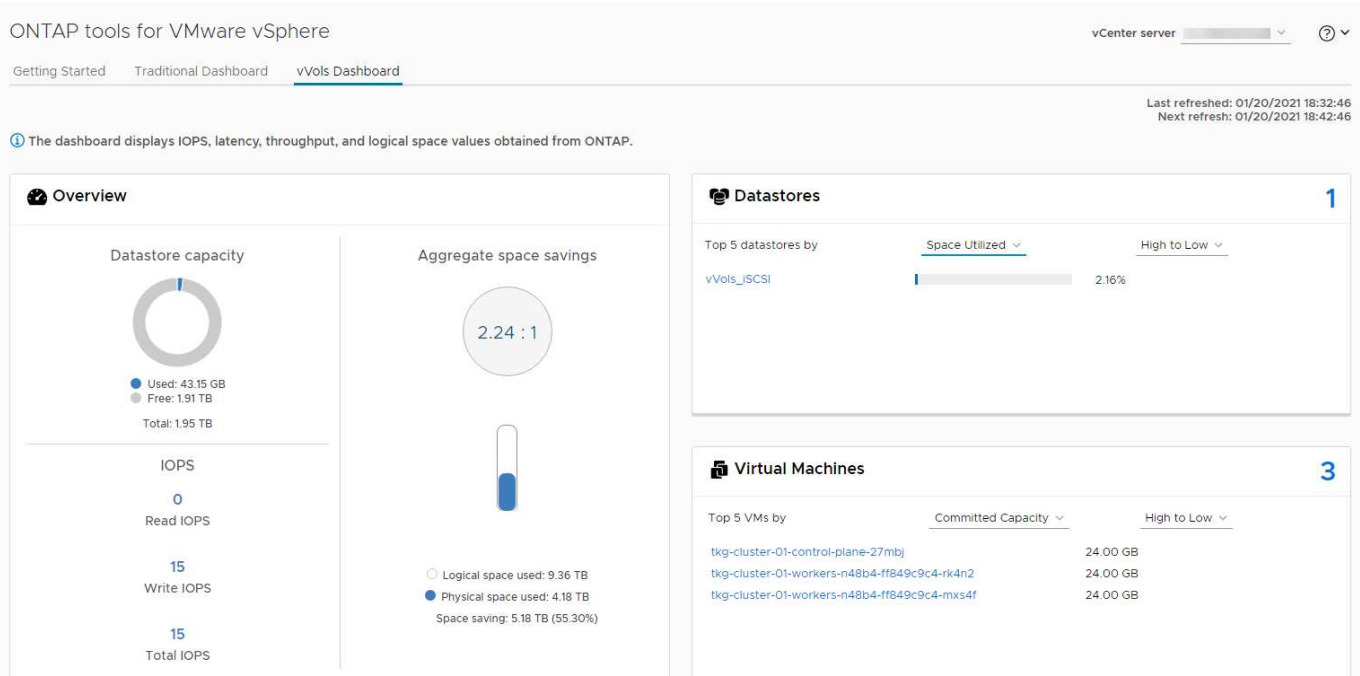
利用VMware vSphere APIS for Storage

AWARENYUIYUHEYUJIYUDEJIYUDEJIYUDEJUDEJIEMIYUDEJUDEJUDEJUDEJUHE值得一看的是、这种方法可以帮助您简化虚拟化存储操作、避免大量琐碎的工作。

在使用VASA之前、VM管理员可以定义VM存储策略、但他们必须与存储管理员一起确定适当的数据存储库、通常使用文档或命名约定。借助 VASA ，存储管理员可以定义一系列存储功能，包括性能，分层，加密和复制。一个卷或一组卷的一组功能称为存储功能配置文件（ Storage Capability Profile ， SCP ）。

SCP支持为VM的数据Vvol设置最小和/或最大QoS。只有 AFF 系统才支持最低 QoS 。适用于 VMware vSphere 的 ONTAP 工具包含一个信息板，用于显示 ONTAP 系统上 VVol 的 VM 粒度性能和逻辑容量。

下图显示了适用于 VMware vSphere 9.8 VVol 的 ONTAP 工具信息板。



定义存储功能配置文件后，可以使用该配置文件来使用存储策略来配置 VM ，以确定其要求。通过 VM 存储策略与数据存储库存储功能配置文件之间的映射， vCenter 可以显示一个兼容数据存储库列表以供选择。这种方法称为基于存储策略的管理。

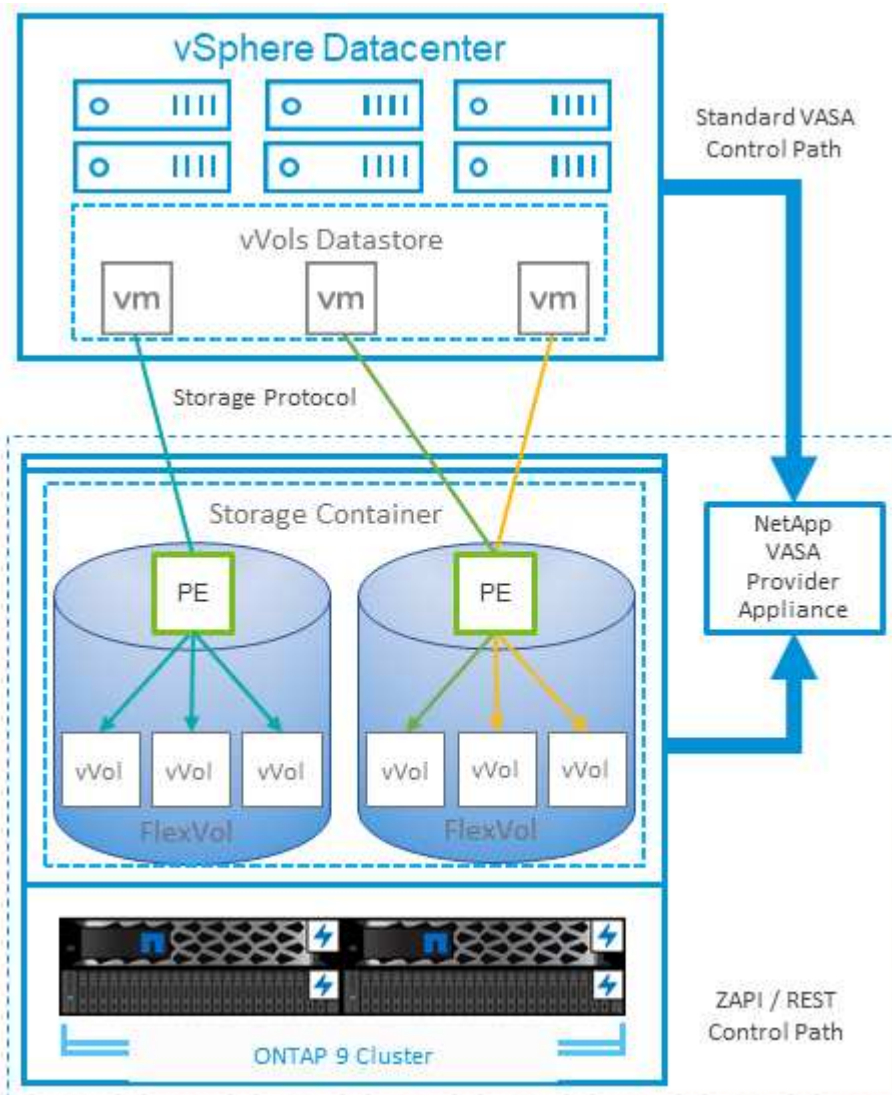
VASA 提供了查询存储并将一组存储功能返回到 vCenter 的技术。VASA 供应商提供程序可在存储系统 API 和构造与 vCenter 可识别的 VMware API 之间进行转换。适用于 ONTAP 的 NetApp VASA Provider 是作为适用于 VMware vSphere 设备 VM 的 ONTAP 工具的一部分提供的、vCenter 插件提供了用于配置和管理 VVOP 数据存储库的界面、并能够定义存储功能配置文件 (Storage Capability profile、SCP)。

ONTAP 同时支持 VMFS 和 NFS VVol 数据存储库。将 VVOL 与 SAN 数据存储库结合使用可带来 NFS 的一些

优势，例如虚拟机级别粒度。下面是一些需要考虑的最佳实践，您可以在中找到追加信息 ["TR-4400"](#)：

- 一个 VVOL 数据存储库可以在多个集群节点上包含多个 FlexVol 卷。最简单的方法是使用一个数据存储库，即使卷具有不同的功能也是如此。SPBM 可确保为 VM 使用兼容的卷。但是，这些卷都必须属于一个 ONTAP SVM，并使用一个协议进行访问。对于每个协议，每个节点一个 LIF 就足够了。避免在一个 VVOL 数据存储库中使用多个 ONTAP 版本，因为存储功能可能因版本而异。
- 使用适用于 VMware vSphere 的 ONTAP 工具插件创建和管理 VVOL 数据存储库。除了管理数据存储库及其配置文件之外，它还会根据需要自动创建一个协议端点来访问 VVol。如果使用 LUN，请注意，LUN PE 会使用 LUN ID 300 及更高版本进行映射。验证 ESXi 主机的高级系统设置 `Disk.MaxLUN` 允许 LUN ID 号大于 300 (默认值为 1,024)。执行此步骤的方法是、在 vCenter 中选择 ESXi 主机、然后选择配置选项卡并查找 `Disk.MaxLUN` 在高级系统设置列表中。
- 请勿将适用于 VMware vSphere 的 VASA Provider，vCenter Server（设备或基于 Windows）或 ONTAP 工具本身安装或迁移到 VVOL 数据存储库中，因为它们相互依赖，因此会限制您在发生断电或其他数据中心中断时对其进行管理的能力。
- 定期备份 VASA Provider 虚拟机。至少每小时为包含 VASA Provider 的传统数据存储库创建一次快照。有关保护和恢复 VASA Provider 的详细信息，请参见此部分 ["知识库文章"](#)。

下图显示了 VVOL 组件。



云迁移和备份

ONTAP 的另一个优势是广泛支持混合云，将内部私有云中的系统与公有云功能相结合。以下是可与 vSphere 结合使用的一些 NetApp 云解决方案：

- *第一方产品。* Amazon FSx for NetApp ONTAP、Google Cloud NetApp Volumes 和 Azure NetApp Files 在领先的公共云环境中提供高性能、多协议托管存储服务。VMware Cloud on AWS (VMC on AWS)、Azure VMware Solution (AVS) 和 Google Cloud VMware Engine (GCVE) 可以直接将它们用作客户操作系统 (GOS) 和计算实例的数据存储或存储。
- *云服务。* 使用 NetApp Backup and Recovery 或 SnapMirror Cloud 通过公共云存储保护来自本地系统的数据。NetApp Copy and Sync 有助于在 NAS 和对象存储之间迁移数据并保持数据同步。NetApp Disaster Recovery 提供了一种经济高效的解决方案，利用 NetApp 技术作为强大且功能强大的灾难恢复解决方案的基础，适用于 DR 到云、DR 到本地以及本地到本地。
- * FabricPool。* FabricPool 可为 ONTAP 数据快速轻松地分层。冷块可以迁移到公有云或私有 StorageGRID 对象存储中的对象存储、并在再次访问 ONTAP 数据时自动重新调用。或者，使用对象层作为已由 SnapVault 管理的数据的第三级保护。这种方法可以让您做到 ["为 VM 存储更多快照"](#) 在主和 / 或二级 ONTAP 存储系统上。
- * ONTAP Select。* 使用 NetApp 软件定义的存储将您的私有云扩展到 Internet 上的远程设施和办公室，您可以在这些设施和办公室使用 ONTAP Select 支持块和文件服务以及您在企业数据中心拥有的相同 vSphere 数据管理功能。

在设计基于虚拟机的应用程序时，请考虑未来的云移动性。例如，不要将应用程序和数据文件放在一起，而是对数据使用单独的 LUN 或 NFS 导出。这使您可以将虚拟机和数据分别迁移到云服务。

要深入了解更多安全主题、请参阅以下资源。

- ["ONTAP Select 文档"](#)
- ["备份和恢复文档"](#)
- ["灾难恢复文档"](#)
- ["适用于 NetApp ONTAP 的 Amazon FSX"](#)
- ["基于 AWS 的 VMware Cloud"](#)
- ["什么是 Azure NetApp Files? "](#)
- ["Azure VMware 解决方案"](#)
- ["Google Cloud VMware 引擎"](#)
- ["什么是 Google Cloud NetApp 卷? "](#)

vSphere 数据加密

如今，通过加密保护空闲数据的需求日益增长。虽然最初的关注点是金融和医疗保健信息、但人们越来越关注保护所有信息、无论是存储在文件、数据库中还是其他数据类型中。

运行 ONTAP 的系统可通过空闲加密轻松保护任何数据。NetApp 存储加密 (NSE) 将自加密驱动器 (Self-Encryption Drive、SE) 与 ONTAP 结合使用来保护 SAN 和 NAS 数据。NetApp 还提供 NetApp 卷加密和 NetApp 聚合加密，这是一种基于软件的简单方法，用于对任何磁盘驱动器上的卷进行加密。这种软件加密不需要特殊的磁盘驱动器或外部密钥管理器、ONTAP 客户可以免费使用。您可以升级并开始使用它、而不会对客户端或应用程序造成任何

中断、并且这些客户端或应用程序已通过FIPS 140-2 1级标准(包括板载密钥管理器)的验证。

可以通过多种方法保护在 VMware vSphere 上运行的虚拟化应用程序的数据。一种方法是在子操作系统级别使用虚拟机中的软件保护数据。vSphere 6.5 等较新的虚拟机管理程序现在支持在 VM 级别进行加密，这是另一种替代方案。但是，NetApp 软件加密简单易用，并且具有以下优势：

- * 对虚拟服务器 CPU 没有影响。 * 某些虚拟服务器环境需要为其应用程序提供每个可用的 CPU 周期，但测试表明，使用虚拟机管理程序级别的加密最多需要 5 倍的 CPU 资源。即使加密软件支持英特尔的AES-NI指令集来卸载加密工作负载(就像NetApp软件加密一样)、但由于需要新CPU来与旧服务器不兼容、因此这种方法可能不可行。
- *包括板载密钥管理器。*NetApp软件加密包括一个板载密钥管理器、无需购买和使用复杂的高可用性密钥管理服务器、即可轻松上手。
- * 对存储效率没有影响。 * 重复数据删除和数据压缩等存储效率技术目前已广泛应用，是经济高效地使用闪存磁盘介质的关键。但是，加密数据通常无法进行重复数据删除或压缩。与其他方法不同，NetApp 硬件和存储加密的运行级别较低，并允许充分利用行业领先的 NetApp 存储效率功能。
- * 轻松的数据存储库粒度加密。 * 借助 NetApp 卷加密，每个卷都获得自己的 AES 256 位密钥。如果需要更改，只需使用一个命令即可。如果您有多个租户或需要为不同部门或应用程序证明独立加密，则此方法非常适合。此加密在数据存储库级别进行管理，比管理单个虚拟机要简单得多。

软件加密入门非常简单。安装许可证后、只需指定密码短语来配置板载密钥管理器、然后创建新卷或执行存储端卷移动以启用加密即可。NetApp 正在努力在其未来版本的 VMware 工具中增加对加密功能的集成支持。

要深入了解更多安全主题、请参阅以下资源。

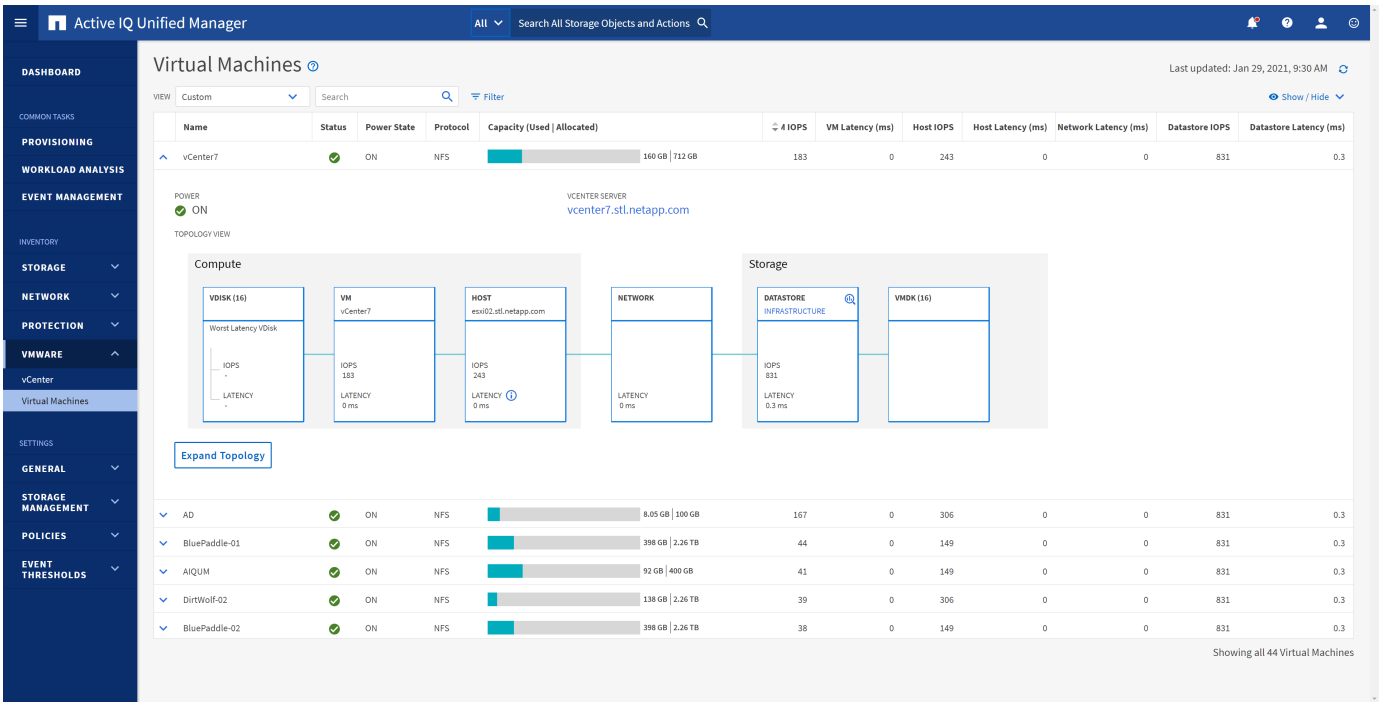
- ["安全技术报告"](#)
- ["安全强化指南"](#)
- ["ONTAP安全性和数据加密产品文档"](#)

Active IQ Unified Manager

通过 Active IQ Unified Manager 可以查看虚拟基础架构中的虚拟机，并监控虚拟环境中的存储和性能问题并对其进行故障排除。

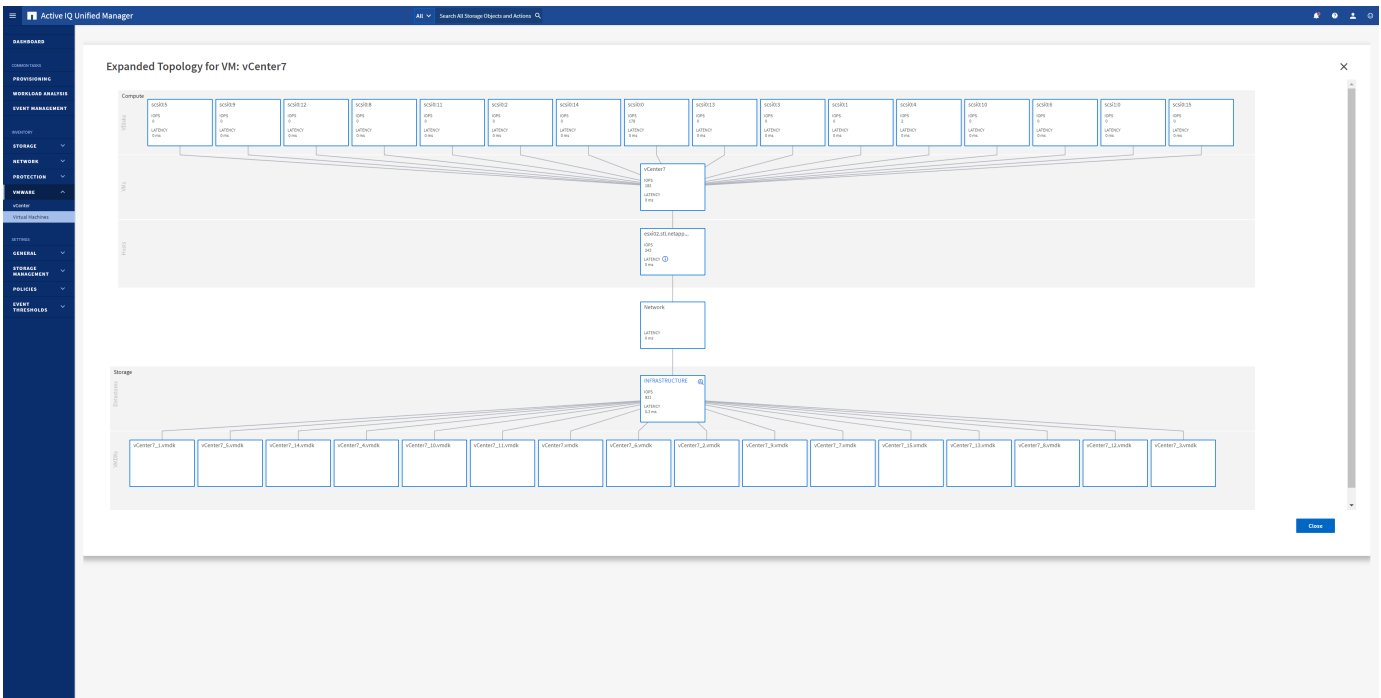
ONTAP 上的典型虚拟基础架构部署包含多个组件，这些组件分布在计算层，网络层和存储层上。VM 应用程序中的任何性能滞后都可能是由于各个层的各个组件同时面临的延迟造成的。

以下屏幕截图显示了 Active IQ Unified Manager 虚拟机视图。



Unified Manager 以拓扑视图形式呈现虚拟环境的底层子系统，用于确定计算节点，网络或存储是否发生延迟问题描述。此视图还会突出显示导致执行补救步骤和解决底层问题描述时出现性能滞后的特定对象。

以下屏幕截图显示了 AIQUM 扩展拓扑。



基于存储策略的管理和虚拟卷

利用VMware vSphere APIS for Storage

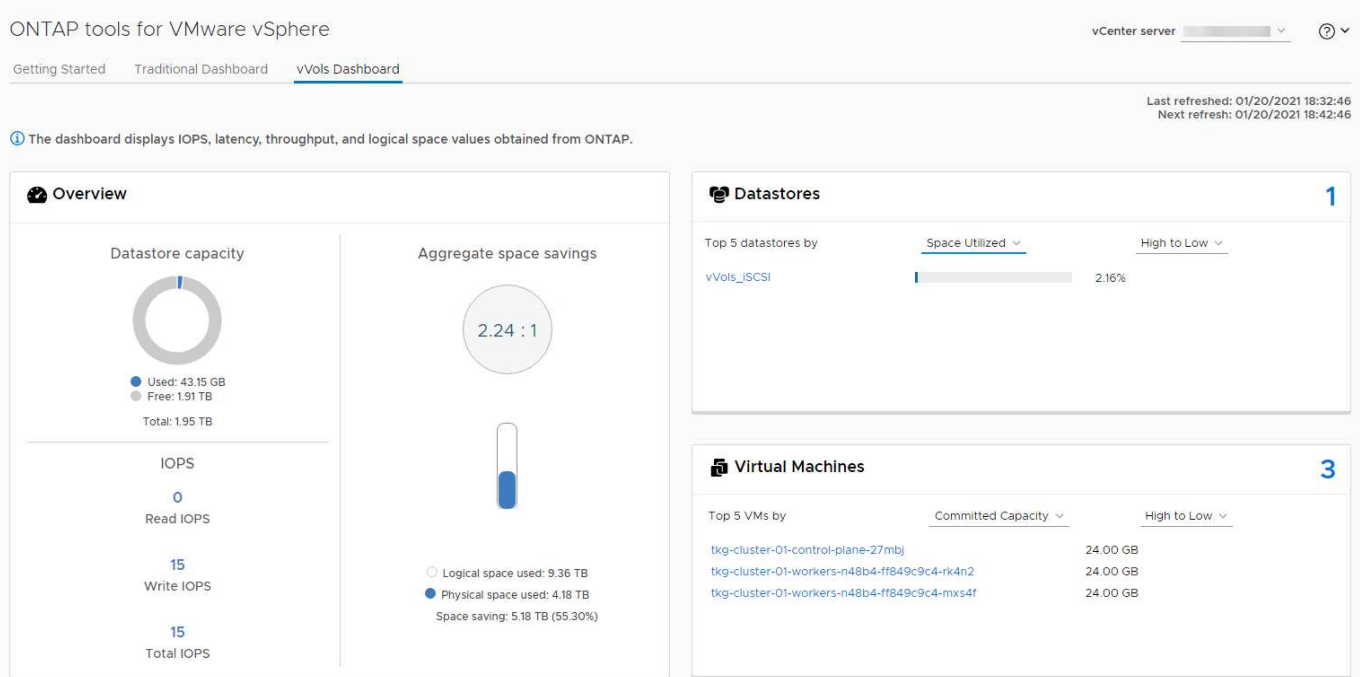
AWARENYUIYUHEYUJIYUDEJIYUDEJIYUDEJUDEJIEMUYUDEJUDEJUDEJUDEJUHE

值得一看的是、这种方法可以帮助您简化虚拟化存储操作、避免大量琐碎的工作。

在使用 VASA 之前，VM 管理员可以定义 VM 存储策略，但他们必须与存储管理员一起确定适当的数据存储库、通常使用文档或命名约定。借助 VASA，存储管理员可以定义一系列存储功能，包括性能，分层，加密和复制。一个卷或一组卷的一组功能称为存储功能配置文件（Storage Capability Profile，SCP）。

SCP 支持为 VM 的数据 VVol 设置最小和/或最大 QoS。只有 AFF 系统才支持最低 QoS。适用于 VMware vSphere 的 ONTAP 工具包含一个信息板，用于显示 ONTAP 系统上 VVol 的 VM 粒度性能和逻辑容量。

下图显示了适用于 VMware vSphere 9.8 VVol 的 ONTAP 工具信息板。



定义存储功能配置文件后，可以使用该配置文件来使用存储策略来配置 VM，以确定其要求。通过 VM 存储策略与数据存储库存储功能配置文件之间的映射，vCenter 可以显示一个兼容数据存储库列表以供选择。这种方法称为基于存储策略的管理。

VASA 提供了查询存储并将一组存储功能返回到 vCenter 的技术。VASA 供应商提供程序可在存储系统 API 和构造与 vCenter 可识别的 VMware API 之间进行转换。适用于 ONTAP 的 NetApp VASA Provider 是作为适用于 VMware vSphere 设备 VM 的 ONTAP 工具的一部分提供的、vCenter 插件提供了用于配置和管理 VVol 数据存储库的界面、并能够定义存储功能配置文件 (Storage Capability profile、SCP)。

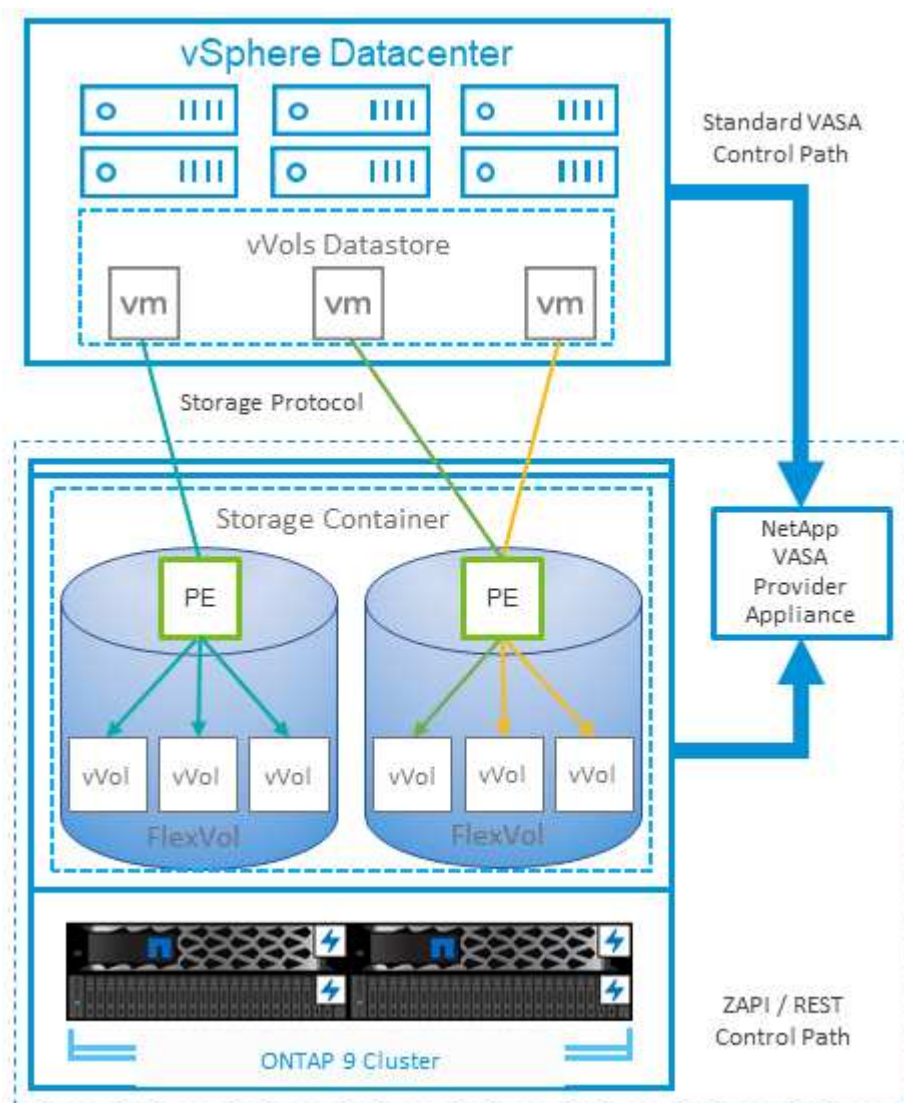
ONTAP 同时支持 VMFS 和 NFS VVol 数据存储库。将 VVOL 与 SAN 数据存储库结合使用可带来 NFS 的一些优势，例如虚拟机级别粒度。下面是一些需要考虑的最佳实践，您可以在中找到追加信息 ["TR-4400"](#)：

- 一个 VVOL 数据存储库可以在多个集群节点上包含多个 FlexVol 卷。最简单的方法是使用一个数据存储库，即使卷具有不同的功能也是如此。SPBM 可确保为 VM 使用兼容的卷。但是，这些卷都必须属于一个 ONTAP SVM，并使用一个协议进行访问。对于每个协议，每个节点一个 LIF 就足够了。避免在一个 VVOL 数据存储库中使用多个 ONTAP 版本，因为存储功能可能因版本而异。
- 使用适用于 VMware vSphere 的 ONTAP 工具插件创建和管理 VVOL 数据存储库。除了管理数据存储库及其配置文件之外，它还会根据需要自动创建一个协议端点来访问 VVol。如果使用 LUN，请注意，LUN PE 会使用 LUN ID 300 及更高版本进行映射。验证 ESXi 主机的高级系统设置 `Disk.MaxLUN` 允许 LUN ID 号大于 300（默认值为 1,024）。执行此步骤的方法是、在 vCenter 中选择 ESXi 主机、然后选择配置选项卡并查找 `Disk.MaxLUN` 在高级系统设置列表中。
- 请勿将适用于 VMware vSphere 的 VASA Provider，vCenter Server（设备或基于 Windows）或 ONTAP

工具本身安装或迁移到 vVOL 数据存储库中，因为它们相互依赖，因此会限制您在发生断电或其他数据中心中断时对其进行管理的能力。

- 定期备份 VASA Provider 虚拟机。至少每小时为包含 VASA Provider 的传统数据存储库创建一次快照。有关保护和恢复 VASA Provider 的详细信息，请参见此部分 ["知识库文章"](#)。

下图显示了 vVOL 组件。



VMware Storage Distributed Resource Scheduler

VMware Storage Distributed Resource Scheduler (SDRS) 是一项 vSphere 功能，可根据当前 I/O 延迟和空间使用情况自动将 VM 放置在数据存储库集群中。

然后，它会在数据存储库集群（也称为 Pod）中的数据存储库之间无中断地移动虚拟机或 VMDK，从而选择最佳数据存储库，以便将虚拟机或 VMDK 放置在数据存储库集群中。数据存储库集群是一组相似的数据存储库，从 vSphere 管理员的角度来看，这些数据存储库会聚合到一个使用单元中。

在将 SDRS 与适用于 VMware vSphere 的 ONTAP 工具结合使用时，您必须先使用此插件创建数据存储库，使用 vCenter 创建数据存储库集群，然后再将此数据存储库添加到其中。创建数据存储库集群后，可以直接从详细信息页面上的配置向导将其他数据存储库添加到数据存储库集群中。

有关 SDRS 的其他 ONTAP 最佳实践包括：

- 除非您有特定要求、否则请勿使用SDRS。
 - 使用ONTAP时不需要SDRS。SDRS无法识别重复数据删除和数据压缩等ONTAP存储效率功能、因此、它可能会做出不适合您环境的决策。
 - SDRS无法识别ONTAP QoS策略、因此可能会做出性能不理想的决策。
 - SDRS无法识别ONTAP Snapshot副本、因此它可能会做出导致快照呈指数级增长的决策。例如、将虚拟机移动到另一个数据存储库会在新数据存储库中创建新文件、从而导致快照增长。对于具有大型磁盘或多个快照的VM尤其如此。然后、如果将虚拟机移回原始数据存储库、则原始数据存储库上的快照将增大。

如果您确实使用SDRS、请考虑以下最佳实践：

- 集群中的所有数据存储库都应使用相同类型的存储（例如 SAS ， SATA 或 SSD ），可以是所有 VMFS 或 NFS 数据存储库，并且具有相同的复制和保护设置。
- 请考虑在默认（手动）模式下使用 SDRS 。通过此方法，您可以查看建议并决定是否应用这些建议。请注意 VMDK 迁移的以下影响：
 - 当SDRS在数据存储库之间移动VMDK时、ONTAP克隆或重复数据删除节省的空间可能会减少、具体取决于重复数据删除或数据压缩在目标上的效果。
 - 在SDRS移动VMDK后、NetApp建议在源数据存储库中重新创建快照、因为空间会被移动的VM锁定。
 - 在同一聚合上的数据存储库之间移动 VMDK 没有什么优势， SDRS 无法查看可能共享该聚合的其他工作负载。

有关SDRS的详细信息，请参见VMware文档，网址为 ["存储DRS常见问题解答"](#)。

建议的 ESXi 主机和其他 ONTAP 设置

NetApp为NFS和块协议开发了一组最佳ESXi主机设置。此外、还提供了有关多路径和HBA超时设置的特定指导、以便根据NetApp和VMware内部测试在ONTAP中正常运行。

可以使用适用于VMware vSphere的ONTAP工具轻松设置这些值：从ONTAP工具概述页面向下滚动到底部、然后单击ESXi主机合规性portlet中的应用建议设置。

下面是当前所有受支持的ONTAP版本的建议主机设置。

主机设置	* NetApp建议值*	需要重新启动
* ESXi高级配置*		
VMFS3.HardwareAcceleratedLocking	保留默认值(1)	否
VMFS3.EnableBlockDelete	保留默认值(0)、但可以根据需要进行更改。有关详细信息、请参见 "VMFS5虚拟机的空间回收"	否
VMFS3.EnableVMFS6Unmap	保留默认值(1)有关详细信息、请参见 "VMware vSphere API：阵列集成(VAAI)"	否

主机设置	* NetApp建议值*	需要重新启动
NFS设置		
newSyncInterval	如果您不使用适用于Kubnetes的vSphere CSI、请按设置 "VMware 知识库 386364"	否
Net.TcpipHeapSize	vSphere 6.0 或更高版本，设置为32。 所有其他NFS配置、设置为30	是的。
Net.TcpipHeapMax	对于大多数vSphere 6.X版本、设置为512 MB。 对于6.5U3、6.7U3和7.0或更高版本、设置为默认值(1024MB)。	是的。
NFS.MaxVolumes	vSphere 6.0或更高版本、请设置为256 所有其他NFS配置均设置为64。	否
NFS41.MaxVolumes	vSphere 6.0或更高版本、请设置为256。	否
NFS.MaxQueueDepth ¹	vSphere 6.0或更高版本、设置为128	是的。
nfs.HeartbeatMaxFailures	对于所有NFS配置、均设置为10	否
nfs.Heartbeat频率	对于所有NFS配置、请设置为12	否
nfs.HeartbeatTimeout	对于所有NFS配置、设置为5。	否
SUNRPC.MaxConnPerIP	vSphere 7.0 到 8.0，设置为 128。 ESXi 8.0 之后的版本中将忽略此设置。	否
* FC/FCoE 设置 *		
路径选择策略	如果使用采用 ALUA 的 FC 路径，则设置为 RR（轮循）。对于所有其他配置，设置为 FIXED。将此值设置为 RR 有助于在所有主动 / 优化路径之间实现负载平衡。固定值适用于较旧的非 ALUA 配置，有助于防止代理 I/O换言之、它有助于防止I/O流向在7-模式下运行Data ONTAP 的环境中高可用性(HA)对的另一节点	否
disk.qFullSampSize	对于所有配置，均设置为 32。 设置此值有助于防止出现 I/O 错误。	否
disk.qFullThreshold	对于所有配置、均设置为8。 设置此值有助于防止出现 I/O 错误。	否
Emulex FC HBA 超时	使用默认值。	否
QLogic FC HBA 超时	使用默认值。	否
* iSCSI 设置 *		

主机设置	* NetApp建议值*	需要重新启动
路径选择策略	对于所有 iSCSI 路径，设置为 RR（轮循）。 将此值设置为 RR 有助于在所有主动 / 优化路径之间实现负载平衡。	否
disk.qFullSampSize	对于所有配置，均设置为 32。 设置此值有助于防止出现 I/O 错误	否
disk.qFullThreshold	对于所有配置、均设置为 8。 设置此值有助于防止出现 I/O 错误。	否



使用VMware vSphere 7.0.1和VMware vSphere ESXi 7.3.2时、NFS高级配置选项MaxQueue深度可能无法正常工作。有关详细信息、请参见"[VMware知识库86331](#)"。

在创建 ONTAP FlexVol 卷和 LUN 时，ONTAP 工具还会指定某些默认设置：

* ONTAP Tool*	默认设置
Snapshot 预留 (-percent-snapshot-space)	0
预留百分比 (-fractional-reserve)	0
访问时间更新 (-atime-update)	false
最小预读 (-min-readahead)	false
计划快照	无
存储效率	enabled
卷保证	无 (精简配置)
卷自动调整大小	grow_shrink
LUN 空间预留	已禁用
LUN 空间分配	enabled

多路径性能设置

虽然当前未使用可用的ONTAP工具进行配置、但NetApp建议使用以下配置选项：

- 在高性能环境中使用非ASA系统或使用单个 LUN 数据存储测试性能时，请考虑将循环 (VMW_PSP_RR) 路径选择策略 (PSP) 的负载平衡设置从默认 IOPS 设置 1000 更改为值 1。看"[VMware 知识库 2069356](#)"了解更多信息。
- 在 vSphere 6.7 Update 1 中，VMware 为 Round Robin PSP 引入了一种新的延迟负载平衡机制。现在，当使用带有 NVMe 命名空间的 HPP（高性能插件）以及 vSphere 8.0u2 及更高版本、iSCSI 和 FCP 连接的 LUN 时，也可以使用延迟选项。新选项在选择 I/O 最佳路径时会考虑 I/O 带宽和路径延迟。NetApp建议在具有非等效路径连接的环境中使用延迟选项，例如一条路径上的网络跳数比另一条路径上的网络跳数更多的情况，或者使用NetApp ASA系统时。看 "[更改延迟轮循的默认参数](#)"了解更多信息。

其他文档

对于采用vSphere 7的FCP和iSCSI、有关详细信息、请参见。["将VMware vSphere 7.x与ONTAP结合使用"](#)对于采用vSphere 8的FCP和iSCSI、有关详细信息、请参见["将VMware vSphere 8.x与ONTAP结合使用"](#)。对于采

用vSphere 7的NVMe-oF、有关详细信息、请参见["对于NVMe-oF、有关详细信息、请参见适用于采用ONTAP的ESXi 7.x的NVMe-oF主机配置"](#)。对于采用vSphere 8的NVMe-oF、有关详细信息、请参见["对于NVMe-oF、有关详细信息、请参见适用于采用ONTAP的ESXi 8.x的NVMe-oF主机配置"](#)

使用工具的虚拟卷(Virtual Volume、ONTAP) 10.

