



FlexPod 数据中心

FlexPod

NetApp
March 25, 2024

目录

FlexPod 数据中心	1
采用 NetApp SnapMirror 业务连续性和 ONTAP 9.10 的 FlexPod 数据中心	1
采用VMware vSphere 7.0、Cisco VXLAN单站点网络结构和NetApp ONTAP 9.7的FlexPod 数据中心—设计	55
采用VMware vSphere 7.0和NetApp ONTAP 9.7的FlexPod Datacenter—部署	55
采用Cisco Intersight和NetApp ONTAP 9.7的FlexPod 数据中心—设计	56
采用Cisco Intersight和NetApp ONTAP 9.7的FlexPod Datacenter—部署	56
采用Cisco Intersight和NetApp ONTAP 9.7的FlexPod 数据中心—设计	56
采用VMware vSphere 6.7 U2、Cisco UCS four-generation Fabric和NetApp ONTAP 9.6的FlexPod Datacenter	57
采用VMware vSphere 6.7 U1、Cisco UCS第四代网络结构和NetApp AFF A系列的FlexPod Datacenter—设计	57
采用VMware vSphere 6.7 U1、Cisco UCS第四代网络结构和NetApp AFF A系列的FlexPod 数据中心	57
采用Cisco ACI Multi-Pod、NetApp MetroCluster IP和VMware vSphere 6.7的FlexPod 数据中心—设计	58
采用Cisco ACI Multi-Pod的FlexPod 数据中心、采用NetApp MetroCluster IP和VMware vSphere 6.7—部署	58

FlexPod 数据中心

采用 NetApp SnapMirror 业务连续性和 ONTAP 9.10 的 FlexPod 数据中心

TR-4920：采用 NetApp SnapMirror 业务连续性和 ONTAP 9.10 的 FlexPod 数据中心

NetApp 公司 Jyh-shing Chen

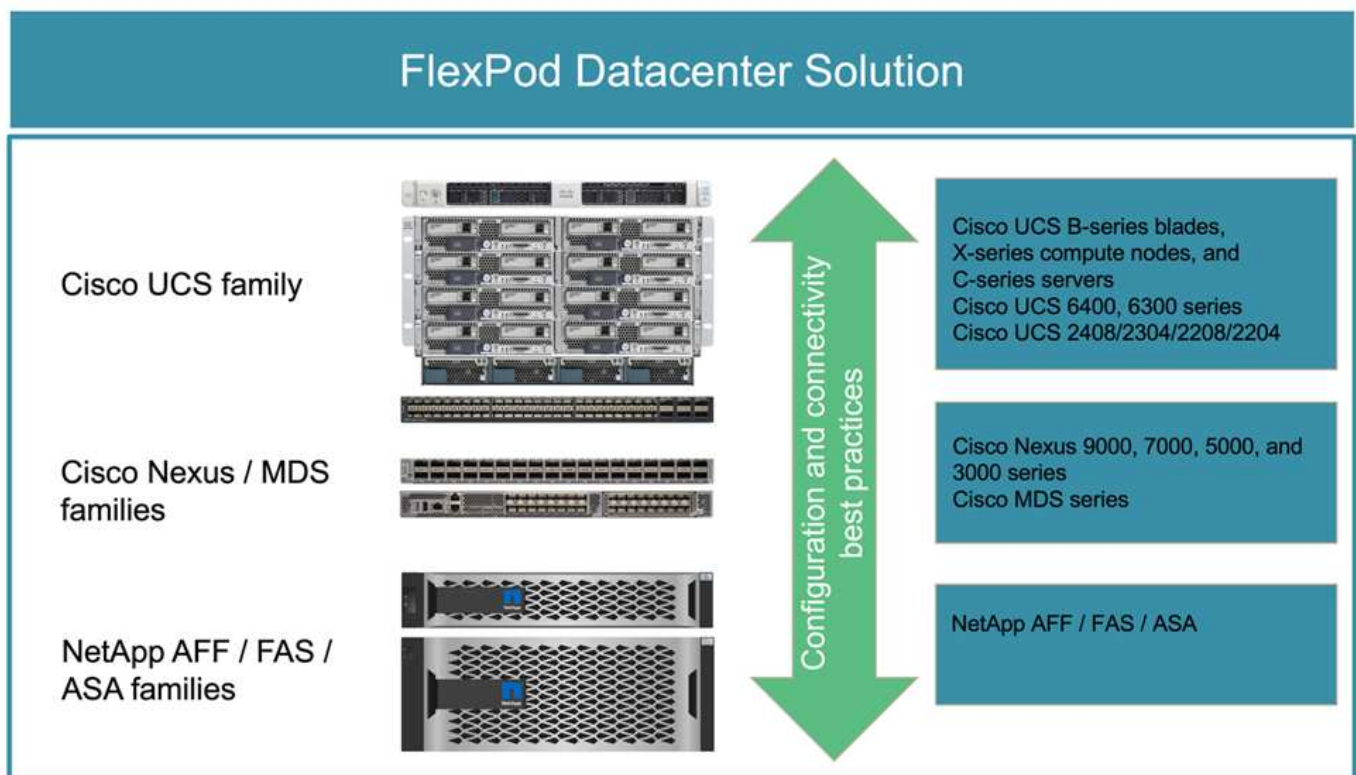
简介

FlexPod 解决方案

FlexPod 是一种最佳实践的融合基础架构数据中心架构，其中包括 Cisco 和 NetApp 的以下组件：

- Cisco Unified Computing System （ Cisco UCS ）
- Cisco Nexus 和 MDS 系列交换机
- NetApp FAS ， NetApp AFF 和 NetApp 全 SAN 阵列（ ASA ）系统

下图展示了用于创建 FlexPod 解决方案的一些组件。这些组件是根据 Cisco 和 NetApp 的最佳实践进行连接和配置的，可为放心运行各种企业工作负载提供理想的平台。



我们提供了大量的 Cisco 验证设计（CVD）和 NetApp 验证架构（NVA）产品组合。这些 CVD 和 NVA 涵盖所有主要数据中心工作负载，是 NetApp 和 Cisco 在 FlexPod 解决方案上持续协作和创新的成果。

FlexPod CVD 和 NVA 在其创建过程中融入了广泛的测试和验证，提供了参考解决方案 架构设计和分步部署指南，可帮助合作伙伴和客户部署和采用 FlexPod 解决方案。通过使用这些 CVD 和 NVA 作为设计和实施指南，企业可以降低风险，减少解决方案 停机时间，并提高所部署 FlexPod 解决方案的可用性，可扩展性，灵活性和安全性。

所示的每个 FlexPod 组件系列（Cisco UCS，Cisco Nexus /MDS 交换机和 NetApp 存储）都提供了平台和资源选项，用于纵向或横向扩展基础架构，同时支持 FlexPod 的配置和连接最佳实践所需的特性和功能。FlexPod 还可以通过部署更多 FlexPod 堆栈来横向扩展，以满足需要多个一致部署的环境的需求。

灾难恢复和业务连续性

企业可以采用多种方法来确保应用程序和数据服务能够从灾难中快速恢复。制定灾难恢复（DR）和业务连续性（Business Continuity，BC）计划，实施满足业务目标的解决方案 以及对灾难情形执行定期测试，可使企业在发生灾难后从灾难中恢复并继续提供关键业务服务。

对于不同类型的应用程序和数据服务，公司可能有不同的灾难恢复和业务连续性要求。在紧急情况或灾难情况下，可能不需要某些应用程序和数据，而在其他应用程序和数据中，则可能需要持续可用以满足业务需求。

对于无法提供的可能会中断业务的任务关键型应用程序和数据服务，需要仔细评估问题解答 问题，例如业务需要考虑的维护和灾难情形， 在发生灾难时，企业可以承受丢失多少数据，以及恢复可以和应该以多快的速度进行。

对于依靠数据服务创收的企业，可能需要使用解决方案 来保护数据服务，该不仅可以承受各种单点故障情形，还可以承受站点中断灾难情形，从而实现持续业务运营。

恢复点目标和恢复时间目标

恢复点目标（RPO）用于衡量您可以承受的丢失数据量，以及可以将数据恢复到的时间点。如果采用每日备份计划，企业可能会丢失一天的数据，因为上次备份以来对数据所做的更改可能会在灾难中丢失。对于业务关键型和任务关键型数据服务，您可能需要零 RPO 以及相关的计划和基础架构来保护数据而不会丢失任何数据。

恢复时间目标（Recovery Time Objective，RTO）用于衡量数据不可用的时间，或者数据服务必须恢复的速度。例如，一家公司可能会实施备份和恢复，由于其大小，因此会对某些数据集使用传统磁带。因此，要从备份磁带还原数据，可能需要几个小时，如果基础架构发生故障，甚至需要几天时间。除了还原数据之外，时间方面的考虑还必须包括恢复基础架构的时间。对于任务关键型数据服务，您可能需要极低的 RTO，因此只能允许数秒或数分钟的故障转移时间来快速恢复数据服务联机，以实现业务连续性。

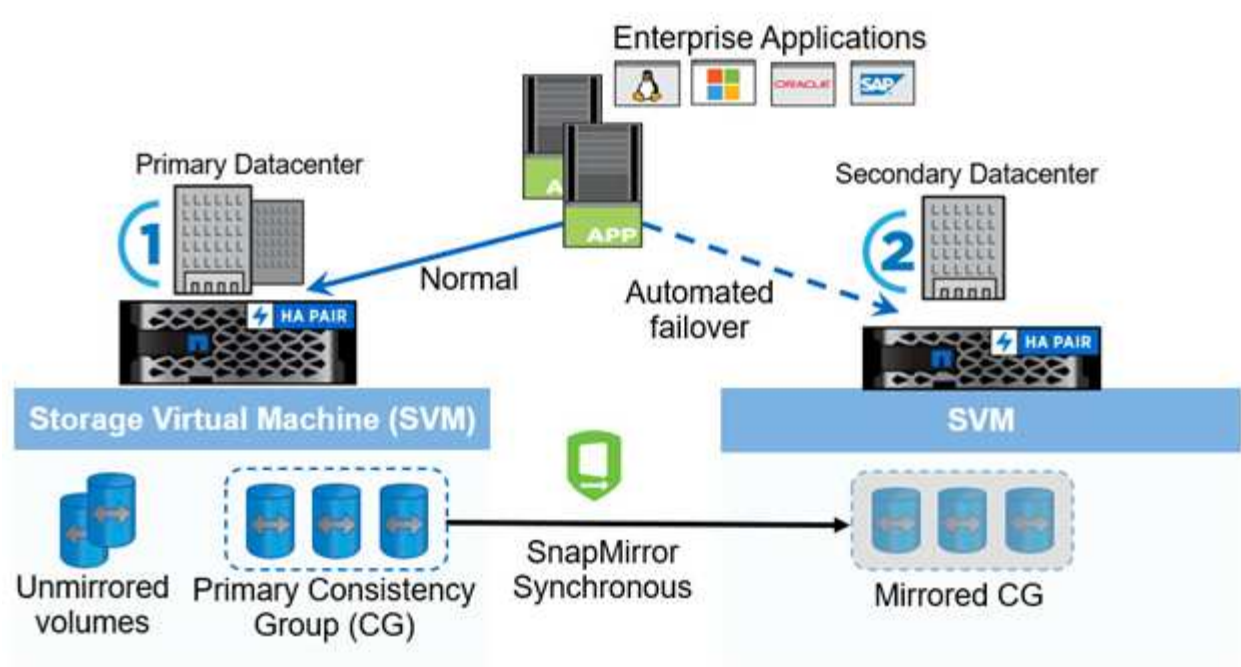
SM — BC

从 ONTAP 9.8 开始，您可以使用 NetApp SM-BC 保护 SAN 工作负载，以实现透明的应用程序故障转移。您可以在两个 AFF 集群或两个 ASA 集群之间创建一致性组关系，以实现数据复制，从而实现零 RPO 和接近零 RTO。

SM-BC 解决方案 可通过 IP 网络使用 SnapMirror 同步技术复制数据。它提供了应用程序级粒度和自动故障转移功能，可使用基于 iSCSI 或 FC 协议的 SAN LUN 保护业务关键型数据服务，例如 Microsoft SQL Server，Oracle 等。部署在第三个站点的 ONTAP 调解器可监控 SM-BC 解决方案，并在站点发生灾难时自动进行故障转移。

一致性组（Consistency Group，CG）是一组 FlexVol 卷，可为需要保护以实现业务连续性的应用程序工作负载提供写入顺序一致性保证。它可以在一个时间点同时为一组卷创建崩溃状态一致的 Snapshot 副本。源 CG 和目标 CG 之间建立了 SnapMirror 关系，也称为 CG 关系。选择作为 CG 一部分的一组卷可以映射到一个应用程序实例，一组应用程序实例或整个解决方案。此外，还可以根据业务需求和变更按需创建或删除 SM-BC 一致性组关系。

如下图所示，一致性组中的数据会复制到另一个 ONTAP 集群，以实现灾难恢复和业务连续性。这些应用程序可连接到两个 ONTAP 集群中的 LUN。I/O 通常由主集群提供服务，如果主集群发生灾难，则会自动从二级集群恢复。在设计 SM-BC 解决方案时，必须观察 CG 关系支持的对象计数（例如，最多 20 个 CG 和最多 200 个端点），以避免超过支持的限制。



"接下来： FlexPod SM-BC 解决方案 。"

FlexPod SM-BC 解决方案

"上一页： 简介。"

解决方案概述

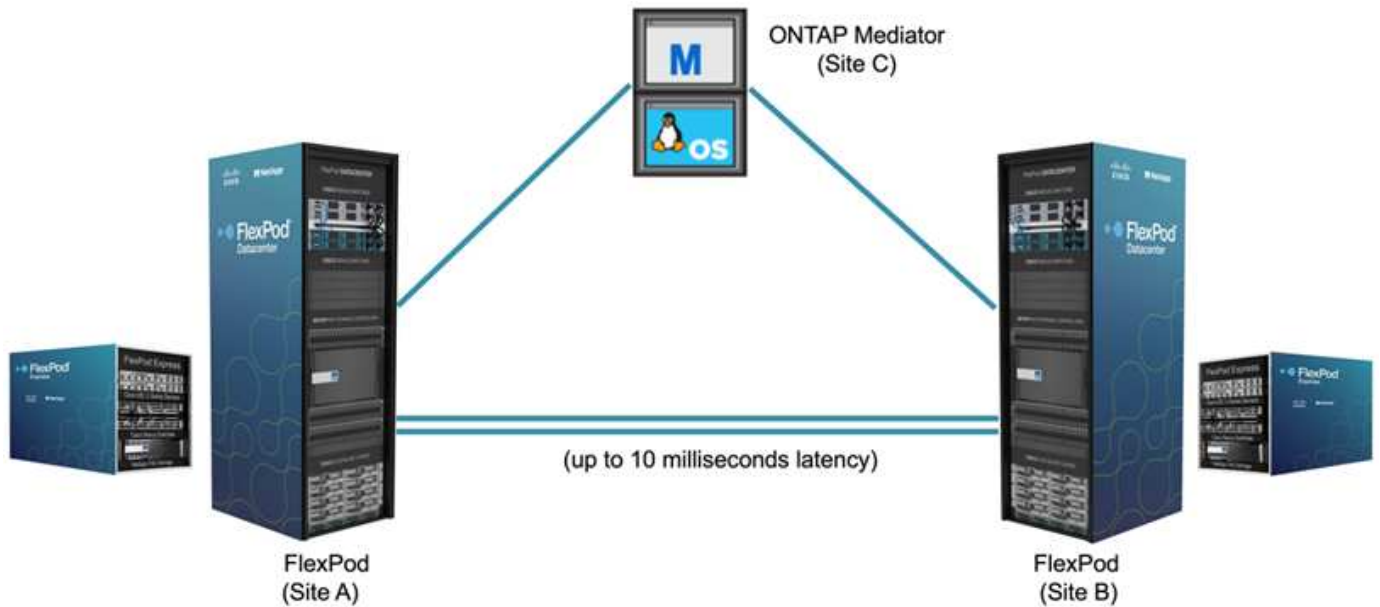
从较高的层面来看， FlexPod SM-BC 解决方案 由两个 FlexPod 系统组成，它们位于两个站点上，彼此连接并配对，可提供高度可用，高度灵活且高度可靠的数据中心解决方案，即使站点发生故障也能提供业务连续性。

除了部署两个新的 FlexPod 基础架构来创建 FlexPod SM-BC 解决方案 之外，还可以在与 SM-BC 兼容的两个现有 FlexPod 基础架构上实施解决方案，或者添加一个新的 FlexPod 以与现有 FlexPod 建立对等关系。

FlexPod SM-BC 解决方案 中的两个 FlexPod 系统无需在配置上完全相同。但是，两个 ONTAP 集群必须属于相同的存储系列，可以是两个 AFF 系统，也可以是两个 ASA 系统，但硬件型号不一定相同。SM-BC 解决方案 不支持 FAS 系统。

这两个 FlexPod 站点需要网络连接，以满足解决方案 带宽和服务质量要求，并且根据 ONTAP SM-BC 解决方案 的要求，站点之间的往返延迟不超过 10 毫秒（10 毫秒）。对于此 FlexPod SM-BC 解决方案 验证，两个 FlexPod 站点通过扩展的第 2 层网络在同一实验室中进行互连。

NetApp ONTAP SM-BC 解决方案 可在两个 NetApp 存储集群之间提供同步复制，以便在园区或城域区域实现高可用性和灾难恢复。部署在第三个站点的 ONTAP 调解器可监控解决方案，并在发生站点灾难时实现自动故障转移。下图简要展示了解决方案 组件。



借助 FlexPod SM-BC 解决方案，您可以在分布式且集成的基础架构上部署基于 VMware vSphere 的私有云。通过集成的解决方案，可以将多个站点作为一个解决方案基础架构进行协调，以保护数据服务免受各种单点故障情形和整个站点故障的影响。

本技术报告重点介绍了 FlexPod SM-BC 解决方案的一些端到端设计注意事项。我们鼓励从业人员参考各种 FlexPod CVD 和 NVA 中提供的信息，了解更多 FlexPod 解决方案实施详细信息。

虽然解决方案已通过根据 CVD 中记录的 FlexPod 最佳实践部署两个 FlexPod 系统进行了验证，但它会考虑到 SM-BC 解决方案的要求。本报告中讨论的已部署 FlexPod SM-BC 解决方案已在各种故障情形以及模拟站点故障情形下进行了故障恢复能力和容错验证。

解决方案要求

FlexPod SM-BC 解决方案旨在满足以下关键要求：

- 业务关键型应用程序和数据服务在发生完整数据中心（站点）故障时的业务连续性
- 灵活的分布式工作负载放置，可在数据中心之间移动工作负载
- 站点关联性，即在正常操作期间从同一数据中心站点本地访问虚拟机数据
- 在发生站点故障时快速恢复，不会丢失任何数据

解决方案组件

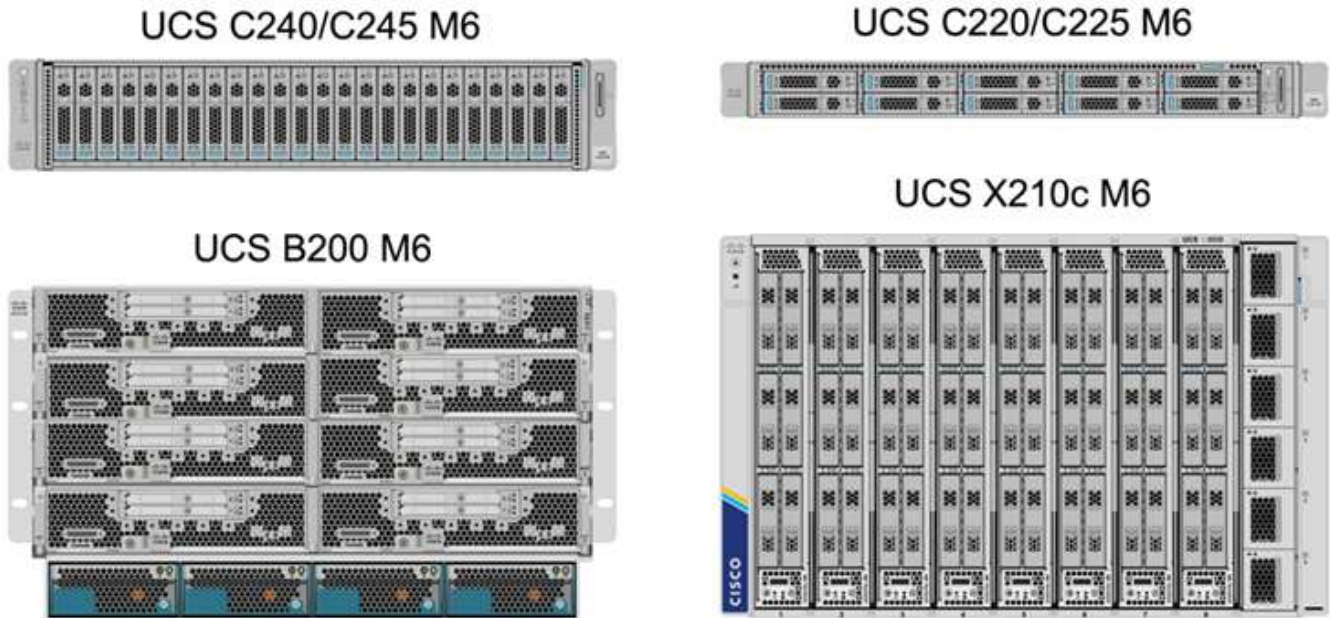
Cisco 计算组件

Cisco UCS 是一种集成计算基础架构，可提供统一计算资源，统一网络结构和统一管理。它使企业能够自动执行并加快应用程序部署，包括虚拟化和裸机工作负载。Cisco UCS 支持多种部署用例，包括远程和分支机构，数据中心和混合云用例。根据特定的解决方案要求，FlexPod Cisco 计算实施可以使用不同规模的各种组件。以下各小节提供了某些 UCS 组件上的追加信息。

UCS 服务器和计算节点

下图显示了 UCS 服务器组件的一些示例，包括 UCS C 系列机架式服务器，采用 B 系列刀片式服务器的 UCS 5108 机箱以及采用 X 系列计算节点的新 UCS X9508 机箱。Cisco UCS C 系列机架式服务器采用一个和两个机

架单元（RU）外形规格，采用 Intel 和 AMD CPU 型号，并具有各种 CPU 速度和核心，内存和 I/O 选项。Cisco UCS B 系列刀片式服务器和新的 X 系列计算节点还具有各种 CPU ，内存和 I/O 选项，它们在 FlexPod 架构中均受支持，可满足各种业务需求。



除了此图所示的最新一代 C220/C225/C240/C245 M6 机架式服务器， B200 M6 刀片式服务器和 X210c 计算节点之外，如果仍然支持前几代机架式和刀片式服务器，也可以使用它们。

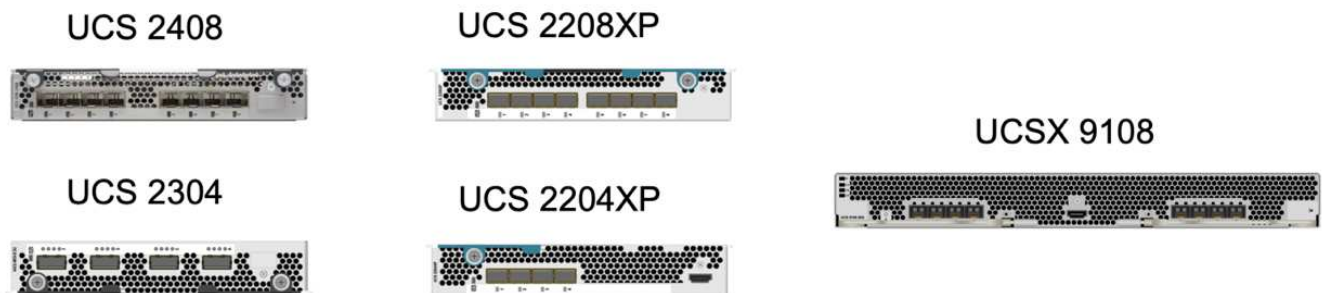
I/O 模块和智能网络结构模块

I/O 模块（ IOM ） / 阵列扩展器和智能阵列模块（ IFM ） 分别为 Cisco UCS 5108 刀片式服务器机箱和 Cisco UCS X9508 X 系列机箱提供统一的网络结构连接。

第四代 UCS IOM 2408 具有八个 25-G 统一以太网端口，用于通过互联阵列（ Fabric Interconnect ， FI ） 连接 UCS 5108 机箱。每个 2408 都通过中板与机箱中的每个刀片式服务器建立了四个 10-G 背板以太网连接。

UCSX 9108 25G IFM 具有八个 25-G 统一以太网端口，用于通过互联阵列连接 UCS X9508 机箱中的刀片式服务器。每个 9108 都有四个 25 G 连接，连接到 X9108 机箱中的每个 UCS X210c 计算节点。9108 IFM 还可与互联阵列配合使用来管理机箱环境。

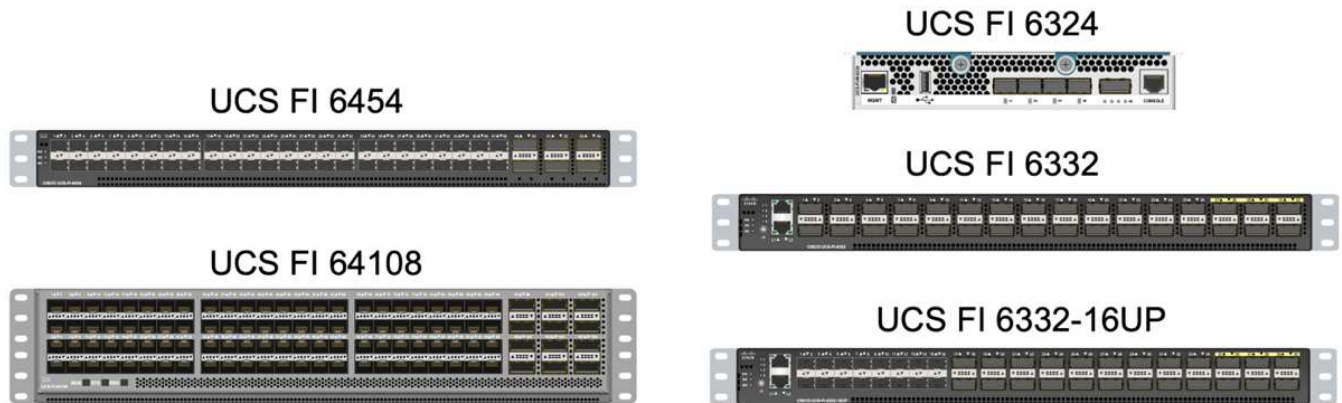
下图显示了 UCS 5108 机箱的 UCS 2408 及更早版本 IOM 以及 X9508 机箱的 9108 IFM 。



UCS 互联阵列

Cisco UCS 互联阵列（Fabric Interconnects，CLI）可为整个 Cisco UCS 提供连接和管理功能。通常作为主动 / 主动对部署，系统的 CLI 会将所有组件集成到一个由 Cisco UCS Manager 或 Cisco Intersight 控制的高可用性管理域中。Cisco UCS CLI 为系统提供一个统一网络结构，具有低延迟和无损的直通交换功能，可使用一组缆线支持 LAN，SAN 和管理流量。

第四代 Cisco UCS FI 有两种变体：UCS FI 6454 和 64108。其中包括支持 10/25 Gbps 以太网端口，1/25-Gbps 以太网端口，40/100-Gbps 以太网上行链路端口以及可支持 10/25 千兆以太网或 8/16/32-Gbps 光纤通道的统一端口。下图显示了第四代 Cisco UCS CLI 以及也支持的第三代型号。



