FlexPod 解决方案

FlexPod

NetApp
March 25, 2024

目录

FlexPod 解决方案

FlexPod 定义

FlexPod 快速技术规格

TR-4293： FlexPod 快速技术规格

NetApp 公司 Karthick Radhakrishnan， Arvind Ramakrishnan， Lindsey Street， Savita Kumari

FlexPod Express 是一种预先设计的最佳实践架构，它基于 Cisco 统一计算系统（Cisco UCS）和 Cisco Nexus 系列交换机构建，存储层使用 NetApp FAS 或 NetApp E 系列存储构建。FlexPod Express 是一个适合运行各种虚拟化虚拟机管理程序，裸机操作系统（OS）和企业工作负载的平台。

FlexPod Express 不仅提供了基线配置，还可以灵活地调整规模并进行优化，以满足多种不同的使用情形和要求。本文档将根据所使用的存储系统，采用 NetApp FAS 的 FlexPod Express 以及采用 E 系列的 FlexPod Express 对 FlexPod Express 配置进行分类。

FlexPod 平台

FlexPod 平台有三种：

- * FlexPod Datacenter 。 * 此平台是一个可大规模扩展的虚拟数据中心基础架构，适合工作负载企业级应用程序，虚拟化， VDI 以及公有和私有云。FlexPod 数据中心具有自己的规格，如中所述 "TR-4036：FlexPod 数据中心技术规格"。
- * FlexPod Express* 。此平台是一个紧凑型融合基础架构，面向远程办公室和边缘使用情形。

本文档提供了 FlexPod 快速平台的技术规格。

FlexPod 规则

FlexPod 设计支持灵活的基础架构，其中包含许多不同的组件和软件版本。

使用规则集作为构建或整合有效 FlexPod 配置的指南。本文档中列出的数字和规则是 FlexPod 的最低要求；可以根据不同环境和使用情形的需要，将其扩展到所包含的产品系列中。

支持的 FlexPod 配置与经验证的 配置

FlexPod 架构由本文档中所述的一组规则定义。Cisco 硬件兼容性列表（Hardware Compatibility List， HCL）和必须支持硬件组件和软件配置 "NetApp 互操作性表工具（IMT）"。

每个 Cisco 验证设计（Cisco Validated Design， CVD）或 NetApp 验证架构（NetApp Verified Architecture， NVA）都是一种可能的 FlexPod 配置。Cisco 和 NetApp 会记录这些配置组合，并通过广泛的端到端测试对其进行验证。如果与这些配置不同的 FlexPod 部署遵循本文档中的准则，并且所有组件在 Cisco HCL 和 NetApp 中均列为兼容，则完全支持这些部署 "IMT"。

例如，如果软件，硬件和配置符合本文档中定义的准则，则完全支持添加其他存储控制器或 Cisco UCS 服务器

并将软件升级到较新版本。

存储软件

FlexPod Express 支持运行 NetApp ONTAP 或 SANtricity 操作系统的存储系统。

NetApp ONTAP

NetApp ONTAP 软件是在 AFF 和 FAS 存储系统上运行的操作系统。ONTAP 提供了一个高度可扩展的存储架构，可实现无中断运行，无中断升级和灵活的数据基础架构。

有关 ONTAP 的详细信息，请参见 "ONTAP 产品页面"。

E 系列 SANtricity 软件

E 系列 SANtricity 软件是在 E 系列存储系统上运行的操作系统。SANtricity 提供了一个高度灵活的系统，可满足不同的应用程序需求，并提供内置的高可用性和各种数据保护功能。

有关详细信息，请参见 "SANtricity 产品页面"。

最低硬件要求

本节介绍不同版本的 FlexPod Express 的最低硬件要求。

采用 NetApp FAS 的 FlexPod Express

使用 NetApp FAS 控制器进行底层存储的 FlexPod 快速解决方案的硬件要求包括本节中所述的配置。

基于 CIMC 的配置（独立机架服务器）

Cisco Integrated Management Controller （ CIMC ）配置包括以下硬件组件：

- 采用冗余配置的两个10 Gbps标准以太网交换机(建议使用Cisco Nexus 31108、并支持Cisco Nexus 3000和9000型号)
- Cisco UCS C 系列独立机架式服务器
- 采用高可用性（ HA ）对配置的两个 AFF C190 ， AFF A250 ， FAS2600 或 FAS 2700 系列控制器，部署为双节点集群

Cisco UCS 管理的配置

Cisco UCS 管理的确认包括以下硬件组件：

- 采用冗余配置的两个 10 Gbps 标准以太网交换机（建议使用 Cisco Nexus 3524 ）
- 一个 Cisco UCS 5108 交流（ AC ）刀片式服务器机箱
- 两个 Cisco UCS 6324 互联阵列
- Cisco UCS B 系列服务器（至少四个 Cisco UCS B200 M5 刀片式服务器）
- 一个 HA 对配置中的两个 AFF C190 ， AFF A250 ， FAS2750 或 FAS2720 控制器（每个控制器需要两个可用的统一目标适配器 2 个端口）

采用 **E** 系列的 **FlexPod Express**

采用 E 系列入门级配置的 FlexPod Express 的硬件要求包括：

- 两个 Cisco UCS 6324 互联阵列
- 一个 Cisco UCS Mini 机箱 5108 AC2 或 DC2 （仅 AC2 和 DC2 机箱支持 Cisco UCS 6324 互联阵列）
- Cisco UCS B 系列服务器（至少两个 Cisco UCS B200 M4 刀片式服务器）
- E 系列 E2824 存储系统的一个 HA 对配置，其中至少加载 12 个磁盘驱动器
- 采用冗余配置的两个 10 Gbps 标准以太网交换机（可以使用数据中心中的现有交换机）

构建解决方案的入门级配置需要这些硬件组件；可以根据需要添加更多刀片式服务器和磁盘驱动器。E 系列 E2824 存储系统可以替换为更高的平台，也可以作为全闪存系统运行。

最低软件要求

本节介绍不同版本的 FlexPod Express 的最低软件要求。

采用 **NetApp AFF** 或 **FAS** 的 **FlexPod Express** 的软件要求

采用 NetApp FAS 的 FlexPod Express 的软件要求包括：

- ONTAP 9.1 或更高版本
- Cisco NX-OS 7.0 （ 3 ） I6 （ 1 ）或更高版本
- 在 Cisco UCS 管理的配置中， Cisco UCS Manager UCS 4.0 （ 1b ）

必须在中列出并支持所有软件 "NetApp IMT"。某些软件功能所需的代码版本可能比先前架构中列出的最低版本更新。

采用 **E** 系列的 **FlexPod Express** 的软件要求

采用 E 系列的 FlexPod Express 的软件要求包括：

- E 系列 SANtricity 软件 11.30 或更高版本
- Cisco UCS Manager 4.0 （ 1b ）。

必须在中列出并支持所有软件 "NetApp IMT"。

连接要求

本节介绍不同版本的 FlexPod Express 的连接要求。

FlexPod Express 与 **NetApp FAS** 的连接要求

采用 NetApp FAS 的 FlexPod Express 的连接要求包括：

- NetApp FAS 存储控制器必须直接连接到 Cisco Nexus 交换机，但 Cisco UCS 管理的配置除外，在该配置中，存储控制器连接到互联阵列。

- 不能在核心 FlexPod 组件之间实时放置任何其他设备。
- 要将 Cisco Nexus 3000/9000 系列交换机连接到 NetApp 存储控制器，需要使用虚拟端口通道（Virtual Port Channel， vPC）。
- 虽然不需要，但建议在整个环境中启用巨型帧支持。

采用 **NetApp E** 系列的 **FlexPod Express** 的连接要求

使用 E 系列的 FlexPod Express 的连接要求包括：

- E 系列存储控制器必须直接连接到互联阵列。
- 不应在核心 FlexPod 组件之间内联放置任何其他设备。
- 互联阵列和以太网交换机之间需要使用 vPC 。

FlexPod Express 与 **NetApp AFF** 的连接要求

采用 NetApp AFF 的 FlexPod Express 的连接要求包括：

- NetApp AFF 存储控制器必须直接连接到 Cisco Nexus 交换机，但 Cisco UCS 管理的配置除外，在该配置中，存储控制器连接到网络结构。互连。
- 不能在核心 FlexPod 组件之间实时放置任何其他设备。
- 要将 Cisco Nexus 3000/9000 系列交换机连接到 NetApp 存储控制器，需要使用虚拟端口通道（Virtual Port Channel， vPC）。
- 虽然不需要，但建议在整个环境中启用巨型帧支持。

其他要求

FlexPod Express 的其他要求包括：

- 所有设备都需要有效的支持合同，包括：
  - Cisco 设备的 SMARTnet 支持
  - 对 NetApp 设备的 SupportEdge Advisor 或 SupportEdge Premium 支持
- 必须在中列出并支持所有软件组件 "NetApp IMT"。
- 必须列出所有 NetApp 硬件组件并在上受支持 "NetApp Hardware Universe"。
- 必须列出所有 Cisco 硬件组件并在上受支持 "Cisco HCL"。

可选功能

本节介绍 FlexPod 快速的可选功能。

iSCSI 启动选项

FlexPod 快速架构使用 iSCSI 启动。iSCSI 启动选项的最低要求包括：

- 在 NetApp 存储控制器上激活的 iSCSI 许可证 / 功能

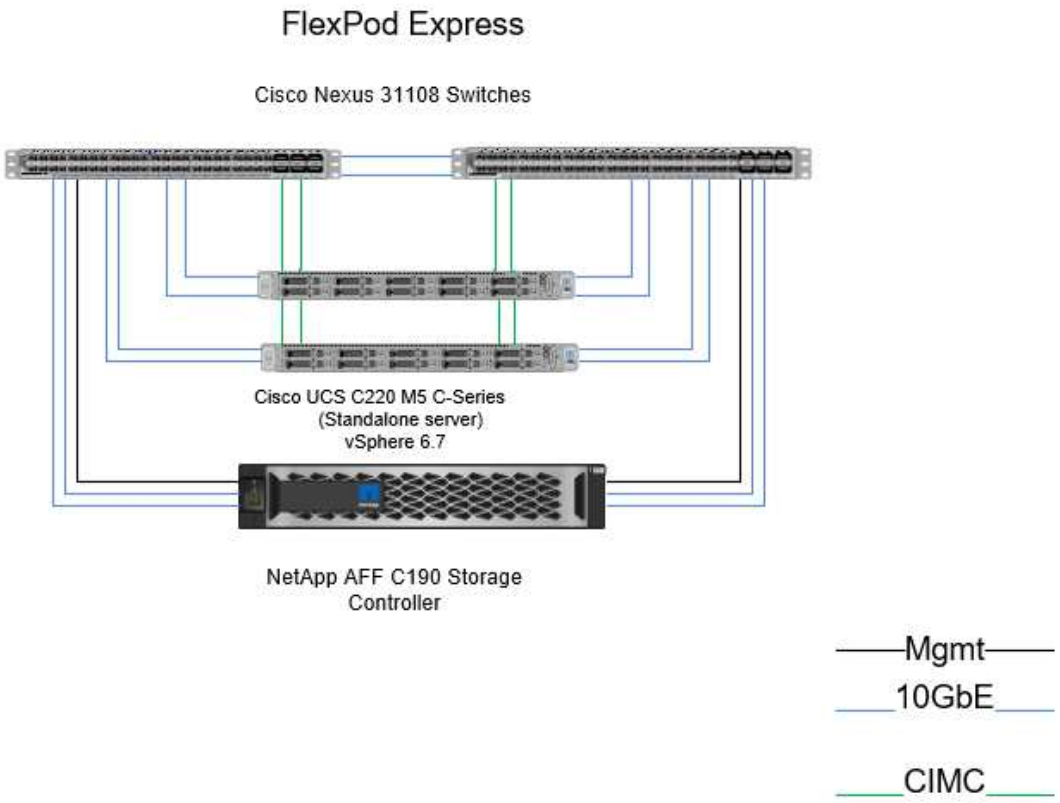
- NetApp 存储控制器 HA 对中每个节点上的一个双端口 10Gbps 以太网适配器
- Cisco UCS 服务器中支持 iSCSI 启动的适配器

配置选项

本节提供了有关 FlexPod 快速架构所需并经过验证的配置的详细信息。

采用 Cisco UCS C 系列和 AFF C190 系列的 FlexPod Express

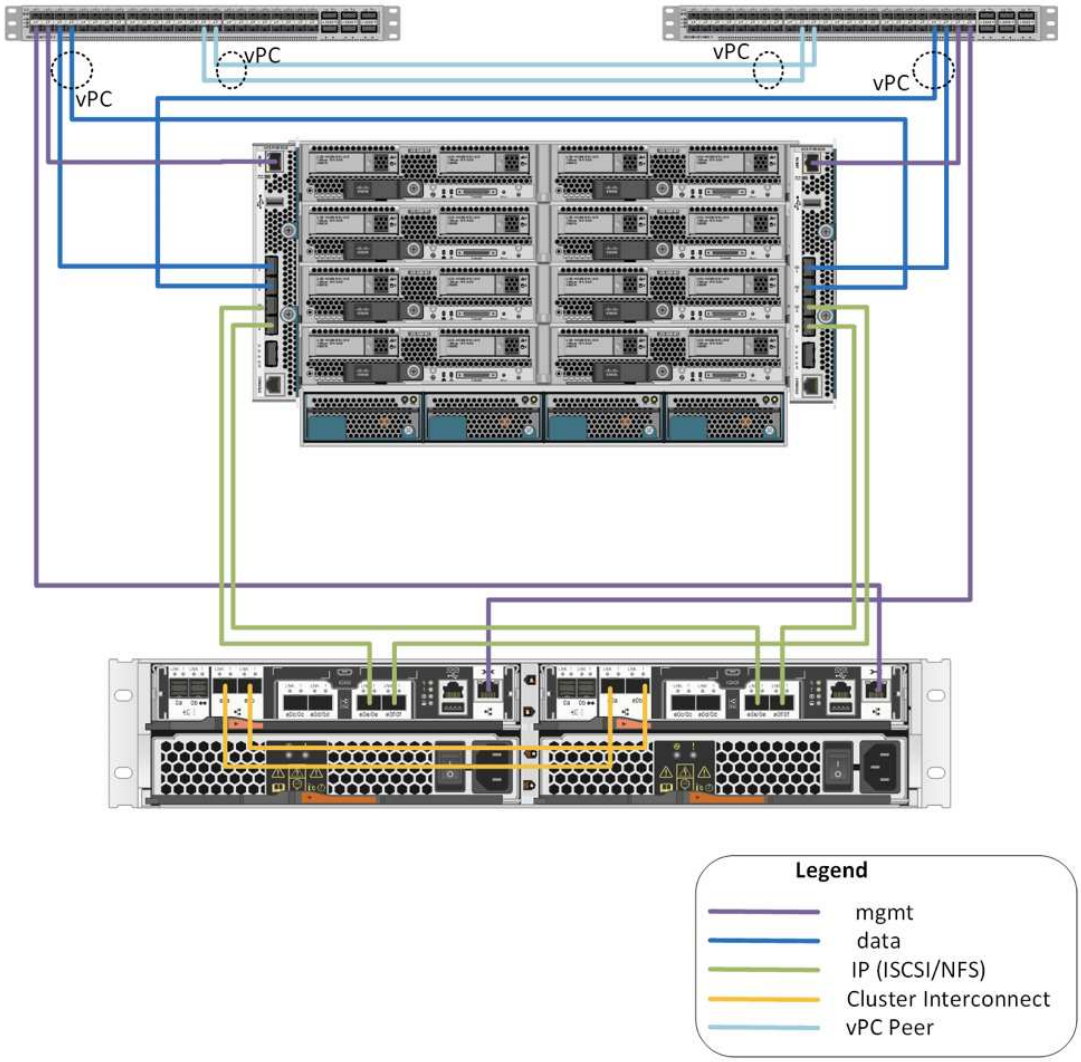
下图显示了采用 Cisco UCS C 系列和 AFF C190 系列解决方案的 FlexPod Express 。此解决方案支持两个 10GbE 上行链路。



有关此配置的详细信息，请参见《适用于 VMware vSphere 6.7 和 NetApp AFF C190 NVA 的 FlexPod 快速部署指南》（正在进行中）。

采用 Cisco UCS Mini ， AFF A220 和 FAS 27502720 的 FlexPod Express

下图显示了采用 Cisco UCS 管理的配置的 FlexPod Express 。



有关此配置的详细信息，请参见 "采用 VMware vSphere 6.7U1 的 FlexPod Express 以及采用基于 IP 的直连存储的 NetApp AFF A220"。

Cisco 组件

Cisco 为 FlexPod 快速设计和架构做出了重大贡献；它为解决方案的计算和网络层做出了贡献。本节介绍可用于 FlexPod Express 的 Cisco UCS 和 Cisco Nexus 组件。

Cisco UCS B 系列刀片式服务器选项

Cisco UCS Mini 平台目前支持的 Cisco UCS B 系列刀片式服务器为 B200 M5 和 B420 M4 。下表列出了 Cisco UCS Mini 平台支持的其他刀片式服务器。

Cisco UCS B 系列服务器	部件号	技术规格
Cisco UCS B200 M5	UCSB-B200-M5	https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-b200-m5-blade-server/model.html

Cisco UCS B 系列服务器	部件号	技术规格
Cisco UCS B200 M4	UCSB-B200-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b200m4-specsheet.pdf
Cisco UCS B420 M4	UCSB-B420-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b420m4-spec-sheet.pdf

Cisco UCS C 系列机架式服务器选项

Cisco UCS C 系列刀片式服务器提供单机架和双机架单元（RU）两种型号，并提供各种 CPU，内存和 I/O 选项。下表中列出的部件号适用于基础服务器，不包括 CPU，内存，磁盘驱动器， PCIe 卡或 Cisco FEX 。FlexPod 提供并支持多个配置选项。

Cisco UCS C 系列机架式服务器	部件号	技术规格
Cisco UCS C220 M4	UCSC-C220-M4S	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m4-sff-spec-sheet.pdf
Cisco UCS C240 M4	UCSC-C240-M4S	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c240m4-sff-spec-sheet.pdf
Cisco UCS C460 M4	UCSC-C460-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c460m4_specsheet.pdf

Cisco Nexus 交换机

所有 FlexPod 快速架构都需要冗余交换机。

采用 NetApp AFF 或 FAS 架构的 FlexPod Express 采用 Cisco Nexus 31108 交换机构建。采用 Cisco UCS Mini（Cisco UCS 管理）架构的 FlexPod Express 可通过使用 Cisco Nexus 3524 交换机进行验证。也可以使用标准交换机部署此配置。

采用 E 系列的 FlexPod Express 可以使用标准交换机进行部署。

下表列出了 Cisco Nexus 系列机箱的部件号，不包括其他 SFP 或附加模块。

Cisco Nexus 系列交换机	部件号	技术规格
Cisco Nexus 3048	N3K-C3048TP-1GE	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-3000-series-switches/data_sheet_c78-685363.html

Cisco Nexus 系列交换机	部件号	技术规格
Cisco Nexus 31108	N3K-C31108PC-V	http://www.cisco.com/c/en/us/products/switches/nexus-31108pc-v-switch/index.html
Cisco Nexus 9396	N9K-C9396PX	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-729405.html
Cisco Nexus 3172	N3K-C3172	https://www.cisco.com/c/en/us/products/collateral/switches/nexus-3000-series-switches/data_sheet_c78-729483.html

Cisco 支持许可选项

FlexPod 快速架构中的所有 Cisco 设备都需要有效的 SMARTnet 支持合同。

所需的许可证以及这些许可证的部件号应由销售代表进行验证，因为它们可能因不同产品而异。

下表列出了 Cisco 支持许可选项。

Cisco 支持许可	许可证指南
SMARTNET 24X7X4	http://www.cisco.com/web/services/portfolio/product-technical-support/smartnet/index.html

NetApp 组件

NetApp 存储控制器在 FlexPod 快速架构中为启动和应用程序数据存储提供了存储基础。本节列出了 FlexPod 快速架构中的不同 NetApp 选项。

NetApp 存储控制器选项

NetApp FAS

在 FlexPod 快速架构中，需要使用冗余 AFF C190 ， AFF A220 或 FAS2750 系列控制器。这些控制器运行 ONTAP 软件。订购存储控制器时，可以在这些控制器上预加载首选软件版本。对于 ONTAP ，可以使用一对集群互连交换机部署集群，也可以采用无交换机集群配置部署集群。

下表列出的部件号适用于空控制器。根据选定的存储平台，可以使用不同的选项和配置。有关这些附加组件的详细信息，请咨询您的销售代表。

存储控制器	**FAS** 部件号	技术规格
FAS2750	根据所选的各个选项	https://www.netapp.com/us/products/storage-systems/hybrid-flash-array/fas2700.aspx

存储控制器	**FAS** 部件号	技术规格
FAS2720	根据所选的各个选项	https://www.netapp.com/us/products/storage-systems/hybrid-flash-array/fas2700.aspx
AFF C190	根据所选的各个选项	https://www.netapp.com/us/products/entry-level-aff.aspx
AFF A220	根据所选的各个选项	https://www.netapp.com/us/documentation/all-flash-fas.aspx
FAS2620	根据所选的各个选项	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx
FAS2650	根据所选的各个选项	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx

E-Series 存储

在 FlexPod 快速架构中，需要一对 NetApp E2800 系列控制器。这些控制器运行 SANtricity 操作系统。

下表列出的部件号适用于空控制器。根据选定的存储平台，可以使用不同的选项和配置。有关这些附加组件的详细信息，请咨询您的销售代表。

存储控制器	部件号	技术规格
E2800	根据所选的各个选项	http://www.netapp.com/us/products/storage-systems/e2800/e2800-tech-specs.aspx

NetApp 以太网扩展模块

NetApp FAS

下表列出了 NetApp FAS10GbE 适配器选项。

组件	部件号	技术规格
NetApp X1117A	X1117A-R6	https://library.netapp.com/ecm/ecm_download_file/ECMM1280307

> FAS2500 和 2600 系列存储系统具有板载 10GbE 端口。
>
> NetApp X1117A 适配器适用于 FAS8020 存储系统。

E-Series 存储

下表列出了 E 系列 10GbE 适配器选项。

组件	部件号
10GbE iSCSI/16 Gb FC 4 端口	X-56025-00-0E-C
10GbE iSCSI/16 Gb FC 2 端口	X-56024-00-0E-C

> E2824 系列存储系统具有板载 10GbE 端口。
>
> 10GbE iSCSI/16 Gb FC 4 端口主机接口卡（HIC）可用于提高端口密度。

板载端口和 HIC 可用作 iSCSI 适配器或 FC 适配器，具体取决于在 SANtricity 操作系统中激活的功能。

有关支持的适配器选项的详细信息，请参见的 " 适配器 " 一节 "NetApp Hardware Universe"。

NetApp 磁盘架和磁盘

NetApp FAS

存储控制器至少需要一个 NetApp 磁盘架。选定的 NetApp 磁盘架类型决定了该磁盘架中可用的驱动器类型。

FAS2700 和 FAS2600 系列控制器作为一种配置提供，其中包括双存储控制器以及位于同一机箱中的磁盘。此配置随 SATA 或 SAS 驱动器提供；因此，除非性能或容量要求要求需要更多磁盘轴，否则不需要额外的外部磁盘架。

> 所有磁盘架部件号均适用于具有两个 AC PSU 的空磁盘架。有关其他部件号，请咨询您的销售代表。
>
> 磁盘驱动器部件号因要购买的磁盘的大小和外形规格而异。有关其他部件号，请咨询您的销售代表。

下表列出了 NetApp 磁盘架选项以及每个磁盘架类型支持的驱动器，这些选项可在 NetApp Hardware Universe 上找到。单击 Hardware Universe 链接，选择要使用的 ONTAP 版本，然后选择磁盘架类型。在磁盘架映像下，单击支持的驱动器以查看特定版本的 ONTAP 和磁盘架支持的驱动器。

磁盘架	部件号	技术规格
DS212C	DS212C-0-12	"磁盘架和存储介质技术规格 NetApp Hardware Universe 上支持的驱动器"
DS224C	DS224C-0-24	"磁盘架和存储介质技术规格 NetApp Hardware Universe 上支持的驱动器"
DS460C	DS460C-0-60	"磁盘架和存储介质技术规格 NetApp Hardware Universe 上支持的驱动器"
DS2246	X559A-R6	"磁盘架和存储介质技术规格 NetApp Hardware Universe 上支持的驱动器"
DS4246	X24M-R6	"磁盘架和存储介质技术规格 NetApp Hardware Universe 上支持的驱动器"

磁盘架	部件号	技术规格
DS4486	DS4486-144TB-R5-C	"磁盘架和存储介质技术规格 NetApp Hardware Universe 上支持的驱动器"

E-Series 存储

对于不在机箱中容纳任何驱动器的存储控制器，至少需要一个 NetApp 磁盘架。选定的 NetApp 磁盘架类型决定了该磁盘架中可用的驱动器类型。

E2800 系列控制器作为一种配置提供，其中包括双存储控制器以及位于受支持磁盘架中的磁盘。此配置随 SSD 或 SAS 驱动器一起提供。

> 磁盘驱动器部件号因要购买的磁盘的大小和外形规格而异。有关其他部件号，请咨询您的销售代表。

下表列出了 NetApp 磁盘架选项以及每个磁盘架类型支持的驱动器，这些选项可在 NetApp Hardware Universe 上找到。单击 Hardware Universe 链接，选择要使用的 ONTAP 版本，然后选择磁盘架类型。在磁盘架映像下，单击支持的驱动器以查看特定版本的 ONTAP 和磁盘架支持的驱动器。

磁盘架	部件号	技术规格
DE460C	E-X5730A-DM-0E-C	"磁盘架技术规格 NetApp Hardware Universe 上支持的驱动器"
DE224C	E-X5721A-DM-0E-C	"磁盘架技术规格 NetApp Hardware Universe 上支持的驱动器"
DE212C	E-X5723A-DM-0E-C	"磁盘架技术规格 NetApp Hardware Universe 上支持的驱动器"

NetApp 软件许可选项

NetApp FAS

下表列出了 NetApp FAS 软件许可选项。

NetApp 软件许可	部件号	技术规格
基本集群许可证	有关许可的详细信息，请咨询 NetApp 销售团队。	

E-Series 存储

下表列出了 E 系列软件许可选项。

NetApp 软件许可	部件号	技术规格
标准功能	有关许可的详细信息，请咨询 NetApp 销售团队。	
高级功能		

NetApp 支持许可选项

SupportEdge Premium 许可证是必需的，这些许可证的部件号因 FlexPod 快速设计中选择的选项而异。

NetApp FAS

下表列出了 NetApp FAS 的 NetApp 支持许可选项。

NetApp 支持许可	部件号	技术规格
SupportEdge 高级版 4 小时现场服务；月数： 36	CS-O2-4 小时	https://www.netapp.com/pdf.html?item=/media/19784-ds-3873.pdf

E-Series 存储

下表列出了适用于 E 系列存储的 NetApp 支持许可选项。

NetApp 支持许可	部件号	技术规格
硬件支持高级版 4 小时现场支持；月数： 36	SVC — O2-4M-E	https://www.netapp.com/pdf.html?item=/media/19784-ds-3873.pdf
软件支持	SW-SSP-O2-4W-E	
初始安装	SVC — INST-O2-4M-E	

电源和布线要求

本节介绍 FlexPod 快速设计的电源和最低布线要求。

电源要求

电源要求基于美国并假定使用交流电源。其他国家或地区的电源要求可能有所不同。此外，大多数组件还提供直流（ DC ）电源选项。有关所需最大电源的其他数据以及其他详细的电源信息，请参阅每个硬件组件的详细技术规格。

有关 Cisco UCS 电源的详细数据，请参见 "Cisco UCS 电源计算器"。

下表列出了每个设备所需的电源端口。

Cisco Nexus 交换机	所需的电源线
Cisco Nexus 3048	每个 Cisco Nexus 3000 系列交换机需要 2 根 C13/C14 电源线
Cisco Nexus 3524	每个 Cisco Nexus 3000 系列交换机需要 2 根 C13/C14 电源线
Cisco Nexus 9396	每个 Cisco Nexus 9000 系列交换机需要 2 根 C13/C14 电源线

Cisco UCS 机箱	所需的电源线
Cisco UCS 5108	每个 Cisco UCS 机箱 2 CA-US515P-C19-US/CAB-US520-C19-US

Cisco UCS B 系列服务器	所需的电源线
Cisco UCS B200 M4	不适用；刀片式服务器由机箱供电
Cisco UCS B420 M4	不适用；刀片式服务器由机箱供电
Cisco UCS B200 M5	不适用；刀片式服务器由机箱供电
Cisco UCS B480 M5	不适用；刀片式服务器由机箱供电

Cisco UCS C 系列服务器	所需的电源端口
Cisco UCS C220 M4	每个 Cisco UCS 服务器使用 2 根 C13/C14 电源线
Cisco UCS C240 M4	
Cisco UCS C460 M4 Cisco UCS C220 M5 Cisco UCS C240 M5 Cisco UCS C480 M5	

NetApp FAS 控制器	所需电源端口（每个 **HA** 对）
FAS2554	2 个 C13/C14
FAS2552	2 个 C13/C14
FAS2520	2 个 C13/C14
FAS8020	2 个 C13/C14

E 系列控制器	所需电源端口（每个 **HA** 对）
E2824	2 个 C14/C20

NetApp FAS 磁盘架	所需的电源端口
DS212C	2 个 C13/C14
DS224C	2 个 C13/C14
DS460C	2 个 C13/C14
DS2246	2 个 C13/C14
DS4246	4 个 C13/C14

E 系列磁盘架	所需的电源端口
DE460C	2 个 C14/C20
DE224C	2 个 C14/C20
DE212C	2 个 C14/C20

最低缆线要求

本节介绍 FlexPod 快速设计的最低缆线要求。大多数 FlexPod 实施都需要额外的缆线，但数量因部署规模和范围而异。

下表列出了每个设备所需的最小缆线数量。

Cisco Nexus 3000 系列交换机	所需的缆线
Cisco Nexus 31108	每个交换机至少需要两根 10GbE 光纤或双轴电缆
Cisco Nexus 3172PQ	
Cisco Nexus 3048	
Cisco Nexus 3524	
Cisco Nexus 9396	
DS212C	
DS2246	SAS 缆线数量取决于磁盘架的特定配置
DS460C	
DS224C	
DS4246	
E2800	• 每个控制器至少需要一根千兆以太网（ 1GbE ）缆线进行管理 • 每个控制器至少需要两根 10GbE 缆线（对于 iSCSI ），或者两根 FC 缆线符合速度要求
DE460C	每个磁盘架 2 根迷你 SAS HD 缆线
DE224C	每个磁盘架 2 根迷你 SAS HD 缆线
DE212C	每个磁盘架 2 根迷你 SAS HD 缆线

技术规格和参考

本节介绍每个 FlexPod 快速组件的其他重要技术规格。

Cisco UCS B 系列刀片式服务器

下表列出了 Cisco UCS B 系列刀片式服务器选项。

组件	**Cisco UCS B200 M4**	**Cisco UCS B420 M4**	**Cisco UCS B200 M5**
处理器支持	Intel Xeon E5-2600	Intel Xeon E5-4600	Intel Xeon 可扩展处理器
最大内存容量	24 个 DIMM ，最大容量为 768 GB	48 个 DIMM ，最大 3 TB	24 个 DIMM ，最大 3072 GB

组件	Cisco UCS B200 M4	Cisco UCS B420 M4	Cisco UCS B200 M5
内存大小和速度	32 GB DDR4； 2133 MHz	64 GB DDR4； 2400MHz	16 GB， 32 GB， 64 GB 和 128 GB DDR4； 266 Mhz
SAN 启动支持	是的。	是的。	是的。
夹层 I/O 适配器插槽	2.	3.	2 个，正面和背面，包括 GPU 支持
I/O 最大吞吐量	80 Gbps	160 Gbps	80 Gbps

Cisco UCS C 系列机架式服务器

下表列出了 Cisco UCS C 系列机架式服务器选项。

组件	Cisco UCS C220 M4	Cisco UCS C240 M4	Cisco UCS C460 M4	Cisco UCS C220 M5
处理器支持	1 或 2 个 Intel E5-2600 系列	1 或 2 个 Intel Xeon E5-2600 系列	2 或 4 个 Intel Xeon E7-4800/8800 系列	Intel Xeon 可扩展处理器（1 或 2）
最大内存容量	1.5 GB	1.5 TB	6 TB	3072 GB
PCIe 插槽	2.	6.	10	2.
外形规格	1 RU	2 RU	4 RU	1 RU

下表列出了 Cisco UCS C 系列机架式服务器选项的产品规格。

组件	Cisco UCS 产品规格
Cisco UCS C220 M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m4-sff-spec-sheet.pdf
Cisco UCS C240 M4	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c240-m4-rack-server/datasheet-c78-732455.html
Cisco UCS C460 M4	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c460-m4-rack-server/datasheet-c78-730907.html
Cisco UCS C220 M5	https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m5-sff-specsheet.pdf

Cisco Nexus 3000 系列交换机

下表列出了 Cisco Nexus 3000 系列交换机选项。

组件	Cisco Nexus 3048	Cisco Nexus 3524	Cisco Nexus 31108	Cisco Nexus 3172PQ
外形规格	1 RU	1 RU	1 RU	1 RU

组件	**Cisco Nexus 3048**	**Cisco Nexus 3524**	**Cisco Nexus 31108**	**Cisco Nexus 3172PQ**
最大 1 Gbps 端口数	48	24	48 （10/40/100 Gbps）	72 个 1/10GbE 端口，或 48 个 1/10GbE 加上 6 个 40GbE 端口
转发速率	132 Mbps	360 Mbps	1.2 个 pps	1 个端口
巨型帧支持	是的。	是的。	是的。	是的。

下表列出了 Cisco Nexus 3000 系列交换机选项的产品规格。

组件	**Cisco Nexus** 产品规格
Cisco Nexus 31108	http://www.cisco.com/c/en/us/products/switches/nexus-31108pc-v-switch/index.html
Cisco Nexus 3172PQ	https://www.cisco.com/c/en/us/products/switches/nexus-3172pq-switch/index.html
Cisco Nexus 3048	https://www.cisco.com/c/en/us/products/switches/nexus-3048-switch/index.html
Cisco Nexus 3172PQ-XL	https://www.cisco.com/c/en/us/products/switches/nexus-3172pq-switch/index.html
Cisco Nexus 3548 XL	https://www.cisco.com/c/en/us/products/switches/nexus-3548-x-switch/index.html
Cisco Nexus 3524 XL	https://www.cisco.com/c/en/us/products/switches/nexus-3524-x-switch/index.html
Cisco Nexus 3548	https://www.cisco.com/c/en/us/products/switches/nexus-3548-x-switch/index.html
Cisco Nexus 3524	https://www.cisco.com/c/en/us/products/switches/nexus-3524-x-switch/index.html

下表列出了 Cisco Nexus 9000 系列交换机选项。

组件	**Cisco Nexus 9396**	**Cisco Nexus 9372**
外形规格	2 RU	1 RU
最大端口数	60	54
10 Gbps SFP+ 上行链路端口	48	48

下表列出了 Cisco Nexus 9000 系列交换机选项数据表。

组件	**Cisco Nexus** 产品规格
Cisco Nexus 9396	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736967.html

组件	**Cisco Nexus** 产品规格
Cisco Nexus 9372	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736967.html
Nexus 9396X	https://www.cisco.com/c/en/us/products/switches/nexus-9396px-switch/index.html?dtid=osscdc000283

NetApp FAS 存储控制器

下表列出了当前的 NetApp FAS 存储控制器选项。

当前组件	**FAS2620**	**FAS2650**
Configuration	一个 2U 机箱中有 2 个控制器	一个 4U 机箱中有 2 个控制器
最大原始容量	1440 TB	1243 TB
内部驱动器	12	24
最大驱动器数（内部和外部）	144.	144.
最大卷大小	100 TB	
最大聚合大小	4 TB	
LUN 的最大数量	每个控制器 2， 048 个	
支持的存储网络	iSCSI， FC， FCoE， NFS 和 CIFS	
NetApp FlexVol 卷的最大数量	每个控制器 1， 000 个。	
NetApp Snapshot 副本的最大数量	每个控制器 255， 000 个	
最大程度地提高 NetApp Flash Pool 智能数据缓存能力	24 TB	

有关 FAS 存储控制器选项的详细信息，请参见 "FAS 型号" 部分 Hardware Universe 。对于 AFF ，请参见 "AFF 型号" 部分。

下表列出了 FAS8020 控制器系统的特征。

组件	**FAS8020**
Configuration	一个 3U 机箱中有 2 个控制器
最大原始容量	2880 TB
最大驱动器数	480
最大卷大小	70 TB
最大聚合大小	324TB
LUN 的最大数量	每个控制器 8， 192 个
支持的存储网络	iSCSI， FC， NFS 和 CIFS
FlexVol 卷的最大数量	每个控制器 1， 000 个

组件	**FAS8020**
最大 Snapshot 副本数	每个控制器 255， 000 个
最大程度地提高 NetApp Flash Cache 智能数据缓存能力	3 TB
最大 Flash Pool 数据缓存	24 TB

下表列出了 NetApp 存储控制器的产品规格。

组件	存储控制器产品规格
FAS2600 系列	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx
FAS2500 系列	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS8000 系列	http://www.netapp.com/us/products/storage-systems/fas8000/fas8000-tech-specs.aspx

NetApp FAS 以太网适配器

下表列出了 NetApp FAS 10GbE 适配器。

组件	**X1117A-R6**
端口数	2.
适配器类型	采用光纤的 SFP+

FAS8000 系列控制器支持 X1117A-R6 SFP+ 适配器。

FAS2600 和 FAS2500 系列存储系统具有板载 10GbE 端口。有关详细信息，请参见 "NetApp 10GbE 适配器产品规格"。

有关基于 AFF 或 FAS 型号的适配器详细信息，请参见 "适配器部分" 在 Hardware Universe 中。

NetApp FAS 磁盘架

下表列出了当前的 NetApp FAS 磁盘架选项。

组件	**DS460C**	**DS224C**	**DS212C**	**DS2246**	**DS4246**
外形规格	4 RU	2 RU	2 RU	2 RU	4 RU
每个机箱的驱动器数	60	24	12	24	24
驱动器外形规格	3.5 英寸大型	2.5 英寸小型计算机	3.5 英寸大型	2.5 英寸小型计算机	3.5 英寸大型
磁盘架 I/O 模块	双 IOM12 模块	双 IOM12 模块	双 IOM12 模块	双 IOM6 模块	双 IOM6 模块

有关详细信息，请参见 NetApp 磁盘架产品规格。

有关磁盘架的详细信息，请参见 NetApp Hardware Universe "磁盘架部分"。

NetApp FAS 磁盘驱动器

NetApp 磁盘的技术规格包括外形规格大小，磁盘容量，磁盘 RPM ，支持控制器和 Data ONTAP 版本要求，位于上的驱动器部分 "NetApp Hardware Universe"。

E 系列存储控制器

下表列出了当前 E 系列存储控制器选项。

当前组件	**E2812**	**E2824**	**E2860**
Configuration	一个 2U 机箱中有 2 个控制器	一个 2U 机箱中有 2 个控制器	一个 4U 机箱中有 2 个控制器
最大原始容量	1800 TB	1756.8 TB	1800 TB
内部驱动器	12	24	60
最大驱动器数（内部和外部）	180		
最大 SSD 数	120		
磁盘池卷的最大卷大小	1024 TB		
最大磁盘池数	20		
支持的存储网络	iSCSI 和 FC		
最大卷数	512		

下表列出了当前 E 系列存储控制器的产品规格。

组件	存储控制器产品规格
E2800	http://www.netapp.com/us/media/ds-3805.pdf

E 系列适配器

下表列出了 E 系列适配器。

组件	**X-56023-0E-C**	**X-56025-00-0E-C**	**X-56027-00-0E-C**	**X-56024-00-0E-C**	**X-56026-00-0E-C**
端口数	2.	4.	4.	2.	2.
适配器类型	10 Gb Base-T	16 G FC 和 10GbE iSCSI	（SAS）。	16 G FC 和 10GbE iSCSI	（SAS）。

E 系列磁盘架

下表列出了 E 系列磁盘架选项。

组件	DE212C	DE224C	DE460C
外形规格	2 RU	2 RU	4 RU
每个机箱的驱动器数	12	24	60
驱动器外形规格	2.5 英寸小型 3.5 英寸	2.5 英寸	2.5 英寸小型 3.5 英寸
磁盘架 I/O 模块	IOM12	IOM12	IOM12

E 系列磁盘驱动器

NetApp 磁盘驱动器的技术规格包括外形规格大小，磁盘容量，磁盘 RPM ，支持控制器和 SANtricity 版本要求，位于上的驱动器部分 "NetApp Hardware Universe"。

以前的架构和设备

FlexPod 是一种灵活的解决方案，允许客户使用当前由 Cisco 和 NetApp 销售的现有设备和新设备。有时， Cisco 和 NetApp 的某些型号设备会被指定为寿命终结。

即使不再提供这些型号的设备，在销售结束日期之前购买其中一种型号的客户也可以在 FlexPod 配置中使用该设备。

此外，还会定期更新 FlexPod Express 架构，以便将 Cisco 和 NetApp 的最新硬件和软件引入 FlexPod Express 解决方案。本节列出了以前的 FlexPod 快速架构及其使用的硬件。

以前的 FlexPod 快速架构

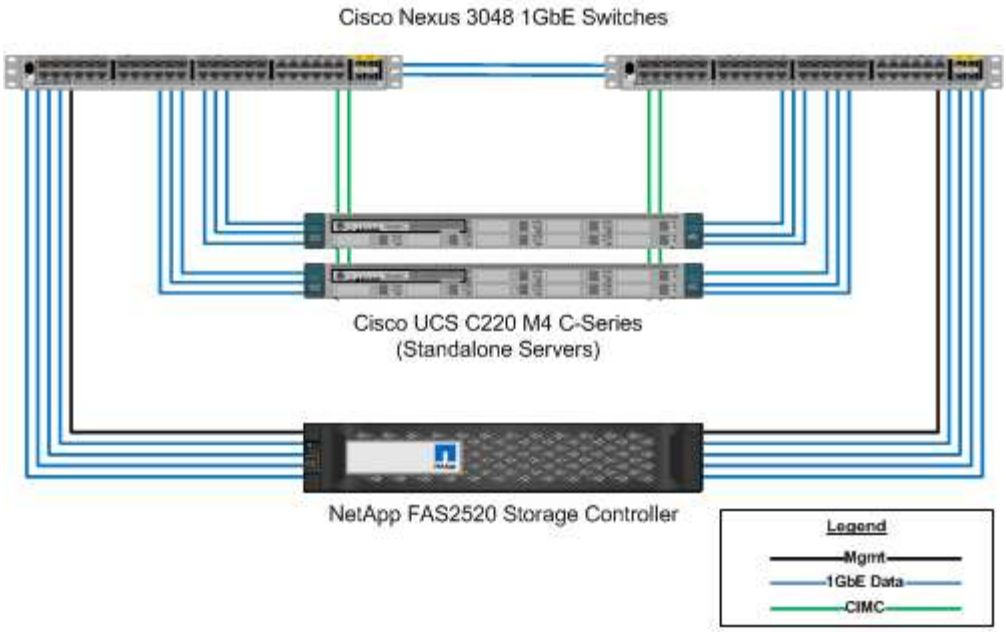
本节介绍以前的 FlexPod 快速架构。

FlexPod Express 中小型配置

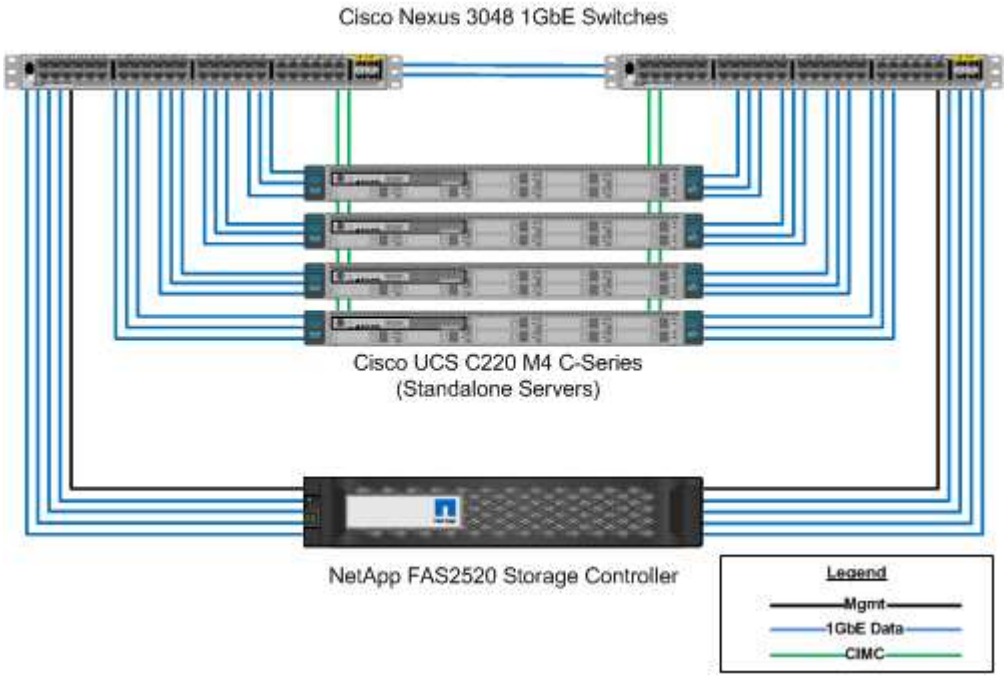
FlexPod Express 中小型配置包括以下组件：

- 一个冗余配置中的两个 Cisco Nexus 3048 交换机
- 至少两个 Cisco UCS C 系列机架式服务器
- 一个 HA 对配置中的两个 FAS2200 或 FAS2500 系列控制器

下图显示了 FlexPod 快速小型配置。



下图显示了 FlexPod 快速介质配置。



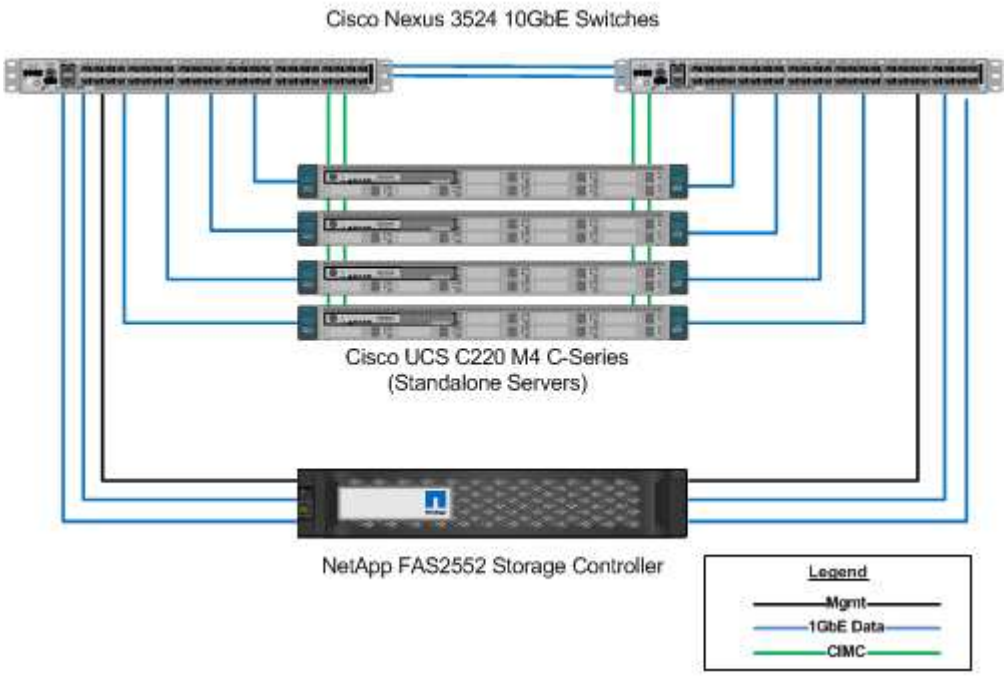
FlexPod Express 大型配置

FlexPod Express 大型配置包括以下组件：

- 采用冗余配置的两个 Cisco Nexus 3500 系列或 Cisco Nexus 9300 系列交换机
- 至少两个 Cisco UCS C 系列机架式服务器
- 一个 HA 对配置中的两个 FAS2552 ， FAS2554 或 FAS8020 控制器（每个控制器需要两个 10GbE 端口）

- 一个具有任何受支持磁盘类型的 NetApp 磁盘架（使用 FAS8020 时）

下图显示了 FlexPod 快速大型配置。



经过 **FlexPod Express** 验证的早期架构

仍支持先前经过 FlexPod Express 验证的架构。架构和部署文档包括：

- "采用 Cisco UCS C 系列和 NetApp FAS2500 系列的 FlexPod Express"
- "采用 VMware vSphere 6.0 的 FlexPod Express： 小型和中型配置"
- "采用 VMware vSphere 6.0 的 FlexPod Express： 大型配置"
- "采用 Microsoft Windows Server 2012 R2 Hyper-V 的 FlexPod Express： 小型和中型配置"
- "采用 Microsoft Windows Server 2012 R2 Hyper-V 的 FlexPod Express： 大型配置"

以前的硬件

下表列出了以前的 FlexPod 快速架构中使用的硬件。

先前架构中使用的硬件	技术规格（如果有）
Cisco UCS C220 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c220-m3-rack-server/data_sheet_c78-700626.html
Cisco UCS C24 M3	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/data_sheet_c78-706103.html
Cisco UCS C22 M3	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/data_sheet_c78-706101.html

先前架构中使用的硬件	技术规格（如果有）
Cisco UCS C240 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c240-m3-rack-server/data_sheet_c78-700629.html
Cisco UCS C260 M2	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/c260m2_specsheet.pdf
Cisco UCS C420 M3	http://www.cisco.com/en/US/products/ps12770/index.html
Cisco UCS C460 M2	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/ps11587/spec_sheet_c17-662220.pdf
Cisco UCS B200 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b200-m3-blade-server/data_sheet_c78-700625.html
Cisco UCS B420 M3	不适用
Cisco UCS B22 M3	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b22m3_specsheet.pdf
Cisco Nexus 3524	http://www.cisco.com/c/en/us/products/switches/nexus-3524-switch/index.html
FAS2240	
FAS2220	http://www.netapp.com/us/products/storage-systems/fas2200/fas2200-tech-specs.aspx
DS4243	不适用

旧设备

下表列出了 NetApp 原有存储控制器选项。

存储控制器	**FAS** 部件号	技术规格
FAS2520	根据所选的各个选项	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2552	根据所选的各个选项	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2554	根据所选的各个选项	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS8020	根据所选的各个选项	http://www.netapp.com/us/products/storage-systems/fas8000/fas8000-tech-specs.aspx

下表列出了适用于 NetApp FAS 的 NetApp 原有磁盘架选项。

磁盘架	部件号	技术规格
DE1600	E-X5682A-DM-0E-R6-C	"磁盘架技术规格 NetApp Hardware Universe 上支持的驱动器"
DE5600	E-X4041A-12-R6	"磁盘架技术规格 NetApp Hardware Universe 上支持的驱动器"
DE6600	X-48564-00-R6	"磁盘架技术规格 NetApp Hardware Universe 上支持的驱动器"

NetApp 原有 FAS 控制器

下表列出了原有的 NetApp FAS 控制器选项。

当前组件	**FAS2554**	**FAS2552**	**FAS2520**
Configuration	一个 4U 机箱中有 2 个控制器	一个 2U 机箱中有 2 个控制器	一个 2U 机箱中有 2 个控制器
最大原始容量	576 TB	509 TB	336 TB
内部驱动器	24	24	12
最大驱动器数（内部和外部）	144.	144.	84.
最大卷大小	60 TB		
最大聚合大小	120 TB		
LUN 的最大数量	每个控制器 2， 048 个		
支持的存储网络	iSCSI， FC， FCoE， NFS 和 CIFS		iSCSI， NFS 和 CIFS
NetApp FlexVol 卷的最大数量	每个控制器 1， 000 个		
NetApp Snapshot 副本的最大数量	每个控制器 255， 000 个		

有关更多 NetApp FAS 型号，请参见 "FAS 型号部分" 在 Hardware Universe 中。

追加信息

要了解有关本文档所述信息的更多信息，请参见以下文档和网站：

- AFF 和 FAS 系统文档中心

  "https://docs.netapp.com/platstor/index.jsp"

- AFF 文档资源页面

  "https://www.netapp.com/us/documentation/all-flash-fas.aspx"

- FAS 存储系统文档资源页面

"https://www.netapp.com/us/documentation/fas-storage-systems.aspx"

- FlexPod

  "https://flexpod.com/"

- NetApp 文档

  "https://docs.netapp.com"

FlexPod 数据中心技术规格

TR-4036： FlexPod 数据中心技术规格

Arvind Ramakrishnan 和 NetApp 公司 Jyh-shing Chen

FlexPod 平台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（ Cisco UCS ）， Cisco Nexus 系列交换机和 NetApp 存储控制器（ AFF ， ASA 或 FAS 系统）构建。

FlexPod 是一个适合运行各种虚拟化虚拟机管理程序以及裸机操作系统和企业工作负载的平台。FlexPod 不仅提供了基线配置，而且还可以灵活地调整规模并进行优化，以满足多种不同的使用情形和要求。

> 在订购完整的 FlexPod 配置之前，请参见 "FlexPod 融合基础架构" 请访问 netapp.com 上的第页，了解这些技术规格的最新版本。

"接下来： FlexPod 平台。"

FlexPod 平台

FlexPod 平台有两种：

- * FlexPod Datacenter 。 * 此平台是一个可大规模扩展的虚拟数据中心基础架构，适合工作负载企业级应用程序，虚拟化，虚拟桌面基础架构 (VDI) 以及私有云和混合云工作负载公有。
- * FlexPod Express* 。此平台是一个紧凑型融合基础架构，面向远程办公室和边缘用例。FlexPod Express 具有自己的规格，这些规格在中进行了说明 "FlexPod 快速技术规格。"

本文档提供了 FlexPod 数据中心平台的技术规格。

FlexPod 规则

FlexPod 设计可提供一个灵活的基础架构，其中包含许多不同的组件和软件版本。

使用规则集作为构建或整合有效 FlexPod 配置的指南。本文档中列出的数字和规则是 FlexPod 配置的最低要求。可以根据不同环境和使用情形的需要在所含产品系列中扩展这些功能。

支持的 **FlexPod** 配置与经验证的 配置

FlexPod 架构由本文档中所述的一组规则定义。硬件组件和软件配置必须受支持 "Cisco UCS 硬件和软件兼容性列表" 和 "NetApp 互操作性表工具（IMT）"。

每个 Cisco 验证设计（Cisco Validated Design， CVD）或 NetApp 验证架构（NetApp Verified Architecture， NVA）都是一种可能的 FlexPod 配置。Cisco 和 NetApp 会记录这些配置组合，并通过广泛的端到端测试对其进行验证。如果与这些配置不同的 FlexPod 部署符合本文档中的准则，并且所有组件均在 Cisco UCS 硬件和软件兼容性列表以及 NetApp 中列为兼容，则完全支持这些部署 "IMT"。

例如，如果软件，硬件和配置符合本文档中定义的准则，则完全支持添加更多存储控制器或 Cisco UCS 服务器并将软件升级到较新版本。

NetApp ONTAP

NetApp ONTAP 软件安装在所有 NetApp FAS， AFF 和 AFF 全 SAN 阵列（ASA）系统上。FlexPod 已通过 ONTAP 软件的验证，可提供高度可扩展的存储架构，支持无中断运行，无中断升级和灵活的数据基础架构。

有关 ONTAP 的详细信息，请参见 "ONTAP 数据管理软件" 产品页面。

Cisco Nexus 切换操作模式

在给定 FlexPod 部署中，可以使用多种 Cisco Nexus 产品作为交换组件。其中大多数选项都使用传统的 Cisco Nexus OS 或 NX-OS 软件。Cisco Nexus 系列交换机在其产品系列中提供了不同的功能。本文档稍后将详细介绍这些功能。

Cisco 在软件定义的网络空间中提供的产品称为应用程序中心基础架构（Application Centric Infrastructure， ACI）。支持 ACI 模式（也称为光纤模式）的 Cisco Nexus 产品系列是 Cisco Nexus 9300 系列。这些交换机也可以部署在 NX-OS 或独立模式下。

Cisco ACI 的目标部署对象是侧重于特定应用程序要求的数据中心部署。应用程序通过一系列配置文件和合同进行实例化，这些配置文件和合同允许从主机或虚拟机（VM）一直通过网络连接到存储。

FlexPod 已通过 Cisco Nexus 交换机的两种操作模式的验证。有关 ACI 和 NX-OS 模式的详细信息，请参见以下 Cisco 页面：

- "Cisco 以应用程序为中心的基础架构"
- "Cisco NX-OS 软件"

最低硬件要求

FlexPod 数据中心配置具有最低硬件要求，包括但不限于交换机，互联阵列，服务器和 NetApp 存储控制器。

您必须使用 Cisco UCS 服务器。C 系列和 B 系列服务器均已在经过验证的设计中使用。Cisco Nexus 阵列扩展器（FEX）是 C 系列服务器的可选配置。

FlexPod 配置具有以下最低硬件要求：

- 采用冗余配置的两个 Cisco Nexus 交换机。此配置可以包含两个来自 Cisco Nexus 5000 ， 7000 或 9000 系列的冗余交换机。这两个交换机的型号应相同，并且应配置为相同的操作模式。

  如果要部署 ACI 架构，则必须遵守以下附加要求：

  - 在主干叶拓扑中部署 Cisco Nexus 9000 系列交换机。
  - 使用三个 Cisco 应用程序策略基础架构控制器（APIC）。
- 采用冗余配置的两个 Cisco UCS 6200 ， 6300 或 6400 系列互联阵列。
- Cisco UCS 服务器：
  - 如果解决方案使用 B 系列服务器，则需要一个 Cisco UCS 5108 B 系列刀片式服务器机箱加上两个 Cisco UCS B 系列刀片式服务器以及两个 2104 ， 2204/8 ， 2408 或 2304 I/O 模块（IOM）。
  - 如果解决方案使用 C 系列服务器，则需要两个 Cisco UCS C 系列机架式服务器。

    对于 Cisco UCS C 系列机架式服务器的大型部署，您可以选择一对 2232PP FEX 模块。但是， 2232PP 不是硬件要求。
- 采用高可用性（HA）对配置的两个 NetApp 存储控制器：

  此配置可以包含任何受支持的 NetApp FAS ， AFF 或 ASA 系列存储控制器。请参见 "NetApp Hardware Universe" 应用程序以获取受支持的 FAS ， AFF 和 ASA 控制器型号的最新列表。

  - HA 配置要求每个控制器具有两个冗余接口来进行数据访问；这些接口可以是 FCoE ， FC 或 10/25/100GB 以太网（GbE）。
  - 如果解决方案使用 NetApp ONTAP ，则需要经过 NetApp 批准的集群互连拓扑。有关详细信息，请参见 "交换机" 选项卡 Hardware Universe 。
  - 如果解决方案使用 ONTAP ，则每个控制器至少需要两个额外的 10/25/100GbE 端口才能进行数据访问。
  - 对于具有两个节点的 ONTAP 集群，您可以配置双节点无交换机集群。
  - 对于具有两个以上节点的 ONTAP 集群，需要一对集群互连交换机。
- 一个具有任何受支持磁盘类型的 NetApp 磁盘架。请参见的磁盘架选项卡 "NetApp Hardware Universe" 有关支持的磁盘架型号的最新列表。

最低软件要求

FlexPod 配置具有以下最低软件要求：

- NetApp ONTAP ：
  - ONTAP 软件版本需要 ONTAP 9.1 或更高版本
- Cisco UCS Manager 版本：
  - Cisco UCS 6200 系列互联阵列— 2.2 （8a）
  - Cisco UCS 6300 系列互联阵列— 3.1 （1e）
  - Cisco UCS 6400 系列互联阵列— 4.0 （1）
- Cisco Intersight 托管模式：

- Cisco UCS 6400 系列互联阵列— 4.1 （2）

- 对于 Cisco Nexus 5000 系列交换机， Cisco NX-OS 软件版本 5.0 （3） N1 （1c）或更高版本，包括 NX-OS 5.1.x
- 对于 Cisco Nexus 7000 系列交换机：
  - 4 插槽机箱需要使用 Cisco NX-OS 软件版本 6.1 （2）或更高版本
  - 9 插槽机箱需要 Cisco NX-OS 软件版本 5.2 或更高版本
  - 10 插槽机箱需要 Cisco NX-OS 软件版本 4.0 或更高版本
  - 18 插槽机箱需要 Cisco NX-OS 软件版本 4.1 或更高版本
- 对于 Cisco Nexus 9000 系列交换机， Cisco NX-OS 软件版本 6.1 （2）或更高版本

> FlexPod 配置中使用的软件必须在 NetApp 中列出并受支持 "IMT"。某些功能可能需要比列出的软件版本更新的软件版本。

连接要求

FlexPod 配置具有以下连接要求：

- 所有组件都需要一个单独的 100 Mbps 以太网 /1 Gb 以太网带外管理网络。
- NetApp 建议您在整个环境中启用巨型帧支持，但这并不是必需的。
- 建议仅将 Cisco UCS 互联阵列设备端口用于 iSCSI 和 NAS 连接。
- 不能在核心 FlexPod 组件之间直列放置任何其他设备。

上行链路连接：

- NetApp 存储控制器上的端口必须连接到 Cisco Nexus 5000 ， 7000 或 9000 系列交换机，才能支持虚拟端口通道（ Virtual Port Channel ， vPC ）。
- 从 Cisco Nexus 5000 ， 7000 或 9000 系列交换机到 NetApp 存储控制器，需要使用 vPC 。
- 从 Cisco Nexus 5000 ， 7000 或 9000 系列交换机到互联阵列需要使用 vPC 。
- 一个 vPC 至少需要两个连接。可以根据应用程序负载和性能要求增加 vPC 中的连接数。

直接连接：

- 可以对直接连接到互联阵列的 NetApp 存储控制器端口进行分组，以启用端口通道。此配置不支持 VPC 。
- 建议将 FCoE 端口通道用于端到端 FCoE 设计。

SAN 启动：

- FlexPod 解决方案是围绕使用 iSCSI ， FC 或 FCoE 协议的 SAN 启动架构设计的。使用从 SAN 启动技术可以为数据中心基础架构提供最灵活的配置，并可在每个基础架构组件中提供丰富的功能。尽管从 SAN 启动是最高效的配置，但从本地服务器存储启动是一种有效且受支持的配置。
- 不支持通过 FC-NVMe 进行 SAN 启动。

其他要求

FlexPod 架构还具有以下与互操作性和支持相关的其他要求：

- 所有硬件和软件组件都必须在 NetApp 上列出并受支持 "IMT"， "Cisco UCS 硬件和软件兼容性列表"和 Cisco UCS 硬件和软件互操作性表工具。
- 所有设备都需要有效的支持合同，包括：
  - Cisco 设备的 SMART Net Total Care （ SMARTnet Total Care ， SMARTnet ）支持
  - 对 NetApp 设备的 SupportEdge Advisor 或 SupportEdge Premium 支持

有关详细信息，请参见 NetApp "IMT"。

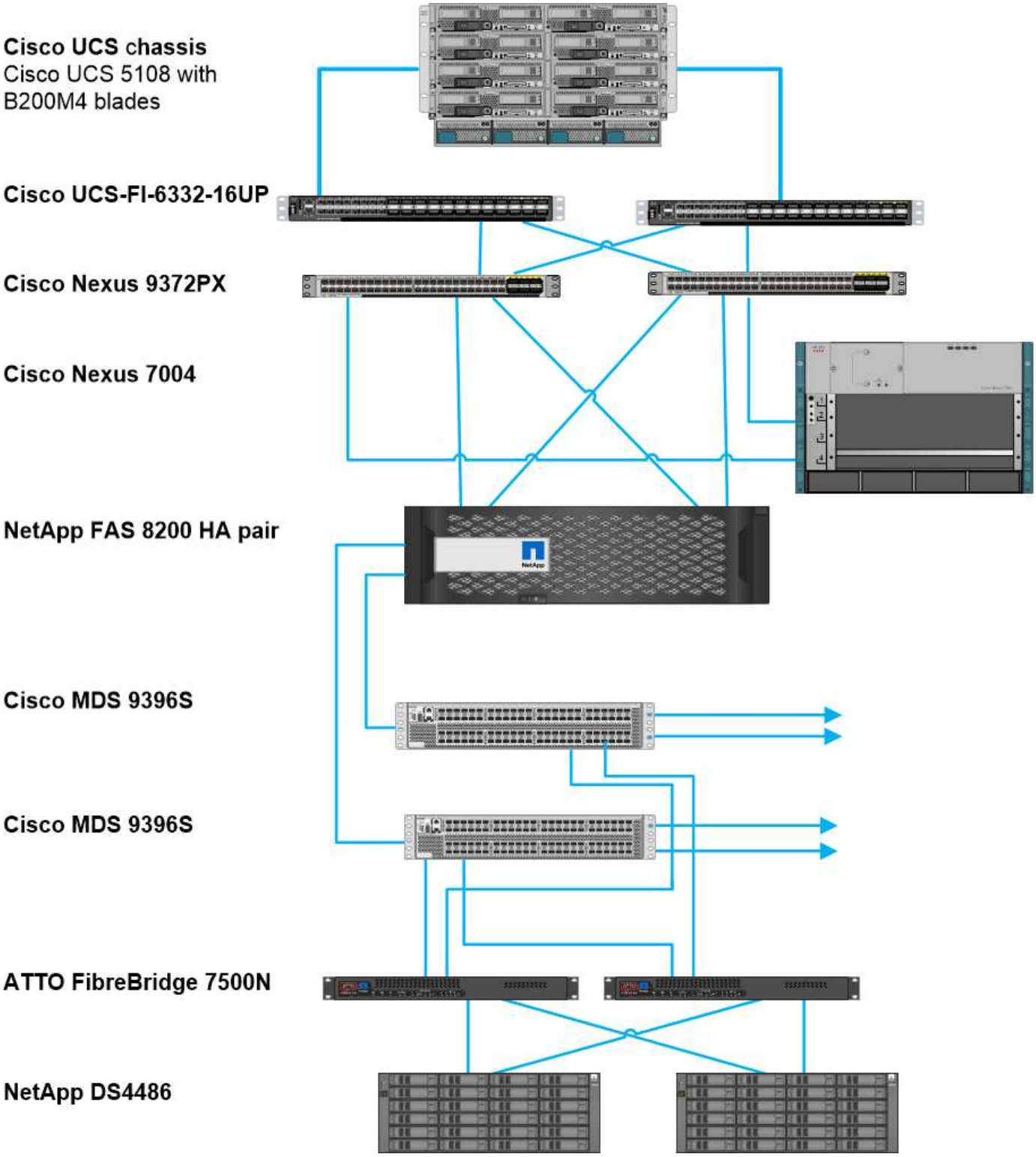
可选功能

NetApp 支持多个可选组件，可进一步增强 FlexPod 数据中心架构。以下各小节概述了可选组件。

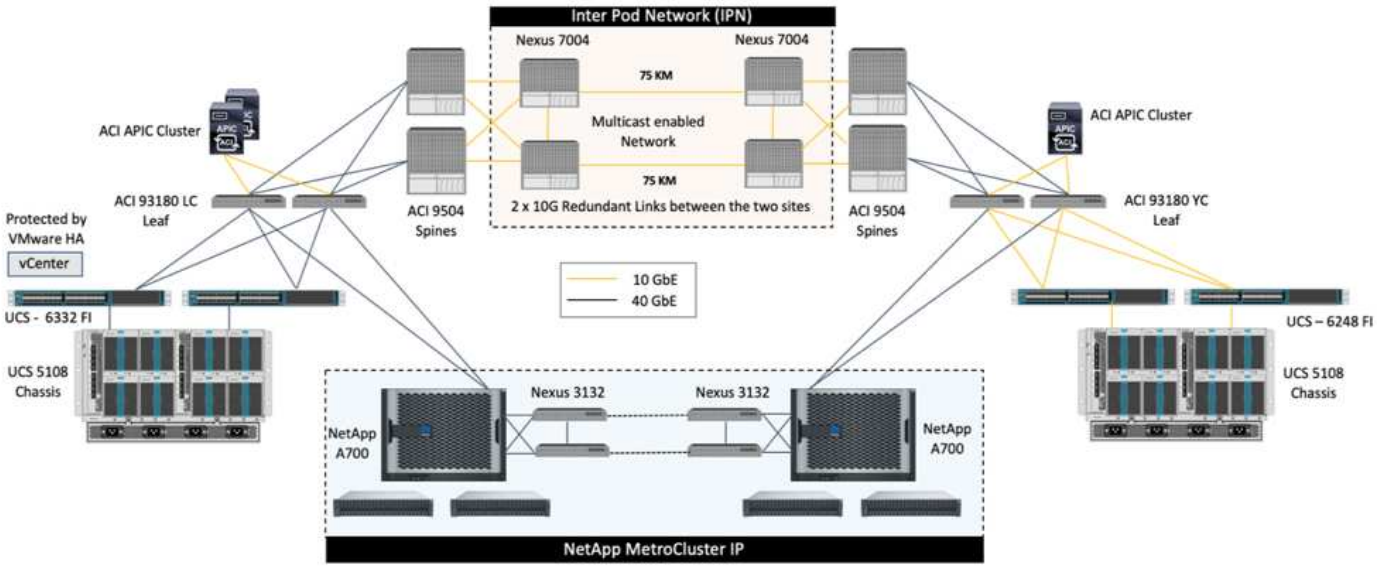
MetroCluster

FlexPod 支持两种 NetApp MetroCluster 软件版本，可在双节点或四节点集群配置中实现持续可用性。MetroCluster 可为关键工作负载提供同步复制。它需要使用连接到 Cisco 交换机的双站点配置。对于 MetroCluster FC ，站点之间支持的最大距离约为 186 英里（ 300 公里），对于 MetroCluster IP ，支持的最大距离约为 435 英里（ 700 公里）。下图分别展示了采用 NetApp MetroCluster 架构的 FlexPod 数据中心和采用 NetApp MetroCluster IP 架构的 FlexPod 数据中心。

下图展示了采用 NetApp MetroCluster 架构的 FlexPod Datacenter 。

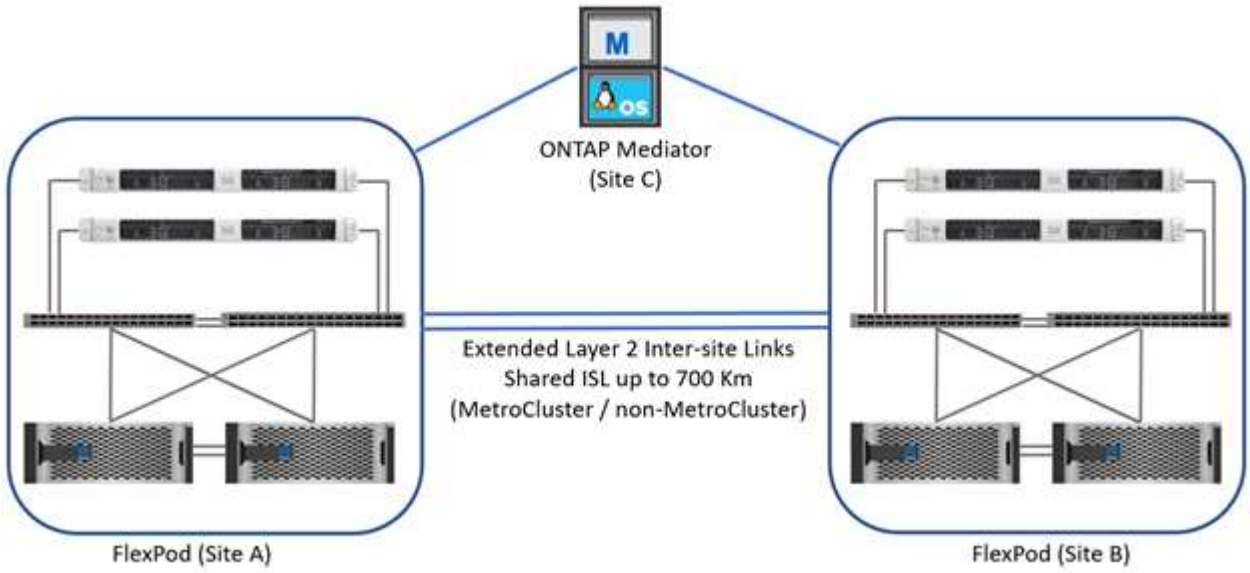


下图展示了采用 NetApp MetroCluster IP 架构的 FlexPod 数据中心。



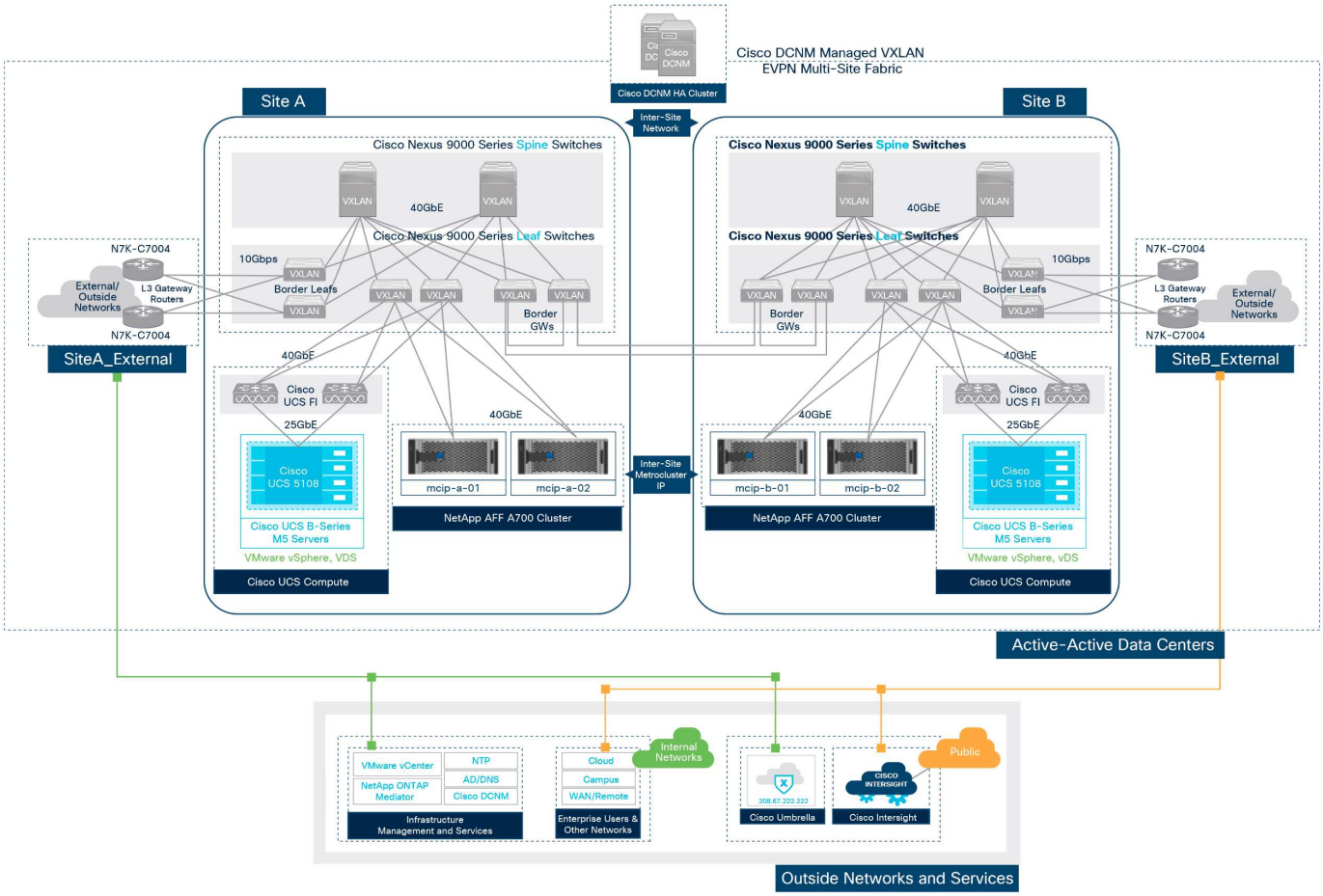
从 ONTAP 9.8 开始，可以在第三个站点部署 ONTAP 调解器，以监控 MetroCluster IP 解决方案，并在发生站点灾难时实现自动计划外切换。

对于具有扩展的第 2 层站点到站点连接的 FlexPod MetroCluster IP 解决方案部署，如果网络带宽和交换机满足下图所示的要求，则可以通过共享 ISL 并将 FlexPod 交换机用作合规的 MetroCluster IP 交换机来节省成本。 其中展示了具有 ISL 共享和合规交换机的 FlexPod MetroCluster IP 解决方案。

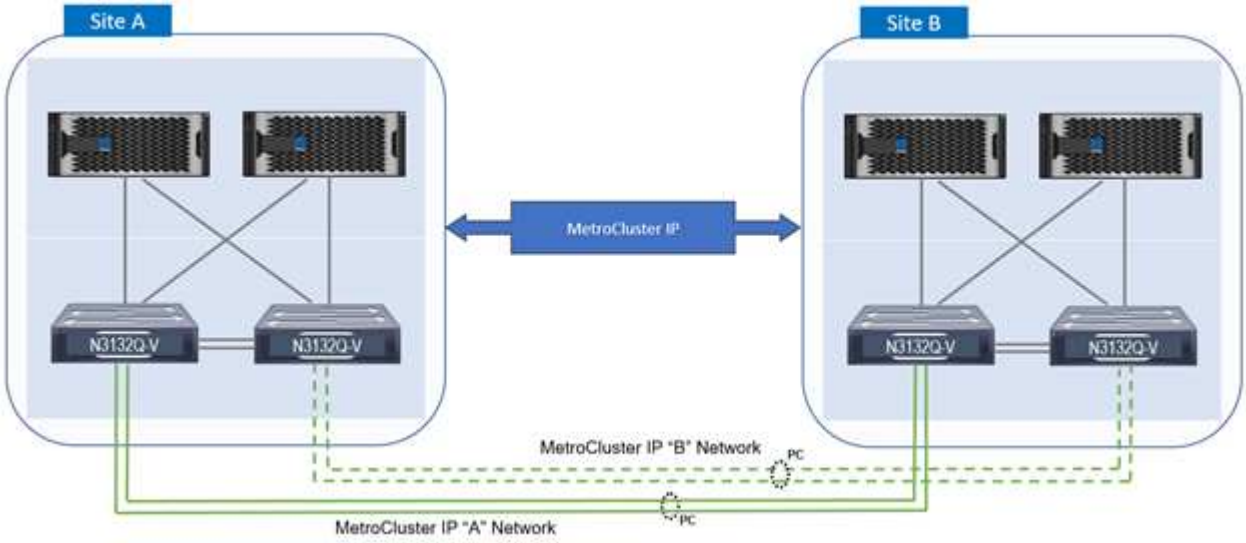


下图显示了采用 VXLAN 多站点网络结构部署的 FlexPod MetroCluster IP 解决方案的 VXLAN 多站点网络结构和 MetroCluster IP 存储网络结构。

- 适用于 FlexPod MetroCluster IP 解决方案的 VXLAN 多站点网络结构



- 适用于 FlexPod MetroCluster IP 解决方案的 MetroCluster IP 存储网络结构



端到端 **FC-NVMe**

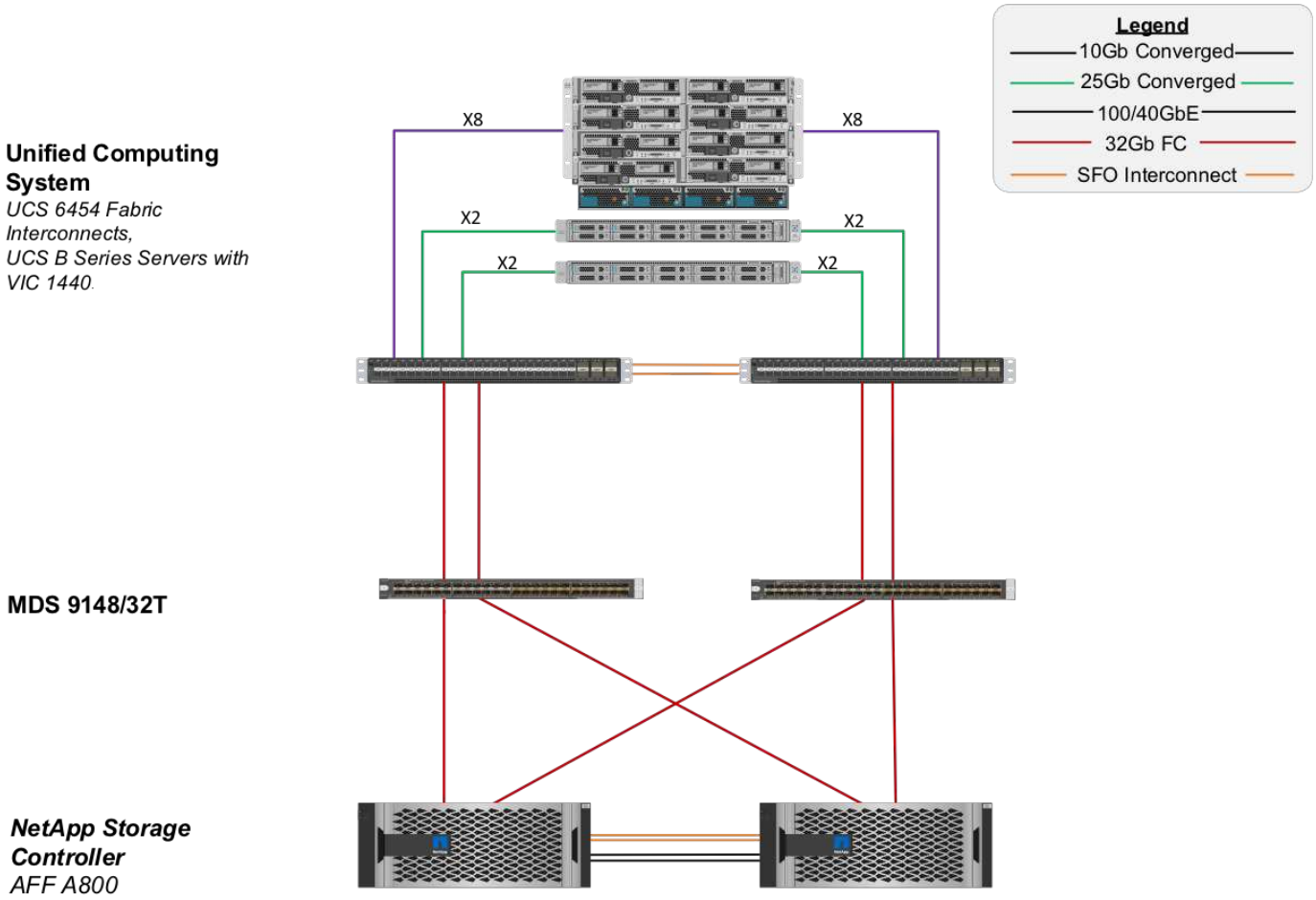
端到端 FC-NVMe 可无缝扩展客户的现有 SAN 基础架构以实现实时应用程序，同时提高 IOPS 和吞吐量并降低延迟。

可以使用现有的 32G FC SAN 传输同时传输 NVMe 和 SCSI 工作负载。

下图显示了采用 Cisco MDS 的适用于 FC 的 FlexPod 数据中心。

有关 FlexPod 配置和性能优势的更多详细信息，请参见 "推出适用于 FlexPod 的端到端 NVMe 白皮书。"

有关 ONTAP 实施的详细信息，请参见 "TR-4684：《使用 NVMe 实施和配置现代 SAN 》"。



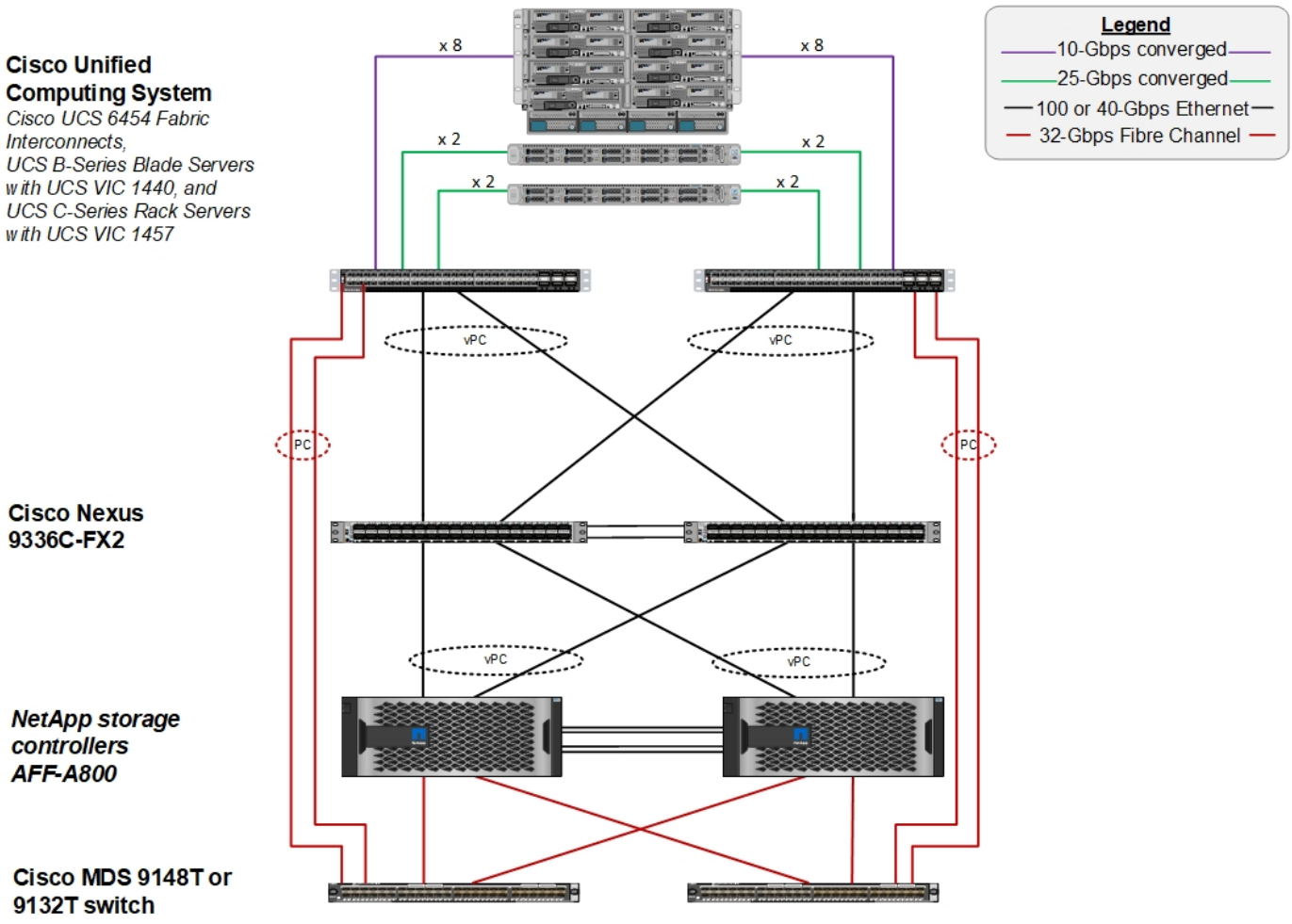
通过 **Cisco MDS** 启动 **FC SAN**

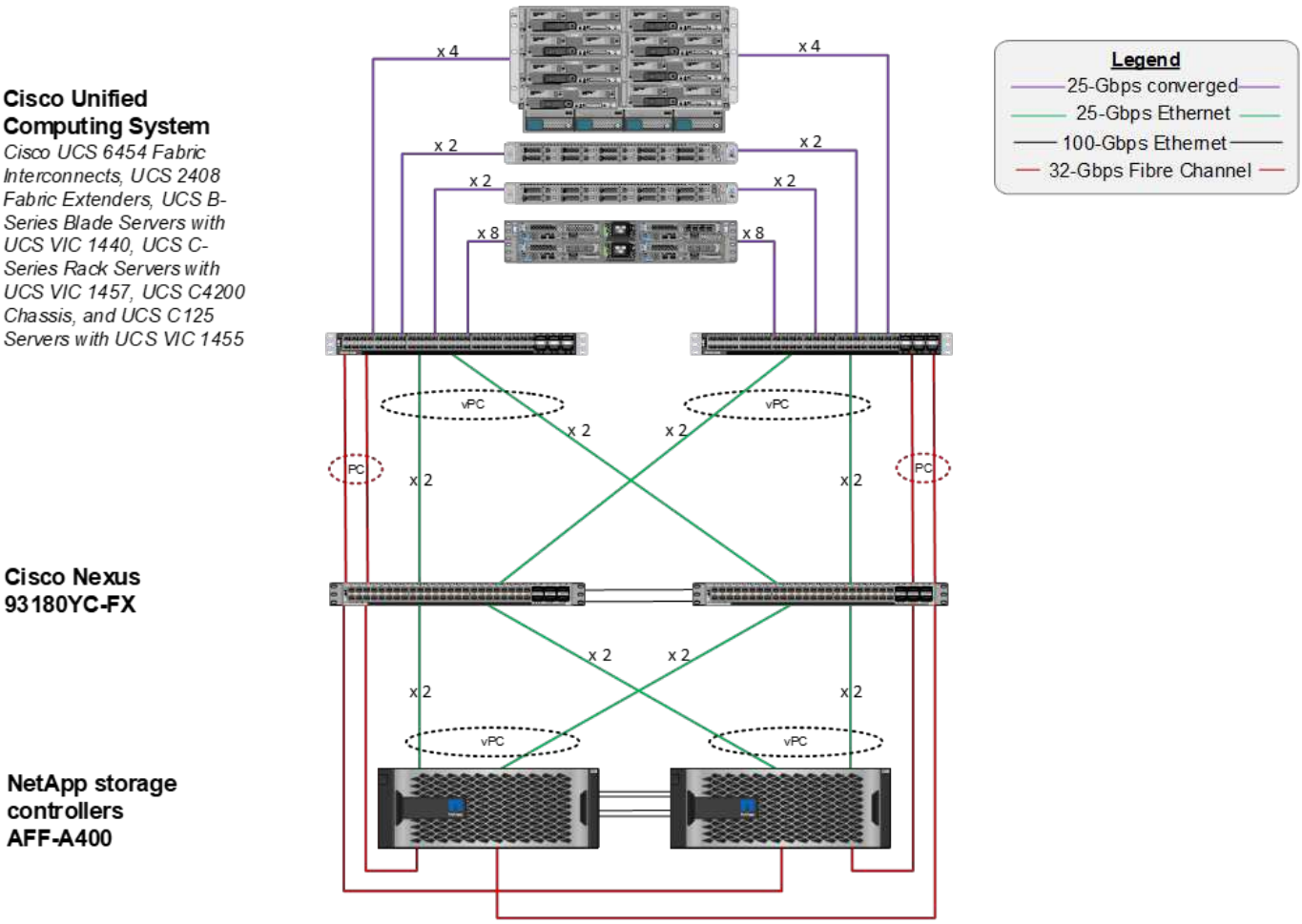
为了通过使用专用 SAN 网络提高可扩展性， FlexPod 通过 Cisco MDS 交换机和 Nexus 交换机支持 FC ，并支持 Cisco Nexus 93108TC-FX 等 FC 。Cisco MDS 中的 FC SAN 启动选项具有以下许可和硬件要求：

- 每个 NetApp 存储控制器至少两个 FC 端口；每个 SAN 网络结构一个端口
- 每个 NetApp 存储控制器上的 FC 许可证
- NetApp 支持的 Cisco MDS 交换机和固件版本 "IMT"

有关基于 MDS 的设计的详细指导，请参见 CVD "《采用 VMware vSphere 6.7U1 的 FlexPod 数据中心光纤通道和 iSCSI 部署指南》"。

下图分别显示了采用 MDS 连接的 FlexPod Datacenter for FC 和采用 Cisco Nexus 93180YC-FX 的 FlexPod Datacenter for FC 的示例。


Cisco Unified Computing System
Cisco UCS 6454 Fabric Interconnects,
UCS B-Series Blade Servers with UCS VIC 1440, and
UCS C-Series Rack Servers with UCS VIC 1457
Cisco Nexus 9336C-FX2
NetApp storage controllers AFF-A800
Cisco MDS 9148T or 9132T switch
x 8
x 8
x 2
x 2
x 2
x 2
vPC
vPC
PC
PC
vPC
vPC
Legend
10-Gbps converged
25-Gbps converged
100 or 40-Gbps Ethernet
32-Gbps Fibre Channel



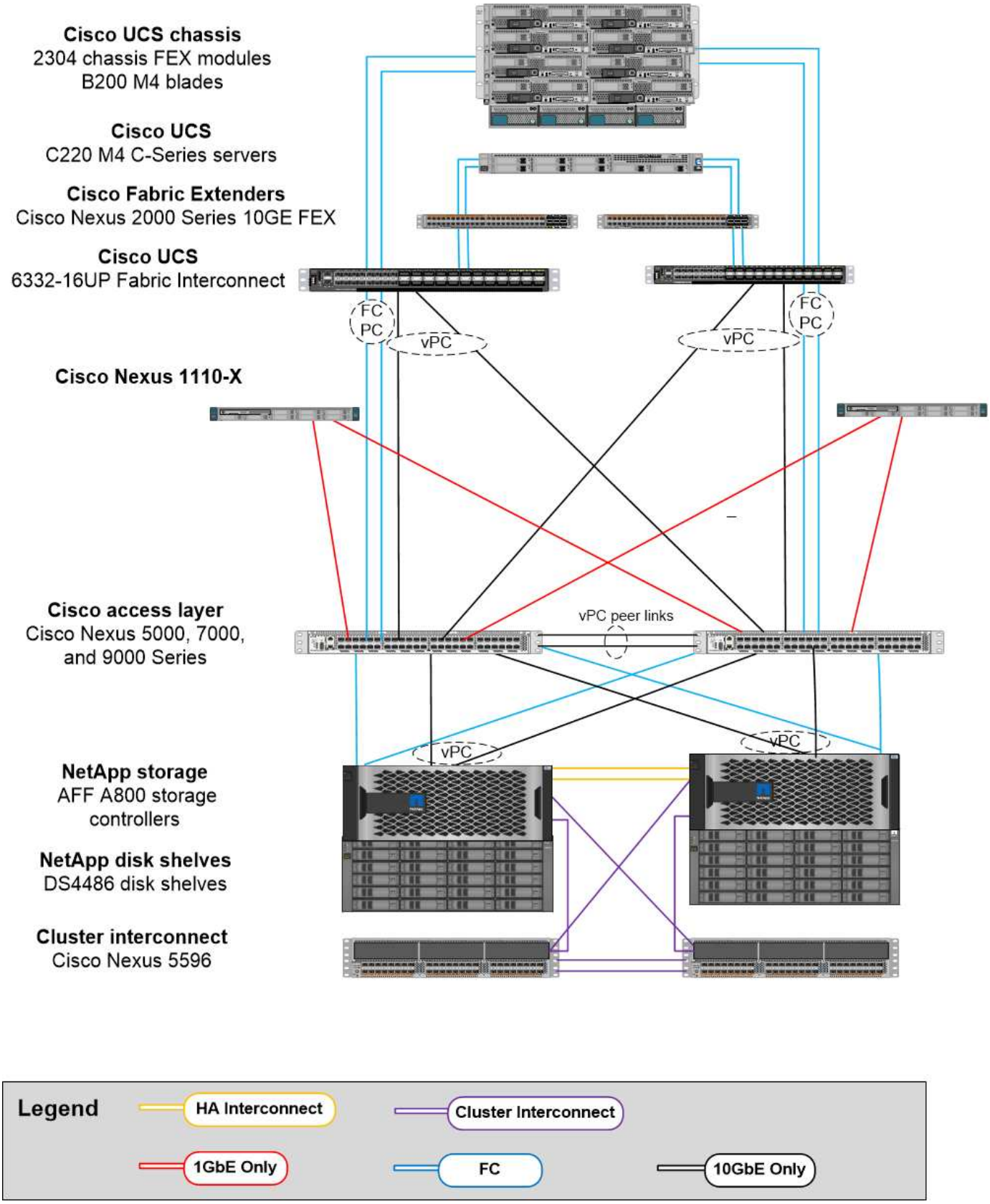
使用 **Cisco Nexus** 启动 **FC SAN**

经典 FC SAN 启动选项具有以下许可和硬件要求：

- 在 Cisco Nexus 5000 系列交换机中执行 FC 分区时，需要为 Cisco Nexus 5000 系列交换机（ FC_FEATURES_PKG ）提供存储协议服务包许可证。
- 在 Cisco Nexus 5000 系列交换机中执行 FC 分区时，需要在互联阵列和 Cisco Nexus 5000 系列交换机之间建立 SAN 链路。为了增加冗余，建议在链路之间使用 SAN 端口通道。
- Cisco Nexus 5010 ， 5020 和 5548P 交换机需要使用单独的 FC 或通用端口（ UP ）模块来连接到 Cisco UCS 互联阵列和 NetApp 存储控制器。
- Cisco Nexus 93180YC-FX 需要 FC 功能许可证才能启用 FC 。
- 每个 NetApp 存储控制器至少需要两个 8/16/32 Gb FC 端口进行连接。
- NetApp 存储控制器上需要具有 FC 许可证。

> 使用 Cisco Nexus 7000 或 9000 系列交换机时，除非在互联阵列中执行 FC 分区，否则不能使用传统 FC 。在这种情况下，不支持交换机的 SAN 上行链路。

下图显示了 FC 连接配置。



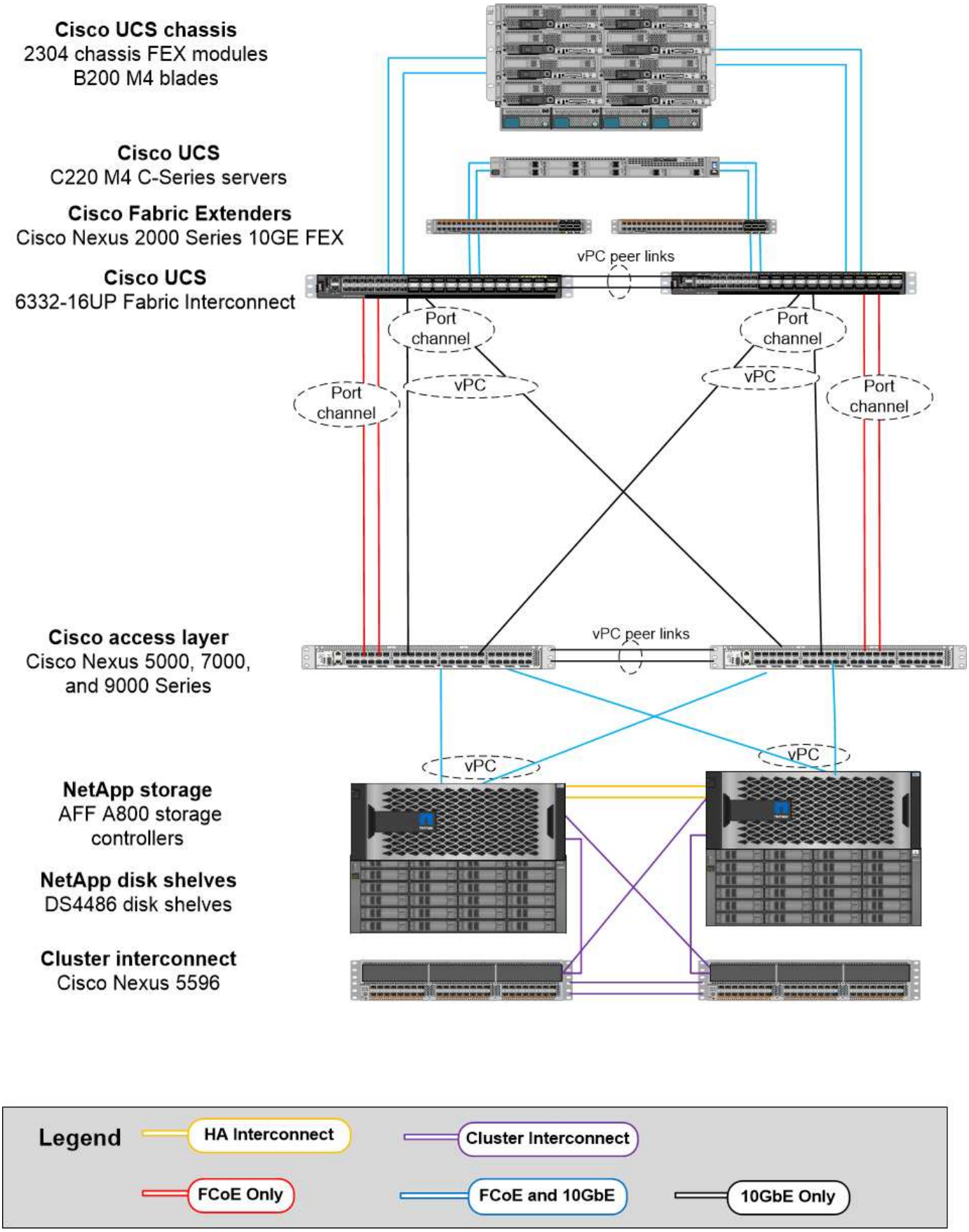
FCoE SAN 启动选项

FCoE SAN 启动选项具有以下许可和硬件要求：

- 在交换机中执行 FC 分区时，需要为 Cisco Nexus 5000 或 7000 系列交换机 `（FC_FEATURES_PKG`）提供存储协议服务包许可证。
- 在交换机中执行 FC 分区时，互联阵列与 Cisco Nexus 5000 或 7000 系列交换机之间需要 FCoE 上行链路。为了增加冗余，还建议在链路之间使用 FCoE 端口通道。
- 除非存在板载统一目标适配器 2 （UTA2）端口，否则每个 NetApp 存储控制器至少需要一个双端口统一目标适配器（UTA）附加卡来实现 FCoE 连接。
- 此选项需要在 NetApp 存储控制器上获得 FC 许可证。
- 如果您使用的是 Cisco Nexus 7000 系列交换机，并且在交换机中执行了 FC 分区，则需要一个能够支持 FCoE 的线卡。

> 除非在互联阵列中执行 FC 分区，并且存储通过设备端口连接到互联阵列，否则使用 Cisco Nexus 9000 系列交换机将不会使用 FCoE 。在这种情况下，不支持通过 FCoE 上行链路连接到交换机。

下图显示了 FCoE 启动场景。

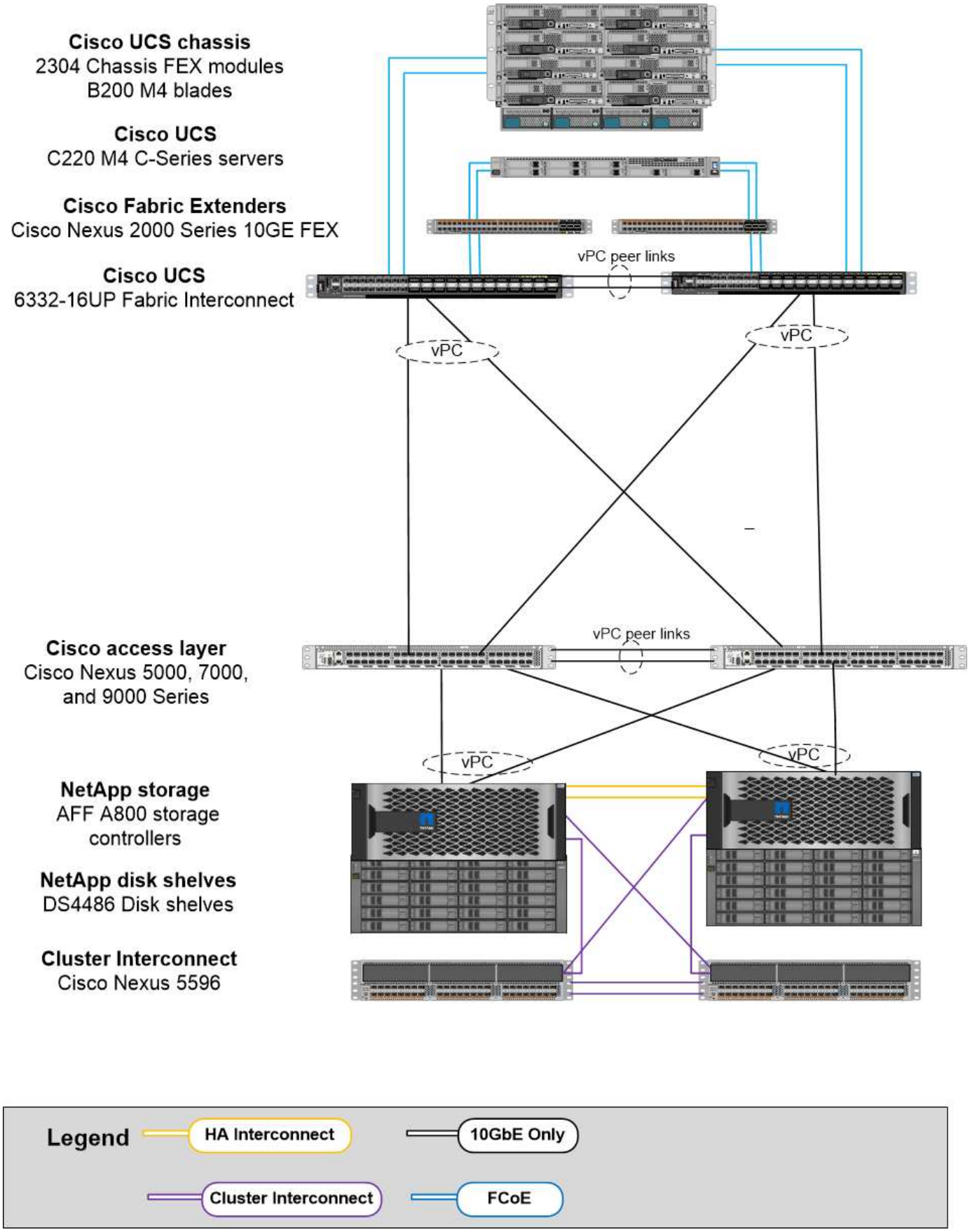

Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
Port channel
vPC
Port channel
vPC
Port channel
Port channel
Cisco access layer
Cisco Nexus 5000, 7000, and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FCoE Only
FCoE and 10GbE
10GbE Only

iSCSI 启动选项

iSCSI 启动选项具有以下许可和硬件要求：

- 需要在 NetApp 存储控制器上安装 iSCSI 许可证。
- Cisco UCS 服务器中需要一个支持 iSCSI 启动的适配器。
- NetApp 存储控制器上需要一个双端口 10Gbps 以太网适配器。

下图显示了使用 iSCSI 启动的纯以太网配置。


Cisco UCS chassis
2304 Chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
vPC
vPC
Cisco access layer
Cisco Nexus 5000, 7000,
and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage
controllers
NetApp disk shelves
DS4486 Disk shelves
Cluster Interconnect
Cisco Nexus 5596
Legend
HA Interconnect
10GbE Only
Cluster Interconnect
FCoE

Cisco UCS 直接连接到 NetApp 存储

NetApp AFF 和 FAS 控制器可以直接连接到 Cisco UCS 互联阵列，而无需任何上游 SAN 交换机。

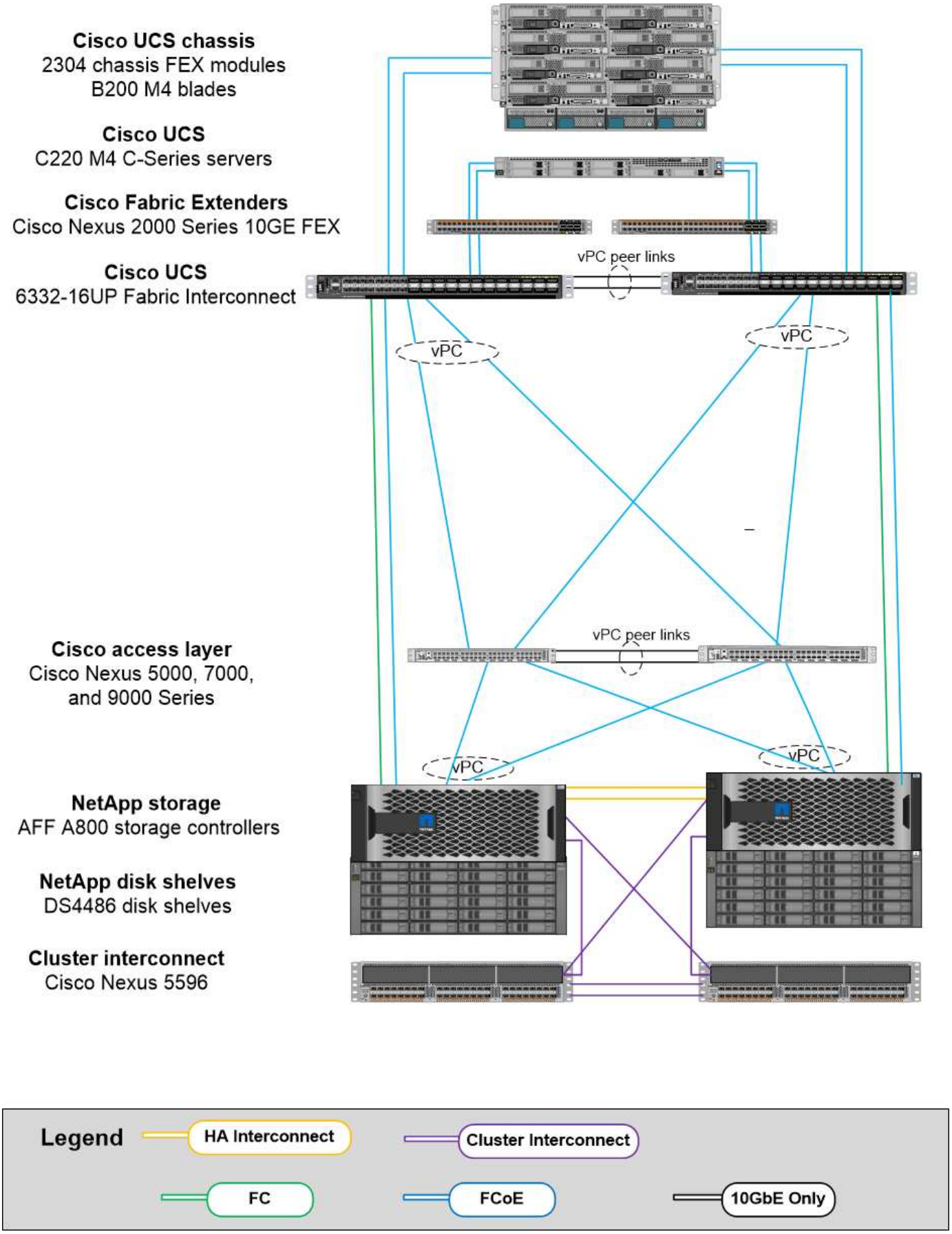
可以使用四种 Cisco UCS 端口类型直接连接到 NetApp 存储：

- * 存储 FC 端口。 * 将此端口直接连接到 NetApp 存储上的 FC 端口。
- * 存储 FCoE 端口。 * 将此端口直接连接到 NetApp 存储上的 FCoE 端口。
- * 设备端口。 * 将此端口直接连接到 NetApp 存储上的 10GbE 端口。
- * 统一存储端口。 * 将此端口直接连接到 NetApp UTA 。

许可和硬件要求如下：

- 需要在 NetApp 存储控制器上获得协议许可证。
- 服务器上需要 Cisco UCS 适配器（启动程序）。有关支持的 Cisco UCS 适配器列表，请参见 NetApp "IMT"。
- NetApp 存储控制器上需要一个目标适配器。

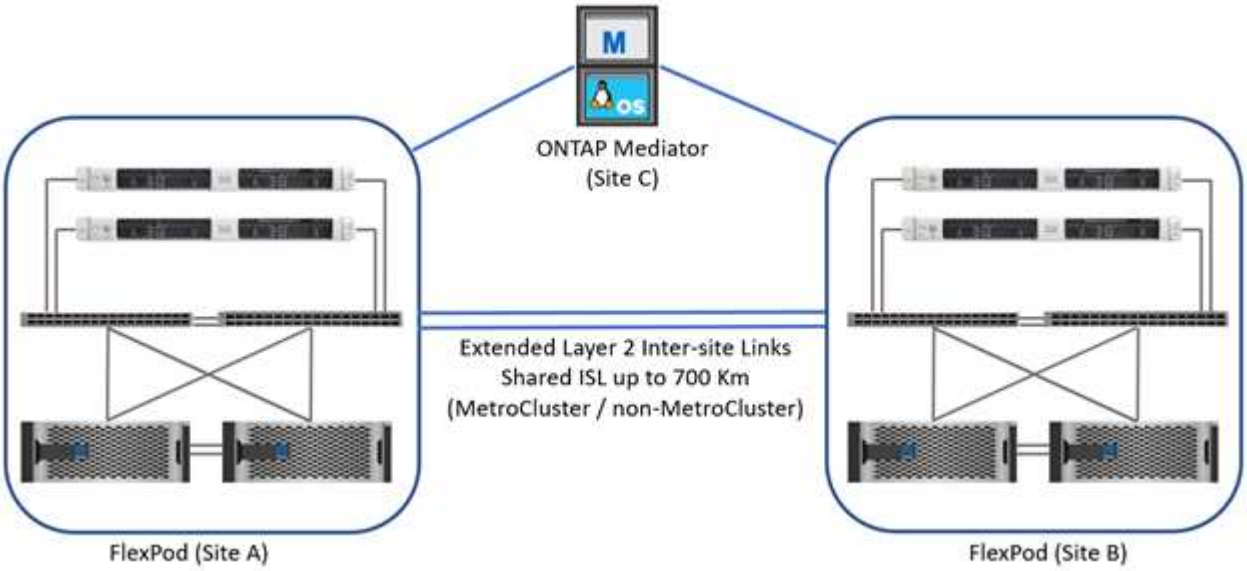
下图显示了 FC 直连配置。


Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
vPC
vPC
Cisco access layer
Cisco Nexus 5000, 7000,
and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FC
FCoE
10GbE Only

• 注： *

- Cisco UCS 配置为 FC 交换模式。
- 从目标到互联阵列的 FCoE 端口配置为 FCoE 存储端口。
- 从目标到互联阵列的 FC 端口配置为 FC 存储端口。

下图显示了 iSCSI/Unified IP 直连配置。



- 注： *
- Cisco UCS 配置为以太网交换模式。
- 从目标到互联阵列的 iSCSI 端口会配置为 iSCSI 数据的以太网存储端口。
- 从目标到互联阵列的以太网端口会配置为 CIFS/NFS 数据的以太网存储端口。

Cisco 组件

Cisco 为 FlexPod 的设计和架构做出了重大贡献，涵盖了解决方案的计算层和网络层。本节介绍可用于 FlexPod 的 Cisco UCS 和 Cisco Nexus 选项。FlexPod 既支持 Cisco UCS B 系列服务器，也支持 C 系列服务器。

Cisco UCS 互联阵列选项

FlexPod 架构需要冗余互联阵列。将多个 Cisco UCS 机箱添加到一对互联阵列时，请记住，环境中的最大机箱数由架构和端口限制决定。

下表中显示的部件号适用于基础互联阵列。它们不包括电源设备（ PSU ）或 SFP+ ， QSF++ 或扩展模块。支持其他互联阵列；请参见 "NetApp IMT" 查看完整列表。

Cisco UCS 互联阵列	部件号	技术规格
Cisco UCS 6332UP	UCS-FI-6332-UP	"Cisco UCS 6332 互联阵列"
Cisco UCS 6454	UCS-FI-6454-U	"Cisco UCS 6454 互联阵列"

Cisco UCS 6454

Cisco UCS 6454 系列提供线速，低延迟，无损 10/25/40/100GbE 以太网和 FCoE 连接，以及支持以太网或 FC 操作的统一端口。44 个 10/25Gbps 端口可作为 10Gbps 或 25Gbps 融合以太网运行，其中 8 个是统一端口，FC 可在 8/16/32Gbps 下运行。对于传统连接，四个端口以 1/25Gbps 的速率运行，六个 QSFP 端口用作 40/100Gbps 上行链路端口或分支端口。您可以与支持 100Gbps 适配器的 NetApp 存储控制器建立 100Gbps 端到端网络连接。有关适配器和平台支持的信息，请参见 "NetApp Hardware Universe"。

有关端口的详细信息，请参见 "Cisco UCS 6454 互联阵列" 产品规格。

有关 100GB QSFP 数据模块的技术规格，请参见 "Cisco 100GBASE QSFP 模块产品规格"。

Cisco UCS B 系列机箱选项

要使用 Cisco UCS B 系列刀片式服务器，您必须具有 Cisco UCS B 系列机箱。下表介绍了 Cisco UCS B 系列机箱选项。

Cisco UCS B 系列机箱	部件号	技术规格
Cisco UCS 5108	N20-C508	"Cisco UCS 5100 系列刀片式服务器机箱"

每个 Cisco UCS 5108 刀片式服务器机箱都必须具有两个 Cisco UCS 2200/23400/2400 系列 IOM ，以便为互联阵列提供冗余连接。

Cisco UCS B 系列刀片式服务器选项

Cisco UCS B 系列刀片式服务器提供半宽和全宽两种型号，并提供各种 CPU ，内存和 I/O 选项。下表列出的部件号适用于基础服务器。它们不包括 CPU ，内存，驱动器或夹层适配器卡。FlexPod 架构中提供并支持多个配置选项。

Cisco UCS B 系列刀片式服务器	部件号	技术规格
Cisco UCS B200 M6	UCSB-B200-M6	"Cisco UCS B200 M6 刀片式服务器"

前几代 Cisco UCS B 系列刀片式服务器可在 FlexPod 架构中使用，前提是它们在上受支持 "Cisco UCS 硬件和软件兼容性列表"。Cisco UCS B 系列刀片式服务器还必须具有有效的 SMARTnet 支持合同。

Cisco UCS X 系列机箱选项

要使用 Cisco UCS X 系列计算节点，您必须使用 Cisco UCS X 系列机箱。下表介绍了 Cisco UCS X 系列机箱选项。

Cisco UCS X 系列刀片式服务器	部件号	技术规格
Cisco UCS 9508 M6	UCSX-9508	"Cisco UCX9508 X 系列机箱"

每个 Cisco UCS 9508 机箱都必须具有两个 Cisco UCS 9108 智能阵列模块（ Intelligent Fabric Module ， IFM ），以便为互联阵列提供冗余连接。

Cisco UCS X 系列设备选项

Cisco UCS X 系列计算节点具有各种 CPU ，内存和 I/O 选项。下表列出的部件号适用于基础节点。它们不包括 CPU ，内存，驱动器或夹层适配器卡。FlexPod 架构中提供并支持多个配置选项。

Cisco UCS X 系列计算节点	部件号	技术规格
Cisco UCS X210c M6	UCSX-210C-M6	"Cisco UCS X210c M6 计算节点"

Cisco UCS C 系列机架式服务器选项

Cisco UCS C 系列机架式服务器提供一个和两个机架单元（ RU ）型号，并提供各种 CPU ，内存和 I/O 选项。下表中列出的部件号适用于基础服务器。它们不包括 CPU ，内存，驱动器，外设组件互连 Express （ PCIe ）卡或 Cisco Fabric Extender 。FlexPod 架构中提供并支持多个配置选项。

下表列出了 Cisco UCS C 系列机架式服务器选项。

Cisco UCS C 系列机架式服务器	部件号	技术规格
Cisco UCS C220 M6	UCSC-C220-M6	"Cisco UCS C220 M6 机架式服务器"
Cisco UCS C225 M6	UCSC-C225-M6	"Cisco UCS C225 M6 机架式服务器"
Cisco UCS C240 M6	UCSC-C240-M6	"Cisco UCS C240 M6 机架式服务器"
Cisco UCS C245 M6	UCSC-C245M6	"Cisco UCS C245 M6 机架式服务器"

前几代 Cisco UCS C 系列服务器可在 FlexPod 架构中使用，前提是它们在上受支持 "Cisco UCS 硬件和软件兼容性列表"。Cisco UCS C 系列服务器还必须具有有效的 SMARTnet 支持合同。

Cisco Nexus 5000 系列交换机选项

在 FlexPod 架构中需要使用冗余 Cisco Nexus 5000 ， 7000 或 9000 系列交换机。下表列出的部件号适用于 Cisco Nexus 5000 系列机箱，不包括 SFP 模块，附加 FC 或以太网模块。

Cisco Nexus 5000 系列交换机	部件号	技术规格
Cisco Nexus 56128P	N5K-C56128P	"Cisco Nexus 5600 平台交换机"
Cisco Nexus 5672UP-16G	N5K-C5672UP-16G	
Cisco Nexus 5596UP	N5K-C5596UP-FA	"Cisco Nexus 5548 和 5596 交换机"
Cisco Nexus 5548UP	N5K-C5548UP-FA	

Cisco Nexus 7000 系列交换机选项

在 FlexPod 架构中需要使用冗余 Cisco Nexus 5000 ， 7000 或 9000 系列交换机。下表列出的部件号适用于 Cisco Nexus 7000 系列机箱；不包括 SFP 模块，线卡或电源，但包括风扇托架。

Cisco Nexus 7000 系列交换机	部件号	技术规格
Cisco Nexus 7004	N7K-C7004	"Cisco Nexus 7000 4 插槽交换机"
Cisco Nexus 7009	N7K-C7009	"Cisco Nexus 7000 9 插槽交换机"
Cisco Nexus 7702	N7K-C7702	"Cisco Nexus 7700 双插槽交换机"
Cisco Nexus 7706	N77-C7706	"Cisco Nexus 7700 6 插槽交换机"

Cisco Nexus 9000 系列交换机选项

在 FlexPod 架构中需要使用冗余 Cisco Nexus 5000 ， 7000 或 9000 系列交换机。下表列出的部件号适用于 Cisco Nexus 9000 系列机箱，不包括 SFP 模块或以太网模块。

Cisco Nexus 9000 系列交换机	部件号	技术规格
Cisco Nexus 93180YC-FX	N9K-C93180YC-FX	"Cisco Nexus 9300 系列交换机"
Cisco Nexus 93180YC-EX	N9K-93180YC-EX	
Cisco Nexus 9336PQ ACI Spine	N9K-C9336PQ	
Cisco Nexus 9332PQ	N9K-C9332PQ	
Cisco Nexus 9336C-x2	N9K-C9336C-x2	
Cisco Nexus 92304QC	N9K-C92304QC.	"Cisco Nexus 9200 系列交换机"
Cisco Nexus 9236C	N9K-9236C	

> 某些 Cisco Nexus 9000 系列交换机还具有其他变体。FlexPod 解决方案支持这些变体。有关 Cisco Nexus 9000 系列交换机的完整列表，请参见 "Cisco Nexus 9000 系列交换机" 在 Cisco 网站上。

Cisco APIC 选项

部署 Cisco ACI 时，除了一节中的各项之外，还必须配置三个 Cisco APIC "Cisco Nexus 9000 系列交换机"。有关 Cisco APIC 大小的详细信息，请参见 "Cisco Application Centric Infrastructure 产品规格。"

有关 APIC 产品规格的详细信息，请参阅上的表 1 至表 3 "Cisco Application Policy Infrastructure Controller 产品规格"。

Cisco Nexus 阵列扩展器选项

对于使用 C 系列服务器的大型 FlexPod 架构，建议使用冗余 Cisco Nexus 2000 系列机架式 FEX 。下表介绍了一些 Cisco Nexus FEX 选项。此外，还支持其他 FEX 型号。有关详细信息，请参见 "Cisco UCS 硬件和软件兼容性列表"。

Cisco Nexus 机架式 **FEX**	部件号	技术规格
Cisco Nexus 2232PP	N2K-C2232PP	"Cisco Nexus 2000 系列阵列扩展器"
Cisco Nexus 2232TM-E	N2K-C2232TM-E	

Cisco Nexus 机架式 FEX	部件号	技术规格
Cisco Nexus 2348UPQ	N2K-C2348UPQ	"Cisco Nexus 2300 平台阵列扩展器"
Cisco Nexus 2348TQCisco Nexus 2348TQE	N2K-C2348TQN2K-C2348TQ-E	

Cisco MDS 选项

Cisco MDS 交换机是 FlexPod 架构中的一个可选组件。在 FC SAN 中实施 Cisco MDS 交换机时，需要使用冗余 SAN 交换机网络结构。下表列出了部分受支持的 Cisco MDS 交换机的部件号和详细信息。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。

Cisco MDS 9000 系列交换机	部件号	Description
Cisco MDS 9148T	DS-C9148T-24IK	"Cisco MDS 9100 系列交换机"
Cisco MDS 9132T	DS-C9132T-MEK9	
Cisco MDS 9396S	DS-C9396S-K9	"Cisco MDS 9300 系列交换机"

Cisco 软件许可选项

要在 Cisco Nexus 交换机上启用存储协议，需要许可证。Cisco Nexus 5000 和 7000 系列交换机都需要存储服务许可证才能为 SAN 启动实施启用 FC 或 FCoE 协议。Cisco Nexus 9000 系列交换机当前不支持 FC 或 FCoE 。

根据您为 FlexPod 解决方案的每个组件选择的选项，这些许可证所需的许可证和部件号会有所不同。例如，软件许可证部件号会根据端口数量以及您选择的 Cisco Nexus 5000 或 7000 系列交换机而有所不同。有关确切的部件号，请咨询您的销售代表。下表列出了 Cisco 软件许可选项。

Cisco 软件许可	部件号	许可证信息
Cisco Nexus 5500 存储许可证， 8 端口， 48 端口和 96 端口	N55-8P-SSK9/N55-48P-SSK9/N55-96P-SSK9	"许可 Cisco NX-OS 软件功能"
Cisco Nexus 5010/5020 存储协议许可证	N5010-SSK9/N5020-SSK9	
Cisco Nexus 5600 存储协议许可证	N56-16p-SSK9/N56722-72p-SSK9/N56128-128P-SSK9	
Cisco Nexus 7000 存储企业许可证	N7K-SAN1K9	
Cisco Nexus 9000 企业服务许可证	N95 — LAN1K9/N93 — LAN1K9	

Cisco 支持许可选项

FlexPod 架构中的所有 Cisco 设备都需要有效的 SMARTnet 支持合同。

所需的许可证以及这些许可证的部件号必须由销售代表进行验证，因为它们可能因不同产品而异。下表列出了 Cisco 支持许可选项。

Cisco 支持许可	许可证指南
Smart Net Total Care 现场高级版	"Cisco Smart Net Total Care 服务"

NetApp 组件

NetApp 存储控制器在 FlexPod 架构中为启动和应用程序数据存储提供了存储基础。NetApp 组件包括存储控制器，集群互连交换机，驱动器和磁盘架以及许可选项。

NetApp 存储控制器选项

在 FlexPod 架构中需要使用冗余 NetApp FAS ， AFF 或 AFF ASA 控制器。这些控制器运行 ONTAP 软件。订购存储控制器后，可以在这些控制器上预加载首选软件版本。对于 ONTAP ，系统会订购一个完整的集群。整个集群包括一对存储控制器和一个集群互连（交换机或无交换机）。

根据选定的存储平台，可以使用不同的选项和配置。有关这些附加组件的详细信息，请咨询您的销售代表。

下表中列出的控制器系列适合在 FlexPod Datacenter 解决方案中使用，因为它们与 Cisco Nexus 交换机的连接是无缝的。请参见 "NetApp Hardware Universe" 有关每个控制器型号的特定兼容性详细信息。

存储控制器系列	技术规格
AFF A-Series	"AFF A-Series 文档"
AFF ASA A 系列	"AFF ASA A 系列文档"
FAS 系列	"FAS 系列文档"

集群互连交换机选项

下表列出了可用于 FlexPod 架构的 Nexus 集群互连交换机。此外， FlexPod 还支持所有 ONTAP 支持的集群交换机，包括非 Cisco 交换机，但前提是它们与要部署的 ONTAP 版本兼容。请参见 "NetApp Hardware Universe" 有关特定交换机型号的其他兼容性详细信息。

集群互连交换机	技术规格
Cisco Nexus 3132Q-V	"NetApp 文档： Cisco Nexus 3132Q-V 交换机"
Cisco Nexus 9336C-x2	"NetApp 文档： Cisco Nexus 9336C-x2 交换机"

NetApp 磁盘架和驱动器选项

所有存储控制器至少需要一个 NetApp 磁盘架。

选定的 NetApp 磁盘架类型决定了该磁盘架中可用的驱动器类型。

> 有关所有磁盘架和磁盘部件号，请咨询您的销售代表。

有关支持的驱动器的详细信息，请单击下表中的 NetApp Hardware Universe 链接，然后选择支持的驱动器。

磁盘架	技术规格
DS224C	"NetApp Hardware Universe 上支持的磁盘架和存储介质驱动器"
DS212C	
DS460C	
NS224	

NetApp 软件许可选项

下表列出了适用于 FlexPod 数据中心架构的 NetApp 软件许可选项。NetApp 软件在 FAS 和 AFF 控制器级别获得许可。

NetApp 软件许可	部件号	技术规格
软件，完整套件（控制器）， -C	SW-8XXX-COMP-BNDC-C	"产品库 A-Z"
软件， ONTAP Essentials （控制器）， -C	SW-8XXX-ONTAP9-C	

NetApp 支持许可选项

FlexPod 架构需要 NetApp SupportEdge Premium 许可证，但这些许可证的部件号因您在 FlexPod 设计中选择的选项而异。例如，根据您选择的 FAS 控制器，软件许可证部件号会有所不同。有关各个支持许可证的确切部件号的信息，请咨询您的销售代表。下表显示了 SupportEdge 许可证的示例。

NetApp 支持许可	部件号	技术规格
SupportEdge Premium 现场 4 小时—月： 36	CS-O2-4 小时	"NetApp SupportEdge Premium"

电源和布线要求

FlexPod 设计对电源和布线具有最低要求。

电源要求

FlexPod 数据中心的电源要求因 FlexPod 数据中心配置的安装位置而异。

有关所需最大功率的详细数据以及其他详细电源信息，请参阅一节中列出的每个硬件组件的技术规格 "技术规格和参考：硬件组件"。

有关 Cisco UCS 电源的详细数据，请参见 "Cisco UCS 电源计算器"。

有关 NetApp 存储控制器电源数据，请参见 "NetApp Hardware Universe"。在平台下，选择要在配置中使用的存储平台（ FAS/V 系列或 AFF ）。选择 ONTAP 版本和存储控制器，然后单击显示结果按钮。

最低缆线要求

所需的缆线和适配器数量和类型因 FlexPod 数据中心部署而异。电缆类型，收发器类型和数量是在设计过程中根据您的要求确定的。下表列出了所需的最小缆线数量。

硬件	型号	所需的缆线
Cisco UCS 机箱	Cisco UCS 5108	每个 Cisco UCS 2104XP ，2204XP 或 2208XP 模块至少需要两根双轴缆线
Cisco UCS 互联阵列	Cisco UCS 6248UP	• 两根 Cat5e 缆线用于管理端口 • 每对互联阵列需要两根 Cat5e 缆线，用于 L1 ， L2 互连 • 每个互联阵列至少需要四根双轴缆线 • 每个互联阵列至少需要四根 FC 缆线
	Cisco UCS 6296UP	Cisco UCS 6332-16UP
	Cisco UCS 6454	Cisco UCS 6332
	• 两根 Cat5e 缆线用于管理端口 • 每对互联阵列需要两根 Cat5e 缆线，用于 L1 ， L2 互连 • 每个互联阵列至少需要四根双轴缆线	Cisco UCS 6324
	• 两个 10/100/1000Mbps 管理端口 • 每个互联阵列至少需要两根双轴缆线	Cisco Nexus 5000 和 7000 系列交换机
	Cisco Nexus 5000 系列	
• 每个交换机至少需要两根 10GbE 光纤或双轴电缆 • 每个交换机至少有两根 FC 缆线（如果需要 FC/FCoE 连接）	Cisco Nexus 7000 系列	Cisco Nexus 9000 系列交换机

硬件	型号	所需的缆线
Cisco Nexus 9000 系列	每个交换机至少需要两根 10GbE 缆线	NetApp FAS 控制器
AFF A-Series	• 每个存储控制器一对 SAS 或 SATA 缆线 • 如果使用的是原有 FC ，则每个控制器至少需要两根 FC 缆线 • 每个控制器至少需要两根 10GbE 缆线 • 每个控制器至少需要一根 GbE 缆线用于管理 • 对于 ONTAP ，每对集群互连交换机需要八根短双轴缆线	
FAS 系列	NetApp 磁盘架	DS212C
每个磁盘架两根 SAS ， SATA 或 FC 缆线		DS224C
		DS460C
		NS224

技术规格和参考资料

技术规格提供了有关 FlexPod 解决方案中硬件组件的详细信息，例如机箱， FEX ，服务器，交换机， 和存储控制器。

Cisco UCS B 系列刀片式服务器机箱

下表所示的 Cisco UCS B 系列刀片式服务器机箱的技术规格包括以下组件：

- 机架单元数
- 最大刀片式服务器数
- 统一网络结构功能
- 每台服务器的中板 I/O 带宽
- FEX 的 I/O 托架数量

组件	**Cisco UCS 5100** 系列刀片式服务器机箱
机架单元	6.
最大全宽刀片式服务器	4.
最大半宽刀片式服务器	8.
支持统一网络结构	是的。
中板 I/O	每个服务器的 I/O 带宽高达 80 Gbps

组件	**Cisco UCS 5100** 系列刀片式服务器机箱
FEX 的 I/O 托架	两个托架，用于 Cisco UCS 2104XP ， 2204/8XP ，2408XP 和 2304 FEX

有关详细信息，请参见 "Cisco UCS 5100 系列刀片式服务器机箱产品规格"。

Cisco UCS B 系列刀片式服务器

下表所示的 Cisco UCS B 系列刀片式服务器的技术规格包括以下组件：

- 处理器插槽数量
- 处理器支持
- 内存容量
- 大小和速度
- SAN 启动支持
- 夹层适配器插槽的数量
- I/O 最大吞吐量
- 外形规格
- 每个机箱的最大服务器数

组件	**Cisco UCS** 产品规格
Cisco UCS B200 M6	"Cisco UCS B200 M6 刀片式服务器"

Cisco UCS C 系列机架式服务器

Cisco UCS C 系列机架式服务器的技术规格包括处理器支持，最大内存容量， PCIe 插槽数量以及外形规格大小。有关兼容 UCS 服务器型号的更多详细信息，请参见 "Cisco 硬件兼容性" 列表下表分别说明了 C 系列机架式服务器产品规格和 Cisco UCS C 系列机箱选项。

组件	**Cisco UCS** 产品规格
Cisco UCS C220 M6	"Cisco UCS C220 M6 机架式服务器"
Cisco UCS C225 M6	"Cisco UCS C225 M6 机架式服务器"
Cisco UCS C240 M6	"Cisco UCS C240 M6 机架式服务器"
Cisco UCS C245 M6	"Cisco UCS C245 M6 机架式服务器"

Cisco UCS X 系列机箱

下表所示的 Cisco UCS X 系列机箱技术规格包括以下组件：

- 机架单元数
- 最大节点数
- 统一网络结构功能

- IFM 的 I/O 托架数量

组件	**Cisco UCS 9508 X** 系列计算节点机箱
机架单元	7.
最大节点数	8.
支持统一网络结构	是的。
IFM 的 I/O 托架	两个用于 Cisco UCS 9108 智能阵列模块（ IFM ）的托架

有关详细信息，请参见 "Cisco UCS X9508 X 系列机箱产品规格"。

Cisco UCS X 系列计算节点

下表所示的 Cisco UCS X 系列计算节点的技术规格包括以下组件：

- 处理器插槽数量
- 处理器支持
- 内存容量
- 大小和速度
- SAN 启动支持
- 夹层适配器插槽的数量
- I/O 最大吞吐量
- 外形规格
- 每个机箱的最大计算节点数

组件	Cisco UCS 产品规格
Cisco UCS X210c M6	"Cisco UCS X210c M6 计算节点"

FlexPod AI ， ML 和 **DL** 的 **GPU** 建议

下表中列出的 Cisco UCS C 系列机架式服务器可在 FlexPod 架构中用于托管 AI ， ML 和 DL 工作负载。Cisco UCS C480 ML M5 服务器专为 AI ， ML 和 DL 工作负载而构建，并使用基于 NVIDIA 的 SXM2 的 GPU ，而其他服务器则使用基于 PCIe 的 GPU 。

下表还列出了可用于这些服务器的建议 GPU 。

服务器	**GPU**
Cisco UCS C220 M6	NVIDIA T4
Cisco UCS C225 M6	NVIDIA T4
Cisco UCS C240 M6	NVIDIA Tesla A10 ， A100
Cisco UCS C245 M6	NVIDIA Tesla A10 ， A100

适用于 **Cisco UCS B** 系列刀片式服务器的 **Cisco UCS VIC** 适配器

适用于 Cisco UCS B 系列刀片式服务器的 Cisco UCS 虚拟接口卡（Virtual Interface Card， VIC）适配器的技术规格包括以下组件：

- 上行链路端口数
- 每端口性能（IOPS）
- 电源
- 刀片式服务器端口数
- 硬件卸载
- 支持单根输入 / 输出虚拟化（SR-IOV）

所有当前经验证的 FlexPod 架构都使用 Cisco UCS VIC 。如果 NetApp 上列出了其他适配器，则支持这些适配器 "IMT" 和与您的 FlexPod 部署兼容，但它们可能无法提供相应参考架构中概述的所有功能。下表显示了 Cisco UCS VIC 适配器产品规格。

组件	**Cisco UCS** 产品规格
Cisco UCS 虚拟接口适配器	"Cisco UCS VIC 数据表"

Cisco UCS 互联阵列

Cisco UCS 互联阵列的技术规格包括外形规格大小，端口和扩展插槽总数以及吞吐量容量。下表显示了 Cisco UCS 互联阵列数据表。

组件	**Cisco UCS** 产品规格
Cisco UCS 6248UP	"Cisco UCS 6200 系列互联阵列"
Cisco UCS 6296UP	
Cisco UCS 6324	"Cisco UCS 6324 互联阵列"
Cisco UCS 6300	"Cisco UCS 6300 系列互联阵列"
Cisco UCS 6454	"Cisco UCS 6400 系列互联阵列"

Cisco Nexus 5000 系列交换机

Cisco Nexus 5000 系列交换机的技术规格，包括外形规格大小，端口总数以及第 3 层模块和子卡支持，均包含在每个型号系列的数据表中。下表列出了这些数据表。

组件	**Cisco Nexus** 产品规格
Cisco Nexus 5548UP	"Cisco Nexus 5548UP 交换机"
Cisco Nexus 5596UP （2U）	"Cisco Nexus 5596UP 交换机"
Cisco Nexus 56128P	"Cisco Nexus 56128P 交换机"
Cisco Nexus 5672UP	"Cisco Nexus 5672UP 交换机"

Cisco Nexus 7000 系列交换机

Cisco Nexus 7000 系列交换机的技术规格（包括外形规格和最大端口数）包含在每个型号系列的产品规格中。下表列出了这些数据表。

组件	**Cisco Nexus** 产品规格
Cisco Nexus 7004	"Cisco Nexus 7000 系列交换机"
Cisco Nexus 7009	
Cisco Nexus 7010	
Cisco Nexus 7018	
Cisco Nexus 7702	"Cisco Nexus 7700 系列交换机"
Cisco Nexus 7706	
Cisco Nexus 7710	
Cisco Nexus 7718	

Cisco Nexus 9000 系列交换机

Cisco Nexus 9000 系列交换机的技术规格包含在每种型号的产品规格中。规格包括外形规格大小，监控器，光纤模块和线卡插槽的数量以及最大端口数量。下表列出了这些数据表。

组件	**Cisco Nexus** 产品规格
Cisco Nexus 9000 系列	"Cisco Nexus 9000 系列交换机"
Cisco Nexus 9500 系列	"Cisco Nexus 9500 系列交换机"
Cisco Nexus 9300 系列	"Cisco Nexus 9300 系列交换机"
Cisco Nexus 9336PQ ACI Spine 交换机	"Cisco Nexus 9336PQ ACI Spine 交换机"
Cisco Nexus 9200 系列	"Cisco Nexus 9200 平台交换机"

Cisco Application Policy Infrastructure 控制器

部署 Cisco ACI 时，除了一节中的各项之外 "Cisco Nexus 9000 系列交换机"，您必须配置三个 Cisco APIC 。下表列出了 Cisco APIC 产品规格。

组件	**Cisco Application Policy Infrastructure** 产品规格
Cisco 应用程序策略基础架构控制器	"Cisco APIC 产品规格"

Cisco Nexus 阵列扩展器详细信息

Cisco Nexus FEX 的技术规格包括速度，固定端口和链路的数量以及外形规格。

下表列出了 Cisco Nexus 2000 系列 FEX 产品规格。

组件	**Cisco Nexus** 阵列扩展器产品规格
Cisco Nexus 2000 系列阵列扩展器	"Nexus 2000 系列 FEX 产品规格"

SFP 模块

有关 SFP 模块的信息，请查看以下资源：

- 有关 Cisco 10 Gb SFP 的信息，请参见 "Cisco 万兆模块"。
- 有关 Cisco 25 Gb SFP 的信息，请参见 "Cisco 25 千兆模块"。
- 有关 Cisco QSFP 模块的信息，请参见 "Cisco 40GBASE QSFP 模块产品规格"。
- 有关 Cisco 100GB SFP 的信息，请参见 "Cisco 100 千兆模块"。
- 有关 Cisco FC SFP 模块的信息，请参见 "Cisco MDS 9000 系列可插拔收发器产品规格"。
- 有关所有受支持的 Cisco SFP 和收发器模块的信息，请参见 "《 Cisco SFP 和 SFP+ 收发器模块安装说明》" 和 "Cisco 收发器模块"。

NetApp 存储控制器

NetApp 存储控制器的技术规格包括以下组件：

- 机箱配置
- 机架单元数
- 内存量
- NetApp FlashCache 缓存
- 聚合大小
- 卷大小
- LUN 数量
- 支持的网络存储
- NetApp FlexVol 卷的最大数量
- 支持的最大 SAN 主机数
- 最大 Snapshot 副本数

FAS 系列

支持在 FlexPod 数据中心中使用所有可用型号的 FAS 存储控制器。有关所有 FAS 系列存储控制器的详细规格，请参见 "NetApp Hardware Universe"。有关特定 FAS 型号的详细信息，请参见下表中列出的平台专用文档。

组件	FAS 系列控制器平台文档
FAS9000 系列	"FAS9000 系列产品规格"
FAS8700 系列	"FAS8700 系列产品规格"
FAS8300 系列	"FAS8300 系列产品规格"
FAS500f 系列	"FAS500f 系列产品规格"
FAS2700 系列	"FAS2700 系列产品规格"