概述

二十年来、ONTAP一直是适用于VMware vSphere环境的领先存储解决方案、并不断增加创新功能、以简化管理并降低成本。

本文档介绍了适用于VMware vSphere虚拟卷(vvol)的ONTAP 功能、包括最新的产品信息和用例以及最佳实践和其他可简化部署和减少错误的信息。



本文档将取代先前发布的技术报告_TR-4400: 《使用ONTAP的VMware vSphere虚拟卷(Vvol)》 _

最佳实践是指南和兼容性列表等其他文档的补充。它们是根据 NetApp 工程师和客户的实验室测试和丰富的现场经验开发的。它们可能不是唯一有效或受支持的实践、但通常是最简单的解决方案、可满足大多数客户的需求。



本文档已进行更新、其中包括vSphere 8.0 Update 3、ONTAP工具10.4版中的新vvol功能以及新的NetApp ASA系统。

虚拟卷(Virtual Volume、Virtual Volume、Virtual Volume)概述

NetApp于2012年开始与VMware合作、为适用于vSphere 5的vSphere APIS for Storage AWARMIVAIVAICHUIAICHUDE(VASA)提供支持。通过早期的VASA Provider、可以在配置文件中定义存储功能、这些功能可用于在配置时筛选数据存储库、并在此后检查是否符合策略。随着时间的推移、这种情况不断发展、增加了一些新功能、以便在配置以及添加虚拟卷或vvol (其中、各个存储对象用于虚拟机文件和虚拟磁盘)方面实现更大的自动化。这些对象可以是LUN、文件、现在适用于vSphere 8 - NVMe命名空间(与ONTAP工具9.13P2结合使用)。NetApp与VMware密切合作、作为2015年随vSphere 6发布的vvol的参考合作伙伴、并再次作为在vSphere 8中基于网络结构使用NVMe的vvol的设计合作伙伴。NetApp将继续增强ONTAP 以利用其最新功能。

需要注意以下几个组件:

VASA Provider

这是一个软件组件、用于处理VMware vSphere与存储系统之间的通信。对于ONTAP 、VASA Provider在一种称为适用于VMware vSphere的ONTAP 工具(简称ONTAP 工具)的设备中运行。ONTAP 工具还包括一个vCenter插件、一个适用于VMware Site Recovery Manager的存储复制适配器(Storage Replication Adapter、SRA)以及用于构建您自己的自动化的REST API服务器。配置ONTAP 工具并将其注册到vCenter后、几乎不再需要直接与ONTAP 系统交互、因为几乎所有存储需求都可以直接在vCenter UI中进行管理、或者通过REST API自动化进行管理。

协议端点(PE)

协议端点是ESXi主机和VMware数据存储库之间的I/O代理。ONTAP VASA Provider会自动创建这些LUN、可以是VVOL数据存储库的每个FlexVol卷一个协议端点LUN (大小为4 MB)、也可以是托管此数据存储库中的FlexVol卷的存储节点上的每个NFS接口(NFS挂载点、LIF)一个。ESXi主机直接装载这些协议端点、而不是装载单个VVOLLUN和虚拟磁盘文件。协议端点由VASA Provider自动创建、挂载、卸载和删除、因此无需对这些端点

进行管理、同时也无需管理任何必要的接口组或导出策略。

虚拟协议端点(VPE)

vSphere 8中的新增功能是、在将基于网络结构的NVMe (NVMe-oF)与vvol结合使用时、协议端点的概念在ONTAP 中不再适用。相反、ESXi主机会在第一个虚拟机启动后自动为每个ANA组建立虚拟PE。ONTAP 会自动为数据存储库使用的每个FlexVol 卷创建ANA组。

使用NVMe-oF for VVOLs的另一个优势是、VASA Provider不需要任何绑定请求。相反、ESXi主机会根据VPE在内部处理VVOI绑定功能。这样可以减少VVOV绑定风暴影响服务的机会。

有关详细信息，请参见 "[NVMe和虚拟卷](#)" 开启 "[vmware.com](#)"

虚拟卷数据存储库

| 虚拟卷数据存储是vVols容器的逻辑数据存储表示，由 VASA 提供商创建和维护。该容器代表由 VASA 提供商管理的存储系统提供的存储容量池。ONTAP工具支持将多个FlexVol卷（称为后备卷）分配给单个vVols数据存储，这些vVols数据存储可以跨越ONTAP集群中的多个节点，将具有不同功能的闪存和混合系统结合起来。管理员可以使用配置向导或 REST API 创建新的FlexVol卷，或者选择预先创建的FlexVol卷作为后备存储（如果有的话）。

虚拟卷(Virtual Volume、Virtual Volume、Virtual Volume)

vVols是存储在vVols数据存储中的实际虚拟机文件和磁盘。使用术语 vVol（单数）指的是单个特定文件、LUN 或命名空间。ONTAP根据数据存储使用的协议创建 NVMe 命名空间、LUN 或文件。vVols)有几种不同的类型；最常见的包括配置卷 (Config，唯一使用 VMFS 文件系统的卷，包含元数据文件，例如虚拟机的 VMX 文件)、数据卷 (Data，虚拟磁盘或 VMDK) 和交换卷 (Swap，在虚拟机启动时创建)。受 VMware 虚拟机加密保护的vVols 类型为“其他”。VMware VM 加密不应与ONTAP卷或聚合加密混淆。

基于政策的管理

VMware vSphere API for Storage Awareness (VASA) 使虚拟机管理员能够轻松使用配置虚拟机所需的任何存储功能，而无需与存储团队进行交互。在 VASA 出现之前，虚拟机管理员可以定义虚拟机存储策略，但必须与存储管理员合作来确定合适的数据存储，通常是通过文档或命名约定来实现的。借助 VASA，具有相应权限的 vCenter 管理员可以定义一系列存储功能，供 vCenter 用户用于配置虚拟机。VM 存储策略与数据存储功能之间的映射关系，使得 vCenter 能够显示可供选择的兼容数据存储列表，并支持其他技术，例如 VCF（以前称为 Aria 和 vRealize）自动化或 VMware vSphere Kubernetes 服务 (VKS)，从分配的策略中自动选择存储。这种方法被称为基于存储策略的管理。虽然 VASA Provider 规则和 VM 存储策略也可以与传统数据存储一起使用，但我们在这里的重点是vVols数据存储。

VM 存储策略

VM存储策略在vCenter中的策略和配置文件下创建。对于虚拟卷、请使用NetApp虚拟卷存储类型提供程序中的规则创建一个规则集。现在、与ONTAP工具9.X相比、ONTAP工具10.X提供了一种更简单的方法、它允许您直接在VM存储策略本身中指定存储属性。

如上所述、使用策略有助于简化配置VM或VMDK的任务。只需选择适当的策略、VASA Provider就会显示支持该策略的VVOs数据存储库、并将VVOV放入一个合规的FlexVol volume中。

使用存储策略部署虚拟机

New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Select storage**
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine (Requires Key Management Server)

VM Storage Policy

Platinum

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Clu
vVolsiSCSI	Compatible	100 GB	40.74 GB	64.88 GB	vVol	
vVolsNFS2202...	Compatible	2 TB	36.88 GB	1.96 TB	vVol	
local-esx01	Incompatible	3.63 TB	1.46 GB	3.63 TB	VMFS 6	
local-esx07	Incompatible	1.81 TB	3.85 GB	1.81 TB	VMFS 6	
local-esx08	Incompatible	1.69 TB	1.43 GB	1.69 TB	VMFS 6	
local-esx09	Incompatible	1.81 TB	3.85 GB	1.81 TB	VMFS 6	
local-esx15	Incompatible	3.63 TB	1.46 GB	3.63 TB	VMFS 6	
tier001_ds	Incompatible	22 TB	23.73 TB	18.09 TB	NFS v3	

CANCEL

BACK

NEXT

一旦虚拟机完成配置，VASA 提供商将继续检查合规性，并在备份卷不再符合策略时通过 vCenter 中的警报提醒虚拟机管理员。

虚拟机存储策略合规性

Storage Policies

VM Storage Policies

AFF_VASA10

VM Storage Policy Compliance

⊗ Noncompliant

Last Checked Date

5/20/2022, 12:59:35 PM

VM Replication Groups

[CHECK COMPLIANCE](#)

NetApp虚拟卷支持

ONTAP自 2012 年首次发布以来就一直支持 VASA 规范。虽然其他NetApp存储系统可能支持 VASA，但本文档重点介绍当前支持的ONTAP 9 版本。

ONTAP

除了AFF、ASA和FAS系统上的ONTAP 9 之外， NetApp还支持ONTAP Select上的 VMware 工作负载、带有 VMware Cloud on AWS 的Amazon FSx for NetApp、带有 Azure VMware Solution 的Azure NetApp Files、带有 Google Cloud VMware Engine 的Google Cloud NetApp Volumes以及 Equinix 中的NetApp Private Storage，但具体功能可能因服务提供商和可用的网络连接而异。

截至本文发布时，超大规模环境仅限于传统的 NFS v3 数据存储；因此，vVols仅适用于本地ONTAP系统，或提供本地系统全部功能的云连接系统，例如NetApp合作伙伴和全球服务提供商托管的系统。

有关ONTAP 的详细信息，请参见 ["ONTAP 产品文档"](#)

有关ONTAP 和 VMware vSphere最佳实践的详细信息、请参见 ["TR-4597"](#)

将ONTAP与虚拟卷结合使用的优势

2015 年，VMware 在 VASA 2.0 中引入了vVols支持，他们将其描述为“一个集成和管理框架，为外部存储（SAN/NAS）提供了一种新的操作模式”。这种运行模式与ONTAP存储相结合，具有诸多优势。

基于政策的管理

如第 1.2 节所述，基于策略的管理允许使用预定义的策略来配置和随后管理虚拟机。这可以从多个方面帮助IT 运维：

- 提高速度。ONTAP工具消除了 vCenter 管理员为存储配置活动向存储团队开具工单的需要。但是，通过限制对特定功能的访问，ONTAP工具在 vCenter 和ONTAP系统中的 RBAC 角色仍然允许独立团队（例如存储团队）或同一团队开展独立活动。
- *更智能的配置。*存储系统功能可通过VASAAPI公开、使配置工作流可以利用高级功能、而虚拟机管理员无需了解如何管理存储系统。
- *配置速度更快。*单个数据存储库可支持不同的存储功能、并根据虚拟机策略自动为虚拟机选择相应的存储功能。
- *避免出错。*存储和VM策略是提前制定的、并根据需要应用、而无需在每次配置VM时自定义存储。如果存储功能偏离定义的策略、则会发出合规警报。如前文所述、通过使用SCP、初始配置可预测且可重复、而根据SCP制定VM存储策略可确保准确放置。
- *更好的容量管理*通过使用VASA和ONTAP工具、可以根据需要查看存储容量、使其降至各个聚合级别、并在容量开始不足时提供多层警报。

在现代SAN上进行VM粒度管理

使用光纤通道和 iSCSI 的 SAN 存储系统是 VMware ESX 最早支持的存储系统，但它们缺乏从存储系统管理单个 VM 文件和磁盘的功能。相反，系统会配置 LUN，然后由 VMFS 管理各个文件。这使得存储系统难以直接管理单个虚拟机的存储性能、克隆和保护。vVols 结合了vVols存储用户已经享有的存储粒度控制，以及ONTAP强大的高性能 SAN 功能。

现在，借助 vSphere 8 和ONTAP tools for VMware vSphere，vVols用于传统 SCSI 协议的那些精细控制功能，现在也可以在现代光纤通道 SAN 中使用 NVMe over Fabrics 来实现，从而在规模上获得更高的性能。借助

vSphere 8.0 更新 1，现在可以部署完整的端到端 NVMe 解决方案，使用vVols，而无需在虚拟机管理程序存储堆栈中进行任何 I/O 转换。

更出色的存储卸载功能

虽然 VAAI 提供各种卸载到存储的操作，但 VASA 提供商可以解决一些问题。SAN VAAI 无法将 VMware 管理的快照卸载到存储系统。NFS VAAI 可以卸载 VM 管理的快照，但对具有存储原生快照的 VM 存在一些限制。由于vVols使用单独的 LUN、命名空间或文件作为虚拟机磁盘，ONTAP可以快速高效地克隆文件或 LUN，从而创建 VM 粒度的快照，不再需要增量文件。NFS VAAI 也不支持热（通电）Storage vMotion 迁移的卸载克隆操作。当使用 VAAI 和传统 NFS 数据存储时，必须关闭虚拟机电源才能卸载迁移任务。ONTAP工具中的 VASA 提供程序可以实现近乎即时、存储高效的热迁移和冷迁移克隆，并且还支持对vVols进行近乎即时的跨卷迁移复制。由于这些显著的存储效率优势，您或许能够充分利用vVols工作负载。**"效率担保"** 程序。同样，如果使用 VAAI 进行跨卷克隆不能满足您的要求，那么借助vVols 的复制体验改进，您很可能能够解决您的业务难题。

常见的卷使用情形

除了这些优势之外、我们还会看到VVOV存储的以下常见使用情形：

- 按需配置虚拟机
 - 私有云或服务提供商的IaaS。
 - 通过Aia (原vReise)套件、OpenStack等利用自动化和流程编排功能。
- 一流磁盘(FCD)
 - VMware vSphere Kubernetes Service (VKS) 持久卷。
 - 通过独立的 VMDK 生命周期管理提供类似 Amazon EBS 的服务。
- 按需配置临时虚拟机
 - 测试/开发实验室
 - 培训环境

使用卷的常见优势

在充分发挥其优势时(例如在上述使用情形中)、此类卷可提供以下具体改进：

- 在ONTAP集群中，克隆可以在单个卷内或跨多个卷快速创建，这比传统的启用 VAAI 的克隆具有优势。它们还具有良好的存储效率。卷内的克隆使用ONTAP文件克隆，类似于FlexClone卷，仅存储源 vVol 文件/LUN/命名空间的更改。因此，用于生产或其他应用程序用途的长期虚拟机可以快速创建，占用空间极小，并且可以受益于虚拟机级别的保护（使用适用于 VMware vSphere 的NetApp SnapCenter插件、VMware 管理的快照或 VADP 备份）和性能管理（使用ONTAP QoS）。使用vVols进行跨卷克隆比使用 VAAI 快得多，因为使用 VASA，我们可以在复制完成之前创建克隆并允许在目标位置访问它。数据块作为后台进程复制到目标 vVol。这与ONTAP对传统 LUN 的非中断式 LUN 迁移的工作方式类似。
- 在将TKG与vSphere CSI结合使用时、Vvol是理想的存储技术、可提供由vCenter管理员管理的离散存储类和容量。
- 亚马逊 EBS 类服务可以通过 FCD 交付，因为 FCD VMDK 顾名思义是 vSphere 中的一等公民，其生命周期可以独立于它可能附加到的虚拟机进行管理。

检查清单

使用此安装检查清单可确保成功部署(针对10.3及更高版本进行了更新)。

4

存储

- 共享存储设备上需要一个数据存储库。或者、您也可以使用与节点1位于同一数据存储库中的内容库、以便使用VAAI快速克隆模板。
- 内容库(仅HA需要)_
- 节点1数据存储库_____
- 节点2数据存储库(可选、但建议用于HA)_
- 节点3数据存储库(可选、但建议用于HA)_

5

部署OVA

- 请注意、此步骤可能需要长达45分钟才能完成
- "部署OVA"使用vSphere Client。
- 在OVA部署的第3步中、选择"自定义此虚拟机的硬件"选项、并在第10步中设置以下内容：
- "启用CPU热添加"
- "内存热插拔"

6

将vCenter添加到ONTAP工具

- "添加vCenter Server实例"在ONTAP工具管理器中。

7

将存储后端添加到ONTAP工具

- "配置ONTAP用户角色和权限"如果不使用管理员、则使用随附的JSON文件。
- 如果您打算使用存储多租户而不是使用 vCenter 中的ONTAP集群凭据将特定 SVM 分配给 vCenter，请按照以下步骤操作：
- "板载集群"在ONTAP工具管理器中、并将其与vCenter关联。
- "板载SVM"在ONTAP工具vCenter UI中。
- 如果*不*在 vCenter 中使用多租户 SVM：
- "板载集群"直接在ONTAP工具vCenter UI中。或者、在这种情况下、如果不使用Vvol、则可以直接添加SVM。

8

配置设备服务(可选)

- 要使用此类卷、您必须先 "编辑设备设置并启用vasa服务"执行此操作。同时、请查看以下两项。
- 如果您计划在生产环境中使用虚拟卷、请 "启用高可用性"使用上面的两个可选IP地址。
- 如果您计划将ONTAP工具Storage Replication Adapter (SRA)用于VMware站点恢复管理器或实时站点恢复， "启用SRA服务"

9

证书(可选)

- 根据VMware、如果在多个vCenter中使用Vvol、则需要CA签名证书。
- VASA服务_____
- 行政事务_____

10

其他部署后任务

- 为HA部署中的VM创建反关联性规则。
- 如果使用HA、则Storage vMotion会将节点2和节点3分隔为不同的数据存储库(可选、但建议使用)。
- "使用管理证书"在ONTAP工具管理器中安装任何必需的CA签名证书。
- 如果您为SRM/vSR启用了SRA以保护传统数据存储库，"[在VMware Live Site Recovery设备上配置SRA](#)"请。
- 配置本地备份 "[RPO几乎为零](#)"。
- 配置定期备份到其他存储介质。

将ONTAP 与虚拟卷结合使用

将VVO与NetApp结合使用的关键是适用于VMware vSphere的ONTAP工具、这些工具作为NetApp ONTAP 9系统的VASA (vSphere存储感知API)提供程序界面。

ONTAP工具还包括vCenter UI扩展、REST API服务、适用于VMware Site Recovery Manager/Live Site Recovery的存储复制适配器、监控和主机配置工具以及一系列可帮助您更好地管理VMware环境的报告。

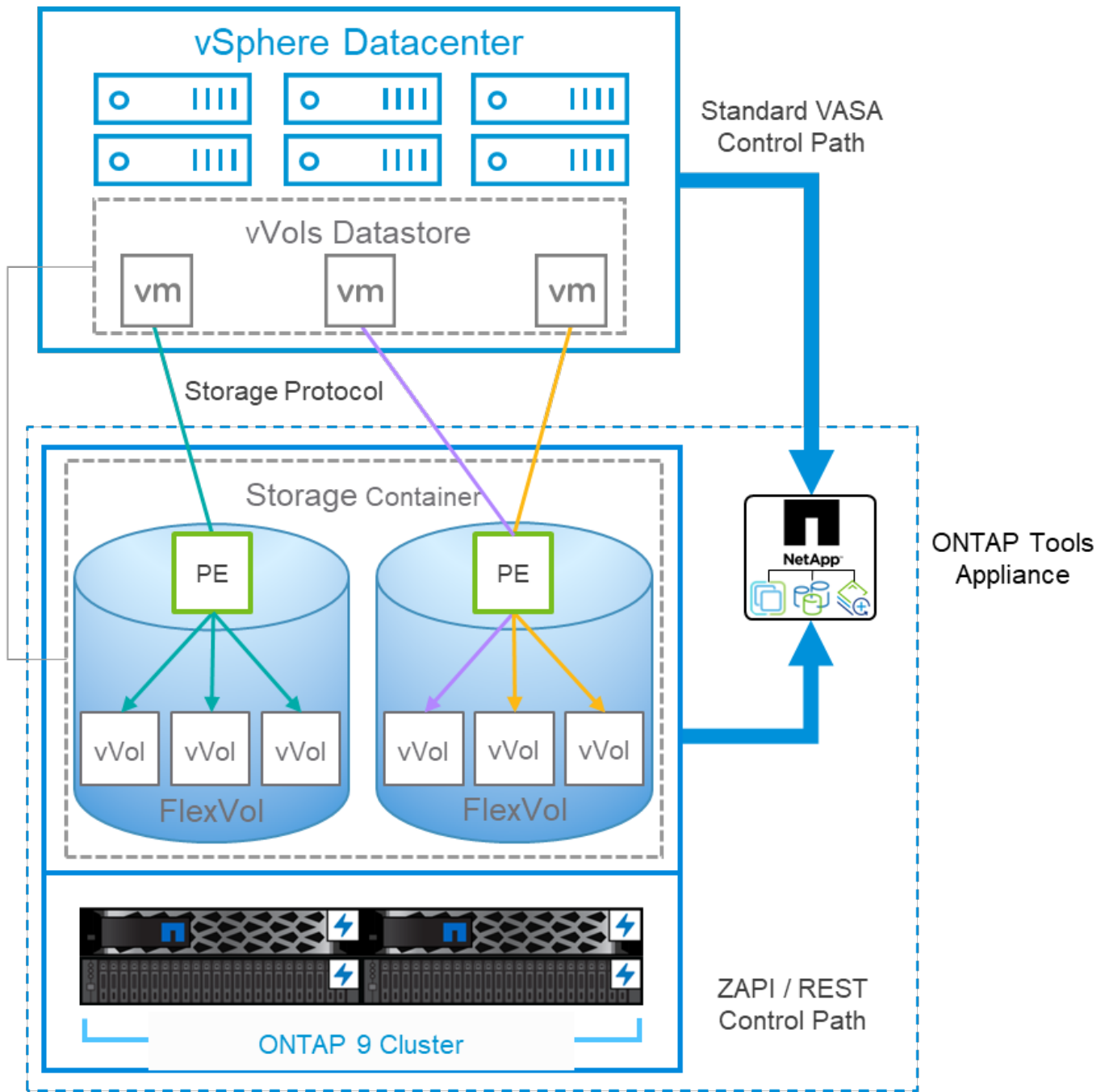
产品和文档

ONTAP One许可证包括在ONTAP系统中使用虚拟卷所需的所有许可。唯一的附加要求是免费的ONTAP工具OVA、它充当VASA Provider。在VVO环境中、VASA Provider软件会将阵列功能转换为策略驱动型属性、这些属性可通过VASA API加以利用、而vSphere管理员无需了解如何在后台管理这些功能。这样、就可以根据策略动态消耗分配的存储容量、从而无需手动创建传统数据存储库并管理其各自的存储消耗率。简而言之、vvol可以消除管理企业级存储的所有复杂性、并将其从vSphere管理员手中抽象出来、以便他们可以专注于虚拟化层。

对于将VMware Cloud Foundation与vSAN结合使用的客户、可以将vvol作为补充存储添加到任何管理或工作负载域。vvol可通过基于通用存储策略的管理框架与vSAN无缝集成。

下一代ONTAP工具10版本系列通过可扩展的容器化微服务架构实现了先前功能的现代化、该架构可通过ESXi上的一个简单OVA格式设备进行部署。ONTAP Tools 10将三个以前的设备和产品的所有功能整合到一个部署中。对于vvol管理、您将对ONTAP工具VASA Provider使用直观的vCenter UI扩展或REST API。请注意、SRA组件适用于传统数据存储库；VMware Site Recovery Manager不会对vvol使用SRA。

在将iSCSI或FCP与统一系统结合使用时、ONTAP会使用VASA Provider架构



产品安装

对于全新安装，请将虚拟设备部署到vSphere环境中。部署后，您可以登录到管理器UI或使用REST API纵向或横向扩展部署、板载vCenter (此操作会将此插件注册到vCenter)、板载存储系统，并将存储系统与vCenter关联起来。只有当您计划对专用SVM使用安全多租户时，才需要在ONTAP工具管理器UI中启用存储系统并将集群与vCenter相关联，否则只需在ONTAP工具vCenter UI扩展中或使用REST API即可将所需的存储集群挂载。

请参阅["部署Virtual Storage"](#)本文档中的或["适用于VMware vSphere的ONTAP工具文档"](#)。



最佳实践是、将ONTAP工具和vCenter设备存储在传统NFS或VMFS数据存储库上、以避免任何相互依赖关系冲突。由于vCenter和ONTAP工具必须在vvol操作期间相互通信、因此请勿将ONTAP工具设备或vCenter Server设备(VCSAS)安装或移动到它们所管理的vvol存储中。如果发生这种情况、重新启动vCenter或ONTAP工具设备可能会导致控制平台访问中断、并且设备无法启动。

可以使用ONTAP支持站点上可下载的升级ISO文件(需要登录)原位升级NetApp工具 ["适用于VMware vSphere 10的ONTAP工具一下载"](#)。按照 ["从适用于VMware vSphere 10.x的ONTAP工具升级到10.3"](#)指南说明升级设备。也可以从ONTAP工具9.13并排升级到10.3。有关该主题的详细信息、请参见 ["从适用于VMware vSphere 9.x的ONTAP工具迁移到10.3"](#)。

要估算虚拟设备的规模并了解配置限制、请参见 ["部署适用于VMware vSphere的ONTAP工具的配置限制"](#)

产品文档

以下文档可帮助您部署ONTAP 工具。

["适用于VMware vSphere的ONTAP工具文档"](#)

入门

- ["发行说明"](#)
- ["适用于VMware vSphere的ONTAP工具概述"](#)
- ["部署 ONTAP 工具"](#)
- ["升级 ONTAP 工具"](#)

使用 ONTAP 工具

- ["配置数据存储库"](#)
- ["配置基于角色的访问控制"](#)
- ["配置高可用性"](#)
- ["修改 ESXi 主机设置"](#)

保护和管理数据存储库

- ["使用ONTAP工具和SnapMirror活动同步配置vSphere Metro Storage Cluster \(VMSC\)"](#)
- ["保护虚拟机"使用SRM](#)
- ["监控集群、数据存储库和虚拟机"](#)

VASA Provider信息板

VASA Provider包括一个信息板、其中包含各个VVO尔VM的性能和容量信息。此信息直接来自ONTAP中有关VVOL文件 和LUN的信息、包括延迟、IOPS、吞吐量等。如果使用当前所有受支持的ONTAP 9版本、则默认情况下会启用此功能。请注意、初始配置完成后、数据可能需要长达30分钟才能填充信息板。

其他最佳实践

在vSphere中使用ONTAP vvol非常简单、并且遵循已发布的vSphere方法(请参见适用于您的ESXi版本的VMware文档中的在vSphere存储下使用虚拟卷)。以下是与ONTAP 结合使用时需要考虑的一些其他实践。

限制

一般来说，ONTAP支持VMware定义的vvol限制(请参见已发布 ["配置最大值"](#))。请始终检查 ["NetApp Hardware Universe"](#)、了解有关LUN、卷空间和文件的数量和大小的更新限制。

使用适用于VMware vSphere的UI扩展或REST API的ONTAP 工具来配置vvol数据存储库*和协议端点

虽然可以使用常规vSphere界面创建vvol数据存储库、但使用ONTAP工具将根据需要自动创建协议端点、并使用ONTAP最佳实践创建FlexVol卷(ASA R2不需要)。只需右键单击主机/集群/数据中心、然后选择_ONTAP tools_和_配置数据存储库_即可。您只需在向导中选择所需的卷选项即可。

切勿将ONTAP 工具设备或vCenter Server设备(VCSA)存储在其所管理的VVOLs数据存储库中。

如果您需要重新启动设备、因为它们在重新启动期间无法重新绑定自己的虚拟卷、则可能会出现"鸡肉和鸡蛋的情况"。您可以将其存储在由其他ONTAP 工具和vCenter部署管理的Vvol数据存储库中。

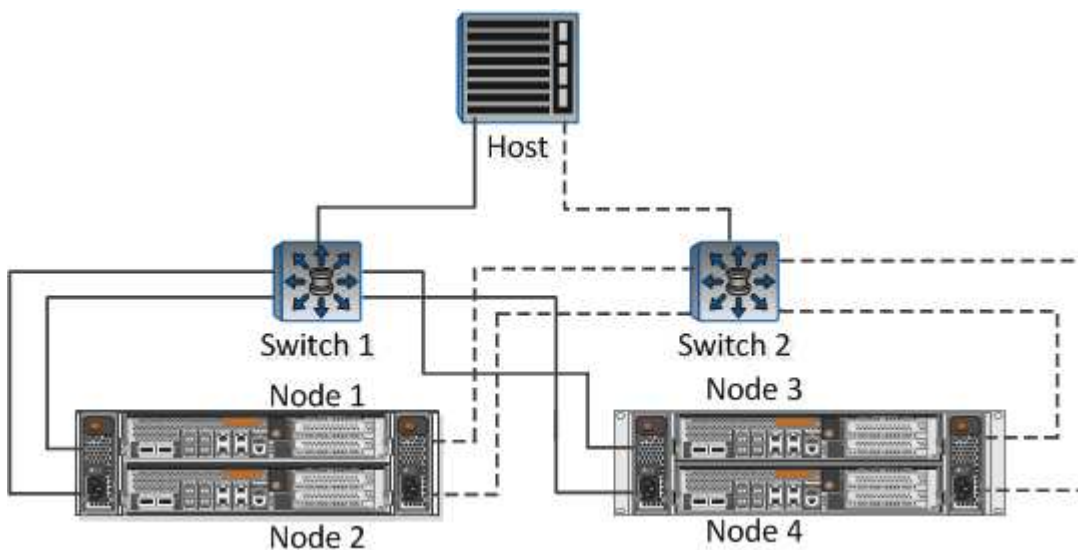
避免在不同ONTAP 版本之间执行虚拟卷操作。

VASA Provider的各个版本中支持的存储功能(例如QoS、特性等)发生了变化、其中一些功能取决于ONTAP 版本。在ONTAP 集群中使用不同版本或在具有不同版本的集群之间移动虚拟卷可能会导致意外行为或合规性警报。

对光纤通道网络结构进行分区、然后再对其使用FCP来创建卷。

ONTAP 工具的VASA提供程序负责根据已发现的受管ESXi主机启动程序管理ONTAP 中的FCP和iSCSI igrou以及NVMe子系统。但是、它不会与光纤通道交换机集成来管理分区。必须先根据最佳实践进行分区、然后才能进行任何配置。以下是单个启动程序分区到四个ONTAP系统的示例：

单个启动程序分区：



有关更多最佳实践、请参见以下文档：

"_TR-4080: 《现代SAN ONTAP 9_最佳实践》"

"_TR-4684使用NVMe-oF实施和配置现代SAN"

根据需要规划备用**FlexVol**卷。

对于非R2系统、可能需要向ASA数据存储库添加多个后备卷、以便在ONTAP集群中分布工作负载、支持不同的策略选项或增加允许的LUN或文件数量。但是、如果需要最大的存储效率、请将所有备份卷放在一个聚合上。或者、如果需要最大的克隆性能、则可以考虑使用一个FlexVol 卷、并将模板或内容库保留在同一个卷中。VASA Provider会将许多VVOLs存储操作(包括迁移、克隆和快照)卸载到ONTAP。如果在一个FlexVol 卷中执行此操作、则会使用节省空间的文件克隆、并且这些克隆几乎可以即时使用。在FlexVol 卷之间执行此操作时、这些副本可以快速可用并使用实时重复数据删除和数据压缩、但只有在使用后台重复数据删除和数据压缩的卷上运行后台作业后、才能最大程度地恢复存储效率。根据源和目标、某些效率可能会降级。

在ASA R2系统中、卷或聚合的概念从用户那里抽象出来、从而消除了这种复杂性。系统会自动处理动态放置、并根据需要创建协议端点。如果需要额外扩展、可以即时自动创建其他协议端点。

请考虑使用最大**IOPS**来控制未知或测试**VM**。

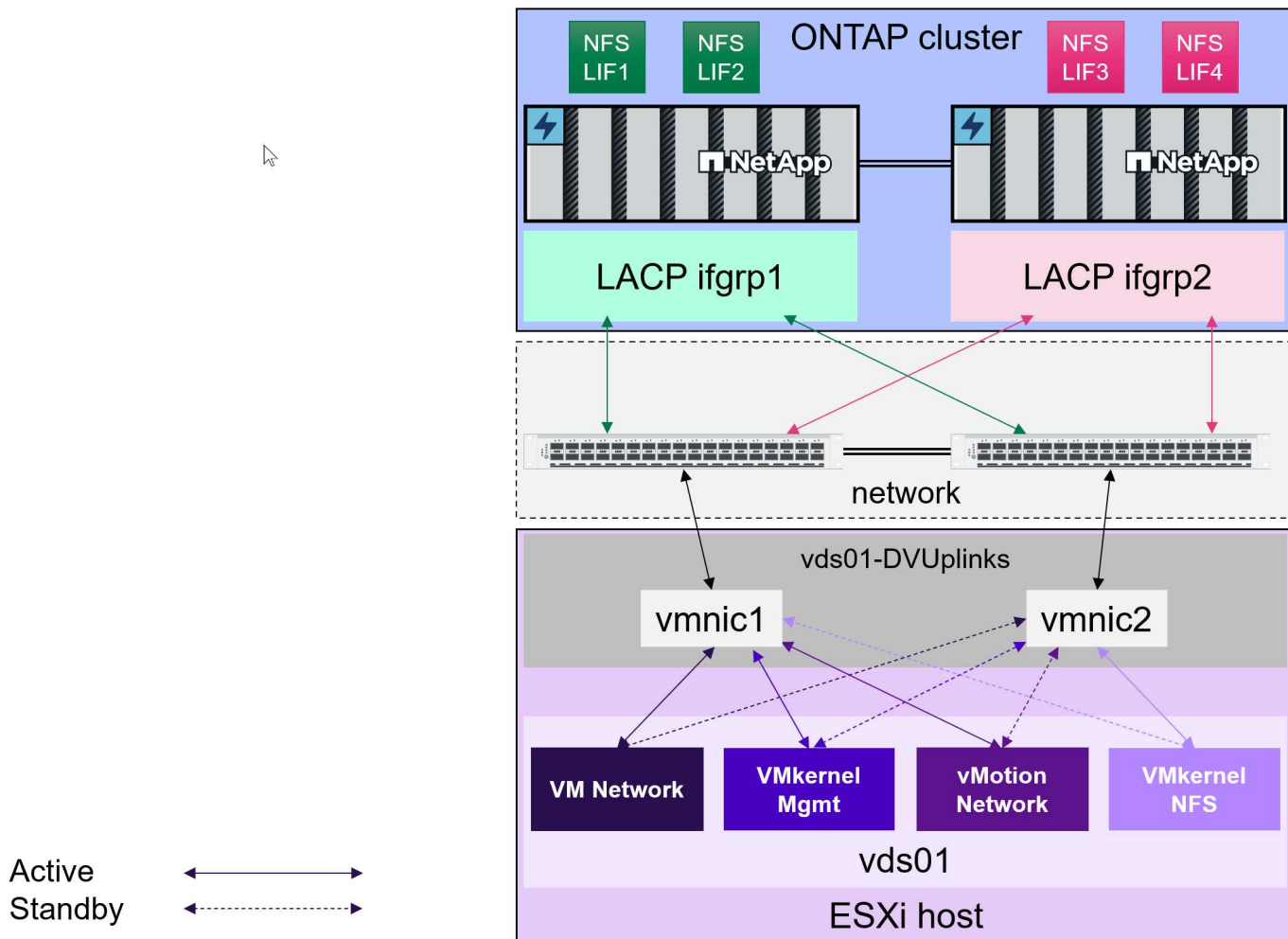
最大IOPS首次在VASA Provider 7.1中推出、可用于将未知工作负载的IOPS限制为特定VVOR、以避免对其他更关键的工作负载产生影响。有关性能管理的详细信息、请参见表4。