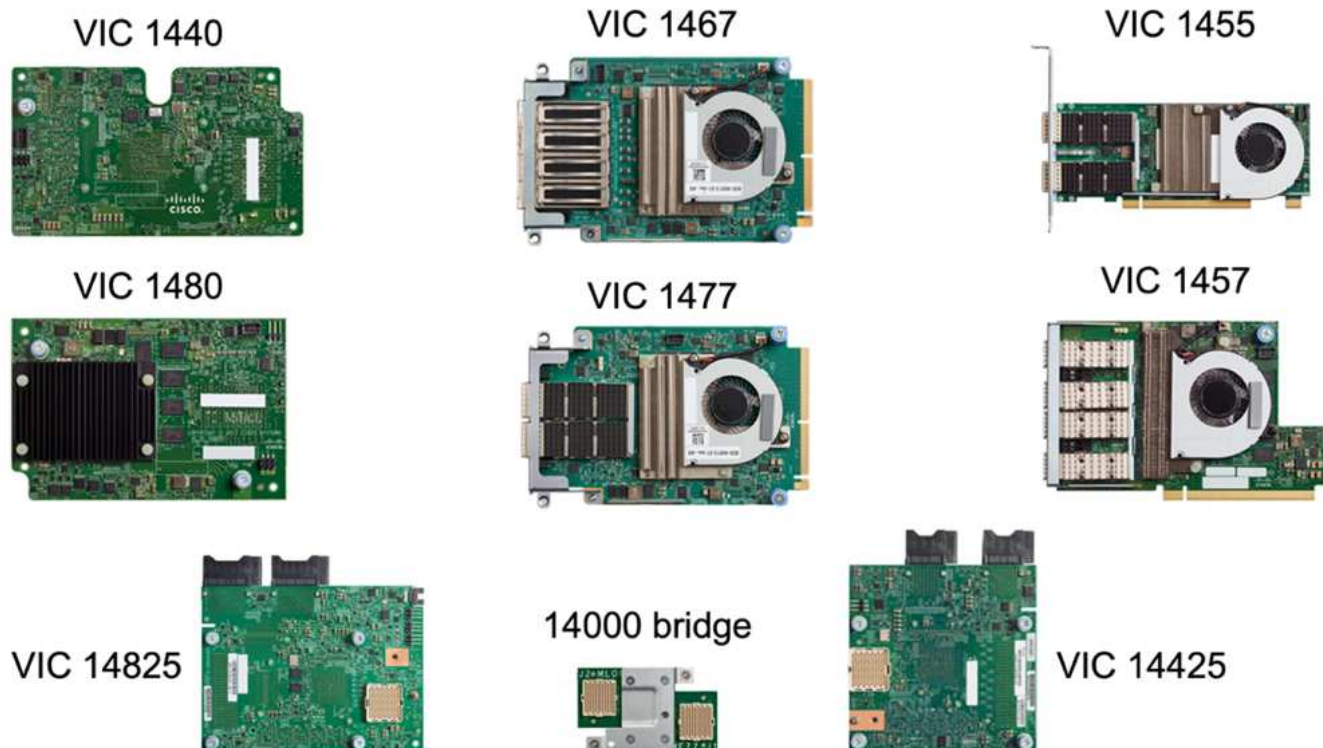
要支持 Cisco UCS X 系列机箱，需要在 Intersight Managed Mode（IMM）下配置第四代互联阵列。但是，在 IMM 模式和 UCSM 托管模式下均可支持 Cisco UCS 5108 B 系列机箱。



UCS FI 6324 采用 IOM 外形规格，并嵌入在 UCS Mini 机箱中，适用于仅需要小型 UCS 域的部署。

UCS 虚拟接口卡

Cisco UCS 虚拟接口卡（Virtual Interface Card，VIC）可为机架式和刀片式服务器统一系统管理以及 LAN 和 SAN 连接。它最多支持 256 个虚拟设备，可以作为虚拟网络接口卡（Virtual Network Interface Card，vNIC），也可以作为使用 Cisco SingleConnect 技术的虚拟主机总线适配器（Virtual Host Bus Adapter，vHBA）。通过虚拟化，VIC 卡大大简化了网络连接，并减少了解决方案部署所需的网络适配器，缆线和交换机端口的数量。下图显示了一些可用于 B 系列和 C 系列服务器以及 X 系列计算节点的 Cisco UCS VIC。



不同的适配器型号支持不同的刀片式服务器和机架服务器，它们具有不同的端口数，端口速度以及模块化主板 LAN（mLOM），夹层卡和 PCIe 接口的外形规格。这些适配器可以支持 10/25/40/100-G 以太网和以太网光纤通道（FCoE）的某些组合。它们整合了 Cisco 的融合网络适配器（Converged Network Adapter，CNA）技术，支持全面的功能集，并简化了适配器管理和应用程序部署。例如，VIC 支持 Cisco 的 Data Center Virtual Machine Fabric Extender（VM-FEX）技术，该技术可将 Cisco UCS 互联阵列端口扩展到虚拟机，从而简化服务器虚拟化部署。

通过在 mLOM，夹层和端口扩展器以及网桥卡配置中组合使用 Cisco VIC，您可以充分利用刀片式服务器可用的带宽和连接。例如，通过使用 VIC 14825（mLOM）和 14425（夹层）上的两个 25-G 链路以及 X210c 计算节点上的 14000（网桥卡），VIC 总带宽为 $2 \times 50\text{-G} + 2 \times 50\text{-G}$ ，或者，采用双 IFM 配置时，每个网络结构 /IFM 需要 100 G，而每个服务器总共需要 200 G。

有关 Cisco UCS 产品系列，技术规格和文档的详细信息，请参见 "[Cisco UCS](#)" 有关信息，请访问网站。

Cisco 交换组件

Nexus 交换机

FlexPod 使用 Cisco Nexus 系列交换机为 Cisco UCS 和 NetApp 存储控制器之间的通信提供以太网交换网络结构。FlexPod 部署支持当前支持的所有 Cisco Nexus 交换机型号，包括 Cisco Nexus 3000，5000，7000 和 9000 系列。

在为 FlexPod 部署选择交换机型号时，需要考虑许多因素，例如性能，端口速度，端口密度，交换机延迟，以及 ACI 和 VXLAN 支持等协议，以实现您的设计目标以及交换机的支持时间跨度。

许多最新的 FlexPod CVD 均使用 Cisco Nexus 9000 系列交换机进行验证，例如 Nexus 9336C-fx2 和 Nexus 93180YC-fx3，这些交换机可在紧凑的 1U 外形规格中提供高性能 40/100G 和 10/25G 端口，低延迟和卓越的能效。可通过上行链路端口和分支缆线支持其他速度。下图显示了几个 Cisco Nexus 9k 和 3k 交换机，包括用于此验证的 Nexus 9336C-x2 和 Nexus 3232C。

Nexus 9336C-FX2



Nexus 93180YC-FX3



Nexus 3232C



请参见 ["Cisco 数据中心交换机"](#) 有关可用 Nexus 交换机及其规格和文档的详细信息。

MDS 交换机

Cisco MDS 9100/9200/9300 系列光纤交换机是 FlexPod 架构中的一个可选组件。这些交换机高度可靠，高度灵活，安全，可提供对网络结构中流量的可见性。下图显示了一些示例 MDS 交换机，这些交换机可用于为 FlexPod 解决方案 构建冗余 FC SAN 网络结构，以满足应用程序和业务需求。

MDS 9132T



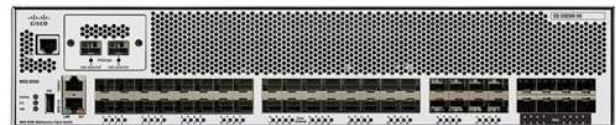
MDS 9148T



MDS 9148S



MDS 9250i



MDS 9396T



Cisco MDS 9132T/9148T/9396T 高性能 32G 多层光纤交换机经济高效，并且高度可靠，灵活且可扩展。高级存储网络特性和功能易于管理，并与整个 Cisco MDS 9000 系列产品组合兼容，可实现可靠的 SAN 实施。

这款下一代硬件平台内置了一流的 SAN 分析和遥测功能。通过检查帧报头提取的遥测数据可以流式传输到分析可视化平台，包括 Cisco Data Center Network Manager。FlexPod 还支持支持 16G FC 的 MDS 交换机，例如 MDS 9148S。此外，除了 FC 协议之外，还支持 FCoE 和 FCIP 协议的多服务 MDS 交换机（例如 MDS 9250i）也属于 FlexPod 解决方案 产品组合。

在 9132T 和 9396T 等半模块化 MDS 交换机上，可以添加额外的端口扩展模块和端口许可证以支持额外的设备连接。在 9148T 等固定交换机上，可以根据需要添加其他端口许可证。这种按需购买的灵活性提供了一个运营支出部分，有助于降低实施和运行基于 MDS 交换机的 SAN 基础架构的资本支出。

请参见 ["Cisco MDS 光纤交换机"](#) 有关可用 MDS 光纤交换机的详细信息，请参见 ["NetApp IMT"](#) 和 ["Cisco 硬件和软件兼容性列表"](#) 有关支持的 SAN 交换机的完整列表。

NetApp 组件

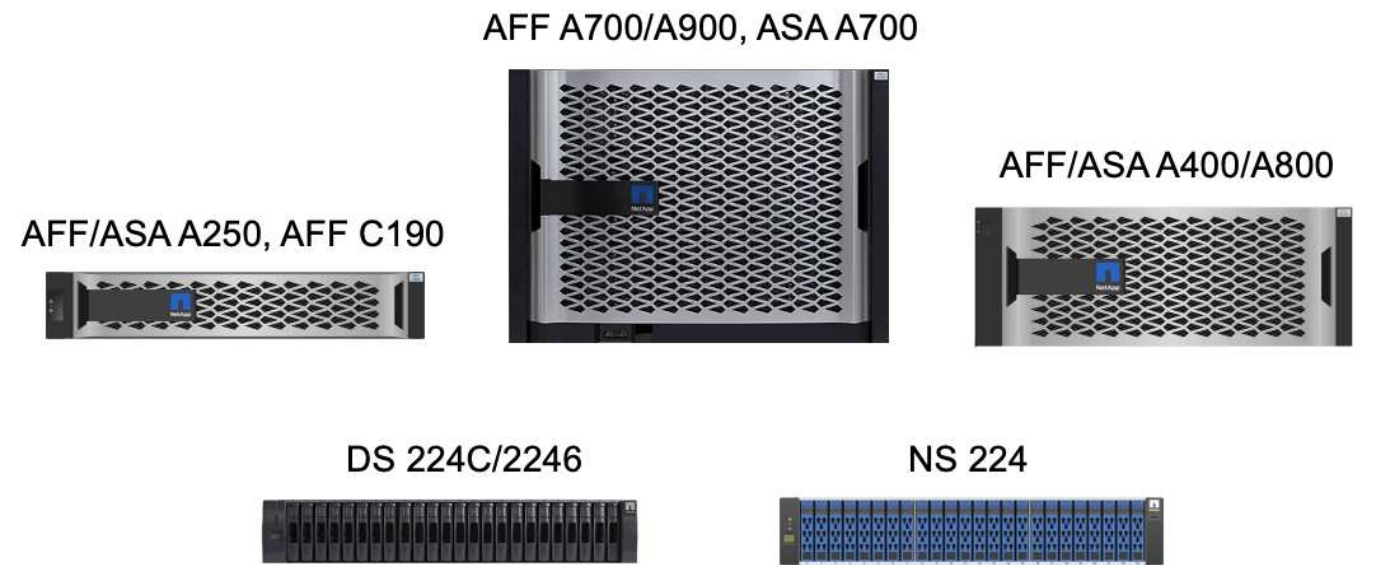
要创建 FlexPod SM-BC 解决方案，需要运行 ONTAP 软件 9.8 或更高版本的冗余 NetApp AFF 或 ASA 控制器。建议在 SM-BC 部署中使用最新的 ONTAP 版本（当前为 9.10.1），以便利用 ONTAP 持续创新，性能和质

量改进以及增加的最大对象数量来支持 SM-BC 。

NetApp AFF 和 ASA 控制器具有行业领先的性能和创新功能，可提供企业级数据保护和功能丰富的数据管理功能。AFF 和 ASA 系统支持端到端 NVMe 技术，包括 NVMe 连接 SSD 和基于光纤通道的 NVMe （ NVMe/FC ）前端主机连接。通过采用基于 NVMe/FC 的 SAN 基础架构，您可以提高工作负载吞吐量并减少 I/O 延迟。但是，基于 NVMe/FC 的数据存储库当前只能用于不受 SM-BC 保护的工作负载，因为 SM-BC 解决方案 当前仅支持 iSCSI 和 FC 协议。

NetApp AFF 和 ASA 存储控制器还为客户提供了一个混合云基础，让他们可以利用 NetApp Data Fabric 带来的无缝数据移动性。借助 Data Fabric ，您可以轻松地将数据从数据生成的边缘获取到使用数据的核心和云，从而利用按需弹性计算以及 AI 和 ML 功能，获得切实可行的业务洞察力。

如下图所示， NetApp 提供了各种存储控制器和磁盘架，可满足您的性能和容量要求。有关 NetApp AFF 和 ASA 控制器功能和规格的信息，请参见下表以获取产品页面的链接。

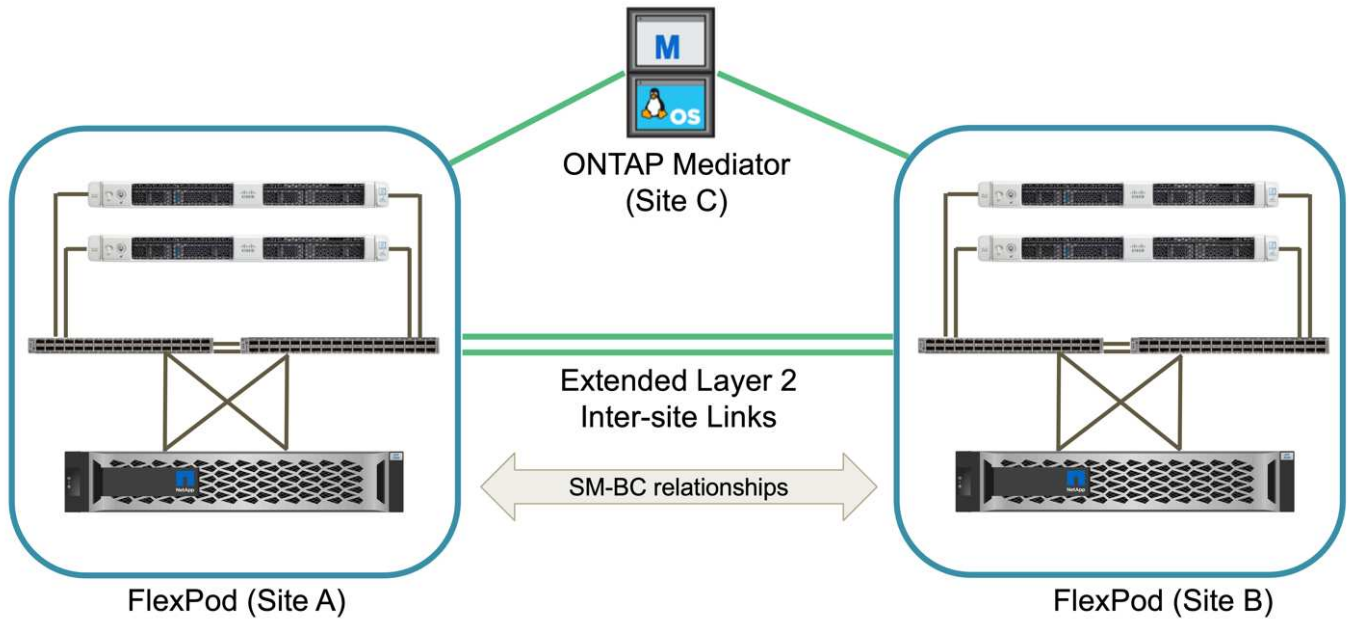


产品系列	技术规格
AFF 系列	"AFF 系列文档"
ASA 系列	"ASA 系列文档"

请参见 ["NetApp 磁盘架和存储介质文档"](#) 和 ["NetApp Hardware Universe"](#) 有关每个存储控制器型号的磁盘架和支持的磁盘架的详细信息。

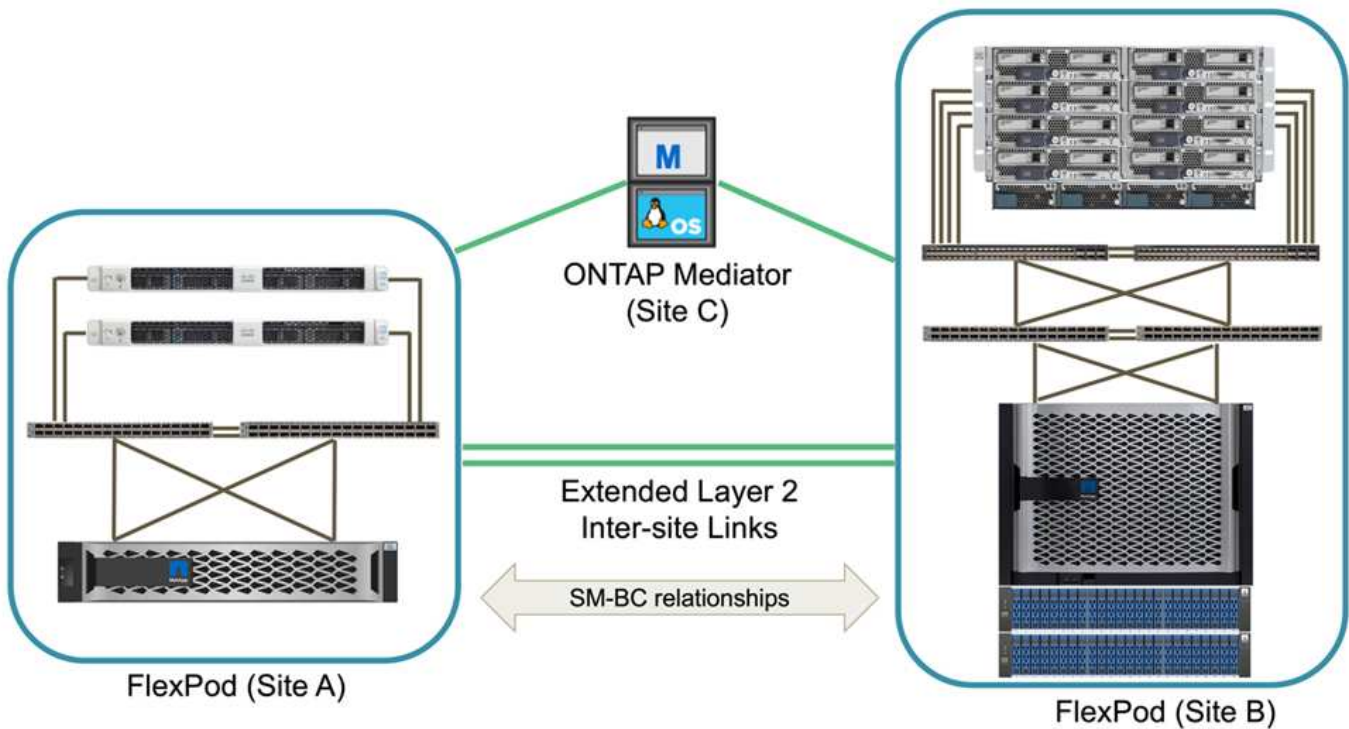
解决方案 拓扑

FlexPod 解决方案的拓扑结构十分灵活，可以纵向扩展或横向扩展以满足不同的解决方案 要求。如果解决方案需要业务连续性保护，并且只需要最少的计算和存储资源，则可以使用简单的解决方案 拓扑，如下图所示。这种简单的拓扑结构使用 UCS C 系列机架服务器和 AFF/ASA 控制器，并在控制器中使用 SSD ，而无需额外的磁盘架。



冗余计算，网络和存储组件通过组件之间的冗余连接互连在一起。这种高可用性设计可提供解决方案 故障恢复能力，并使 IT 能够承受单点故障情形。多站点设计和 ONTAP SM-BC 同步数据复制关系可提供业务关键型数据服务，尽管可能会发生单站点存储故障。

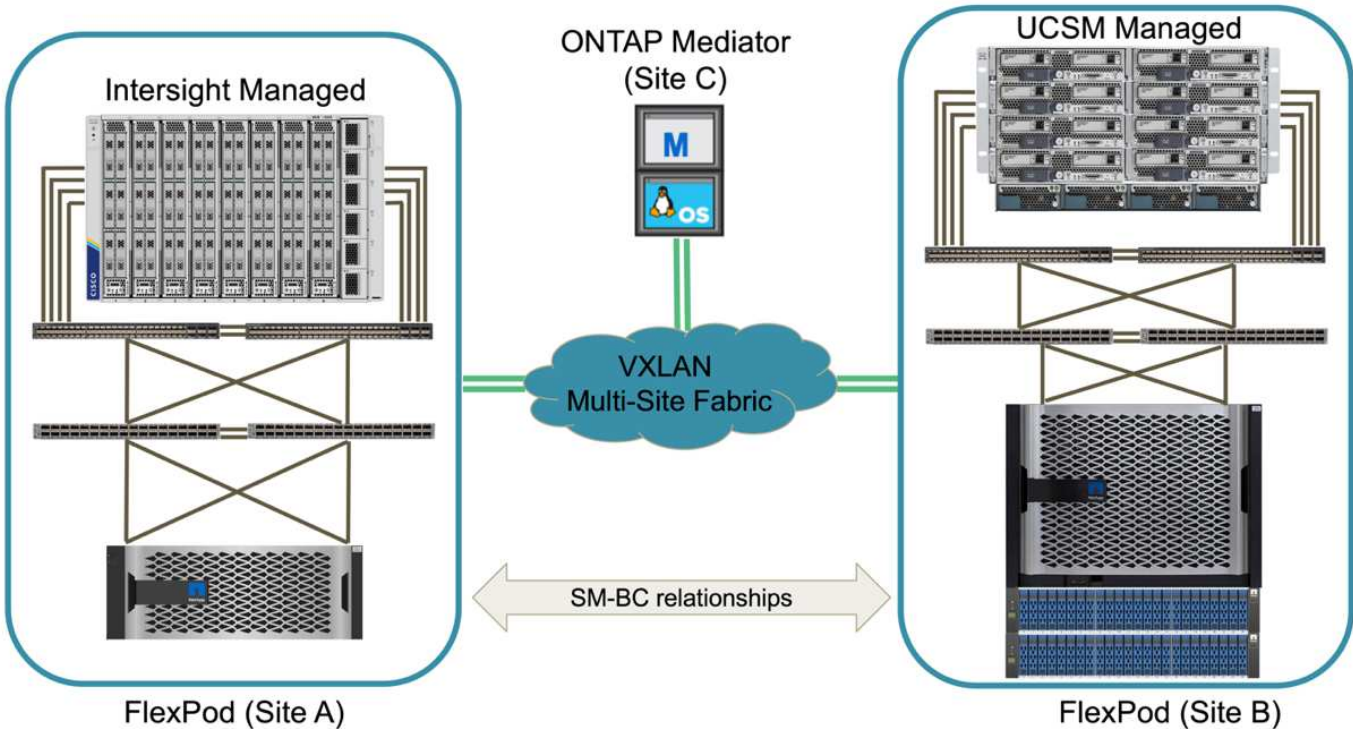
在城域中，数据中心和分支机构之间的公司可能使用的非对称部署拓扑可能如下图所示。对于这种非对称设计，数据中心需要具有更多计算和存储资源的更高性能 FlexPod。但是，分支机构的需求较低，并且 FlexPod 可以小得多。



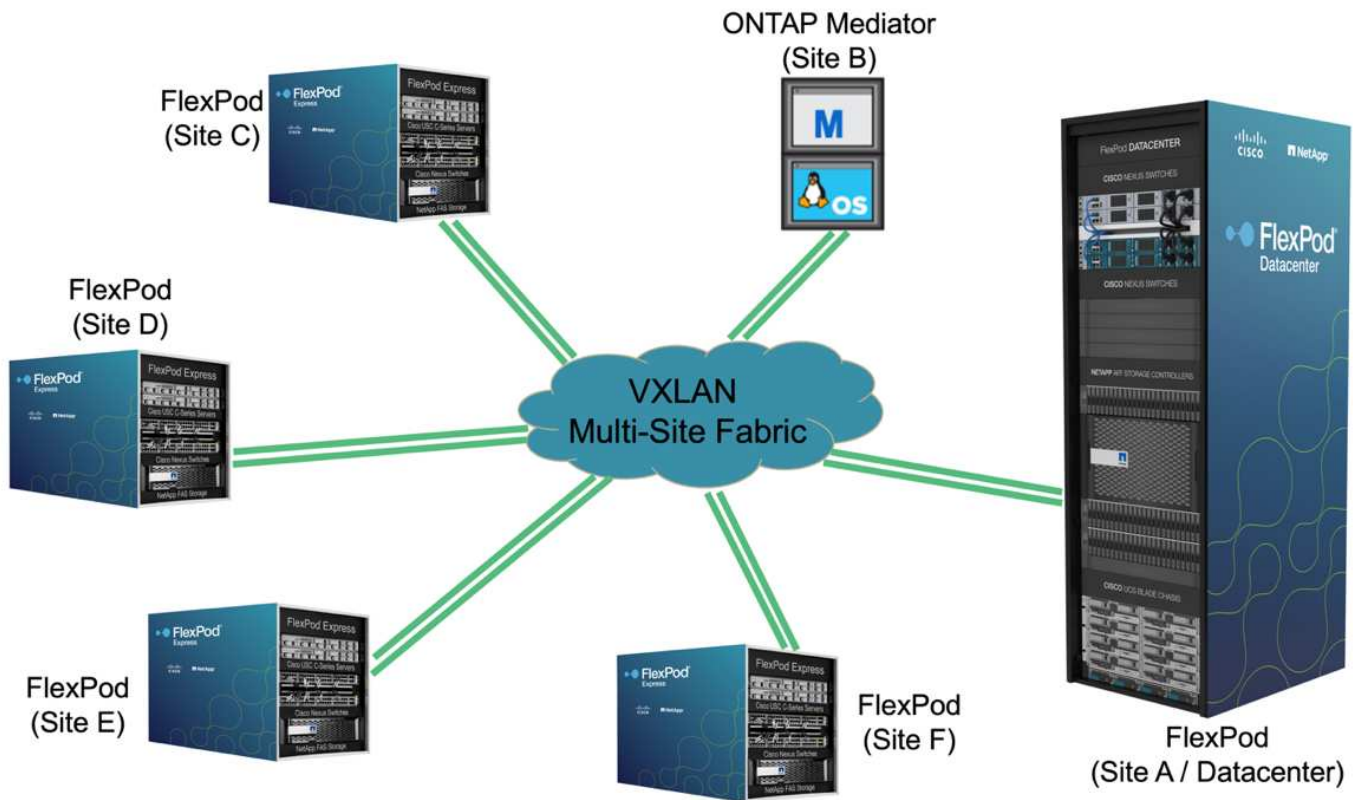
对于计算和存储资源需求较高的公司以及多个站点，基于 VXLAN 的多站点网络结构可以使多个站点拥有无缝网络结构，从而提高应用程序的移动性，从而可以从任何站点为应用程序提供服务。

可能存在使用 Cisco UCS 5108 机箱和 B 系列刀片式服务器的现有 FlexPod 解决方案，这些服务器必须受新

FlexPod 实例的保护。新的 FlexPod 实例可以使用最新的 UCS X9508 机箱，其中 X210c 计算节点由 Cisco Intersight 管理，如下图所示。在这种情况下，每个站点上的 FlexPod 系统都连接到一个更大的数据中心网络结构，而这些站点则通过互连网络进行连接，形成一个 VXLAN 多站点网络结构。



对于在域中设有数据中心和多个分支机构的公司，这些公司都需要受到保护才能提供业务连续性， 可以实施下图所示的 FlexPod SM-BC 部署拓扑，以保护关键应用程序和数据服务，使所有分支站点实现零 RPO 和接近零 RTO 目标。



对于此部署模式，每个分支机构都与数据中心建立所需的 SM-BC 关系和一致性组。您必须考虑支持的 SM-BC 对象限制，以便整体一致性组关系和端点计数不会超过数据中心支持的最大值。

"接下来：解决方案 验证概述。"

解决方案验证

解决方案 验证—概述

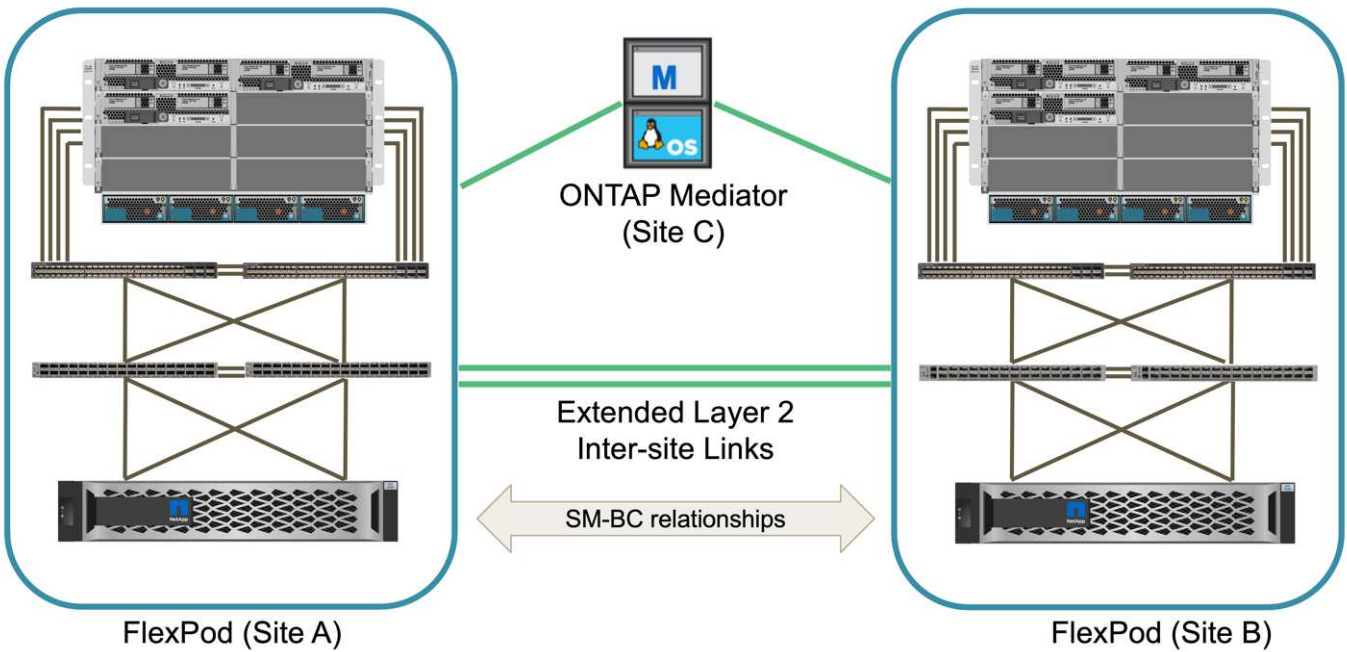
"先前版本：FlexPod SM-BC 解决方案。"