AFF A-Series

支持在 FlexPod 中使用所有当前型号的 NetApp AFF A 系列存储控制器。追加信息可在中找到 "AFF 技术规格" 数据表和中的 "NetApp Hardware Universe"。有关特定 AFF 型号的详细信息，请参见下表中列出的平台专用文档。

组件	**AFF A** 系列控制器平台文档
NetApp AFF A800	"AFF A800 平台文档"
NetApp AFF A700	"AFF A700 平台文档"
NetApp AFF A700s	"AFF A700s 平台文档"
NetApp AFF A400	"AFF A400 平台文档"
NetApp AFF A250	"AFF A250 平台文档"

AFF ASA A 系列

支持在 FlexPod 中使用所有当前型号的 NetApp AFF ASA A 系列存储控制器。追加信息可在所有 SAN 阵列文档资源， ONTAP AFF 全 SAN 阵列系统技术报告和 NetApp Hardware Universe 中找到。有关特定 AFF 型号的详细信息，请参见下表中列出的平台专用文档。

组件	**AFF A** 系列控制器平台文档
NetApp AFF ASA A800	"AFF ASA A800 平台文档"
NetApp AFF ASA A700	"AFF ASA A700 平台文档"
NetApp AFF ASA A400	"AFF ASA A400 平台文档"
NetApp AFF ASA A250	"AFF ASA A250 平台文档"
NetApp AFF ASA A220	"AFF ASA A220 平台文档"

NetApp 磁盘架

NetApp 磁盘架的技术规格包括外形规格大小，每个机箱的驱动器数量以及磁盘架 I/O 模块；下表提供了此文档。有关详细信息，请参见 "NetApp 磁盘架和存储介质技术规格" 和 "NetApp Hardware Universe"。

组件	**NetApp FAS/AFF** 磁盘架文档
NetApp DS212C 磁盘架	"DS212C 磁盘架文档"
NetApp DS224C 磁盘架	"DS224C 磁盘架文档"
NetApp DS460C 磁盘架	"DS460C 磁盘架文档"
NetApp NS224 NVMe-SSD 磁盘架	"NS224 磁盘架文档"

NetApp 驱动器

NetApp 驱动器的技术规格包括外形规格大小，磁盘容量，磁盘 RPM ，支持控制器和 ONTAP 版本要求。这些规格可在的驱动器部分中找到 "NetApp Hardware Universe"。

旧设备

FlexPod 是一款灵活的解决方案，可让您使用当前由 Cisco 和 NetApp 销售的现有设备和新设备。有时， Cisco 和 NetApp 的某些型号设备会被指定为寿命终结（ EOL ）。

即使这些设备型号已不再可用，但如果您在可用性终止（ EOA ）日期之前购买了其中一种型号，则可以在 FlexPod 配置中使用该设备。有关 FlexPod 中支持的不再销售的原有设备型号的完整列表，请参见 "NetApp 服务和支持产品计划的可用性终止索引"。

有关原有 Cisco 设备的详细信息，请参见的 Cisco EOL 和 EOA 通知 "Cisco UCS C 系列机架式服务器"，"Cisco UCS B 系列刀片式服务器"，和 "Nexus 交换机"。

原有 FC 网络结构支持包括以下内容：

- 2 GB 网络结构
- 4 GB 网络结构

原有软件包括以下内容：

- 在 7- 模式， 7.3.5 及更高版本下运行的 NetApp Data ONTAP
- ONTAP 8.1.x 至 9.0.x
- Cisco UCS Manager 1.3 及更高版本
- Cisco UCS Manager 2.1 至 2.2.7

从何处查找追加信息

要了解有关本文档所述信息的更多信息，请查看以下文档和网站：

- NetApp 产品文档

  "https://docs.netapp.com/"

- NetApp 支持沟通

  "https://mysupport.netapp.com/info/communications/index.html"

- NetApp 互操作性表工具（ IMT ）

  "https://mysupport.netapp.com/matrix/#welcome"

- NetApp Hardware Universe

  "https://hwu.netapp.com/"

- NetApp 支持

  "https://mysupport.netapp.com/"

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

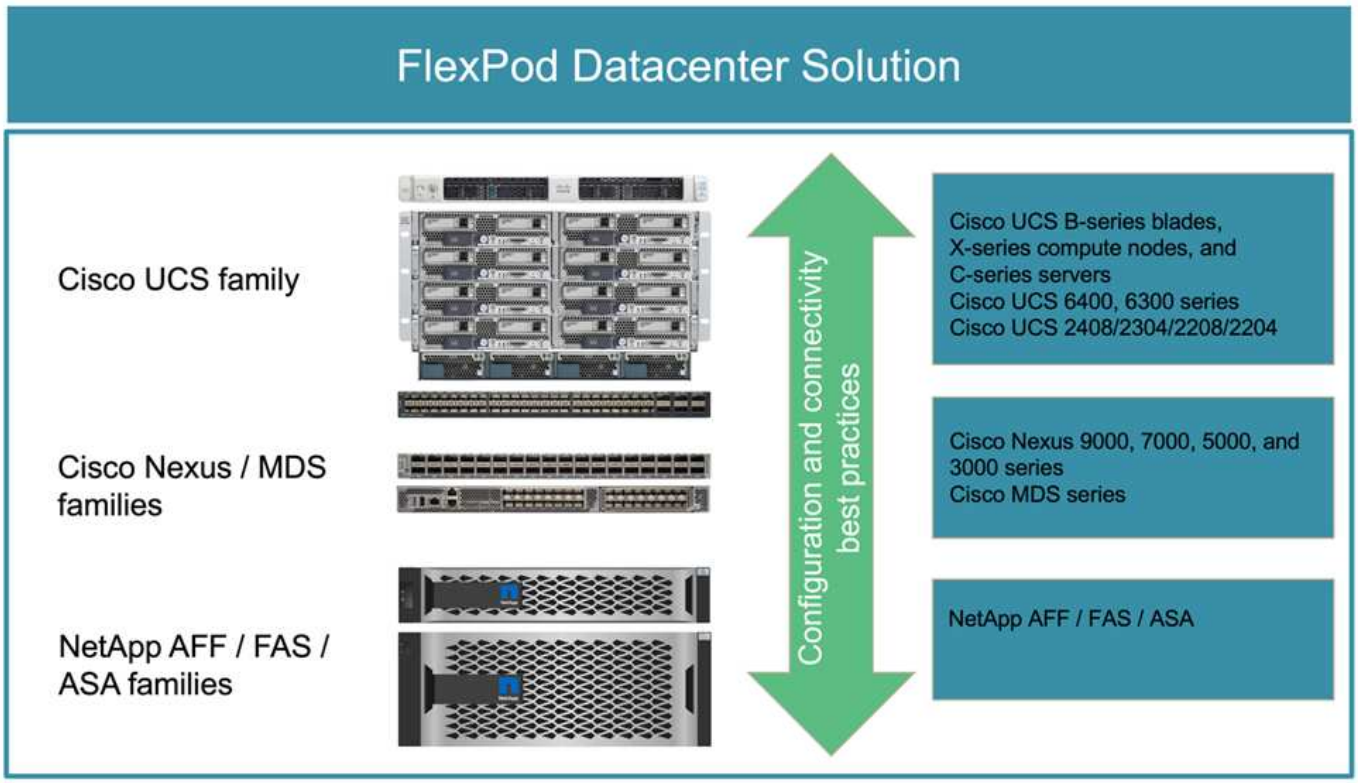
简介

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。

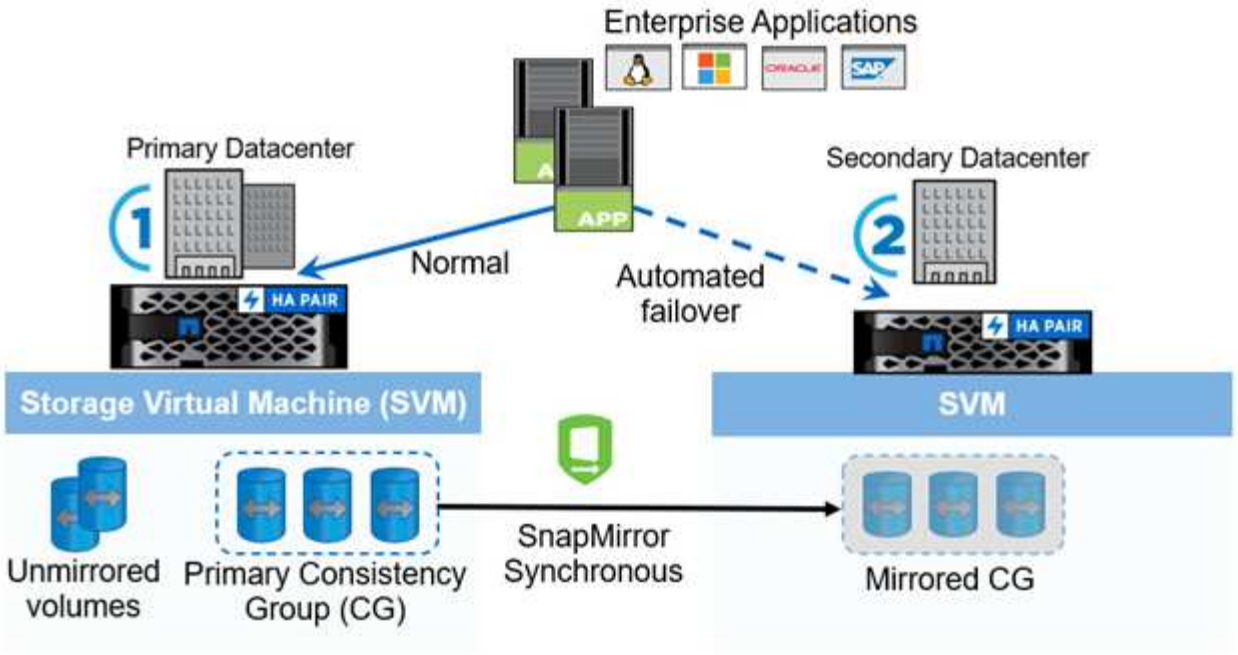
SM — BC

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

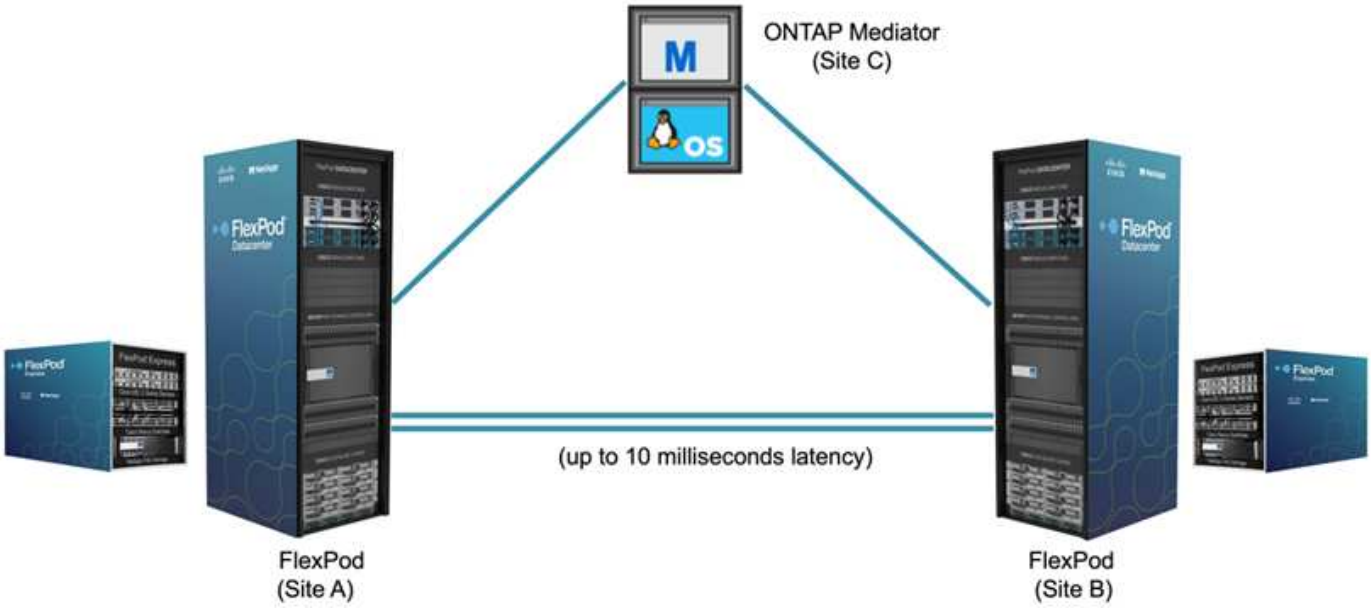
从较高的层面来看， FlexPod SM-BC 解决方案 由两个 FlexPod 系统组成，它们位于两个站点上，彼此连接并配对，可提供高度可用，高度灵活且高度可靠的数据中心解决方案 ，即使站点发生故障也能提供业务连续性。

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

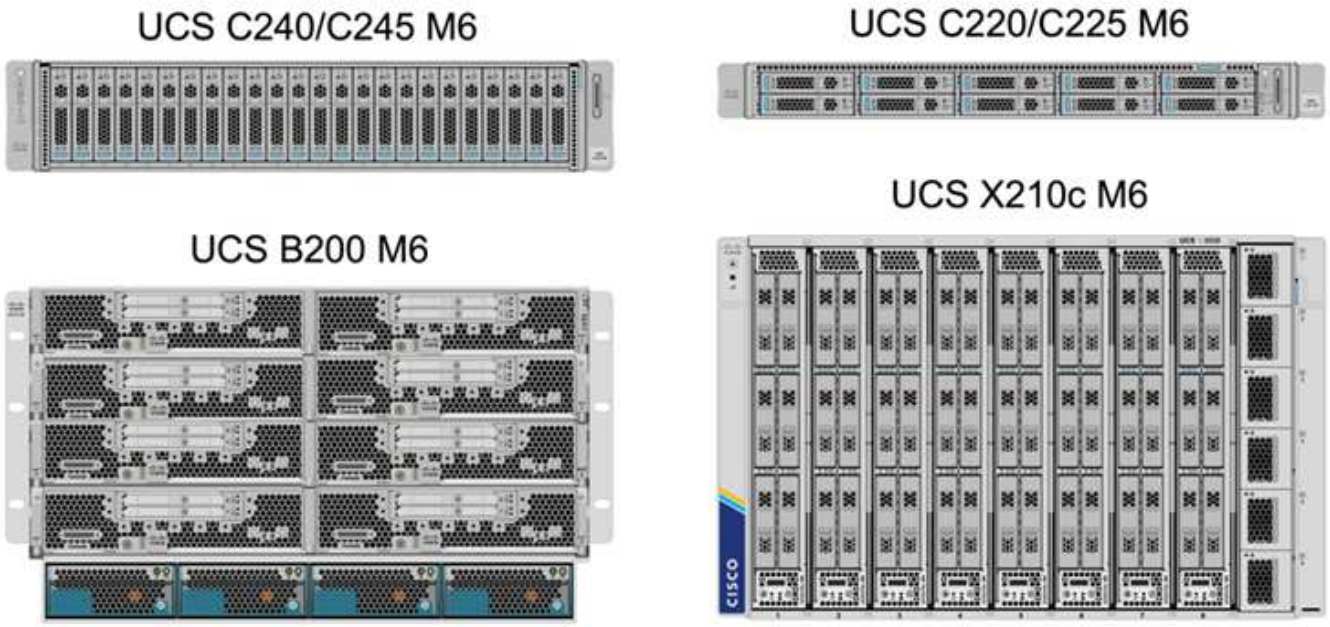
Cisco 计算组件

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。

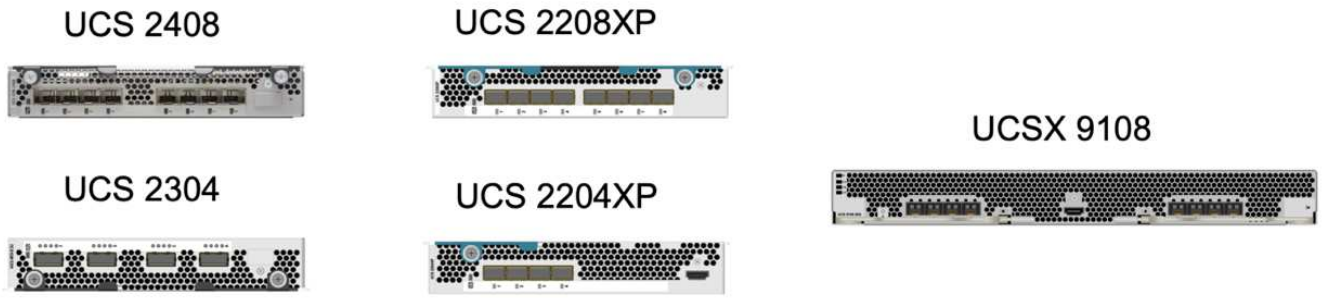
I/O 模块和智能网络结构模块

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。

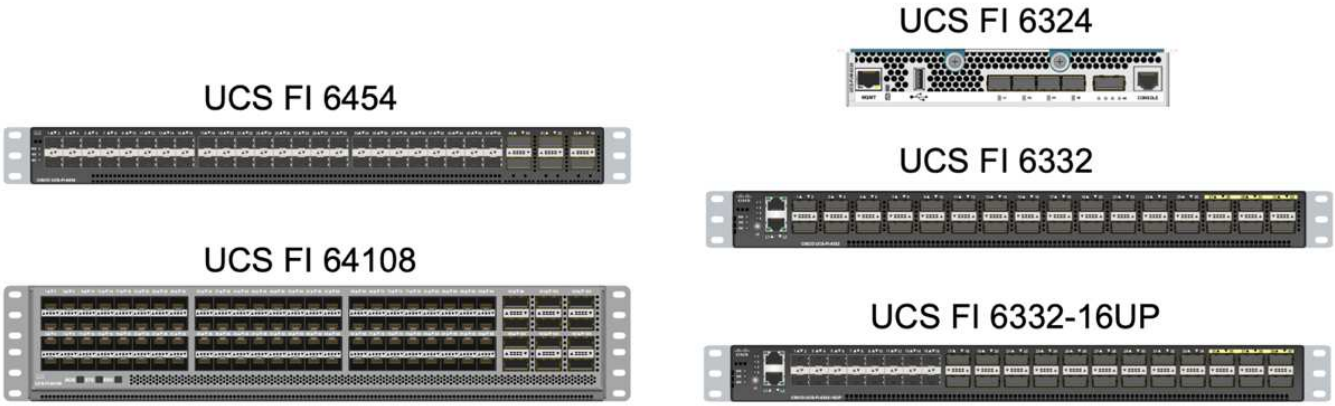
下图显示了 UCS 5108 机箱的 UCS 2408 及更早版本 IOM 以及 X9508 机箱的 9108 IFM 。



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。

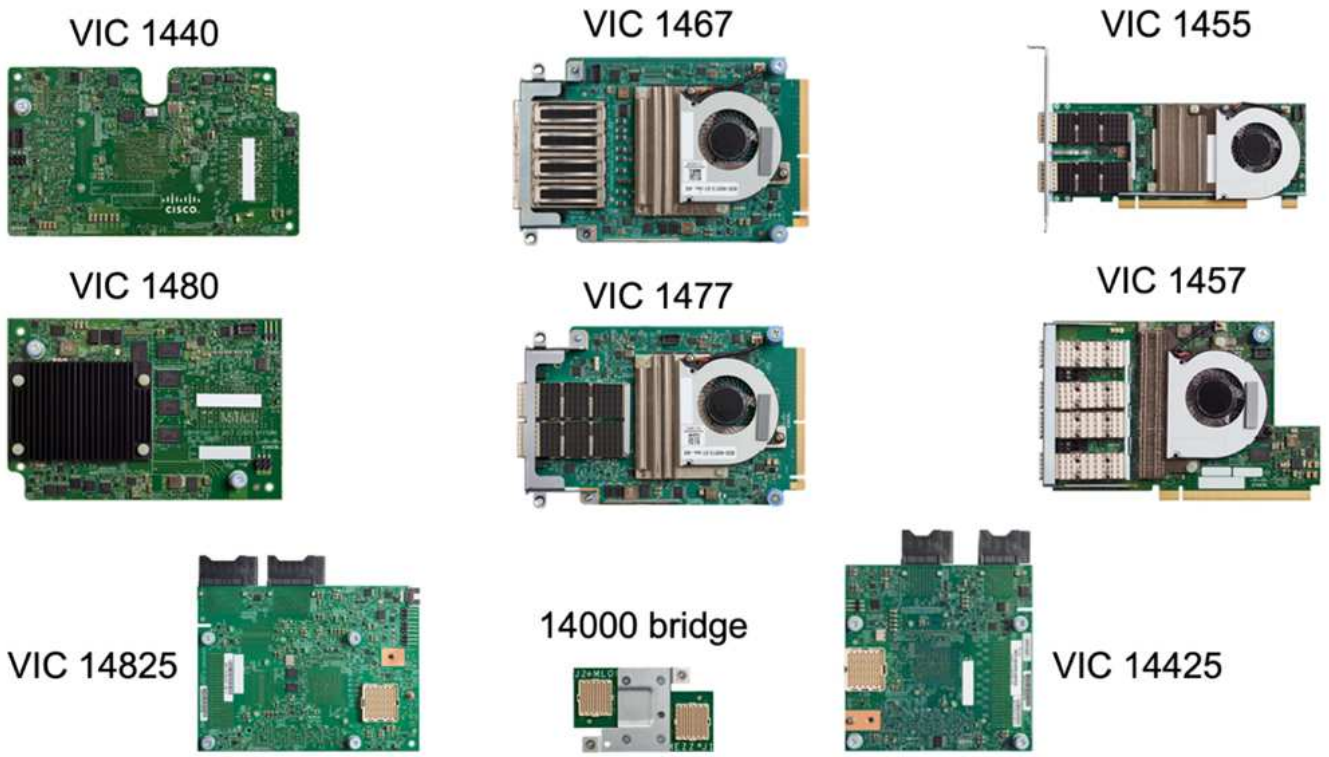


要支持 Cisco UCS X 系列机箱，需要在 Intersight Managed Mode （IMM）下配置第四代互联阵列。但是，在 IMM 模式和 UCSM 托管模式下均可支持 Cisco UCS 5108 B 系列机箱。

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 x 50-G + 2 x 50-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。

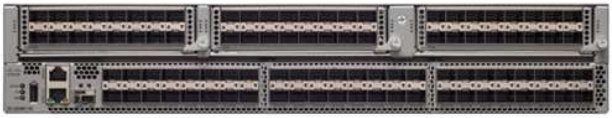
MDS 9132T

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

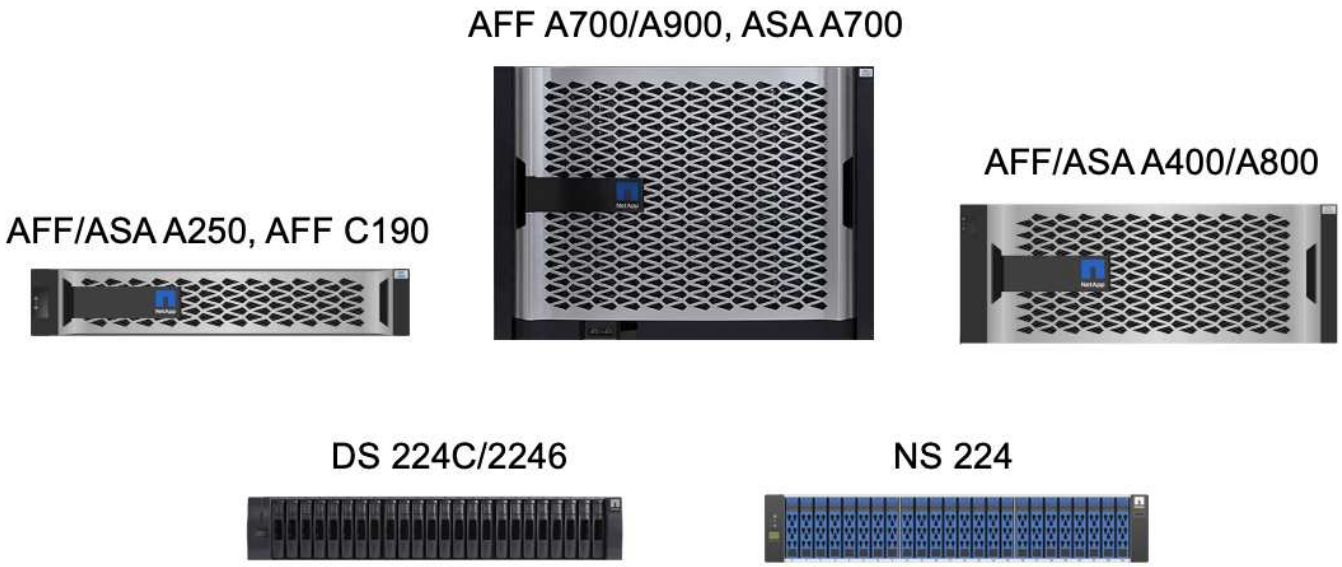
要创建 FlexPod SM-BC 解决方案 ，需要运行 ONTAP 软件 9.8 或更高版本的冗余 NetApp AFF 或 ASA 控制器。建议在 SM-BC 部署中使用最新的 ONTAP 版本（当前为 9.10.1 ），以便利用 ONTAP 持续创新，性能和质

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。

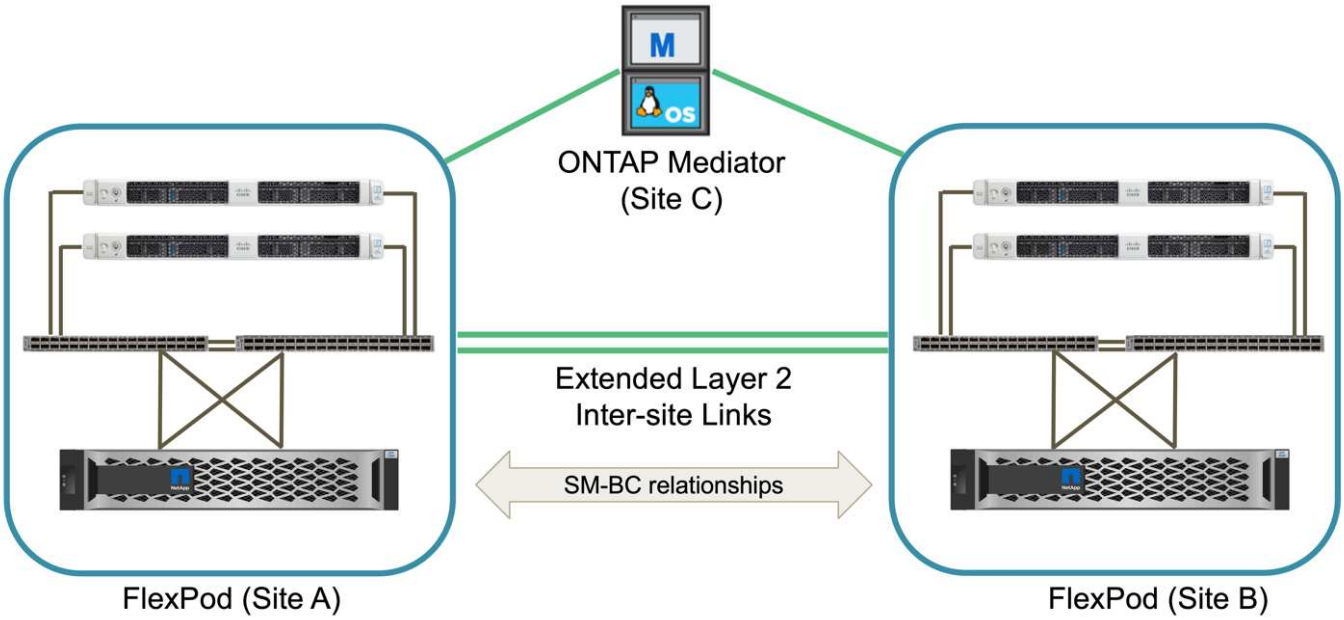


产品系列	技术规格
AFF 系列	"AFF 系列文档"
ASA 系列	"ASA 系列文档"

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。

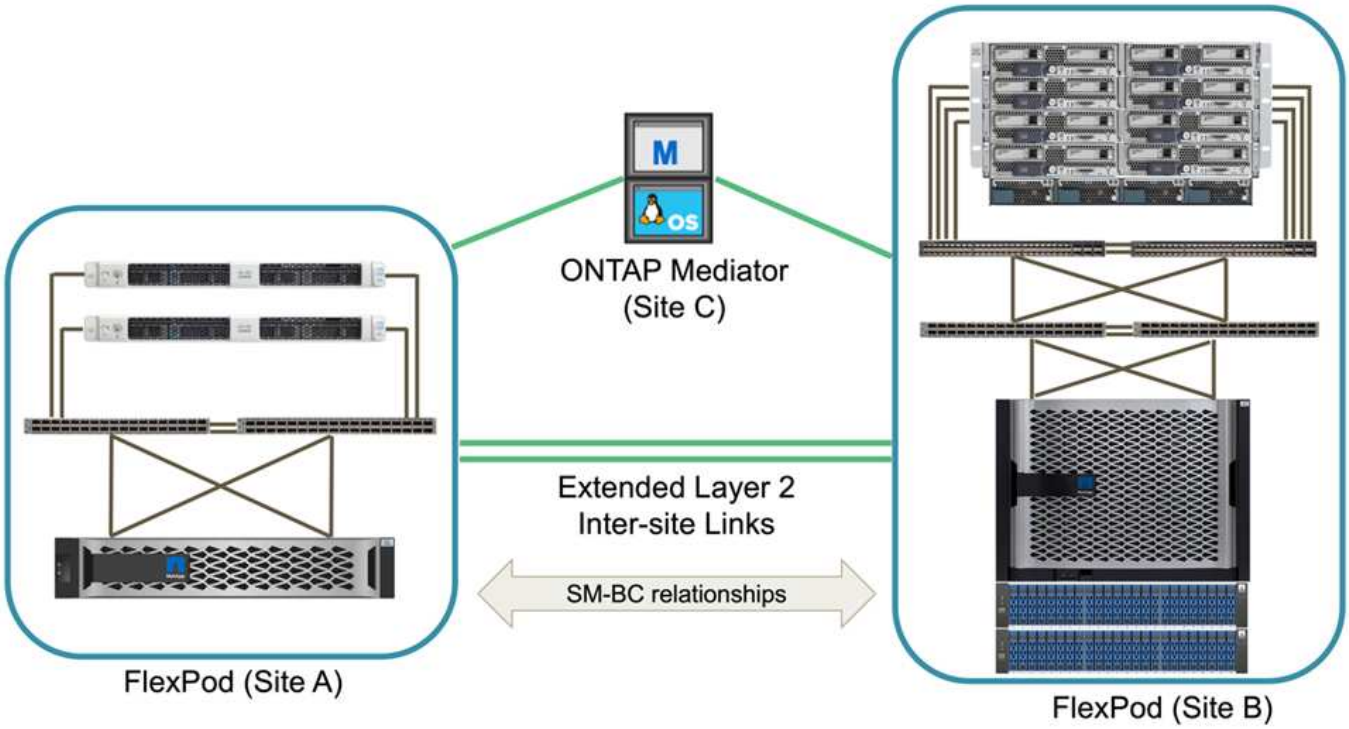
解决方案 拓扑

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。

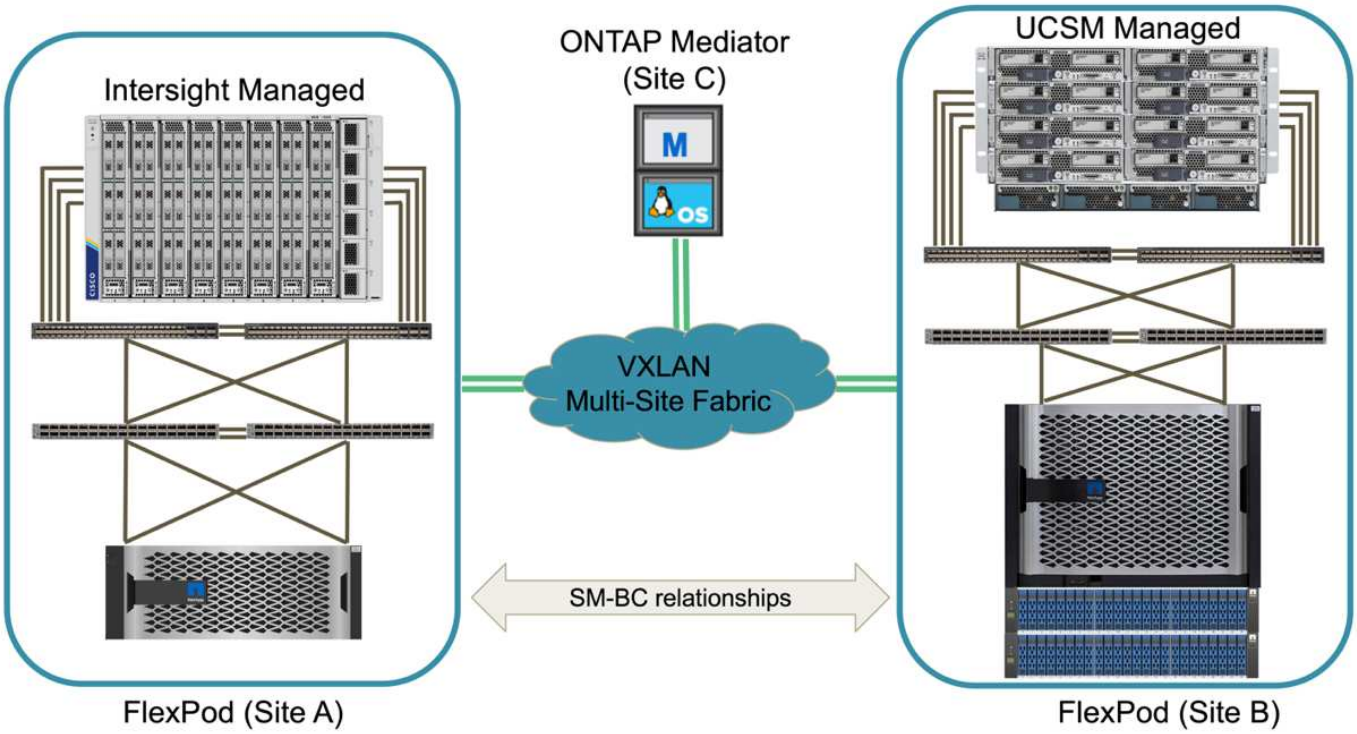
在城域中，数据中心和分支机构之间的公司可能使用的非对称部署拓扑可能如下图所示。对于这种非对称设计，数据中心需要具有更多计算和存储资源的更高性能 FlexPod 。但是，分支机构的需求较低，并且 FlexPod 可以小得多。



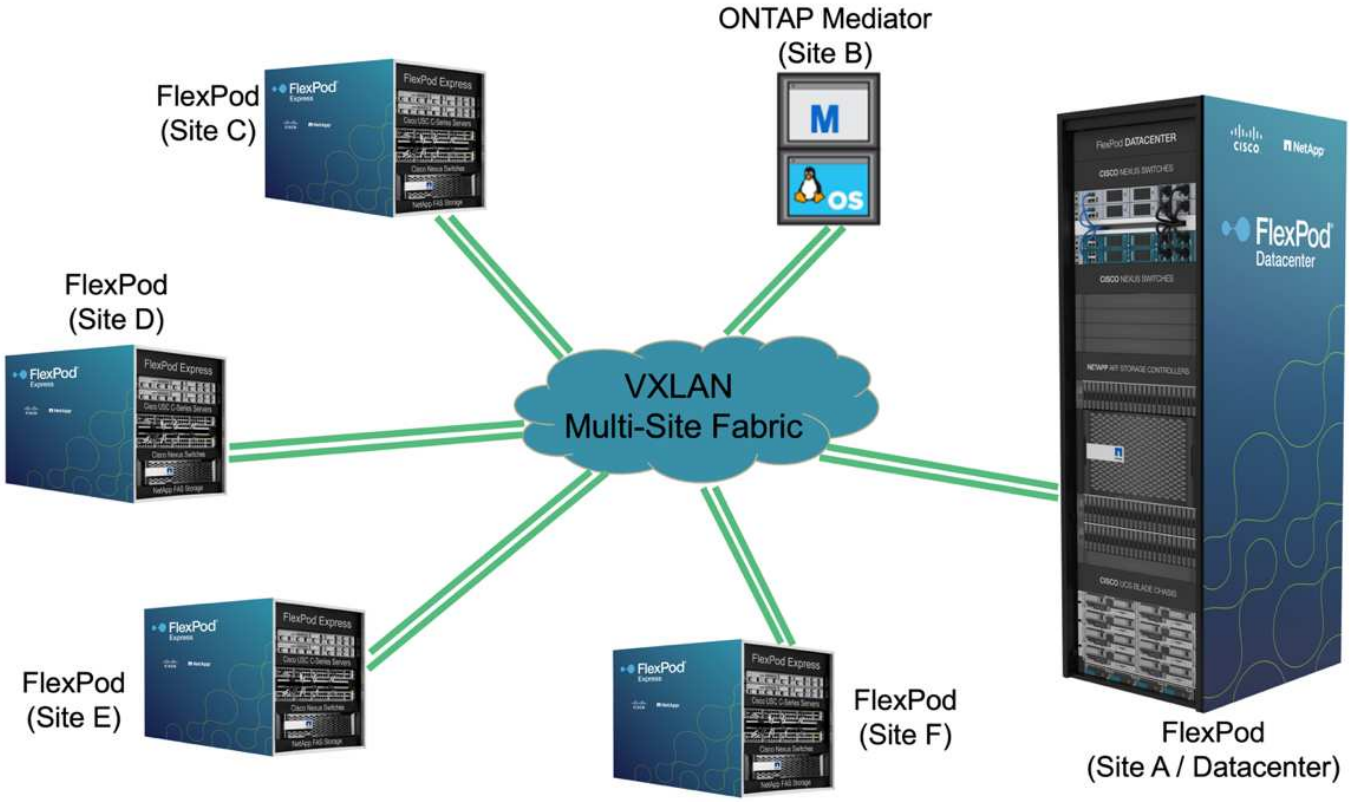
对于计算和存储资源需求较高的公司以及多个站点，基于 VXLAN 的多站点网络结构可以使多个站点拥有无缝网络结构，从而提高应用程序的移动性，从而可以从任何站点为应用程序提供服务。

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。



对于在城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

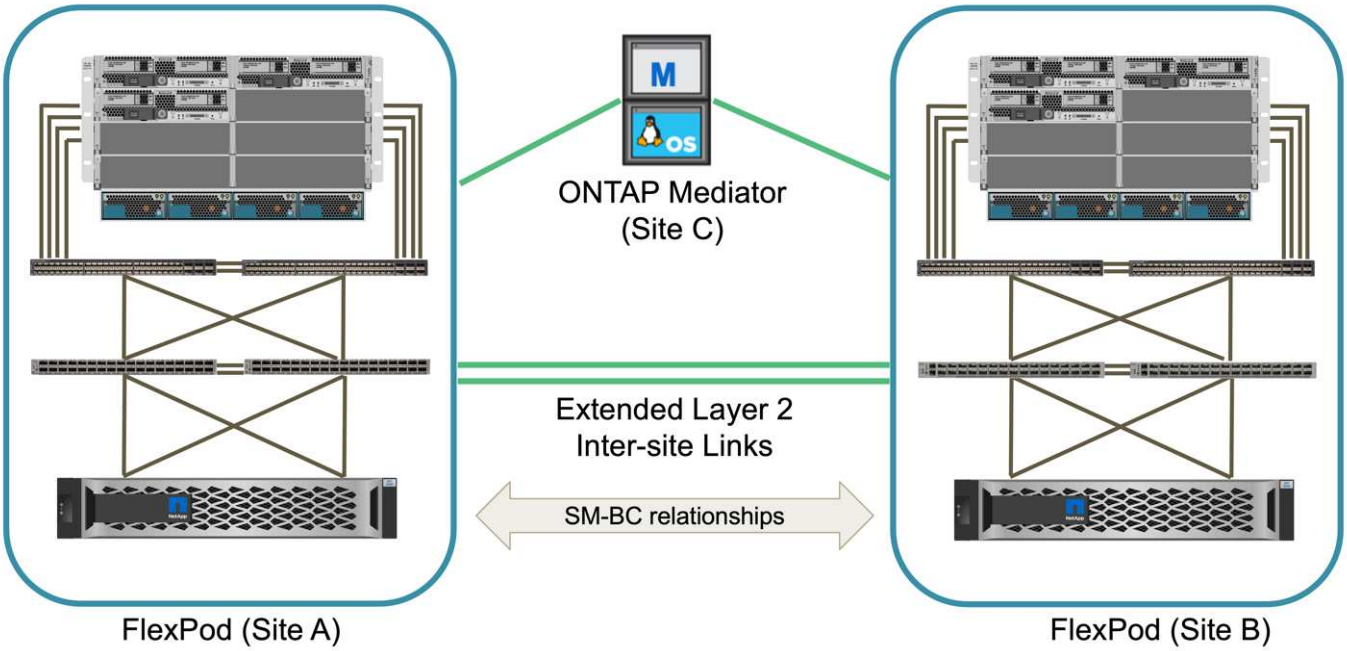
"先前版本： FlexPod SM-BC 解决方案 。"

FlexPod SM-BC 解决方案 的设计和实施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/"
- "Cisco UCS 硬件和软件互操作性工具"
- "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.
	NetApp 收获	21.11.1-1	1.
虚拟化	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。"

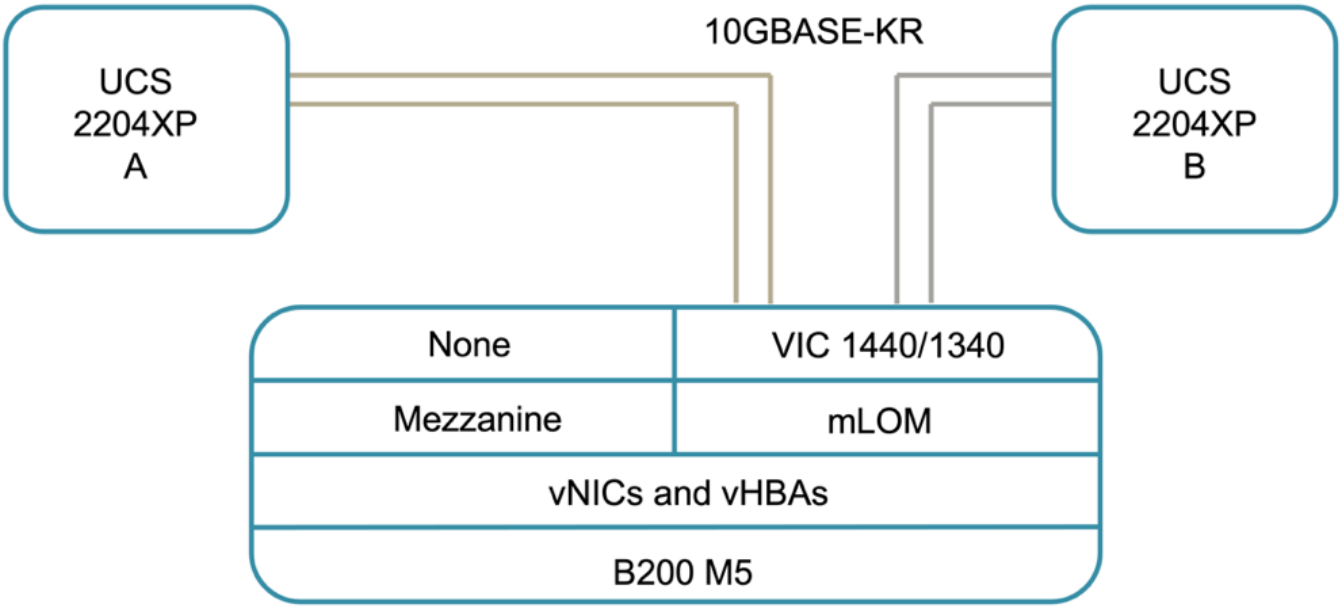
解决方案 验证—计算

"Preivous ： 解决方案 验证—概述。"

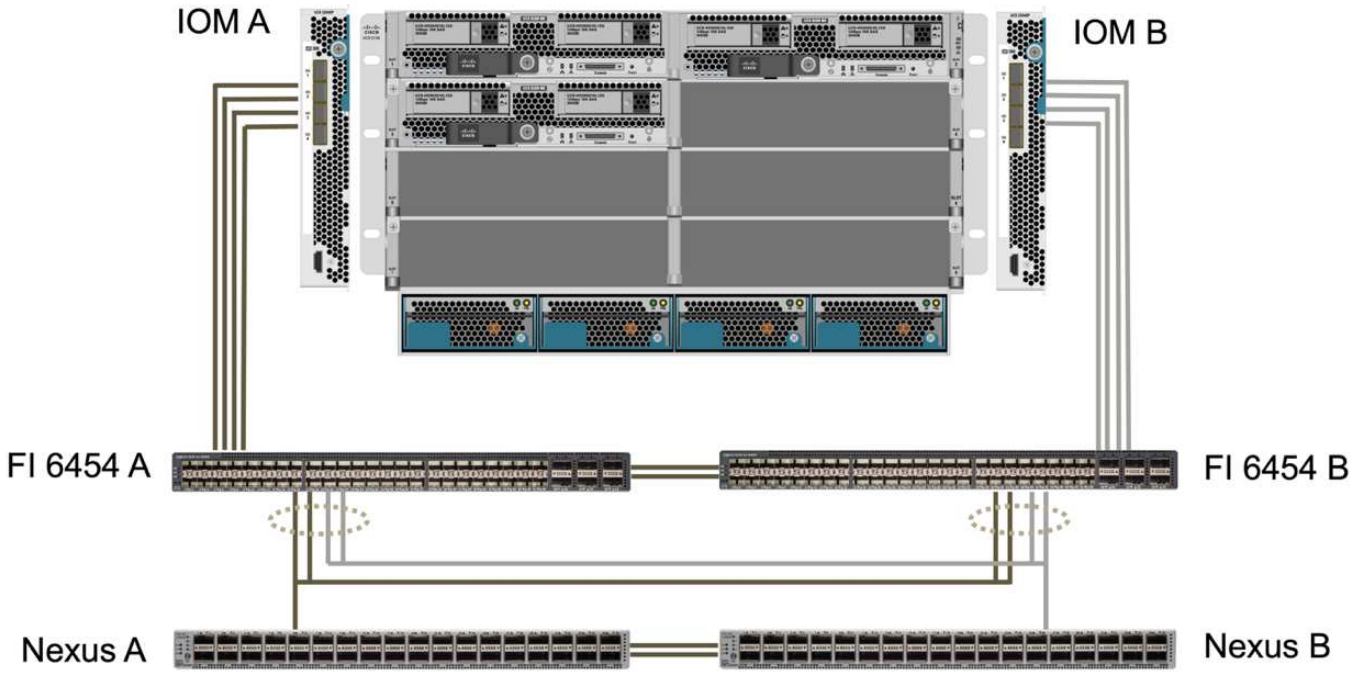
FlexPod SM-BC 解决方案 的计算配置遵循典型的 FlexPod 解决方案 最佳实践。以下各节重点介绍了用于验证的一些连接和配置。此外，还重点介绍了与 SM-BC 相关的一些注意事项，以提供实施参考和指导。

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
	L1	UCS 6454 FI B	L1
	L2		L2
UCS 6454 FI B	1.	IOM B	1.
	2.		2.
	3.		3.
	4.		4.
	25.	Nexus A	1/13/3
	26		1/13/4
	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。

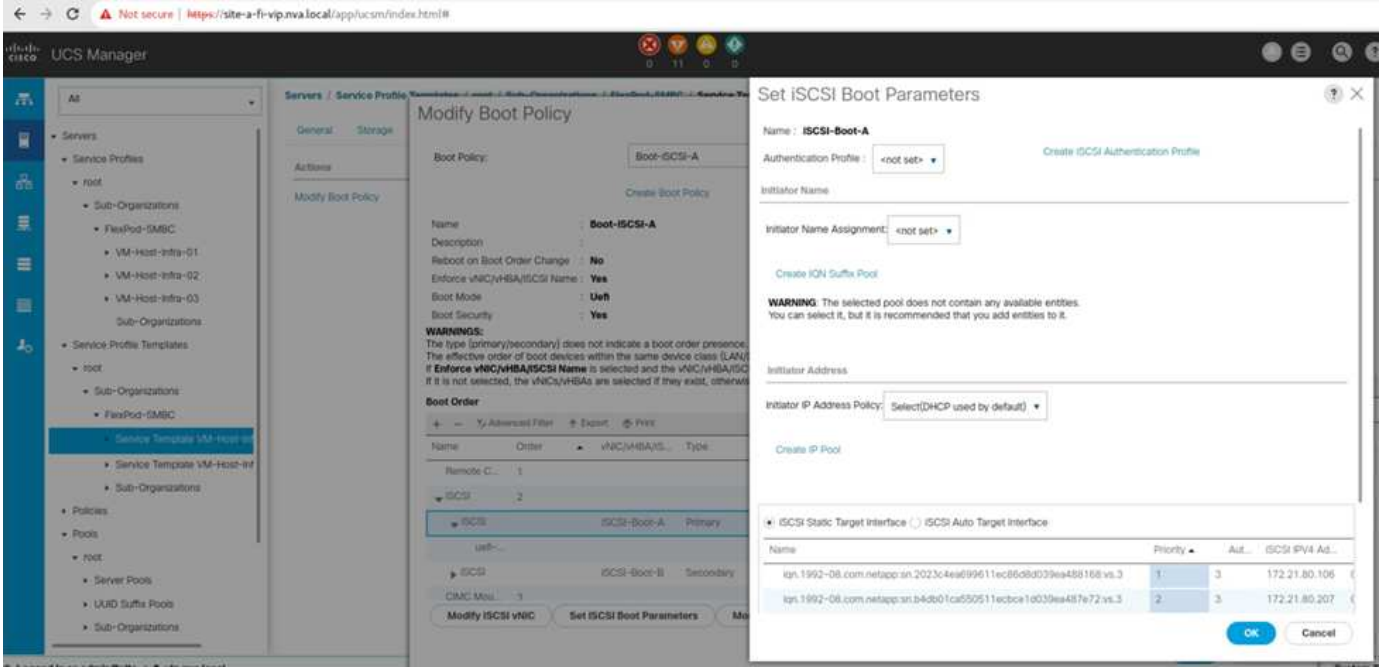
对于 VMware ESXi 主机，创建的服务配置文件支持以下功能：

- 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。"

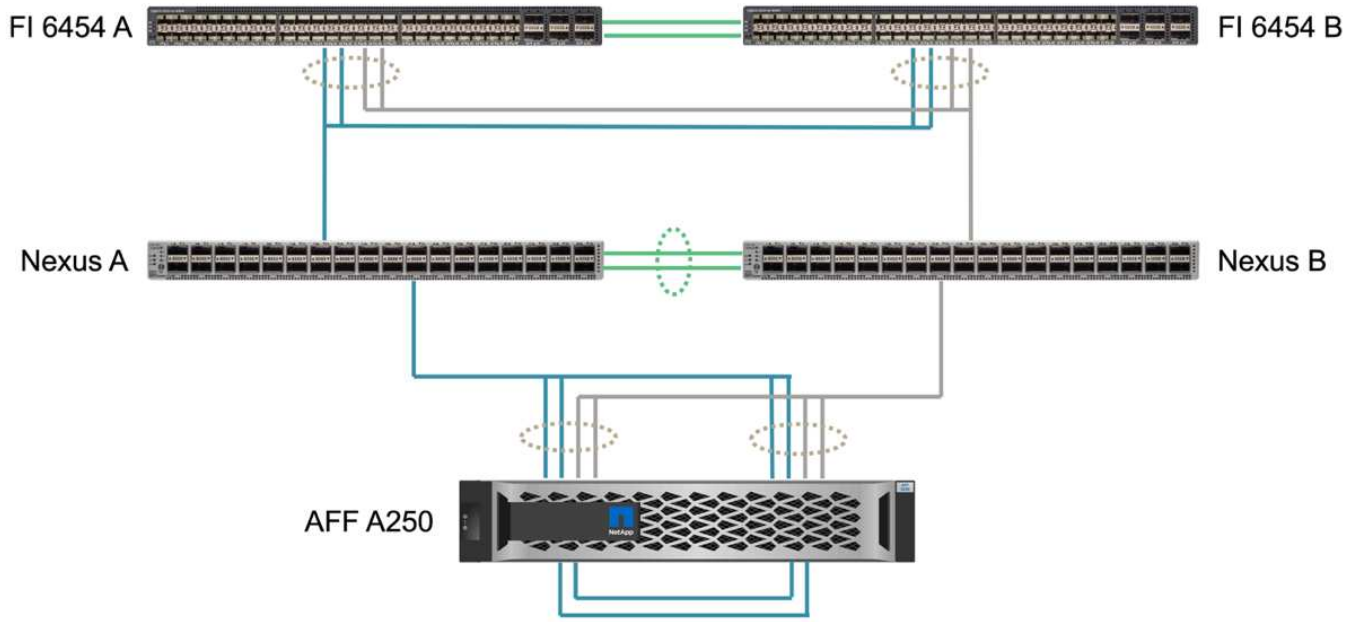
FlexPod SM-BC 解决方案 的网络配置遵循每个站点的典型 FlexPod 解决方案 最佳实践。对于站点间连接，解决方案 验证配置会将两个站点上的 FlexPod Nexus 交换机连接在一起，以提供站点间连接，从而扩展两个站点之间的 VLAN 。以下各节重点介绍了用于验证的一些连接和配置。

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

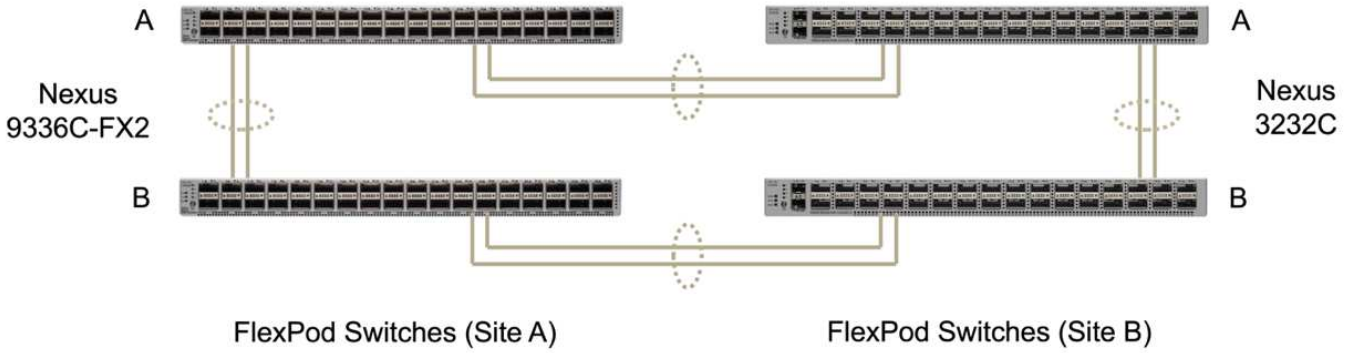
信速度。为了简单起见，这两个 AFF A250 控制器在逻辑上是并排显示的，用于布线图。两个存储控制器之间的两个连接允许存储形成无交换机集群。



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 IOM A 到 FI A 的路径，而 IOM B 到 FI B 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。"

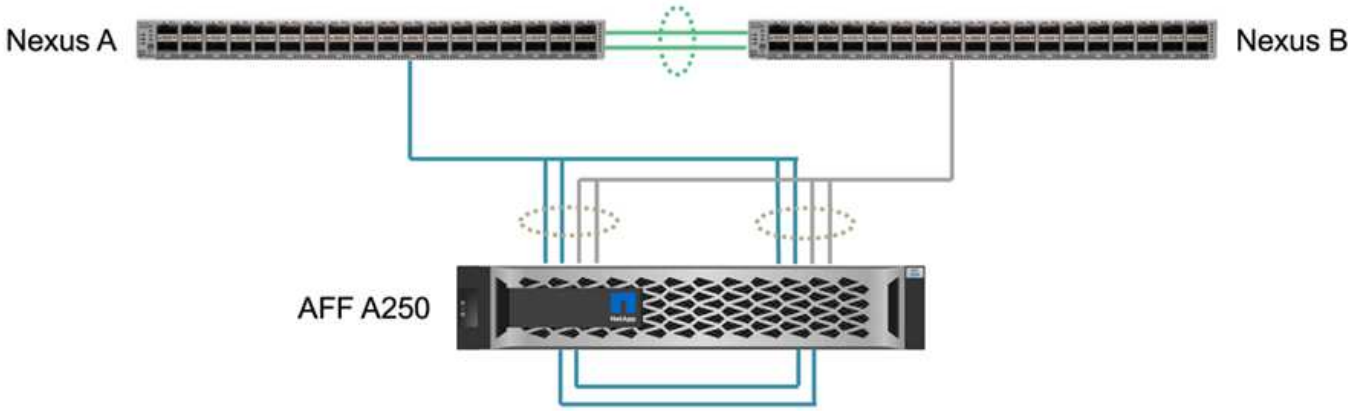
解决方案 验证—存储

"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。



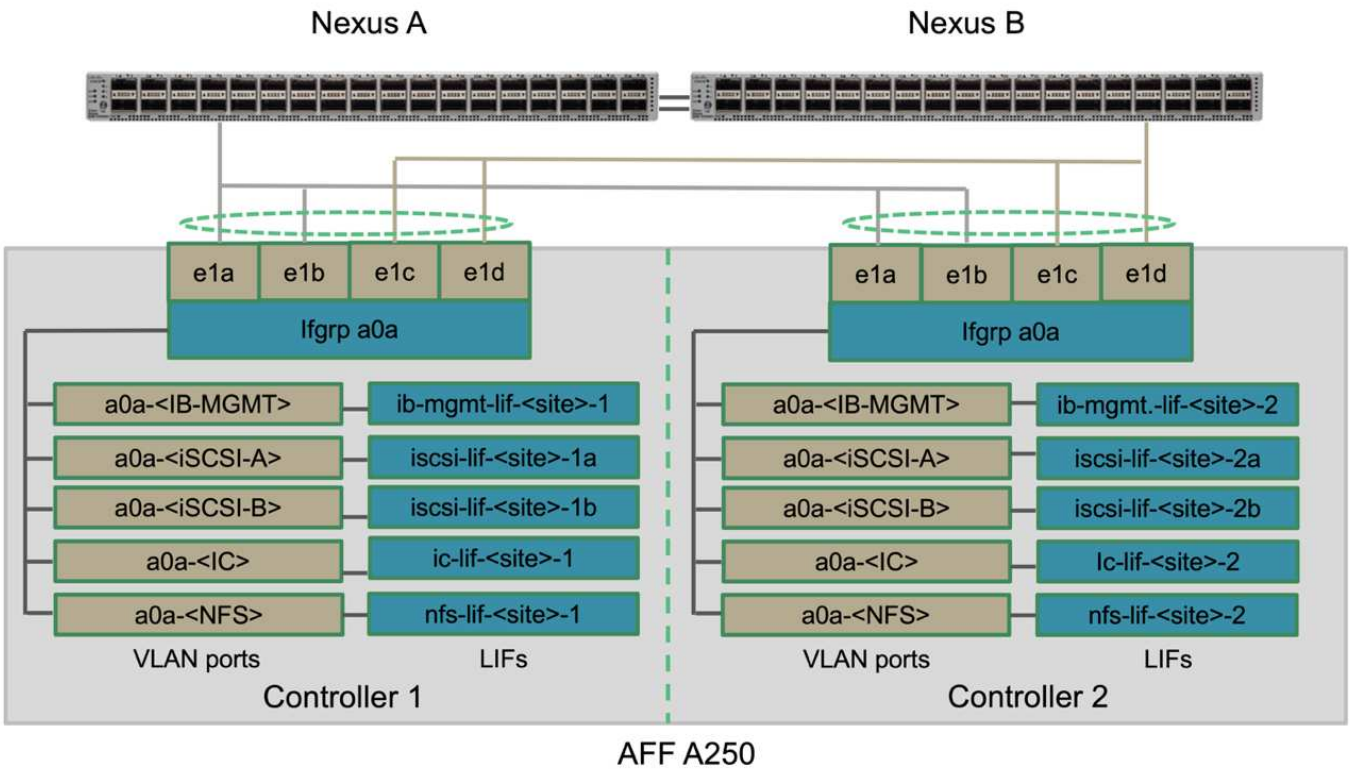
本地设备	本地端口	远程设备	远程端口
AFF A250 A	e0c	AFF A250 B	e0c
	e0d		e0d
	e1a	Nexus A	1 月 10 日
	e1b		1/2 年 10 月 1 日
	e1c	Nexus B	1 月 10 日
	e1d		1/2 年 10 月 1 日
AFF A250 B	e0c	AFF A250 A	e0c
	e0d		e0d
	e1a	Nexus A	3 月 1 日
	e1b		4 月 1 日
	e1c	Nexus B	3 月 1 日
	e1d		4 月 1 日

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。

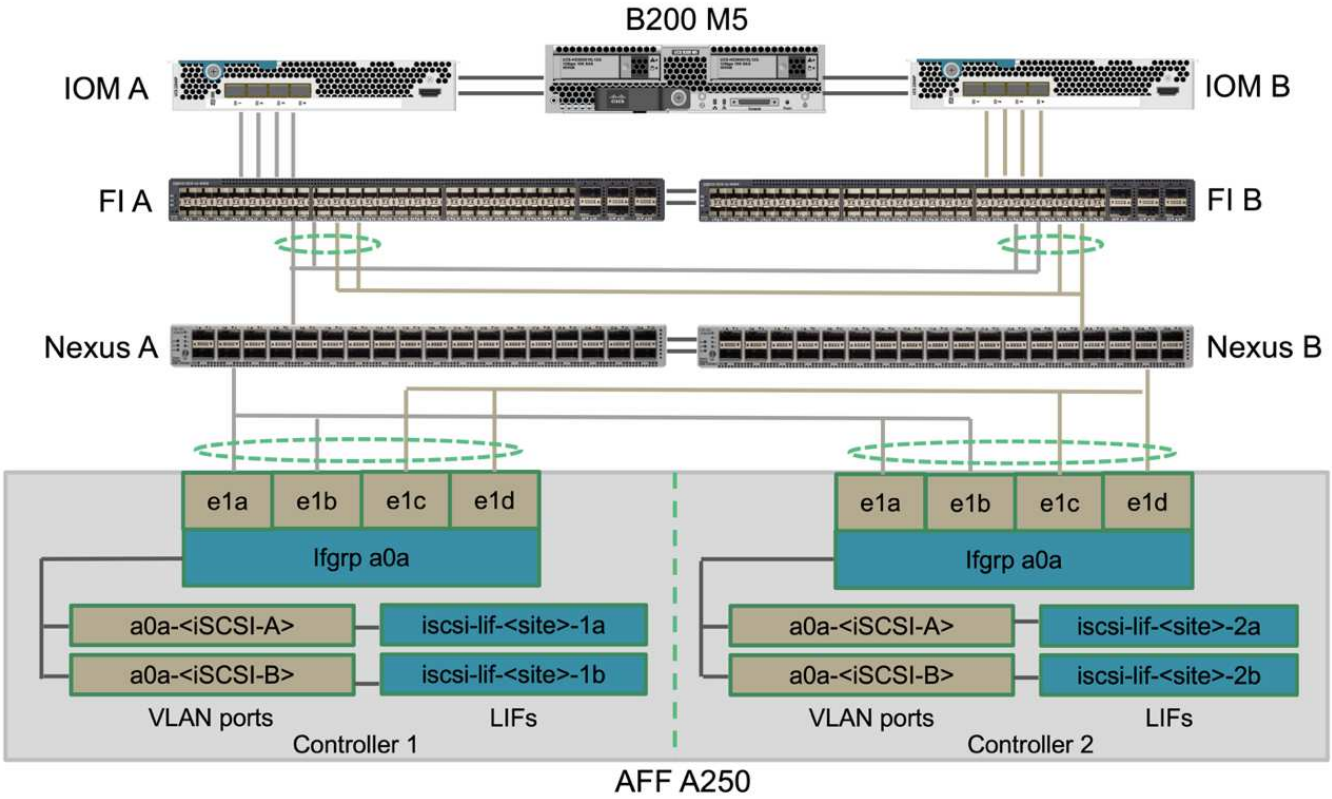


SAN 启动

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。

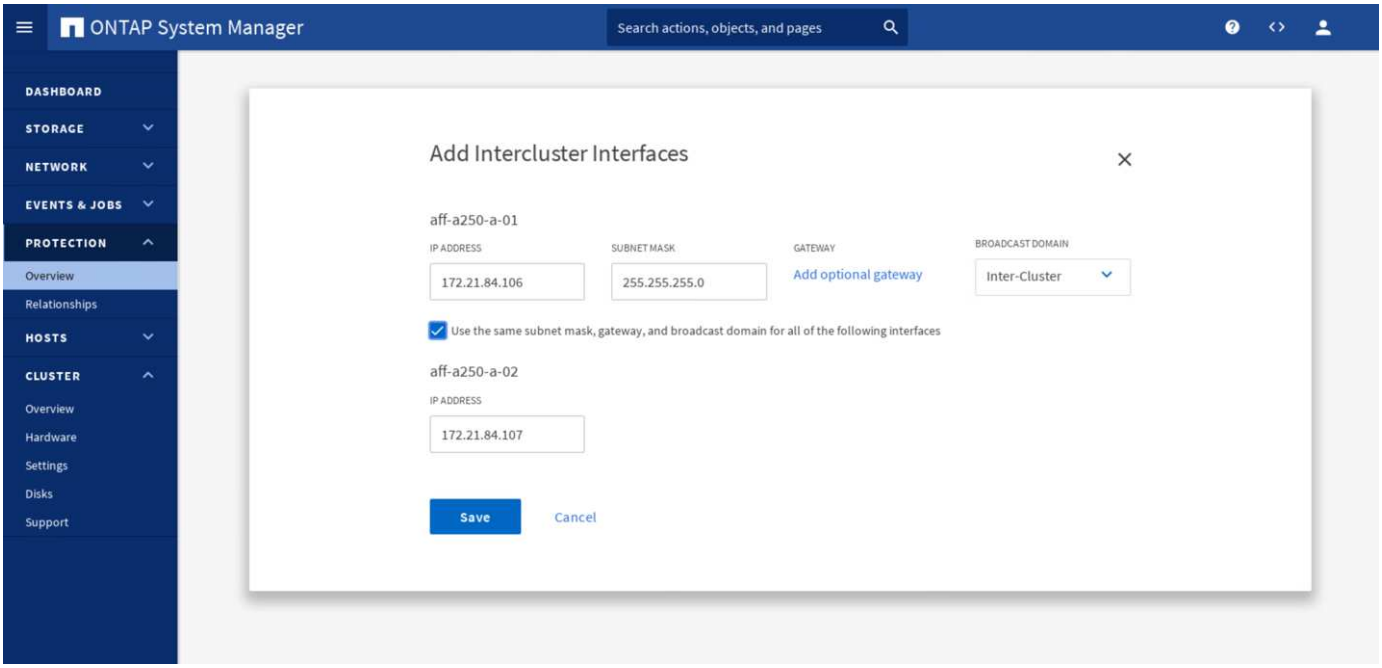
下图显示了从 NetApp 存储对 Cisco UCS 服务器进行 iSCSI SAN 启动的连接。在 iSCSI SAN 启动中，每个 Cisco UCS 服务器都分配有两个 iSCSI vNIC （每个 SAN 网络结构一个），用于提供从服务器一直到存储的冗余连接。连接到 Nexus 交换机（在此示例中为 e1a ， e1b ， e1c 和 e1d ）的 10/25G 以太网存储端口将分组在一起，形成一个接口组（ ifgrp ）（在此示例中为 a0a ）。iSCSI VLAN 端口在 ifgrp 上创建， iSCSI LIF 在 iSCSI VLAN 端口上创建。

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 。



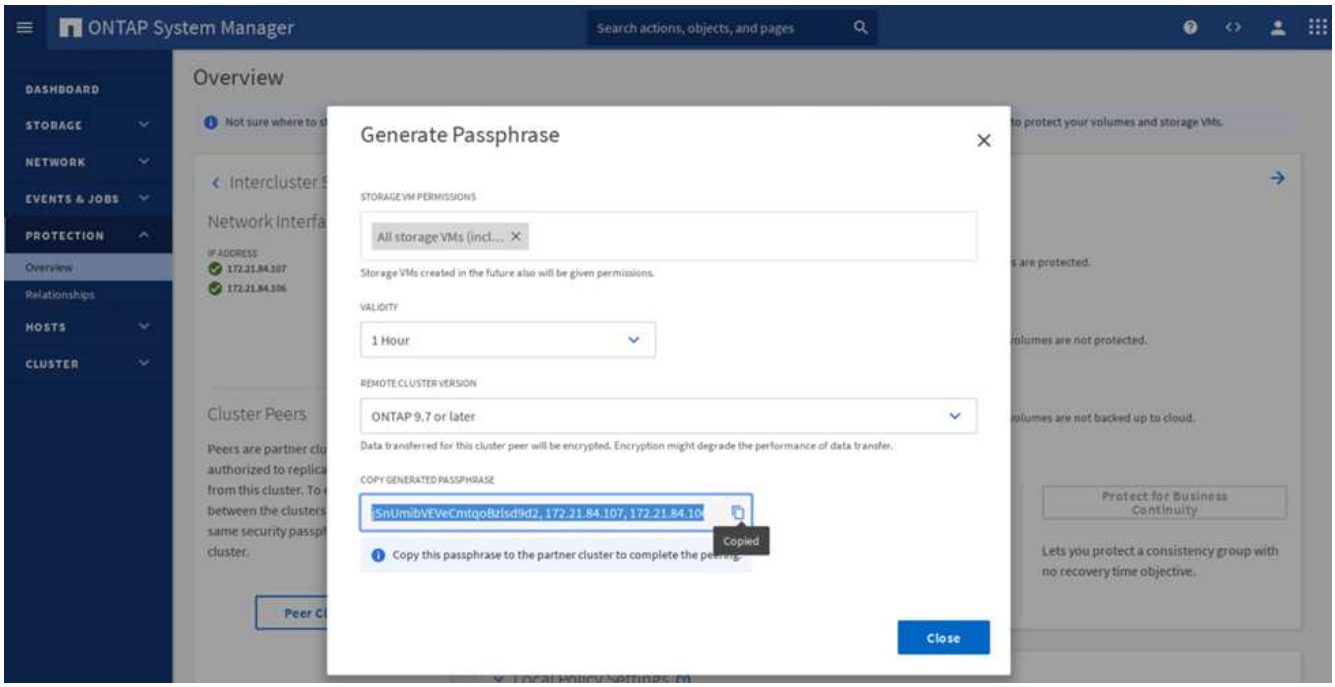
集群对等

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 。

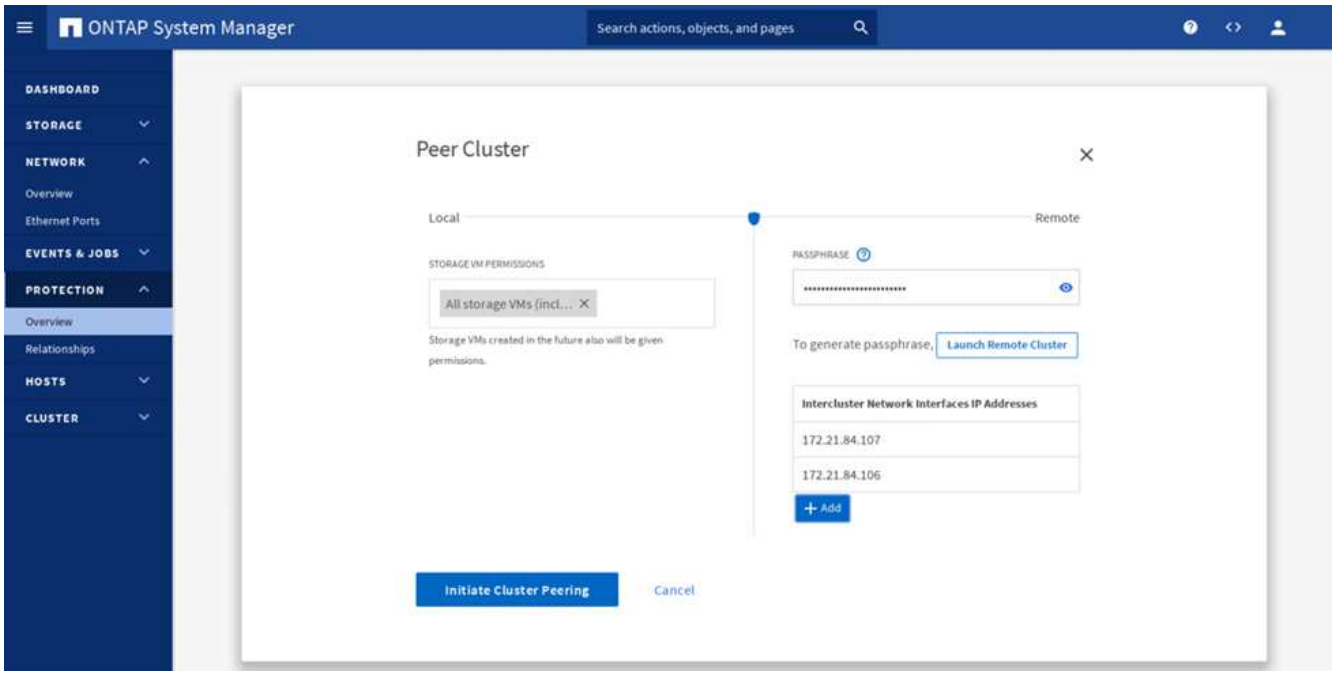


要将这两个集群建立对等关系，请完成以下步骤：

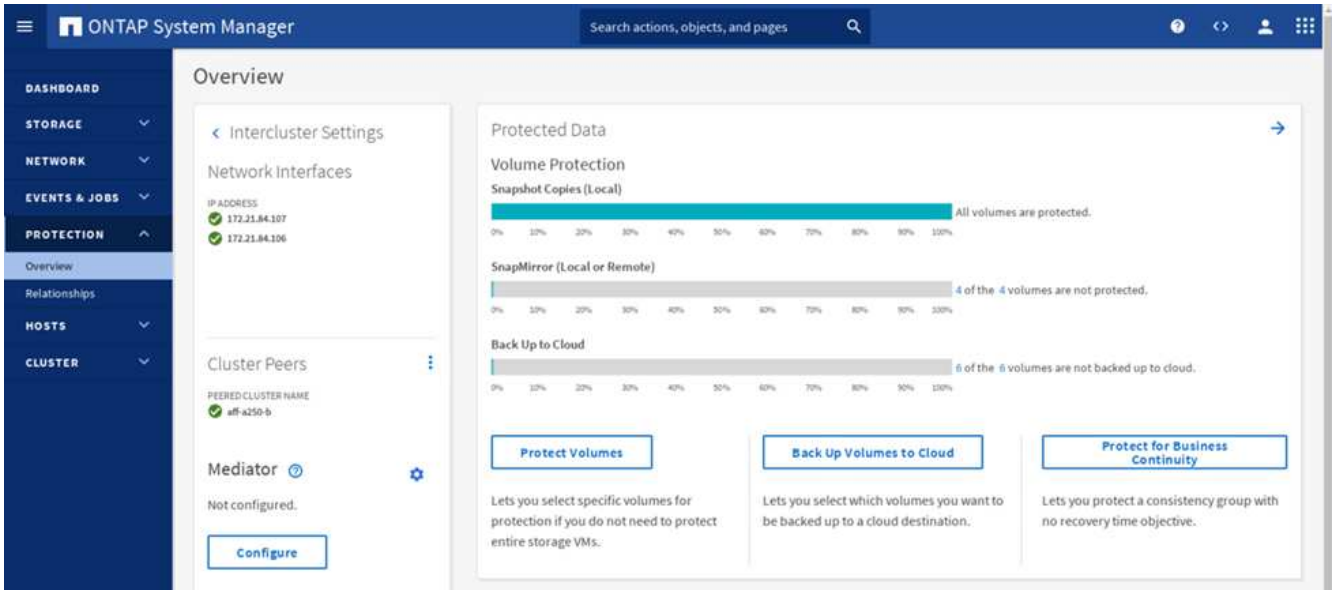
1. 在第一个集群中生成集群对等密码短语。



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。

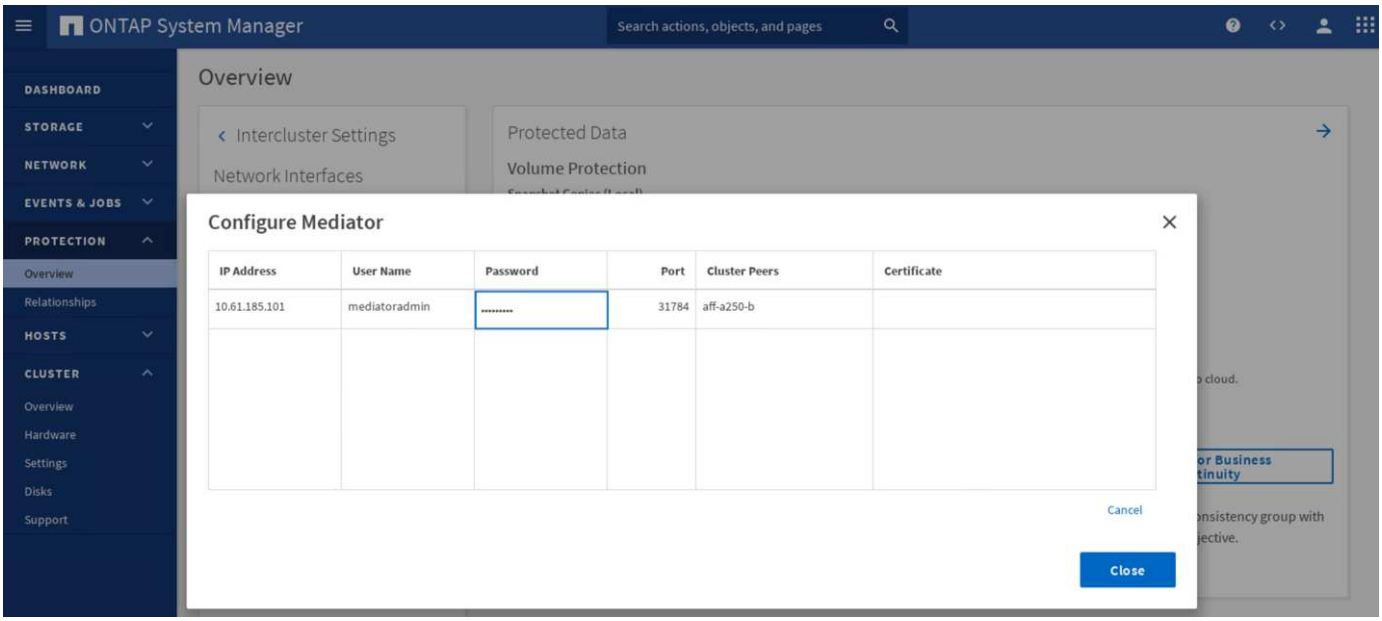


ONTAP 调解器安装和配置

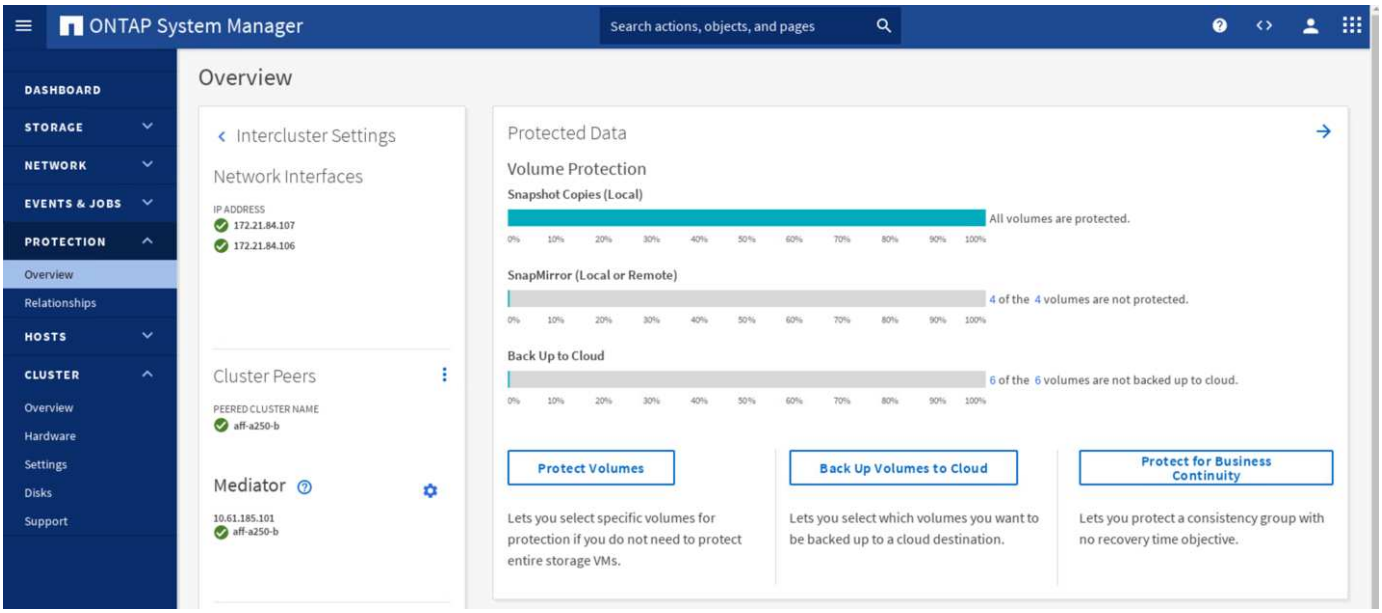
ONTAP 调解器为 SM-BC 关系中的 ONTAP 集群建立仲裁。它可以在检测到故障时协调自动故障转移，并有助于避免在每个集群同时尝试建立主集群控制时出现脑裂情况。

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。



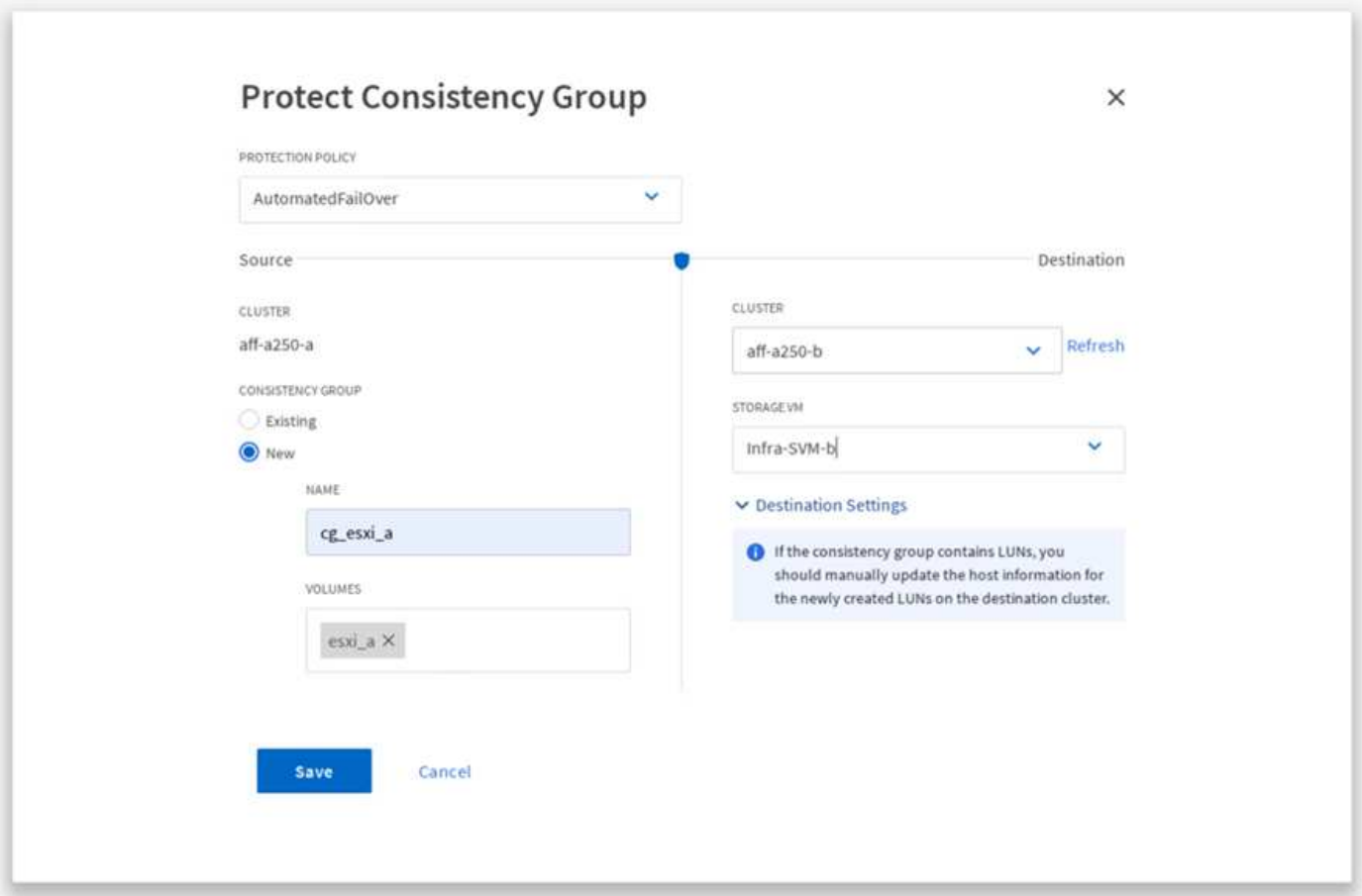
SM-BC 一致性组

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。

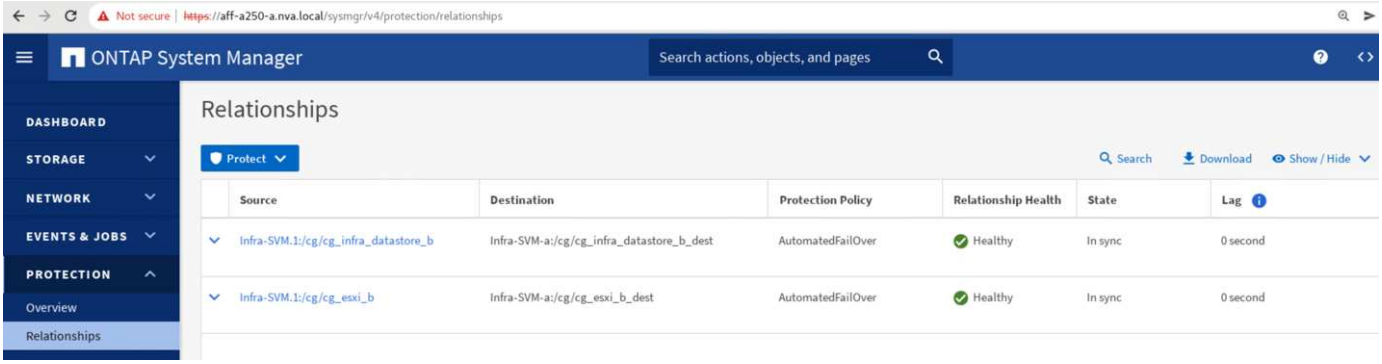


下表列出了验证测试中创建的四个一致性组以及每个一致性组中包含的卷。

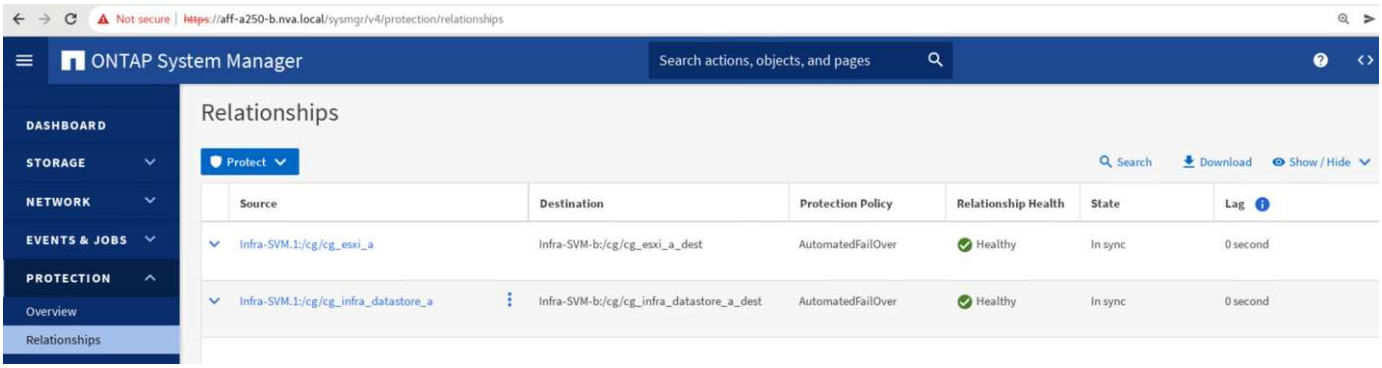
System Manager	一致性组	Volumes
站点 A	CG_ESXi_A	ESXi_A
站点 A	CG_infra_datastore_A	infra_datastore_A_01 infra_datastore_A_02
站点 B	CG_ESXi_b	ESXi b
站点 B	cG_infra_datastore_b.	infra_datastore_b_01 infra_datastore_b_02

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

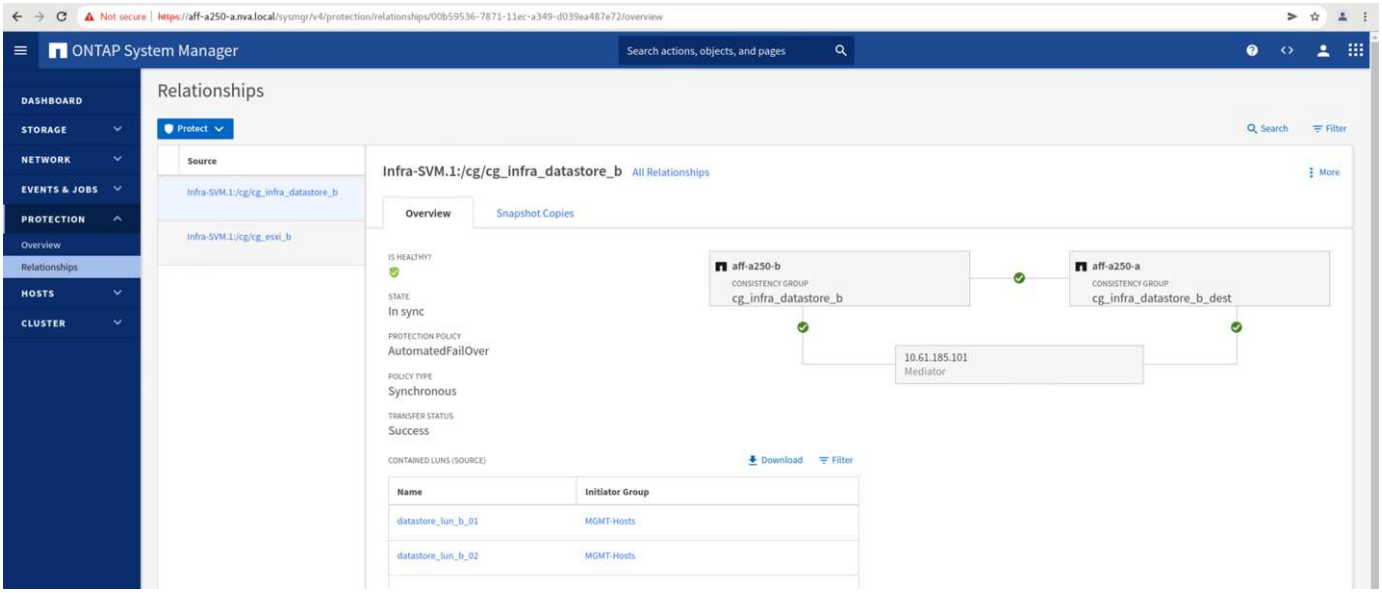
此屏幕截图显示了站点 A 上的一致性组关系



此屏幕截图显示了站点 B 上的一致性组关系



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



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。"

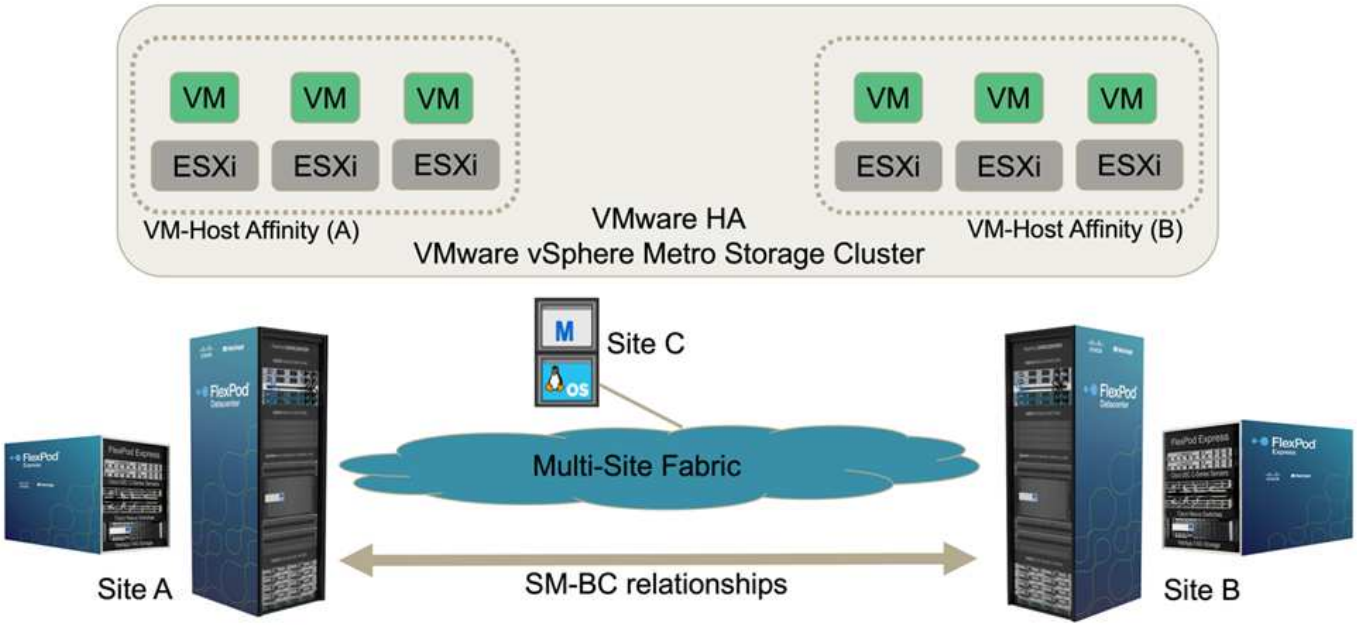
在多站点 FlexPod SM-BC 解决方案 中，一个 VMware vCenter 可管理整个解决方案 的虚拟基础架构资源。两个数据中心中的主机都属于一个 VMware HA 集群，该集群跨越两个数据中心。主机可以访问 NetApp SM-BC 解决方案 ，在此可以从两个站点访问具有定义的 SM-BC 关系的存储。

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。

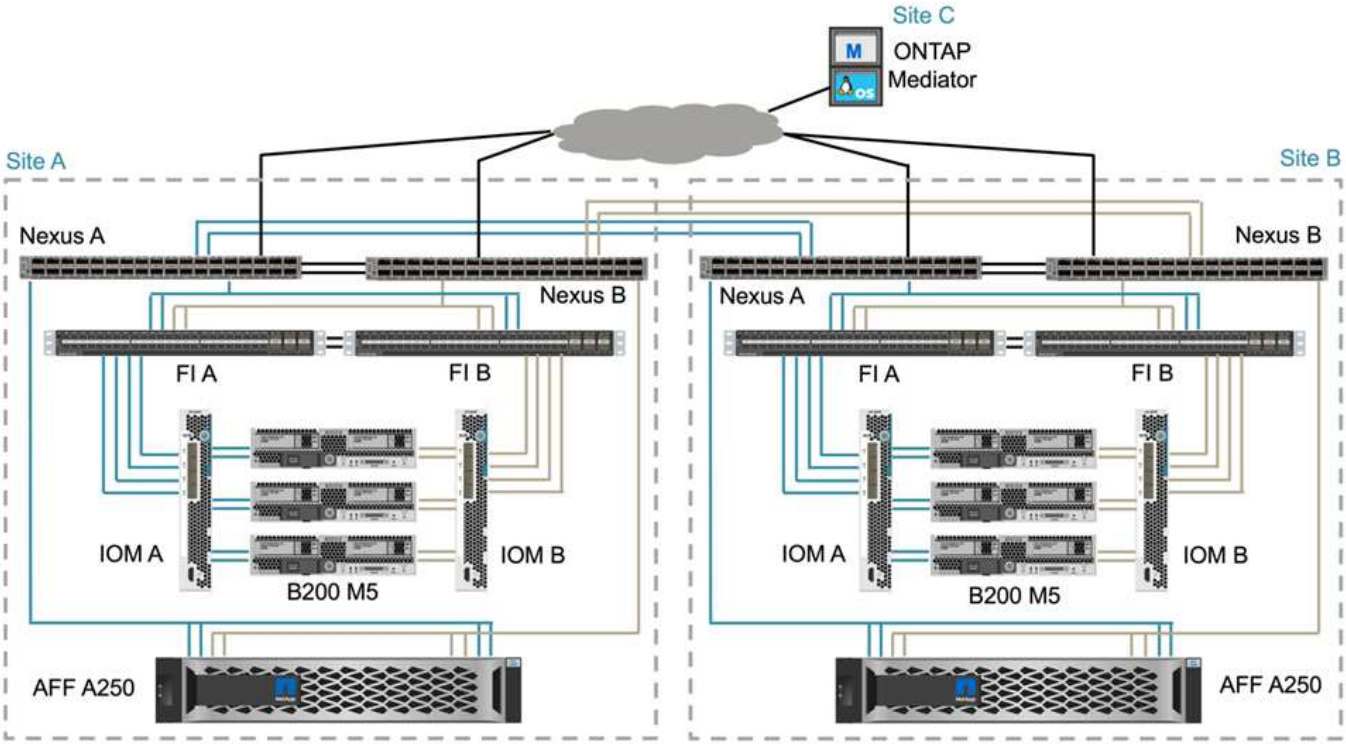
但是，如果配置允许 VM 在两个站点上运行，则可以确保 VM 可以通过远程站点主机上的 VMware HA 重新启动，以提供解决方案 故障恢复能力。要使虚拟机能够同时在两个站点上运行，必须在所有 ESXi 主机上挂载所有 iSCSI 共享数据存储库，以确保站点之间虚拟机的 vMotion 操作顺畅。

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

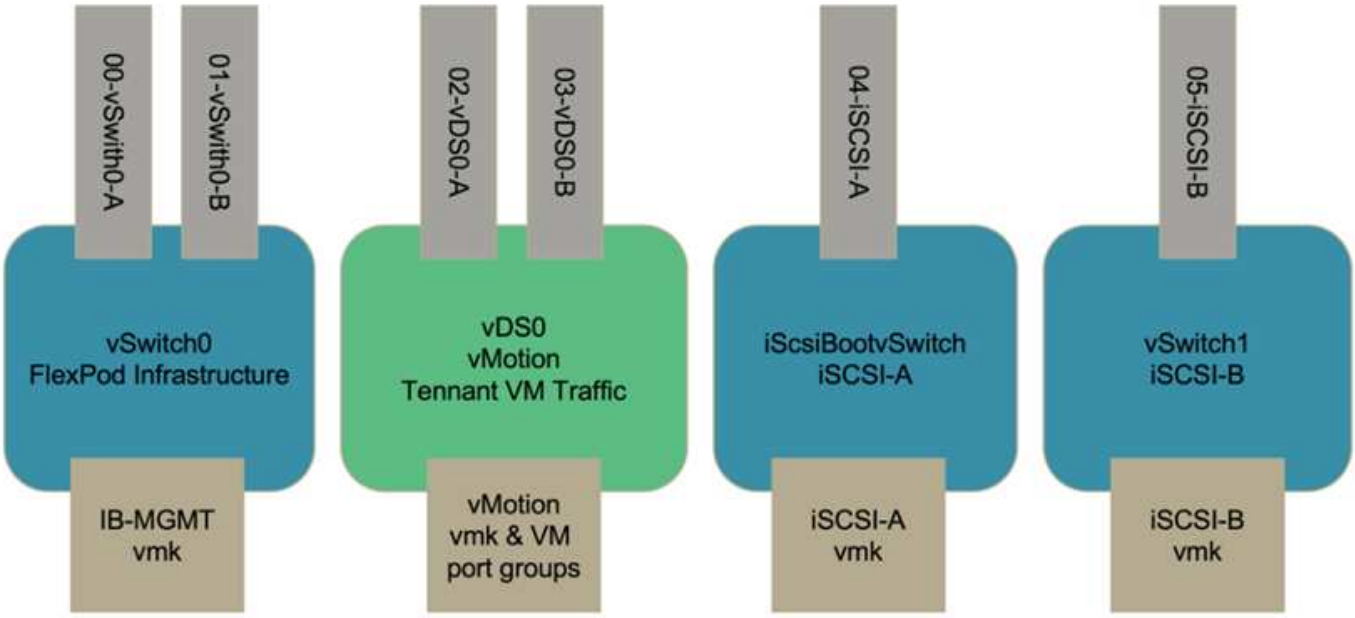
要求，也可以将其添加到现有 FlexPod 解决方案中。

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

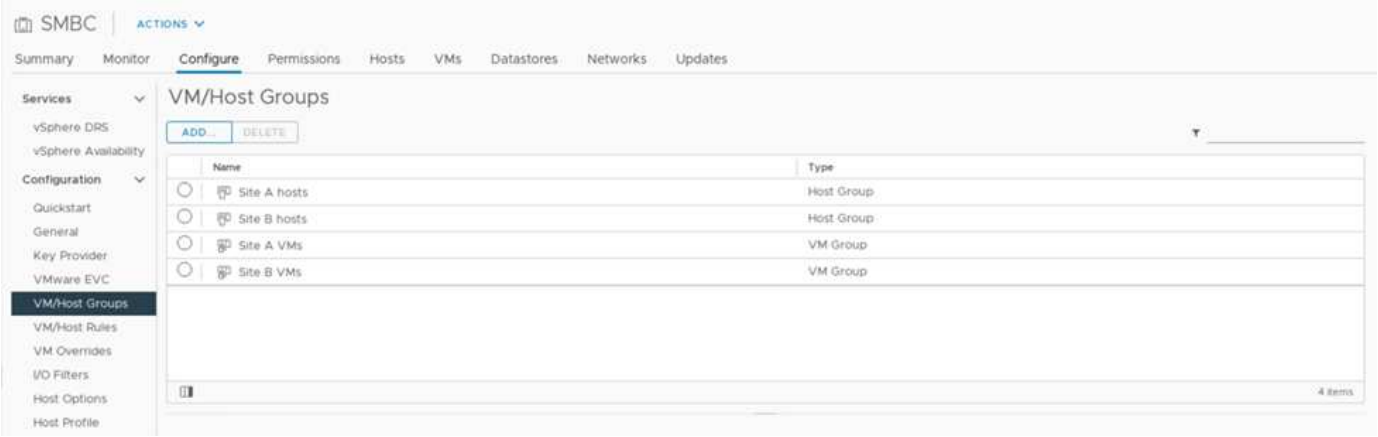
要使虚拟机能够在两个 SM-BC 站点的任何 ESXi 主机上运行，所有 ESXi 主机都必须从两个站点挂载 iSCSI 数

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。

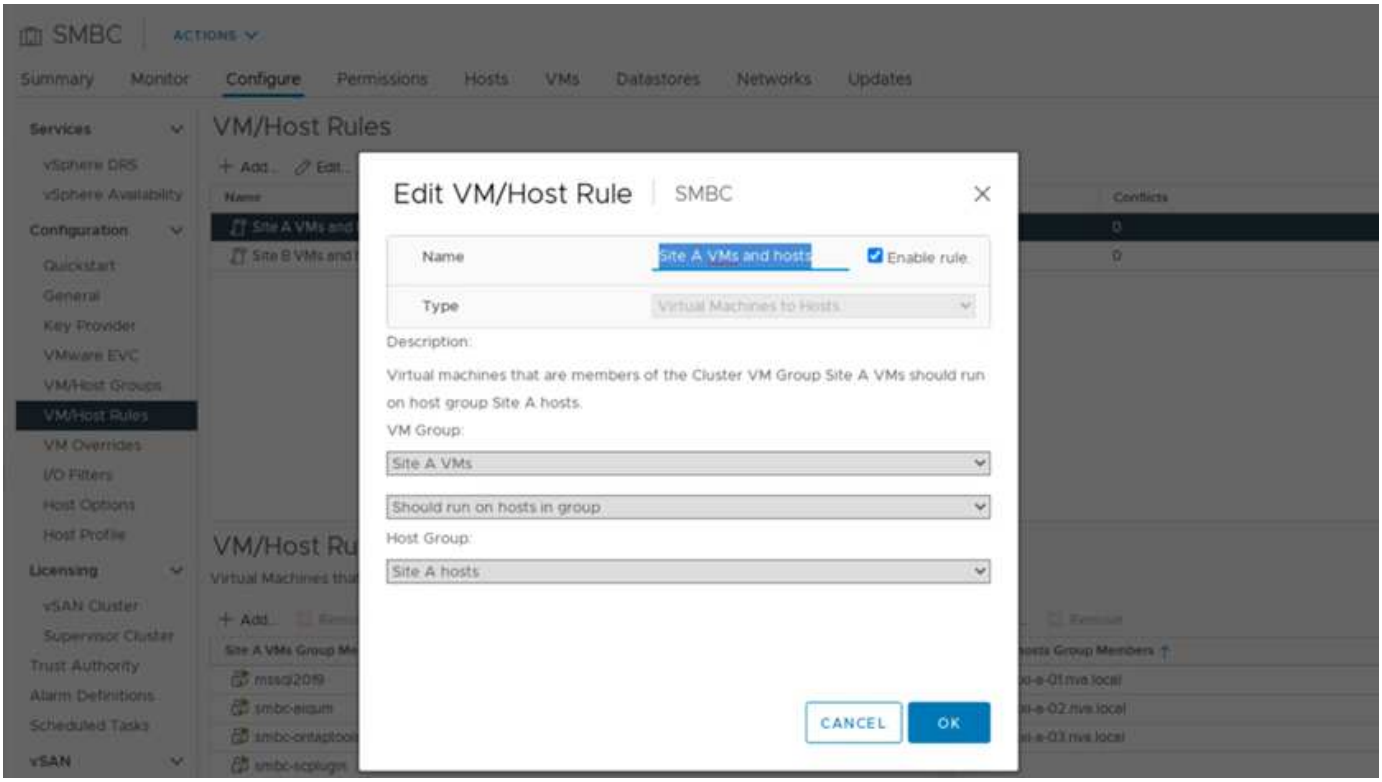
对于使用本地数据存储库的虚拟机，如果将其迁移到远程站点的主机，则其对虚拟磁盘的访问将变得远程，从而由于站点之间的物理距离而增加读取操作延迟。因此，最佳做法是将虚拟机保留在本地主机上，并利用站点上的本地存储。

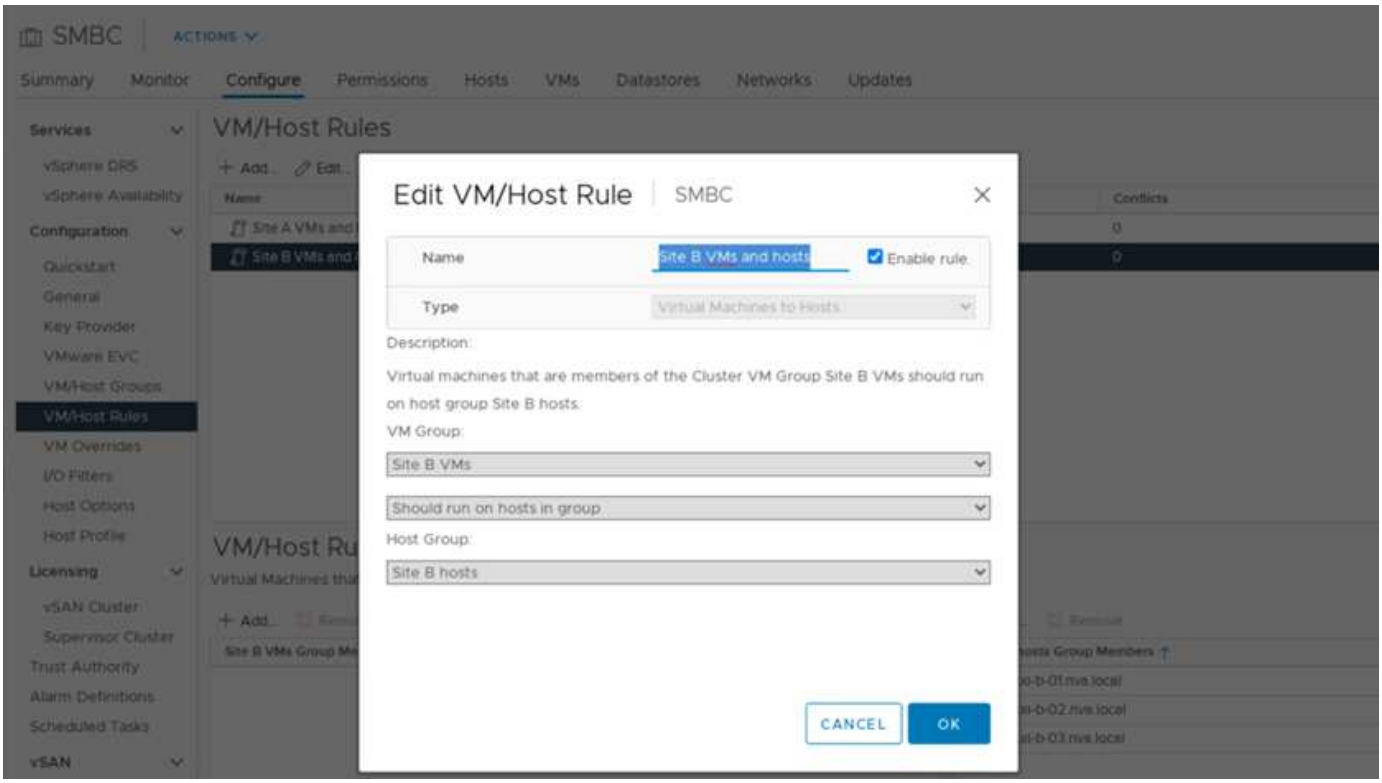
通过使用 VM/ 主机关联性机制，您可以使用 VM/ 主机组为位于特定站点的虚拟机和主机创建 VM 组和主机组。使用 VM/ 主机规则，您可以为要遵循的 VM 和主机指定策略。要在站点维护或灾难情形下允许跨站点进行虚拟机迁移，请使用 " 应在组中的主机上运行 " 策略规范来实现这种灵活性。

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。

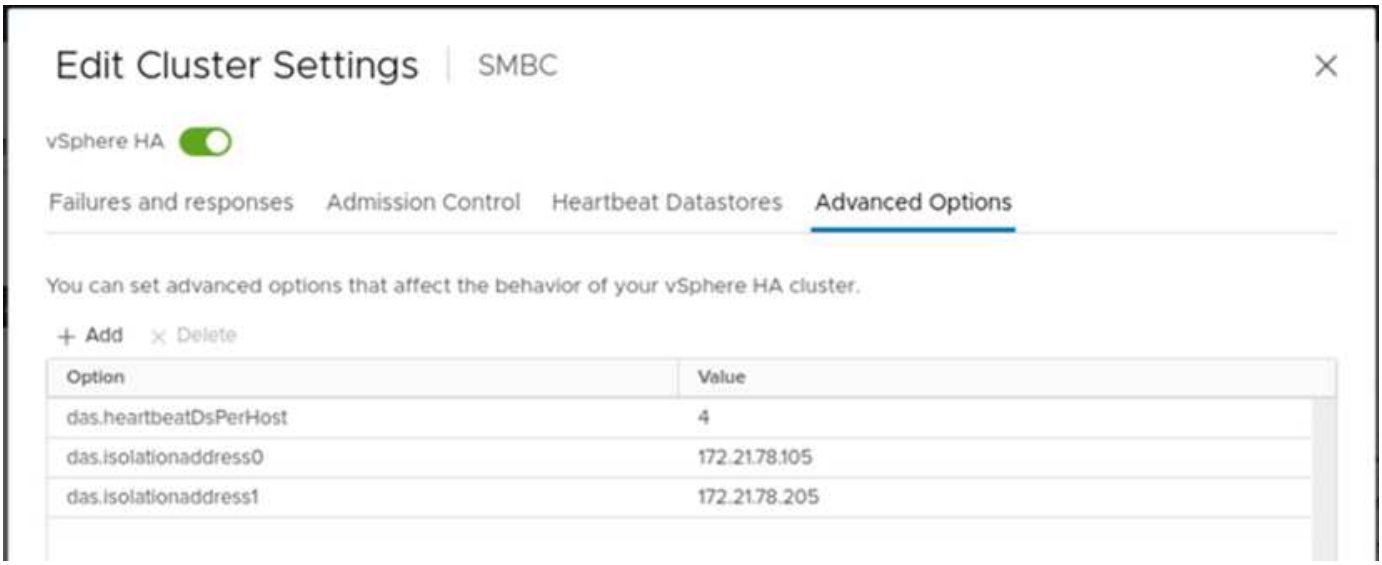




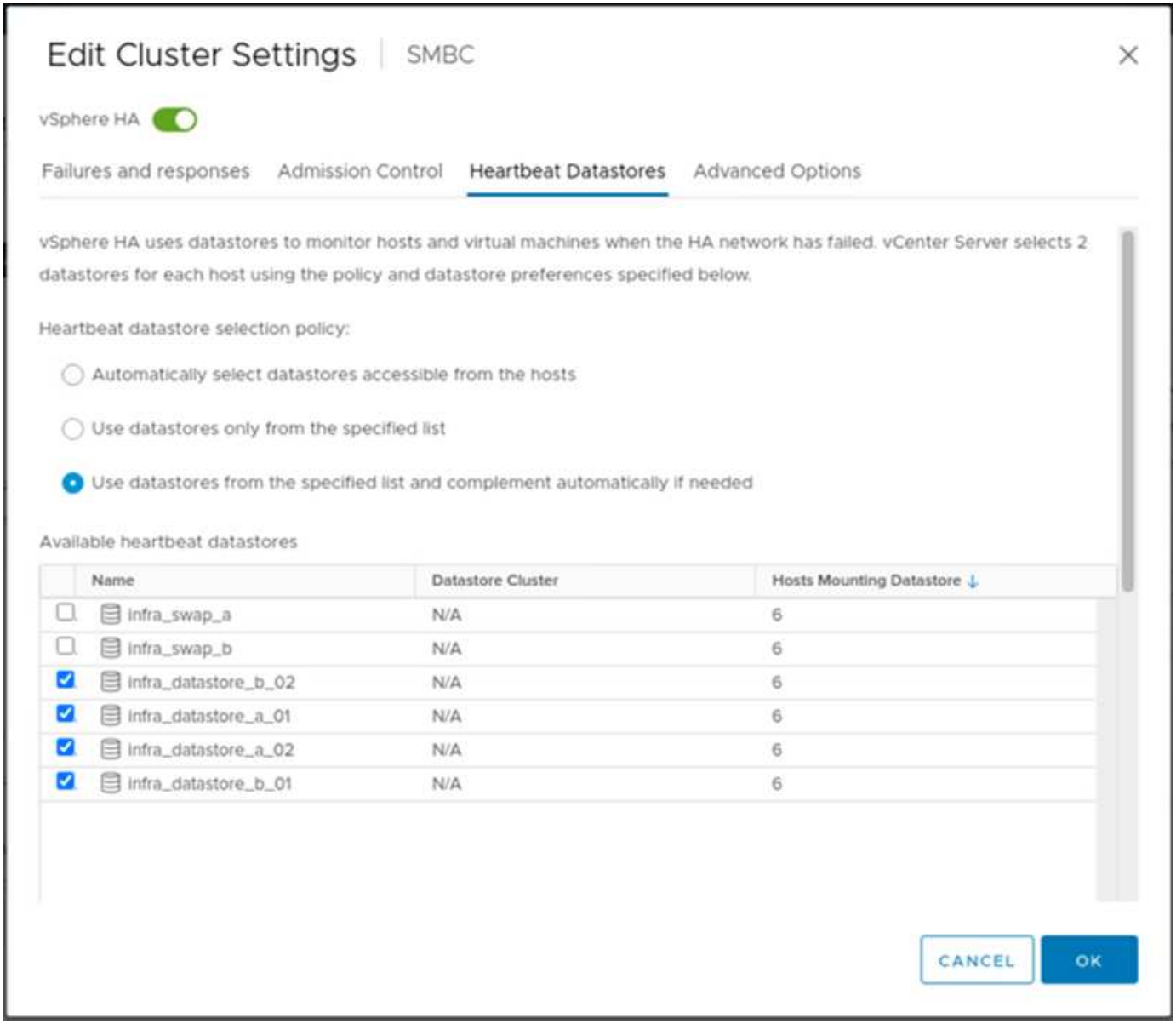
vSphere HA 检测信号

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 `D ss.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。



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

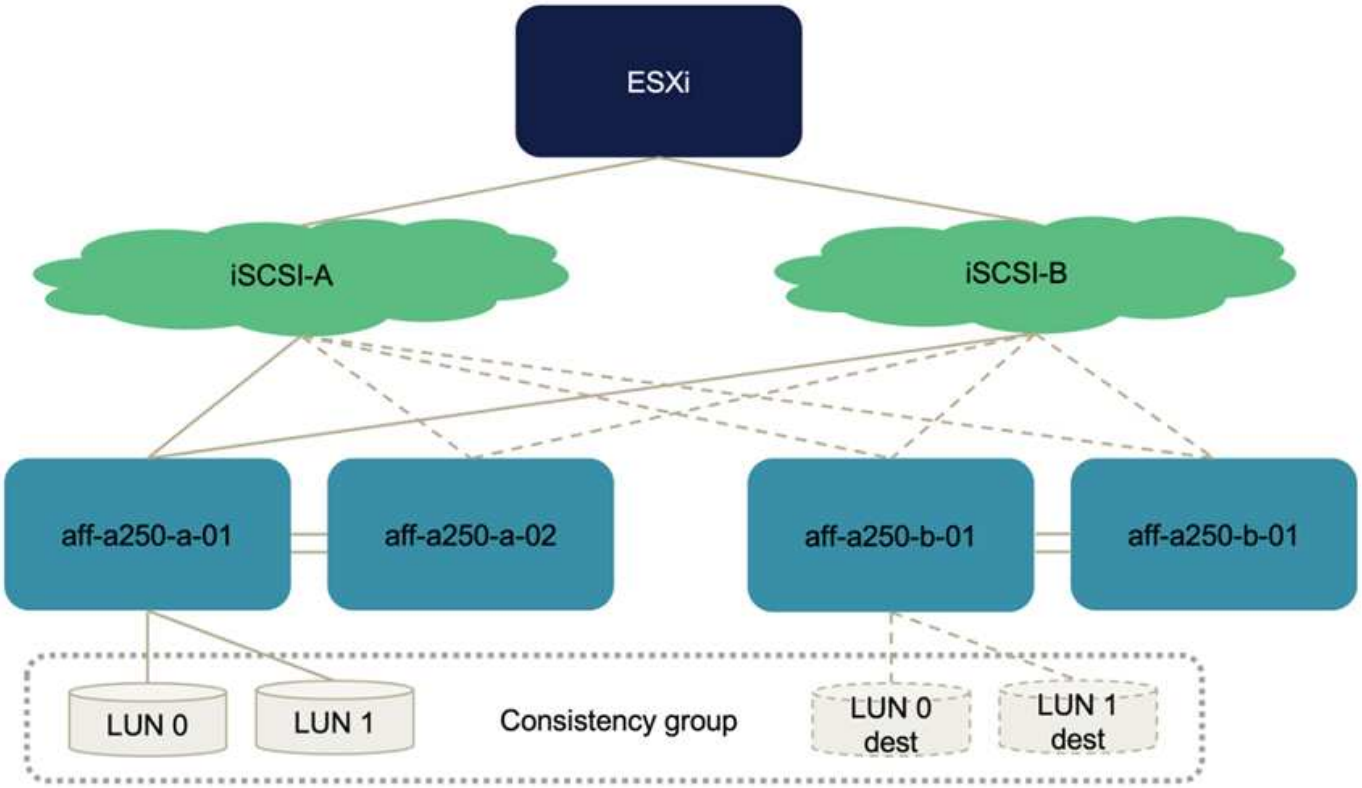
解决方案 中的 ESXi 主机已配置为从 iSCSI SAN 启动。使用 SAN 启动可以简化更换服务器时的服务器管理，因为服务器的服务配置文件可以与新服务器关联，以便在不更改任何其他配置的情况下启动它。

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。

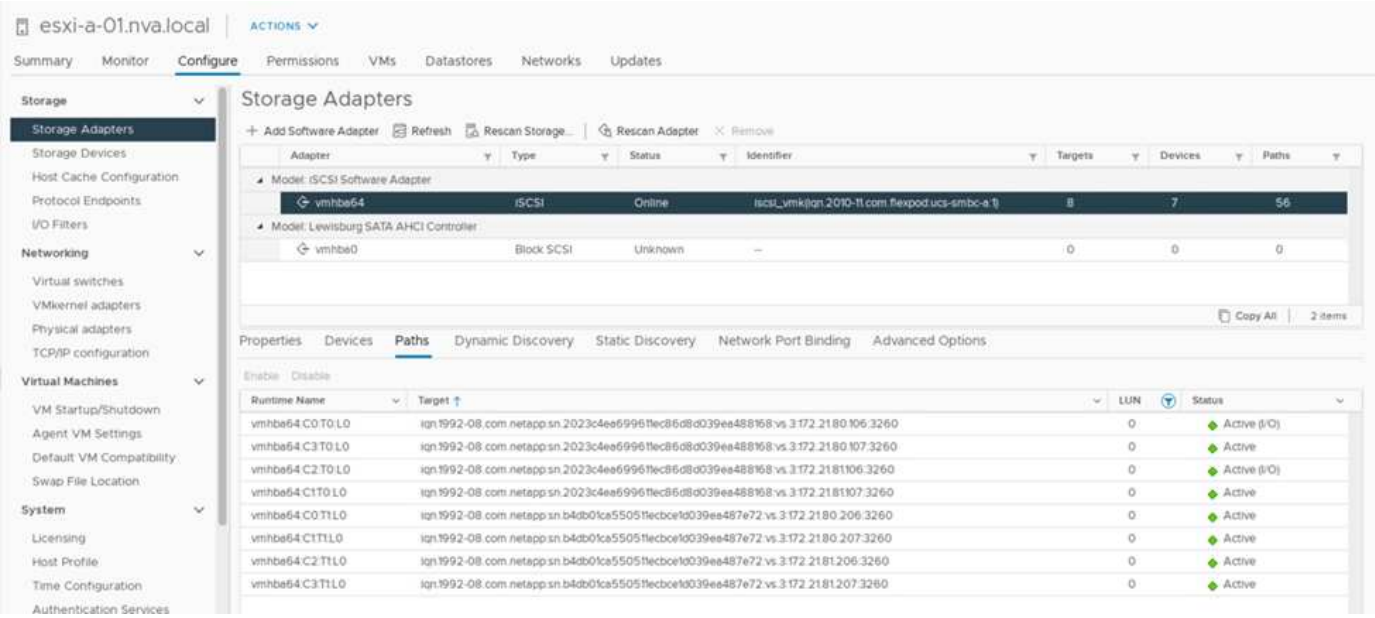
在配置 SM-BC 一致性组关系之前，存储控制器 HA 对托管的 iSCSI LUN 具有四个路径，根据最佳实践的实施情况，每个 iSCSI 网络结构有两个路径。主机可以通过两个 iSCSI VLAN/ 网络结构访问 LUN 到 LUN 托管控制器，也可以通过控制器的高可用性配对节点访问 LUN 。

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。



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。

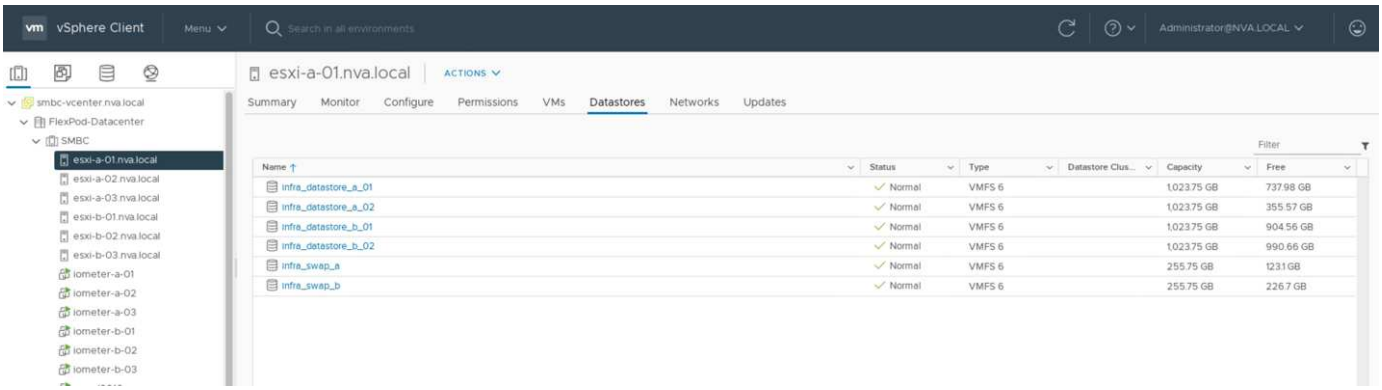
VMware vMotion 和 VM/ 主机关联性测试

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。

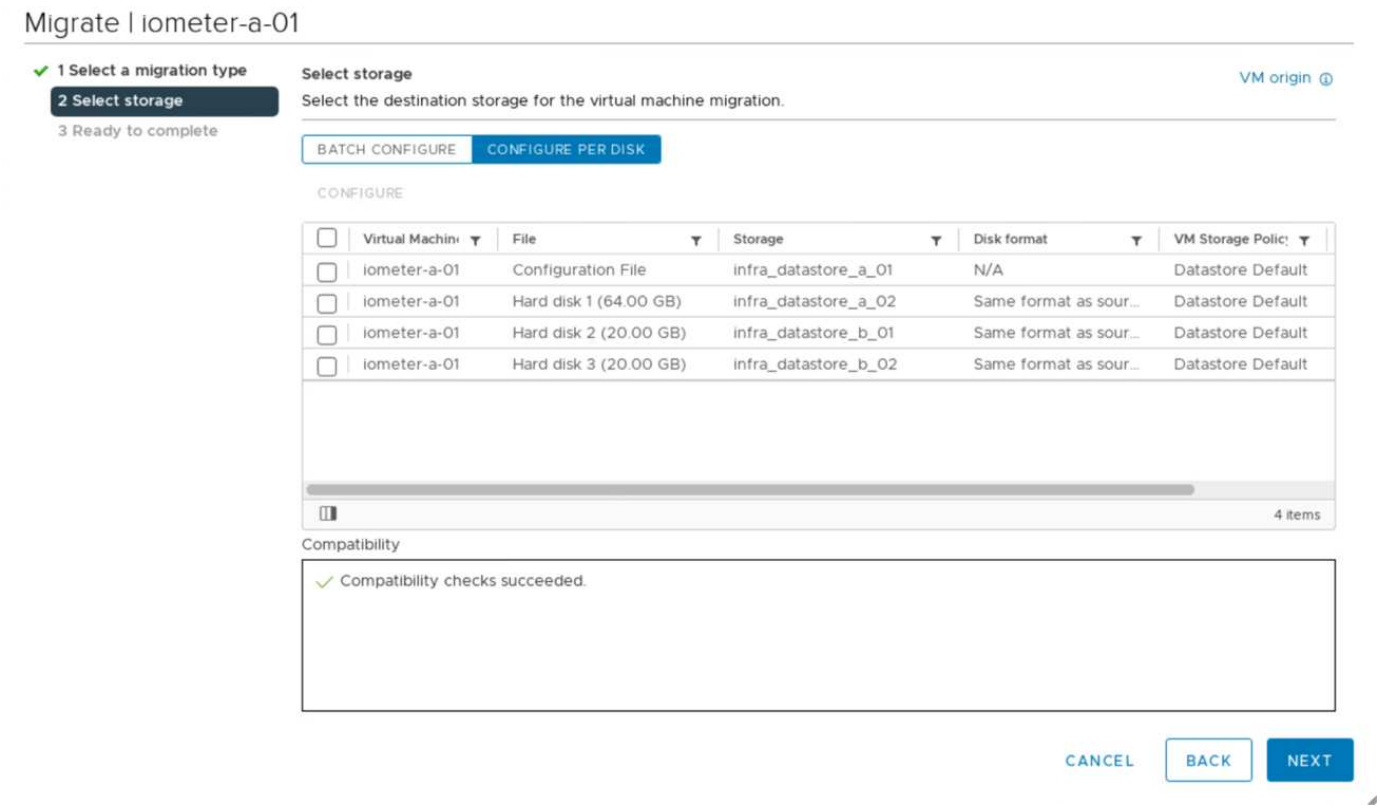
要允许虚拟机使用任何一个 SM-BC 站点的存储服务，集群中的所有主机都必须挂载两个站点的 iSCSI 数据存储库，以便在两个站点之间迁移虚拟机，并在发生灾难故障转移时进行迁移。

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。



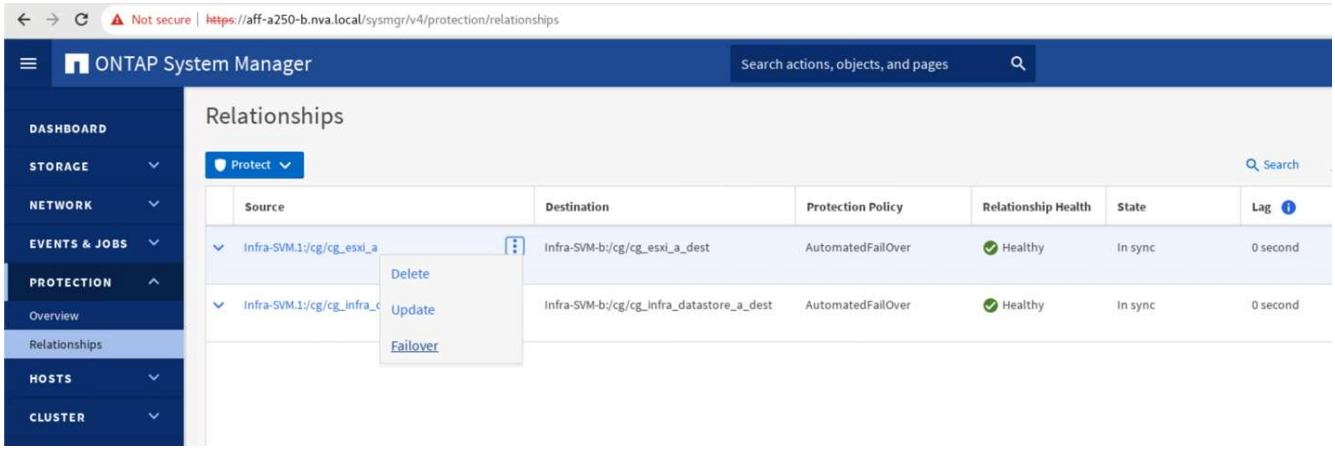
对虚拟机在同一站点以及不同站点的不同主机上的 vMotion 进行了测试，并取得了成功。在站点间手动迁移虚拟机后， VM/ 主机关联性规则会激活虚拟机并将其迁移回正常情况下所属的组。

计划内存储故障转移

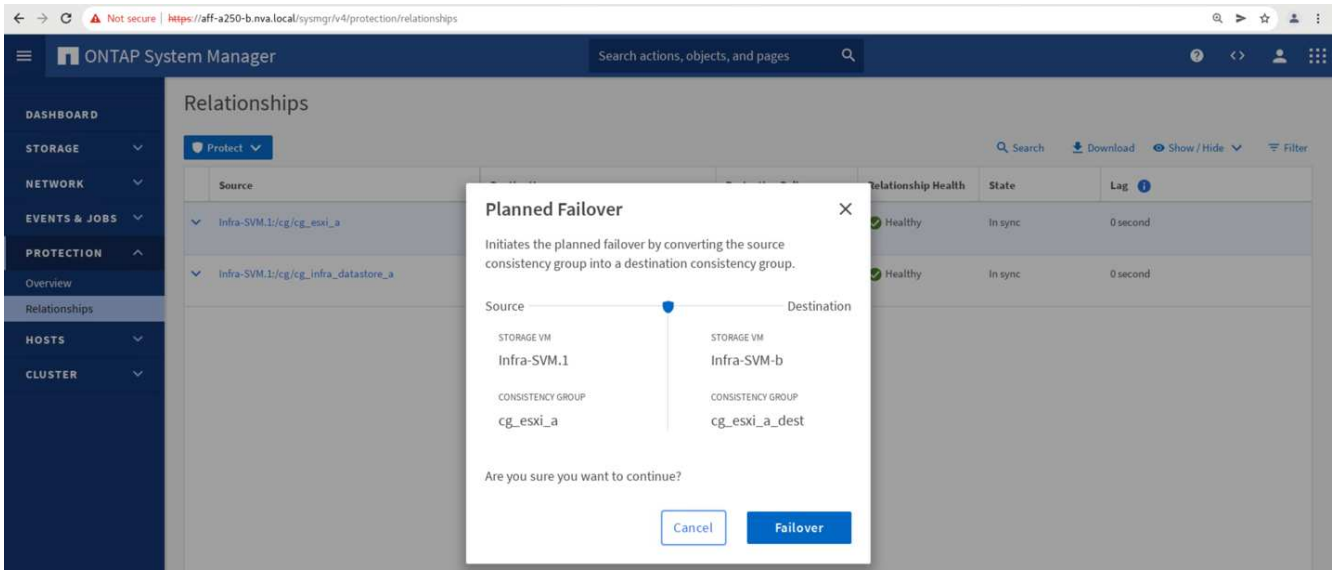
应在初始配置后对解决方案 执行计划内存储故障转移操作，以确定解决方案 在存储故障转移后是否正常工作。此测试有助于确定可能导致 I/O 中断的任何连接或配置问题。定期测试和解决任何连接或配置问题有助于在发生实际站点灾难时提供无中断的数据服务。也可以在计划的存储维护活动之前使用计划的存储故障转移，以便可以从不受影响的站点提供数据服务。

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。

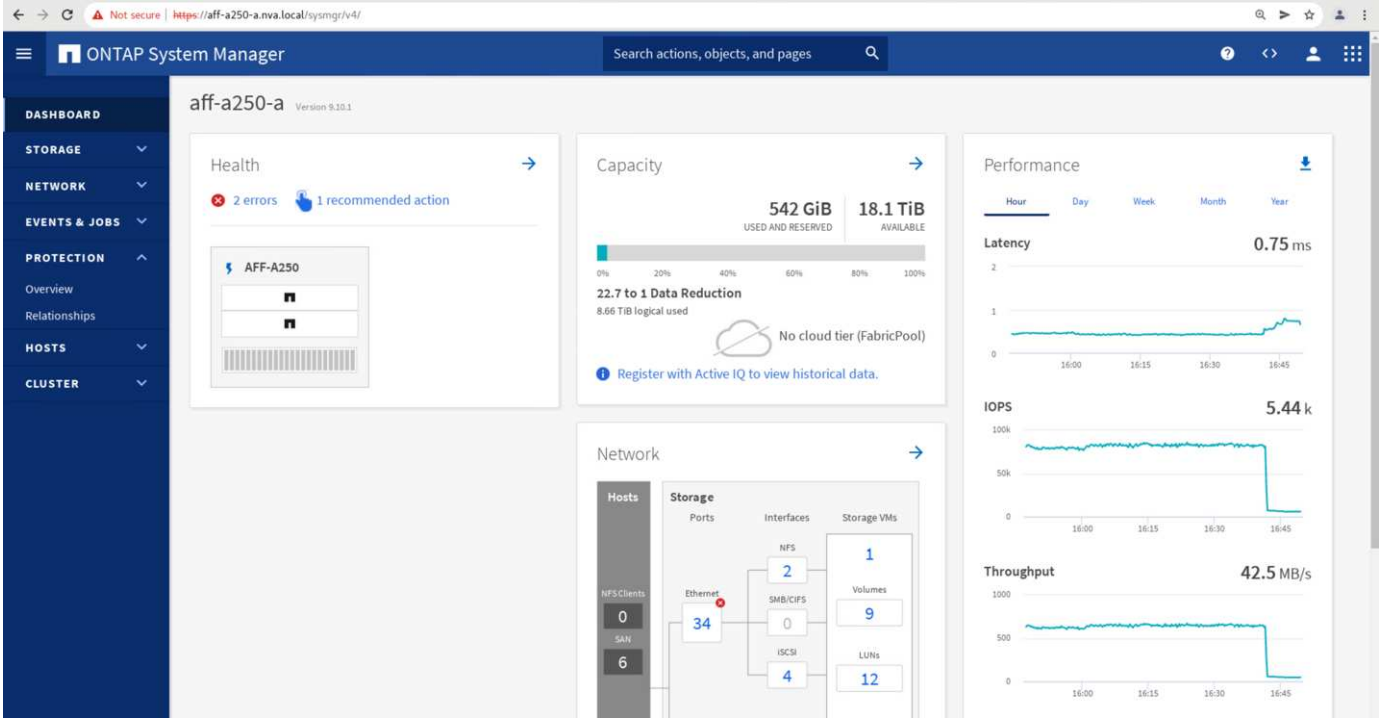
1. 导航到保护 > 关系屏幕，确认一致性组关系状态为 `in Sync` 。如果它仍处于 `Synchronizing` 状态，请等待状态变为 `in Sync` ，然后再执行故障转移。
2. 展开源名称旁边的点，然后单击故障转移。



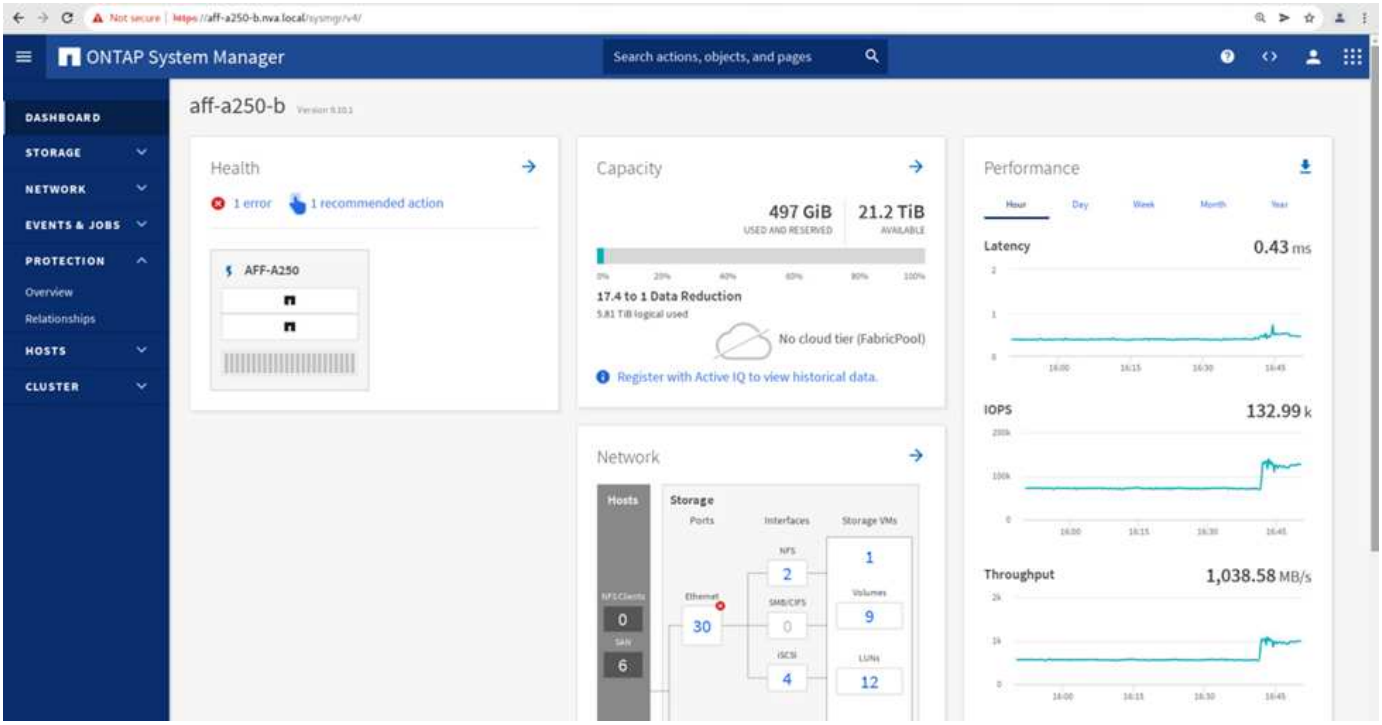
3. 确认故障转移以启动操作。



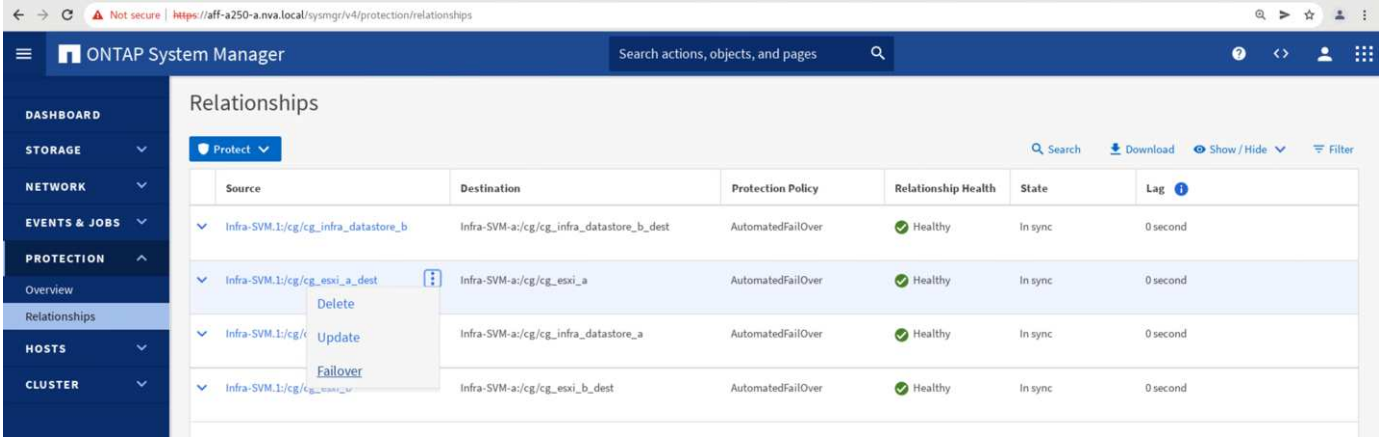
在站点 B System Manager 图形用户界面上对两个一致性组 `CG_ESXi_A` 和 `CG_infra_datastore_A` 启动故障转移后不久，为这两个一致性组提供服务的站点 A I/O 便移至站点 B因此，站点 A 的 I/O 会显著减少，如站点 A System Manager 性能窗格中所示。