*确保您具有足够的数据Lifs。*请参阅 "[部署Virtual Storage](#)"。

遵循所有协议最佳实践。

请参见NetApp和VMware针对您选择的协议提供的其他最佳实践指南。一般而言，除了上述情况外，没有任何其他变化。

*使用基于NFS v3*的Vvol的网络配置示例



在AFF、ASA、ASA R2和FAS系统上部署虚拟卷

请遵循以下最佳实践为虚拟机创建虚拟卷存储。

配置vols数据存储库涉及几个步骤。NetApp的ASA R2系统专为VMware工作负载而设计、可提供与传统ONTAP系统不同的用户体验。使用ASA R2系统时、ONTAP工具10.3或更高版本所需的设置步骤更少、并且包含针对新存储架构优化的UI扩展和REST API支持。

准备使用ONTAP工具创建虚拟卷存储库

如果您已经在使用ONTAP工具来管理、自动化和报告现有VMFS或基于NFS的传统存储、则可以跳过部署过程的前两个步骤。您还可以参考此完整说明["检查清单"](#)来部署和配置ONTAP工具。

1. 创建存储虚拟机 (SVM) 及其协议配置。请注意，ASA r2 系统可能不需要这样做，因为它们通常已经有一个用于数据服务的 SVM。您可以选择 NVMe/FC (仅限ONTAP工具 9.13)、NFSv3、NFSv4.1、iSCSI、FCP 或这些选项的组合。NVMe/TCP 和 NVMe/FC 也可与ONTAP工具 10.3 及更高版本配合使用，用于传统的 VMFS 数据存储。您可以使用ONTAP系统管理器向导或集群 shell 命令行。
 - "为SVM分配本地层(聚合)"适用于所有非ASA R2系统。
 - 对于每个交换机/网络结构连接、每个节点至少需要一个LIF。作为最佳实践、为每个节点创建两个或更多基于FCP、iSCSI或NVMe的协议。每个节点一个LIF足以支持基于NFS的卷、但此LIF应受LACP ifgroup保护。有关详细信息、请参见 ["配置文件配置概览"](#)和 ["将物理端口组合在一起以创建接口组"](#)。

- 如果您打算对租户 vCenter 使用 SVM 范围的凭据，则每个 SVM 至少需要一个管理 LIF。
- 如果您计划使用 SnapMirror，请确保您的源和目标 ["ONTAP 集群和 SVM 已建立对等关系"](#)。
- 对于非 ASA r2 系统，此时可以创建卷，但最佳实践是让 ONTAP 工具中的 *Provision Datastore* 向导创建它们。唯一的例外是，如果您计划将 vVols 复制与 VMware Site Recovery Manager 和 ONTAP 工具 9.13 一起使用。使用已存在的 FlexVol 卷和已建立的 SnapMirror 关系，设置起来会更容易。请注意不要在任何用于 vVols 的卷上启用 QoS，因为这将由 SPBM 和 ONTAP 工具进行管理。

2. ["部署适用于 VMware vSphere 的 ONTAP 工具"](#) 使用从 NetApp 支持站点下载的 OVA。

- ONTAP tools 10.0 及更高版本支持每个设备运行多个 vCenter 服务器；您不再需要为每个 vCenter 部署一个 ONTAP tools 设备。
 - 如果您计划将多个 vCenter 连接到单个 ONTAP 工具实例，则必须创建并安装 CA 签名的证书。请参阅 ["管理证书"](#) 步骤如下。
- 从 10.3 版本开始，ONTAP 工具现在可以部署为单节点小型设备，适用于大多数非 vVols 工作负载。



- 推荐的最佳实践是 ["横向扩展 ONTAP 工具"](#) 10.3 及更高版本对所有生产工作负载采用 3 节点高可用性 (HA) 配置。对于实验室或测试目的，可以使用单节点部署。
- 生产环境中使用 vVols 的最佳实践建议是消除任何单点故障。创建反亲和性规则，防止 ONTAP 工具虚拟机在同一主机上同时运行。初始部署之后，还建议使用存储 vMotion 将 ONTAP 工具 VM 放入不同的数据存储中。了解更多 ["在不使用 vSphere DRS 的情况下使用关联规则"](#) 或者 ["创建 VM-VM 关联性规则"](#)。您还应该安排定期备份，和/或 ["使用内置配置备份实用程序"](#)。

1. 为您的环境配置 ONTAP 工具 10.3。

- ["添加 vCenter Server 实例"](#) 在 ONTAP 工具管理器 UI 中。
- ONTAP 工具 10.3 支持安全多租户。如果您不需要安全多租户、只需转到 vCenter 中的 ONTAP 工具菜单、单击 `_Storage Backends_` 并单击 `_add_` 按钮即可 ["添加 ONTAP 集群"](#)。
- 在要将特定 Storage Virtual Machine (SVM) 委派给特定 vCenter 的安全多租户环境中、您必须执行以下操作。
 - 登录到 ONTAP 工具管理器用户界面
 - ["载入存储集群"](#)
 - ["将存储后端与 vCenter Server 实例相关联"](#)
 - 向 vCenter 管理员提供特定的 SVM 凭据，管理员随后会将 SVM 添加为 vCenter 中 ONTAP 工具存储后端菜单中的存储后端。



- 最佳做法是为存储帐户创建 RBAC 角色。
- ONTAP 工具包含一个 JSON 文件，其中包含 ONTAP 工具存储帐户所需的必要角色权限。您可以将 JSON 文件上传到 ONTAP 系统管理器，以简化 RBAC 角色和用户的创建。
- 有关 ONTAP RBAC 角色的详细信息，请参见 ["配置 ONTAP 用户角色和权限"](#)。



之所以需要在 ONTAP 工具管理器 UI 中对整个集群进行配置，是因为用于 vVols 的许多 API 仅在集群级别可用。

使用ONTAP工具创建虚拟卷存储库

右键单击要创建ONTAP 数据存储库的主机、集群或数据中心、然后选择_ VMware tools _>_ Provision DataData 存储 库_。

The screenshot shows the 'Create datastore' dialog box with the 'Type' step selected. The left sidebar lists five steps: 1 Type, 2 Name and protocol, 3 Storage, 4 Storage attributes, and 5 Summary. The main area is titled 'Type' and contains the following fields:

- Destination:** Cluster-01
- Datastore type:** Three radio buttons are present: NFS (unselected), VMFS (unselected), and vVols (selected).

- 选择"vols"并提供有意义的名称、然后选择所需协议。您也可以提供数据存储库的问题描述。
 - ONTAP Tools 10.3与ASA R2。

The screenshot shows the 'Create datastore' dialog box with the 'Name and protocol' step selected. The left sidebar lists five steps: 1 Type, 2 Name and protocol, 3 Storage, 4 Storage attributes, and 5 Summary. The main area is titled 'Name and protocol' and contains the following fields:

- Datastore name:** vVols_Datastore
- Protocol:** iSCSI

- 选择ASA R2系统SVM、然后单击_n机_。

Create datastore

- 1 Type
- 2 Name and protocol
- 3 Storage
- 4 Summary

Storage

Choose a storage VM where the datastore will be created.

	Storage VM name	Tier	Platform type	QoS configured
<input type="radio"/>	rtp-a400-c02 / svm_iscsi	Performance	AFF	No
<input type="radio"/>	rtp-a400-c02 / svm_cluster	Performance	AFF	No
<input checked="" type="radio"/>	rtp-a1k-c01 / svm1	Performance	ASA r2	No

Manage Columns 3 Storage VMs

Advanced options

• 单击_Finish_

Create datastore

- 1 Type
- 2 Name and protocol
- 3 Storage
- 4 Summary

Summary

A new datastore will be created with these settings.

Type

Destination: Cluster-01
Datastore type: v vols

Name

Datastore name: vVols_Datastore
Protocol: iSCSI

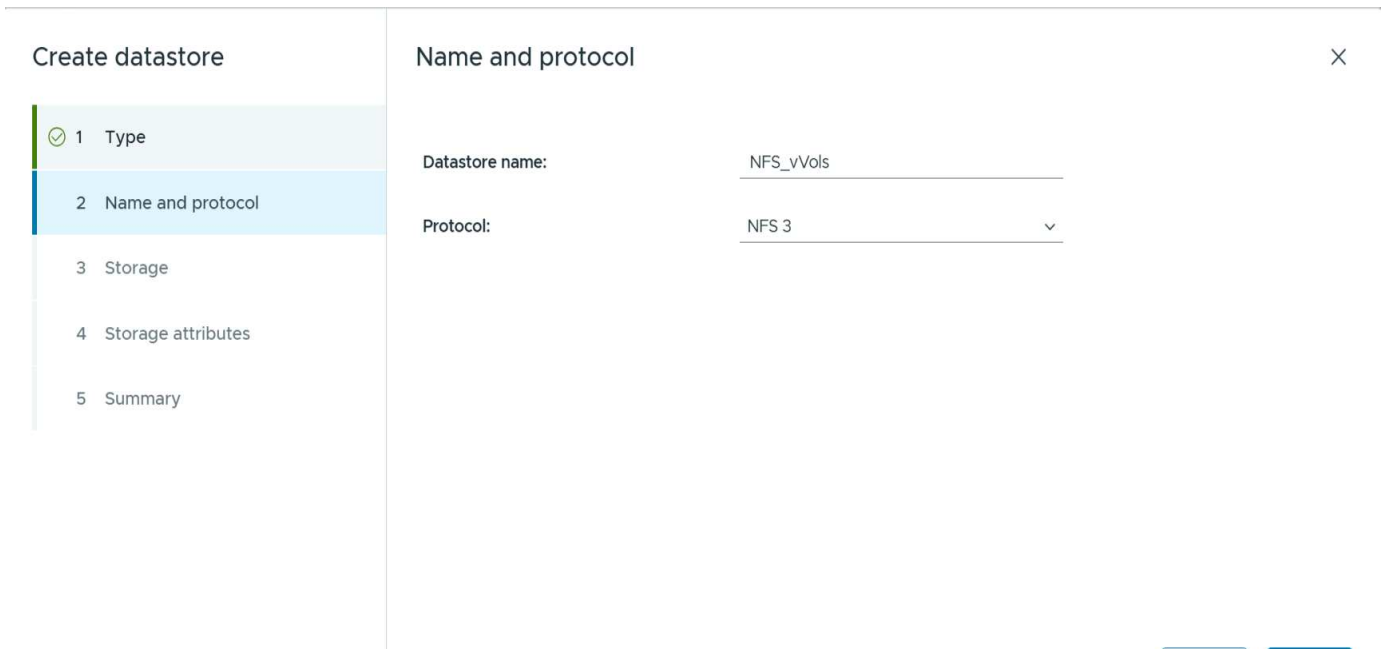
Storage

Storage VM: rtp-a1k-c01/svm1

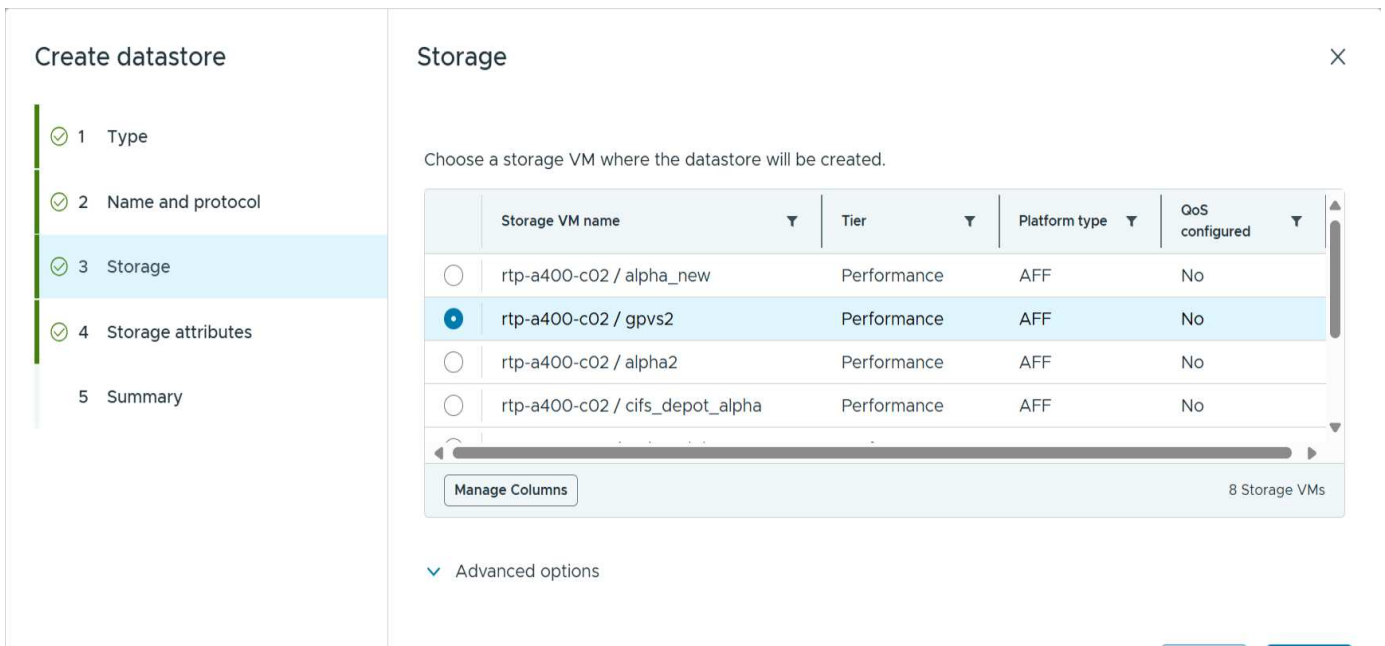
• 就是这么简单!

◦ ONTAP工具 10.3, 以及ASA r2 之前的ONTAP FAS、AFF和ASA。

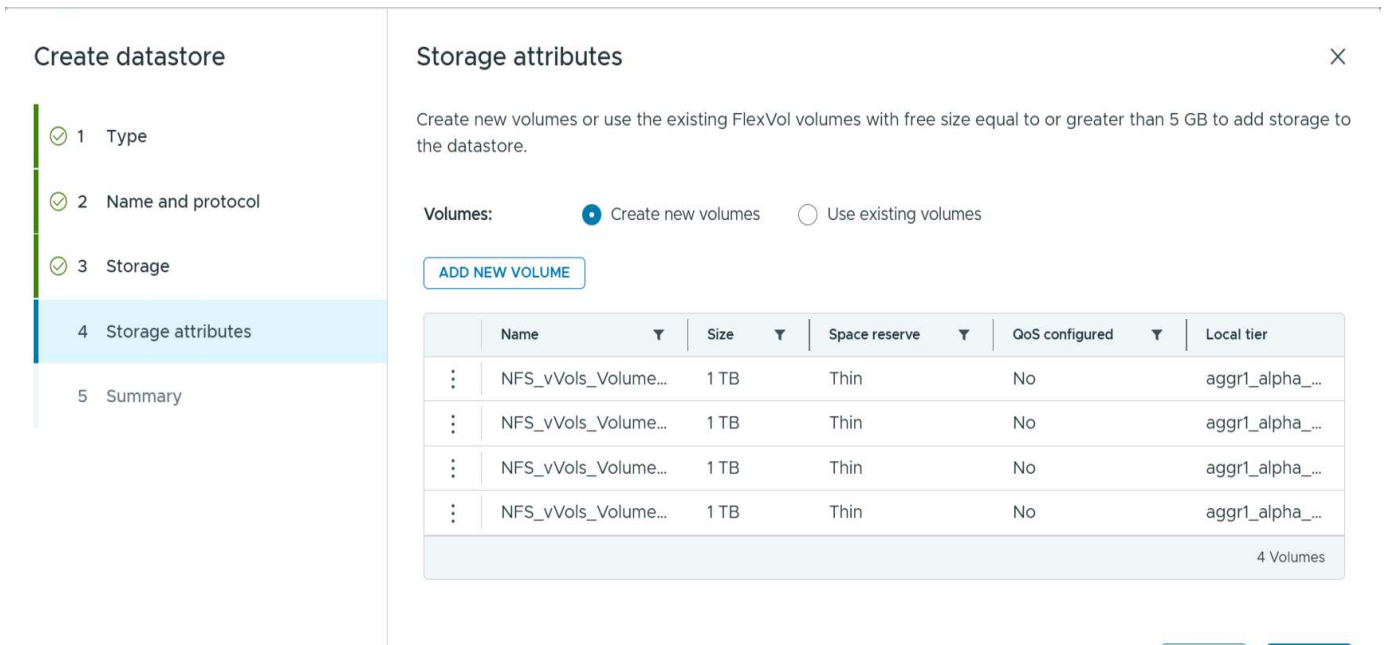
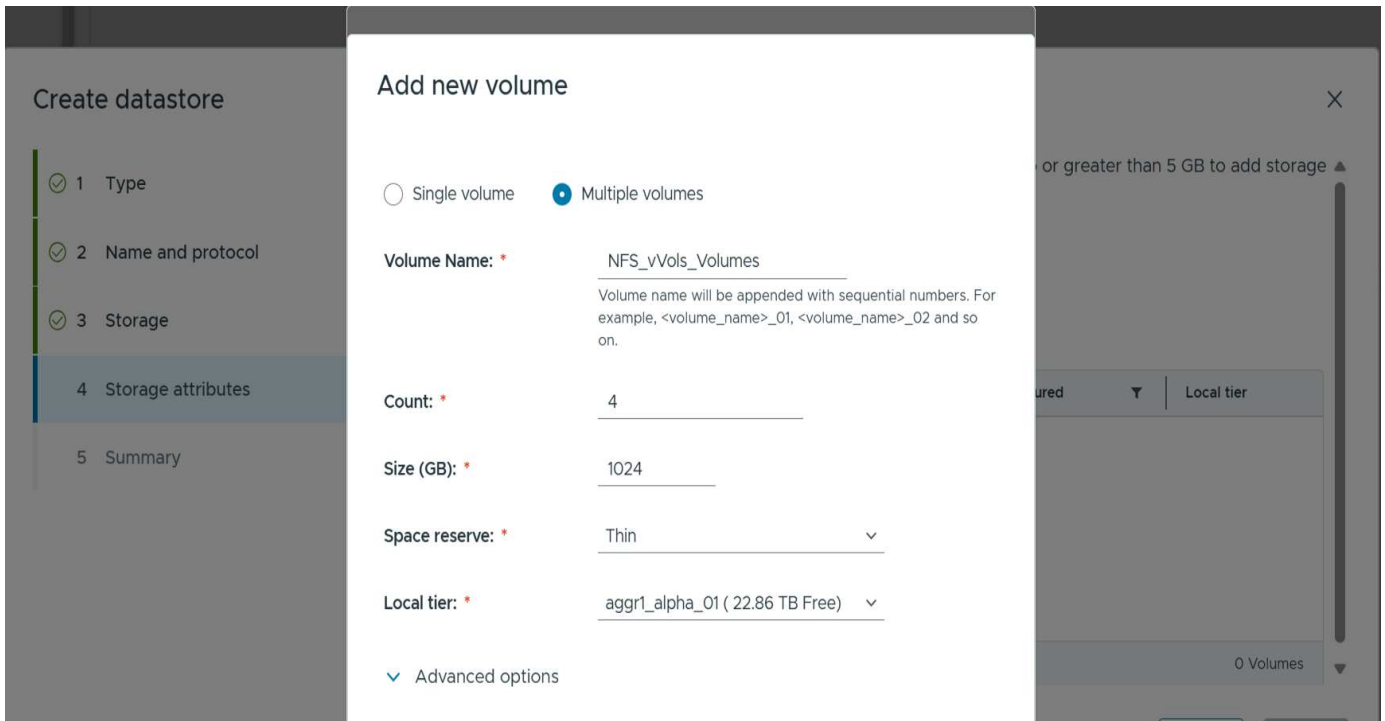
• 选择协议



- 选择SVM并单击_nXT。



- 单击“添加新卷”或“使用现有卷”，然后指定属性。请注意，在ONTAP工具 10.3 中，您可以同时请求创建多个卷。您还可以手动添加多个卷，以在ONTAP集群中实现卷的平衡。点击“下一步”



• 单击_Finish_

Create datastore

- 1 Type
- 2 Name and protocol
- 3 Storage
- 4 Storage attributes
- 5 Summary

Summary

A new datastore will be created with these settings.

Type

Destination: Cluster-01
Datastore type: v vols

Name

Datastore name: NFS_vVols
Protocol: NFS 3

Storage

Storage VM: rtp-a400-c02/gpvs2

Storage attributes

Create volumes

- 您可以在数据存储库的配置选项卡的ONTAP工具菜单中查看已分配的卷。

Volume name	Local tier	Thin provisioned	Space utilized (%)	vVols count	QoS configured
NFS_vVols_Volumes_01	aggr1_alpha_01	Yes	0%		No
NFS_vVols_Volumes_04	aggr1_alpha_01	Yes	0%		No
NFS_vVols_Volumes_03	aggr1_alpha_01	Yes	0%		No
NFS_vVols_Volumes_02	aggr1_alpha_01	Yes	0%	1	No

- 现在、您可以从vCenter UI中的_policies and Profile _菜单创建虚拟机存储策略。

将VM从传统数据存储库迁移到Vvol

将VM从传统数据存储库迁移到Vvol数据存储库就像在传统数据存储库之间移动VM一样简单。只需选择虚拟机、然后从操作列表中选择迁移、并选择迁移类型_change storage only"。出现提示时、选择与您的Vvol数据存储库匹配的VM存储策略。对于SAN VMFS到Vvol的迁移、可以使用vSphere 6.0及更高版本卸载迁移副本操作、但不能从NAS VMDK卸载到Vvol。

使用策略管理VM

要实现基于策略的存储配置自动化，您需要创建与所需存储功能相对应的虚拟机存储策略。



与先前版本一样、ONTAP工具10.0及更高版本不再使用存储功能配置文件。而是直接在VM存储策略本身中定义存储功能。

正在创建VM存储策略

在 vSphere 中，虚拟机存储策略用于管理可选功能，例如存储 I/O 控制或 vSphere 加密。它们还与vVols一起使用，以便为虚拟机应用特定的存储功能。使用“ NetApp ”存储类型。有关使用ONTAP工具 VASA Provider 的示例，请参阅链接：[vmware-vvols-ontap.html#Best Practices\[使用 NFS v3 上的vVols进行网络配置的示例\]](#)。“ NetApp.clustered.Data. ONTAP.VP.VASA10”存储的规则将与非基于 vVols 的数据存储一起使用。

创建存储策略后、即可在配置新VM时使用该策略。

VM Storage Policies

CREATE

Quick Filter Enter value

Name	vc
<input type="checkbox"/> VM Encryption Policy	vcf-vc01.ontappmtme.openenglab.netapp.com
<input type="checkbox"/> vSAN Default Storage Policy	vcf-vc01.ontappmtme.openenglab.netapp.com
<input type="checkbox"/> vVol No Requirements Policy	vcf-vc01.ontappmtme.openenglab.netapp.com
<input type="checkbox"/> Management Storage Policy - Regular	vcf-vc01.ontappmtme.openenglab.netapp.com
<input type="checkbox"/> Management Storage policy - Thin	vcf-vc01.ontappmtme.openenglab.netapp.com
<input type="checkbox"/> Management Storage Policy - Large	vcf-vc01.ontappmtme.openenglab.netapp.com
<input type="checkbox"/> Management Storage Policy - Stretched	vcf-vc01.ontappmtme.openenglab.netapp.com
<input type="checkbox"/> Management Storage Policy - Stretched Lite	vcf-vc01.ontappmtme.openenglab.netapp.com
<input type="checkbox"/> Management Storage Policy - Single Node	vcf-vc01.ontappmtme.openenglab.netapp.com
<input type="checkbox"/> Management Storage policy - Encryption	vcf-vc01.ontappmtme.openenglab.netapp.com
<input type="checkbox"/> Host-local PMem Default Storage Policy	vcf-vc01.ontappmtme.openenglab.netapp.com
<input type="checkbox"/> vSAN ESA Default Policy - RAIDS	vcf-vc01.ontappmtme.openenglab.netapp.com
<input type="checkbox"/> vSAN/ESA Default Policy - RAIDS	vcf-vc01.ontappmtme.openenglab.netapp.com

Deselect All

Create VM Storage Policy

- 1 Name and description
- 2 Policy structure
- 3 Storage compatibility
- 4 Review and finish

Create VM Storage Policy

- 1 Name and description
- 2 Policy structure
- 3 NetApp.clustered.Data.ONTAP.VP.vvol rules
- 4 Storage compatibility
- 5 Review and finish

Name and description

vCenter Server: VCF-VC01.ONTAPPMTME.OPENENGLAB.NETAPP.COM

Name: NetApp VM Storage Policy

Description:

Policy structure

Host based services

Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc. Host based services will be applied in addition to any datastore specific rules.

Enable host based rules

Datastore specific rules

Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.

Enable rules for "vSAN" storage

Enable rules for "vSANDirect" storage

Enable rules for "VMFS" storage

Enable rules for "NetApp.clustered.Data.ONTAP.VP.vvol" storage

Enable tag based placement rules

Tanzu on vSphere Storage topology

Create a Zonal rule for storage topology that will be applied to all other datastore-specific rules in this storage policy.

Enable Zonal topology for multi-zone Supervisor

Create VM Storage Policy

- 1 Name and description
- 2 Policy structure
- 3 **NetApp.clustered.Data.ONTAP.VP.vvol rules**
- 4 Storage compatibility
- 5 Review and finish

NetApp.clustered.Data.ONTAP.VP.vvol rules

×

Placement Tags

Platform Type ⓘ AFF

Tier ⓘ Performance

Space Efficiency ⓘ Thin

ADD RULE ▾

QoS IOPS

Create VM Storage Policy

- 1 Name and description
- 2 Policy structure
- 3 **NetApp.clustered.Data.ONTAP.VP.vvol rules**
- 4 Storage compatibility
- 5 Review and finish

NetApp.clustered.Data.ONTAP.VP.vvol rules

×

Placement Tags

Platform Type ⓘ AFF

Tier ⓘ Performance

Space Efficiency ⓘ Thin

QoS IOPS ⓘ

REMOVE

MaxThroughput IOPS ⓘ 10000

MinThroughput IOPS ⓘ 1000

Create VM Storage Policy

- 1 Name and description
- 2 Policy structure
- 3 NetApp.clustered.Data.ONTAP.VP.vvol rules
- 4 **Storage compatibility**
- 5 Review and finish

Storage compatibility

×

COMPATIBLE INCOMPATIBLE

Expand datastore clusters

Compatible storage 4 TB (3.8 TB free)

Quick Filter

Name	Datacenter	Type	Free Space	Capacity	Warnings
 NFS_vVols	Raleigh	vVol	3.80 TB	4.00 TB	

Create VM Storage Policy

- 1 Name and description
- 2 Policy structure
- 3 NetApp.clustered.Data.ONTAP.VP.vvol rules
- 4 Storage compatibility
- 5 Review and finish

Review and finish X

General

Name	NetApp VM Storage Policy
Description	
vCenter Server	vcf-vc01.ontappmtme.openenglab.netapp.com

NetApp.clustered.Data.ONTAP.VP.vvol rules

Placement

Platform Type	AFF
Tier	Performance
Space Efficiency	Thin
QoS IOPS	
MaxThroughput IOPS	10,000
MinThroughput IOPS	1,000

CANCEL BACK FINISH

使用ONTAP工具进行性能管理

ONTAP工具使用自己的平衡放置算法将新的VVOI放置在VVOI数据存储库中具有统一或经典ASA系统的最佳FlexVol volume中、或者具有ASA R2系统的存储可用性区域(Storage Availability Zone、SAZ)中。放置取决于后备存储与VM存储策略的匹配。这样可以确保数据存储库和后备存储满足指定的性能要求。

更改性能功能（例如最小和最大 IOPS）需要注意具体的配置。

- 可以在VM策略中指定*最小和最大IOX*。
 - 更改策略中的 IOPS 不会改变vVols上的 QoS，直到将 VM 策略重新应用到使用该策略的 VM。或者，您可以创建一个具有所需 IOPS 的新策略，并将其应用于目标虚拟机。一般来说，建议为不同的服务层级定义单独的虚拟机存储策略，然后在虚拟机上更改虚拟机存储策略即可。
 - ASA、ASA r2、AFF和FAS人格类型具有不同的 IOP 设置。所有闪光灯系统都支持最小和最大 IOP 设置；但是，非AFF系统只能使用最大 IOP 设置。
- ONTAP 工具使用当前支持的ONTAP 版本创建单个非共享QoS策略。因此、每个单独的VMDK都将收到自己分配的IOPS。

正在重新应用虚拟机存储策略

VM Storage Policies

CREATE CHECK EDIT CLONE **REAPPLY** DELETE

Filter

<input type="checkbox"/>	Name	VC
<input type="checkbox"/>	Management Storage Policy - Large	vm-is-vcenter01.vtme.netapp.com
<input type="checkbox"/>	VVol No Requirements Policy	vm-is-vcenter01.vtme.netapp.com
<input type="checkbox"/>	Management Storage Policy - Stretched Lite	vm-is-vcenter01.vtme.netapp.com
<input type="checkbox"/>	VM Encryption Policy	vm-is-vcenter01.vtme.netapp.com
<input type="checkbox"/>	Management Storage policy - Encryption	vm-is-vcenter01.vtme.netapp.com
<input type="checkbox"/>	Management Storage Policy - Single Node	vm-is-vcenter01.vtme.netapp.com
<input type="checkbox"/>	Management Storage policy - Thin	vm-is-vcenter01.vtme.netapp.com
<input checked="" type="checkbox"/>	AFF_ISCSI_VMSP	vm-is-vcenter01.vtme.netapp.com
<input type="checkbox"/>	Host-local PMem Default Storage Policy	vm-is-vcenter01.vtme.netapp.com
<input checked="" type="checkbox"/>	1	

14 items

保护卷

以下各节概述了将VMware vvol与ONTAP存储结合使用的过程和最佳实践。

VASA Provider高可用性

NetApp VASA Provider与vCenter插件和REST API服务器(以前称为Virtual Storage Console [VSC])以及Storage Replication Adapter一起作为虚拟设备的一部分运行。如果VASA Provider不可用、则使用vvol的VM将继续运行。但是、无法创建新的vvol数据存储库、也无法创建vvol或将其绑定到vSphere。这意味着、由于vCenter无法请求创建交换vVol、因此无法启动使用vVol的VM。并且正在运行的VM无法使用vMotion迁移到其他主机、因为vvol无法绑定到新主机。

VASA Provider 7.1及更高版本支持一些新功能、可确保服务在需要时可用。它包括用于监控VASA Provider和集成数据库服务的新监视程序进程。如果检测到故障、则会更新日志文件、然后自动重新启动服务。

vSphere管理员必须使用与保护其他任务关键型VM免受软件、主机硬件和网络故障影响相同的可用性功能来配置进一步的保护。要使用这些功能、无需对虚拟设备进行其他配置；只需使用标准vSphere方法进行配置即可。它们已通过测试、并受NetApp支持。

vSphere High Availability可轻松配置为在发生故障时在主机集群中的另一主机上重新启动虚拟机。vSphere Fault Tolerance可通过创建一个持续复制并可随时接管的二级虚拟机来提高可用性。有关这些功能的追加信息、请参见 ["适用于VMware vSphere的ONTAP 工具文档\(为ONTAP 工具配置高可用性\)"](#)以及VMware vSphere文档(请在ESXi和vCenter Server下查找vSphere可用性)。

ONTAP 工具VASA Provider会自动实时将vvol配置备份到托管ONTAP 系统、其中vvol信息存储在FlexVol 卷元数据中。如果ONTAP 工具设备因任何原因而不可用、您可以轻松快速地部署新设备并导入配置。有关VASA Provider恢复步骤的详细信息、请参见此知识库文章：

["如何执行VASA Provider灾难恢复—解决方案指南"](#)

卷复制

许多ONTAP 客户使用NetApp SnapMirror将其传统数据存储库复制到二级存储系统、然后在发生灾难时使用二

级系统恢复单个VM或整个站点。在大多数情况下、客户会使用软件工具来管理此问题、例如适用于VMware vSphere的NetApp SnapCenter插件等备份软件产品或VMware Site Recovery Manager等灾难恢复解决方案(以及ONTAP工具中的存储复制适配器)。

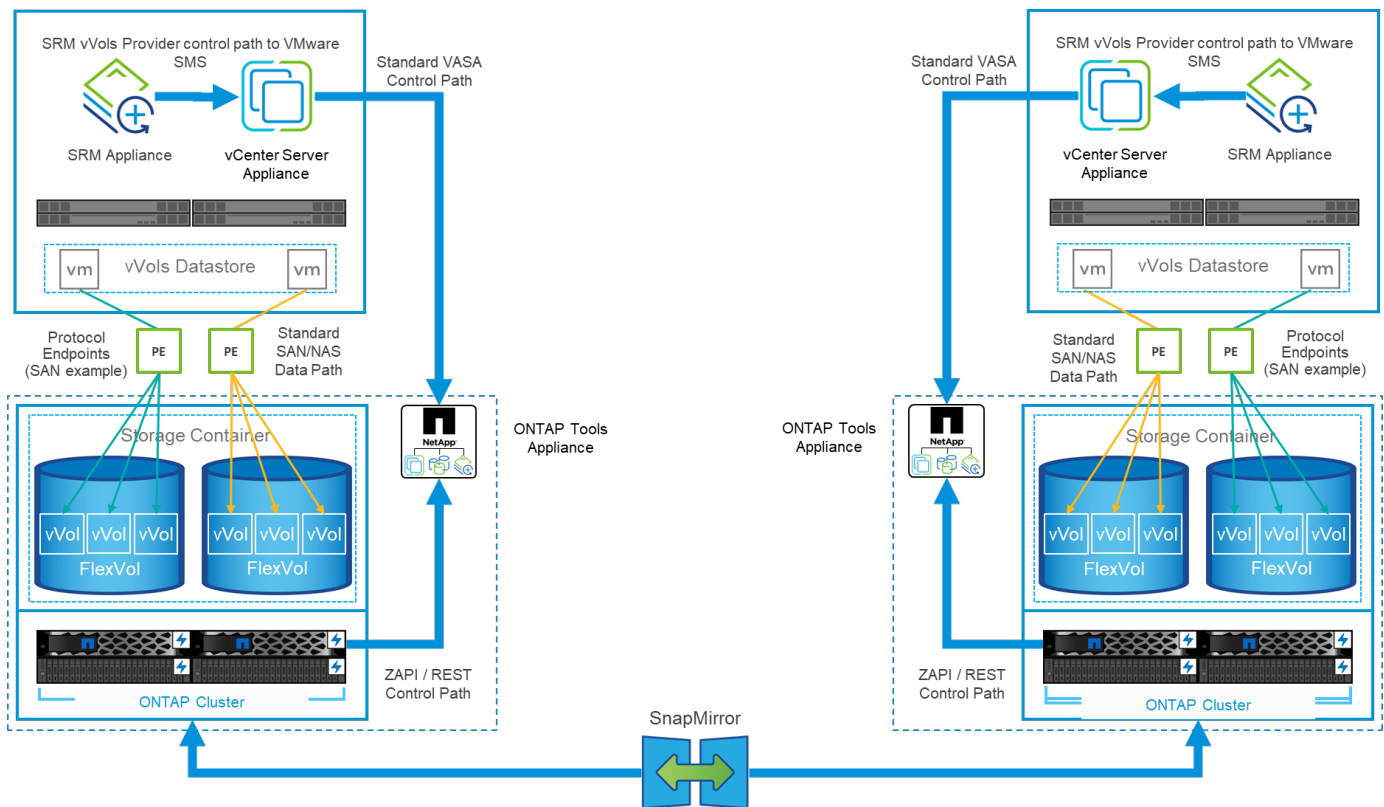
这种对软件工具的要求对于管理vols复制更为重要。虽然某些方面可以通过本机功能进行管理(例如、由VMware管理的vvol快照会卸载到使用快速、高效的文件或LUN克隆的ONTAP)、但通常需要通过业务流程来管理复制和恢复。有关vvol的元数据受ONTAP和VASA Provider保护、但要在二级站点上使用这些元数据、需要进行额外处理。