FlexPod SM-BC 解决方案 的设计和 implement 详细信息取决于具体的 FlexPod 情况配置和解决方案 目标。在定义了一般业务连续性要求之后，可以通过以下方式创建 FlexPod SM-BC 解决方案：使用两个新的 FlexPod 系统实施全新的解决方案，在另一个站点添加新的 FlexPod 以与现有 FlexPod 配对，或者将两个现有 FlexPod 系统配对在一起。

由于 FlexPod 解决方案在配置方面具有灵活性，因此可以使用所有受支持的 FlexPod 配置和组件。本节其余部分将提供有关对基于 VMware 的虚拟基础架构解决方案 执行实施验证的信息。除了与 SM-BC 相关的方面之外，此实施遵循标准 FlexPod 部署流程。请查看适用于您的特定配置的可用 FlexPod CVD 和 NVA，了解一般 FlexPod 实施详细信息。

验证拓扑

为了验证 FlexPod SM-BC 解决方案，我们会使用 NetApp，Cisco 和 VMware 提供的受支持技术组件。解决方案 具有运行 ONTAP 9.10.1 的 NetApp AFF A250 HA 对，站点 A 的双 Cisco Nexus 9336C-f2 交换机和站点 B 的双 Cisco Nexus 3232C 交换机以及两个站点的 Cisco UCS 6454 FI，和三个 Cisco UCS B200 M5 服务器，这些服务器位于运行 VMware vSphere 7.0u2 并由 UCS Manager 和 VMware vCenter 服务器管理的每个站点上。下图显示了组件级解决方案 验证拓扑，其中两个 FlexPod 系统在站点 A 上运行，站点 B 通过扩展的第 2 层站点间链路连接，ONTAP 调解器在站点 C 上运行



硬件和软件：

下表列出了用于解决方案 验证的硬件和软件。请务必注意， Cisco ， NetApp 和 VMware 都具有互操作性表，用于确定是否支持任何特定的 FlexPod 实施：

- ["http://support.netapp.com/matrix/"](http://support.netapp.com/matrix/)
- ["Cisco UCS 硬件和软件互操作性工具"](#)
- ["http://www.vmware.com/resources/compatibility/search.php"](http://www.vmware.com/resources/compatibility/search.php)

类别	组件	软件版本	数量
计算	Cisco UCS 互联阵列 6454	4.2 (1f)	4 个 (每个站点 2 个)
	Cisco UCS B200 M5 服务器	4.2 (1f)	6 个 (每个站点 3 个)
	Cisco UCS IOM 2204XP	4.2 (1f)	4 个 (每个站点 2 个)
	Cisco VIC 1440 (PID : UCSB-MLOM-40G-04)	5.2 (1a)	2 个 (每个站点 1 个)
	Cisco VIC 1340 (PID : UCSB-MLOM-40G-03)	4.5 (1a)	4 个 (每个站点 2 个)
网络	Cisco Nexus 9336C-x2	9.3 (6)	2 (站点 A)
	Cisco Nexus 3232C	9.3 (6)	2 (站点 B)
存储	NetApp AFF A250	9.10.1	4 个 (每个站点 2 个)
	NetApp System Manager	9.10.1	2 个 (每个站点 1 个)
	NetApp Active IQ Unified Manager	9.10.	1.
	适用于 VMware vSphere 的 NetApp ONTAP 工具	9.10.	1.
	适用于 VMware vSphere 的 NetApp SnapCenter 插件	4.6	1.
	NetApp ONTAP 调解器	1.3	1.
	NAbox	3.0.2	1.
虚拟化	NetApp 收获	21.11.1-1	1.
	VMware ESXi	7.0U2	6 个 (每个站点 3 个)
	VMware ESXi nenic 以太网驱动程序	1.0.35.0	6 个 (每个站点 3 个)
	VMware vCenter	7.0U2	1.
	适用于 VMware VAAI 的 NetApp NFS 插件	2.0	6 个 (每个站点 3 个)
测试	Microsoft Windows	2022 年	1.
	Microsoft SQL Server	2019 年	1.

类别	组件	软件版本	数量
	Microsoft SQL Server Management Studio	18.10	1.
	HammerDB	4.3	1.
	Microsoft Windows	10	6 个（每个站点 3 个）
	IOmeter	1.1.0	6 个（每个站点 3 个）

"接下来：解决方案 验证—计算。"

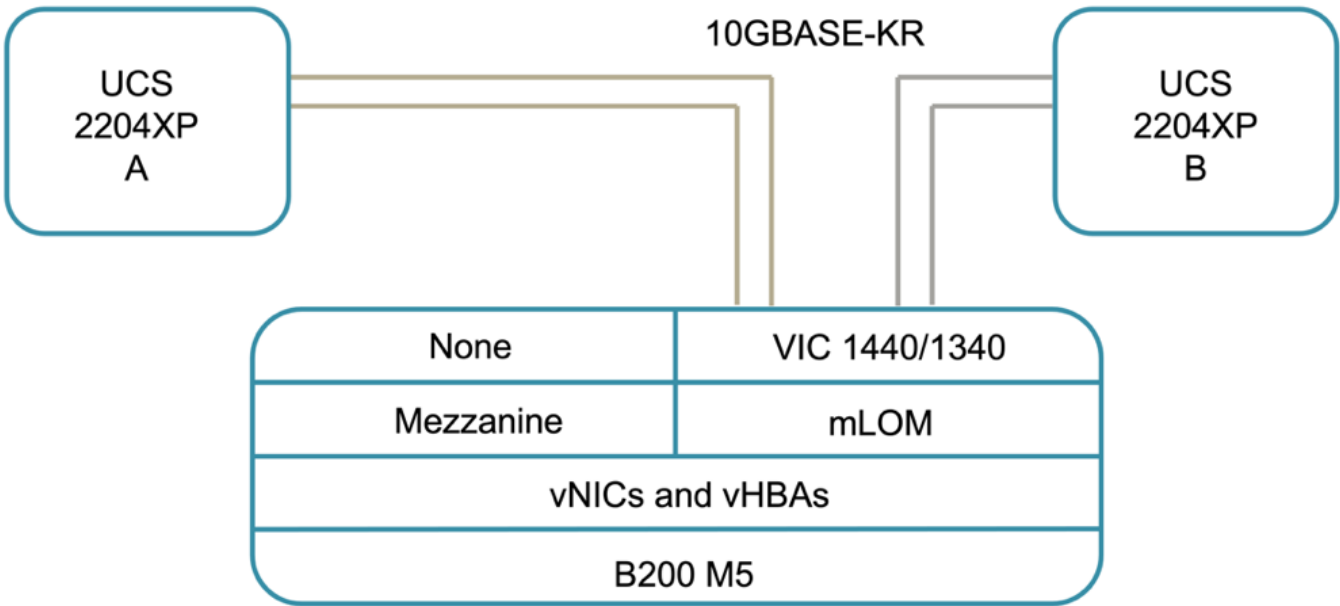
解决方案 验证—计算

"Previous：解决方案 验证—概述。"

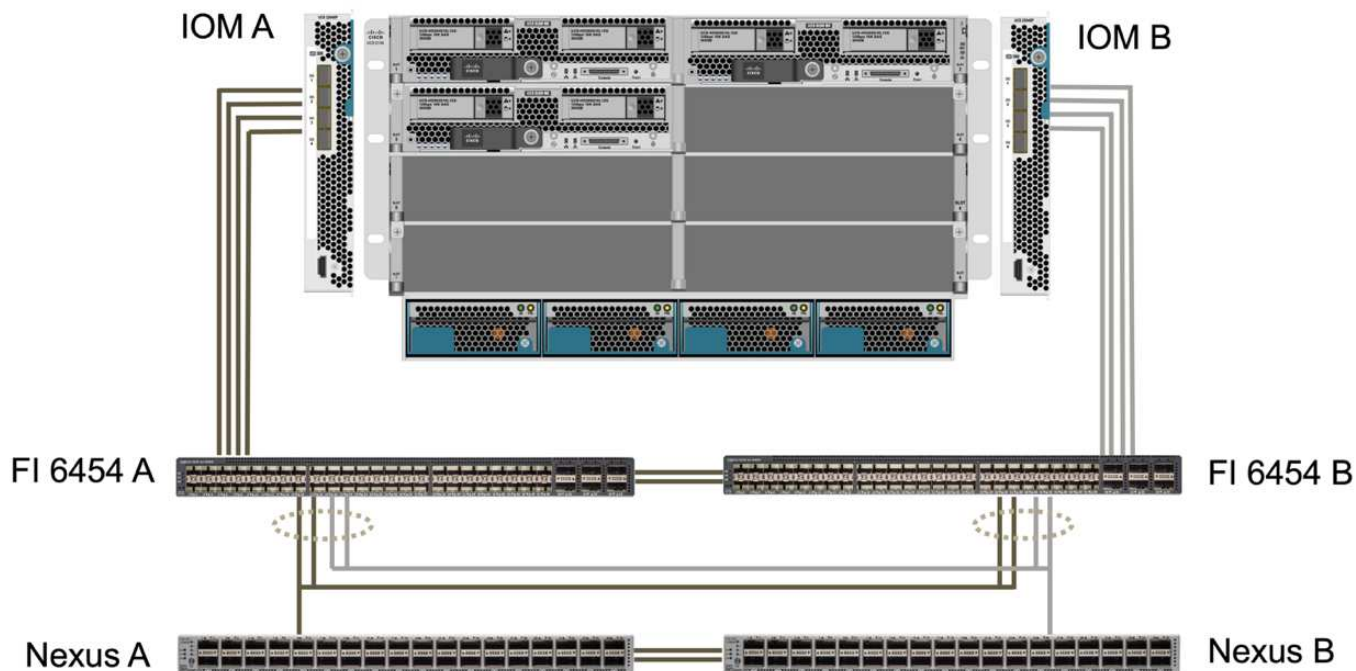
FlexPod SM-BC 解决方案 的计算配置遵循典型的 FlexPod 解决方案 最佳实践。以下各节重点介绍了用于验证的一些连接和配置。此外，还重点介绍了与 SM-BC 相关的一些注意事项，以提供实施参考和指导。

连接

UCS B200 刀片式服务器与 IOM 之间的连接由 UCS VIC 卡通过 UCS 5108 机箱背板连接提供。用于验证的 UCS 2204XP 阵列扩展器具有 16 个 10 G 端口，每个端口可连接到八个半宽刀片式服务器，例如，每个服务器两个。为了增加服务器连接带宽，可以添加一个基于夹层的额外 VIC，将服务器连接到备用 UCS 2408 IOM，该 IOM 可为每个服务器提供四个 10G 连接。



UCS 5108 机箱与用于验证的 UCS 6454 FI 之间的连接由使用四个 10G 连接的 IOM 2204XP 提供。FI 端口 1 到 4 已配置为这些连接的服务器端口。FI 端口 25 到 28 配置为本地站点的 Nexus 交换机 A 和 B 的网络上行链路端口。下图和表提供了要连接到 UCS 5108 机箱和 Nexus 交换机的 UCS 6454 CLI 的连接图和端口连接详细信息。



本地设备	本地端口	远程设备	远程端口
UCS 6454 FI A	1.	IOM A	1.
	2.		2.
	3.		3.
	4.		4.
	25.	Nexus A	1/13/1
	26		1/2/1/13/2
	27	Nexus B	1/13/3
	28		1/13/4
UCS 6454 FI B	L1	UCS 6454 FI B	L1
	L2		L2
	1.	IOM B	1.
	2.		2.
	3.		3.
	4.		4.
	25.	Nexus A	1/13/3
	26		1/13/4
UCS 6454 FI B	27	Nexus B	1/13/1
	28		1/2/1/13/2
	L1	UCS 6454 FI A	L1

本地设备	本地端口	远程设备	远程端口
	L2		L2



尽管站点 A 使用的是 Nexus 9336C-FX 2 交换机，而站点 B 使用的是 Nexus 3232C 交换机，但上述连接对于站点 A 和 B 都是相似的。使用 40G 到 4x10G 分支缆线进行 Nexus 到 FI 连接。连接到 Nexus 的 FI 会利用端口通道，并且在 Nexus 交换机上配置了虚拟端口通道，以便将连接聚合到每个 FI。



如果使用的是 IOM，FI 和 Nexus 交换机组件的不同组合，请务必对环境组合使用适当的缆线和端口速度。



可以使用支持高速连接或更多连接的组件来增加带宽。通过添加与支持冗余的组件的附加连接，可以实现更多冗余。

服务配置文件

使用 UCS Manager（UCSM）或 Cisco Intersight 管理的互联阵列的刀片式服务器机箱可以使用 UCSM 中提供的服务配置文件和 Intersight 中的服务器配置文件对服务器进行抽象化。此验证使用 UCSM 和服务配置文件来简化服务器管理。使用服务配置文件，只需将原始服务配置文件与新硬件相关联，即可更换或升级服务器。

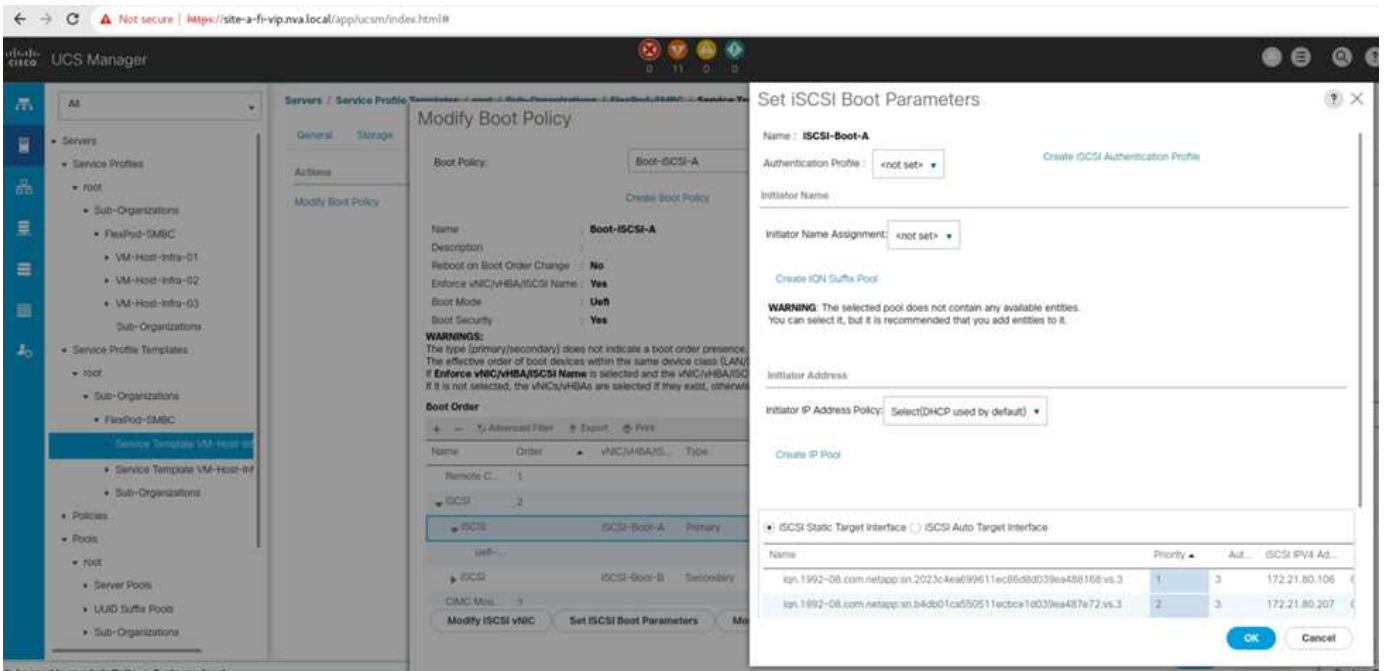
对于 VMware ESXi 主机，创建的服务配置文件支持以下功能：

- 使用 iSCSI 协议从任一站点的 AFF A250 存储启动 SAN。
- 为以下服务器创建了六个 vNIC：
 - 两个冗余 vNIC（vSwitch0-A 和 vSwitch0-B）可传输带内管理流量。或者，这些 vNIC 也可由不受 SM-BC 保护的 NFS 协议数据使用。
 - vSphere 分布式交换机使用两个冗余 vNIC（VDS-A 和 VDS-B）来传输 VMware vMotion 和其他应用程序流量。
 - iSCSI-A vSwitch 使用 iSCSI-A vNIC 访问 iSCSI-A 路径。
 - iSCSI-B vSwitch 使用 iSCSI-B vNIC 提供对 iSCSI-B 路径的访问。

SAN 启动

对于 iSCSI SAN 启动配置，iSCSI 启动参数设置为允许从两个 iSCSI 网络结构进行 iSCSI 启动。为了适应在主集群不可用时从二级集群提供 iSCSI SAN 启动 LUN 的 SM-BC 故障转移场景，iSCSI 静态目标配置应包括站点 A 和站点 B 的目标此外，要最大程度地提高启动 LUN 的可用性，请将 iSCSI 启动参数设置配置为从所有存储控制器启动。

可以在设置 iSCSI 启动参数对话框下的服务配置文件模板的启动策略中配置 iSCSI 静态目标，如下图所示。下表显示了建议的 iSCSI 启动参数设置配置，该配置实施了上述启动策略以实现高可用性。



iSCSI 网络结构	优先级	iSCSI 目标	iSCSI LIF
iSCSI A	1.	站点 A iSCSI 目标	站点 A 控制器 1 iSCSI A LIF
	2.	站点 B iSCSI 目标	站点 B 控制器 2 iSCSI A LIF
iSCSI B	1.	站点 B iSCSI 目标	站点 B 控制器 1 iSCSI B LIF
	2.	站点 A iSCSI 目标	站点 A 控制器 2 iSCSI B LIF

"接下来：解决方案 验证—网络。"

解决方案 验证—网络

"先前版本：解决方案 验证—计算。"

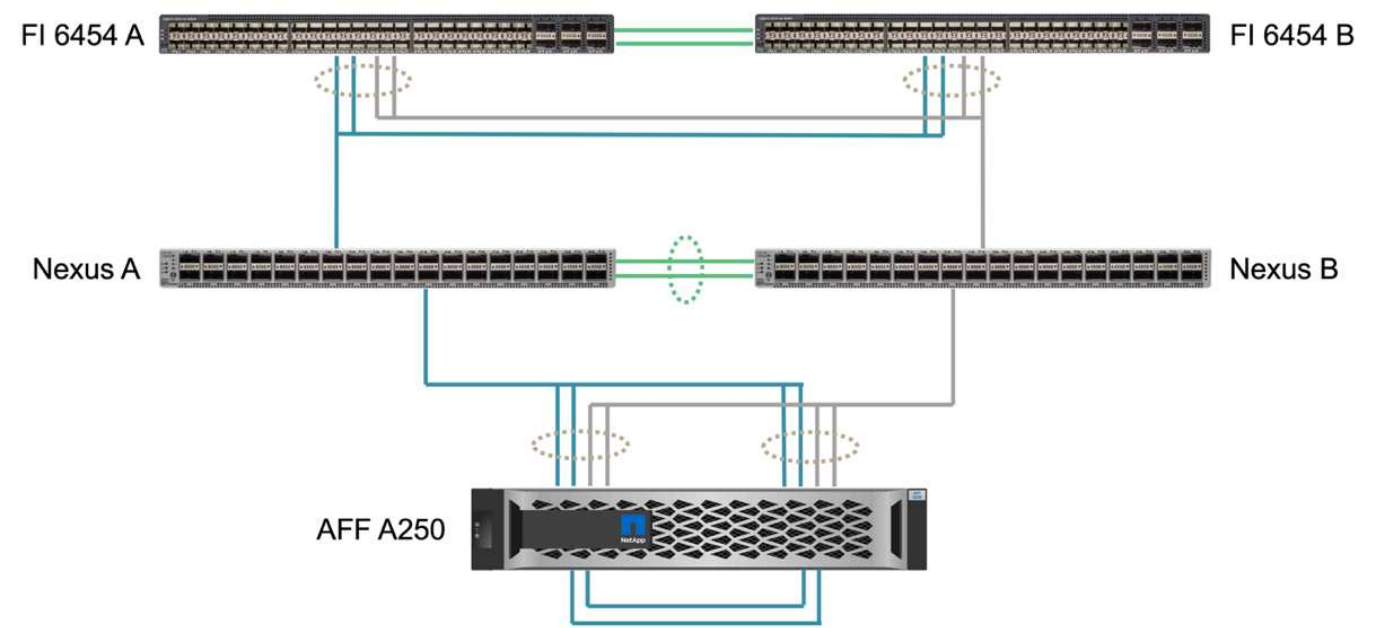
FlexPod SM-BC 解决方案 的网络配置遵循每个站点的典型 FlexPod 解决方案 最佳实践。对于站点间连接，解决方案 验证配置会将两个站点上的 FlexPod Nexus 交换机连接在一起，以提供站点间连接，从而扩展两个站点之间的 VLAN 。以下各节重点介绍了用于验证的一些连接和配置。

连接

每个站点上的 FlexPod Nexus 交换机均可通过高可用性配置在 UCS 计算和 ONTAP 存储之间提供本地连接。冗余组件和冗余连接可在发生单点故障时提供故障恢复能力。

下图显示了每个站点的 Nexus 交换机本地连接。除了图中显示的内容之外，还会为每个组件提供未显示的控制台和管理网络连接。40G 到 4 x 10G 分支缆线用于将 Nexus 交换机连接到 UCS CLI 和 ONTAP AFF A250 存储控制器。或者，也可以使用 100G 到 4 x 25G 分支缆线来提高 Nexus 交换机与 AFF A250 存储控制器之间的通

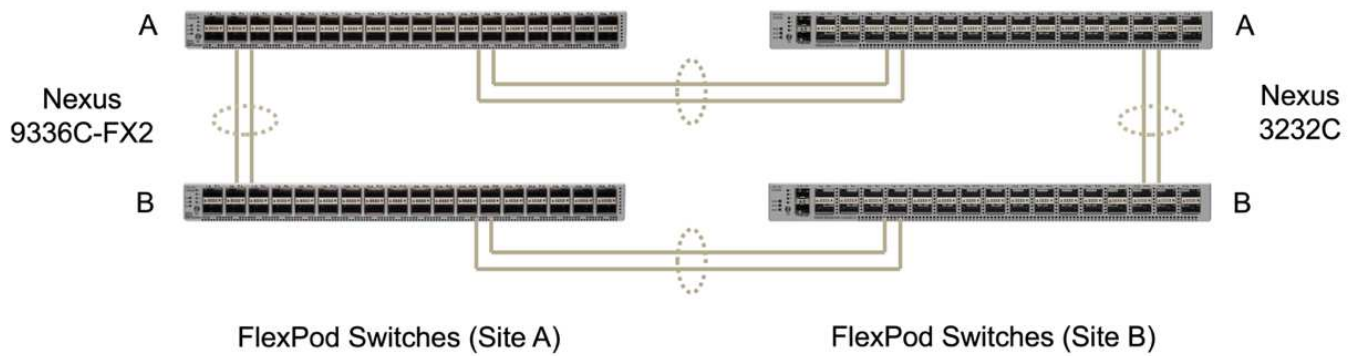
信速度。为了简单起见，这两个 AFF A250 控制器在逻辑上是并排显示的，用于布线图。两个存储控制器之间的两个连接允许存储形成无交换机集群。



下表显示了每个站点的 Nexus 交换机和 AFF A250 存储控制器之间的连接。

本地设备	本地端口	远程设备	远程端口
Nexus A	1 月 10 日	AFF A250 A	e1a
	1/2 年 10 月 1 日		e1b
	3 月 1 日	AFF A250 B	e1a
	4 月 1 日		e1b
Nexus B	1 月 10 日	AFF A250 A	e1c
	1/2 年 10 月 1 日		e1d
	3 月 1 日	AFF A250 B	e1c
	4 月 1 日		e1d

下图显示了站点 A 和站点 B 上的 FlexPod 交换机之间的连接，并在随附的表中列出了布线详细信息。每个站点的两个交换机之间的连接用于 vPC 对等链路。另一方面，站点间交换机之间的连接提供站点间链路。这些链路可将 VLAN 扩展到多个站点，用于集群间通信，SM-BC 数据复制，带内管理以及远程站点资源的数据访问。



本地设备	本地端口	远程设备	远程端口
站点 A 交换机 A	33	站点 B 交换机 A	31
	34		32
	25.	站点 A 交换机 B	25.
	26		26
站点 A 交换机 B	33	站点 B 交换机 B	31
	34		32
	25.	站点 A 交换机 A	25.
	26		26
站点 B 交换机 A	31	站点 A 交换机 A	33
	32		34
	25.	站点 B 交换机 B	25.
	26		26
站点 B 交换机 B	31	站点 A 交换机 B	33
	32		34
	25.	站点 B 交换机 A	25.
	26		26



上表从每个 FlexPod 交换机的角度列出了连接。因此，该表包含重复的信息以供阅读。

端口通道和虚拟端口通道

端口通道使用链路聚合控制协议（LACP）实现带宽聚合和链路故障恢复能力，从而实现链路聚合。虚拟端口通道（Virtual Port Channel，vPC）允许在逻辑上将两个 Nexus 交换机之间的端口通道连接显示为一个。这样可以进一步提高单链路故障或单交换机故障等情况下的故障恢复能力。

在到达 Nexus 交换机之前，存储的 UCS 服务器流量会采用 IOMA 到 FIA 的路径，而 IOMB 到 FIB 的路径。由于连接到 Nexus 交换机的 FI 使用的是 FI 端的端口通道，而 Nexus 交换机端的虚拟端口通道，因此 UCS 服务器可以有效地使用通过这两个 Nexus 交换机的路径，并可在发生单点故障时继续运行。在这两个站点之间，Nexus 交换机是互连的，如上图所示。站点之间有两个链路，每个链路用于连接交换机对，它们也使用端口通道配置。

通过在冗余配置中将每个站点的存储控制器与本地 Nexus 交换机互连，可以实现带内管理，集群间和 iSCSI/NFS 数据存储协议连接。每个存储控制器都连接到两个 Nexus 交换机。这四个连接会配置为存储上接口组的一部分，以提高故障恢复能力。在 Nexus 交换机端，这些端口也属于交换机之间的 vPC 。

下表列出了每个站点的端口通道 ID 和使用情况。

端口通道 ID	使用情况
10	本地 Nexus 对等链路
15	互联阵列 A 链路
16	光纤互连 B 链路
27	存储控制器 A 链路
28	存储控制器 B 链路
100	站点间交换机 A 链路
200	站点间交换机 B 链路

VLAN

下表列出了为设置 FlexPod SM-BC 解决方案 验证环境而配置的 VLAN 及其使用情况。

Name	VLAN ID	使用情况
本机 VLAN	2	VLAN 2 用作原生 VLAN ， 而不是默认 VLAN （ 1 ）
OOB-MGMT-VLAN	33 ： 33	设备的带外管理 VLAN
IB-MGMT-VLAN	3334	用于 ESXi 主机， VM 管理等的带内管理 VLAN
NFS-VLAN	3335	用于 NFS 流量的可选 NFS VLAN
iSCSI-A-VLAN	3336	用于 iSCSI 流量的 iSCSI-A 网络结构 VLAN
iSCSI-B-VLAN	3337	用于 iSCSI 流量的 iSCSI-B 网络结构 VLAN
vmotion-vlan	3338	VMware vMotion 流量 VLAN
VM-Traffic-VLAN	3339	VMware VM 流量 VLAN
集群间 VLAN	3340	用于 ONTAP 集群对等通信的集群间 VLAN