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。

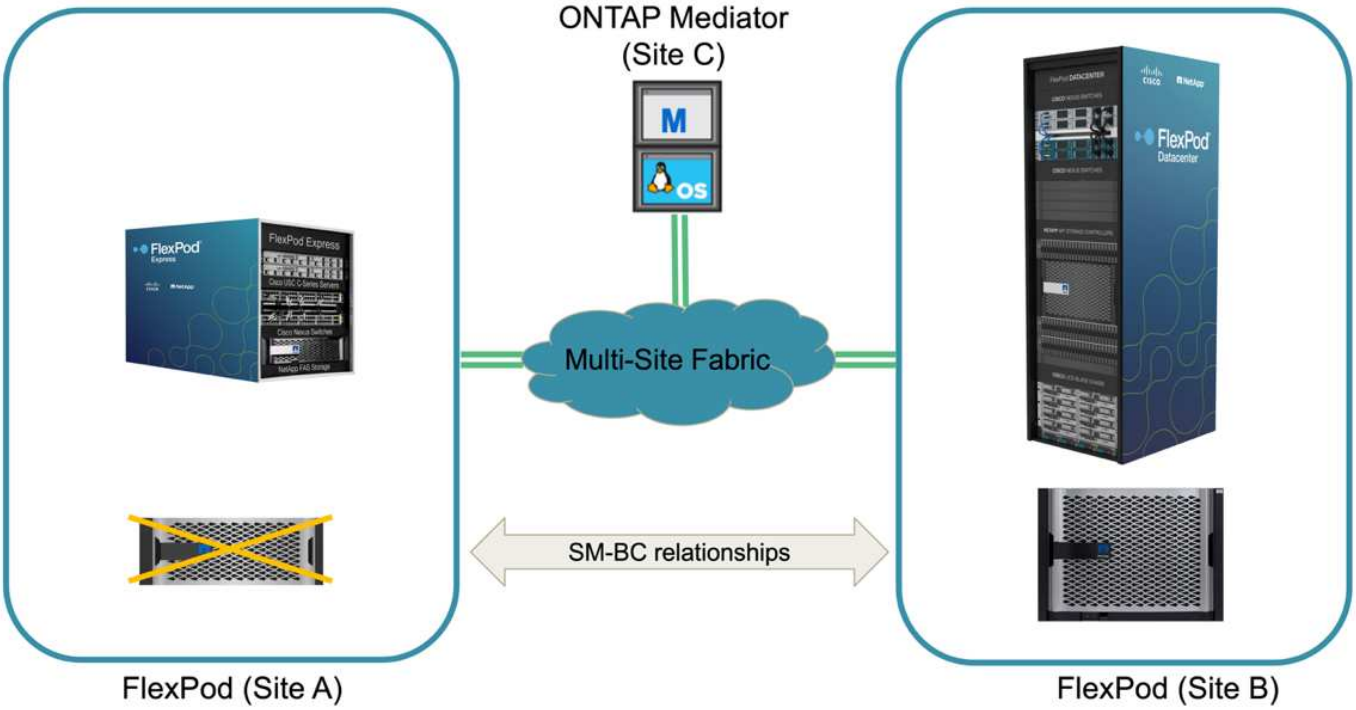


随着 I/O 从站点 A 透明地迁移到站点 B ，现在可以关闭站点 A 存储控制器以进行计划内维护。完成维护工作或测试并恢复站点 A 存储集群并使其正常运行后，请先检查并等待一致性组保护状态重新更改为同步 ` ，然后再执行故障转移，将故障转移 `I/O` 从站点 `B` 返回到站点 `A`请注意，站点因维护或测试而关闭的时间越长，同步数据以及将一致性组返回到处于同步 状态的 `所需的时间就越长。



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



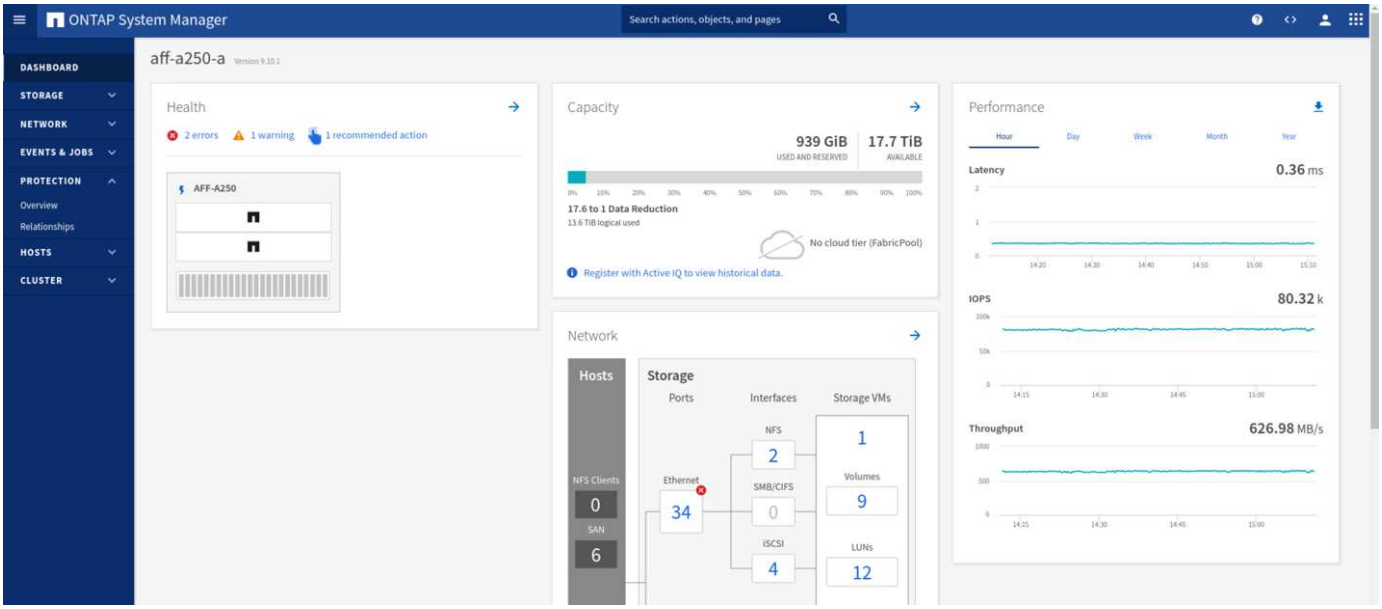
要模拟站点 A 的存储灾难，可以通过物理关闭电源开关来关闭站点 A 的两个存储控制器，从而停止为控制器供电。 或者使用存储控制器服务处理器的 system power management 命令关闭控制器。

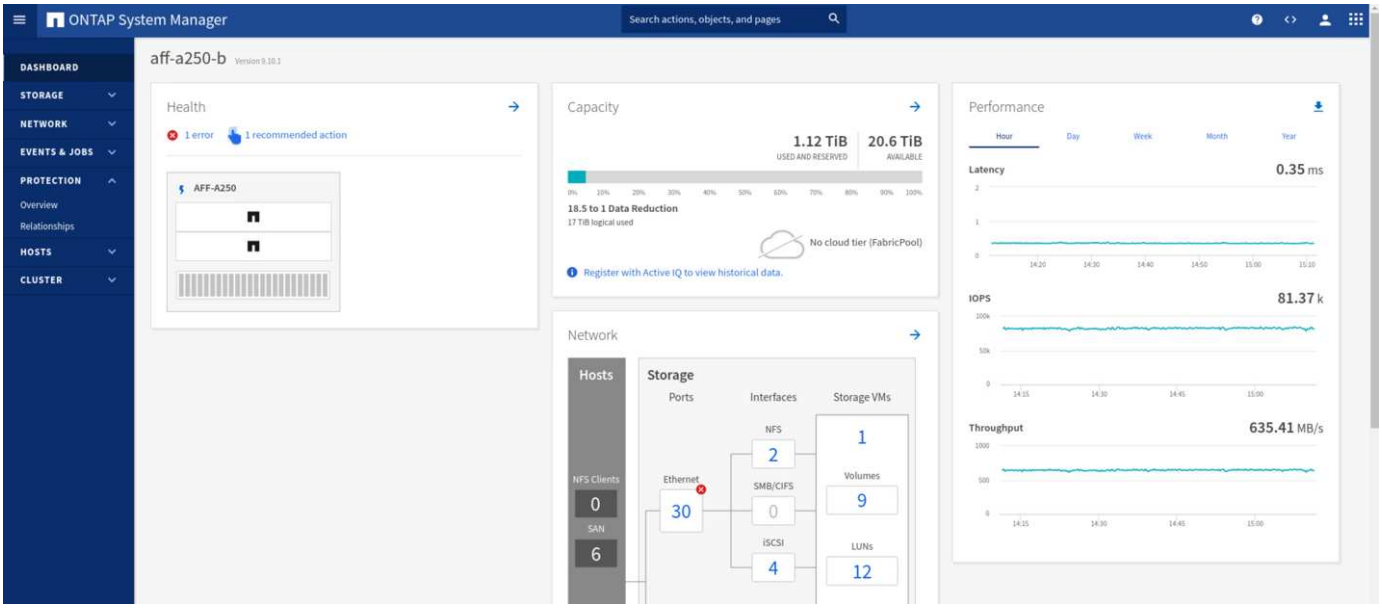
当站点 A 的存储集群断电时，站点 A 存储集群提供的数据服务会突然停止。然后，用于监控第三个站点的 SM-BC 解决方案 的 ONTAP 调解器会检测站点的存储故障情况，并使 SM-BC 解决方案 能够执行自动计划外故障转移。这样，站点 B 存储控制器就可以继续为与站点 A 建立的 SM-BC 一致性组关系中配置的 LUN 提供数据服务

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 。

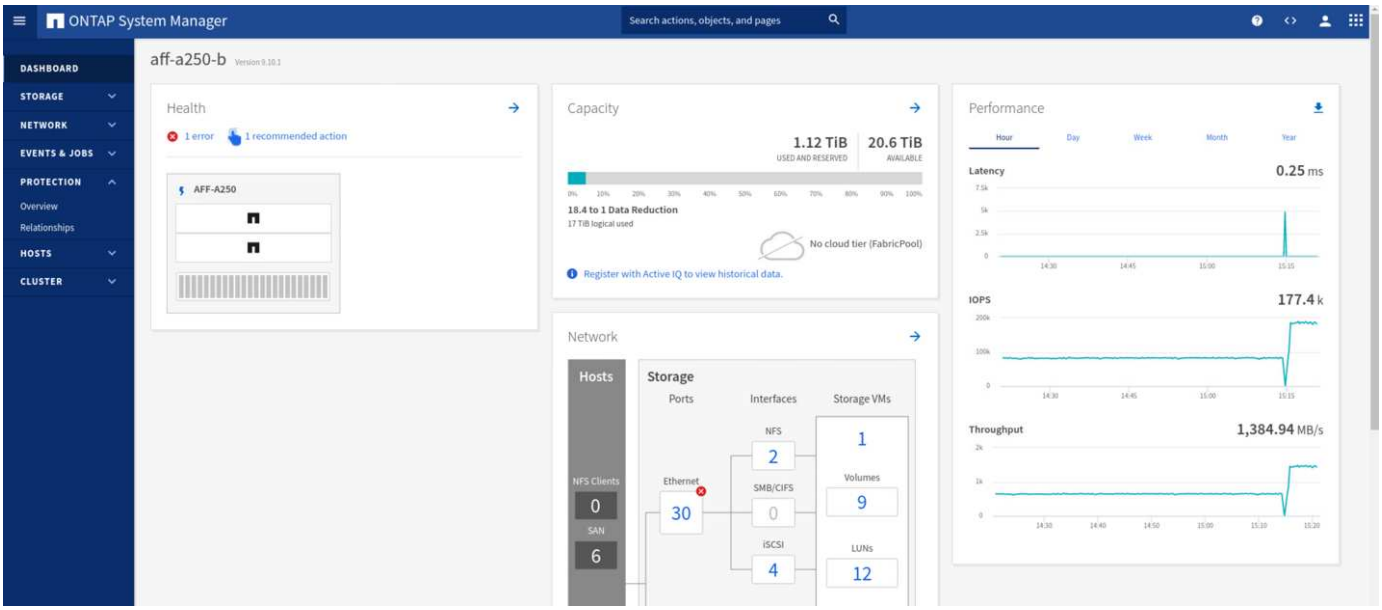
在验证测试期间，两个站点的 VM 上的 IOMeter 工具会为其本地数据存储库生成 I/O 。关闭站点 A 集群后， I/O 会短暂暂停，然后恢复。请参见以下两个数据，分别查看发生灾难前站点 A 和站点 B 存储集群的信息板，这些

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

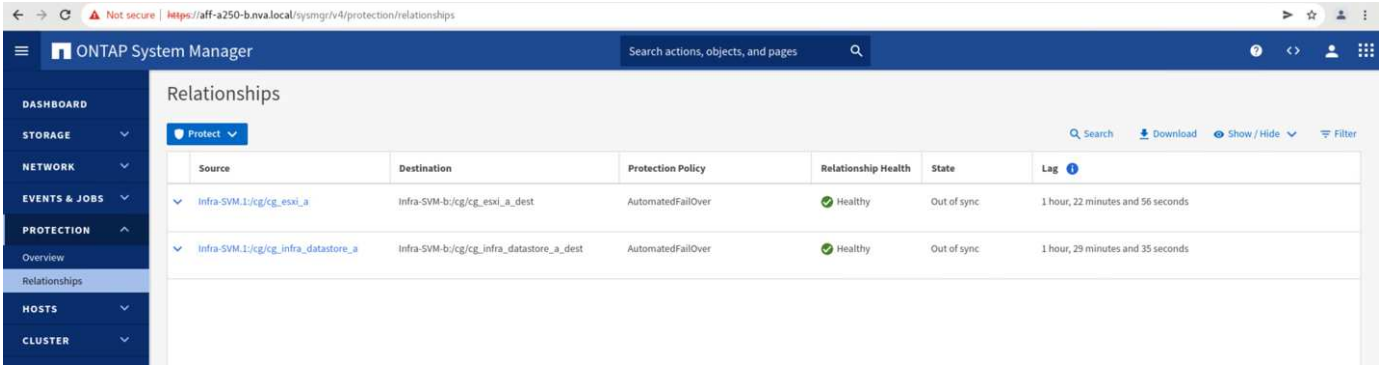




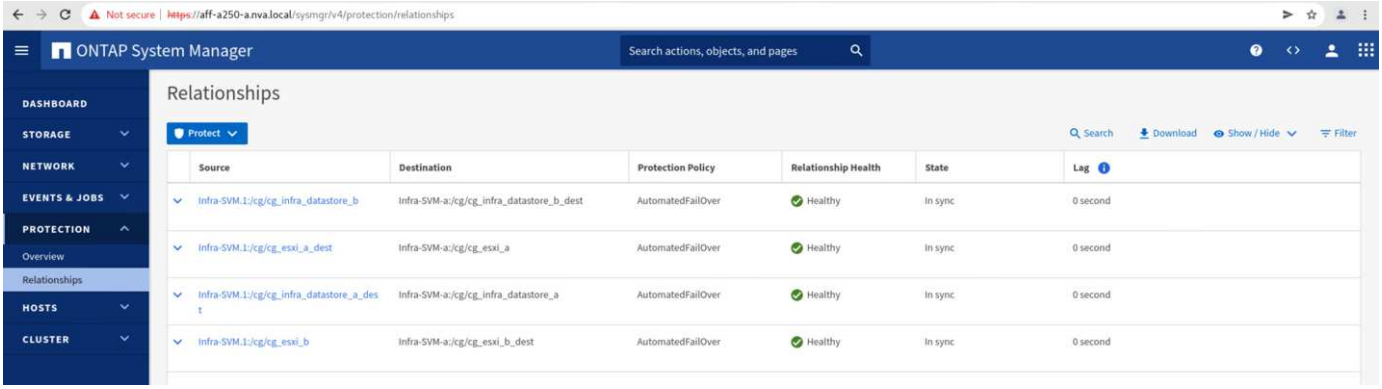
关闭站点 A 的存储控制器后，我们可以直观地验证站点 B 存储控制器 I/O 是否急剧增加，以便代表站点 A 提供额外的数据服务（请参见下图）。此外， IOMeter VM 的 GUI 还显示，尽管站点 A 存储集群发生中断， I/O 仍会继续。请注意，如果有其他数据存储库由不受 SM-BC 关系保护的 LUN 提供支持，则在发生存储灾难时，这些数据存储库将无法再访问。因此，必须评估各种应用程序数据的业务需求，并将其正确放置在受 SM-BC 关系保护的数据存储库中，以确保业务连续性。



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。



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



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 。

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。

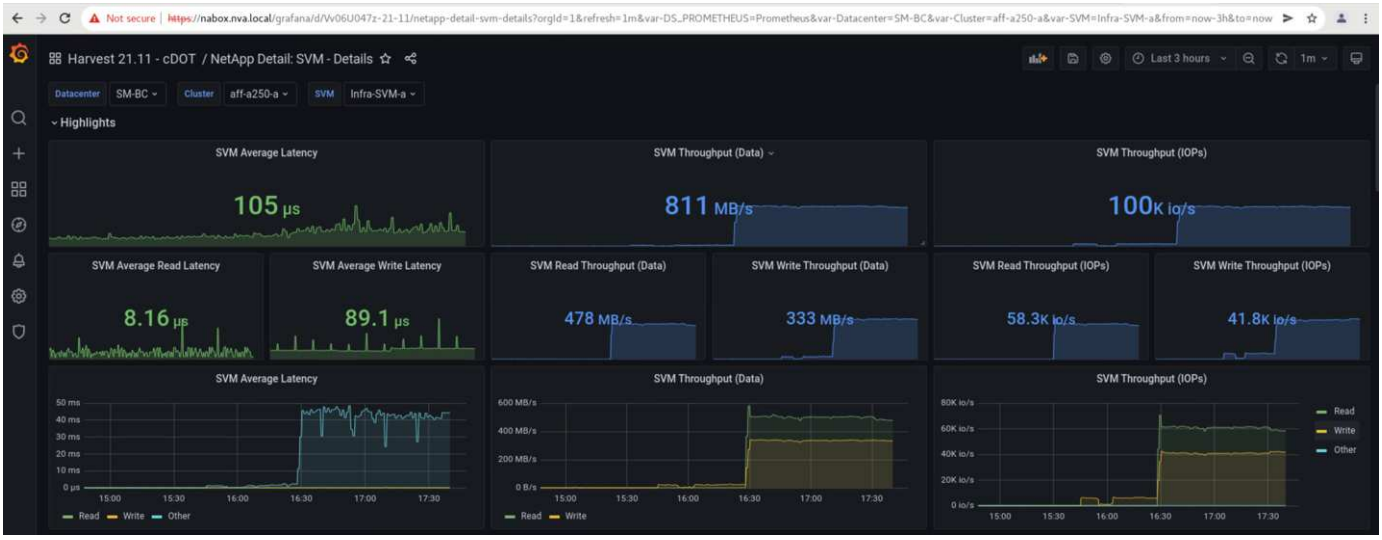
对于计划外站点灾难模拟，服务器和存储控制器已关闭，以模拟站点灾难。VMware HA 功能可检测已关闭的虚拟机，并在运行正常的站点上重新启动这些虚拟机。此外，在第三个站点运行的 ONTAP 调解器会检测站点故障，而运行正常的站点会启动故障转移，并开始按预期为故障站点提供数据服务。

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。

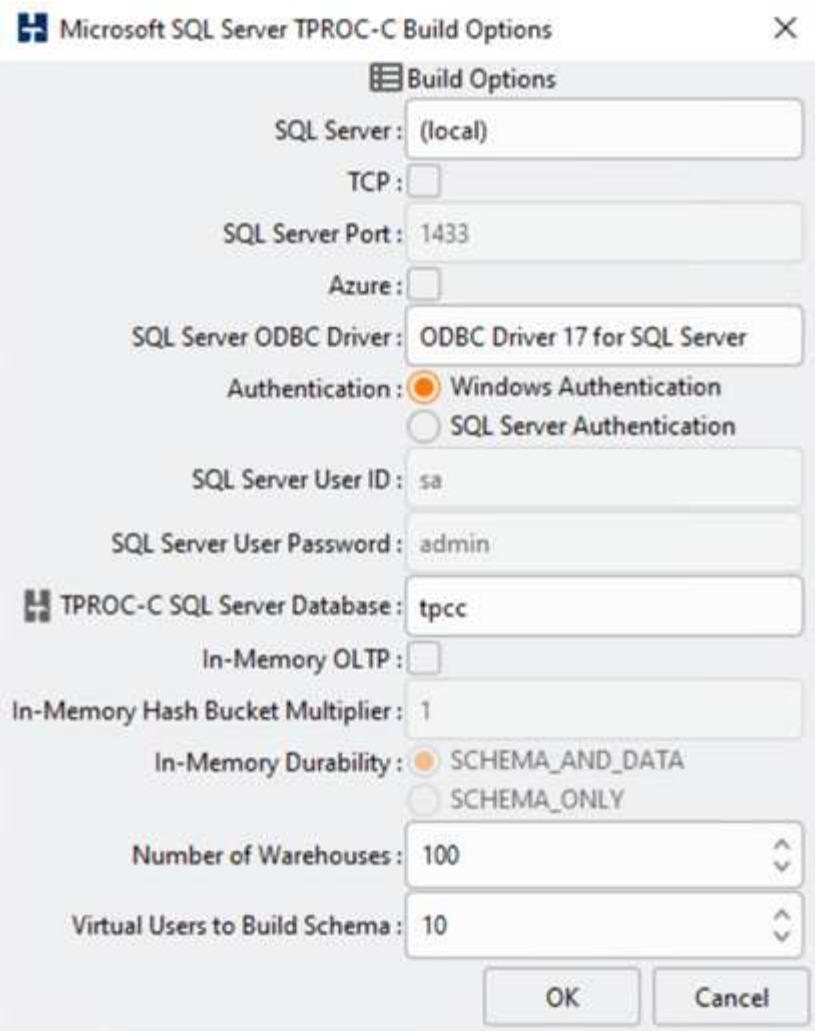


Microsoft SQL Server

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。

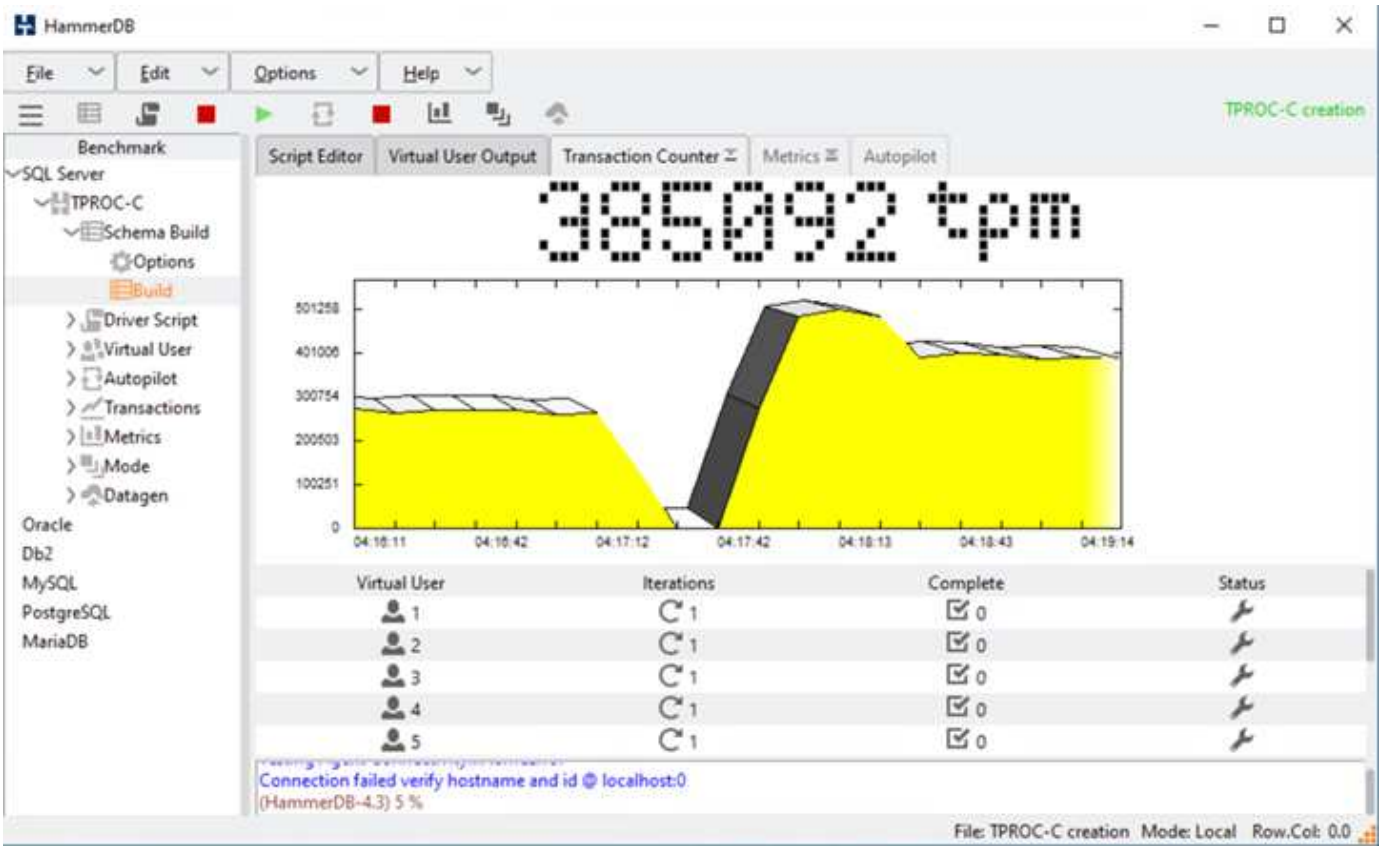
作为 FlexPod SM-BC 解决方案 业务关键型工作负载验证的一部分，安装在 Windows Server 2022 虚拟机上的 Microsoft SQL Server 2019 与 IOMeter 虚拟机一起提供，用于执行计划内和计划外存储故障转移测试。在 Windows Server 2022 VM 上，安装了 SQL Server Management Studio 来管理 SQL 服务器。在测试中，使用 HammerDB 数据库工具生成数据库事务。

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。



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 NAbox 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 NAbox 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 Nanbox 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"

- 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"

- 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"

- NetApp 产品文档

  "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"

- 《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"

- 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"

- 《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

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"

- NAbox

  "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"

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"

- VMware vSphere 城域存储集群（VMSC）

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-vmsc"

- VMware vSphere Metro Storage Cluster 建议的实践

  "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"

- 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"

Microsoft SQL 和 HammerDB

- Microsoft 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"

- HammerDB 网站

  "https://www.hammerdb.com"

兼容性表

- Cisco UCS 硬件兼容性列表

  "https://ucshcltool.cloudapps.cisco.com/public/"

- NetApp 互操作性表工具

  "https://support.netapp.com/matrix/"

- NetApp Hardware Universe

"https://hwu.netapp.com"

- VMware 兼容性指南

  "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 fout-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"

混合云

采用Cloud Volumes ONTAP for Epic的FlexPod 混合云

TR-4960：《FlexPod 混合云与适用于Epic的Cloud Volumes ONTAP 》

与以下合作伙伴：

NetApp公司Kamini Singh

实现数字化转型的关键在于利用数据完成更多工作。医院需要生成大量数据、才能有效地运营组织并为患者提供服务。在治疗患者以及管理员工计划和医疗资源时、系统会收集和处理相关信息。

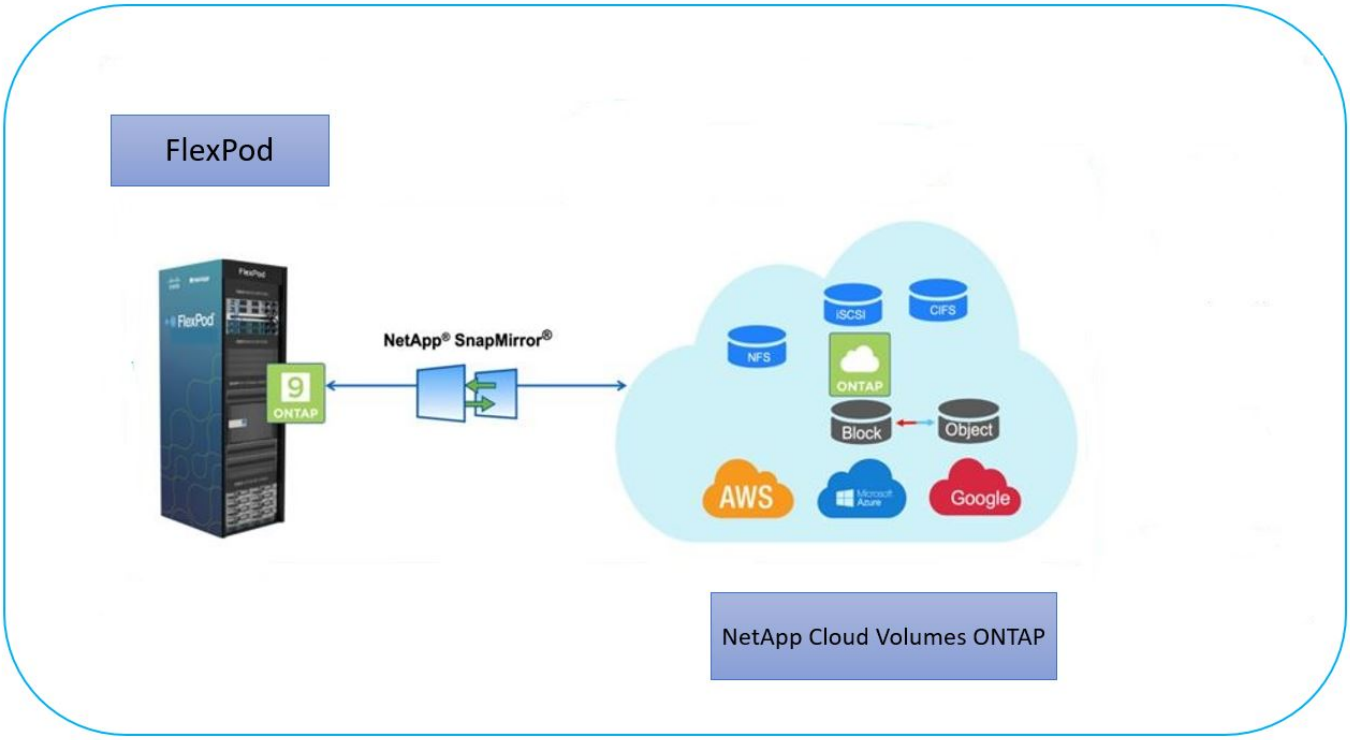
医疗保健数据的规模不断扩大、而且这些数据可以提供宝贵的洞察力、这使得医疗保健数据服务和数据保护变得既重要又具有挑战性。首先、医疗保健数据必须可用且受到保护、才能满足数据恢复、医疗业务连续性或合规性要求。

第二、必须随时提供医疗保健数据以供分析。这种分析通常采用基于人工智能(AI)和机器学习(ML)的方法来帮助医疗企业改进其解决方案并创造业务价值。

第三、随着医疗业务的增长、数据服务基础架构和数据保护方法必须适应医疗保健数据的增长。此外、由于需要将数据从创建数据的边缘移动到核心和云、以便使用数据分析或归档所需的资源、数据移动性变得越来越重要。

NetApp为包括医疗保健在内的企业级应用程序提供了一个数据管理解决方案 、我们可以指导医院完成数字化转型之旅。NetApp Cloud Volumes ONTAP 提供了用于医疗保健数据管理的解决方案 、可将数据从FlexPod 数据中心高效复制到AWS等公共云上部署的Cloud Volumes ONTAP。

通过利用经济高效且安全的公共云资源、Cloud Volumes ONTAP 通过高效的数据复制、内置存储效率和简单的灾难恢复测试增强了基于云的灾难恢复(Disaster Recovery、DR)。这些系统采用统一的控制和简单的拖放操作进行管理、可提供经济高效的保护、防止出现任何类型的错误、故障或灾难。Cloud Volumes ONTAP 提供了NetApp SnapMirror技术作为块级数据复制的解决方案 、可通过增量更新使目标保持最新。



audience

本文档面向NetApp和合作伙伴解决方案工程师(SE)以及专业服务人员。NetApp假定读者具备以下背景知识：

- 深入了解SAN和NAS概念
- 熟悉NetApp ONTAP 存储系统的技术知识
- 熟悉ONTAP 软件的配置和管理技术

解决方案的优势

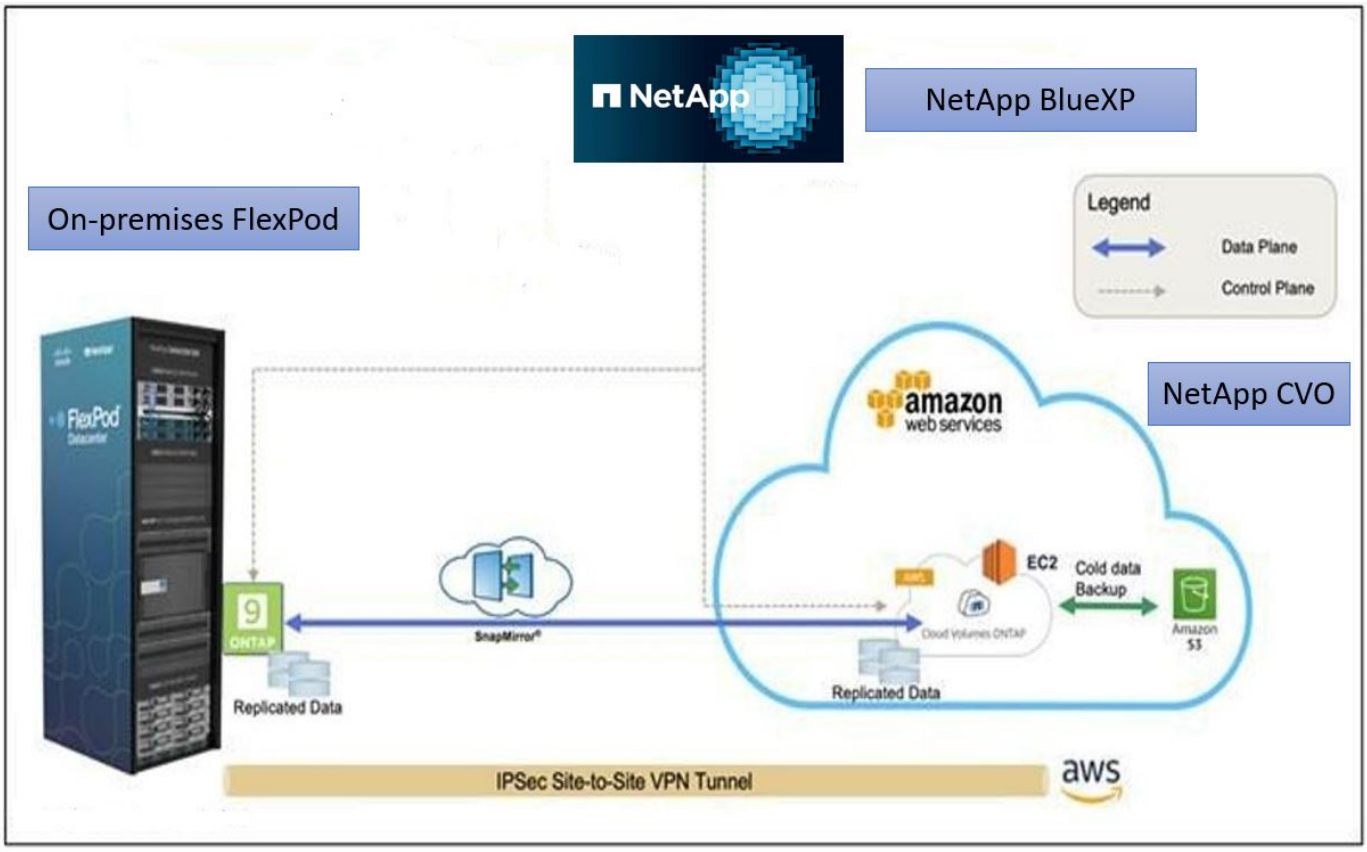
与NetApp Cloud Volumes ONTAP 集成的FlexPod 数据中心为医疗保健工作负载提供了以下优势：

- 自定义保护。 Cloud Volumes ONTAP 提供从ONTAP 到云的块级数据复制、通过增量更新使目标保持最新。用户可以指定同步计划来确定何时传输源上的更改。这样可以为各种医疗保健数据提供自定义保护。
- *故障转移和故障恢复。*发生灾难时、存储管理员可以快速为云卷设置故障转移。恢复主站点后、在灾难恢复环境中创建的新数据将同步回源卷、以便重新建立二级数据复制。这样、医疗保健数据便可轻松恢复、而不会造成中断。
- *效率。*二级云副本的存储空间和成本通过数据压缩、精简配置和重复数据删除进行了优化。医疗保健数据以经过压缩和重复数据删除的形式在块级别传输、从而加快传输速度。数据也会自动分层到低成本对象存储、并且只有在访问时才会返回到高性能存储、例如在灾难恢复情形下。这样可以显著降低持续存储成本。
- 勒索软件保护。 NetApp BlueXP勒索软件保护功能可扫描内部环境和云环境中的数据源、检测安全漏洞并提供其当前安全状态和风险评分。然后、它将提供可操作的建议、您可以进一步调查并遵循这些建议进行修复。通过这种方式、您可以保护您的关键医疗保健数据免受勒索软件攻击。

解决方案 拓扑

本节介绍解决方案 的逻辑拓扑。下图显示了由FlexPod 内部环境、在Amazon Web Services (AWS)上运行

的NetApp Cloud Volumes ONTAP (CVO)和NetApp BlueXP SaaS平台组成的解决方案 拓扑。



控制平面和数据平面会在端点之间清晰地指示。通过利用安全的站点到站点VPN连接、数据平面在FlexPod 的纯闪存FAS 上运行的ONTAP 实例与AWS中的NetApp CVO实例之间运行。将医疗保健工作负载数据从内部FlexPod 数据中心复制到NetApp Cloud Volumes ONTAP 时、会通过NetApp SnapMirror复制来处理。此外、此解决方案 还支持将NetApp CVO实例中的冷数据备份和分层到AWS S3。

"接下来：解决方案 组件。"

解决方案组件

"先前版本：解决方案 概述。"

FlexPod

FlexPod 是一组定义的硬件和软件、可为虚拟化和非虚拟化解决方案奠定集成基础。FlexPod 包括NetApp ONTAP 存储、Cisco Nexus网络、Cisco MDS存储网络和Cisco统一计算系统(Cisco UCS)。

医疗保健组织正在寻找解决方案 、以简化数字化转型并改善患者体验和结果。借助FlexPod 、您可以获得一个安全、可扩展的平台、该平台可提高效率、并使员工能够更快地做出更明智的决策、从而为患者提供更好的护理。

FlexPod 是满足医疗保健工作负载需求的理想平台、因为它具有以下优势：

- 优化操作、更快地获得洞察力并获得更好的患者结果。
- 利用可扩展且可靠的基础架构简化映像应用程序。

- 借助经验证的方法快速高效地部署特定于医疗保健的应用程序、例如EHR。

EHR

电子健康记录(Electronic Health Records、EHRs)为大中型医疗团队、医院和综合医疗保健组织提供软件。客户还包括社区医院、学术机构、儿童组织、安全网络提供商和多医院系统。EHR集成软件涵盖临床、访问和收入功能、并扩展到家庭。

医疗保健提供商组织仍然面临着最大程度地发挥其在行业领先的EHRs上的巨大投资优势的压力。客户在为EHR解决方案和任务关键型应用程序设计数据中心时、通常会为其数据中心架构确定以下目标：

- EHR应用程序的高可用性
- 高性能
- 在数据中心轻松实施EHR
- 灵活性和可扩展性、支持通过新的EHR版本或应用程序实现增长
- 成本效益
- 易管理性，稳定性和易支持性
- 强大的数据保护，备份，恢复和业务连续性

FlexPod 已通过EHR验证、支持一个平台、其中包含采用Intel Xeon处理器的Cisco UCS、Red Hat Enterprise Linux (RHEL)以及采用VMware ESXi的虚拟化。此平台加上EHR在运行ONTAP 的NetApp存储方面的高舒适性级别排名、让客户有信心通过FlexPod 在完全托管的私有云中运行其医疗保健应用程序、该私有云也可以连接到任何公共云提供商。

NetApp BlueXP

BlueXP (原NetApp Cloud Manager)是一款基于SaaS的企业级管理平台、IT专家和云架构师可以利用NetApp云解决方案集中管理混合多云基础架构。它提供了一个集中式系统、用于查看和管理内部和云存储、支持混合、多个云提供商和客户。有关详细信息，请参见 "BlueXP"。

连接器

借助Connector实例、BlueXP可以管理公共云环境中的资源和流程。BlueXP提供的许多功能都需要连接器、并且可以部署在云或内部网络中。

连接器在以下位置受支持：

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- 内部部署

要了解有关Connector的更多信息、请参见 "连接器页面"。

NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP 是一款软件定义的存储产品、可在云中运行ONTAP 数据管理软件、为文件和块工作负载提供高级数据管理。借助Cloud Volumes ONTAP 、您可以优化云存储成本并提高应用程序性能、同时

增强数据保护、安全性和合规性。

主要优势包括：

- *存储效率。*利用内置的重复数据删除、数据压缩、精简配置和即时克隆功能最大限度地降低存储成本。
- *高可用性。*在云环境发生故障时提供企业级可靠性和持续运营。
- 数据保护。 Cloud Volumes ONTAP 使用行业领先的NetApp复制技术SnapMirror将内部数据复制到云、以便可以轻松地为多种使用情形提供二级副本。Cloud Volumes ONTAP 还与云备份相集成、提供备份和还原功能、以保护云数据并对其进行长期归档。
- *数据分层。*按需在高性能和低性能存储池之间切换、而无需使应用程序脱机。
- *应用程序一致性。*使用NetApp SnapCenter 技术提供NetApp Snapshot副本的一致性。
- 数据安全。 Cloud Volumes ONTAP 支持数据加密、并提供防病毒和勒索软件保护。
- *隐私合规性控制。*与Cloud Data sense集成有助于您了解数据环境并识别敏感数据。

有关更多详细信息，请参见 "Cloud Volumes ONTAP"。

NetApp Active IQ Unified Manager

借助NetApp Active IQ Unified Manager 、您可以通过一个经过重新设计的直观界面监控ONTAP 存储集群、从而利用社区智慧和AI分析提供智能。它可以全面洞察存储环境及其运行的虚拟机的运行状况、性能和主动性。当存储基础架构发生问题描述 时、Unified Manager可以通知您问题描述 的详细信息、以帮助识别根发生原因。通过虚拟机信息板、您可以查看虚拟机的性能统计信息、以便调查从vSphere主机向下经过网络并最终到达存储的整个I/O路径。

某些事件还提供了可用于更正问题描述 的补救措施。您可以为事件配置自定义警报、以便在发生问题时、通过电子邮件和SNMP陷阱通知您。通过Active IQ Unified Manager 、您可以通过预测容量和使用趋势来规划用户的存储需求、以便在出现问题之前采取行动、防止做出长期可能导致其他问题的被动短期决策。

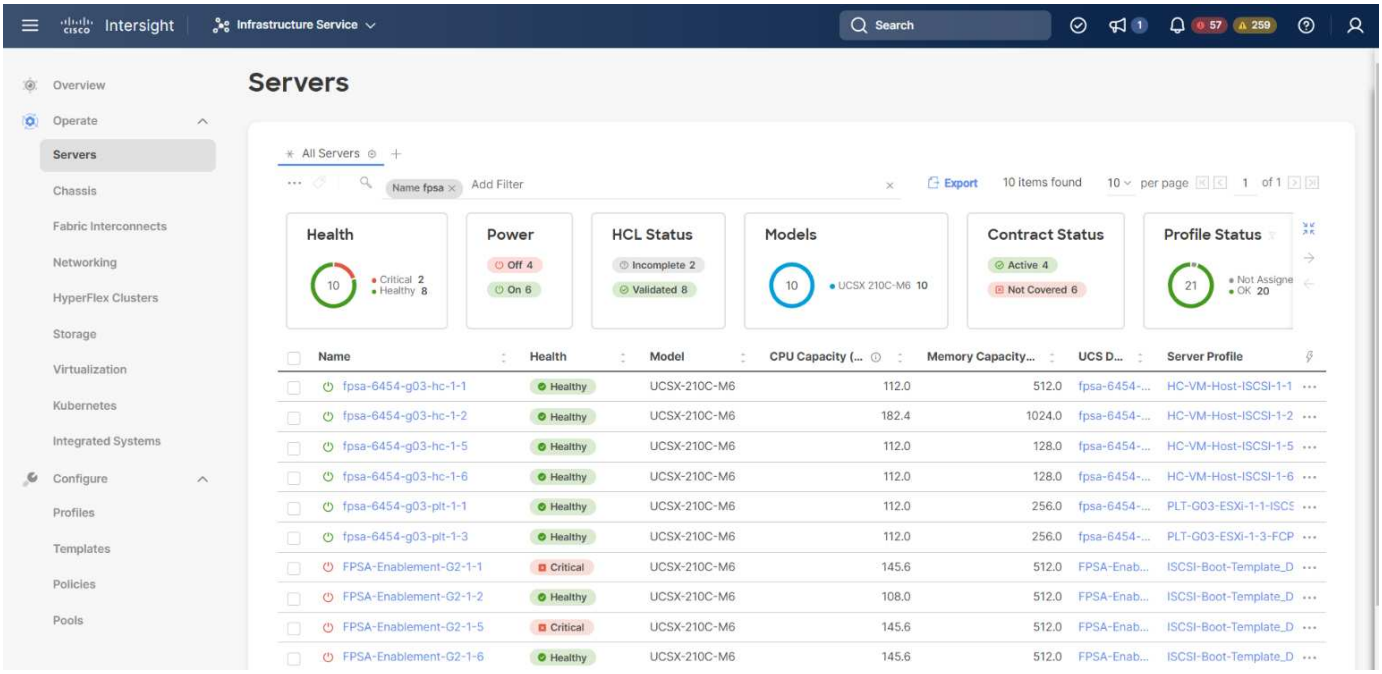
有关详细信息，请参见 "Active IQ Unified Manager"。

Cisco Intersight

Cisco Intersight是一个SaaS平台、可为传统和云原生应用程序和基础架构提供智能自动化、可观察性和优化功能。该平台有助于推动IT团队的变革、并提供专为混合云设计的运营模式。Cisco Intersight具有以下优势：

- 更快的交付速度。 Intersight通过基于敏捷性的软件开发模式、以云或客户数据中心的服务形式提供、并经常进行更新和持续创新。这样、客户就可以专注于满足关键业务需求。
- 简化操作。 Intersight使用一个安全的SaaS交付工具、该工具具有通用清单、身份验证和API、可在整个堆栈和所有位置运行、从而简化操作、消除团队之间的孤岛。这样、您就可以管理内部、VM、K8s、无服务器、自动化、 在内部和公共云中实现优化并控制成本。
- *持续优化。*您可以利用Cisco Intersight在每一层提供的智能以及Cisco TAC提供的智能来持续优化您的环境。这种智能将转换为建议的可自动化操作、以便您可以实时适应任何变化：从移动工作负载和监控物理服务器的运行状况到为您使用的公共云提供成本降低建议。

Cisco Intersight支持两种管理操作模式：UCSM受管模式(Umm)和Intersight受管模式(IMM)。在初始设置互联阵列期间、您可以为光纤连接的Cisco UCS系统选择本机UCSM受管模式(Umm)或视间受管模式(IMM)。在此解决方案 中、使用原生 IMM。下图显示了Cisco Intersight信息板。



VMware vSphere 7.0

VMware vSphere是一个虚拟化平台、可将大量基础架构(包括CPU、存储和网络)作为一个无缝、多功能且动态的操作环境进行全面管理。与管理单个计算机的传统操作系统不同、VMware vSphere可将整个数据中心的基础架构聚合在一起、从而创建一个具有资源的动力中心、这些资源可以快速动态地分配给任何需要的应用程序。

有关VMware vSphere及其组件的详细信息、请参见 "VMware vSphere"。

VMware vCenter Server

VMware vCenter Server可通过一个控制台统一管理所有主机和VM、并对集群、主机和VM进行聚合性能监控。通过VMware vCenter Server、管理员可以深入了解计算集群、主机、虚拟机、存储、子操作系统、 虚拟基础架构的其他关键组件。VMware vCenter可管理VMware vSphere环境中提供的丰富功能。

有关详细信息、请参见 "VMware vCenter"。

硬件和软件版本

此混合云解决方案 可扩展到运行中定义的受支持软件、固件和硬件版本的任何FlexPod 环境 "NetApp 互操作性表工具"， "UCS硬件和软件兼容性"，和 "VMware 兼容性指南"。

下表显示了内部FlexPod 硬件和软件版本。

组件	产品	**version**
计算	Cisco UCS X210c M6	5.0 (1b)
	Cisco UCS互联阵列6454	4.2 (2a)
网络	Cisco Nexus 9336C-x2 NX-OS	9.3 (9)
存储	NetApp AFF A400	ONTAP 9.11.1P2
	适用于 VMware vSphere 的 NetApp ONTAP 工具	9.11

组件	产品	**version**
	适用于 VMware VAAI 的 NetApp NFS 插件	2.0
	NetApp Active IQ Unified Manager	9.11P1
软件	VMware vSphere	7.0 (U3)
	VMware ESXi nenic 以太网驱动程序	1.0.35.0
	VMware vCenter设备	7.0.3
	Cisco Intersight Assist虚拟设备	1.0.9-342

下表显示了NetApp BlueXP和Cloud Volumes ONTAP 版本。

供应商	产品	**version**
NetApp	BlueXP	3.9.24
	Cloud Volumes ONTAP	ONTAP 9.11

"下一步：安装和配置。"

安装和配置

"先前版本：解决方案 组件。"

NetApp Cloud Volumes ONTAP 部署

完成以下步骤以配置Cloud Volumes ONTAP 实例：

1. 准备公共云服务提供商环境。

   您必须捕获解决方案 配置的公共云服务提供商的环境详细信息。例如、对于Amazon Web Services (AWS)环境准备、您需要AWS访问密钥、AWS机密密钥以及区域、VPC、子网等其他网络详细信息。

2. 配置VPC端点网关。

   要启用VPC与AWS S3服务之间的连接、需要使用VPC端点网关。此操作用于在CVO上启用备份、CVO是网关类型的端点。

3. 访问NetApp BlueXP。

   要访问NetApp BlueXP和其他云服务、您需要注册 "NetApp BlueXP"。要在BlueXP帐户中设置工作空间和用户、请单击 "此处"。您需要一个有权直接从BlueXP在云提供商中部署Connector的帐户。您可以从下载BlueXP策略 "此处"。

4. 部署Connector。

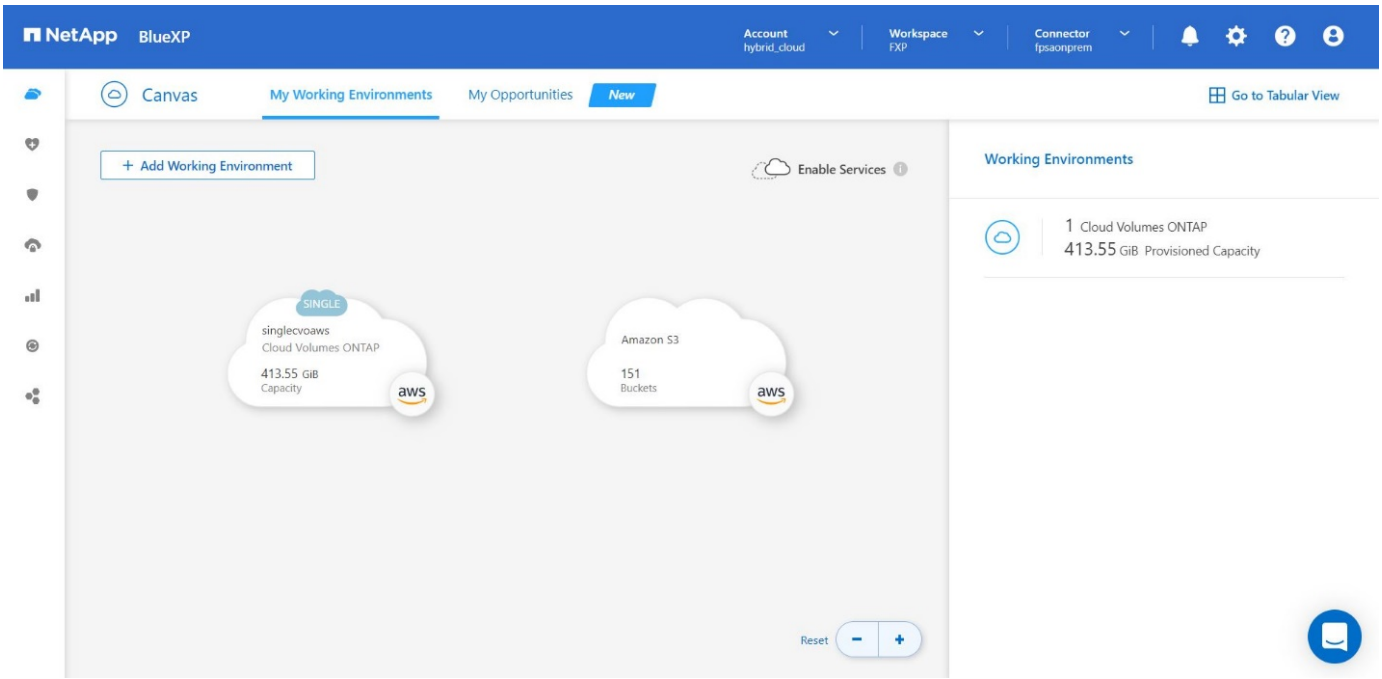
   在添加Cloud Volume ONTAP 工作环境之前、您必须先部署Connector。如果您尝试在没有连接器的情况下创建首个Cloud Volumes ONTAP 工作环境、BlueXP将提示您。要从BlueXP在AWS中部署Connector、请参见此内容 "链接。"。

5. 在AWS中启动Cloud Volumes ONTAP。

   您可以在单系统配置中或在 AWS 中作为 HA 对启动 Cloud Volumes ONTAP 。 "阅读分步说明"。

   有关这些步骤的详细信息、请参见 "AWS中的Cloud Volumes ONTAP 快速入门指南"。

   在此解决方案 中、我们在AWS中部署了单节点Cloud Volumes ONTAP 系统。下图展示了具有单节点CVO实例的NetApp BlueXP信息板。



内部**FlexPod** 部署

要了解采用UCS X系列的FlexPod 、VMware和NetApp ONTAP 的设计详细信息、请参见 "采用Cisco UCS X系列的FlexPod 数据中心" 设计指南。本文档提供了在FlexPod 数据中心基础架构中整合Cisco Intersight-managed UCS X系列平台的设计指导。

有关部署内部FlexPod 实例的信息、请参见 "本部署指南"。

本文档提供了在FlexPod 数据中心基础架构中整合Cisco Intersight-managed UCS X系列平台的部署指导。本文档介绍了成功部署的配置和最佳实践。

FlexPod 既可以部署在UCS托管模式下、也可以部署在Cisco Intersight托管模式(IMM)下。如果要在UCS托管模式下部署FlexPod 、请参见此内容 "设计指南" 这是 "部署指南"。

使用Ansible可以通过基础架构作为代码自动部署FlexPod。下面是用于端到端FlexPod 部署的GitHub存储库的链接：

- 可以看到在UCS托管模式、NetApp ONTAP 和VMware vSphere下使用Cisco UCS的FlexPod 的可识别配置 "此处"。
- 可以看到在IMM、NetApp ONTAP 和VMware vSphere中使用Cisco UCS的FlexPod 的可识别配置 "此处"。

内部**ONTAP** 存储配置

本节介绍特定于此解决方案 的一些重要ONTAP 配置步骤。

1. 在运行iSCSI服务的情况下配置SVM。

```
1. vserver create –vserver Healthcare_SVM –rootvolume
Healthcare_SVM_root –aggregate aggr1_A400_G0312_01 –rootvolume-security-
style unix
2. vserver add-protocols -vserver Healthcare_SVM -protocols iscsi
3. vserver iscsi create -vserver Healthcare_SVM

   To verify:

   A400-G0312::> vserver iscsi show -vserver Healthcare_SVM
   Vserver: Healthcare_SVM
   Target Name:
   iqn.1992-08.com.netapp:sn.1fbf00f438c111ed866cd039ea91fb56:vs.3
   Target Alias: Healthcare_SVM
   Administrative Status: up
```

   如果在集群配置期间未安装iSCSI许可证、请确保在创建iSCSI服务之前安装此许可证。

2. 创建FlexVol 卷。

```
1. volume create -vserver Healthcare_SVM -volume hc_iscsi_vol -aggregate
aggr1_A400_G0312_01 -size 500GB -state online -policy default -space
guarantee none
```

3. 添加用于iSCSI访问的接口。

```
1. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01a
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node01-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
2. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01b
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node01-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> -status-admin up
3. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02a
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node02-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
4. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02b
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node02-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> -status-admin up
```

在此解决方案 中、我们创建了四个iSCSI逻辑接口(LIF)、每个节点上两个。

在部署了vCenter并向其添加了所有ESXi主机的情况下启动并运行FlexPod 实例后、我们需要部署一个Linux VM、该VM充当连接和访问NetApp ONTAP 存储的服务器。在此解决方案 中、我们已在vCenter中安装CentOS 8实例。

4. 创建LUN。

```
1. lun create -vserver Healthcare_SVM -path /vol/hc_iscsi_vol/iscsi_lun1
-size 200GB -ostype linux -space-reserve disabled
```

对于EHR操作数据库(ODB)、日志和应用程序工作负载、EHR建议将存储作为iSCSI LUN提供给服务器。如果您的AIX和RHEL操作系统版本支持、则NetApp还支持使用FCP和NVMe/FC、从而提高性能。FCP和NVMe/FC可以同时位于同一个网络结构中。

5. 创建igroup。

```
1. igroup create -vserver Healthcare_SVM -igroup ehr -protocol iscsi
-ostype linux -initiator iqn.1994-05.com.redhat:8e91e9769336
```

igroup用于允许服务器访问LUN。对于Linux主机、可以在文件中找到服务器IQN `/etc/iscsi/initiatorname.iscsi`。

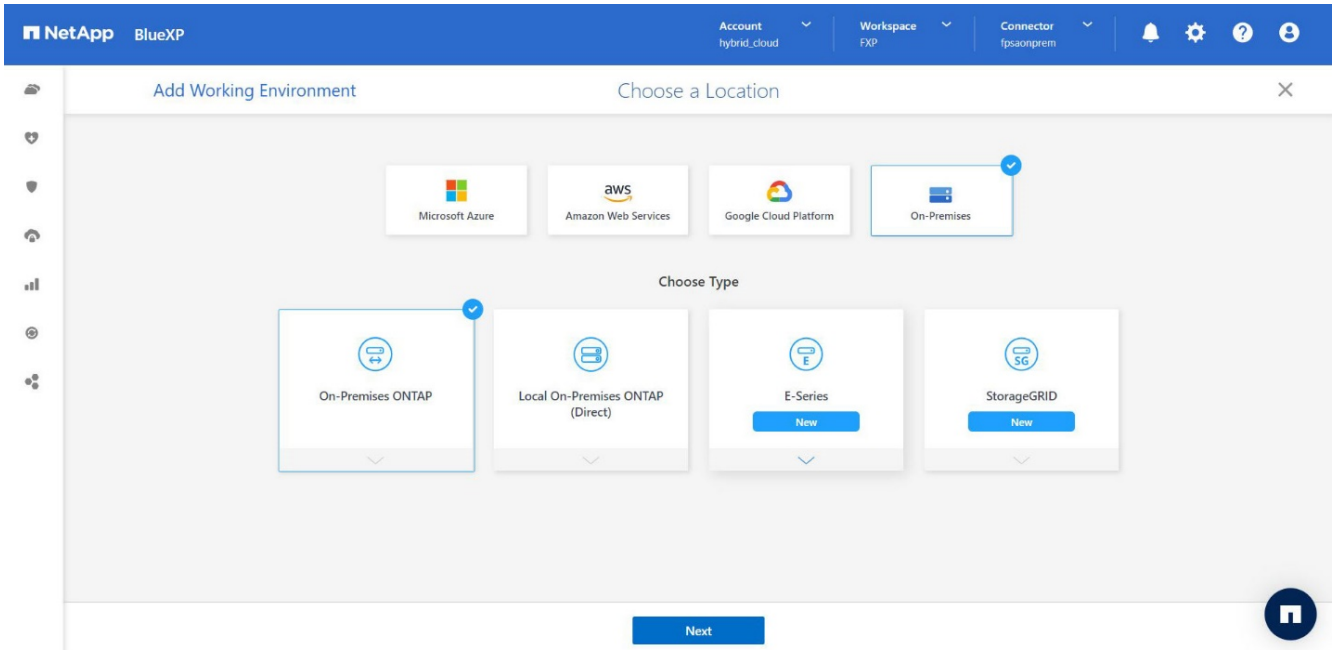
6. 将 LUN 映射到 igroup 。

```
1. lun mapping create -vserver Healthcare_SVM -path
/vol/hc_iscsi_vol/iscsi_lun1 -igroup ehr -lun-id 0
```

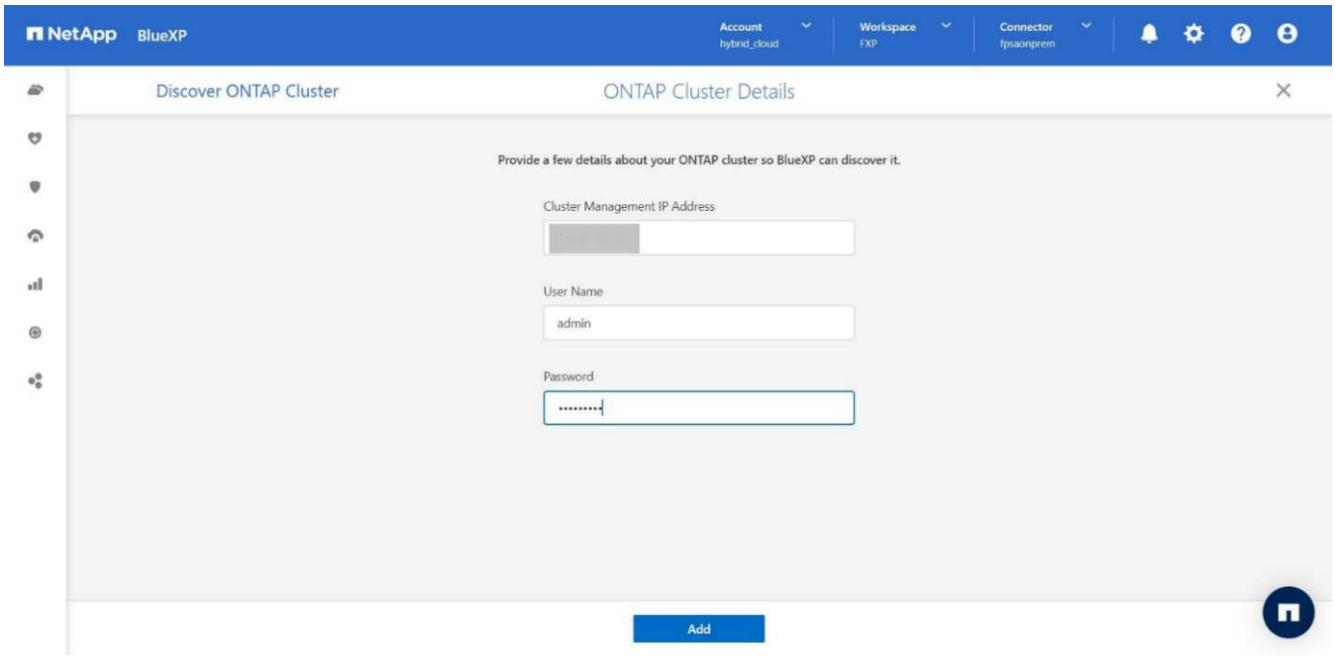
将内部**FlexPod** 存储添加到**BlueXP**

要使用NetApp BlueXP将FlexPod 存储添加到工作环境、请完成以下步骤。

1. 从导航菜单中、选择*存储*>*画布*。
2. 在"画布"页面上、单击*添加工作环境*并选择*内部部署*。
3. 选择*内部部署ONTAP *。单击 * 下一步 * 。

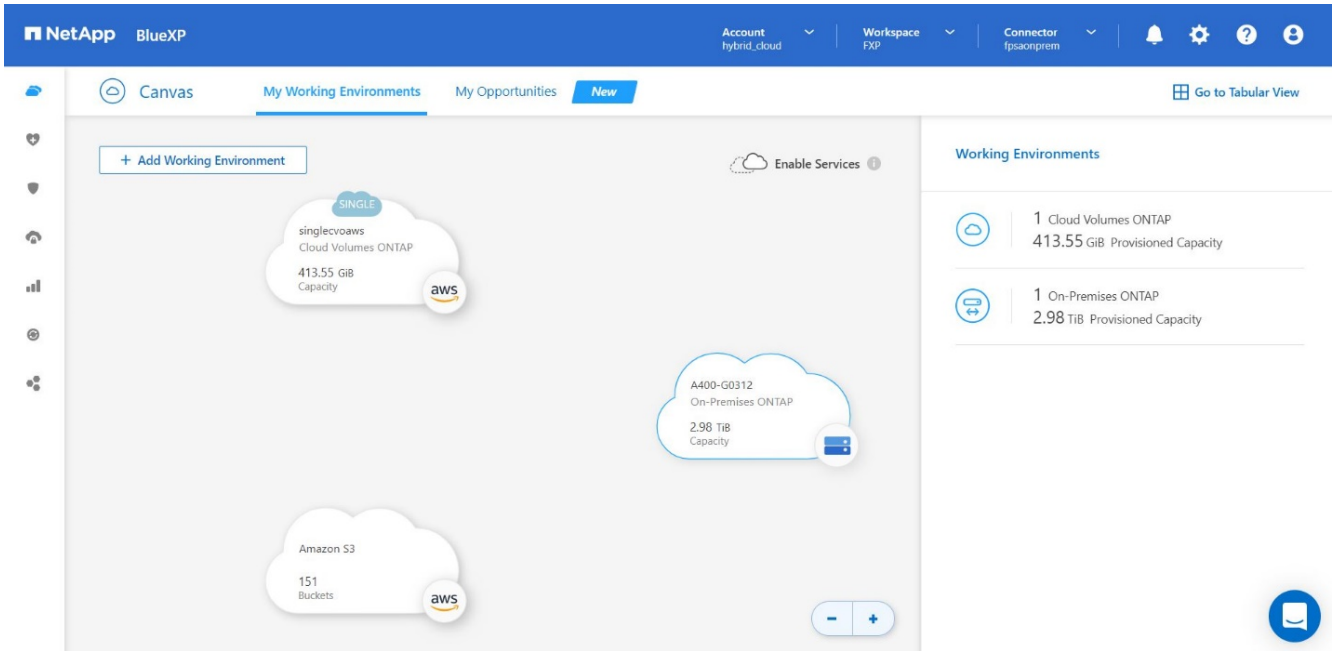


4. 在 "ONTAP 集群详细信息 " 页面上，输入管理员用户帐户的集群管理 IP 地址和密码。然后单击*添加*。



5. 在详细信息和凭据页面上、输入工作环境的名称和问题描述 、然后单击*执行*。

   BlueXP会发现ONTAP 集群并将其添加为Canvas上的工作环境。



有关详细信息、请参见页面 "发现内部ONTAP 集群"。

"下一步：SAN配置。"

SAN 配置

"先前版本：安装和配置。"

本节介绍EHR为使软件与NetApp存储实现最佳集成而需要的主机端配置。在此部分中、我

们将专门讨论Linux操作系统的主机集成。使用 "NetApp 互操作性表工具（IMT）" 验证所有版本的软件和固件。

> 以下配置步骤特定于此解决方案 中使用的CentOS 8主机。

NetApp主机实用程序套件

NetApp建议在连接到和访问NetApp存储系统的主机的操作系统上安装NetApp Host Utility Kit (Host Utilities)。支持本机Microsoft多路径I/O (MPIO)。操作系统必须支持多路径的非对称逻辑单元访问(ALUA)。安装Host Utilities可为NetApp存储配置主机总线适配器(HBA)设置。

可以下载NetApp Host Utilities "此处"。在此解决方案 中、我们已在主机上安装Linux Host Utilities 7.1。

```
[root@hc-cloud-secure-1 ~]# rpm -ivh netapp_linux_unified_host_utilities-
7-1.x86_64.rpm
```

发现**ONTAP** 存储

确保iSCSI服务在应进行登录时正在运行。要为目标上的特定门户或目标上的所有门户设置登录模式、请使用 `iscsiadm` 命令：

```
[root@hc-cloud-secure-1 ~]# rescan-scsi-bus.sh
[root@hc-cloud-secure-1 ~]# iscsiadm -m discovery -t sendtargets -p
<iscsi-lif-ip>
[root@hc-cloud-secure-1 ~]# iscsiadm -m node -L all
```

现在、您可以使用 `sanlun` 显示有关连接到主机的LUN的信息。确保以root身份登录到主机。

```
[root@hc-cloud-secure-1 ~]# sanlun lun show
controller(7mode/E-Series)/
                                     device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
---
Healthcare_SVM                        /dev/sdb host33  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1

Healthcare_SVM                        /dev/sdc host34  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1
```

配置多路径

设备映射程序多路径(DM-Multipath)是Linux中的本机多路径实用程序。它可用于实现冗余并提高性能。它可以聚合或组合服务器和存储之间的多个I/O路径、从而在操作系统级别创建一个设备。

1. 在系统上设置DM-Multipath之前、请确保您的系统已更新并包含 `device-mapper-multipath` 软件包。

```
[root@hc-cloud-secure-1 ~]# rpm -qa|grep multipath
device-mapper-multipath-libs-0.8.4-31.el8.x86_64
device-mapper-multipath-0.8.4-31.el8.x86_64
```

2. 配置文件为 `/etc/multipath.conf` 文件按如下所示更新配置文件。

```
[root@hc-cloud-secure-1 ~]# cat /etc/multipath.conf
defaults {
   path_checker      readsector0
   no_path_retry      fail
}
devices {
   device {
      vendor         "NETAPP  "
      product         "LUN.*"
      no_path_retry     queue
      path_checker      tur
   }
}
```

3. 启用并启动多路径服务。

```
[root@hc-cloud-secure-1 ~]# systemctl enable multipathd.service
[root@hc-cloud-secure-1 ~]# systemctl start  multipathd.service
```

4. 添加可加载的内核模块 `dm-multipath` 并重新启动多路径服务。最后、检查多路径状态。

```
[root@hc-cloud-secure-1 ~]# modprobe -v dm-multipath
insmod /lib/modules/4.18.0-408.el8.x86_64/kernel/drivers/md/dm-
multipath.ko.xz

[root@hc-cloud-secure-1 ~]# systemctl restart multipathd.service

[root@hc-cloud-secure-1 ~]# multipath -ll
3600a09803831494c372b545a4d786278 dm-2 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 33:0:0:0 sdb 8:16 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
`- 34:0:0:0 sdc 8:32 active ready running
```

有关这些步骤的详细信息、请参见 "此处"。

创建物理卷

使用 `pvcreate` 用于初始化块设备以用作物理卷的命令。初始化类似于格式化文件系统。

```
[root@hc-cloud-secure-1 ~]# pvcreate /dev/sdb
Physical volume "/dev/sdb" successfully created.
```

创建卷组

要从一个或多个物理卷创建卷组、请使用 `vgcreate` 命令：此命令将按名称创建一个新卷组、并至少向其中添加一个物理卷。

```
[root@hc-cloud-secure-1 ~]# vgcreate datavg /dev/sdb
Volume group "datavg" successfully created.
```

。 `vgdisplay` 命令可用于以固定形式显示卷组属性(例如大小、块区、物理卷数量等)。

```
[root@hc-cloud-secure-1 ~]# vgdisplay datavg
  --- Volume group ---
  VG Name               datavg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  1
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                0
  Open LV               0
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               <200.00 GiB
  PE Size               4.00 MiB
  Total PE              51199
  Alloc PE / Size       0 / 0
  Free  PE / Size       51199 / <200.00 GiB
  VG UUID               C7jmI0-J0SS-Cq91-t6b4-A9xw-nTfi-RXcy28
```

创建逻辑卷

创建逻辑卷时、系统会使用卷组中的物理卷上的可用块区从卷组中划分逻辑卷。

```
[root@hc-cloud-secure-1 ~]# lvcreate - l 100%FREE -n datalv datavg
Logical volume "datalv" created.
```

此命令将创建一个名为的逻辑卷 `datalv` 这将使用卷组中的所有未分配空间 `datavg`。

创建文件系统

```
[root@hc-cloud-secure-1 ~]# mkfs.xfs -K /dev/datavg/datalv
meta-data=/dev/datavg/datalv     isize=512    agcount=4, agsize=13106944
blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=0 inobtcount=0
data     =                       bsize=4096   blocks=52427776, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=25599, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

创建要挂载的文件夹

```
[root@hc-cloud-secure-1 ~]# mkdir /file1
```

挂载文件系统

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1

[root@hc-cloud-secure-1 ~]# df -k
Filesystem                 1K-blocks    Used Available Use% Mounted on
devtmpfs                     8072804       0   8072804   0% /dev
tmpfs                        8103272       0   8103272   0% /dev/shm
tmpfs                        8103272    9404   8093868   1% /run
tmpfs                        8103272       0   8103272   0% /sys/fs/cgroup
/dev/mapper/cs-root         45496624 5642104  39854520  13% /
/dev/sda2                    1038336  258712    779624  25% /boot
/dev/sda1                     613184    7416    605768   2% /boot/efi
tmpfs                        1620652      12   1620640   1% /run/user/42
tmpfs                        1620652       0   1620652   0% /run/user/0
/dev/mapper/datavg-datalv 209608708 1494520 208114188   1% /file1
```

有关这些任务的详细信息、请参见页面 "使用CLI命令管理LVM"。

数据生成

`Dgen.pl` 是EHR I/O模拟器(GenerateIO)的perl脚本数据生成器。LUN中的数据是使用EHR生成的 `Dgen.pl` 脚本。此脚本用于创建类似于EHR数据库中的数据。

```
[root@hc-cloud-secure-1 ~]# cd GenerateIO-1.17.3/

[root@hc-cloud-secure-1 GenerateIO-1.17.3]# ./dgen.pl --directory /file1
--jobs 80

[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37
dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38
dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39
dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40
dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80

[root@hc-cloud-secure-1 file1]# df -k .
Filesystem                 1K-blocks  Used       Available  Use%  Mounted
on
/dev/mapper/datavg-datalv  209608708  178167156  31441552   85%   /file1
```

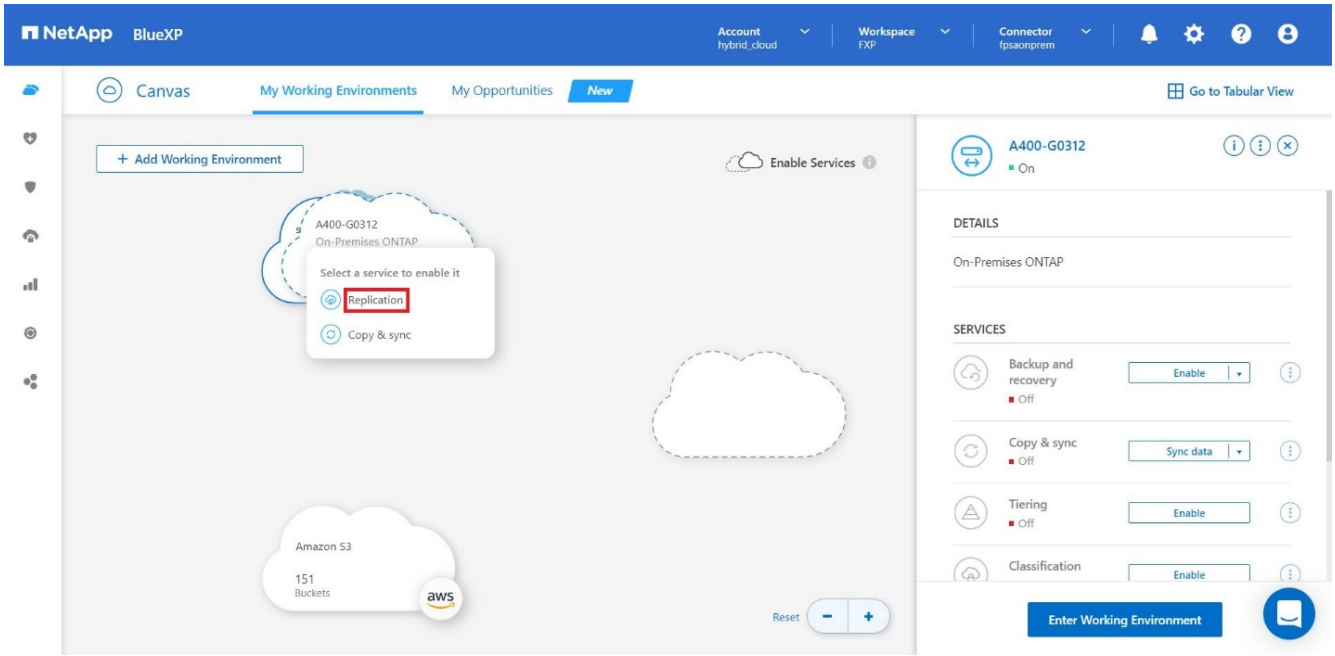
运行时、 `Dgen.pl` 默认情况下、脚本使用文件系统的85%来生成数据。

在内部**ONTAP** 和**Cloud Volumes ONTAP** 之间配置**SnapMirror**复制

NetApp SnapMirror 可通过 LAN 或 WAN 高速复制数据，从而在虚拟和传统环境中实现高数据可用性和快速数据复制。在将数据复制到 NetApp 存储系统并持续更新二级数据时，您的数据将保持最新，并在需要时保持可用。不需要外部复制服务器。

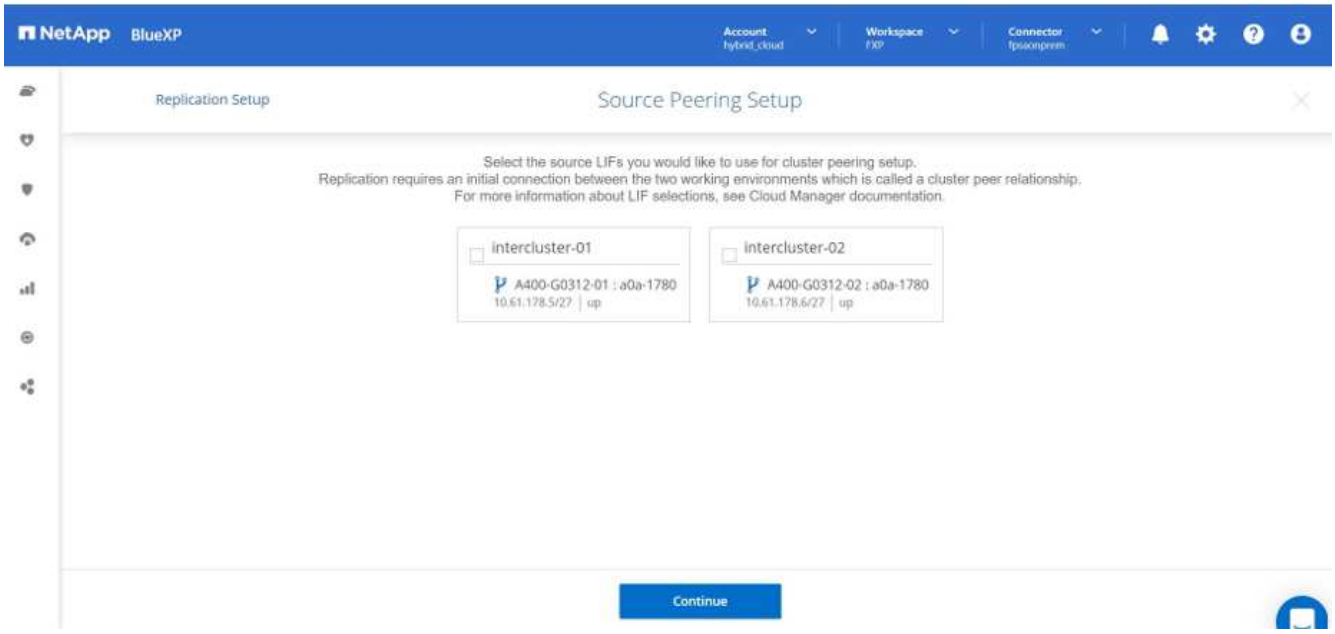
完成以下步骤以在内部ONTAP 系统和CVO之间配置SnapMirror复制。

1. 从导航菜单中、选择*存储*>*画布*。
2. 在Canvas中、选择包含源卷的工作环境、将其拖动到要将该卷复制到的工作环境中、然后选择*复制*。

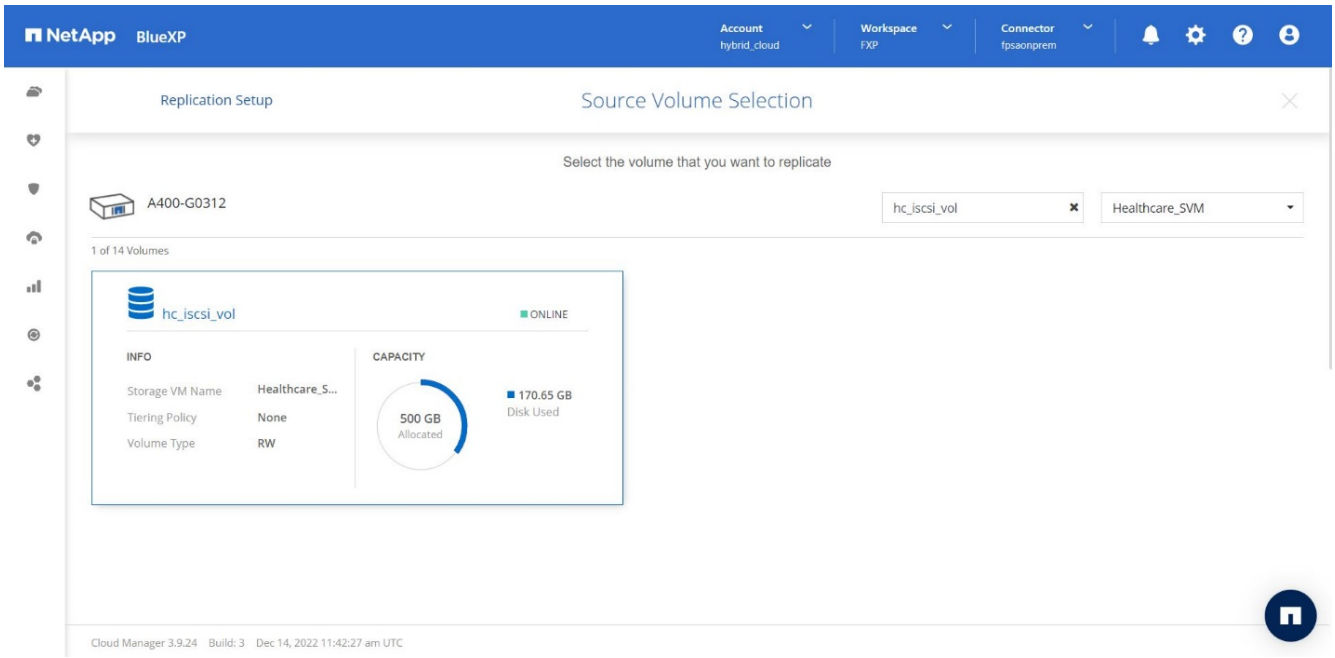


其余步骤将介绍如何在Cloud Volumes ONTAP 和内部ONTAP 集群之间创建同步关系。

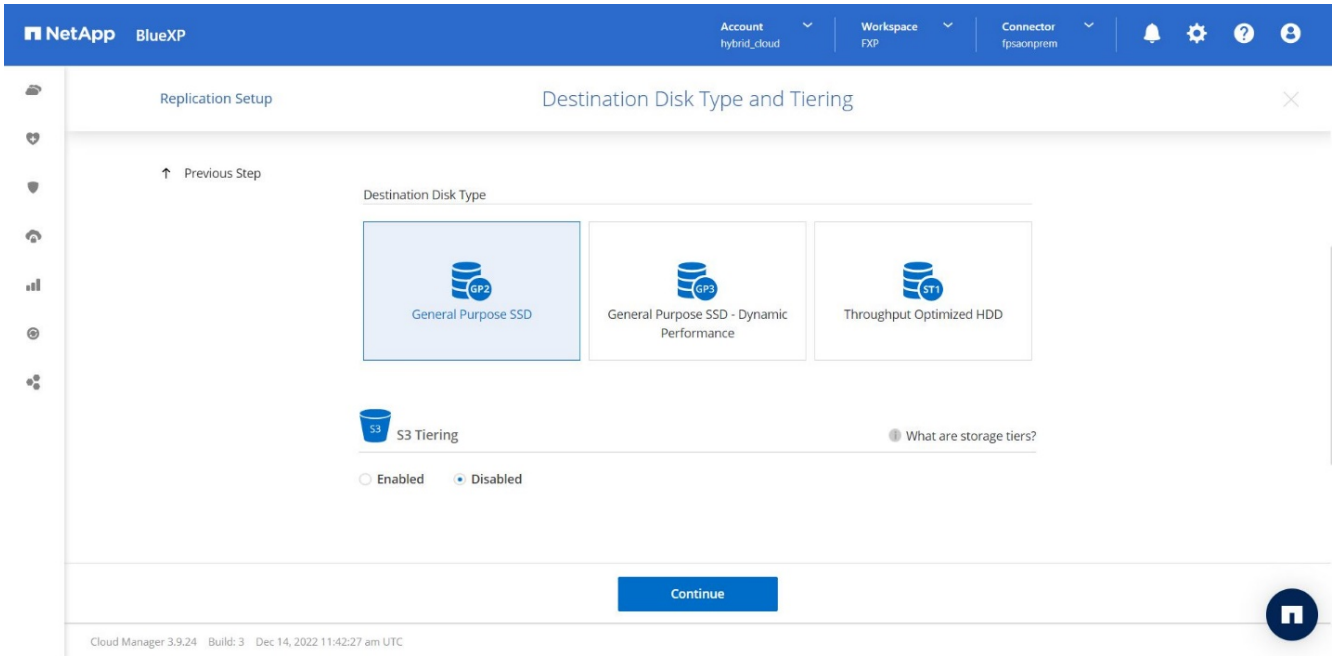
3. *源和目标对等设置。*如果显示此页面、请为集群对等关系选择所有集群间LIF。



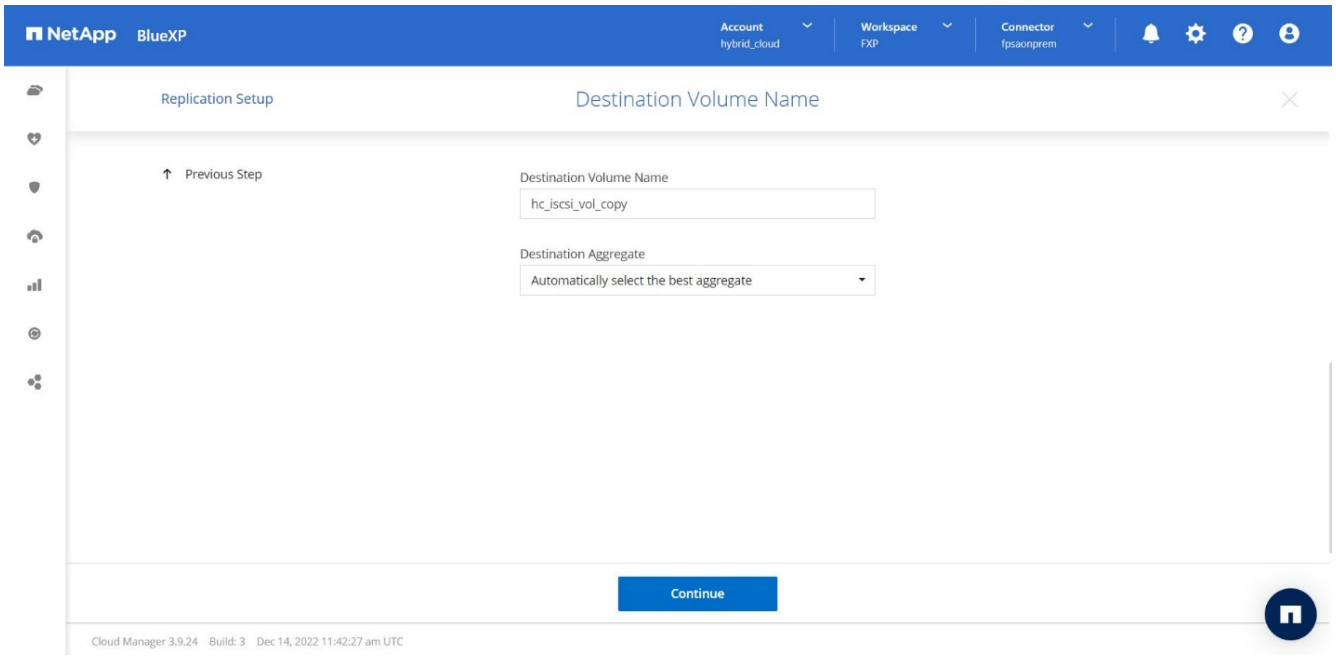
4. *源卷选择。*选择要复制的卷。



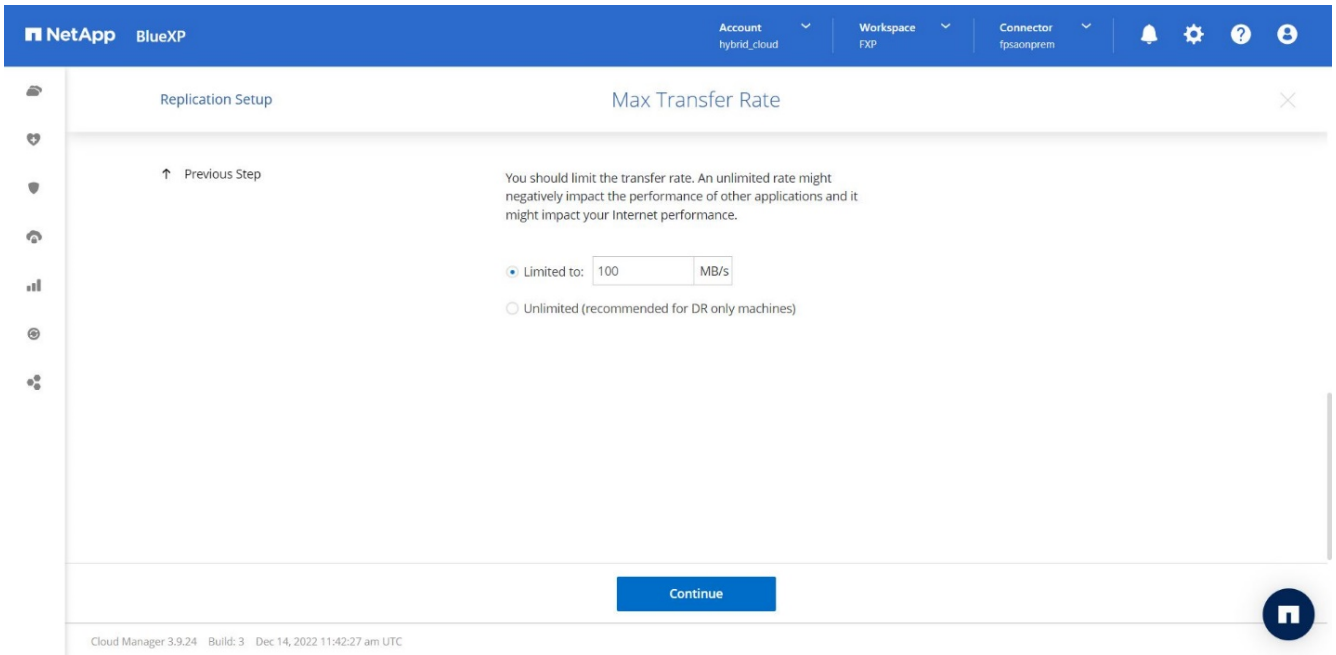
5. *目标磁盘类型和分层。*如果目标是Cloud Volumes ONTAP 系统、请选择目标磁盘类型、然后选择是否要启用数据分层。



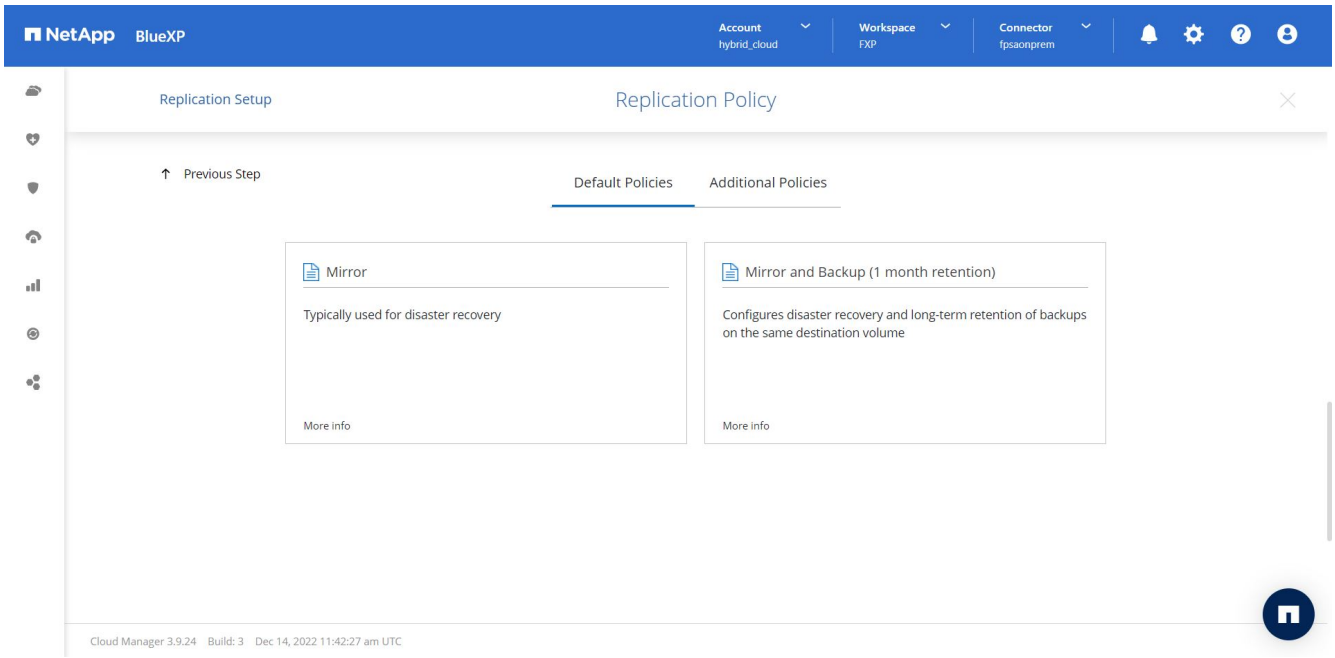
6. *目标卷名称：*指定目标卷名称并选择目标聚合。如果目标是 ONTAP 集群，则还必须指定目标 Storage VM 。



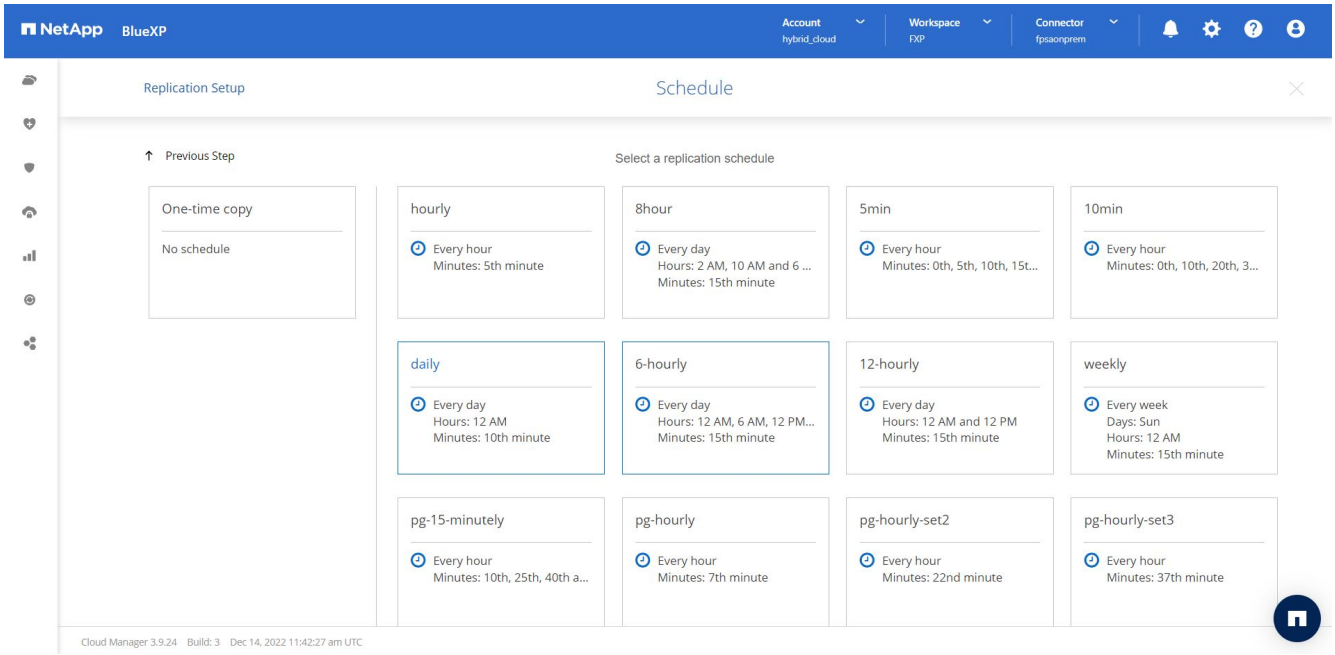
7. *最大传输速率。*指定可传输数据的最大速率(以MB/秒为单位)。



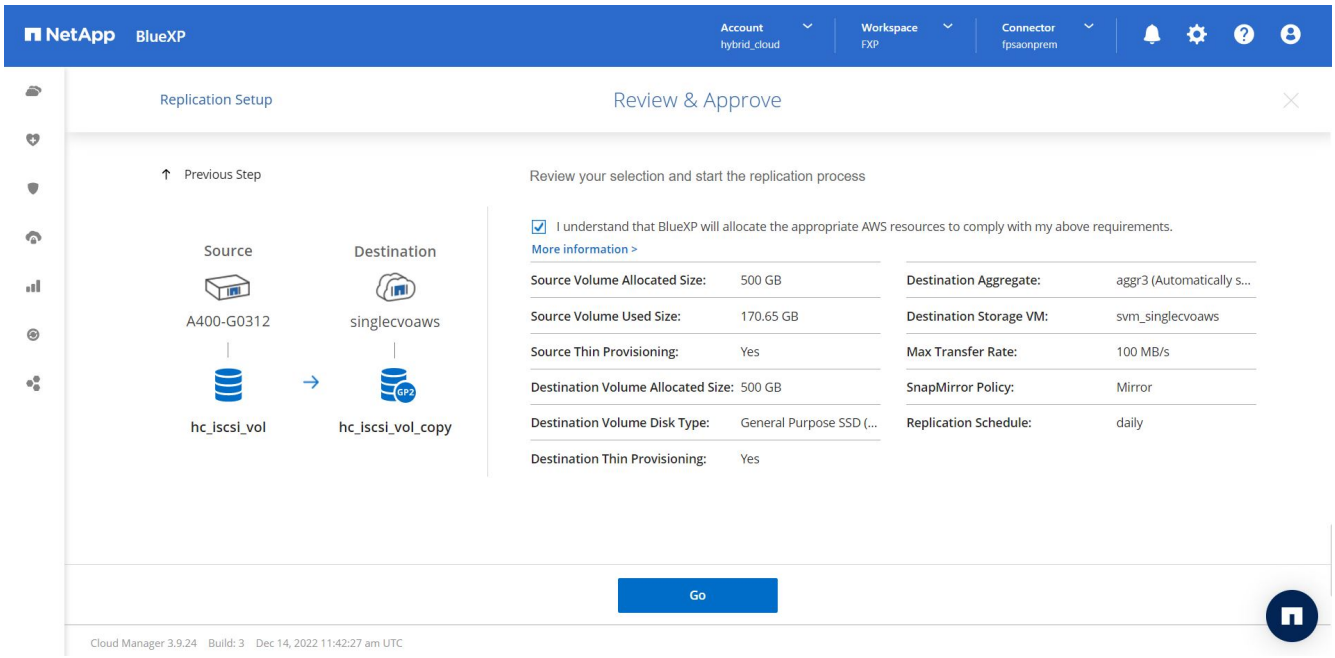
8. 复制策略。*选择一个默认策略或单击*其他策略、然后选择一个高级策略。如需帮助，"了解复制策略"。



9. *计划。*选择一次性副本或重复计划。有多个默认计划可用。如果您需要其他计划、则必须在上创建新计划 `destination cluster` 使用 System Manager 。

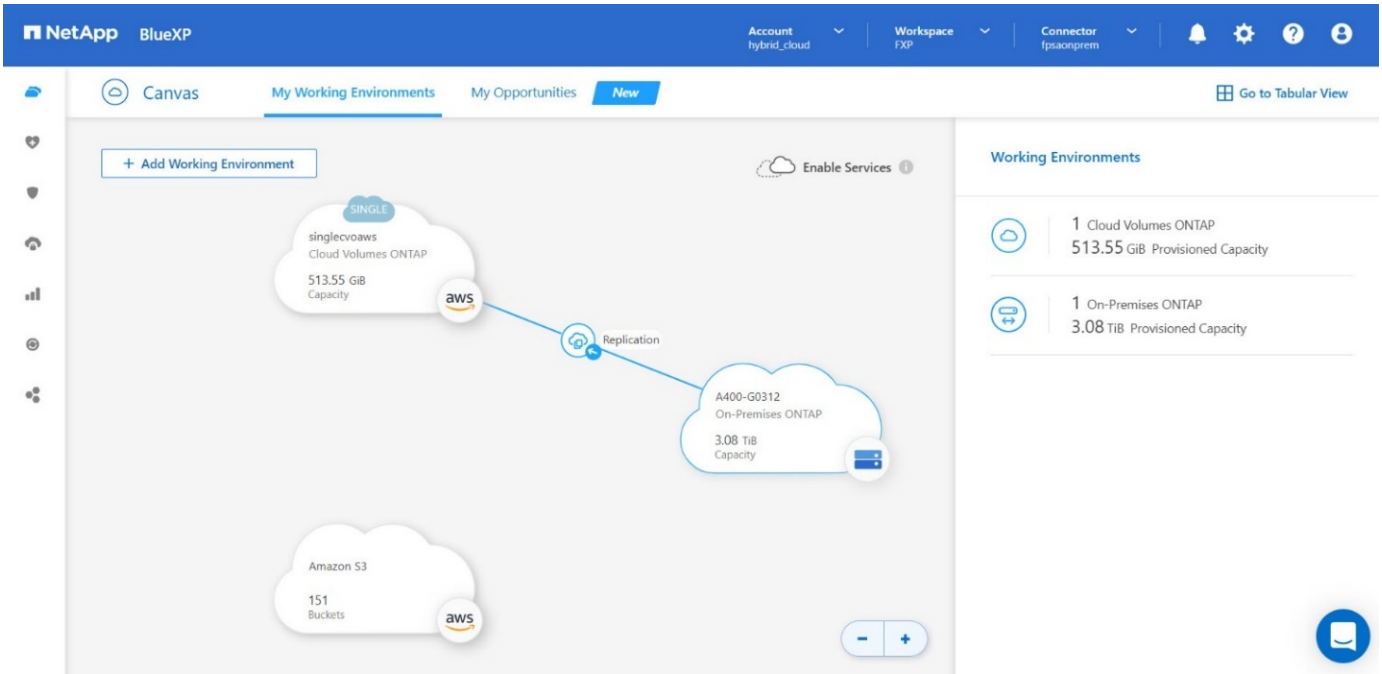


10. 查看。*查看您选择的内容、然后单击*执行。

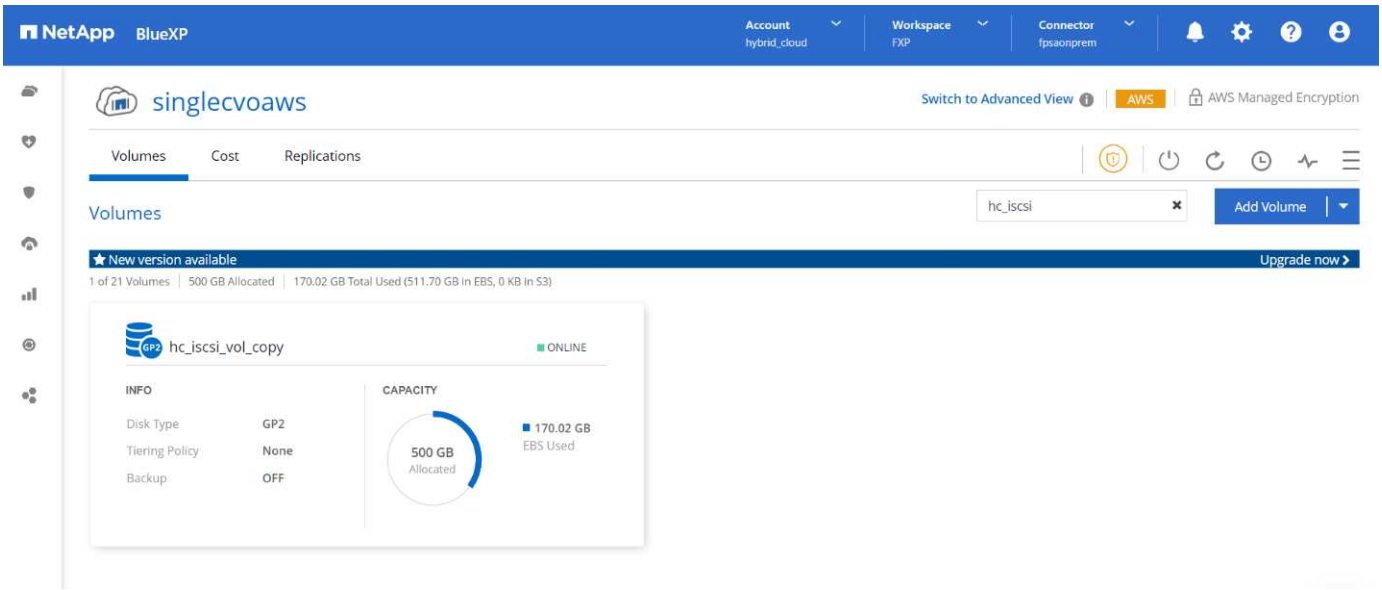


有关这些配置步骤的详细信息、请参见 "此处"。

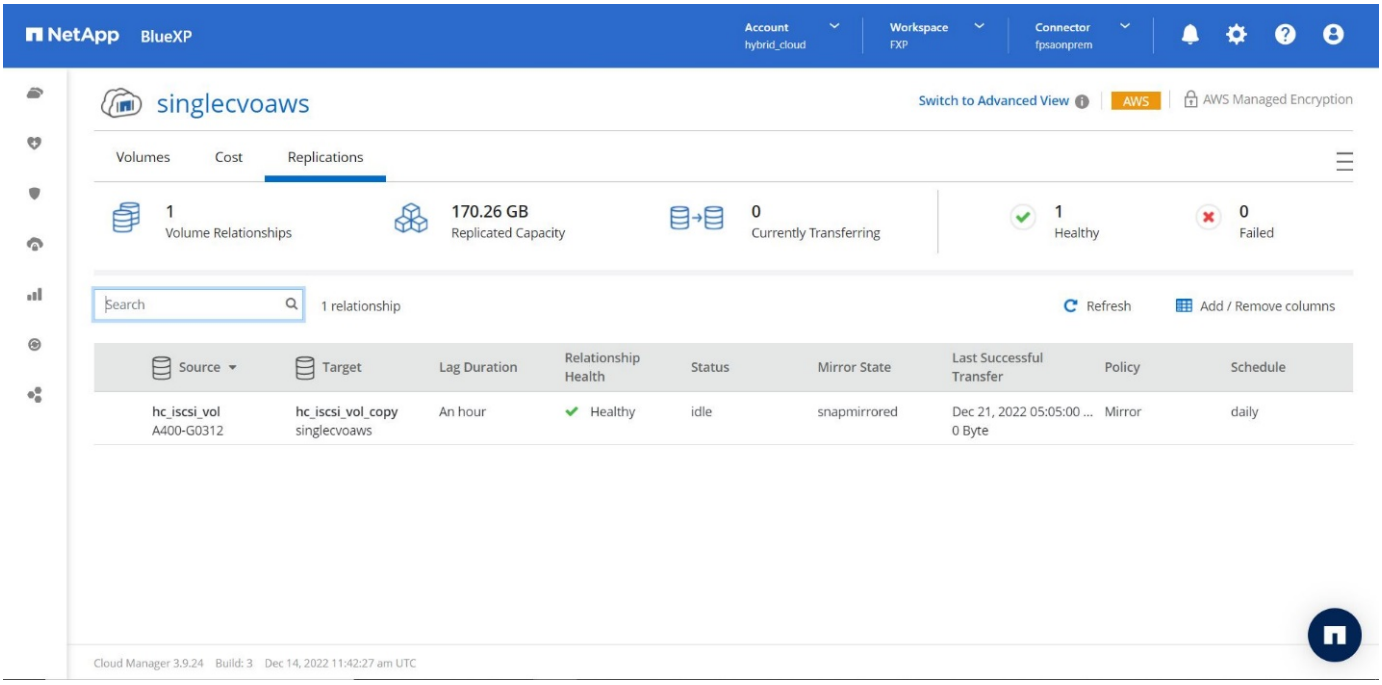
BlueXP将启动数据复制过程。现在、您可以看到在内部ONTAP 系统和Cloud Volumes ONTAP 之间建立的*复制*服务。



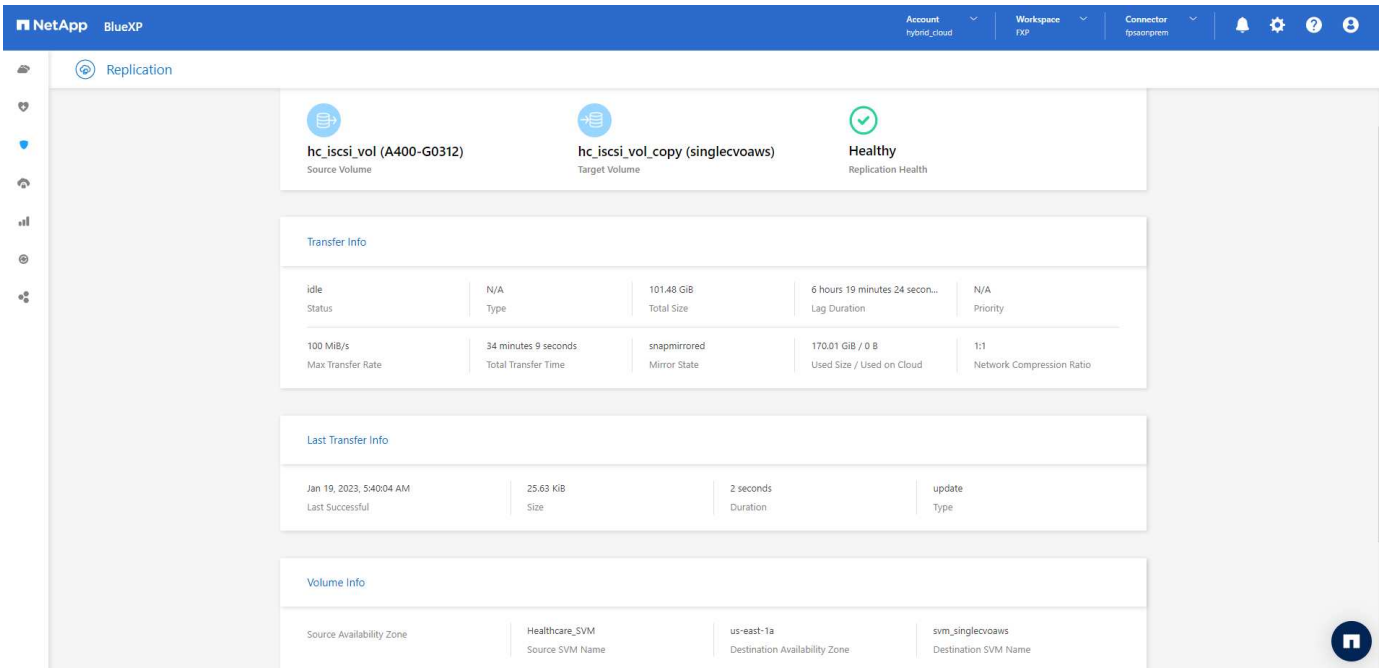
在Cloud Volumes ONTAP 集群中、您可以看到新创建的卷。



您还可以验证是否已在内部卷和云卷之间建立SnapMirror关系。



有关复制任务的详细信息、请参见*复制*选项卡。



"接下来：解决方案验证。"

解决方案验证

"先前版本：SAN配置。"

在本节中、我们将介绍一些解决方案 使用情形。

- SnapMirror的主要使用情形之一是数据备份。通过将数据复制到同一集群或远程目标、可以将SnapMirror用作主备份工具。
- 使用灾难恢复环境运行应用程序开发测试(开发/测试)。
- 灾难恢复。
- 数据分发和远程数据访问。

值得注意的是、此解决方案 中验证的相对较少的使用情形并不代表SnapMirror复制的整个功能。

应用程序开发和测试(开发/测试)

为了加快应用程序开发速度、您可以在灾难恢复站点快速克隆复制的数据并将其用于开发/测试应用程序。灾难恢复和开发/测试环境的主机代管可以显著提高备份或灾难恢复设施的利用率、并且按需开发/测试克隆可以根据需要提供尽可能多的数据副本、以便更快地投入生产。

NetApp FlexClone技术可用于快速创建SnapMirror目标FlexVol 卷的读写副本、以便您可以对二级副本进行读写访问、以确认所有生产数据是否可用。

要使用灾难恢复环境执行应用程序开发/测试、请完成以下步骤：

1. 创建生产数据的副本。为此、请为内部卷执行应用程序快照。应用程序快照创建包括三个步骤： `Lock`，`Snap`，和 `Unlock`。

    a. 暂停文件系统、以便暂停I/O并保持应用程序一致性。在步骤C中发出unquiesce命令之前、任何写入文件

系统的应用程序都会保持等待状态步骤a、b和c通过透明的流程或工作流执行、不会影响应用程序SLA。

```
[root@hc-cloud-secure-1 ~]# fsfreeze -f /file1
```

此选项请求在进行新修改时冻结指定的文件系统。任何尝试写入冻结文件系统的进程都会被阻止、直到文件系统被解除冻结为止。

b. 为内部卷创建快照。

```
A400-G0312::> snapshot create -vserver Healthcare_SVM -volume
hc_iscsi_vol -snapshot kamini
```

c. 取消暂停文件系统以重新启动I/O

```
[root@hc-cloud-secure-1 ~]# fsfreeze -u /file1
```

此选项用于取消冻结文件系统并允许操作继续。冻结阻止的任何文件系统修改均不会被阻止、并允许完成。

此外、还可以使用NetApp SnapCenter 执行应用程序一致的快照、NetApp在SnapCenter 中对上述工作流进行了完整的编排。有关详细信息、请参见 "此处"。

2. 执行SnapMirror更新操作以使生产系统和灾难恢复系统保持同步。

```
singlecvoaws::> snapmirror update -destination-path
svm_singlecvoaws:hc_iscsi_vol_copy -source-path
Healthcare_SVM:hc_iscsi_vol

Operation is queued: snapmirror update of destination
“svm_singlecvoaws:hc_iscsi_vol_copy”.
```

也可以通过BlueXP图形用户界面的*复制*选项卡执行SnapMirror更新。

3. 根据先前创建的应用程序快照创建FlexClone实例。

```
singlecvoaws::> volume clone create -flexclone kamini_clone -type RW
-parent-vserver svm_singlecvoaws -parent-volume hc_iscsi_vol_copy
-junction-active true -foreground true -parent-snapshot kamini

[Job 996] Job succeeded: Successful
```

对于上一项任务、也可以创建新的快照、但您必须按照上述相同步骤来确保应用程序一致性。

4. 激活FlexClone卷以在云中启动EHR实例。

```
singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path
/vol/kamini_clone/iscsi_lun1 -igroup ehr-igroup -lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                  Igroup    LUN ID
Protocol
---------- -------------- --------------- -----  --------   ------
---------
svm_singlecvoaws
                 /vol/kamini_clone/iscsi_lun1    ehr-igroup   0    iscsi
```

5. 在云中的EHR实例上执行以下命令以访问数据或文件系统。
   a. 发现ONTAP 存储。检查多路径状态。

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show

Output:
controller(7mode/E-Series)/         device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
---------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                    /vol/kamini_clone/iscsi_lun1
sudo multipath -ll

Output:
3600a09806631755a452b543041313053 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

   b. 激活卷组。

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

c. 挂载文件系统并显示文件系统信息的摘要。

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                 1K-blocks  Used     Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708 183987096  25621612  88%
/file1
```

这证明您可以使用灾难恢复环境进行应用程序开发/测试。通过在灾难恢复存储上执行应用程序开发/测试、您可以更多地利用资源、否则这些资源可能会在大部分时间处于闲置状态。

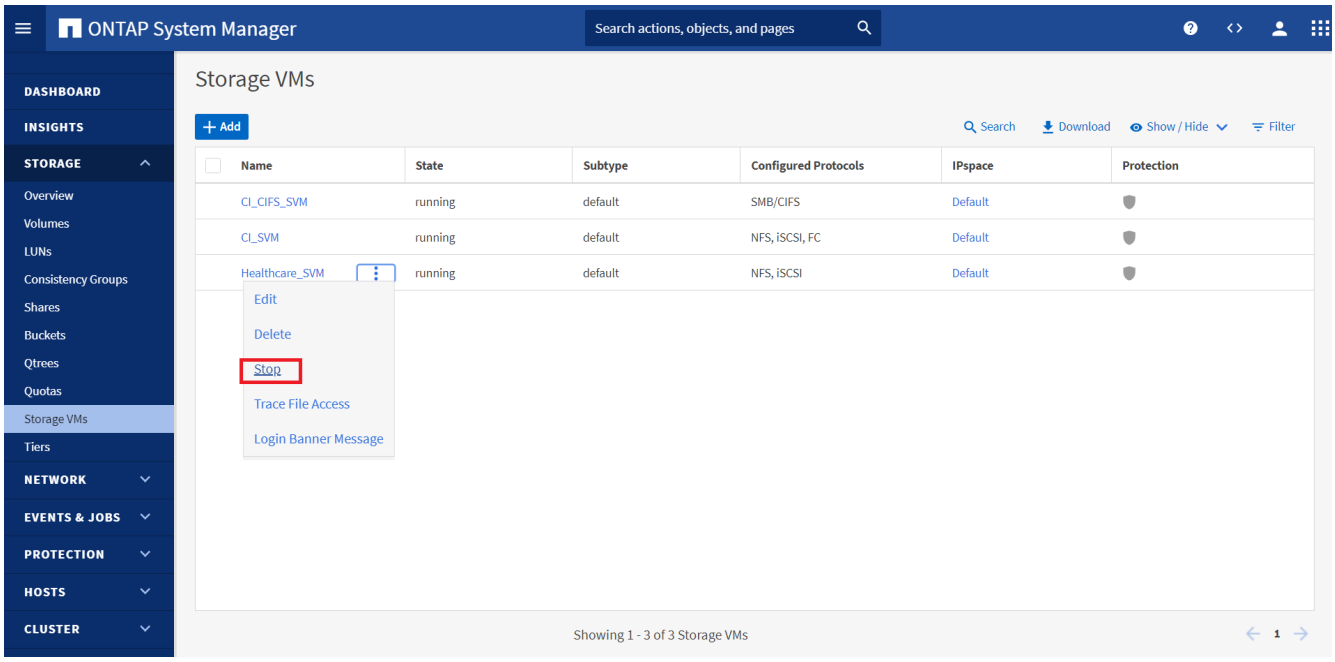
灾难恢复

SnapMirror技术也用作灾难恢复计划的一部分。如果将关键数据复制到其他物理位置、则发生严重灾难时、不必对业务关键型应用程序的数据长时间不可用进行发生原因 处理。客户端可以通过网络访问复制的数据、直到生产站点从损坏、意外删除、自然灾难等中恢复为止。

如果要故障恢复到主站点、SnapMirror可提供一种高效的方法来重新同步灾难恢复站点与主站点、只需反转SnapMirror关系、即可仅将更改过的数据或新数据从灾难恢复站点传输回主站点。主生产站点恢复正常应用程序操作后、SnapMirror将继续向灾难恢复站点传输数据、而无需再进行基线传输。

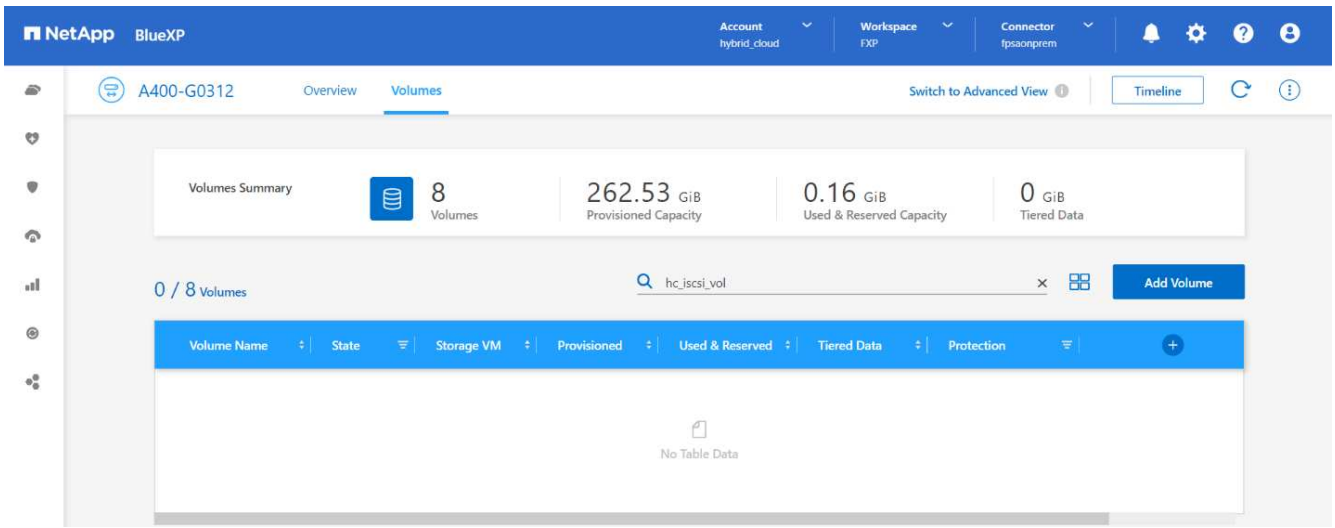
要验证成功的灾难恢复方案、请完成以下步骤：

1. 通过停止托管内部ONTAP 卷的SVM在源(生产)端模拟灾难 (`hc_iscsi_vol`）。



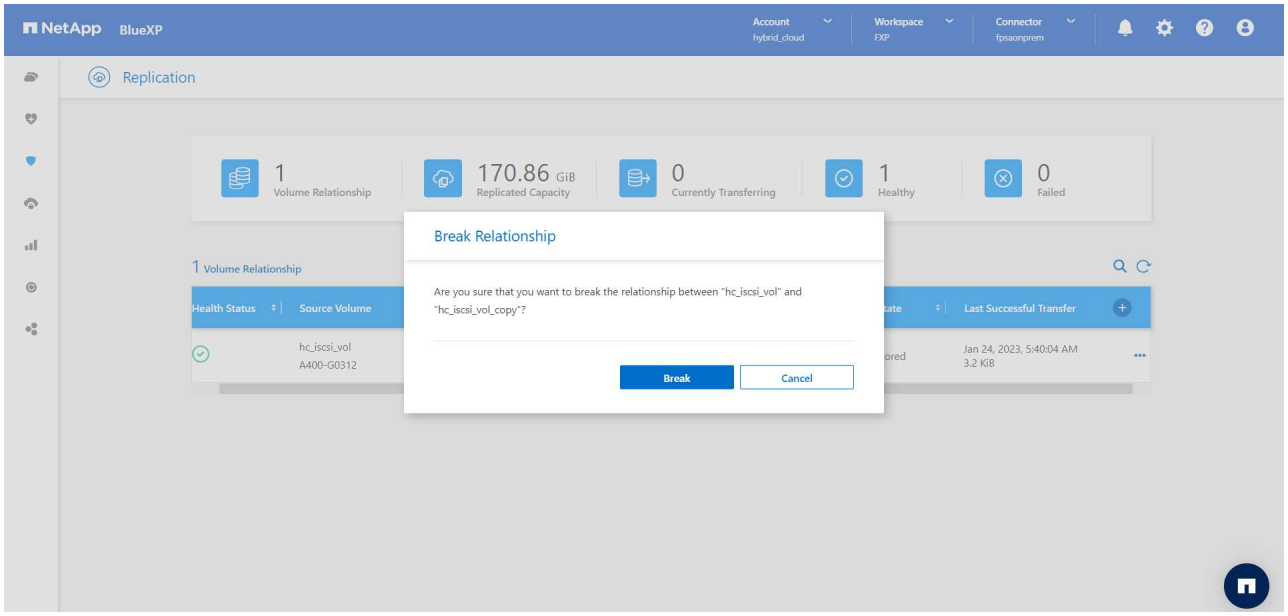
确保已在FlexPod 实例中的内部ONTAP 和AWS中的Cloud Volumes ONTAP 之间设置SnapMirror复制、以便您可以频繁创建应用程序快照。

停止SVM后、将显示 `hc_iscsi_vol` 卷在BlueXP中不可见。



2. 在CVO中激活灾难恢复。

   a. 中断本地ONTAP 和Cloud Volumes ONTAP 之间的SnapMirror复制关系、并提升CVO目标卷(`hc_iscsi_vol_copy`)到生产环境。



断开SnapMirror关系后、目标卷类型将从数据保护(DP)更改为读/写(RW)。

```
singlecvoaws::> volume show -volume hc_iscsi_vol_copy -fields typev
server          volume            type
--------------- ----------------- ----
svm_singlecvoaws hc_iscsi_vol_copy RW
```

b. 激活Cloud Volumes ONTAP 中的目标卷以在云中的EC2实例上启动EHR实例。

```
singlecvoaws::> lun mapping create -vserver svm_singlecvoaws -path
/vol/hc_iscsi_vol_copy/iscsi_lun1 -igroup ehr-igroup -lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                Igroup   LUN ID
Protocol
---------- ----------------------------------  --------  ------
---------
svm_singlecvoaws
            /vol/hc_iscsi_vol_copy/iscsi_lun1  ehr-igroup  0    iscsi
```

c. 要访问云中EHR实例上的数据和文件系统、请首先发现ONTAP 存储并验证多路径状态。

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
Output:
controller(7mode/E-Series)/         device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                  /vol/hc_iscsi_vol_copy/iscsi_lun1
sudo multipath -ll
Output:
3600a09806631755a452b543041313051 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

d. 然后激活卷组。

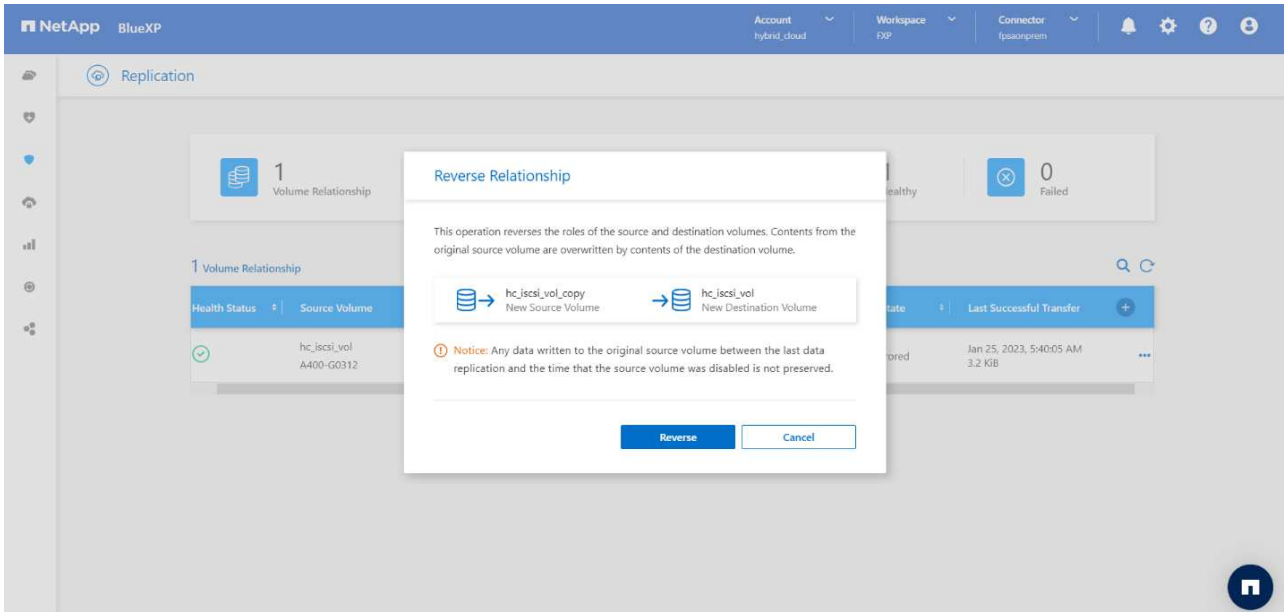
```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

e. 最后、挂载文件系统并显示文件系统信息。

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                 1K-blocks  Used      Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708  183987096  25621612  88%
/file1
```

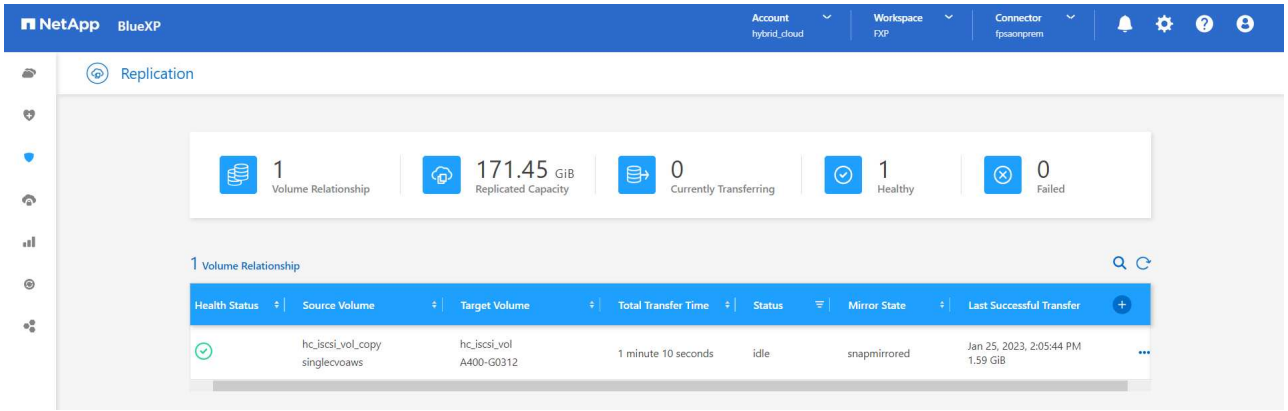
此输出显示、用户可以通过网络访问复制的数据、直到生产站点从灾难中恢复为止。

f. 反转SnapMirror关系。此操作将反转源卷和目标卷的角色。



执行此操作时、原始源卷中的内容将被目标卷的内容覆盖。当您要重新激活脱机的源卷时，这非常有用。

现在是CVO卷 (`hc_iscsi_vol_copy`)将成为源卷、内部卷也将成为源卷 (`hc_iscsi_vol`)将成为目标卷。



在上次数据复制和源卷禁用之间写入到原始源卷的任何数据都不会保留。

a. 要验证对CVO卷的写入访问、请在云中的EHR实例上创建一个新文件。