ONTAP 工具9.7.1与VMware Site Recovery Manager (SRM) 8.3版结合使用、可利用NetApp SnapMirror技术增加对灾难恢复和迁移工作流程编排的支持。

在ONTAP SRM对的初始支持版本中、需要先预创建FlexVol卷并启用SnapMirror保护、然后再将其用作9.7.1数据存储的后备卷。从ONTAP 工具9.10开始、不再需要此过程。现在、您可以向现有备份卷添加SnapMirror保护、并更新VM存储策略、以便利用与SRM集成的灾难恢复和迁移流程编排及自动化功能、实现基于策略的管理。

目前、VMware SRM是NetApp支持的唯一适用于vvol的灾难恢复和迁移自动化解决方案、ONTAP 工具将检查是否存在已向vCenter注册的SRM 8.3或更高版本服务器、然后再允许您启用vvol复制。虽然可以利用ONTAP 工具REST API创建您自己的服务。

使用SRM进行的卷复制



MetroCluster 支持

虽然ONTAP 工具无法触发MetroCluster 切换、但它支持在统一vSphere Metro Storage Cluster (VMSC)配置中使用NetApp MetroCluster 系统作为Vvol的后备卷。MetroCluster 系统的切换将按常规方式进行。

虽然NetApp SnapMirror业务连续性(SM-BC)也可用作VMSC配置的基础、但Vvol目前不支持它。

有关NetApp MetroCluster 的详细信息、请参见以下指南：

["TR-4689 MetroCluster IP解决方案 架构和设计"](#)

["TR-4705 NetApp MetroCluster 解决方案 架构和设计"](#)

["VMware知识库2031038 NetApp MetroCluster 的VMware vSphere支持"](#)

《vCenter Server备份概述》

保护VM有多种方法、例如使用子系统内备份代理、将VM数据文件附加到备份代理或使用定义的API (如VMware VADP)。可以使用相同的机制来保护V卷、许多NetApp合作伙伴都支持VM备份、包括Vvol。

如前文所述、VMware vCenter管理的快照会卸载到节省空间的快速ONTAP 文件/LUN克隆。这些快照可用于快速手动备份、但受vCenter限制、最多不超过32个快照。您可以使用vCenter根据需要创建快照和还原。

从适用于VMware vSphere (SCV) 4.6的SnapCenter 插件开始、如果与ONTAP 工具9.10及更高版本结合使用、则可通过支持SnapMirror和SnapVault 复制的ONTAP FlexVol 卷快照为基于Vvol的VM添加崩溃状态一致的备份和恢复功能。每个卷最多支持1023个快照。SCV还可以使用SnapMirror和镜像存储策略在二级卷上存储更多快照、保留时间更长。

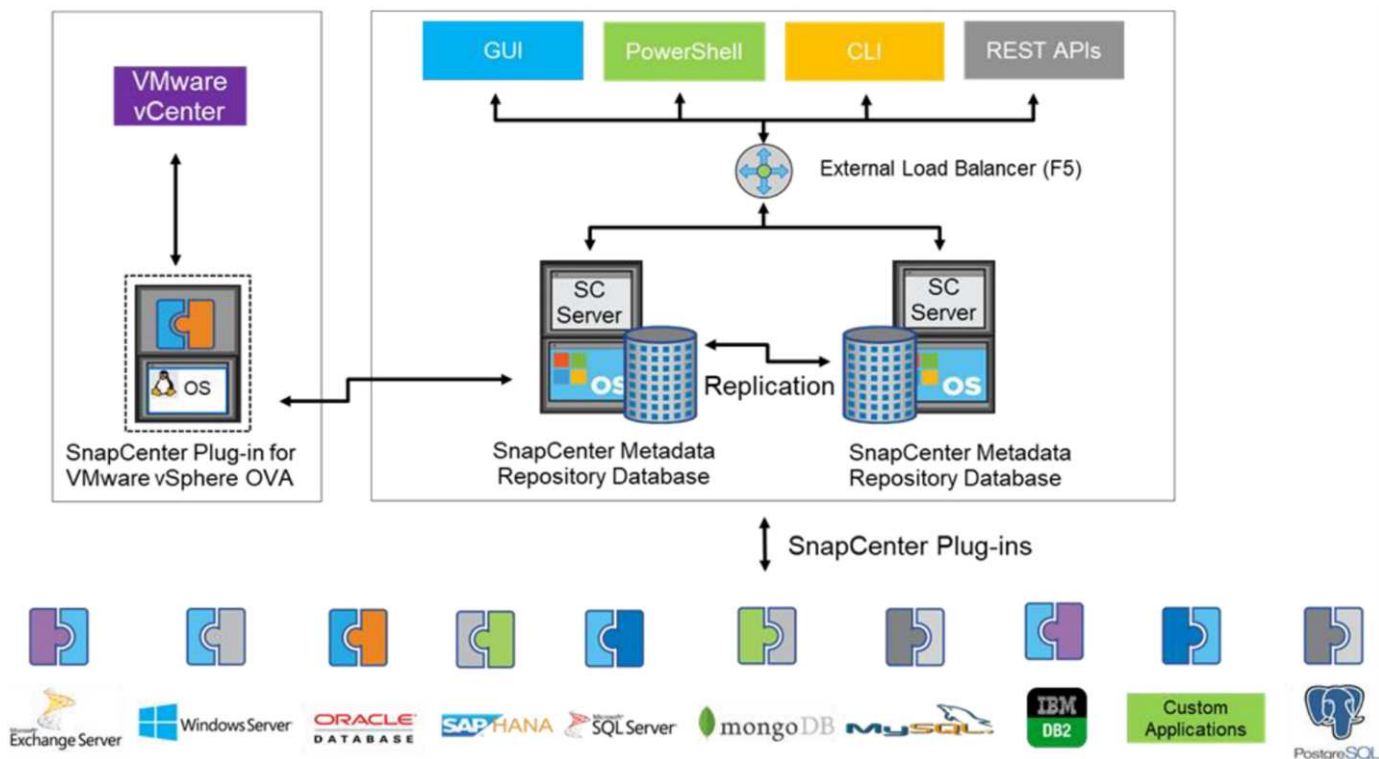
vSphere 8.0支持是在SCV 4.7中引入的、它使用一个隔离的本地插件架构。vSphere 8.0U1支持已添加到SCV 4.8中、并已完全过渡到新的远程插件架构。

适用于VMware vSphere的vvol Backup with SnapCenter 插件

现在、借助NetApp SnapCenter、您可以基于标记和/或文件夹为Vvol创建资源组、以便为基于Vvol的VM自动利用ONTAP基于FlexVol的快照。这样、您可以定义备份和恢复服务、当VM在环境中动态配置时、这些服务将自动保护VM。

适用于VMware vSphere的SnapCenter 插件部署为注册为vCenter扩展的独立设备、可通过vCenter UI或REST API进行管理、以实现备份和恢复服务自动化。

SnapCenter 架构



由于其他SnapCenter插件在撰写本文时尚不支持虚拟卷、因此我们将在本文档中重点介绍独立部署模式。

由于SnapCenter 使用ONTAP FlexVol 快照、因此vSphere不会产生任何开销、也不会像使用vCenter托管快照的传统VM那样对性能造成任何影响。此外、由于选择控制的功能通过REST API公开、因此可以使用VMware Aia Automation、Ansible、Terraform等工具以及几乎任何其他能够使用标准REST API的自动化工具轻松创建自动化工作流。

有关 SnapCenter REST API 的信息，请参见 ["REST API 概述"](#)

有关适用于 VMware vSphere 的 SnapCenter 插件 REST API 的信息，请参见 ["适用于 VMware vSphere 的 SnapCenter 插件 REST API"](#)

最佳实践

以下最佳实践可帮助您充分利用SnapCenter 部署。

- SCV同时支持vCenter Server RBAC和ONTAP RBAC、并包括预定义的vCenter角色、这些角色会在注册插件时自动为您创建。您可以阅读有关支持的RBAC类型的更多信息 ["此处"](#)。
 - 使用vCenter UI使用所述的预定义角色分配特权最低的帐户访问权限 ["此处"](#)。
 - 如果在SnapCenter 服务器中使用SCV，则必须分配_SnapCenterAdmin_角色。
 - ONTAP RBAC是指用于添加和管理SCV使用的存储系统的用户帐户。ONTAP RBAC不适用于基于虚拟卷的备份。阅读有关ONTAP RBAC和SCV的更多信息 ["此处"](#)。
- 使用SnapMirror将备份数据集复制到另一个系统、以创建源卷的完整副本。如前所述、您还可以使用镜像存储策略长期保留备份数据、而不受源卷快照保留设置的影响。这两种机制都支持使用这两种方法的卷。

- 由于SCV还需要适用于VMware vSphere的ONTAP 工具来实现Vvol功能、因此请始终查看NetApp互操作性表工具(IMT)以了解特定版本的兼容性
- 如果要将vvol复制与VMware SRM结合使用、请注意策略RPO和备份计划
- 使用符合组织定义的恢复点目标(Recovery Point目标、Recovery Point目标、RPO)的保留设置设计备份策略
- 在资源组上配置通知设置、以便在备份运行时收到状态通知(请参见下面的图10)

资源组通知选项

Edit Resource Group

- ✓ 1. General info & notification
- ✓ 2. Resource
- ✓ 3. Spanning disks
- ✓ 4. Policies
- ✓ 5. Schedules
- ✓ 6. Summary

vCenter Server:

Name:

Description:

Notification:

Email send from:

Email send to:

Email subject:

Latest Snapshot name Enable _recent suffix for latest Snapshot Copy ⓘ

Custom snapshot format: Use custom name format for Snapshot copy

Note that the Plug-in for VMware vSphere cannot do the following:

使用这些文档开始使用选择控制阀

["了解适用于 VMware vSphere 的 SnapCenter 插件"](#)

["部署适用于 VMware vSphere 的 SnapCenter 插件"](#)

故障排除

追加信息 提供了多种故障排除资源。

NetApp 支持站点

除了有关NetApp虚拟化产品的各种知识库文章之外，NetApp支持站点还提供了一个方便的产品登录页面 "[适用于 VMware vSphere 的 ONTAP 工具](#)"。此门户可通过链接访问NetApp社区中的文章、下载内容、技术报告和VMware解决方案讨论。可从以下位置获取：

["_ NetApp 支持站点 _"](#)

有关其他解决方案 文档、请访问：

["VMware虚拟化NetApp解决方案，由Broadcom提供"](#)

产品故障排除

ONTAP 工具的各种组件(例如vCenter插件、VASA Provider和Storage Replication Adapter)都记录在NetApp文档库中。但是、每个都有一个单独的知识库子部分、并且可能具有特定的故障排除过程。这些说明解决了使用VASA Provider时可能遇到的最常见问题。

VASA Provider UI问题

有时、vCenter vSphere Web Client会遇到与Serenity组件相关的问题、从而导致无法显示适用于ONTAP的VASA Provider菜单项。请参见部署指南或本知识库中的解决VASA Provider注册问题 ["文章"](#)。

配置卷数据存储库失败

有时、在创建Vvol数据存储库时、vCenter服务可能会超时。要更正此错误、请重新启动vmware-sps服务、然后使用vCenter菜单("Storage"(存储)>"New DataStorage"(新建数据存储库)重新挂载Vvol数据存储库。此问题将在《管理指南》中的"使用vCenter Server 6.5配置Vvol数据存储库失败"一节中进行介绍。

升级Unified Appliance无法挂载ISO

由于vCenter中的错误、用于将Unified Appliance从一个版本升级到下一个版本的ISO可能无法挂载。如果ISO能够连接到vCenter中的设备、请按照本知识库中的过程进行操作 ["文章"](#) 以解决此问题。

采用ONTAP的VMware Site Recovery Manager

使用ONTAP进行VMware实时站点恢复

自二十多年前 ESX 引入现代数据中心以来，ONTAP一直是 VMware vSphere 以及最近的 Cloud Foundation 的领先存储解决方案。NetApp不断推出创新系统，例如最新一代ASA A 系列，以及SnapMirror主动同步等功能。这些进步简化了管理，增强了弹性，并降低了IT 基础设施的总拥有成本 (TCO)。

本文档介绍了适用于 VMware Live Site Recovery (VLSR)（以前称为 Site Recovery Manager (SRM)，VMware 业界领先的灾难恢复 (DR) 软件）的ONTAP解决方案，包括最新产品信息和最佳实践，以简化部署、降低风险并简化持续管理。



本文档取代了之前发布的技术报告《TR-4900：使用 ONTAP 的 VMware Site Recovery Manager》

最佳实践是指南和兼容性工具等其他文档的补充。它们是根据 NetApp 工程师和客户的实验室测试和丰富的现场经验开发的。在某些情况下，建议的最佳实践可能不适合您的环境；但是，它们通常是最简单的解决方案，可满足大多数客户的需求。

本文档重点介绍与适用于VMware vSphere 10.4的ONTAP工具(包括NetApp存储复制适配器[SRA]和VASA Provider [VP])以及VMware Live Site Recovery 9结合使用时、ONTAP 9最新版本中的功能。

为什么要将**ONTAP**与甚量卷请求或**SRM**结合使用？

由ONTAP提供支持的NetApp数据管理平台是 VLSR 最广泛采用的存储解决方案之一。原因有很多：一个安全、高性能、统一协议（NAS 和 SAN 结合）的数据管理平台，提供行业定义的存储效率、多租户、服务质量控制、使用空间高效快照的数据保护以及使用SnapMirror的复制。所有这些都利用原生混合多云集成来保护 VMware 工作负载，并提供大量自动化和编排工具。

当您使用SnapMirror进行基于阵列的复制时，您可以利用 ONTAP 最成熟、最成熟的技术之一。SnapMirror为您提供安全、高效的数据传输优势，仅复制更改的文件系统块，而不是整个虚拟机或数据存储区。即使这些块也利用了空间节省功能，例如重复数据删除、压缩和压缩。现代ONTAP系统现在使用与版本无关的SnapMirror，让您灵活地选择源集群和目标集群。SnapMirror确实已成为最强大的灾难恢复工具之一。

无论您使用的是传统的 NFS、iSCSI 还是光纤通道连接的数据存储（现在支持vVols数据存储），VLSR 都能提供强大的第一方产品，利用ONTAP的最佳功能进行灾难恢复或数据中心迁移规划和编排。

VLSR 如何利用 ONTAP 9

VLSR 可通过与适用于 VMware vSphere 的 ONTAP 工具集成来利用 ONTAP 系统的高级数据管理技术，VMware vSphere 是一种虚拟设备，其中包括三个主要组件：

- 无论您使用的是SAN还是NAS、ONTAP工具vCenter插件(以前称为虚拟存储控制台(VSC))均可简化存储管理和效率功能、提高可用性并降低存储成本和运营开销。它使用最佳实践配置数据存储库，并为 NFS 和块存储环境优化 ESXi 主机设置。为了获得所有这些优势、在将vSphere与运行ONTAP的系统结合使用时、NetApp建议使用此插件。
- ONTAP工具VASA Provider支持VMware vStorage APIs for Storage Aware (VASA)框架。VASA Provider 可将 vCenter Server 与 ONTAP 连接起来，以帮助配置和监控 VM 存储。这样、便可支持VMware虚拟卷(vvol)并管理VM存储策略和单个VM vvol性能。此外，它还提供警报，用于监控容量以及配置文件合规性。
- SRA 与 VLSR 结合使用，用于管理传统 VMFS 和 NFS 数据存储库的生产站点和灾难恢复站点之间的 VM 数据复制，并用于无中断测试灾难恢复副本。它有助于自动执行发现，恢复和重新保护任务。它既包含一个SRA服务器设备、又包含用于Windows SRM服务器和vrr设备的SRA适配器。

在 VLSR 服务器上安装并配置 SRA 适配器以保护非 vVols 数据存储区后，您可以开始配置 vSphere 环境以进行灾难恢复的任务。

SRA为VSR服务器提供了一个命令和控制界面、用于管理包含VMware虚拟机(VM)的ONTAP FlexVol卷以及对其进行保护的SnapMirror复制。

VLSR 可以使用 NetApp 专有的FlexClone技术无中断地测试您的 DR 计划，以便在您的 DR 站点几乎即时地克隆受保护的数据存储。VLSR 创建了一个沙箱来进行安全测试，以便在发生真正的灾难时保护您的组织和客户，让您对组织在灾难期间执行故障转移的能力充满信心。

如果发生真正的灾难甚至是计划内迁移，VLSR 允许您通过最终 SnapMirror 更新（如果您选择这样做）向数据集发送任何最后一分钟的更改。然后，它会中断镜像并将数据存储库挂载到灾难恢复主机。此时，您可以根据预先规划的策略按任意顺序自动启动 VM 。



虽然ONTAP系统允许您将同一集群中的SVM配对以进行SnapMirror复制、但这种情况不会通过VLSR的测试和认证。因此、建议在使用VLSR时仅使用不同集群中的SVM。

采用 **ONTAP** 的 **VLSR** 以及其他使用情形：混合云和迁移

将 VLSR 部署与ONTAP高级数据管理功能相集成，与本地存储选项相比，可以大幅提高规模和性能。但更重要的是，它带来了混合云的灵活性。混合云可让您通过使用FabricPool将高性能阵列中未使用的数据块分层到您首选的超大规模器（可以是本地 S3 存储，例如NetApp StorageGRID）来节省资金。您还可以将SnapMirror用于基于边缘的系统，并使用软件定义的ONTAP Select或基于云的 DR "[Equinix Metal 上的NetApp存储](#)"或其他托管ONTAP服务。

借助FlexClone、您可以在云服务提供商的数据中心内执行测试故障转移、存储占用空间接近零。现在，保护您的组织的成本比以往任何时候都低。

VLSR 还可用于执行计划内迁移，方法是利用 SnapMirror 将 VM 从一个数据中心高效地传输到另一个数据中心，甚至在同一个数据中心内高效地传输 VM，无论您自己还是通过任意数量的 NetApp 合作伙伴服务提供商。

部署最佳实践

以下各节概述了ONTAP和VMware SRM的部署最佳实践。

使用最新版本的**ONTAP**工具10

与先前版本相比、ONTAP工具10提供了以下显著改进：

- 测试故障转移速度加快8倍*
- 清理和重新保护速度加快2倍*
- 故障转移速度加快32%*
- 扩展性更强
- 对共享站点布局的本机支持

*这些改进基于内部测试、可能因环境而异。

SMT 的 **SVM** 布局 and 分段

借助 ONTAP，Storage Virtual Machine（SVM）的概念可在安全多租户环境中提供严格的分段。一个 SVM 上的 SVM 用户无法从另一个 SVM 访问或管理资源。这样，您就可以利用 ONTAP 技术，为在同一集群上管理自己 SRM 工作流的不同业务单位创建单独的 SVM，从而提高整体存储效率。

请考虑使用 SVM 范围的帐户和 SVM 管理 LIF 管理 ONTAP，这样不仅可以改进安全控制，还可以提高性能。使用 SVM 范围的连接时，性能本身就会更高，因为处理整个集群中的所有资源（包括物理资源）并不需要 SRA。相反，它只需要了解抽象到特定 SVM 的逻辑资产。

管理 **ONTAP 9** 系统的最佳实践

如前所述，您可以使用集群或 SVM 范围的凭据和管理 LIF 来管理 ONTAP 集群。为了获得最佳性能、您可能需要考虑在不使用Vvol的情况下使用SVM范围的凭据。但是，在执行此操作时，您应了解一些要求，并且确实会丢失某些功能。

- 默认 vsadmin SVM 帐户没有执行 ONTAP 工具任务所需的访问级别。因此、您需要创建新的SVM帐户。 "[配置ONTAP用户角色和权限](#)"使用随附的JSON文件。这可以用于 SVM 或集群范围的帐户。
- 由于vCenter UI插件、VASA Provider和SRA服务器都是完全集成的微服务、因此您必须按照在适用于ONTAP的vCenter UI工具中添加存储的方式向SRM中的SRA适配器添加存储。否则， SRA 服务器可能无法识别通过 SRA 适配器从 SRM 发送的请求。
- 使用SVM范围的凭据时、不会执行NFS路径检查、除非首先 "[板载集群](#)"使用ONTAP工具管理器并将其与vCenter关联。这是因为物理位置从 SVM 中进行了逻辑抽象。不过，这并不是一个值得关注的发生原因，因为现代 ONTAP 系统在使用间接路径时不再出现任何明显的性能下降。
- 可能不会报告因存储效率而节省的聚合空间。
- 如果支持，则无法更新负载共享镜像。
- 可能不会在使用 SVM 范围的凭据管理的 ONTAP 系统上执行 EMS 日志记录。

操作最佳实践

以下各节概述了VMware SRM和ONTAP存储的最佳操作实践。

数据存储库和协议

- 如果可能，请始终使用 ONTAP 工具配置数据存储库和卷。这样可以确保卷， 接合路径， LUN ， igroup ， 导出策略， 以及其他设置均以兼容的方式进行配置。
- 通过 SRA 使用基于阵列的复制时， SRM 支持在 ONTAP 9 中使用 iSCSI ， 光纤通道和 NFS 版本 3 。对于使用传统或 VVol 数据存储库的 NFS 版本 4.1 ， SRM 不支持基于阵列的复制。
- 要确认连接，请始终验证您是否可以从目标 ONTAP 集群在灾难恢复站点挂载和卸载新的测试数据存储库。测试要用于数据存储库连接的每个协议。最佳做法是使用 ONTAP 工具创建测试数据存储库，因为它正在按照 SRM 的指示执行所有数据存储库自动化。
- 每个站点的 SAN 协议都应是同构的。您可以混合使用 NFS 和 SAN ， 但不应在站点内混合使用 SAN 协议。例如、您可以在站点A中使用FCP、而在站点B中使用iSCSI。您不应在站点A中同时使用FCP和iSCSI
- 之前的指南建议创建LIF以定位数据。也就是说，始终使用物理拥有卷的节点上的 LIF 挂载数据存储库。虽然这仍然是最佳实践、但在ONTAP 9的现代版本中、这不再是一项要求。如果给定了集群范围的凭据、则ONTAP工具仍会尽可能选择在数据本地的各个LUN之间进行负载平衡、但这并不是高可用性或高性能的要求。
- 可以将ONTAP 9配置为在自动调整大小无法提供足够的紧急容量时自动删除快照、以便在空间不足的情况下保持正常运行时间。此功能的默认设置不会自动删除由SnapMirror创建的快照。如果删除了SnapMirror快照、则NetApp SRA将无法反转和重新同步受影响卷的复制。要防止ONTAP删除SnapMirror快照、请将快照自动删除功能配置为"try"。

```
snap autodelete modify -volume -commitment try
```

- 对于包含SAN数据存储库的卷和NFS数据存储库、 `grow_shrink`` 应将卷自动调整设置为 ``grow`。有关此主题的更多信息，请访问"[将卷配置为自动增长和缩减其大小](#)"。
- 如果恢复计划中的数据存储库数量和保护组数量达到最低、则SRM的性能最佳。因此、您应考虑在受SRM保护的環境中优化虚拟机密度、在这种环境中、应使用最重要的是RTO。
- 使用Distributed Resource Scheduler (DRS)帮助平衡受保护和恢复ESXi集群上的负载。请记住、如果您计划故障恢复、则在运行重新保护时、先前受保护的集群将成为新的恢复集群。DRS将有助于平衡两个方向的

放置。

- 如有可能、请避免对SRM使用IP自定义、因为这会增加您的RTO。

关于阵列对

系统会为每个阵列对创建一个阵列管理器。使用 SRM 和 ONTAP 工具，每个阵列配对都在 SVM 的范围内完成，即使您使用的是集群凭据也是如此。这样，您可以根据租户分配给他们管理的 SVM 在租户之间划分灾难恢复工作流。您可以为一个给定集群创建多个阵列管理器、这些阵列管理器可以是非对称的。您可以在不同的 ONTAP 9 集群之间扇出或扇入。例如，可以将集群 1 上的 SVMA 和 SVM-B 复制到集群 2 上的 SVM-C，集群 3 上的 SVM-D，反之亦然。

在 SRM 中配置阵列对时，应始终按照将其添加到 ONTAP 工具的方式在 SRM 中添加这些阵列对，也就是说，它们必须使用相同的用户名，密码和管理 LIF。此要求可确保 SRA 与阵列正确通信。以下屏幕截图说明了集群在 ONTAP 工具中的显示方式以及如何将其添加到阵列管理器中。

The screenshot shows the vSphere Client interface. On the left is a navigation pane with 'Storage Systems' selected. The main area displays a table of storage systems:

Name	Type	IP Address
cluster2	Cluster	cluster2.demo.netapp.com

Below the table is a dialog box titled 'Edit Local Array Manager'. It contains the following fields:

- 'Enter a name for the array manager on "vc2.demo.netapp.com":' with the value 'vc2_array_manager'.
- 'Storage Array Parameters' section.
- 'Storage Management IP Address or Hostname' with the value 'cluster2.demo.netapp.com'.

A red arrow points from the IP address 'cluster2.demo.netapp.com' in the table to the 'Storage Management IP Address or Hostname' input field in the dialog box.

关于复制组

复制组包含同时恢复的虚拟机的逻辑集合。由于 ONTAP SnapMirror 复制是在卷级别进行的，因此卷中的所有 VM 都位于同一个复制组中。

对于复制组以及如何在 FlexVol 卷之间分布虚拟机，需要考虑几个因素。对于缺少聚合级重复数据删除的旧版 ONTAP 系统、将相似的 VM 分组在同一个卷中可以提高存储效率、但分组会增加卷的大小并减少卷 I/O 并行性。在现代 ONTAP 系统中、可以通过在同一聚合中的 FlexVol 卷之间分布虚拟机、从而利用聚合级重复数据删除并在多个卷之间实现更大的 I/O 并行处理能力、从而在性能和存储效率之间实现最佳平衡。您可以同时恢复卷中的 VM，因为一个保护组（如下所述）可以包含多个复制组。这种布局的缺点是、数据块可能会通过缆线多次传输、因为 SnapMirror 不会考虑聚合重复数据删除。

对于复制组，最后要考虑的一点是，每个复制组本身都是一个逻辑一致性组（不要与 SRM 一致性组相混淆）。这是因为卷中的所有 VM 都会使用同一个快照一起传输。因此，如果您的虚拟机必须彼此一致，请考虑将其存储在同一个 FlexVol 中。

关于保护组

保护组用于定义从受保护站点一起恢复的组中的 VM 和数据存储库。受保护站点是指在正常稳定状态操作期间，在保护组中配置的 VM 所在的站点。请务必注意，即使 SRM 可能会为一个保护组显示多个阵列管理器，一个保护组也不能跨越多个阵列管理器。因此，您不应将 VM 文件跨越不同 SVM 上的数据存储库。

关于恢复计划

恢复计划定义了在同一过程中恢复的保护组。可以在同一恢复计划中配置多个保护组。此外，要为执行恢复计划提供更多选项，可以在多个恢复计划中包含一个保护组。

通过恢复计划，SRM 管理员可以定义恢复工作流，方法是将 VM 分配给优先级组，优先级组从 1（最高）到 5（最低）不等，默认值为 3（中等）。在优先级组中，可以为 VM 配置依赖关系。

例如，您的公司可能拥有一个第1层业务关键型应用程序、该应用程序的数据库依赖于Microsoft SQL Server。因此，您决定将 VM 置于优先级组 1 中。在优先级组 1 中，您开始规划订单以启动服务。您可能希望Microsoft Windows域控制器在Microsoft SQL Server之前启动、而Microsoft SQL Server需要在应用程序服务器之前联机、依此类推。您可以将所有这些VM添加到优先级组、然后设置依赖关系、因为依赖关系仅适用于给定优先级组。

NetApp 强烈建议您与应用程序团队合作，了解故障转移场景中所需的操作顺序，并相应地构建恢复计划。

测试故障转移

作为最佳实践、每当对受保护VM存储的配置进行更改时、都应始终执行测试故障转移。这样可以确保在发生灾难时、您可以相信Site Recovery Manager可以在预期的Recovery目标范围内还原服务。

NetApp 还建议偶尔确认子系统中的应用程序功能，尤其是在重新配置 VM 存储之后。

执行测试恢复操作时，会在 ESXi 主机上为 VM 创建一个专用测试气泡网络。但是，此网络不会自动连接到任何物理网络适配器，因此不会在 ESXi 主机之间提供连接。为了允许在灾难恢复测试期间不同 ESXi 主机上运行的 VM 之间进行通信，在灾难恢复站点的 ESXi 主机之间创建了一个物理专用网络。要验证测试网络是否为专用网络，可以通过物理方式或使用 VLAN 或 VLAN 标记来隔离测试气泡网络。必须将此网络与生产网络隔离，因为在恢复 VM 后，不能将其放置在 IP 地址可能与实际生产系统冲突的生产网络上。在 SRM 中创建恢复计划时，可以选择创建的测试网络作为测试期间 VM 连接到的专用网络。

验证测试并使其不再需要后，请执行清理操作。运行清理会将受保护的 VM 恢复到其初始状态，并将恢复计划重置为就绪状态。

故障转移注意事项

除了本指南中所述的操作顺序之外，在对站点进行故障转移时还需要考虑其他几个注意事项。

您可能需要应对的一个问题描述是站点之间的网络差异。某些环境可能能够在主站点和灾难恢复站点使用相同的网络 IP 地址。此功能称为延伸型虚拟 LAN（VLAN）或延伸型网络设置。其他环境可能要求主站点使用与灾难恢复站点相对的不同网络 IP 地址（例如，在不同的 VLAN 中）。

VMware 提供了多种方法来解决此问题。例如，VMware NSX-T Data Center 等网络虚拟化技术可从操作环境中将整个网络堆栈从第 2 层抽象为第 7 层，从而提供更便携的解决方案。了解更多信息 "[SRM的NSX-T选项](#)"。

通过 SRM，您还可以在虚拟机恢复后更改其网络配置。此重新配置包括IP地址、网关地址和DNS服务器设置等设置。恢复计划中VM的属性设置中可以指定不同的网络设置、这些设置会在恢复后应用于各个VM。

要将 SRM 配置为对多个 VM 应用不同的网络设置，而无需编辑恢复计划中每个 VM 的属性，VMware 提供了一个名为 dr-ip-customizer 的工具。要了解如何使用此实用程序、请参见 ["VMware文档"](#)。

重新保护

恢复后，恢复站点将成为新的生产站点。由于恢复操作中断了 SnapMirror 复制，因此新生产站点不会受到任何未来灾难的影响。最佳实践是，在恢复后立即将新生产站点保护到另一站点。如果原始生产站点正常运行，VMware 管理员可以使用原始生产站点作为新的恢复站点来保护新生产站点，从而有效地反转保护方向。只有在发生非灾难性故障时，才可重新保护。因此，原始 vCenter Server，ESXi 服务器，SRM 服务器和相应的数据库最终必须可恢复。如果没有可用的保护组和新的恢复计划，则必须创建新的保护组和恢复计划。

故障恢复

从根本上说，故障恢复操作是指方向与以前不同的故障转移。作为最佳实践，在尝试故障恢复或换句话说，故障转移到原始站点之前，您应验证原始站点是否已恢复到可接受的功能级别。如果原始站点仍然受到影响，您应延迟故障恢复，直到故障得到充分修复为止。

另一个故障恢复最佳实践是，始终在完成重新保护之后以及执行最终故障恢复之前执行测试故障转移。此操作将验证原始站点上的系统是否可以完成此操作。

重新保护原始站点

在故障恢复之后、您应与所有利益相关方确认其服务已恢复正常、然后再再次运行重新保护。

在故障恢复后运行重新保护实际上会使环境恢复到最初的状态，同时重新运行从生产站点到恢复站点的 SnapMirror 复制。

复制拓扑

在 ONTAP 9 中，集群管理员可以看到集群的物理组件，但使用集群的应用程序和主机无法直接看到这些物理组件。物理组件提供了一个共享资源池，用于构建逻辑集群资源。应用程序和主机仅通过包含卷和 LIF 的 SVM 访问数据。

每个 NetApp SVM 在 Site Recovery Manager 中都被视为一个唯一阵列。VLSR 支持某些阵列到阵列（或 SVM 到 SVM）复制布局。

一个虚拟机不能在多个 VLSR 阵列上拥有虚拟机磁盘（Virtual Machine Disk，VMDK）或 RDM 数据，原因如下：

- VLSR 只能识别 SVM，而不能识别单个物理控制器。
- SVM 可以控制跨越集群中多个节点的 LUN 和卷。

最佳实践

要确定可支持性，请牢记以下规则：要使用 VLSR 和 NetApp SRA 保护 VM，VM 的所有部分都必须仅位于一个 SVM 上。此规则适用于受保护站点和恢复站点。

支持的 SnapMirror 布局

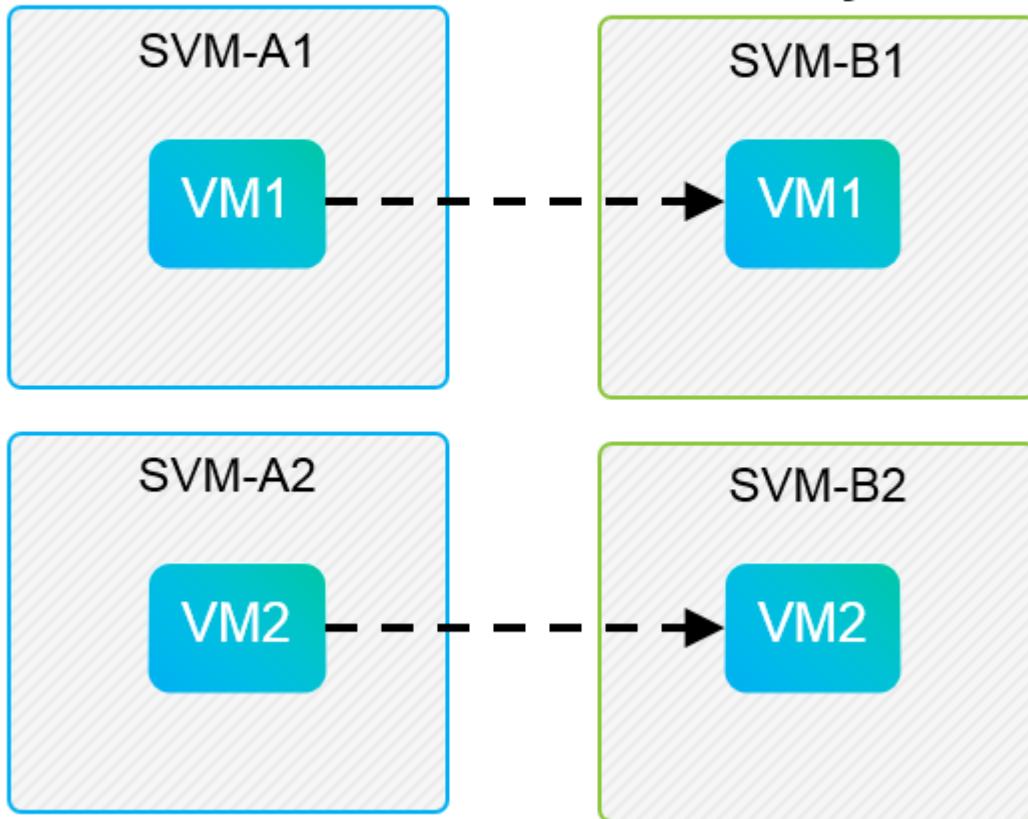
下图显示了 VLSR 和 SRA 支持的 SnapMirror 关系布局方案。复制卷中的每个 VM 在每个站点上仅拥有一个 VLSR 阵列（SVM）上的数据。