虽然 SM-BC 不支持 NFS 或 CIFS 协议以实现业务连续性，但您仍可以将其用于不需要保护业务连续性的工作负载。未为此验证创建 NFS 数据存储库。

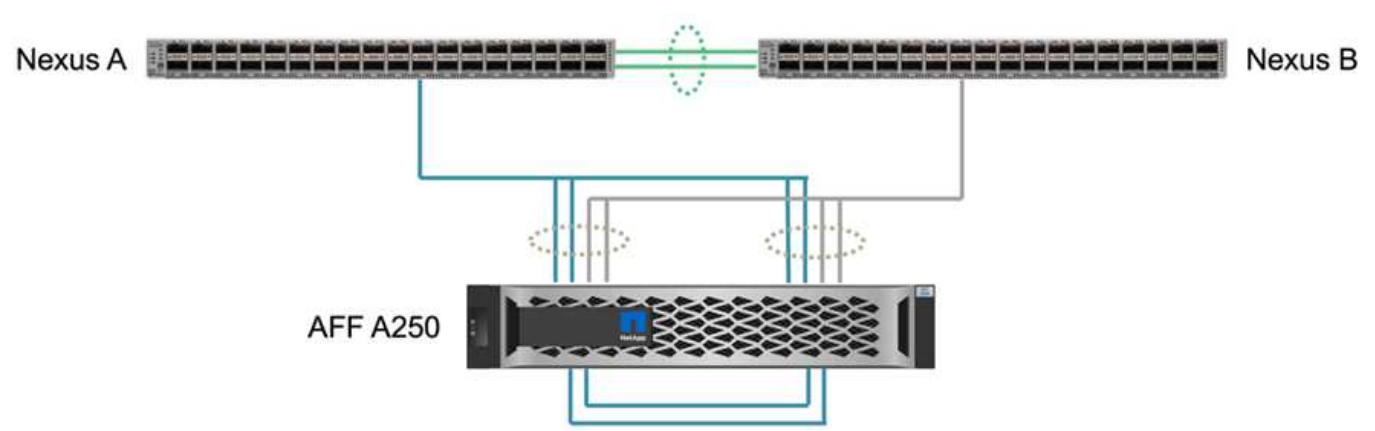
"接下来：解决方案 验证—存储。"

["先前版本：解决方案 验证 - 网络。"](#)

FlexPod SM-BC 解决方案 的存储配置遵循每个站点的典型 FlexPod 解决方案 最佳实践。对于 SM-BC 集群对等和数据复制，它们使用在两个站点的 FlexPod 交换机之间建立的站点间链路。以下各节重点介绍了用于验证的一些连接和配置。

连接

本地站点的 Nexus 交换机可提供与本地 UCS CLI 和刀片式服务器的存储连接。通过站点之间的 Nexus 交换机连接，远程 UCS 刀片式服务器也可以访问存储。下图和表显示了每个站点的存储控制器的存储连接图和连接列表。



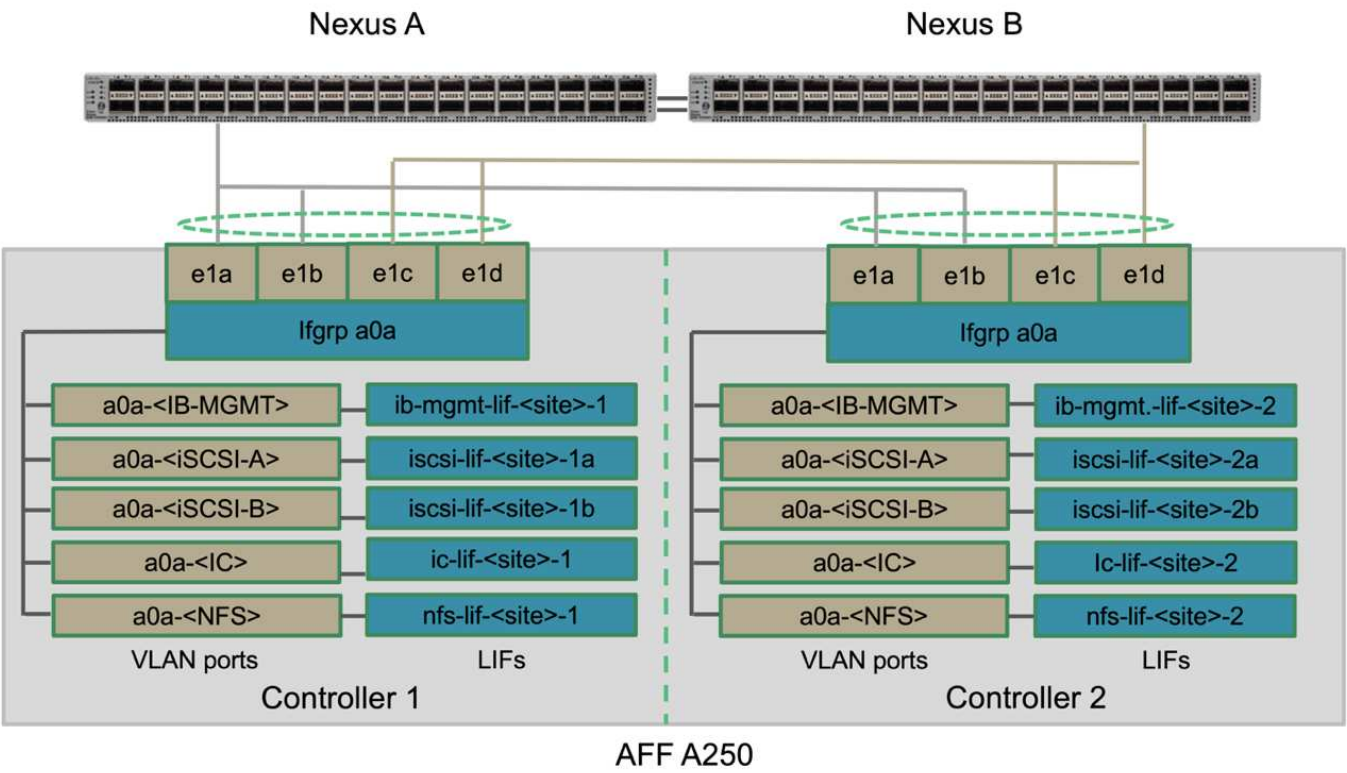
本地设备	本地端口	远程设备	远程端口
AFF A250 A	e0c	AFF A250 B	e0c
	e0d		e0d
	e1a	Nexus A	1 月 10 日
	e1b		1/2 年 10 月 1 日
	e1c	Nexus B	1 月 10 日
AFF A250 B	e0c	AFF A250 A	e0c
	e0d		e0d
	e1a	Nexus A	3 月 1 日
	e1b		4 月 1 日
	e1c	Nexus B	3 月 1 日
	e1d		4 月 1 日

连接和接口

每个存储控制器上的两个物理端口连接到每个 Nexus 交换机，用于进行带宽聚合和冗余以进行此验证。这四个

连接参与存储上的接口组配置。Nexus 交换机上的相应端口参与 vPC ， 以实现链路聚合和故障恢复能力。

带内管理， 集群间和 NFS/iSCSI 数据存储协议使用 VLAN 。在接口组上创建 VLAN 端口， 用于隔离不同类型的流量。相应功能的逻辑接口（ Logical Interface ， LIF ）在相应的 VLAN 端口之上创建。下图显示了物理连接， 接口组， VLAN 端口和逻辑接口之间的关系。

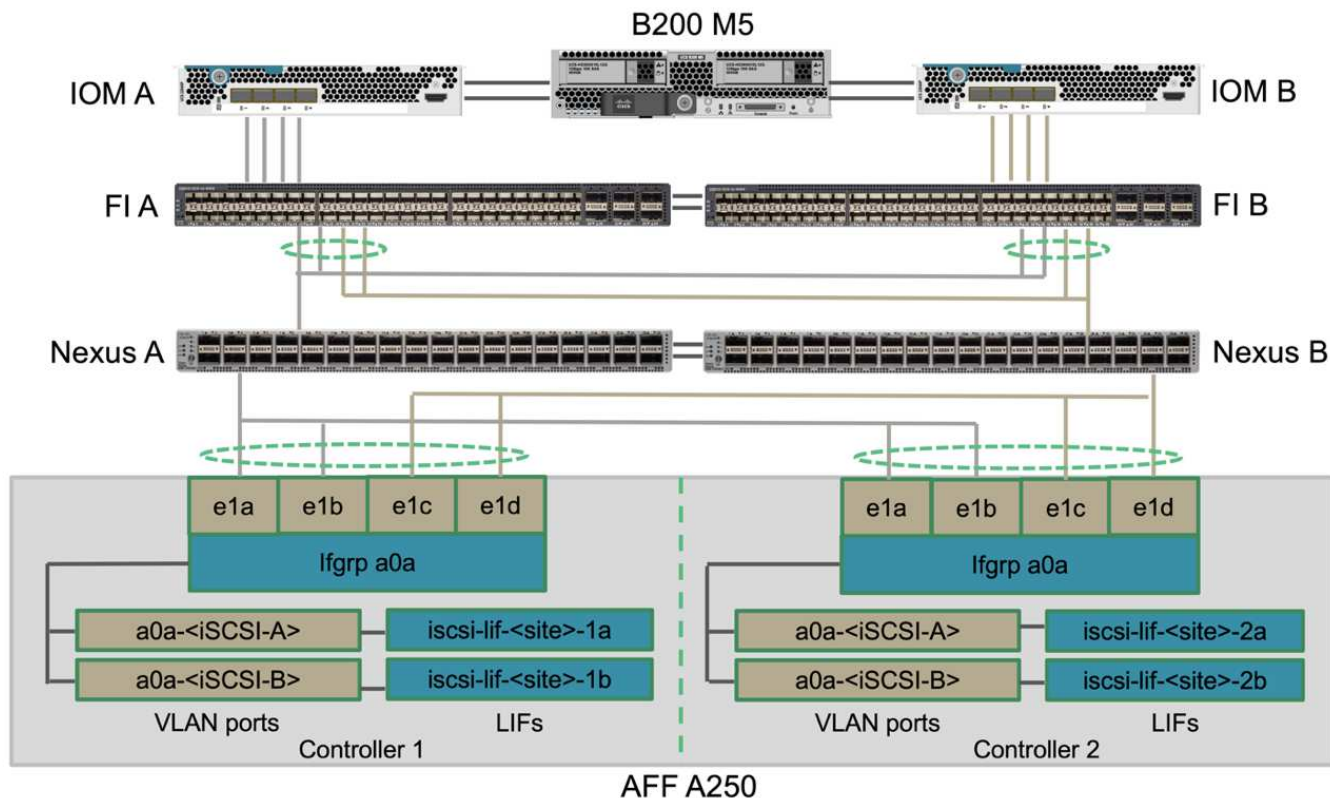


SAN 启动

NetApp 建议在 FlexPod 解决方案 中为 Cisco UCS 服务器实施 SAN 启动。通过实施 SAN 启动，您可以在 NetApp 存储系统中安全地保护操作系统，从而提高性能和灵活性。对于此解决方案 ， 已验证 iSCSI SAN 启动。

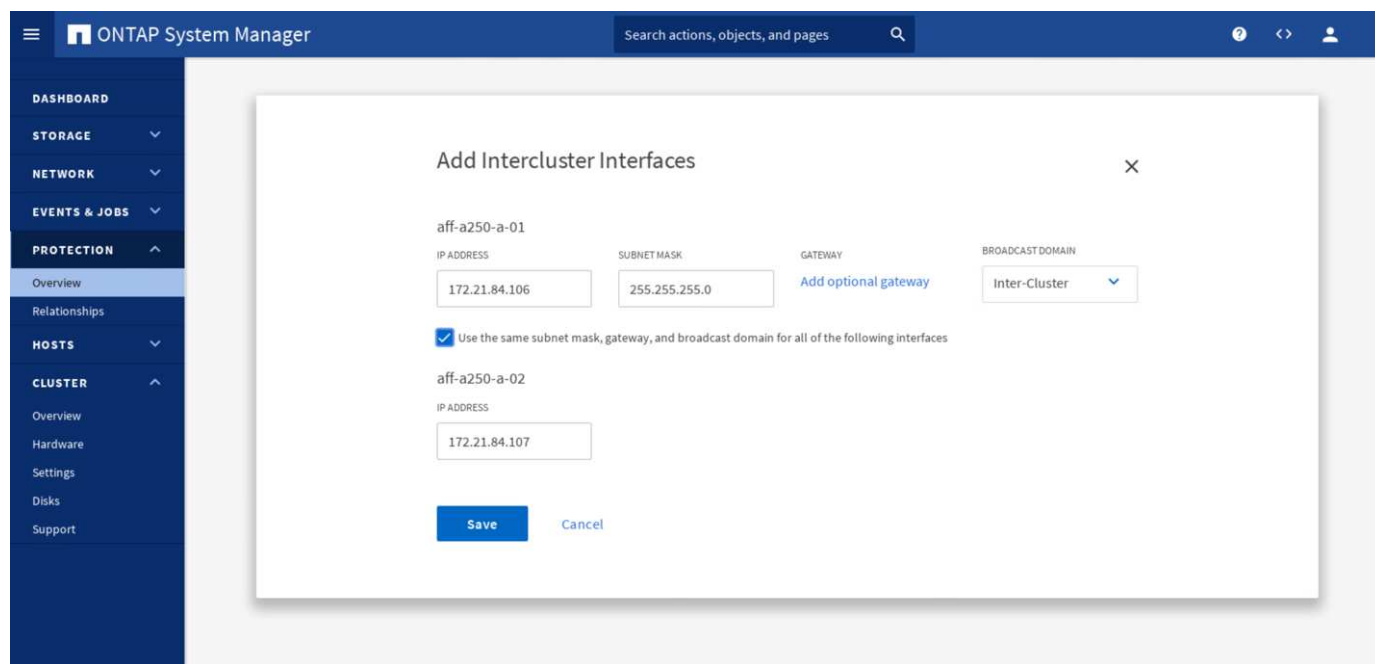
下图显示了从 NetApp 存储对 Cisco UCS 服务器进行 iSCSI SAN 启动的连接。在 iSCSI SAN 启动中，每个 Cisco UCS 服务器都分配有两个 iSCSI vNIC （每个 SAN 网络结构一个）， 用于提供从服务器一直到存储的冗余连接。连接到 Nexus 交换机（在此示例中为 e1a ， e1b ， e1c 和 e1d ）的 10/25G 以太网存储端口将分组在一起， 形成一个接口组（ ifgrp ）（在此示例中为 a0a ）。iSCSI VLAN 端口在 ifgrp 上创建， iSCSI LIF 在 iSCSI VLAN 端口上创建。

每个 iSCSI 启动 LUN 都会通过 iSCSI LIF 映射到从中启动的服务器， 方法是将启动 LUN 与其启动 igroup 中的服务器 iSCSI 限定名称（ IQN ）相关联。服务器的启动 igroup 包含两个 IQN ， 每个 vNIC/SAN 网络结构一个。此功能仅允许授权服务器访问专为该服务器创建的启动 LUN 。



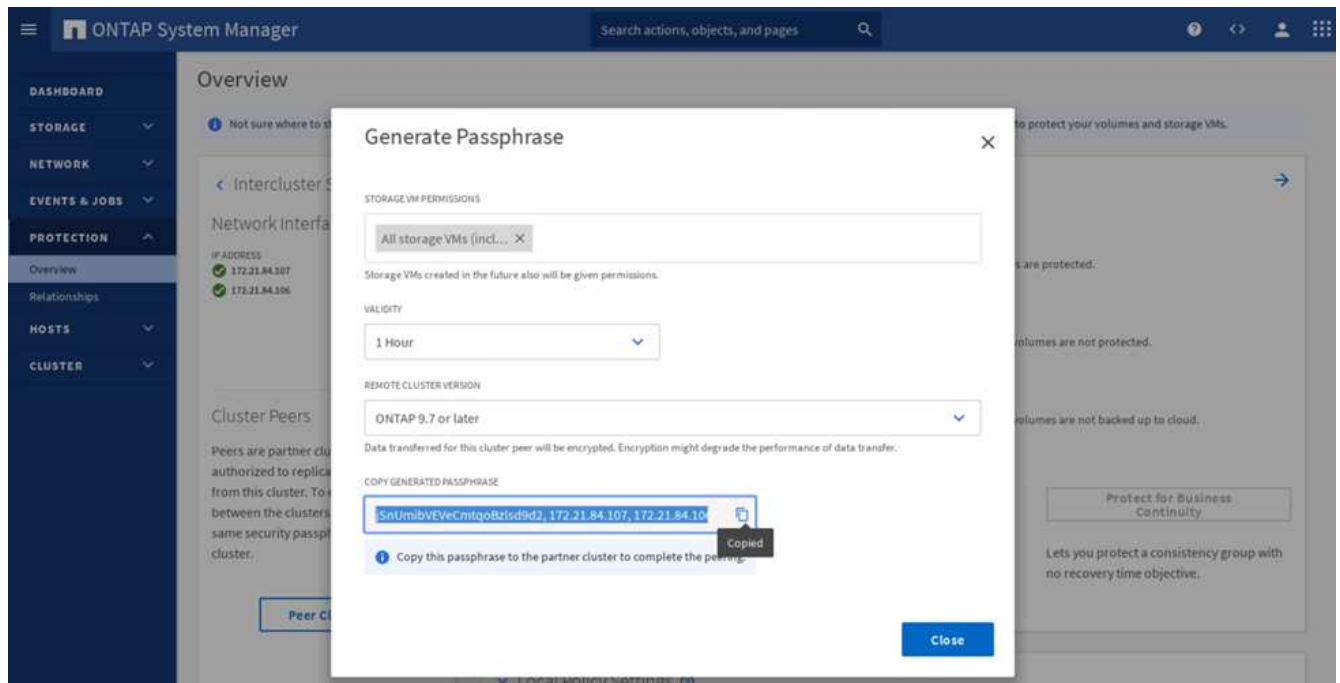
集群对等

ONTAP 集群对等方通过集群间 LIF 进行通信。使用 ONTAP 系统管理器可在 " 保护 "> 概述 " 窗格下创建所需的集群间 LIF 。

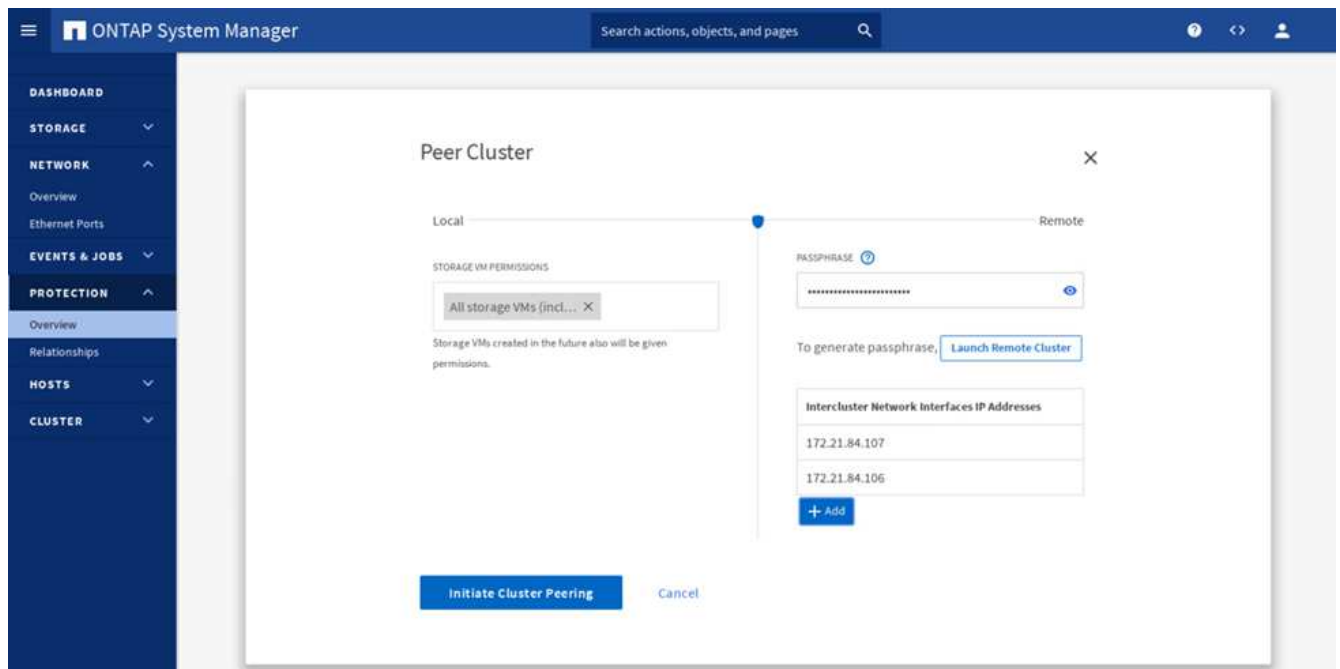


要将这两个集群建立对等关系，请完成以下步骤：

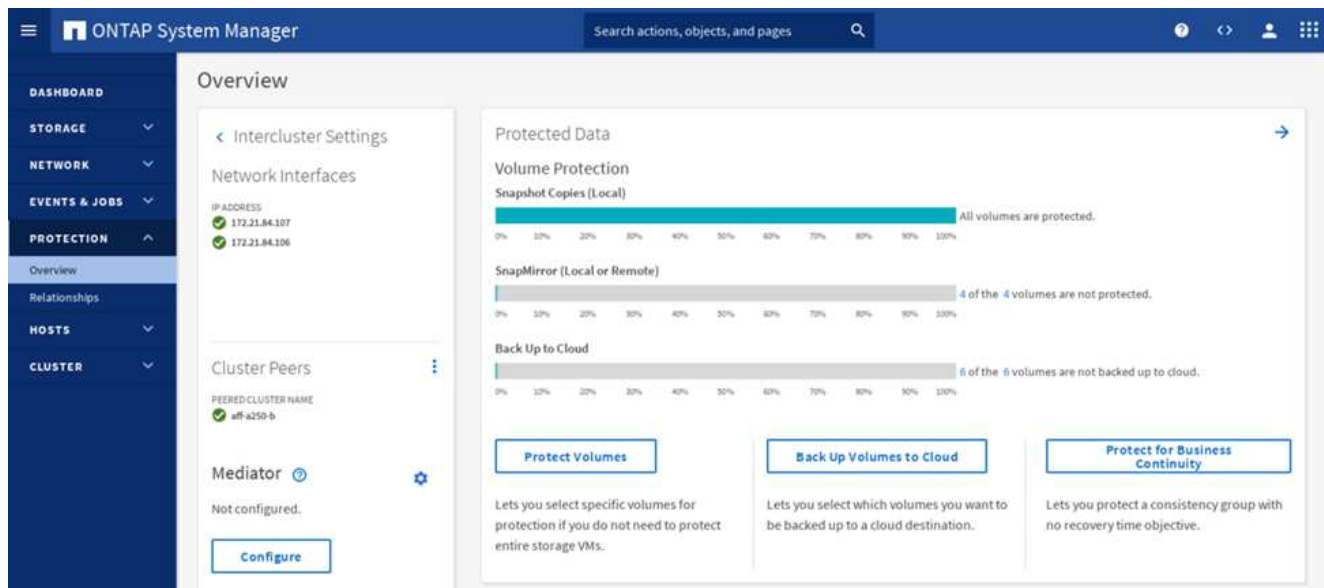
1. 在第一个集群中生成集群对等密码短语。



2. 在第二个集群中调用对等集群选项，并提供密码短语和集群间 LIF 信息。



3. System Manager 保护 > 概述窗格显示集群对等信息。

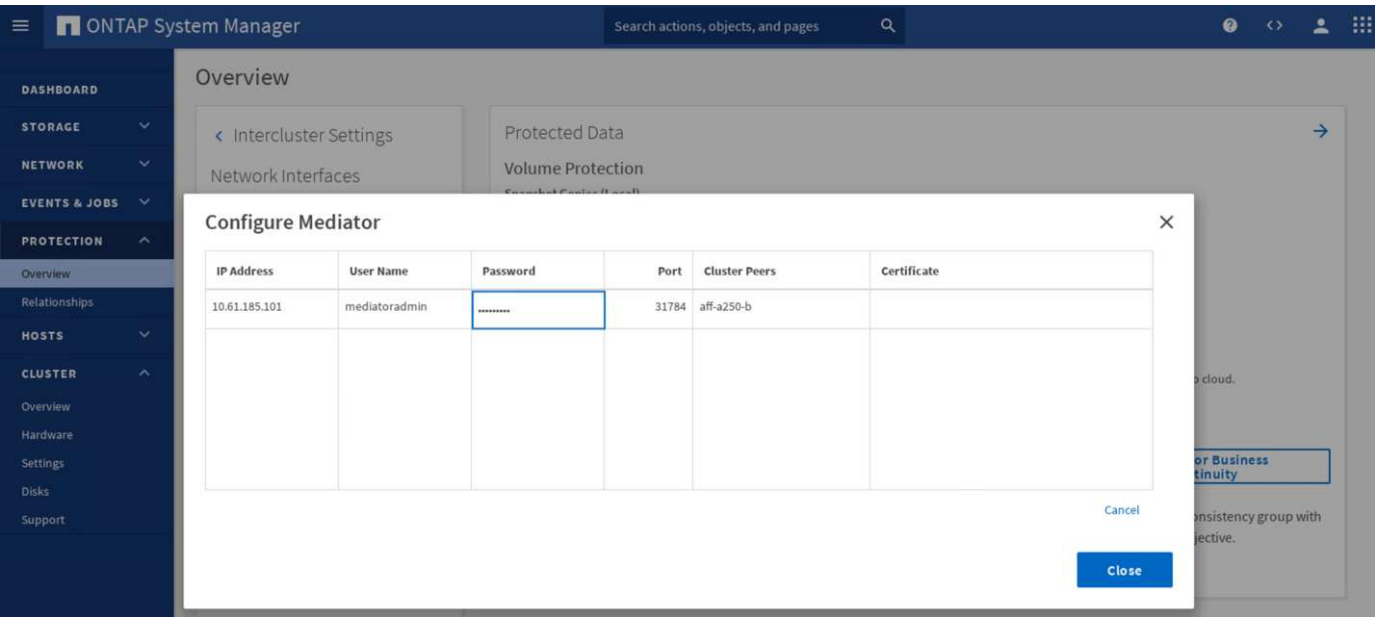


ONTAP 调解器安装和配置

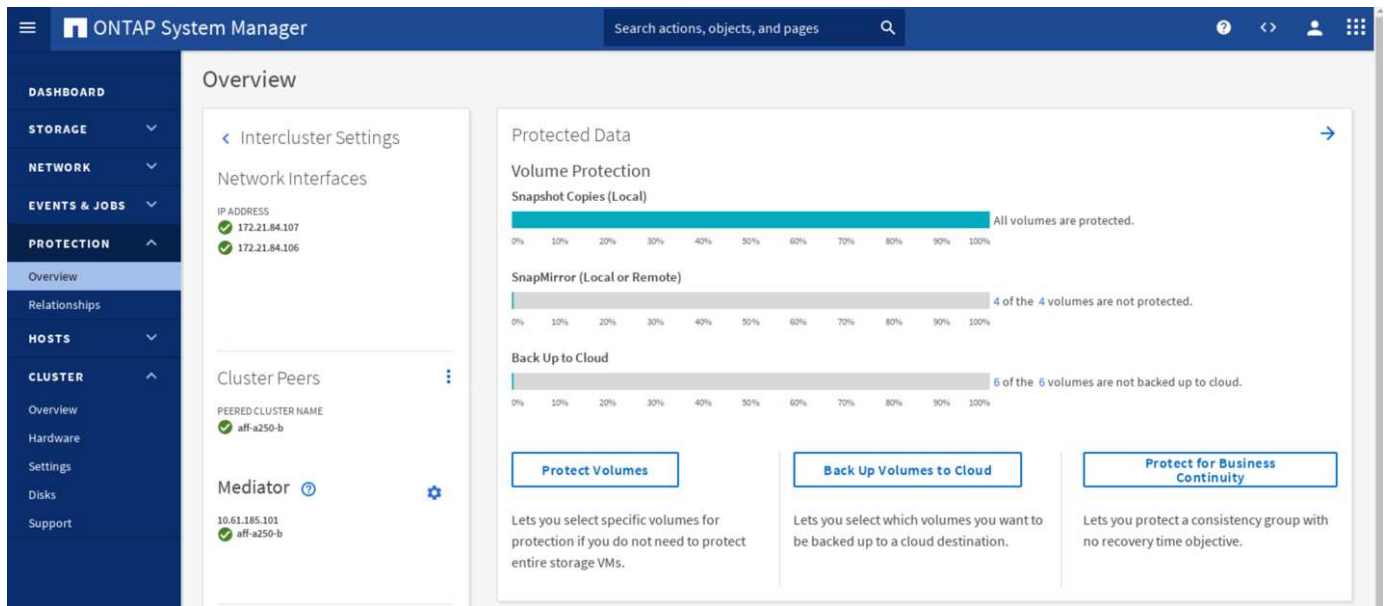
ONTAP 调解器为 SM-BC 关系中的 ONTAP 集群建立仲裁。它可以在检测到故障时协调自动故障转移，并有助于避免在每个集群同时尝试建立主集群控制时出现脑裂情况。

安装 ONTAP 调解器之前，请查看 ["安装或升级 ONTAP 调解器服务"](#) 第页，了解前提条件，支持的 Linux 版本以及在各种受支持的 Linux 操作系统上安装它们的过程。

安装 ONTAP 调解器后，您可以将 ONTAP 调解器的安全证书添加到 ONTAP 集群中，然后在 System Manager 保护 > 概述窗格中配置 ONTAP 调解器。以下屏幕截图显示了 ONTAP 调解器配置 GUI。



提供必要信息后，已配置的 ONTAP 调解器将显示在 System Manager 保护 > 概述窗格中。



SM-BC 一致性组

一致性组为跨越一组指定卷的应用程序工作负载提供写入顺序一致性保证。对于 ONTAP 9.10.1，以下是一些重要限制。

- 一个集群中的最大 SM-BC 一致性组关系数为 20。
- 每个 SM-BC 关系支持的最大卷数为 16。
- 一个集群中的最大源端点和目标端点总数为 200。

有关更多详细信息，请参见上的 ONTAP SM-BC 文档 ["限制和限制"](#)。

在验证配置中，使用 ONTAP 系统管理器创建一致性组，以保护两个站点的 ESXi 启动 LUN 和共享数据存储库 LUN。要访问一致性组创建对话框，请转到 "保护" > "概述" > "保护业务连续性" > "保护一致性组"。要创建一致性组，请提供创建所需的源卷，目标集群和目标 Storage Virtual Machine 信息。

Protect Consistency Group

×

PROTECTION POLICY

AutomatedFailOver

Source

Destination

CLUSTER

aff-a250-a

CLUSTER

aff-a250-b

Refresh

CONSISTENCY GROUP

Existing

New

STORAGE VM

Infra-SVM-b

NAME

cg_esxi_a

VOLUMES

esxi_a

Destination Settings

If the consistency group contains LUNs, you should manually update the host information for the newly created LUNs on the destination cluster.