```
cd /file1/
sudo touch newfile
```

当生产站点关闭时、客户端仍可访问数据、并对Cloud Volumes ONTAP 卷执行写入操作、该卷现在是源卷。

如果要故障恢复到主站点、SnapMirror可提供一种高效的方法来重新同步灾难恢复站点与主站点、只需反转SnapMirror关系、即可仅将更改过的数据或新数据从灾难恢复站点传输回主站点。主生产站点恢复正常应用程序操作后、SnapMirror将继续向灾难恢复站点传输数据、而无需再进行基线传输。

本节说明了在生产站点发生灾难时成功解决灾难恢复方案的方法。现在、数据可以安全地由应用程序使用、这些

应用程序现在可以在源站点完成还原期间为客户端提供服务。

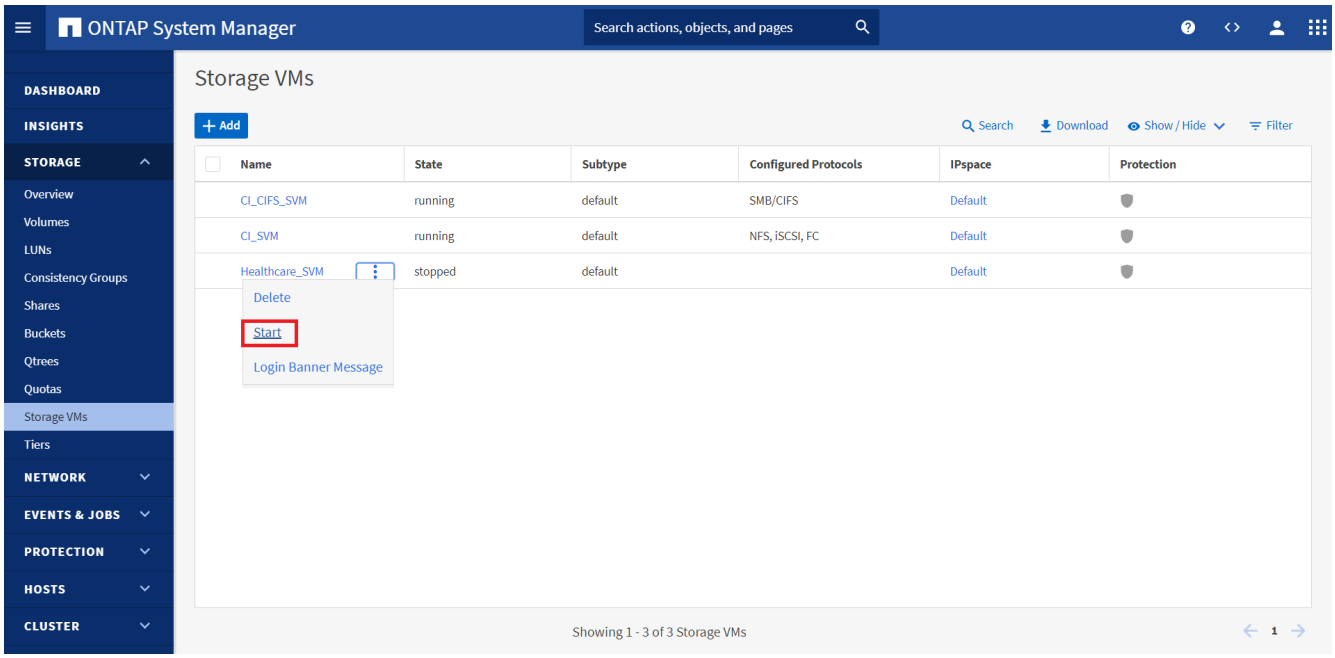
验证生产站点上的数据

恢复生产站点后、您必须确保还原原始配置、并且客户端能够从源站点访问数据。

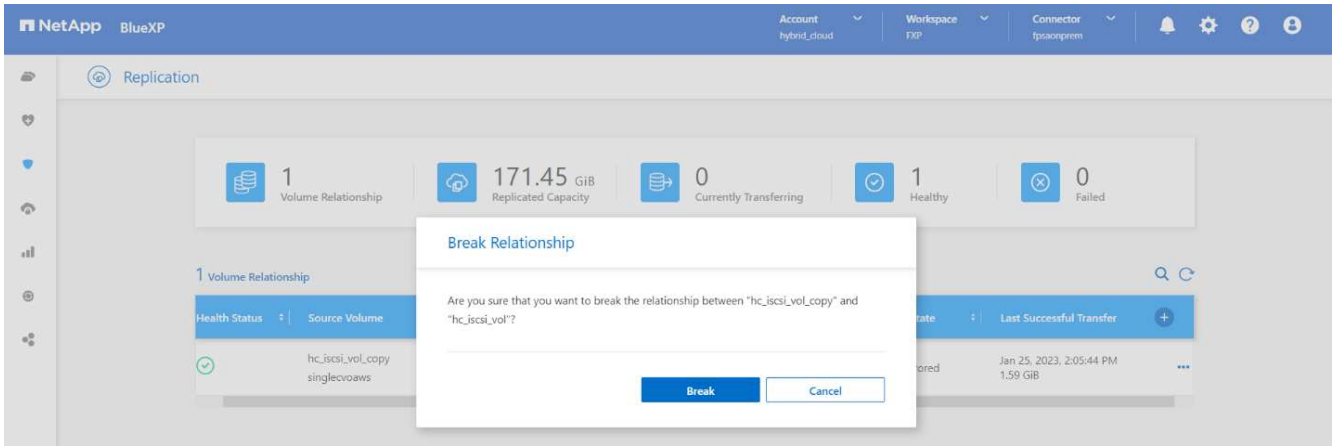
在本节中、我们将讨论启动源站点、恢复内部ONTAP 和Cloud Volumes ONTAP 之间的SnapMirror关系、并最终对源端执行数据完整性检查

以下操作步骤 可用于验证生产站点上的数据：

1. 确保源站点现在已启动。为此、请启动托管内部ONTAP 卷的SVM (`hc_iscsi_vol`）。



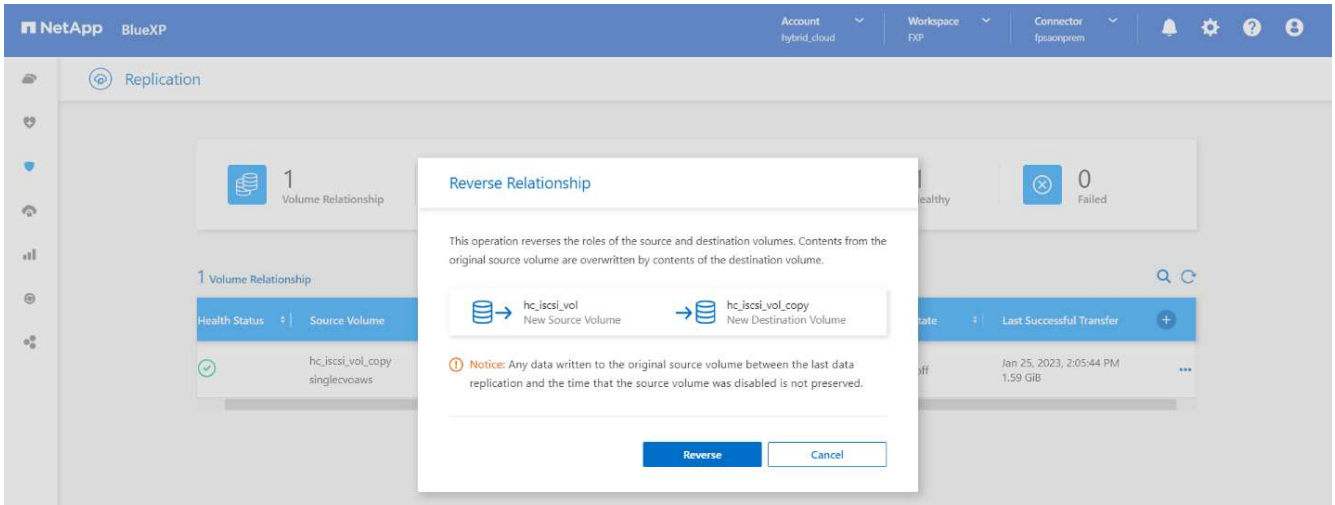
2. 中断Cloud Volumes ONTAP 和内部ONTAP 之间的SnapMirror复制关系、并提升内部卷 (`hc_iscsi_vol`)恢复生产。



断开SnapMirror关系后、内部卷类型将从数据保护(DP)更改为读/写(RW)。

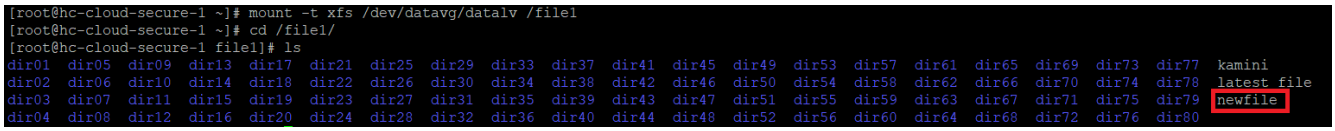
```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver         volume        type
--------------- ------------- ----
Healthcare_SVM hc_iscsi_vol RW
```

3. 反转SnapMirror关系。现在、是内部部署的ONTAP 卷 (`hc_iscsi_vol`)将成为源卷和之前的源卷、并成为Cloud Volumes ONTAP 卷 (`hc_iscsi_vol_copy`)将成为目标卷。



通过执行以下步骤、我们已成功还原原始配置。

4. 重新启动内部EHR实例。挂载文件系统并验证 `newfile` 在生产中断时、您在云中的EHR实例上创建的数据现在也存在。



我们可以推断、从源到目标的数据复制已成功完成、并且数据完整性已保持不变。这样就完成了对生产站点上数据的验证。

"接下来：总结。"

结论

"先前版本：解决方案 验证。"

构建混合云是大多数医疗保健组织随时提供数据可用性的目标。在此解决方案 中、我们实施了采用Cloud Volumes ONTAP 的FlexPod 混合云解决方案 、利用NetApp SnapMirror复制技术验证了一些用于备份和恢复医疗保健应用程序和工作负载的用例。

FlexPod 是Cisco和NetApp战略合作伙伴关系中经过严格测试和预先验证的融合基础架构、旨在提供可预测的低延迟系统性能和高可用性。这种方法可为EHR系统用户带来较高的舒适程度、并最终获得最佳响应时间。

借助NetApp、您可以像在内部数据中心运行NetApp存储功能一样、在云中运行EHR生产、灾难恢复、备份或分层。借助NetApp Cloud Volumes ONTAP 、NetApp可提供在云中有效运行EHR所需的企业级功能和性能。NetApp云选项可提供基于iSCSI的块和基于NFS或SMB的文件。

此解决方案 可满足医疗保健组织的需求、并使其能够朝着数字化转型迈出一步。它还可以帮助他们高效地管理应用程序和工作负载。

"下一步：从何处查找追加信息。"

从何处查找追加信息

"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 主页

  "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"

- NetApp BlueXP

  "https://bluexp.netapp.com/"

- NetApp Cloud Volumes ONTAP

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html"

- 在 AWS 中快速启动 Cloud Volumes ONTAP

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html"

- SnapMirror 复制

  "https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html"

- TR-3928：《NetApp Epic最佳实践》

  https://www.netapp.com/pdf.html?item=/media/17137-tr3928pdf.pdf

- TR-4693 ：《适用于 Epic EHR 的 FlexPod 数据中心部署指南》

  "https://www.netapp.com/media/10658-tr-4693.pdf"

- 适用于Epic的FlexPod

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.html"

- NetApp 互操作性表工具

"http://support.netapp.com/matrix/"

- Cisco UCS 硬件和软件互操作性工具

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- VMware 兼容性指南

  "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	2023年3月	初始版本

适用于Google云平台的FlexPod 混合云与NetApp Cloud Volumes ONTAP 和Cisco Intersight

TR-4939：《适用于Google云平台的FlexPod 混合云与NetApp Cloud Volumes ONTAP 和Cisco Intersight》

NetApp公司Ruchika Lahoti

简介

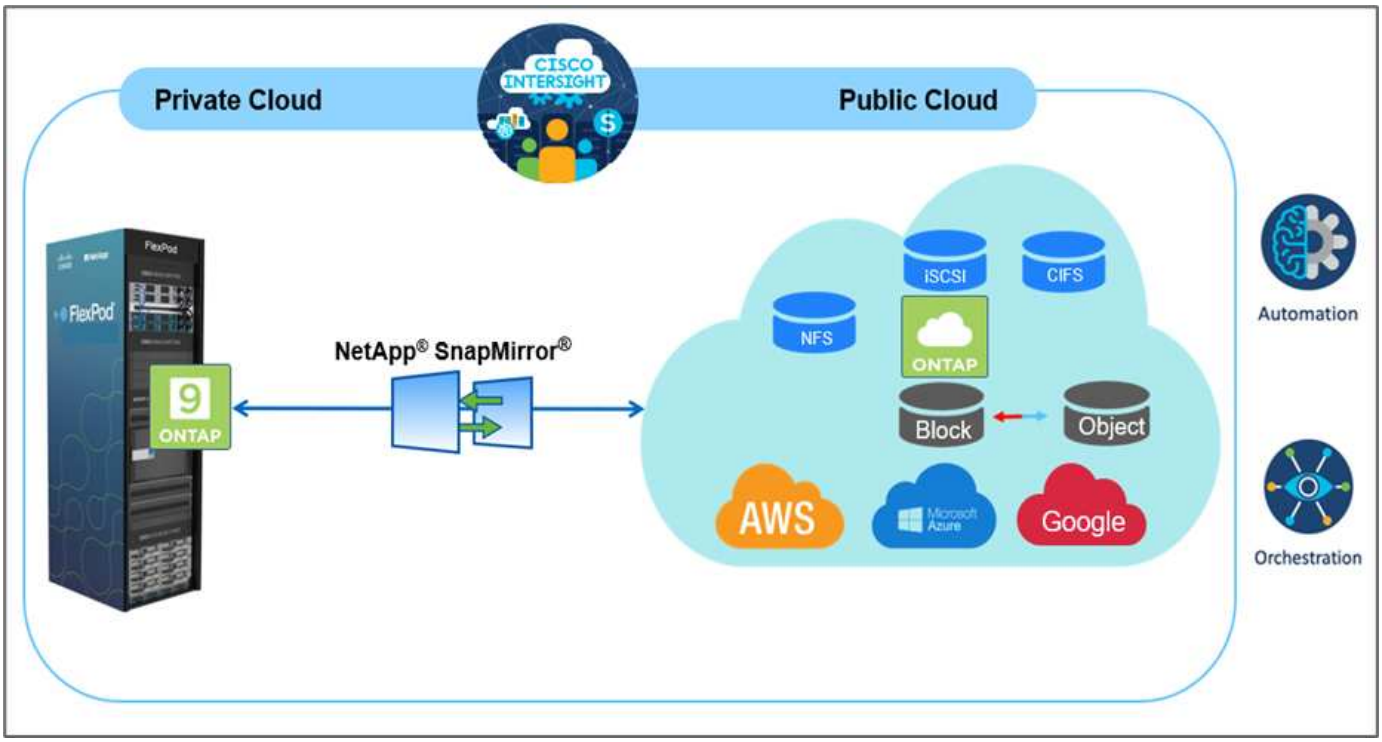
利用灾难恢复(DR)保护数据是实现业务连续性的一个关键目标。灾难恢复允许组织将业务运营故障转移到二级位置、然后高效可靠地恢复并故障恢复到主站点。自然灾害、网络故障、软件漏洞和人为错误等多种问题都使制定灾难恢复策略成为IT的首要任务。

对于灾难恢复、主站点上运行的所有工作负载都必须在灾难恢复站点上复制。组织还必须拥有所有企业数据的最新副本、包括数据库、文件服务、NFS和iSCSI存储等。由于生产环境中的数据会不断更新、因此必须定期将更改传输到灾难恢复站点。

对于大多数组织来说、部署灾难恢复环境都是一项挑战、因为需要基础架构和站点独立性。所需的资源数量以及设置、测试和维护二级数据中心的成本可能非常高、通常会接近整个生产环境的成本。在保持数据持续同步并建立无缝故障转移和故障恢复的同时、尽可能减少数据占用空间并提供充分的保护、这是一项极具挑战性的任务。构建灾难恢复站点后、接下来的挑战是从生产环境复制数据并保持数据同步。

本技术报告将FlexPod 融合基础架构解决方案 、基于Google Cloud的NetApp Cloud Volumes ONTAP 和Cisco Intersight汇集在一起、构成了一个用于灾难恢复的混合云数据中心。在本解决方案 中、我们将讨论如何使用Cisco Intersight Cloud Orchestrator设计和执行内部ONTAP 工作流。我们还将讨论部署NetApp Cloud Volumes ONTAP 以及使用适用于HashiCorp Terraform的Cisco Intersight服务在FlexPod 和Cloud Volumes ONTAP 之间编排和自动化数据复制和灾难恢复。

下图提供了解决方案 概述。



此解决方案 具有多种优势、包括：

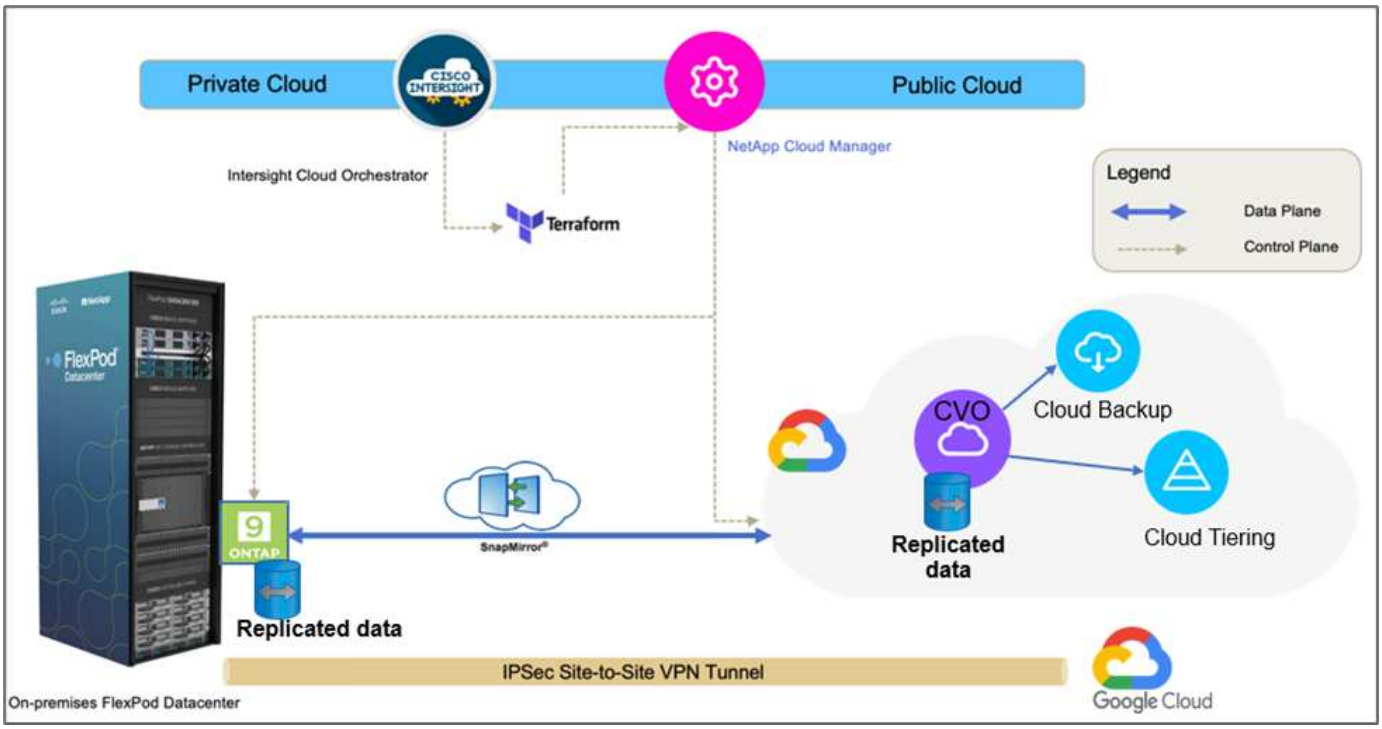
- 流程编排和自动化。 Cisco Intersight通过提供通过自动化交付的一致的流程编排框架、简化了FlexPod 混合云基础架构的日常运营。
- 自定义保护。 Cloud Volumes ONTAP 提供从ONTAP 到云的块级数据复制、通过增量更新使目标保持最新。用户可以根据所传输源的更改、指定每5分钟或每小时的同步计划。
- *无缝故障转移和故障恢复。*发生灾难时、存储管理员可以快速故障转移到云卷。恢复主站点后、在灾难恢复环境中创建的新数据将同步回源卷、从而重新建立二级数据复制。
- *效率：*二级云副本的存储空间和成本通过数据压缩、精简配置和重复数据删除进行优化。数据以经过压缩和重复数据删除的形式在块级别传输、从而提高传输速度。数据也会自动分层到低成本对象存储、并且只有在访问时才会返回到高性能存储、例如在灾难恢复情形下。这样可以显著降低持续存储成本。
- *提高了IT工作效率。*使用Intersight作为一个安全的企业级基础架构和应用程序生命周期管理平台、可以简化解决方案 的配置管理以及手动任务的大规模自动化。

audience

本文档的受众包括但不限于：销售工程师、现场顾问、专业服务人员、IT经理、 合作伙伴工程师、站点可靠性工程师、云架构师、云工程师以及希望利用专为提高IT效率和实现IT创新而构建的基础架构的客户。

解决方案 拓扑

本节介绍解决方案 的逻辑拓扑。下图显示了内部FlexPod 环境、在Google Cloud上运行的NetApp Cloud Volumes ONTAP 、Cisco Intersight和NetApp Cloud Manager的解决方案 拓扑。



控制平面和数据平面会在端点之间清晰地指示。数据平面使用安全的站点到站点VPN连接将FlexPod 全闪存FAS上运行的ONTAP 实例连接到Google Cloud上的NetApp Cloud Volumes ONTAP 实例。

将工作负载数据从FlexPod 复制到NetApp Cloud Volumes ONTAP 由NetApp SnapMirror处理、整个过程使用Cisco Intersight Cloud Orchestrator在内部环境和云环境中进行协调。Cisco Intersight Cloud Orchestrator使用适用于NetApp Cloud Manager的Terraform资源提供商来执行与NetApp Cloud Volumes ONTAP 部署相关的操作并建立数据复制关系。

> 此解决方案 还支持将驻留在NetApp Cloud Volumes ONTAP 实例中的冷数据备份和分层到Google云存储。

"接下来：解决方案 组件。"

解决方案组件

"上一步：解决方案概述。"

FlexPod

FlexPod 是一组定义的硬件和软件、可为虚拟化和非虚拟化解决方案奠定集成基础。FlexPod 包括NetApp ONTAP 存储、Cisco Nexus网络、Cisco MDS存储网络和Cisco统一计算系统(Cisco UCS)。该设计非常灵活、可以将网络、计算和存储安装到一个数据中心机架中、也可以根据客户的数据中心设计进行部署。端口密度允许网络组件容纳多种配置。

Cisco Intersight

Cisco Intersight是一个SaaS平台、可为传统和云原生应用程序和基础架构提供智能自动化、可观察性和优化功能。该平台有助于推动IT团队的变革、并提供专为混合云设计的运营模式。Cisco Intersight具有以下优势：

- *交付速度更快。*由于采用基于敏捷性的软件开发模式、可从云或客户数据中心以服务的形式交付、并经常进行更新和持续创新。这样、客户就可以专注于加快业务部门的交付速度。

- *简化操作。*通过使用一个安全的SaaS交付工具以及通用清单、身份验证和API在整个堆栈和所有位置运行、简化操作、消除团队之间的孤岛。从内部管理物理服务器和虚拟机管理程序到虚拟机、K8s、无服务器、自动化、 在内部和公有 云之间实现优化和成本控制。
- *持续优化。*利用Cisco Intersight在每一层提供的智能以及Cisco TAC持续优化您的环境。这种智能功能可转换为建议的可自动操作、因此您可以实时适应每个变化：从移动工作负载和监控物理服务器的运行状况到您使用的公有 云的成本降低建议。

Cisco Intersight支持两种管理操作模式：UCSM受管模式(Umm)和Intersight受管模式(IMM)。在初始设置互联阵列期间、您可以为光纤连接的Cisco UCS系统选择原生 Umm或IMM。在此解决方案 中、使用原生 IMM。

Cisco Intersight许可

Cisco Intersight使用基于订阅的许可证、该许可证包含多个层。

Cisco Intersight许可证层如下：

- * Cisco Intersight Essentials。*包括所有基本功能以及以下功能：
  - Cisco UCS Central
  - Cisco IMC Supervisor授权
  - 使用服务器配置文件进行基于策略的配置
  - 固件管理
  - 与硬件兼容性列表(Hardware Compatibility List、HCL)的兼容性评估
- * Cisco Intersight Advantage。*包括Essentials层的特性和功能以及以下功能：
  - 在物理计算、网络、存储、VMware虚拟化和AWS公有 云之间使用小工具、清单、容量、利用率功能以及跨域清单关联。
  - Cisco安全咨询服务、客户可以在此服务中收到有关受影响端点设备的重要安全警报和现场通知。
- * Cisco Intersight Premier。*除了在高级版中提供的功能之外、Cisco Intersight Premier还提供以下功能：
  - 适用于Cisco和第三方计算、网络、存储、集成系统、虚拟化、 容器和公共云平台
  - Cisco UCS Director的完整订阅授权、无需额外费用。

有关Intersight许可以及每个许可支持的功能的详细信息、请参见 "此处"。

> 在本解决方案 中、我们使用适用于HashiCorp Terraform的Intersight Cloud Orchestrator和Intersight服务。具有Intersight Premier许可证的用户可以使用这些功能、因此必须启用此许可层。

Terraform Cloud与ICO集成

您可以使用Cisco Intersight Cloud Orchestrator (ICO)创建和执行调用Terraform Cloud (TFC) API的工作流。调用Web API请求任务支持将Terraform Cloud作为目标、并且可以使用HTTP方法为其配置Terraform Cloud API。因此、工作流可以组合使用多个任务、这些任务使用通用API任务和其他操作调用多个Terraform Cloud API。要使用ICO功能、您需要获得Premier许可证。

Cisco Intersight Assist

Cisco Intersight Assist可帮助您将端点设备添加到Cisco Intersight。一个数据中心可能包含多个不直接与Cisco

Intersight连接的设备。Cisco Intersight支持但不直接连接到的任何设备都需要连接机制。Cisco Intersight Assist可提供此连接机制、并帮助您将设备添加到Cisco Intersight中。

Cisco Intersight Virtual Appliance中提供了Cisco Intersight Assist、该设备以Open Virtual Appliance (OVA)文件格式包含的可部署虚拟机的形式进行分发。您可以在ESXi服务器上安装此设备。有关详细信息，请参见 "《Cisco Intersight Virtual Appliance入门指南》"。

将Intersight Assist申请到Intersight后、您可以使用通过Intersight Assist选项申请端点设备。有关详细信息，请参见 "入门"。

NetApp Cloud Volumes ONTAP

- 利用内置的重复数据删除、数据压缩、精简配置和克隆功能最大限度地降低存储成本。
- 在云环境发生故障时提供企业级可靠性和持续运营。
- Cloud Volumes ONTAP 使用行业领先的复制技术NetApp SnapMirror将内部数据复制到云中、因此可以轻松地为多种使用情形提供二级副本。
- Cloud Volumes ONTAP 还与Cloud Backup Service 集成、提供备份和还原功能、以保护和长期归档云数据。
- 按需在高性能和低性能存储池之间切换、而无需使应用程序脱机。
- 使用NetApp SnapCenter 提供Snapshot副本的一致性。
- Cloud Volumes ONTAP 支持数据加密，并提供防病毒和勒索软件保护。
- 与 Cloud Data sense 集成有助于您了解数据环境并识别敏感数据。

Cloud Central

Cloud Central提供了一个中央位置、用于访问和管理NetApp云数据服务。这些服务使您能够在云中运行关键应用程序、创建自动化灾难恢复站点、备份 SaaS 数据、并在多个云中有效地迁移和控制数据。有关详细信息，请参见 "Cloud Central"。

Cloud Manager

Cloud Manager是一款基于SaaS的企业级管理平台、IT专家和云架构师可以利用NetApp云解决方案集中管理其混合多云基础架构。它提供了一个集中式系统、用于查看和管理内部和云存储、以支持多个混合云提供商和客户。有关详细信息，请参见 "Cloud Manager"。

连接器

借助Connector、Cloud Manager可以管理公有 云环境中的资源和流程。要使用Cloud Manager提供的许多功能、需要使用Connector实例、并且可以部署在云或内部网络中。连接器在以下位置受支持：

- AWS
- Microsoft Azure
- Google Cloud
- 内部部署

NetApp Active IQ Unified Manager

借助NetApp Active IQ Unified Manager 、您可以通过一个经过重新设计的直观界面监控ONTAP 存储集群、该

界面可利用社区智慧和AI分析提供智能信息。它可以全面洞察存储环境及其运行的虚拟机的运行情况、性能和主动式情况。当存储基础架构发生问题描述 时、Unified Manager可以通知您问题描述 的详细信息、以帮助识别根发生原因。通过虚拟机信息板、您可以查看虚拟机的性能统计信息、以便调查从vSphere主机向下经过网络并最终到达存储的整个I/O路径。

某些事件还提供了更正问题描述 所需的补救措施。您可以为事件配置自定义警报、以便在发生问题时、通过电子邮件和SNMP陷阱通知您。Active IQ Unified Manager 可以预测容量和使用趋势、以便在出现问题之前主动采取行动、从而防止做出长期可能导致其他问题的被动短期决策、从而为用户的存储需求进行规划。

VMware vSphere

VMware vSphere是一个虚拟化平台、可将大量基础架构(包括CPU、存储和网络等资源)作为一个无缝、多功能且动态的操作环境进行全面管理。与管理单个计算机的传统操作系统不同、VMware vSphere可将整个数据中心的基础架构聚合在一起、从而创建一个具有资源的动力中心、这些资源可以快速动态地分配给任何需要的应用程序。

有关VMware vSphere的详细信息、请参见 "此链接。"。

VMware vSphere vCenter

VMware vCenter Server可通过一个控制台统一管理所有主机和VM、并对集群、主机和VM进行聚合性能监控。通过VMware vCenter Server、管理员可以深入了解计算集群、主机、虚拟机、存储、子操作系统、 虚拟基础架构的其他关键组件。VMware vCenter可管理VMware vSphere环境中提供的丰富功能。

硬件和软件版本

此混合云解决方案 可以扩展到运行NetApp互操作性表工具和Cisco UCS硬件兼容性列表中定义的受支持软件、固件和硬件版本的任何FlexPod 环境。

在我们的内部环境中用作基线平台的FlexPod 解决方案 是根据所述准则和规格进行部署的 "此处"。

此环境中的网络基于ACI。有关详细信息，请参见 "此处"。

- 有关详细信息、请参见以下链接：
- "NetApp 互操作性表工具"
- "VMware 兼容性指南"
- "Cisco UCS 硬件和软件互操作性工具"

下表显示了FlexPod 硬件和软件版本。

组件	产品	**version**
计算	Cisco UCS X210C-M6	5.0 (1b)
	Cisco UCS互联阵列6454	4.2 (2a)
网络	Cisco Nexus 9332C (Spine)	14.2 (7秒)
	Cisco Nexus 9336C-x2 (叶)	14.2 (7秒)
	Cisco ACI	4.2 (7秒)
存储	NetApp AFF A220	9.11.1

组件	产品	**version**
	适用于 VMware vSphere 的 NetApp ONTAP 工具	9.10.
	适用于VMware VAAI的NetApp NFS插件	2.0-15
	Active IQ Unified Manager	9.11
软件	vSphere ESXi	7.0 (U3)
	VMware vCenter设备	7.0.3
	Cisco Intersight Assist虚拟设备	1.0.11-306

Terraform配置在Terraform Cloud for Business帐户上执行。Terraform配置使用适用于NetApp Cloud Manager的Terraform提供程序。

下表列出了供应商、产品和版本。

组件	产品	**version**
HashiCorp	Terraform	1.2.7.

下表显示了Cloud Manager和Cloud Volumes ONTAP 的版本。

组件	产品	**version**
NetApp	Cloud Volumes ONTAP	9.11
	Cloud Manager	3.9.21

"接下来：安装和配置—部署FlexPod。"

安装和配置

部署**FlexPod**

"先前版本：解决方案 组件。"

要了解FlexPod 设计和部署详细信息、包括各种设计要素的配置以及相关最佳实践、请参见 "经过Cisco验证的FlexPod 设计"。

FlexPod 既可以部署在UCS托管模式下、也可以部署在Cisco Intersight托管模式下。如果您要在UCS托管模式下部署FlexPod 、可以找到最新的Cisco验证设计 "此处"。

Cisco Unified Compute System (Cisco UCS) X系列是一款全新的模块化计算系统、可通过云进行配置和管理。它旨在满足现代应用程序的需求、并通过适应性强、适应未来需求的模块化设计提高运营效率、灵活性和可扩展性。有关在FlexPod 基础架构中整合Cisco Intersight-托管UCS X系列平台的设计指南、请参见 "此处"。

可以找到部署了Cisco ACI的FlexPod "此处"。

"接下来：Cisco Intersight配置。"

Cisco Intersight配置

"先前版本：部署FlexPod。"

要配置Cisco Intersight和Intersight Assist、请参见Cisco为FlexPod 发现的经验证的设计 "此处"。

"接下来：Terraform Cloud Integration with ICO前提条件。"

Terraform Cloud Integration with ICO前提条件

"先前版本：Cisco Intersight配置。"

操作步骤 1：连接Cisco Intersight和Terraform Cloud

1. 通过提供相关的Terraform Cloud帐户详细信息来声明或创建Terraform云目标。
2. 为私有云创建Terraform Cloud Agent目标、以便客户可以在数据中心安装代理并与Terraform Cloud进行通信。

   有关详细信息、请参见 "此链接。"。

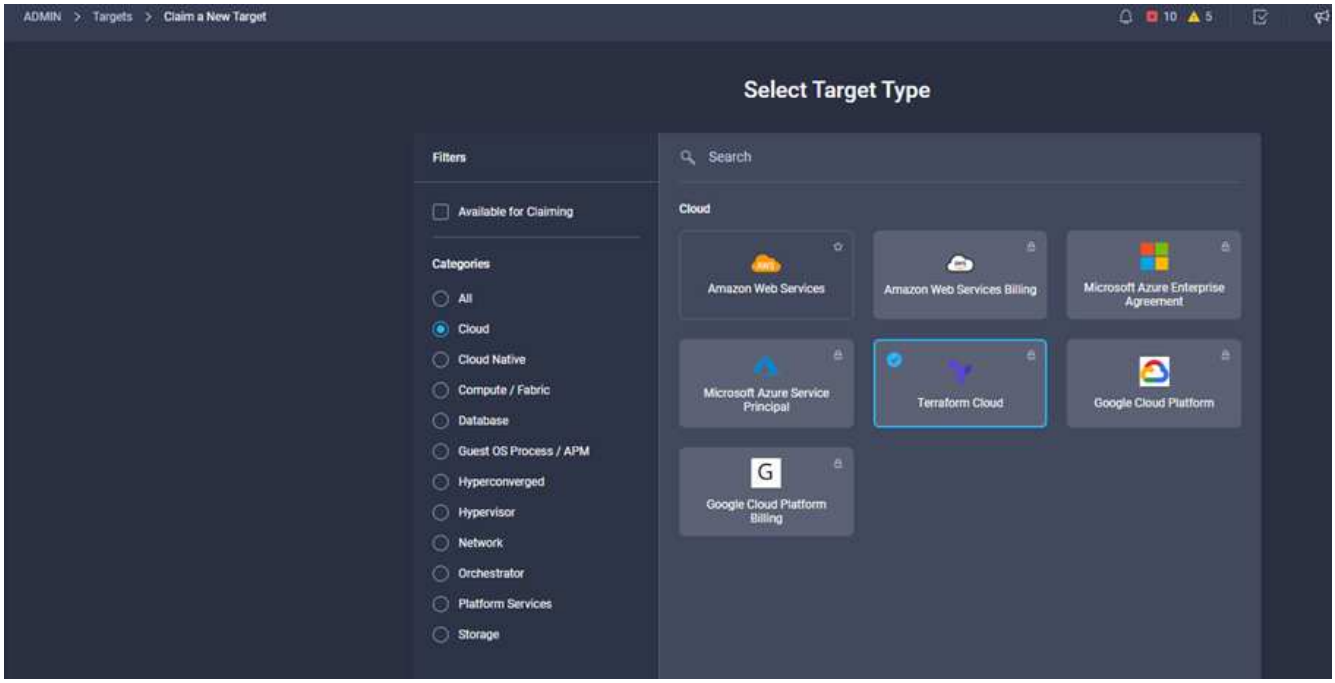
操作步骤 2：生成用户令牌

在为Terraform Cloud添加目标时、您必须从Terraform Cloud设置页面提供用户名和API令牌。

1. 登录到Terraform Cloud并转到*用户令牌*： "https://app.terraform.io/app/settings/tokens"。
2. 单击*创建新的API令牌*。
3. 分配一个要记住的名称并将令牌保存在安全位置。

操作步骤 3：声明Terraform云目标

1. 使用帐户管理员、设备管理员或设备技术人员权限登录到Intersight。
2. 导航到*管理>目标>申请新目标*。
3. 在*类别*中、单击*云*。
4. 单击* Terraform Cloud*并单击*开始*。



5. 输入目标的名称、Terraform Cloud的用户名、API令牌以及Terraform Cloud中的默认组织、如下图所示。
6. 在*默认受管主机*字段中、确保添加以下链接以及其他受管主机：
   - github.com
   - github-releases.githubusercontent.com

如果输入的所有内容均正确无误、您将在* Intersight Targets*部分中看到Terraform Cloud目标。

操作步骤 **4**：添加**Terraform**云代理

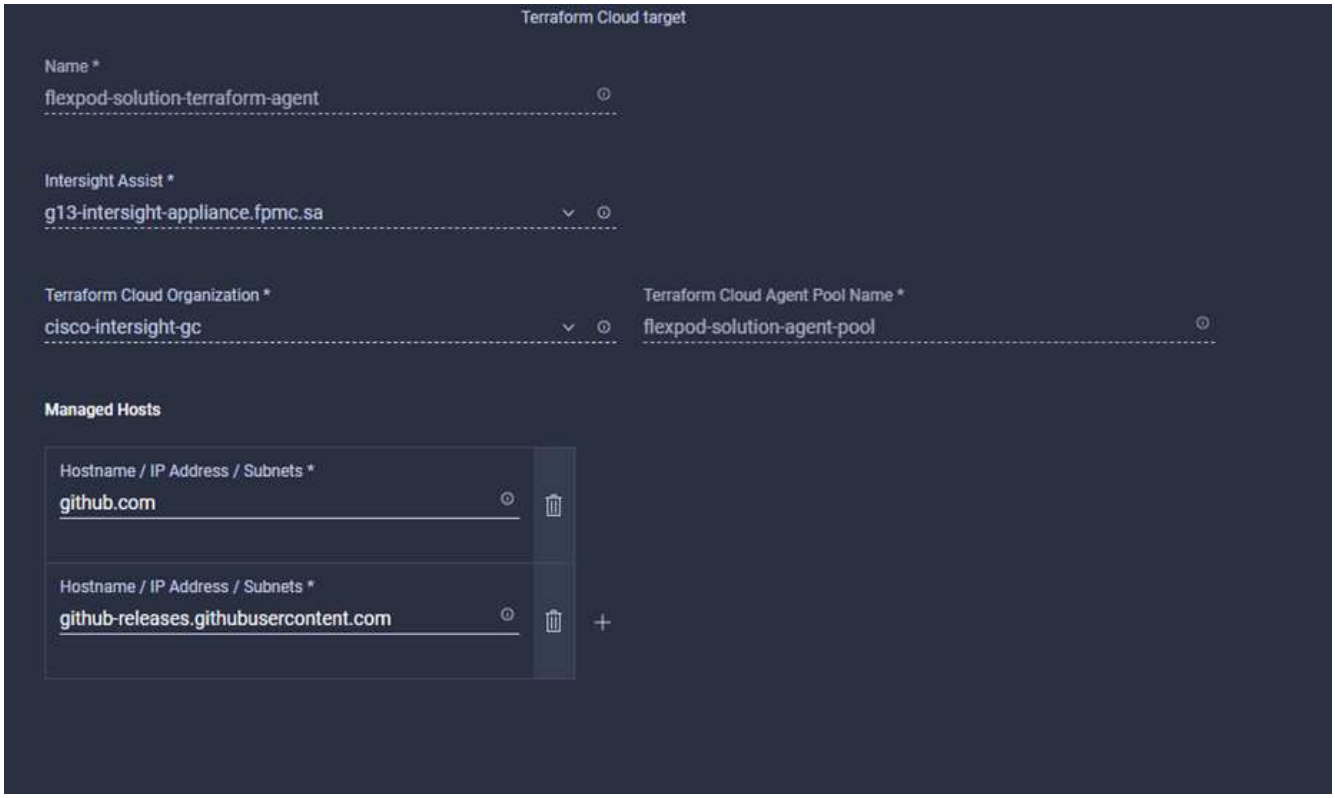
前提条件

- Terraform Cloud目标。
- 在部署Terraform Cloud Agent之前、向Intersight申请了Intersight协助。

> 每次协助只能申请五名代理。

> 创建与Terraform的连接后、必须启动Terraform代理才能执行Terraform代码。

1. 从Terraform Cloud目标的下拉列表中单击*声明Terraform Cloud Agent*。
2. 输入Terraform Cloud代理的详细信息。以下屏幕截图显示了Terraform代理的配置详细信息。



> 您可以更新任何Terraform Agent属性。如果目标处于*未连接*状态且从未处于*已连接*状态、则尚未为Terraform代理生成令牌。

在代理验证成功并生成代理令牌后、您无法重新配置组织和/或代理池。Terraform代理的成功部署状态为*已连接*。

启用并申请Terraform Cloud集成后、您可以在Cisco Intersight Assist中部署一个或多个Terraform Cloud代理。Terraform Cloud代理将建模为Terraform Cloud目标的子目标。申请代理目标时、您会看到一条消息、指示目标申请正在进行中。

几秒钟后、目标将移至*已连接*状态、Intersight平台会将HTTPS数据包从代理路由到Terraform Cloud网关。

您的Terraform代理应正确声明、并应在目标下显示为*已连接*。

"下一步：配置公有 云服务提供商。"

配置公有 云服务提供商

"先前版本：Terraform Cloud Integration with ICO前提条件。"

操作步骤 1：访问NetApp Cloud Manager

要访问NetApp Cloud Manager和其他云服务、您需要注册 "NetApp Cloud Central"。

要在Cloud Central帐户中设置工作空间和用户、请单击 "此处"。

操作步骤 **2**：部署连接器

要在Google Cloud中部署Connector、请参见此内容 "链接。"。

"接下来：自动部署混合云NetApp存储。"

自动部署混合云**NetApp**存储

"先前版本：配置公有 云服务提供商。"

Google Cloud

您必须先启用API并创建一个服务帐户、以便为Cloud Manager提供部署和管理与Connector位于同一项目或不同项目中的Cloud Volumes ONTAP 系统的权限。

在Google Cloud项目中部署连接器之前、请确保此连接器未在内部或其他云提供商中运行。

在直接从 Cloud Manager 部署 Connector 之前，必须具有两组权限：

- 您需要使用有权从Cloud Manager启动Connector VM实例的Google帐户部署Connector。
- 部署Connector时、系统会提示您选择VM实例。Cloud Manager 可从服务帐户中获得代表您创建和管理Cloud Volumes ONTAP 系统的权限。权限可通过向服务帐户附加自定义角色来提供。您需要设置两个YAML文件、这些文件包含用户和服务帐户所需的权限。了解如何使用 "用于设置权限的YAML文件" 此处。

请参见 "此详细视频" 所有必需的前提条件。

Cloud Volumes ONTAP 部署模式和架构

Cloud Volumes ONTAP 可作为单节点系统和高可用性(HA)节点对在Google Cloud中使用。根据要求、我们可以选择Cloud Volumes ONTAP 部署模式。不支持将单节点系统升级到 HA 对。如果要在单节点系统和HA对之间切换、则必须部署新系统并将现有系统中的数据复制到新系统。

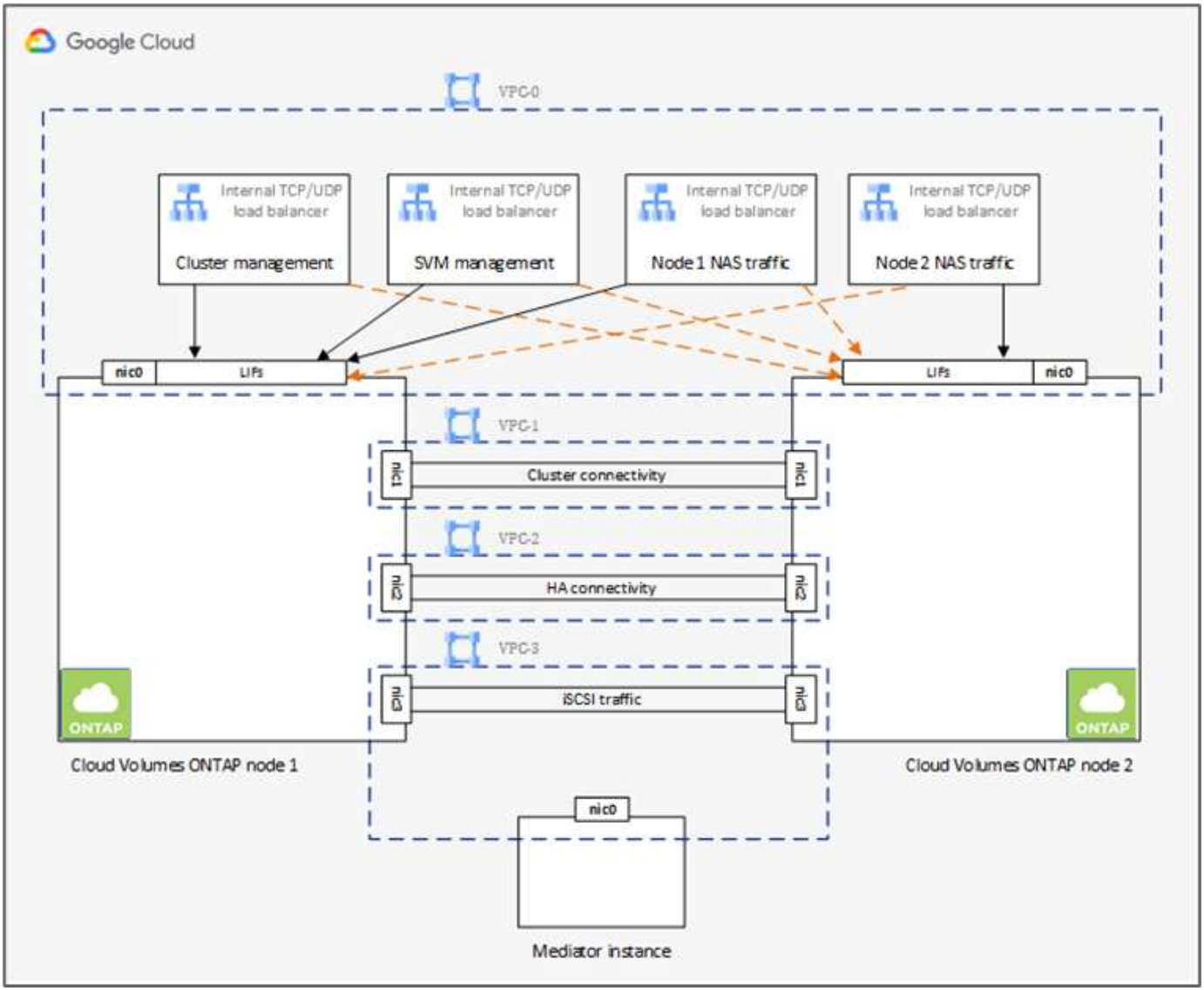
Google Cloud中的高可用性**Cloud Volumes ONTAP**

Google Cloud支持跨多个地理区域和一个区域内的多个区域部署资源。HA部署由两个ONTAP 节点组成、这两个节点使用Google Cloud中提供的功能强大的n1标准或n2标准计算机类型。数据会在两个Cloud Volumes ONTAP 节点之间同步复制、以便在发生故障时提供可用性。Cloud Volumes ONTAP 的高可用性部署要求每个VPC具有四个VPC和一个专用子网。四个vPC中的子网应配置非重叠的CIDR范围。

这四个VPC用于以下用途：

- VPC 0支持与数据和Cloud Volumes ONTAP 节点的入站通信。
- VPC 1可在Cloud Volumes ONTAP 节点之间提供集群连接。
- VPC 2支持在节点之间进行非易失性RAM (NVRAM)复制。
- VPC 3用于连接到HA调解器实例、以及用于节点重建的磁盘复制流量。

下图显示了Goggle Cloud中的高可用性Cloud Volumes ONTAP。



有关详细信息，请参见 "此链接。"。

有关Google Cloud中Cloud Volumes ONTAP 的网络连接要求、请参见 "此链接。"。

有关数据分层的详细信息、请参见 "此链接。"。

设置环境前提条件

可以使用Terraform配置自动创建Cloud Volumes ONTAP 集群、在内部卷和云卷之间配置SnapMirror、创建云卷等。这些Terraform配置托管在Terraform Cloud for Business帐户上。使用Intersight Cloud Orchestrator、您可以编排任务、例如在Terraform Cloud for Business帐户中创建工作空间、将所有必需的变量添加到工作空间、执行Terraform计划等。

对于这些自动化和业务流程任务、需要满足一些要求并提供一些数据、如以下各节所述。

GitHub 存储库

您需要一个GitHub帐户来托管Terraform代码。Intersight Orchestrator在Terraform Cloud for Business帐户中创建新的工作空间。此工作空间配置了版本控制工作流。为此、您需要将Terraform配置保留在GitHub存储库中、并在创建工作空间时将其作为输入提供。

"此GitHub链接" 使用各种资源提供Terraform配置。您可以通过派生此存储库并在GitHub帐户中创建副本。

在此存储库中、`provider.tf`定义了所需的Terraform提供程序。使用适用于NetApp Cloud Manager的Terraform提供程序。

`variables.tf`具有所有变量声明。这些变量的值将作为Intersight Cloud Orchestrator的工作流输入进行输入。这样可以方便地将值传递到工作空间并执行Terraform配置。

`resources.tf`定义了向工作环境添加内部ONTAP 、在Google Cloud上创建单节点Cloud Volumes ONTAP 集群、在内部和Cloud Volumes ONTAP 之间建立SnapMirror关系、在Cloud Volumes ONTAP 上创建云卷等所需的各种资源。

在此存储库中：

- `provider.tf`将NetApp Cloud Manager定义为所需的Terraform提供程序。
- `variables.tf`具有可变声明、这些声明可用作Intersight Cloud Orchestrator工作流的输入。这样可以方便地将值传递到工作空间并执行Terraform配置。
- `resources.tf`定义各种资源、用于向工作环境添加内部ONTAP 、在Google Cloud上创建单节点Cloud Volumes ONTAP 集群、在内部和Cloud Volumes ONTAP 之间建立SnapMirror关系、在Cloud Volumes ONTAP 上创建云卷等。

您可以添加一个额外的资源块来在Cloud Volumes ONTAP 上创建多个卷、也可以使用count或`for_each` Terraform构造。

要将Terraform工作空间、模块和策略集连接到包含Terraform配置的git存储库、Terraform Cloud需要访问GitHub repo.

添加客户端、客户端的OAuth令牌ID将用作Intersight Cloud Orchestrator的工作流输入之一。

1. 登录到Terraform Cloud for Business帐户。导航到*设置>提供程序*。
2. 单击*添加VCS提供程序*。
3. 选择您的版本。
4. 按照*设置提供程序*下的步骤进行操作。
5. 您可以在* VCS Provider*中看到已添加的客户端。记下OAuth令牌ID。

刷新**NetApp Cloud Manager API**操作的令牌

除了 Web 浏览器界面之外， Cloud Manager 还具有一个 REST API ，可使软件开发人员通过 SaaS 界面直接访问 Cloud Manager 功能。Cloud Manager 服务由多个不同的组件组成，这些组件共同构成一个可扩展的开发平台。通过刷新令牌、您可以生成要添加到每个API调用的授权标头中的访问令牌。

在不直接调用API的情况下、NetApp-cloudmanager提供程序会使用刷新令牌并将Terraform资源转换为相应的API调用。您需要从为NetApp Cloud Manager API操作生成刷新令牌 "NetApp Cloud Central"。

要在Cloud Manager上创建资源、例如创建Cloud Volumes ONTAP 集群、配置SnapMirror等、您需要Cloud Manager Connector的客户端ID。

1. 登录到Cloud Manager： "https://cloudmanager.netapp.com/"。
2. 单击 * 连接器 * 。

3. 单击 * 管理连接器 * 。
4. 单击省略号并复制连接器ID。

开发**Cisco Intersight Cloud Orchestrator**工作流

在以下情况下、Cisco Intersight可提供Cisco Intersight Cloud Orchestrator：

- 您已安装Intersight Premier许可证。
- 您可以是帐户管理员、存储管理员、虚拟化管理员或服务器管理员、并且至少已为您分配一台服务器。

工作流设计器

工作流设计器可帮助您创建新工作流(以及任务和数据类型)并编辑现有工作流、以管理Cisco Intersight中的目标。

要启动工作流设计器、请转到*流程编排>工作流*。信息板会在*我的工作流*、*示例工作流*和*所有工作流*选项卡下显示以下详细信息：

- 验证状态
- 上次执行状态
- 按执行计数显示的前几个工作流
- 工作流类别排名靠前
- 系统定义的工作流数量
- 按目标划分的前几个工作流

您可以使用信息板创建、编辑、克隆或删除选项卡。要创建自己的自定义视图选项卡、请单击*+*并指定名称、然后选择需要显示在列、标记列和小工具中的参数。如果某个选项卡没有*锁定*图标、则可以重命名该选项卡。

信息板下是一个工作流表格列表、其中显示了以下信息：

- 显示名称
- Description
- 系统定义
- 默认版本
- 执行
- 上次执行状态
- 验证状态
- 上次更新时间
- 组织

"Actions"列可用于执行以下操作：

- *执行。*执行工作流。
- *历史记录。*显示工作流执行历史记录。

- *管理版本。*创建和管理工作流的版本。
- *删除。*删除工作流。
- *重试。*重试失败的工作流。

工作流

创建包含以下步骤的工作流：

- *定义工作流。*指定显示名称、问题描述 和其他重要属性。
- *定义工作流输入和工作流输出。*指定执行工作流必须使用哪些输入参数、以及成功执行时生成的输出
- *添加工作流任务。*在工作流设计器中添加工作流执行其功能所需的一个或多个工作流任务。
- *验证工作流。*验证工作流以确保在连接任务输入和输出时没有错误。

为内部**FlexPod** 存储创建工作流

要为内部FlexPod 存储配置工作流、请参见 "此链接。"。

"接下来：灾难恢复工作流。"

灾难恢复工作流

"先前版本：自动部署混合云NetApp存储。"

步骤顺序如下：

1. 定义工作流。
    - 为工作流创建一个用户友好的简短名称、例如Disaster Recovery Workflow。
2. 定义工作流输入。我们为此工作流提供了以下信息：
    - 卷选项(卷名称、挂载路径)
    - 卷容量
    - 与新数据存储库关联的数据中心
    - 托管数据存储库的集群
    - 要在vCenter中创建的新数据存储库的名称
    - 新数据存储库的类型和版本
    - Terraform组织的名称
    - Terraform工作空间
    - Terraform工作空间的问题描述
    - 执行Terraform配置所需的变量(敏感和非敏感)
    - 启动计划的原因
3. 添加工作流任务。

    与FlexPod 中的操作相关的任务包括：

- 在FlexPod 中创建卷。
- 向创建的卷添加存储导出策略。
- 将新创建的卷映射到VMware vCenter中的数据存储库。

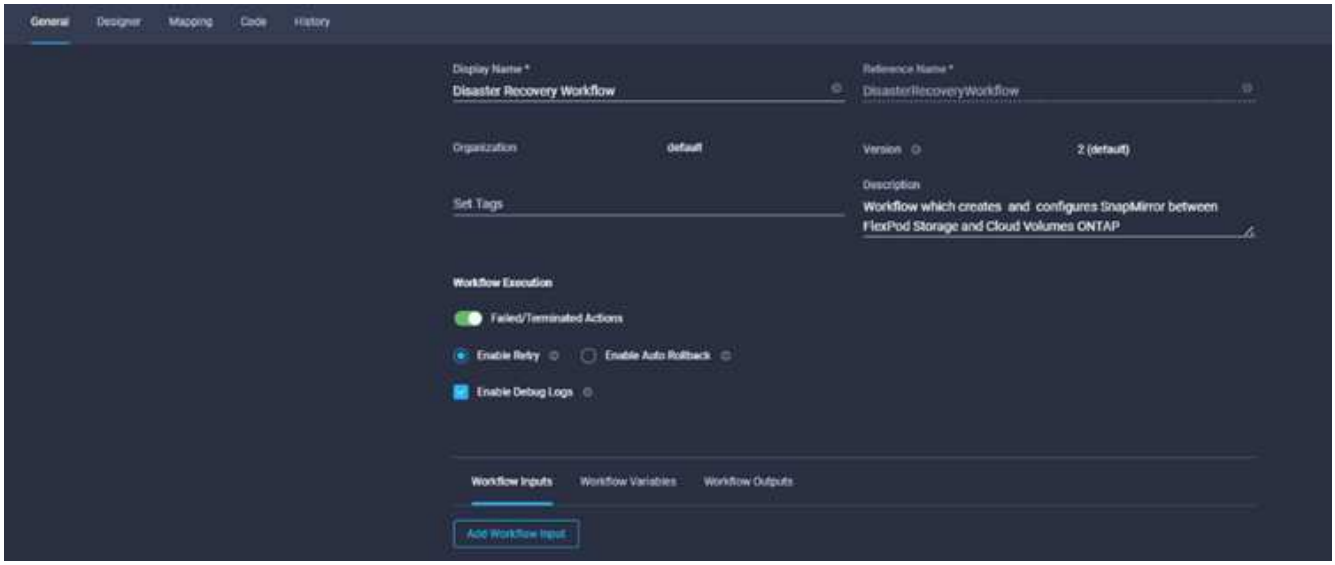
  与创建Cloud Volumes ONTAP 集群相关的任务：

- 添加Terraform工作空间
- 添加Terraform变量
- 添加Terraform敏感变量
- 启动新的Terraform计划
- 确认Terraform运行

4. 验证工作流。

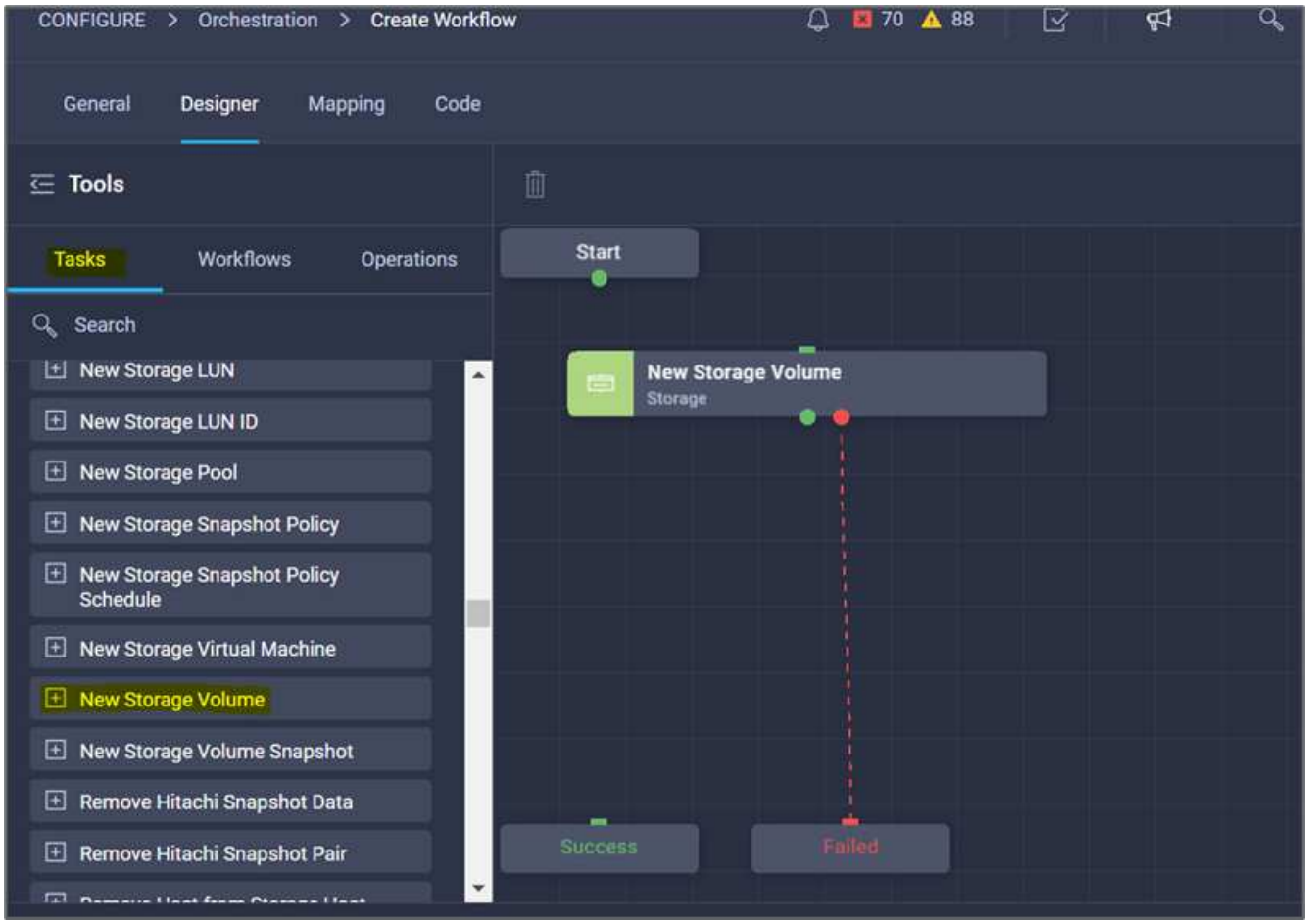
操作步骤 **1**：创建工作流

1. 单击左侧导航窗格中的*流程编排*、然后单击*创建工作流*。
2. 在*常规*选项卡中：
   a. 提供显示名称(灾难恢复工作流)。
   b. 选择组织、设置标记并提供问题描述。
3. 单击保存。

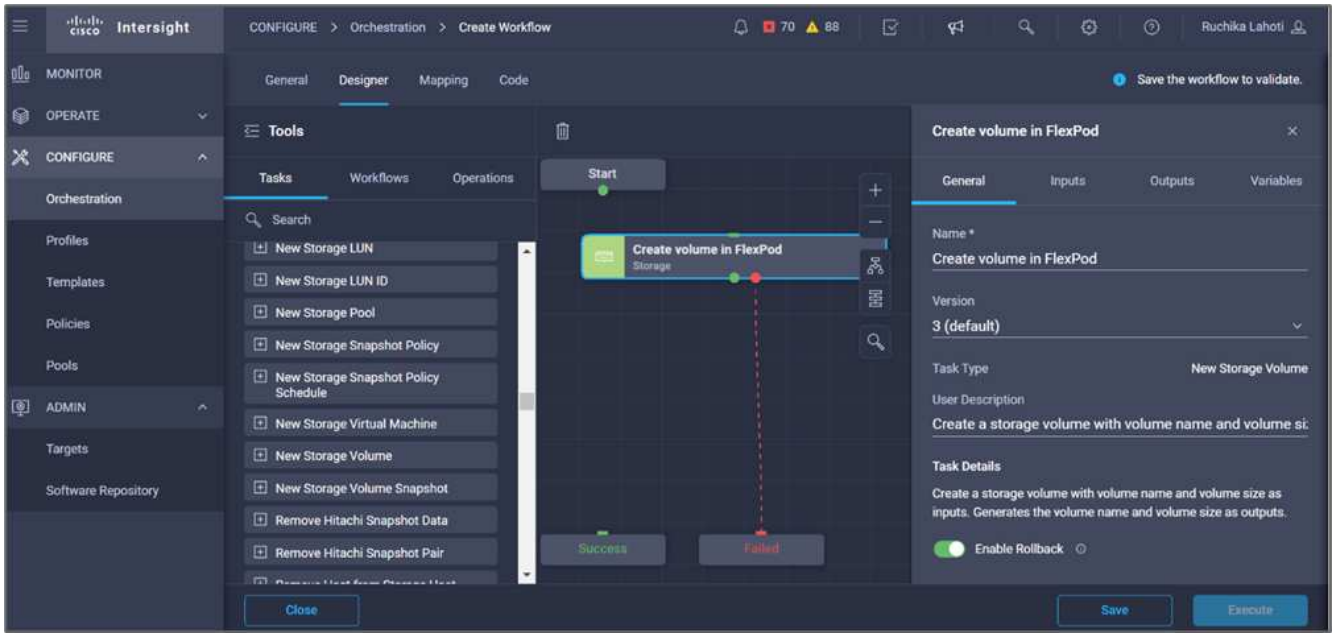


操作步骤 **2.**在**FlexPod** 中创建新卷

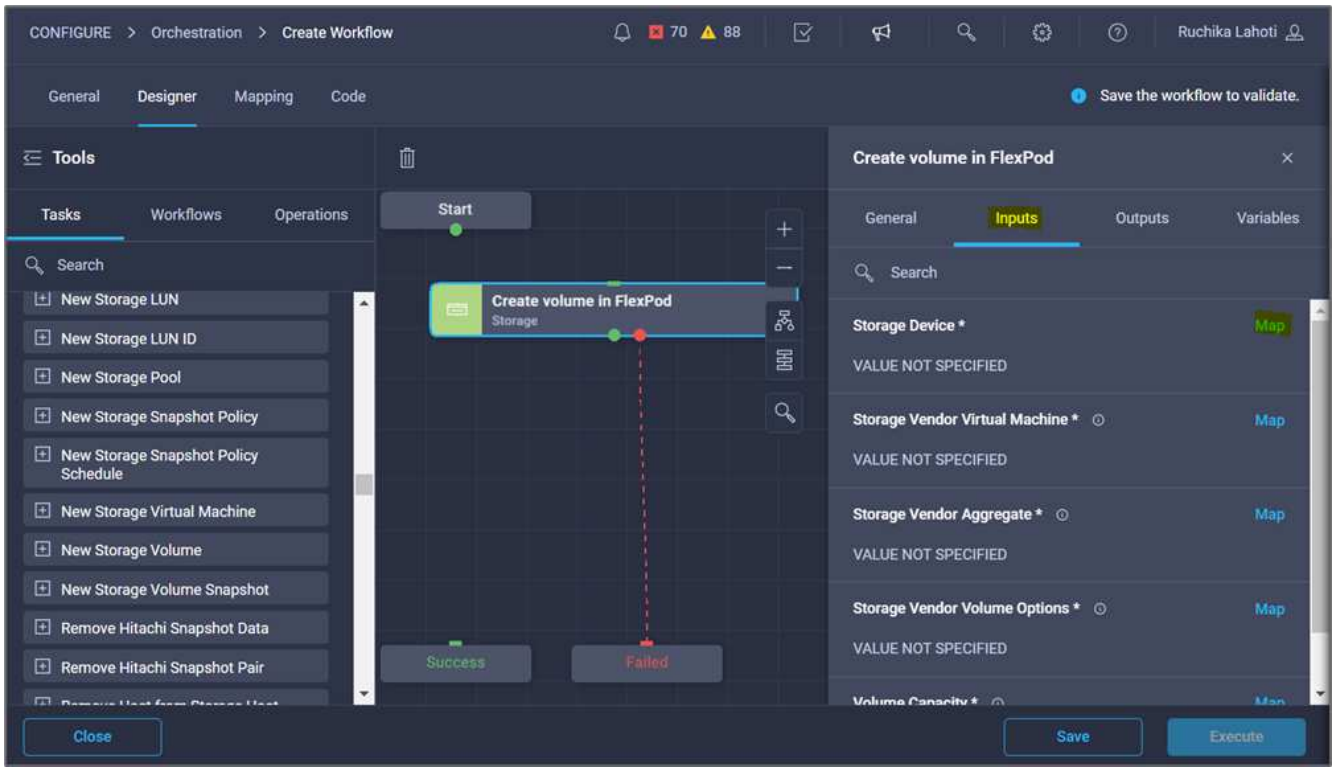
1. 转到*设计器*选项卡、然后单击*工具*部分中的*任务*。
2. 将*存储>新存储卷*任务从*工具*部分拖放到*设计*区域中。
3. 单击*新建存储卷*。



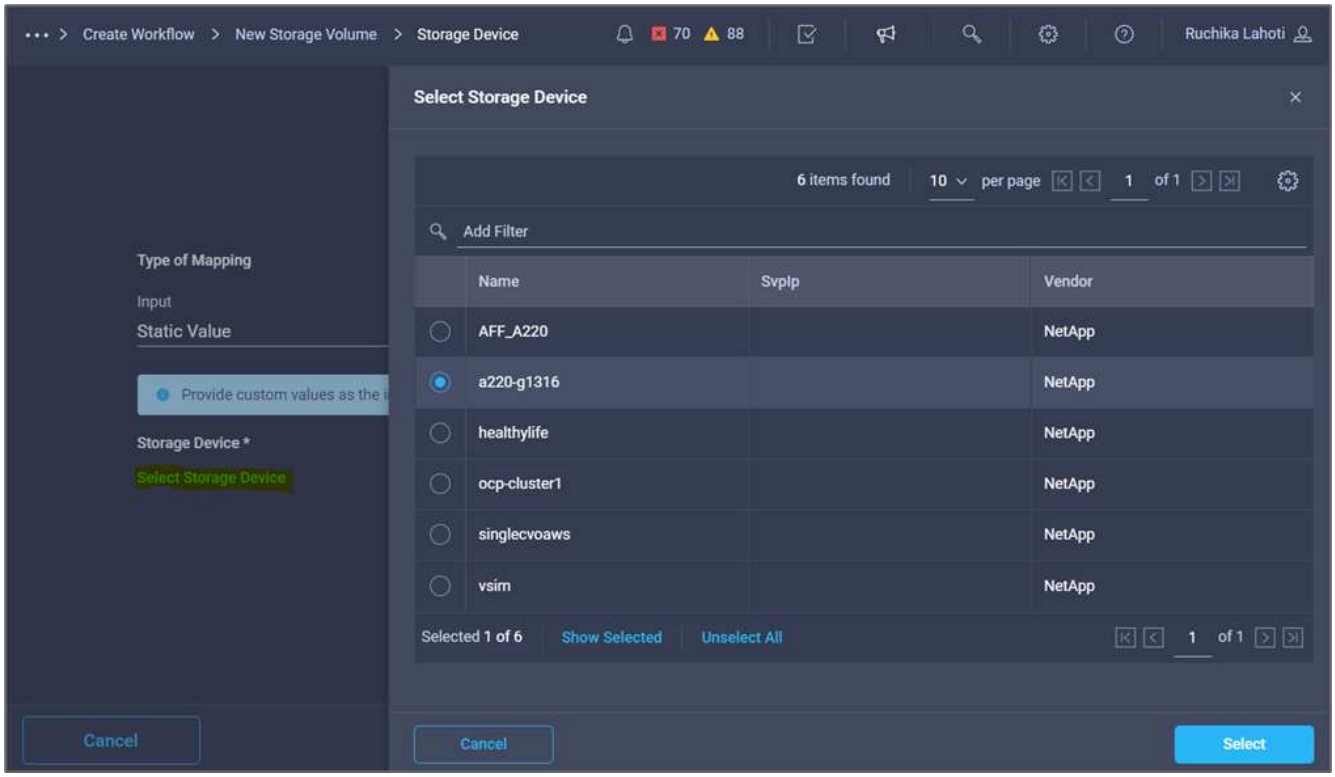
4. 在*任务属性*区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。在此示例中、任务的名称是*在FlexPod 中创建卷*。



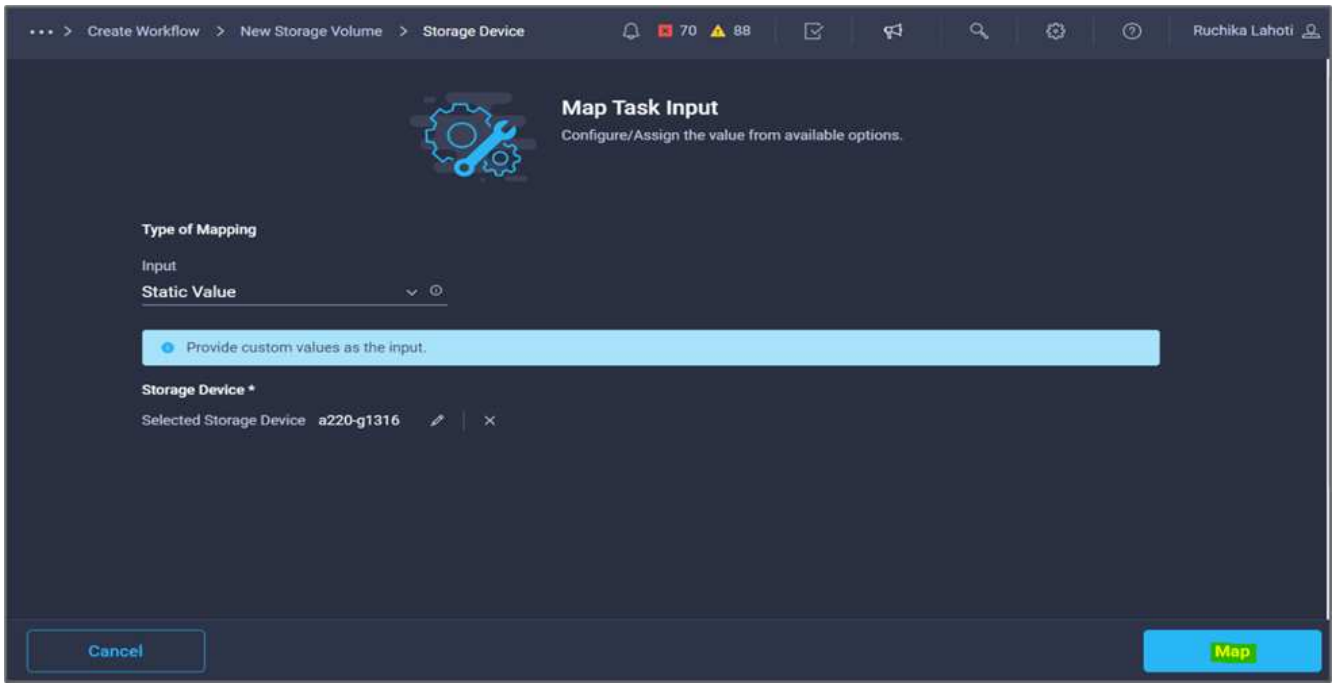
5. 在*任务属性*区域中、单击*输入*。
6. 单击*存储设备*字段中的*映射*。



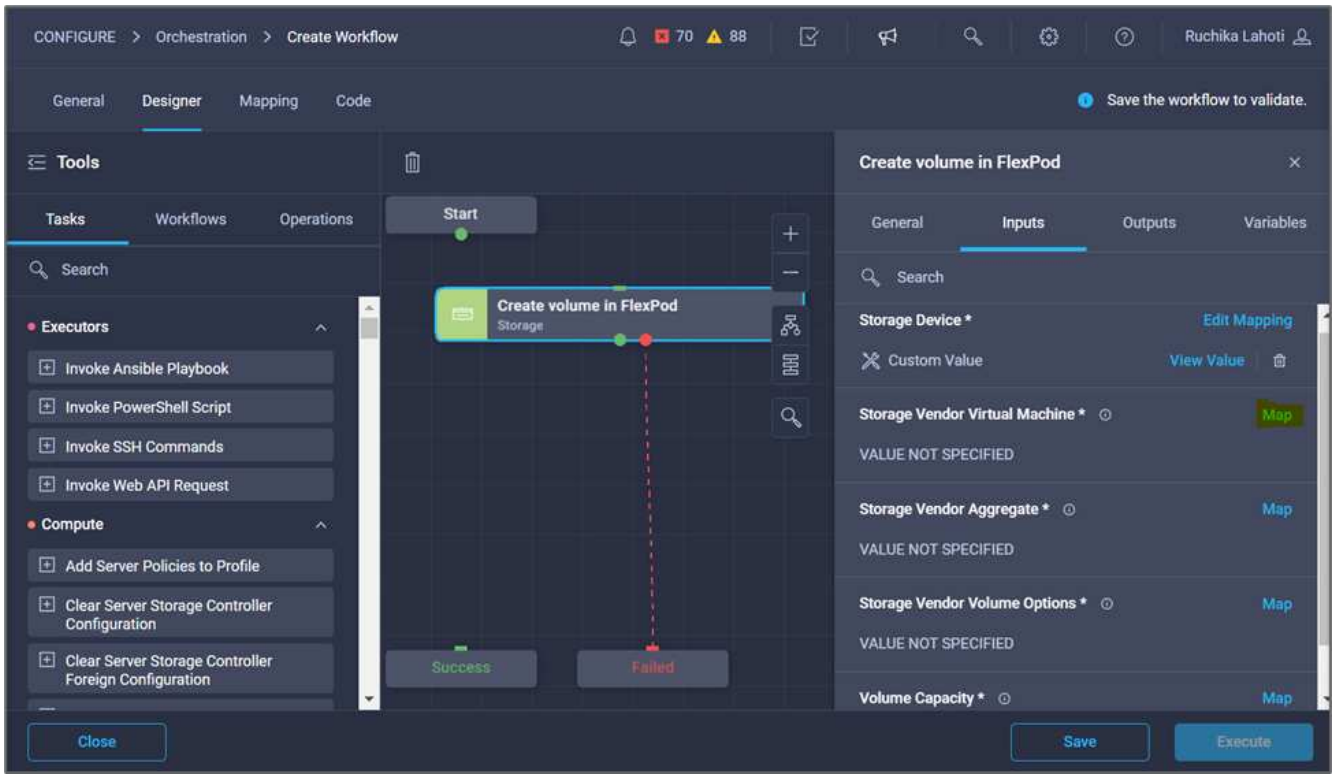
7. 选择*静态值*、然后单击*选择存储设备*。
8. 单击已添加的存储目标、然后单击*选择*。



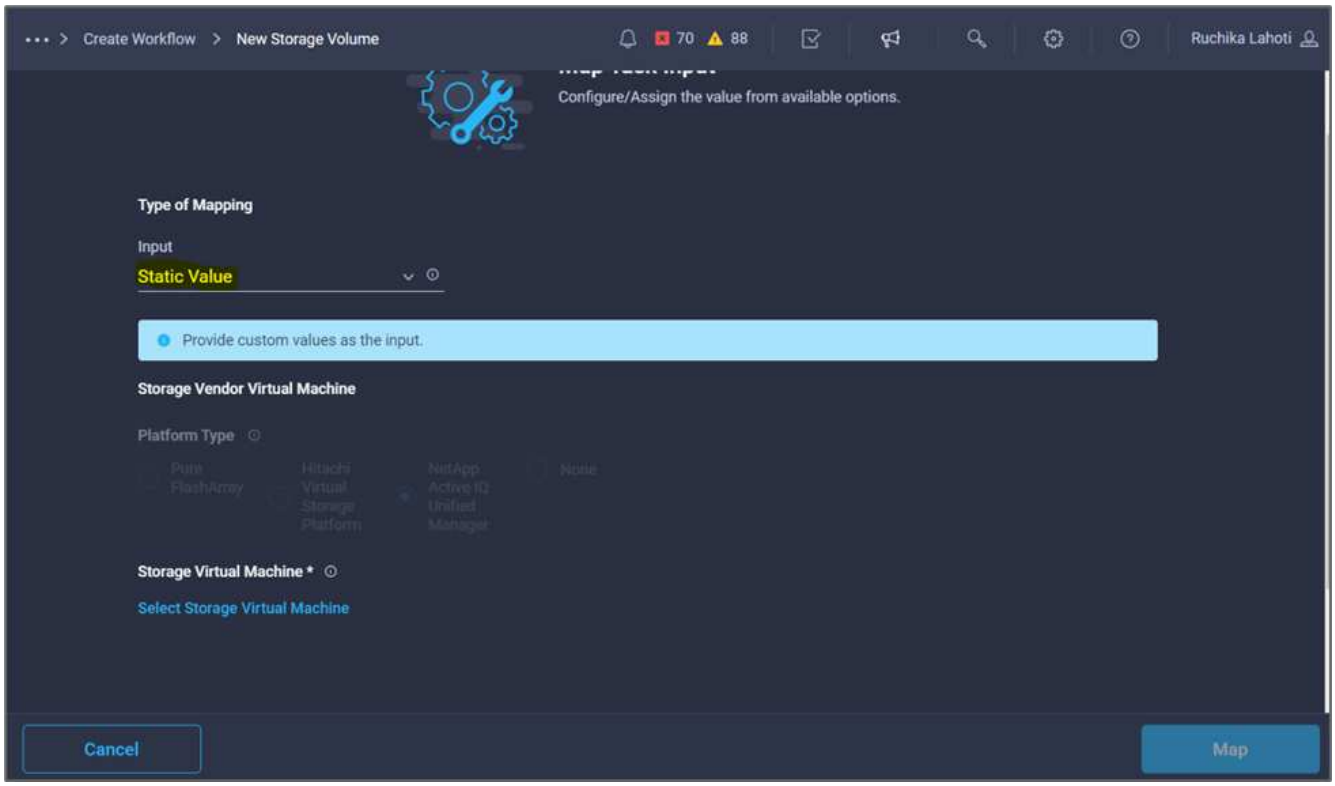
9. 单击*映射*。



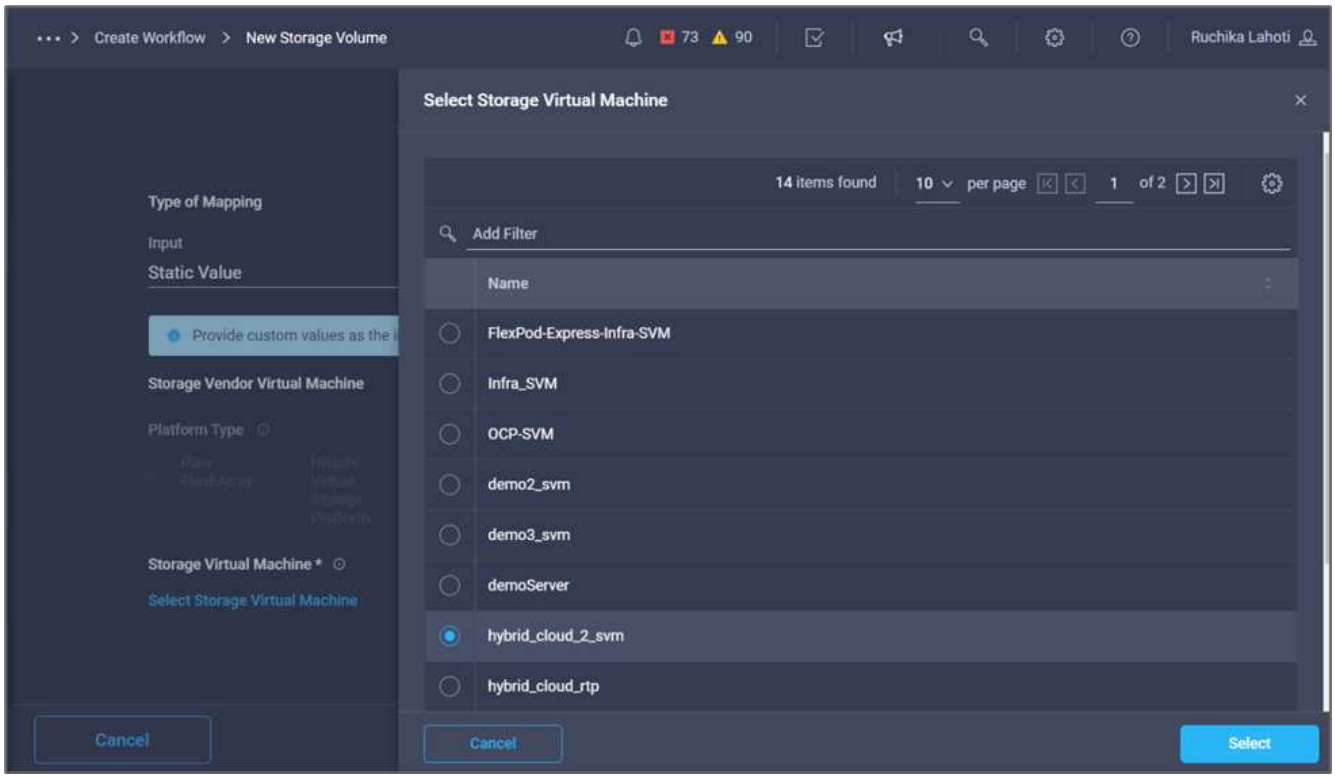
10. 单击*存储供应商虚拟机*字段中的*映射*。



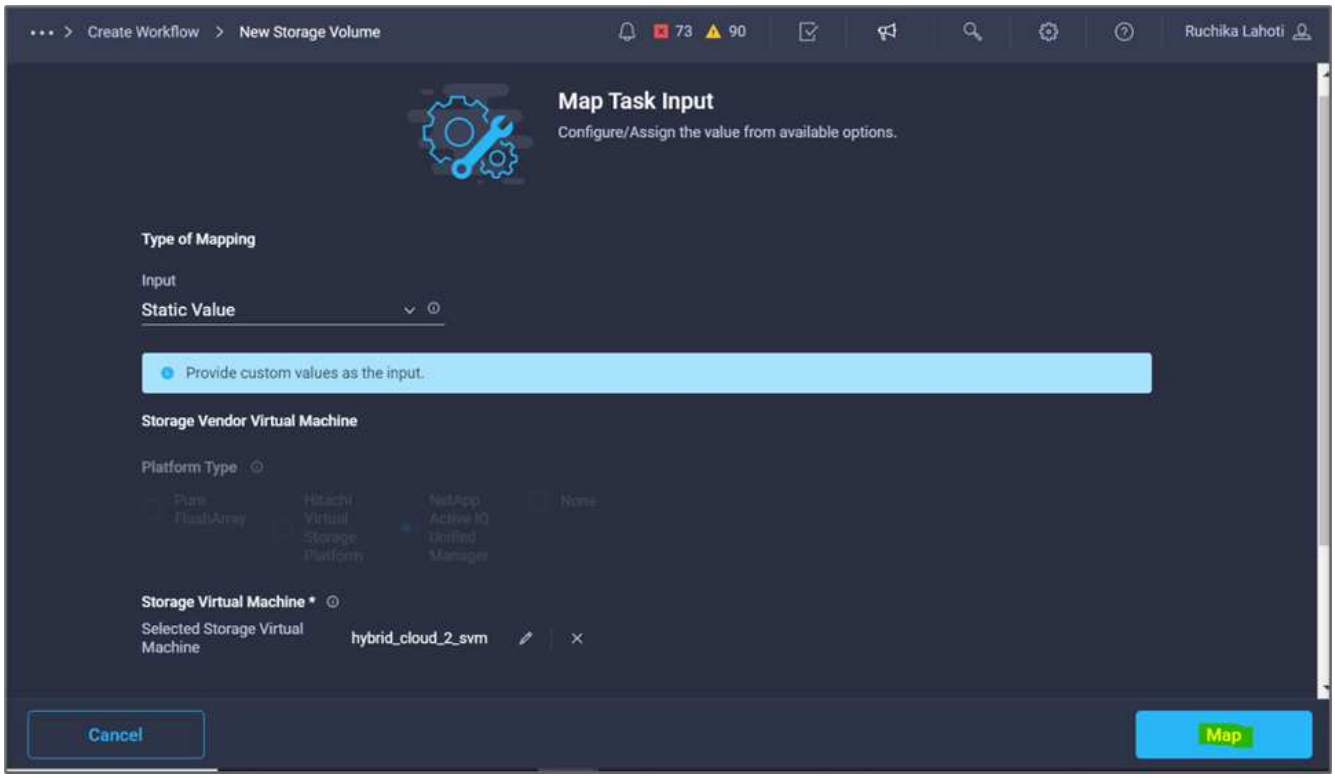
11. 选择*静态值*、然后单击*选择Storage Virtual Machine*。



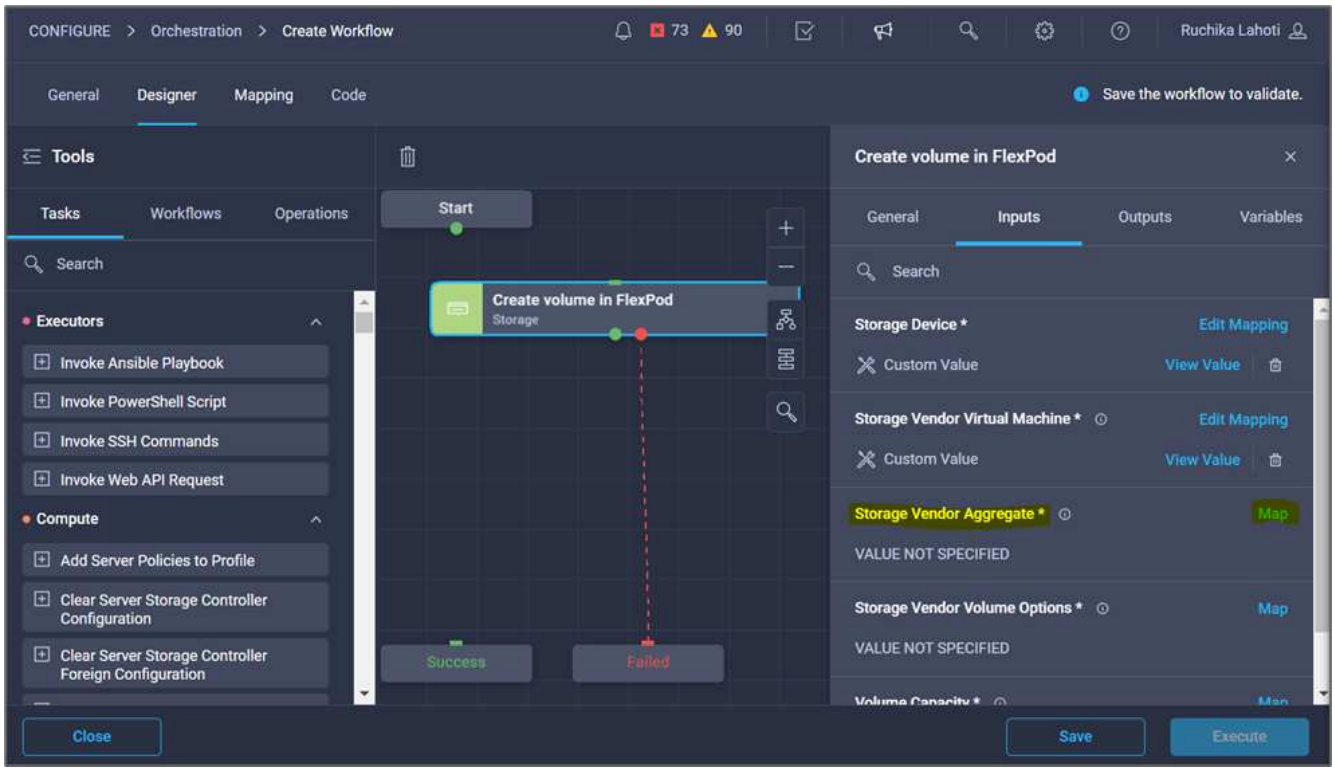
12. 选择需要创建卷的Storage Virtual Machine、然后单击*选择*。



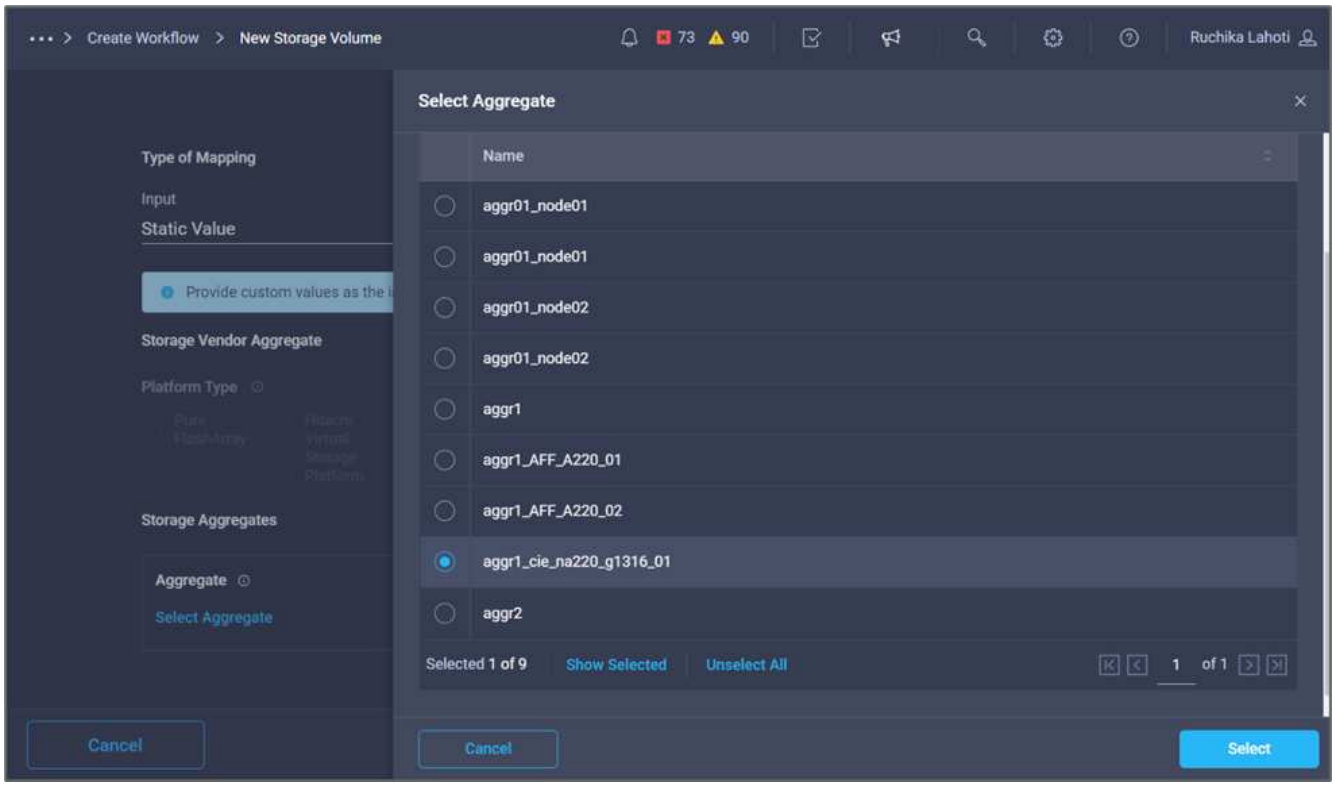
13. 单击*映射*。



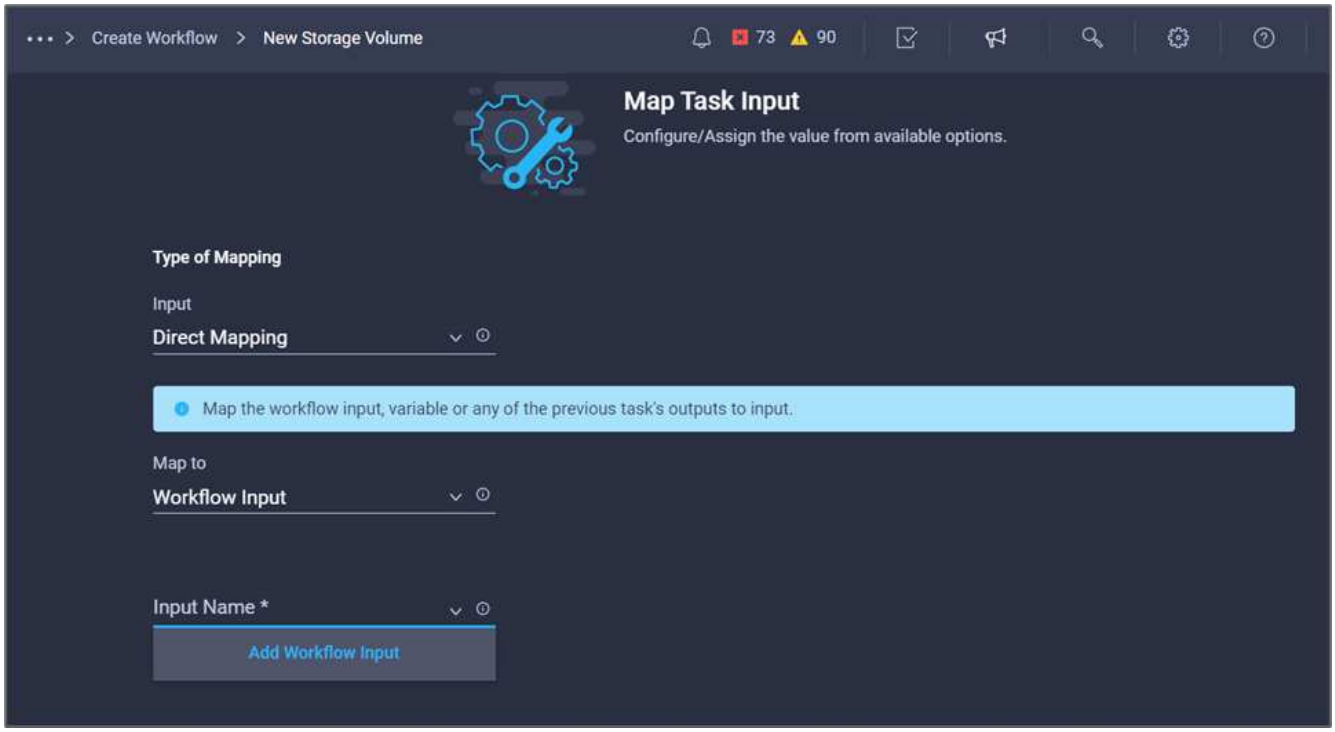
14. 单击*存储供应商聚合*字段中的*映射*。



15. 选择*静态值*、然后单击*选择存储聚合*。选择聚合并单击*选择*。

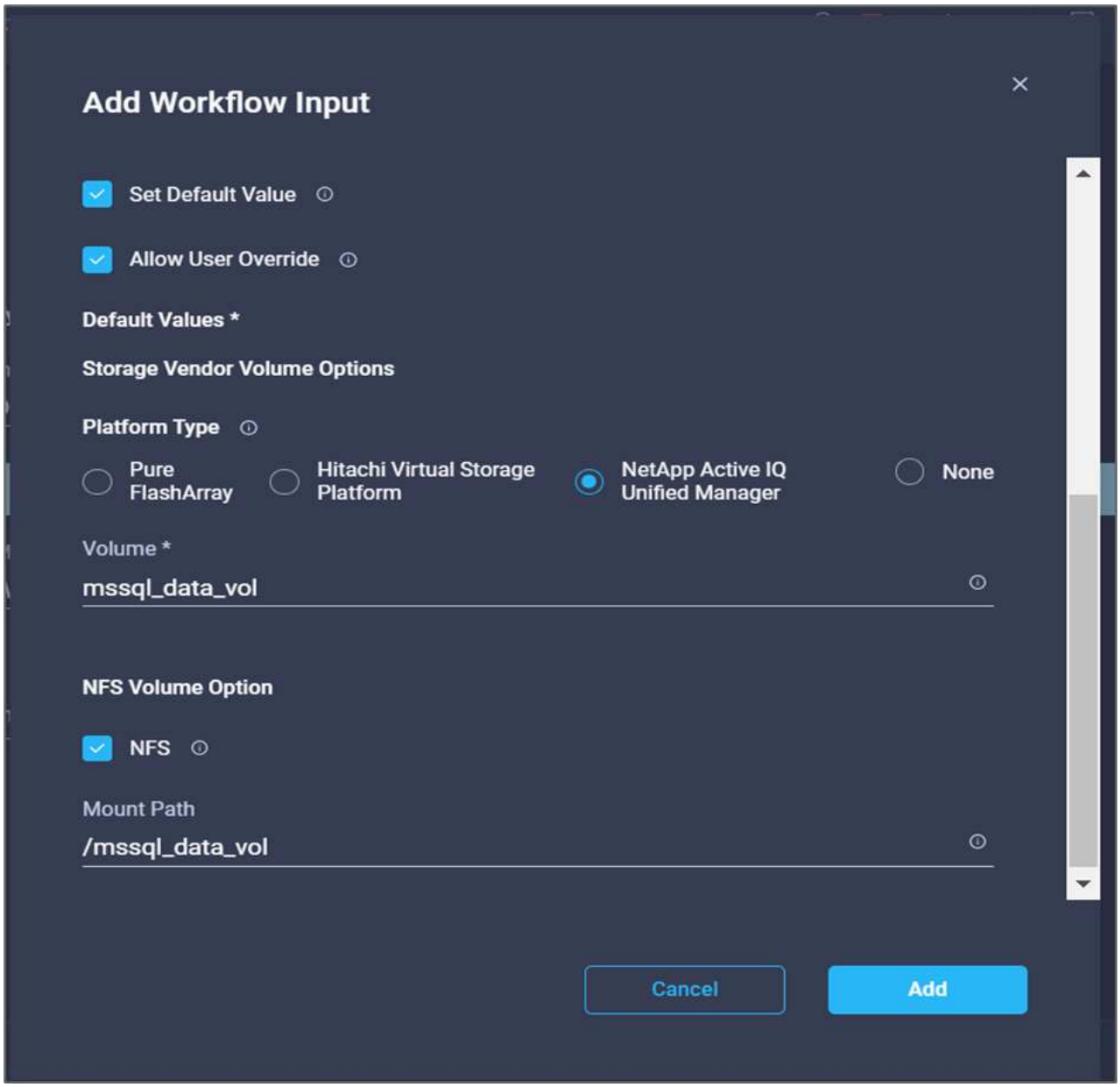


16. 单击*映射*。
17. 单击*存储供应商卷选项*字段中的*映射*。
18. 选择*直接映射*、然后单击*工作流输入*。

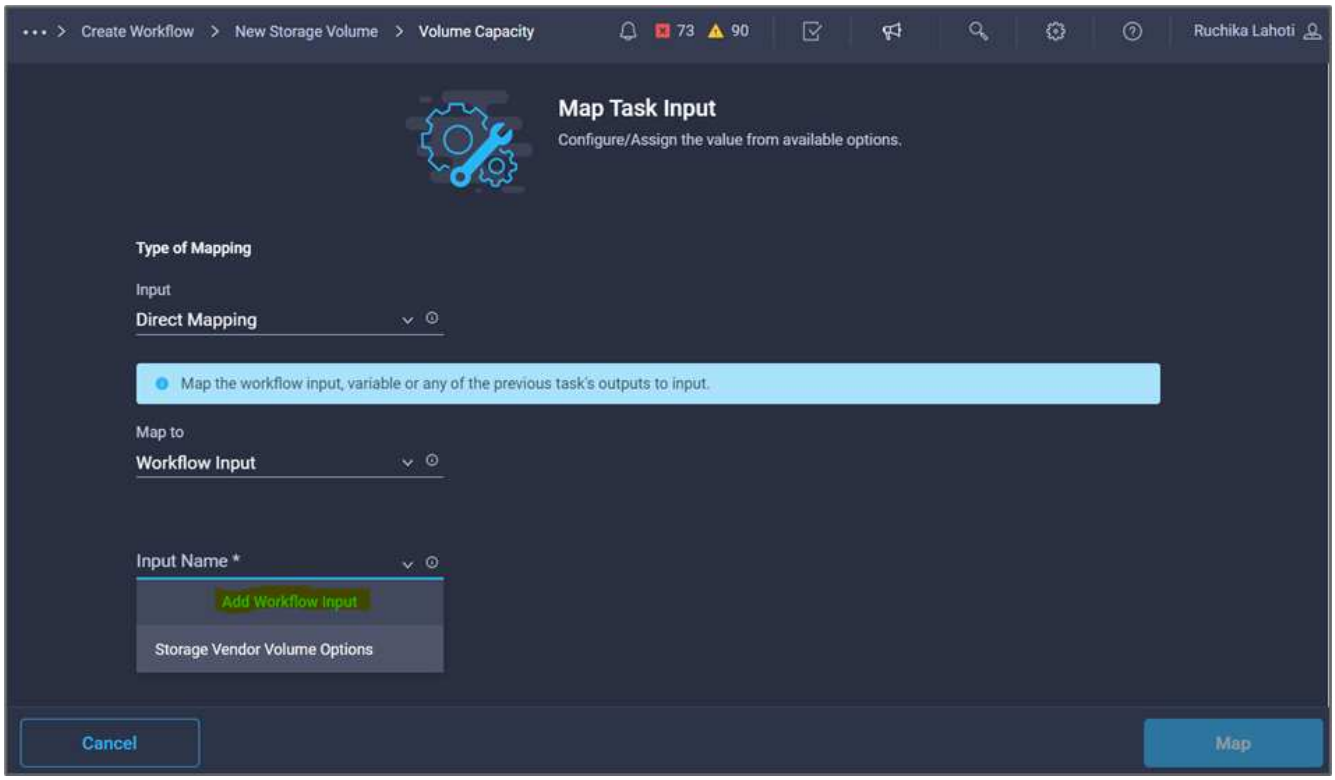


19. 在添加输入向导中、完成以下步骤：
    a. 提供显示名称和参考名称(可选)。

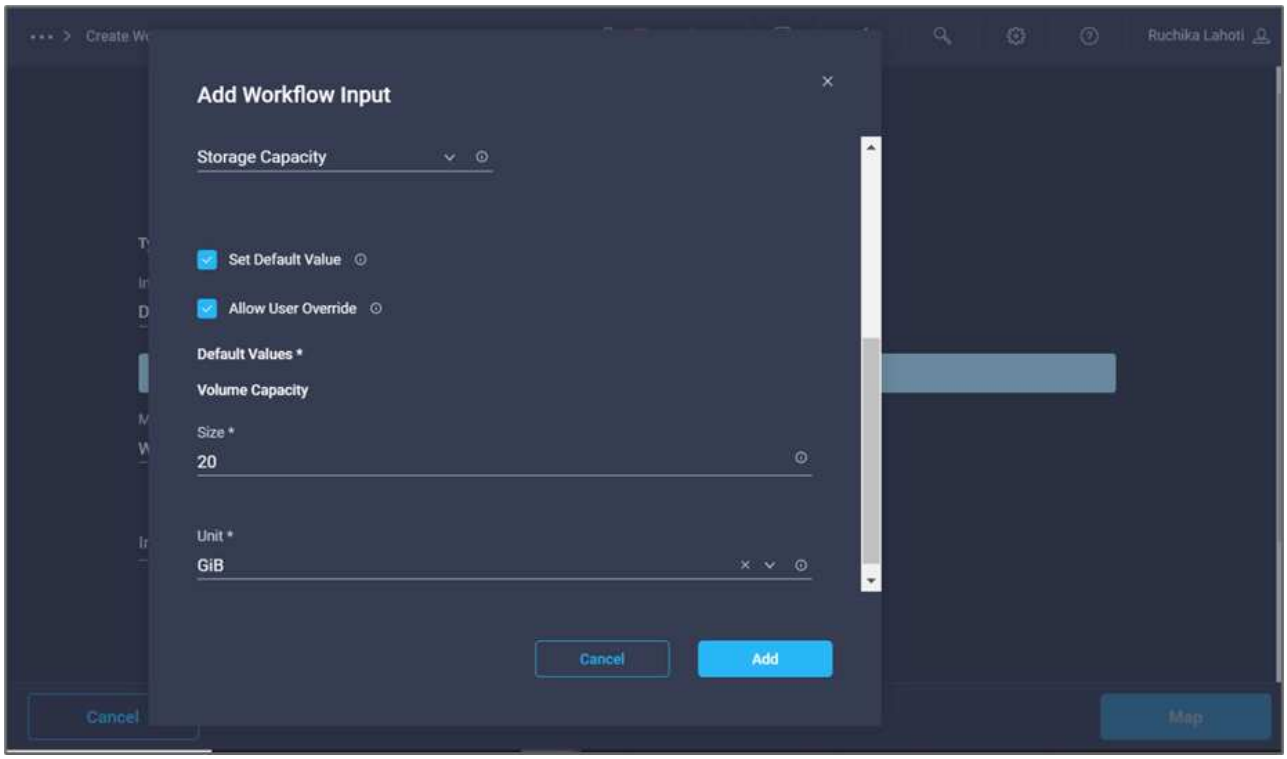
b. 确保为*类型*选择了*存储供应商卷选项*。
c. 单击*设置默认值并覆盖*。
d. 单击*必需*。
e. 将*平台类型*设置为* NetApp Active IQ Unified Manager *。
f. 在*卷*下为创建的卷提供默认值。
g. 单击*。nfs*。如果设置了NFS、则会创建NFS卷。如果此值设置为false、则会创建SAN卷。
h. 提供挂载路径、然后单击*添加*。



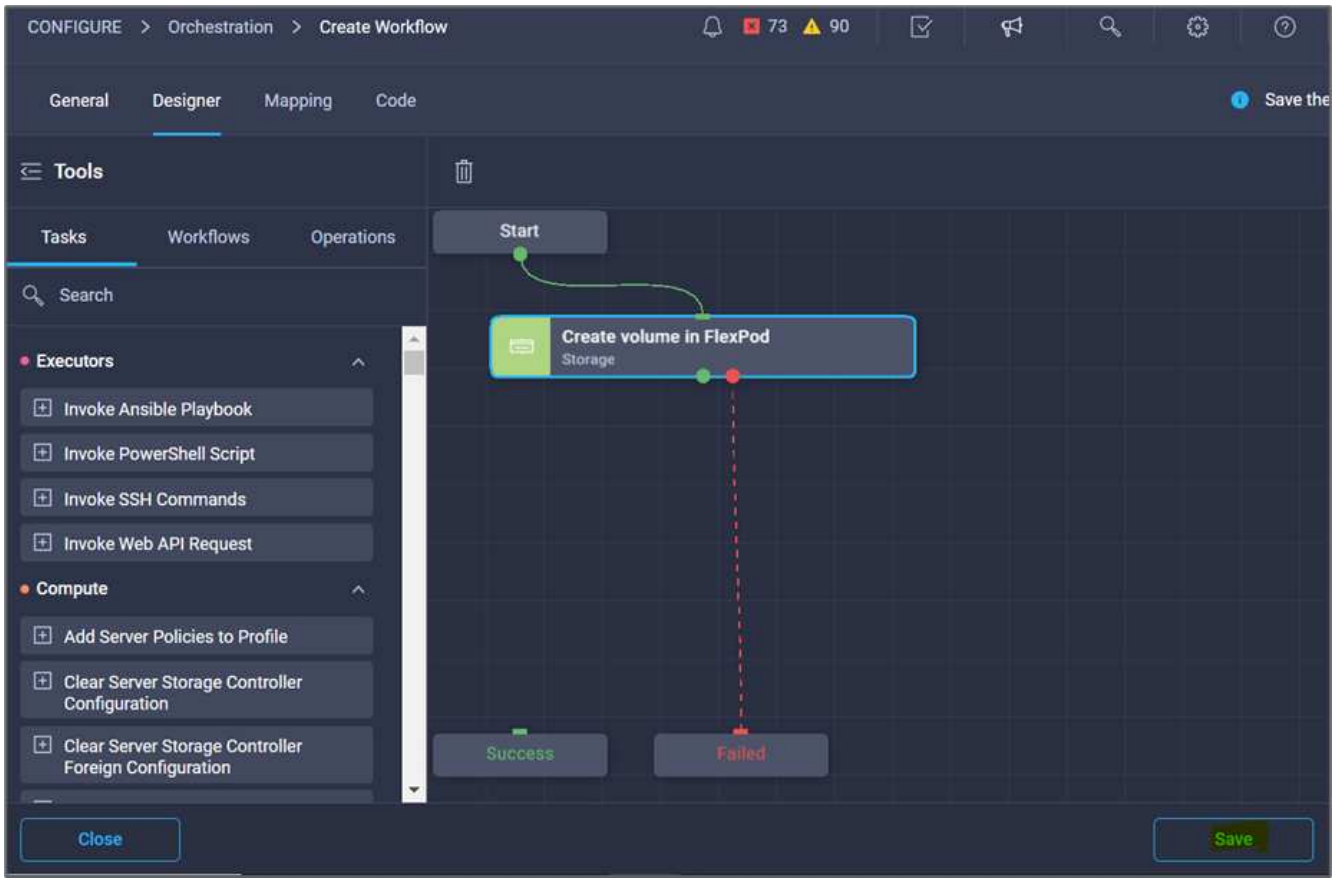
20. 单击*映射*。
21. 单击*卷容量*字段中的*映射*。
22. 选择*直接映射*、然后单击*工作流输入*。
23. 单击*输入名称*和*创建工作流输入*。



24. 在添加输入向导中：
    a. 提供显示名称和参考名称(可选)。
    b. 单击*必需*。
    c. 对于*类型*、选择*存储容量*。
    d. 单击*设置默认值并覆盖*。
    e. 为卷大小和单位提供默认值。
    f. 单击 * 添加 * 。



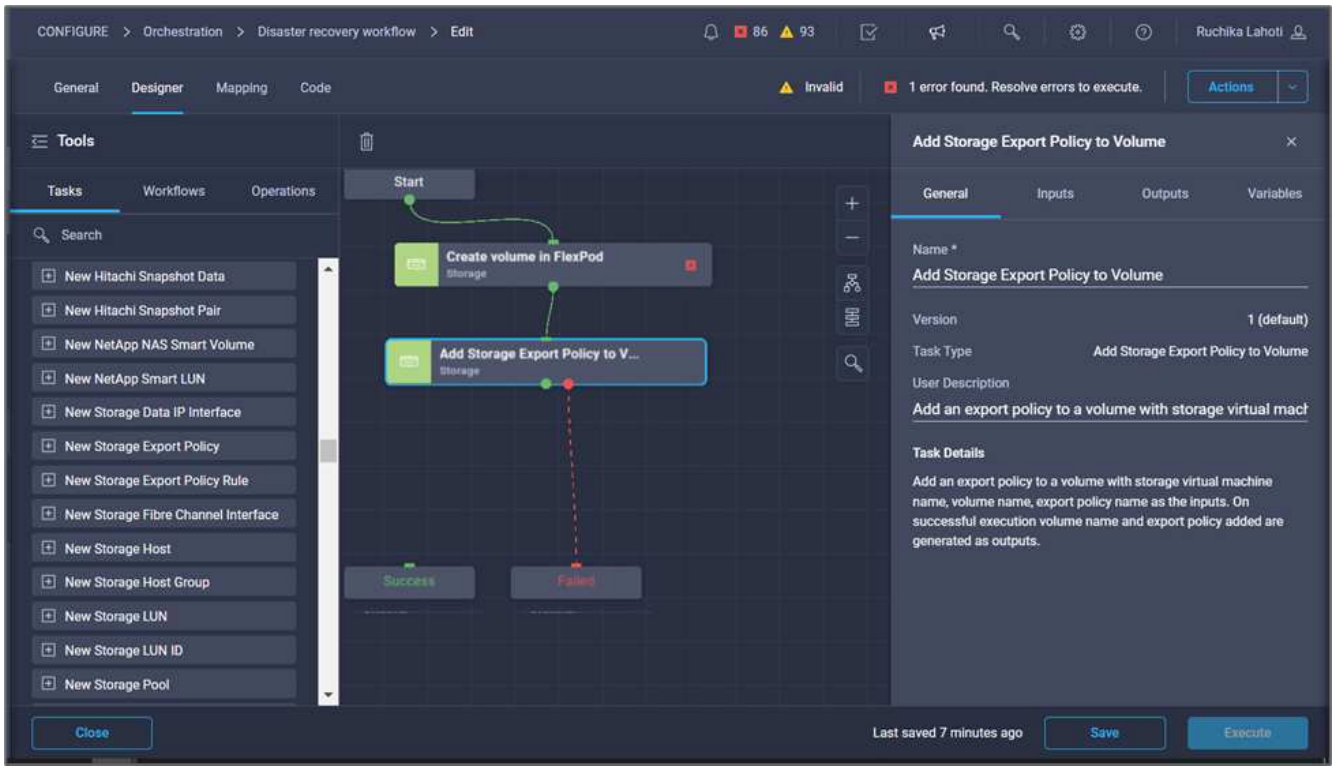
25. 单击*映射*。
26. 使用Connector在*启动*和*在FlexPod 中创建卷*任务之间创建连接、然后单击*保存*。



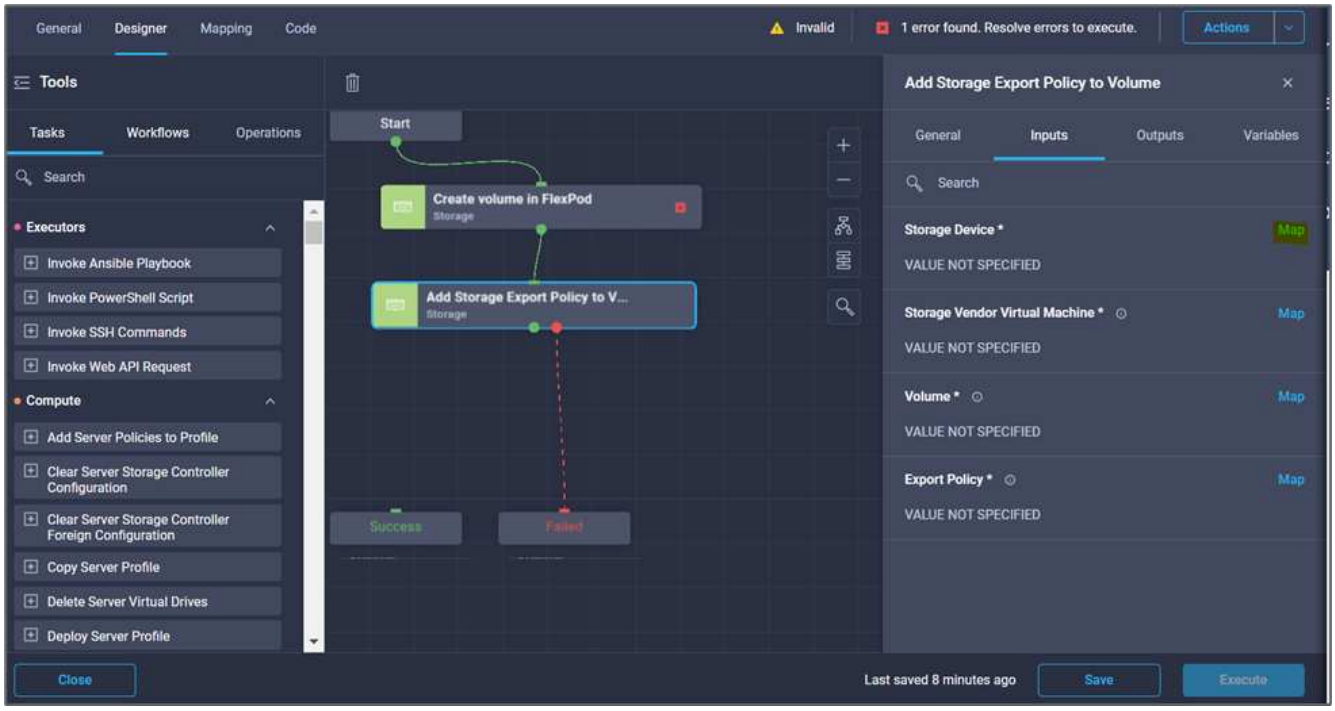
现在忽略此错误。显示此错误的原因是、*在FlexPod 中创建卷*和*成功*任务之间没有连接、而这是指定成功过渡所必需的。

操作步骤 **3**：添加存储导出策略

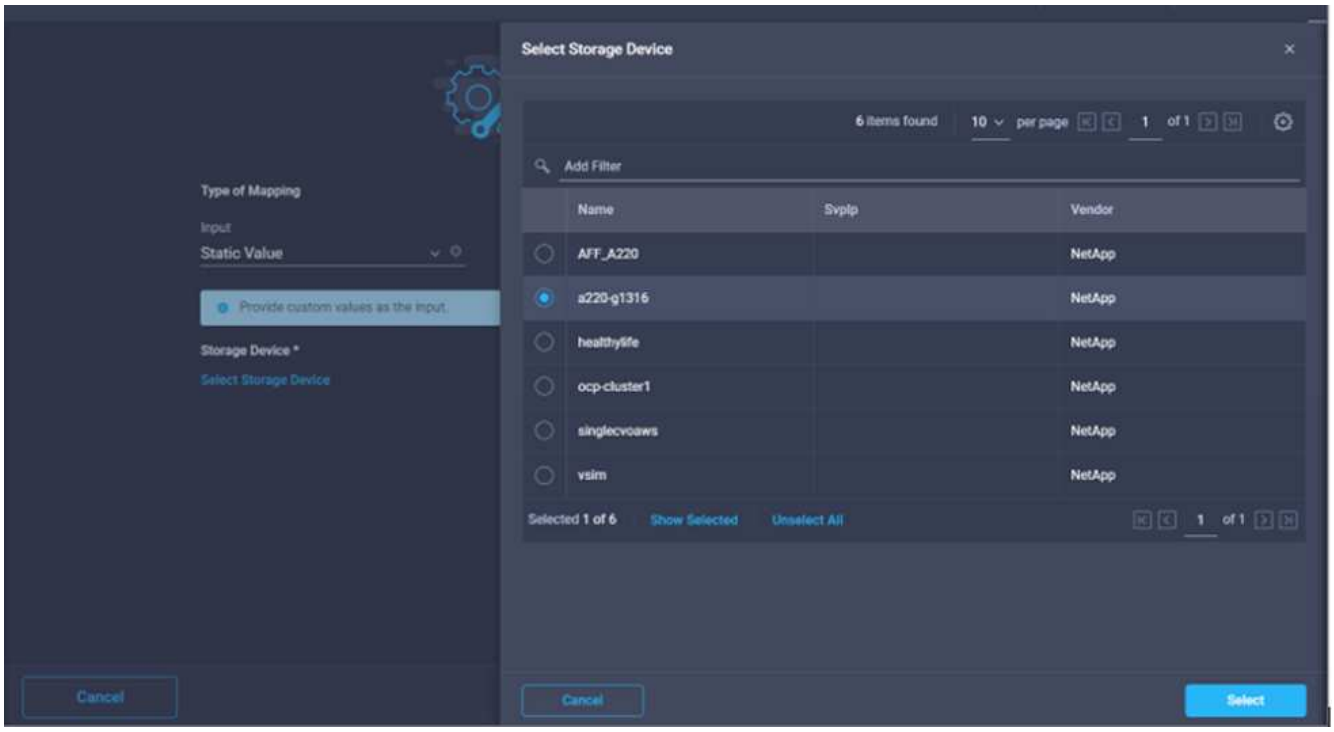
1. 转到*设计器*选项卡、然后单击*工具*部分中的*任务*。
2. 从*设计*区域的*工具*部分拖放*存储>将存储导出策略添加到卷*任务。
3. 单击*将存储导出策略添加到卷*。在*任务属性*区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。在此示例中、任务的名称是添加存储导出策略。
4. 使用连接器在*在FlexPod 中创建卷*和*添加存储导出策略*任务之间建立连接。单击 * 保存 * 。



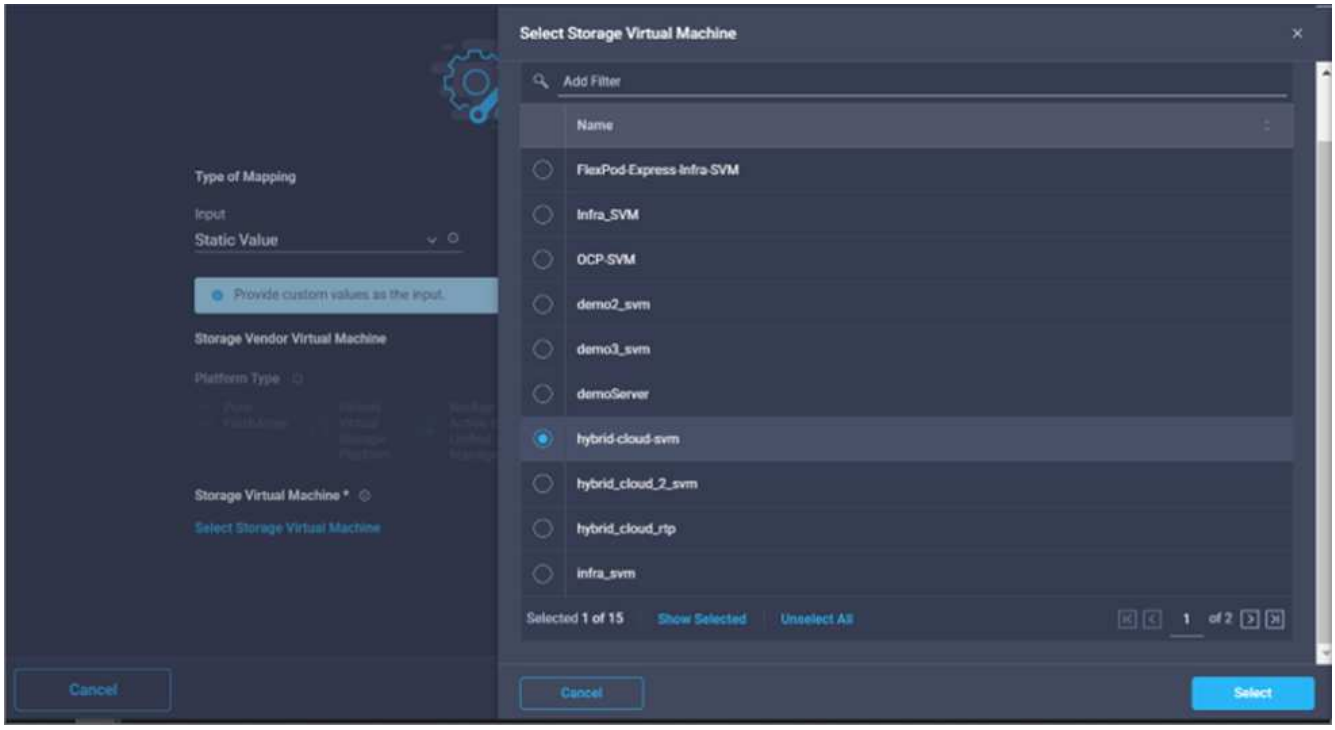
5. 在*任务属性*区域中、单击*输入*。
6. 单击*存储设备*字段中的*映射*。



7. 选择*静态值*、然后单击*选择存储设备*。选择在创建上一个创建新存储卷任务时添加的相同存储目标。
8. 单击*映射*。

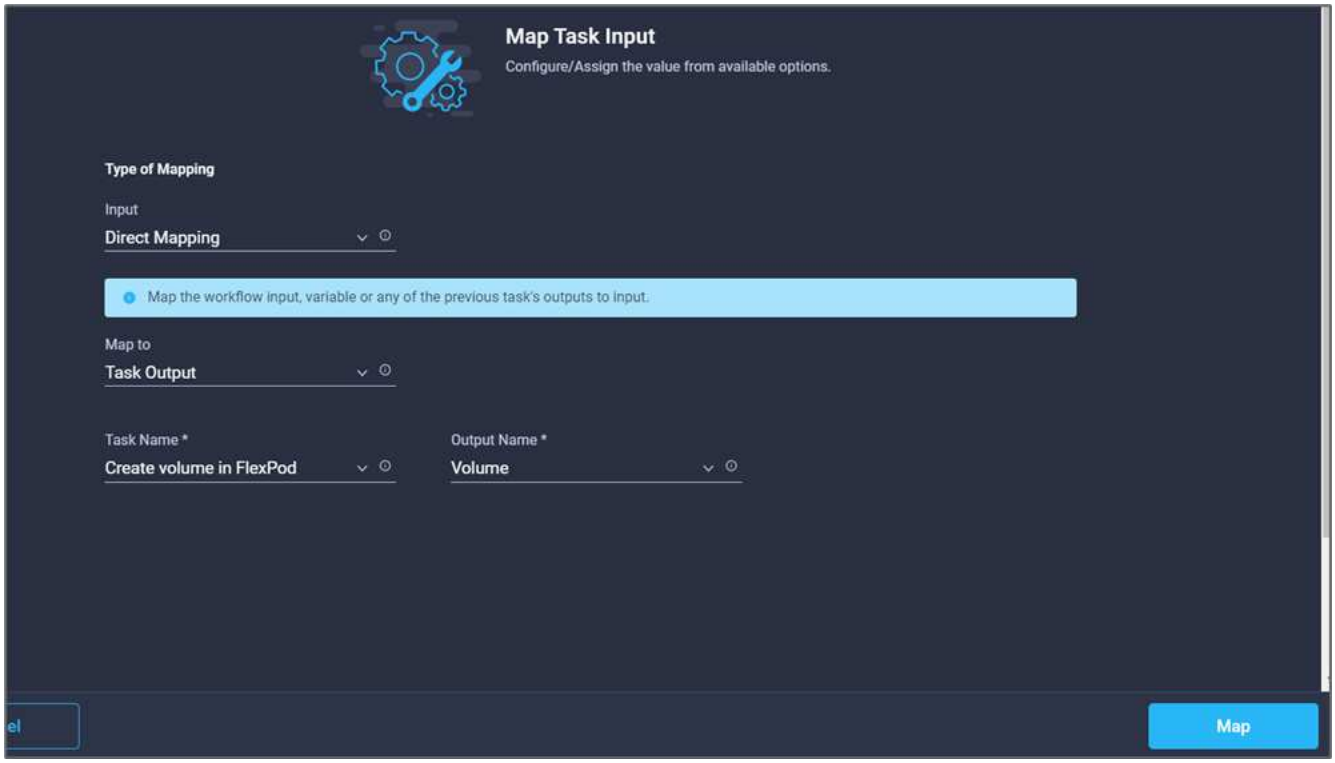


9. 单击*存储供应商虚拟机*字段中的*映射*。
10. 选择*静态值*、然后单击*选择Storage Virtual Machine*。选择在创建上一个创建新存储卷任务时添加的相同Storage Virtual Machine。

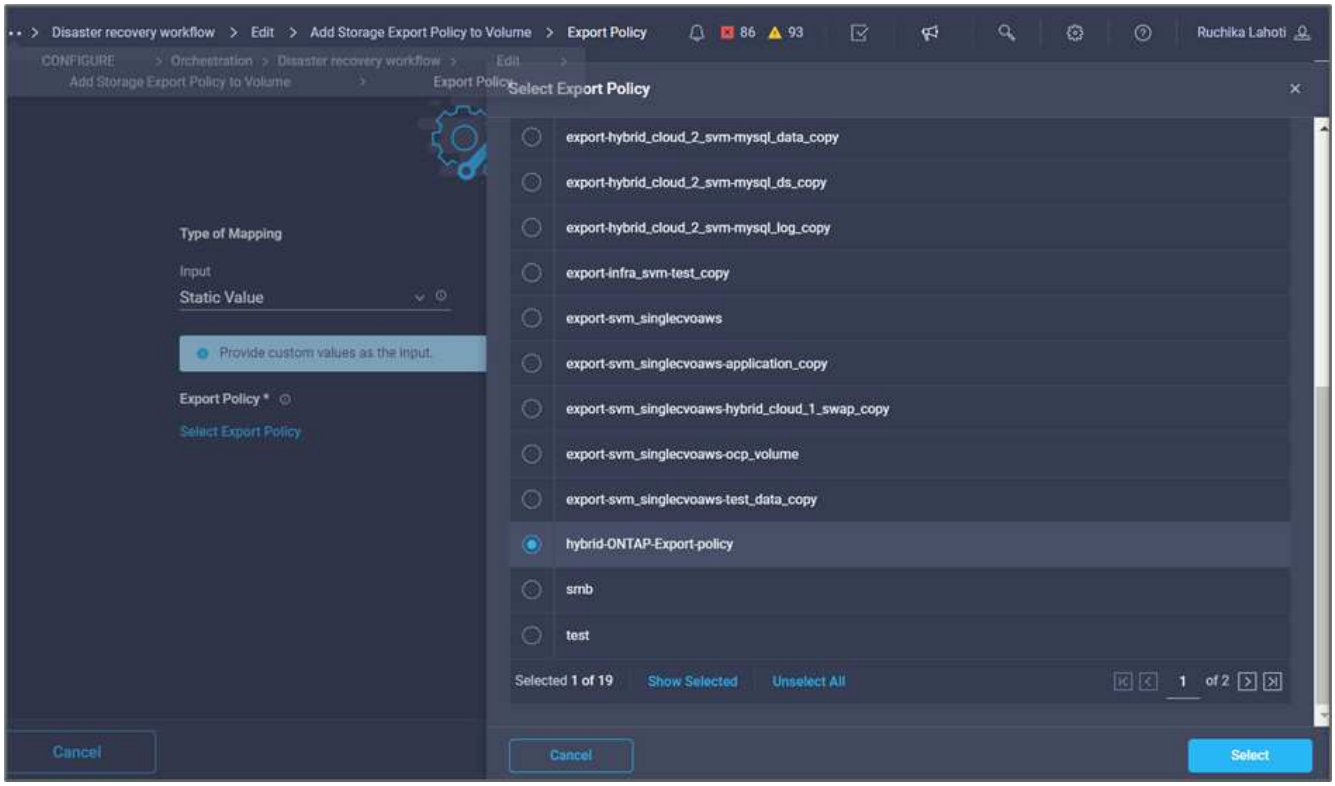


11. 单击*映射*。
12. 单击*卷*字段中的*映射*。
13. 单击*任务名称*、然后单击*在FlexPod 中创建卷*。单击*输出名称*、然后单击*卷*。

> 在Cisco Intersight Cloud Orchestrator中、您可以提供上一个任务的输出作为新任务的输入。在此示例中、*在FlexPod 中创建卷*任务提供了*卷*详细信息、作为*添加存储导出策略*任务的输入。



14. 单击*映射*。
15. 单击*导出策略*字段中的*映射*。
16. 选择*静态值*、然后单击*选择导出策略*。选择已创建的导出策略。

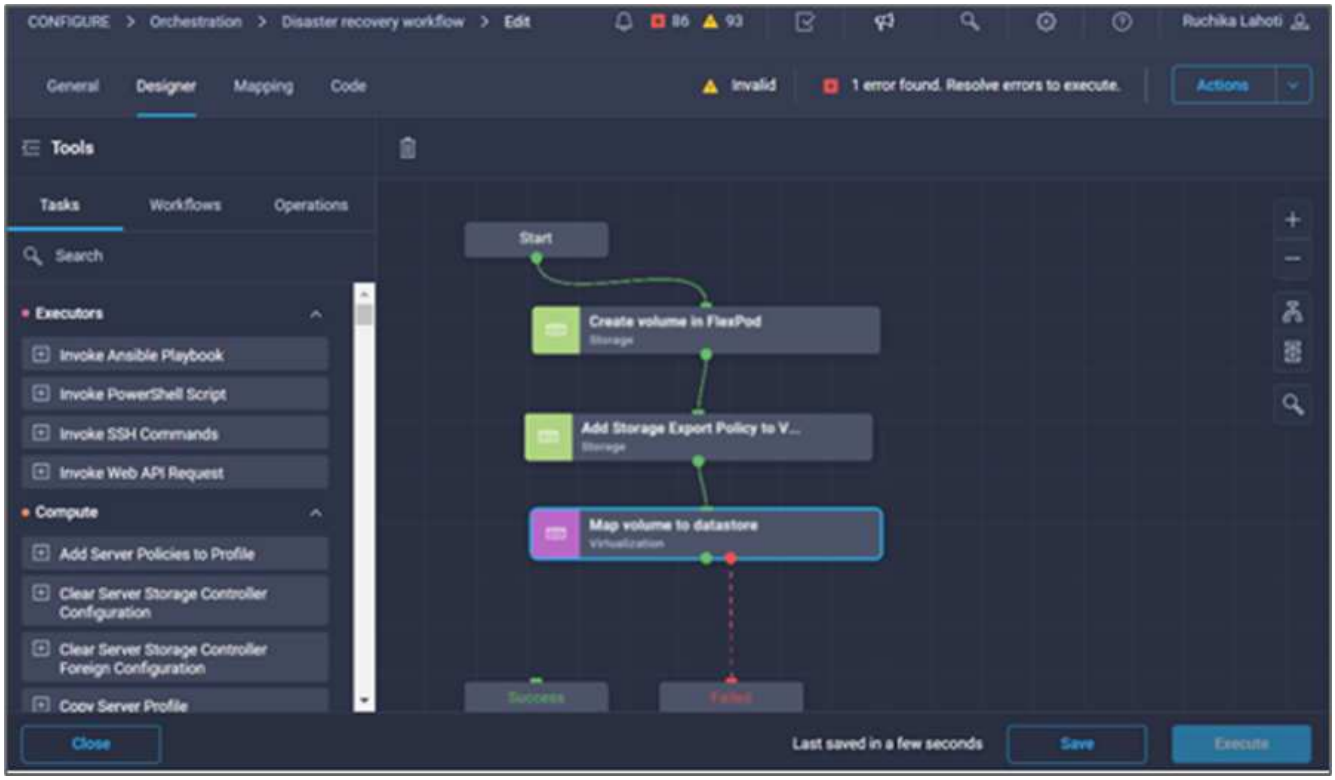


17. 单击*映射*、然后单击*保存*。

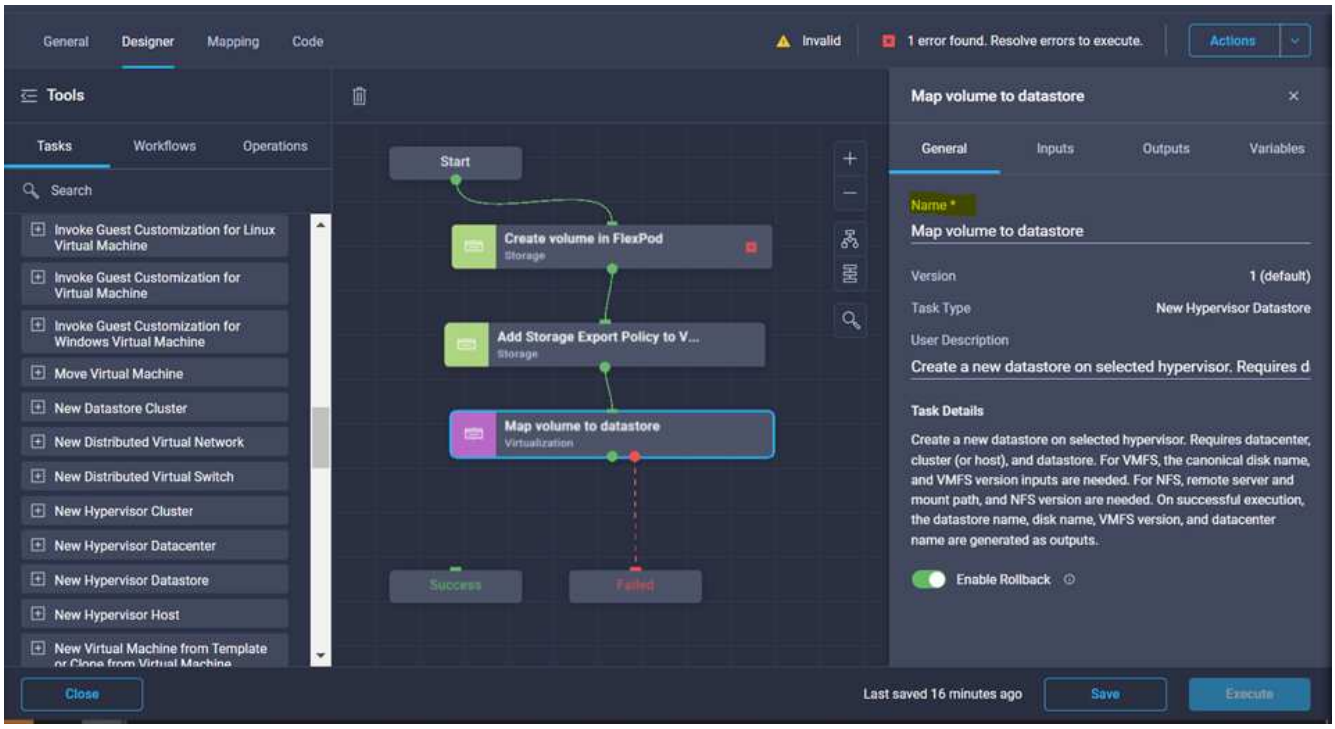
> 此时将向卷添加导出策略。接下来、创建一个新的数据存储库来映射已创建的卷。

操作步骤 **4**：将**FlexPod** 卷映射到数据存储库

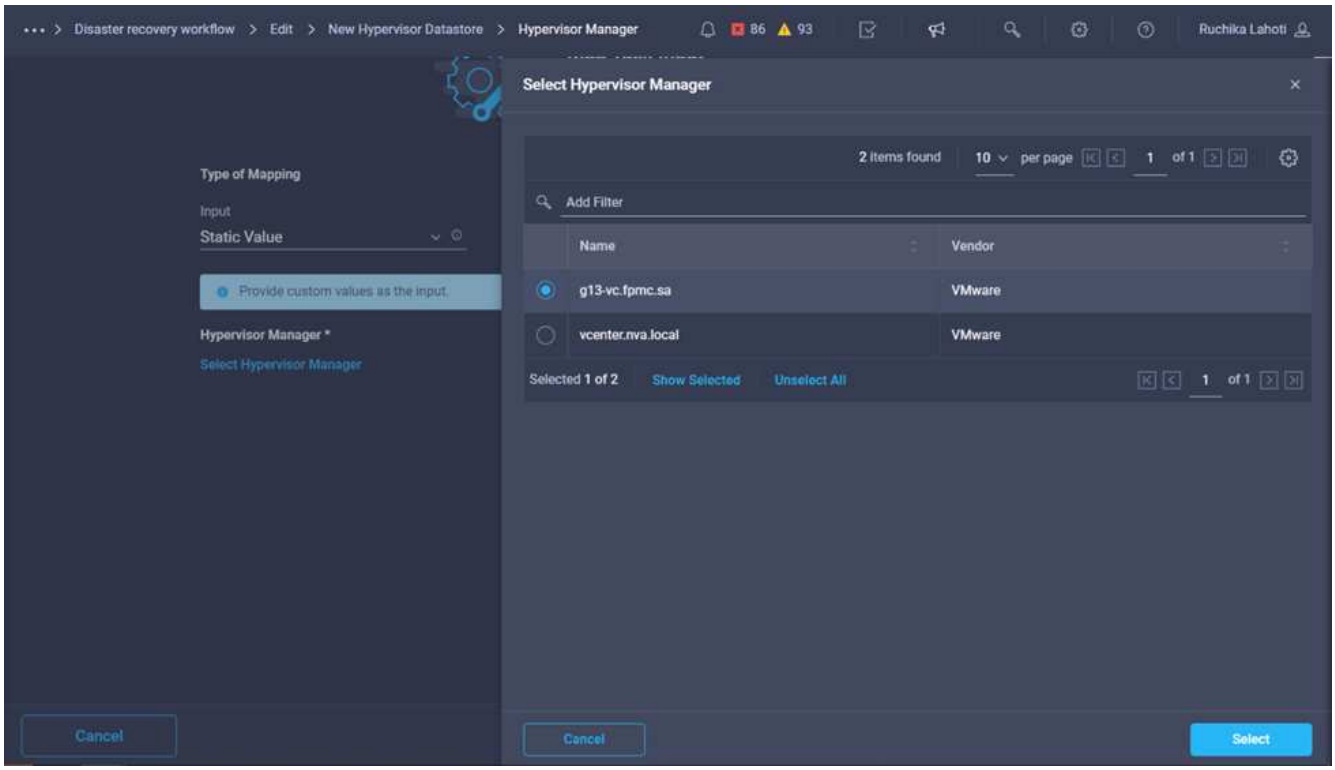
1. 转到*设计器*选项卡、然后单击*工具*部分中的*任务*。
2. 从*设计*区域的*工具*部分拖放*虚拟化>新虚拟机管理程序数据存储库*任务。
3. 使用Connector在*添加存储导出策略*和*新建虚拟机管理程序数据存储库*任务之间建立连接。单击 * 保存 * 。



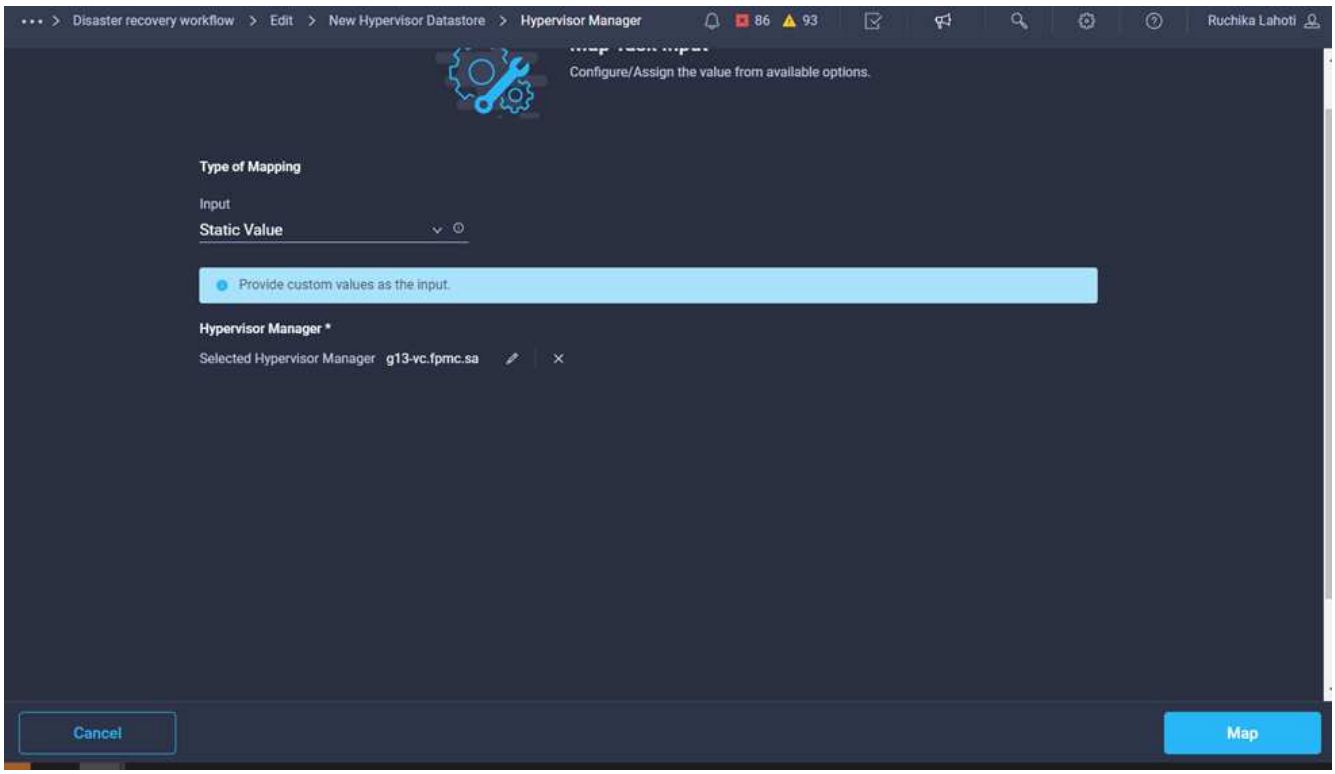
4. 单击*新建虚拟机管理程序数据存储库*。在*任务属性*区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。在此示例中、任务的名称是*将卷映射到数据存储库*。



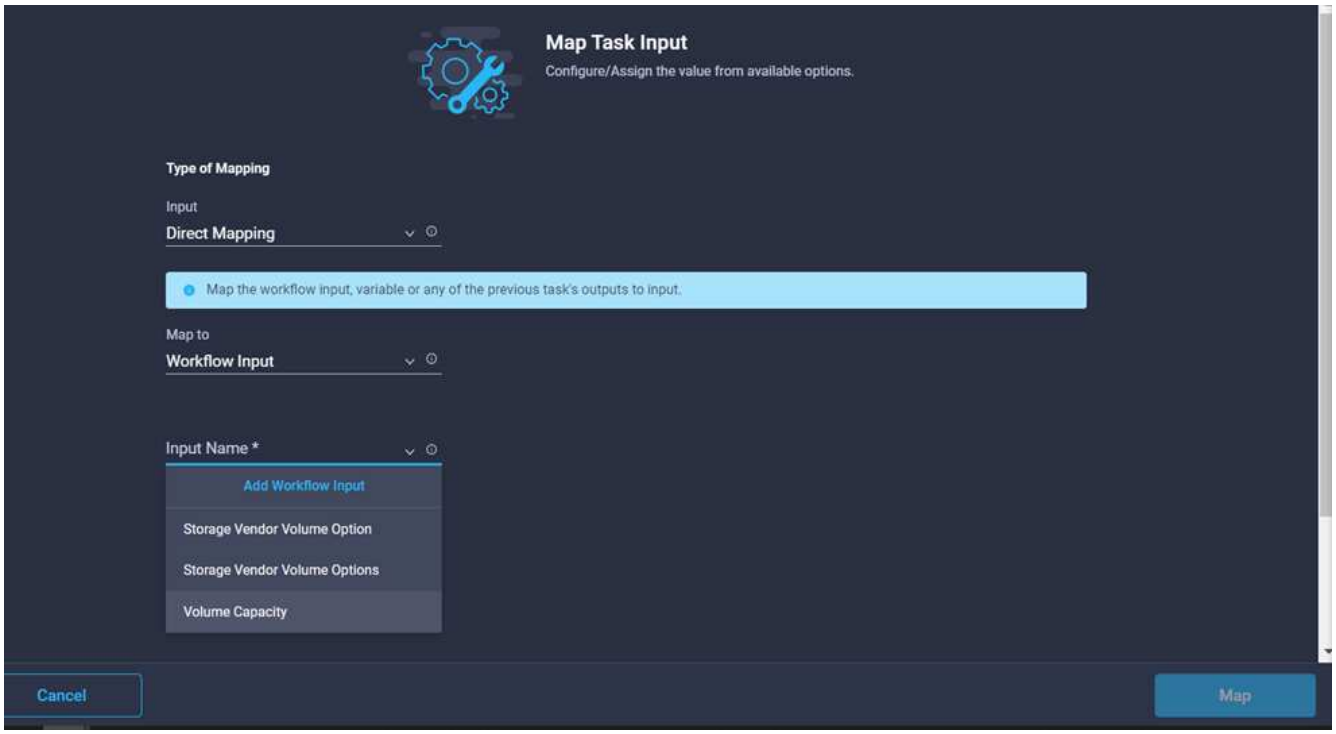
5. 在*任务属性*区域中、单击*输入*。
6. 单击*虚拟机管理程序管理器*字段中的*映射*。
7. 选择*静态值*、然后单击*选择虚拟机管理程序管理器*。单击VMware vCenter目标。



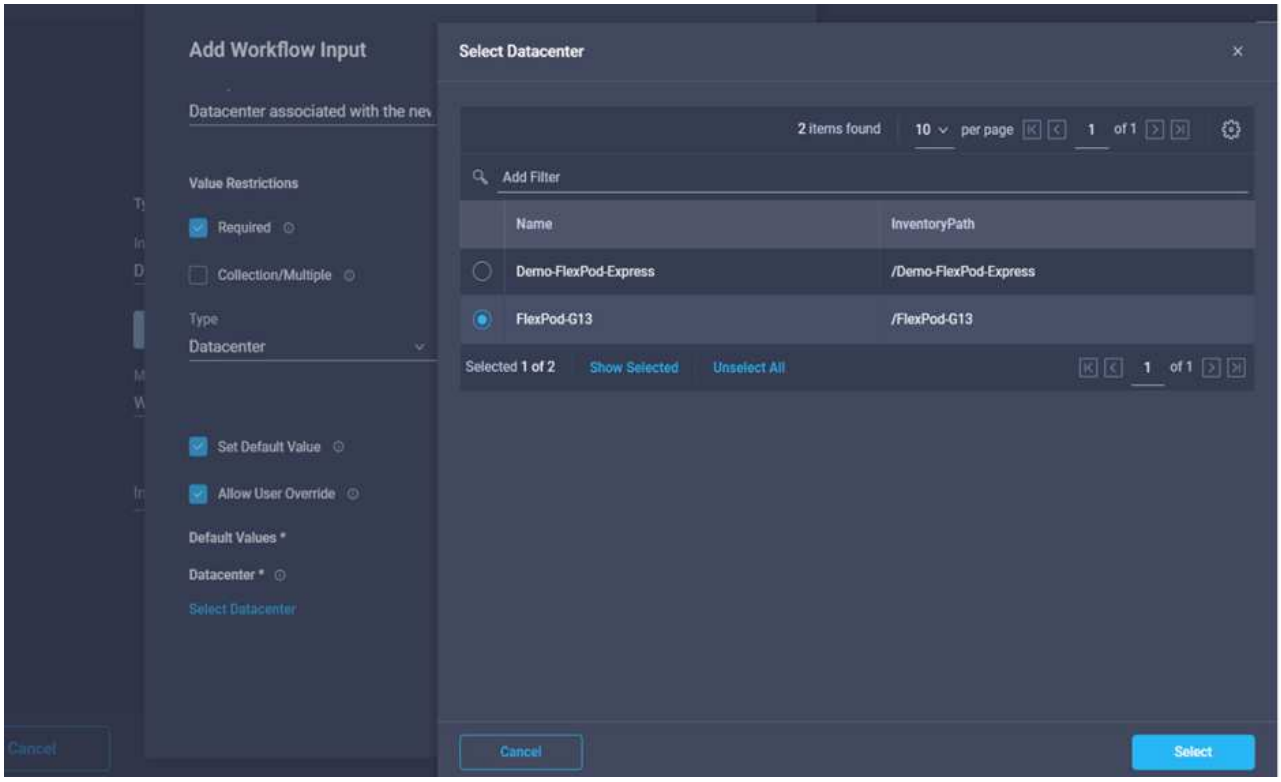
8. 单击*映射*。



9. 单击*数据中心*字段中的*映射*。这是与新数据存储库关联的数据中心。
10. 选择*直接映射*、然后单击*工作流输入*。
11. 单击*输入名称*、然后单击*创建工作流输入*。

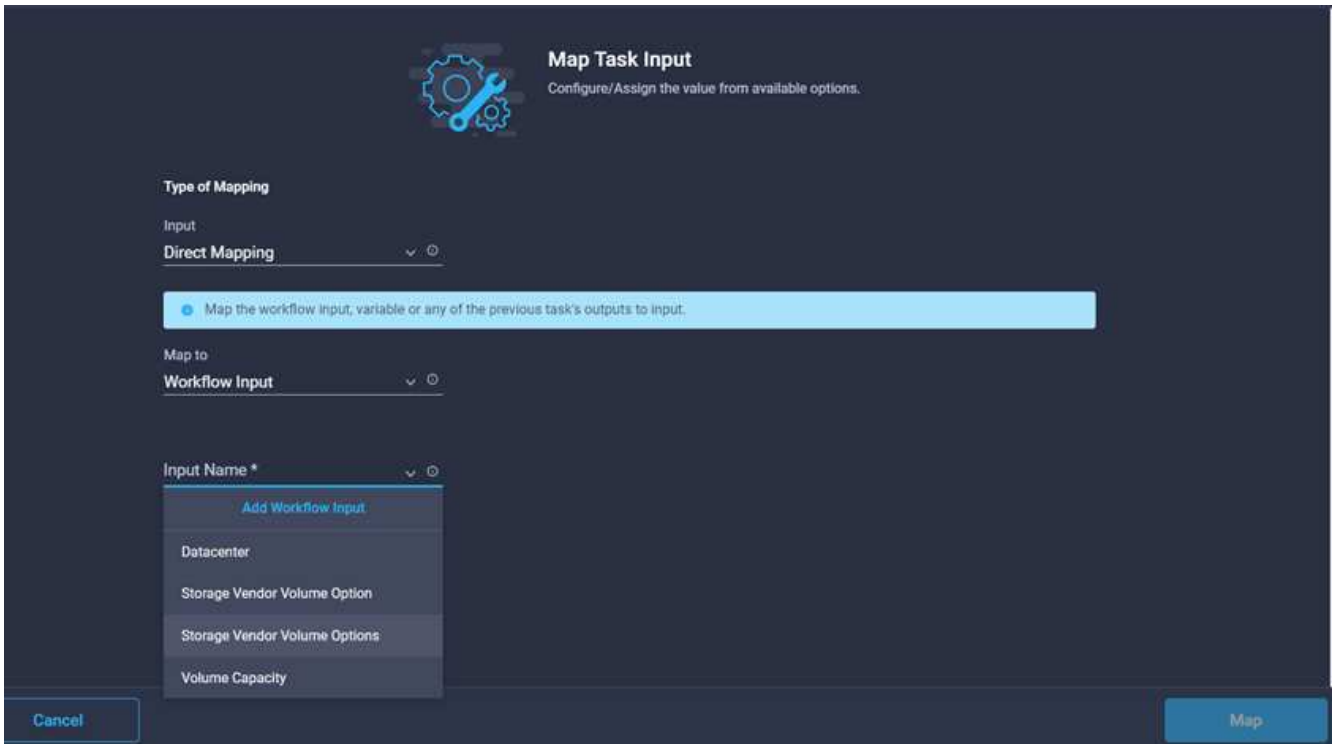


12. 在添加输入向导中、完成以下步骤：
    a. 提供显示名称和参考名称(可选)。
    b. 选择*数据中心*作为类型。
    c. 单击*设置默认值并覆盖*。
    d. 单击*选择数据中心*。
    e. 单击与新数据存储库关联的数据中心、然后单击*选择*。

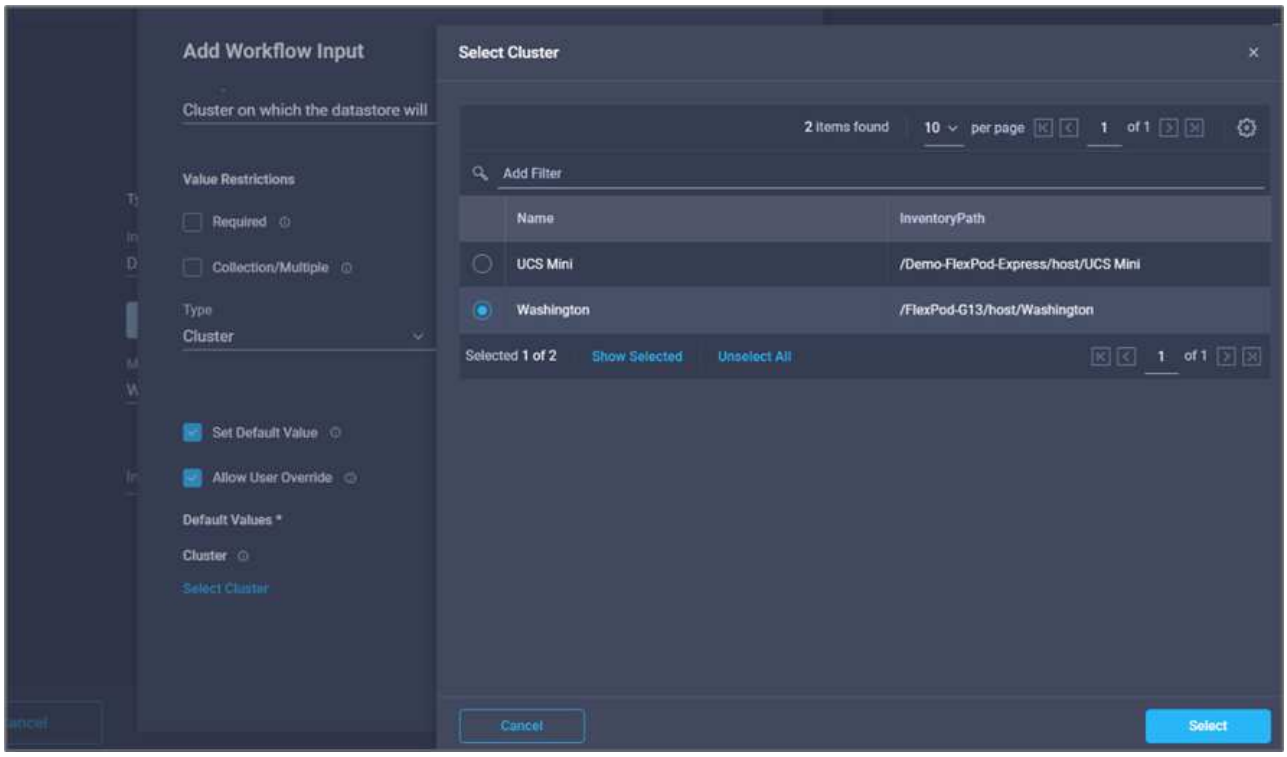


- 单击 * 添加 * 。

13. 单击*映射*。
14. 单击*集群*字段中的*映射*。
15. 选择*直接映射*、然后单击*工作流输入*。

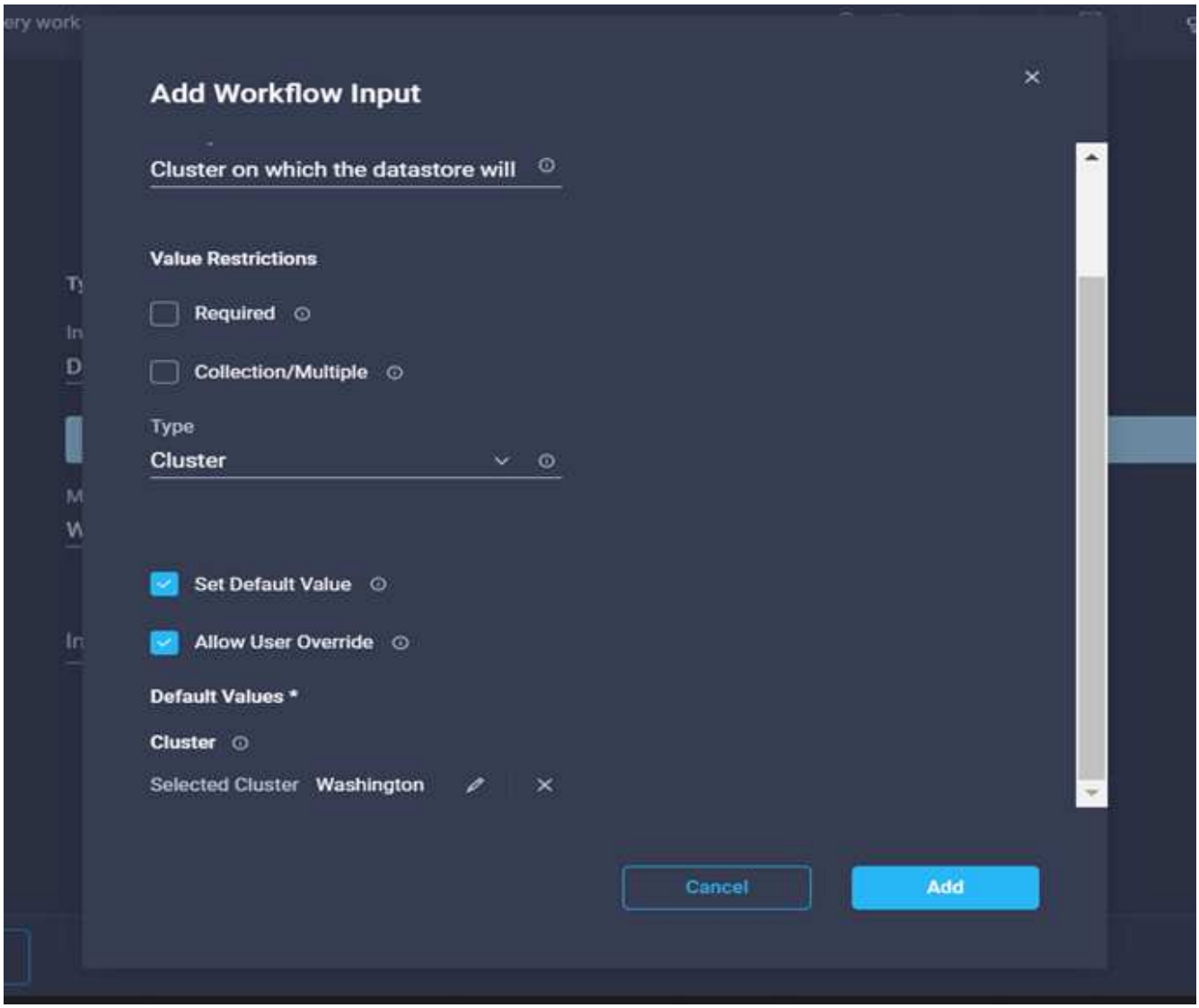


16. 在添加输入向导中、完成以下步骤：
    a. 提供显示名称和参考名称(可选)。
    b. 单击*必需*。
    c. 选择Cluster作为类型。
    d. 单击*设置默认值并覆盖*。
    e. 单击*选择集群*。
    f. 单击与新数据存储库关联的集群。
    g. 单击 * 选择 * 。

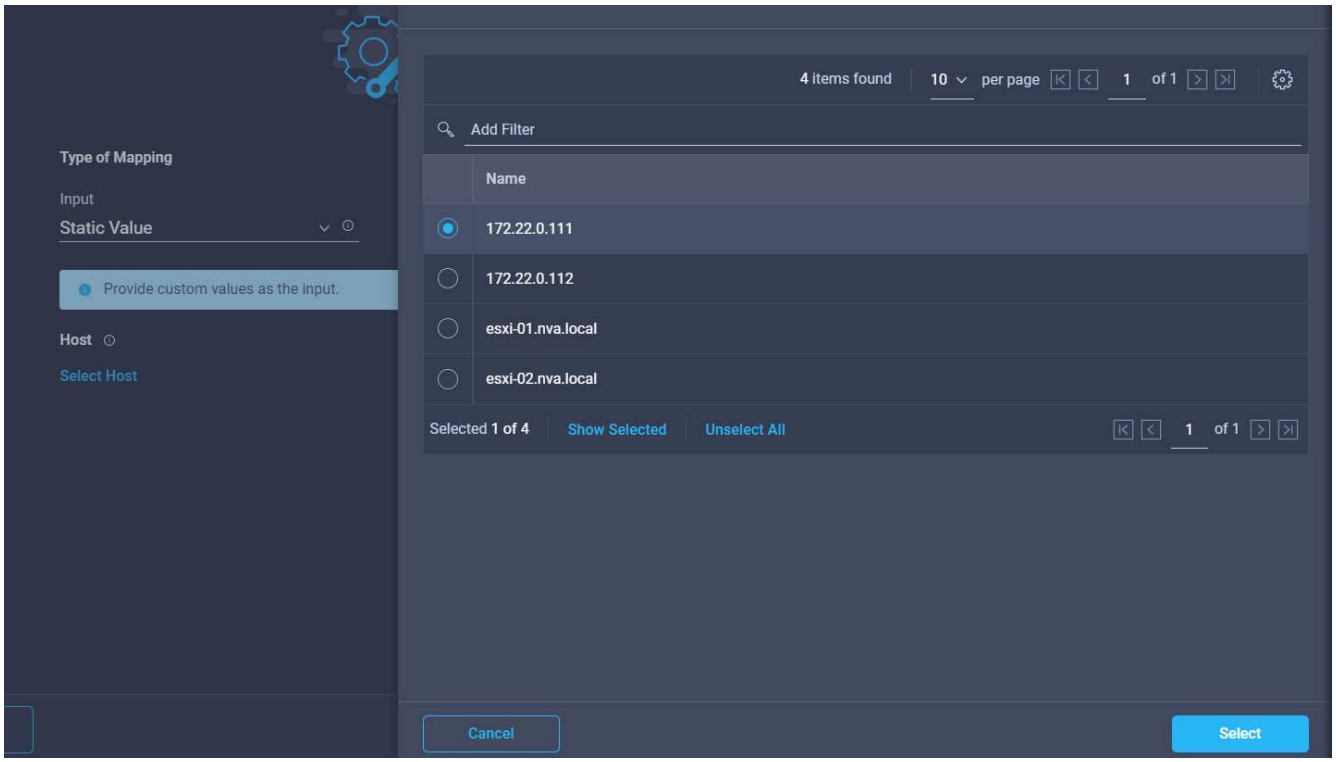


h. 单击 * 添加 * 。

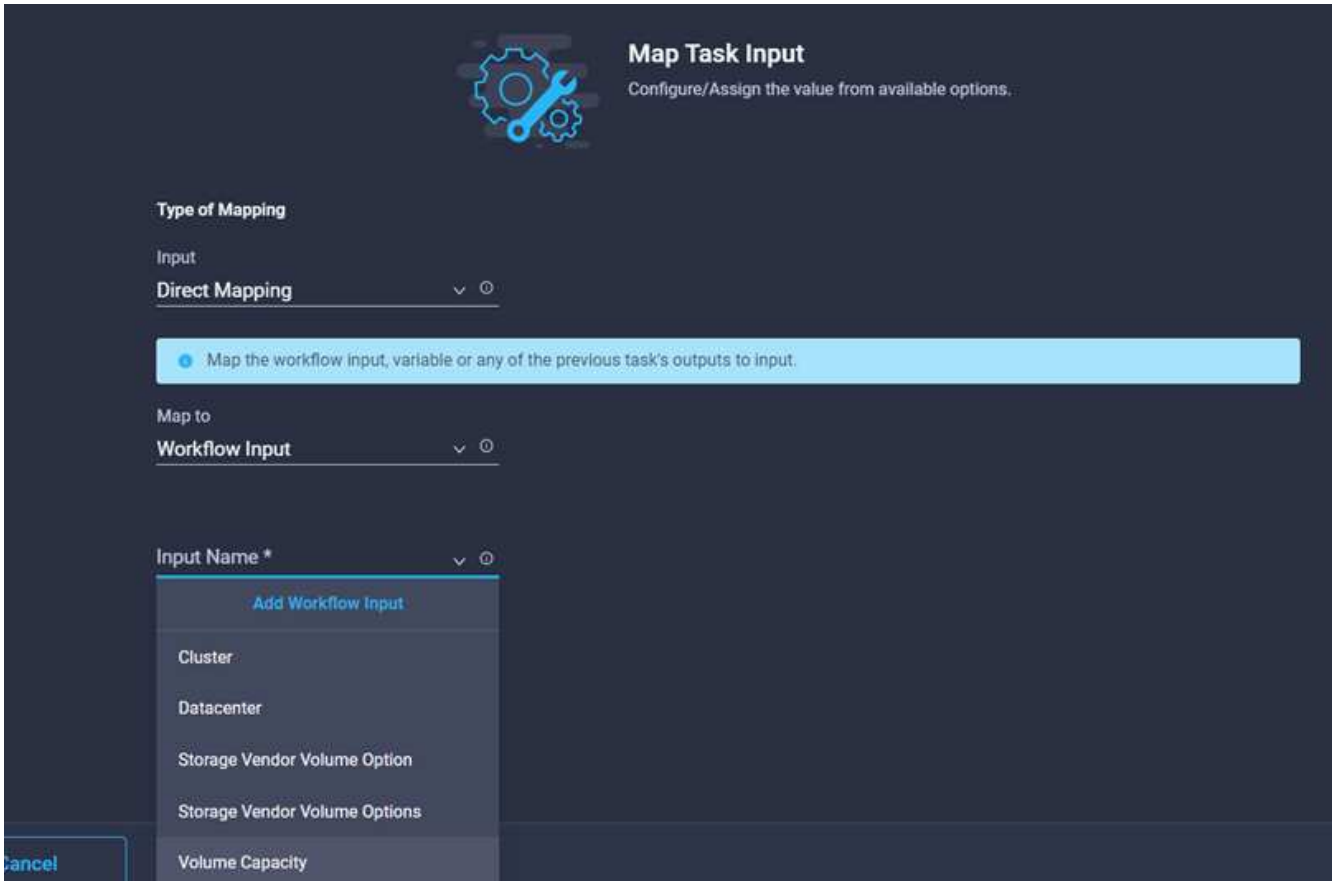
17. 单击*映射*。
18. 单击*主机*字段中的*映射*。



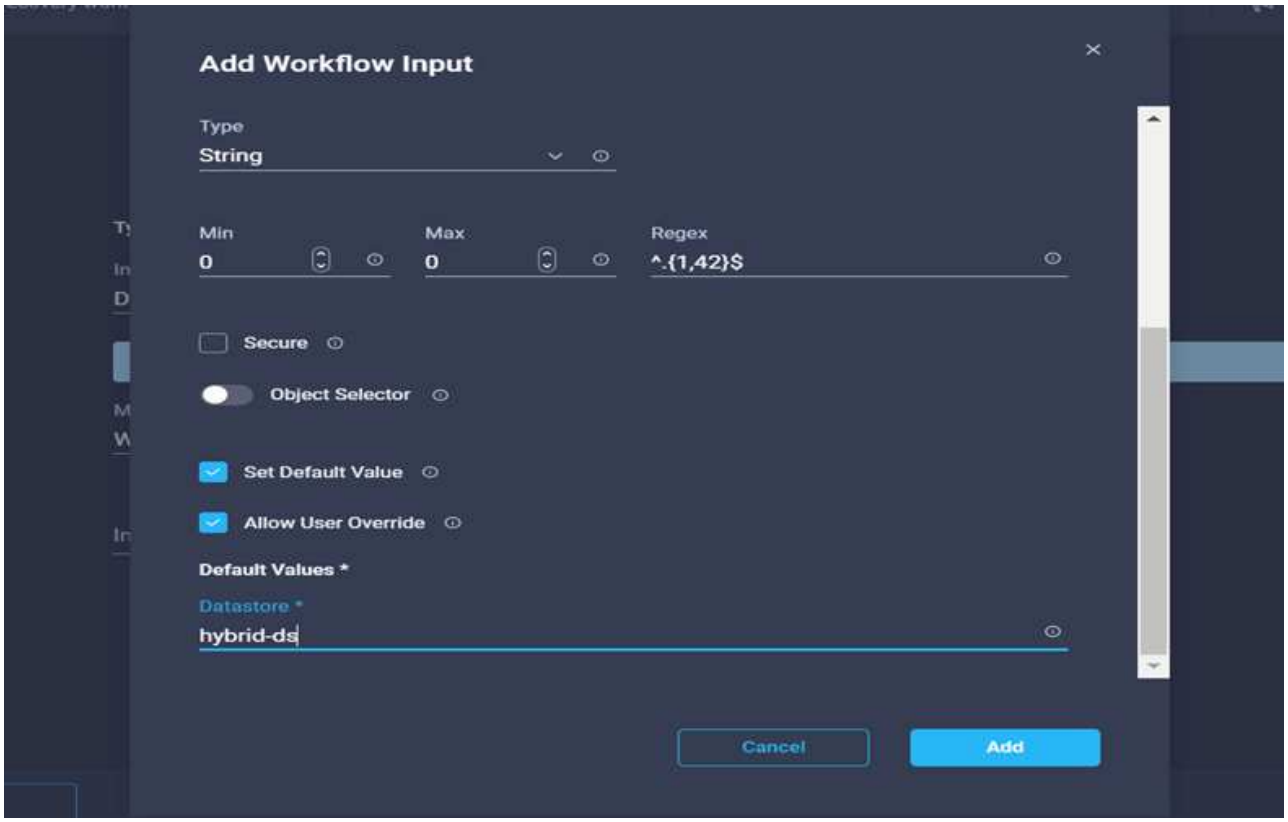
19. 选择*静态值*、然后单击要托管数据存储库的主机。如果指定了集群、则会忽略主机。



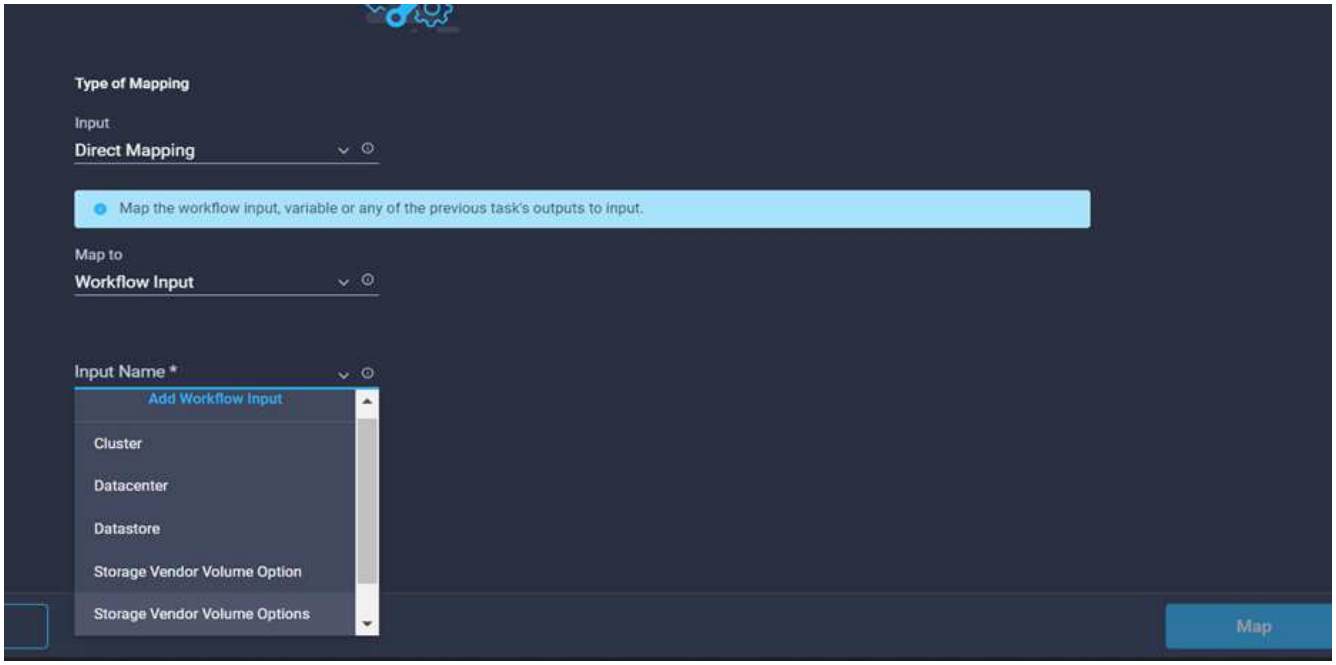
20. 单击*选择并映射*。
21. 单击*数据存储库*字段中的*映射*。
22. 选择*直接映射*、然后单击*工作流输入*。
23. 单击*输入名称*和*创建工作流输入*。



24. 在添加输入向导中：
    a. 提供显示名称和参考名称(可选)。
    b. 单击*必需*。
    c. 单击*设置默认值并覆盖*。
    d. 为数据存储库提供默认值、然后单击*添加*。

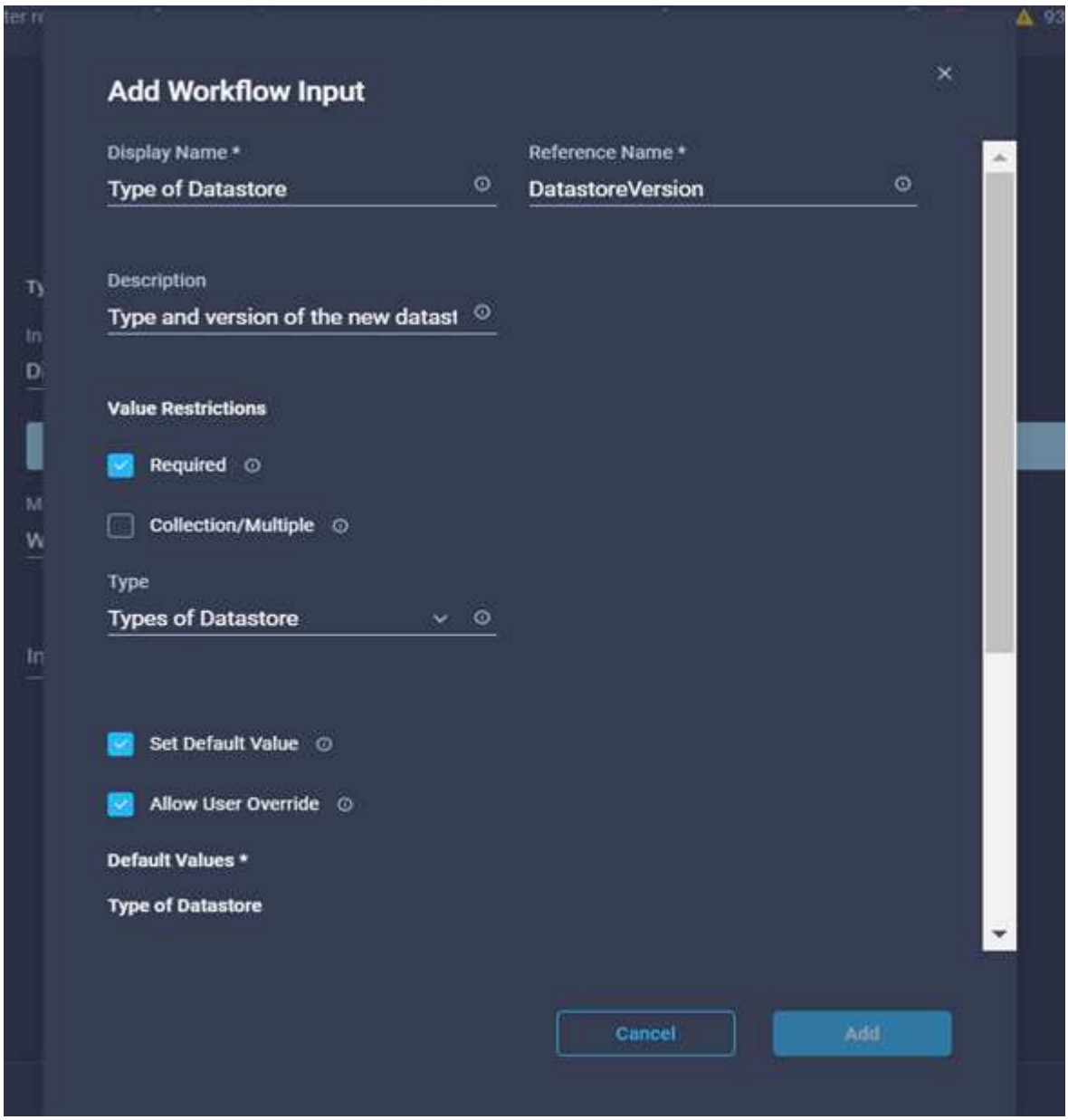


25. 单击*映射*。
26. 单击输入字段*数据存储库类型*中的*映射*。
27. 选择*直接映射*、然后单击*工作流输入*。
28. 单击*输入名称*和*创建工作流输入*。



29. 在添加输入向导中、完成以下步骤：
    a. 提供显示名称和参考名称(可选)、然后单击*必需*。

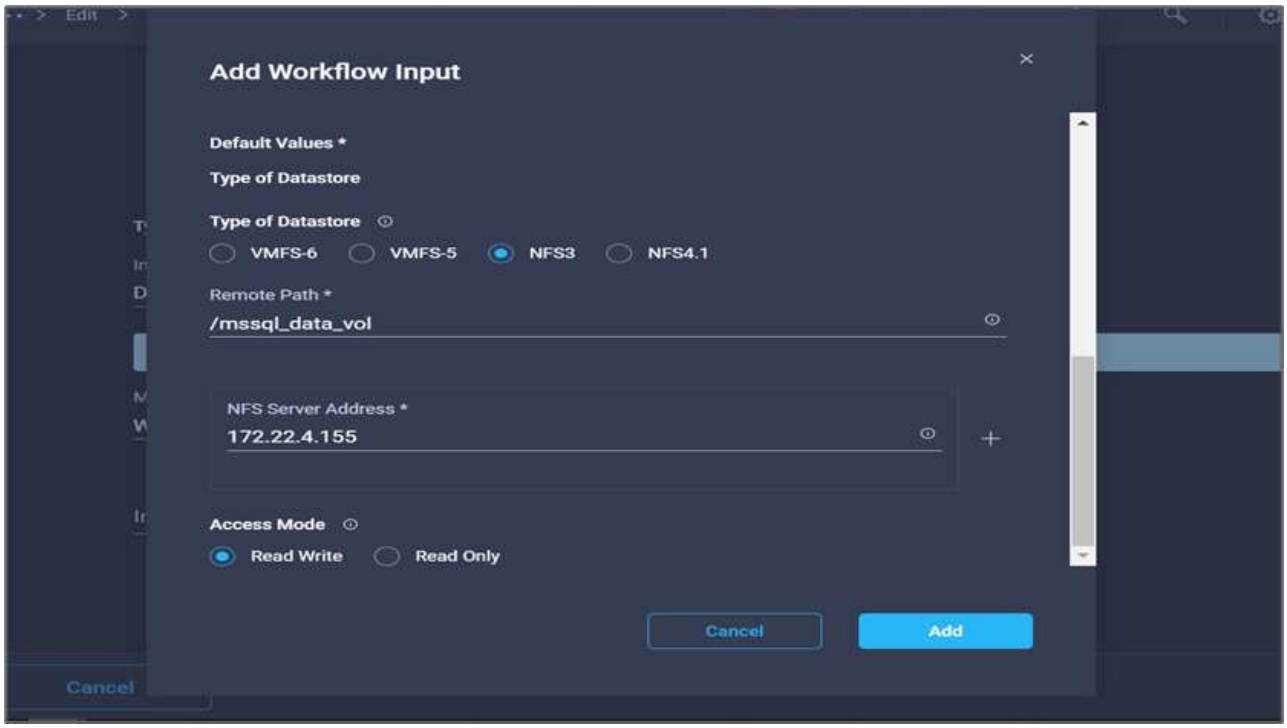
b. 确保选择类型*数据存储库类型*、然后单击*设置默认值和覆盖*。



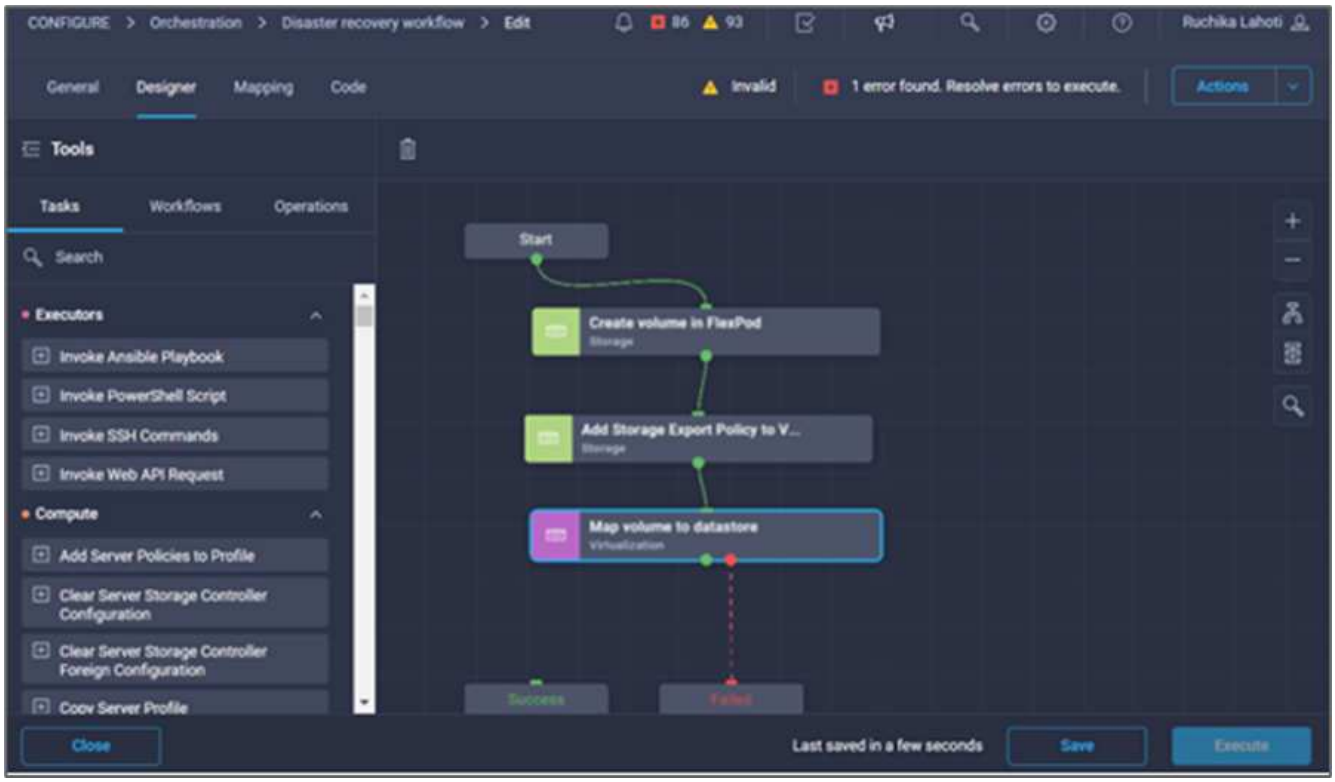
c. 提供远程路径。这是NFS挂载点的远程路径。

d. 在NFS服务器地址中提供远程NFS服务器的主机名或IP地址。

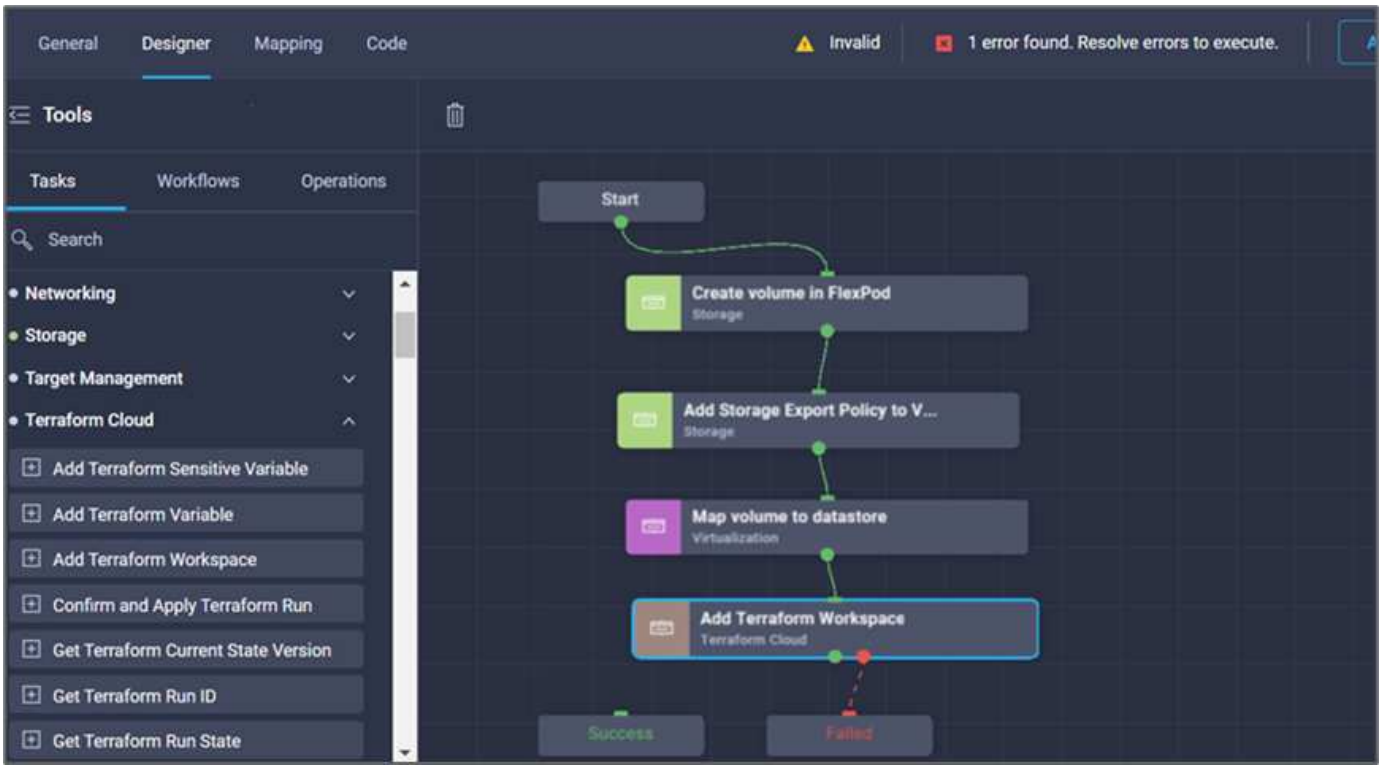
e. 单击*访问模式*。访问模式适用于NFS服务器。如果卷导出为只读、请单击只读。单击 * 添加 * 。



30. 单击*映射*。
31. 单击 * 保存 * 。

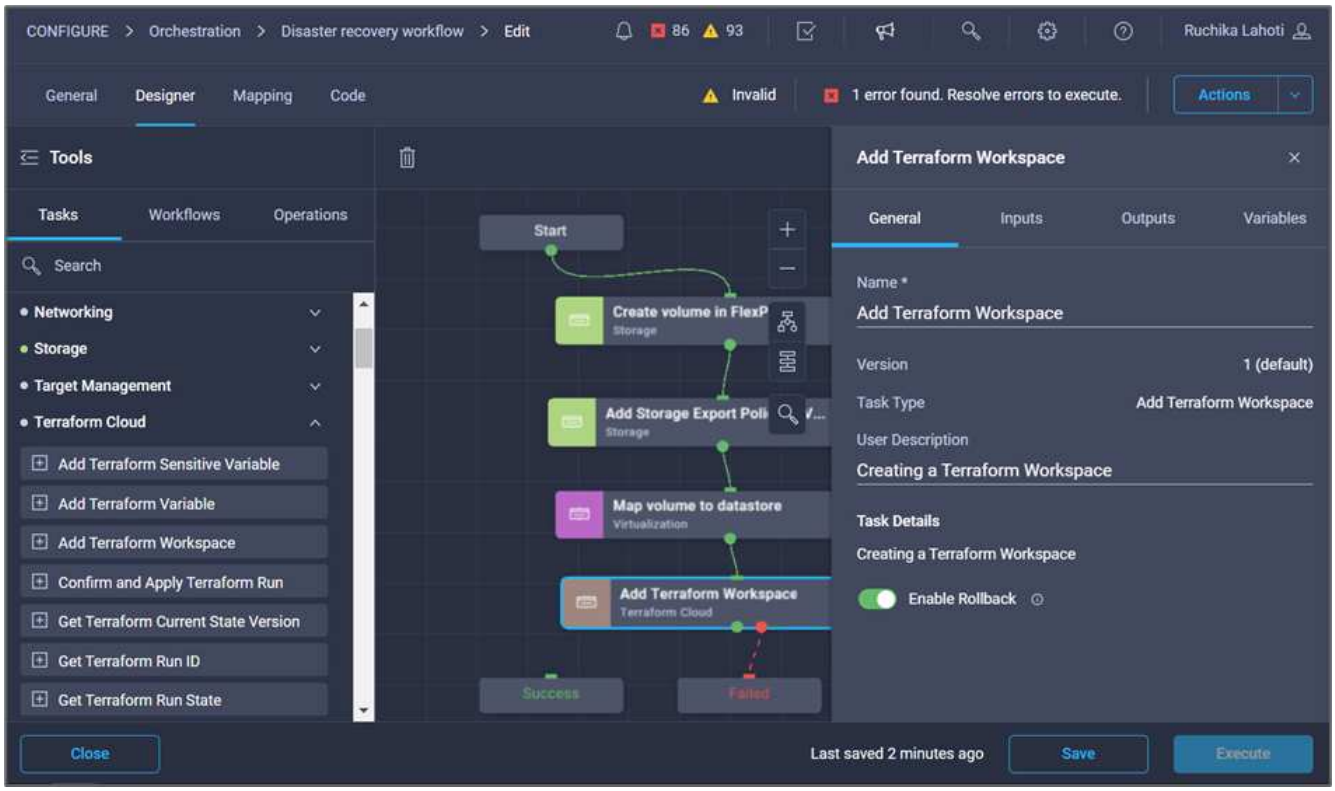


此操作将完成创建数据存储库的任务。在内部FlexPod 数据中心中执行的所有任务均已完成。

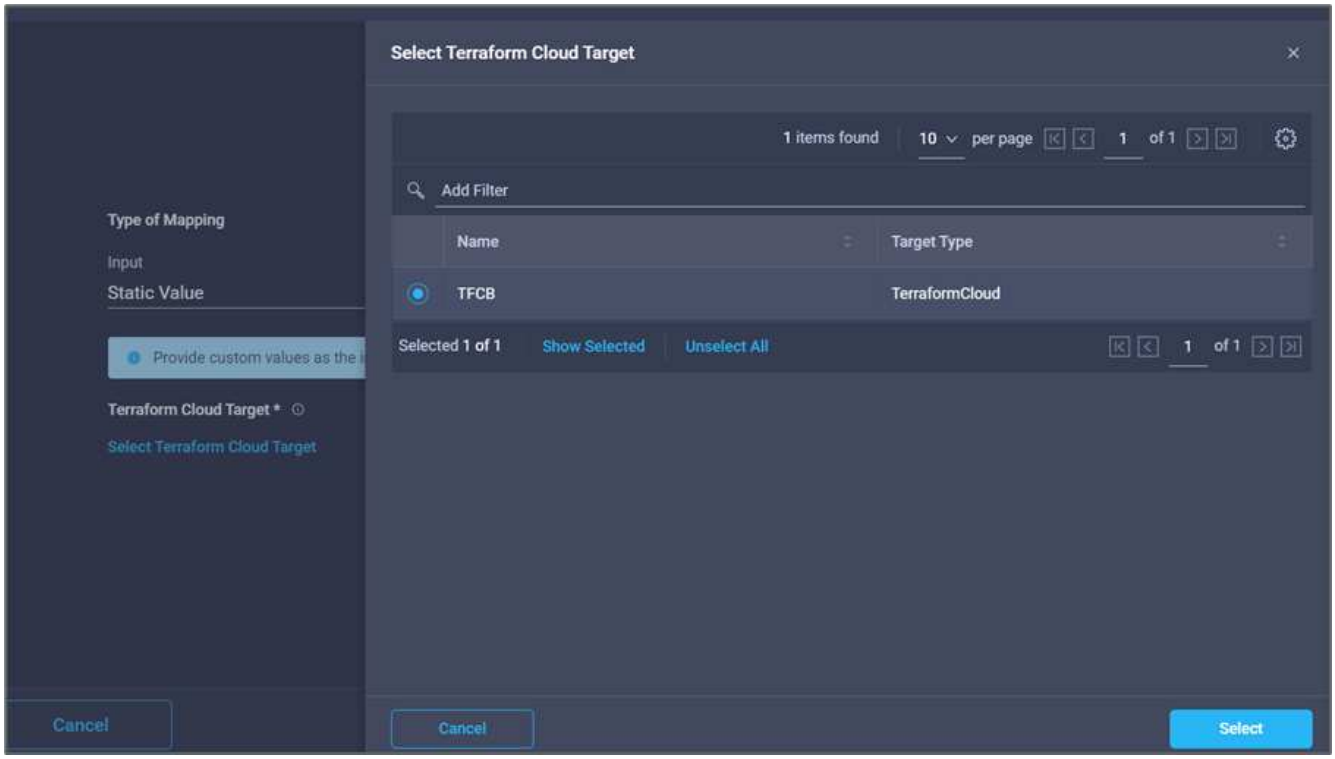


操作步骤 **5**：添加新的**Terraform**工作空间

1. 转到*设计器*选项卡、然后单击*工具*部分中的*任务*。
2. 从"设计"区域的"工具"部分拖放* Terraform Cloud >添加Terraform Workspace*任务。
3. 使用Connector将*映射卷连接到数据存储库*和*添加Terraform Workspace*任务、然后单击*保存*。
4. 单击*添加Terraform Workspace*。在任务属性区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。

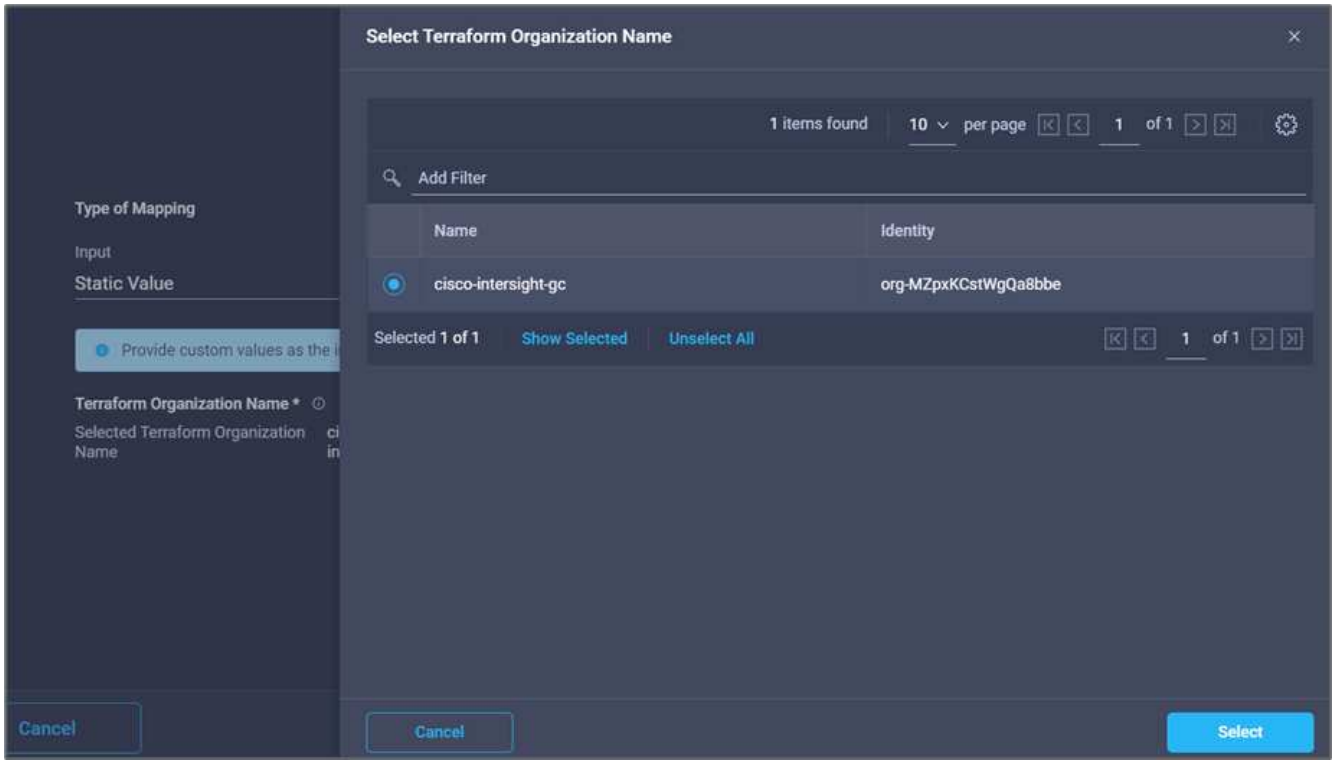


5. 在任务属性区域中、单击*输入*。
6. 单击输入字段* Terraform Cloud Target*中的*映射*。
7. 选择*静态值*、然后单击*选择Terraform Cloud Target*。选择按照中所述添加的Terraform Cloud for Business帐户 "为HashiCorp Terraform配置Cisco Intersight Service""。

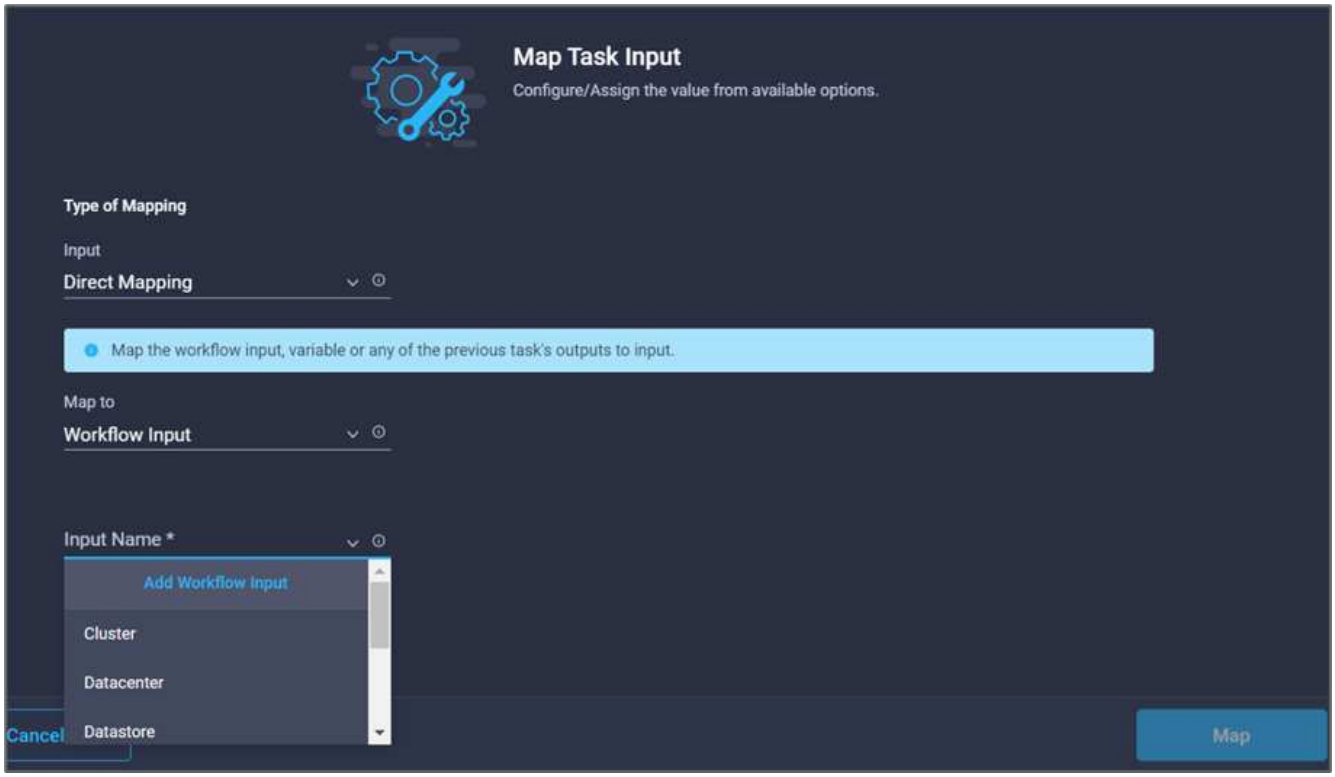


8. 单击*映射*。

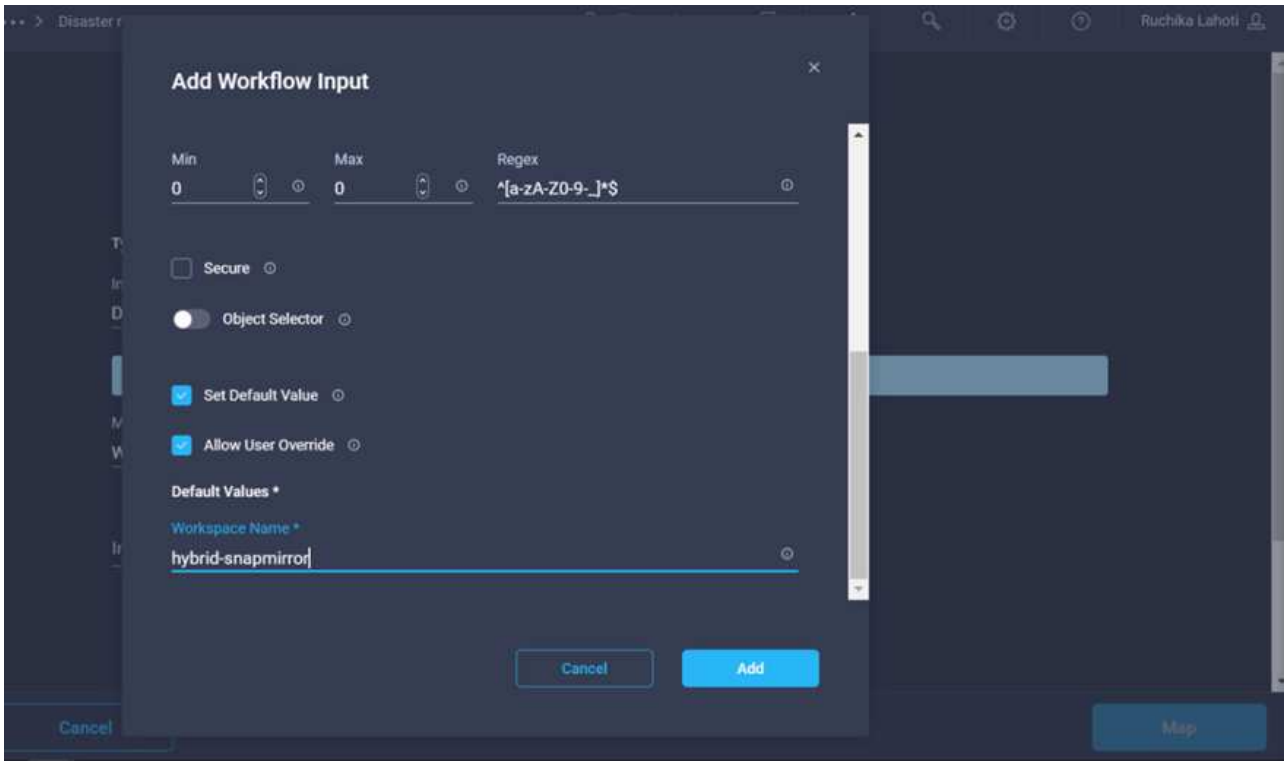
9. 单击输入字段* Terraform Organization Name*中的*映射*。
10. 选择*静态值*、然后单击*选择Terraform Organization*。在Terraform Cloud for Business帐户中选择您所属的Terraform组织的名称。



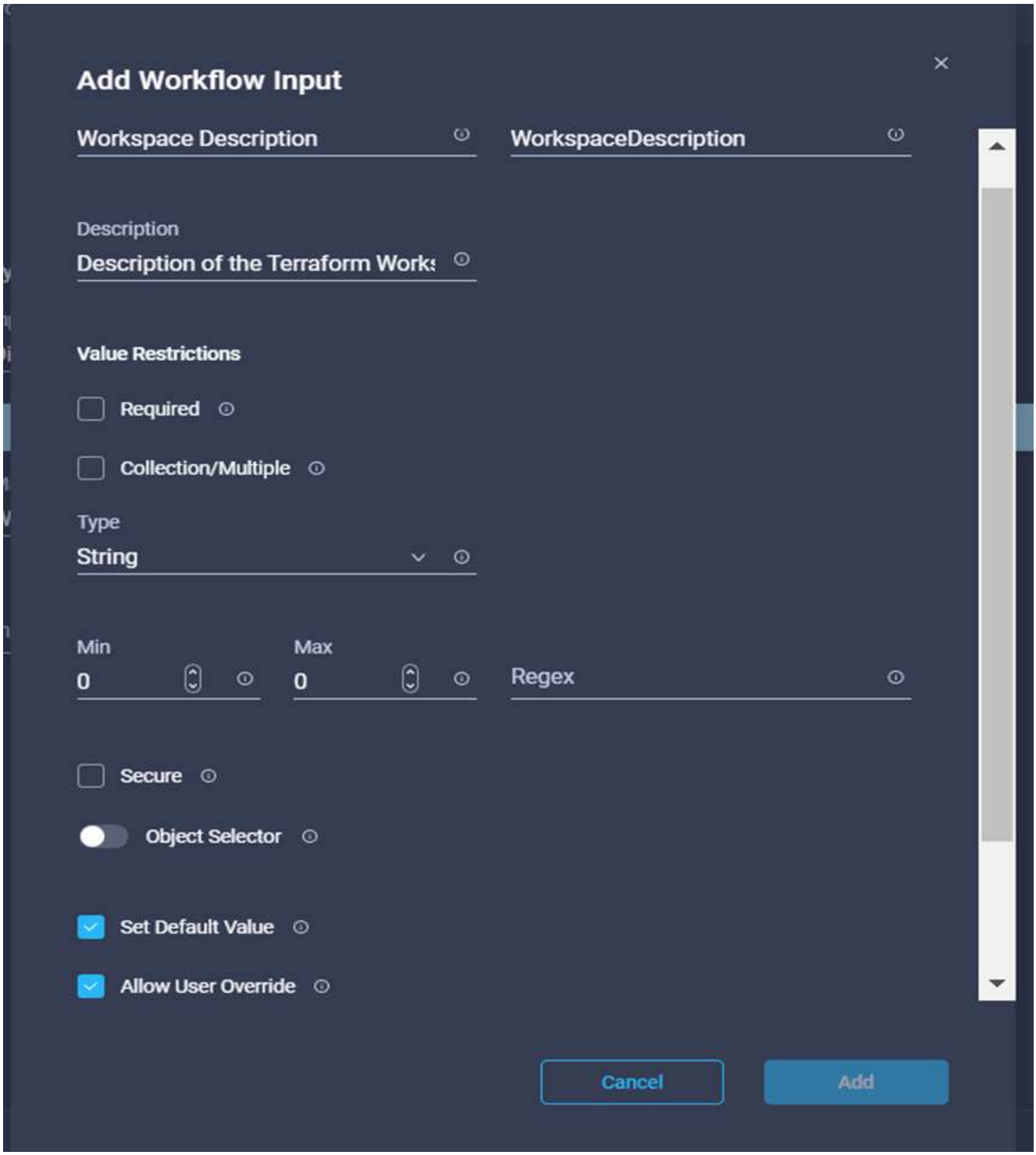
11. 单击*映射*。
12. 单击* Terraform Workspace Name*字段中的*映射*。这是Terraform Cloud for Business帐户中的新工作空间。
13. 选择*直接映射*、然后单击*工作流输入*。
14. 单击*输入名称*和*创建工作流输入*。



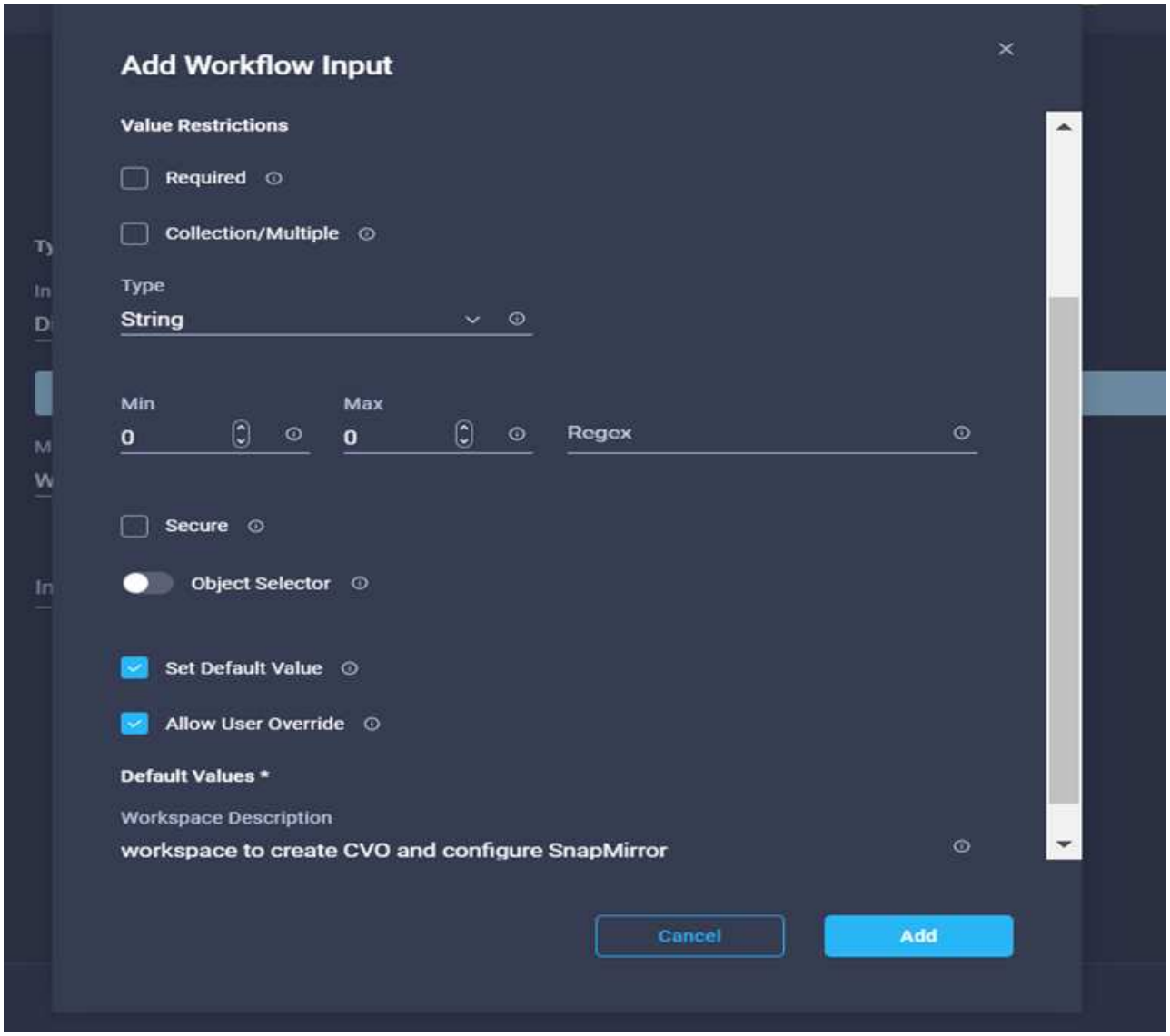
15. 在添加输入向导中、完成以下步骤：
    a. 提供显示名称和参考名称(可选)。
    b. 单击*必需*。
    c. 确保为*类型*选择*字符串*。
    d. 单击*设置默认值并覆盖*。
    e. 提供工作空间的默认名称。
    f. 单击 * 添加 * 。



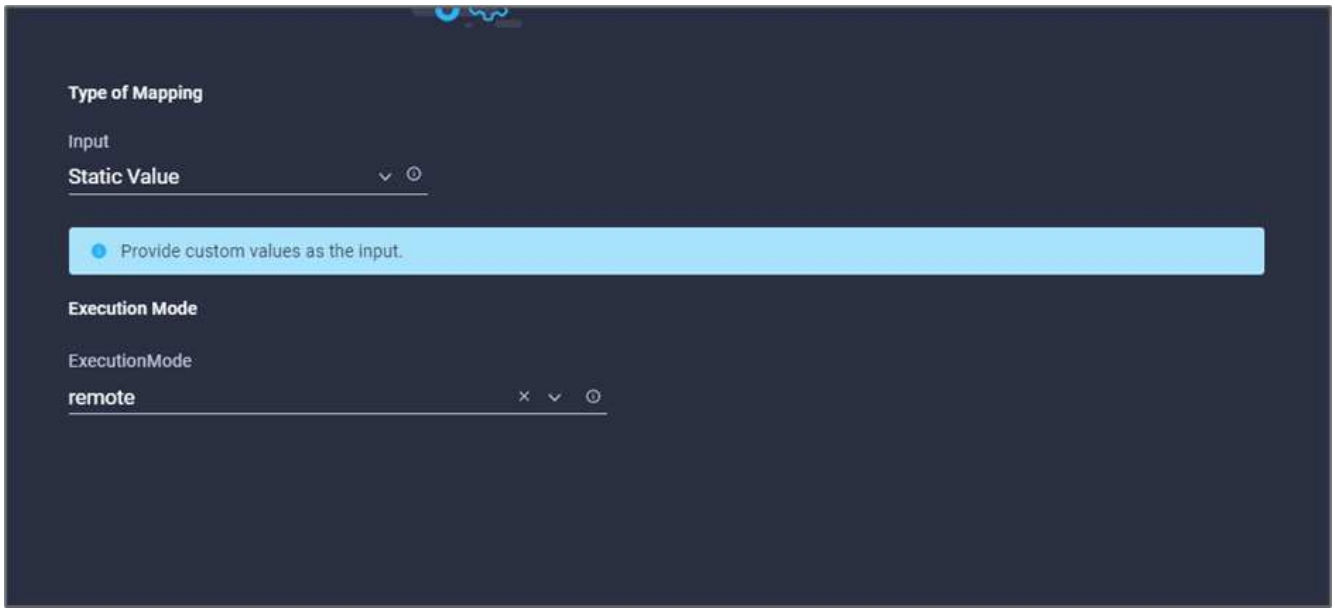
16. 单击*映射*。
17. 单击*工作空间问题描述 字段中的*映射。
18. 选择*直接映射*、然后单击*工作流输入*。
19. 单击*输入名称*和*创建工作流输入*。



20. 在添加输入向导中、完成以下步骤：
    a. 提供显示名称和参考名称(可选)。
    b. 确保为*类型*选择*字符串*。
    c. 单击*设置默认值并覆盖*。
    d. 提供工作空间问题描述 、然后单击*添加*。



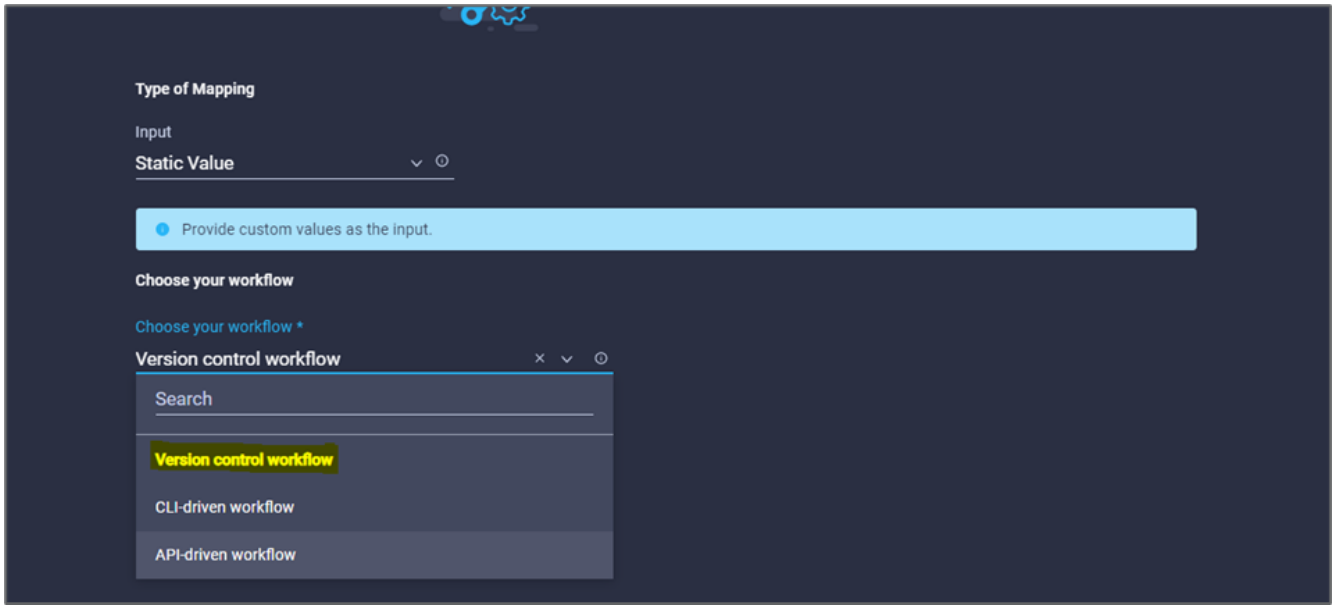
21. 单击*映射*。
22. 单击*执行模式*字段中的*映射*。
23. 选择*静态值*、单击*执行模式*、然后单击*远程*。



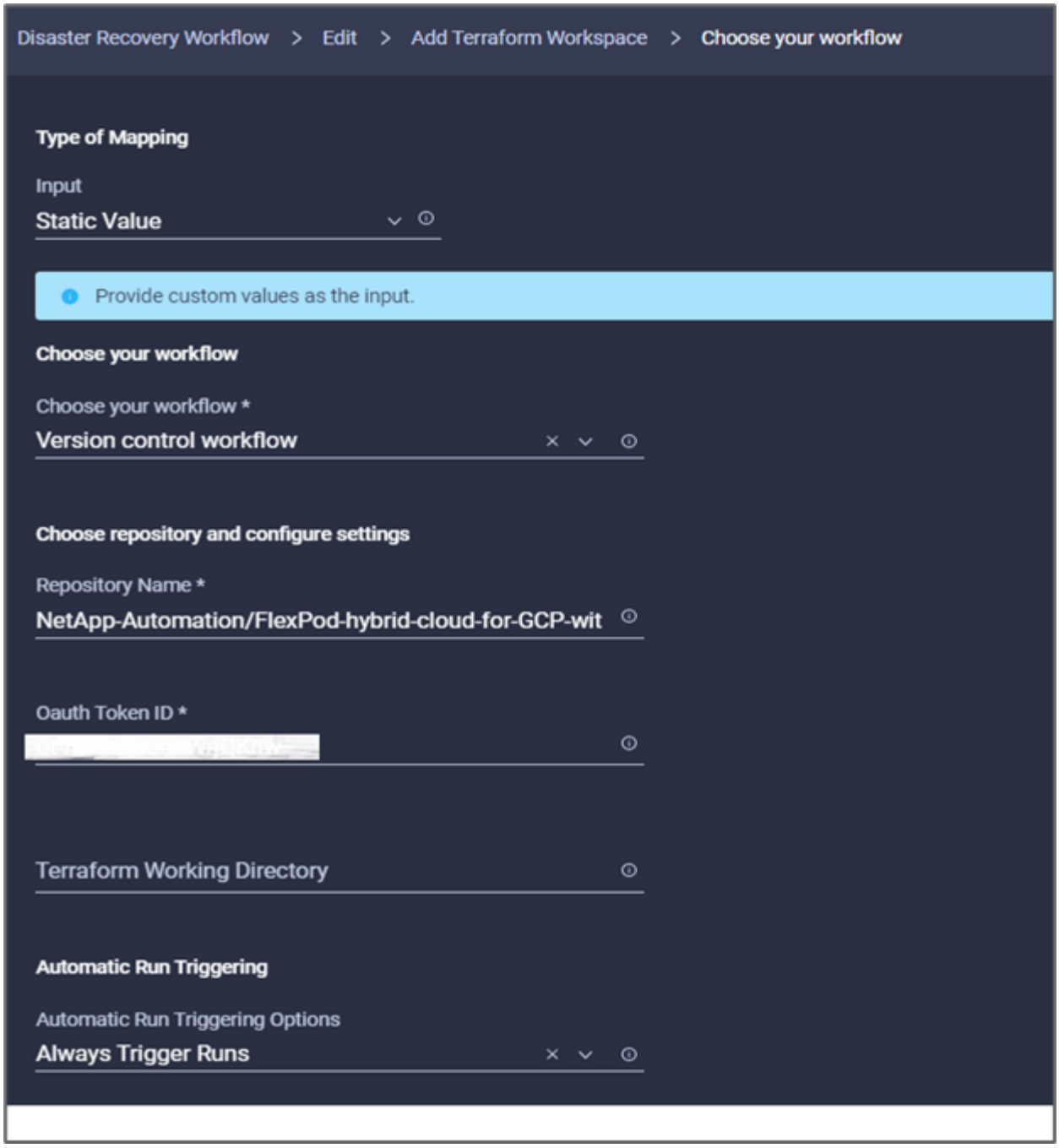
24. 单击*映射*。
25. 单击*应用方法*字段中的*映射*。
26. 选择*静态值*、然后单击*应用方法*。单击*手动应用*。

27. 单击*映射*。
28. 单击*用户界面*字段中的*映射*。
29. 选择*静态值*、然后单击*用户界面*。单击*控制台U*。

30. 单击*映射*。
31. 单击输入字段中的*映射*并选择您的工作流。
32. 选择*静态值*、然后单击*选择您的工作流*。单击*版本控制工作流*。



33. 提供以下GitHub存储库详细信息：
    a. 在*存储库名称*中、输入一节中详细介绍的存储库名称 ""设置环境前提条件""。
    b. 按照一节中的详细说明提供OAuth令牌ID ""设置环境前提条件""。
    c. 选择*自动运行触发*选项。

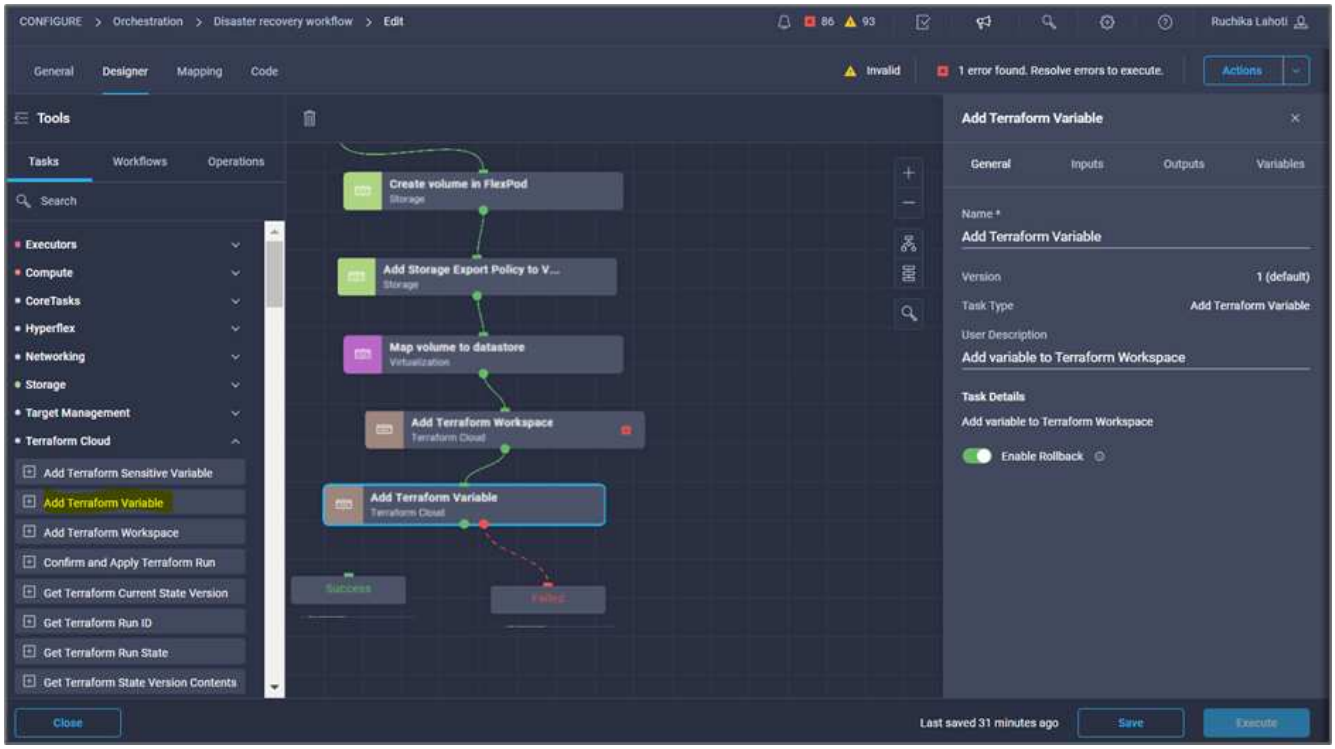


34. 单击*映射*。
35. 单击 * 保存 * 。

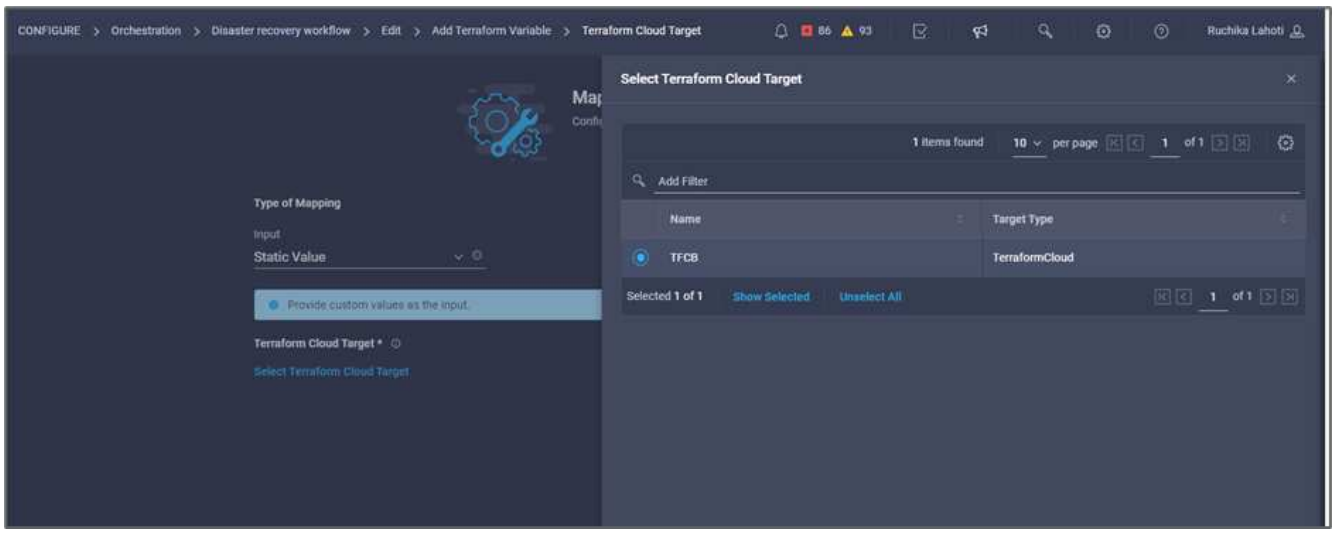
这将完成在Terraform Cloud for Business帐户中创建工作空间的任务。

操作步骤 **6**：向工作空间添加非敏感变量

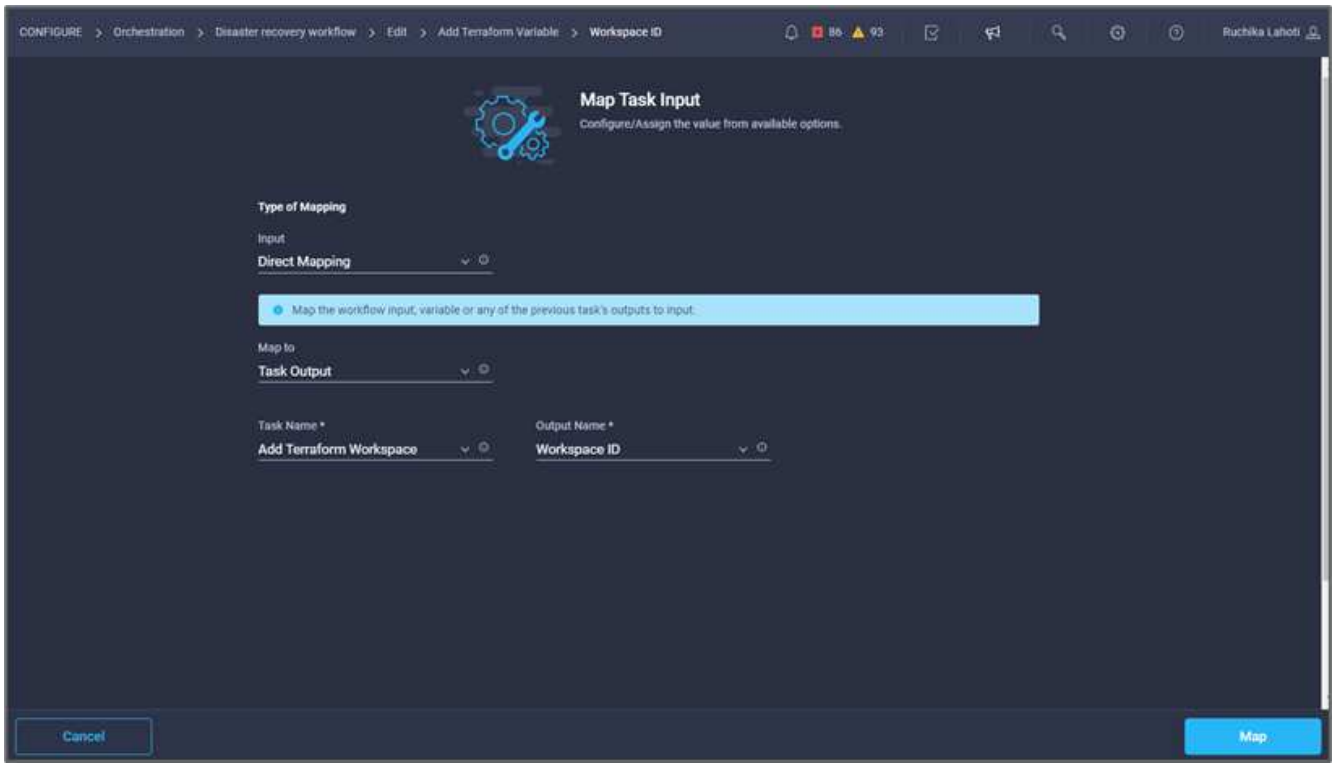
1. 转到*设计器*选项卡、然后单击*工具中的工作流*部分。
2. 从*设计*区域的*工具*部分拖放* Terraform >添加Terraform变量*工作流。
3. 使用Connector连接*添加Terraform Workspace*和*添加Terraform Variables*任务。单击 * 保存 * 。
4. 单击*添加Terraform变量*。在*工作流属性*区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。



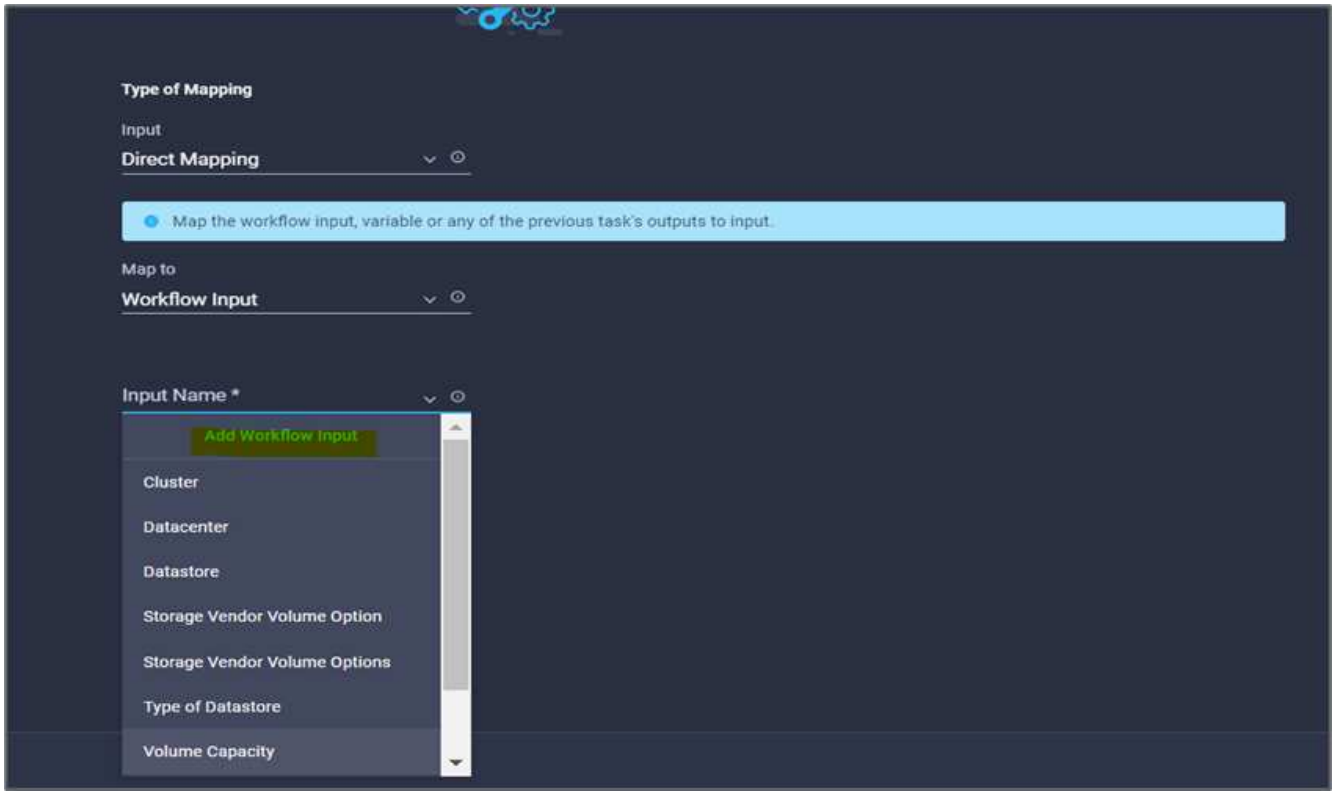
5. 在*工作流属性*区域中、单击*输入*。
6. 单击* Terraform Cloud Target*字段中的*映射*。
7. 选择*静态值*、然后单击*选择Terraform Cloud Target*。选择按照中所述添加的Terraform Cloud for Business帐户 "为HashiCorp Terraform配置Cisco Intersight Service""。



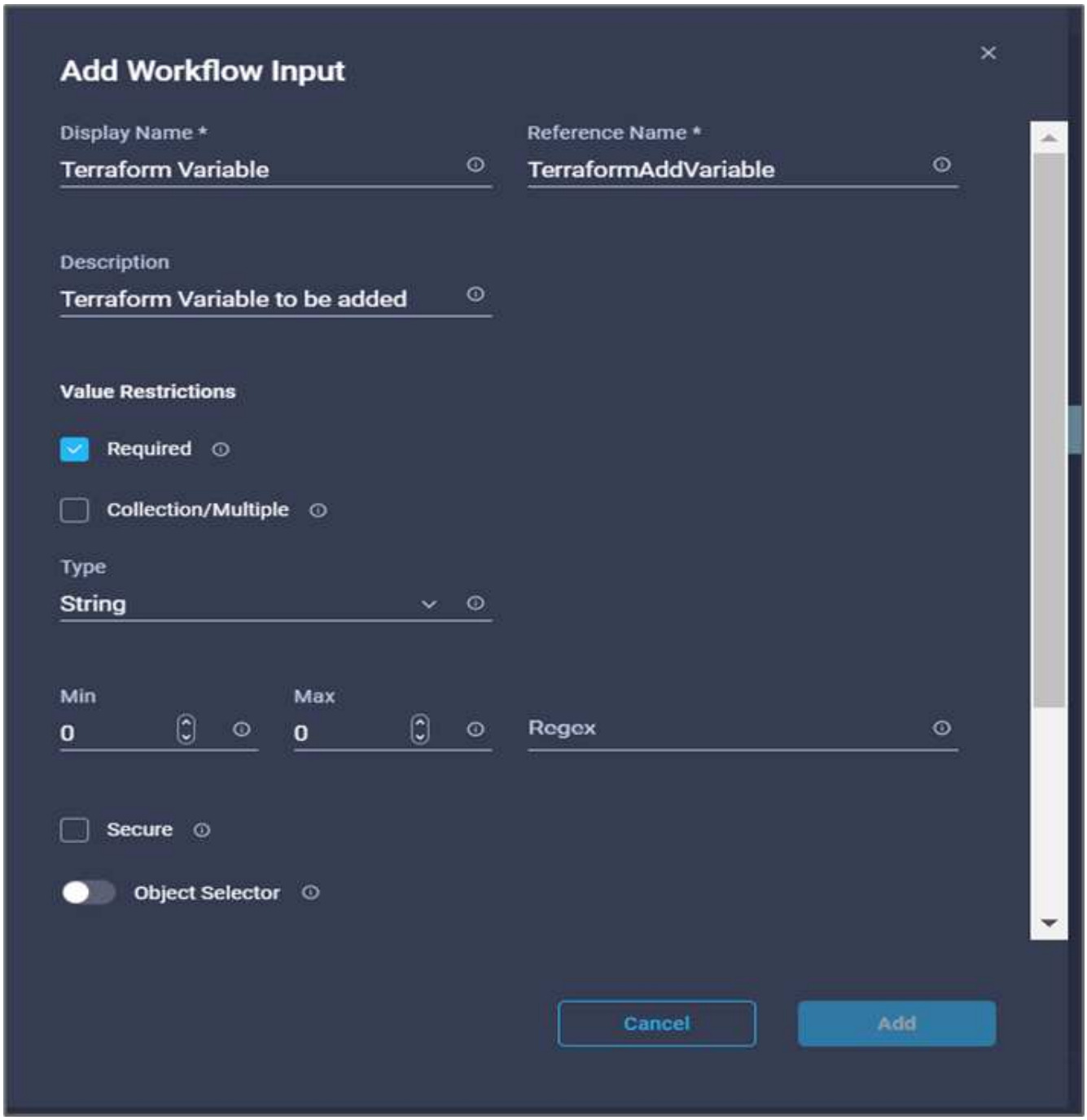
8. 单击*映射*。
9. 单击* Terraform Organization Name 字段中的*映射。
10. 选择*静态值*、然后单击*选择Terraform Organization*。在Terraform Cloud for Business帐户中选择您所属的Terraform组织的名称。



11. 单击*映射*。
12. 单击* Terraform Workspace Name*字段中的*映射*。
13. 选择*直接映射*、然后单击*任务输出*。
14. 单击*任务名称*、然后单击*添加Terraform Workspace*。



15. 单击*输出名称*、然后单击*工作空间名称*。
16. 单击*映射*。
17. 单击*添加变量选项*字段中的*映射*。
18. 选择*直接映射*、然后单击*工作流输入*。
19. 单击*输入名称*和*创建工作流输入*。

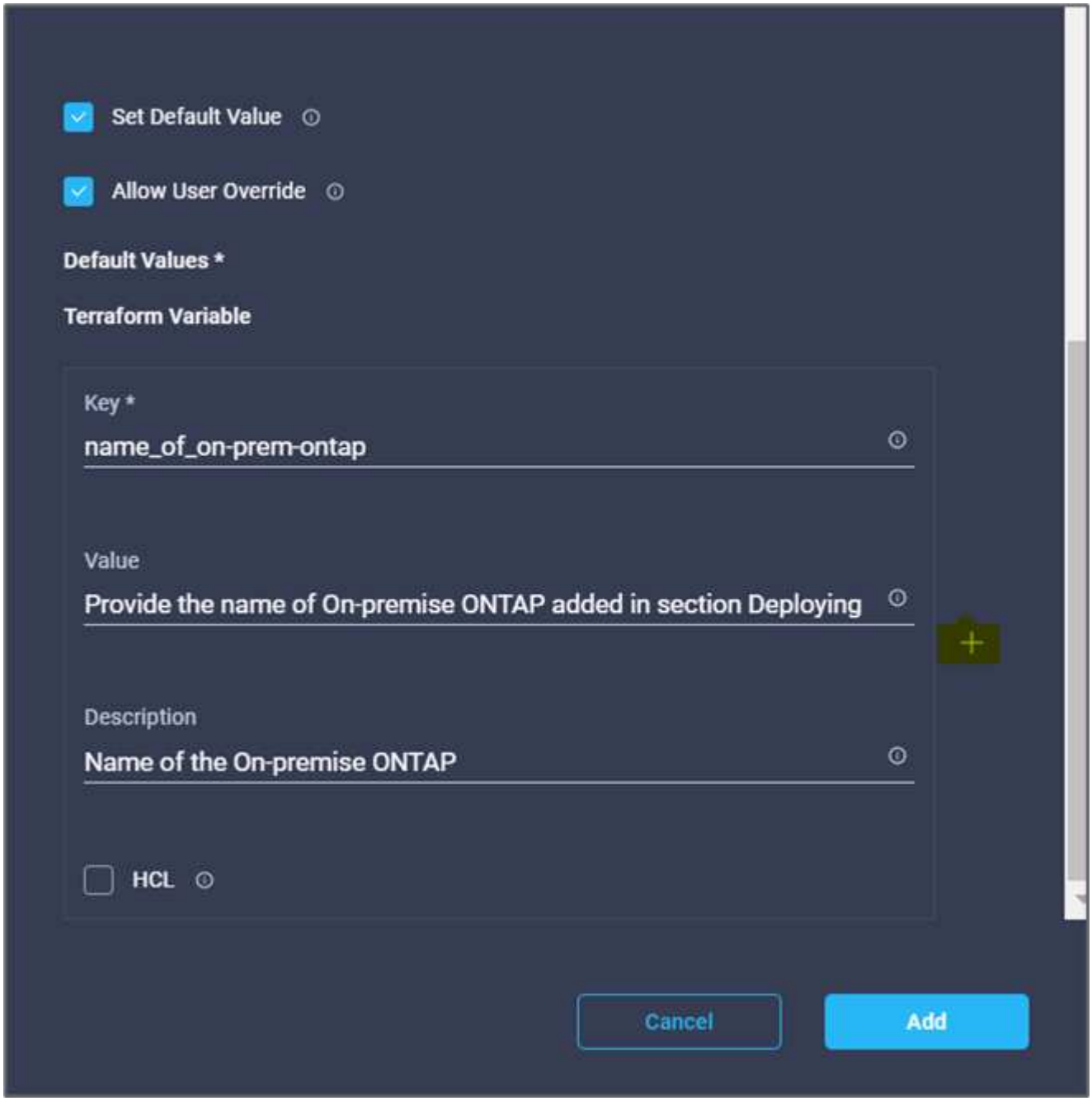


20. 在添加输入向导中、完成以下步骤：
    a. 提供显示名称和参考名称(可选)。
    b. 确保为*类型*选择*字符串*。

c. 单击*设置默认值并覆盖*。

d. 单击*变量类型*、然后单击*非敏感变量*。

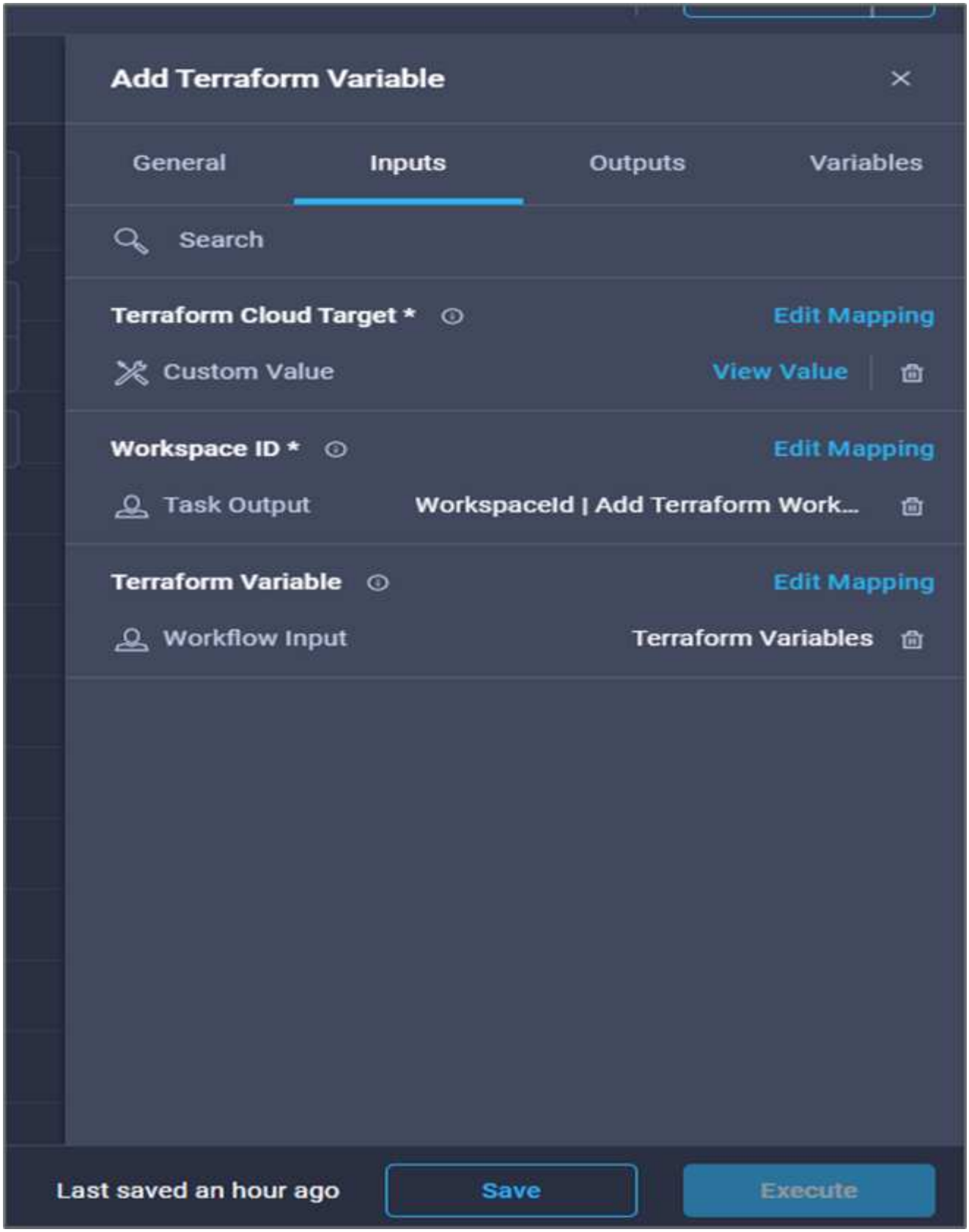
21. 在*添加Terraform变量*部分中、提供以下信息：
    - 密钥`name_of_on-prem-ontap`
    - *值。*请提供内部ONTAP 的名称。
    - 内部ONTAP 的*问题描述。*名称。
22. 单击*+*以添加其他变量。



23. 添加所有Terraform变量、如下表所示。您还可以提供默认值。

Terraform变量名称	Description
name__of_on-prem-ontap	内部ONTAP (FlexPod)的名称
on-prem-ontap_cluster_IP	存储集群管理接口的IP地址
on-prem-ontap_user_name	存储集群的管理员用户名
分区	要创建工作环境的GCP区域
子网ID	要创建工作环境的GCP子网ID
vpc_id	要创建工作环境的VPC ID
capacity_package_name	要使用的许可证类型
source_volume	源卷的名称
source_storage_vm_name	源SVM的名称
destination_volume	Cloud Volumes ONTAP 上的卷名称
schedule_of_replication	默认值为1小时
name_of_volume_to_create_on_CVO	云卷的名称
工作空间ID	要创建工作环境的workspace ID
项目ID	要创建工作环境的project_id
name_of_CVO_cluster	Cloud Volumes ONTAP 工作环境的名称
gcp_service_account	Cloud Volumes ONTAP 工作环境的gcp_service_account

24. 单击*映射*、然后单击*保存*。



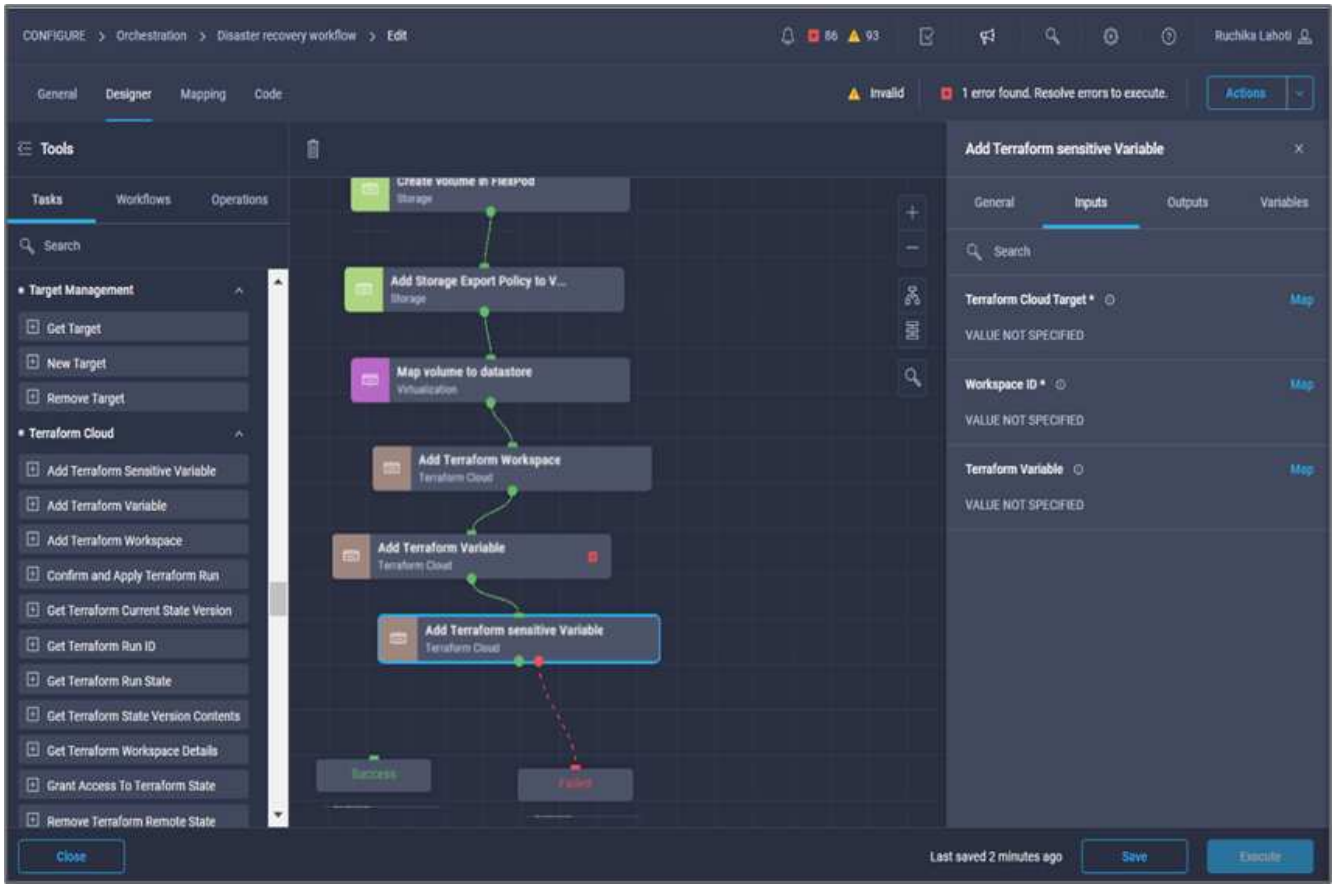
此时、将完成向工作空间添加所需Terraform变量的任务。接下来、将所需的敏感Terraform变量添加到工作空间中。您也可以将这两者合并到一个任务中。

操作步骤 **7**：向工作空间添加敏感变量

1. 转到*设计器*选项卡、然后从*工具*部分中单击*工作流*。
2. 从*设计*区域的*工具*部分拖放* Terraform >添加Terraform变量*工作流。
3. 使用Connector连接两个*添加Terraform Workspace*任务。单击 * 保存 * 。

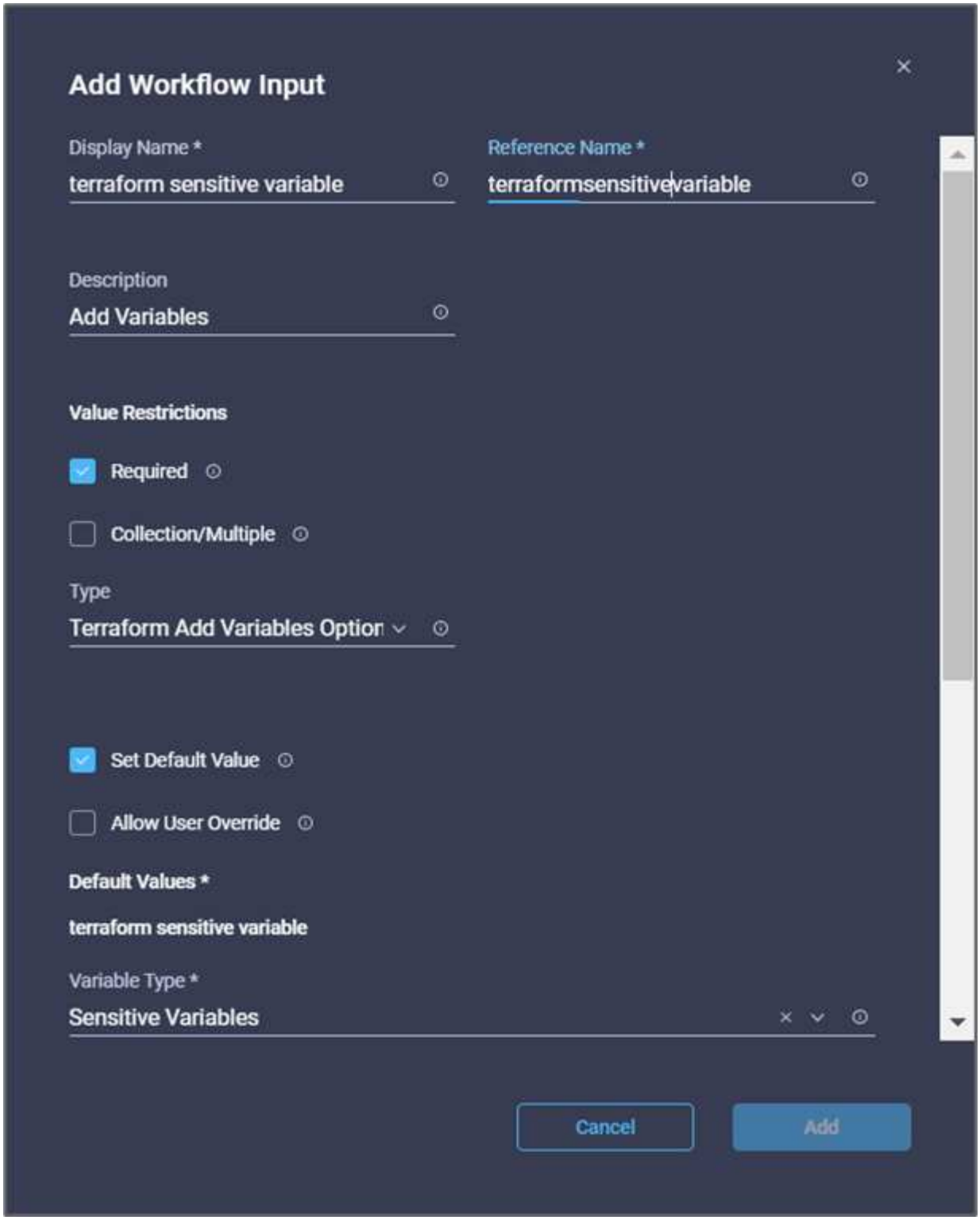
> 此时将显示一条警告、指示这两个任务的名称相同。现在忽略此错误、因为您将在下一步中更改任务名称。

4. 单击*添加Terraform变量*。在*工作流属性*区域中、单击*常规*选项卡。将名称更改为*添加Terraform敏感变量*。



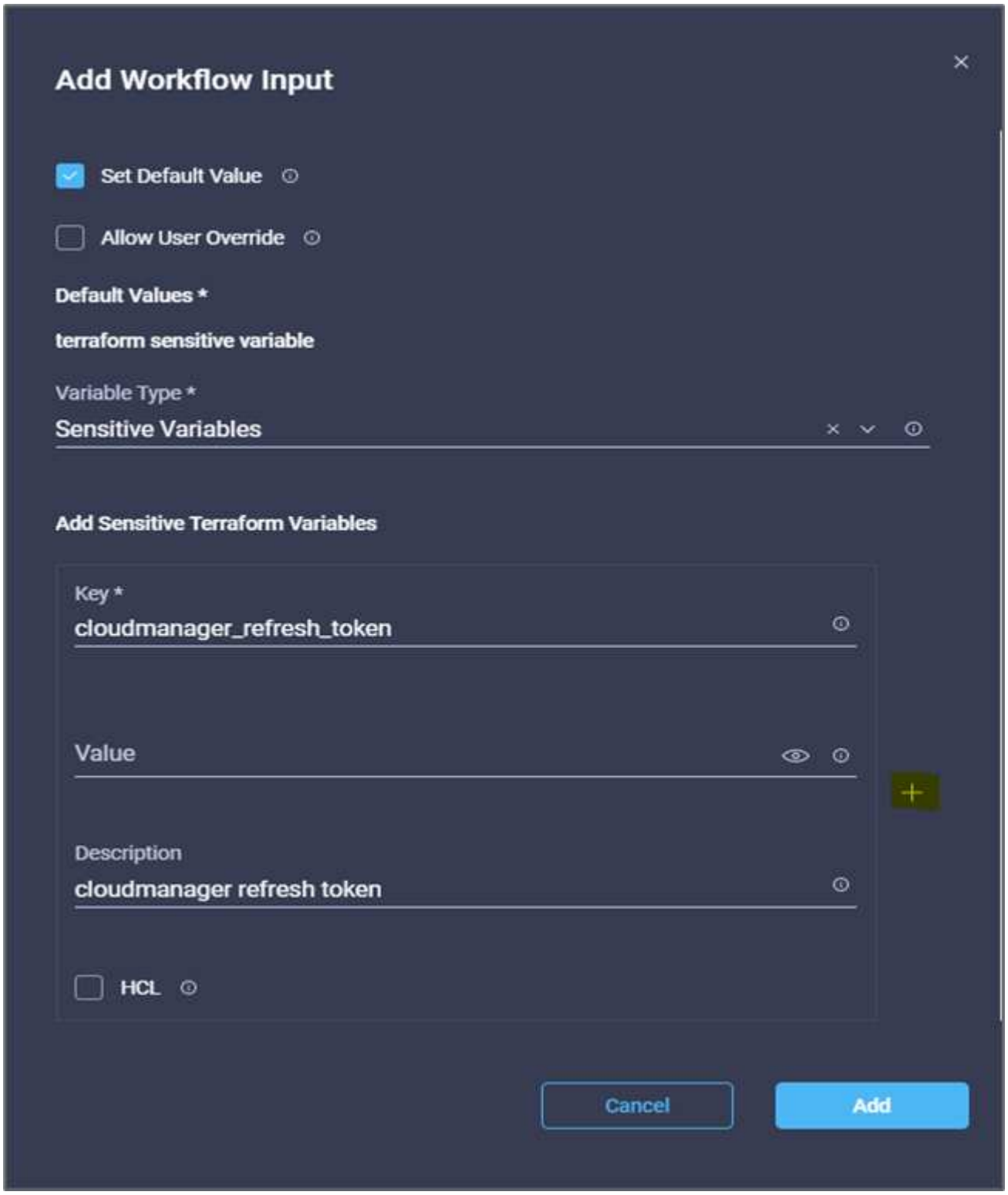
5. 在*工作流属性*区域中、单击*输入*。
6. 单击* Terraform Cloud Target*字段中的*映射*。
7. 选择*静态值*、然后单击*选择Terraform Cloud Target*。选择在部分中添加的Terraform Cloud for Business帐户 "为HashiCorp Terraform配置Cisco Intersight Service"。 "
8. 单击*映射*。
9. 单击* Terraform Organization Name*字段中的*映射*。
10. 选择*静态值*、然后单击*选择Terraform Organization*。在Terraform Cloud for Business帐户中选择您所属的Terraform组织的名称。
11. 单击*映射*。
12. 单击* Terraform Workspace Name*字段中的*映射*。

13. 选择*直接映射*、然后单击*任务输出*。
14. 单击*任务名称*、然后单击*添加Terraform Workspace*。
15. 单击*输出名称*、然后单击输出*工作空间名称*。
16. 单击*映射*。
17. 单击*添加变量选项*字段中的*映射*。
18. 选择*直接映射*、然后单击*工作流输入*。
19. 单击*输入名称*和*创建工作流输入*。
20. 在添加输入向导中、完成以下步骤：
    a. 提供显示名称和参考名称(可选)。
    b. 请务必为此类型选择* Terraform Add Variables Options*。
    c. 单击*设置默认值*。
    d. 单击*变量类型*、然后单击*敏感变量*。
    e. 单击 * 添加 * 。



21. 在*添加Terraform变量*部分中、提供以下信息：
    - 键。`cloudmanager_refresh_token`。
    - *值。*输入NetApp Cloud Manager API操作的刷新令牌。
    - *。问题描述。*刷新令牌。

有关为NetApp Cloud Manager API操作获取刷新令牌的详细信息、请参见一节 ""设置环境前提条件。""



22. 添加下表所示的所有Terraform敏感变量。您还可以提供默认值。

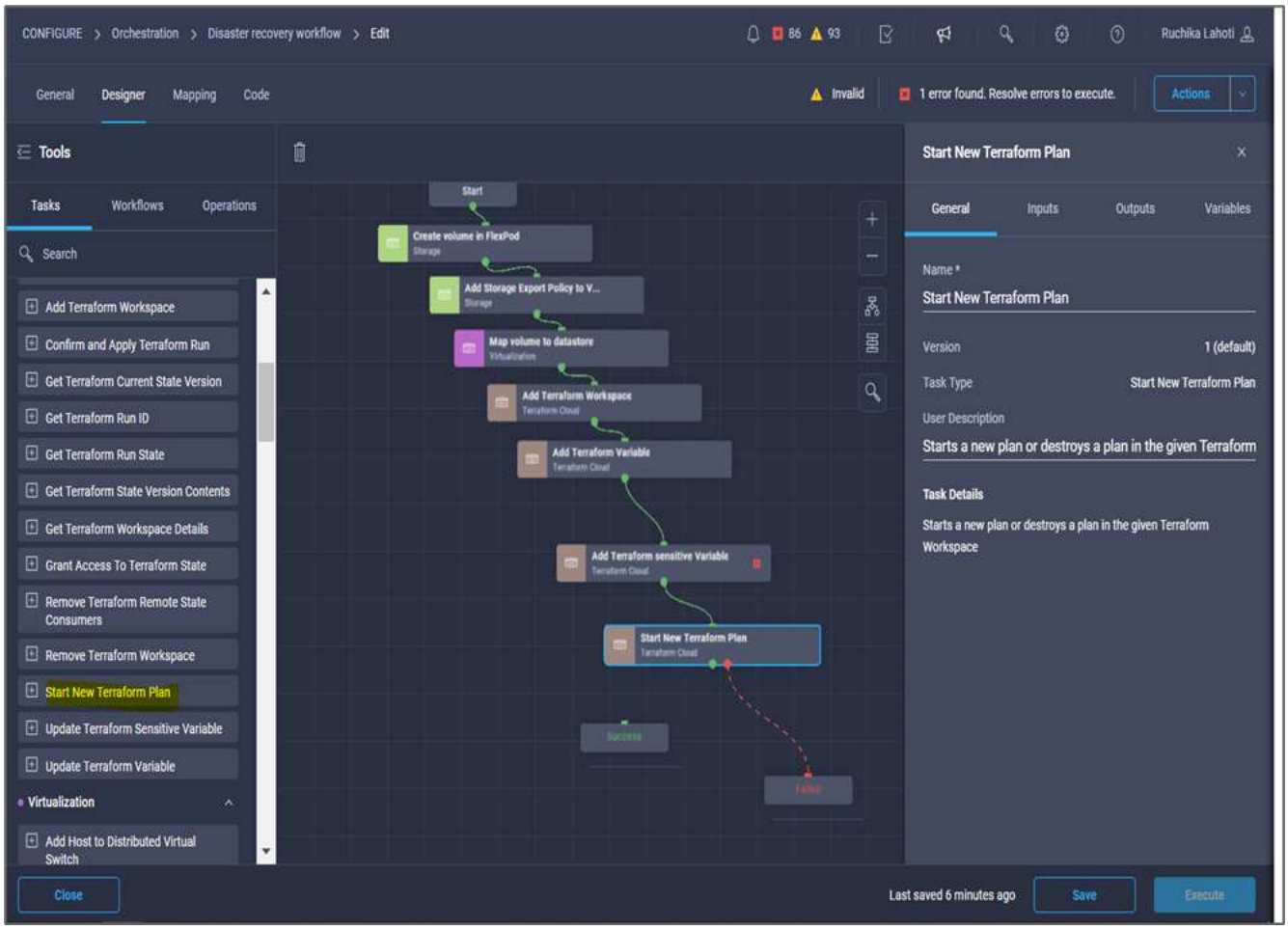
Terraform敏感变量名称	Description
cloudmanager_refresh_token	刷新令牌。请从以下位置获取：

Terraform敏感变量名称	Description
connector_id	Cloud Manager Connector的客户端ID。请从获取
CVO_admin_password	Cloud Volumes ONTAP 的管理员密码
on-prem-ontap_user_password	存储集群的管理员密码

23. 单击*映射*。此操作将完成向工作空间添加所需的Terraform敏感变量的任务。接下来、在已配置的工作空间中启动新的Terraform计划。

操作步骤 **8**：启动新的**Terraform**计划

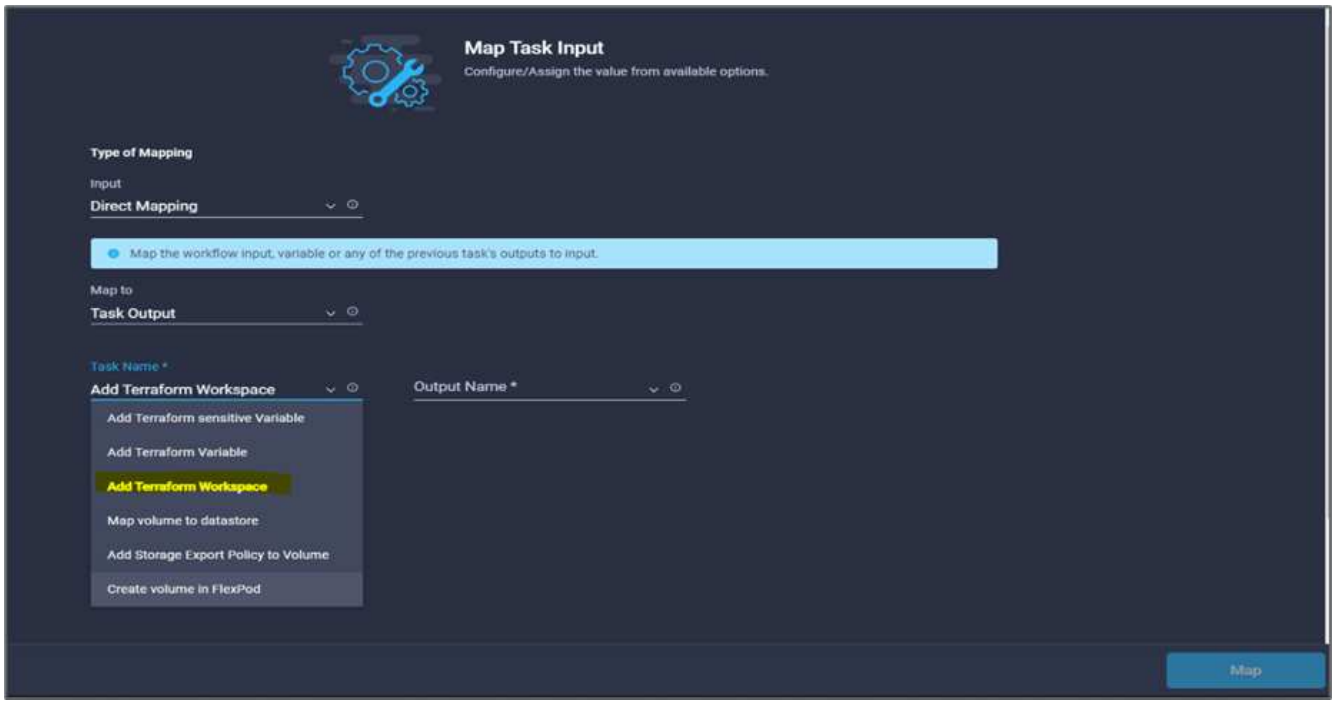
1. 转到*设计器*选项卡、然后单击*工具*部分中的*任务*。
2. 从*设计*区域的*工具*部分拖放* Terraform Cloud >启动新的Terraform Plan*任务。
3. 使用Connector在任务*添加Terraform敏感变量*和*启动新的Terraform计划任务*之间建立连接。单击 * 保存 * 。
4. 单击*启动新的Terraform计划*。在*任务属性*区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。



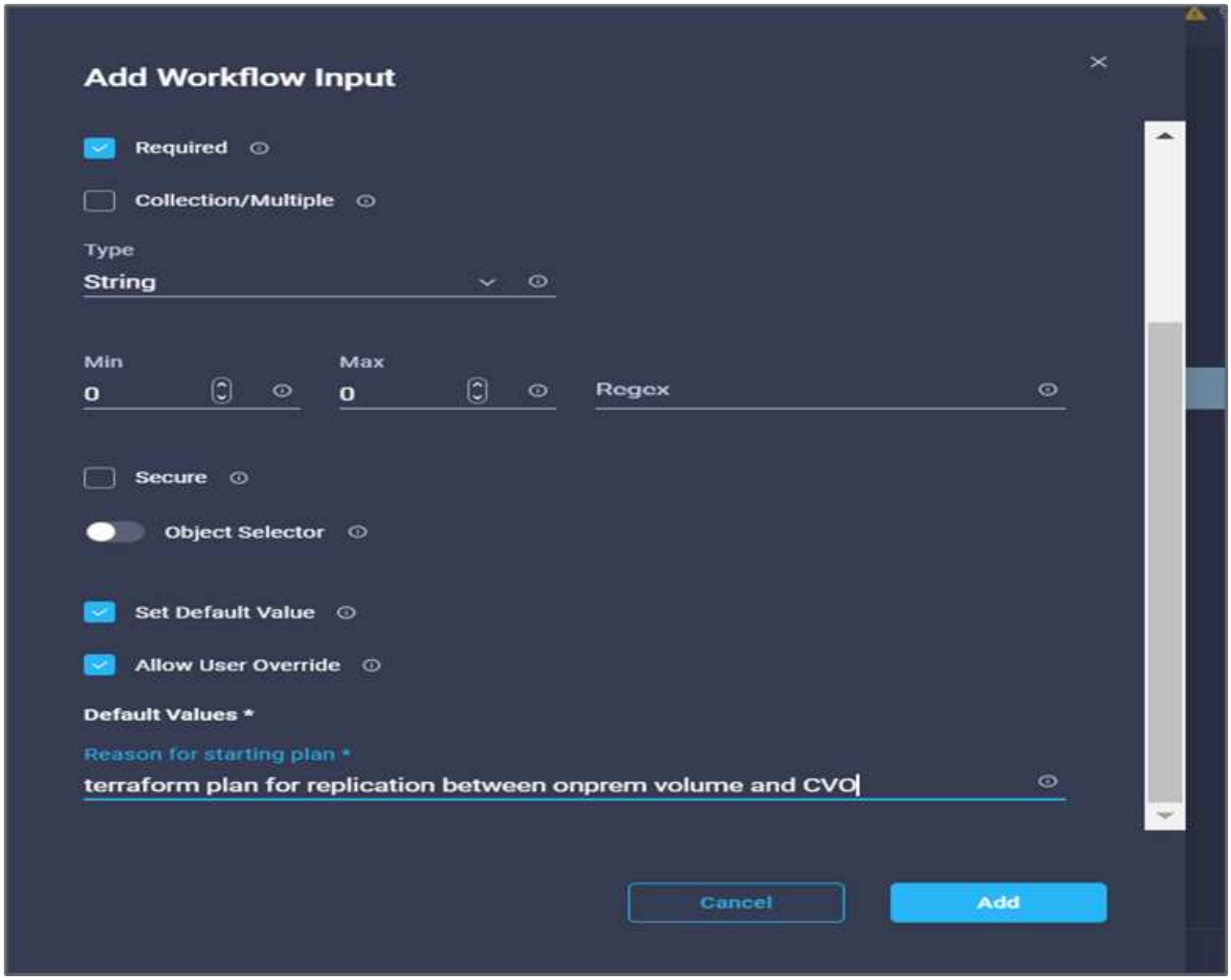
5. 在*任务属性*区域中、单击*输入*。
6. 单击* Terraform Cloud Target*字段中的*映射*。
7. 选择*静态值*、然后单击*选择Terraform Cloud Target*。选择在"为HashiCorp Terraform配置Cisco Intersight

Service "一节中添加的Terraform Cloud for Business帐户。

8. 单击*映射*。
9. 单击*工作空间ID*字段中的*映射*。
10. 选择*直接映射*、然后单击*任务输出*。
11. 单击*任务名称*、然后单击*添加Terraform Workspace*。



12. 单击*输出名称*、工作空间**ID**、然后单击*映射*。
13. 在*启动计划的原因*字段中单击*映射*。
14. 选择*直接映射*、然后单击*工作流输入*。
15. 单击*输入名称*、然后单击*创建工作流输入*。
16. 在添加输入向导中、完成以下步骤：
    a. 提供显示名称和参考名称(可选)。
    b. 确保为*类型*选择*字符串*。
    c. 单击*设置默认值并覆盖*。
    d. 输入*启动计划的原因*的默认值、然后单击*添加*。



17. 单击*映射*。
18. 单击*计划操作*字段中的*映射*。
19. 选择*静态值*、然后单击*计划操作*。单击*新计划*。

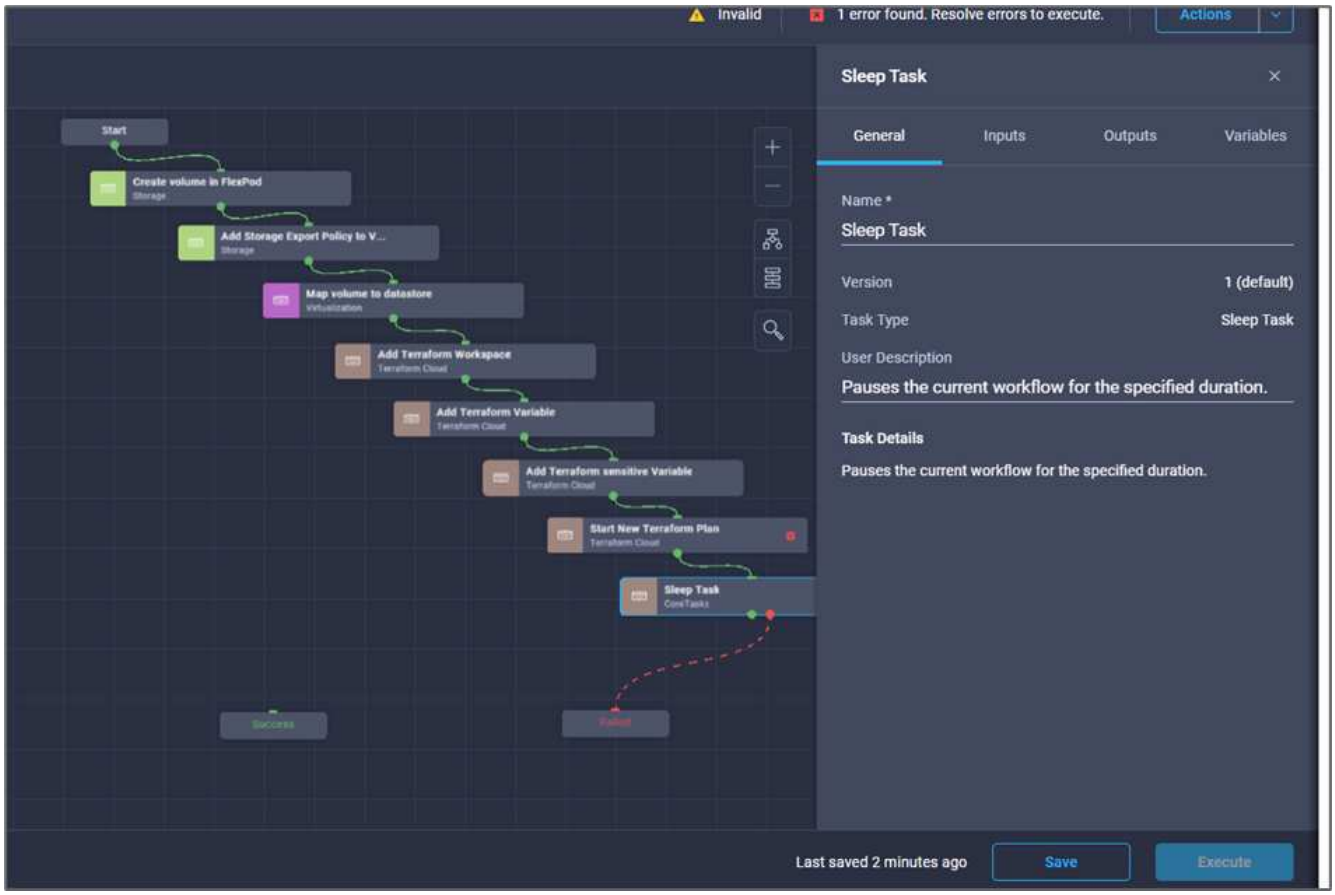
20. 单击*映射*。
21. 单击 * 保存 * 。

此时、您将完成在Terraform Cloud for Business帐户中添加Terraform计划的任务。接下来、创建一个休眠任务几秒钟。

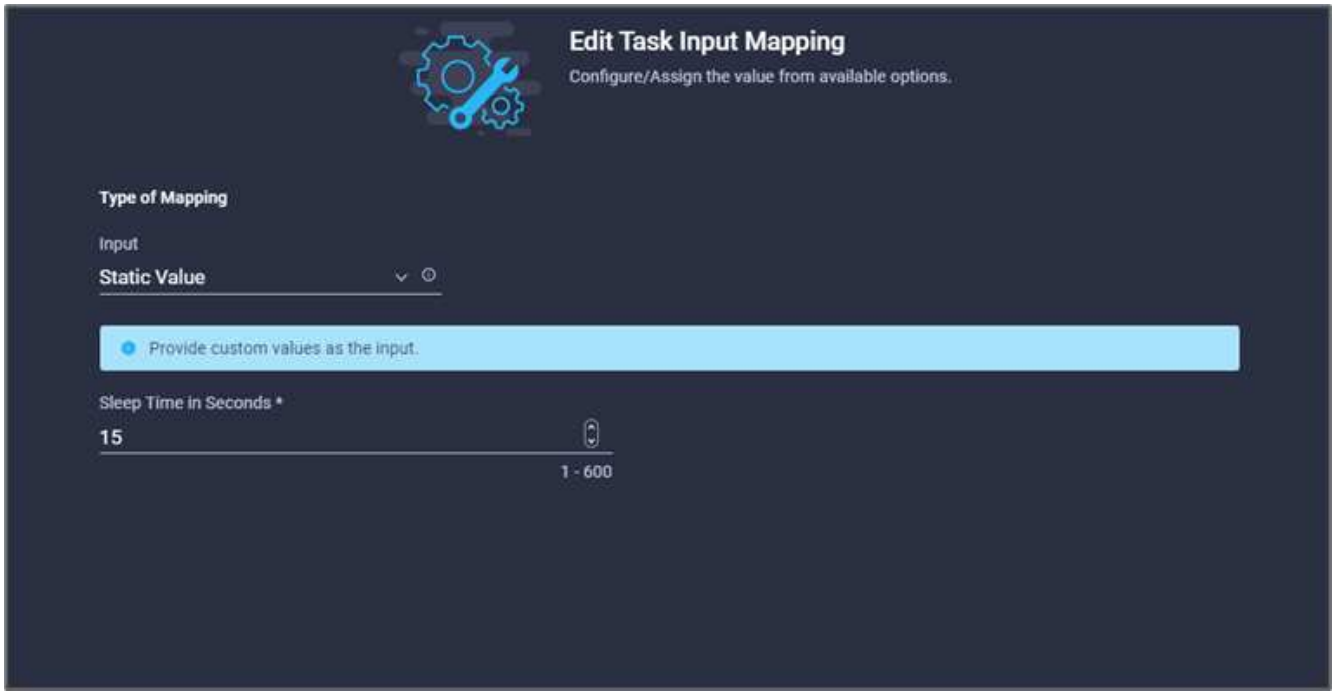
操作步骤 **9**：同步的休眠任务

Terraform Apply需要运行ID、而RunID是在Terraform Plan任务中生成的。在Terraform Plan和Terraform Apply操作之间等待几秒钟可避免时间问题。

1. 转到*设计器*选项卡、然后单击*工具*部分中的*任务*。
2. 从*设计*区域的*工具*部分拖放*核心任务>睡眠任务*。
3. 使用Connector连接任务*启动新的Terraform Plan*和*休眠任务*。单击 * 保存 * 。



4. 单击*休眠任务*。在*任务属性*区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。在此示例中、任务的名称是*同步*。
5. 在*任务属性*区域中、单击*输入*。
6. 单击*以秒为单位的睡眠时间*字段中的*映射*。
7. 选择*静态值*并输入*以15 表示*以秒为单位的睡眠时间。

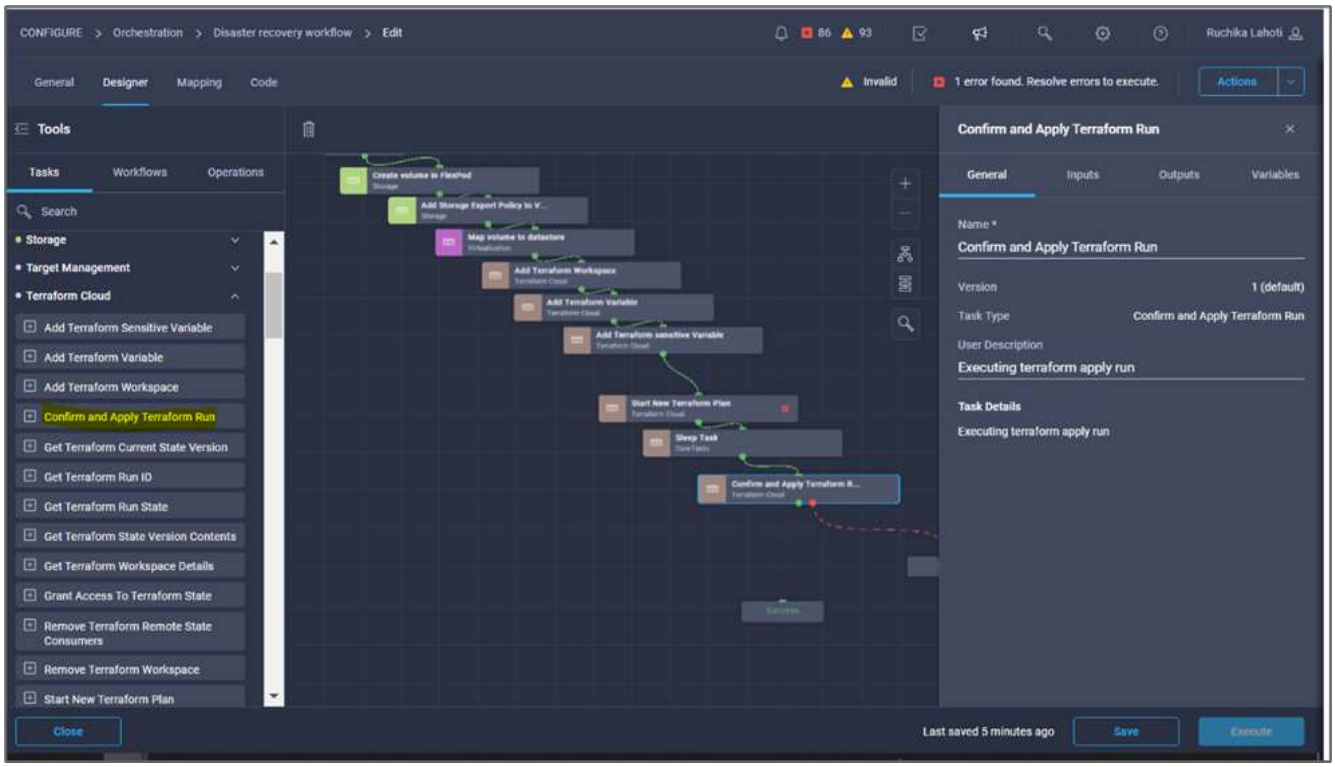


8. 单击*映射*。
9. 单击 * 保存 * 。

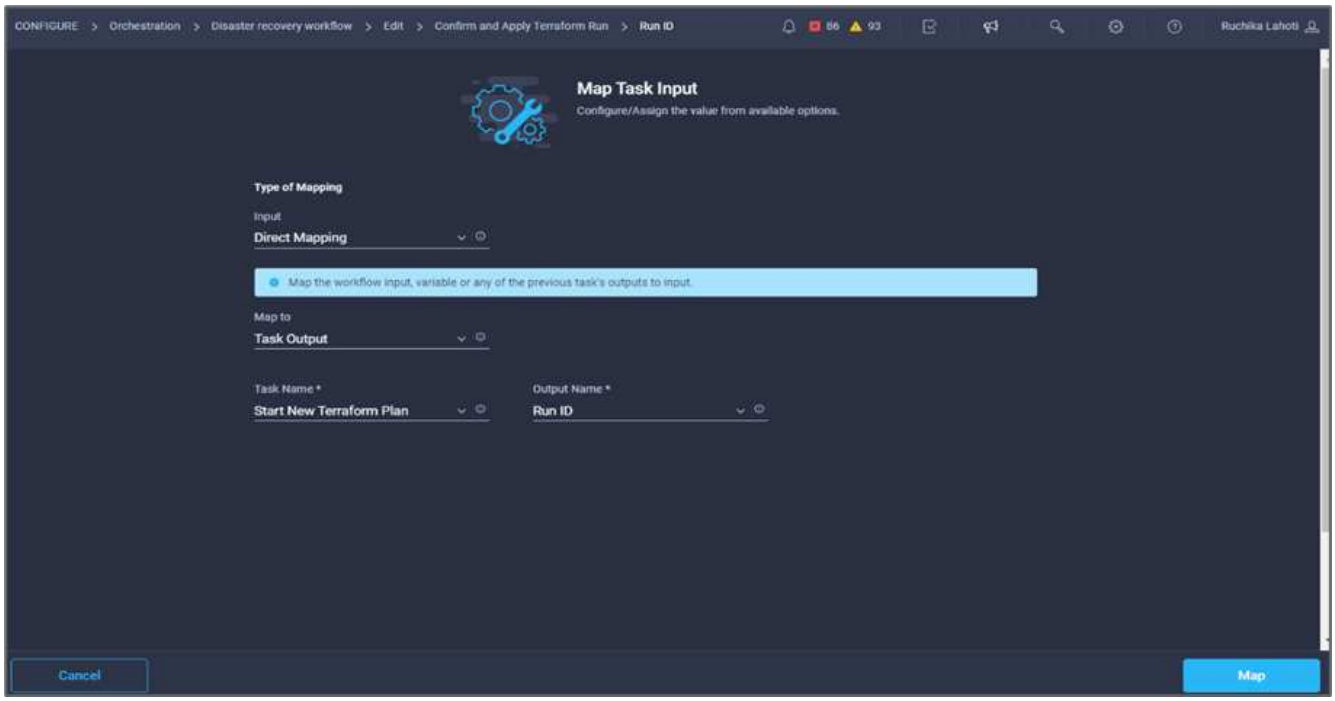
此操作将完成休眠任务。接下来、创建此工作流的最后一个任务、确认并应用Terraform Run。

操作步骤 **10**：确认并应用**Terraform Run**

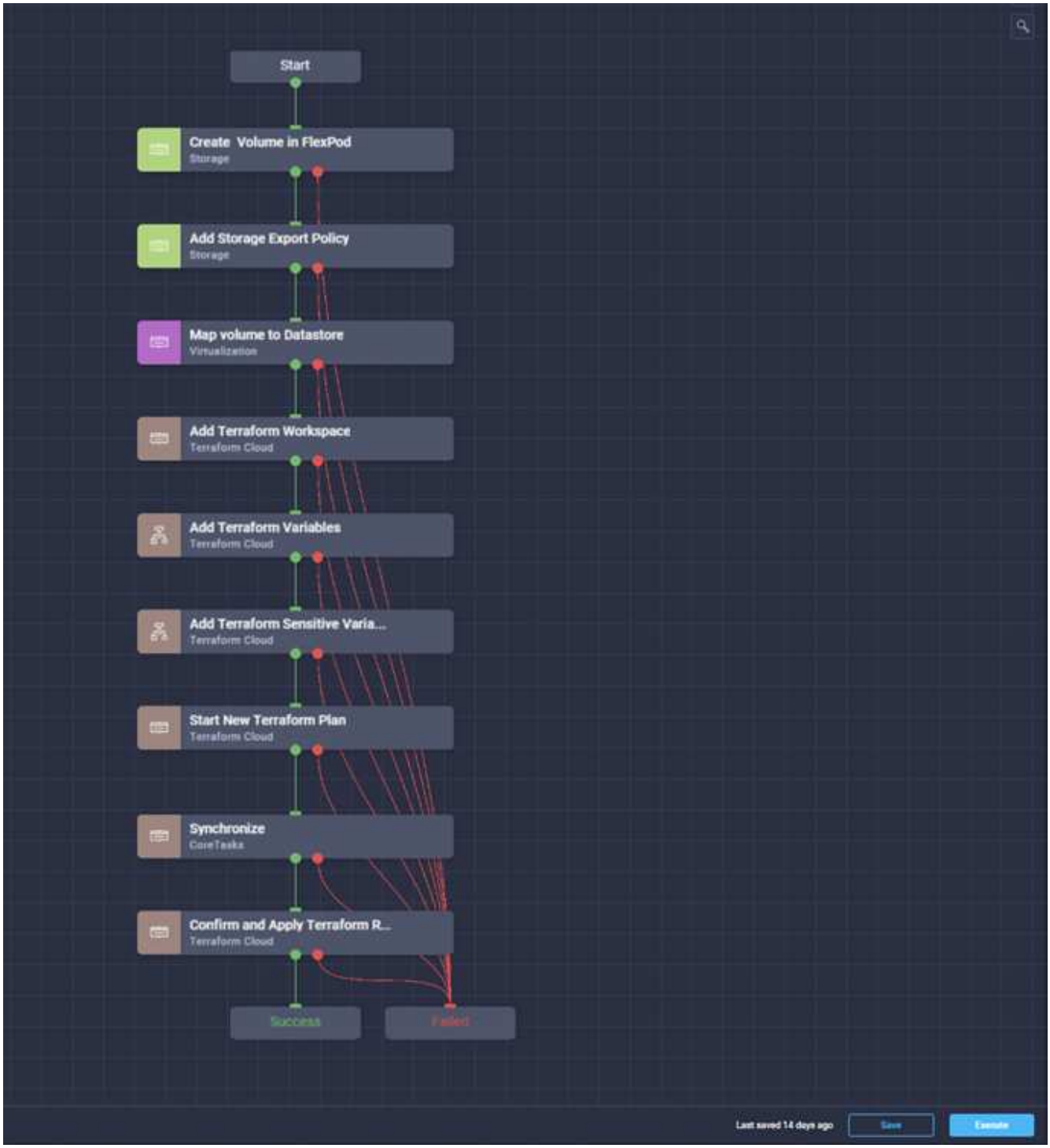
1. 转到*设计器*选项卡、然后单击*工具*部分中的*任务*。
2. 从*设计*区域的*工具*部分拖放* Terraform Cloud >确认并应用Terraform Run*任务。
3. 使用连接器连接任务*同步*和*确认并应用Terraform Run*。单击 * 保存 * 。
4. 单击*确认*和*应用Terraform Run*。在*任务属性*区域中、单击*常规*选项卡。您也可以更改此任务的名称和问题描述。



5. 在*任务属性*区域中、单击*输入*。
6. 单击* Terraform Cloud Target*字段中的*映射*。
7. 选择*静态值*、然后单击*选择Terraform Cloud Target*。选择添加在中的Terraform Cloud for Business帐户 "为HashiCorp Terraform配置Cisco Intersight Service"。 "
8. 单击*映射*。
9. 单击*运行ID*字段中的*映射*。
10. 选择*直接映射*、然后单击*任务输出*。
11. 单击*任务名称*、然后单击*开始新的Terraform计划*。
12. 单击*输出名称*、然后单击*运行ID*。



13. 单击*映射*。
14. 单击 * 保存 * 。
15. 单击*自动对齐工作流*、以便对齐所有任务。单击 * 保存 * 。



此时将完成确认并应用Terraform运行任务。使用Connector在*确认并应用Terraform Run*任务与*成功*和*失败*任务之间建立连接。

操作步骤 **11**：导入**Cisco**构建的工作流

通过Cisco Intersight Cloud Orchestrator、您可以将工作流从Cisco Intersight帐户导出到您的系统、然后将其导入到其他帐户。通过导出可导入到您帐户中的已构建工作流、创建了一个JSON文件。

中提供了工作流组件的JSON文件 "GitHub 存储库"。

"接下来：从控制器执行Terraform。"

从控制器执行**Terraform**

"上一步：灾难恢复工作流。"

我们可以使用控制器执行Terraform计划。如果您已经使用ICO工作流执行了Terraform计划、则可以跳过本节。

前提条件

解决方案 的设置首先从可访问Internet的管理工作站开始、然后再从可正常运行的Terraform安装开始。

有关安装Terraform的指南、请参见 "此处"。

克隆**GitHub repo**

此过程的第一步是将GitHub repoo克隆到管理工作站上的新空文件夹中。要克隆GitHub存储库、请完成以下步骤：

1. 在管理工作站上、为项目创建一个新文件夹。在此文件夹中创建一个名为`/root/snapmirror-CVO`的新文件夹、并将GitHub repo.
2. 在管理工作站上打开命令行或控制台界面、然后将目录更改为刚刚创建的新文件夹。
3. 使用以下命令克隆GitHub集合：