SnapMirror Replication



Protected Site

Recovery Site

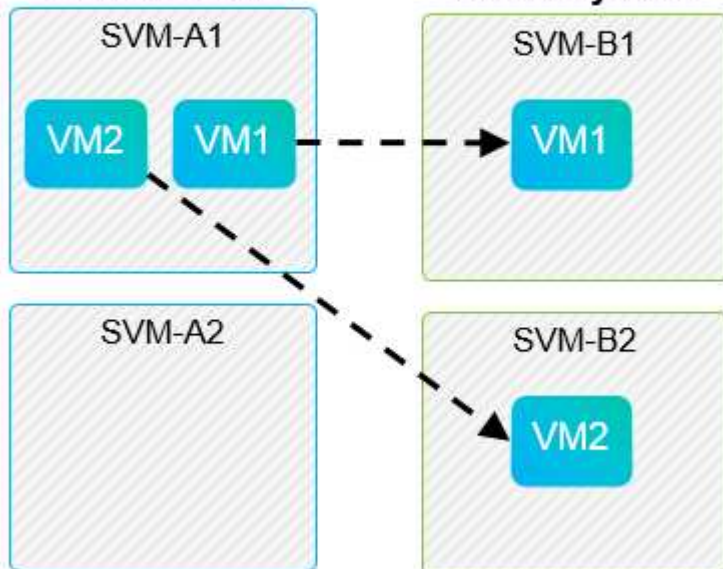


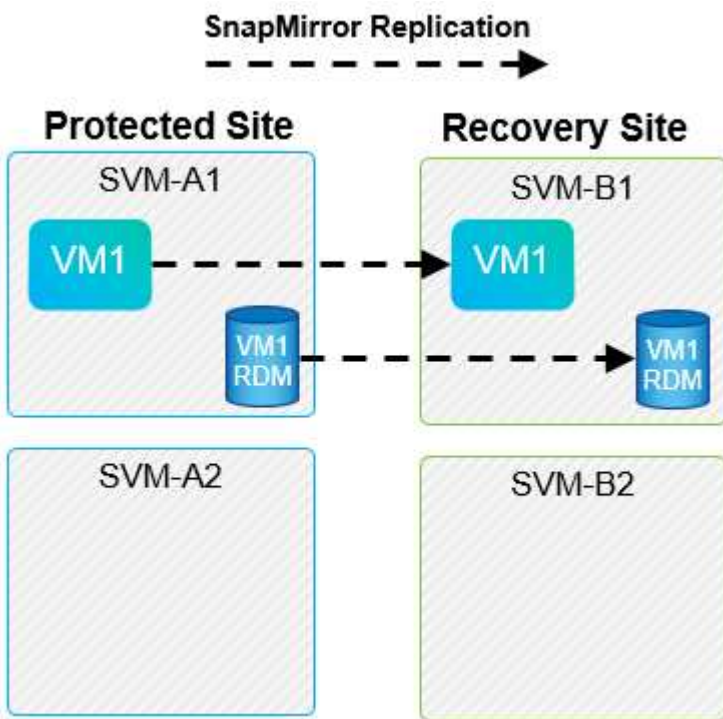
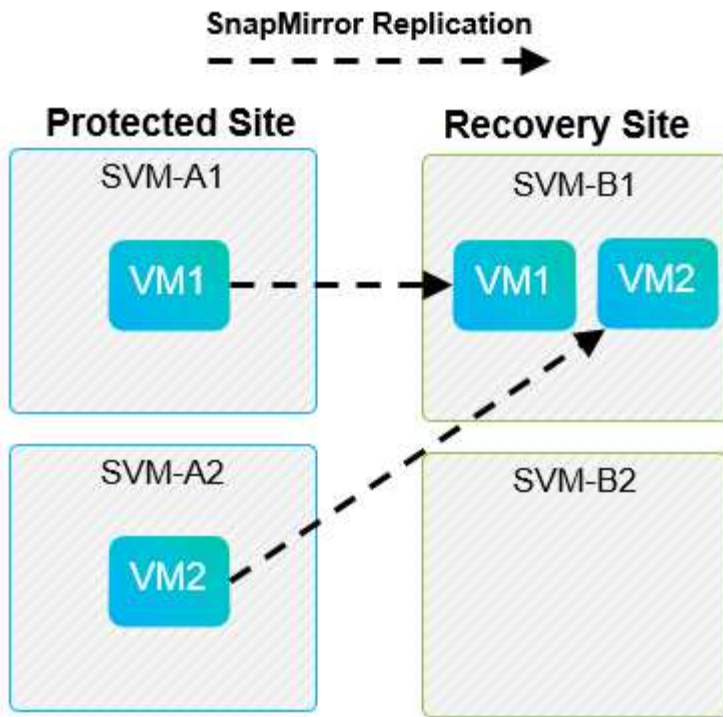
SnapMirror Replication



Protected Site

Recovery Site





VMFS 支持SnapMirror主动同步

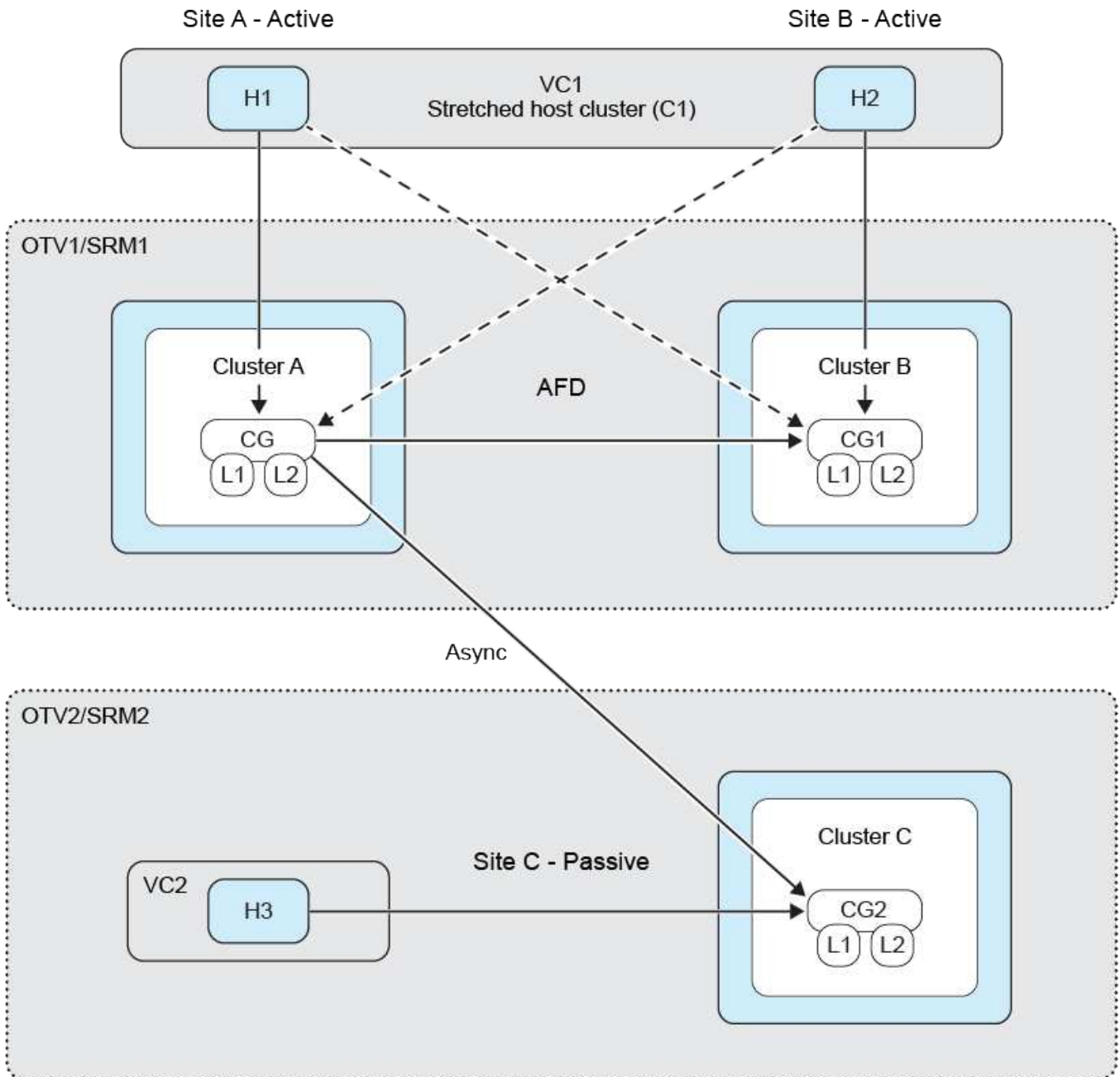
ONTAP工具 10.3 及更高版本还支持使用SnapMirror主动同步 (SMAs) 保护您的 VMFS 数据存储库。这使得两个相对较近的数据中心（称为故障域）之间的业务连续性能够实现透明的故障转移。然后可以通过带有 VLSR 的ONTAP工具 SRA 使用异步SnapMirror来协调远距离灾难恢复。

["了解ONTAP SnapMirror主动同步"](#)

数据存储区被收集在一个一致性组 (CG) 中，并且所有数据存储区的虚拟机都将作为同一 CG 的成员保持写入顺

序一致。

一些示例可能是柏林和汉堡的站点受 SMas 保护，第三个站点副本使用 SnapMirror 异步并受 VLSR 保护。另一个例子可能是使用 SMas 保护纽约和新泽西的站点，并保护芝加哥的第三个站点。



支持的阵列管理器布局

在 VLSR 中使用基于阵列的复制 (ABR) 时，保护组会隔离到一个阵列对中，如以下屏幕截图所示。在此场景中，`svm1` 和 `svm2` 与恢复站点上的和 `svm4` 建立对等关系 `svm3`。但是，在创建保护组时，您只能选择两个阵列对中的一个。

New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete

Type

Select the type of protection group you want to create:

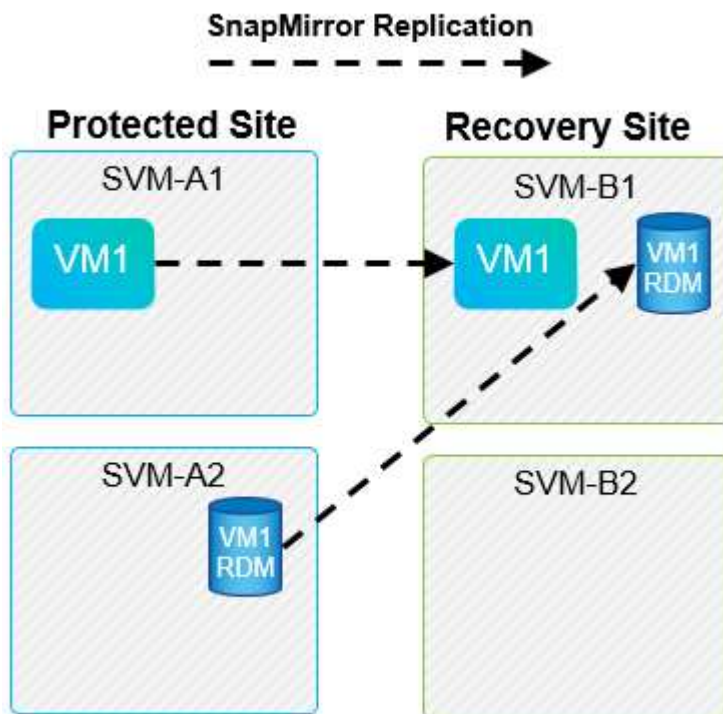
- Datastore groups (array-based replication)**
Protect all virtual machines which are on specific datastores.
- Individual VMs (vSphere Replication)**
Protect specific virtual machines, regardless of the datastores.
- Virtual Volumes (vVol replication)**
Protect virtual machines which are on replicated vVol storage.
- Storage policies (array-based replication)**
Protect virtual machines with specific storage policies.

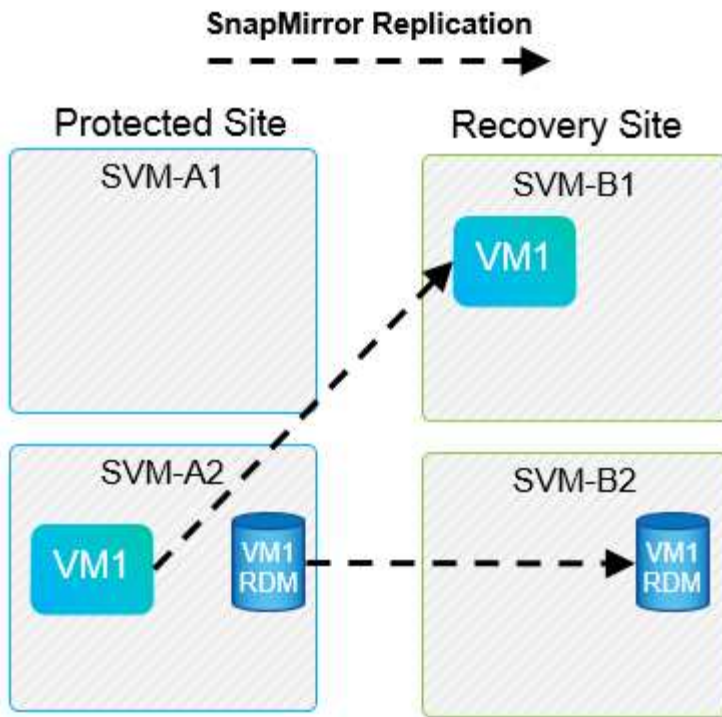
Select array pair

	Array Pair	Array Manager Pair
<input type="radio"/>	✓ cluster1:svm1 ↔ cluster2:svm2	vc1 array manager ↔ vc2 array manager
<input type="radio"/>	✓ cluster1:svm3 ↔ cluster2:svm4	vc1 trad datastores ↔ vc2 trad datastores

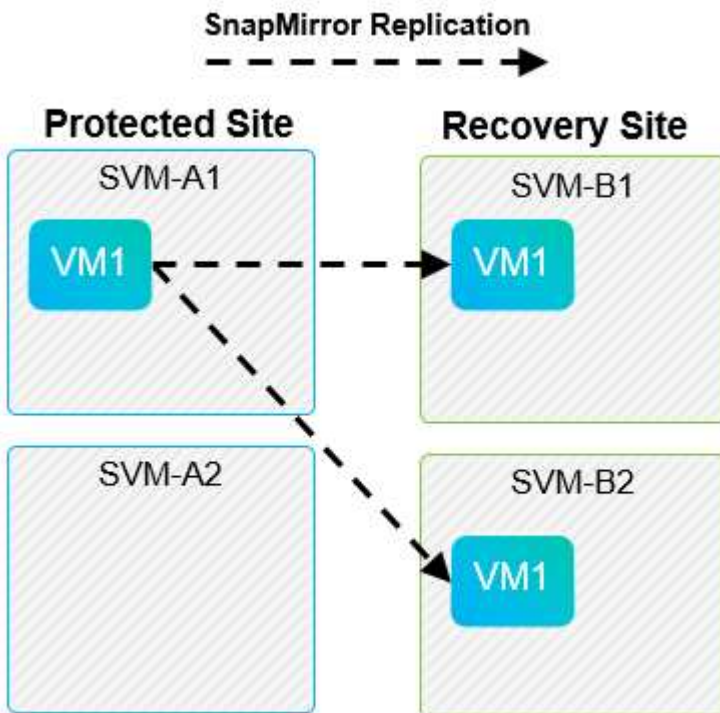
不支持的布局

不受支持的配置会在单个虚拟机所拥有的多个 SVM 上包含数据（VMDK 或 RDM）。在下图所示的示例中、`VM1`无法使用VSR配置保护、因为 `VM1`数据位于两个SVM上。



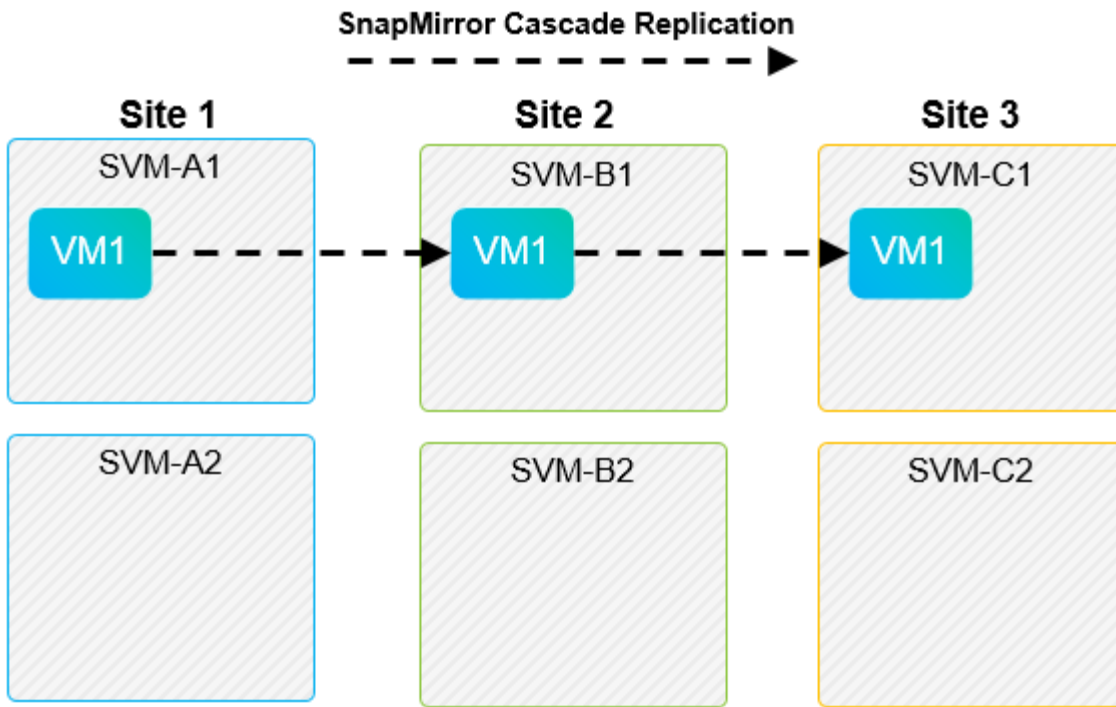


如果任何复制关系将单个 NetApp 卷从一个源 SVM 复制到同一 SVM 或不同 SVM 中的多个目标，则称为 SnapMirror 扇出。VLSR 不支持扇出。在下图所示的示例中，`VM1` 无法配置用于在虚拟卷访问请求中进行保护，因为它会使用 SnapMirror 复制到两个不同位置。



SnapMirror 级联

VLSR 不支持 SnapMirror 关系的级联，即，将源卷复制到目标卷，同时使用 SnapMirror 将目标卷复制到另一个目标卷。在下图所示的情形中，不能使用 VLSR 在任何站点之间进行故障转移。



SnapMirror 和 SnapVault

NetApp SnapVault 软件支持在 NetApp 存储系统之间对企业数据进行基于磁盘的备份。SnapVault 和 SnapMirror 可以同时位于同一环境中；但是，VLSR 仅支持 SnapMirror 关系的故障转移。



NetApp SRA支持 `mirror-vault` 策略类型。

SnapVault 是为 ONTAP 8.2 从头开始重建的。虽然以前的 Data ONTAP 7- 模式用户应该发现相似之处，但此版本的 SnapVault 已进行了重大改进。其中一项重大进步是，能够在 SnapVault 传输期间保持主数据的存储效率。

一个重要的架构变化是，ONTAP 9 中的 SnapVault 在卷级别进行复制，而不是像 7- 模式 SnapVault 那样在 qtree 级别进行复制。此设置意味着 SnapVault 关系的源必须为卷，并且该卷必须复制到 SnapVault 二级系统上其自身的卷。

在使用 SnapVault 的环境中、会在主存储系统上创建专门命名的快照。根据所实施的配置、可以通过 SnapVault 计划或 NetApp Active IQ Unified Manager 等应用程序在主系统上创建命名快照。然后、在主系统上创建的命名快照会复制到 SnapMirror 目标、并从该目标存储到 SnapVault 目标。

可以在级联配置中创建源卷，在级联配置中，卷会复制到灾难恢复站点中的 SnapMirror 目标，然后从该位置存储到 SnapVault 目标。也可以在扇出关系中创建源卷，其中一个目标是 SnapMirror 目标，另一个目标是 SnapVault 目标。但是，在发生 VLSR 故障转移或复制反转时，SRA 不会自动重新配置 SnapVault 关系以使用 SnapMirror 目标卷作为存储源。

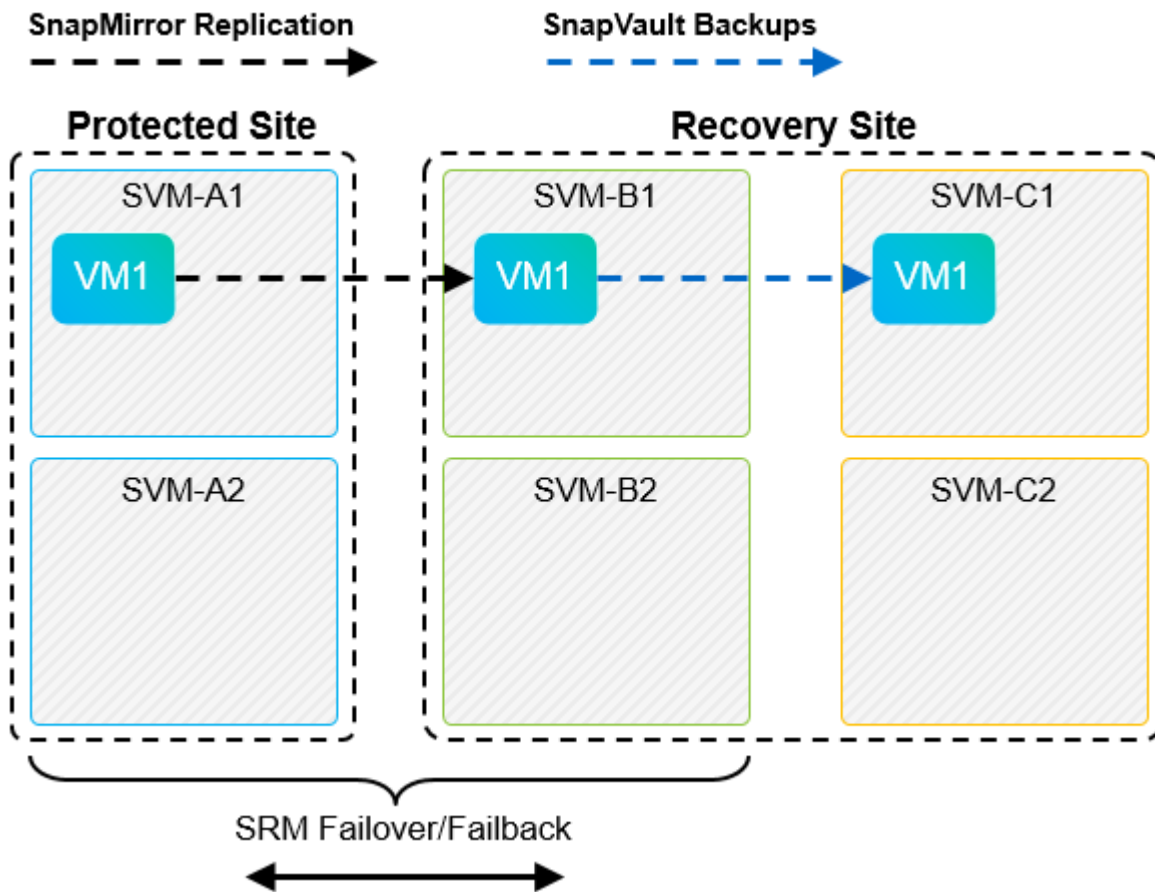
有关 ONTAP 9 的 SnapMirror 和 SnapVault 的最新信息，请参阅 ["TR-4015 《适用于 ONTAP 9 的 SnapMirror 配置最佳实践指南》](#)。

最佳实践

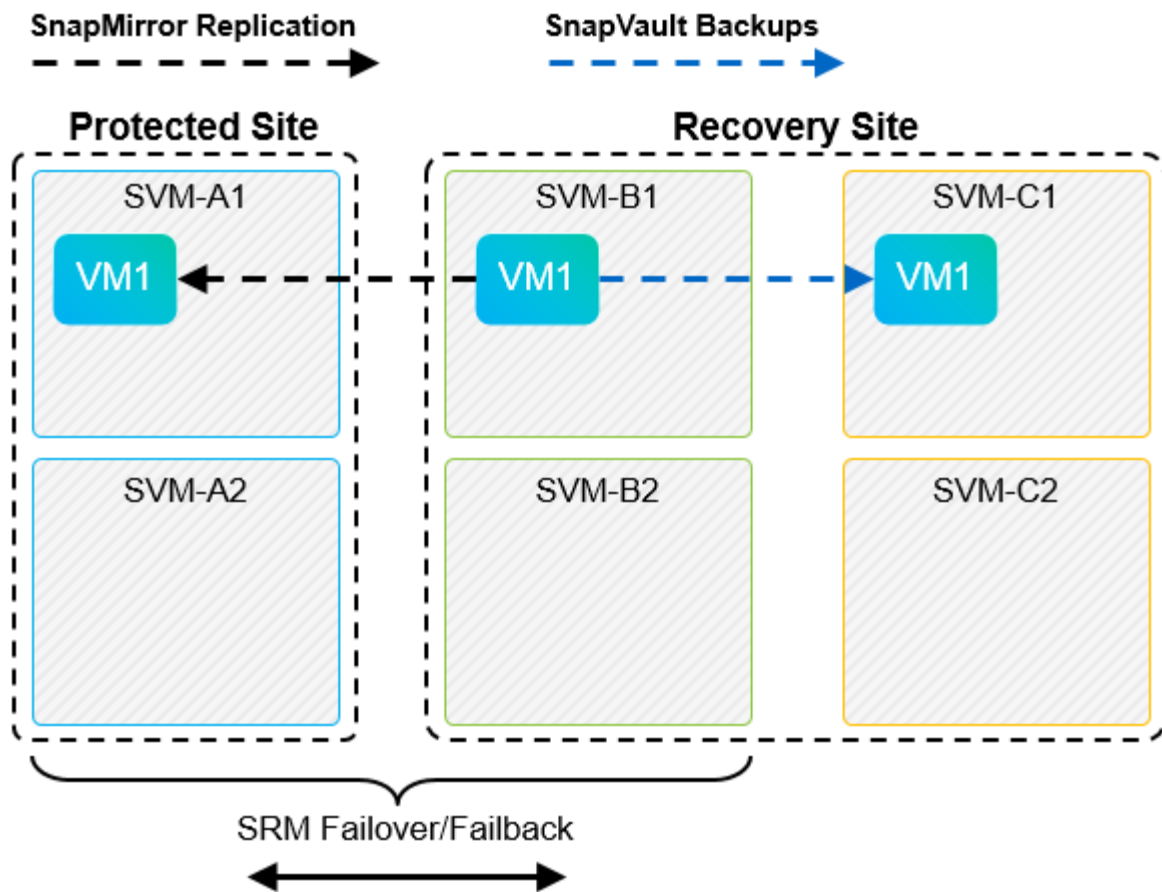
如果在同一环境中使用 SnapVault 和 VLSR，NetApp 建议使用 SnapMirror 到 SnapVault 级联配置，其中通常会从灾难恢复站点的 SnapMirror 目标执行 SnapVault 备份。发生灾难时，此配置会使主站点无法访问。通过将 SnapVault 目标保留在恢复站点上，可以在故障转移后重新配置 SnapVault 备份，以便在恢复站点上运行时可以继续执行 SnapVault 备份。

在 VMware 环境中，每个数据存储库都有一个通用唯一标识符（UUID），每个 VM 都有一个唯一的受管对象 ID（MOID）。在故障转移或故障恢复期间，VLSR 不会维护这些 ID。由于 VLSR 在故障转移期间不会维护数据存储库 UUID 和 VM MOID，因此，在 VLSR 故障转移后，必须重新配置依赖这些 ID 的所有应用程序。例如，NetApp Active IQ Unified Manager 可将 SnapVault 复制与 vSphere 环境进行协调。

下图显示了 SnapMirror 到 SnapVault 的级联配置。如果 SnapVault 目标位于灾难恢复站点或不受主站点中断影响的三级站点上，则可以重新配置环境，以便在故障转移后继续备份。



下图显示了使用 VLSR 将 SnapMirror 复制反转回主站点后的配置。此外，还对环境进行了重新配置，使 SnapVault 备份从现在的 SnapMirror 源进行。此设置为 SnapMirror SnapVault 扇出配置。



在vsrm执行故障恢复并再次反转SnapMirror关系后、生产数据将返回到主站点。现在，此数据将通过 SnapMirror 和 SnapVault 备份获得与故障转移到灾难恢复站点之前相同的保护方式。

在 Site Recovery Manager 环境中使用 qtree

qtrees是一种特殊目录、可用于为NAS应用文件系统配额。ONTAP 9 允许创建 qtree ，而 qtree 可以存在于使用 SnapMirror 复制的卷中。但是、SnapMirror不允许复制单个qtree或进行qtree级复制。所有 SnapMirror 复制仅在卷级别进行。因此，NetApp 不建议在 VLSR 中使用 qtree 。

FC 和 iSCSI 混合环境

借助支持的 SAN 协议（FC ， FCoE 和 iSCSI ）， ONTAP 9 可提供 LUN 服务，即创建 LUN 并将其映射到连接的主机。由于集群由多个控制器组成，因此，多路径 I/O 可管理多个逻辑路径，并将其连接到任何单个 LUN 。主机上使用非对称逻辑单元访问（ALUA），以便选择 LUN 的优化路径并使其处于活动状态以进行数据传输。如果指向任何 LUN 的优化路径发生变化（例如，由于移动了包含 LUN 的卷）， ONTAP 9 会自动识别此更改并无中断地进行调整。如果优化路径不可用， ONTAP 可以无中断地切换到任何其他可用路径。

VMware VLSR 和 NetApp SRA 支持在一个站点使用 FC 协议，而在另一个站点使用 iSCSI 协议。但是，不支持在同一 ESXi 主机或同一集群中的不同主机中混合使用 FC 连接的数据存储库和 iSCSI 连接的数据存储库。VLSR 不支持此配置，因为在 VLSR 故障转移或测试故障转移期间， VLSR 会在请求中包括 ESXi 主机中的所有 FC 和 iSCSI 启动程序。

最佳实践

VLSR 和 SRA 支持在受保护站点和恢复站点之间混合使用 FC 和 iSCSI 协议。但是，每个站点只能配置一个 FC 或 iSCSI 协议，而不能在同一站点上同时配置这两个协议。如果要求在同一站点同时配置 FC 和 iSCSI 协议，NetApp 建议某些主机使用 iSCSI，而其他主机使用 FC。在这种情况下，NetApp 还建议设置 VLSR 资源映射，以便将 VM 配置为故障转移到一组主机或另一组主机。

使用卷复制时对voISRM/SRM进行故障排除

使用ONTAP工具9.13P2时、使用vvol复制时、vSR和SRM中的工作流与使用SRA和传统数据存储库时的工作流明显不同。例如，没有阵列管理器概念。因此、`discoverarrays`和`discoverdevices`命令永远不会显示出来。

在进行故障排除时，了解下面列出的新工作流非常有用：

1. queryReplicationPeer：发现两个故障域之间的复制协议。
2. queryFaultDomain：发现故障域层次结构。
3. queryReplicationGroup：发现源域或目标域中的复制组。
4. syncReplicationGroup：同步源和目标之间的数据。
5. queryPointInTimeReplica：发现目标上的时间点副本。
6. testFailoverReplicationGroupStart：开始测试故障转移。
7. testFailoverReplicationGroupStop：结束测试故障转移。
8. promoteReplicationGroup：将当前正在测试的组提升为生产组。
9. prepareFailoverReplicationGroup：准备灾难恢复。
10. failoverReplicationGroup：执行灾难恢复。
11. reverseReplicateGroup：启动反向复制。
12. queryMatchingContainer：查找可能使用给定策略满足配置请求的容器（以及主机或复制组）。
13. queryResourceMetadata：从 VASA 提供程序中发现所有资源的元数据，资源利用率可以作为问题解答返回给 queryMatchingContainer 函数。

配置 VVOL 复制时，最常见的错误是无法发现 SnapMirror 关系。之所以出现这种情况，是因为卷和 SnapMirror 关系是在 ONTAP 工具的权限范围之外创建的。因此，最佳做法是，在尝试创建复制的 VVOL 数据存储库之前，始终确保 SnapMirror 关系已完全初始化，并且您已在两个站点的 ONTAP 工具中运行重新发现。

追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- 适用于VMware vSphere 10.x的ONTAP工具资源"<https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab>"
- 适用于VMware vSphere 9.x的ONTAP工具资源"<https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab>"
- TR-4597：适用于 ONTAP 的 VMware vSphere "<https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html>"

- TR-4400：采用 ONTAP 的 VMware vSphere 虚拟卷
["https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html"](https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html)
- TR-4015 ONTAP 9 SnapMirror配置最佳实践指南 <https://www.netapp.com/pdf.html?item=/media/17229-tr-4015-snapmirror-configuration-ontap.pdf>
- VMware Live Site Recovery文档["https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html"](https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html)

要验证您的特定环境是否支持本文档所述的确切产品和功能版本、请参见"互操作性表工具 (IMT)"NetApp支持站点上的。NetApp IMT 定义了可用于构建 NetApp 支持的配置的产品组件和版本。具体结果取决于每个客户是否按照已发布的规格进行安装。

采用ONTAP的vSphere Metro存储集群

采用ONTAP的vSphere Metro存储集群

VMware行业领先的vSphere虚拟机管理程序可部署为延伸型集群、称为vSphere Metro Storage Cluster (VMSC)。

NetApp@MetroCluster™和SnapMirror主动同步(以前称为SnapMirror业务连续性或SMBC)均支持VMSC解决方案，如果一个或多个故障域发生完全中断，则可以提供高级业务连续性。不同故障模式的故障恢复能力取决于您选择的配置选项。



本文档可替代先前发布的技术报告_TR-4128：《基于NetApp MetroCluster的vSphere》_

适用于vSphere环境的持续可用性解决方案

ONTAP架构是一个灵活且可扩展的存储平台，为数据存储提供 SAN (FCP、iSCSI 和 NVMe-oF) 和 NAS (NFS v3 和 v4.1) 服务。NetApp AFF、ASA和FAS存储系统使用ONTAP操作系统为客户存储访问提供附加协议，如 S3 和 SMB/CIFS。

NetApp MetroCluster使用NetApp的HA (控制器故障转移或CFO)功能来防止控制器发生故障。它还包括本地SyncMirror技术、灾难时集群故障转移(集群灾难故障转移或CFOD)、硬件冗余和地理分隔、以实现高可用性。SyncMirror通过将数据写入两个丛(本地磁盘架上主动提供数据的本地丛和通常不提供数据的远程丛)、在MetroCluster配置的两部分之间同步镜像数据。所有MetroCluster组件(例如控制器、存储、缆线、交换机(用于光纤MetroCluster)和适配器)都具有硬件冗余。

非MetroCluster系统和ASA R2系统上提供的NetApp SnapMirror主动同步功能可通过FCP和iSCSI SAN协议提供数据存储库粒度保护。通过它、您可以保护整个VMSC、也可以有选择地保护高优先级工作负载。与主动-备用解决方案NetApp MetroCluster不同、它可以同时对本地和远程站点进行主动-主动访问。从ONTAP 9.15.1开始、SnapMirror主动同步支持对称主动/主动功能、可通过双向同步复制从受保护LUN的两个副本执行读写I/O操作、从而使两个LUN副本均可在本地处理I/O操作。在ONTAP 9.151之前的版本中、SnapMirror主动同步仅支持非对称主动/主动配置、即二级站点上的数据代理到LUN的主副本。

要在两个站点之间创建VMware HA/DRS集群、需要使用vCenter Server Appliance (VCA)来管理ESXi主机。vSphere管理、vMotion®和虚拟机网络通过两个站点之间的冗余网络进行连接。管理HA/DRS集群的vCenter Server可以连接到两个站点上的ESXi主机、并且应使用vCenter HA进行配置。

请参见 "[如何在vSphere Client中创建和配置集群](#)" 配置vCenter HA。

您还应参考 "[VMware vSphere Metro Storage Cluster 建议的实践](#)"。

什么是vSphere Metro Storage Cluster?

vSphere Metro Storage Cluster (vMSC) 是一种经过认证的配置，可保护虚拟机 (VM) 和容器免受故障影响。这是通过使用延伸存储概念以及 ESXi 主机集群来实现的，这些集群分布在不同的故障域中，例如机架、建筑物、校园甚至城市。NetApp MetroCluster和SnapMirror主动同步存储技术用于为主机集群提供零恢复点目标 (RPO=0) 保护。vMSC 配置旨在确保即使整个物理或逻辑“站点”发生故障，数据也始终可用。作为 vMSC 配置一部分的存储设备必须在成功完成 vMSC 认证过程后进行认证。所有受支持的存储设备都可以在 "[《VMware存储兼容性指南》](#)"。