Save

Cancel

下表列出了验证测试中创建四个一致性组以及每个一致性组中包含的卷。

System Manager	一致性组	Volumes
站点 A	CG_ESXi_A	ESXi_A
站点 A	CG_infra_datastore_A	infra_datastore_A_01 infra_datastore_A_02
站点 B	CG_ESXi_b	ESXi b
站点 B	cG_infra_datastore_b.	infra_datastore_b_01 infra_datastore_b_02

创建一致性组后，它们将显示在站点 A 和站点 B 中相应的保护关系下

此屏幕截图显示了站点 A 上的一致性组关系

Source	Destination	Protection Policy	Relationship Health	State	Lag
Infra-SVM.1/cg/cg_infra_datastore_b	Infra-SVM-a/cg/cg_infra_datastore_b_dest	AutomatedFailOver	Healthy	In sync	0 second
Infra-SVM.1/cg/cg_esxi_b	Infra-SVM-a/cg/cg_esxi_b_dest	AutomatedFailOver	Healthy	In sync	0 second

此屏幕截图显示了站点 B 上的一致性组关系

Source	Destination	Protection Policy	Relationship Health	State	Lag
Infra-SVM.1/cg/cg_esxi_a	Infra-SVM-b/cg/cg_esxi_a_dest	AutomatedFailOver	Healthy	In sync	0 second
Infra-SVM.1/cg/cg_infra_datastore_a	Infra-SVM-b/cg/cg_infra_datastore_a_dest	AutomatedFailOver	Healthy	In sync	0 second

此屏幕截图显示了 CG_infra_datastore_b 组的一致性组关系详细信息。

Overview

IS HEALTHY?

STATE: In sync

PROTECTION POLICY: AutomatedFailOver

POLICY TYPE: Synchronous

TRANSFER STATUS: Success

CONTAINED LUNS (SOURCE)

Name	Initiator Group
datastore_lun_b_01	MGMT-Hosts
datastore_lun_b_02	MGMT-Hosts

Diagram showing relationship between **aff-a250-b** (CONSISTENCY GROUP: cg_infra_datastore_b) and **aff-a250-a** (CONSISTENCY GROUP: cg_infra_datastore_b_dest) via mediator **10.61.185.101**.

卷， LUN 和主机映射

创建一致性组后， SnapMirror 会同步源卷和目标卷，以便数据始终保持同步。远程站点上的目标卷包含卷名称，并且 _dest 结尾为。例如，对于站点 A 集群中的 ESXi_A 卷，站点 B 中有相应的 ESXi_A_Dest 数据保护（ DP ）卷

此屏幕截图显示了站点 A 的卷信息

```
aff-a250-a::> vol show -vserver Infra-SVM-a
Vserver   Volume           Aggregate      State      Type      Size   Available Used%
-----
Infra-SVM-a esxi_a         aggr1_aff_a250_a_01 online RW      320GB   315.9GB   1%
Infra-SVM-a esxi_b_dest    aggr1_aff_a250_a_02 online DP      3.86GB   638.4MB  83%
Infra-SVM-a infra_datastore_a_01 aggr1_aff_a250_a_01 online RW    1TB  717.6GB  29%
Infra-SVM-a infra_datastore_a_02 aggr1_aff_a250_a_02 online RW    1TB  828.4GB  19%
Infra-SVM-a infra_svm_root aggr1_aff_a250_a_01 online RW     1GB   966.5MB   0%
Infra-SVM-a infra_svm_root_m01 aggr1_aff_a250_a_01 online LS     1GB   966.6MB   0%
Infra-SVM-a infra_svm_root_m02 aggr1_aff_a250_a_02 online LS     1GB   966.6MB   0%
Infra-SVM-a vol_infra_datastore_b_01_dest aggr1_aff_a250_a_01 online DP 138.7GB 31.52GB 76%
Infra-SVM-a vol_infra_datastore_b_02_dest aggr1_aff_a250_a_01 online DP 49.37GB 9.03GB 80%
9 entries were displayed.
```

此屏幕截图显示站点 B 的卷信息

```
aff-a250-b::> vol show -vserver Infra-SVM-b
Vserver   Volume           Aggregate      State      Type      Size   Available Used%
-----
Infra-SVM-b esxi_a_dest    aggr1_aff_a250_b_02 online DP     4.10GB   768.2MB  80%
Infra-SVM-b esxi_b         aggr1_aff_a250_b_01 online RW      320GB   315.8GB   1%
Infra-SVM-b infra_datastore_b_01 aggr1_aff_a250_b_01 online RW    1TB  911.9GB  10%
Infra-SVM-b infra_datastore_b_02 aggr1_aff_a250_b_02 online RW    1TB  964.0GB   5%
Infra-SVM-b infra_svm_root aggr1_aff_a250_b_01 online RW     1GB   966.9MB   0%
Infra-SVM-b infra_svm_root_m01 aggr1_aff_a250_b_01 online LS     1GB   967.0MB   0%
Infra-SVM-b infra_svm_root_m02 aggr1_aff_a250_b_02 online LS     1GB   967.0MB   0%
Infra-SVM-b vol_infra_datastore_a_01_dest aggr1_aff_a250_b_02 online DP 270.0GB 27.39GB 89%
Infra-SVM-b vol_infra_datastore_a_02_dest aggr1_aff_a250_b_02 online DP 202.8GB 28.20GB 85%
9 entries were displayed.
```

为了便于透明的应用程序故障转移，还需要将镜像的 SM-BC LUN 映射到目标集群中的主机。这样，主机就可以正确查看源集群和目标集群中 LUN 的路径。以下两个屏幕截图捕获了站点 A 和站点 B 的 `igroup show` 和 `lun show` 输出。通过创建的映射，集群中的每个 ESXi 主机都将其自己的 SAN 启动 LUN 视为 ID 0，并将所有四个共享 iSCSI 数据存储库 LUN 视为 ID 0。

此屏幕截图显示了站点 A 集群的主机 `igroup` 和 LUN 映射。

```

aff-a250-a:> igroup show
Vserver   Igroup      Protocol OS Type  Initiators
-----
Infra-SVM-a MGMT-Hosts iscsi    vmware  iqn.2010-11.com.flexpod:ucs-smbc-a:1
                               iqn.2010-11.com.flexpod:ucs-smbc-a:2
                               iqn.2010-11.com.flexpod:ucs-smbc-a:3
                               iqn.2010-11.com.flexpod:ucs-smbc-b:1
                               iqn.2010-11.com.flexpod:ucs-smbc-b:2
                               iqn.2010-11.com.flexpod:ucs-smbc-b:3
Infra-SVM-a VM-Host-Infra-a-01 iscsi    vmware  iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-a VM-Host-Infra-a-02 iscsi    vmware  iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-a VM-Host-Infra-a-03 iscsi    vmware  iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-a VM-Host-Infra-b-01 iscsi    vmware  iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-a VM-Host-Infra-b-02 iscsi    vmware  iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-a VM-Host-Infra-b-03 iscsi    vmware  iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-a:> lun show -m
Vserver   Path                                     Igroup   LUN ID  Protocol
-----
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-01          VM-Host-Infra-a-01  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-02          VM-Host-Infra-a-02  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-03          VM-Host-Infra-a-03  0  iscsi
Infra-SVM-a /vol/esxi_a/swap_lun_a              MGMT-Hosts    13  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-01      VM-Host-Infra-b-01  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-02      VM-Host-Infra-b-02  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-03      VM-Host-Infra-b-03  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/swap_lun_b            MGMT-Hosts    23  iscsi
Infra-SVM-a /vol/infra_datastore_a_01/datastore_lun_a_01 MGMT-Hosts    11  iscsi
Infra-SVM-a /vol/infra_datastore_a_02/datastore_lun_a_02 MGMT-Hosts    12  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_01_dest/datastore_lun_b_01 MGMT-Hosts    21  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_02_dest/datastore_lun_b_02 MGMT-Hosts    22  iscsi
12 entries were displayed.

```

此屏幕截图显示了站点 B 集群的主机 igroup 和 LUN 映射。

```

aff-a250-b:> igroup show
Vserver    Igroup      Protocol OS Type  Initiators
-----
Infra-SVM-b MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-b:1
                               iqn.2010-11.com.flexpod:ucs-smbc-b:2
                               iqn.2010-11.com.flexpod:ucs-smbc-b:3
                               iqn.2010-11.com.flexpod:ucs-smbc-a:1
                               iqn.2010-11.com.flexpod:ucs-smbc-a:2
                               iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-a-01 iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-b VM-Host-Infra-a-02 iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-b VM-Host-Infra-a-03 iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-b-01 iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-b VM-Host-Infra-b-02 iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-b VM-Host-Infra-b-03 iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-b:> lun show -m
Vserver    Path                                          Igroup    LUN ID  Protocol
-----
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-01      VM-Host-Infra-a-01  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-02      VM-Host-Infra-a-02  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-03      VM-Host-Infra-a-03  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/swap_lun_a          MGMT-Hosts    13  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-01        VM-Host-Infra-b-01  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-02        VM-Host-Infra-b-02  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-03        VM-Host-Infra-b-03  0  iscsi
Infra-SVM-b /vol/esxi_b/swap_lun_b              MGMT-Hosts    23  iscsi
Infra-SVM-b /vol/infra_datastore_b_01/datastore_lun_b_01 MGMT-Hosts    21  iscsi
Infra-SVM-b /vol/infra_datastore_b_02/datastore_lun_b_02 MGMT-Hosts    22  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_01_dest/datastore_lun_a_01 MGMT-Hosts    11  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_02_dest/datastore_lun_a_02 MGMT-Hosts    12  iscsi
12 entries were displayed.

```

"接下来：解决方案 验证—虚拟化。"

解决方案 验证—虚拟化

"先前版本：解决方案 验证—存储。"

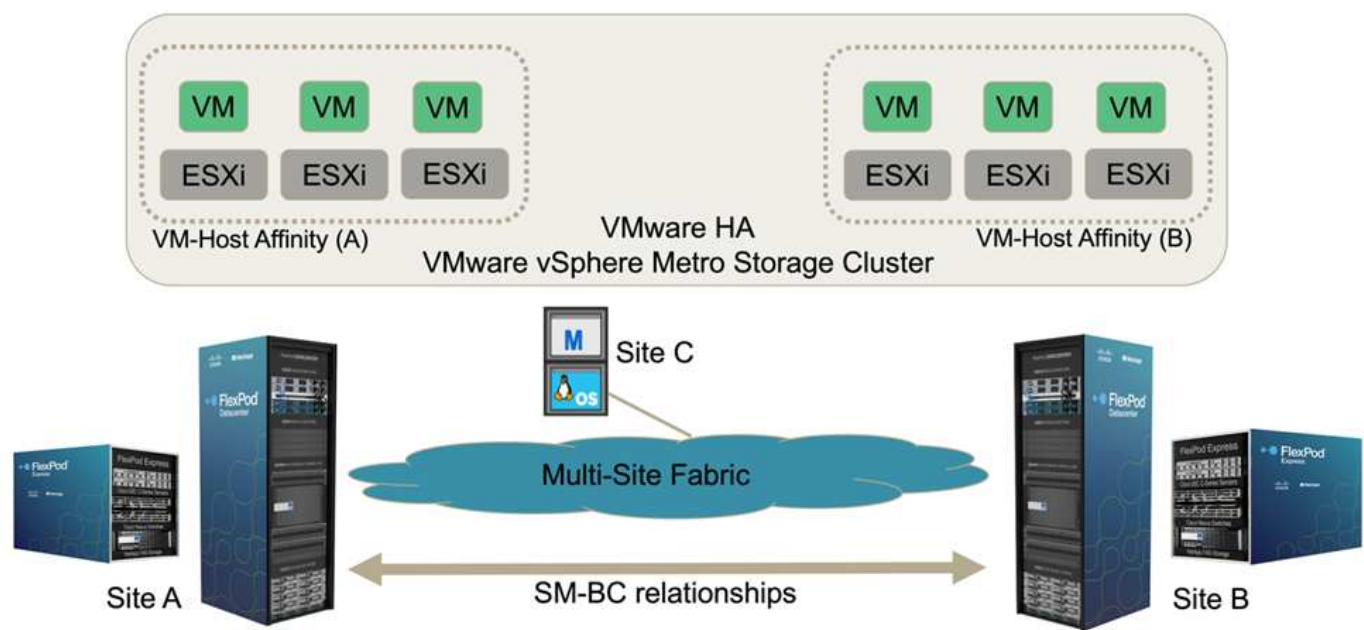
在多站点 FlexPod SM-BC 解决方案 中，一个 VMware vCenter 可管理整个解决方案 的虚拟基础架构资源。两个数据中心中的主机都属于一个 VMware HA 集群，该集群跨越两个数据中心。主机可以访问 NetApp SM-BC 解决方案 ，在此可以从两个站点访问具有定义的 SM-BC 关系的存储。

SM-BC 解决方案 存储符合 VMware vSphere Metro Storage Cluster （VMSC）功能中的统一访问模式，可避免灾难和停机。为了获得最佳虚拟机性能，虚拟机磁盘应托管在本地 NetApp AFF A250 系统上，以便在正常操作下最大限度地减少 WAN 链路之间的延迟和流量。

在设计实施过程中，必须确定虚拟机在两个站点之间的分布情况。您可以根据站点首选项和应用程序要求确定这两个站点之间的虚拟机站点关联性和应用程序分布。VMware 集群 VM/ 主机组和 VM/ 主机规则用于配置 VM/ 主机关联性，以确保 VM 在所需站点的主机上运行。

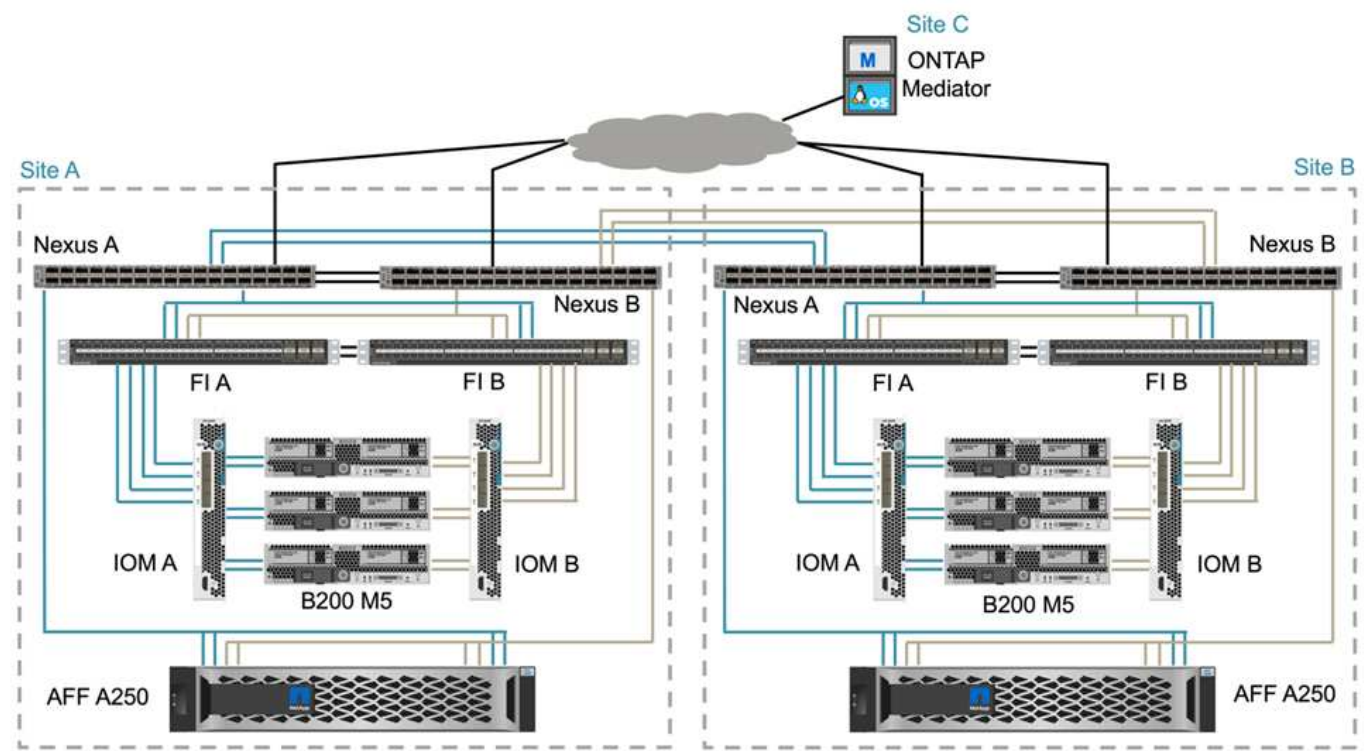
但是，如果配置允许 VM 在两个站点上运行，则可以确保 VM 可以通过远程站点主机上的 VMware HA 重新启动，以提供解决方案 故障恢复能力。要使虚拟机能够同时在两个站点上运行，必须在所有 ESXi 主机上挂载所有 iSCSI 共享数据存储库，以确保站点之间虚拟机的 vMotion 操作顺畅。

下图显示了一个高级 FlexPod SM-BC 解决方案 虚拟化视图，其中包括 VMware HA 和 VMSC 功能，可为计算和存储服务提供高可用性。主动 - 主动数据中心解决方案 架构支持站点之间的工作负载移动，并提供灾难恢复 / 业务连续性保护。



端到端网络连接

FlexPod SM-BC 解决方案 包括每个站点的 FlexPod 基础架构，站点之间的网络连接以及在第三个站点部署的 ONTAP 调解器，以满足所需的 RPO 和 RTO 目标。下图显示了每个站点的 Cisco UCS B200M5 服务器与站点内和站点间具有 SM-BC 功能的 NetApp 存储之间的端到端网络连接。



在此解决方案 验证中，每个站点的 FlexPod 部署架构都是相同的。但是，解决方案 支持非对称部署，如果满足

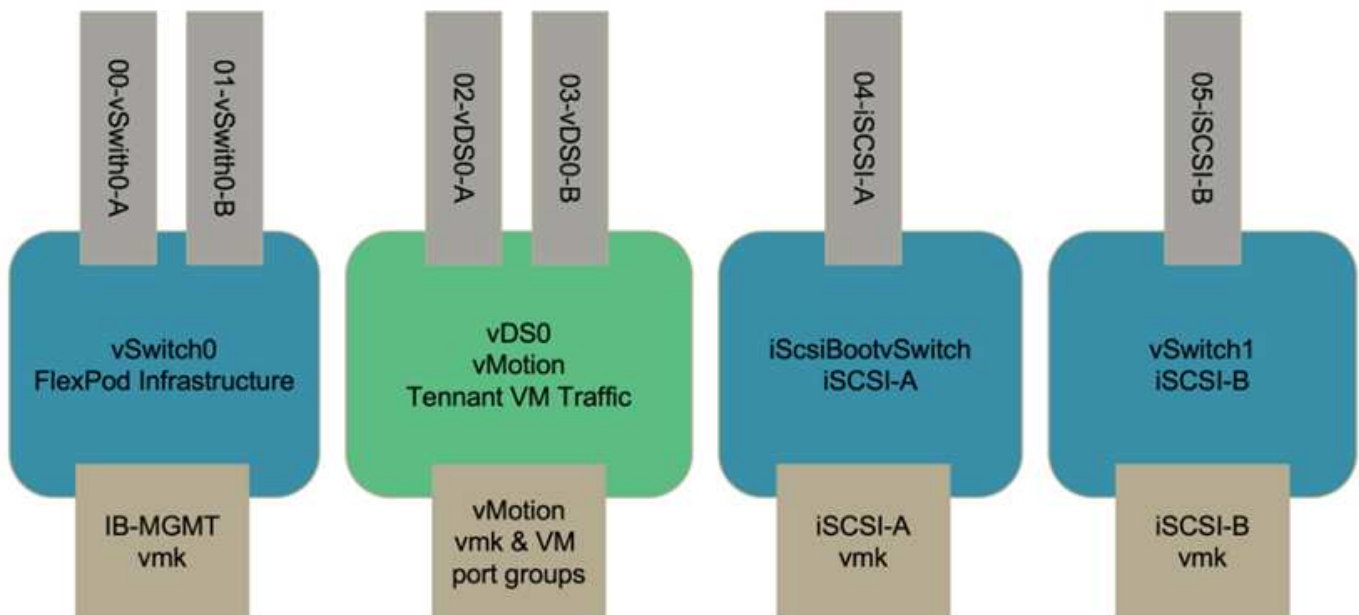
要求，也可以将其添加到现有 FlexPod 解决方案中。

扩展的第 2 层架构用于无缝的多站点数据网络结构，可在每个数据中心的端口通道 Cisco UCS 计算和 NetApp 存储之间提供连接，并在数据中心之间提供连接。端口通道配置以及虚拟端口通道配置（如果适用）用于计算层，网络层和存储层之间以及跨站点链路之间的带宽聚合和容错。因此，UCS 刀片式服务器可以连接并多路径访问本地和远程 NetApp 存储。

虚拟网络

无论主机位于何处，集群中的每个主机都使用相同的虚拟网络进行部署。此设计使用 VMware 虚拟交换机（vSwitch）和 VMware 虚拟分布式交换机（VDS）来分隔不同的流量类型。VMware vSwitch 主要用于 FlexPod 基础架构网络，而 VDS 用于应用程序网络，但不是必需的。

每个虚拟交换机（vSwitch，VDS）部署有两个上行链路；ESXi 虚拟机管理程序级别的上行链路在 Cisco UCS 软件上称为 vmnic 和虚拟 NIC（vNIC）。vNIC 会使用 Cisco UCS 服务配置文件在每个服务器的 Cisco UCS VIC 适配器上创建。定义了六个 vNIC，两个用于 vSwitch0，两个用于 vDS0，两个用于 vSwitch1，两个用于 iSCSI 上行链路，如下图所示。



vSwitch0 是在 VMware ESXi 主机配置期间定义的，它包含用于管理的 FlexPod 基础架构管理 VLAN 和 ESXi 主机 VMkernel（VMK）端口。对于所需的任何关键基础架构管理虚拟机，还会在 vSwitch0 上放置一个基础架构管理虚拟机端口组。

请务必将此类管理基础架构虚拟机放置在 vSwitch0 上，而不是 VDS 上，因为如果 FlexPod 基础架构已关闭或重新启动，而您尝试在最初运行该管理虚拟机的主机以外的主机上激活该管理虚拟机，它可以在 vSwitch0 上的网络上正常启动。如果 VMware vCenter 是管理虚拟机，则此过程尤其重要。如果 vCenter 位于 VDS 上，并移至另一台主机，然后再启动，则它在启动后将无法连接到网络。

在此设计中使用了两个 iSCSI 启动 vSwitch。Cisco UCS iSCSI 启动需要使用单独的 vNIC 进行 iSCSI 启动。这些 vNIC 使用适当网络结构的 iSCSI VLAN 作为原生 VLAN，并连接到相应的 iSCSI 启动 vSwitch。或者，您也可以通过部署新的 VDS 或使用现有 VDS 在 VDS 上部署 iSCSI 网络。

VM 主机关联性组和规则

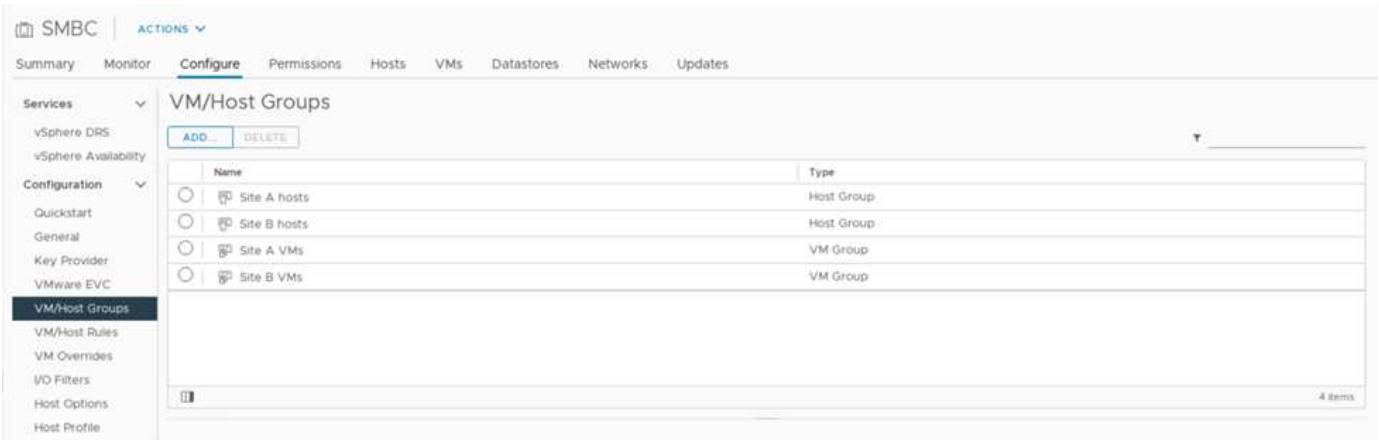
要使虚拟机能够在两个 SM-BC 站点的任何 ESXi 主机上运行，所有 ESXi 主机都必须从两个站点挂载 iSCSI 数

据存储库。如果所有 ESXi 主机均已正确挂载两个站点中的数据存储库，则可以在使用 vMotion 的任何主机之间迁移虚拟机，并且虚拟机仍可访问从这些数据存储库创建的所有虚拟磁盘。