```
Git clone https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO
```

1. 将目录更改为名为`snapmirror-CVO`的新文件夹。
    - Terraform执行*

- *初始化。*初始化(本地) Terraform环境。通常、每个会话仅执行一次。
- *计划。*将Terraform状态与云中的"正常运行"状态进行比较、然后构建并显示执行计划。这不会更改部署(只读)。
- *应用。*从计划阶段应用计划。这可能会更改部署(读取和写入)。
- *销毁。*受此特定Terraform环境管理的所有资源。

  有关详细信息，请参见 "此处"。

"接下来：解决方案验证。"

解决方案验证

"先前：从控制器执行Terraform。"

在本节中、我们将通过一个示例数据复制工作流回顾解决方案 、并采取一些衡量指标来验证从FlexPod 中运行的NetApp ONTAP 实例到Google Cloud上运行的NetApp Cloud Volumes ONTAP 的数据复制完整性。

我们在此解决方案 中使用了Cisco Intersight工作流编排程序、并将继续在我们的用例中使用此流程编排程序。

值得注意的是、此解决方案 中使用的一组有限的Cisco Intersight工作流并不代表Cisco Intersight所配备的一整套工作流。您可以根据特定要求创建自定义工作流、并通过Cisco Intersight触发这些工作流。

要验证成功的灾难恢复场景、请先使用SnapMirror将数据从ONTAP 中属于FlexPod 的卷移动到Cloud Volumes ONTAP。然后、您可以尝试从Google云计算实例访问数据、然后进行数据完整性检查。

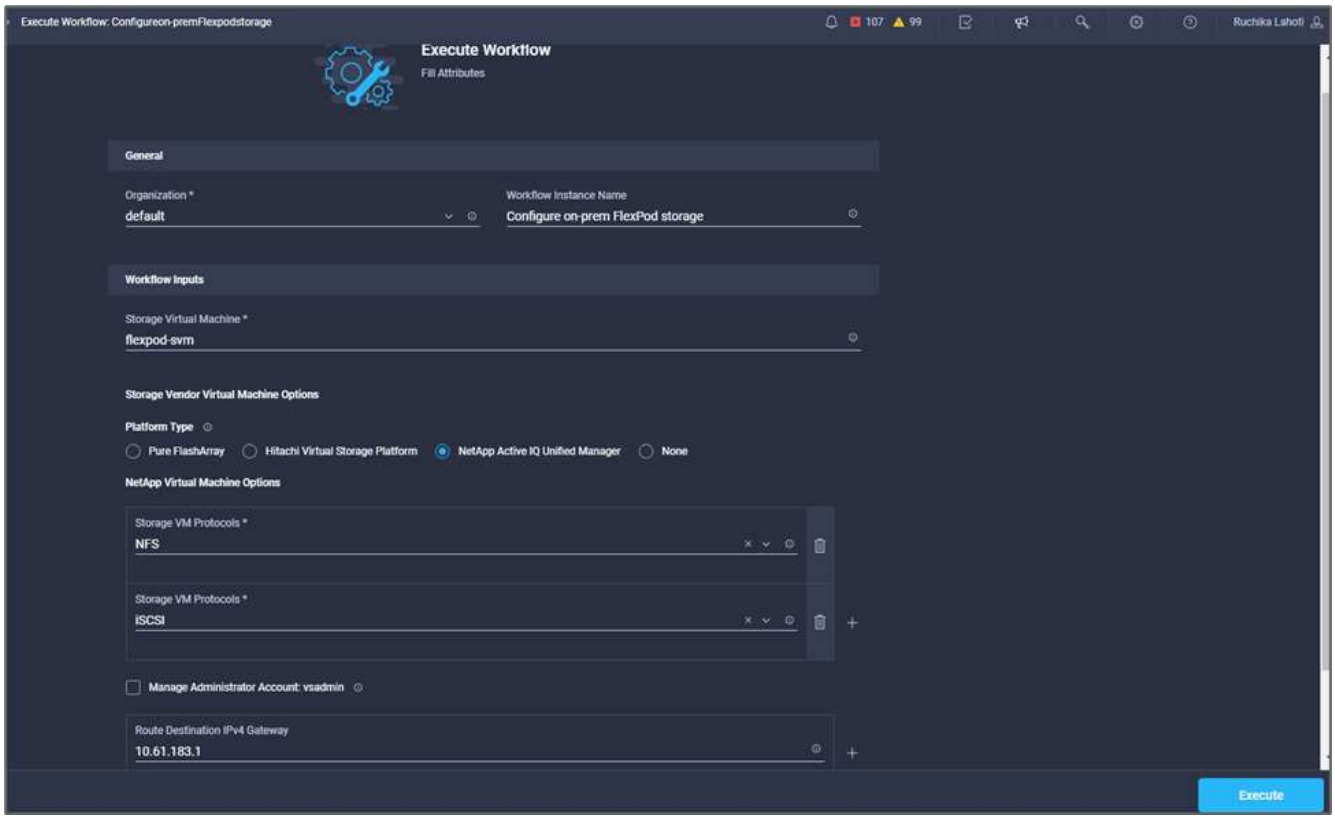
以下高级步骤用于验证此解决方案 的成功标准：

1. 对FlexPod 中ONTAP 卷中的示例数据集生成SHA256校验和。
2. 在FlexPod 中的ONTAP 和Cloud Volumes ONTAP 之间设置卷SnapMirror关系。
3. 将示例数据集从FlexPod 复制到Cloud Volumes ONTAP。
4. 中断SnapMirror关系并将Cloud Volumes ONTAP 中的卷提升为生产卷。
5. 将包含数据集的Cloud Volumes ONTAP 卷映射到Google Cloud中的计算实例。
6. 在Cloud Volumes ONTAP 中的示例数据集上生成SHA256校验和。
7. 比较源和目标上的校验和；可能是两端的校验和都匹配。

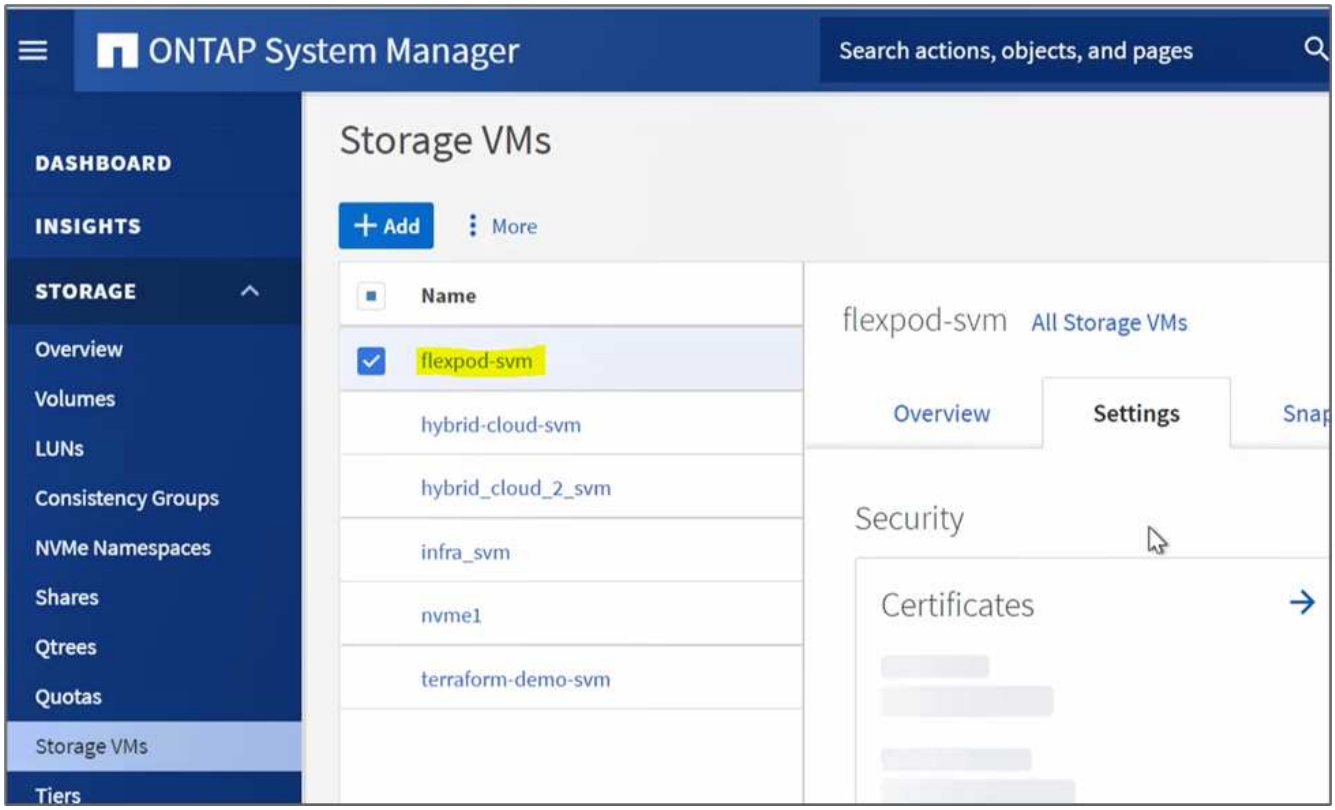
要执行内部工作流、请完成以下步骤：

1. 在Intersight中为内部部署FlexPod 创建工作流。

2. 提供所需输入并执行工作流。

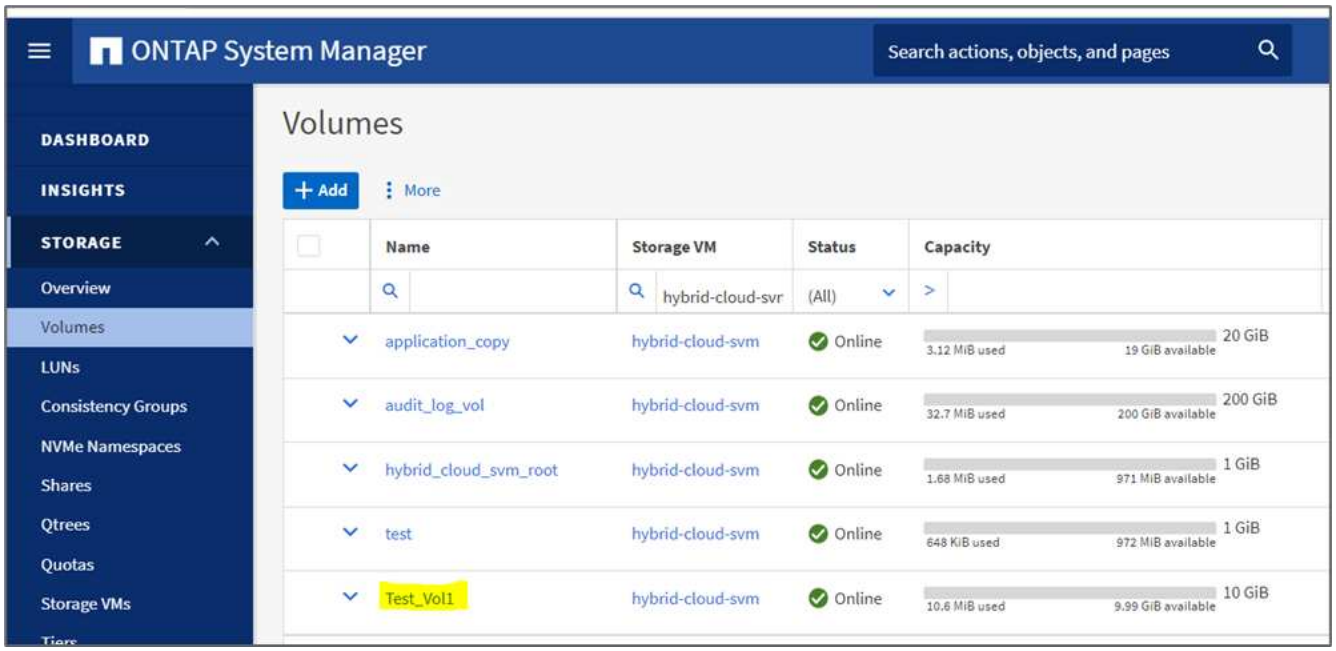


3. 在系统管理器中验证新创建的SVM。



4. 创建并执行另一个灾难恢复工作流、以便在内部FlexPod 中创建卷、并在FlexPod 和Cloud Volumes ONTAP 中的此卷之间建立SnapMirror关系。

5. 在ONTAP 系统管理器中验证新创建的卷。

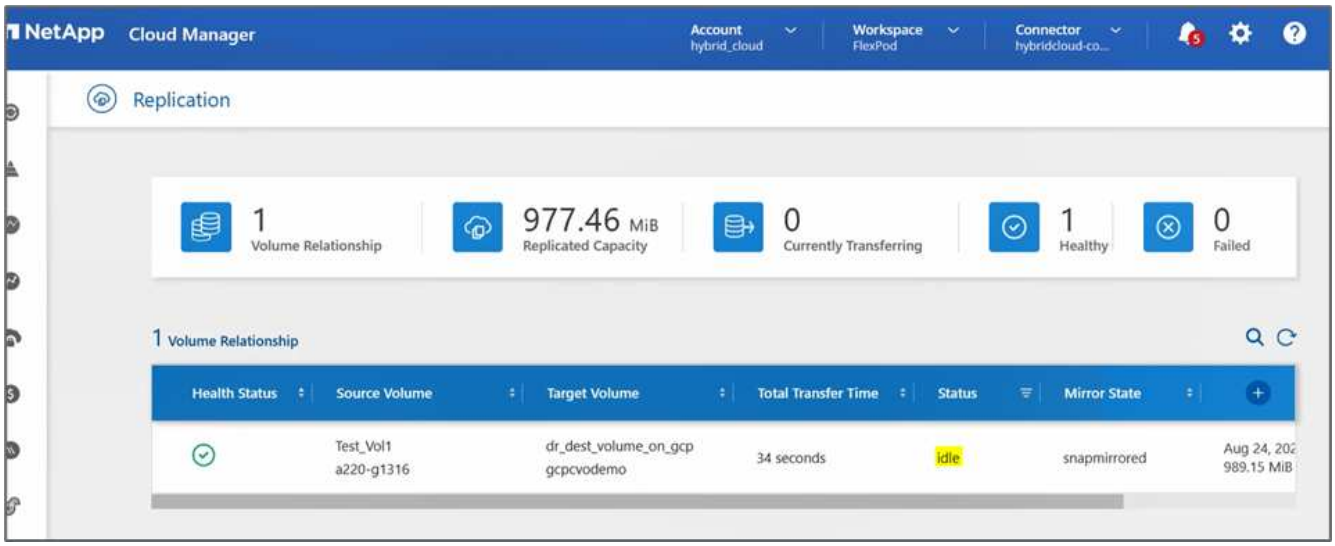


6. 将同一个NFS卷挂载到内部虚拟机、然后复制样本数据集并执行校验和。