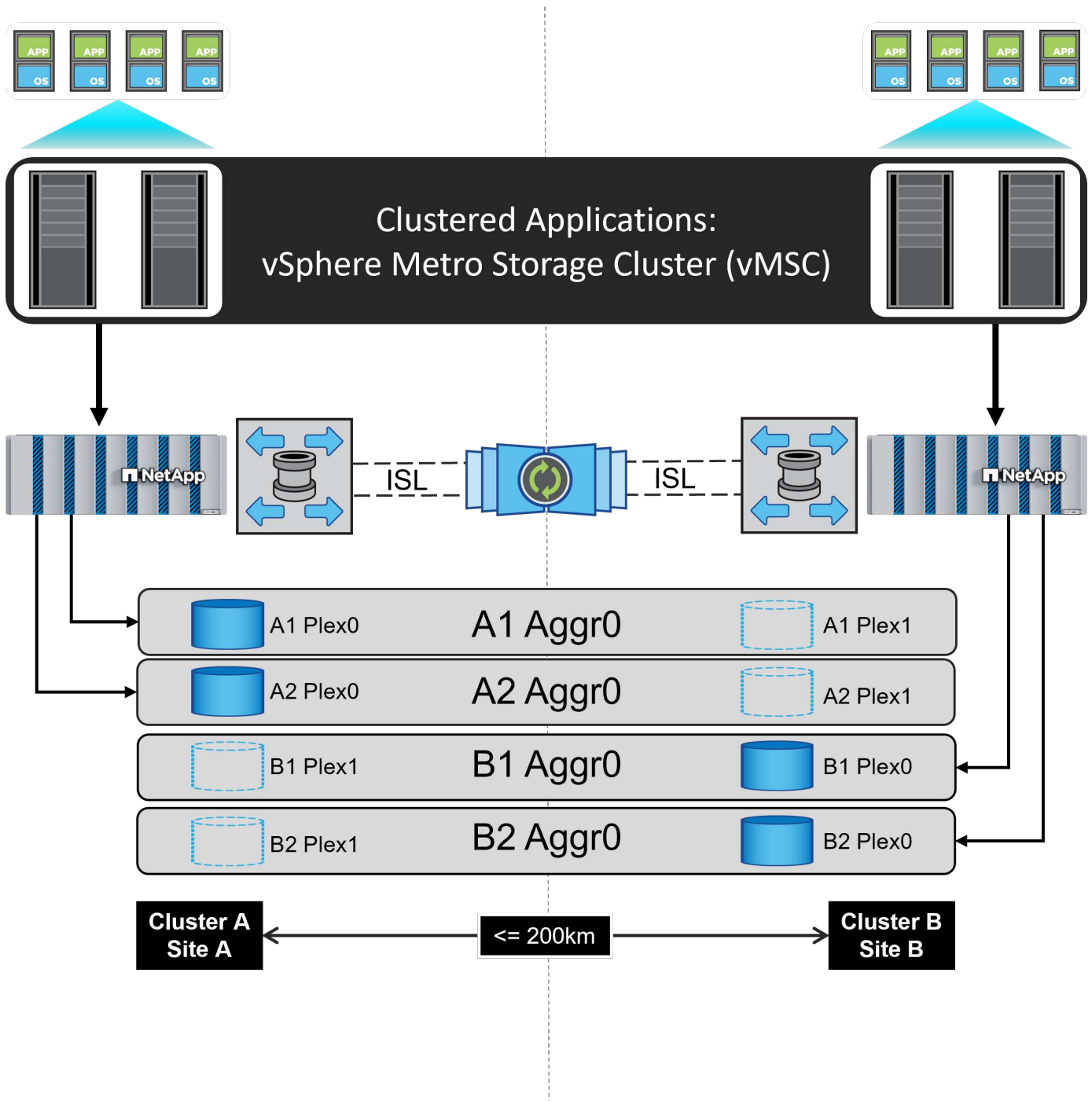
如果您需要有关vSphere Metro Storage Cluster设计准则的详细信息、请参阅以下文档：

- "[NetApp MetroCluster支持VMware vSphere](#)"
- "[VMware vSphere支持NetApp SnapMirror业务连续性](#)" (现在称为SnapMirror活动同步)

NetApp MetroCluster可以部署在两种不同的配置中、以便与vSphere结合使用：

- 延伸型MetroCluster
- 光纤MetroCluster

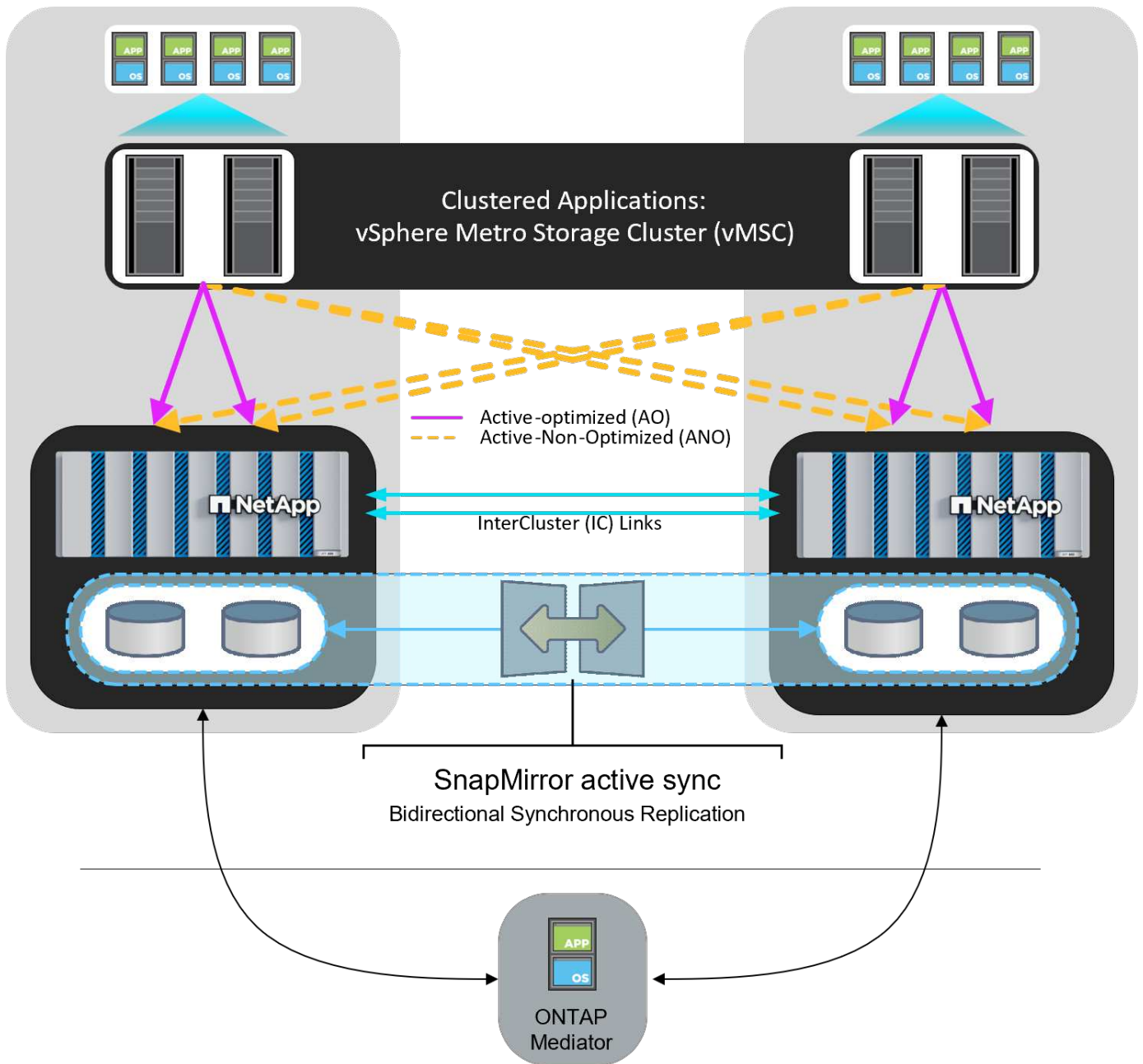
下图展示了延伸型MetroCluster的高层面拓扑图。



请参见 "[MetroCluster 文档](#)" 了解MetroCluster的特定设计和部署信息。

SnapMirror主动同步也可以通过两种不同的方式进行部署。

- 非对称
- 对称活动同步(ONTAP 9.15.1)



有关SnapMirror主动同步的特定设计和部署信息、请参见 "[NetApp文档](#)"。

VMware vSphere解决方案概述

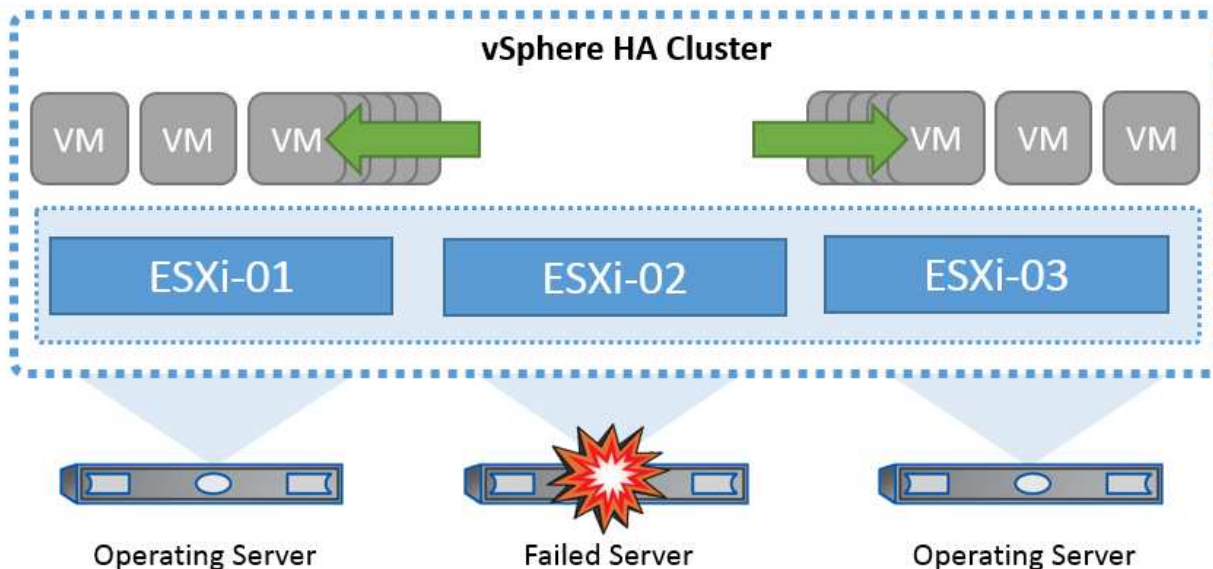
vCenter Server Appliance (VCSA) 是一个功能强大的集中式管理系统和 vSphere 的单一管理界面，使管理员能够有效地操作 ESXi 集群。它支持虚拟机配置、vMotion 操作、高可用性 (HA)、分布式资源调度器 (DRS)、VMware vSphere Kubernetes 服务 (VKS) 等关键功能。它是 VMware 云环境中的一个重要组成部分，在设计时应考虑到服务的可用性。

vSphere高可用性

VMware的集群技术可将ESXi服务器分组到虚拟机的共享资源池中、并提供vSphere高可用性(HA)。vSphere HA可为虚拟机中运行的应用程序提供易于使用的高可用性。在集群上启用HA功能后、每个ESXi服务器都会与其他主机保持通信、以便在任何ESXi主机无响应或隔离时、HA集群可以在集群中的无故障主机之间协商恢复

该ESXi主机上运行的虚拟机。如果操作系统发生故障、vSphere HA可以在同一物理服务器上重新启动受影响的虚拟机。vSphere HA可以减少计划内停机、防止计划外停机、并从中断中快速恢复。

vSphere HA 集群从故障服务器恢复虚拟机。



请务必了解、VMware vSphere不了解NetApp MetroCluster或SnapMirror主动同步、并且会根据主机和VM组关联性配置将vSphere集群中的所有ESXi主机视为符合HA集群操作条件的主机。

主机故障检测

HA集群创建完成后，集群中的所有主机都会参与选举，其中一台主机将成为主主机。每个从设备都会向主设备发送网络心跳信号，而主设备反过来也会向所有从设备主机发送网络心跳信号。vSphere HA 集群的主主机负责检测从主机的故障。

根据检测到的故障类型、可能需要对主机上运行的虚拟机进行故障转移。

在vSphere HA集群中、检测到三种类型的主机故障：

- 故障—主机停止运行。
- 隔离—主机变为网络隔离。
- 分区-主机与主主机断开网络连接。

主主机监控集群中的从主机。此通信通过每秒交换一次网络检测信号来完成。当主主机停止从从主机接收这些检测信号时、它会先检查主机活动性、然后再声明主机出现故障。主主机执行的活动性检查用于确定从主机是否正在与某个数据存储库交换检测搏。此外、主主机还会检查该主机是否对发送到其管理IP地址的ICMP ping做出响应、以检测它是仅与其主节点隔离还是与网络完全隔离。它通过对默认网关执行pinging来实现此目的。可以手动指定一个或多个隔离地址、以提高隔离验证的可靠性。



NetApp建议至少指定两个额外的隔离地址、并且每个地址都是站点本地地址。这将提高隔离验证的可靠性。

主机隔离响应

隔离响应是 vSphere HA 中的一项设置，用于确定当 vSphere HA 集群中的主机失去其管理网络连接但仍继续运行时，在虚拟机上触发的操作。此设置有三个选项：“禁用”、“关闭并重启虚拟机”和“关闭电源并重启虚拟机”。

“关机”比“断电”更好，“断电”不会将最近的更改刷新到磁盘或提交事务。如果虚拟机在 300 秒内没有关闭，则会将其断电。要更改等待时间，请使用高级选项 `das.isolationshutdowntimeout`。

在HA启动隔离响应之前、它会首先检查vSphere HA主代理是否拥有包含VM配置文件的数据存储库。否则、主机将不会触发隔离响应、因为没有主节点可重新启动VM。主机将定期检查数据存储库状态、以确定是否由具有主角色的vSphere HA代理声明数据存储库。



NetApp建议将“主机隔离响应”设置为“已禁用”。

如果主机与vSphere HA主主机隔离或分区、并且主主机无法通过检测信号数据存储库或ping进行通信、则可能发生脑裂情况。主节点会声明隔离的主机已停止运行、并在集群中的其他主机上重新启动VM。现在存在脑裂情况、因为虚拟机有两个实例正在运行、其中只有一个实例可以读取或写入虚拟磁盘。现在、可以通过配置虚拟机组件保护(VM Component Protection、VMCP)来避免脑裂情况。

VM组件保护(VMCP)

vSphere 6中与HA相关的一项增强功能是VMCP。VMCP可针对块(FC、iSCSI、FCoE)和文件存储(NFS)提供增强的保护、使其免受所有路径关闭(APD)和永久设备丢失(PDL)情况的影响。

永久设备丢失(永久设备丢失)(财产和财产)

PDL 是指存储设备永久发生故障或被管理员移除且预计不会恢复的情况。NetApp存储阵列向 ESXi 发出 SCSI Sense 代码，声明该设备已永久丢失。在 vSphere HA 的“故障条件和 VM 响应”部分，您可以配置检测到 PDL 条件后应采取的响应。



NetApp建议将“带有 PDL 的数据存储的响应”设置为“关闭电源并重新启动虚拟机”。当检测到此情况时，虚拟机将在 vSphere HA 集群中运行正常的宿主主机上立即重新启动。

所有路径已关闭(APD)

APD 是指存储设备对主机不可见，且没有通往阵列的路径时发生的情况。ESXi 认为这是设备的暂时性问题，预计该设备将再次可用。

检测到APD情况时、计时器将启动。140秒后、系统将正式声明APD条件、并且设备会标记为APD超时。超过140秒后、HA将开始计算VM故障转移APD延迟中指定的分钟数。指定时间过后、HA将重新启动受影响的虚拟机。您可以根据需要将VMCP配置为以不同方式响应("Disabled (已禁用)"、"VM Events (问题描述事件)"或"Power Off and Restart VM (关闭并重新启动VM)")。



- NetApp建议将"Response for Data with APD"配置为"关闭并重新启动VM (保守)"。
- 保守性是指 HA 能够重启虚拟机的可能性。当设置为保守模式时，HA 仅在知道另一台主机可以重启受 APD 影响的虚拟机时才会重启该虚拟机。对于“积极型”HA，即使不知道其他主机的状态，它也会尝试重启虚拟机。如果没有主机可以访问虚拟机所在的存储区域，则可能导致虚拟机无法重启。
- 如果APD状态为已解决、并且在超时时间之前还原了对存储的访问、则HA不会不必要地重新启动虚拟机、除非您明确对此虚拟机进行配置。如果即使环境已从APD条件中恢复、也需要响应、则应将APD超时后APD恢复的响应配置为重置VM。
- NetApp建议将APD超时后APD恢复的响应配置为已禁用。

为NetApp SnapMirror活动同步实施VMware DRS

VMware DRS是一项将主机资源聚合到集群中的功能、主要用于在虚拟基础架构中的集群内进行负载平衡。VMware DRS主要计算在集群中执行负载平衡所需的CPU和内存资源。由于vSphere无法识别延伸型集群、因此在进行负载平衡时、它会考虑两个站点中的所有主机。

适用于NetApp MetroCluster的VMware DRS实施

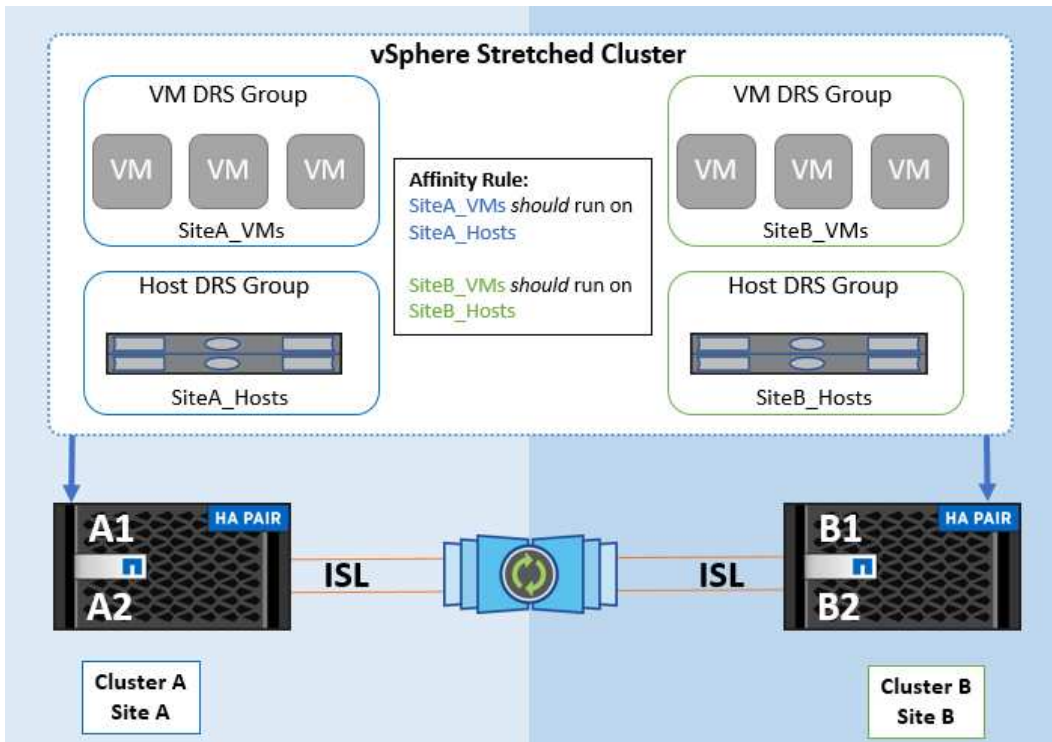
To avoid cross-site traffic, NetApp recommends configuring DRS affinity rules to manage a logical separation of VMs. This will ensure that, unless there is a complete site failure, HA and DRS will only use local hosts. 如果为集群创建DRS关联性规则、则可以指定vSphere在虚拟机故障转移期间如何应用该规则。

您可以为 vSphere HA 故障转移行为指定两种类型的规则：

- VM反关联性规则会强制指定的虚拟机在故障转移操作期间保持分离状态。
- 在故障转移操作期间、VM主机关联性规则会将指定的虚拟机放置在特定主机或已定义主机组的成员上。

使用VMware DRS中的VM主机关联性规则、可以在站点A和站点B之间进行逻辑隔离、以便VM与配置为给定数据存储库的主读/写控制器的阵列在同一站点的主机上运行。此外、VM主机关联性规则还可以使虚拟机保持在存储本地、从而确保在站点间发生网络故障时虚拟机连接。

以下是VM主机组和关联性规则的示例。



最佳实践

NetApp建议实施"应该"规则、而不是"必须"规则、因为如果发生故障、vSphere HA会违反这些规则。使用"必须"规则可能会导致服务中断。

服务的可用性应始终优先于服务的性能。如果整个数据中心发生故障，“必须”规则必须从 VM 主机亲缘性组中选择主机，并且当数据中心不可用时，虚拟机将不会重新启动。

使用NetApp MetroCluster实施VMware存储DRS

通过VMware Storage DRS功能、可以将数据存储库聚合到一个单元中、并在超过存储I/O控制(SIIOC)阈值时平衡虚拟机磁盘。

默认情况下、启用了存储DRS的DRS集群会启用存储I/O控制。通过存储I/O控制、管理员可以控制在I/O拥塞期间分配给虚拟机的存储I/O量、这样、在分配I/O资源时、更重要的虚拟机就可以优先于不太重要的虚拟机。

存储DRS使用Storage vMotion将虚拟机迁移到数据存储库集群中的不同数据存储库。在NetApp MetroCluster环境中、需要在该站点的数据存储库中控制虚拟机迁移。例如、在站点A的主机上运行的虚拟机A最好在站点A的SVM数据存储库中进行迁移否则、虚拟机将继续运行、但性能会下降、因为虚拟磁盘读/写操作将通过站点间链路从站点B进行。

*使用ONTAP存储时、建议禁用存储DRS。



- 通常、不需要或不建议将存储DRS用于ONTAP存储系统。
- ONTAP提供自己的存储效率功能、例如重复数据删除、数据压缩和数据缩减、这些功能可能会受到存储DRS的影响。
- 如果您正在使用ONTAP快照，则存储 vMotion 会在快照中留下 VM 的副本，这可能会增加存储利用率，并可能影响NetApp SnapCenter等备份应用程序，这些应用程序会跟踪 VM 及其ONTAP快照。

《VMSC设计和实施准则》

本文档概述了使用ONTAP存储系统的VMSC的设计和实施工。指南。

NetApp存储配置

有关NetApp MetroCluster的设置说明，请访问 ["MetroCluster 文档"](#)。有关SnapMirror活动同步(SMA)的说明，请参见 ["SnapMirror 业务连续性概述"](#)。

配置MetroCluster后、对其进行管理就像管理传统ONTAP环境一样。您可以使用命令行界面(CLI)、System Manager或Ans得 等各种工具设置Storage Virtual Machine (SVM)。配置SVM后、在集群上创建要用于正常操作的逻辑接口(Logical Interface、Li)、卷和逻辑单元号(Logical Unit Number、LUN)。这些对象将自动通过集群对等网络复制到另一个集群。

如果未使用MetroCluster、或者您的ONTAP系统不支持MetroCluster、例如ASA R2系统、则可以使用SnapMirror主动同步、它可以在不同故障域的多个ONTAP集群之间提供数据存储库粒度保护和主动-主动访问。SMA使用一致性组(一致性组、CGS)确保一个或多个数据存储库之间的写入顺序一致性、您可以根据应用程序和数据存储库要求创建多个CGS。对于需要在多个数据存储库之间同步数据的应用程序、一致性组尤其有用。例如、分布在数据存储库之间的子系统LVM。此外、SMA还支持原始设备映射(Raw Device Mapping、RDM)以及通过子系统内iSCSI启动程序连接到子系统的存储。有关一致性组的详细信息，请访问 ["一致性组概述"](#)。

与MetroCluster相比、使用SnapMirror活动同步管理VMSC配置有一些不同。首先、SMA是一种仅SAN配置、SnapMirror活动同步无法保护任何NFS数据存储库。其次、您必须将两个LUN副本映射到ESXi主机、以使其能够访问这两个故障域中复制的数据存储库。第三、您必须为要使用SnapMirror主动同步保护的数据存储库创建一个或多个一致性组。最后、您必须为创建的一致性组创建SnapMirror策略。所有这些操作都可以通过ONTAP工具vCenter插件中的"保护集群"向导轻松完成、也可以使用ONTAP命令行界面或System Manager手动完成。

使用适用于SnapMirror活动同步的ONTAP工具vCenter插件

ONTAP工具vCenter插件提供了一种简单直观的方法来为VMSC配置SnapMirror活动同步。您可以使用ONTAP工具vCenter插件在两个ONTAP集群之间创建和管理SnapMirror活动同步关系。此插件提供了一个易于使用的界面、用于高效地建立和管理这些关系。有关ONTAP工具vCenter插件的详细信息，请访问 ["适用于 VMware vSphere 的 ONTAP 工具"](#)，或者直接跳转到 ["使用主机集群保护进行保护"](#)。

VMware vSphere配置

创建vSphere HA集群

创建vSphere HA集群是一个多步骤过程、有关详细信息、请参见 ["如何在docs.vmware.com上的vSphere Client中创建和配置集群"](#)。简而言之、您必须先创建一个空集群、然后使用vCenter添加主机并指定集群的vSphere HA和其他设置。



本文档中的任何内容均不会取代 ["VMware vSphere Metro Storage Cluster 建议的实践"](#)。本内容仅供参考、不能替代VMware官方文档。

要配置HA集群、请完成以下步骤：

1. 连接到vCenter UI。
2. 在主机和集群中、浏览到要创建HA集群的数据中心。

- 右键单击数据中心对象、然后选择"New Cluster"(新建集群)。在基础下、确保已启用vSphere DRS和vSphere HA。完成向导。

New Cluster

1 Basics

2 Image

3 Review

Basics

Name	MCC Cluster
Location	Raleigh
vSphere DRS	<input checked="" type="checkbox"/>
vSphere HA	<input checked="" type="checkbox"/>
vSAN	<input type="checkbox"/>
	<input type="checkbox"/> Enable vSAN ESA ⓘ

Manage all hosts in the cluster with a single image ⓘ

Choose how to set up the cluster's image

- Compose a new image
- Import image from an existing host in the vCenter inventory
- Import image from a new host

Manage configuration at a cluster level ⓘ

- 选择集群并转到配置选项卡。选择vSphere HA、然后单击编辑。
- 在"Host Monitoring"(主机监控)下、选择"Enable Host Monitoring"(启用主机监控)选项。

Edit Cluster Settings | MCC Cluster

vSphere HA

Failures and responses | Admission Control | Heartbeat Datastores | Advanced Options

You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application.

Enable Host Monitoring ⓘ

> Host Failure Response	Restart VMs ▾
> Response for Host Isolation	Disabled ▾
> Datastore with PDL	Power off and restart VMs ▾
> Datastore with APD	Power off and restart VMs - Conservative restart policy ▾
> VM Monitoring	Disabled ▾

CANCEL OK

1. 仍在故障和响应选项卡上的VM监控下、选择仅VM监控选项或VM和应用程序监控选项。

Edit Cluster Settings | MCC Cluster ×

> Response for Host Isolation Disabled

> Datastore with PDL Power off and restart VMs

> Datastore with APD Power off and restart VMs - Conservative restart policy

▼ VM Monitoring

Enable heartbeat monitoring

VM monitoring resets individual VMs if their VMware tools heartbeats are not received within a set time. Application monitoring resets individual VMs if their in-guest heartbeats are not received within a set time.

Disabled

VM Monitoring Only

Turns on VMware tools heartbeats. When heartbeats are not received within a set time, the VM is reset.

VM and Application Monitoring

Turns on application heartbeats. When heartbeats are not received within a set time, the VM is reset.

CANCEL OK

1. 在"Admission Control"(准入控制)下、将HA准入控制选项设置为"Cluster Resource resource"(集群资源预留)；使用50% CPU/MEM。

vSphere HA

Failures and responses | Admission Control | Heartbeat Datastores | Advanced Options

Admission control is a policy used by vSphere HA to ensure failover capacity within a cluster. Raising the number of potential host failures will increase the availability constraints and capacity reserved.

Host failures cluster tolerates: 1
Maximum is one less than number of hosts in cluster.

Define host failover capacity by: Cluster resource Percentage

Override calculated failover capacity.

Reserved failover CPU capacity: 50 % CPU

Reserved failover Memory capacity: 50 % Memory

Reserve Persistent Memory failover capacity

Override calculated Persistent Memory failover capacity

CANCEL OK

1. 单击"确定"。
2. 选择DRS并单击编辑。
3. 除非您的应用程序要求、否则请将自动化级别设置为手动。

vSphere DRS

Automation | Additional Options | Power Management | Advanced Options

Automation Level: Manual
DRS generates both power-on placement recommendations, and migration recommendations for virtual machines. Recommendations need to be manually applied or ignored.

Migration Threshold: Conservative (Less Frequent vMotions) | Aggressive (More Frequent vMotions)

Predictive DRS: Enable

Virtual Machine Automation: Enable

1. 启用VM组件保护、请参见 "docs.vmware.com"。
2. 对于采用MetroCluster的VMSC、建议使用以下附加vSphere HA设置：

失败	响应
主机故障	重新启动VM
主机隔离	已禁用
具有永久设备丢失(永久设备丢失)的数据存储库	关闭并重新启动VM
所有路径均已关闭的数据存储库(APD)	关闭并重新启动VM
子系统不检测信号	重置虚拟机
VM重新启动策略	由虚拟机的重要性决定
主机隔离响应	关闭并重新启动VM
对使用了基于数据存储库的数据存储库的响应	关闭并重新启动VM
使用APD响应数据存储库	关闭并重新启动VM (保守)
APD的VM故障转移延迟	3分钟
响应APD恢复并显示APD超时	已禁用
VM监控敏感度	预设为高

配置用于检测信号的存储库

当管理网络出现故障时、vSphere HA使用数据存储库监控主机和虚拟机。您可以配置vCenter选择检测信号数据存储库的方式。要为数据存储库配置检测信号、请完成以下步骤：

1. 在数据存储库检测信号部分中、选择使用指定列表中的数据存储库并根据需要自动完成。
2. 从两个站点中选择要vCenter使用的数据存储库、然后按OK。

vSphere HA









Failures and responses Admission Control **Heartbeat Datastores** Advanced Options

vSphere HA uses datastores to monitor hosts and virtual machines when the HA network has failed. vCenter Server selects 4 datastores for each host using the policy and datastore preferences specified below.

Heartbeat datastore selection policy:

- Automatically select datastores accessible from the hosts
- Use datastores only from the specified list
- Use datastores from the specified list and complement automatically if needed

Available heartbeat datastores

	Name ↑	Datastore Cluster	Hosts Mounting Datastore
<input checked="" type="checkbox"/>	 d11	N/A	2
<input checked="" type="checkbox"/>	 d12	N/A	2
<input checked="" type="checkbox"/>	 d21	N/A	2
<input checked="" type="checkbox"/>	 d22	N/A	2
<input type="checkbox"/>	 d31	N/A	2
<input type="checkbox"/>	 d32	N/A	2
<input type="checkbox"/>	 d41	N/A	2
<input type="checkbox"/>	 d42	N/A	2

11 items

CANCEL OK

配置高级选项

如果HA集群中的主机与网络或集群中的其他主机断开连接、则会发生隔离事件。默认情况下、vSphere HA将使用其管理网络的默认网关作为默认隔离地址。但是、您可以为要执行ping操作的主机指定其他隔离地址、以确定是否应触发隔离响应。添加两个可执行ping操作的隔离IP、每个站点一个。请勿使用网关IP。使用的vSphere HA高级设置为"as.isolationaddress"。为此、您可以使用ONTAP或调解器IP地址。

有关详细信息，请参见 ["VMware vSphere Metro Storage Cluster 建议的实践"](#)

vSphere HA

Failures and responses Admission Control Heartbeat Datastores **Advanced Options**

You can set advanced options that affect the behavior of your vSphere HA cluster.

+ Add ✕ Delete

Option	Value
das.IgnoreRedundantNetWarning	true
das.Isolationaddress0	10.61.99.100
das.Isolationaddress1	10.61.99.110
das.heartbeatDsPerHost	4

4 items

添加名为ds.heartbeatDsPerHost的高级设置可以增加检测信号数据存储库的数量。使用四个检测信号数据存储库(HB DSS)—每个站点两个。使用"从列表中选择但恭维"选项。这是必需的、因为如果一个站点发生故障、您仍需要两个HB DSS。但是、这些数据不必通过MetroCluster或SnapMirror主动同步进行保护。

有关详细信息，请参见 ["VMware vSphere Metro Storage Cluster 建议的实践"](#)

适用于NetApp MetroCluster的VMware DRS关联

在本节中、我们将为MetroCluster环境中每个站点\集群的VM和主机创建DRS组。然后、我们配置VM\Host规则、使VM主机与本地存储资源的关联性保持一致。例如、站点A的VM属于VM组sitea_vm、站点A的主机属于主机组sitea_hosts。接下来、在VMHost规则中、我们说明site_vm应在sitea_hosts中的主机上运行。



- NetApp强烈建议使用规范“*应在组中的主机上运行”，而不是规范“必须在组中的主机上运行”。如果站点A主机发生故障、则需要通过vSphere HA在站点B的主机上重新启动站点A的VM、但后一种规范不允许HA重新启动站点B上的VM、因为这是一条硬规则。前一种规范是一种软规则、在发生HA时会违反该规范、从而实现可用性而非性能。
- 您可以创建基于事件的警报、当虚拟机违反VM-主机关联性规则时触发该警报。在vSphere Client中、为虚拟机添加新警报、然后选择"VM is violating VM-Host Affinity Rule "作为事件触发器。有关创建和编辑警报的详细信息、请参阅["vSphere监控和性能"](#)文档。

创建DRS主机组

要创建特定于站点A和站点B的DRS主机组、请完成以下步骤：

1. 在vSphere Web Client中、右键单击清单中的集群、然后选择设置。
2. 单击VM\Host Groups。
3. 单击添加。
4. 键入组的名称(例如、sitea_hosts)。
5. 从类型菜单中、选择主机组。
6. 单击Add、然后从站点A中选择所需主机、然后单击OK。
7. 重复上述步骤、为站点B添加另一个主机组
8. 单击确定。

创建DRS VM组

要创建特定于站点A和站点B的DRS VM组、请完成以下步骤：

1. 在vSphere Web Client中、右键单击清单中的集群、然后选择设置。
2. 单击VM\Host Groups。
3. 单击添加。
4. 键入组的名称(例如、sitea_VMs.)。
5. 从Type菜单中、选择VM Group。
6. 单击添加并从站点A选择所需的VM、然后单击确定。
7. 重复上述步骤、为站点B添加另一个主机组
8. 单击确定。

创建VM主机规则

要创建特定于站点A和站点B的DRS相关性规则、请完成以下步骤：

1. 在vSphere Web Client中、右键单击清单中的集群、然后选择设置。
2. 单击VM\Host Rule。
3. 单击添加。
4. 键入规则的名称(例如、sitea_affinity)。
5. 验证是否已选中"Enable Rule (启用规则)"选项。
6. 从类型菜单中、选择虚拟机到主机。
7. 选择VM组(例如、sitea_vm)。
8. 选择主机组(例如、sitea_hosts)。
9. 重复上述步骤、为站点B添加另一个VM\Host规则
10. 单击确定。

Name	sitea_affinity <input checked="" type="checkbox"/> Enable rule.
Type	Virtual Machines to Hosts ▼

Virtual machines that are members of the Cluster VM Group sitea_vms should run on host group sitea_hosts.

VM Group:

sitea_vms ▼
Should run on hosts in group ▼

Host Group:

sitea_hosts ▼

CANCEL OK

根据需要创建数据存储库集群

要为每个站点配置数据存储库集群、请完成以下步骤：

1. 使用vSphere Web Client、浏览到"Storage"(存储)下HA集群所在的数据中心。
2. 右键单击数据中心对象、然后选择"Storage"(存储)>"New Datastore Cluster"(新建数据存储库集群)。

*使用ONTAP存储时、建议禁用存储DRS。



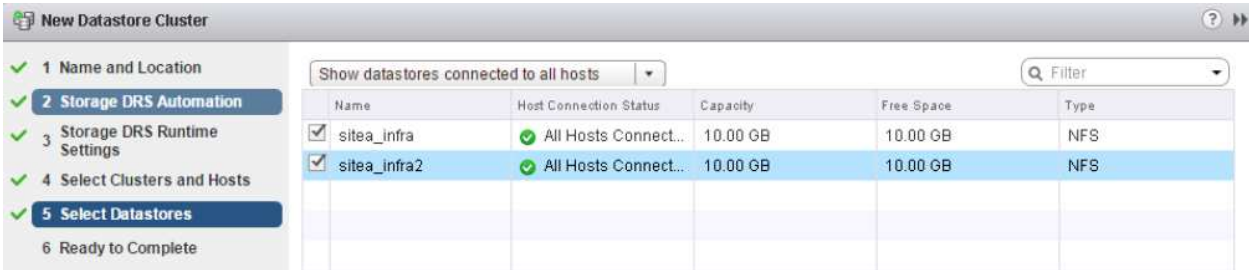
- 通常、不需要或不建议将存储DRS用于ONTAP存储系统。
- ONTAP提供自己的存储效率功能、例如重复数据删除、数据压缩和数据缩减、这些功能可能会受到存储DRS的影响。
- 如果您使用的是ONTAP快照、则Storage vMotion会在快照中保留VM副本、这可能会提高存储利用率、并可能影响NetApp SnapCenter等跟踪VM及其ONTAP快照的备份应用程序。

Storage DRS automation	
Cluster automation level	<input checked="" type="radio"/> No Automation (Manual Mode) vCenter Server will make migration recommendations for virtual machine storage, but will not perform automatic migrations.
	<input type="radio"/> Fully Automated Files will be migrated automatically to optimize resource usage.