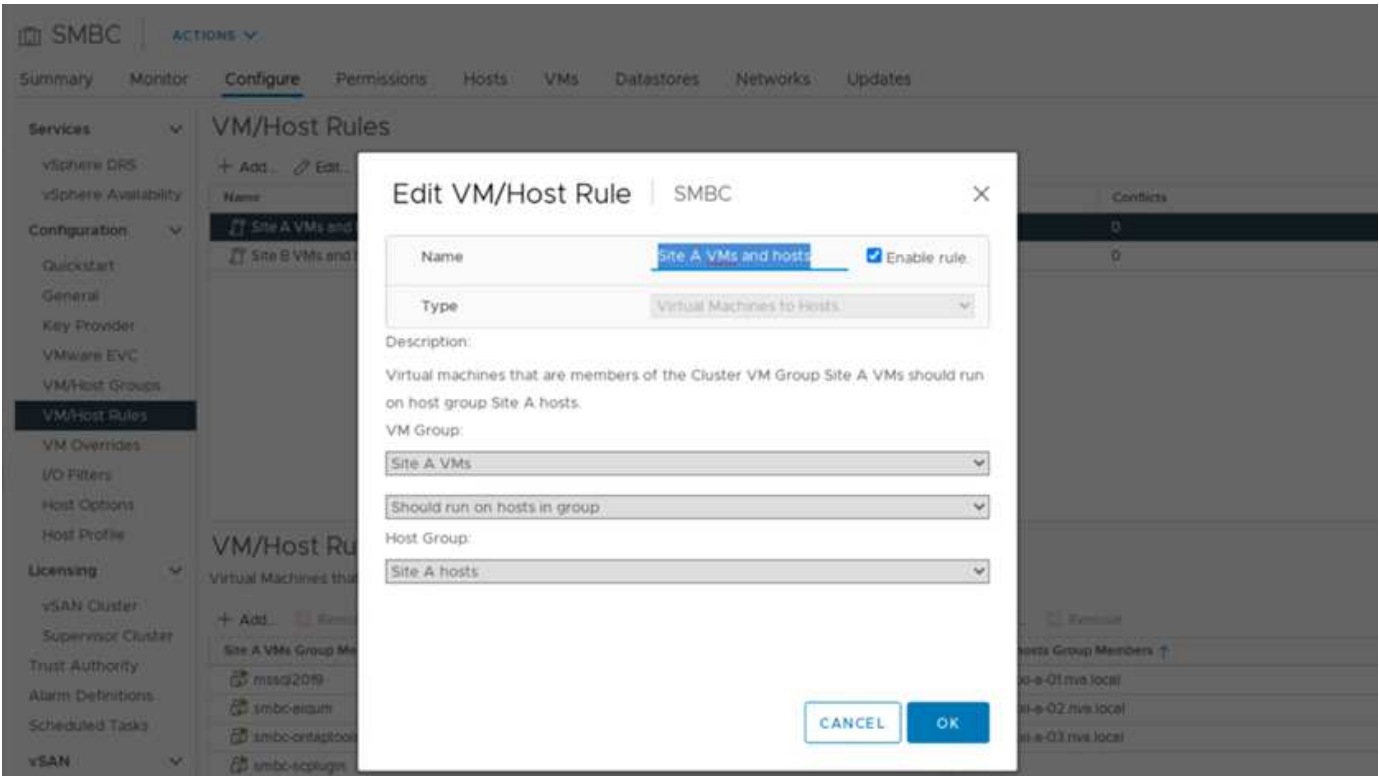
对于使用本地数据存储库的虚拟机，如果将其迁移到远程站点的主机，则其对虚拟磁盘的访问将变得远程，从而由于站点之间的物理距离而增加读取操作延迟。因此，最佳做法是将虚拟机保留在本地主机上，并利用站点上的本地存储。

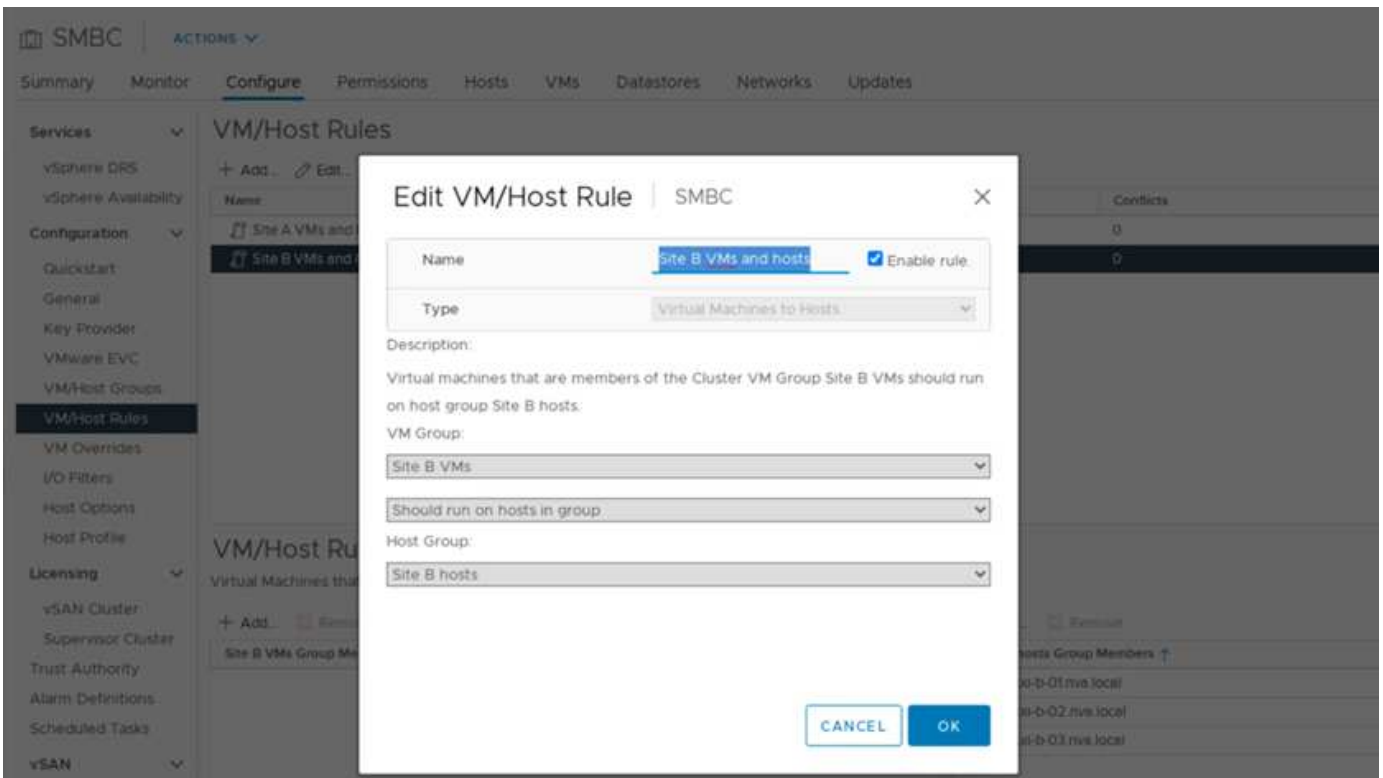
通过使用 VM/ 主机关联性机制，您可以使用 VM/ 主机组为位于特定站点的虚拟机和主机创建 VM 组和主机组。使用 VM/ 主机规则，您可以为要遵循的 VM 和主机指定策略。要在站点维护或灾难情形下允许跨站点进行虚拟机迁移，请使用 " 应在组中的主机上运行 " 策略规范来实现这种灵活性。

以下屏幕截图显示了为站点 A 和站点 B 主机及 VM 创建的两个主机组和两个 VM 组



此外，以下两个图显示了为站点 A 和站点 B VM 创建的 VM/ 主机规则，这些 VM 将使用 " 应在组中的主机上运行 " 策略在其各自站点的主机上运行。

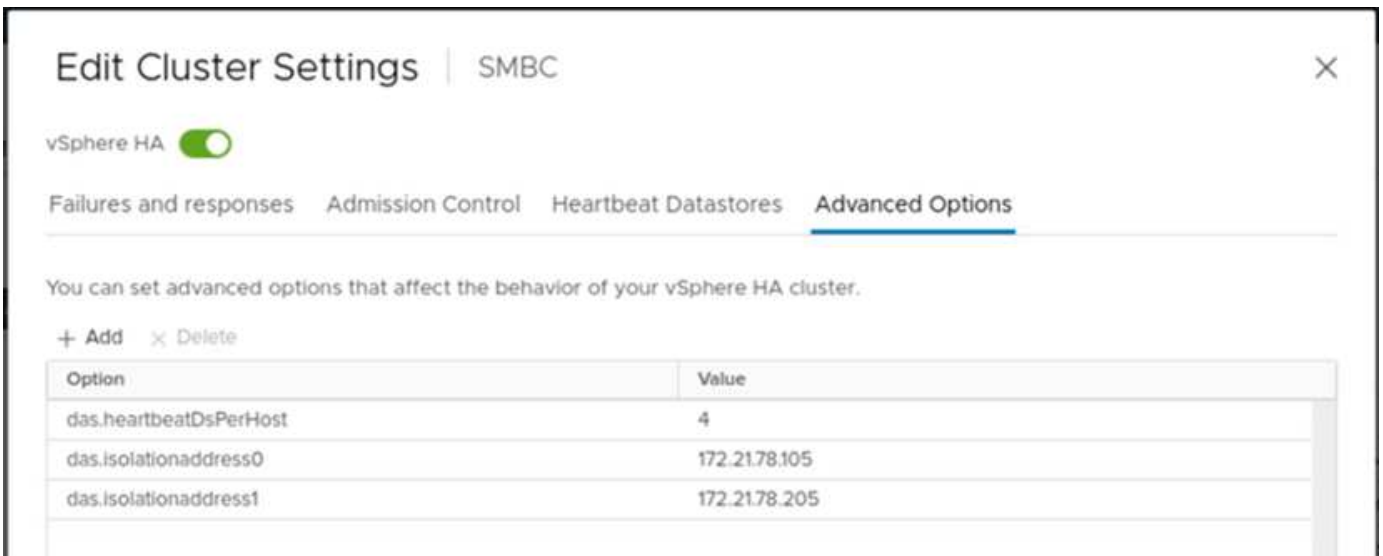




vSphere HA 检测信号

VMware vSphere HA 具有用于主机状态验证的检测信号机制。主要检测信号机制是通过网络连接实现的，而二级检测信号机制是通过数据存储库实现的。如果未收到检测信号，则它会通过对默认网关或手动配置的隔离地址执行 Ping 操作来确定它是否与网络隔离。对于数据存储库检测信号，VMware 建议将延伸型集群的检测信号数据存储库从最少 2 个增加到 4 个。

对于解决方案 验证，使用两个 ONTAP 集群管理 IP 地址作为隔离地址。此外，还添加了建议的 vSphere HA 高级选项 `das.s.batDsPerHost`，其值为 4，如下图所示。



对于检测信号数据存储库，指定集群中的四个共享数据存储库并自动进行补充，如下图所示。

Edit Cluster Settings | SMBC

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 2 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 type="checkbox"/>	infra_swap_a	N/A	6
<input type="checkbox"/>	infra_swap_b	N/A	6
<input checked="" type="checkbox"/>	infra_datastore_b_02	N/A	6
<input checked="" type="checkbox"/>	infra_datastore_a_01	N/A	6
<input checked="" type="checkbox"/>	infra_datastore_a_02	N/A	6
<input checked="" type="checkbox"/>	infra_datastore_b_01	N/A	6

CANCEL

OK

有关 VMware HA 集群和 VMware vSphere Metro 存储集群的其他最佳实践和配置，请参见 ["创建和使用 vSphere HA 集群"](#)，["VMware vSphere 城域存储集群（VMSC）"](#) 和 VMware 知识库 ["采用 NetApp SnapMirror 业务连续性（SM-BC）和 VMware vSphere 城域存储集群（VMSC）的 NetApp ONTAP"](#)。

"接下来：解决方案 验证—经验证的场景。"

解决方案 验证—经验证的场景

"先前版本：解决方案 验证—虚拟化。"

FlexPod 数据中心 SM-BC 解决方案 可为各种单点故障情形以及站点灾难提供数据服务保护。每个站点上实施的冗余设计可提供高可用性，而具有跨站点同步数据复制功能的 SM-BC 实施可保护数据服务，使其免受站点范围内灾难的影响。已对部署的解决方案 进行了验证，以确定其所需的解决方案 功能以及解决方案 可保护的各种故障情形。

我们会使用多种测试用例来验证解决方案 功能，并模拟部分和完整的站点故障情形。为了最大限度地减少与现有 FlexPod 数据中心解决方案在 Cisco 验证设计计划下执行的测试的重复，本报告重点介绍了解决方案 中与 SM-BC 相关的方面。我们提供了一些常规 FlexPod 验证，供实践人员进行实施验证。

为了进行解决方案 验证，在两个站点的所有 ESXi 主机上为每个 ESXi 主机创建一个 Windows 10 虚拟机。安装了 IOmeter 工具，并使用该工具为从共享本地 iSCSI 数据存储库映射的两个虚拟数据磁盘生成 I/O。配置的 IOmeter 工作负载参数包括 8 KB I/O，75% 读取和 50% 随机，每个数据磁盘具有 8 个未完成的 I/O 命令。对于执行的大多数测试场景，IOmeter I/O 的继续发生原因 表示此场景不会造成数据服务中断。

由于 SM-BC 对于数据库服务器等业务应用程序至关重要，测试中还包括 Windows Server 2022 虚拟机上的 Microsoft SQL Server 2019 实例，用于确认在本地站点的存储不可用且远程站点存储恢复数据服务而不使用应用程序时，应用程序仍会继续运行 中断。

ESXi 主机 iSCSI SAN 启动测试

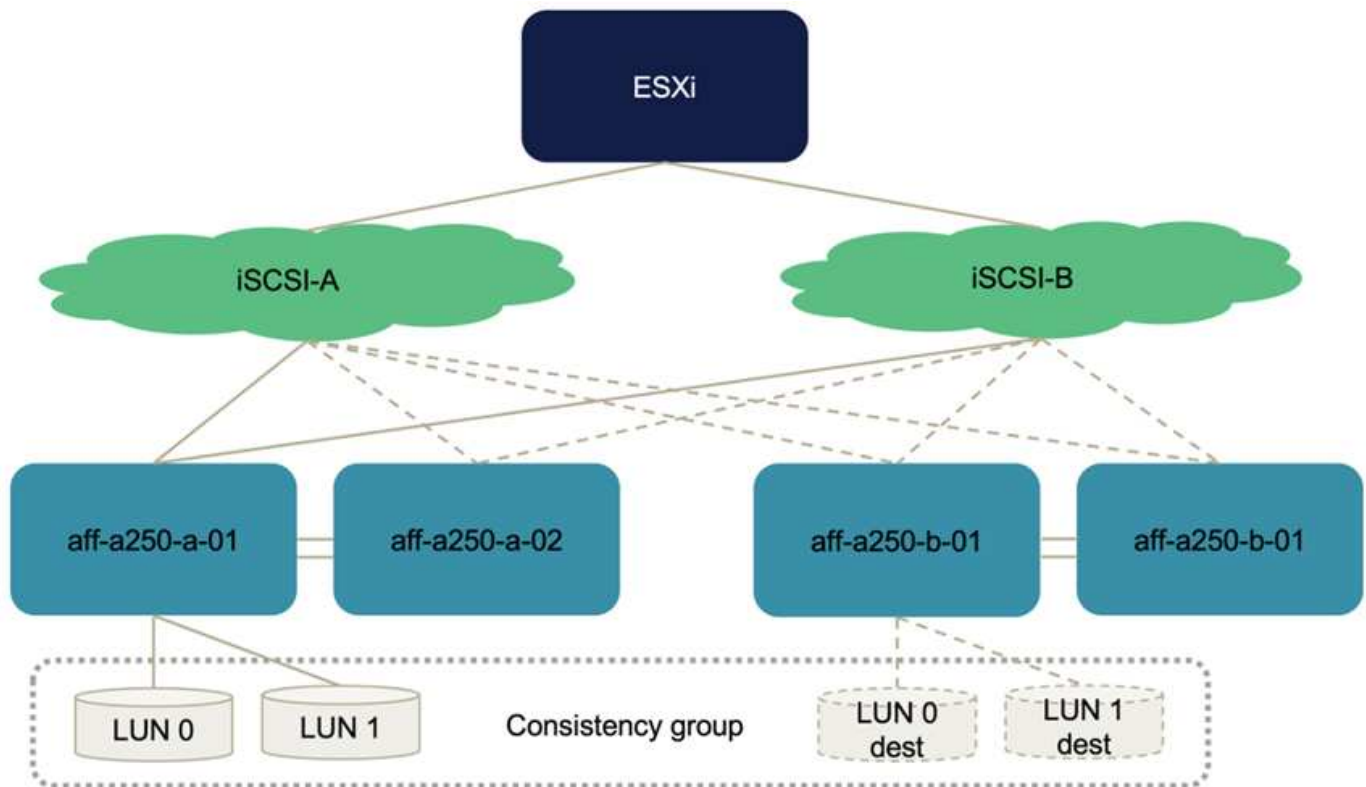
解决方案 中的 ESXi 主机已配置为从 iSCSI SAN 启动。使用 SAN 启动可以简化更换服务器时的服务器管理，因为服务器的服务配置文件可以与新服务器关联，以便在不更改任何其他配置的情况下启动它。

除了从本地 iSCSI 启动 LUN 启动站点上的 ESXi 主机之外，还会执行测试，以便在 ESXi 主机的本地存储控制器处于接管状态或其本地存储集群完全不可用时启动该主机。这些验证场景可确保根据设计正确配置 ESXi 主机，并可在存储维护或灾难恢复期间启动以实现业务连续性。

在配置 SM-BC 一致性组关系之前，存储控制器 HA 对托管的 iSCSI LUN 具有四个路径，根据最佳实践的实施情况，每个 iSCSI 网络结构有两个路径。主机可以通过两个 iSCSI VLAN/ 网络结构访问 LUN 到 LUN 托管控制器，也可以通过控制器的高可用性配对节点访问 LUN。

配置 SM-BC 一致性组关系并将镜像 LUN 正确映射到启动程序后，LUN 的路径数会增加一倍。在此实施中，它会从具有两个主动 / 优化路径和两个主动 / 非优化路径变为具有两个主动 / 优化路径和六个主动 / 非优化路径。

下图说明了 ESXi 主机访问 LUN 时可以使用的路径，例如 LUN 0。由于 LUN 连接到站点 A 控制器 01，因此只有通过该控制器直接访问 LUN 的两个路径处于活动 / 优化状态，其余六个路径均处于活动 / 非优化状态。



以下 storage-device-path 信息的屏幕截图显示了 ESXi 主机如何查看这两种类型的设备路径。两个主动 / 优化路径显示为具有 主动 (I/O) 路径状态，而六个主动 / 非优化路径仅显示为 主动。另请注意，目标列显示了两个 iSCSI 目标以及用于访问这些目标的相应 iSCSI LIF IP 地址。

esxi-a-01.nva.local

Summary Monitor **Configure** Permissions VMs Datastores Networks Updates

Storage

Storage Adapters

Storage Devices

Host Cache Configuration

Protocol Endpoints

I/O Filters

Networking

Virtual switches

VMkernel adapters

Physical adapters

TCP/IP configuration

Virtual Machines

VM Startup/Shutdown

Agent VM Settings

Default VM Compatibility

Swap File Location

System

Licensing

Host Profile

Time Configuration

Authentication Services

Storage Adapters

+ Add Software Adapter Refresh Rescan Storage... Rescan Adapter Remove

Adapter	Type	Status	Identifier	Targets	Devices	Paths
Model: iSCSI Software Adapter						
vmhba64	iSCSI	Online	iscsi_umiq(ign.2010-11.com.flexpod.ucs-smbc-a.1)	8	7	56
Model: Lewisburg SATA AHCI Controller						
vmhba0	Block SCSI	Unknown	-	0	0	0

Properties Devices **Paths** Dynamic Discovery Static Discovery Network Port Binding Advanced Options

Enable Disable

Runtime Name	Target	LUN	Status
vmhba64 C0:T0:L0	ign.1992-08.com.netapp.sn.2023c4ee6996f1ecb6d8d039ee488168 vs. 3.172.2180.106.3260	0	Active (I/O)
vmhba64 C3:T0:L0	ign.1992-08.com.netapp.sn.2023c4ee6996f1ecb6d8d039ee488168 vs. 3.172.2180.107.3260	0	Active
vmhba64 C2:T0:L0	ign.1992-08.com.netapp.sn.2023c4ee6996f1ecb6d8d039ee488168 vs. 3.172.2181106.3260	0	Active (I/O)
vmhba64 C1:T0:L0	ign.1992-08.com.netapp.sn.2023c4ee6996f1ecb6d8d039ee488168 vs. 3.172.2181107.3260	0	Active
vmhba64 C0:T1:L0	ign.1992-08.com.netapp.sn.b4db0fca5505f1ecb6d8d039ee488168 vs. 3.172.2180.206.3260	0	Active
vmhba64 C1:T1:L0	ign.1992-08.com.netapp.sn.b4db0fca5505f1ecb6d8d039ee488168 vs. 3.172.2180.207.3260	0	Active
vmhba64 C2:T1:L0	ign.1992-08.com.netapp.sn.b4db0fca5505f1ecb6d8d039ee488168 vs. 3.172.2181206.3260	0	Active
vmhba64 C3:T1:L0	ign.1992-08.com.netapp.sn.b4db0fca5505f1ecb6d8d039ee488168 vs. 3.172.2181207.3260	0	Active

当其中一个存储控制器因维护或升级而关闭时，到达已关闭控制器的两条路径将不再可用，而是显示路径状态 dead。

如果由于手动故障转移测试或自动灾难故障转移，一致性组在主存储集群上发生故障转移，则二级存储集群将继续为 SM-BC 一致性组中的 LUN 提供数据服务。由于 LUN 标识会保留下来，并且数据已同步复制，因此受 SM-BC 一致性组保护的所有 ESXi 主机启动 LUN 仍可从远程存储集群访问。

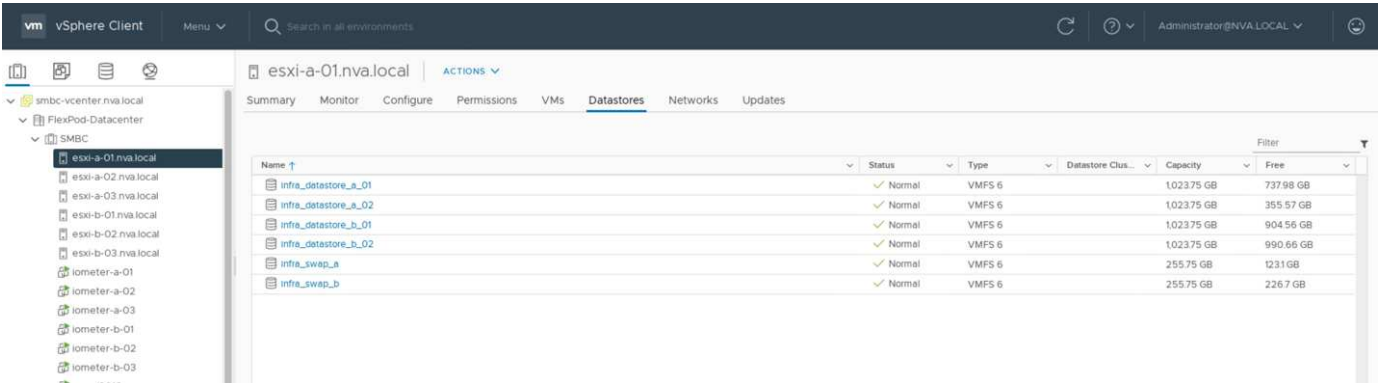
VMware vMotion 和 VM/ 主机关联性测试

虽然通用 FlexPod VMware Datacenter 解决方案 支持多协议，例如 FC ， iSCSI ， NVMe 和 NFS ， 但 FlexPod SM-BC 解决方案 功能支持通常用于业务关键型解决方案的 FC 和 iSCSI SAN 协议。此验证仅使用基于 iSCSI 协议的数据存储库和 iSCSI SAN 启动。

要允许虚拟机使用任何一个 SM-BC 站点的存储服务，集群中的所有主机都必须挂载两个站点的 iSCSI 数据存储库，以便在两个站点之间迁移虚拟机，并在发生灾难故障转移时进行迁移。

对于在虚拟基础架构上运行的不需要跨站点实施 SM-BC 一致性组保护的应用程序，也可以使用 NFS 协议和 NFS 数据存储库。在这种情况下，在为 VM 分配存储时必须谨慎，这样，业务关键型应用程序才能正确使用受 SM-BC 一致性组保护的 SAN 数据存储库来提供业务连续性。

以下屏幕截图显示主机已配置为从两个站点挂载 iSCSI 数据存储库。



您可以选择在两个站点的可用 iSCSI 数据存储库之间迁移虚拟机磁盘，如下图所示。出于性能考虑，最好让虚拟机使用其本地存储集群中的存储来减少磁盘 I/O 延迟。由于物理往返距离延迟约为每 100 公里 1 毫秒，因此当两个站点相隔一定距离时尤其如此。

Migrate | iometer-a-01

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE

CONFIGURE PER DISK

CONFIGURE

<input type="checkbox"/>	Virtual Machine	File	Storage	Disk format	VM Storage Policy
<input type="checkbox"/>	iometer-a-01	Configuration File	infra_datastore_a_01	N/A	Datastore Default
<input type="checkbox"/>	iometer-a-01	Hard disk 1 (64.00 GB)	infra_datastore_a_02	Same format as sour...	Datastore Default
<input type="checkbox"/>	iometer-a-01	Hard disk 2 (20.00 GB)	infra_datastore_b_01	Same format as sour...	Datastore Default
<input type="checkbox"/>	iometer-a-01	Hard disk 3 (20.00 GB)	infra_datastore_b_02	Same format as sour...	Datastore Default

4 items

Compatibility

✓

Compatibility checks succeeded.