```
root@hybridcloudbackup:/snapmirror_demo# mount -t nfs 172.22.4.157:/Test_Vol1 /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo# df -kh
Filesystem                 Size  Used Avail Use% Mounted on
udev                       1.9G     0  1.9G   0% /dev
tmpfs                      394M  1.1M  393M   1% /run
/dev/sda2                   16G   11G  4.2G  72% /
tmpfs                      2.0G     0  2.0G   0% /dev/shm
tmpfs                      5.0M     0  5.0M   0% /run/lock
tmpfs                      2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1                  55M   55M     0 100% /snap/core18/1705
/dev/loop2                  69M   69M     0 100% /snap/lxd/14804
/dev/loop0                  28M   28M     0 100% /snap/snapd/7264
172.22.4.157:/Test_Vol1     10G  512K   10G   1% /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo#
```

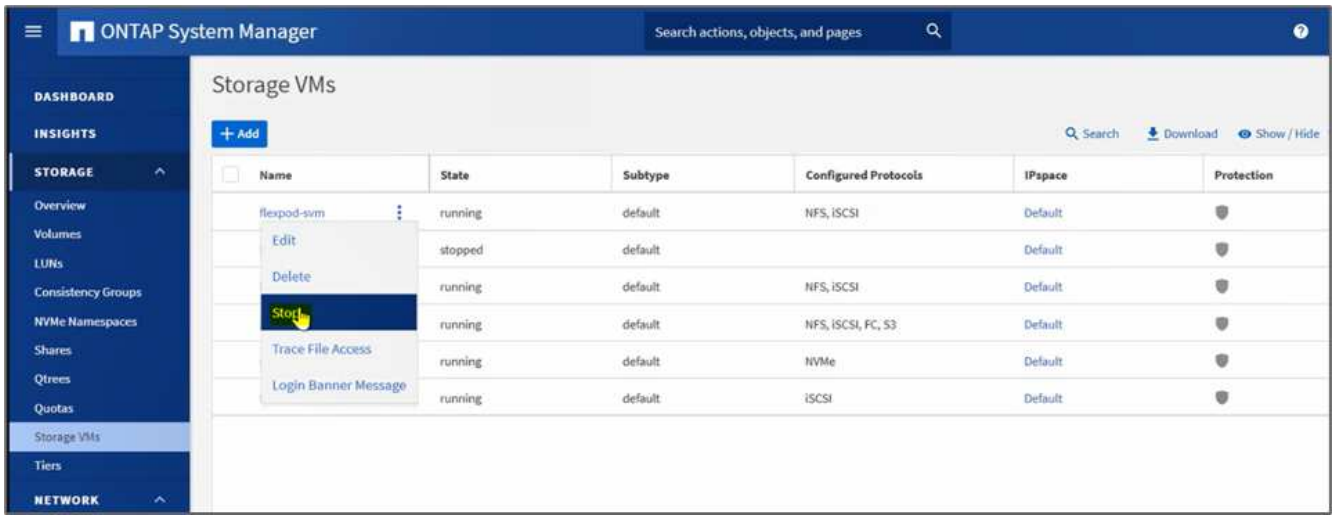
```
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo# sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo#
```

7. 在Cloud Manager中检查复制状态。根据数据大小、数据传输可能需要几分钟的时间。完成后、您可以将SnapMirror状态显示为*闲置*。

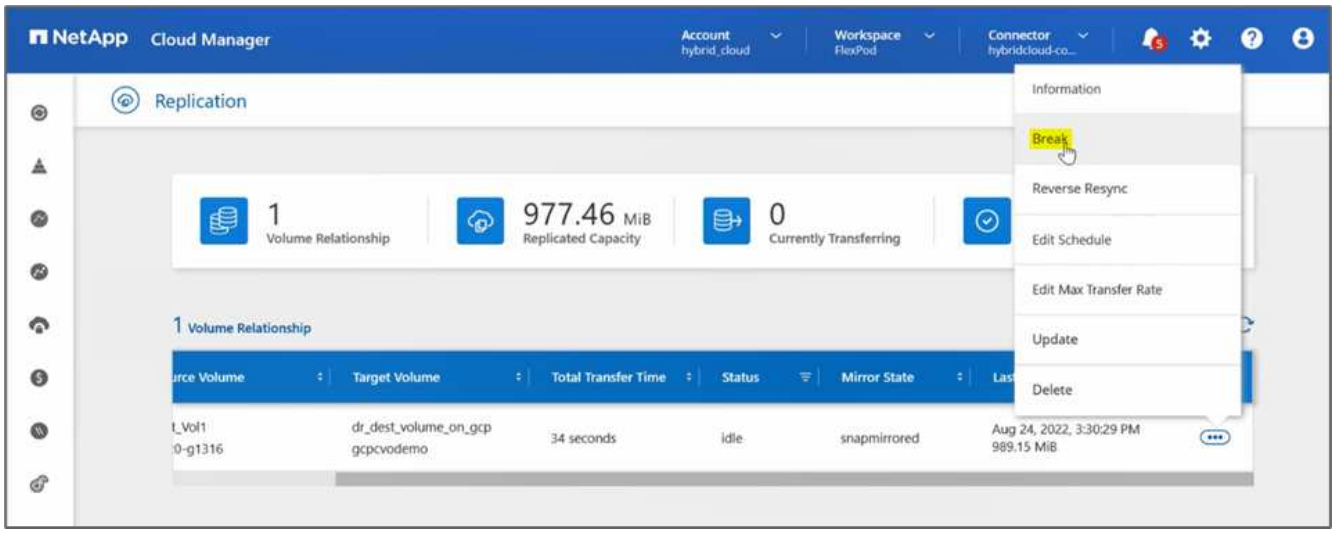


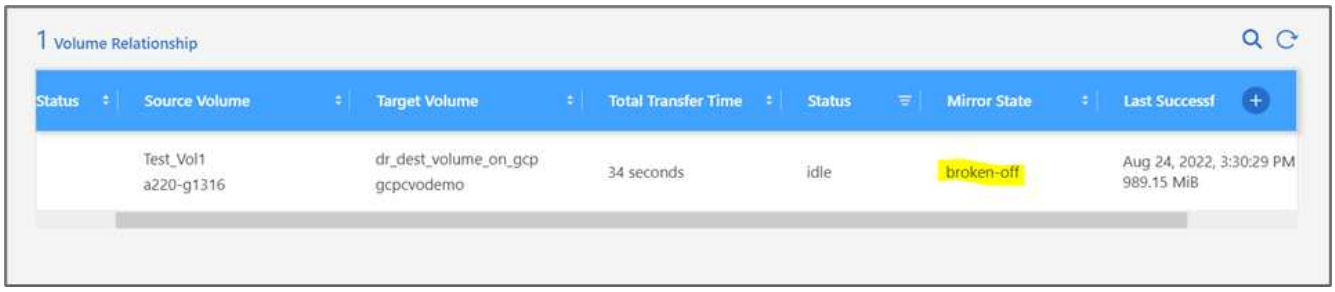
8. 数据传输完成后、通过停止托管`Test_vol1`卷的SVM来模拟源端的灾难。

   停止SVM后、在Cloud Manager中看不到`Test_vol1`卷。

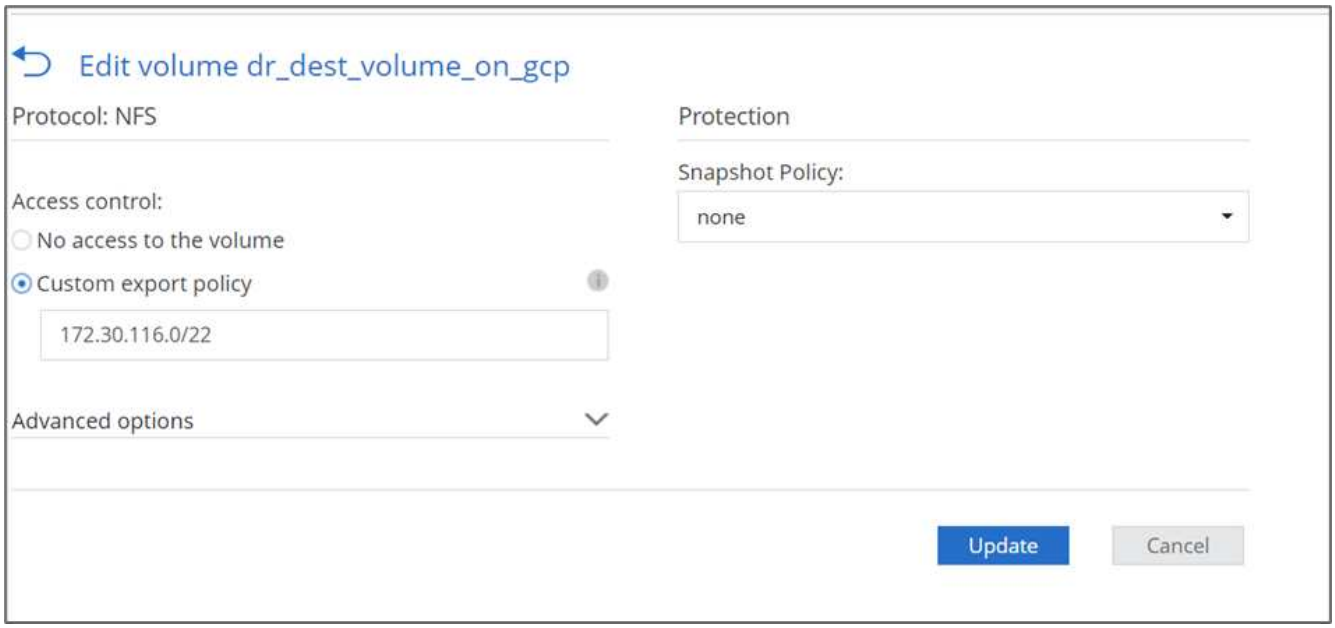


9. 中断复制关系并将Cloud Volumes ONTAP 目标卷提升为生产卷。

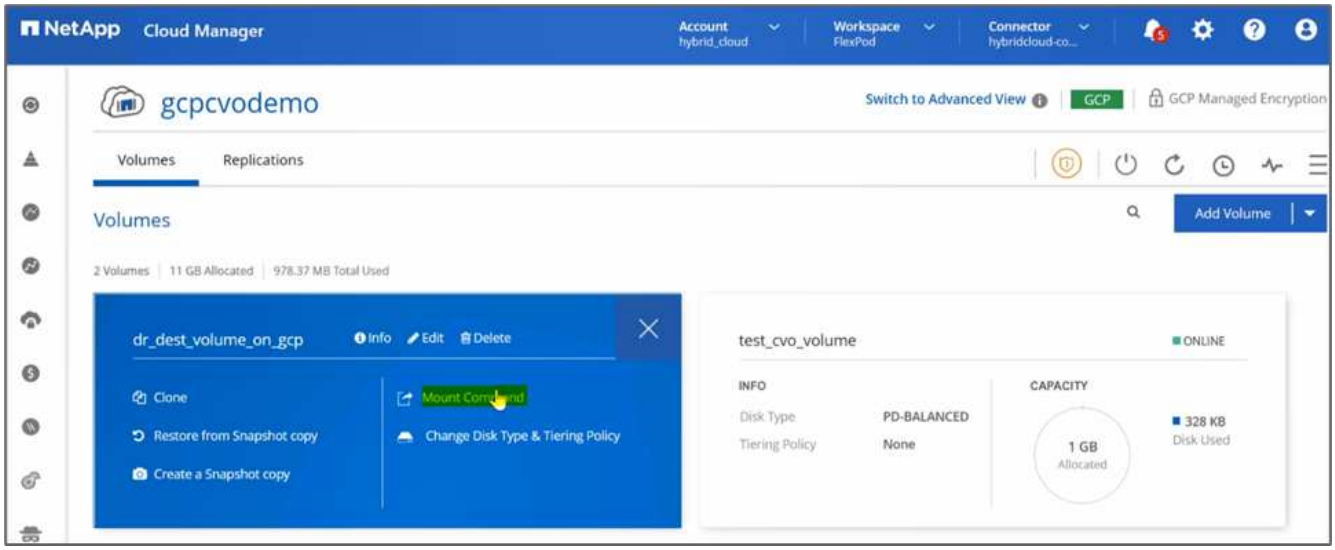




10. 编辑卷并通过将其与导出策略关联来启用客户端访问。



11. 获取卷的即用挂载命令。



12. 将卷挂载到计算实例、验证目标卷中是否存在数据、然后生成`sample_datase_2GB`文件的SHA256校验和。

```
drwxr-xr-x 21 root   root             4096 Aug 24 10:20 ../
-rwxr-xr-x  1 nobody 4294967294 1015306240 Aug 24 09:59 test.zip*
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$ sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
```

13. 比较源(FlexPod)和目标(Cloud Volumes ONTAP)的校验和值。
14. 校验和与源和目标匹配。

您可以确认已成功完成从源到目标的数据复制、并保持数据完整性。现在、在源站点完成还原期间、应用程序可以安全地使用这些数据为客户端提供服务。

"接下来：总结。"

结论

"先前版本：解决方案 验证。"

在此解决方案 中、我们使用了NetApp云数据服务、Cloud Volumes ONTAP 和FlexPod 数据中心基础架构、使用由Cisco Intersight Cloud Orchestrator提供支持的公有 云构建灾难恢复解决方案。FlexPod 解决方案 不断发展、可帮助客户实现应用程序和业务交付流程的现代化。借助此解决方案 、您可以使用公有 云作为瞬时或全时灾难恢复计划的首选位置来构建BCDr计划、同时保持较低的灾难恢复解决方案 成本。

内部FlexPod 和NetApp Cloud Volumes ONTAP 之间的数据复制由成熟的SnapMirror技术处理、但您也可以选择其他NetApp数据传输和同步工具、如Cloud Sync 、以满足您的数据移动性需求。基于TLS/AES的内置加密技术可确保传输中数据的安全性。

无论您是为应用程序制定临时灾难恢复计划、还是为企业制定全职灾难恢复计划、此解决方案 中使用的产品组合都可以大规模满足这两项要求。在Cisco Intersight Workflow Orchestrator的支持下、可以通过预构建的工作流自动执行此操作、不仅无需重新构建流程、还可以加快BCDr计划的实施速度。

借助Cisco Intersight Cloud Orchestrator提供的自动化和流程编排功能、解决方案 可以轻松方便地管理FlexPod

内部部署和混合云中的数据复制。

从何处查找追加信息

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：

GitHub

- 使用的所有Terraform配置

  "https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO"

- 用于导入工作流的JSON文件

  "https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows"

Cisco Intersight

- Cisco Intersight帮助中心

  "https://intersight.com/help/saas/home"

- Cisco Intersight Cloud Orchestrator文档：

  "https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator"

- Cisco Intersight Service for HashiCorp Terraform文档

  "https://intersight.com/help/saas/features/terraform_cloud/admin"

- Cisco Intersight数据表

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html"

- Cisco Intersight Cloud Orchestrator数据表

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html"

- 适用于HashiCorp Terraform的Cisco Intersight Service数据表

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html"

FlexPod

- FlexPod 主页

  "https://www.flexpod.com"

- 适用于 FlexPod 的 Cisco 验证设计和部署指南

"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"

- 采用Cisco UCS X系列的FlexPod 数据中心

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

互操作性

- NetApp 互操作性表工具

  "http://support.netapp.com/matrix/"

- Cisco UCS 硬件和软件互操作性工具

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- VMware 兼容性指南

  "http://www.vmware.com/resources/compatibility/search.php"

NetApp Cloud Volumes ONTAP 参考文档

- NetApp Cloud Manager

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- Cloud Volumes ONTAP

  https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-gcp.html

- Cloud Volumes ONTAP TCO计算器

  https://cloud.netapp.com/google-cloud-calculator

- Cloud Volumes ONTAP 规模估算工具

  "https://cloud.netapp.com/cvo-sizer"

- 云评估工具

  https://cloud.netapp.com/assessments

- NetApp混合云

  https://cloud.netapp.com/hybrid-cloud

- Cloud Manager API 文档

  "https://docs.netapp.com/us-en/occm/reference_infrastructure_as_code.html"

对问题进行故障排除

"https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_(CVO)"

Terraform

- Terraform Cloud

  "https://www.terraform.io/cloud"

- Terraform文档

  "https://www.terraform.io/docs/"

- NetApp Cloud Manager注册表

  "https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/lates"

GCP

- 适用于GCP的ONTAP 高可用性

  "https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick"

- GCP的基础

  https://netapp.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=f3d0368b-7165-4d43-a76e-ae01011853d6

采用NetApp Astra和适用于Red Hat OpenShift的Cisco Intersight的FlexPod 混合云

TR-4936：采用NetApp Astra和适用于Red Hat OpenShift的Cisco Intersight的FlexPod 混合云

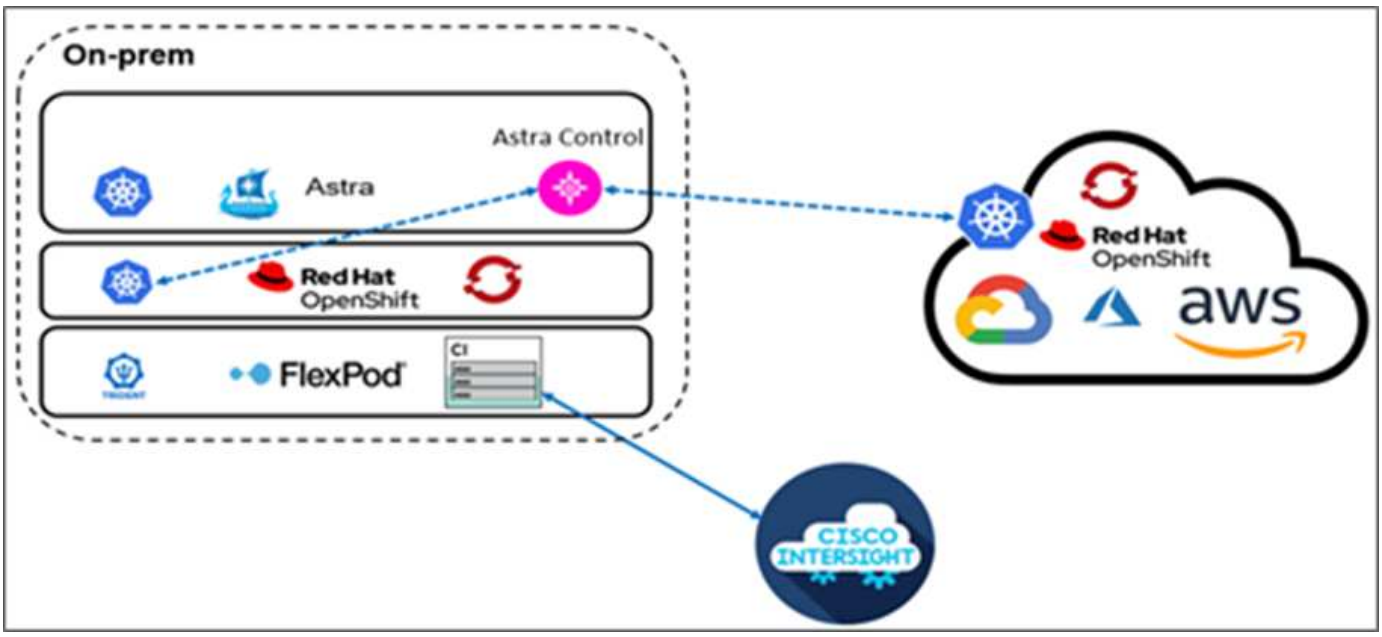
Abhinav Singh

简介

随着容器和Kubernetes成为开发、部署、运行、管理和扩展容器化应用程序的实际选择、企业越来越多地在这些应用程序上运行业务关键型应用程序。业务关键型应用程序在很大程度上依赖于状态。有状态应用程序具有关联的状态、数据和配置信息、并依靠先前的数据事务来执行其业务逻辑。在Kubernetes上运行的业务关键型应用程序仍然像传统应用程序一样具有可用性和业务连续性要求。服务中断可能会严重影响公司的收入、工作效率和声誉损失。因此、在集群、内部数据中心和混合云环境内部和之间快速轻松地保护、恢复和移动Kubernetes工作负载至关重要。企业已经认识到将业务转变为混合云模式的优势、将应用程序现代化到云原生外形规格的优势也在他们的市场中居高不下。

本技术报告将NetApp Astra控制中心与基于FlexPod 融合基础架构解决方案 的Red Hat OpenShift容器平台结合在一起、并扩展到Amazon Web Services (AWS)以构成混合云数据中心。以熟悉为基础 "FlexPod 和Red Hat OpenShift"本文档介绍了NetApp Astra控制中心、从安装、配置、应用程序保护工作流以及内部和云之间的应用程序迁移开始。同时、还讨论了在将NetApp Astra控制中心用于在Red Hat OpenShift上运行的容器化应用程序时、应用程序感知型数据管理功能(例如备份和恢复、业务连续性)的优势。

下图显示了解决方案 概述。



audience

本文档的目标受众包括首席技术官(CTO)、应用程序开发人员、Cloud解决方案 架构师、站点可靠性工程师(SRE)、开发运营工程师、ITOps以及专注于设计、托管和管理容器化应用程序的专业服务团队。

NetApp Astra Control—主要用例

NetApp Astra Control旨在为使用Cloud原生 微服务的客户简化应用程序保护：

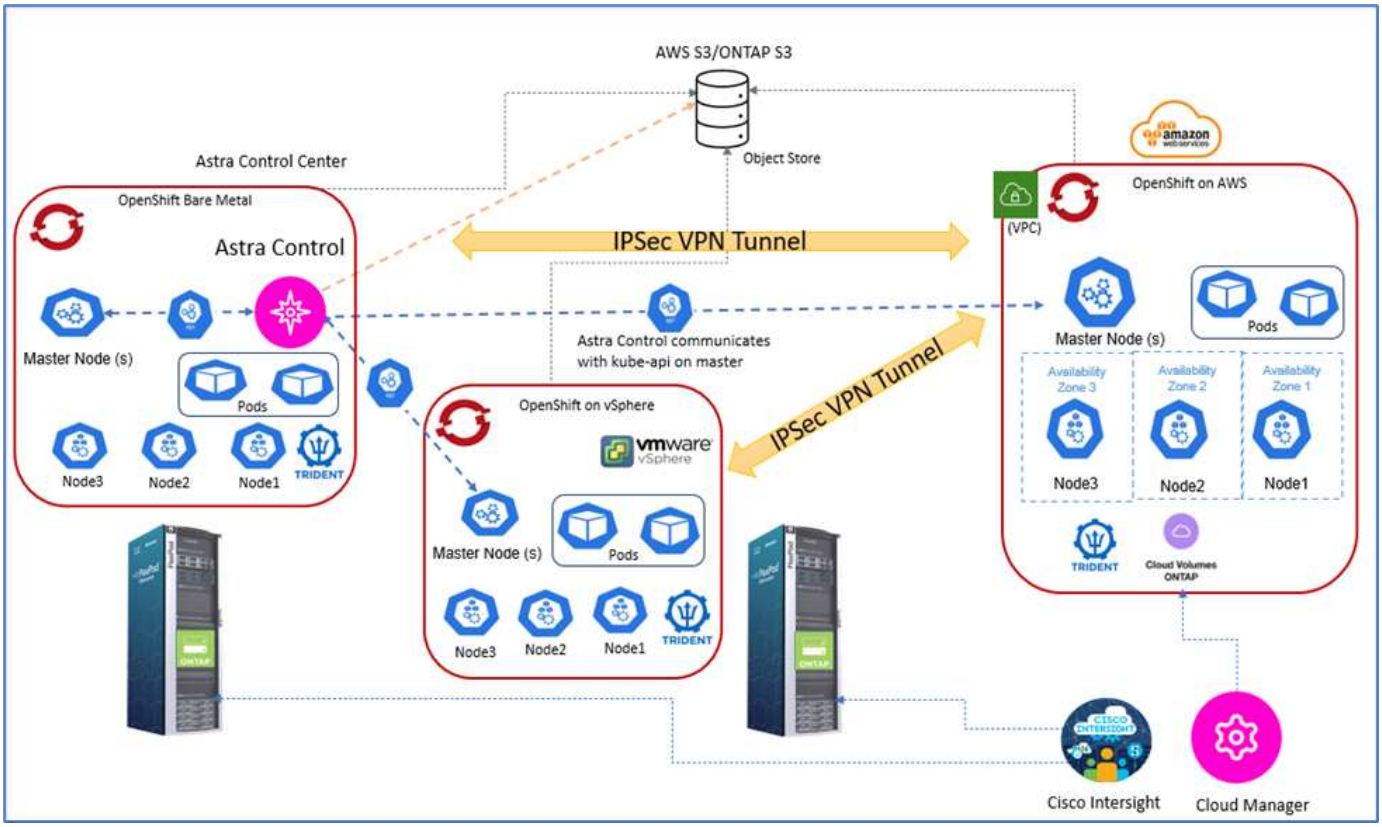
- *使用快照的时间点(PIT)应用程序表示。*借助Astra Control、您可以为容器化应用程序创建端到端快照、其中包括Kubernetes上运行的应用程序的配置详细信息以及相关的永久性存储。发生意外事件时、可以单击按钮将应用程序还原到已知正常状态。
- *完整副本应用程序备份。*借助Astra Control、您可以按预定义的计划执行完整的应用程序备份、该计划可用于自动将应用程序还原到同一K8s集群或另一个K8s集群。
- *应用程序可移植性和克隆迁移。*借助Astra Control、您可以将整个应用程序及其数据从一个Kubernetes集群克隆到另一个集群或同一个K8s集群中。无论集群位于何处、此功能还有助于在K8s集群之间移植或迁移应用程序(只需在克隆后删除源应用程序实例即可)。
- *自定义应用程序一致性。*借助Astra Control、您可以利用执行挂钩来控制应用程序暂停状态的定义。将‘pre’和‘post '执行挂钩置于快照和备份工作流中、在创建快照或备份之前、您的应用程序将以您自己的方式暂停。
- *自动执行应用程序级灾难恢复(DR)。*借助Astra Control、您可以为容器化应用程序配置业务连续性灾难恢复(Business Continuity Disaster Recovery、BCDr)计划。后端使用NetApp SnapMirror、并自动完成灾难恢复工作流的实施。

解决方案 拓扑

本节介绍解决方案 的逻辑拓扑。

下图显示了解决方案 拓扑结构、其中包括运行OpenShift容器平台集群的FlexPod 内部环境以及采用NetApp Cloud Volumes ONTAP 、Cisco Intersight和NetApp Cloud Manager SaaS平台的AWS上的自管理OpenShift容

器平台集群。



第一个OpenShift容器平台集群是在FlexPod 上安装的裸机集群、第二个OpenShift容器平台集群部署在FlexPod上运行的VMware vSphere上、第三个OpenShift容器平台集群部署为 "专用集群" 作为一个自助管理基础架构、迁移到AWS上的现有虚拟私有云(VPC)中。

在此解决方案 中、FlexPod 通过站点到站点VPN连接到AWS、但是、客户也可以使用直接连接实施扩展到混合云。Cisco Intersight用于管理FlexPod 基础架构组件。

在此解决方案 中、Astra控制中心负责管理在FlexPod 和AWS上运行的OpenShift容器平台集群上托管的容器化应用程序。Astra控制中心安装在FlexPod 上运行的OpenShift裸机实例上。Astra Control与主节点上的Kube-API进行通信、并持续监控Kubernetes集群是否发生更改。添加到K8s集群中的任何新应用程序都会自动发现并提供管理。

容器化应用程序的PIT表示可以使用Astra控制中心捕获为快照。可以通过计划的保护策略或按需触发应用程序快照。对于Astra支持的应用程序、快照的崩溃状态是一致的。应用程序快照构成永久性卷中应用程序数据的快照、以及与该应用程序关联的各种Kubernetes资源的应用程序元数据。

可以使用使用预定义的备份计划或按需使用Astra Control创建应用程序的完整副本备份。对象存储用于存储应用程序数据的备份。NetApp ONTAP S3、NetApp StorageGRID 以及任何通用S3实施均可用作对象存储。

"接下来：解决方案 组件。"

解决方案组件

"上一步：解决方案概述。"

FlexPod

FlexPod 是一组定义的硬件和软件，可为虚拟化和非虚拟化解决方案奠定集成基础。FlexPod 包括NetApp ONTAP 存储、Cisco Nexus网络、Cisco MDS存储网络、Cisco统一计算系统(Cisco UCS)。该设计非常灵活、可以将网络、计算和存储安装到一个数据中心机架中、也可以根据客户的数据中心设计进行部署。端口密度允许网络组件容纳多种配置。

Astra Control

Astra Control为公有 云和内部环境中托管的云原生应用程序提供应用程序感知型数据保护服务。Astra Control可为在Kubernetes上运行的容器化应用程序提供数据保护、灾难恢复和迁移功能。

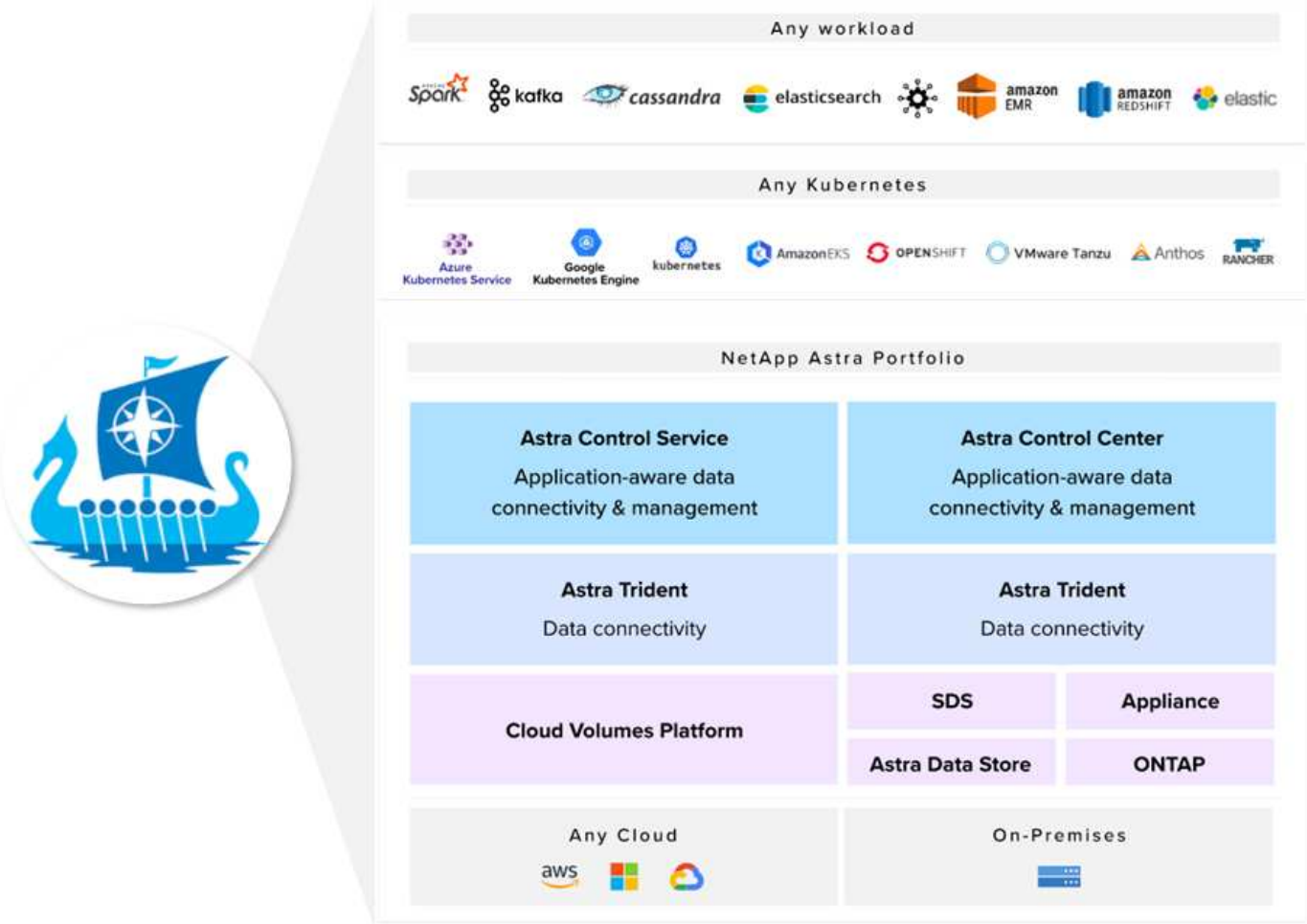
功能

Astra Control 为 Kubernetes 应用程序数据生命周期管理提供了关键功能：

- 自动管理永久性存储
- 创建应用程序一致的按需快照和备份
- 自动执行策略驱动的快照和备份操作
- 在混合云环境中将应用程序和关联数据从一个Kubernetes集群迁移到另一个集群
- 将应用程序克隆到同一个K8s集群或另一个K8s集群
- 直观显示应用程序保护状态
- 提供图形用户界面和完整的REST API列表、用于利用现有内部工具实施所有保护工作流。

Astra Control为容器化应用程序提供了一个单一的管理平台可视化视图、其中包括对在Kubernetes集群上创建的相关资源的深入了解。您可以使用一个门户查看所有云或所有数据中心中的所有集群、所有应用程序。您可以在所有环境(内部或公有 云)中使用Astra Control API来实施数据管理工作流。

下图显示了Astra Control功能。



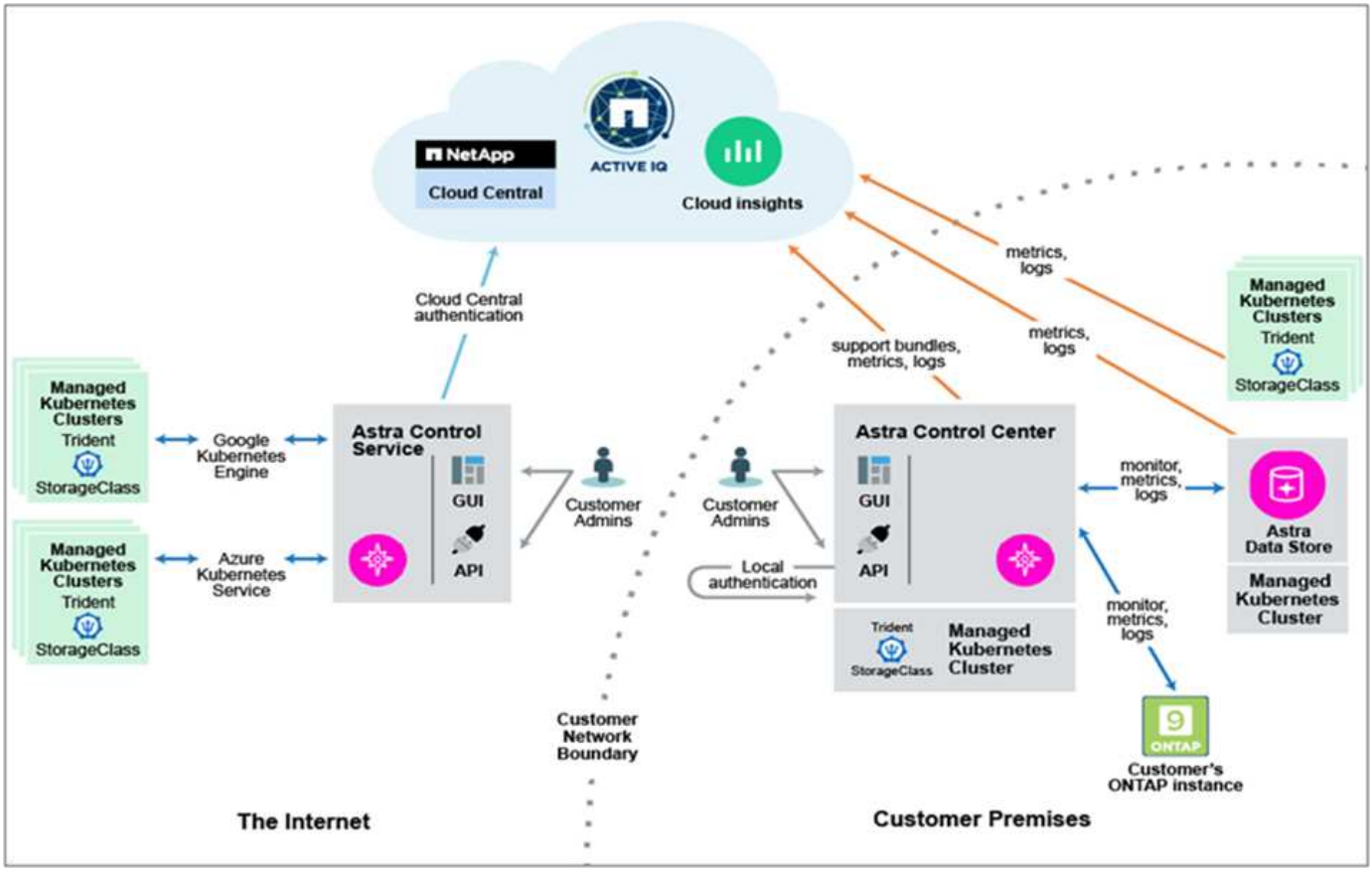
Astra Control消费模式

Astra Control有两种消费模式：

- * Astra Control Service。* NetApp托管的一项完全托管服务、可在Google Kubernetes Engine (GKEE) Azure Kubernetes Service (AKS)中为Kubernetes集群提供应用程序感知型数据管理。
- * Astra Control Center。*自管理软件、可为内部和混合云环境中运行的Kubernetes集群提供应用程序感知型数据管理。

本技术报告利用Astra控制中心管理Kubernetes上运行的云原生应用程序。

下图显示了Astra Control架构。



Astra Trident

Astra Trident是一款完全受支持的开源存储编排程序、适用于容器和Kubernetes分发版。它从一开始就经过精心设计、可帮助您使用行业标准界面(如)满足容器化应用程序的持久性需求 "容器存储接口(CSI)"。借助Astra Trident、微服务和容器化应用程序可以利用NetApp存储系统产品组合提供的企业级存储服务。

Astra Trident作为Pod部署在Kubernetes集群上、并为您的Kubernetes工作负载提供动态存储编排服务。它可以帮助您的容器化应用程序快速轻松地使用NetApp广泛的产品组合中的永久性存储、其中包括NetApp ONTAP (NetApp AFF 、NetApp FAS 、NetApp ONTAP Select 、云、 和适用于NetApp ONTAP 的Amazon FSx) 、NetApp Element 软件(NetApp SolidFire)以及Azure NetApp Files 服务、Google Cloud上的云卷服务和AWS上的云卷服务。在FlexPod 环境中、Astra Trident用于为容器动态配置和管理永久性卷、这些容器由NetApp FlexVol 卷和ONTAP 存储平台(例如NetApp AFF 和FAS 系统以及Cloud Volumes ONTAP)上托管的LUN提供支持。Trident在实施Astra Control提供的应用程序保护方案方面也发挥着关键作用。有关Astra Trident的详细信息、请参见 "Astra Trident文档。"

存储后端

要使用Astra Trident、您需要受支持的存储后端。Trident后端定义了Trident与存储系统之间的关系。它会告诉Trident如何与该存储系统通信、以及Trident如何从该存储系统配置卷。Trident将自动从后端提供符合存储类定义的要求的存储池。

- ONTAP AFF 和 FAS 存储后端。作为存储软件和硬件平台、ONTAP 可提供核心存储服务、支持多个存储访问协议以及存储管理功能、例如NetApp Snapshot副本和镜像。
- Cloud Volumes ONTAP 存储后端
- "Astra 数据存储" 存储后端

NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP 是一款软件定义的存储产品、可为文件和块工作负载提供高级数据管理。借助Cloud Volumes ONTAP 、您可以优化云存储成本并提高应用程序性能、同时增强数据保护、安全性和合规性。

主要优势包括：

- 利用内置的重复数据删除，数据压缩，精简配置和克隆功能最大限度地降低存储成本。
- 在云环境发生故障时，确保企业级可靠性和持续运行。
- Cloud Volumes ONTAP 利用NetApp行业领先的复制技术SnapMirror将内部数据复制到云中、因此可以轻松地为多种使用情形提供二级副本。
- Cloud Volumes ONTAP 还与 Cloud Backup Service 集成，提供备份和还原功能，以保护云数据并对其进行长期归档。
- 按需在高性能和低性能存储池之间切换，而无需使应用程序脱机。
- 使用NetApp SnapCenter 确保Snapshot副本的一致性。
- Cloud Volumes ONTAP 支持数据加密，并提供防病毒和勒索软件保护。
- 与 Cloud Data sense 集成有助于您了解数据环境并识别敏感数据。

Cloud Central

Cloud Central提供了一个中央位置、用于访问和管理NetApp云数据服务。通过这些服务、您可以在云中运行关键应用程序、创建自动化灾难恢复站点、备份数据以及跨多个云有效迁移和控制数据。有关详细信息，请参见 "Cloud Central。"

Cloud Manager

Cloud Manager是一款基于SaaS的企业级管理平台、IT专家和云架构师可以利用NetApp的云解决方案集中管理其混合多云基础架构。它提供了一个集中式系统、用于查看和管理内部和云存储、支持混合、多个云提供商和客户。有关详细信息，请参见 "Cloud Manager"。

连接器

Connector是一个实例、可使Cloud Manager管理公有 云环境中的资源和流程。要使用Cloud Manager提供的许多功能、需要使用Connector。连接器可以部署在云或内部网络中。

连接器在以下位置受支持：

- AWS
- Microsoft Azure
- Google Cloud
- 在您的内部环境中

要了解有关Connector的更多信息、请参见 "此链接。"

NetApp Cloud Insights

Cloud Insights 是一款NetApp云基础架构监控工具、可用于监控由Astra控制中心管理的Kubernetes集群的性能

和利用率。Cloud Insights 将存储使用量与工作负载相关联。在 Astra 控制中心中启用 Cloud Insights 连接后，遥测信息将显示在 Astra 控制中心 UI 页面中。

NetApp Active IQ Unified Manager

借助NetApp Active IQ Unified Manager 、您可以通过一个经过重新设计的直观界面监控ONTAP 存储集群、该界面可通过社区智慧和AI分析提供智能。它可以全面洞察存储环境及其运行的虚拟机(VM)的运行状况、性能和主动式能力。当存储基础架构发生问题描述 时、Unified Manager可以通知您问题描述 的详细信息、以帮助您确定根发生原因。通过VM信息板、您可以查看VM的性能统计信息、以便调查从VMware vSphere主机到网络最后再到存储的整个I/O路径。某些事件还提供了可用于更正问题描述 的补救措施。您可以为事件配置自定义警报、以便在发生问题时、通过电子邮件和SNMP陷阱通知您。Active IQ Unified Manager 可以预测容量和使用趋势、以便在出现问题之前主动采取行动、从而防止做出长期可能导致其他问题的被动短期决策、从而为用户的存储需求进行规划。

Cisco Intersight

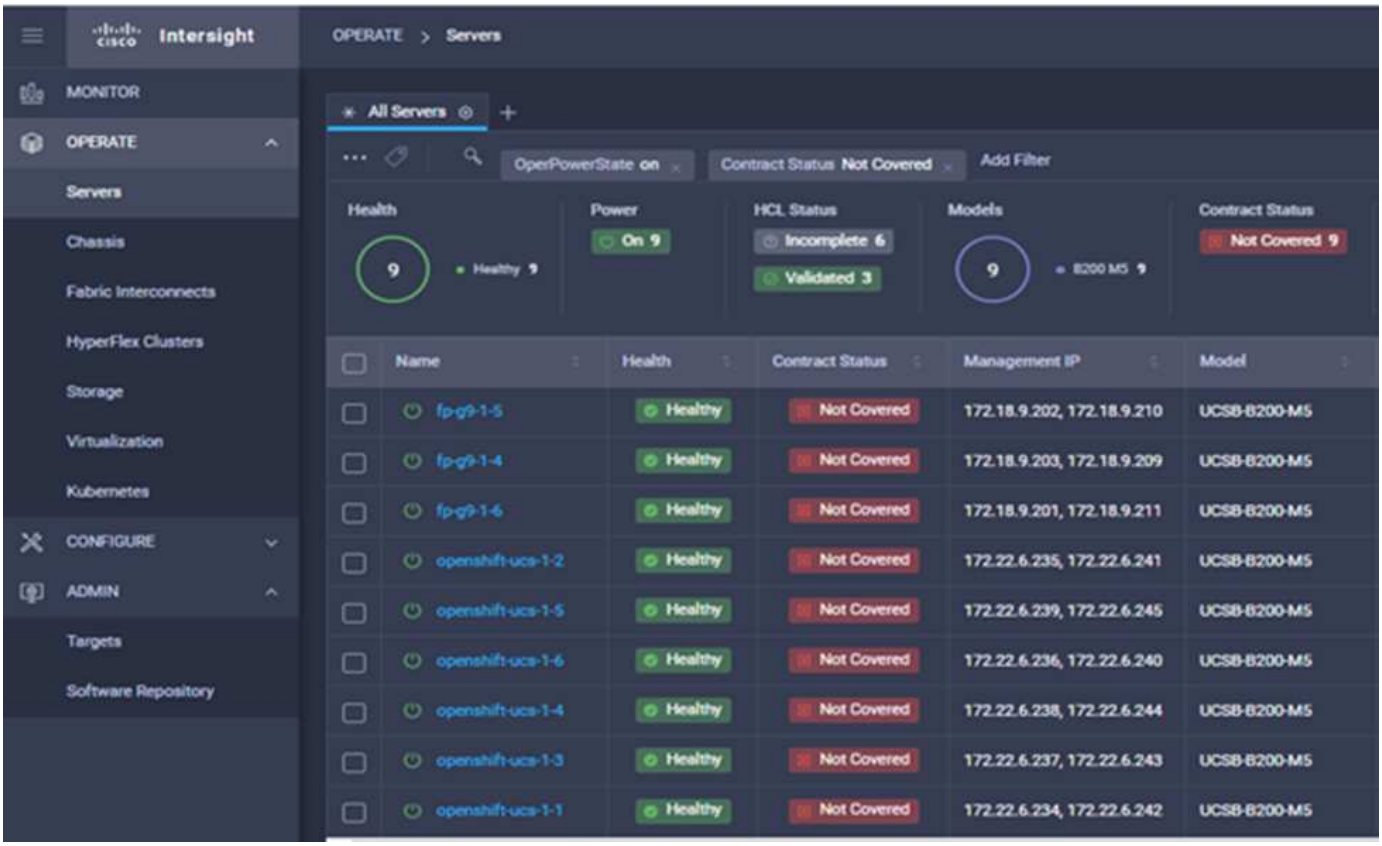
Cisco Intersight是一个SaaS平台、可为传统和云原生应用程序和基础架构提供智能自动化、可观察性和优化功能。该平台可帮助IT团队推动变革、并提供专为混合云设计的运营模式。

Cisco Intersight具有以下优势：

- *交付速度更快。*由于采用基于敏捷性的软件开发模式、可从云或客户数据中心以服务的形式交付、并经常进行更新和持续创新。这样、客户就可以专注于加快业务部门的交付速度。
- *简化操作。*通过使用一个安全的SaaS交付工具以及通用清单、身份验证和API在整个堆栈和所有位置之间运行、简化操作、消除团队之间的孤岛。从内部管理物理服务器和虚拟机管理程序到虚拟机、K8s、无服务器、自动化、 在内部和公有 云之间实现优化和成本控制。
- *持续优化。*利用Cisco Intersight在每一层提供的智能以及Cisco TAC持续优化您的环境。这种智能功能可转换为建议的可自动操作、因此您可以实时适应每个变化：从移动工作负载和监控物理服务器的运行状况到自动调整K8s集群大小、再到您所使用的公有 云的成本降低建议。

Cisco Intersight支持两种管理操作模式：UCSM受管模式(Umm)和Intersight受管模式(IMM)。在首次设置互联阵列期间、您可以为光纤连接的Cisco UCS系统选择原生 Umm或IMM。在此解决方案 中、使用原生 Umm。

下图显示了Cisco Intersight信息板。

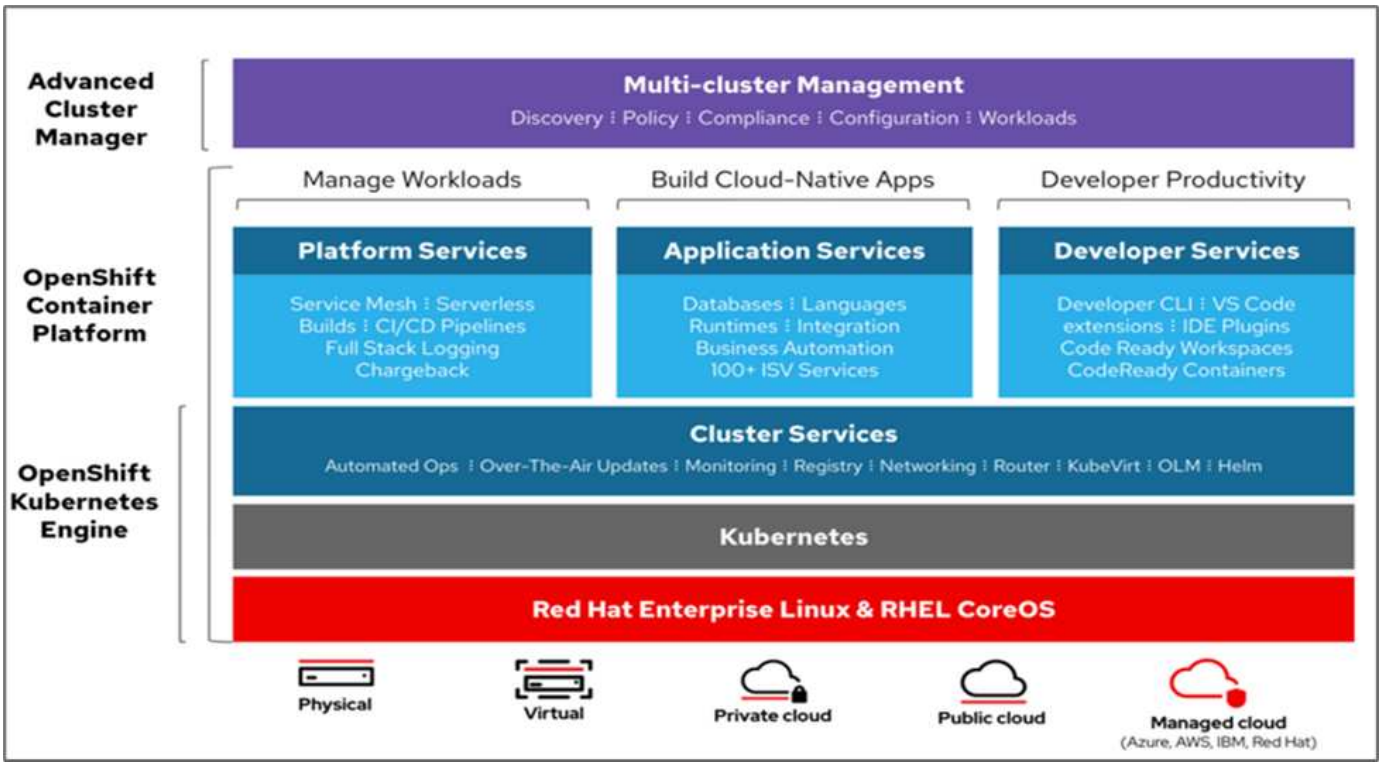


Red Hat OpenShift 容器平台

Red Hat OpenShift容器平台是一个容器应用程序平台、它将CRI-O和Kubernetes汇集在一起、并提供一个API和Web界面来管理这些服务。CRI-O是Kubernetes容器运行时接口(CRI)的实施、可使用与Open Container Initiative (OCI)兼容的运行时。它是使用Docker作为Kubernetes运行时的轻型替代方案。

OpenShift容器平台允许客户创建和管理容器。容器是独立的进程、在其自身环境中运行、独立于操作系统和底层基础架构。OpenShift容器平台有助于开发、部署和管理基于容器的应用程序。它提供了一个自助服务平台、可按需创建、修改和部署应用程序、从而加快开发和发布生命周期。OpenShift容器平台具有一个基于微服务的架构、该架构包含可协同工作的小型分离单元。它在Kubernetes集群上运行、其中包含有关对象的数据存储在etcd中、etcd是一个可靠的集群模式密钥值存储。

下图概述了Red Hat OpenShift容器平台。



Kubernetes基础架构

在OpenShift容器平台中、Kubernetes跨一组CRI-O运行时主机管理容器化应用程序、并提供部署、维护和应用程序扩展机制。CRI-O服务软件包、实例化和运行容器化应用程序。

Kubernetes集群由一个或多个主节点和一组工作节点组成。此解决方案 设计包括硬件和软件堆栈中的高可用性(HA)功能。Kubernetes集群设计为在HA模式下运行、其中包含三个主节点和至少两个辅助节点、以帮助确保集群不会出现单点故障。

Red Hat核心操作系统

OpenShift容器平台使用Red Hat Enterprise Linux CoreOS (RHCOS)、这是一种面向容器的操作系统、它结合了CoreOS和Red Hat Atomic Host操作系统的一些最佳特性和功能。RHCOS专门为从OpenShift容器平台运行容器化应用程序而设计、可与新工具配合使用、以实现快速安装、基于操作员的管理和简化的升级。

RHCOS包括以下功能：

- IGNITION、OpenShift容器平台将其用作首次启动系统配置、用于首次启动和配置计算机。
- CRI-O是一种Kubernetes原生 容器运行时实施、它与操作系统紧密集成、可提供高效且优化的Kubernetes体验。CRI-O可提供运行、停止和重新启动容器的功能。它完全取代了OpenShift容器平台3中使用的Docker容器引擎。
- Kubernetes的主节点代理Kubelet负责启动和监控容器。

VMware vSphere 7.0

VMware vSphere是一个虚拟化平台、可将大量基础架构(包括CPU、存储和网络等资源)作为一个无缝、多功能且动态的操作环境进行全面管理。与管理单个计算机的传统操作系统不同、VMware vSphere可将整个数据中心的基础架构聚合在一起、从而创建一个具有资源的动力中心、这些资源可以快速动态地分配给任何需要的应用程序。

有关详细信息，请参见 "VMware vSphere"。

VMware vSphere vCenter

VMware vCenter Server可通过一个控制台统一管理所有主机和VM、并对集群、主机和VM进行聚合性能监控。通过VMware vCenter Server、管理员可以深入了解计算集群、主机、虚拟机、存储、子操作系统、 虚拟基础架构的其他关键组件。VMware vCenter可管理VMware vSphere环境中提供的丰富功能。

硬件和软件版本

可以将此解决方案 扩展到运行中定义的受支持软件、固件和硬件版本的任何FlexPod 环境 "NetApp 互操作性表工具" 和 "Cisco UCS硬件兼容性列表。" OpenShift集群以裸机方式安装在FlexPod 和VMware vSphere上。

要管理多个OpenShift (K8s)集群、只需要一个Astra控制中心实例、而每个OpenShift集群上都安装了Trident CSI。Astra控制中心可以安装在其中任何一个OpenShift集群上。在此解决方案 中、Astra控制中心安装在OpenShift裸机集群上。

下表列出了OpenShift的FlexPod 硬件和软件版本。

组件	产品	**version**
计算	Cisco UCS互联阵列6454	4.1 (3c)
	Cisco UCS B200 M5服务器	4.1 (3c)
网络	Cisco Nexus 9336C-x2 NX-OS	9.3 (8)
存储	NetApp AFF A700	9.11.1
	NetApp Astra 控制中心	22.04.0
	NetApp Astra Trident CSI插件	22.04.0
	NetApp Active IQ Unified Manager	9.11
软件	VMware ESXi nenic 以太网驱动程序	1.0.35.0
	vSphere ESXi	7.0 (U2)
	VMware vCenter设备	7.0 U2b
	Cisco Intersight Assist虚拟设备	1.0.9-342
	OpenShift容器平台	4.9.
	OpenShift容器平台主节点	RHCOS 4.9
	OpenShift容器平台工作节点	RHCOS 4.9

下表列出了AWS上OpenShift的软件版本。

组件	产品	**version**
计算	主实例类型：m5.xlarge	不适用
	员工实例类型：m5.large	不适用
网络	虚拟私有云传输网关	不适用

组件	产品	**version**
存储	NetApp Cloud Volumes ONTAP	9.11.1
	NetApp Astra Trident CSI插件	22.04.0
软件	OpenShift容器平台	4.9.
	OpenShift容器平台主节点	RHCOS 4.9
	OpenShift容器平台工作节点	RHCOS 4.9

"接下来：适用于OpenShift容器平台4的FlexPod 裸机安装。"

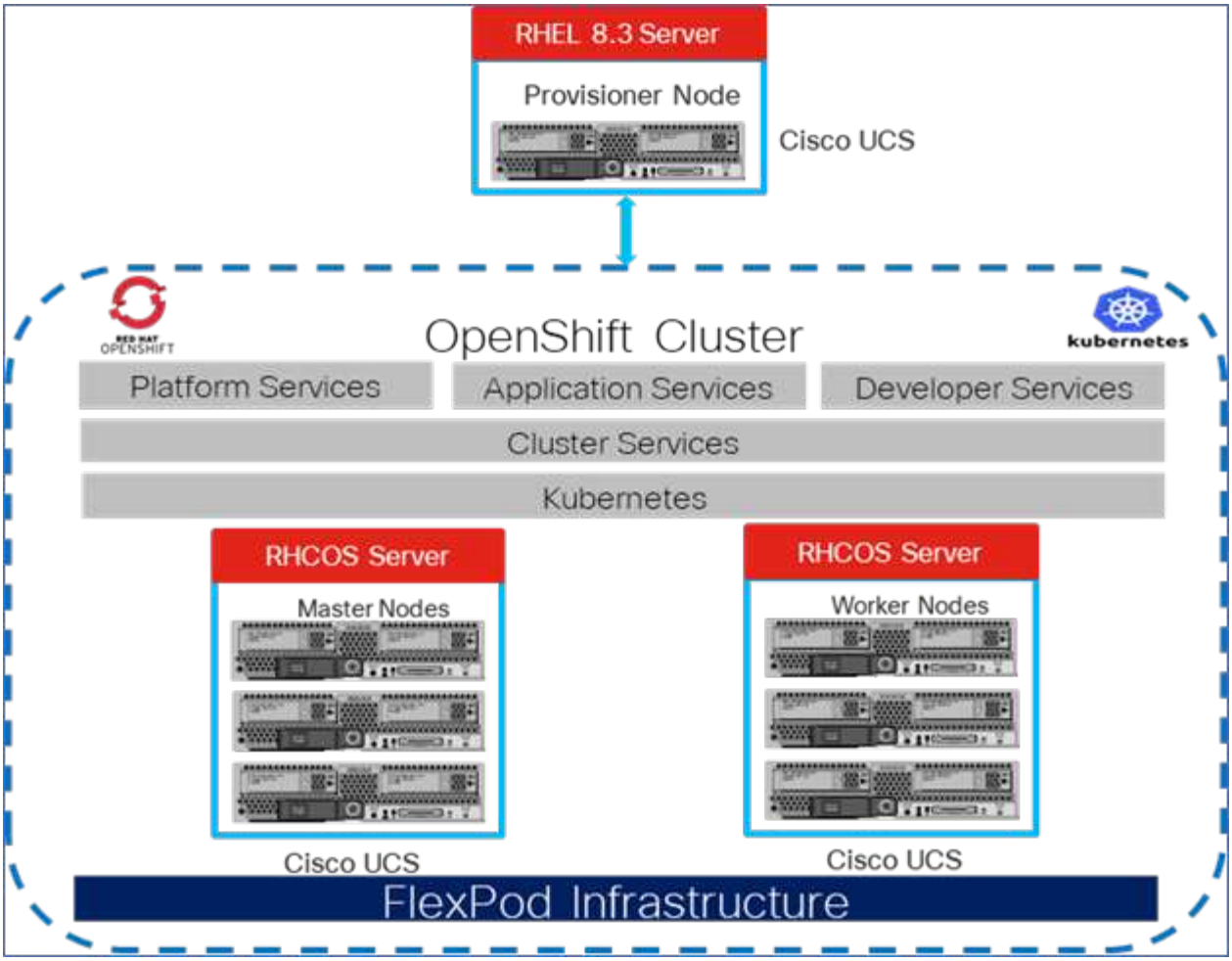
安装和配置

适用于**OpenShift**容器平台**4**的**FlexPod** 裸机安装

"先前版本：解决方案 组件。"

要了解适用于OpenShift容器平台4的FlexPod 裸机设计、部署详细信息以及NetApp Astra Trident安装和配置、请参见 "采用OpenShift的FlexPod Cisco经验证的设计和部署指南(CVD)"。此CVD涵盖使用Ansible的FlexPod 和OpenShift容器平台部署。CVD还提供了有关准备工作节点、Astra Trident安装、存储后端和存储类配置的详细信息、这些配置是部署和配置Astra控制中心的几个前提条件。

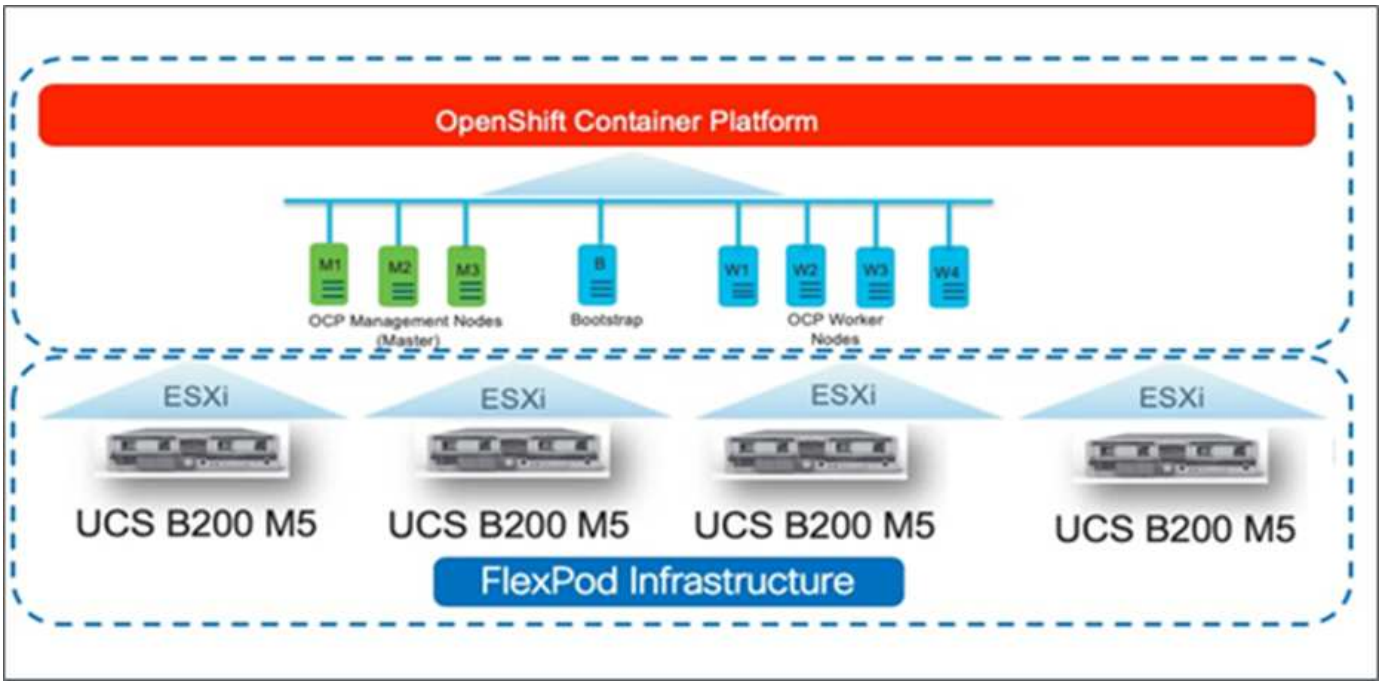
下图显示了FlexPod 上的OpenShift容器平台4裸机。



VMware安装上的适用于OpenShift容器平台4的FlexPod

有关在运行VMware vSphere的FlexPod 上部署Red Hat OpenShift容器平台4的详细信息、请参见 "适用于OpenShift容器平台的FlexPod 数据中心4."。

下图显示了vSphere上适用于OpenShift容器平台4的FlexPod。

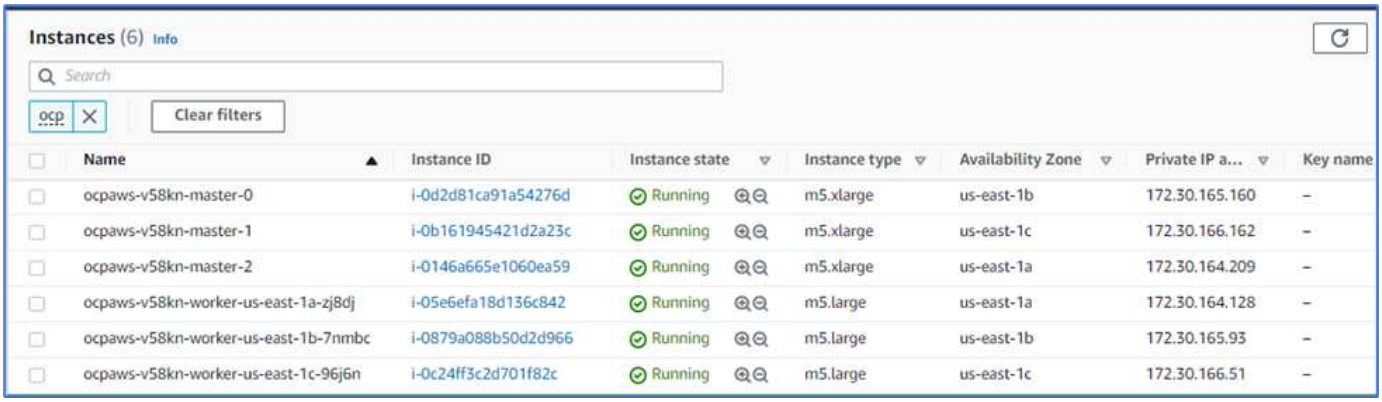


"接下来：在AWS上运行Red Hat OpenShift。"

AWS上的Red Hat OpenShift

"先前版本：适用于OpenShift容器平台4的FlexPod 裸机安装。"

AWS上会部署一个单独的自管理OpenShift容器平台4集群作为灾难恢复站点。主节点和工作节点跨越三个可用性区域、以实现高可用性。



Instances (6) Info

Search

ocp | Clear filters

Name	Instance ID	Instance state	Instance type	Availability Zone	Private IP a...	Key name
ocpaws-v58kn-master-0	i-0d2d81ca91a54276d	Running	m5.xlarge	us-east-1b	172.30.165.160	–
ocpaws-v58kn-master-1	i-0b161945421d2a23c	Running	m5.xlarge	us-east-1c	172.30.166.162	–
ocpaws-v58kn-master-2	i-0146a665e1060ea59	Running	m5.xlarge	us-east-1a	172.30.164.209	–
ocpaws-v58kn-worker-us-east-1a-zj8dj	i-05e6efa18d136c842	Running	m5.large	us-east-1a	172.30.164.128	–
ocpaws-v58kn-worker-us-east-1b-7nmbc	i-0879a088b50d2d966	Running	m5.large	us-east-1b	172.30.165.93	–
ocpaws-v58kn-worker-us-east-1c-96j6n	i-0c24ff3c2d701f82c	Running	m5.large	us-east-1c	172.30.166.51	–

```
[ec2-user@ip-172-30-164-92 ~]$ oc get nodes
NAME                              STATUS   ROLES    AGE   VERSION
ip-172-30-164-128.ec2.internal    Ready    worker   29m   v1.22.8+f34b40c
ip-172-30-164-209.ec2.internal    Ready    master   36m   v1.22.8+f34b40c
ip-172-30-165-160.ec2.internal    Ready    master   33m   v1.22.8+f34b40c
ip-172-30-165-93.ec2.internal     Ready    worker   30m   v1.22.8+f34b40c
ip-172-30-166-162.ec2.internal    Ready    master   36m   v1.22.8+f34b40c
ip-172-30-166-51.ec2.internal     Ready    worker   28m   v1.22.8+f34b40c
```

OpenShift部署为 "专用集群" 添加到AWS上的现有VPC中。专用OpenShift容器平台集群不会公开外部端点、只能从内部网络访问、并且在Internet上不可见。使用NetApp Cloud Manager部署单节点NetApp Cloud Volumes ONTAP 、它为Astra Trident提供存储后端。

有关在AWS上安装OpenShift的详细信息、请参见 "OpenShift文档"。

"下一步：NetApp Cloud Volumes ONTAP。"

NetApp Cloud Volumes ONTAP

"先前版本：AWS上的Red Hat OpenShift。"

NetApp Cloud Volumes ONTAP 实例部署在AWS上、并用作Astra Trident的后端存储。在添加Cloud Volumes ONTAP 工作环境之前、必须先部署连接器。如果您尝试在没有连接器的情况下创建首个Cloud Volumes ONTAP 工作环境、Cloud Manager将提示您。要在AWS中部署Connector、请参见 "创建连接器"。

要在AWS上部署Cloud Volumes ONTAP 、请参见 "AWS快速入门"。

部署Cloud Volumes ONTAP 后、您可以在OpenShift容器平台集群上安装Astra Trident并配置存储后端和Snapshot类。

"接下来：在OpenShift容器平台上安装Astra Control Center。"

在**OpenShift**容器平台上安装**Astra Control Center**

"先前版本：NetApp Cloud Volumes ONTAP。"

您可以将Astra控制中心安装在FlexPod 上运行的OpenShift集群上、也可以安装在具有Cloud Volumes ONTAP 存储后端的AWS上。在此解决方案 中、Astra控制中心部署在OpenShift裸机集群上。

可以使用所述的标准过程安装Astra控制中心 "此处" 或从Red Hat OpenShift OperatorHub获取。Astra控制操作员是Red Hat认证的操作员。在此解决方案 中、使用Red Hat OperatorHub安装Astra控制中心。

环境要求

- Astra控制中心支持多个Kubernetes分发版；对于Red Hat OpenShift、支持的版本包括Red Hat OpenShift容器平台4.8或4.9。
- 除了环境和最终用户的应用程序资源要求之外、Astra控制中心还需要以下资源：

组件	要求
存储后端容量	至少500 GB可用
工作节点	至少3个辅助节点、每个节点具有4个CPU核心和12 GB RAM
完全限定域名(FQDN)地址	Astra 控制中心的 FQDN 地址
Astra Trident	已安装并配置 Astra Trident 21.04 或更高版本

组件	要求
入口控制器或负载平衡器	配置入口控制器以使用URL或负载平衡器公开Astra控制中心、以提供IP地址、并将其解析为FQDN

- 您必须具有可将Astra Control Center构建映像推送到的现有私有映像注册表。您需要提供用于上传映像的映像注册表的URL。

> 执行某些工作流时会提取某些映像、并在必要时创建和销毁容器。

- Astra 控制中心要求创建一个存储类并将其设置为默认存储类。Astra 控制中心支持由 Astra Trident 提供的以下 ONTAP 驱动程序：
  - ontap-NAS
  - ontap-nas-flexgroup
  - ontap-san
  - ontap-san-economy.

> 我们假设已部署的OpenShift集群安装了Astra Trident并配置了ONTAP 后端、同时还定义了默认存储类。

- 对于OpenShift环境中的应用程序克隆、Astra Control Center需要允许OpenShift挂载卷并更改文件所有权。要修改ONTAP 导出策略以允许执行这些操作、请运行以下命令：

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

> 要将第二个OpenShift操作环境添加为托管计算资源、请确保已启用Astra Trident卷快照功能。要使用Astra Trident启用和测试卷快照、请参见官方信息 "Astra Trident说明"。

- 答 "VolumeSnapClass" 应在管理应用程序的所有Kubernetes集群上进行配置。这也可能包括安装了Astra控制中心的K8s集群。Astra控制中心可以管理运行该控制中心的K8s集群上的应用程序。

应用程序管理要求

- *许可。*要使用Astra控制中心管理应用程序、您需要获得Astra控制中心许可证。
- *命名空间。*命名空间是可由Astra控制中心作为应用程序进行管理的最大实体。您可以选择根据现有命名空间中的应用程序标签和自定义标签筛选出组件、并将部分资源作为应用程序进行管理。
- *存储类。*如果您安装的应用程序明确设置了StorageClass、并且需要克隆该应用程序、则克隆操作的目标集群必须具有最初指定的StorageClass。将显式设置了StorageClass的应用程序克隆到不具有相同StorageClass的集群失败。
- * Kubernetes Resources。*使用非Astra Control捕获的Kubernetes资源的应用程序可能无法提供完整的应用程序数据管理功能。Astra Control可以捕获以下Kubernetes资源：

Kubernetes资源		
ClusterRole	ClusterRoleBinding.	配置映射
自定义资源定义	自定义资源	cronjob
DemonSet	HorizontalPodAutoscaler	传入
DeploymentConfig	MutatingWebhook	PersistentVolumeClaim
POD	PodDisruptionBuget	播客模板
网络策略	ReplicaSet	Role
RoleBinding.	路由	机密
验证 Webhook		

使用 **OpenShift OperatorHub** 安装 **Astra** 控制中心

以下操作步骤 将使用Red Hat OperatorHub安装Astra控制中心。在此解决方案 中、Astra控制中心安装在运行于FlexPod 上的裸机OpenShift集群上。

1. 从下载 Astra 控制中心捆绑包（`Astra-control-center-[version].tar.gz`） "NetApp 支持站点"。
2. 从下载Astra控制中心证书和密钥的.zip文件 "NetApp 支持站点"。
3. 验证捆绑包的签名。

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. 提取Astra映像。

```
tar -vxzf astra-control-center-[version].tar.gz
```

5. 更改为 Astra 目录。

```
cd astra-control-center-[version]
```

6. 将映像添加到本地注册表。

```
For Docker:
docker login [your_registry_path]OR
For Podman:
podman login [your_registry_path]
```

7. 使用相应的脚本加载映像、标记映像并将其推送到本地注册表。

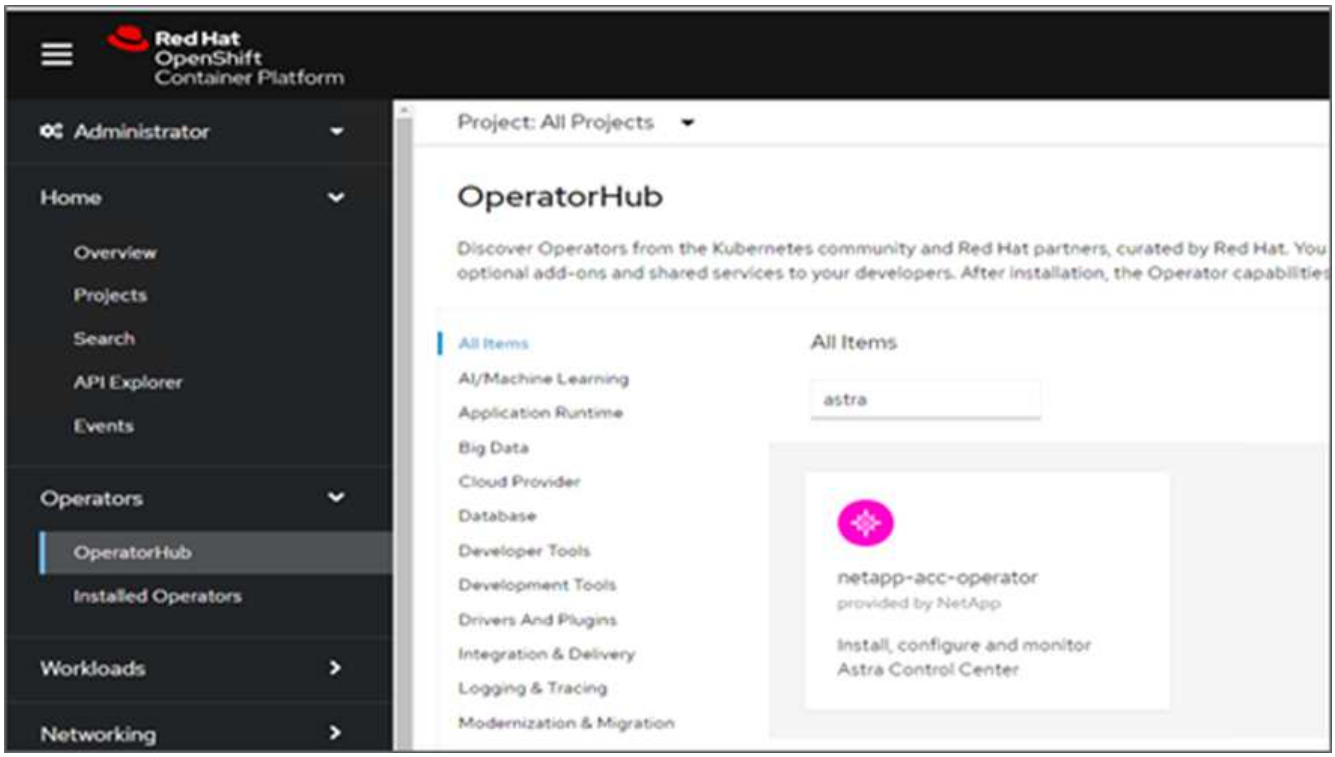
对于 Docker：

```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

对于 Podman：

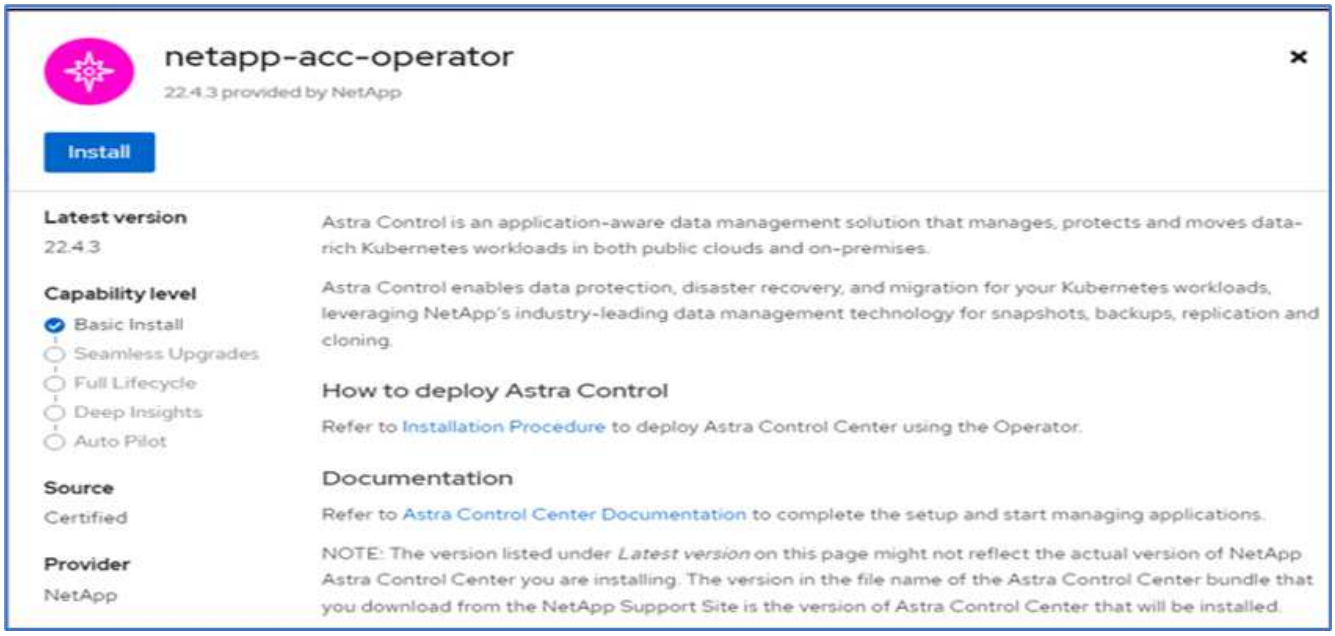
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```

8. 登录到裸机OpenShift集群Web控制台。从侧面菜单中、选择Operators > OperatorHub。输入`Astra`以列出`NetApp-Acc-operator`。

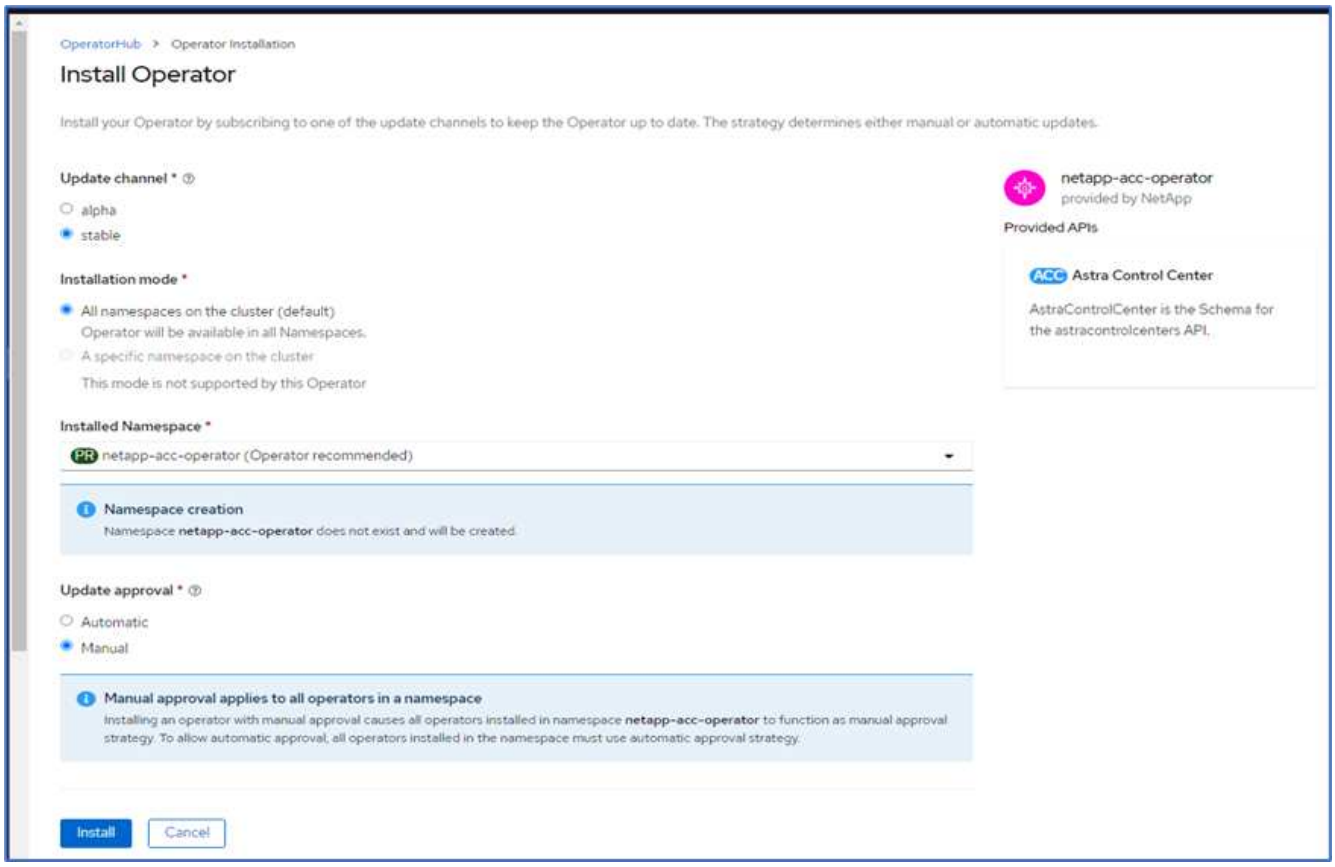


`NetApp-Acc-operator`是一个经过认证的Red Hat OpenShift操作员、并列在OperatorHub目录下。

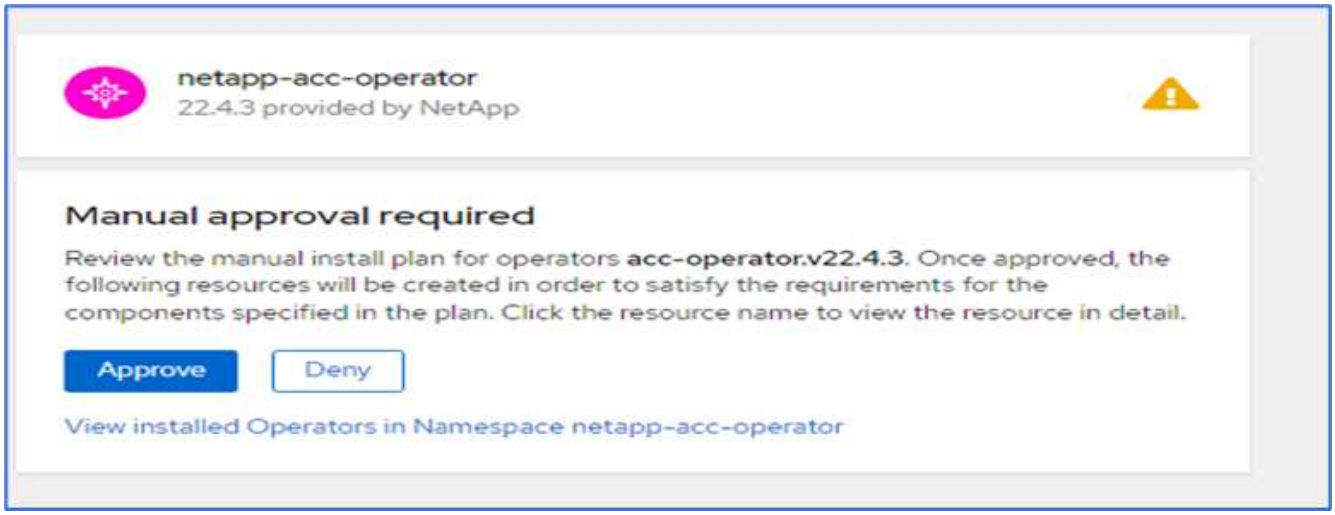
9. 选择`NetApp-Acc-operator`、然后单击安装。



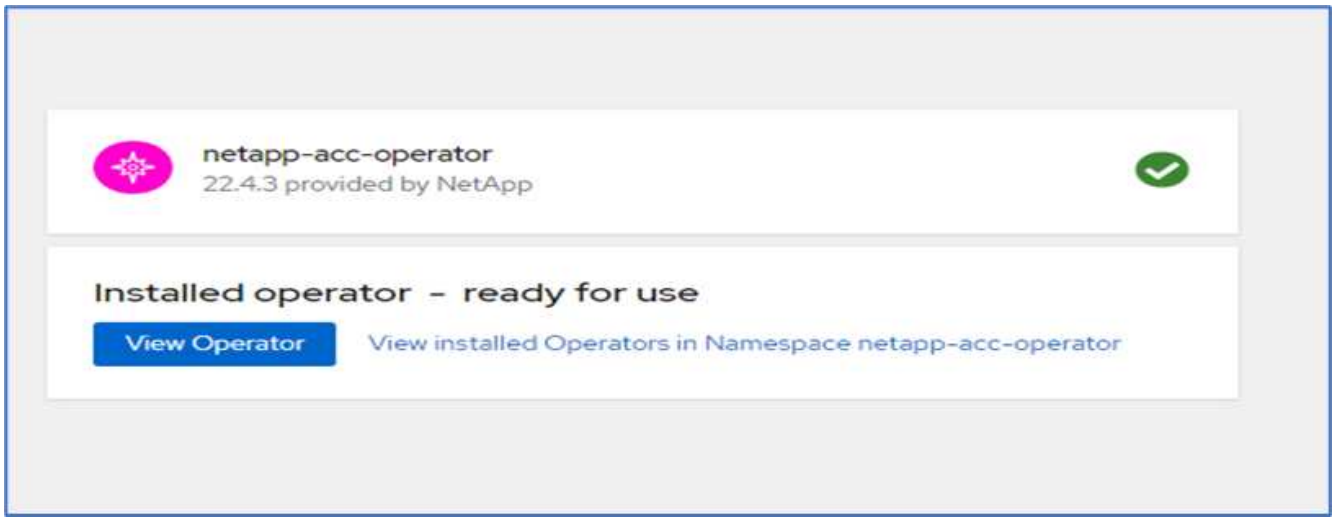
10. 选择相应的选项、然后单击安装。



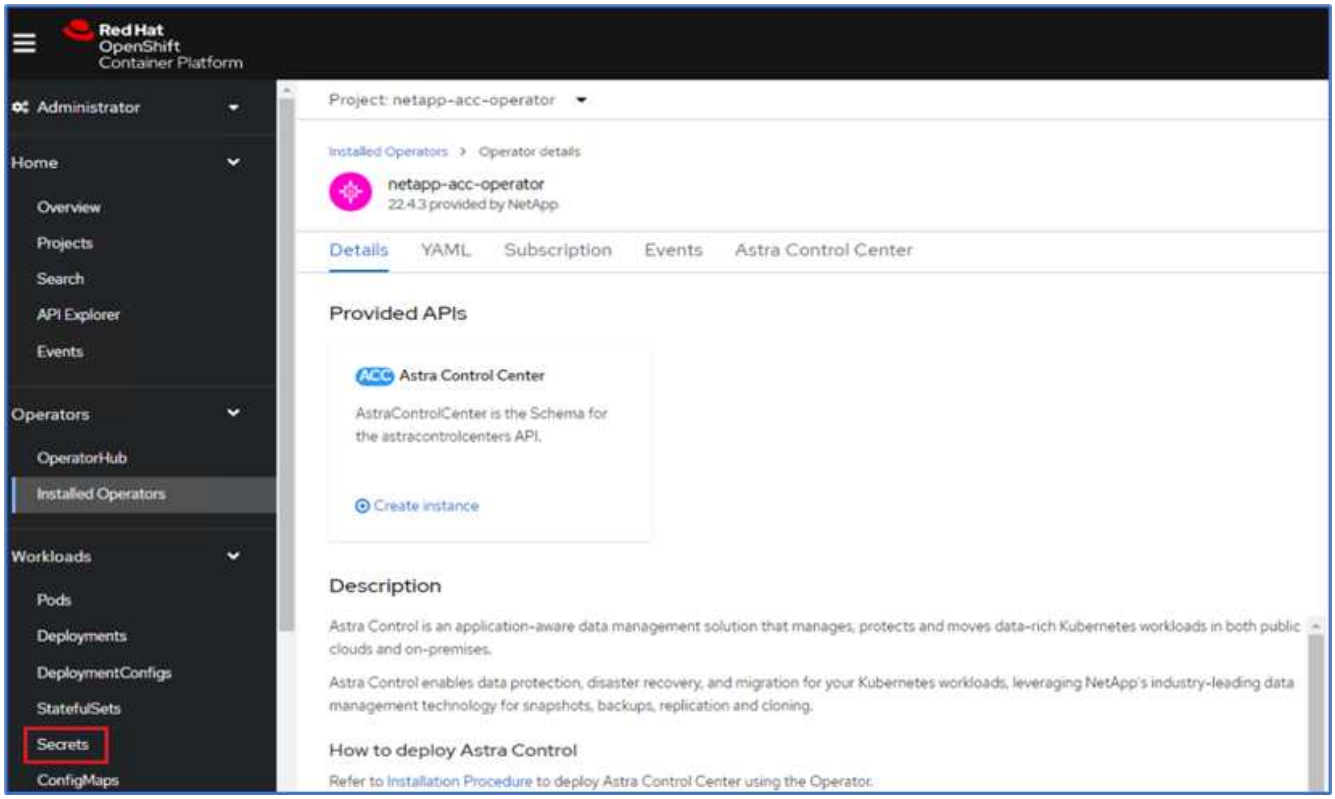
11. 批准安装并等待操作员安装。



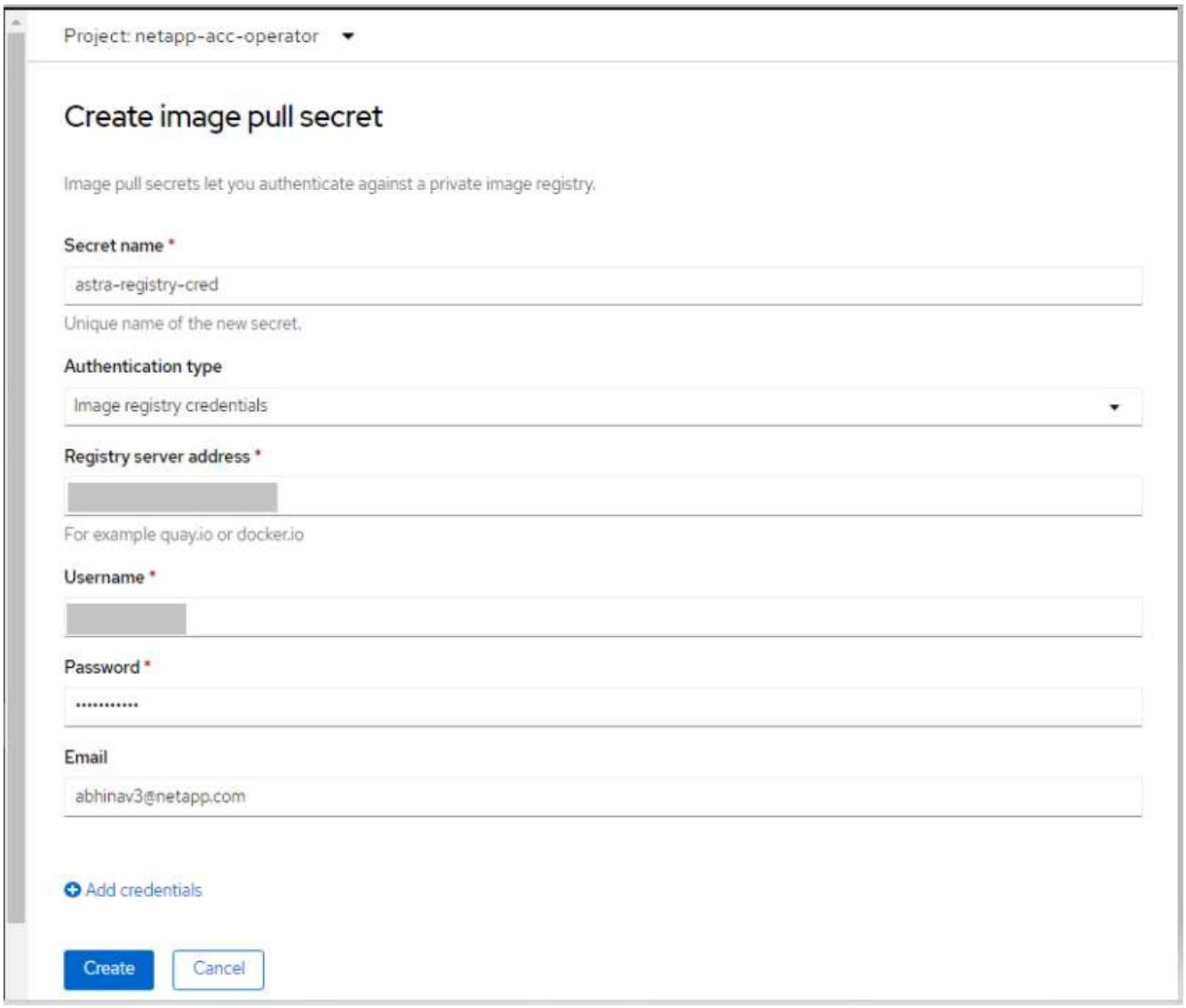
12. 在此阶段、操作员已成功安装并准备就绪、可以使用。单击View Operator开始安装Astra Control Center。



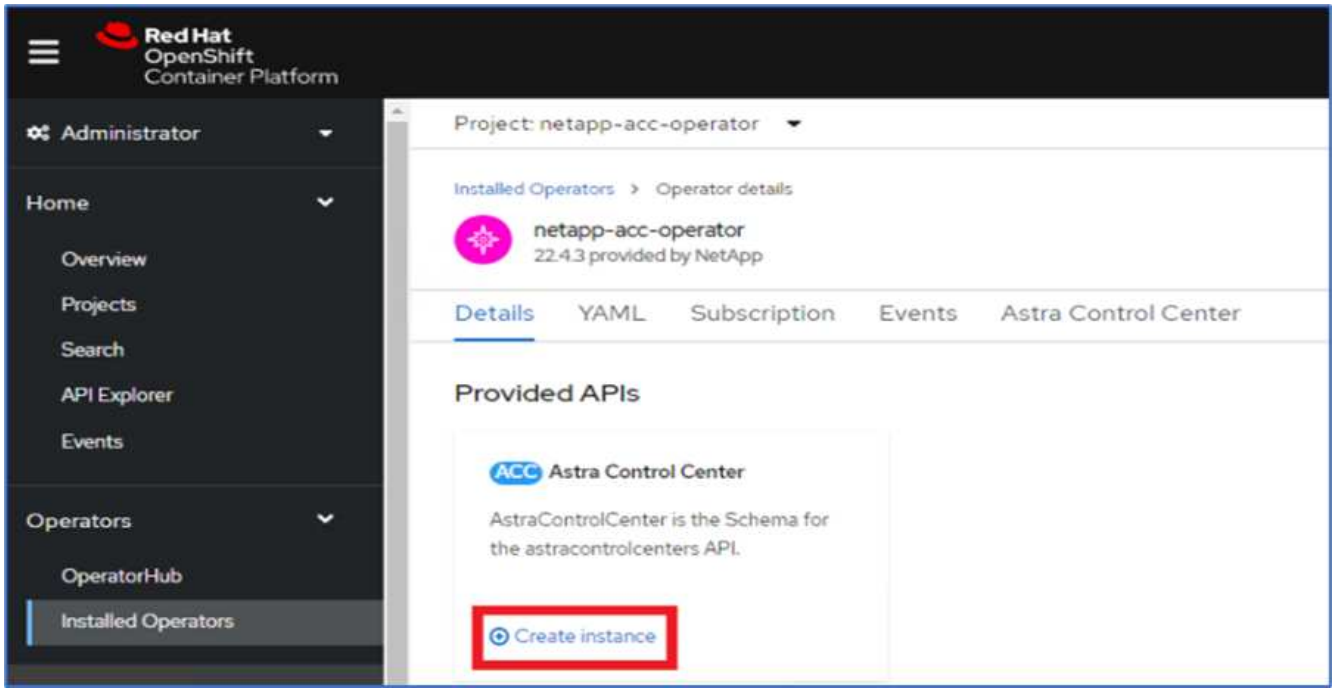
13. 在安装Astra控制中心之前、请创建Pull密钥、以便从先前推送的Docker注册表下载Astra映像。



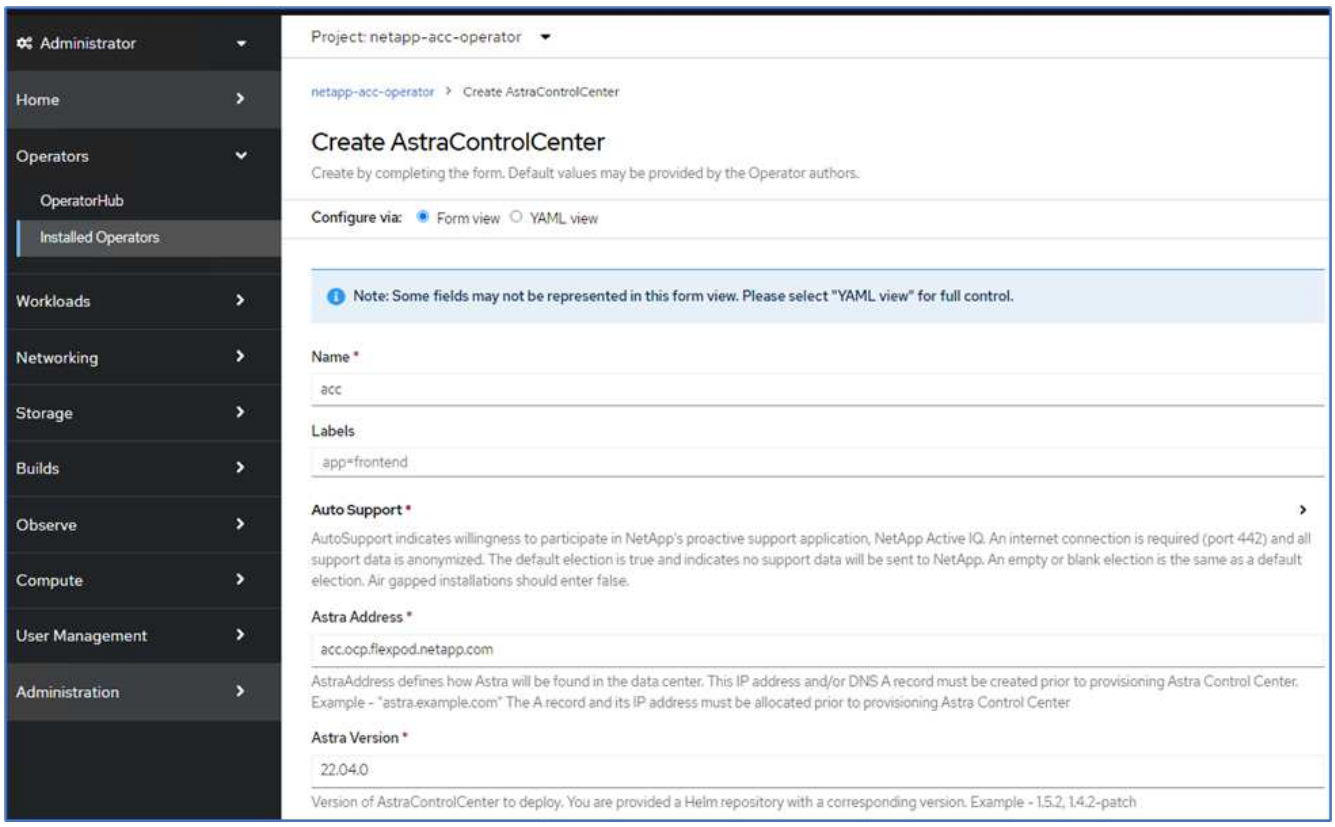
14. 要从Docker私有repod中提取Astra控制中心映像、请在`NetApp-Acc-operator`命名空间中创建一个密钥。此机密名称将在Astra控制中心YAML清单中稍后提供。



15. 从侧面菜单中、选择Operators > Installed Operators、然后单击提供的API部分下的Create Instance。

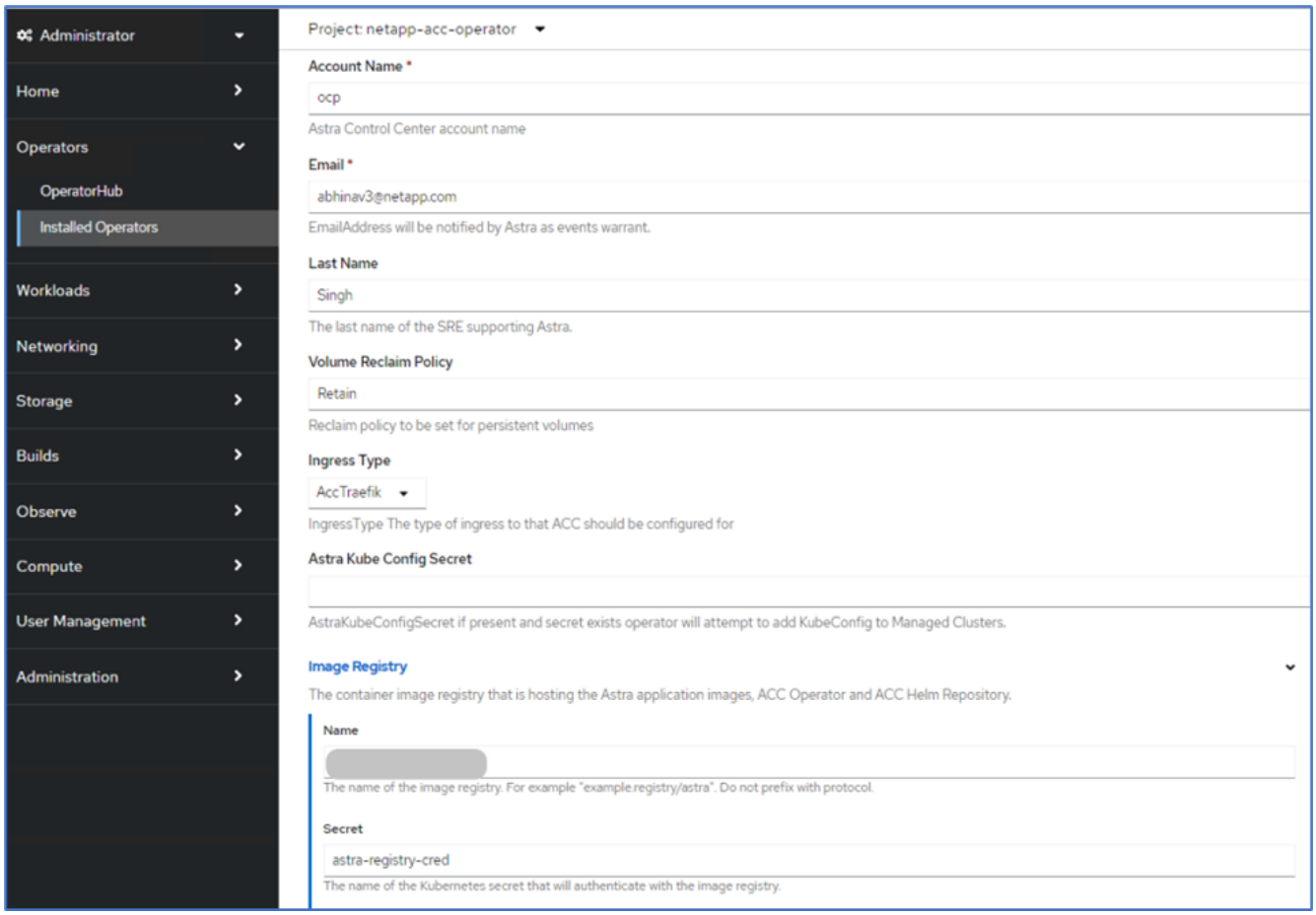


16. 填写创建AstraControlCenter表单。提供名称、Astra地址和Astra版本。



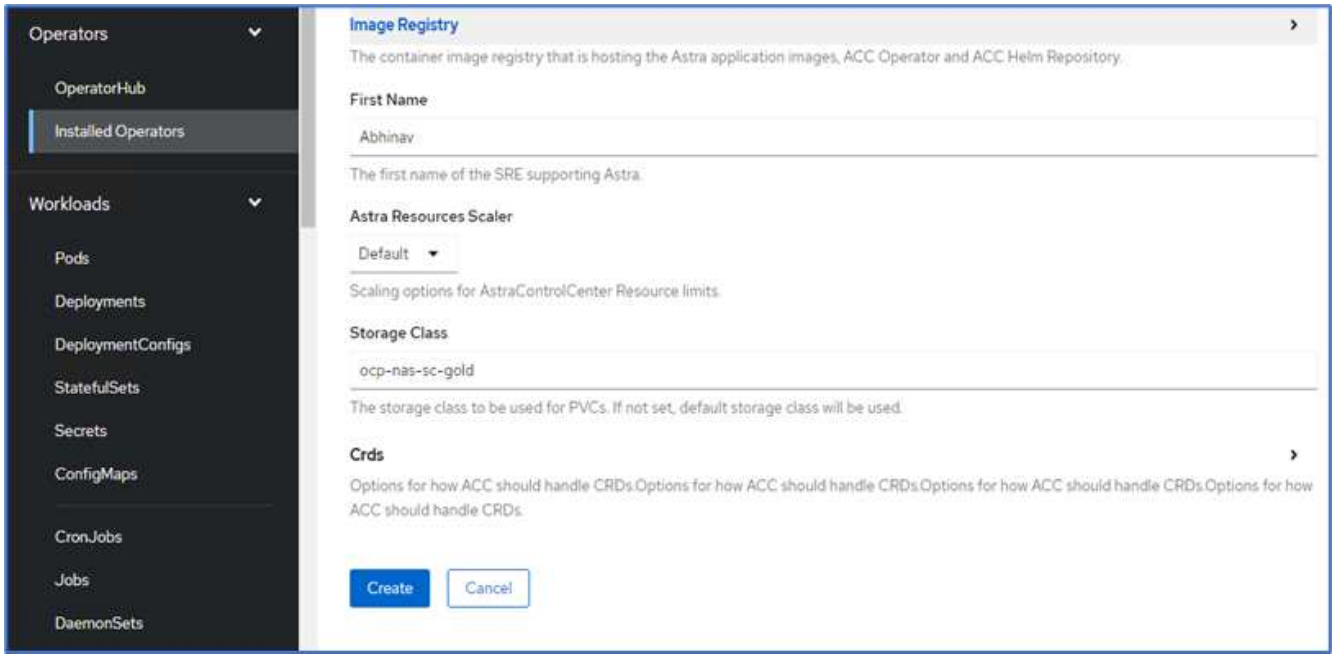
> 在Astra Address下、提供Astra控制中心的FQDN地址。此地址用于访问Astra控制中心Web控制台。FQDN还应解析为可访问的IP网络、并应在DNS中进行配置。

17. 输入帐户名称、电子邮件地址、管理员姓氏、并保留默认卷回收策略。如果使用的是负载平衡器、请将"传入类型"设置为`AccTraefik`。否则、请为`In防护.Controller`选择Generic。在映像注册表下、输入容器映像注册表路径和密钥。

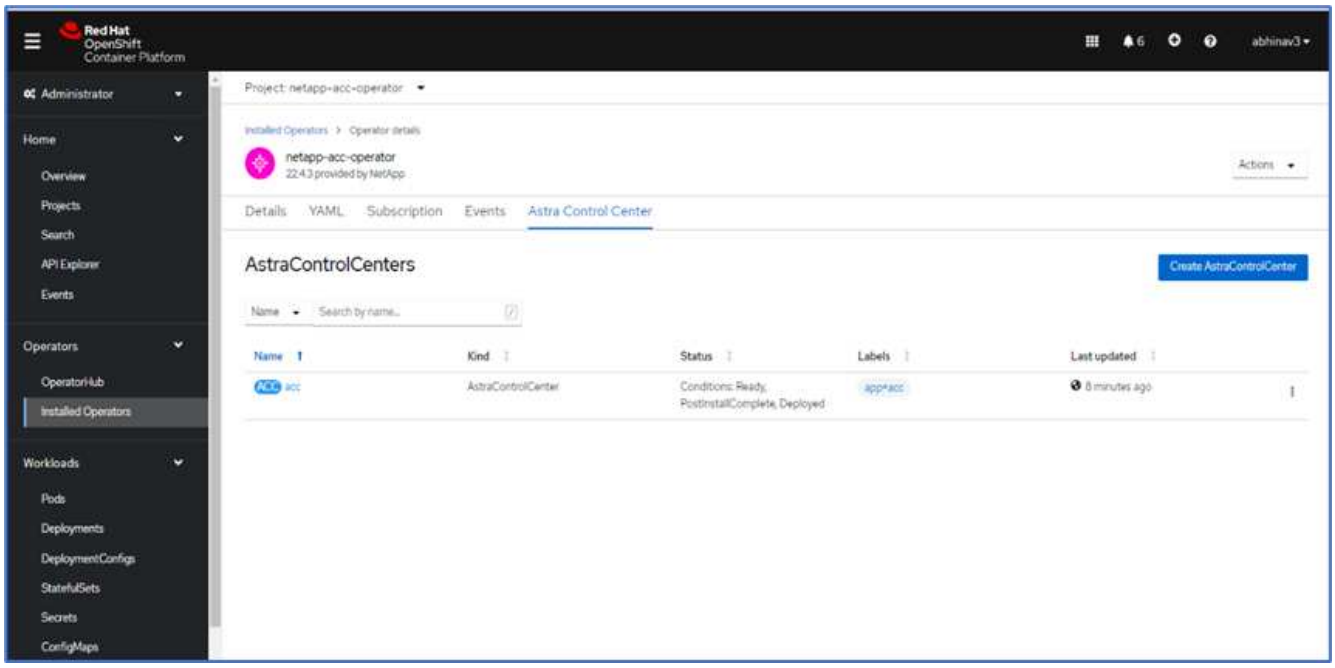


在此解决方案 中、使用了金属负载平衡器。因此、入口类型为AccTraefik。这会将Astra控制中心traefik网关公开为loadbalancer类型的Kubernetes服务。

18. 输入管理员的名字、配置资源扩展并提供存储类。单击创建。



Astra控制中心实例的状态应从"Deploying (部署)"更改为"Ready (就绪)"。



19. 确认所有系统组件均已成功安装、并且所有Pod均已运行。

```
root@abhinav-ansible# oc get pods -n netapp-acc-operator
NAME                                                READY   STATUS
RESTARTS   AGE
acc-helm-repo-77745b49b5-7zg2v                      1/1     Running   0
10m
acc-operator-controller-manager-5c656c44c6-tqnmn    2/2     Running   0
13m
activity-589c6d59f4-x2sfs                           1/1     Running   0
6m4s
api-token-authentication-4q5lj                      1/1     Running   0
5m26s
api-token-authentication-pzptd                      1/1     Running   0
5m27s
api-token-authentication-tbtg6                      1/1     Running   0
5m27s
asup-669df8d49-qps54                                1/1     Running   0
5m26s
authentication-5867c5f56f-dnpp2                     1/1     Running   0
3m54s
bucketservice-85495bc475-5zcc5                      1/1     Running   0
5m55s
cert-manager-67f486bbc6-txhh6                       1/1     Running   0
9m5s
cert-manager-cainjector-75959db744-4l5p5            1/1     Running   0
9m6s
cert-manager-webhook-765556b869-g6wdf               1/1     Running   0
```

```
9m6s
cloud-extension-5d595f85f-txrfl                    1/1     Running   0
5m27s
cloud-insights-service-674649567b-5s4wd            1/1     Running   0
5m49s
composite-compute-6b58d48c69-46vhc                 1/1     Running   0
6m11s
composite-volume-6d447fd959-chnrt                  1/1     Running   0
5m27s
credentials-66668f8ddd-8qc5b                       1/1     Running   0
7m20s
entitlement-fd6fc5c58-wxnmh                        1/1     Running   0
6m20s
features-756bbb7c7c-rgcrm                          1/1     Running   0
5m26s
fluent-bit-ds-278pg                                1/1     Running   0
3m35s
fluent-bit-ds-5pqc6                                1/1     Running   0
3m35s
fluent-bit-ds-8l7cq                                1/1     Running   0
3m35s
fluent-bit-ds-9qbft                                1/1     Running   0
3m35s
fluent-bit-ds-nj475                                1/1     Running   0
3m35s
fluent-bit-ds-x9pd8                                1/1     Running   0
3m35s
graphql-server-698d6f4bf-kftwc                     1/1     Running   0
3m20s
identity-5d4f4c87c9-wjz6c                          1/1     Running   0
6m27s
influxdb2-0                                        1/1     Running   0
9m33s
krakend-657d44bf54-8cb56                           1/1     Running   0
3m21s
license-594bbdc-rghdg                              1/1     Running   0
6m28s
login-ui-6c65fbbbd4-jg8wz                          1/1     Running   0
3m17s
loki-0                                             1/1     Running   0
9m30s
metrics-facade-75575f69d7-hnlk6                    1/1     Running   0
6m10s
monitoring-operator-65dff79cfb-z78vk               2/2     Running   0
3m47s
nats-0                                             1/1     Running   0
```

```
10m
nats-1                                                  1/1     Running   0
9m43s
nats-2                                                  1/1     Running   0
9m23s
nautilus-7bb469f857-4hlc6                               1/1     Running   0
6m3s
nautilus-7bb469f857-vz94m                               1/1     Running   0
4m42s
openapi-8586db4bcd-gwwvf                                1/1     Running   0
5m41s
packages-6bdb949cfb-nrq8l                               1/1     Running   0
6m35s
polaris-consul-consul-server-0                          1/1     Running   0
9m22s
polaris-consul-consul-server-1                          1/1     Running   0
9m22s
polaris-consul-consul-server-2                          1/1     Running   0
9m22s
polaris-mongodb-0                                       2/2     Running   0
9m22s
polaris-mongodb-1                                       2/2     Running   0
8m58s
polaris-mongodb-2                                       2/2     Running   0
8m34s
polaris-ui-5df7687dbd-trcnf                             1/1     Running   0
3m18s
polaris-vault-0                                         1/1     Running   0
9m18s
polaris-vault-1                                         1/1     Running   0
9m18s
polaris-vault-2                                         1/1     Running   0
9m18s
public-metrics-7b96476f64-j88bw                         1/1     Running   0
5m48s
storage-backend-metrics-5fd6d7cd9c-vcb4j                1/1     Running   0
5m59s
storage-provider-bb85ff965-m7qrq                        1/1     Running   0
5m25s
telegraf-ds-4zqgz                                       1/1     Running   0
3m36s
telegraf-ds-cp9x4                                       1/1     Running   0
3m36s
telegraf-ds-h4n59                                       1/1     Running   0
3m36s
telegraf-ds-jnp2q                                       1/1     Running   0
```

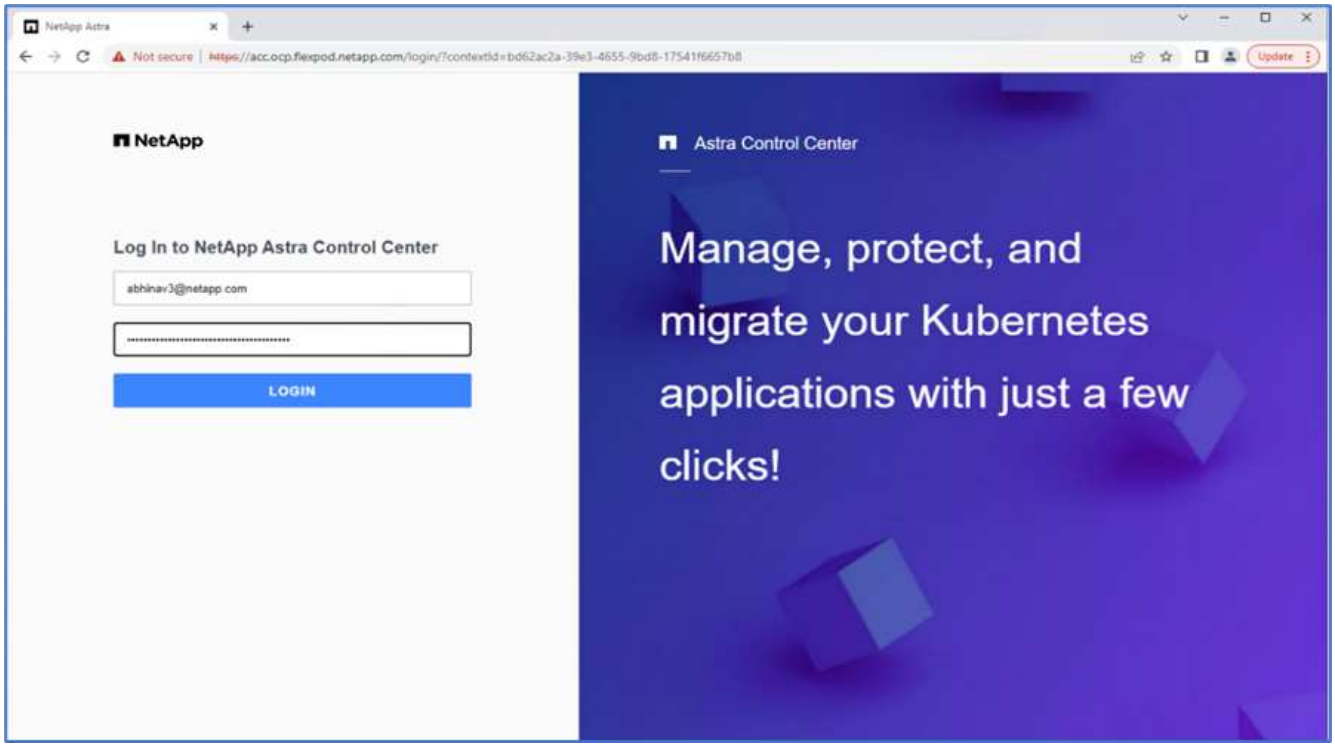
```
3m36s
telegraf-ds-pdz5j                                    1/1     Running   0
3m36s
telegraf-ds-znqtp                                    1/1     Running   0
3m36s
telegraf-rs-rt64j                                    1/1     Running   0
3m36s
telemetry-service-7dd9c74bfc-sfkzt                   1/1     Running   0
6m19s
tenancy-d878b7fb6-wf8x9                              1/1     Running   0
6m37s
traefik-6548496576-5v2g6                             1/1     Running   0
98s
traefik-6548496576-g82pq                             1/1     Running   0
3m8s
traefik-6548496576-psn49                             1/1     Running   0
38s
traefik-6548496576-qrkfd                             1/1     Running   0
2m53s
traefik-6548496576-srs6r                             1/1     Running   0
98s
trident-svc-679856c67-78kbt                          1/1     Running   0
5m27s
vault-controller-747d664964-xmn6c                    1/1     Running   0
7m37s
```

每个POD的状态应为"runned"。部署系统Pod可能需要几分钟的时间。

20. 所有Pod运行时、运行以下命令以检索一次性密码。在输出的YAML版本中、检查`status.deploymentState`字段中的已部署值、然后复制`status.uuid`值。密码为`Acc-`、后跟UUID值。(Acc-UUID)。

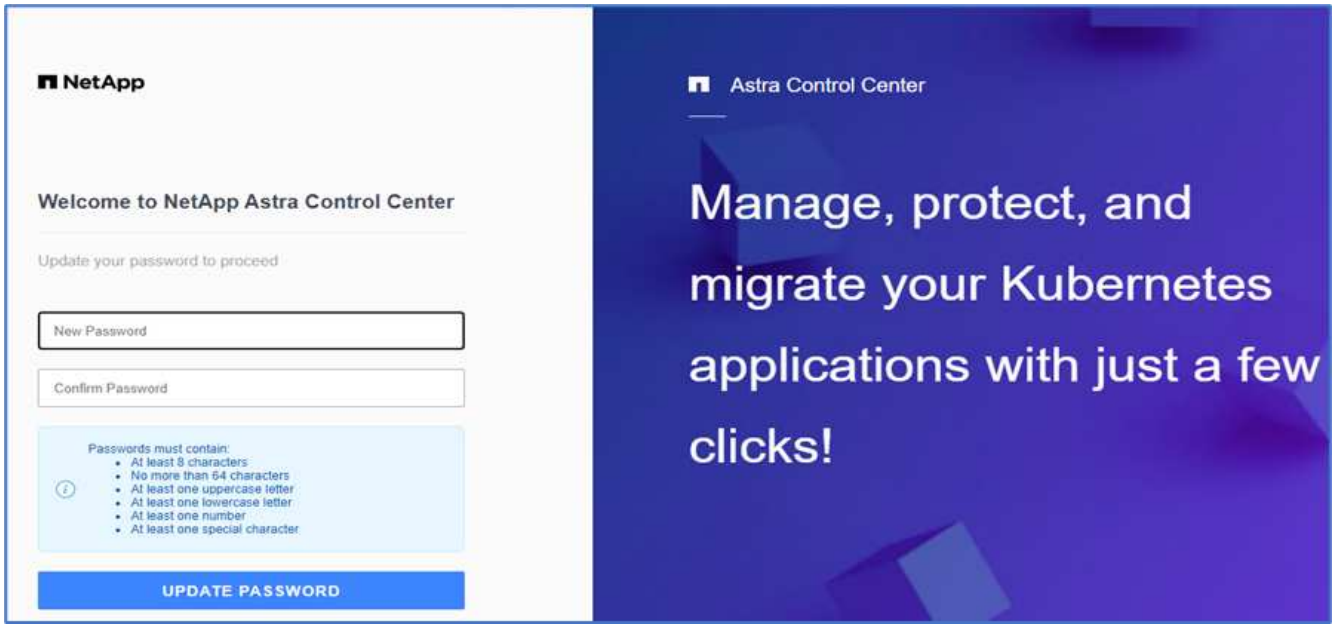
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. 在浏览器中、使用您提供的FQDN导航到URL。
22. 使用默认用户名(即安装期间提供的电子邮件地址)和一次性密码Acc-UUID登录。