1. 选择HA集群、然后单击"Next"(下一步)。



1. 选择属于站点A的数据存储库、然后单击下一步。



1. 查看选项、然后单击完成。
2. 重复上述步骤以创建站点B数据存储库集群、并验证是否仅选择了站点B的数据存储库。

vCenter Server可用性

您的vCenter Server设备(VCSA)应通过vCenter HA进行保护。通过vCenter HA、您可以在一个主动-被动HA对中部署两个VCSA。每个故障域一个。您可以在上阅读有关vCenter HA的更多信息 "docs.vmware.com"。

计划内和计划外事件的故障恢复能力

NetApp MetroCluster和SnapMirror主动同步是功能强大的工具，可提高NetApp硬件和ONTAP®软件的高可用性和无中断运行。

这些工具可为整个存储环境提供站点范围的保护、确保数据始终可用。无论您使用的是独立服务器、高可用性服务器集群、容器还是虚拟化服务器、NetApp技术都可以在因断电、散热或网络连接中断、存储阵列关闭或操作错误而导致全面中断时无缝地保持存储可用性。

MetroCluster和SnapMirror主动同步提供了三种在发生计划内或计划外事件时保持数据连续性的基本方法：

- 冗余组件、用于防止出现单组件故障
- 影响单个控制器的事件的本地HA接管
- 全面的站点保护—通过将存储和客户端访问从源集群移动到目标集群、快速恢复服务

这意味着在单个组件发生故障时可以无缝地继续运行、并在更换故障组件后自动恢复为冗余操作。

除单节点集群(通常为软件定义的本体、例如ONTAP Select)之外、所有ONTAP集群都具有称为接管和交还的内置HA功能。集群中的每个控制器都会与另一个控制器配对、形成一个HA对。这些对可确保每个节点在本地连接到存储。

接管是一个自动化过程、其中一个节点接管另一个节点的存储以维护数据服务。相反、恢复过程会恢复正常操作。接管可以是计划内的(例如在执行硬件维护或ONTAP升级时)、也可以是计划外的(因节点崩溃或硬件故障而

导致)。

在接管期间、MetroCluster配置中的NAS LUN会自动进行故障转移。但是、SAN Lifs不会进行故障转移；它们将继续使用逻辑单元号(Logical Unit Number、LUN)的直接路径。

有关HA接管和交还的详细信息，请参见 "[HA对管理概述](#)"。值得注意的是、此功能并不特定于MetroCluster或SnapMirror活动同步。

如果一个站点脱机或作为计划内活动进行站点范围维护、则会使用MetroCluster进行站点切换。另一个站点接管脱机集群的存储资源(磁盘和聚合)的所有权、故障站点上的SVM将联机并在灾难站点上重新启动、从而保留其完整身份、以供客户端和主机访问。

使用SnapMirror主动同步时、由于两个副本会同时使用、因此现有主机将继续运行。要确保正确进行站点故障转移、需要使用ONTAP调解器。

使用MetroCluster的VMSC的故障情形

以下各节概述了VMSC和NetApp MetroCluster系统的各种故障情形的预期结果。

单个存储路径故障

在这种情况下、如果组件(例如HBA端口、网络端口、前端数据交换机端口或FC或以太网缆线)发生故障、ESXi主机会将存储设备的特定路径标记为无活动。如果通过在HB/网络/交换机端口提供故障恢复能力来为存储设备配置多个路径、则ESXi最好执行路径切换。在此期间、虚拟机将保持运行状态、而不会受到影响、因为通过提供存储设备的多个路径、可以确保持续可用性。



在这种情况下、MetroCluster的行为没有变化、所有数据存储库在其各自的站点中仍保持完好。

最佳实践

在使用NFS/iSCSI卷的环境中、NetApp建议为标准vSwitch中的NFS vmkernel端口至少配置两个网络上行链路、并且在为分布式vSwitch映射NFS vmkernel接口的端口组上配置相同的网络上行链路。NIC绑定可以配置为主动-主动或主动-备用。

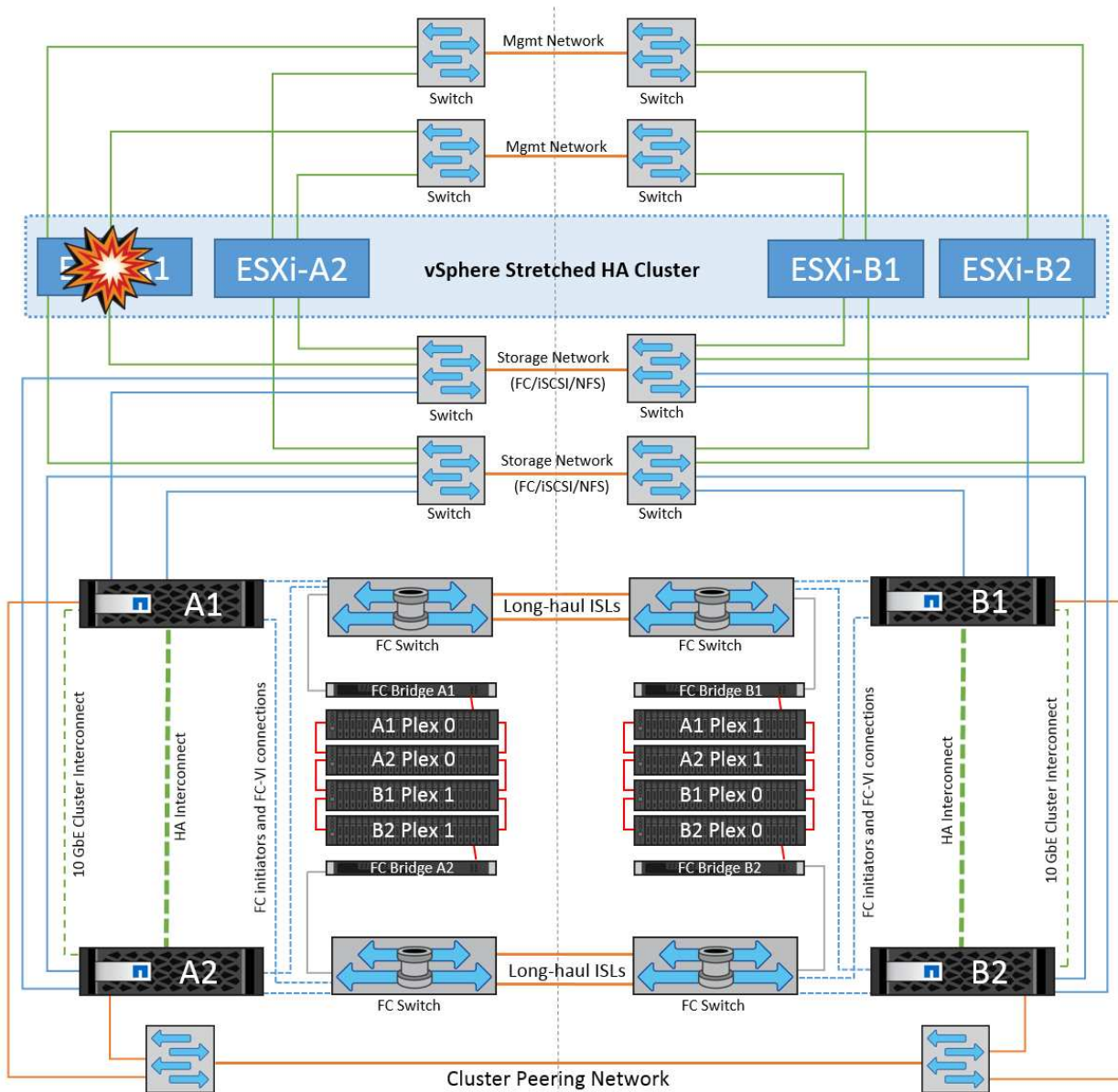
此外、对于iSCSI LUN、必须通过将vmkernel接口绑定到iSCSI网络适配器来配置多路径。有关详细信息、请参阅vSphere存储文档。

最佳实践

在使用光纤通道LUN的环境中、NetApp建议至少配置两个HBA、以确保HHBA/Port级别的故障恢复能力。NetApp还建议配置分区的最佳做法是、为单个目标分区配置单个启动程序。

应使用虚拟存储控制台(VSC)设置多路径策略、因为它会为所有新的和现有的NetApp存储设备设置策略。

单个ESXi主机故障



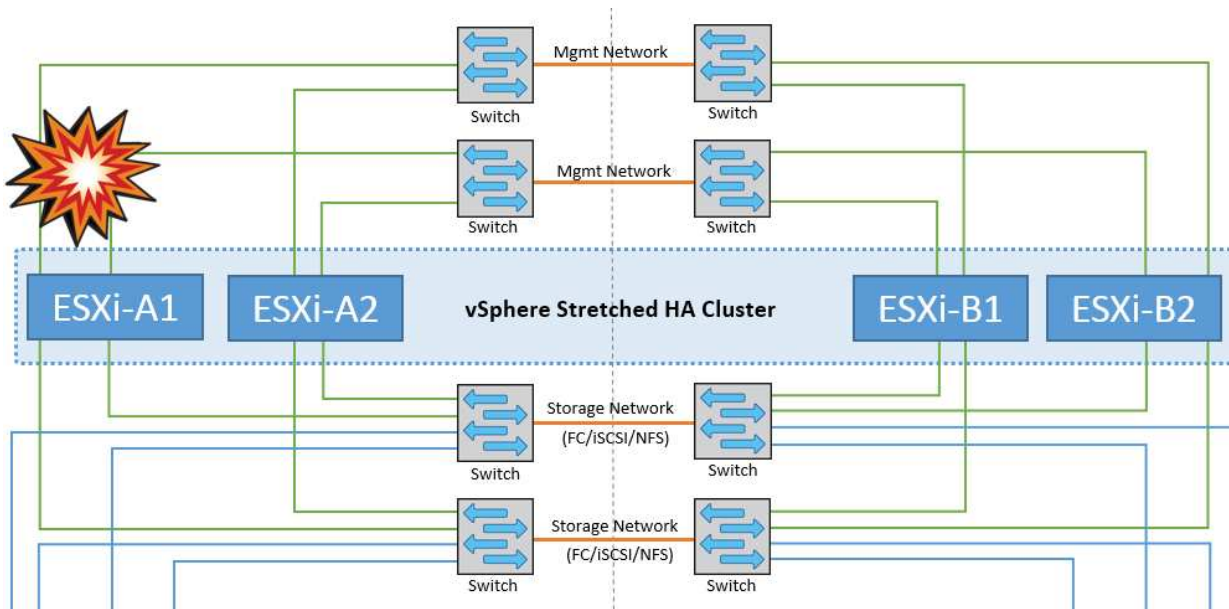
在这种情况下、如果ESXi主机发生故障、VMware HA集群中的主节点会检测到主机故障、因为它不再接收网络检测信号。为了确定主机是否确实已关闭或仅为网络分区、主节点会监控数据存储库检测点、如果没有检测点、它会对故障主机的管理IP地址执行屏显操作来执行最终检查。如果所有这些检查均为否定、则主节点会将此主机声明为故障主机、并且在此故障主机上运行的所有虚拟机都会在集群中的无故障主机上重新启动。

如果已配置DRS VM和主机关联性规则(VM组site_VMs中的VM应运行主机组site_hosts中的主机)、则HA主节点会首先检查站点A上的可用资源如果站点A上没有可用主机、主节点将尝试重新启动站点B主机上的VM

如果本地站点存在资源限制、则虚拟机可能会在另一站点的ESXi主机上启动。但是、如果将虚拟机迁移回本地站点中任何无故障的ESXi主机时违反了任何规则、则定义的DRS VM和主机关联性规则将会进行更正。如果DRS设置为手动、则NetApp建议调用DRS并应用建议以更正虚拟机放置。

在这种情况下、MetroCluster的行为没有变化、所有数据存储库在其各自的站点中仍保持完好。

ESXi主机隔离

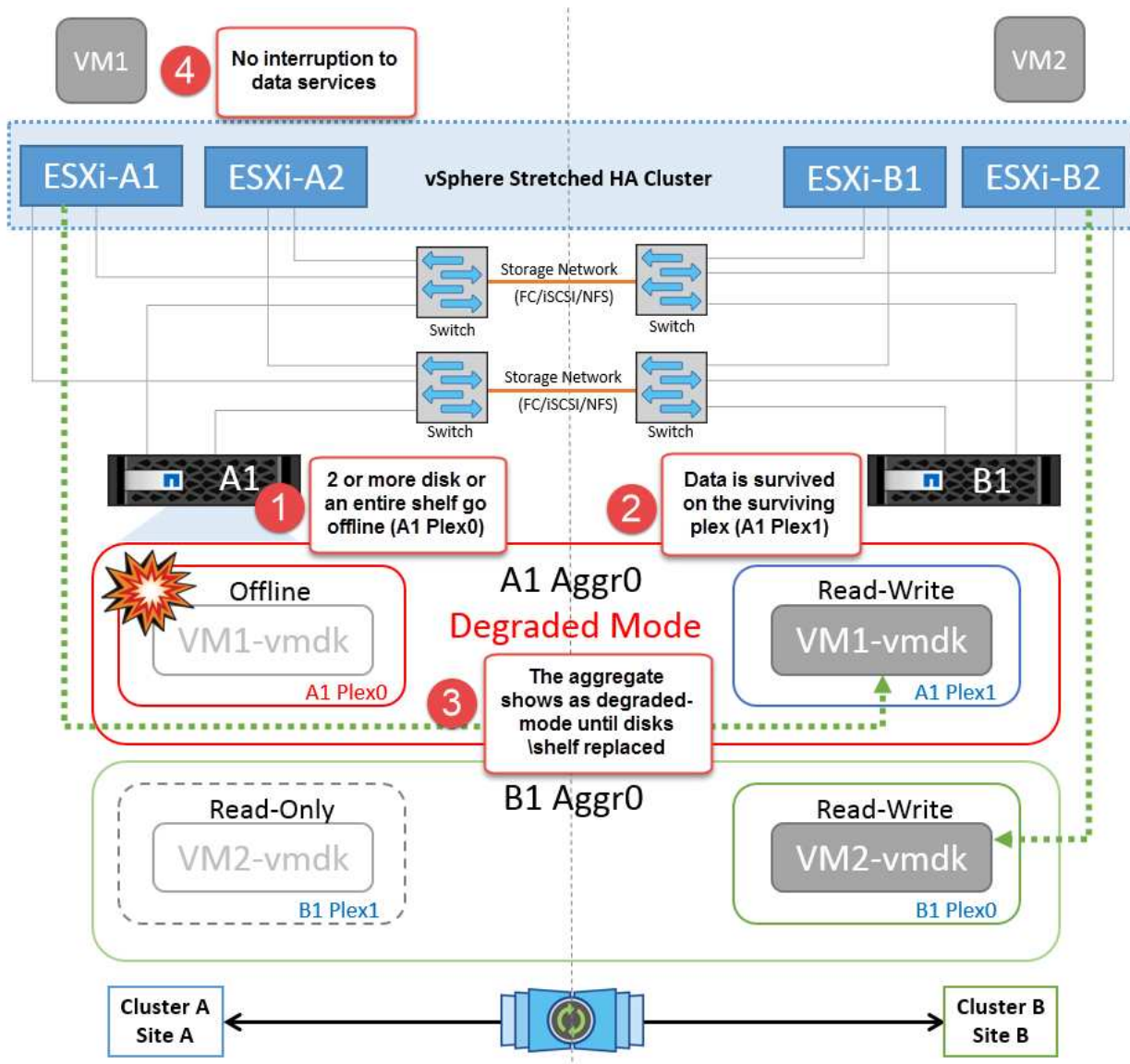


在这种情况下、如果ESXi主机的管理网络关闭、HA集群中的主节点将不会收到任何检测信号、因此此主机将在网络中隔离。要确定数据存储库是发生故障还是仅被隔离、主节点会开始监控数据存储库检测信号。如果存在、则主节点会声明主机已隔离。根据配置的隔离响应、主机可以选择关闭电源、关闭虚拟机、甚至保持虚拟机处于打开状态。隔离响应的默认间隔为30秒。

在这种情况下、MetroCluster的行为没有变化、所有数据存储库在其各自的站点中仍保持完好。

磁盘架故障

在这种情况下、出现两个以上磁盘或整个磁盘架故障。数据从无故障丛提供、而不会中断数据服务。磁盘故障可能会影响本地丛或远程丛。聚合将显示为降级模式、因为只有一个丛处于活动状态。更换故障磁盘后、受影响的聚合将自动重新同步以重建数据。重新同步后、聚合将自动恢复为正常镜像模式。如果一个RAID组中有两个以上的磁盘出现故障、则必须重建丛。

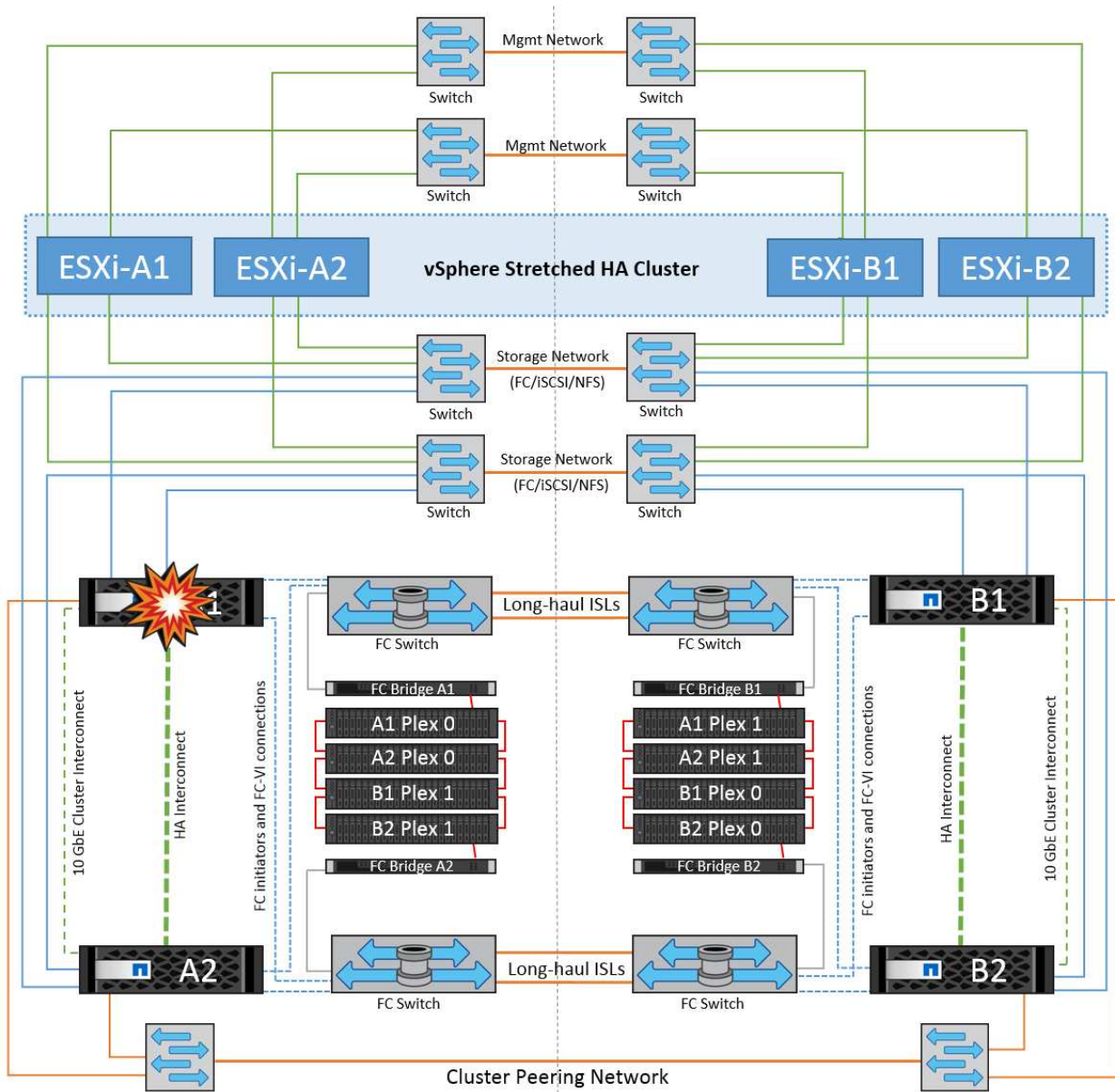


*[注释]

- 在此期间、虚拟机I/O操作不会受到影响、但性能会下降、因为数据是通过ISL链路从远程磁盘架访问的。

单个存储控制器故障

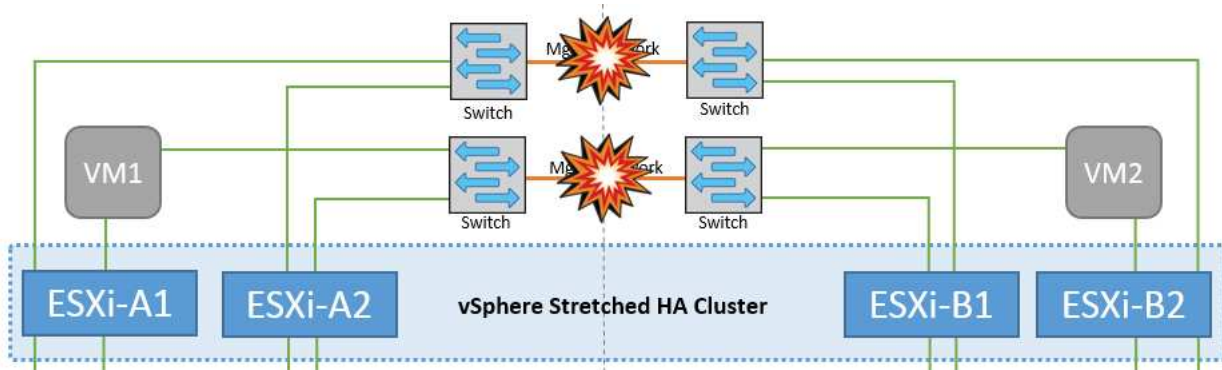
在这种情况下、一个站点上的两个存储控制器之一发生故障。由于每个站点都有一个HA对、因此一个节点发生故障会透明地自动触发故障转移到另一个节点。例如、如果节点A1发生故障、其存储和工作负载将自动传输到节点A2。虚拟机不会受到影响、因为所有的plexes都保持可用。第二个站点节点(B1和B2)不受影响。此外、vSphere HA不会执行任何操作、因为集群中的主节点仍将接收网络检测信号。



如果故障转移是滚动灾难的一部分(节点A1故障转移到A2)、则在后续发生A2故障或站点A完全故障时、站点B可能会发生灾难后切换

交换机间链路故障

管理网络发生交换机间链路故障

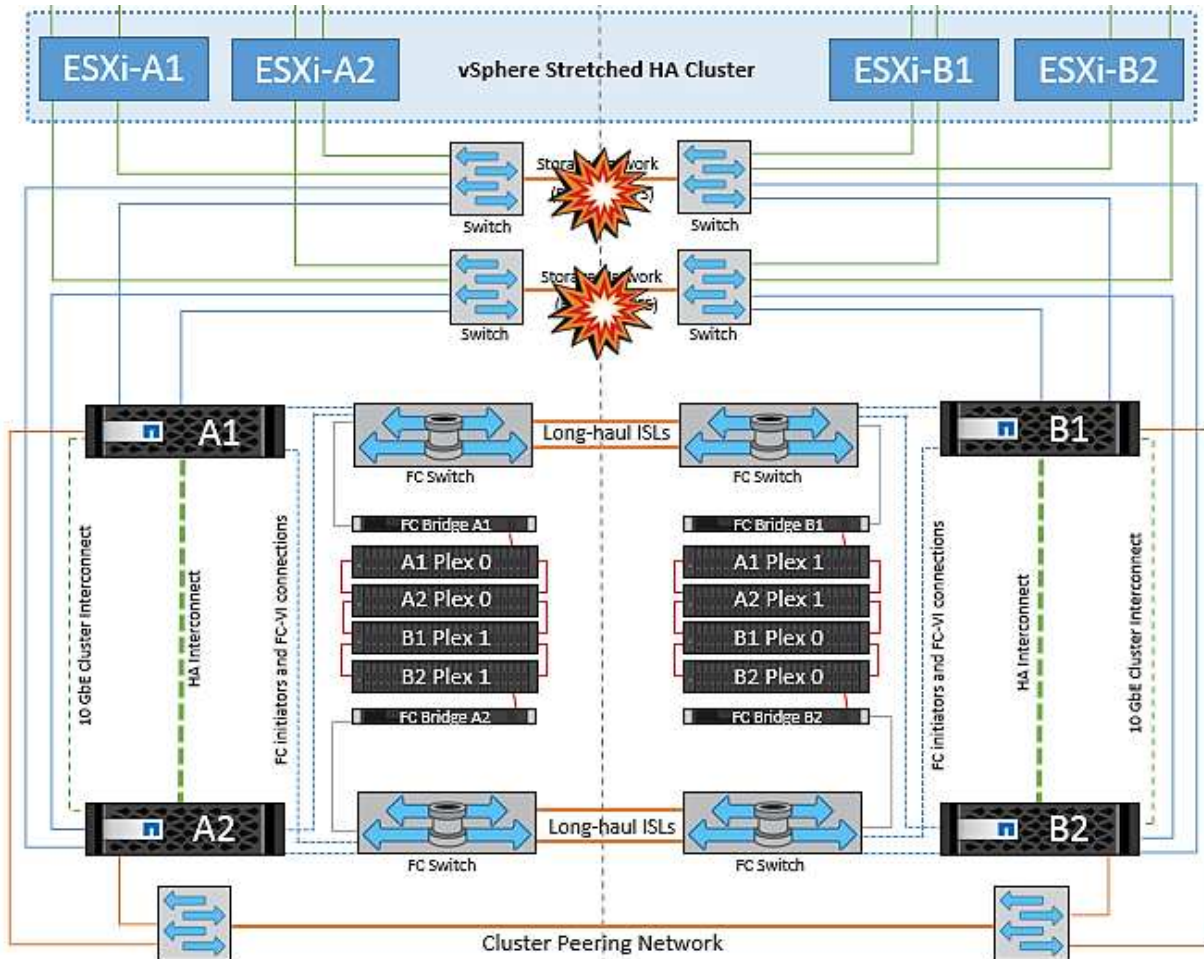


在这种情况下、如果前端主机管理网络的ISL链路发生故障、站点A的ESXi主机将无法与站点B的ESXi主机进行通信这将导致网络分区、因为特定站点上的ESXi主机将无法向HA集群中的主节点发送网络检测点。因此、由于分区、会有两个网段、每个网段中都有一个主节点、用于保护VM免受特定站点中主机故障的影响。



在此期间、虚拟机将保持运行状态、并且MetroCluster行为在此情形下不会发生任何变化。所有数据存储库在其各自的站点中仍保持完好。

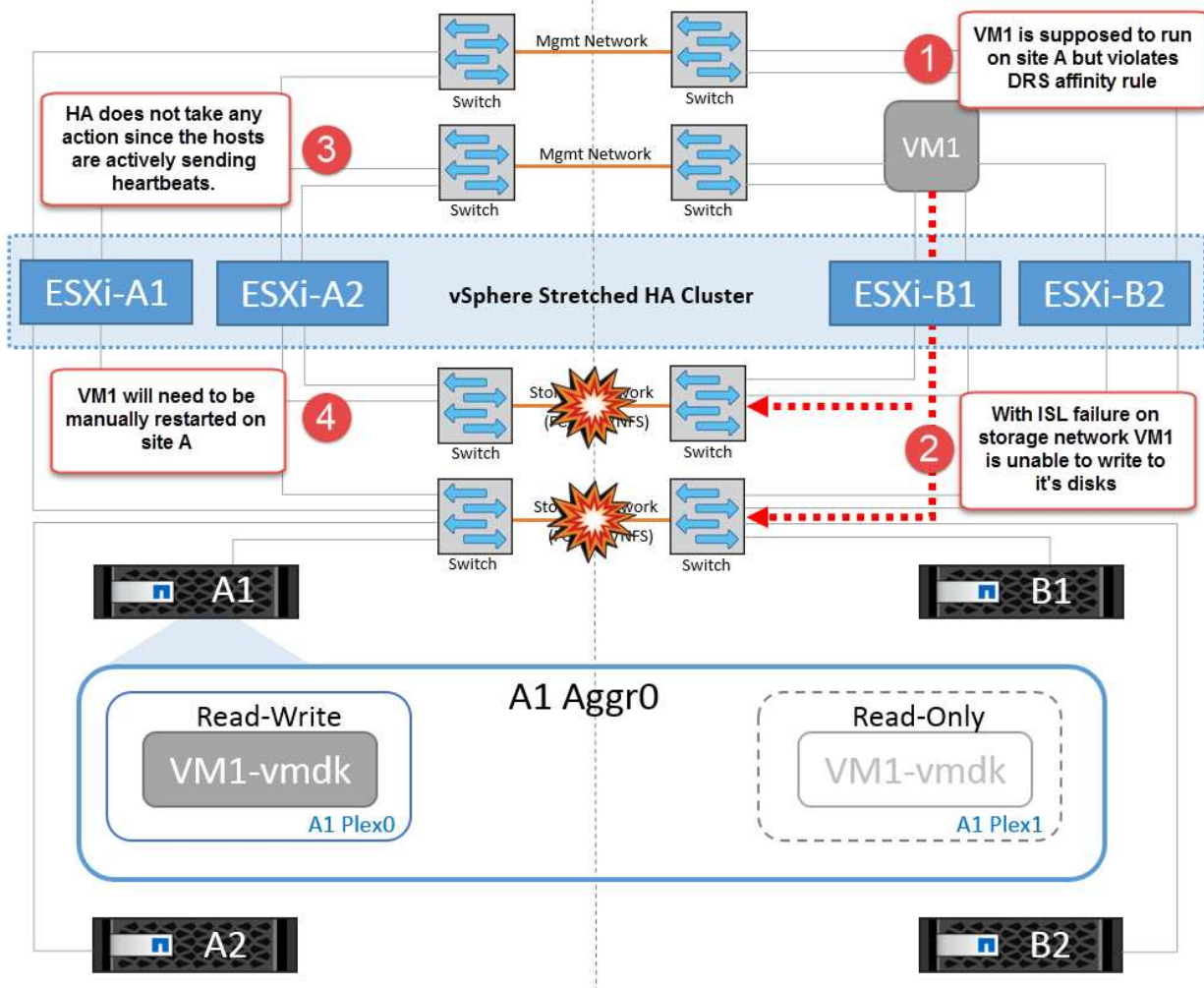
存储网络发生交换机间链路故障



在这种情况下、如果后端存储网络上的ISL链路发生故障、站点A的主机将无法访问站点B上集群B的存储卷或LUN、反之亦然。定义了VMware DRS规则、以便主机-存储站点关联性有利于虚拟机在站点内运行而不会受到影响。

在此期间、虚拟机会在其各自的站点上保持运行状态、并且在此情形下、MetroCluster的行为没有变化。所有数据存储库在其各自的站点中仍保持完好。

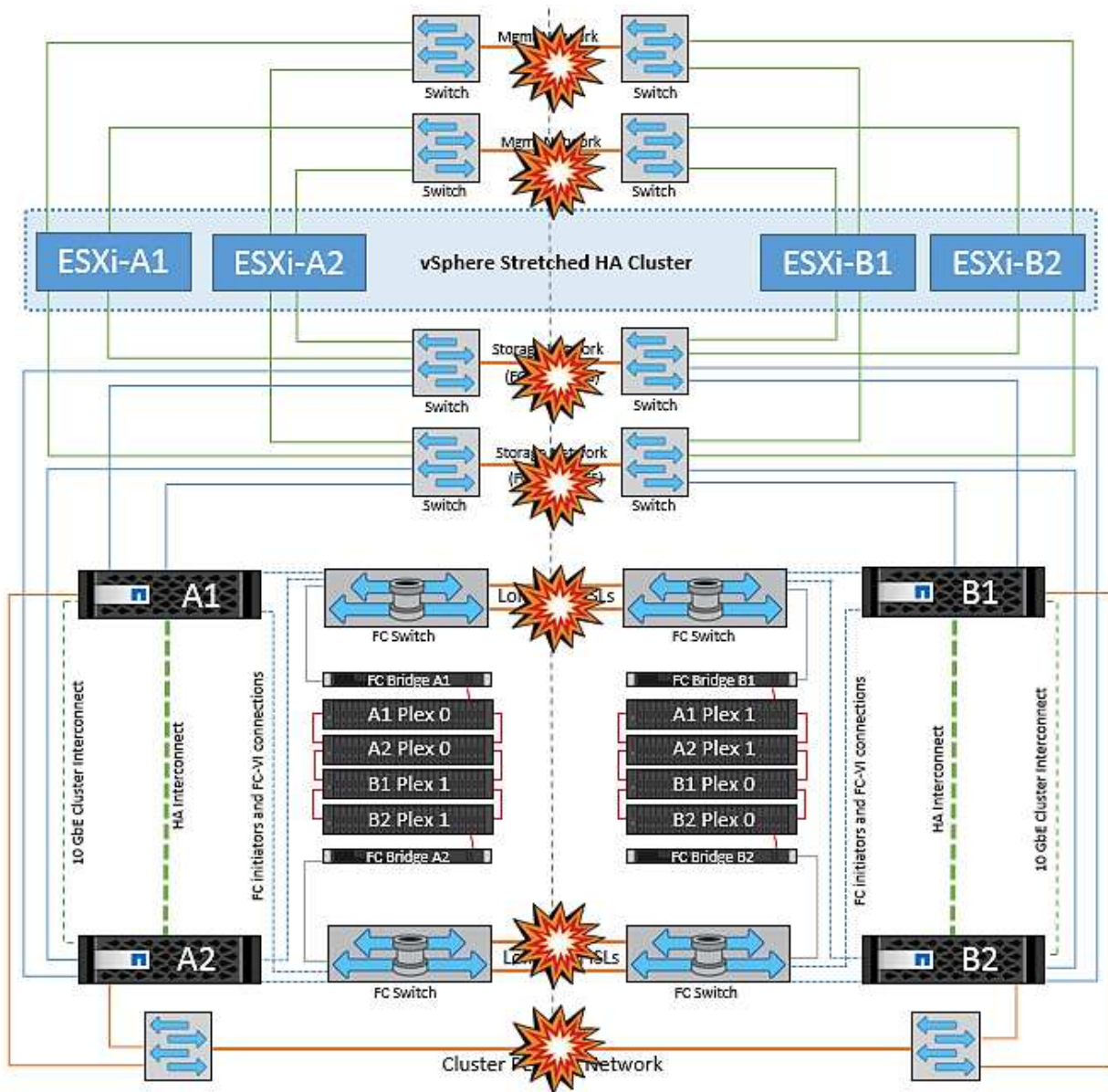
如果出于某种原因违反了相关性规则(例如、VM1本应从站点A运行、而其磁盘位于本地集群A节点上、但却在站点B的主机上运行)、则可以通过ISL链路远程访问虚拟机的磁盘。由于ISL链路故障、在站点B上运行的VM1将无法向其磁盘写入数据、因为存储卷的路径已关闭、并且该特定虚拟机已关闭。在这些情况下、VMware HA不会执行任何操作、因为主机正在主动发送检测信号。这些虚拟机需要在其各自的站点中手动关闭和启动。下图显示了违反DRS关联性规则的虚拟机。