CANCEL

BACK

NEXT

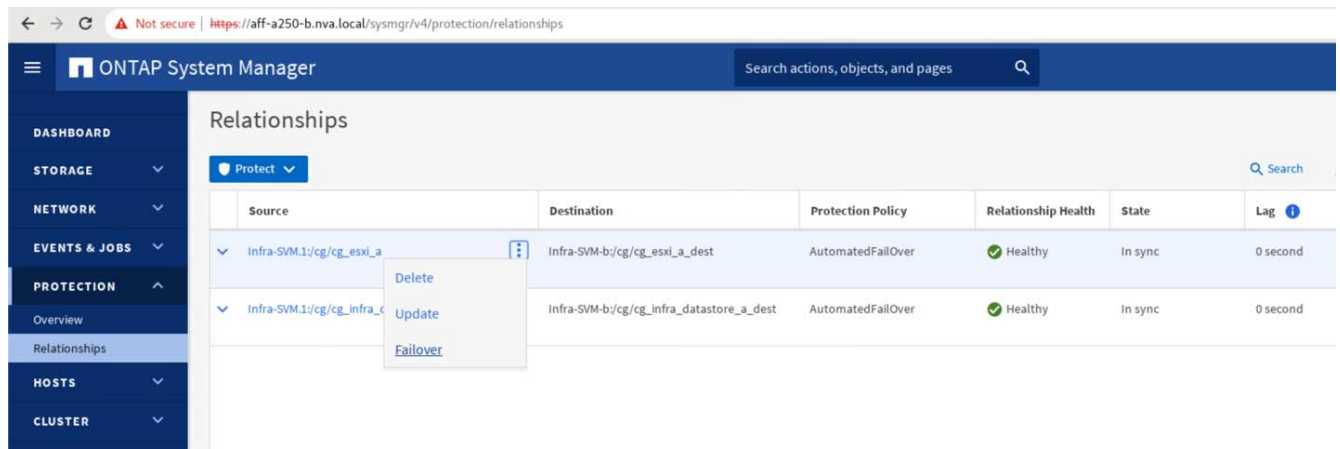
对虚拟机在同一站点以及不同站点的不同主机上的 vMotion 进行了测试，并取得了成功。在站点间手动迁移虚拟机后， VM/ 主机关联性规则会激活虚拟机并将其迁移回正常情况下所属的组。

计划内存储故障转移

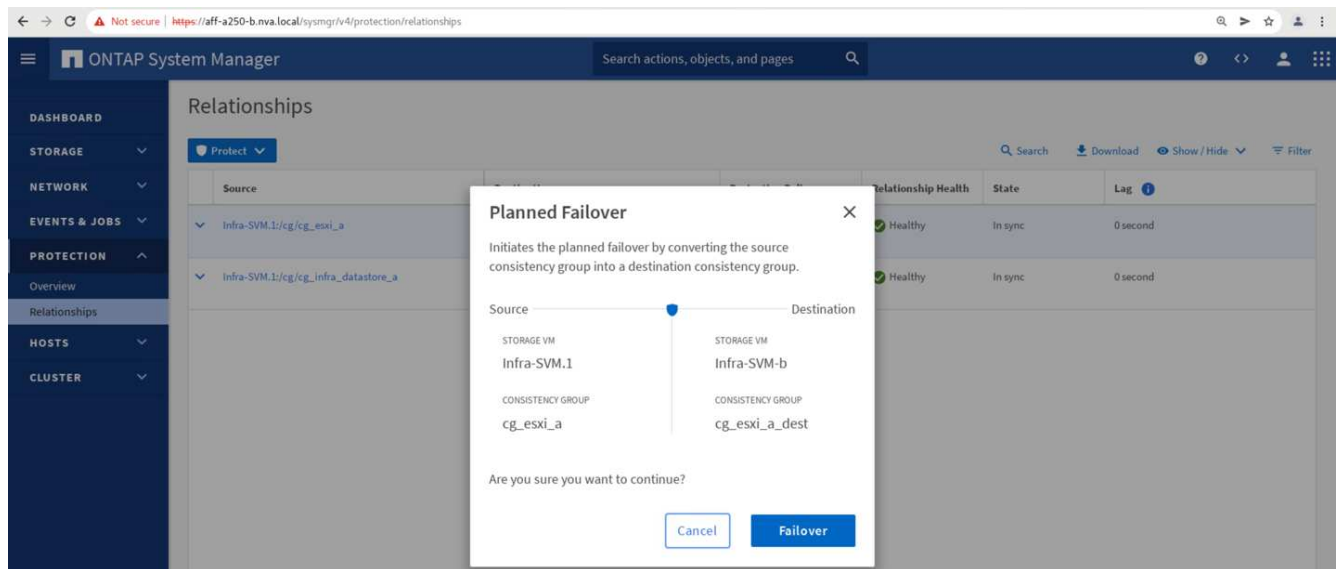
应在初始配置后对解决方案 执行计划内存储故障转移操作，以确定解决方案 在存储故障转移后是否正常工作。此测试有助于确定可能导致 I/O 中断的任何连接或配置问题。定期测试和解决任何连接或配置问题有助于在发生实际站点灾难时提供无中断的数据服务。也可以在计划的存储维护活动之前使用计划的存储故障转移，以便可以从不受影响的站点提供数据服务。

要启动站点 A 存储数据服务到站点 B 的手动故障转移，您可以使用站点 B ONTAP 系统管理器执行此操作。

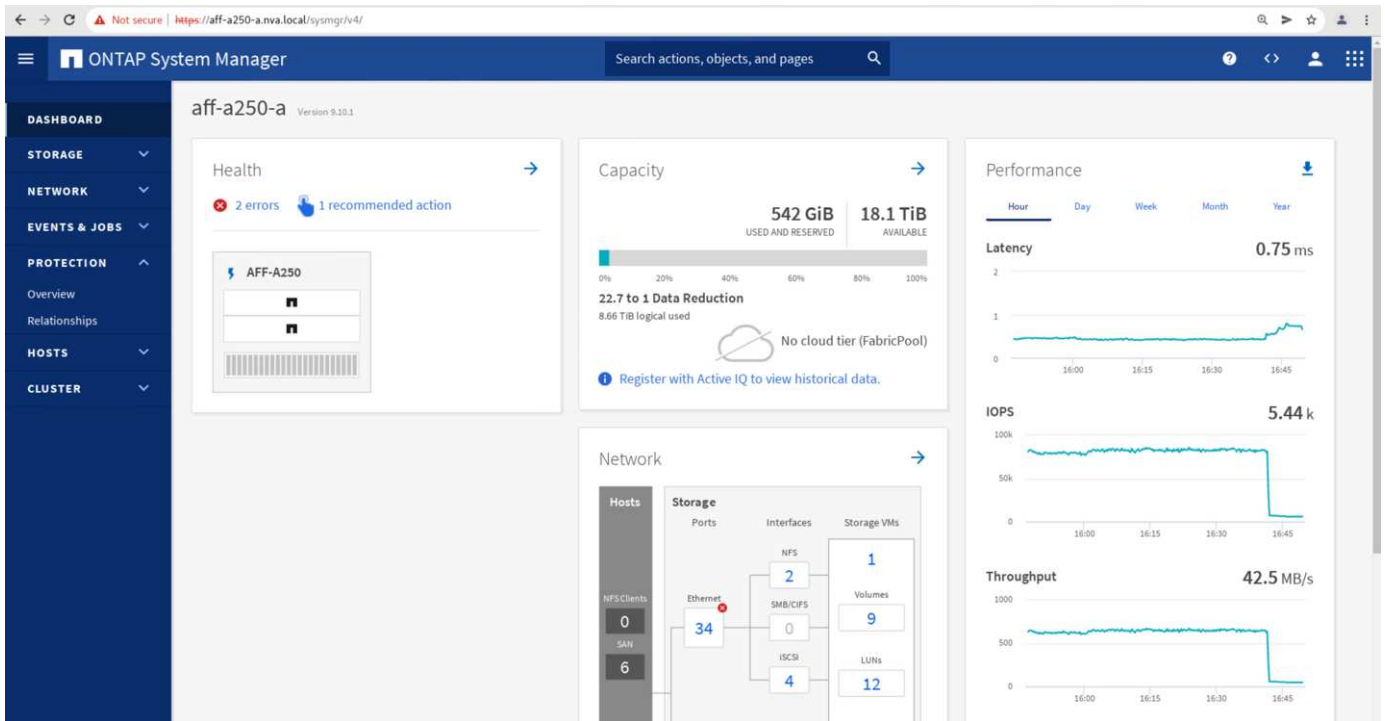
1. 导航到保护 > 关系屏幕，确认一致性组关系状态为 in Sync 。如果它仍处于 Synchronizing 状态，请等待状态变为 in Sync ，然后再执行故障转移。
2. 展开源名称旁边的点，然后单击故障转移。



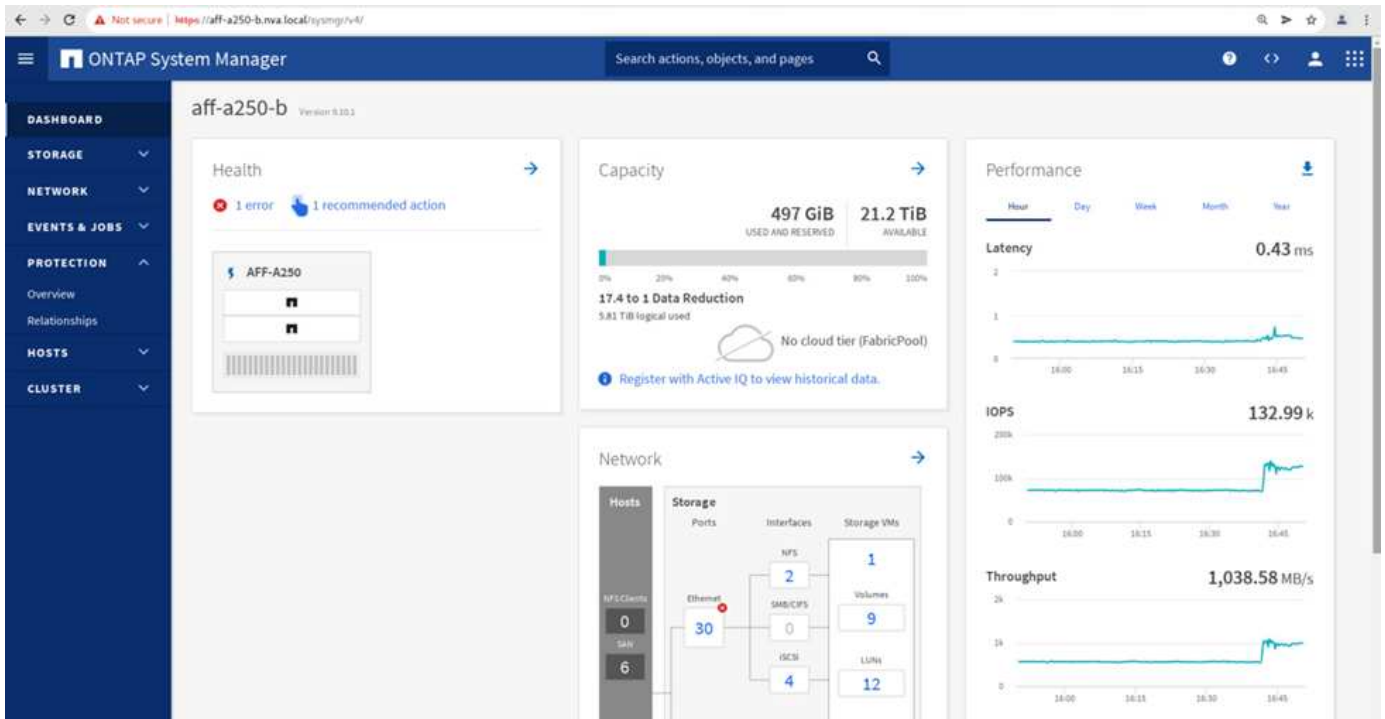
3. 确认故障转移以启动操作。



在站点 B System Manager 图形用户界面上对两个一致性组 CG_ESXi_A 和 CG_infra_datastore_A 启动故障转移后不久，为这两个一致性组提供服务的站点 A I/O 便移至站点 B 因此，站点 A 的 I/O 会显著减少，如站点 A System Manager 性能窗格中所示。



另一方面，站点 B System Manager 信息板的 "性能" 窗格显示 IOPS 显著增加，这是因为提供了从站点 A 转移到大约 130,000 IOPS 的额外 I/O。并达到大约 1GB/秒的吞吐量，同时 I/O 延迟保持在 1 毫秒以下。



随着 I/O 从站点 A 透明地迁移到站点 B，现在可以关闭站点 A 存储控制器以进行计划内维护。完成维护工作或测试并恢复站点 A 存储集群并使其正常运行后，请先检查并等待一致性组保护状态重新更改为同步，然后再执行故障转移，将故障转移 I/O 从站点 B 返回到站点 A。请注意，站点因维护或测试而关闭的时间越长，同步数据以及将一致性组返回到处于同步状态所需的时间就越长。

Not secure | https://aff-a250-a.nva.local/symgr/v4/protection/relationships

ONTAP System Manager

Search actions, objects, and pages

Relationships

Protect

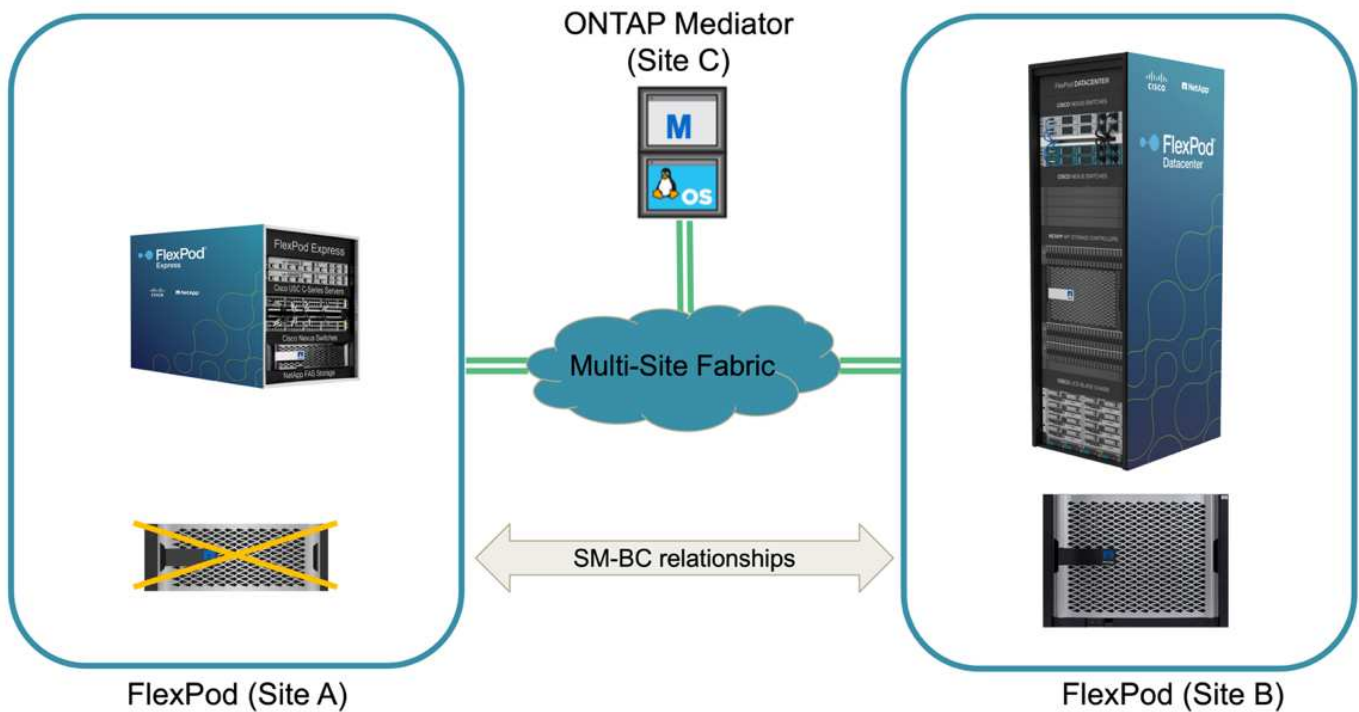
Search Download Show/Hide Filter

Source	Destination	Protection Policy	Relationship Health	State	Lag
▼ Infra-SVM.1:/cg/cg_infra_datastore_b	Infra-SVM-a:/cg/cg_infra_datastore_b_dest	AutomatedFailOver	Healthy	In sync	0 second
▼ Infra-SVM.1:/cg/cg_esxi_a_dest	Infra-SVM-a:/cg/cg_esxi_a	AutomatedFailOver	Healthy	In sync	0 second
▼ Infra-SVM.1:/cg/cg/	Infra-SVM-a:/cg/cg_infra_datastore_a	AutomatedFailOver	Healthy	In sync	0 second
▼ Infra-SVM.1:/cg/cg/	Infra-SVM-a:/cg/cg_esxi_b_dest	AutomatedFailOver	Healthy	In sync	0 second

Delete Update Failover

计划外存储故障转移

发生实际灾难或进行灾难模拟期间，可能会发生计划外存储故障转移。例如，请参见下图，其中站点 A 的存储系统发生断电，触发计划外存储故障转移，站点 A LUN 的数据服务受 SM-BC 关系保护，然后从站点 B 继续提供



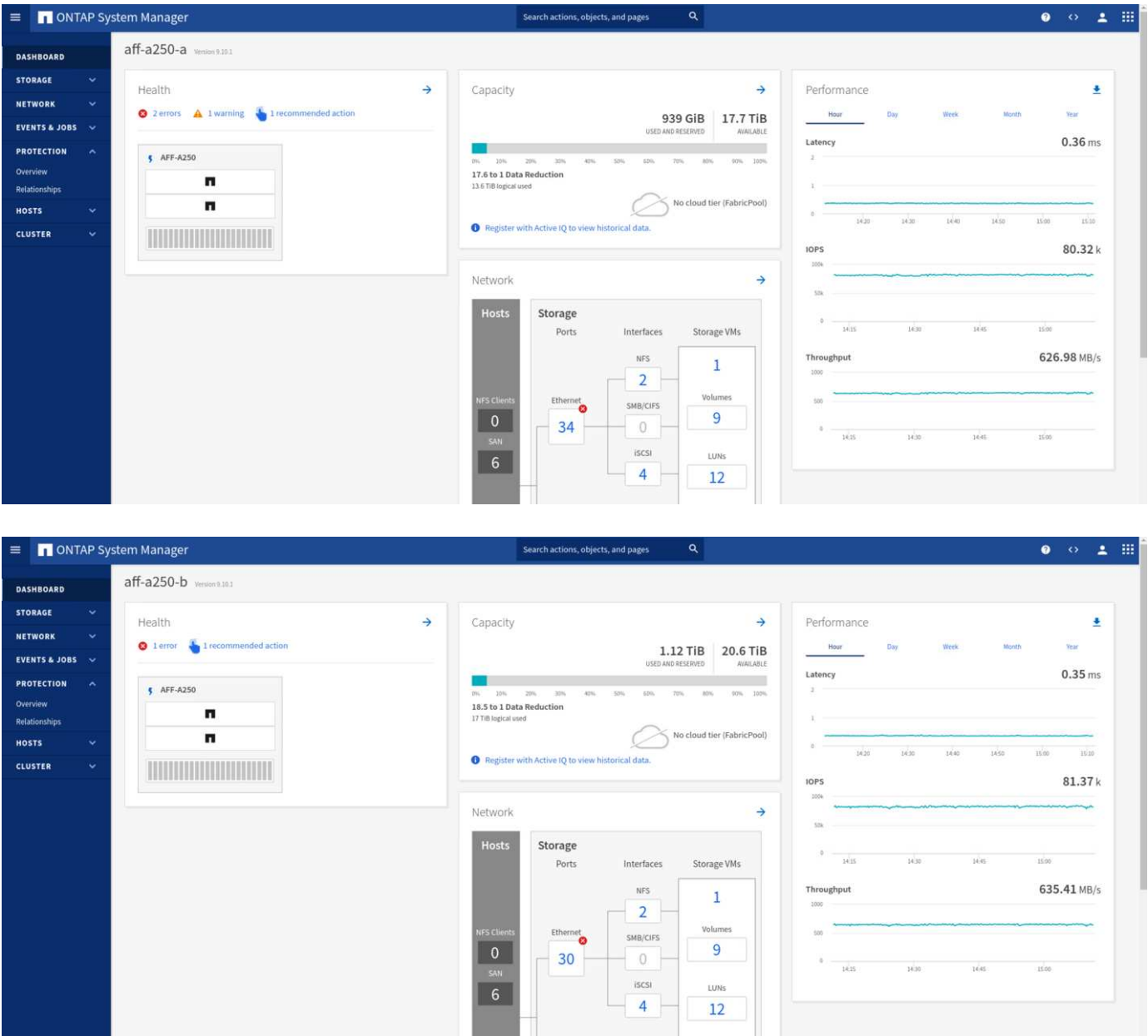
要模拟站点 A 的存储灾难，可以通过物理关闭电源开关来关闭站点 A 的两个存储控制器，从而停止为控制器供电。或者使用存储控制器服务处理器的 system power management 命令关闭控制器。

当站点 A 的存储集群断电时，站点 A 存储集群提供的数据服务会突然停止。然后，用于监控第三个站点的 SM-BC 解决方案的 ONTAP 调解器会检测站点的存储故障情况，并使 SM-BC 解决方案能够执行自动计划外故障转移。这样，站点 B 存储控制器就可以继续为与站点 A 建立的 SM-BC 一致性组关系中配置的 LUN 提供数据服务

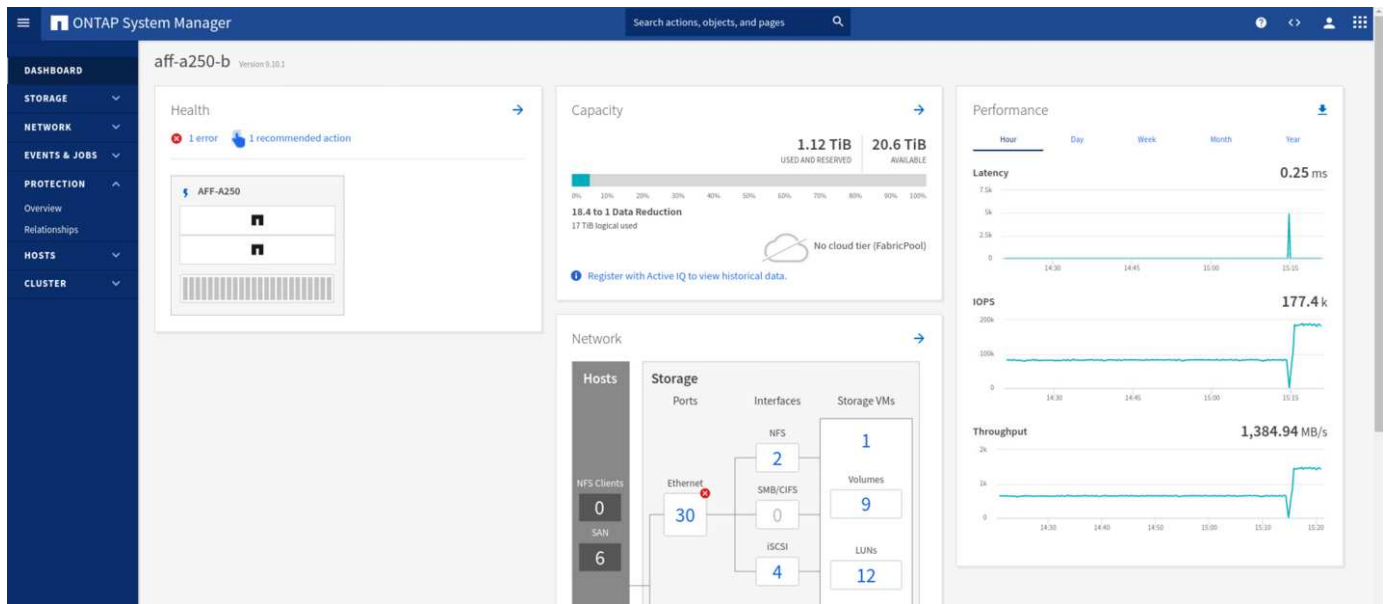
从应用程序角度来看，操作系统会短暂暂停数据服务，同时检查 LUN 的路径状态，然后恢复正常运行的站点 B 存储控制器的可用路径上的 I/O。

在验证测试期间，两个站点的 VM 上的 IOMeter 工具会为其本地数据存储库生成 I/O。关闭站点 A 集群后，I/O 会短暂暂停，然后恢复。请参见以下两个数据，分别查看发生灾难前站点 A 和站点 B 存储集群的信息板，这些

信息板显示每个站点的 IOPS 约为 80 ， 000 次，吞吐量约为 600 MB/ 秒。



关闭站点 A 的存储控制器后，我们可以直观地验证站点 B 存储控制器 I/O 是否急剧增加，以便代表站点 A 提供额外的数据服务（请参见下图）。此外，IOMeter VM 的 GUI 还显示，尽管站点 A 存储集群发生中断，I/O 仍会继续。请注意，如果有其他数据存储库由不受 SM-BC 关系保护的 LUN 提供支持，则在发生存储灾难时，这些数据存储库将无法再访问。因此，必须评估各种应用程序数据的业务需求，并将其正确放置在受 SM-BC 关系保护的数据存储库中，以确保业务连续性。



当站点 A 集群关闭时，一致组的关系会显示 不同步 状态，如下图所示。重新打开站点 A 存储控制器的电源后，存储集群将启动，站点 A 和站点 B 之间的数据同步将自动进行。

The screenshot shows the 'Relationships' page in the ONTAP System Manager. The table lists two relationships that are 'Out of sync'.

Source	Destination	Protection Policy	Relationship Health	State	Lag
infra-SVM.1/cg/cg_esxi_a	infra-SVM-b/cg/cg_esxi_a_dest	AutomatedFailOver	Healthy	Out of sync	1 hour, 22 minutes and 56 seconds
infra-SVM.1/cg/cg_infra_datastore_a	infra-SVM-b/cg/cg_infra_datastore_a_dest	AutomatedFailOver	Healthy	Out of sync	1 hour, 29 minutes and 35 seconds

在将数据服务从站点 B 返回到站点 A 之前，您必须检查站点 A System Manager 并确保 SM-BC 关系正常运行且状态恢复同步。确认一致性组处于同步状态后，可以启动手动故障转移操作，将一致性组关系中的数据服务返回到站点 A

The screenshot shows the 'Relationships' page in the ONTAP System Manager after a failover. The table lists four relationships that are now 'In sync'.

Source	Destination	Protection Policy	Relationship Health	State	Lag
infra-SVM.1/cg/cg_infra_datastore_b	infra-SVM-a/cg/cg_infra_datastore_b_dest	AutomatedFailOver	Healthy	In sync	0 second
infra-SVM.1/cg/cg_esxi_a_dest	infra-SVM-a/cg/cg_esxi_a	AutomatedFailOver	Healthy	In sync	0 second
infra-SVM.1/cg/cg_infra_datastore_a_dest	infra-SVM-a/cg/cg_infra_datastore_a	AutomatedFailOver	Healthy	In sync	0 second
infra-SVM.1/cg/cg_esxi_b	infra-SVM-a/cg/cg_esxi_b_dest	AutomatedFailOver	Healthy	In sync	0 second

完成站点维护或站点故障

站点可能需要进行站点维护，断电或受到飓风或地震等自然灾害的影响。因此，您必须练习计划内和计划外站点故障情形，以确保 FlexPod SM-BC 解决方案 配置正确，使其在所有业务关键型应用程序和数据服务发生此类故障时不受影响。已验证以下与站点相关的场景。

- 通过将虚拟机和关键数据服务迁移到另一站点来规划站点维护方案
- 通过关闭服务器和存储控制器以进行灾难模拟而发生计划外站点中断的情形

要使站点做好计划内站点维护的准备，需要将受影响的虚拟机迁移出站点并执行 vMotion 以及手动故障转移 SM-BC 一致性组关系，以便将虚拟机和关键数据服务迁移到备用站点。测试按两个不同的顺序执行：首先执行 vMotion，然后执行 SM-BC 故障转移和先执行 SM-BC 故障转移，再执行 vMotion，以确认虚拟机继续运行且数据服务未中断。

在执行计划内迁移之前，请更新 VM/ 主机关联性规则，以便站点上当前运行的 VM 自动迁移出正在维护的站点。以下屏幕截图显示了修改站点 A VM/ 主机关联性规则以使 VM 自动从站点 A 迁移到站点 B 的示例。您还可以选择临时禁用关联性规则，以便可以手动迁移 VM，而不是指定现在需要在站点 B 上运行 VM。

Edit VM/Host Rule
SMBC

Name
Site A VMs and hosts
☒ Enable rule.

Type
Virtual Machines to Hosts

Description:

Virtual machines that are members of the Cluster VM Group Site A VMs must run on host group Site B hosts.