如果您输入的密码三次不正确、则管理员帐户将锁定15分钟。

23. 更改密码并继续。

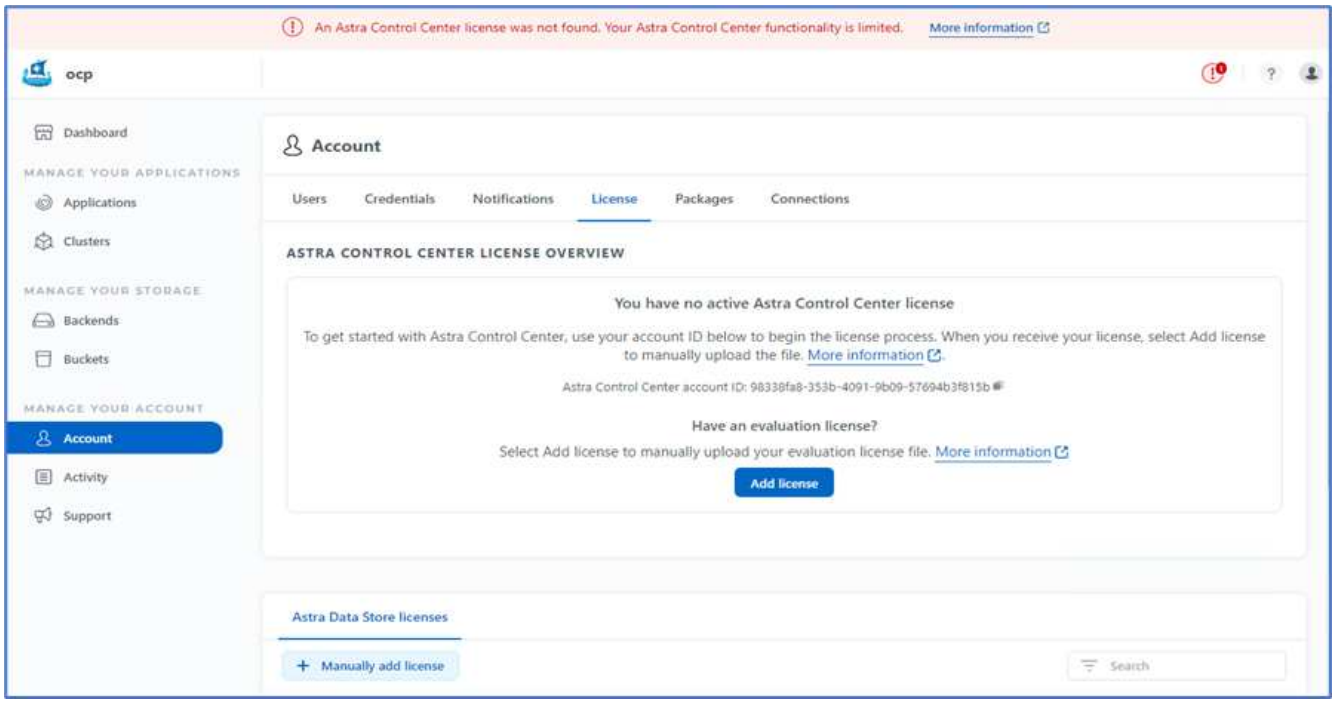


有关Astra控制中心安装的详细信息、请参见 "Astra控制中心安装概述" 页面。

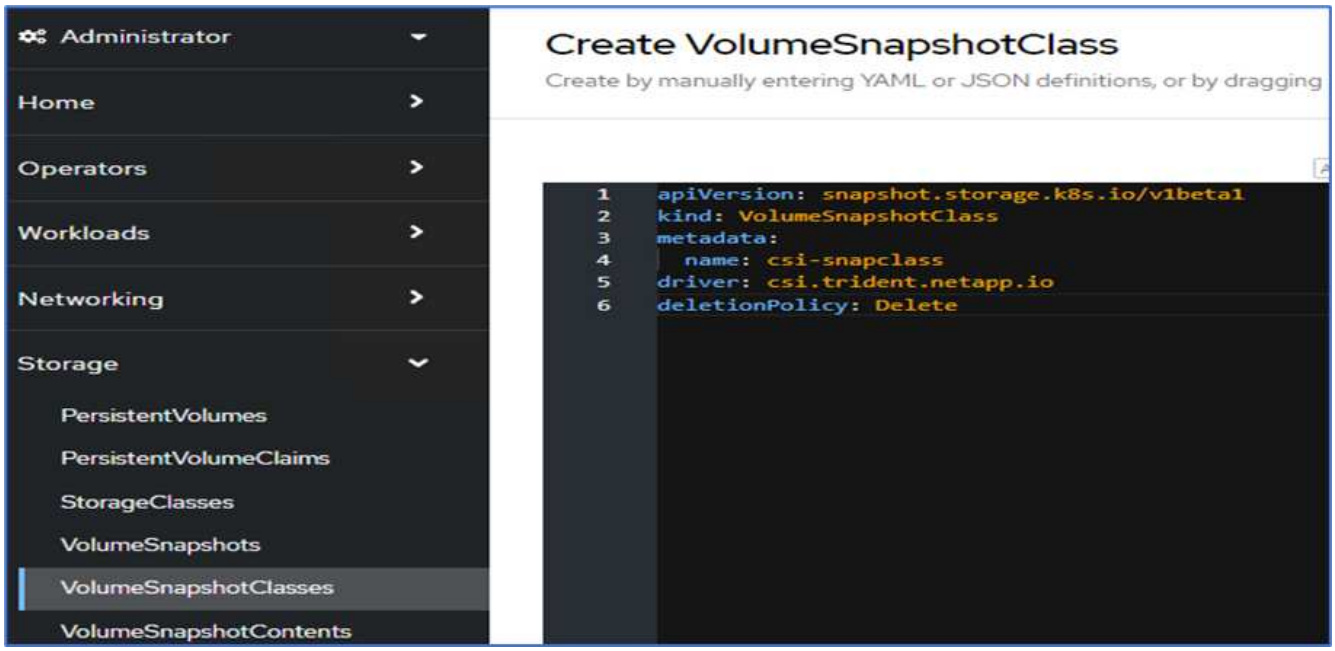
设置 **Astra** 控制中心

安装Astra控制中心后、登录到用户界面、上传许可证、添加集群、管理存储以及添加存储分段。

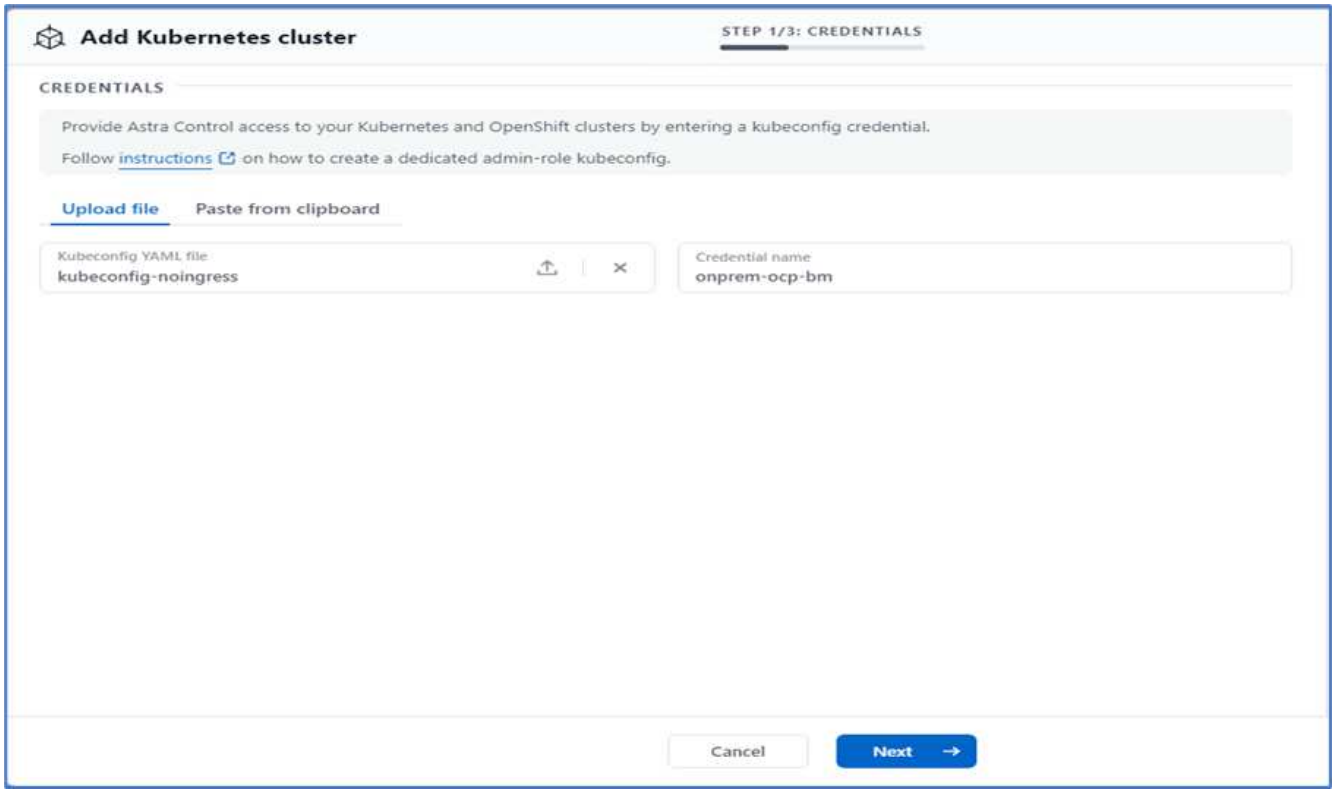
1. 在主页上的Account下、转到License选项卡并选择Add License以上传Astra许可证。



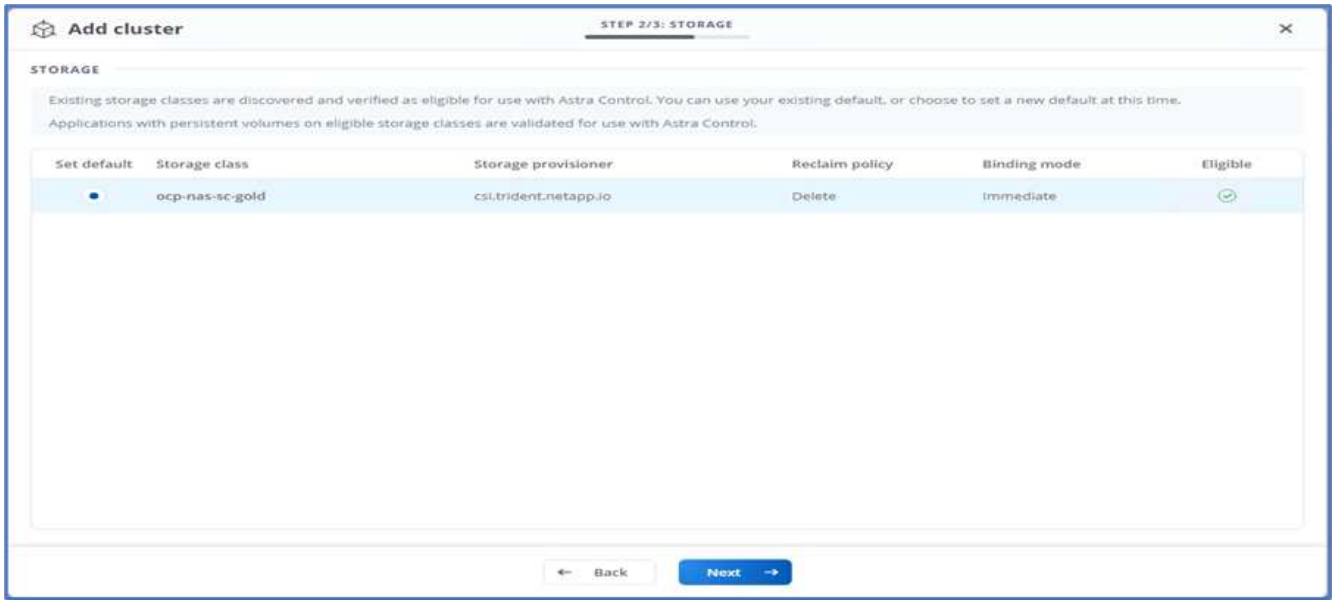
2. 在添加OpenShift集群之前、请从OpenShift Web控制台创建Astra Trident卷快照类。卷快照类配置了`csi.trident.netapp.io`驱动程序。



3. 要添加Kubernetes集群、请转到主页上的Clusters、然后单击Add Kubernetes Cluster。然后上传集群的`kubeconfig`文件并提供凭据名称。单击下一步。



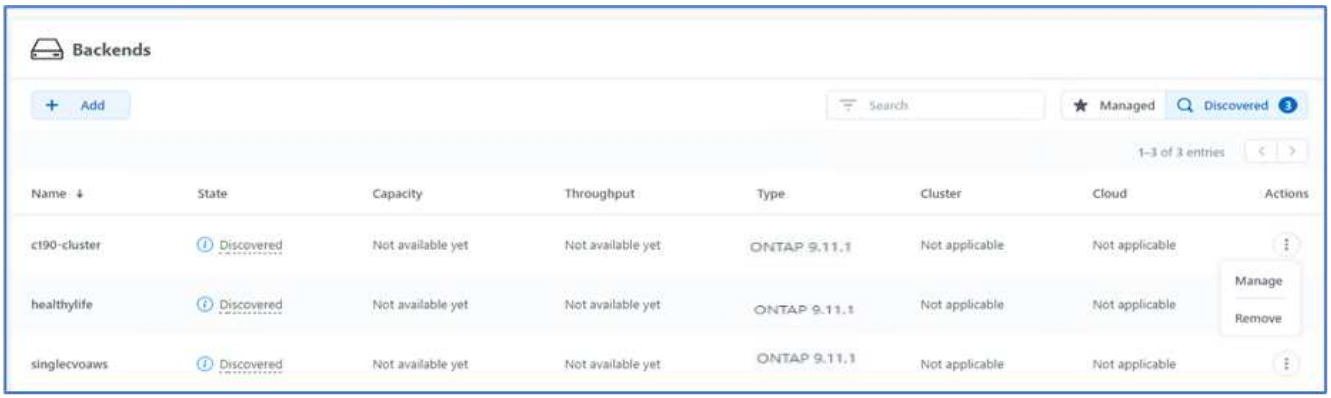
4. 系统会自动发现现有存储类。选择默认存储类、单击下一步、然后单击添加集群。



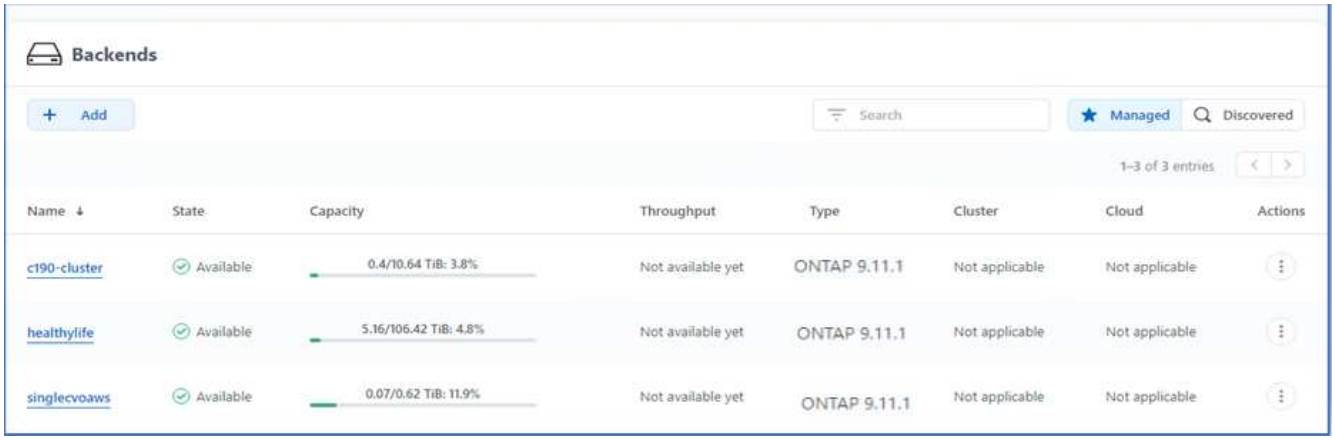
5. 只需几分钟即可添加集群。要添加其他OpenShift容器平台集群、请重复步骤1–4。

> 要将其他OpenShift操作环境添加为托管计算资源、请确保使用Astra Trident "VolumeSnapshotClass对象" 已定义。

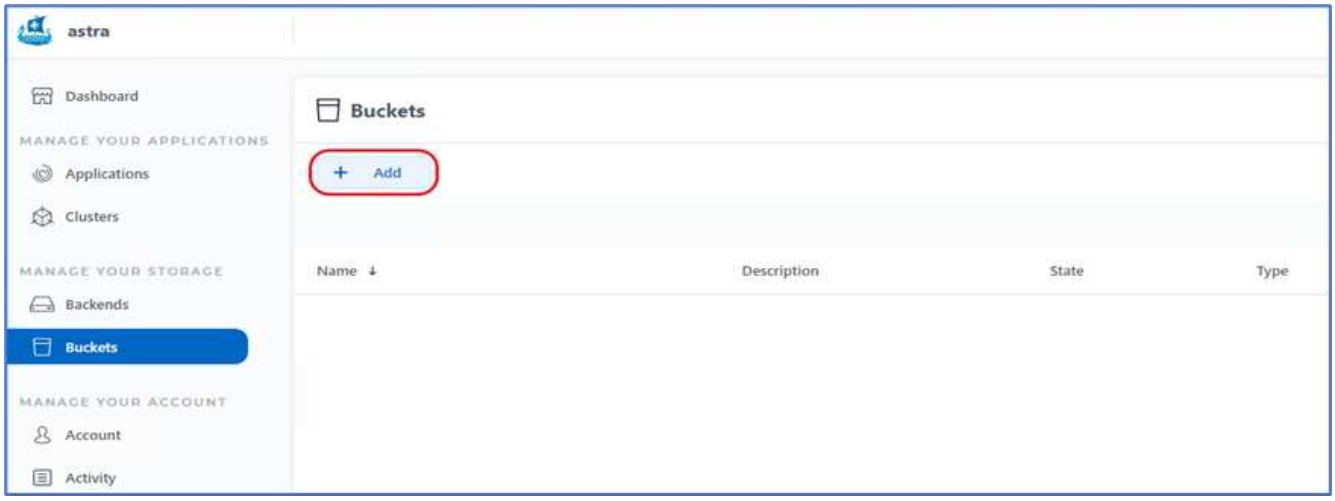
6. 要管理存储、请转至后端、单击"Actions against the backend that you would like to manage"下的三个点。单击Manage。



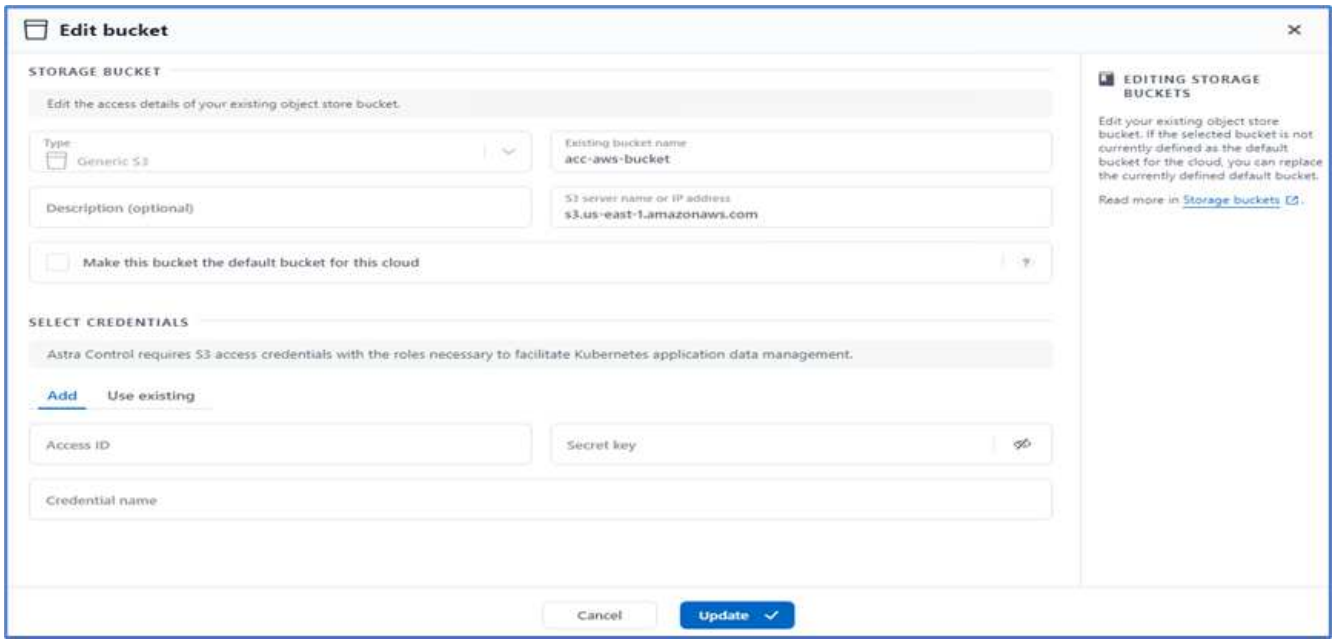
7. 提供ONTAP 凭据、然后单击下一步。查看相关信息、然后单击受管。后端应类似于以下示例。



8. 要将存储分段添加到Astra Control、请选择Bucket并单击Add。

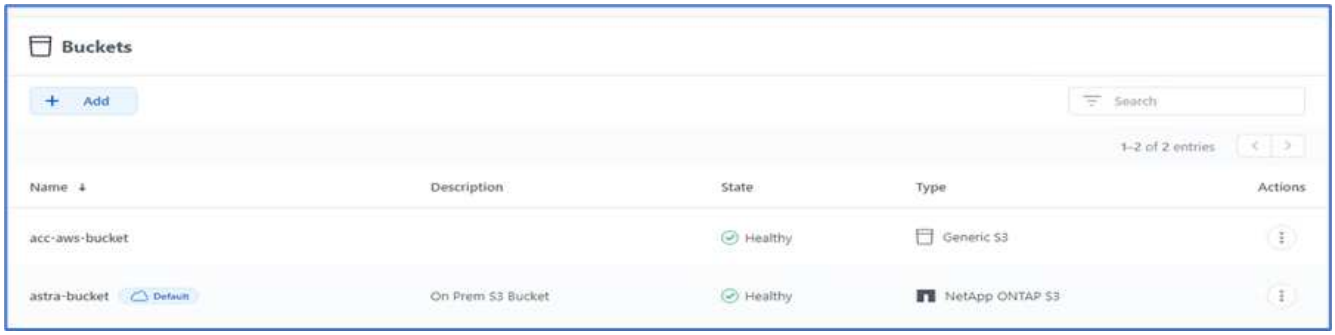


9. 选择存储分段类型并提供存储分段名称、S3服务器名称或IP地址和S3凭据。单击更新。



在此解决方案 中、AWS S3和ONTAP S3存储分段均已使用。您也可以使用StorageGRID。

存储分段状态应为运行状况良好。



作为向Astra控制中心注册Kubernetes集群以实现应用程序感知型数据管理的一部分、Astra Control会自动创建角色绑定和NetApp监控命名空间、以便从应用程序Pod和工作节点收集指标和日志。将一个受支持的基于ONTAP的存储类设置为默认值。

你先请 "将集群添加到 Astra Control 管理中"、您可以在集群上安装应用程序(在Astra Control之外)、然后转到Astra Control中的应用程序页面来管理这些应用程序及其资源。有关使用Astra管理应用程序的详细信息、请参见 "应用程序管理要求"。

"接下来：解决方案 验证概述。"

解决方案验证

概述

"先前版本：在OpenShift容器平台上安装Astra Control Center。"

在本节中、我们将回顾解决方案 以及一些使用情形：

- 将有状态应用程序从远程备份还原到云中运行的另一个OpenShift集群。
- 将有状态应用程序还原到OpenShift集群中的同一命名空间。
- 通过从一个FlexPod 系统(OpenShift容器平台裸机)克隆到另一个FlexPod 系统(VMware上的OpenShift容器平台)来实现应用程序移动性。

值得注意的是、此解决方案 仅验证了少数使用情形。此验证并不代表Astra控制中心的全部功能。

"接下来：使用远程备份恢复应用程序。"

通过远程备份恢复应用程序

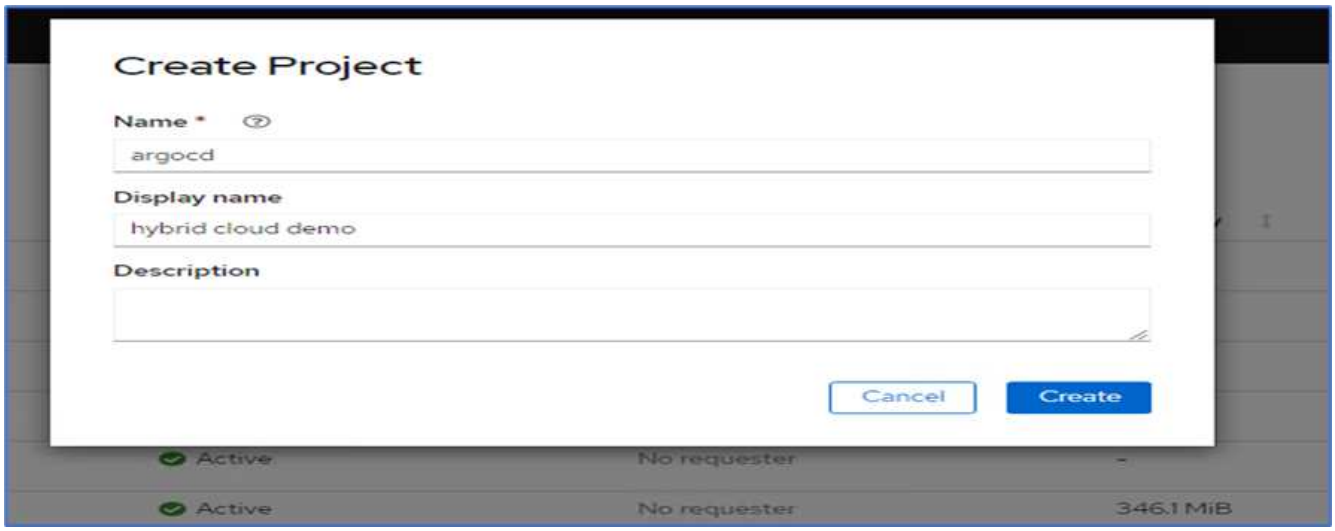
"上一步：解决方案 验证概述。"

借助Astra、您可以进行完整的应用程序一致的备份、用于将应用程序及其数据还原到在内部数据中心或公有 云中运行的不同Kubernetes集群。

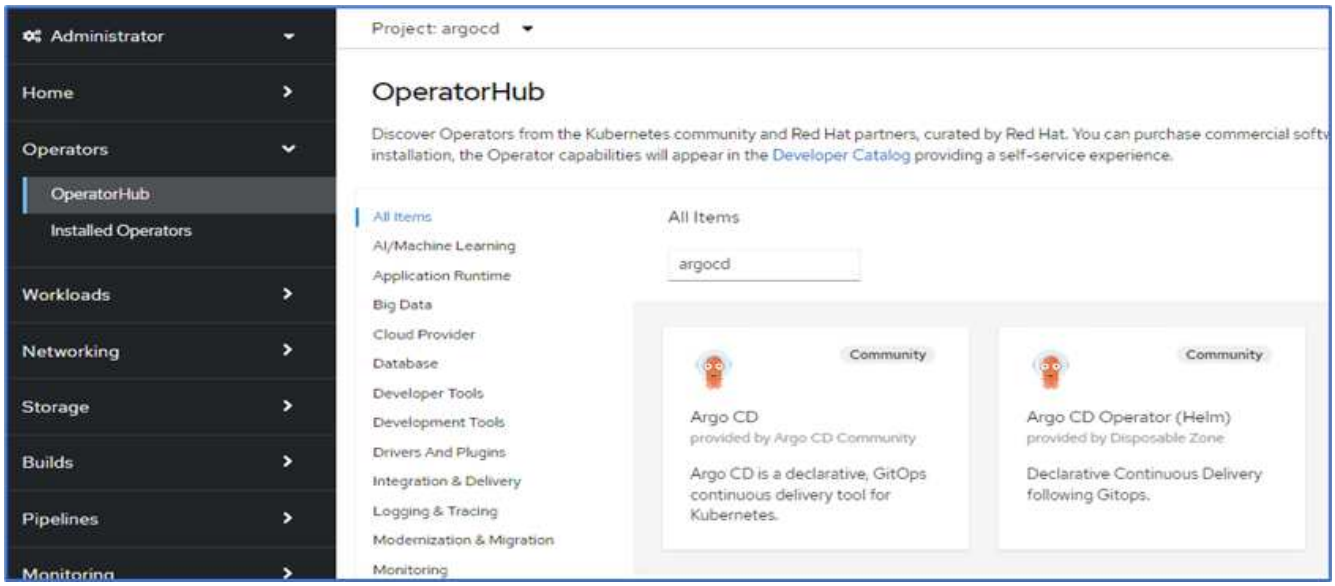
要验证应用程序恢复是否成功、请模拟FlexPod 系统上运行的应用程序的内部故障、并使用远程备份将应用程序还原到云中运行的K8s集群。

此示例应用程序是一个使用MySQL作为数据库的价目表应用程序。为了实现部署自动化、我们使用了 "Argo CD" 工具。Argo CD是一款适用于Kubernetes的声明性GitOps持续交付工具。

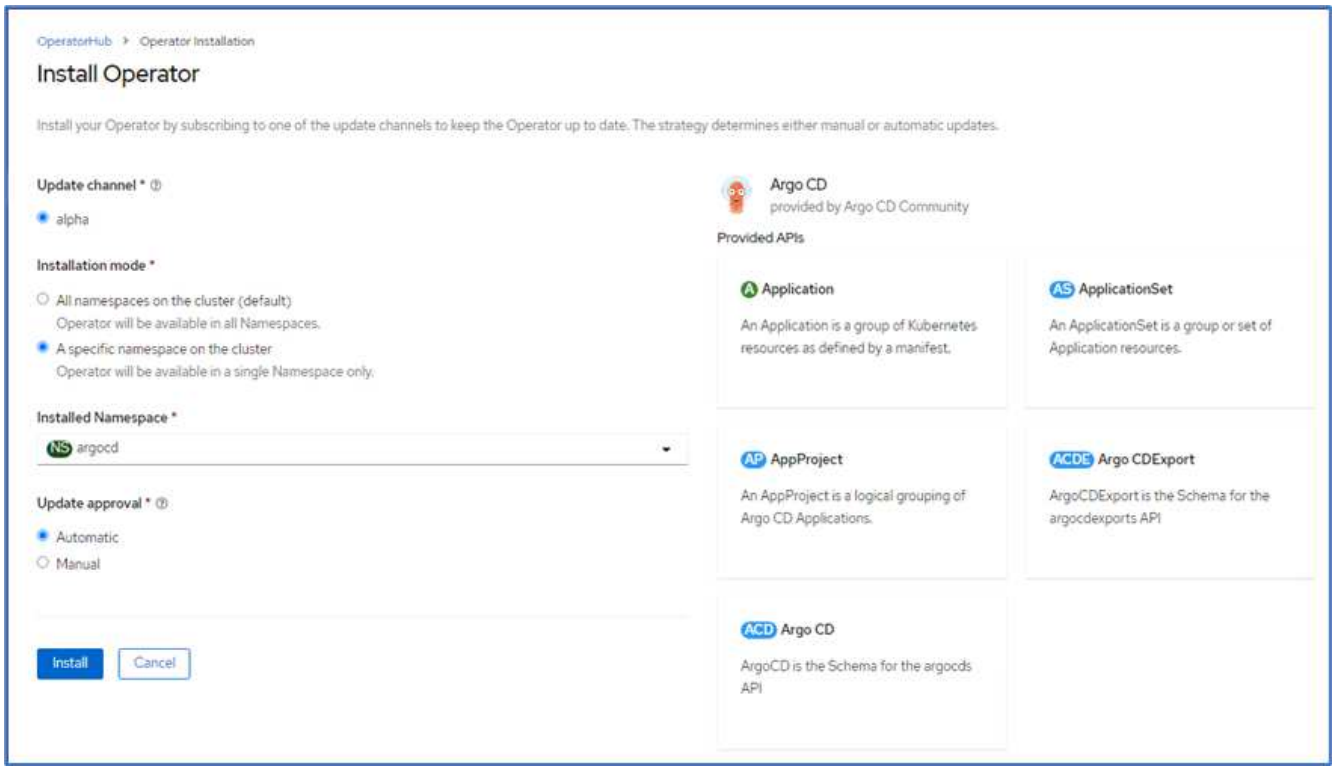
1. 登录到内部OpenShift集群并创建一个名为`argocd`的新项目。



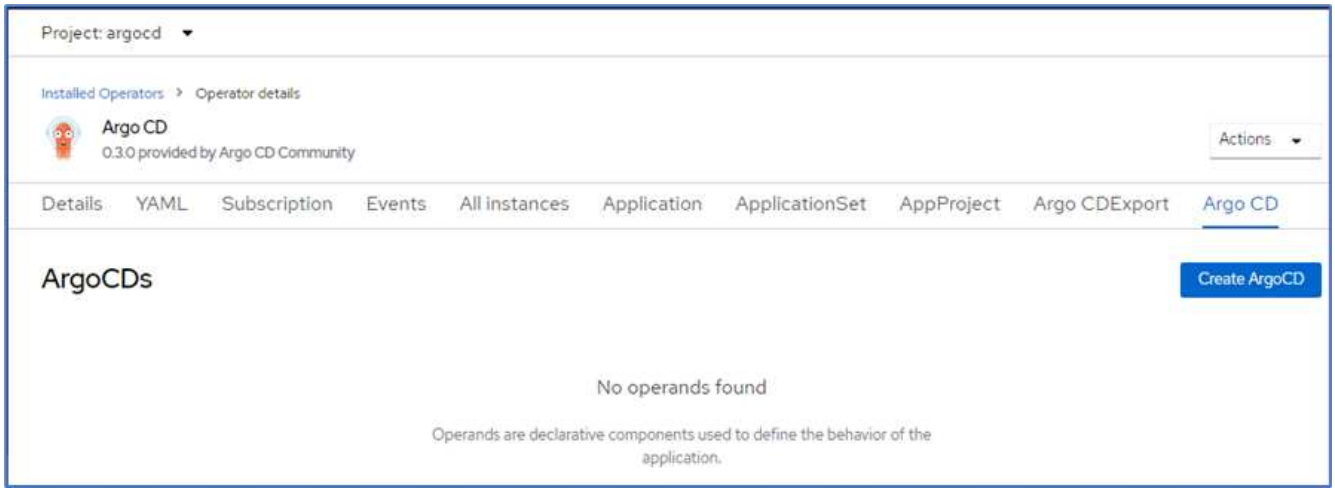
2. 在OperatorHub中、搜索`argocd`并选择Argo CD operator。



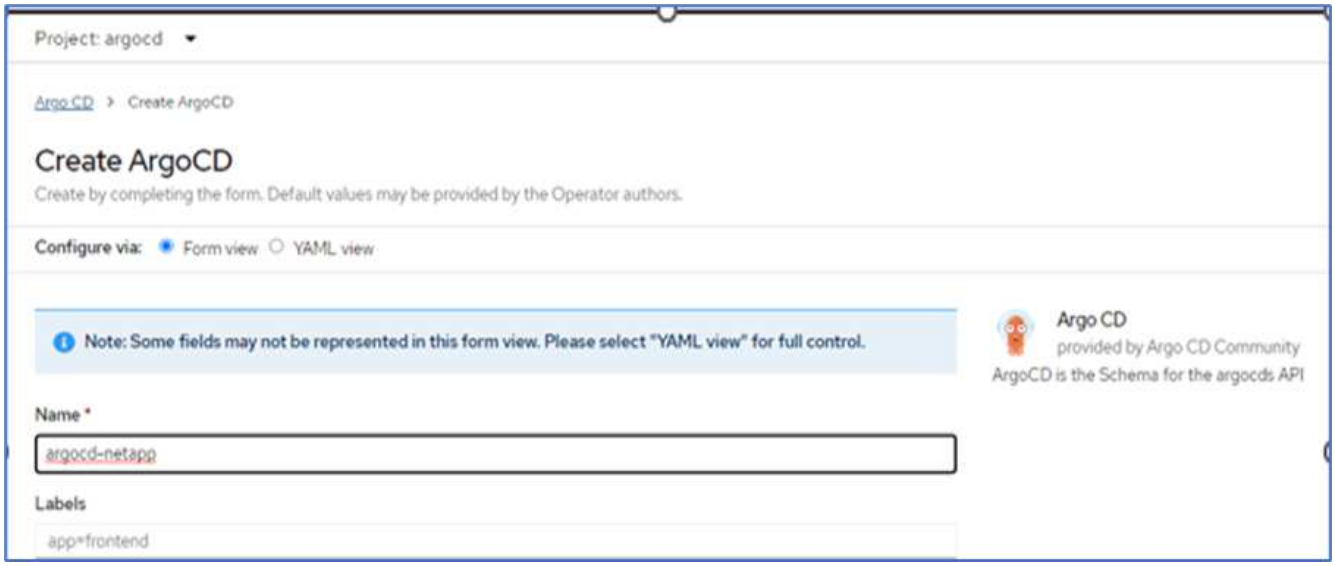
3. 在`argocd`命名空间中安装操作符。



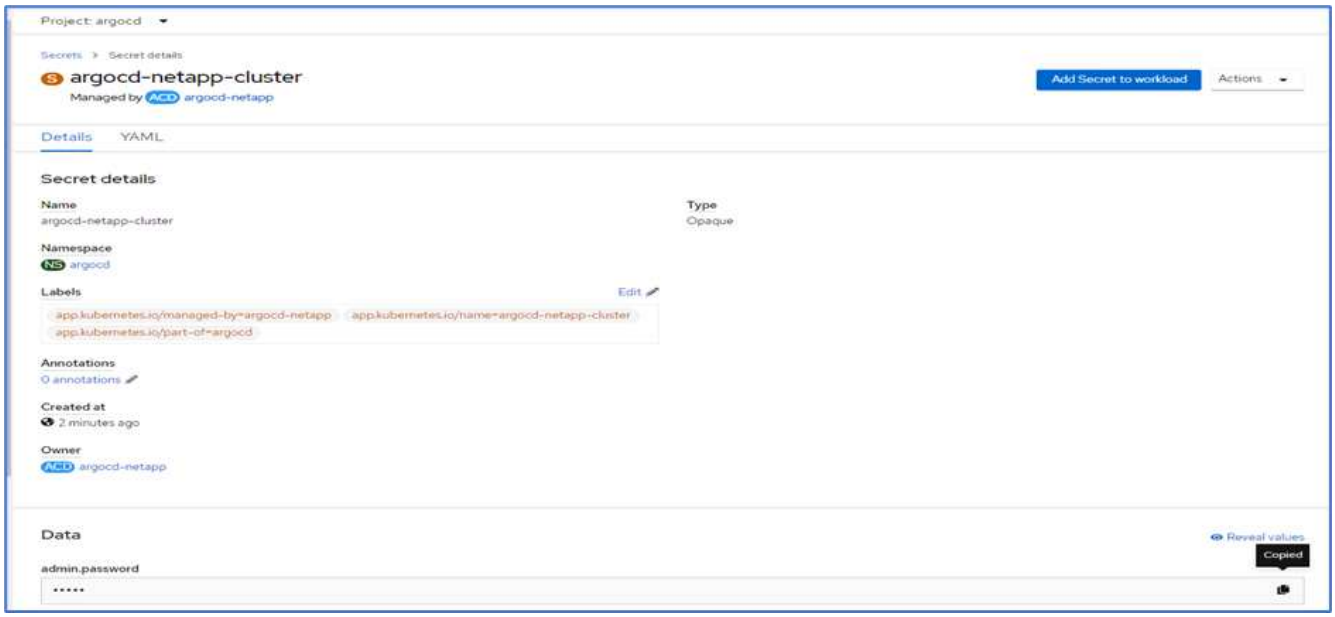
4. 转到运算符并单击创建ArgoCD。



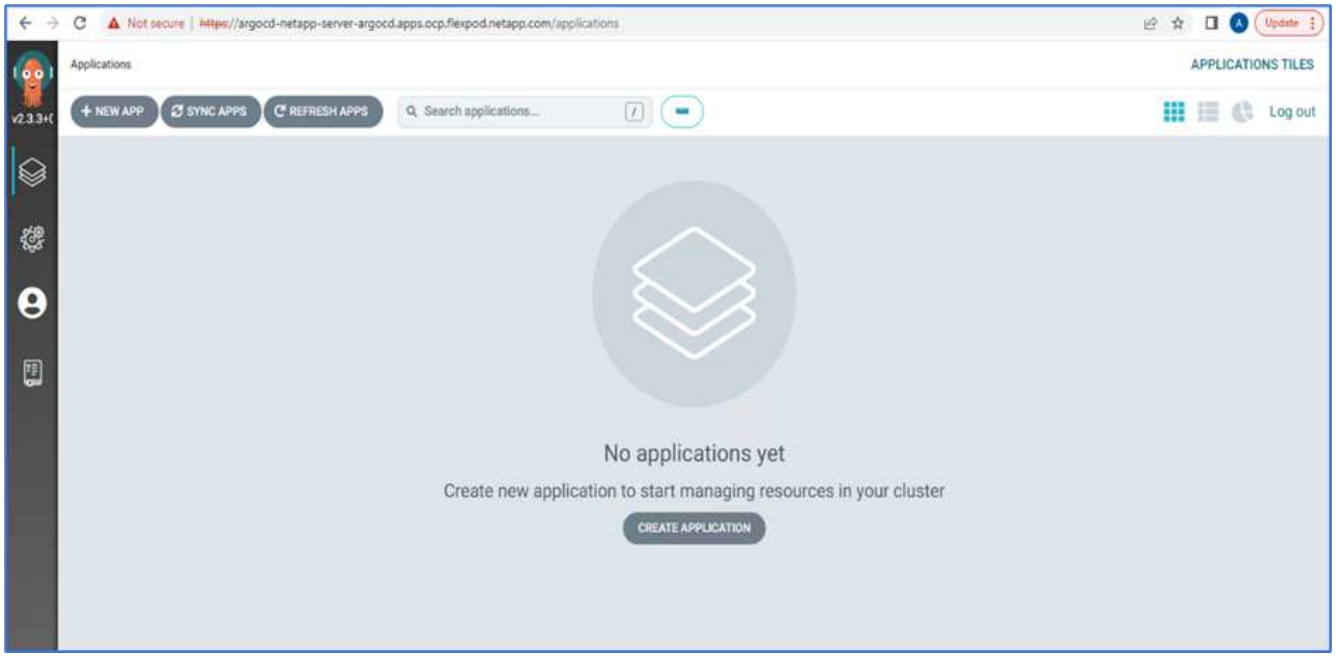
5. 要在`argocd`项目中部署Argo CD实例、请提供一个名称、然后单击创建。



6. 要登录到Argo CD、默认用户为admin、密码位于名为`argocd-netapp-cluster`的机密文件中。



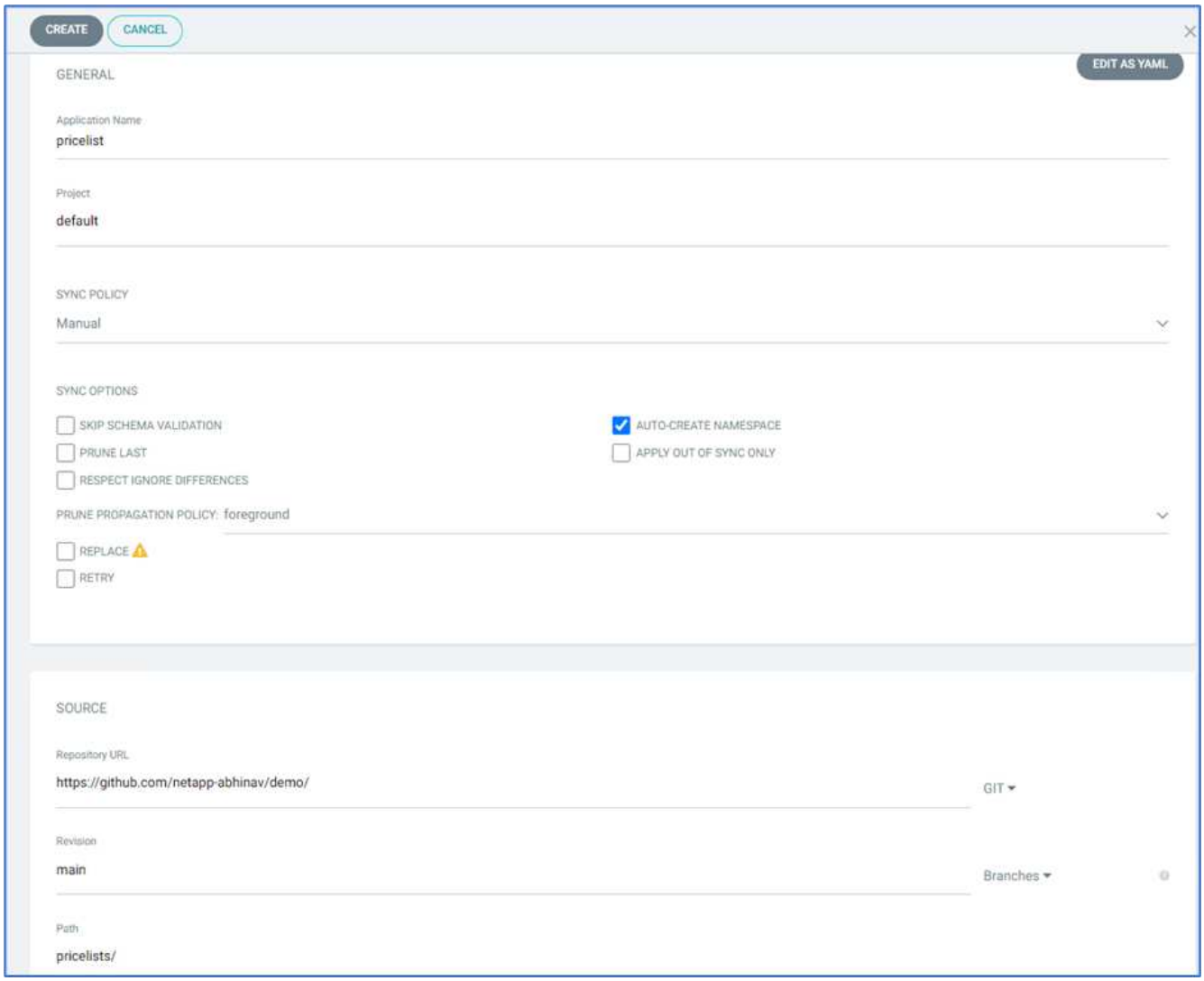
7. 从侧面菜单中、选择路由>位置、然后单击`argocd` routes的URL。输入用户名和密码。



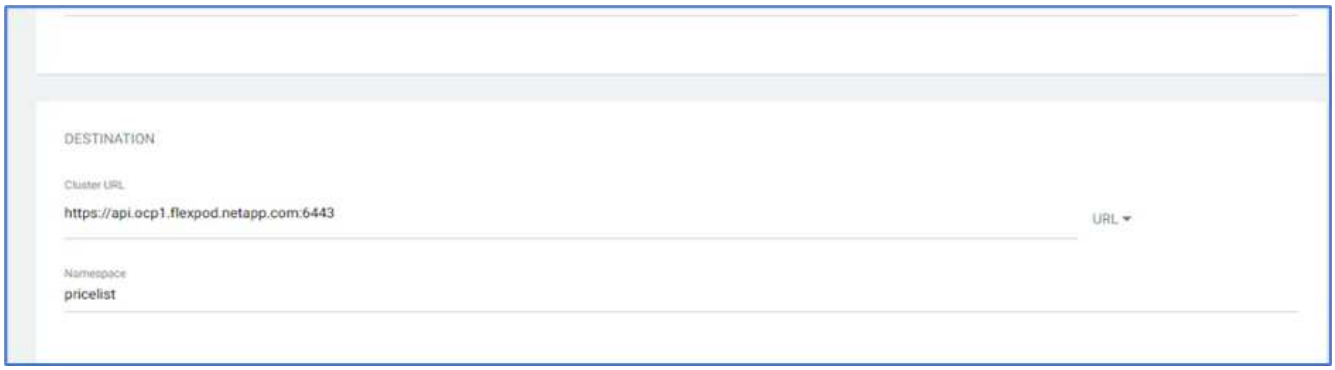
8. 通过CLI将内部OpenShift集群添加到Argo CD。

```
####Login to Argo CD####
abhinav3@abhinav-ansible$ argocd-linux-amd64 login argocd-netapp-server-
argocd.apps.ocp.flexpod.netapp.com --insecure
Username: admin
Password:
'admin:login' logged in successfully
Context'argocd-netapp-server-argocd.apps.ocp.flexpod.netapp.com' updated
####List the On-Premises OpenShift cluster####
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add
ERRO[0000] Choose a context name from:
CURRENT  NAME
CLUSTER              SERVER
*        default/api-ocp-flexpod-netapp-com:6443/abhinav3
api-ocp-flexpod-netapp-com:6443
https://api.ocp.flexpod.netapp.com:6443
         default/api-ocp1-flexpod-netapp-com:6443/abhinav3
api-ocp1-flexpod-netapp-com:6443
https://api.ocp1.flexpod.netapp.com:6443
####Add On-Premises OpenShift cluster###
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add default/api-
ocp1-flexpod-netapp-com:6443/abhinav3
WARNING: This will create a service account `argocd-manager` on the
cluster referenced by context `default/api-ocp1-flexpod-netapp-
com:6443/abhinav3` with full cluster level admin privileges. Do you want
to continue [y/N]? y
INFO[0002] ServiceAccount "argocd-manager" already exists in namespace
"kube-system"
INFO[0002] ClusterRole "argocd-manager-role" updated
INFO[0002] ClusterRoleBinding "argocd-manager-role-binding" updated
Cluster 'https://api.ocp1.flexpod.netapp.com:6443' added
```

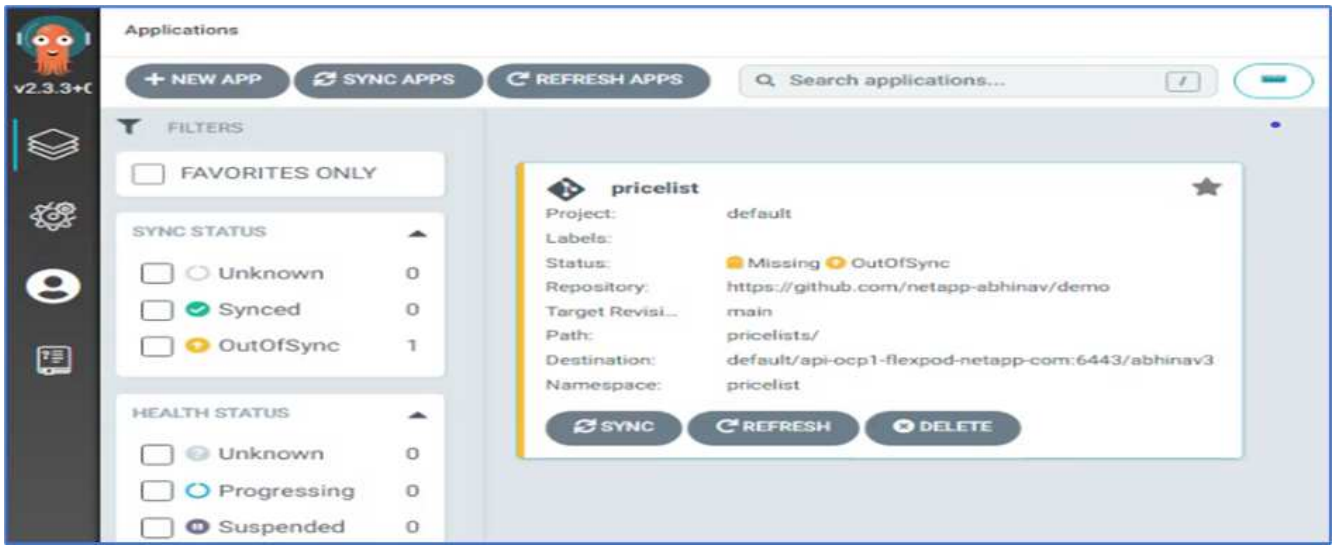
9. 在ArgoCD UI中、单击新应用程序并输入有关应用程序名称和代码存储库的详细信息。



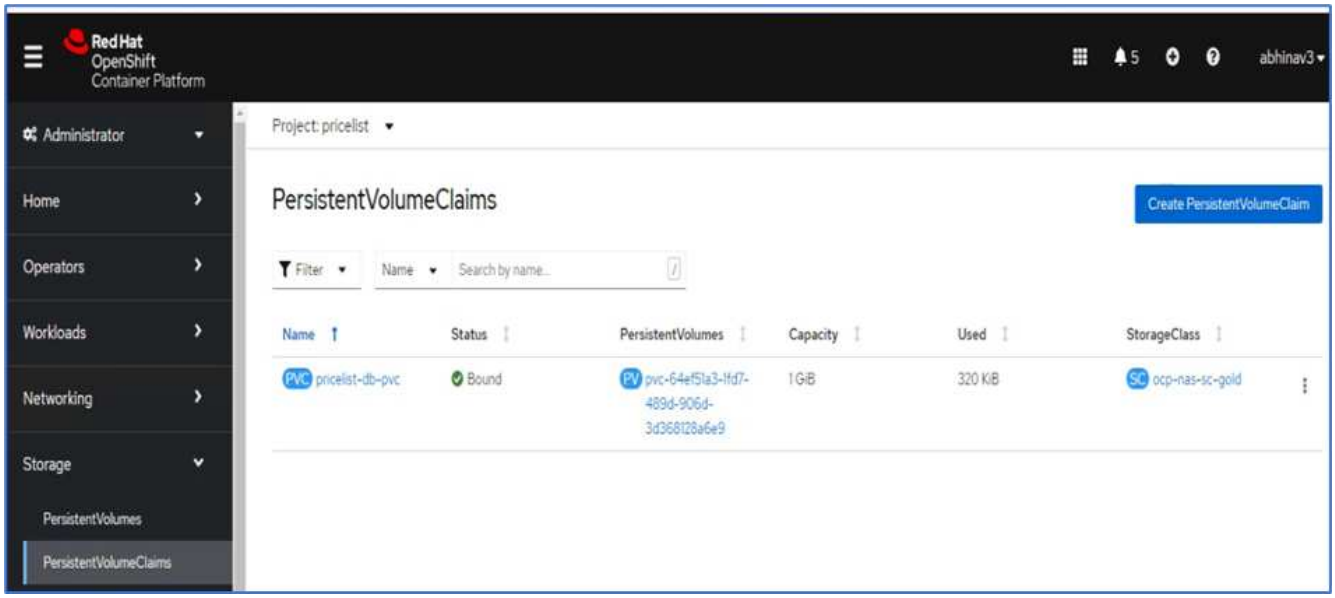
10. 输入要随命名空间一起部署应用程序的OpenShift集群。



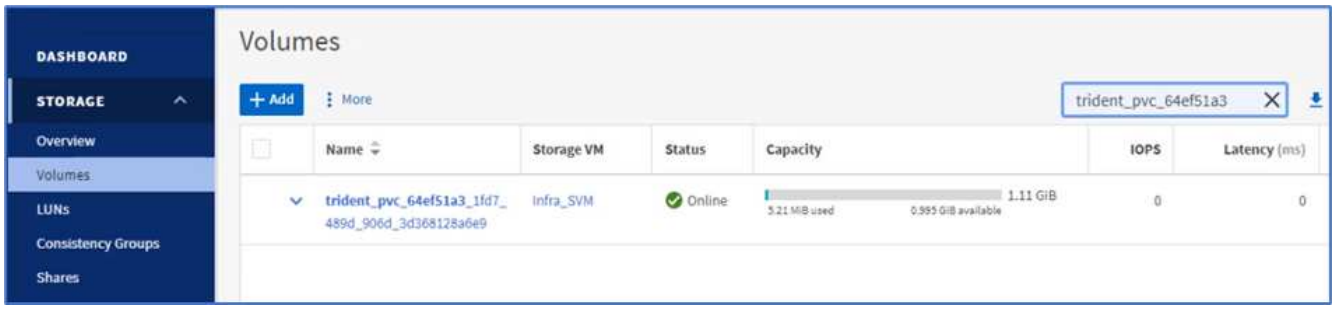
11. 要在内部OpenShift集群上部署此应用、请单击同步。



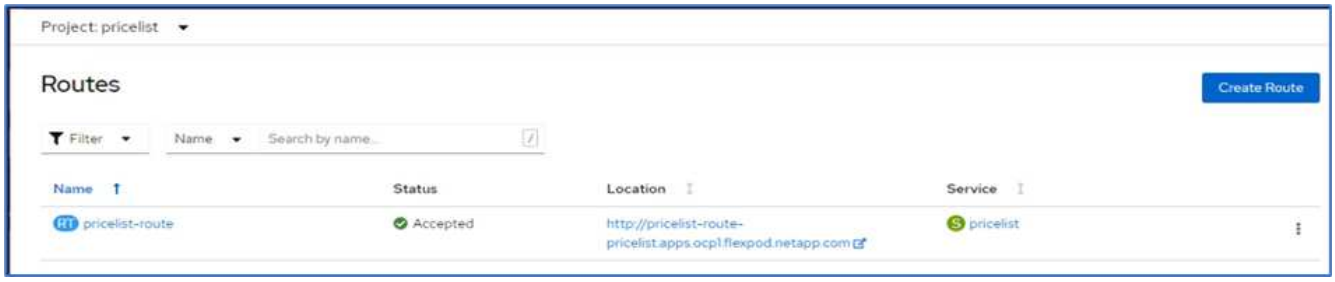
12. 在OpenShift容器平台控制台中、转至项目价目表、然后在存储下验证PVC的名称和大小。



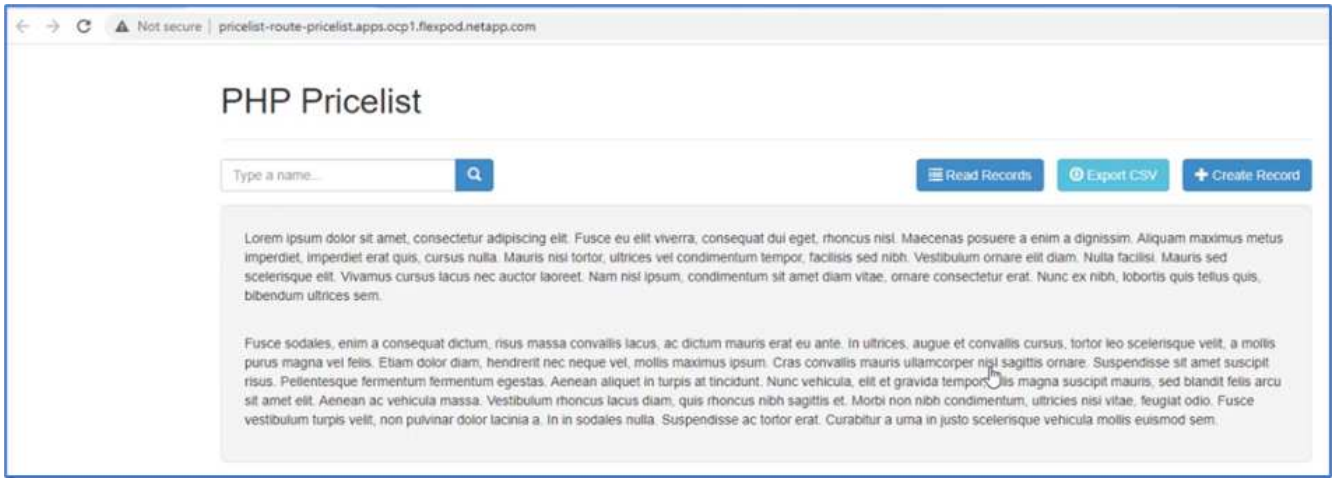
13. 登录到System Manager并验证PVC。



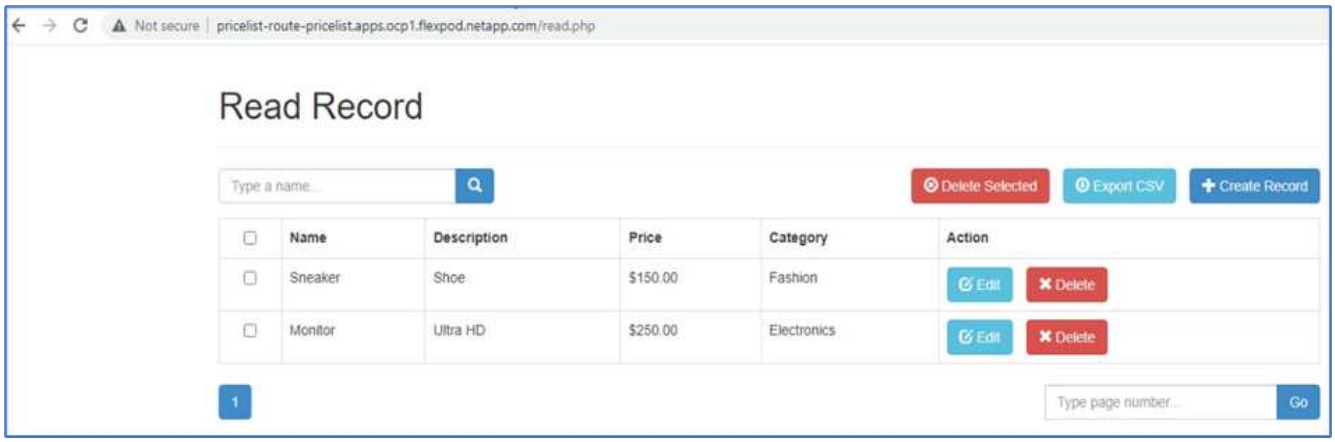
14. Pod运行后、从侧面菜单中选择Networking > routes、然后单击Location下的URL。



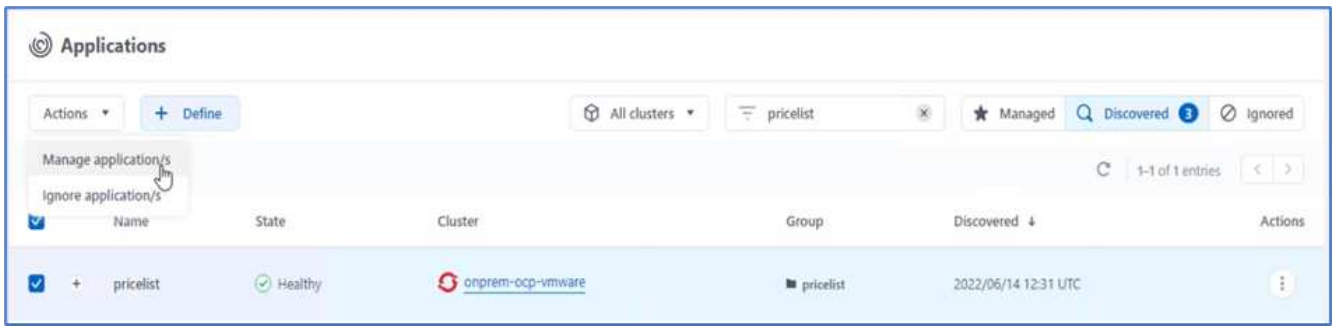
15. 此时将显示Pricelist应用程序主页。



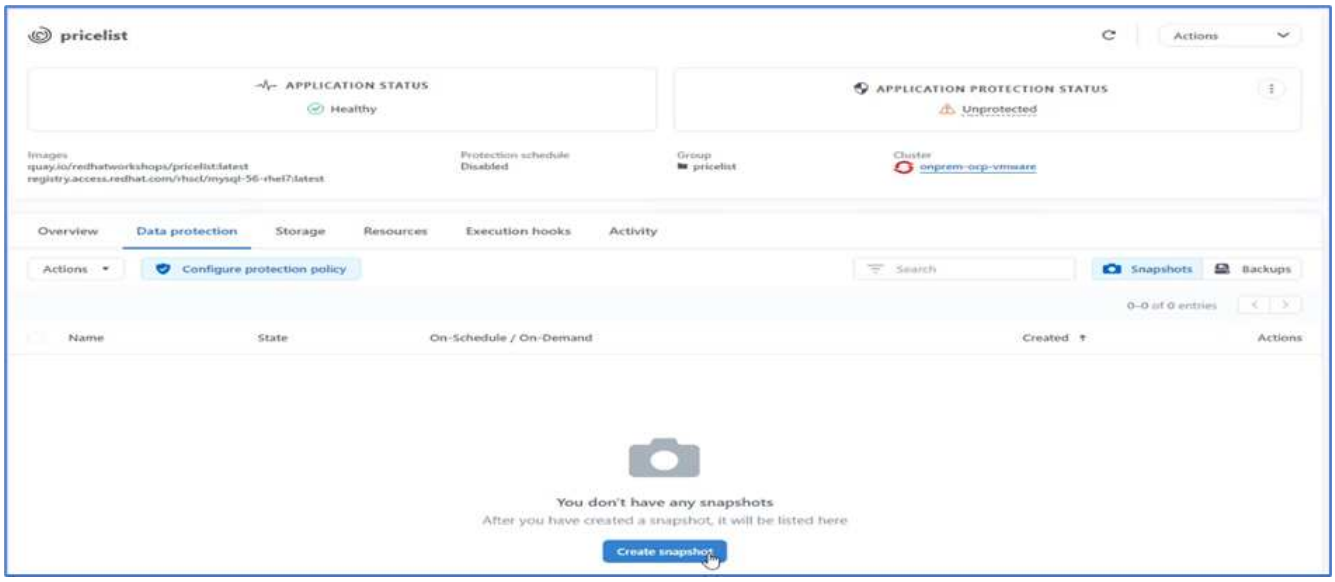
16. 在网页上创建一些记录。



17. 此应用程序会在Astra控制中心中发现。要管理此应用程序、请转到"应用程序">"已发现"、选择"价目表"应用程序、然后单击"操作"下的"管理应用程序"。

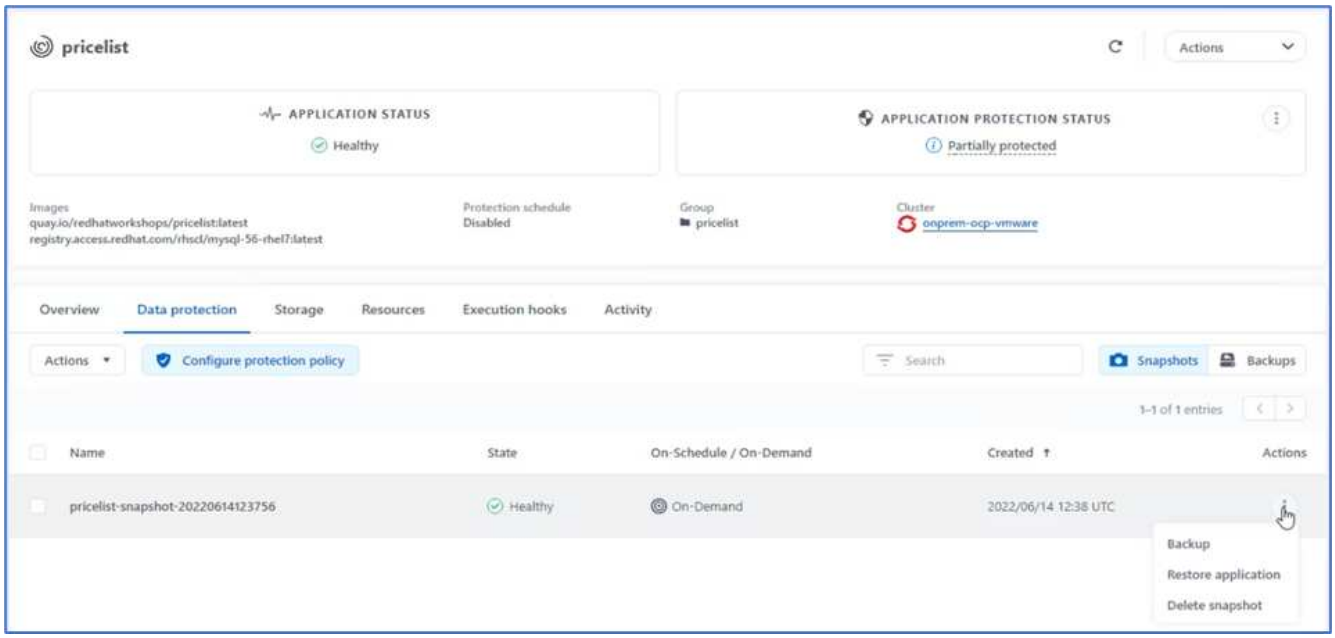


18. 单击Pricelist应用程序、然后选择Data Protection。此时、不应存在快照或备份。单击Create Snapshot以创建按需快照。

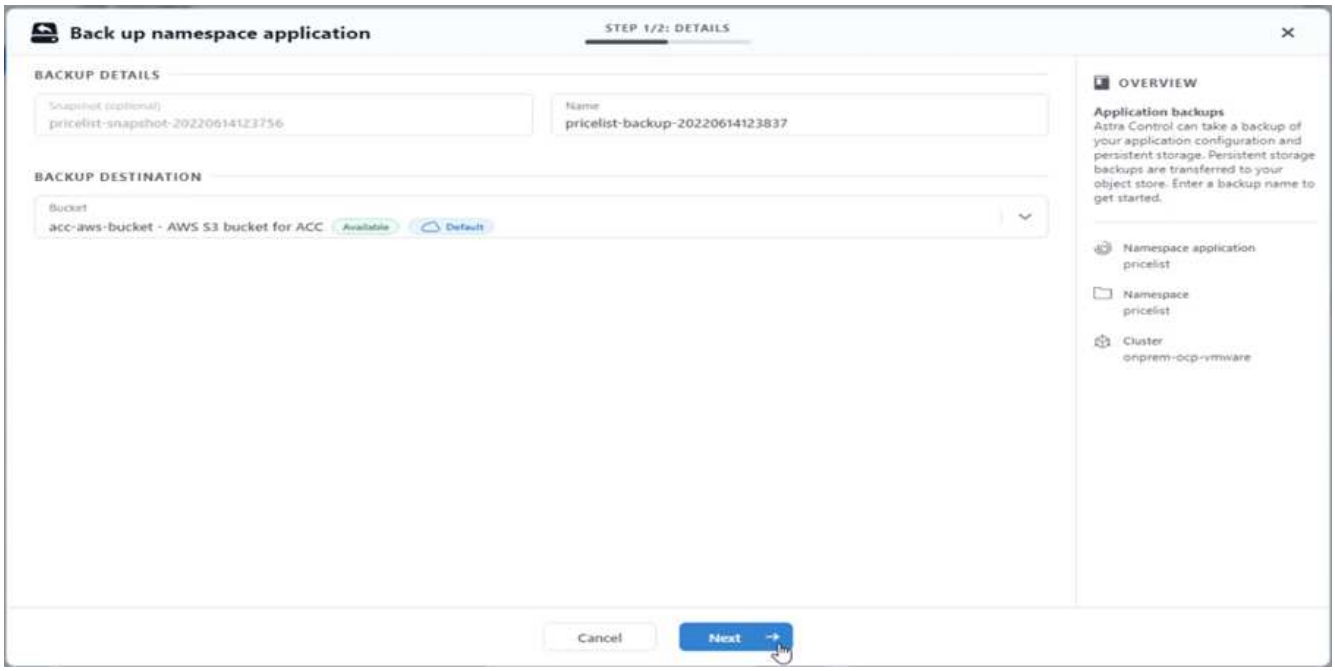


NetApp Astra控制中心既支持按需快照、也支持计划快照和备份。

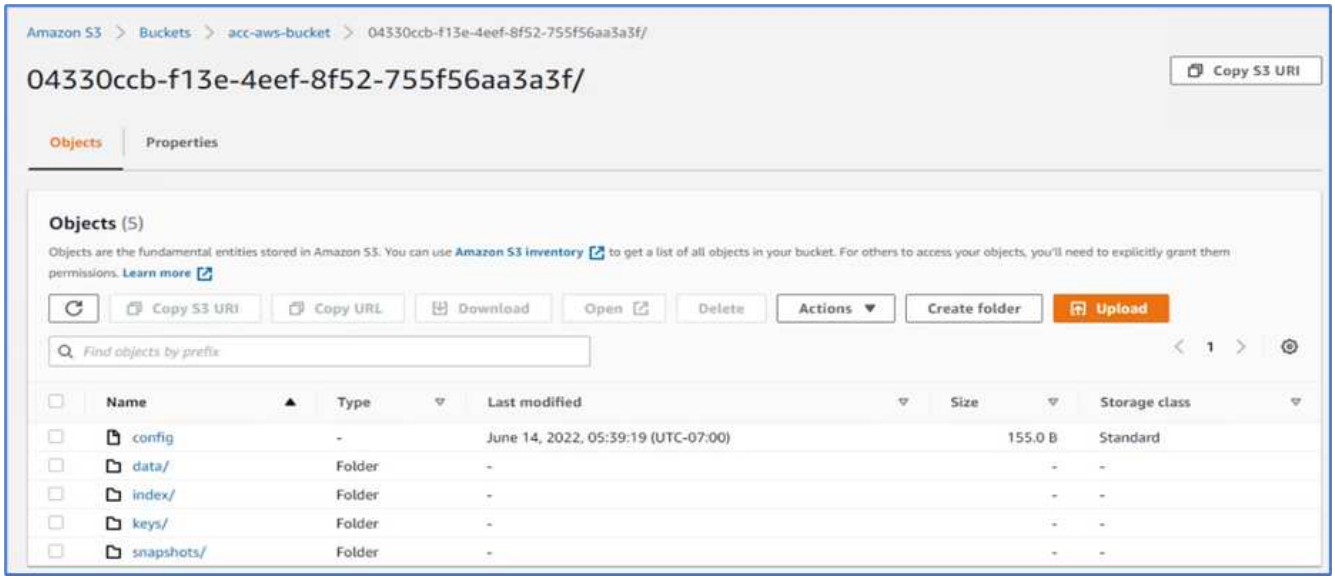
19. 创建快照并使其运行状况良好后、使用该快照创建远程备份。此备份存储在S3存储分段中。



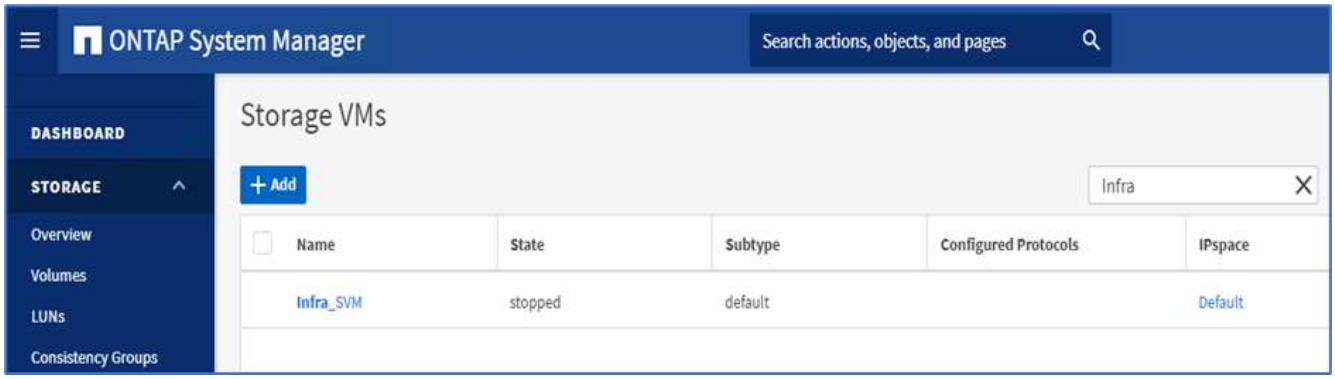
20. 选择AWS S3存储分段并启动备份操作。



21. 备份操作应在AWS S3存储分段中创建一个包含多个对象的文件夹。



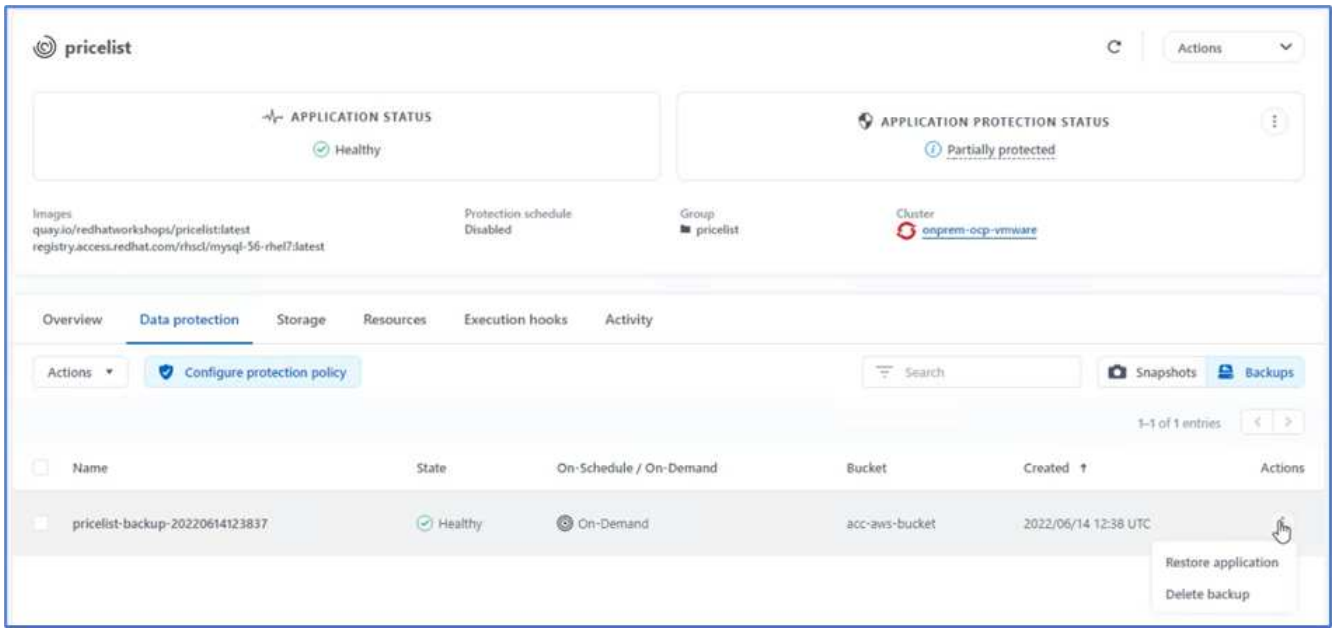
22. 远程备份完成后、通过停止托管PV后备卷的Storage Virtual Machine (SVM)来模拟内部灾难。



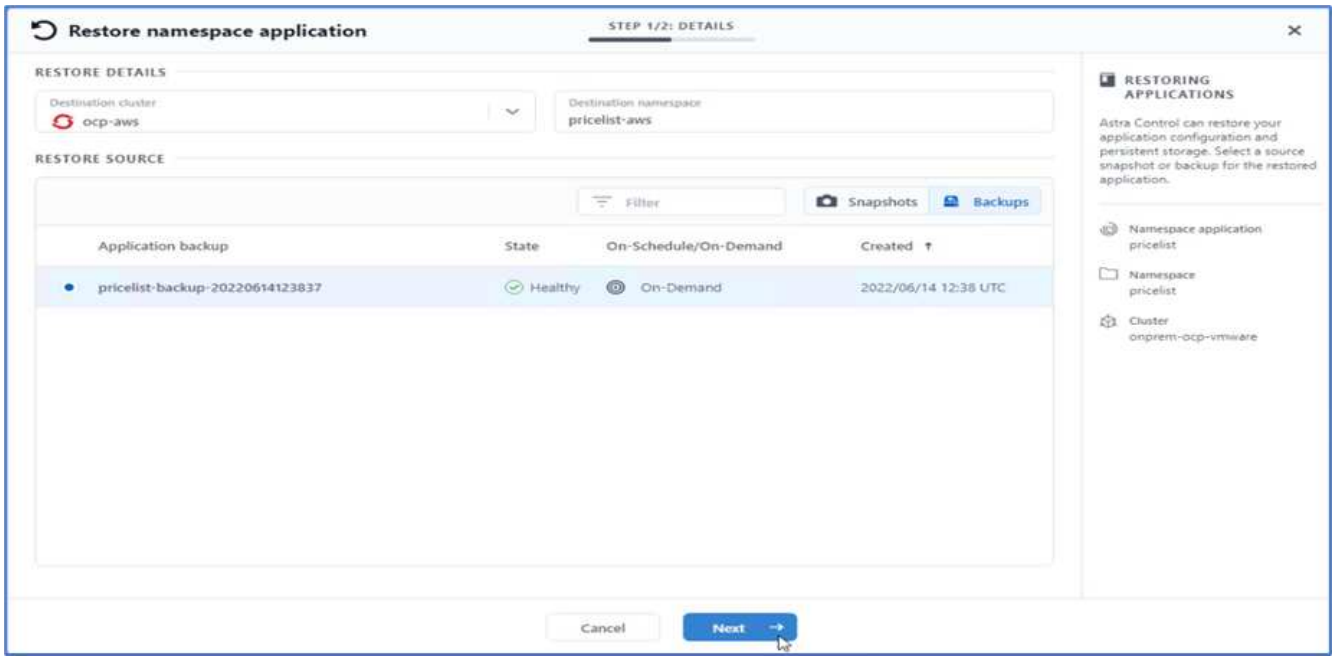
23. 刷新网页以确认中断。此网页不可用。

正如预期、网站已关闭、因此、让我们使用Astra快速从远程备份恢复应用程序、并将其恢复到AWS中运行的OpenShift集群。

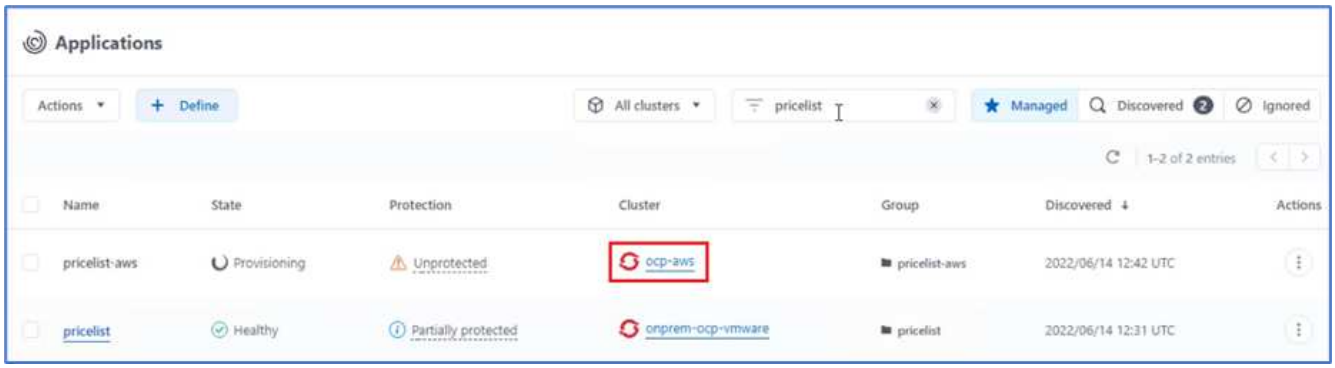
24. 在Astra Control Center中、单击Pricelist应用程序、然后选择Data Protection > Backups。选择备份、然后单击操作下的还原应用程序。



25. 选择`OCP-AWS`作为目标集群、并为命名空间提供一个名称。单击按需备份、下一步、然后单击还原。

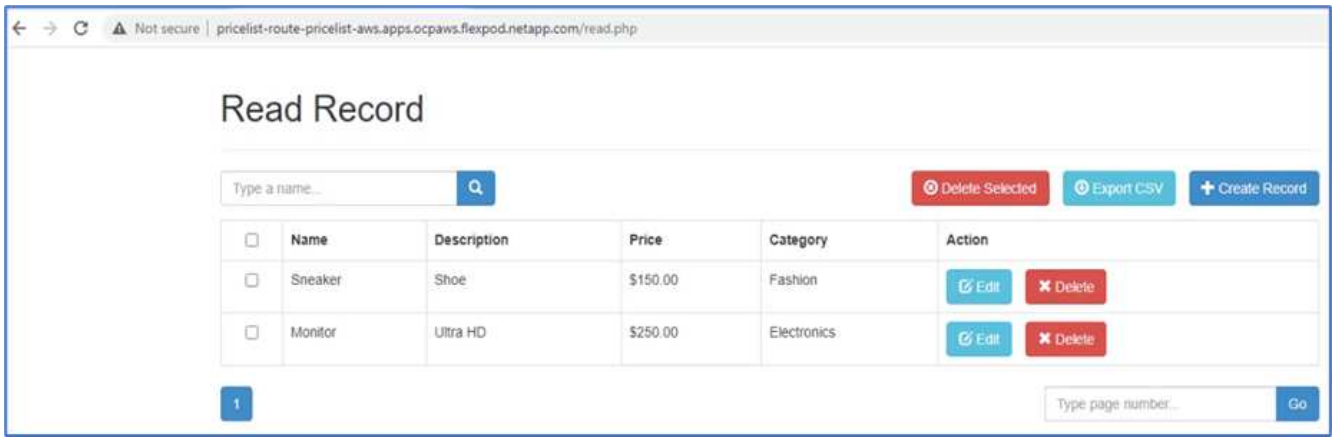


26. 在AWS中运行的OpenShift集群上会显示一个名为`pricelist-app`的新应用程序。



27. 在OpenShift Web控制台中验证相同的。

28. 运行`pricelist-AWS`项目下的所有Pod后、转到routes并单击URL以启动网页。



此过程将验证价格表应用程序是否已成功还原、以及在Astra控制中心的帮助下、在AWS上无缝运行的OpenShift集群上是否保持了数据完整性。

利用**Snapshot**副本和**DevTest**应用程序移动性保护数据

此用例由两部分组成、如下各节所述。

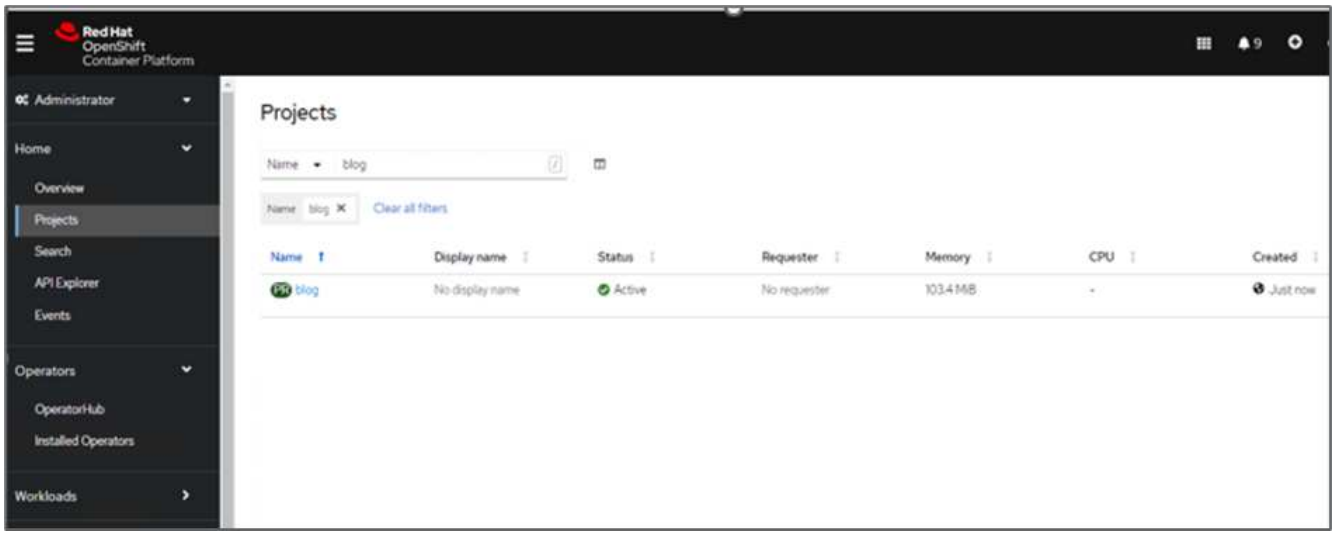
第**1**部分

借助Astra控制中心、您可以创建应用程序感知型快照以实现本地数据保护。如果意外删除或损坏数据、您可以使用先前记录的快照将应用程序和关联数据还原到已知正常状态。

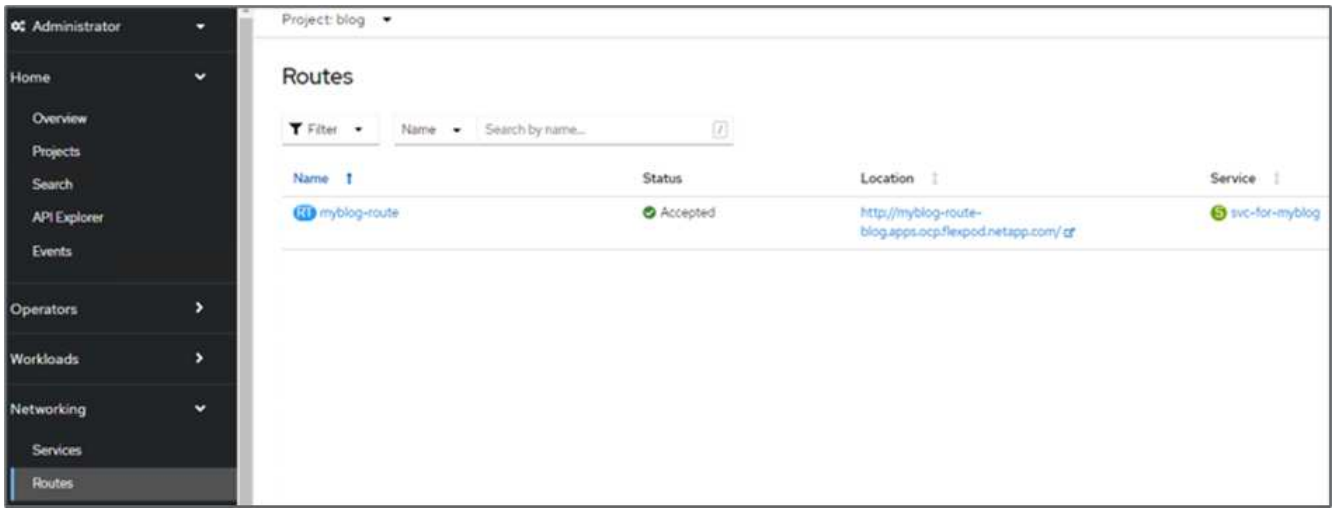
在这种情况下、开发和测试(DevTest)团队部署了一个示例有状态应用程序(博客站点)、该应用程序是一个Ghost博客应用程序、并添加了一些内容、然后将该应用程序升级到最新版本。Ghost应用程序对数据库使用SQLite。在升级应用程序之前、可以使用Astra控制中心创建一个快照(按需)来进行数据保护。详细步骤如下：

1. 部署示例博客应用程序并从ArgoCD进行同步。

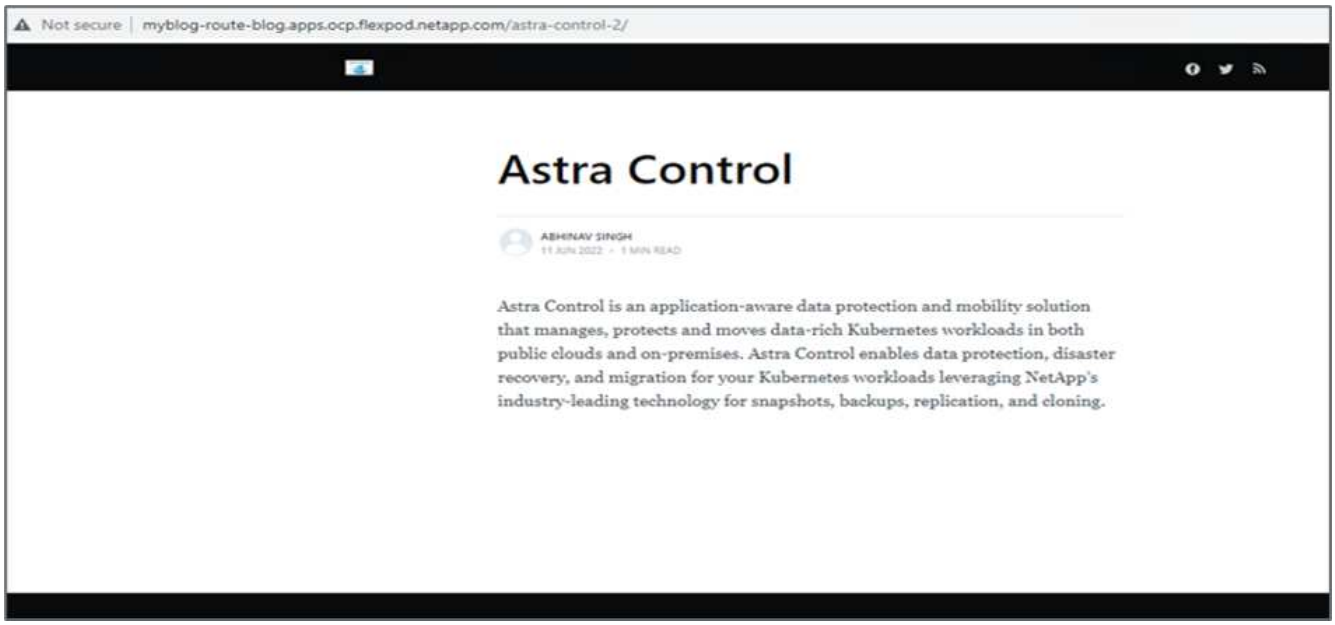
2. 登录到第一个OpenShift集群、转到Project、然后在搜索栏中输入Bllog。



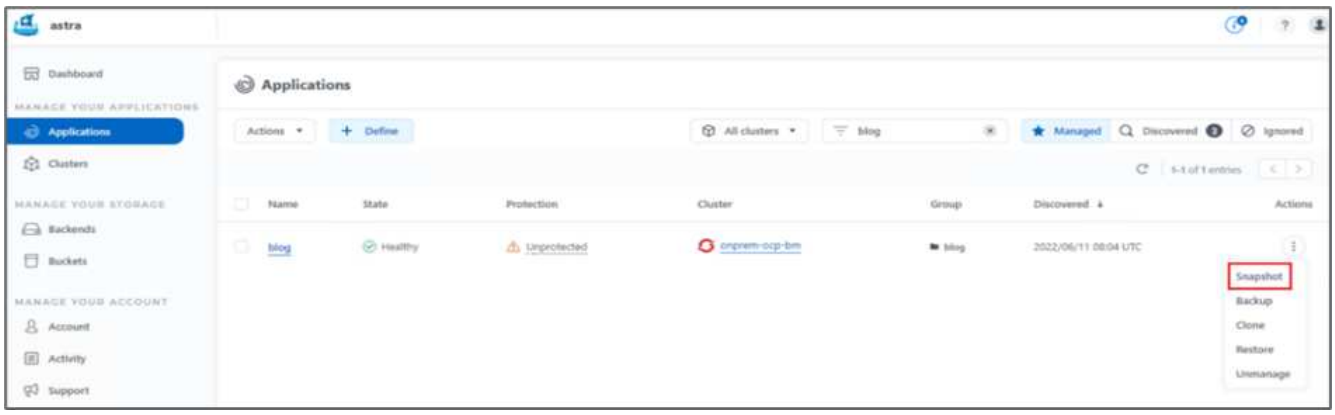
3. 从侧面菜单中、选择网络>路由、然后单击URL。



4. 此时将显示博客主页。向博客站点添加一些内容并发布。



5. 转到Astra控制中心。首先从"已发现"选项卡管理应用程序、然后创建Snapshot副本。

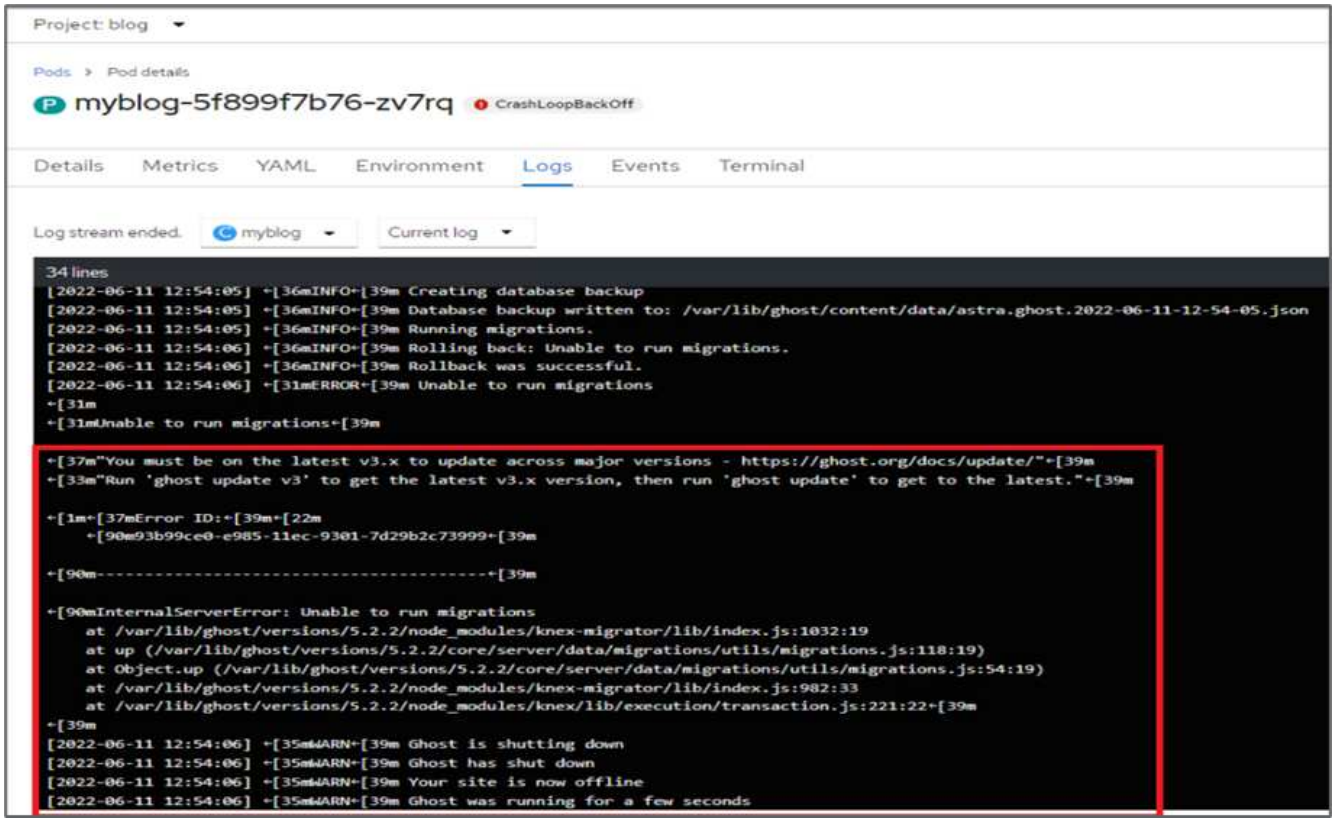


您还可以通过按定义的计划创建快照、备份或同时创建这两者来保护应用程序。有关详细信息，请参见 "通过快照和备份保护应用程序"。

6. 成功创建按需快照后、将应用程序升级到最新版本。当前映像版本为`Ghost：3.6-alpine`、目标版本为`Ghost：Latest`。要升级此应用程序、请直接更改Git存储库并将其同步到Argo CD。

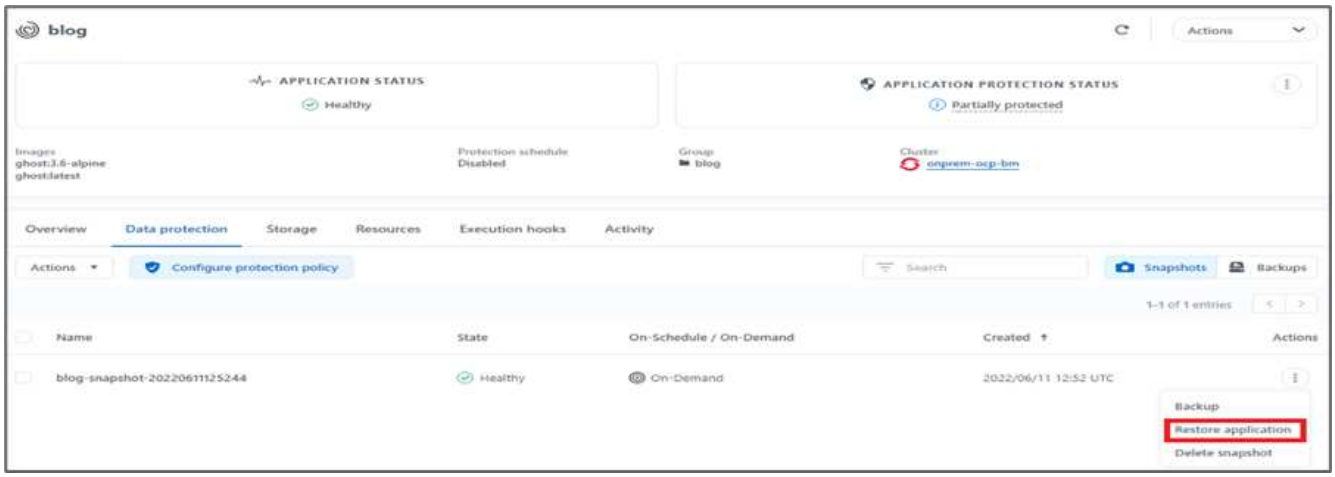
```
spec:
  containers:
  - name: myblog
    image: ghost:latest
    imagePullPolicy: Always
    ports:
    - containerPort: 2368
```

7. 您可以看到、由于博客站点关闭以及整个应用程序损坏、不支持直接升级到最新版本。

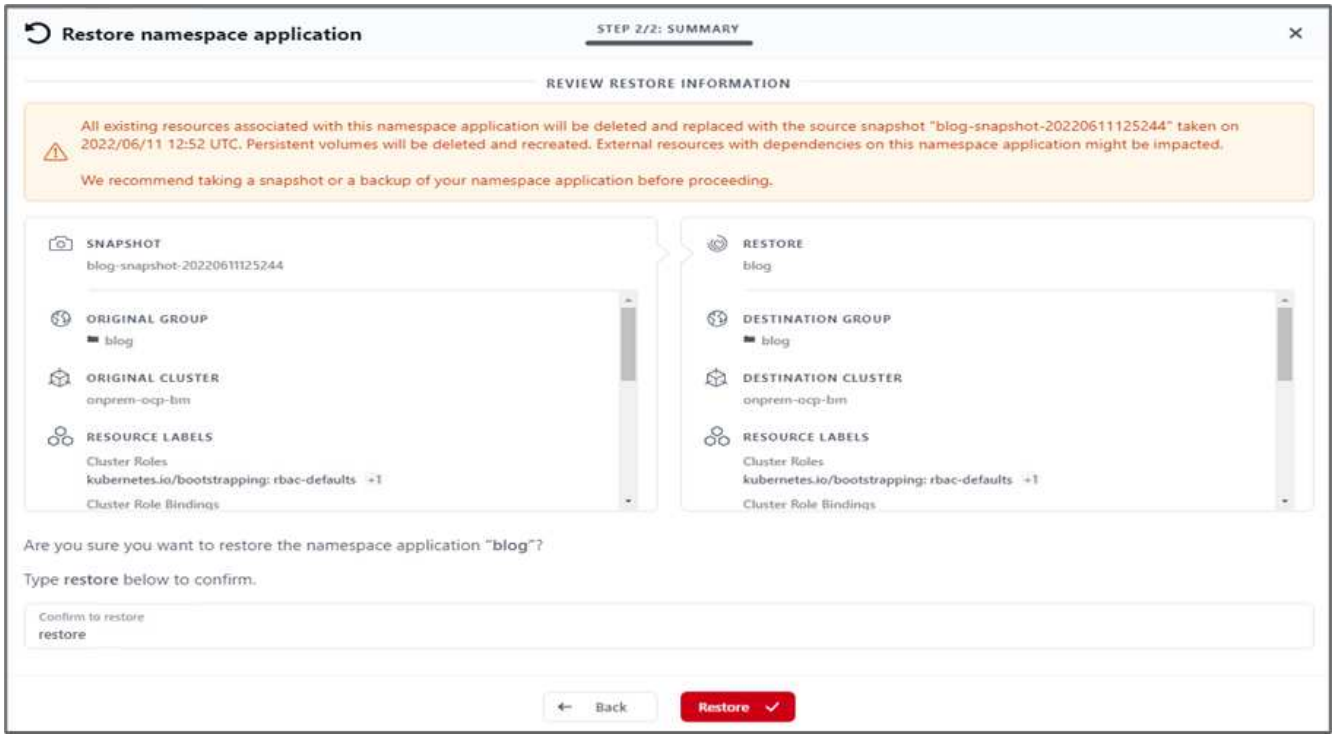


8. 要确认博客站点不可用、请刷新URL。

9. 从快照还原应用程序。

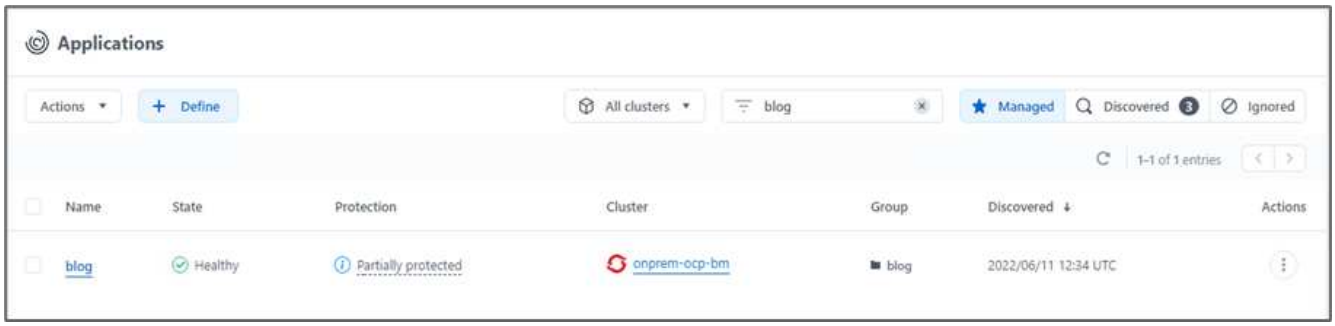


10. 此应用程序将在同一个OpenShift集群上还原。

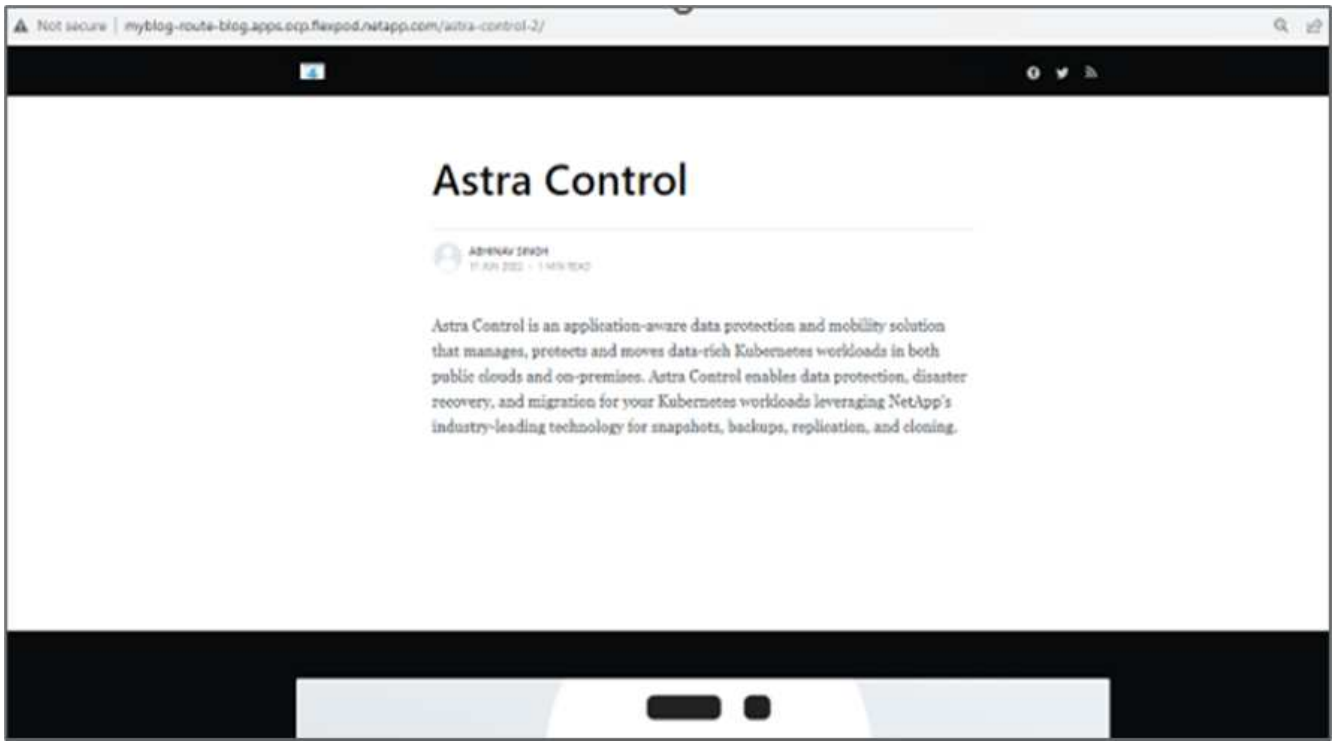


11. 应用程序还原过程将立即启动。

12. 只需几分钟、即可从可用快照成功还原应用程序。



13. 要查看此网页是否可用、请刷新此URL。

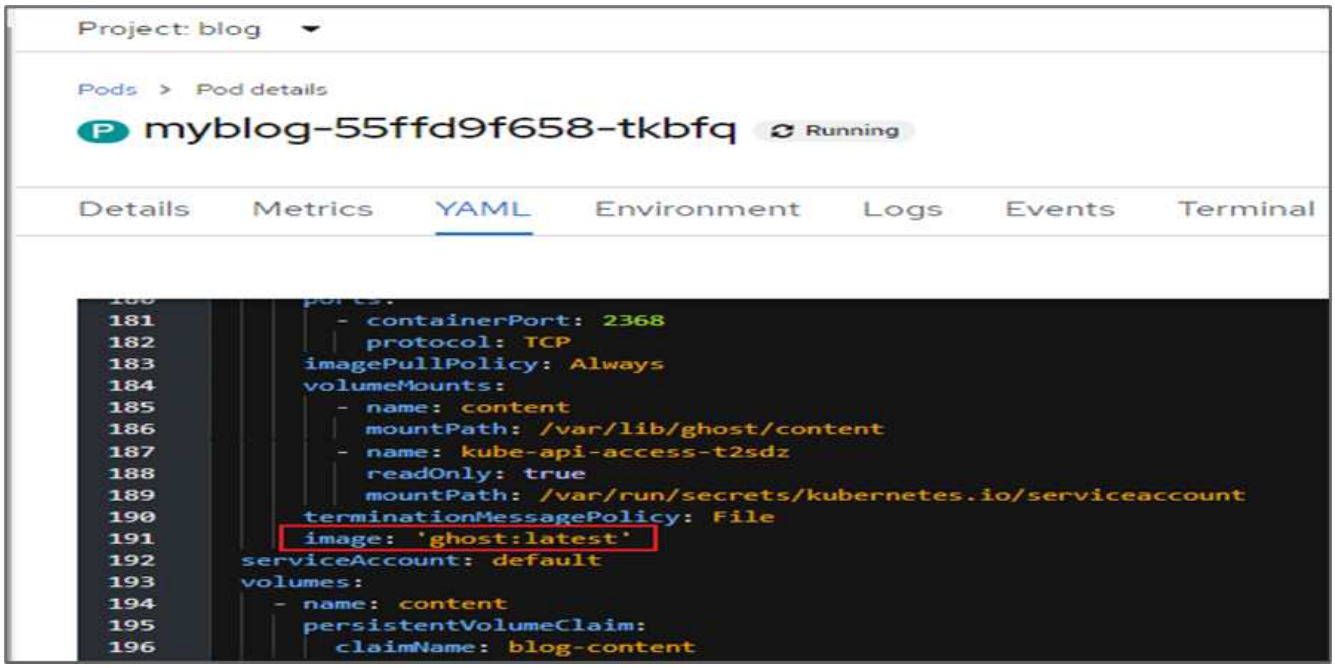


在Astra控制中心的帮助下、DevTest团队可以使用快照成功恢复博客站点应用程序及其关联数据。

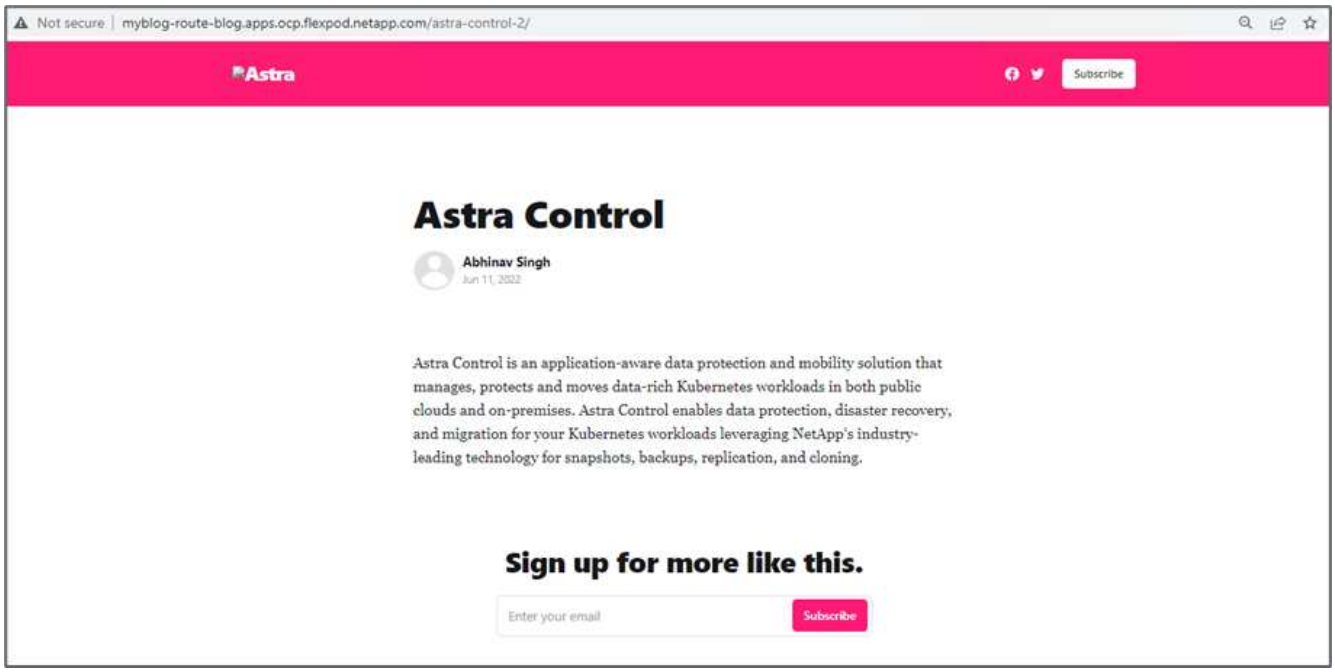
第**2**部分

借助Astra控制中心、您可以将整个应用程序及其数据从一个Kubernetes集群移动到另一个集群、无论这些集群位于何处(内部或云中)。

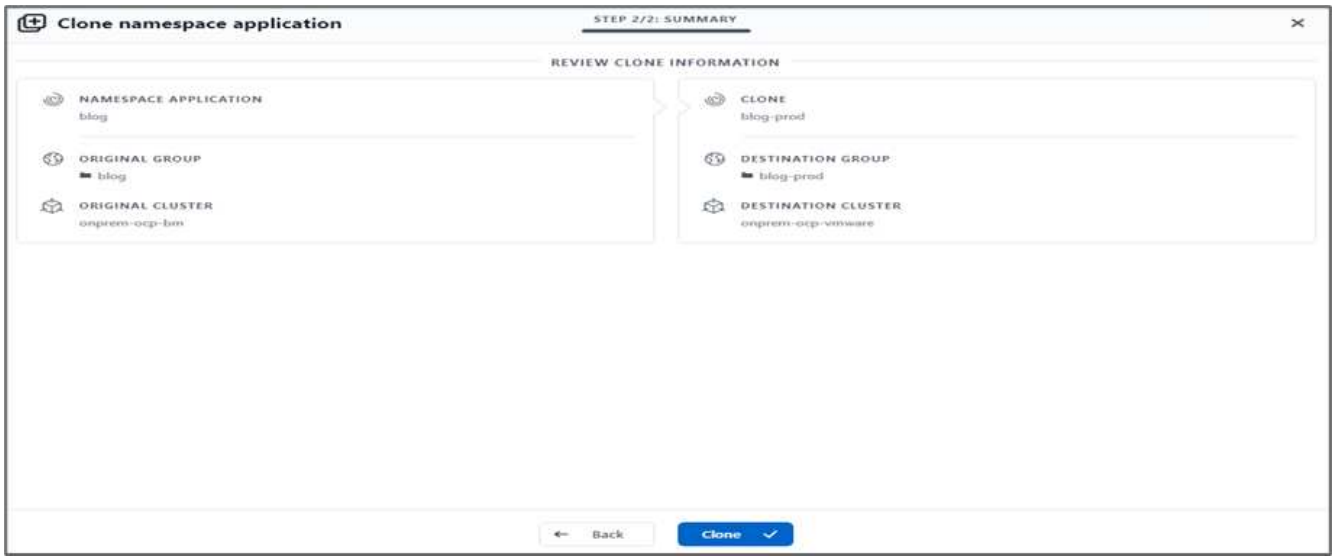
1. DevTest团队最初会先将应用程序升级到受支持的版本(`ghost-4.6. alpine`)、然后再升级到最终版本(`ghost-latest`)以使其可投入生产。然后、他们会将克隆的应用程序升级到在其他FlexPod 系统上运行的生产OpenShift集群。
2. 此时、该应用程序将升级到最新版本、并可克隆到生产集群。



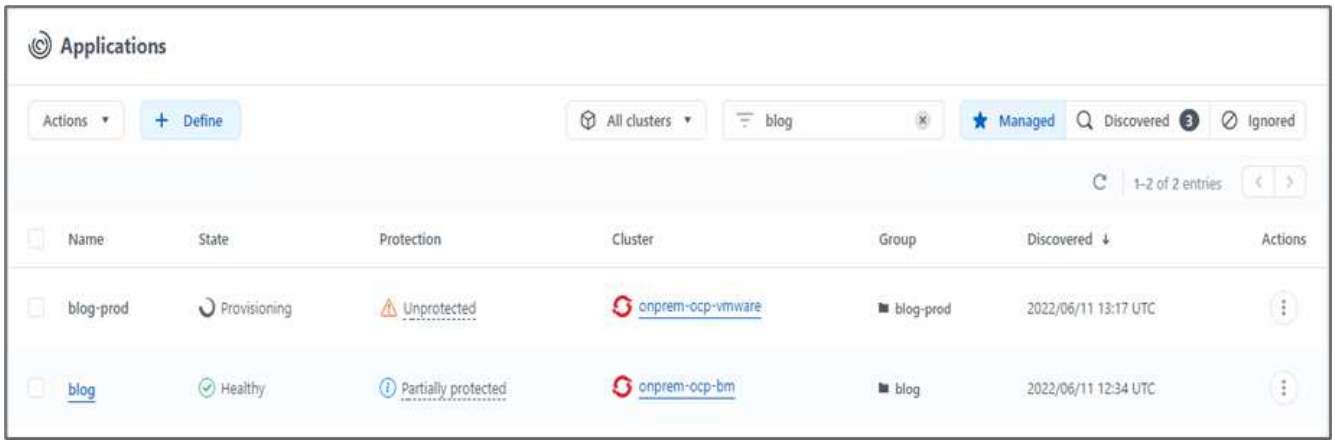
3. 要验证新主题、请刷新博客站点。



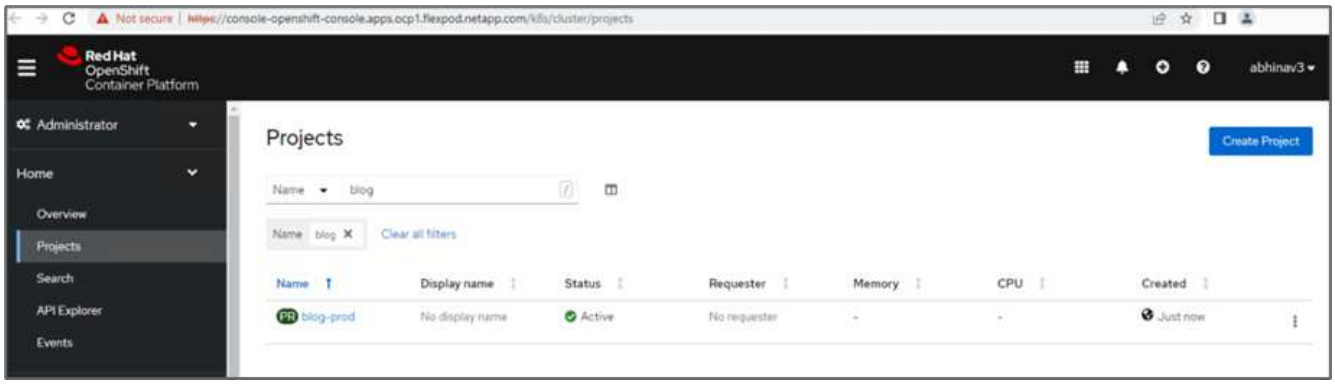
4. 从Astra控制中心、将应用程序克隆到在VMware vSphere上运行的另一个生产OpenShift集群。



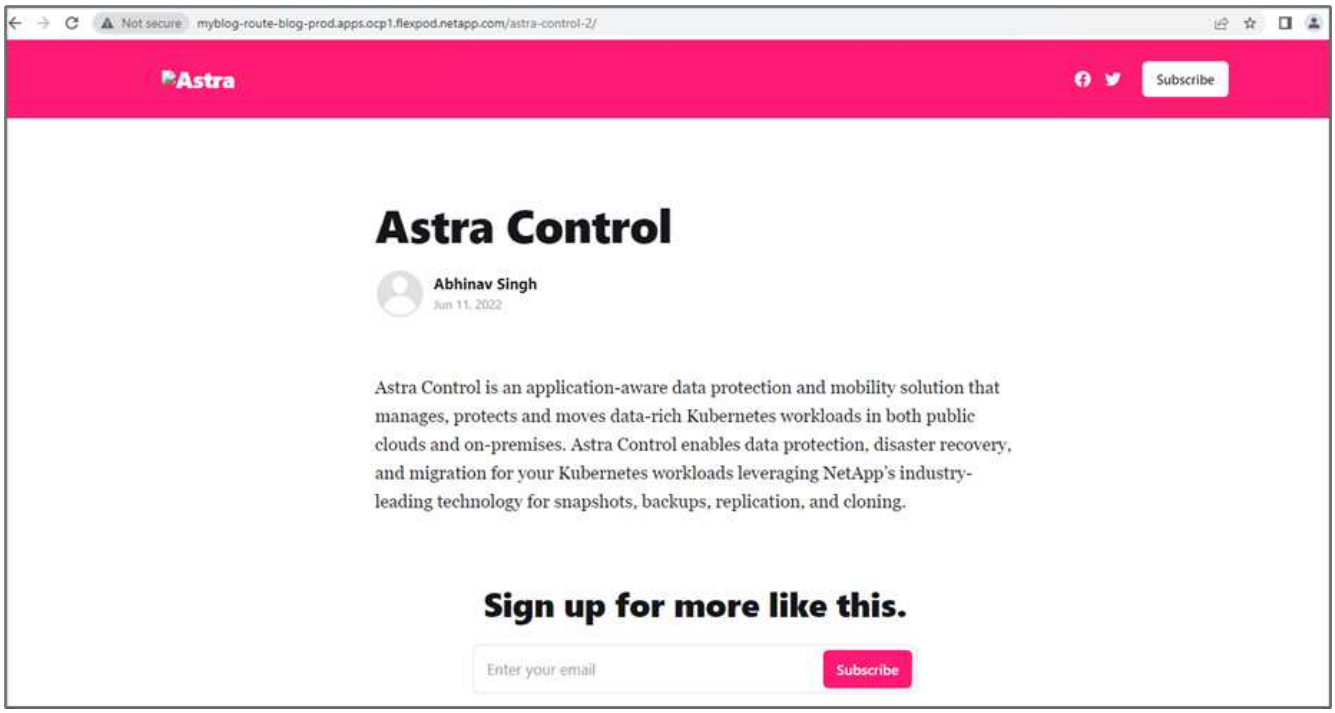
现在、生产OpenShift集群中会配置一个新的应用程序克隆。



5. 登录到生产OpenShift集群并搜索项目博客。



6. 从侧面菜单中、选择Networking > routes、然后单击Location下的URL。此时将显示与此内容相同的主页。



Astra控制中心解决方案 验证到此结束。现在、无论Kubernetes集群位于何处、您都可以将整个应用程序及其数据从一个Kubernetes集群克隆到另一个Kubernetes集群。

"接下来：总结。"

结论

"先前：使用远程备份恢复应用程序。"

在此解决方案 中、我们使用NetApp Astra产品组合为在FlexPod 和AWS上运行的容器化应用程序实施了保护计划。NetApp Astra控制中心和Astra Trident以及Cloud Volumes ONTAP 、Red Hat OpenShift和FlexPod 基础架构构成了此解决方案 的核心组件。

我们展示了通过捕获快照保护应用程序的能力、并执行完整备份来在云和内部环境中运行的不同K8s集群之间还原应用程序。

此外、我们还演示了如何跨K8s集群克隆应用程序、从而使客户能够将其应用程序迁移到所需位置的所选K8s集群。

FlexPod 不断发展、客户可以利用它来实现应用程序和业务交付流程的现代化。借助此解决方案 、FlexPod 客户可以放心地为云原生应用程序构建BCDr计划、并将公有 云作为一个位置来实施瞬时或全时灾难恢复计划、同时保持较低的解决方案 成本。

使用Astra Control、您可以将整个应用程序及其数据从一个Kubernetes集群移动到另一个集群、无论这些集群位于何处。它还可以帮助您加快云原生应用程序的部署、操作和保护速度。

故障排除

有关故障排除指导、请参见 "联机文档"。

从何处查找追加信息

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：

- FlexPod 主页

  "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"

- 使用Ansible为VMware部署基础架构代码FlexPod

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html#AnsibleAutomationWorkflowandSolutionDeployment"

- 使用Ansible将基础架构作为Red Hat OpenShift裸机的代码进行FlexPod 部署

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_iac_redhat_openshift.html"

- Cisco UCS 硬件和软件互操作性工具

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Cisco Intersight数据表

  "https://intersight.com/help/saas/home"

- NetApp Astra文档

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra 控制中心

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Trident

  "https://docs.netapp.com/us-en/trident/index.html"

- NetApp Cloud Manager

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- NetApp Cloud Volumes ONTAP

  "https://docs.netapp.com/us-en/occm/task_getting_started_aws.html"

- Red Hat OpenShift

  "https://www.openshift.com/"

- NetApp 互操作性表工具

  "http://support.netapp.com/matrix/"

版本历史记录

version	Date	文档版本历史记录
版本 1.0	2022年7月	针对ACC22.04.0的版本。

适用于 FlexPod 的 NetApp Cloud Insights

TR-4868：《适用于 FlexPod 的 NetApp Cloud Insights 》

NetApp 公司 Alan Cowles

与以下合作伙伴：

本技术报告详细介绍的解决方案是 NetApp Cloud Insights 服务的配置，用于监控运行 NetApp ONTAP 的 NetApp AFF A800 存储系统，该存储系统是作为 FlexPod Datacenter 解决方案的一部分部署的。

客户价值

此处详细介绍的解决方案为有意在混合云环境中全面监控解决方案的客户提供了价值，其中 ONTAP 作为主存储系统进行部署。其中包括使用 NetApp AFF 和 FAS 存储系统的 FlexPod 环境。

用例

此解决方案适用场景的使用情形如下：

- 希望监控作为 FlexPod 解决方案一部分部署的 ONTAP 存储系统中的各种资源和利用率的组织。
- 希望对使用 AFF 或 FAS 系统的 FlexPod 解决方案中发生的问题进行故障排除并缩短解决时间的组织。
- 对成本优化预测感兴趣的组织，包括自定义信息板，用于提供有关资源浪费的详细信息，以及在包括 ONTAP 在内的 FlexPod 环境中可以节省哪些成本。

目标受众

解决方案的目标受众包括以下组：

- IT 主管以及关注成本优化和业务连续性的人员。
- 对数据中心或混合云设计和管理感兴趣的解决方案架构师。
- 负责故障排除和意外事件解决的技术支持工程师。

您可以对 Cloud Insights 进行配置，以提供多种有用的数据类型，这些数据可用于协助进行规划，故障排除，维护以及确保业务连续性。使用 Cloud Insights 监控 FlexPod Datacenter 解决方案，并在易于理解的自定义信息板中显示聚合的数据； 不仅可以预测部署中的资源何时需要扩展以满足需求，还可以确定导致系统出现问题的特定应用程序或存储卷。这有助于确保所监控的基础架构可预测并根据预期运行，从而使组织能够按定义的 SLA 交付并根据需要扩展基础架构，从而避免浪费和额外成本。

架构

在本节中，我们将回顾 FlexPod 数据中心融合基础架构的架构，包括由 Cloud Insights 监控的 NetApp AFF A800 系统。

解决方案技术

FlexPod Datacenter 解决方案由以下最低组件组成，可提供高度可用，易于扩展，经验证且受支持的融合基础架构环境。

- 两个 NetApp ONTAP 存储节点（一个 HA 对）
- 两个 Cisco Nexus 数据中心网络交换机
- 两个 Cisco MDS 光纤交换机（ FC 部署可选）
- 两个 Cisco UCS 互联阵列
- 一个带有两个 Cisco UCS B 系列刀片式服务器的 Cisco UCS 刀片式服务器机箱

或

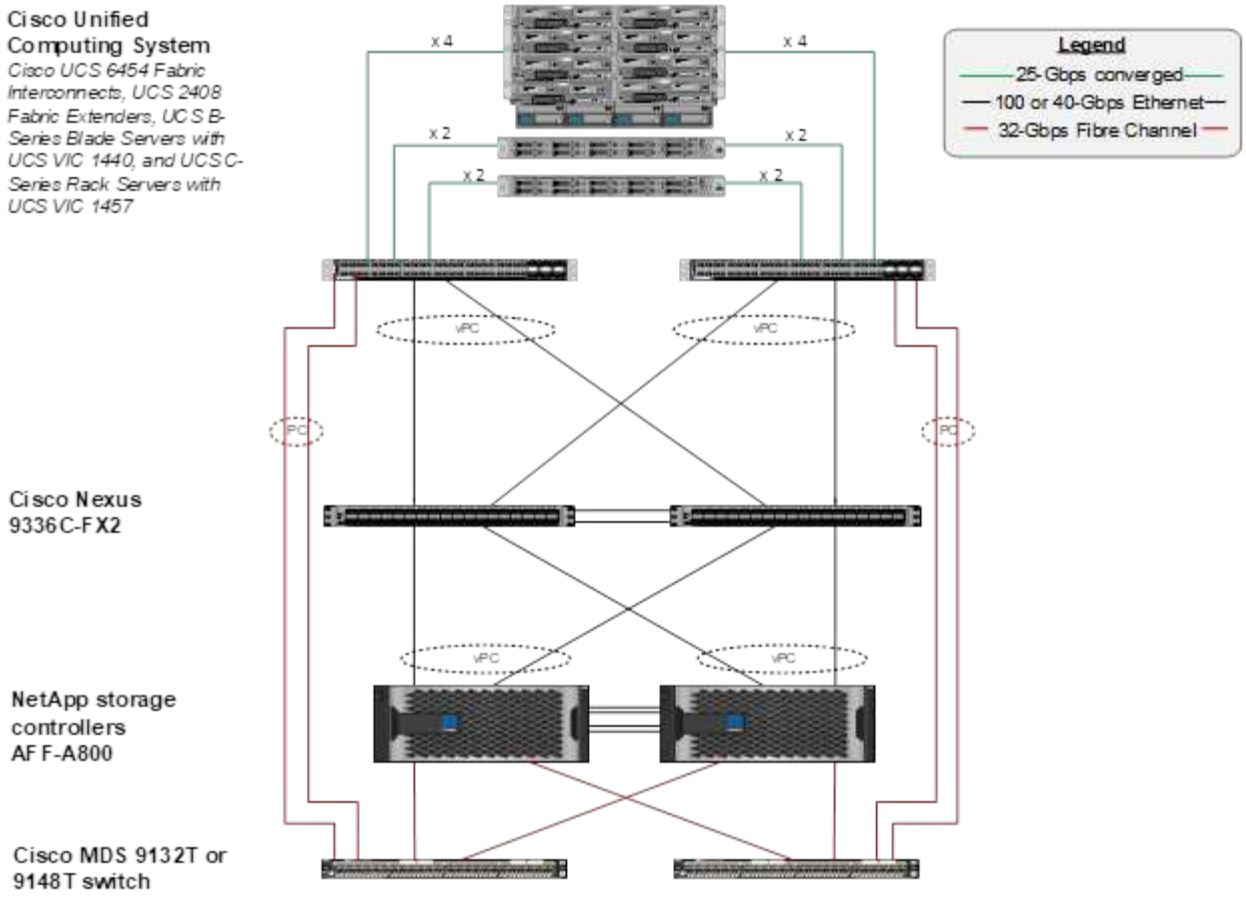
- 两个 Cisco UCS C 系列机架式服务器

要使 Cloud Insights 收集数据，组织必须将采集单元部署为其 FlexPod 数据中心环境中的虚拟机或物理机，或者部署在可与从中收集数据的组件联系的位置。您可以在运行多个受支持的 Windows 或 Linux 操作系统的系统上安装采集单元软件。下表列出了此软件的解决方案组件。

操作系统	**version**
Microsoft Windows	10
Microsoft Windows Server	2012 ， 2012 R2 ， 2016 ， 2019
Red Hat Enterprise Linux	7.2 – 7.6
CentOS	7.2 – 7.6
Oracle Enterprise Linux	7.5
Debian	9
Ubuntu	18.04 LTS

架构图

下图显示了解决方案架构。



硬件要求

下表列出了实施解决方案所需的硬件组件。在任何特定解决方案实施中使用的硬件组件可能会因客户要求而异。

硬件	数量
Cisco Nexus 9336C-x2	2.
Cisco UCS 6454 互联阵列	2.
Cisco UCS 5108 刀片式服务器机箱	1.
Cisco UCS 2408 阵列扩展器	2.
Cisco UCS B200 M5 刀片式服务器	2.
NetApp AFF A800	2.

软件要求

下表列出了实施解决方案所需的软件组件。在任何特定解决方案实施中使用的软件组件可能会因客户要求而异。

软件	**version**
Cisco Nexus 固件	9.3 （5）
Cisco UCS 版本	4.1 （2a）
NetApp ONTAP 版本	9.7

软件	**version**
NetApp Cloud Insights 版本	2020 年 9 月，基本版
Red Hat Enterprise Linux	7.6
VMware vSphere	6.7U3.