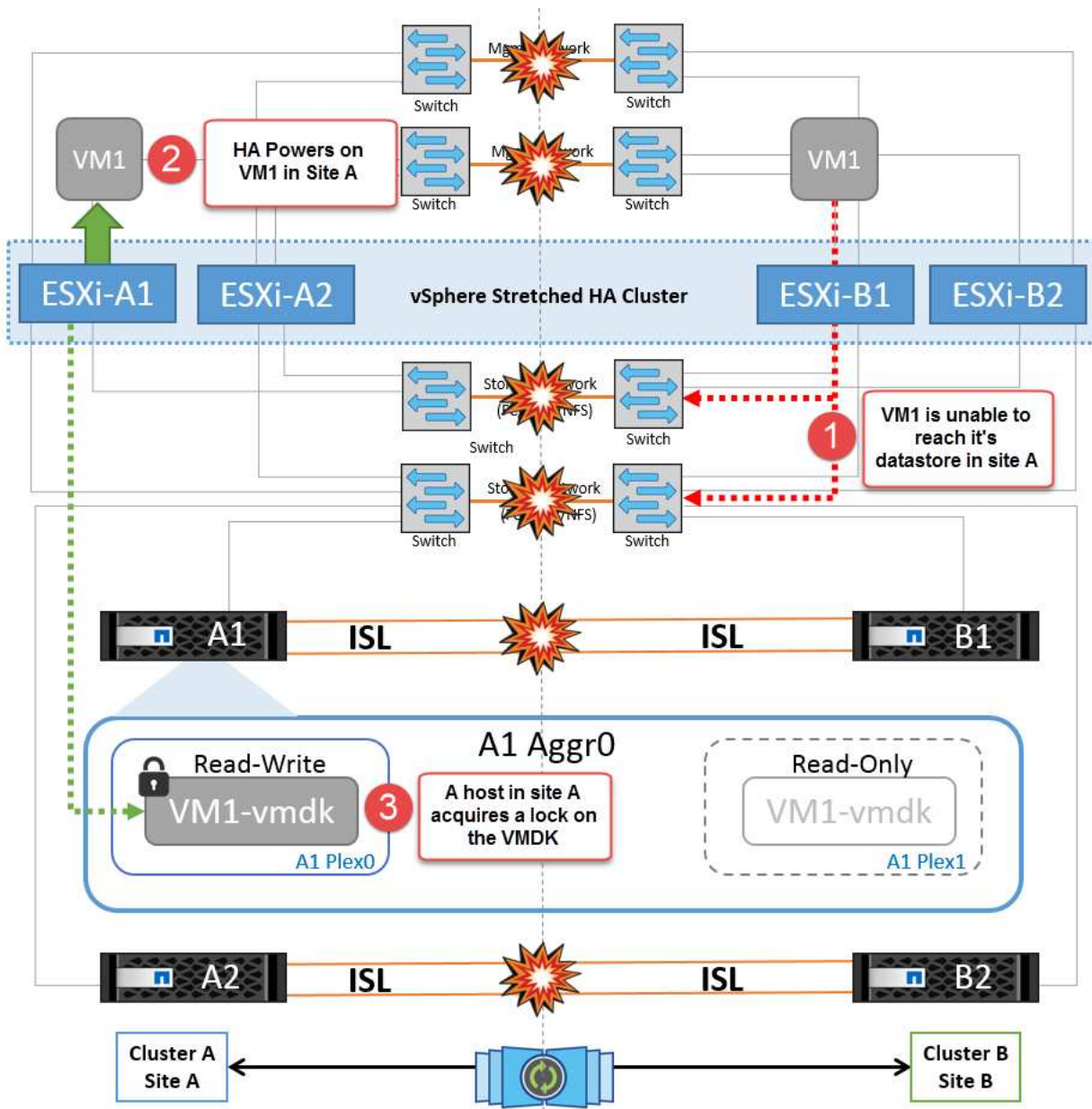
所有交换机间故障或完整数据中心分区

在此场景中、两个站点之间的所有ISL链路均已关闭、并且两个站点彼此隔离。如前文所述(例如、管理网络和存储网络出现ISL故障)、虚拟机不会在完全ISL故障时受到影响。

在站点之间对ESXi主机进行分区后、vSphere HA代理将检查数据存储库检测点、并且在每个站点中、本地ESXi主机将能够将此数据存储库检测点更新到其各自的读/写卷/LUN。站点A中的主机将假定站点B上的其他ESXi主机发生故障、因为不存在网络/数据存储库检测点。站点A上的vSphere HA将尝试重新启动站点B的虚拟机、但最终将失败、因为存储ISL故障将无法访问站点B的数据存储库。站点B也会出现类似情况



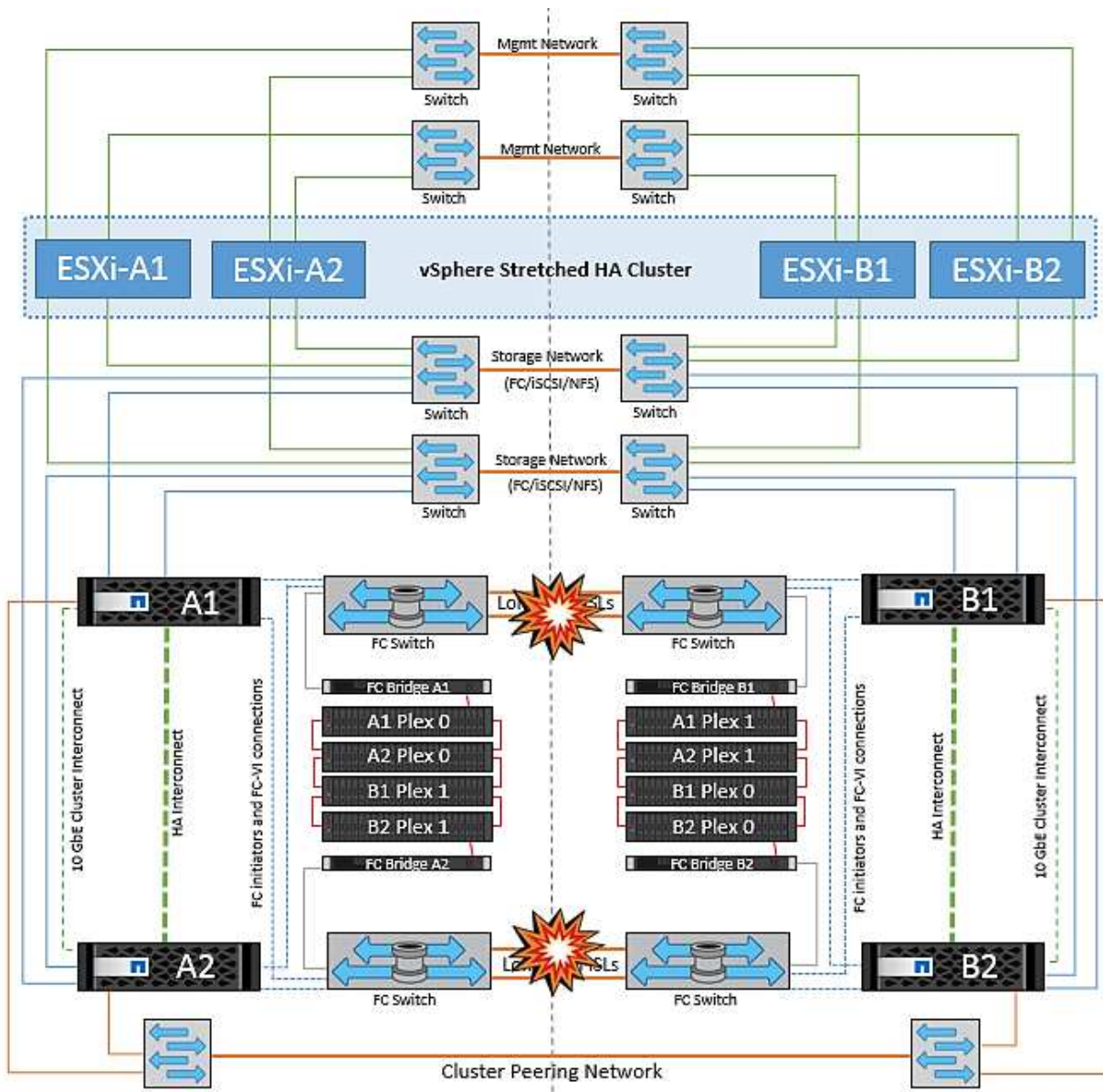
NetApp建议确定是否有任何虚拟机违反了DRS规则。从远程站点运行的任何虚拟机都将关闭、因为它们将无法访问数据存储库、vSphere HA将在本地站点上重新启动该虚拟机。ISL链路恢复联机后、远程站点上运行的虚拟机将被终止、因为不能存在两个使用相同MAC地址运行的虚拟机实例。



NetApp MetroCluster中的两个网络结构上的交换机间链路均出现故障

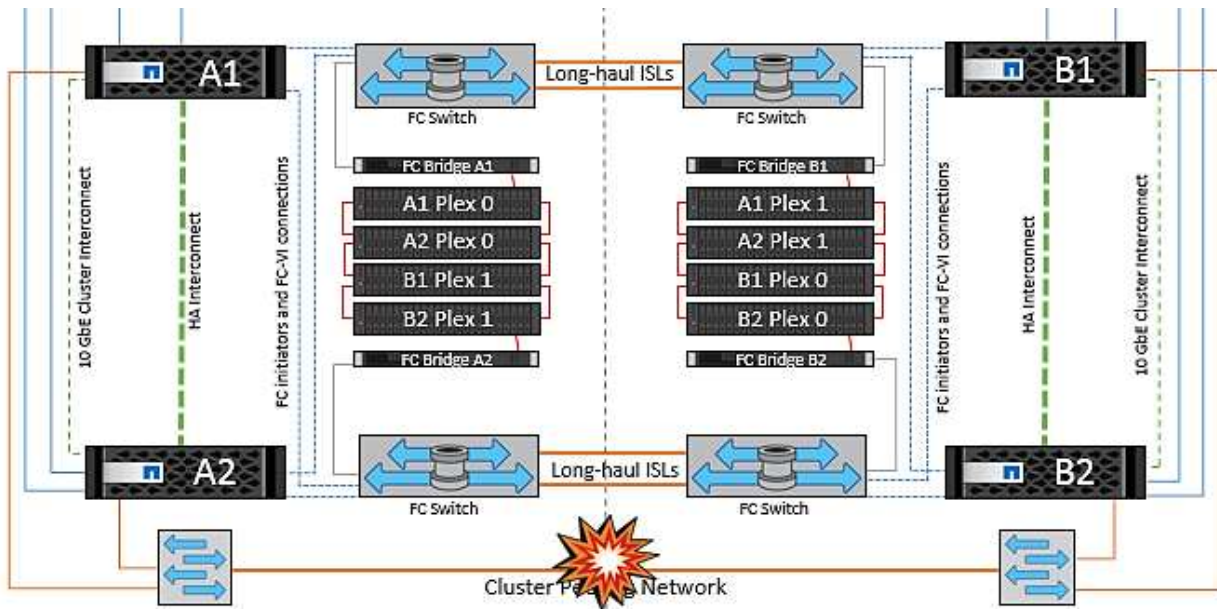
如果一个或多个ISL发生故障、流量将继续通过其余链路。如果两个网络结构上的所有ISO都发生故障、以致于站点之间没有用于存储和NVRAM复制的链路、则每个控制器将继续提供其本地数据。至少还原一个ISL后、将自动重新同步所有plexes。

在所有ISL关闭后发生的任何写入操作都不会镜像到另一站点。因此、如果在配置处于此状态时发生灾难切换、则会丢失未同步的数据。在这种情况下、需要手动干预才能在切换后进行恢复。如果很可能在很长时间内不会有任何可用的CRL、则管理员可以选择关闭所有数据服务、以避免在发生灾难时需要切换时数据丢失的风险。在至少有一个ISL可用之前、应权衡执行此操作与发生灾难时需要切换的可能性。或者、如果在级联情形下、CRL发生故障、管理员可以在所有链路发生故障之前触发到某个站点的计划内切换。



对等集群链路故障

在对等集群链路故障情形下、由于网络结构的CRL仍处于活动状态、因此两个站点上的数据服务(读取和写入)将继续提供给两个plexs。任何集群配置更改(例如、添加新SVM、在现有SVM中配置卷或LUN)都无法传播到其他站点。这些卷保存在本地CRS元数据卷中、并在恢复对等集群链路后自动传播到另一集群。如果需要强制切换才能还原对等集群链路、则在切换过程中、系统将从正常运行的站点上元数据卷的远程复制副本自动重做未完成的集群配置更改。



站点完全瘫痪

在完整站点A发生故障的情况下、站点B的ESXi主机无法从站点A的ESXi主机获取网络检测信号、因为它们已关闭。站点B的HA主节点将验证数据存储库检测点是否不存在、并声明站点A的主机出现故障、然后尝试在站点B中重新启动站点A虚拟机在此期间、存储管理员将执行切换以恢复运行正常的站点上故障节点的服务、从而恢复站点B上站点A的所有存储服务当站点A的卷或LUN在站点B上可用后、HA主代理将尝试在站点B中重新启动站点A的虚拟机

如果vSphere HA主代理尝试重新启动虚拟机(包括注册虚拟机并打开虚拟机电源)失败、则会在出现延迟后重试重新启动。重新启动之间的延迟最长可配置为30分钟。vSphere HA尝试这些重新启动的次数最多(默认为六次)。



只有在布局管理器找到合适的存储之后、HA主节点才会开始尝试重新启动、因此、如果站点完全发生故障、则可能会在执行切换后发生。

如果站点A已切换、则可以通过故障转移到运行正常的节点来无缝处理其中一个运行正常的站点B节点的后续故障。在这种情况下、四个节点的工作现在仅由一个节点执行。在这种情况下、恢复将包括向本地节点执行一次恢复。然后、在还原站点A后、将执行切回操作以还原配置的稳定状态操作。

程。NetApp 的渗透测试（笔测试）由一组经过批准且值得信赖的第三方公司执行。其测试范围包括使用复杂的利用方法或工具对与恶意入侵者或黑客类似的应用程序或软件发起攻击。

产品安全功能

适用于VMware vSphere的ONTAP工具在每个版本中都包含以下安全功能。

- 默认情况下，* 登录横幅。* SSH 处于禁用状态，如果从 VM 控制台启用，则仅允许一次性登录。用户在登录提示符中输入用户名后，将显示以下登录横幅：
- 警告：* 禁止未经授权访问此系统，并将受到法律的起诉。访问此系统即表示您同意，如果怀疑未经授权使用，您的操作可能会受到监控。

用户通过SSH通道完成登录后、将显示以下文本：

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- * 基于角色的访问控制（Role-Based Access Control，RBAC）。* ONTAP 工具与两种类型的 RBAC 控制相关联：
 - 原生 vCenter Server 特权
 - vCenter 插件的特定特权。有关详细信息，请参见 ["此链接。"](#)。
- * 加密通信通道。* 所有外部通信均使用 TLS 1.2 版通过 HTTPS 进行。
- * 最小端口暴露。* 只有必要的端口在防火墙上处于打开状态。

下表介绍了打开的端口详细信息。

TCP v4/v6 端口号	方向	功能
8143.	入站	用于 REST API 的 HTTPS 连接
8043	入站	HTTPS 连接
9060	入站	HTTPS 连接 用于基于 https 的 SOAP 连接 必须打开此端口、客户端才能连接到ONTAP工具API服务器。
22.	入站	SSH（默认为禁用）
9080	入站	HTTPS 连接— VP 和 SRA —仅从环回进行内部连接
9083.	入站	HTTPS 连接— VP 和 SRA 用于基于 https 的 SOAP 连接
1162.	入站	VP SNMP 陷阱数据包

TCP v4/v6 端口号	方向	功能
1527.	仅限内部	Derby 数据库端口，仅在此计算机与自身之间，不接受外部连接—仅限内部连接
443.	双向	用于连接到 ONTAP 集群

- * 支持证书颁发机构（CA）签名证书。* 适用于 VMware vSphere 的 ONTAP 工具支持 CA 签名证书。请参见此内容 ["知识库文章"](#) 有关详细信息 ...
- * 审核日志记录。* 支持包可以下载，并且非常详细。ONTAP 工具会将所有用户登录和注销活动记录在一个单独的日志文件中。VASA API 调用会记录在专用的 VASA 审核日志（本地 CXF.log）中。
- * 密码策略。* 遵循以下密码策略：
 - 密码不会记录在任何日志文件中。
 - 密码不会以纯文本形式传达。
 - 密码是在安装过程本身期间配置的。
 - 密码历史记录是一个可配置的参数。
 - 密码最短期限设置为 24 小时。
 - 已禁用密码字段的自动完成。
 - ONTAP 工具使用 SHA256 哈希对所有存储的凭据信息进行加密。

SnapCenter 插件 VMware vSphere

适用于 VMware vSphere 的 NetApp SnapCenter 插件软件工程部门使用以下安全开发活动：

- 威胁建模。* 威胁建模的目的是在软件开发生命周期早期发现功能，组件或产品中的安全缺陷。威胁模型是影响应用程序安全性的所有信息的结构化表示。从本质上说，它是从安全性角度来看待应用程序及其环境的。
- * 动态应用程序安全测试 (DAST)。* 用于检测处于运行状态的应用程序上的易受到攻击的情况的技术。Dast 会测试 Web 应用程序公开的 HTTP 和 HTML 接口。
- * 第三方代码货币。* 在开发软件和使用开源软件 (OSS) 的过程中、解决可能与您的产品中所含的 OSS 相关的安全漏洞非常重要。这是一项持续努力、因为 OSS 组件的版本可能随时报告新发现的漏洞。
- * 漏洞扫描。* 漏洞扫描的目的是在 NetApp 产品发布给客户之前检测其常见和已知安全漏洞。
- * 渗透测试。* 渗透测试是指评估系统、Web 应用程序或网络以发现攻击者可能利用的安全漏洞的过程。NetApp 的渗透测试（笔测试）由一组经过批准且值得信赖的第三方公司执行。其测试范围包括使用复杂的利用方法或工具对恶意入侵者或黑客等应用程序或软件发起攻击。
- * 产品安全事件响应活动。* 安全漏洞在公司内部和外部均已发现、如果不及时解决、可能会对 NetApp 的声誉造成严重风险。为了便于执行此过程、产品安全意外事件响应团队 (PSIRT) 会报告并跟踪漏洞。

产品安全功能

适用于 VMware vSphere 的 NetApp SnapCenter 插件在每个版本中都包含以下安全功能：

- * 限制 Shell 访问。* 默认情况下、SSH 处于禁用状态、只有在从 VM 控制台启用一次性登录后、才允许进行此

类登录。

- *登录横幅中显示访问警告。*用户在登录提示符中输入用户名后、将显示以下登录横幅：
- 警告：* 禁止未经授权访问此系统，并将受到法律的起诉。访问此系统即表示您同意，如果怀疑未经授权使用，您的操作可能会受到监控。

用户通过SSH通道完成登录后、将显示以下输出：

```
Linux vscl 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- * 基于角色的访问控制（ Role-Based Access Control ， RBAC ）。* ONTAP 工具与两种类型的 RBAC 控制相关联：
 - 本机vCenter Server特权。
 - VMware vCenter插件的特定特权。有关详细信息，请参见 "[基于角色的访问控制（ Role-Based Access Control ， RBAC ）](#)"。
- *加密通信通道。*所有外部通信均使用TLS通过HTTPS进行。
- * 最小端口暴露。* 只有必要的端口在防火墙上处于打开状态。

下表提供了打开的端口详细信息。

TCP v4/v6端口号	功能
8144.	用于 REST API 的 HTTPS 连接
8080	用于OVA GUI的HTTPS连接
22.	SSH (默认情况下处于禁用状态)
3306.	MySQL (仅限内部连接；默认情况下、外部连接处于禁用状态)
443.	nginx (数据保护服务)

- *支持证书颁发机构(CA)签名证书。*适用于VMware vSphere的SnapCenter 插件支持CA签名证书的功能。请参见 "[如何创建和/或将SSL证书导入到适用于VMware vSphere的SnapCenter 插件\(SCV\)](#)"。
- *密码策略。*以下密码策略有效：
 - 密码不会记录在任何日志文件中。
 - 密码不会以纯文本形式传达。
 - 密码是在安装过程本身期间配置的。
 - 所有凭据信息均使用SHA256哈希进行存储。
- *基本操作系统映像。*本产品随附Debian基础操作系统、用于OVA、但访问受限且Shell访问已禁用。这样可以减少攻击占用空间。每个SnapCenter 版本基础操作系统都会更新最新的安全修补程序、以最大限度地提

高安全性。

NetApp针对适用于VMware vSphere设备的SnapCenter 插件开发软件功能和安全修补程序、然后将其作为捆绑软件平台发布给客户。由于这些设备包括特定的Linux子操作系统依赖关系以及我们的专有软件、因此NetApp建议您不要更改子操作系统、因为这很可能会影响NetApp设备。这可能会影响NetApp支持此设备的能力。NetApp建议测试和部署我们最新的设备代码版本、因为发布这些代码版本是为了修补任何与安全相关的问题。

适用于VMware vSphere的ONTAP工具安全强化指南

适用于VMware vSphere 9.13的ONTAP工具安全强化指南

适用于VMware vSphere的ONTAP工具的安全强化指南提供了一套全面的说明、用于配置最安全的设置。

这些指南适用于设备本身的应用程序和子操作系统。

验证适用于VMware vSphere 9.13的ONTAP工具安装包的完整性

客户可以通过两种方法验证其ONTAP工具安装包的完整性。

1. 验证校验和
2. 验证签名

OTV安装包的下载页面上提供了校验和。用户必须根据下载页面上提供的校验和验证已下载软件包的校验和。

验证ONTAP工具OVA的签名

vapp安装包以tarball的形式提供。此tarball包含虚拟设备的中间证书和根证书、以及自述文件和OVA软件包。README文件可指导用户如何验证vapp OVA软件包的完整性。

客户还必须上传vCenter 7.0U3和更高版本上提供的根证书和中间证书。对于7.0.1和7.0.U三e之间的vCenter版本、VMware不支持验证证书的功能。客户不需要上传vCenter 6.x的任何证书

将可信根证书上传到vCenter

1. 使用VMware vSphere Client登录到vCenter Server。
2. 为administrator@vsphere.local或vCenter Single Sign-On Administrators组的其他成员指定用户名和密码。如果您在安装期间指定了其他域、请以管理员身份@mydomain登录。
3. 导航到证书管理UI：a.从主菜单中、选择管理。b.在证书下、单击证书管理。
4. 如果系统提示您、请输入vCenter Server的凭据。
5. 在可信根证书下、单击添加。
6. 单击浏览并选择证书.prom文件(OTV_OVA_inter_root_CERT_chain.prom)的位置。
7. 单击添加。此时、证书将添加到存储中。

请参见 ["将可信根证书添加到证书存储"](#) 有关详细信息 ...在部署vapp时(使用OVA文件)、可以在"查看详细信息"页面上验证vapp包的数字签名。如果下载的vapp软件包为正版、"发布者"列将显示"可信证书"(如以下屏幕截图所示)。

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details**
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Review details

Verify the template details.

Publisher	Entrust Code Signing CA - OVCS2 (Trusted certificate)
Product	Virtual Appliance - NetApp Inc. ONTAP tools for VMware vSphere
Version	See appliance for version
Vendor	NetApp Inc.
Description	Virtual Appliance - NetApp Inc. ONTAP tools for VMware vSphere for netapp storage systems. For more information or support please visit https://www.netapp.com/
Download size	2.2 GB
Size on disk	3.9 GB (thin provisioned)
	53.0 GB (thick provisioned)

Activate
Go to System

CANCEL BACK NEXT

验证ONTAP工具ISO和SRA tar.gz的签名

NetApp会在产品下载页面上与客户共享其代码签名证书、以及OTV-ISO和sra.tgz的产品zip文件。

用户可以从代码签名证书中提取公共密钥、如下所示：

```
#> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-key name>
```

然后，应使用公共密钥验证ISO和tgz产品zip的签名，如下所示：

```
#> openssl dgst -sha256 -verify <public-key> -signature <signature-file>  
<binary-name>
```

示例

```
#> openssl x509 -in OTV_ISO_CERT.pem -pubkey -noout > OTV_ISO.pub
#> openssl dgst -sha256 -verify OTV_ISO.pub -signature netapp-ontap-tools-
for-vmware-vmware-9.12-upgrade-iso.sig netapp-ontap-tools-for-vmware-
vsphere-9.12-upgrade.iso
Verified OK => response
```

ONTAP工具的端口和协议9.13.

此处列出的是支持在适用于VMware vSphere服务器的ONTAP工具与其他实体(如受管存储系统、服务器和其他组件)之间进行通信所需的端口和协议。

OTV需要入站和出站端口

请注意下表、其中列出了ONTAP工具正常运行所需的入站和出站端口。请务必确保仅为远程计算机的连接打开表中提到的端口、而为远程计算机的连接应阻止所有其他端口。这将有助于确保系统的安全性和安全性。

下表介绍了打开的端口详细信息。

TCP v4/v6端口#	* 方向 *	函数
8143.	入站	用于 REST API 的 HTTPS 连接
8043	入站	HTTPS 连接
9060	入站	HTTPS连接+ 用于基于HTTPS的SOAP连接+ 必须打开此端口、客户端才能连接到ONTAP工具API服务器。
22.	入站	SSH (默认为禁用)
9080	入站	HTTPS 连接— VP 和 SRA —仅从环回进行内部连接
9083.	入站	HTTPS连接- VP和SRA 用于基于HTTPS的SOAP连接
1162.	入站	VP SNMP 陷阱数据包
8443	入站	远程插件
1527.	仅限内部	Derby数据库端口、仅在此计算机与自身之间、不接受外部连接— 仅限内部连接
8150	仅限内部	日志完整性服务在端口上运行
443.	双向	用于连接到 ONTAP 集群

控制对Derby数据库的远程访问

管理员可以使用以下命令访问derby数据库。可通过ONTAP工具本地VM和远程服务器通过以下步骤访问它：

```
java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
connect 'jdbc:derby://<OTV-
IP>:1527//opt/netapp/vpserver/vvoldb;user=<user>;password=<password>';
```

示例:

```
root@UnifiedVSC:~# java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
ij version 10.15
ij> connect 'jdbc:derby://localhost:1527//opt/netapp/vpserver/vvoldb;user=app;password=
ij> show tables;
TABLE_SCHEM          |TABLE_NAME          |REMARKS
-----|-----|-----
SYS                  |SYSALIASES          |
SYS                  |SYSCHECKS           |
SYS                  |SYSCOLPERMS         |
SYS                  |SYSCOLUMNS         |
SYS                  |SYSCONGLOMERATES   |
SYS                  |SYSCONSTRAINTS     |
SYS                  |SYSDEPENDS         |
SYS                  |SYSFILES            |
SYS                  |SYSFOREIGNKEYS     |
SYS                  |SYSKEYS             |
SYS                  |SYSPERMS            |
```

适用于VMware vSphere 9.13访问点(用户)的ONTAP工具

适用于VMware vSphere的ONTAP工具安装会创建和使用三种类型的用户:

1. System User: root用户帐户
2. 应用程序用户: 管理员用户、maintuser和数据库用户帐户
3. 支持用户: diag用户帐户

1.系统用户

system(root)用户是通过在底层操作系统(DeBM)上安装ONTAP工具来创建的。

- 默认系统用户"root"是通过安装ONTAP工具在Debian上创建的。其默认值为禁用、可通过"aint"控制台临时启用。

2.应用程序用户

应用程序用户在ONTAP工具中命名为本地用户。这些用户是在ONTAP工具应用程序中创建的。下表列出了应用程序用户的类型:

* 用户 *	* 问题描述 *
管理员用户	它是在ONTAP工具安装期间创建的、用户在部署ONTAP工具时提供凭据。用户可以选择在"aint"控制台中更改密码。密码将在90天后过期、用户应更改此密码。
维护用户	它是在ONTAP工具安装期间创建的、用户在部署ONTAP工具时提供凭据。用户可以选择在"aint"控制台中更改密码。此用户为维护用户、创建此用户名是为了执行维护控制台操作。
数据库用户	它是在ONTAP工具安装期间创建的、用户在部署ONTAP工具时提供凭据。用户可以选择在"aint"控制台中更改密码。密码将在90天后过期、用户应更改此密码。

3.支持用户(diag用户)

在ONTAP工具安装期间、系统会创建一个支持用户。此用户可用于在服务器发生任何问题描述或中断时访问ONTAP工具并收集日志。默认情况下、此用户处于禁用状态、但可以通过"aint"控制台临时启用。需要注意的是、此用户将在特定时间段后自动禁用。

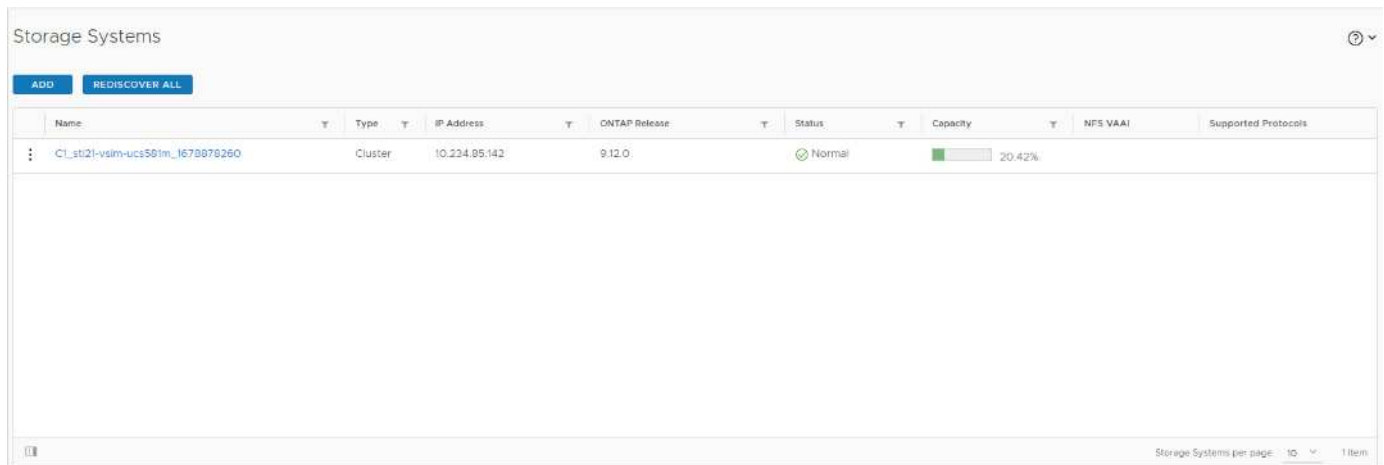
ONTAP工具9.13相互TLS (基于证书的身份验证)

ONTAP 9.7及更高版本支持相互TLS通信。从适用于VMware和vSphere 9.12的ONTAP工具开始、可使用相互TLS与新添加的集群进行通信(具体取决于ONTAP版本)。

ONTAP

对于先前添加的所有存储系统：在升级期间、所有添加的存储系统都将获得自动信任、并配置基于证书的身份验证机制。

如以下屏幕截图所示、集群设置页面将显示为每个集群配置的相互TLS (基于证书的身份验证)的状态。



Name	Type	IP Address	ONTAP Release	Status	Capacity	NFS VAAI	Supported Protocols
CL_st121-vs1m-ucs561m_1679878260	Cluster	10.224.05.142	9.12.0	Normal	20.42%		

集群添加

在集群添加工作流期间、如果要添加的集群支持MTLS、则默认情况下会配置MTLS。用户无需为此执行任何配置。以下屏幕截图显示了在添加集群期间向用户显示的屏幕。

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server 10.224.58.52 ▼

Name or IP address:

Username:

Password:

Port:

443

Advanced options ▲

ONTAP Cluster
Certificate:

Automatically fetch Manually upload

CANCEL

ADD

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server	10.224.58.52 
Name or IP address:	10.234.85.142
Username:	admin
Password:
Port:	443
Advanced options	

CANCEL

ADD

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

10.234.85.52

Authorize Cluster Certificate

Host 10.234.85.142 has identified itself with a self-signed certificate.

[Show certificate](#)

Do you want to trust this certificate?

NO

YES

CANCEL

ADD

Authorize Cluster Certificate

Host 10.234.85.142 has identified itself with a self-signed certificate.

[Hide certificate](#)

Certificate Information

This certificate identifies the 10.234.85.142 host.

Issued By

Name (CN or DN): C1_sti21-vsimsim-ucs581m_1678878260

Issued To

Name (CN or DN): C1_sti21-vsimsim-ucs581m_1678878260

Validity

Issued On: 03/15/2023 11:16:06

Expires On: 03/14/2024 11:16:06

Fingerprint Information

SHA-1 Fingerprint: 2C:38:E3:5C:4B:F3:5D:3F:39:C8:CE:4A:8
2:C1:A6:EE:34:53:A0:F3

SHA-256 Fingerprint: 05:0F:FE:CD:B0:C6:FC:6F:EB:8A:FC:86:F
7:E3:EF:D4:8D:CA:02:92:9B:E1:A4:70:84:
52:F8:76:98:64:FA:23

Do you want to trust this certificate?

NO

YES

集群编辑

在集群编辑操作期间、有两种情形：

- 如果ONTAP证书过期、则用户必须获取新证书并上传。
- 如果OTV证书过期、则用户可以通过选中复选框来重新生成它。
 - 为ONTAP生成新的客户端证书_

Modify Storage System

Settings Provisioning Options

IP address or hostname: ▼

Port:

Username:

Password:

Upload Certificate (Optional) [BROWSE](#)

Skip monitoring of this storage system

Generate a new client certificate for ONTAP

CANCEL

OK



ONTAP工具9.13 HTTPS证书

默认情况下、ONTAP工具会使用安装期间自动创建的自签名证书来保护对Web UI的HTTPS访问。ONTAP工具提供以下功能：

1. 重新生成HTTPS证书

在ONTAP工具安装期间、会安装HTTPS CA证书、并将该证书存储在密钥库中。用户可以选择通过maine控制台重新生成HTTPS证书。

通过导航到"Application Configuration"(应用程序配置)→"Re-generate certificates"(重新生成证书)、可以在_maint_控制台中访问上述选项

ONTAP工具9.13登录横幅

用户在登录提示符中输入用户名后、将显示以下登录横幅。请注意、SSH在默认情况下处于禁用状态、如果从VM控制台启用了SSH、则只允许一次性登录。

```
WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.
```

用户通过 SSH 通道完成登录后，将显示以下文本：

```
Linux UnifiedVSC 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21)
x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

ONTAP工具的非活动超时9.13.

为了防止未经授权的访问、系统会设置非活动超时、以便在使用授权资源时自动注销在特定时间段内处于非活动状态的用户。这样可以确保只有授权用户才能访问资源、并有助于保持安全性。

- 默认情况下、vSphere Client会话会在空闲120分钟后关闭、需要用户重新登录才能继续使用客户端。您可以通过编辑webclient.properties文件来更改超时值。您可以配置vSphere Client的超时 "[配置vSphere Client超时值](#)"
- ONTAP工具的web-cli会话注销时间为30分钟。

每个用户的最大并发请求数(网络安全保护/DOS攻击)适用于VMware vSphere的ONTAP工具9.13

默认情况下、每个用户的最大并发请求数为48个。ONTAP工具中的root用户可以根据其环境的要求更改此值。此值不应设置为非常高的值，因为它提供了一种防止拒绝服务(DOS)攻击的机制。

用户可以在*_opt/NetApp/vscserver/etc/dosfilterParams.json*文件中更改最大并发会话数和其他受支持的参数。

我们可以通过以下参数配置筛选器：

- **delayMs**：在考虑之前，所有请求超出速率限制的延迟(以毫秒为单位)。提供-1仅拒绝请求。
- **throttleMs**：等待信标的非同步等待时间。

- **maxRequestMs**: 允许此请求运行的时间长度。
- **ipWhitelist**: 不受速率限制的IP地址的逗号分隔列表。(可以是vCenter、ESXi和SRA IP)
- **maxRequestsPerSec**: 每秒从连接发出的最大请求数。

*dosfilterParams file:*中的默认值

```
{ "delayMs": "-1",
  "throttleMs": "1800000",
  "maxRequestMs": "300000",
  "ipWhitelist": "10.224.58.52",
  "maxRequestsPerSec": "48" }
```

ONTAP工具的网络时间协议(NTP)配置9.13.

有时、由于网络时间配置的差异、可能会出现安全问题。请务必确保网络中的所有设备都具有准确的时间设置、以防止出现此类问题。

虚拟设备

您可以从虚拟设备的维护控制台配置NTP服务器。用户可以在_System Configuration_ => _Add new NTP Server_ 选项下添加NTP服务器详细信息

默认情况下、NTP的服务为ntpd.这是一项传统服务、在某些情况下不适用于虚拟机。

*Debian

在Debian上、用户可以访问/etc/ntp.conf文件以获取NTP服务器详细信息。

ONTAP工具的密码策略9.13.

首次部署ONTAP工具或升级到9.12或更高版本的用户需要同时遵循管理员和数据库用户的强密码策略。在部署过程中、系统将提示新用户输入其密码。对于升级到9.12或更高版本的brownfield用户、维护控制台中将提供遵循强密码策略的选项。

- 用户登录maIT控制台后、系统将根据复杂规则集检查密码、如果发现未遵循此规则、则会要求用户重置相同密码。
- 密码默认有效期为90天、75天后、用户将开始收到更改密码的通知。
- 需要在每个周期设置新密码、系统不会将最后一个密码作为新密码。
- 每当用户登录maIT控制台时、它都会检查密码策略、如以下屏幕截图、然后再加载主菜单：


```
Maintenance Console : "Netapp ONTAP tools for VMware vSphere"
Discovered interfaces: eth0 (ENABLED)
validating password policies
```

- 如果发现不符合密码策略、或者不符合ONTAP工具9.11或更早版本的升级设置。然后、用户将看到以下屏幕以重置密码：

```
Your Administrator and Database password is expired or does not match password policy:
-----
1 ) Change 'administrator' user password
2 ) Change database password
x ) Exit
Enter your choice: _
```

- 如果用户尝试设置弱密码或再次提供最后一个密码、则用户将看到以下错误：

```
Changing password for administrator.
User: administrator
Enter new password:
Retype new password:
Password doesn't matches the password policy.
For security reasons, it is recommended to use a password that is of eight to thirty characters and
contains a minimum of one upper, one lower, one digit, and one special character.
Enter new password:
Retype new password:
Check if new decoder works ?
New decoder worked successfully
08-02/23 13:36:53 Your new password must be different
Error updating sra credential file
Press ENTER to continue._
```

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。