VM Group:

Site A VMs

Must run on hosts in group

Host Group:

Site B hosts

CANCEL

OK

迁移虚拟机和存储服务后，您可以关闭服务器，存储控制器，磁盘架和交换机的电源，并执行所需的站点维护活动。完成站点维护并恢复 FlexPod 实例后，您可以更改 VM 的主机组关联性以返回到其原始站点。之后，您应将 " 必须在组中的主机上运行 " VM/ 主机站点关联性规则改回 " 应在组中的主机上运行 "，以便在发生灾难时，虚拟机可以在另一站点的主机上运行。在验证测试中，所有虚拟机均已成功迁移到另一站点，在对 SM-BC 关系执行故障转移后，数据服务继续正常运行。

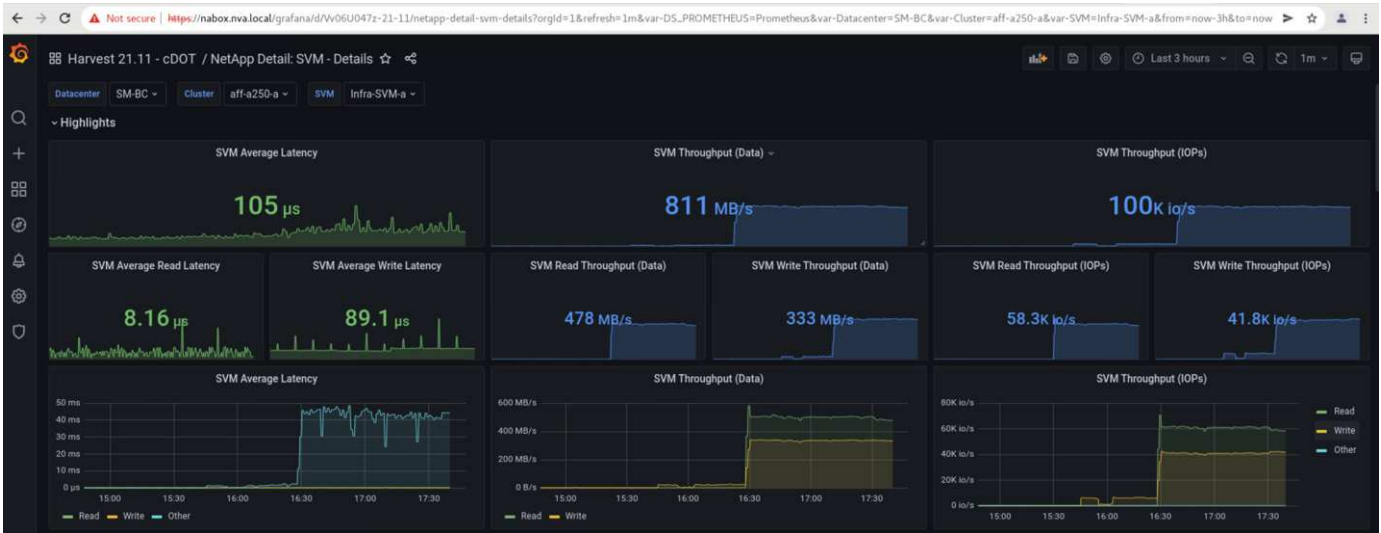
对于计划外站点灾难模拟，服务器和存储控制器已关闭，以模拟站点灾难。VMware HA 功能可检测已关闭的虚拟机，并在运行正常的站点上重新启动这些虚拟机。此外，在第三个站点运行的 ONTAP 调解器会检测站点故障，而运行正常的站点会启动故障转移，并开始按预期为故障站点提供数据服务。

以下屏幕截图显示了存储控制器的服务处理器 CLI 用于突然关闭站点 A 集群以模拟站点 A 存储灾难。

```
[BMC aff-a250-a-01>
[BMC aff-a250-a-01>
[BMC aff-a250-a-01>
[BMC aff-a250-a-01>system power off
Chassis Power Control: Down/Off
BMC aff-a250-a-01>

[BMC aff-a250-a-02>
[BMC aff-a250-a-02>
[BMC aff-a250-a-02>
[BMC aff-a250-a-02>system power off
Chassis Power Control: Down/Off
BMC aff-a250-a-02>
```

以下两个屏幕截图显示了由 NetApp 收集数据工具捕获并显示在 NASbox 监控工具的 Grafana 信息板中的存储集群的 Storage Virtual Machine 信息板。如 IOPS 和吞吐量图的右侧所示，站点 B 集群会在站点 A 集群关闭后立即接管集群 A 的存储工作负载。





Microsoft SQL Server

Microsoft SQL Server 是一种广泛采用和部署的数据库平台，适用于企业 IT。Microsoft SQL Server 2019 版为其关系和分析引擎提供了许多新功能和增强功能。它支持在内部，云中和混合环境中运行应用程序的工作负载，两者可以结合使用。此外，它还可以部署在多个平台上，包括 Windows，Linux 和容器。

作为 FlexPod SM-BC 解决方案 业务关键型工作负载验证的一部分，安装在 Windows Server 2022 虚拟机上的 Microsoft SQL Server 2019 与 IOMeter 虚拟机一起提供，用于执行计划内和计划外存储故障转移测试。在 Windows Server 2022 VM 上，安装了 SQL Server Management Studio 来管理 SQL 服务器。在测试中，使用 HammerDB 数据库工具生成数据库事务。

HammerDB 数据库测试工具配置为使用 Microsoft SQL Server TPROC-C 工作负载进行测试。对于架构构建配置，这些选项已更新为使用包含 10 个虚拟用户的 100 个仓库，如以下屏幕截图所示。

Microsoft SQL Server TPROC-C Build Options

Build Options

SQL Server: (local)

TCP: ☐

SQL Server Port: 1433

Azure: ☐

SQL Server ODBC Driver: ODBC Driver 17 for SQL Server

Authentication: ☒ Windows Authentication
☐ SQL Server Authentication

SQL Server User ID: sa

SQL Server User Password: admin

TPROC-C SQL Server Database: tpcc

In-Memory OLTP: ☐

In-Memory Hash Bucket Multiplier: 1

In-Memory Durability: ☒ SCHEMA_AND_DATA
☐ SCHEMA_ONLY

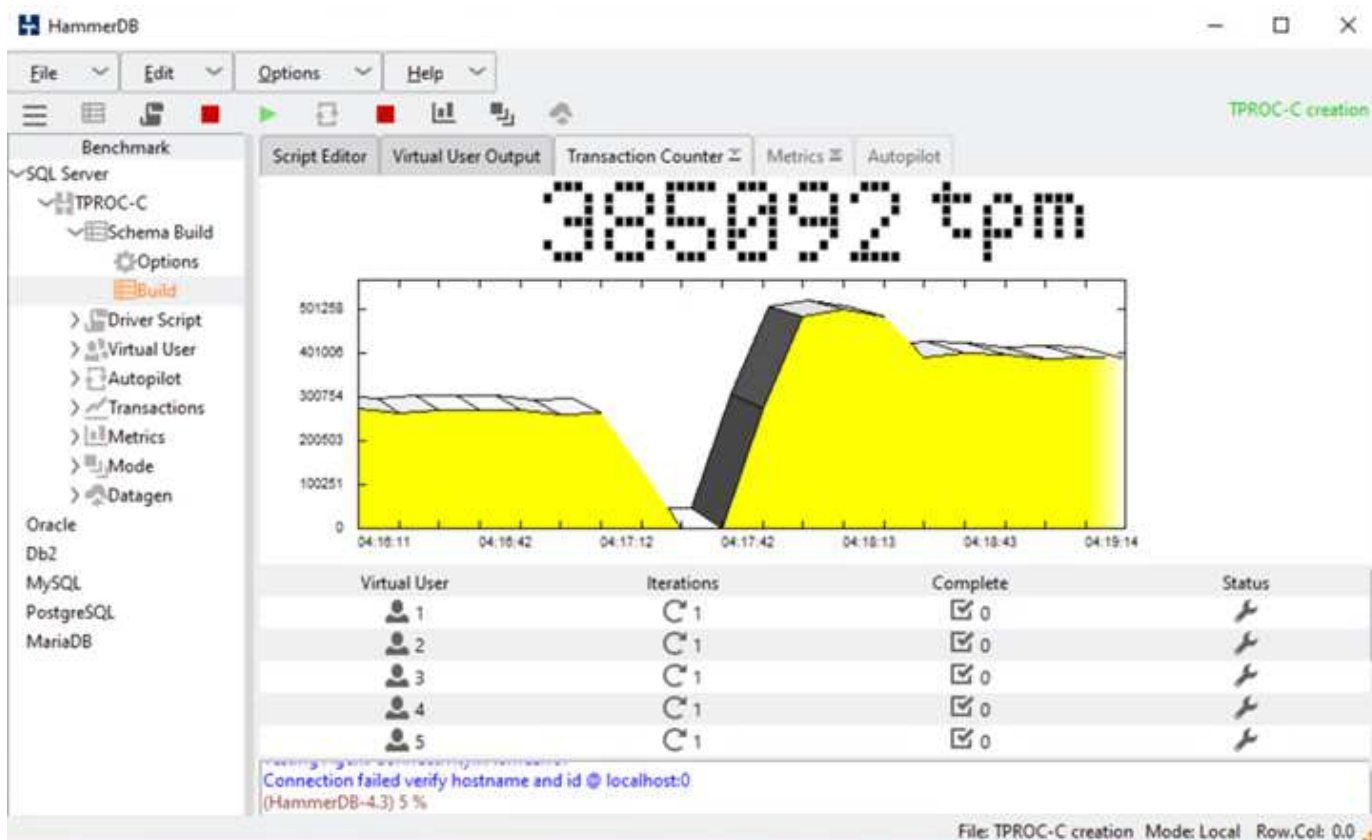
Number of Warehouses: 100

Virtual Users to Build Schema: 10

OK Cancel

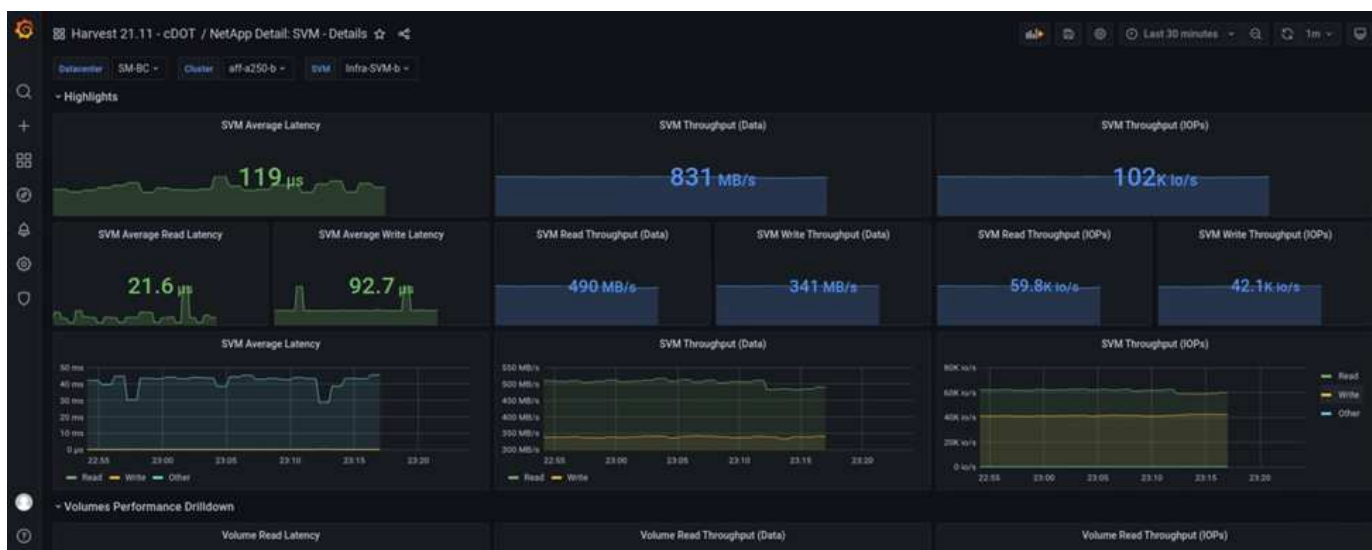
更新架构构建选项后，架构构建过程便已启动。几分钟后，由于使用 `system processor` 命令行界面命令大约同时关闭了双节点 AFF A250 存储集群的两个节点，因此出现了计划外模拟站点 B 存储集群故障。

在短暂暂停数据库事务后，启动了用于灾难修复的自动故障转移，并恢复了事务。以下屏幕截图显示了该时间的 HammerDB 事务计数器屏幕截图。由于 Microsoft SQL Server 的数据库通常驻留在站点 B 存储集群上，因此，当站点 B 的存储发生故障时，事务会短暂暂停，然后在发生自动故障转移后恢复。



存储集群指标是通过在安装了 NetApp 收集监控工具的情况下使用 NAbbox 工具捕获的。结果将显示在 Storage Virtual Machine 和其他存储对象的预定义 Grafana 信息板中。此信息板可提供延迟，吞吐量，IOPS 和其他详细信息的度量值，站点 B 和站点 A 的读取和写入统计信息将分开

此屏幕截图显示了站点 B 存储集群的 NAbbox Grafana 性能信息板。



在引入灾难之前，站点 B 存储集群的 IOPS 约为 100,000 IOPS。然后，由于发生灾难，性能指标在图形的右侧急剧下降到零。由于站点 B 存储集群已关闭，因此在发生灾难后，无法从站点 B 集群收集任何数据。

另一方面，在自动故障转移之后，站点 A 存储集群的 IOPS 从站点 B 中接管了其他工作负载。在以下屏幕截图中，您可以轻松地在 IOPS 和吞吐量图的右侧看到额外的工作负载，其中显示了站点 A 存储集群的 NAbbox Grafana 性能信息板。



上述存储灾难测试场景确认，在数据库所在的站点 B 上，Microsoft SQL Server 工作负载可以在存储集群完全中断的情况下继续运行。检测到灾难并发生故障转移后，应用程序会透明地使用站点 A 存储集群提供的数据服务。

在计算层，当特定站点上运行的 VM 发生主机故障时，VM 会通过 VMware HA 功能自动重新启动。要使站点计算完全中断，VM/ 主机关联性规则允许在运行正常的站点上重新启动 VM。但是，要使业务关键型应用程序能够提供无中断服务，需要使用基于应用程序的集群，例如 Microsoft 故障转移集群或基于 Kubernetes 容器的应用程序架构，以避免应用程序停机。请参见有关实施基于应用程序的集群的相关文档，该文档不在本技术报告的讨论范围之内。

"接下来：总结。"

结论

"先前版本：解决方案 验证—经验证的场景。"

采用 SM-BC 的 FlexPod 数据中心采用主动 - 主动数据中心设计，为业务关键型工作负载提供业务连续性和灾难恢复。解决方案 通常会将部署在不同地理位置分散的城域中的两个数据中心互连在一起。NetApp SM-BC 解决方案 使用同步复制来保护业务关键型数据服务免受站点故障的影响。解决方案 要求两个 FlexPod 部署站点的往返网络延迟低于 10 毫秒。

部署在第三个站点上的 NetApp ONTAP 调解器可监控 SM-BC 解决方案，并在检测到站点灾难时实现自动故障转移。采用 VMware HA 和延伸型 VMware vSphere Metro Storage Cluster 的 VMware vCenter 配置可与 NetApp SM-BC 无缝结合使用，从而使解决方案 能够满足所需的零 RPO 和接近零 RTO 目标。

如果 FlexPod SM-BC 解决方案 符合要求，也可以部署在现有 FlexPod 基础架构上，或者通过向现有 FlexPod 添加额外的 FlexPod 解决方案 来实现业务连续性目标。NetApp 和 Cisco 还提供了其他管理，监控和自动化工具，例如 Cisco Intersight，Ansible 和 HashiCorp Terraform 自动化工具，您可以轻松监控解决方案，深入了解其运行情况，并自动执行其部署和操作。

从业务关键型应用程序（例如 Microsoft SQL Server）的角度来看，即使站点存储中断，驻留在受 ONTAP SM-BC CG 关系保护的 VMware 数据存储库上的数据库仍然可用。验证测试期间已验证，数据库所在存储集群断电后，将发生 SM-BC CG 关系故障转移，Microsoft SQL Server 事务将继续进行，而不会造成应用程序中断。

借助应用程序粒度数据保护，可以为业务关键型应用程序创建 ONTAP SM-BC CG 关系，以满足零 RPO 和接近零 RTO 要求。为了使运行 Microsoft SQL Server 应用程序的 VMware 集群能够在站点存储中断的情况下继续运行，每个站点上 ESXi 主机的启动 LUN 也会受到 SM-BC CG 关系的保护。

借助 FlexPod 的灵活性和可扩展性，您可以从规模合适的基础架构入手，随着业务需求的变化不断扩展和发展。通过这一经过验证的设计，您可以在分布式集成基础架构上可靠地部署基于 VMware vSphere 的私有云，从而提供一个可在多种单点故障情形下以及站点故障下进行故障恢复的解决方案，以保护关键业务数据服务。

["下一步：从何处查找追加信息和版本历史记录。"](#)

从何处查找追加信息和版本历史记录

["上一篇：结论。"](#)

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：

FlexPod

- FlexPod 主页

["https://www.flexpod.com"](https://www.flexpod.com)

- 适用于 FlexPod 的 Cisco 验证设计和部署指南

["https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"](https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html)

- Cisco 服务器—统一计算系统（ Unified Computing System ， UCS ）

["https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html"](https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html)

- NetApp 产品文档

["https://www.netapp.com/support-and-training/documentation/"](https://www.netapp.com/support-and-training/documentation/)

- 采用 UCS 托管模式的 FlexPod Datacenter 4.2 （ 1 ） ， VMware vSphere 7.0 U2 和 NetApp ONTAP 9.9 设计指南

["https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2_design.html"](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2_design.html)

- 《采用 UCS 托管模式的 FlexPod UCS 4.2 （ 1 ） ， VMware vSphere 7.0 U2 和 NetApp ONTAP 9.9 部署指南》

["https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html"](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html)

- 采用 Cisco UCS X 系列， VMware 7.0 U2 和 NetApp ONTAP 9.9 的 FlexPod 数据中心设计指南

["https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html)

- 《采用 Cisco UCS X 系列， VMware 7.0 U2 和 NetApp ONTAP 9.9 的 FlexPod 数据中心部署指南》

["https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmware_7u2.h"](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmware_7u2.html)

tml"

- 《采用 Cisco UCS Mini 和 NetApp AFF/FAS NVA 的 VMware vSphere 7.0 FlexPod 快速设计指南》

<https://www.netapp.com/pdf.html?item=/media/22621-nva-1154-DESIGN.pdf>

- 《适用于采用 Cisco UCS Mini 和 NetApp AFF/FAS NVA 的 VMware vSphere 7.0 的 FlexPod 快速部署指南》

<https://www.netapp.com/pdf.html?item=/media/21938-nva-1154-DEPLOY.pdf>

- 采用 VXLAN 多站点前端网络结构的 FlexPod MetroCluster IP

<https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/flexpod-metrocluster-ip-vxlan-multi-site-wp.pdf>

- NAbbox

<https://nabox.org>

- NetApp 收获

<https://github.com/NetApp/harvest/releases>

SM — BC

- SM — BC

<https://docs.netapp.com/us-en/ontap/smbc/index.html>

- TR-4878 : 《 SnapMirror 业务连续性 (SM-BC) ONTAP 9.8 》

<https://www.netapp.com/pdf.html?item=/media/21888-tr-4878.pdf>

- 如何正确删除 SnapMirror 关系 ONTAP 9

https://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/SnapMirror/How_to_correctly_delete_a_SnapMirror_relationship_ONTAP_9

- SnapMirror 同步灾难恢复基础知识

<https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-synchronous-disaster-recovery-basics-concept.html>

- 异步 SnapMirror 灾难恢复基础知识

<https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-disaster-recovery-concept.html#data-protection-relationships>

- 数据保护和灾难恢复

<https://docs.netapp.com/us-en/ontap/data-protection-disaster-recovery/index.html>

- 安装或升级 ONTAP 调解器服务

["https://docs.netapp.com/us-en/ontap/mediator/index.html"](https://docs.netapp.com/us-en/ontap/mediator/index.html)

VMware vSphere HA 和 vSphere Metro Storage Cluster

- 创建和使用 vSphere HA 集群

["https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html"](https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html)

- VMware vSphere 城域存储集群（VMSC）

["https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-vmcsc"](https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-vmcsc)

- VMware vSphere Metro Storage Cluster 建议的实践

["https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-recommended-practices"](https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-recommended-practices)

- 采用 NetApp SnapMirror 业务连续性（SM-BC）和 VMware vSphere Metro Storage Cluster（VMSC）的 NetApp ONTAP。（83370）

["https://kb.vmware.com/s/article/83370"](https://kb.vmware.com/s/article/83370)

- 使用 VMware vSphere Metro Storage Cluster 和 ONTAP 保护第 1 层应用程序和数据库

["https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-tier-1-applications-and-databases-with-VMware-vSphere-Metro-Storage/ba-p/171636"](https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-tier-1-applications-and-databases-with-VMware-vSphere-Metro-Storage/ba-p/171636)

Microsoft SQL 和 HammerDB

- Microsoft SQL Server 2019

["https://www.microsoft.com/en-us/sql-server/sql-server-2019"](https://www.microsoft.com/en-us/sql-server/sql-server-2019)

- 《在 VMware vSphere 上构建 Microsoft SQL Server 最佳实践指南》

["https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf"](https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf)

- HammerDB 网站

["https://www.hammerdb.com"](https://www.hammerdb.com)

兼容性表

- Cisco UCS 硬件兼容性列表

["https://ucshcltool.cloudapps.cisco.com/public/"](https://ucshcltool.cloudapps.cisco.com/public/)

- NetApp 互操作性表工具

["https://support.netapp.com/matrix/"](https://support.netapp.com/matrix/)

- NetApp Hardware Universe

["https://hww.netapp.com"](https://hww.netapp.com)

- VMware 兼容性指南

["http://www.vmware.com/resources/compatibility/search.php"](http://www.vmware.com/resources/compatibility/search.php)

版本历史记录

version	Date	文档版本历史记录
版本 1.0	2022 年 4 月	初始版本。

采用VMware vSphere 7.0、Cisco VXLAN单站点网络结构和NetApp ONTAP 9.7的FlexPod 数据中心—设计

NetApp公司Cisco Abhinav Singh Ramesh Isaac

Cisco验证设计(CVD)由系统和解决方案组成、这些系统和解决方案经过设计、测试和记录、可帮助客户部署并改进部署。这些设计将广泛的技术和产品整合到一个解决方案组合中、这些解决方案是为满足客户的业务需求而开发的。Cisco和NetApp合作推出了FlexPod、作为各种工作负载的基础、并提供了强大、高效且可扩展的架构设计、以满足客户需求。FlexPod 解决方案 是一种经过验证的方法、用于部署Cisco和NetApp技术和产品以构建共享私有云和公共云基础架构。

["采用VMware vSphere 7.0、Cisco VXLAN单站点网络结构和NetApp ONTAP 9.7的FlexPod 数据中心—设计"](#)

采用VMware vSphere 7.0和NetApp ONTAP 9.7的FlexPod Datacenter—部署

NetApp公司Cisco Sree Lakshmi Lan的John George

本文档介绍了在NetApp AFF A400全闪存存储系统上使用NetApp ONTAP 9.7的Cisco和NetApp FlexPod Datacenter、采用第二代Intel Xeon可扩展处理器的Cisco UCS Manager统一软件版本4.1 (2)以及VMware vSphere 7.0。Cisco UCS Manager (UCSM) 4.1 (2)提供以下整合支持：

- 所有当前的Cisco UCS互联阵列型号：6200、6300、6324 (Cisco UCS Mini)
- 6400/16
- 2200/23400/2400系列IOM
- Cisco UCS B 系列
- Cisco UCS C 系列

此外、还包括Cisco Intersight和NetApp Active IQ SaaS管理平台。

采用NetApp ONTAP 9.7、Cisco UCS统一软件版本4.1 (2)和VMware vSphere 7.0的FlexPod 数据中心包含一个基于Cisco统一计算系统(Cisco UCS)、Cisco Nexus 9000系列交换机、MDS 9000多层光纤交换机构建的预先设

计的最佳实践数据中心架构、 以及运行ONTAP 9.7数据管理软件的NetApp AFF A系列存储阵列。

["采用VMware vSphere 7.0和NetApp ONTAP 9.7的FlexPod Datacenter—部署"](#)

采用Cisco Intersight和NetApp ONTAP 9.7的FlexPod 数据中心—设计

NetApp公司Cisco Scott kovacs的John George

本文档介绍了Cisco和NetApp FlexPod 解决方案、这是一种经验证的将Cisco和NetApp技术部署为共享云基础架构的方法。这种经过验证的设计为在FlexPod 上部署VMware vSphere提供了一个框架、VMware vSphere是企业级数据中心中最受欢迎的虚拟化平台。

["采用Cisco Intersight和NetApp ONTAP 9.7的FlexPod 数据中心—设计"](#)

采用Cisco Intersight和NetApp ONTAP 9.7的FlexPod Datacenter—部署

NetApp公司Cisco Scott kovacs的John George

当前数据中心设计的行业趋势是共享基础架构。通过将虚拟化与经过预先验证的IT平台结合使用、企业客户已经踏上了云之旅、从应用程序孤岛向可快速部署的共享基础架构过渡、从而提高了灵活性并降低了成本。Cisco和NetApp携手推出了FlexPod、该产品使用同类最佳的存储、服务器和网络组件作为各种工作负载的基础、能够快速、自信地部署高效的架构设计。

["采用Cisco Intersight和NetApp ONTAP 9.7的FlexPod Datacenter—部署"](#)

采用Cisco Intersight和NetApp ONTAP 9.7的FlexPod 数据中心—设计

NetApp公司Cisco Scott kovacs的John George

本文档介绍了一个经过验证的解决方案、用于将Cisco和NetApp技术部署为共享云基础架构。这种经过验证的设计为在FlexPod 上部署VMware vSphere提供了一个框架、VMware vSphere是企业级数据中心中最受欢迎的虚拟化平台。

FlexPod 是一款领先的集成基础架构、支持广泛的企业工作负载和用例。借助此解决方案、客户可以在集成基础架构上快速可靠地部署基于VMware vSphere的私有云。

["采用Cisco Intersight和NetApp ONTAP 9.7的FlexPod 数据中心—设计"](#)

采用VMware vSphere 6.7 U2、Cisco UCS fourth-generation Fabric和NetApp ONTAP 9.6的FlexPod Datacenter

NetApp公司Cisco Sree Lakshmi Lan的John George

本文档介绍采用NetApp ONTAP 9.6的Cisco和NetApp FlexPod Datacenter、采用第二代Intel Xeon可扩展处理器的Cisco UCS Manager统一软件版本4.0 (4)以及VMware vSphere 6.7 U2。Cisco UCS Manager (UCSM) 4.0 (4)提供以下整合支持：

- 所有当前的Cisco UCS互联阵列型号：6200、6300、6324 (Cisco UCS Mini)
- 6454
- 2200/23400/2400系列IOM
- Cisco UCS B 系列
- Cisco UCS C系列。

采用NetApp ONTAP 9.6、Cisco UCS统一软件4.0 (4)版和VMware vSphere 6.7 U2的FlexPod Datacenter是一种基于Cisco统一计算系统(Cisco UCS)、Cisco Nexus 9000系列交换机、MDS 9000多层光纤交换机构建的预先设计的最佳实践数据中心架构。 以及运行ONTAP 9的NetApp AFF A系列存储阵列。

["采用VMware vSphere 6.7 U2、Cisco UCS第四代网络结构和NetApp ONTAP 9.6的FlexPod 数据中心"](#)

采用VMware vSphere 6.7 U1、Cisco UCS第四代网络结构和NetApp AFF A系列的FlexPod Datacenter—设计

NetApp公司Cisco Sree Lakshmi Lan的John George

本文档介绍了Cisco和NetApp FlexPod 解决方案、这是一种经验证的将Cisco和NetApp技术部署为共享云基础架构的方法。这种经过验证的设计为在FlexPod 上部署VMware vSphere提供了一个框架、VMware vSphere是企业级数据中心中最受欢迎的虚拟化平台。

FlexPod 是一款领先的集成基础架构、支持广泛的企业工作负载和用例。借助此解决方案、客户可以在集成基础架构上快速可靠地部署基于VMware vSphere的私有云。

建议的解决方案 架构基于使用统一软件版本的Cisco统一计算系统(Cisco UCS)构建、以支持Cisco UCS硬件平台、包括Cisco UCS B系列刀片式服务器和C系列机架式服务器、Cisco UCS 6454互联阵列、Cisco Nexus 9000系列交换机、Cisco MDS光纤通道交换机、和NetApp全闪存系列存储阵列。此外、它还包括VMware vSphere 6.7 Update 1、它提供了许多新功能、用于优化存储利用率和促进私有云。

["采用VMware vSphere 6.7 U1、Cisco UCS第四代网络结构和NetApp AFF A系列的FlexPod Datacenter—设计"](#)

采用VMware vSphere 6.7 U1、Cisco UCS第四代网络结构和NetApp AFF A系列的FlexPod 数据中心

NetApp公司Cisco Scott kovacs的John George

本文档介绍了采用Cisco UCS Manager统一软件版本4.0 (2)和VMware vSphere 6.7 U1

的Cisco和NetApp FlexPod Datacenter。Cisco UCS Manager (UCSM) 4.0 (2)可为所有当前的Cisco UCS互联阵列型号(6200、6300、6324 (Cisco UCS Mini))、6454、2200/2300系列IOM、Cisco UCS B系列和Cisco UCS C系列提供整合支持。采用Cisco UCS统一软件版本4.0 (2)和VMware vSphere 6.7 U1的FlexPod 数据中心是一种预先设计的最佳实践数据中心架构、它基于Cisco统一计算系统(UCS)、Cisco Nexus 9000系列交换机、MDS 9000多层光纤交换机、以及运行ONTAP 9存储操作系统的NetApp AFF A系列存储阵列。

["采用VMware vSphere 6.7 U1、Cisco UCS第四代网络结构和NetApp AFF A系列的FlexPod 数据中心"](#)

采用Cisco ACI Multi-Pod、NetApp MetroCluster IP和VMware vSphere 6.7的FlexPod 数据中心—设计

NetApp公司Cisco Arvind Ramakrishnan的Haseeb Niazi

本文档介绍了如何将Cisco ACI Multi-Pod和NetApp MetroCluster IP解决方案 集成到FlexPod 数据中心中、以提供高度可用的多数据中心解决方案。利用多数据中心架构、可以利用无中断工作负载移动性在两个数据中心之间平衡工作负载、从而无需持续中断即可在站点之间迁移服务。

采用ACI Multi-Pod和NetApp MetroCluster IP解决方案 的FlexPod 具有以下优势：

- 跨数据中心无缝移动工作负载
- 站点间策略一致
- 跨地理位置分散的数据中心的第2层扩展
- 在维护期间更好地避免停机
- 避免灾难和恢复

["采用Cisco ACI Multi-Pod、NetApp MetroCluster IP和VMware vSphere 6.7的FlexPod 数据中心—设计"](#)

采用Cisco ACI Multi-Pod的FlexPod 数据中心、采用NetApp MetroCluster IP和VMware vSphere 6.7—部署

Haseeb Niazi、Cisco Ramesh Issac、Cisco Arvind Ramakrishnan、NetApp

Cisco和NetApp合作推出了一系列FlexPod 解决方案、支持战略数据中心平台。FlexPod 解决方案 提供了一个集成的架构、该架构整合了计算、存储和网络的最佳设计实践、通过验证集成架构以确保各个组件之间的兼容性、从而最大程度地降低IT风险。此外、解决方案 还通过提供书面设计指导、部署指导和支持来解决IT难题、这些指导和支持可在部署的各个阶段(规划、设计和实施)中使用。

["采用Cisco ACI Multi-Pod的FlexPod 数据中心、采用NetApp MetroCluster IP和VMware vSphere 6.7—部署"](#)

版权信息

版权所有 © 2024 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，本文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。