用例详细信息

此解决方案适用场景的使用情形如下：

- 使用提供给 NetApp Active IQ 数字顾问的数据分析环境，以评估存储系统风险并提供存储优化建议。
- 通过实时检查系统统计信息对部署在 FlexPod Datacenter 解决方案中的 ONTAP 存储系统中的问题进行故障排除。
- 生成自定义信息板，以便轻松监控在 FlexPod 数据中心融合基础架构中部署的 ONTAP 存储系统的特定关注点。

设计注意事项

FlexPod Datacenter 解决方案是由 Cisco 和 NetApp 设计的一种融合基础架构，可为运行企业工作负载提供动态，高可用性和可扩展的数据中心环境。解决方案中的计算和网络资源由 Cisco UCS 和 Nexus 产品提供，存储资源由 ONTAP 存储系统提供。当更新的硬件型号或软件和固件版本可用时，解决方案设计会定期进行增强。这些详细信息以及解决方案设计和部署的最佳实践均包含在 Cisco Validated Design （ CVD ）或 NetApp Verified Architecture （ NVA ）文档中，并定期发布。

我们提供了详细介绍 FlexPod Datacenter 解决方案设计的最新 CVD 文档 "此处"。

部署适用于 **FlexPod** 的 **Cloud Insights**

要部署解决方案，您必须完成以下任务：

1. 注册 Cloud Insights 服务
2. 创建要配置为采集单元的 VMware 虚拟机（ VM ）
3. 安装 Red Hat Enterprise Linux （ RHEL ）主机
4. 在 Cloud Insights 门户中创建采集单元实例并安装软件
5. 将受监控的存储系统从 FlexPod 数据中心添加到 Cloud Insights 。

注册 **NetApp Cloud Insights** 服务

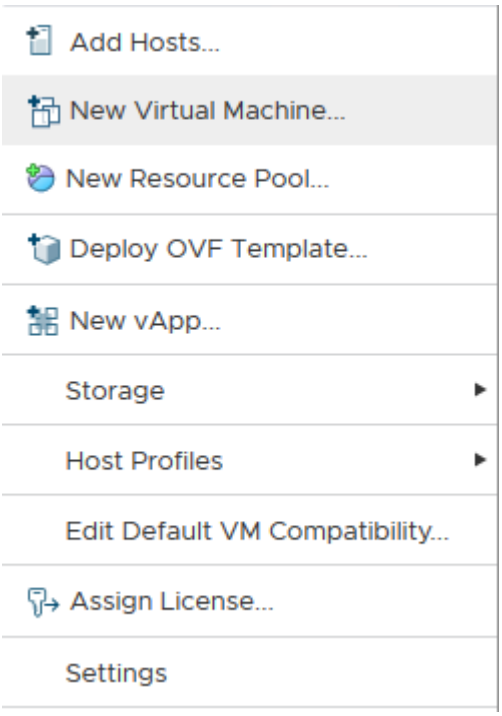
要注册 NetApp Cloud Insights 服务，请完成以下步骤：

1. 转至 "https://cloud.netapp.com/cloud-insights"
2. 单击屏幕中央的按钮开始 14 天免费试用，或者单击右上角的链接注册或使用现有 NetApp Cloud Central 帐户登录。

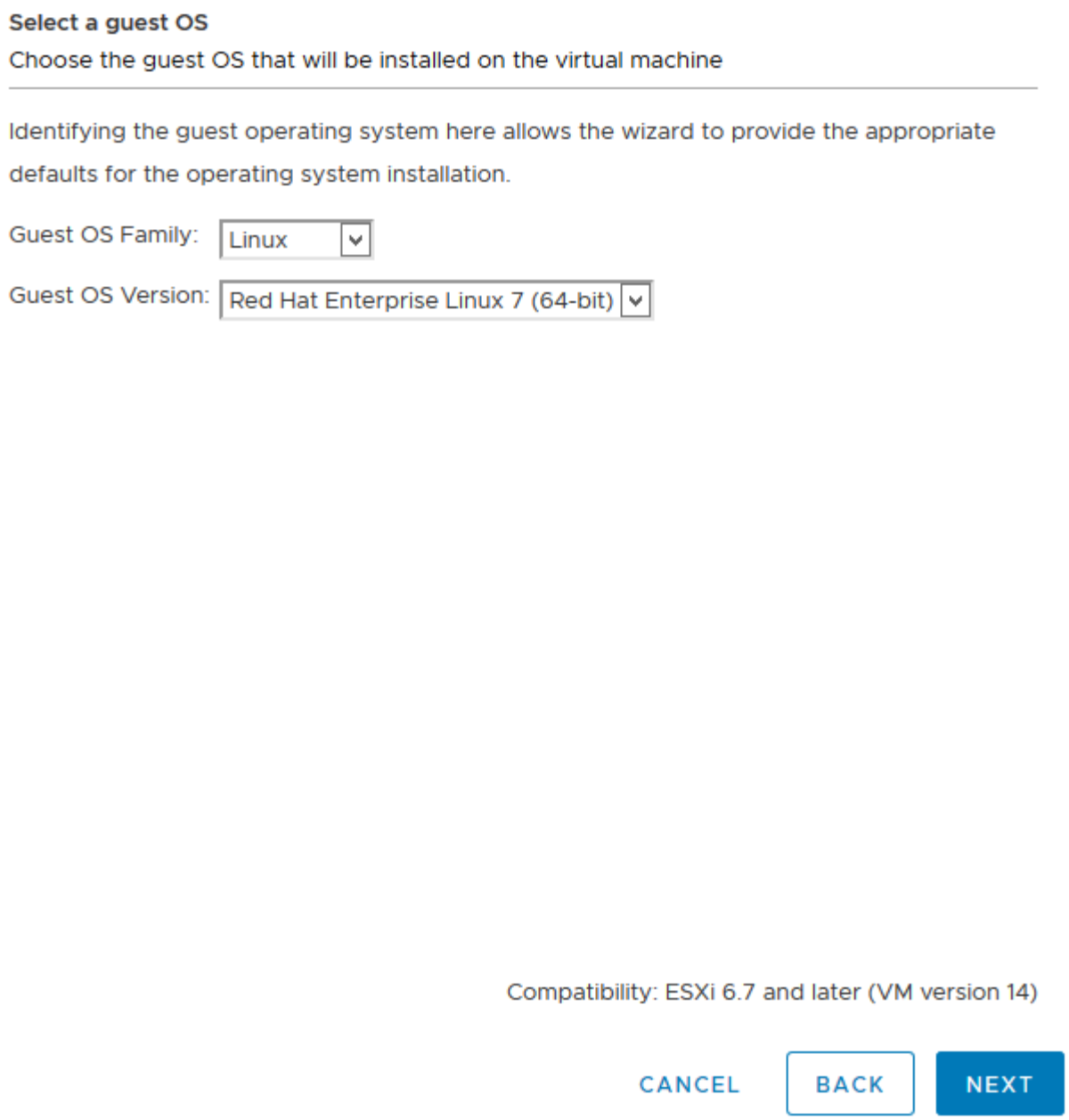
创建要配置为采集单元的 **VMware** 虚拟机

要创建 VMware VM 以配置为采集单元，请完成以下步骤：

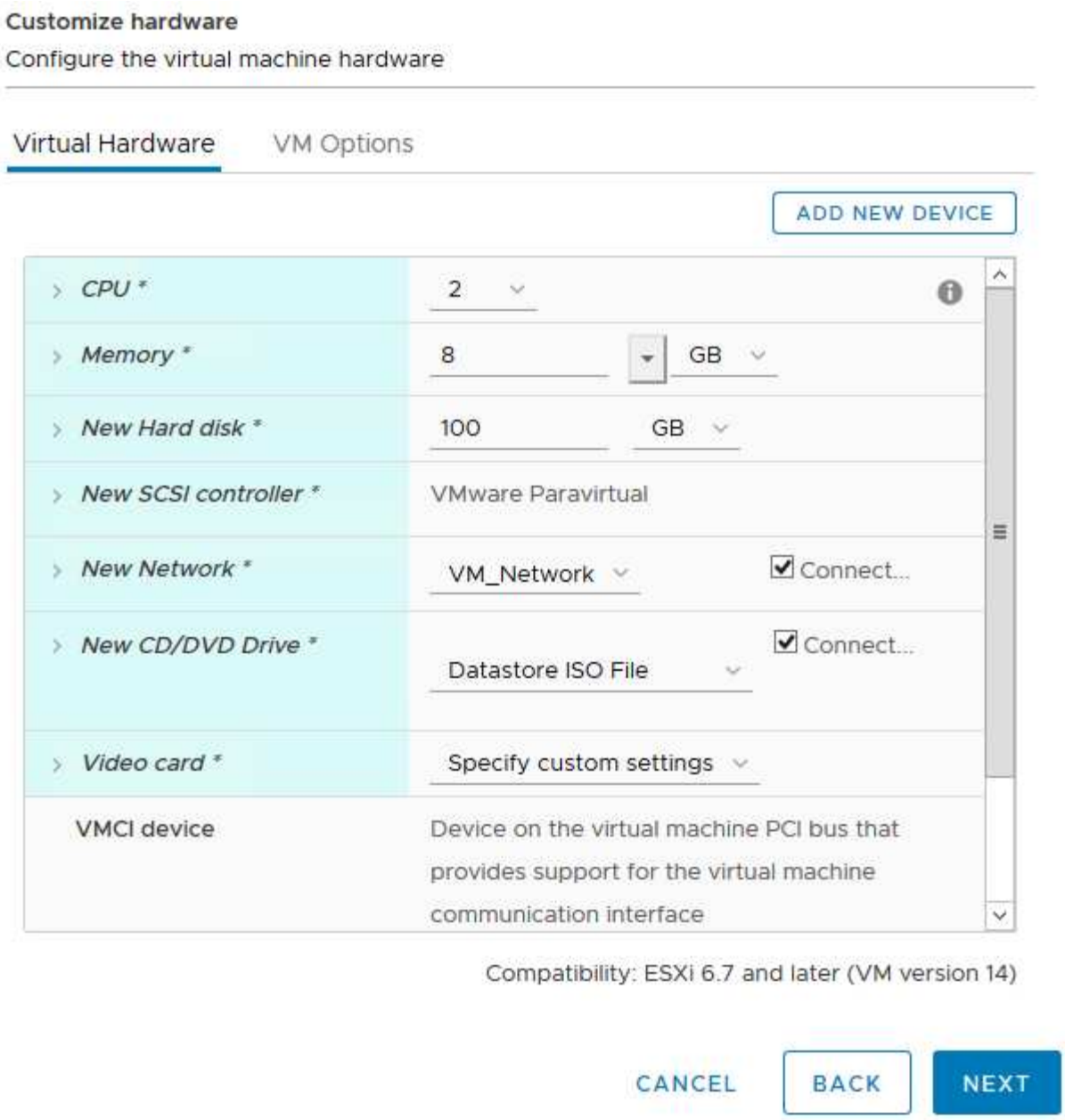
1. 启动 Web 浏览器并登录到 VMware vSphere ，然后选择要托管 VM 的集群。
2. 右键单击该集群，然后从菜单中选择创建虚拟机。



3. 在新建虚拟机向导中，单击下一步。
4. 指定虚拟机的名称并选择要将其安装到的数据中心，然后单击下一步。
5. 在以下页面上，选择要将虚拟机安装到的集群，节点或资源组，然后单击下一步。
6. 选择托管 VM 的共享数据存储库，然后单击下一步。
7. 确认虚拟机的兼容模式已设置为 `ESXi 6.7` 或更高版本 ，然后单击下一步。
8. 选择子操作系统系列 Linux ，子操作系统版本： Red Hat Enterprise Linux 7 （64 位）。



9. 下一页用于自定义虚拟机上的硬件资源。Cloud Insights 采集单元需要以下资源。选择资源后，单击下一步：
   a. 两个 CPU
   b. 8 GB RAM
   c. 100 GB 硬盘空间
   d. 一种可通过端口 443 上的 SSL 连接访问 FlexPod 数据中心和 Cloud Insights 服务器中资源的网络。
   e. 要从中启动的选定 Linux 分发版（Red Hat Enterprise Linux）的 ISO 映像。

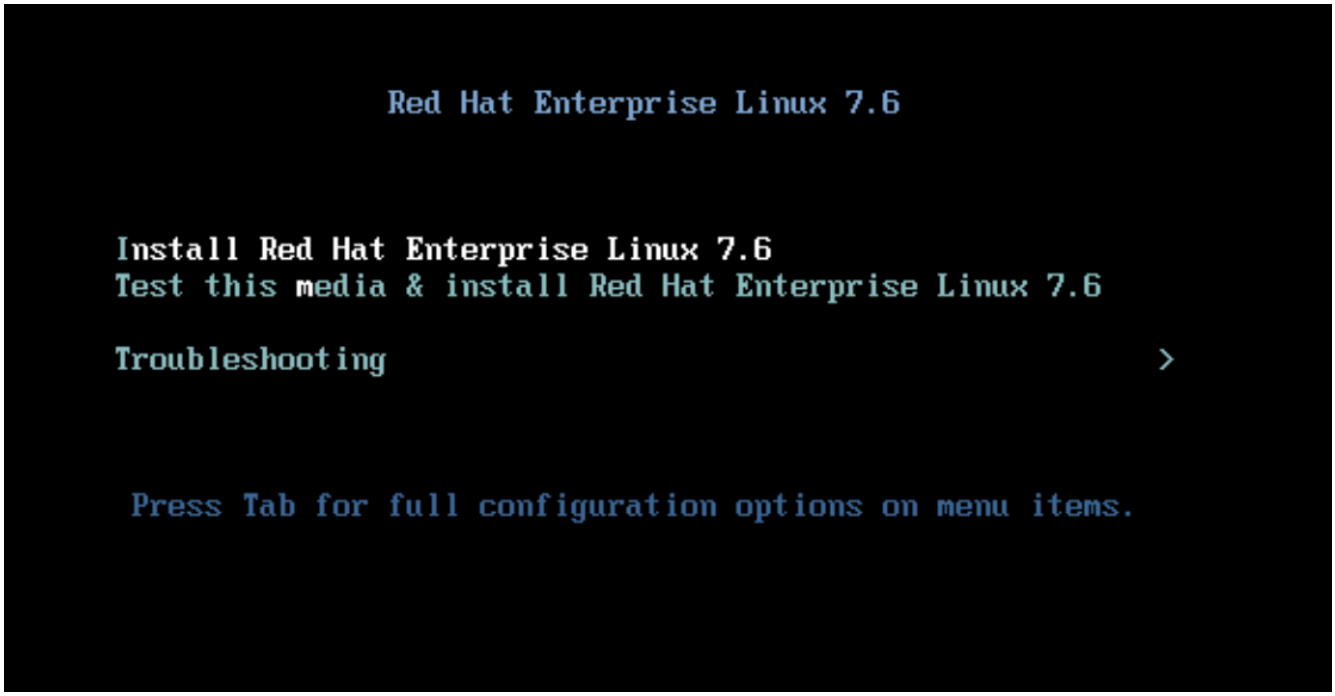


10. 要创建虚拟机，请在准备完成页面上查看设置，然后单击完成。

安装 **Red Hat Enterprise Linux**

要安装 Red Hat Enterprise Linux ，请完成以下步骤：

1. 启动虚拟机，单击窗口以启动虚拟控制台，然后选择安装 Red Hat Enterprise Linux 7.6 选项。

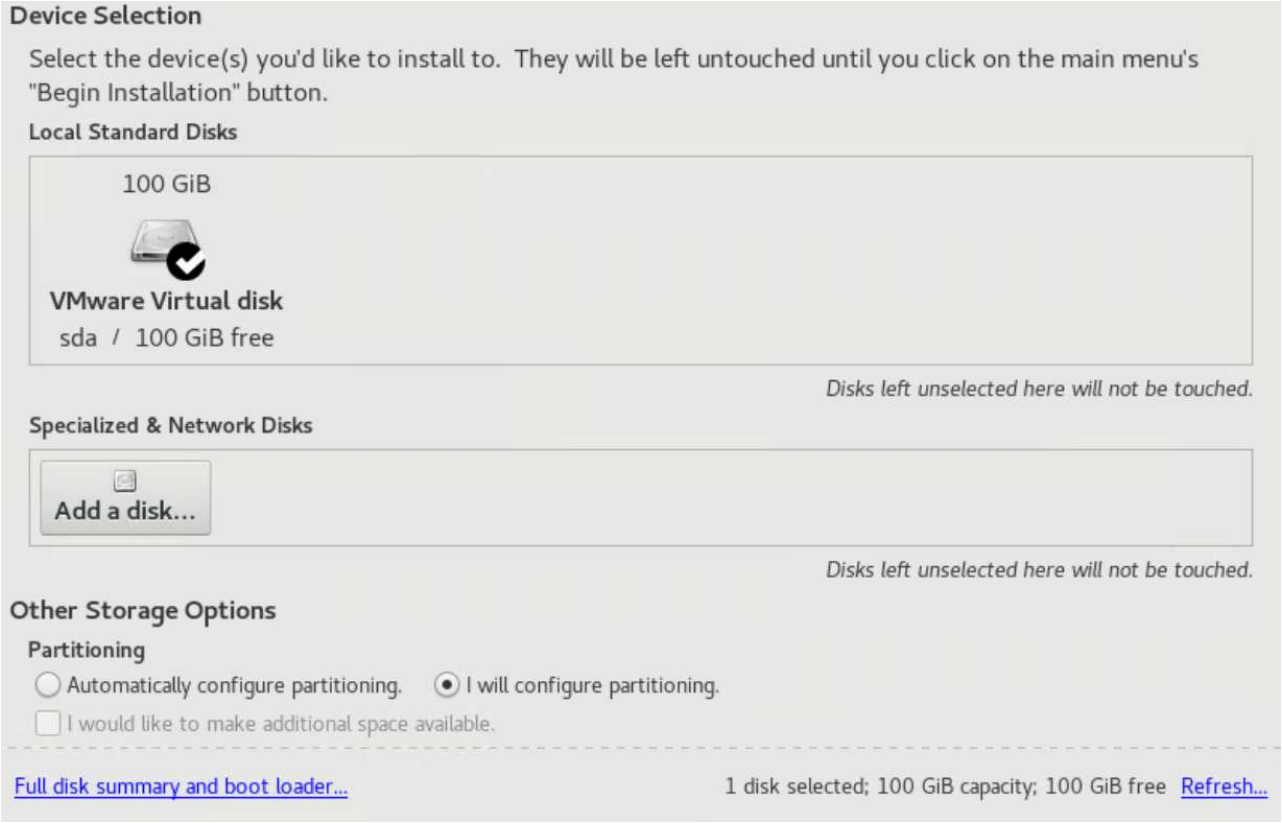


2. 选择首选语言，然后单击 Continue 。

   下一页是安装摘要。大多数选项都应接受默认设置。

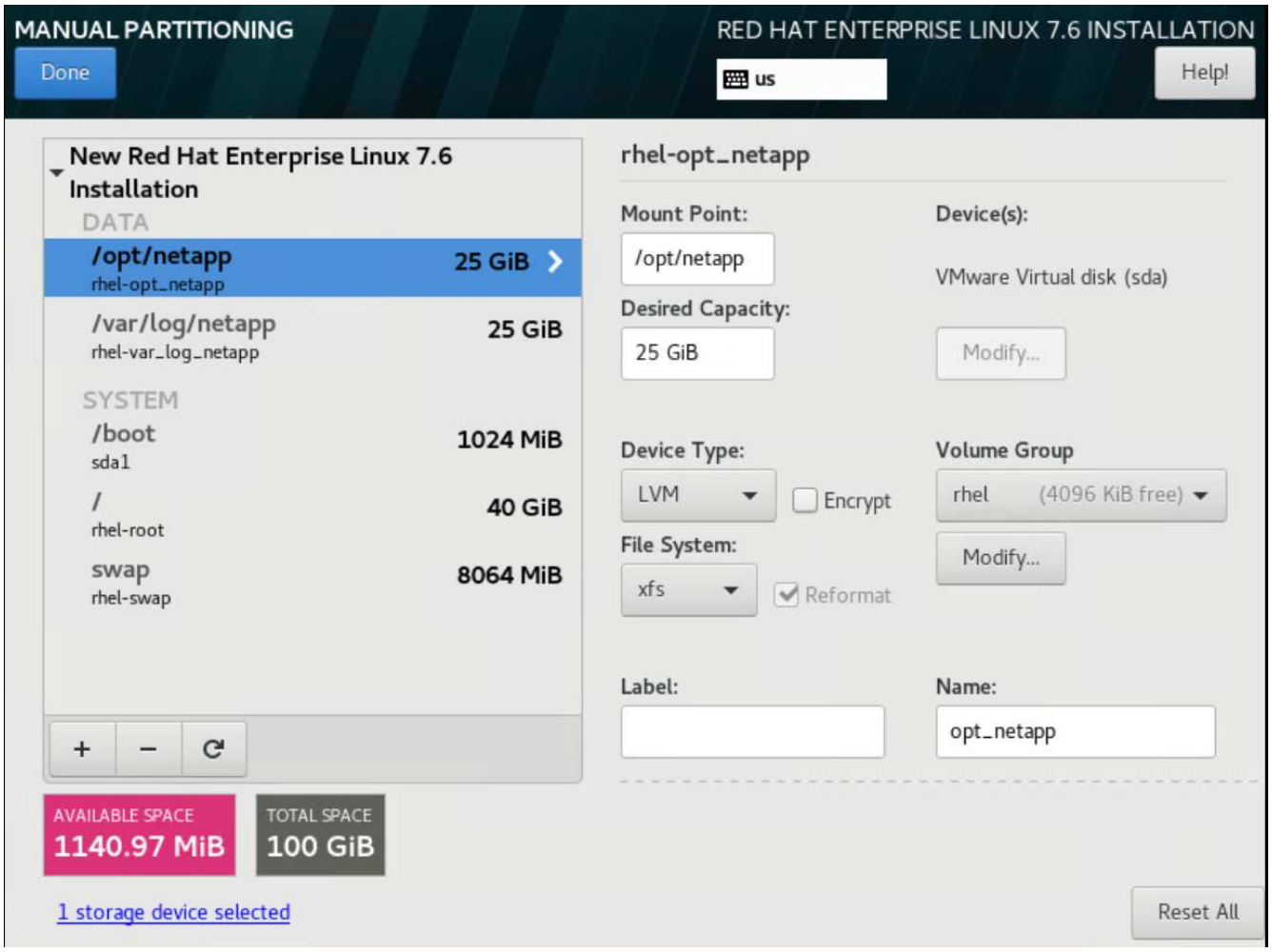
3. 您必须通过执行以下选项来自定义存储布局：

   a. 要自定义服务器的分区，请单击安装目标。
   b. 确认已选择具有黑色复选标记的 100 GiB VMware 虚拟磁盘，然后选择 I will Configure Partitioning 单选按钮。



c. 单击 Done 。

此时将显示一个新菜单，用于自定义分区表。每个为 ` /opt/NetApp` 和 ` /var/log/NetApp` 专用 25 GB 。您可以自动将其余存储分配给系统。

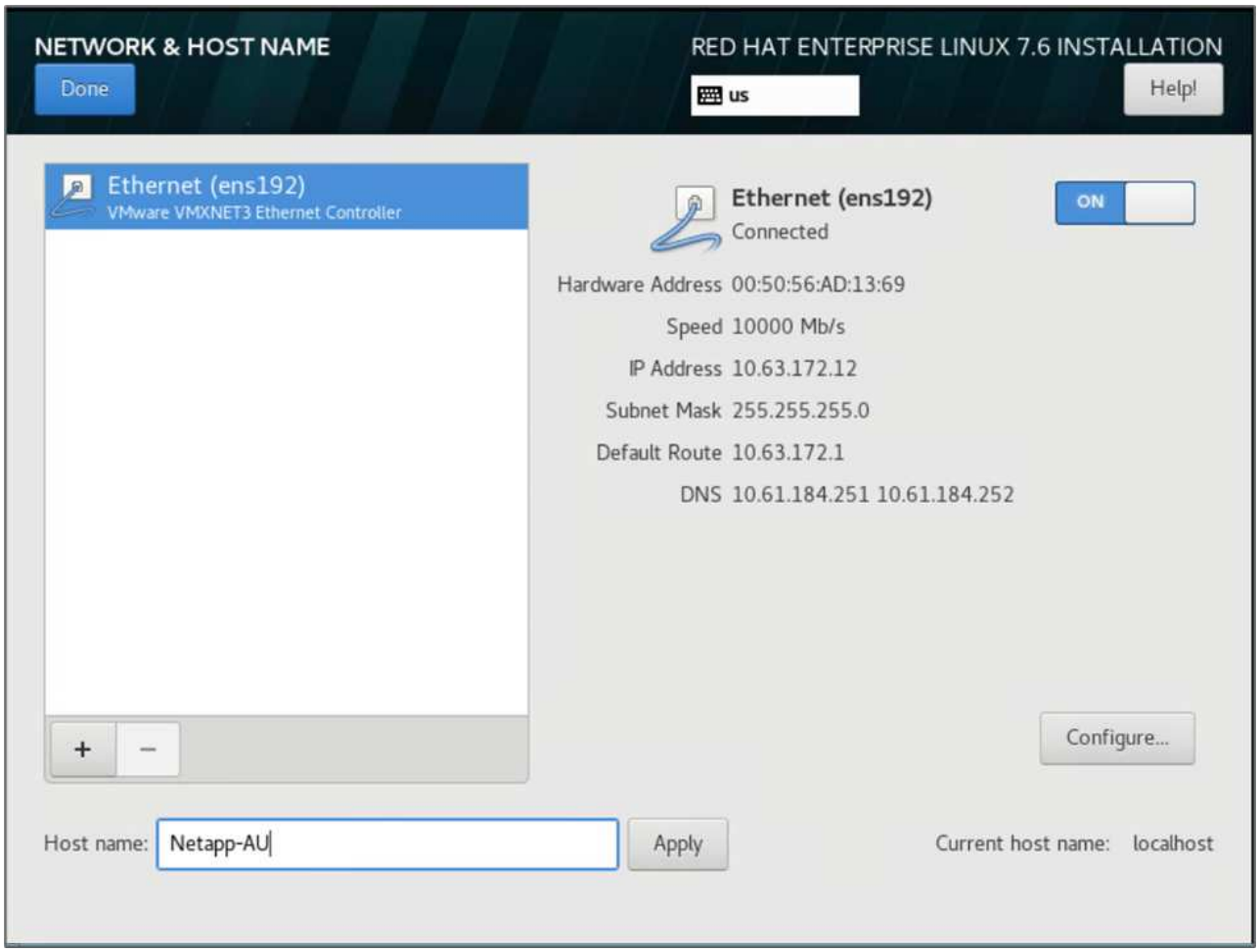


a. 要返回到安装摘要，请单击完成。

4. 单击网络和主机名。

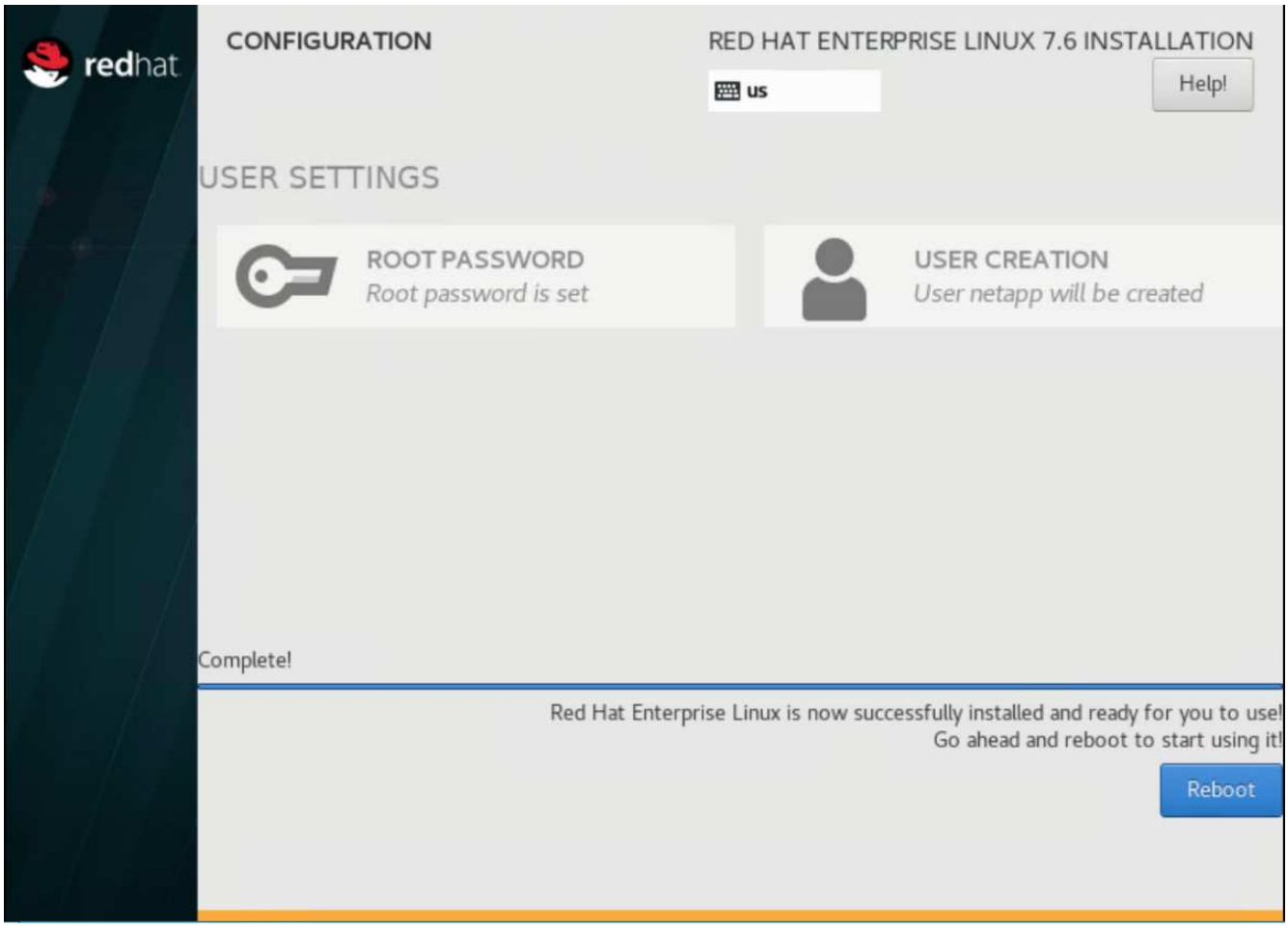
   a. 输入服务器的主机名。

   b. 单击滑块按钮打开网络适配器。如果在网络上配置了动态主机配置协议（DHCP），您将收到一个 IP 地址。如果不是，请单击配置，然后手动分配地址。



c. 。单击 Done 以返回到 Installation Summary 。

5. 在安装摘要页面上，单击开始安装。
6. 在安装进度页面上，您可以设置 root 密码或创建本地用户帐户。安装完成后，单击重新启动以重新启动服务器。



7. 系统重新启动后，登录到服务器并将其注册到 Red Hat 订阅管理器。

```
[root@Netapp-AU ~]# subscription-manager register
Registering to: subscription.rhsm.redhat.com:443/subscription
Username: alan.cowles@netapp.com
Password:
The system has been registered with ID: a47f2e7b-81cd-4757-85c7-eb1818c2c2a1
The registered system name is: Netapp-AU
[root@Netapp-AU ~]#
```

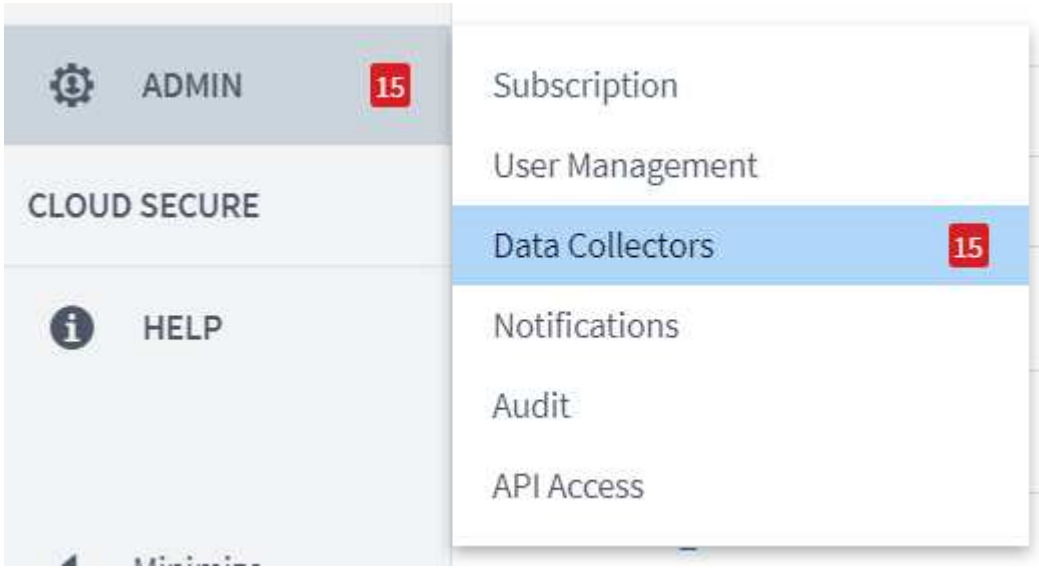
8. 附加 Red Hat Enterprise Linux 的可用订阅。

```
[root@Netapp-AU ~]# subscription-manager attach --pool=8a85f99b710f3b1901713b90b9e154cf
Successfully attached a subscription for: Red Hat Enterprise Linux, Standard Support (128 Sockets, NFR, Partner Only)
[root@Netapp-AU ~]#
```

在 **Cloud Insights** 门户中创建采集单元实例并安装软件

要在 Cloud Insights 门户中创建采集单元实例并安装软件，请完成以下步骤：

1. 从 Cloud Insights 的主页中，将鼠标悬停在主菜单左侧的 "Admin" 条目上，然后从菜单中选择 "Data Collectors" 。

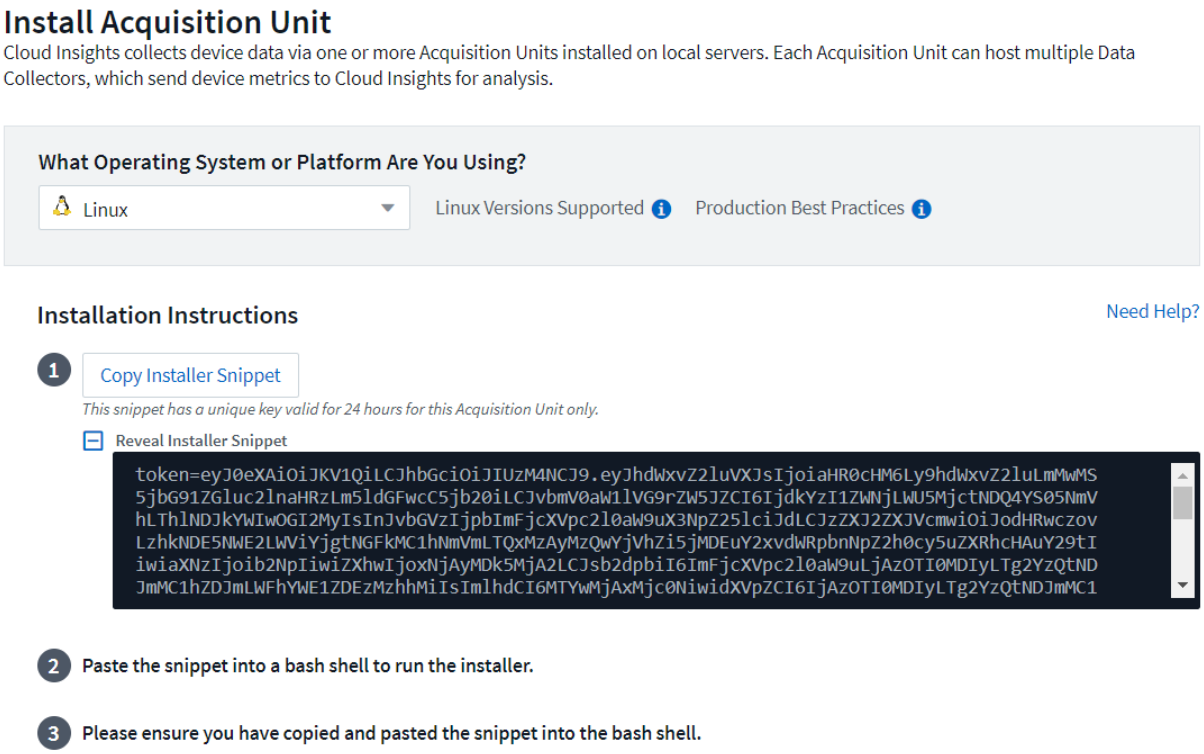


2. 在数据收集器页面的顶部中间，单击采集单元的链接。

3. 要创建新的采集单元，请单击右侧的按钮。

4. 选择要用于托管采集单元的操作系统，然后按照以下步骤从网页复制安装脚本。

   在此示例中，它是一个 Linux 服务器，提供一个代码片段和一个令牌，用于粘贴到主机的命令行界面中。此网页将等待采集单元连接。



5. 将此代码片段粘贴到已配置的 Red Hat Enterprise Linux 计算机的 CLI 中，然后单击 Enter 。

```
[root@Netapp-AU ~]# token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJhdWxvZ2luVXJsIjoiaHR0cHM6Ly9hdWxvZ2luLmMwMS5jbG91ZGluc
2lnaHRzLm5ldGFwcC5jb20iLCJvbmV0aW1lVG9rZW5JZCI6IjQ5ZTY0MGM5LTY5MTItNDQ4Yi04YmI4LTIwNGY2OTQ2YzY1YSIsInJvbGVzIjpbImFjcXVpc
2l0aW9uX3NpZ25lciJdLCJzZXJ2ZXJVcmwiOiJodHRwczovLzhkNDE5NWE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZi5jMDEuY2xvdWRpbnNpZ2h0c
y5uZXRhcHAuY29tIiwiaXNzIjoib2NpIiwiZXhwIjoxNjAyMTgyNzg2LCJsb2dpbiI6ImFjcXVpc2l0aW9uLjc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZ
TcxZjk0ODRiZCIsImlhdCI6MTYwMjA5NjMyNiwidXVpZCI6Ijc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZTcxZjk0ODRiZCIsInRlbmFudCI6IjhkNDE5N
WE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZiIsInRlbmFudFN1YmRvbWFpbiI6InBzMTMyNSJ9.RvWLR3wH1_k6fIOCiO_h-Wok2STfFPDj7VksmXqw
-GZ-JqSIe8SZE4Sv3DuWrWM6 domainUrl=https://8d4195a6-ebb8-4ad0-a6ef-41302340b5af.c01.cloudinsights.netapp.com/rest/v1/au
version=1.253.0 bootstrap=cloudinsights-au-install-bootstrap.sh && curl $proxy_auth_scheme -H "Authorization: Bearer $to
ken" -o $bootstrap $domainUrl/installerBootstrap && sudo chmod 755 $bootstrap && sudo /bin/bash -c "TOKEN=$token HTTPS_P
ROXY=$https_proxy PROXY_AUTH_SCHEME=$proxy_auth_scheme AU_VERSION=$version INSTALLER_NAME=cloudinsights-linux-au-install
er-$version INSTALLER_URL=$domainUrl/installers/linux/$version ./$bootstrap"
```

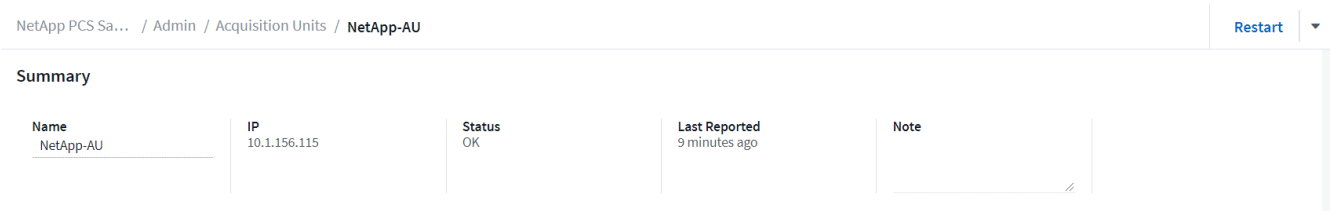
安装程序会下载一个压缩的软件包并开始安装。安装完成后，您会收到一条消息，指出采集单元已注册到 NetApp Cloud Insights 中。

```
Welcome to CloudInsights (R) ..
Acquisition Unit

NetApp (R)
Installation: /opt/netapp/cloudinsights
Logs:         /opt/netapp/cloudinsights/logs -> /var/log/netapp/cloudinsights

To control the CloudInsights service:
  sudo cloudinsights-service.sh --help
To uninstall:
  sudo cloudinsights-uninstall.sh --help

1/8 Acquisition Unit Starting
2/8 Connecting to Cloud Insights
3/8 Sending Certificate-Signing Request..
4/8 Logging in to Cloud Insights
5/8 Updating Security Settings..
6/8 Downloading Data Collection Modules
7/8 Registering to Cloud Insights
8/8 Acquisition Unit Ready

Acquisition Unit has been installed successfully.
[root@Netapp-AU ~]#
```

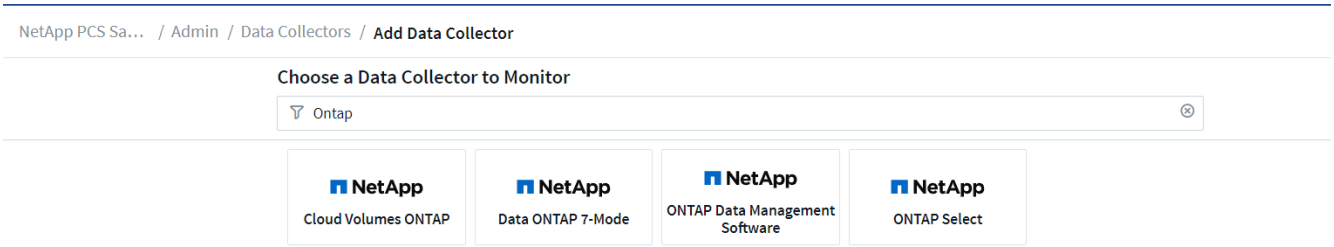
将受监控的存储系统从 **FlexPod** 数据中心添加到 **Cloud Insights**

要从 FlexPod 部署添加 ONTAP 存储系统，请完成以下步骤：

1. 返回到 Cloud Insights 门户上的 Acquisition Units 页面，找到列出的新注册的单元。要显示单元的摘要，请单击该单元。

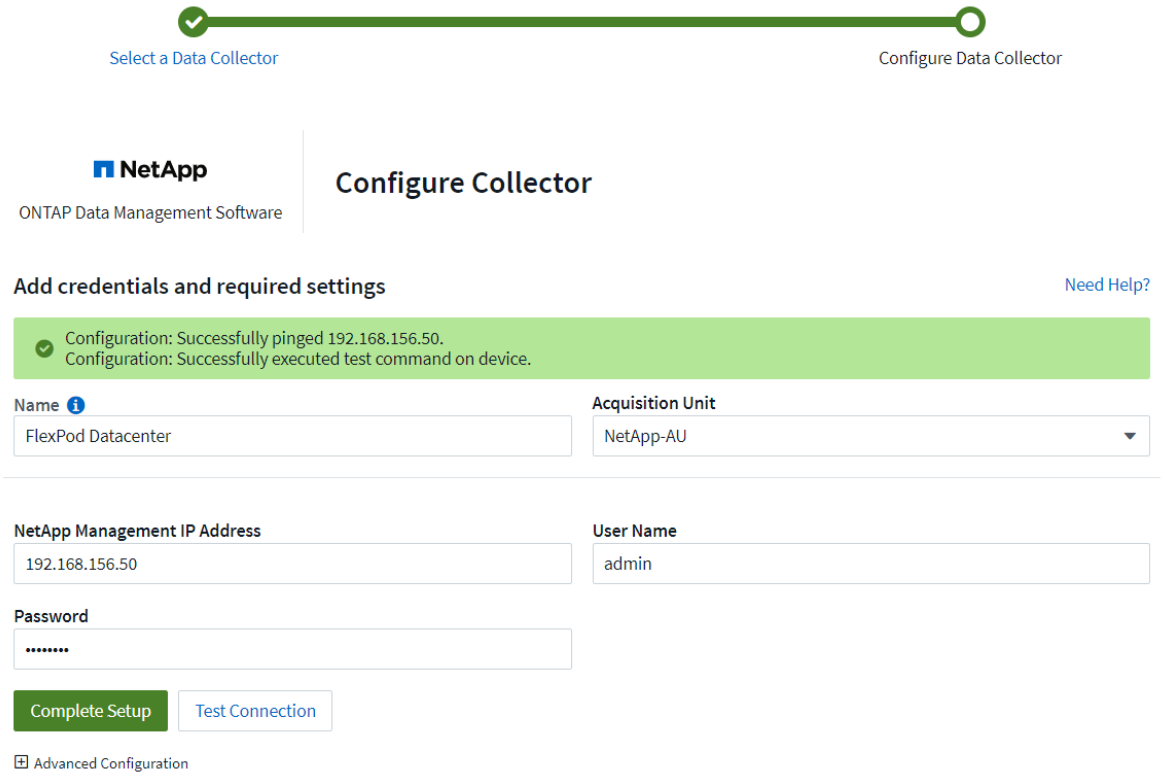


2. 要启动向导以添加存储系统，请在摘要页面上单击用于创建数据收集器的按钮。第一页显示可从中收集数据的所有系统。使用搜索栏搜索 ONTAP 。



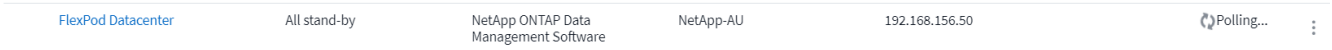
3. 选择 ONTAP 数据管理软件。

   此时将显示一个页面，用于为部署命名并选择要使用的采集单元。您可以提供 ONTAP 系统的连接信息和凭据，并对连接进行测试以确认。



4. 单击 Complete Setup 。

   此门户将返回到 " 数据收集器 " 页面，而数据收集器将开始首次轮询，以便从 FlexPod 数据中心的 ONTAP 存储系统收集数据。



用例

通过设置并配置 Cloud Insights 来监控您的 FlexPod Datacenter 解决方案，我们可以在信

息板上探索一些可执行的任务，以评估和监控您的环境。在本节中，我们重点介绍了 Cloud Insights 的五个主要用例：

- Active IQ 集成
- 探索实时信息板
- 创建自定义信息板
- 高级故障排除
- 存储优化

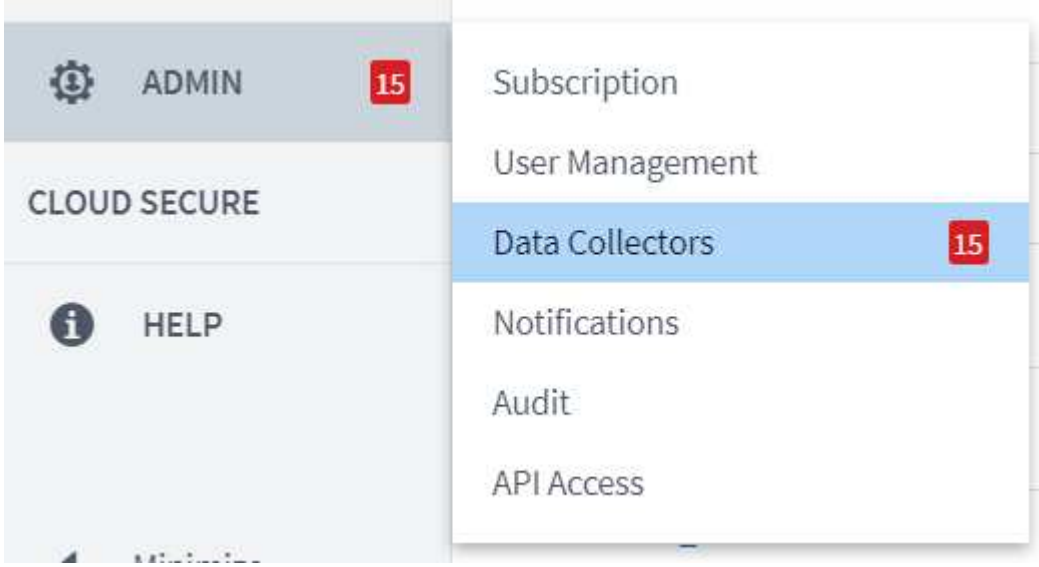
Active IQ 集成

Cloud Insights 已完全集成到 Active IQ 存储监控平台中。作为 FlexPod Datacenter 解决方案的一部分部署的 ONTAP 系统会自动配置为通过每个系统内置的 AutoSupport 功能将信息发送回 NetApp 。这些报告会按计划生成，或者在系统中检测到故障时动态生成。通过 AutoSupport 传输的数据会进行聚合，并显示在 Cloud Insights 的 Active IQ 菜单下易于访问的信息板中。

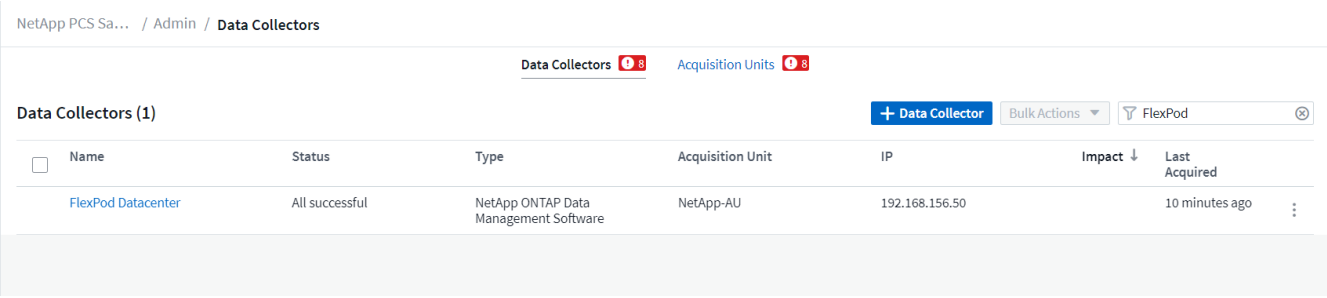
通过 Cloud Insights 信息板访问 Active IQ 信息

要通过 Cloud Insights 信息板访问 Active IQ 信息，请完成以下步骤：

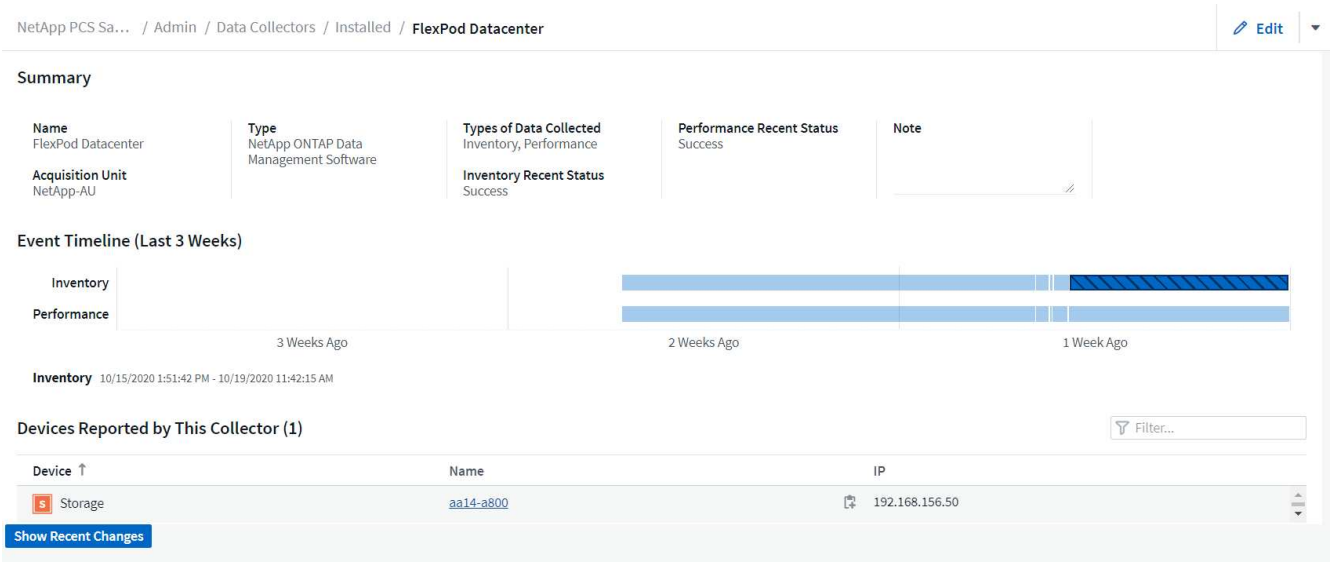
1. 单击左侧管理菜单下的 Data Collector 选项。



2. 筛选环境中的特定 Data Collector 。在此示例中，我们按术语 FlexPod 进行筛选。

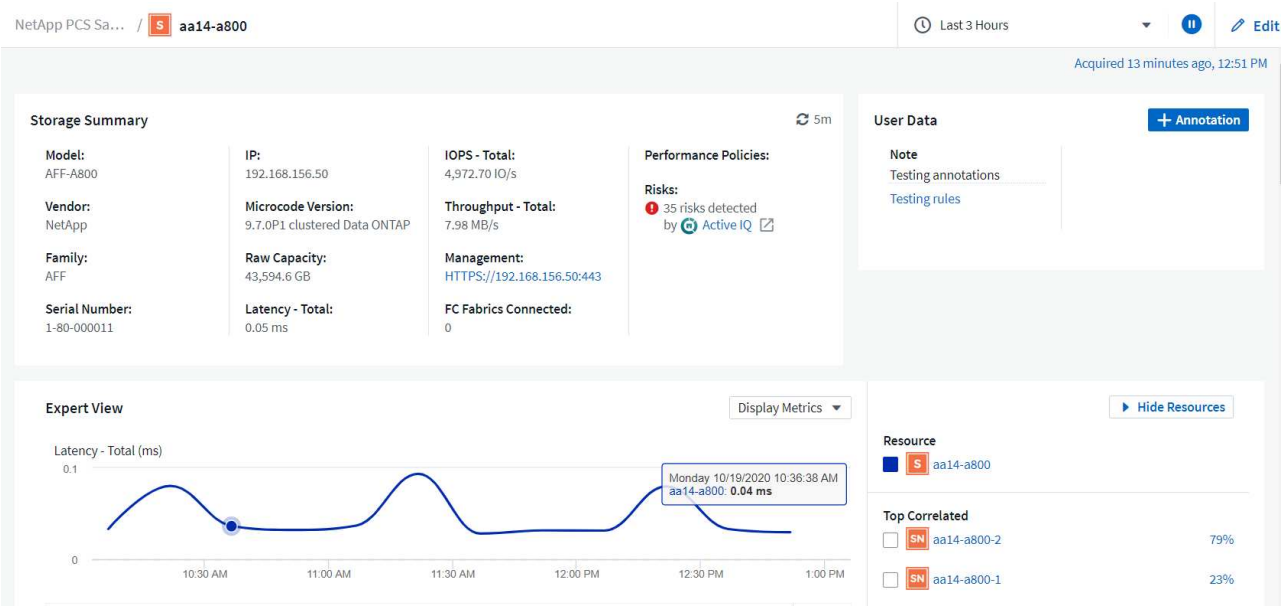


3. 单击 Data Collector 以获取该收集器所监控的环境和设备的摘要。

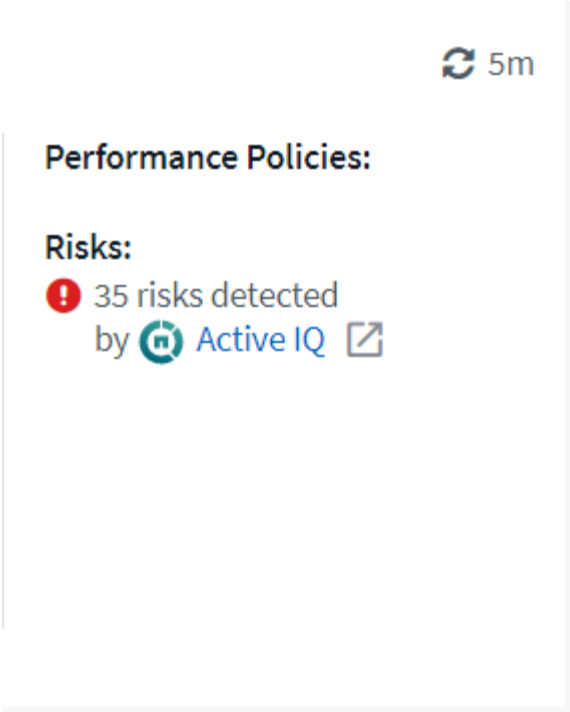


在底部附近的设备列表下，单击要监控的 ONTAP 存储系统的名称。此时将显示一个信息板，其中包含有关系统的信息，包括以下详细信息：

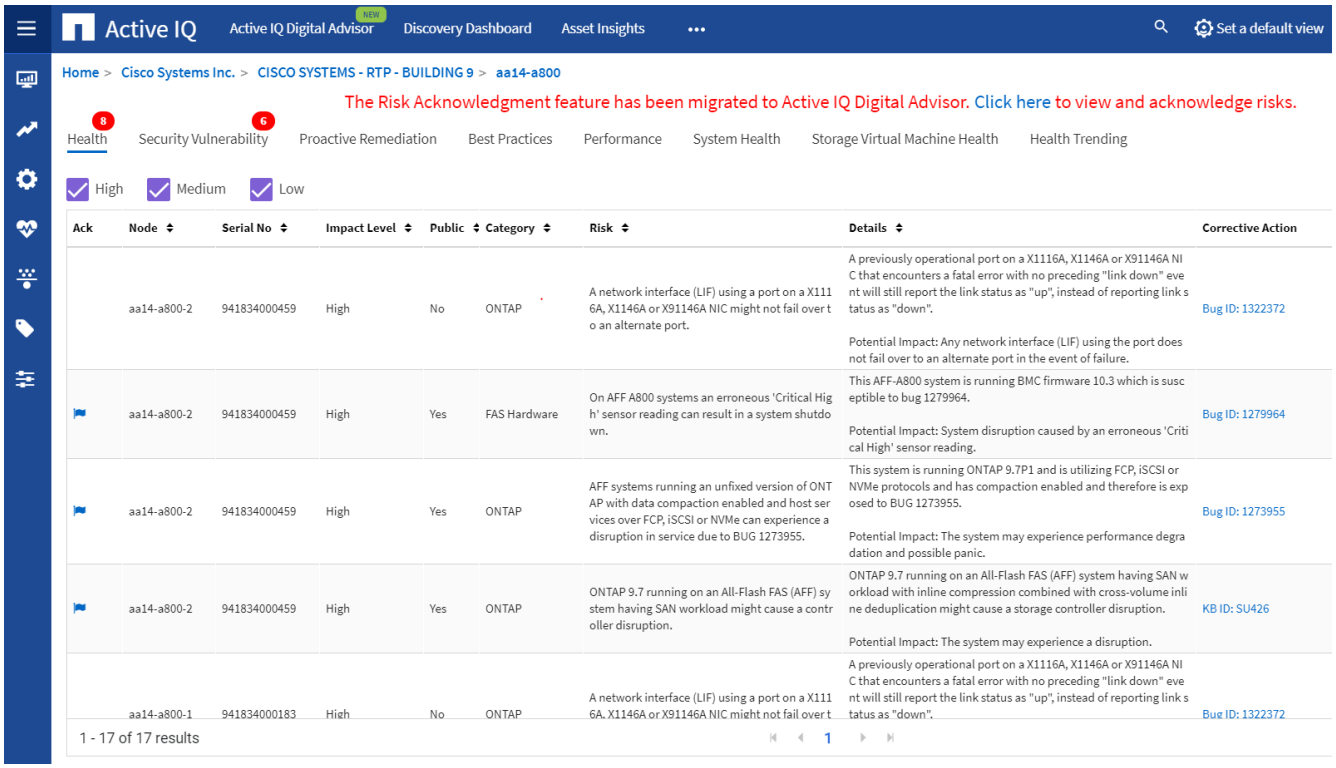
- 型号
- 系列
- ONTAP 版本
- 原始容量
- 平均 IOPS
- 平均延迟
- 平均吞吐量



此外，在此页面上的性能策略部分下，您可以找到指向 NetApp Active IQ 的链接。



4. 要打开一个新的浏览器选项卡并转到风险缓解页面，其中显示了哪些节点受到影响，风险有多严重以及需要采取哪些适当措施来更正已确定的问题，请单击 Active IQ 链接。

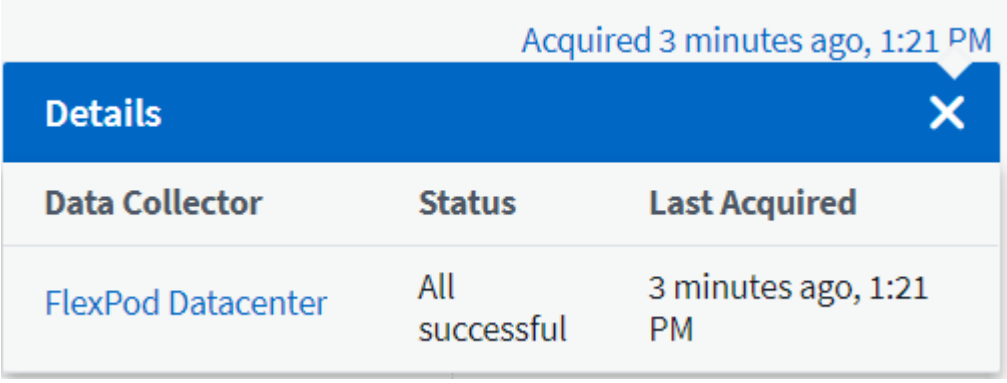


浏览实时信息板

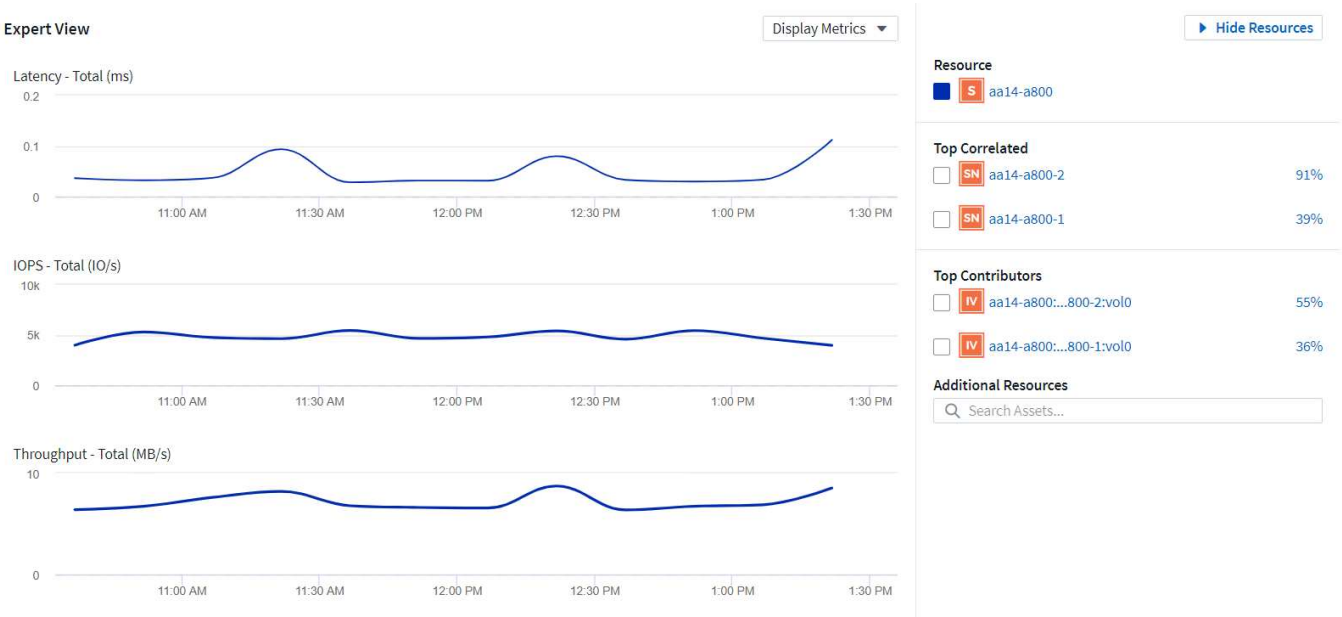
Cloud Insights 可以显示从 FlexPod Datacenter 解决方案中部署的 ONTAP 存储系统轮询的信息的实时信息板。Cloud Insights 采集单元定期收集数据，并使用收集的信息填充默认存储系统信息板。

通过 **Cloud Insights** 信息板访问实时图形

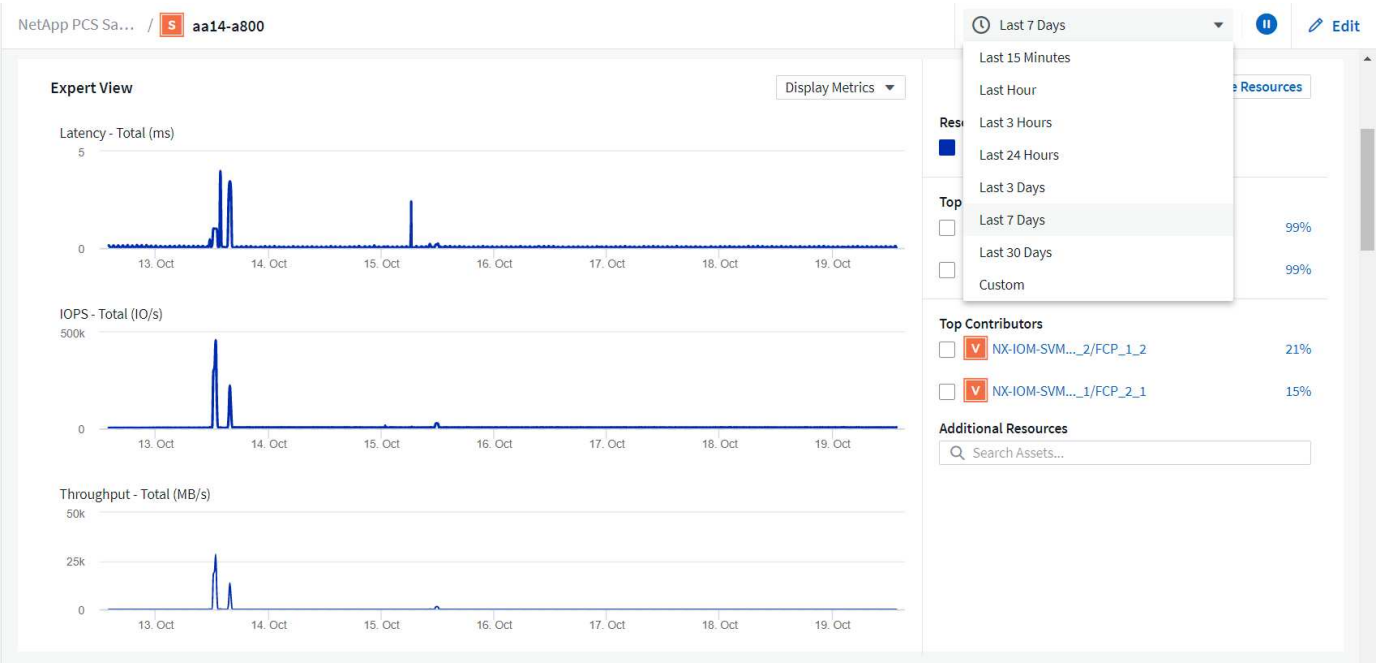
在存储系统信息板中，您可以看到 Data Collector 上次更新信息的时间。下图显示了这方面的一个示例。



默认情况下，存储系统信息板会在 "Expert View" 部分中显示多个交互式图形，这些图形显示所轮询的存储系统或每个节点的系统范围指标，包括：延迟， IOPS 和吞吐量。下图显示了这些默认图形的示例。



默认情况下，图形显示过去三小时的信息，但您可以将其设置为多个不同的值或存储系统信息板右上角下拉列表中的自定义值。如下图所示。



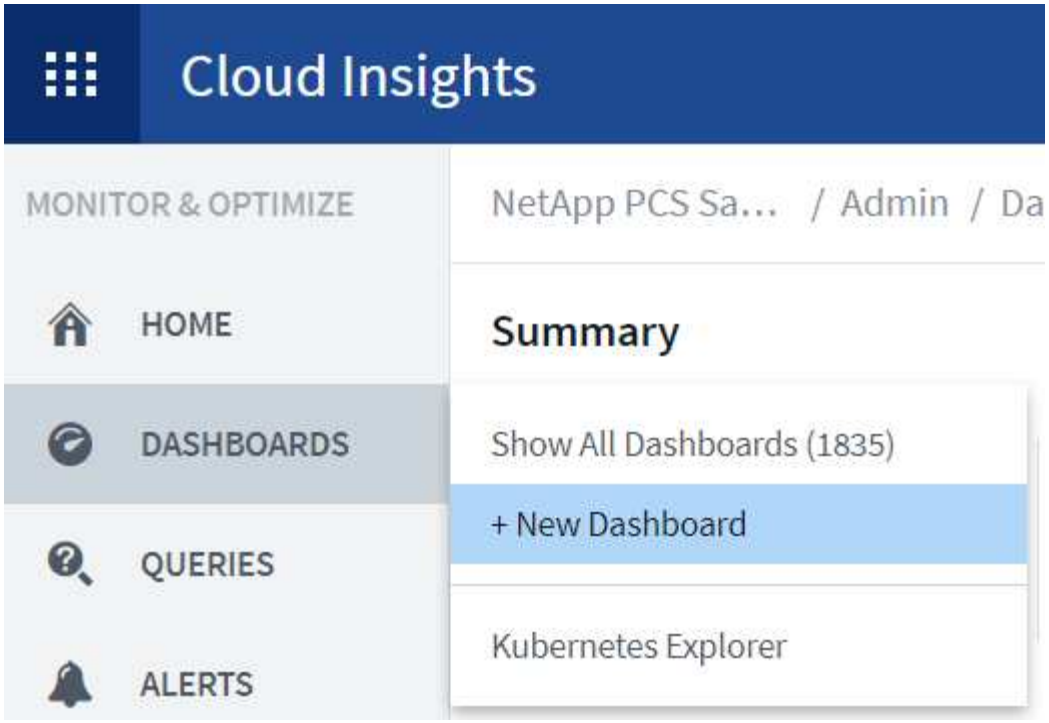
创建自定义信息板

除了使用显示系统范围信息的默认信息板之外，您还可以使用 Cloud Insights 创建完全自定义的信息板，以便集中精力关注 FlexPod Datacenter 解决方案中特定存储卷的资源使用情况。 因此，在融合基础架构中部署的应用程序需要依靠这些卷才能有效运行。这样做可以帮助您更好地了解特定应用程序及其在数据中心环境中使用的资源。

创建自定义信息板以评估存储资源

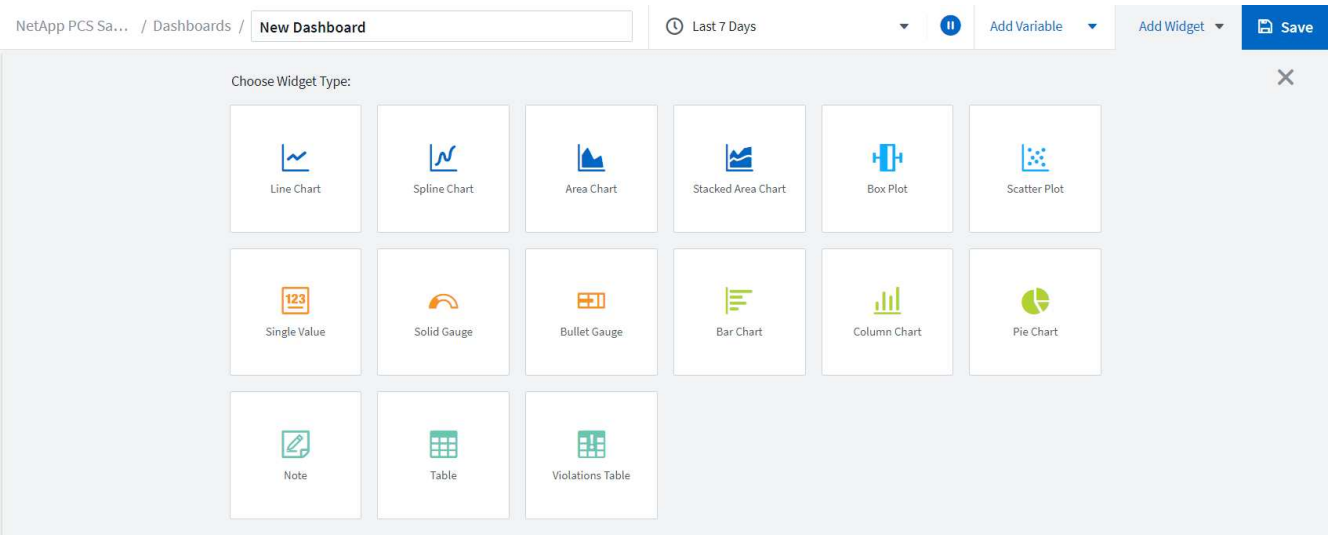
要创建自定义信息板以评估存储资源，请完成以下步骤：

1. 要创建自定义信息板，请将鼠标悬停在 Cloud Insights 主菜单上的 Dashboards 上，然后单击下拉列表中的 + New Dashboard 。



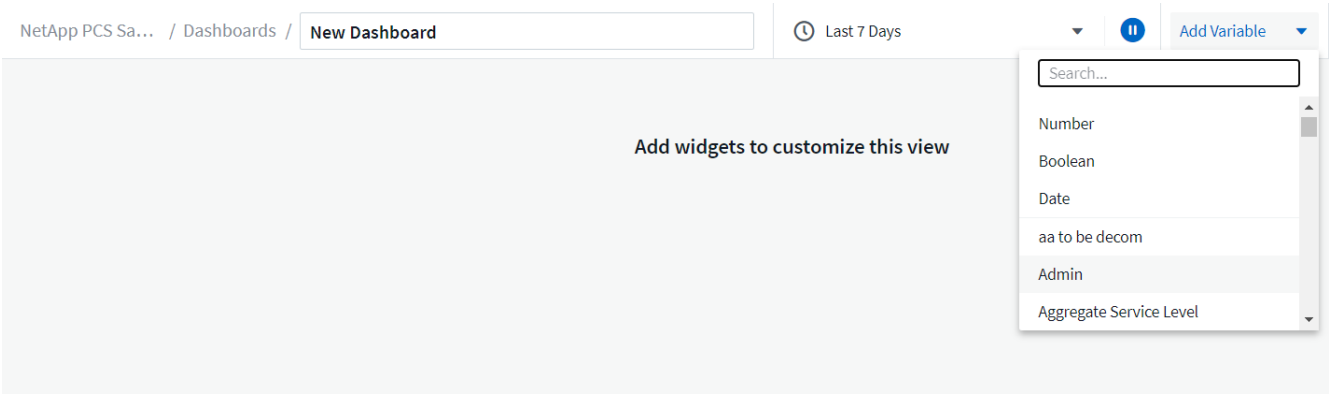
此时将打开 "New Dashboard" 窗口。

2. 为信息板命名，然后选择用于显示数据的小工具类型。您可以从多种图形类型中选择，甚至可以从注释或表类型中选择以显示收集的数据。



3. 从添加变量菜单中选择自定义变量。

   这样，所提供的数据就可以集中显示更具体或更专业的因素。



4. 要创建自定义信息板，请选择要使用的小工具类型，例如饼图以按卷显示存储利用率：

   a. 从添加小工具下拉列表中选择饼图小工具。

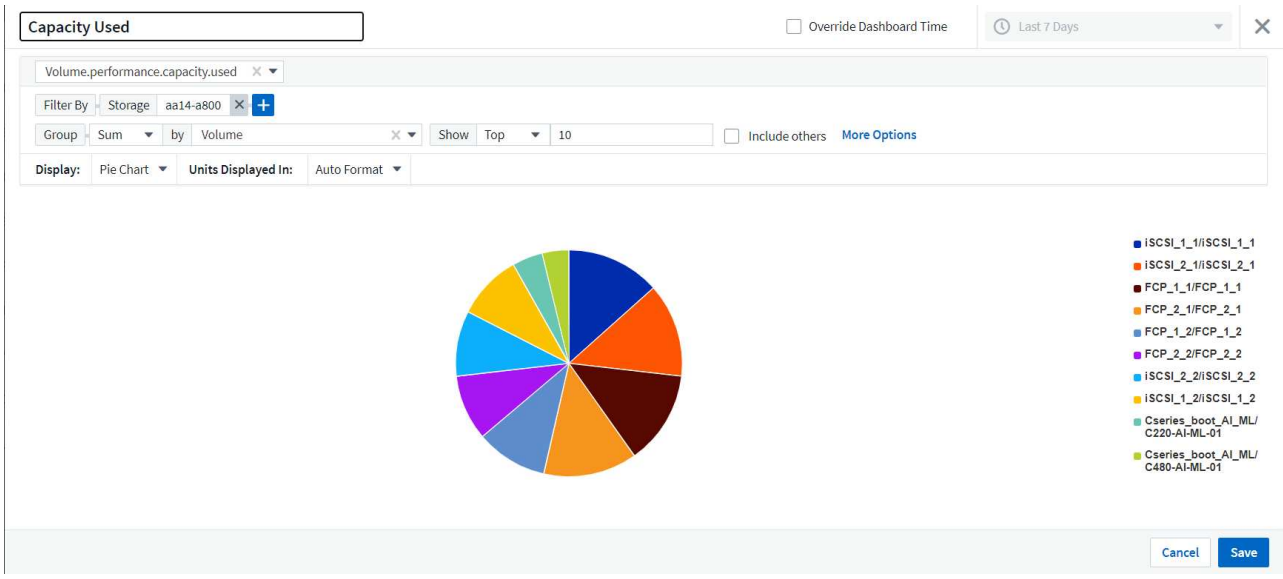
   b. 使用描述性标识符为小工具命名，例如 `Capacity used` 。

   c. 选择要显示的对象。例如，您可以按关键字卷搜索并选择 `volume.performance.capacity.used` 。

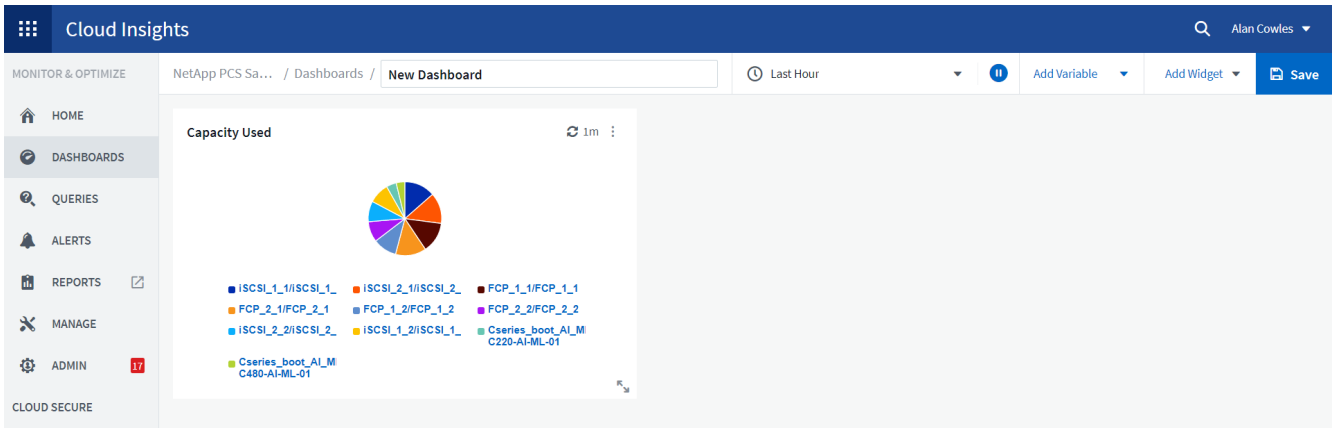
   d. 要按存储系统进行筛选，请使用筛选器并在 FlexPod Datacenter 解决方案中键入存储系统的名称。

   e. 自定义要显示的信息。默认情况下，此选项将显示 ONTAP 数据卷并列出排名前 10 位的卷。

   f. 要保存自定义信息板，请单击 Save 。



保存自定义小工具后，浏览器将返回到 " 新建信息板 " 页面，在此页面中显示新创建的小工具，并允许执行交互操作，例如修改数据轮询期。



高级故障排除

Cloud Insights 支持将高级故障排除方法应用于 FlexPod 数据中心融合基础架构中的任何存储环境。使用上述每个功能的组件： Active IQ 集成，具有实时统计信息的默认信息板以及自定义信息板，可以尽早检测到可能出现的问题并快速解决。使用 Active IQ 中的风险列表，客户可以找到报告的可能导致问题描述的配置错误，或者发现已报告的错误以及可对其进行补救的代码修补版本。通过观察 Cloud Insights 主页上的实时信息板，可以帮助您发现系统性能模式，这种模式可能是问题呈上升趋势的早期指标，并有助于迅速解决问题。最后，客户可以创建自定义信息板，从而可以专注于其基础架构中最重要的资产，并直接监控这些资产，以确保满足其业务连续性目标。

存储优化

除了故障排除之外，还可以使用 Cloud Insights 收集的数据来优化部署在 FlexPod 数据中心融合基础架构解决方案中的 ONTAP 存储系统。如果某个卷的延迟较高，可能是因为多个具有高性能需求的 VM 共享同一个数据存储库，则此信息将显示在 Cloud Insights 信息板上。利用这些信息，存储管理员可以选择将一个或多个 VM 迁移到其他卷，在聚合层之间或 ONTAP 存储系统中的节点之间迁移存储卷，从而实现性能优化的环境。从 Active IQ 与 Cloud Insights 集成中收集的信息可以突出显示导致性能低于预期的配置问题，并提供建议的更正操作，如果实施，可以修复任何问题，并确保存储系统经过优化。

视频和演示

您可以观看有关使用 NetApp Cloud Insights 评估内部环境中资源的视频演示 "此处"。

您可以观看使用 NetApp Cloud Insights 监控基础架构并为基础架构设置警报阈值的视频演示 "此处"。

您可以观看使用 NetApp Cloud Insights 评估环境中各个应用程序的视频演示 "此处"。

追加信息

要了解有关本文档中所述信息的更多信息，请查看以下网站：

- Cisco 产品文档

  "https://www.cisco.com/c/en/us/support/index.html"

- FlexPod 数据中心

  "https://www.flexpod.com"

- NetApp Cloud Insights

  "https://cloud.netapp.com/cloud-insights"

- NetApp 产品文档

  "https://docs.netapp.com"

采用 FabricPool 的 FlexPod —将非活动数据分层到 Amazon AWS S3

TR-4801： 采用 FabricPool 的 FlexPod —将非活动数据分层到 Amazon AWS S3

NetApp 公司 Scott kovacs

闪存存储价格持续下降，因此可供以前不考虑使用闪存存储的工作负载和应用程序使用。但是，最高效地利用存储投资对于 IT 经理来说仍然至关重要。IT 部门仍然需要在极少或根本不增加预算的情况下提供性能更高的服务。为了帮助满足这些需求， NetApp FabricPool 允许您利用云的经济效益，将不常用的数据从昂贵的内部闪存存储迁移到公有云中更经济高效的存储层。将不常访问的数据迁移到云中可释放 AFF 或 FAS 系统上的宝贵闪存存储空间，从而将更多业务关键型工作负载容量提供给高性能闪存层。

本技术报告介绍了 NetApp 和 Cisco 在 FlexPod 融合基础架构架构环境下 ONTAP 的 FabricPool 数据分层功能。您应熟悉 FlexPod 数据中心融合基础架构架构和 ONTAP 存储软件，以便从本技术报告中讨论的概念中充分受益。在熟悉 FlexPod 和 ONTAP 的基础上，我们将讨论 FabricPool ，它的工作原理以及如何使用它来更高效地利用内部闪存存储。本报告中的大部分内容在中进行了更详细的介绍 "TR-4598： FabricPool 最佳实践" 和其他 ONTAP 产品文档。此内容针对 FlexPod 基础架构进行了精简，并不能完全涵盖 FabricPool 的所有使用情形。ONTAP 9.6 提供了所有已研究的功能和概念。

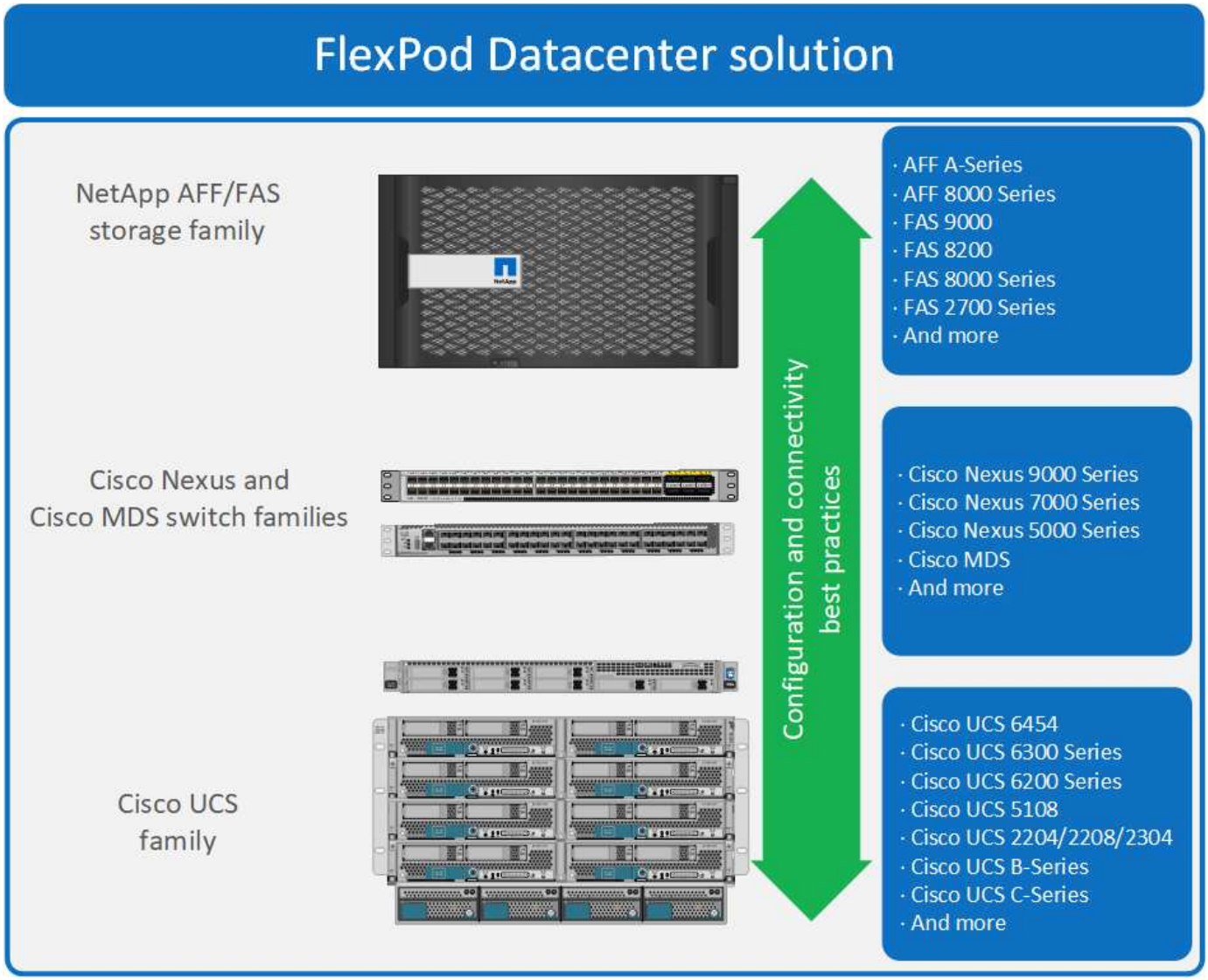
中提供了有关 FlexPod 的追加信息 "TR-4036 FlexPod 数据中心技术规格"。

FlexPod 概述和架构

FlexPod 概述

FlexPod 是一组定义的硬件和软件，可为虚拟化和非虚拟化解决方案奠定集成基础。FlexPod 在一个软件包中包含 NetApp AFF 存储， Cisco Nexus 网络， Cisco MDS 存储网络， Cisco 统一计算系统（ Cisco UCS ）和 VMware vSphere 软件。该设计非常灵活，可以将网络，计算和存储安装到一个数据中心机架中，也可以根据客户的数据中心设计进行部署。端口密度允许网络组件容纳多种配置。

FlexPod 架构的一个优势是能够自定义或灵活调整环境以满足客户的需求。FlexPod 单元可以根据需求和需求的变化轻松进行扩展。一个单元既可以纵向扩展（向 FlexPod 单元添加资源），也可以横向扩展（添加更多 FlexPod 单元）。FlexPod 参考架构重点介绍了光纤通道和基于 IP 的存储解决方案的故障恢复能力，成本效益以及部署简便性。存储系统能够在一个接口上提供多个协议，这为客户提供了一个选择并保护了他们的投资，因为它确实是一种 " 一次线 " 架构。下图显示了 FlexPod 的许多硬件组件。

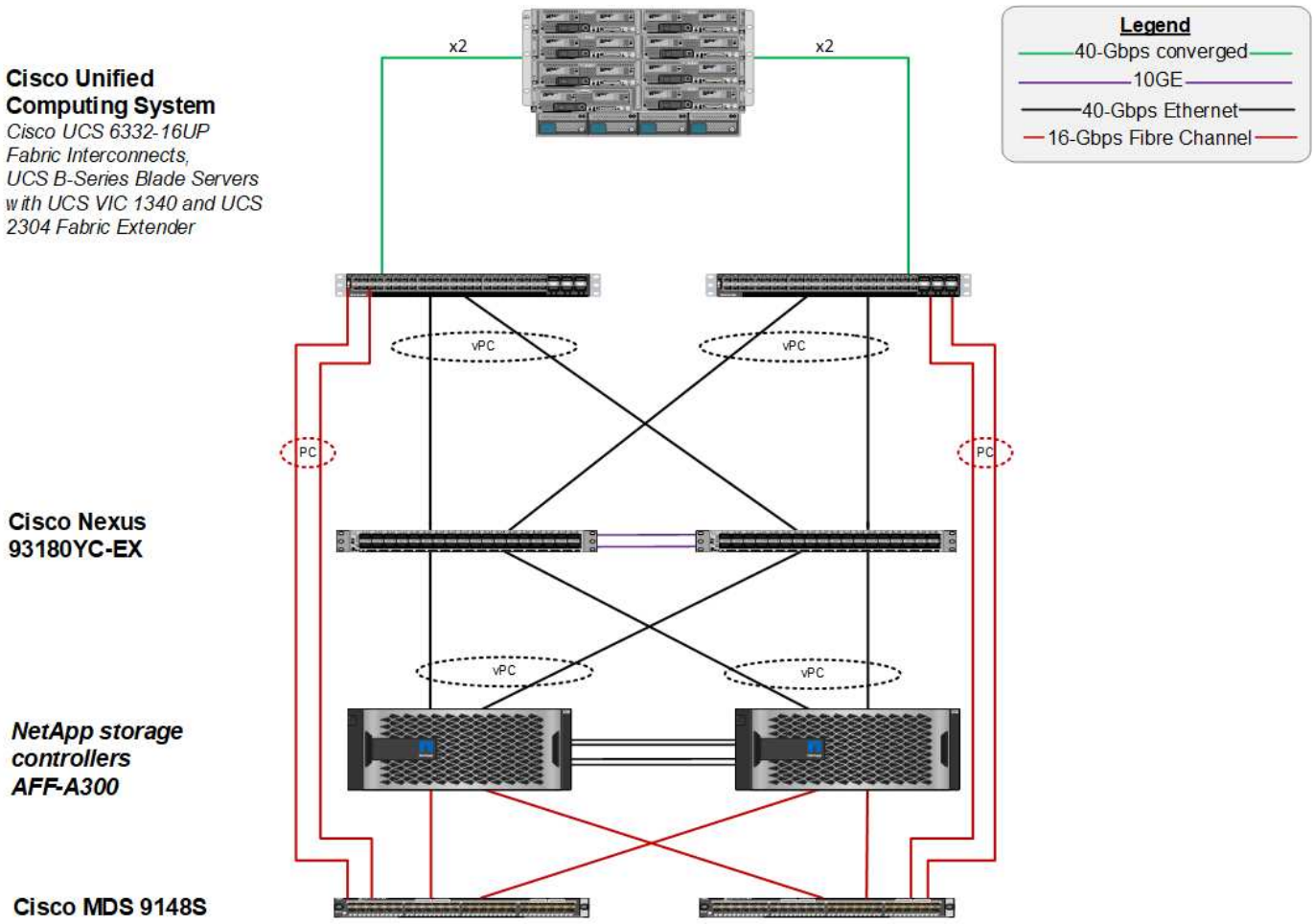


FlexPod 架构

下图显示了 VMware vSphere 和 FlexPod 解决方案的组件以及 Cisco UCS 6454 互联阵列所需的网络连接。此设计包含以下组件：

- Cisco UCS 5108 刀片式服务器机箱与 Cisco UCS 互联阵列之间的端口通道 40 Gb 以太网连接
- Cisco UCS 互联阵列与 Cisco Nexus 9000 之间的 40 Gb 以太网连接
- Cisco Nesxus 9000 和 NetApp AFF A300 存储阵列之间的 40 Gb 以太网连接

随着 Cisco UCS 互联阵列和 NetApp AFF A300 之间的 Cisco MDS 交换机的推出，这些基础架构选项得以扩展。此配置可使 FC 启动的主机对共享存储进行 16 Gb FC 块级访问。此参考架构强化了一次线连接策略，因为在向该架构添加额外存储时，不需要从主机重新布线到 Cisco UCS 互联阵列。



FabricPool

FabricPool 概述

FabricPool 是 ONTAP 中的一种混合存储解决方案，它使用全闪存（ SSD ）聚合作为性能层，并将公有云服务中的对象存储作为云层。根据数据是否经常访问，此配置可以基于策略移动数据。ONTAP 平台上的 AFF 和纯 SSD 聚合在 FabricPool 中均支持 FAS 。数据处理在块级别执行，全闪存性能层中经常访问的数据块标记为热块，不常访问的数据块标记为冷块。

使用 FabricPool 有助于降低存储成本，而不会影响性能，效率，安全性或保护。FabricPool 对企业级应用程序是透明的，它可以降低存储 TCO ，而无需重新构建应用程序基础架构，从而充分利用云效率。

FlexPod 可以从 FabricPool 的存储分层功能中受益，从而更高效地利用 ONTAP 闪存存储。非活动虚拟机（ VM ），不常用的 VM 模板以及 NetApp SnapCenter for vSphere 中的 VM 备份可能会占用数据存储库卷中的宝贵空间。将冷数据移至云层可为 FlexPod 基础架构上托管的高性能任务关键型应用程序释放空间和资源。

> 光纤通道和 iSCSI 协议通常需要较长的时间才能发生超时（ 60 到 120 秒），但它们不会像 NAS 协议那样重试建立连接。如果 SAN 协议超时，则必须重新启动应用程序。即使是短暂的中断，也可能对使用 SAN 协议的生产应用程序造成灾难性的后果，因为无法保证与公有云的连接。为了避免这种问题描述， NetApp 建议在对 SAN 协议访问的数据进行分层时使用私有云。

在 ONTAP 9.6 中， FabricPool 与所有主要公有云提供商相集成：阿里云对象存储服务， Amazon AWS S3 ，Google 云存储， IBM 云对象存储和 Microsoft Azure Blob 存储。本报告重点介绍了 Amazon AWS S3 存储作为云对象层的选择。

复合聚合

通过将 ONTAP 闪存聚合与云对象存储（例如 AWS S3 存储分段）关联来创建 FabricPool 实例，以创建复合聚合。在复合聚合中创建卷时，它们可以利用 FabricPool 的分层功能。将数据写入卷时， ONTAP 会为每个数据块分配一个温度。首次写入块时，会为其分配温度为 " 热 " 。随着时间的推移，如果不访问数据，则会经历一个冷却过程，直到最终将其分配为冷状态为止。然后，这些不常访问的数据块将从性能 SSD 聚合分层到云对象存储。

ONTAP 中的卷分层策略会修改块从指定为冷存储到移动到云对象存储这段时间。通过修改 ONTAP 设置，控制块变冷所需的天数，可以进一步细化。数据分层的候选对象包括传统卷快照，适用于 vSphere 的 SnapCenter VM 备份和其他基于 NetApp Snapshot 的备份，以及 vSphere 数据存储库中任何不常用的块，例如 VM 模板和不常访问的 VM 数据。

非活动数据报告

ONTAP 中提供了非活动数据报告（ IDR ）功能，用于帮助评估可从聚合分层的冷数据量。默认情况下，ONTAP 9.6 会启用 IDR ，并使用默认的 31 天散热策略来确定卷中的哪些数据处于非活动状态。

> 分层的冷数据量取决于卷上设置的分层策略。此数量可能与 IDR 使用默认 31 天冷却期检测到的冷数据量不同。

对象创建和数据移动

FabricPool 可在 NetApp WAFL 块级别运行，并可运行散热块，将这些块串联到存储对象中，然后将这些对象迁移到云层。每个 FabricPool 对象均为 4 MB ，由 1 ， 024 个 4 KB 块组成。根据领先云提供商的性能建议，对象大小固定为 4 MB ，不能更改。如果读取冷块并使其变热，则只会提取 4 MB 对象中请求的块并将其移回性能层。整个对象和整个文件都不会迁移回。仅迁移必要的块。

> 如果 ONTAP 检测到顺序读取的机会，则会在读取数据块之前从云层请求数据块以提高性能。

默认情况下，只有在性能聚合利用率超过 50% 时，才会将数据移至云层。可以将此阈值设置为较低的百分比，以便将性能闪存层上的少量数据存储移至云。如果分层策略是仅在聚合接近容量时移动冷数据，则这可能很有用。

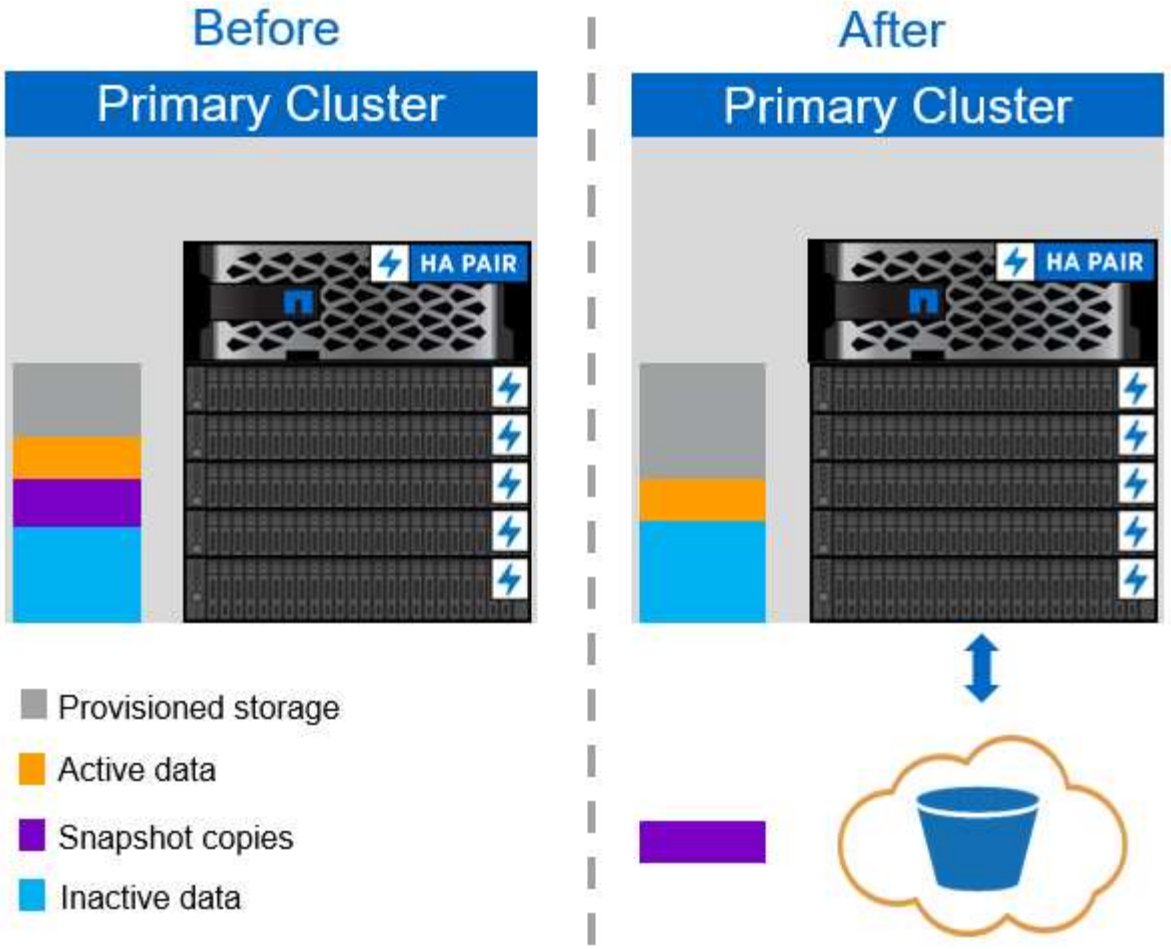
如果性能层利用率超过 70% 的容量，则冷数据将直接从云层读取，而不会回写到性能层。通过防止对使用率较高的聚合执行冷数据回写， FabricPool 可保留聚合以用于活动数据。

回收性能层空间

如前文所述， FabricPool 的主要使用情形是帮助最高效地使用高性能内部闪存存储。FlexPod 虚拟基础架构的卷快照和 VM 备份形式的冷数据可能会占用大量昂贵的闪存存储。通过实施以下两种分层策略之一，可以释放有价值的性能层存储：仅快照或自动。

仅 **Snapshot** 分层策略

下图所示的仅 Snapshot 分层策略将占用空间但未与活动文件系统共享块的 VM 的冷卷快照数据和 SnapCenter for vSphere 备份移动到云对象存储中。仅 Snapshot 分层策略会将冷数据块移至云层。如果需要还原，则云中的冷块会变热并移回内部的性能闪存层。

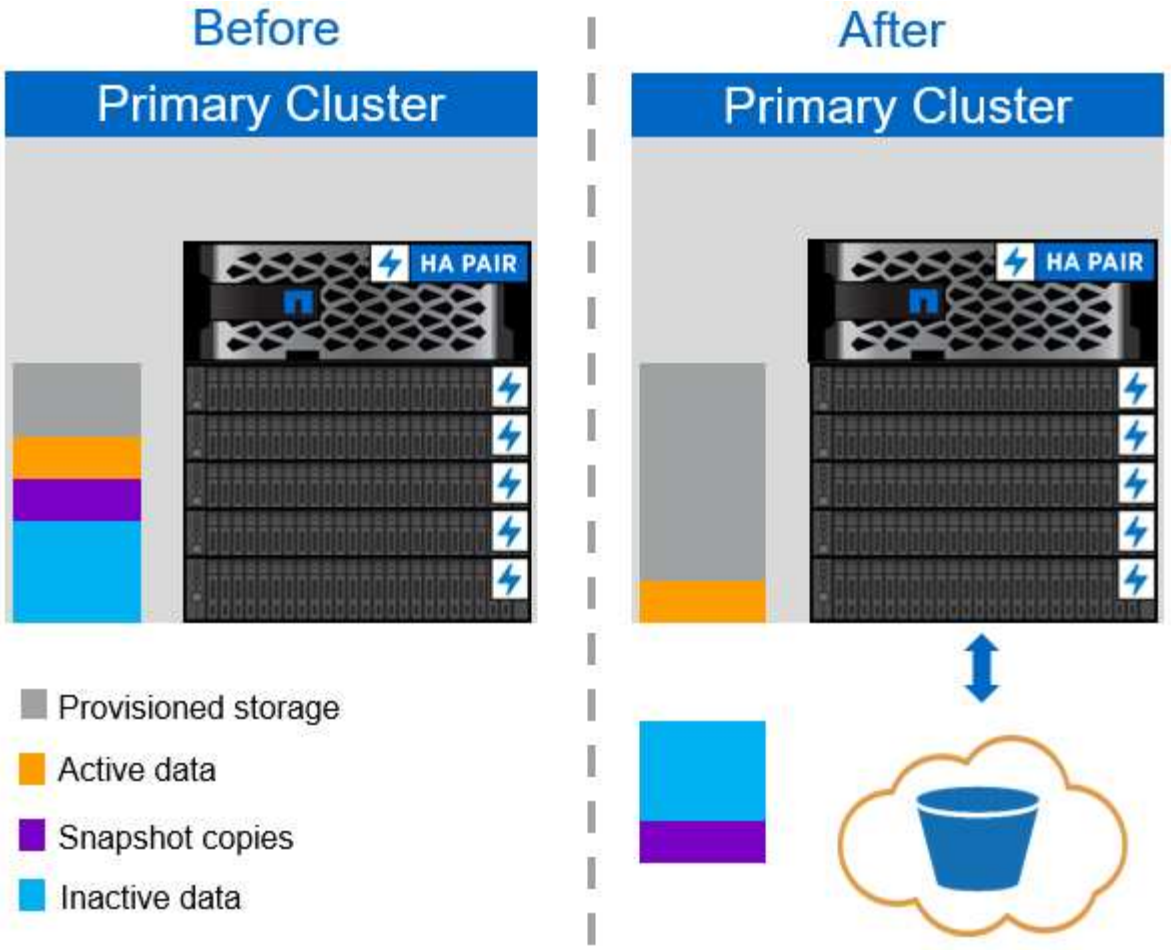


自动分层策略

下图所示的 FabricPool 自动分层策略不仅会将冷快照数据块移至云，还会移动活动文件系统中的任何冷块。这可能包括 VM 模板以及数据存储库卷中未使用的任何 VM 数据。移动哪些冷块由卷的 `tiering-minimum-cooling-days` 设置控制。如果应用程序随机读取云层中的冷块，则这些块会变热并恢复到性能层。但是，如果冷块通过防病毒扫描程序等顺序进程读取，则这些块将保持冷状态并保留在云对象存储中；它们不会移回性能层。

使用自动分层策略时，不常访问的热块将以云连接的速度从云层中回滚。如果应用程序对延迟敏感，则可能会影响虚拟机性能，在对数据存储库使用自动分层策略之前，应考虑这一点。NetApp 建议将集群间 LIF 放置在速度为 10GbE 的端口上，以获得足够的性能。

> 在将对象存储附加到 FabricPool 聚合之前，应使用对象存储配置器测试该对象存储的延迟和吞吐量。



所有分层策略

与 " 自动 " 和 " 仅 Snapshot " 策略不同，所有分层策略会将整个数据卷立即移动到云层。此策略最适合二级数据保护或归档卷，对于这些卷，数据必须出于历史或法规目的进行保留，但很少被访问。不建议对 VMware 数据存储库卷使用 all 策略，因为写入数据存储库的任何数据都会立即移至云层。后续读取操作将从云执行，可能会给驻留在数据存储库卷中的 VM 和应用程序带来性能问题。

安全性

安全性是云和 FabricPool 关注的核心问题。性能层支持 ONTAP 的所有原生安全功能，在将数据传输到云层时，数据移动也会受到保护。FabricPool 使用 "AES-256-GCM" 在性能层上使用加密算法，并将此加密端到云层进行维护。移动到云对象存储的数据块通过传输层安全（ Transport Layer Security ， TLS ） v1.2 进行保护，以保持存储层之间的数据机密性和完整性。

> 支持通过未加密连接与云对象存储进行通信，但 NetApp 不建议这样做。

数据加密

数据加密对于保护知识产权，贸易信息和个人身份客户信息至关重要。FabricPool 完全支持 NetApp 卷加密（ NetApp Volume Encryption ， NVE ）和 NetApp 存储加密（ NetApp Storage Encryption ， NSE ），以维护现有数据保护策略。将性能层上的所有加密数据移动到云层时，这些数据仍保持加密状态。客户端加密密钥归 ONTAP 所有，服务器端对象存储加密密钥归相应的云对象存储所有。未使用 NVE 加密的任何数据都将使用 AES-256-GCM 算法进行加密。不支持其他 AES-256 密码。

使用 NSE 或 NVE 是可选的，使用 FabricPool 不需要。

FabricPool 要求

FabricPool 要求使用 ONTAP 9.2 或更高版本，并在本节列出的任何平台上使用 SSD 聚合。其他 FabricPool 要求取决于所附加的云层。对于容量固定且相对较小的入门级 AFF 平台，例如 NetApp AFF C190 ， FabricPool 可以非常高效地将非活动数据移至云层。

平台

以下平台支持 FabricPool：

- NetApp AFF
  - A800
  - A700S ， A700
  - A320 ， A300
  - A220 ， A200
  - C190
  - AFF8080 ， AFF8060 和 AFF8040
- NetApp FAS
  - FAS9000
  - FAS8200
  - FAS8080 ， FAS8060 和 FAS8040
  - FAS2750 ， FAS2720
  - FAS2650 ， FAS2620

只有 FAS 平台上的 SSD 聚合才能使用 FabricPool 。

- 云层
  - 阿里云对象存储服务（标准，不常访问）
  - Amazon S3 （ Standard ， Standard-IA ， One Zone-IA ，智能分层）
  - Amazon Commercial Cloud Services （ C2S ）
  - Google Cloud Storage （多区域，区域，近线，冷线）
  - IBM Cloud Object Storage （标准，存储，冷存储， Flex ）
  - Microsoft Azure Blob Storage （热存储和冷存储）

集群间 **LIFs**

使用 FabricPool 的集群高可用性（ HA ）对需要两个集群间逻辑接口（ LIF ）才能与云层进行通信。NetApp 建议在其他 HA 对上创建集群间 LIF ，以便将云层无缝附加到这些节点上的聚合。

ONTAP 用于连接到 AWS S3 对象存储的 LIF 必须位于 10 Gbps 端口上。

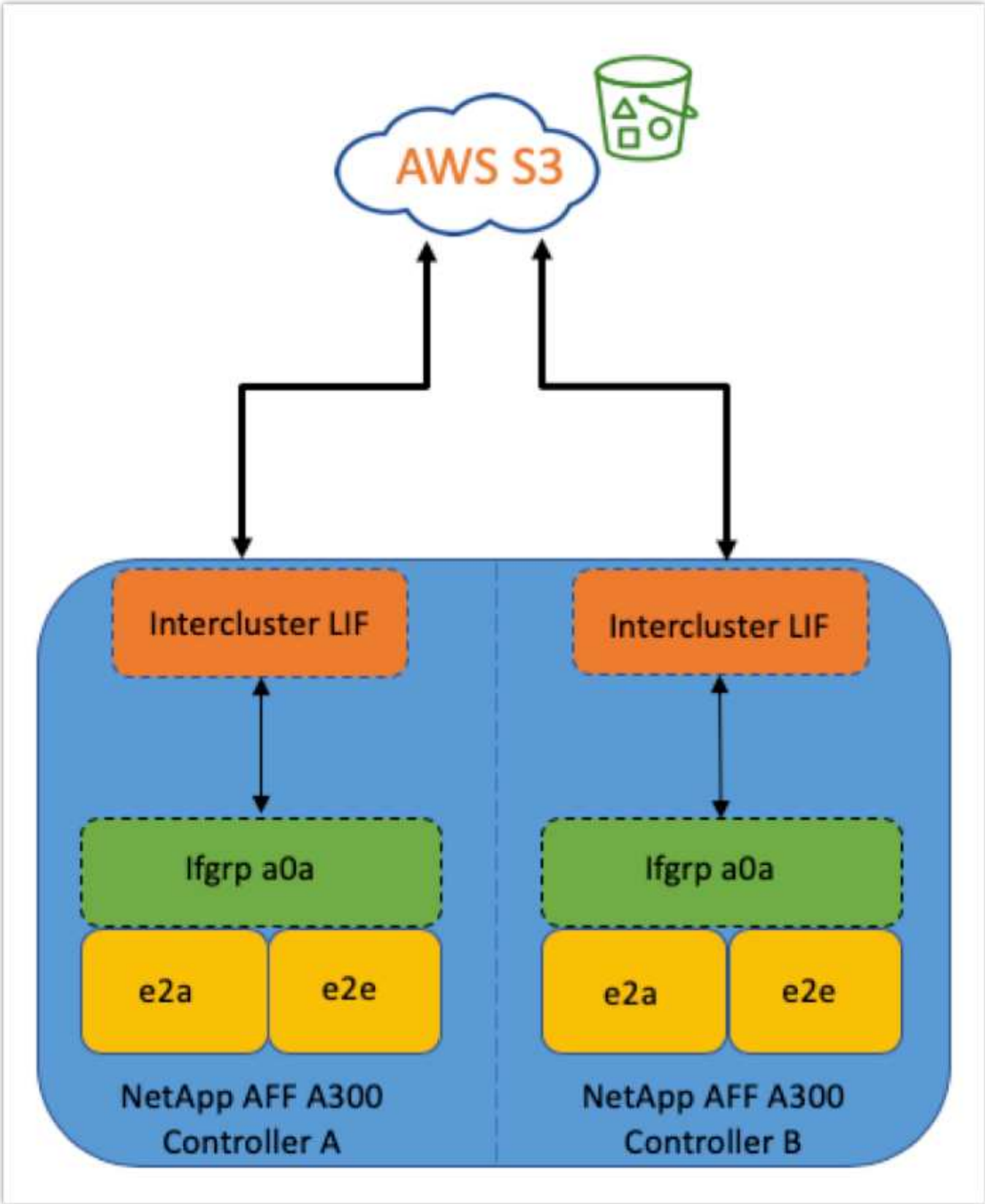
如果在具有不同路由的节点上使用多个克隆用户 LIF ， NetApp 建议将其放置在不同的 IP 空间中。在配置期间， FabricPool 可以从多个 IP 空间中进行选择，但无法选择 IP 空间中的特定集群间 LIF 。

> 禁用或删除集群间 LIF 会中断与云层的通信。

连接

FabricPool 读取延迟是与云层连接的函数。使用 10 Gbps 端口的集群间 LIF （如下图所示）可提供充足的性能。NetApp 建议验证特定网络环境的延迟和吞吐量，以确定其对 FabricPool 性能的影响。

> 在低性能环境中使用 FabricPool 时，必须继续满足客户端应用程序的最低性能要求，并相应地调整恢复时间目标。



对象存储配置程序

对象存储配置程序（如下图所示）可通过 ONTAP 命令行界面访问，它可在将对象存储连接到 FabricPool 聚合之前测试这些对象存储的延迟和吞吐量性能。

必须先将云层添加到 ONTAP 中，然后才能将其与对象存储配置程序结合使用。

使用以下命令从 ONTAP 中的高级权限模式启动对象存储配置程序：

```
storage aggregate object-store profiler start -object-store-name <name>
-node <name>
```

要查看结果，请运行以下命令：

```
storage aggregate object-store profiler show
```

云层提供的性能与性能层上的性能不同（通常为 GB/ 秒）。虽然 FabricPool 聚合可以轻松提供类似于 SATA 的性能，但对于不需要类似 SATA 的性能的分层解决方案，它们还可以承受高达 10 秒的延迟和低吞吐量。

```
bb09-a300-2::*> storage aggregate object-store profiler show
Object store config name: aws_infra_fp_bk_1
Node name: bb09-a300-2-1
Status: Active. Issuing GETs
Start time: 10/3/2019 12:37:24

Op      Size       Total     Failed            Latency(ms)          Throughput
                                        min       max       avg
-------------------------------------------------------------------------------
PUT     4MB        1084      0         336       5951      2817      69.55MB
GET     4KB        158636    0         27        1132      41        32.22MB
GET     8KB        0         0         0         0         0         0B
GET     32KB       0         0         0         0         0         0B
GET     256KB      0         0         0         0         0         0B
5 entries were displayed.
```

Volumes

存储精简配置是 FlexPod 虚拟基础架构管理员的标准做法。NetApp Virtual Storage Console （ VSC ）无需任何空间保证（精简配置）即可为 VMware 数据存储库配置存储卷，并根据 NetApp 最佳实践使用优化的存储效率设置。如果使用 VSC 创建 VMware 数据存储库，则无需执行其他操作，因为不应为该数据存储库卷分配空间保证。

FabricPool 无法将云层附加到包含使用 " 无 " 以外的空间保证的卷的聚合（例如 " 卷 " ）。

```
volume modify -space-guarantee none
```

设置 `spage-guarantee none` 参数可为卷提供精简配置。此保证类型的卷所占用的空间量会随着数据的添加而增加，而不是由初始卷大小决定。这种方法对于 FabricPool 至关重要，因为卷必须支持热数据并恢复到性能层的云层数据。

许可

在为 AFF 和 FAS 混合闪存系统附加第三方对象存储提供程序（例如 Amazon S3 ）作为云层时， FabricPool 需要基于容量的许可证。

FabricPool 许可证以永久或按期限（ 1 年或 3 年）形式提供。

当存储在云层上的数据量（已用容量）达到许可容量时，分层到云层将停止。除非增加许可证容量，否则无法对其他数据进行分层，包括使用所有分层策略将 SnapMirror 副本分层到卷。虽然分层停止，但仍可从云层访问数据。在增加许可容量之前，其他冷数据仍会保留在 SSD 上。

购买任何新的 ONTAP 9.5 或更高版本的集群时都会附带一个 10 TB 容量的基于期限的免费 FabricPool 许可证，但可能会产生额外的支持成本。可以以 1 TB 为增量购买 FabricPool 许可证（包括现有许可证的额外容量）。

只能从不包含 FabricPool 聚合的集群中删除 FabricPool 许可证。

> FabricPool 许可证在集群范围内有效。购买许可证时、您应具有UUID (`cluster identify show`）。有关其他许可信息，请参见 "NetApp 知识库"。

Configuration

软件版本

下表显示了经过验证的硬件和软件版本。

层	**Device**	图像	注释
存储	NetApp AFF A300	ONTAP 9.6P2	
计算	采用 Cisco UCS VIC 1340 的 Cisco UCS B200 M5 刀片式服务器	4.0 版（ 4b ）	
网络	Cisco Nexus 6332-16UP 互联阵列	4.0 版（ 4b ）	
	NX-OS 独立模式下的 Cisco Nexus 93180YC-EX 交换机	版本 7.0 （ 3 ） i7 （ 6 ）	
存储网络	Cisco MDS 9148S	8.3 （ 2 ）版	
虚拟机管理程序		VMware vSphere ESXi 6.7U2	ESXi 6.7.013006603
		VMware vCenter Server	vCenter Server 6.7.0.30000 内部版本 13639309
云提供商		Amazon AWS S3	具有默认选项的标准 S3 存储分段

中概述了 FabricPool 的基本要求 "FabricPool 要求"。满足所有基本要求后，完成以下步骤以配置 FabricPool：

1. 安装 FabricPool 许可证。

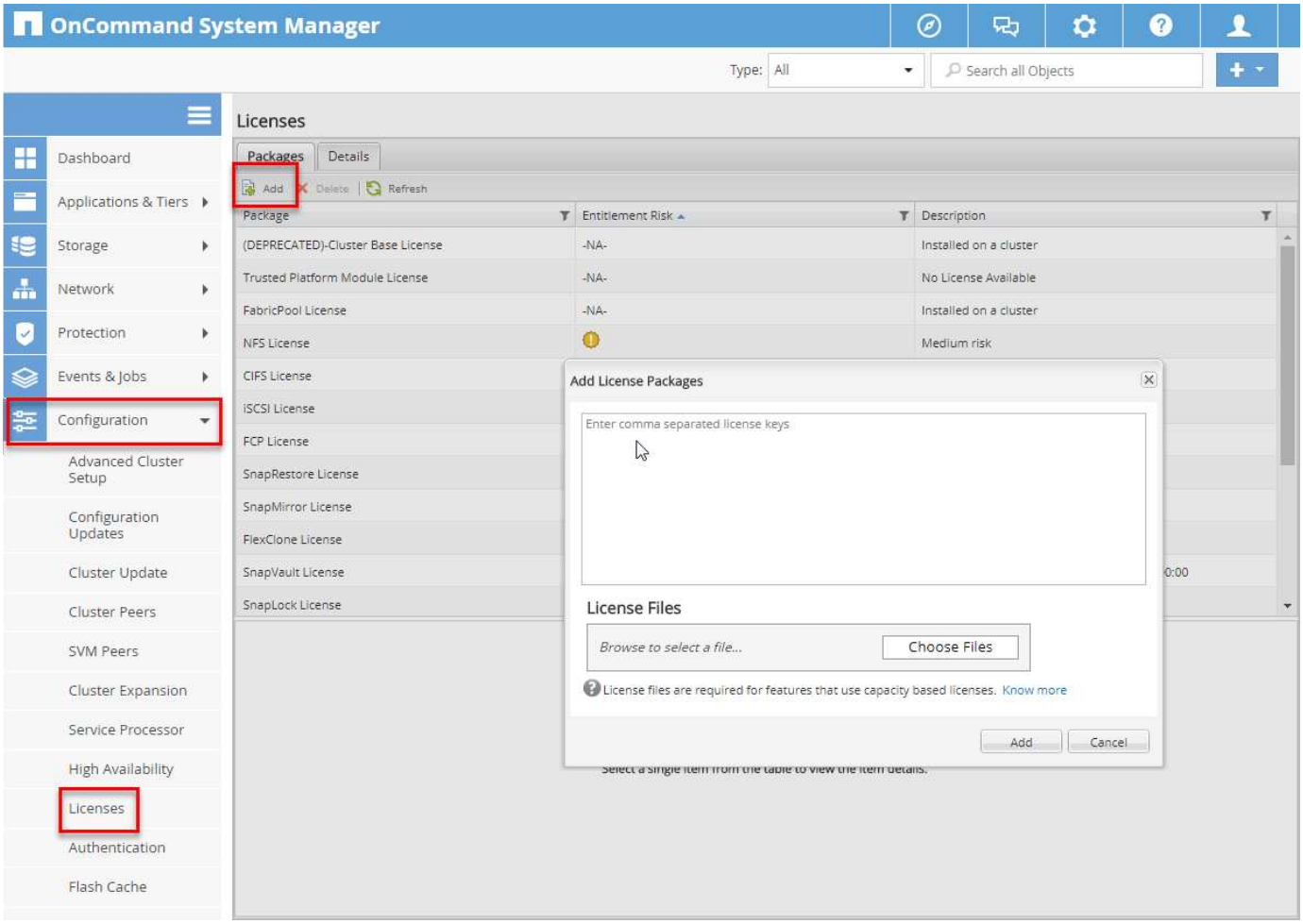
2. 创建 AWS S3 对象存储分段。
3. 将云层添加到 ONTAP 。
4. 将云层附加到聚合。
5. 设置卷分层策略。

"下一步：安装 FabricPool 许可证。"

安装 **FabricPool** 许可证

获取 NetApp 许可证文件后，您可以使用 OnCommand System Manager 进行安装。要安装许可证文件，请完成以下步骤：

1. 单击配置。
2. 单击集群。
3. 单击许可证。
4. 单击添加。
5. 单击选择文件以浏览并选择文件。
6. 单击添加。



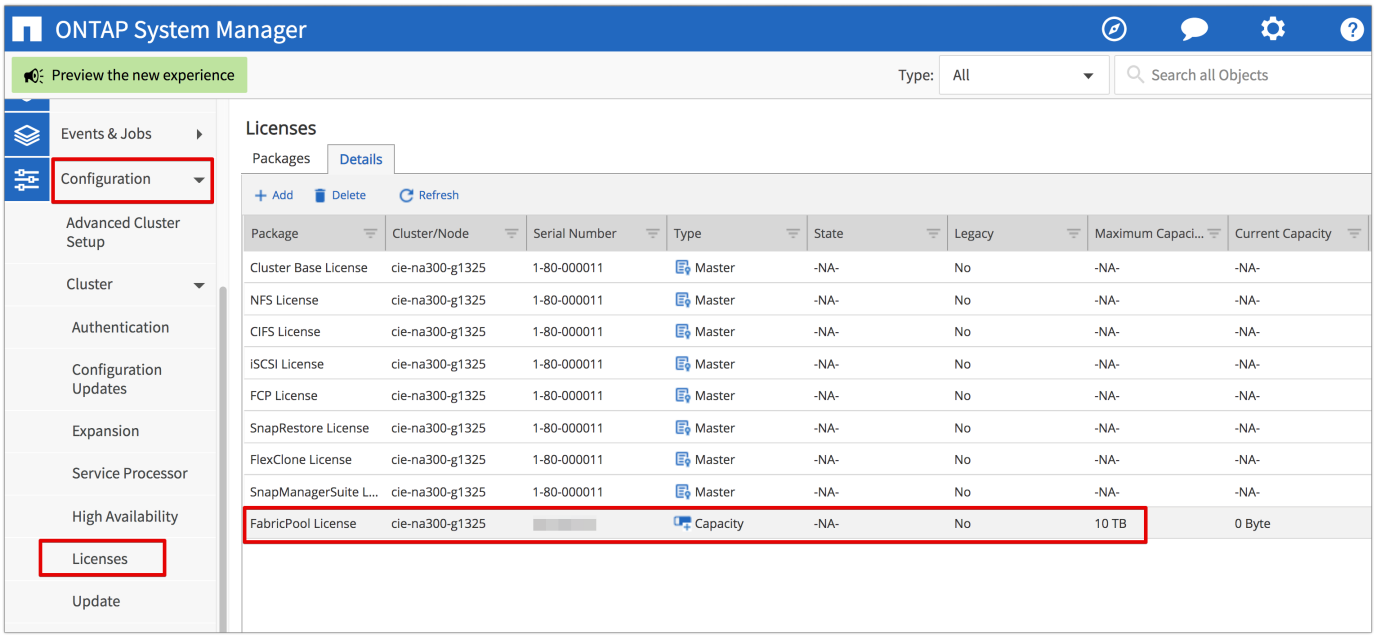
许可证容量

您可以使用 ONTAP 命令行界面或 OnCommand 系统管理器查看许可证容量。要查看许可的容量，请在 ONTAP 命令行界面中运行以下命令：

```
system license show-status
```

在 OnCommand 系统管理器中，完成以下步骤：

1. 单击配置。
2. 单击许可证。
3. 单击详细信息选项卡。



最大容量和当前容量列在 FabricPool 许可证行中。

"接下来：创建 AWS S3 存储分段。"

创建 **AWS S3** 存储分段

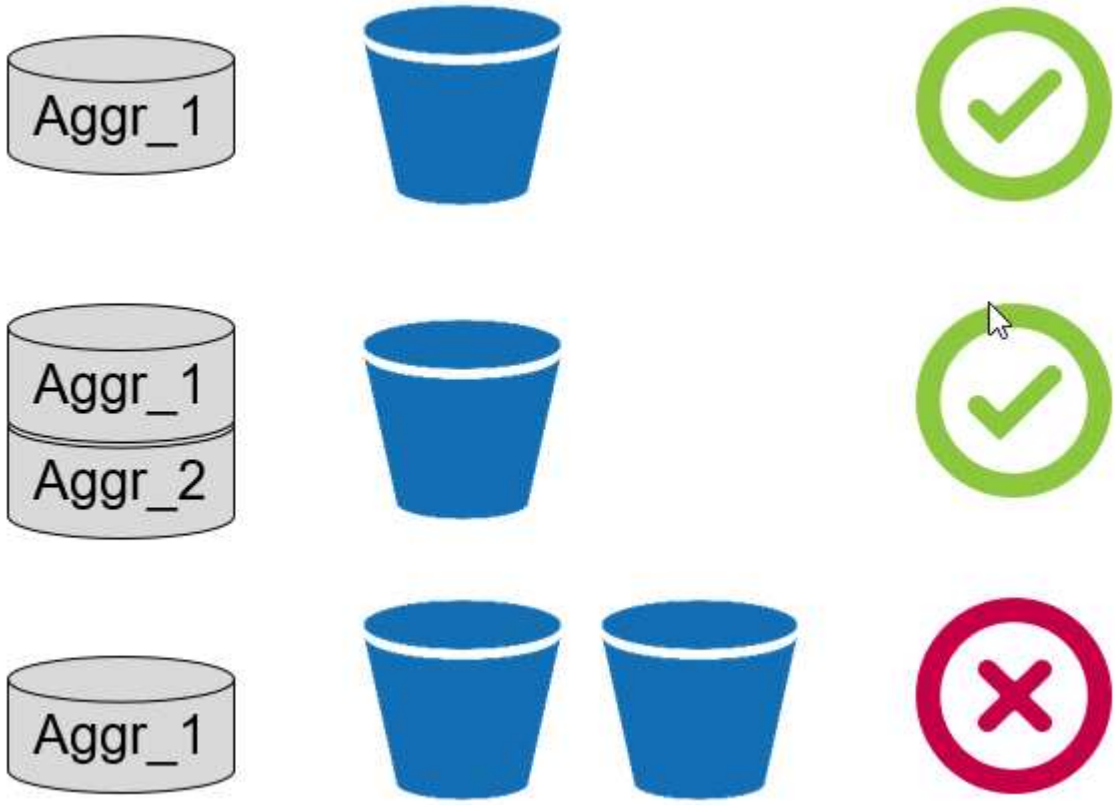
存储分段是用于保存数据的对象存储容器。您必须先提供存储数据的存储分段的名称和位置，然后才能将其作为云层添加到聚合中。

> 无法使用 OnCommand System Manager， OnCommand Unified Manager 或 ONTAP 创建存储分段。

FabricPool 支持为每个聚合连接一个存储分段，如下图所示。一个存储分段可以附加到一个聚合，一个存储分段可以附加到多个聚合。但是，不能将单个聚合附加到多个分段。虽然一个存储分段可以附加到一个集群中的多个聚合，但 NetApp 不建议将一个存储分段附加到多个集群中的聚合。

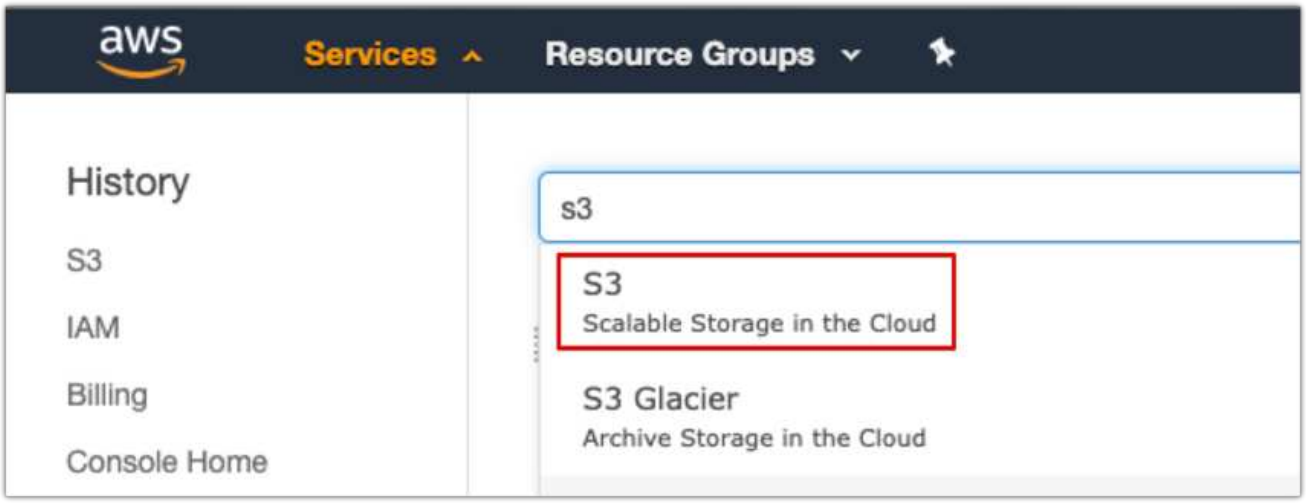
在规划存储架构时，请考虑分段到聚合关系可能会对性能产生何种影响。许多对象存储提供程序都会在存储分段

或容器级别设置支持的最大 IOPS 数。需要最高性能的环境应使用多个分段，以减少对象存储 IOPS 限制可能影响多个 FabricPool 聚合的性能的可能性。将单个存储分段或容器附加到集群中的所有 FabricPool 聚合对于重视易管理性而不是云层性能的环境来说，可能会更加有利。



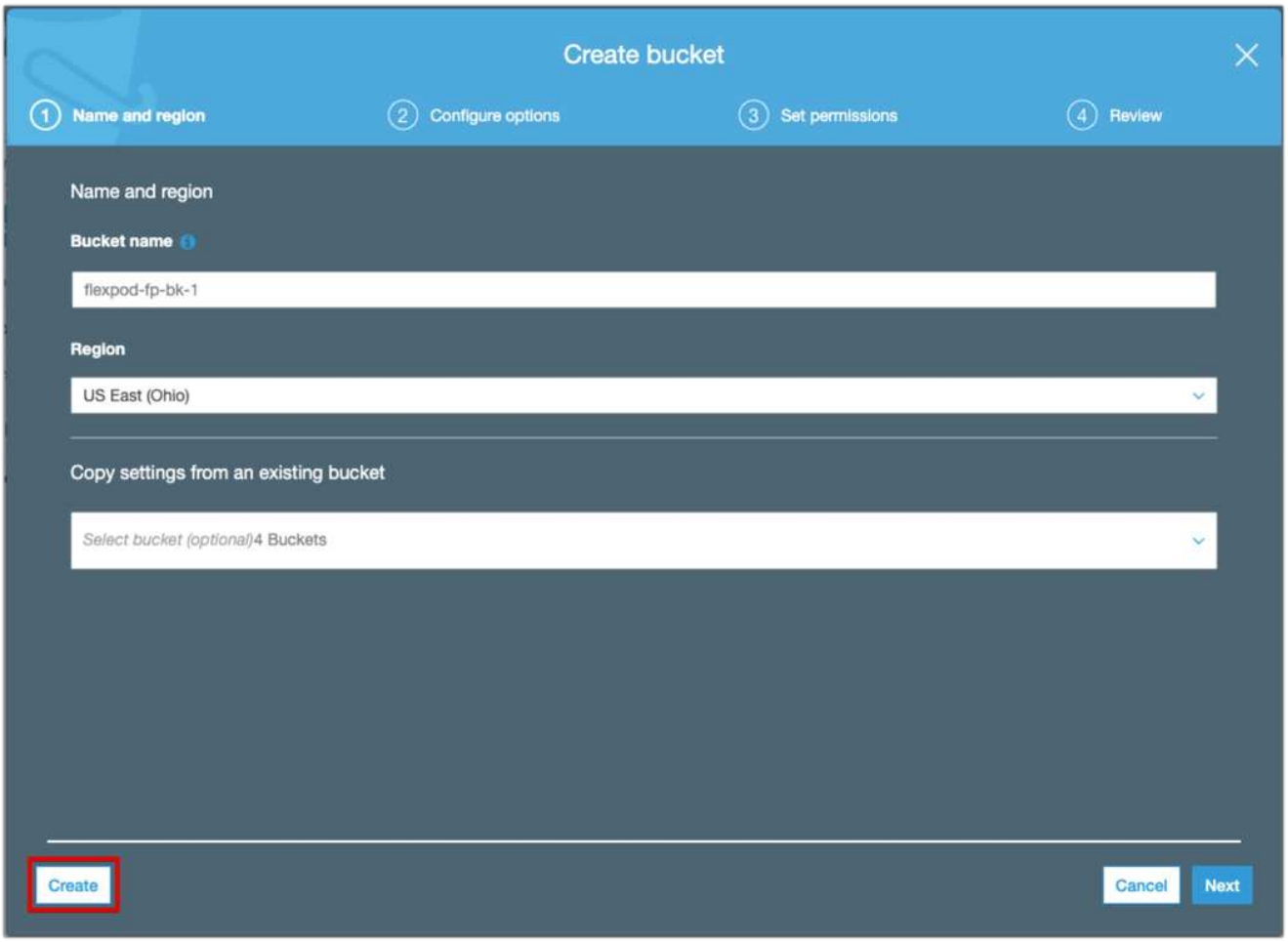
创建 **S3** 存储区。

1. 在 AWS 管理控制台中的主页页面中，在搜索栏中输入 s3 。
2. 在云中选择 S3 可扩展存储。



3. 在 S3 主页上，选择创建存储分段。

4. 输入符合 DNS 要求的名称，然后选择要创建存储分段的区域。



5. 单击创建以创建对象存储分段。

"接下来：将云层添加到 ONTAP"

将云层添加到 **ONTAP**

在将对象存储附加到聚合之前，必须将其添加到 ONTAP 并由其标识。可以使用 OnCommand 系统管理器或 ONTAP 命令行界面完成此任务。

FabricPool 支持将 Amazon S3 ， IBM 对象云存储和 Microsoft Azure Blob 存储对象存储作为云层。

您需要以下信息：

- 服务器名称（ FQDN ）；例如， `s3.amazonaws.com`
- 访问密钥 ID
- 机密密钥
- 容器名称（存储分段名称）

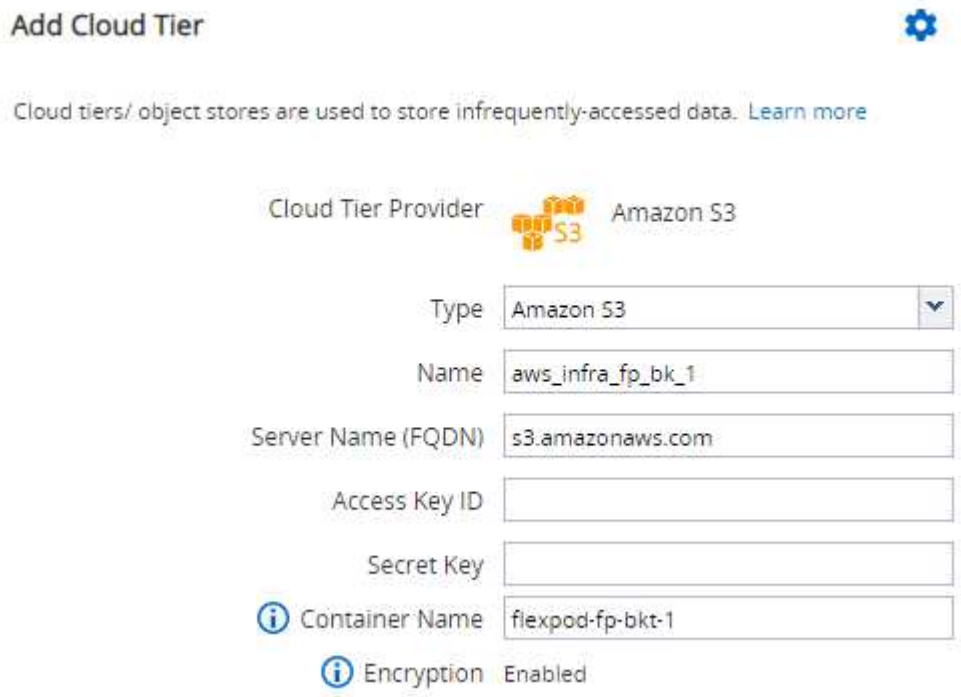
OnCommand 系统管理器

要使用 OnCommand System Manager 添加云层，请完成以下步骤：

1. 启动 OnCommand 系统管理器。
2. 单击存储。
3. 单击聚合和磁盘。
4. 单击 Cloud Tiers 。
5. 选择对象存储提供程序。
6. 根据需要填写对象存储提供程序的文本字段。

   在容器名称字段中，输入对象存储的分段或容器名称。

7. 单击保存并附加聚合。



ONTAP 命令行界面

要使用 ONTAP 命令行界面添加云层，请输入以下命令：

```
object-store config create
-object-store-name <name>
-provider-type <AWS>
-port <443/8082> (AWS)
-server <name>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ssl-enabled true
-ipspace default
```

"下一步：将云层附加到 ONTAP 聚合。"

将云层附加到 **ONTAP** 聚合

在将对象存储添加到 ONTAP 并由其标识后，必须将其附加到聚合才能创建 FabricPool 。可以使用 OnCommand 系统管理器或 ONTAP 命令行界面完成此任务。

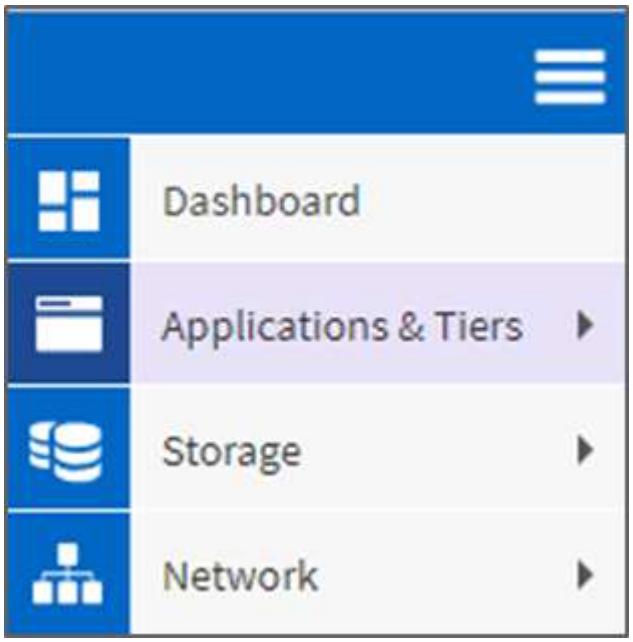
可以将多种类型的对象存储连接到一个集群，但每个聚合只能附加一种类型的对象存储。例如，一个聚合可以使用 Google Cloud ，另一个聚合可以使用 Amazon S3 ，但一个聚合无法同时附加到这两个聚合。

将云层附加到聚合是一项永久性操作。无法从已附加到的聚合中取消附加云层。

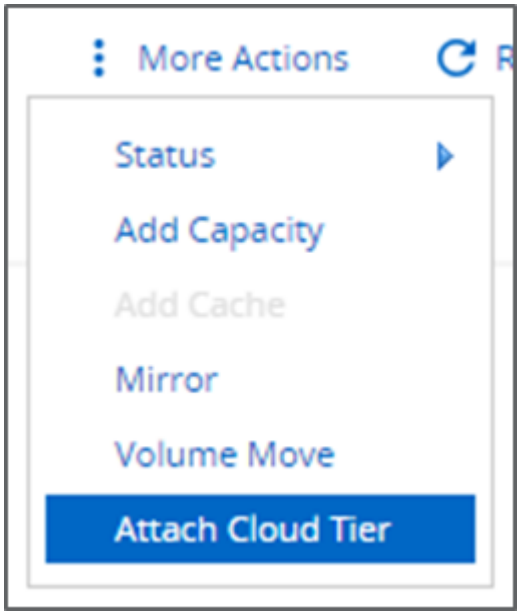
OnCommand 系统管理器

要使用 OnCommand System Manager 将云层附加到聚合，请完成以下步骤：

1. 启动 OnCommand 系统管理器。
2. 单击应用程序和层。



3. 单击存储层。
4. 单击某个聚合。
5. 单击操作并选择附加云层。



6. 选择云层。
7. 查看并更新聚合上卷的分层策略（可选）。默认情况下，卷分层策略设置为仅 Snapshot 。
8. 单击保存。

ONTAP 命令行界面

要使用 ONTAP 命令行界面将云层附加到聚合，请运行以下命令：

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <name>
```

示例

```
storage aggregate object-store attach -aggregate aggr1 -object-store-name
- aws_infra_fp_bk_1
```

"下一步：设置卷分层策略。"

设置卷分层策略

默认情况下，卷使用无卷分层策略。创建卷后，可以使用 OnCommand 系统管理器或 ONTAP 命令行界面更改卷分层策略。

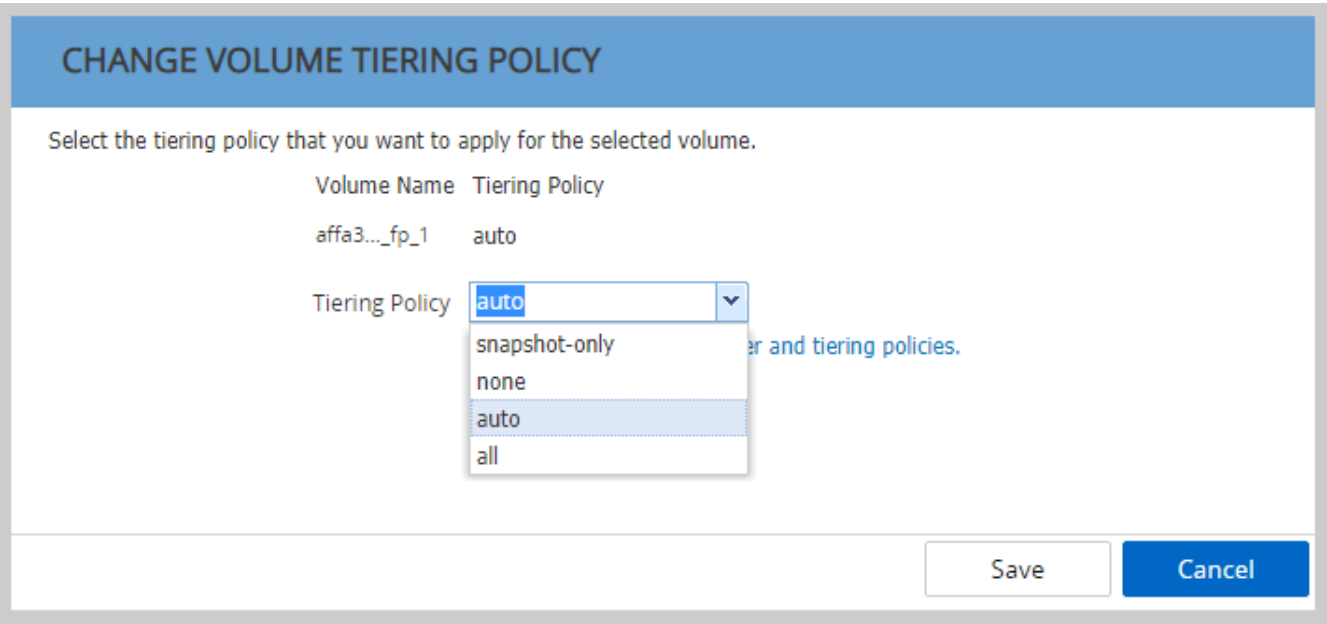
在与 FlexPod 结合使用时， FabricPool 提供了三种卷分层策略：自动，仅 Snapshot 和无。

- * 自动 *
  - 卷中的所有冷块都会移至云层。假设聚合的利用率超过 50% ，则非活动块大约需要 31 天才能变冷。使用 `tiering-minimum-cooling-days` 设置，自动冷却期可在 2 天到 63 天之间进行调整。
  - 如果随机读取卷中分层策略设置为 " 自动 " 的冷块，则这些冷块会变热并写入性能层。
  - 如果卷中分层策略设置为自动的冷块按顺序读取，则这些冷块将保持冷状态并保留在云层上。它们不会写入性能层。
- * 仅 Snapshot *
  - 卷中未与活动文件系统共享的冷 Snapshot 块将移至云层。假设聚合的利用率超过 50% ，则非活动快照块变冷大约需要 2 天时间。使用 `tiering-minimum-cooling-days` 设置，仅 Snapshot 散热期可从 2 天调整为 63 天。
  - 读取卷中分层策略设置为仅 Snapshot 的冷块时，这些冷块会变热并写入性能层。
- * 无（默认） *
  - 设置为使用无作为分层策略的卷不会将冷数据分层到云层。
  - 将分层策略设置为无会阻止新的分层。
  - 先前已移至云层的卷数据将保留在云层中，直到变热为止，并会自动移回性能层。

OnCommand 系统管理器

要使用 OnCommand 系统管理器更改卷的分层策略，请完成以下步骤：

1. 启动 OnCommand 系统管理器。
2. 选择一个卷。
3. 单击更多操作并选择更改分层策略。
4. 选择要应用于卷的分层策略。
5. 单击保存。



ONTAP 命令行界面

要使用 ONTAP 命令行界面更改卷的分层策略，请运行以下命令：

```
volume modify -vserver <svm_name> -volume <volume_name>
-tiering-policy <auto|snapshot-only|all|none>
```

"下一步：设置卷分层最小冷却天数。"

设置卷分层最小冷却天数

`tiering-minimum-cooling-days` 设置可确定在使用自动或仅 Snapshot 策略的卷中的非活动数据被视为冷数据并符合分层条件之前必须经过多少天。

自动

自动分层策略的默认 **分层最小冷却天数** 设置为 31 天。

由于读取会使块温度保持较高，因此增加此值可能会减少符合分层条件的数据量，并增加性能层上保留的数据量。

如果要将此值从默认 31 天减少，请注意，数据在标记为冷之前不应再处于活动状态。例如，如果多天工作负载要在第 7 天执行大量写入，则应将卷的 `tiering-minimum-cooling-days` 设置设置为不低于 8 天。

> 对象存储与文件或块存储不是事务存储。如果对卷中作为对象存储的文件进行更改，而这些文件的最小散热天数过长，则可能会创建新对象，碎片化现有对象，并增加存储效率低下的问题。

仅 Snapshot

仅 Snapshot 分层策略的默认 `tiering-minimum-cooling-days` 设置为 2 天。至少 2 天可以为后台进程提供更多时间，以实现最高的存储效率，并防止日常数据保护进程不得不从云层读取数据。

ONTAP 命令行界面

要使用 ONTAP 命令行界面更改卷的 `tiering-minimum-cooling-days` 设置，请运行以下命令：

```
volume modify -vserver <svm_name> -volume <volume_name> -tiering-minimum
-cooling-days <2-63>
```

需要高级权限级别。

> 在自动和仅 Snapshot 之间更改分层策略（反之亦然）会重置性能层上块的非活动时间。例如，如果将分层策略设置为仅 Snapshot ，则使用自动卷分层策略且性能层上的数据处于非活动状态 20 天的卷将将性能层数据非活动重置为 0 天。

性能注意事项

调整性能层的大小

在考虑规模估算时，请记住，性能层应能够执行以下任务：

- 支持热数据
- 支持冷数据，直到分层扫描将数据移至云层
- 支持热数据并写入到性能层的云层数据
- 支持与附加云层关联的 WAFL 元数据

对于大多数环境， FabricPool 聚合上的性能容量比为 1： 10 非常保守，同时可显著节省存储空间。例如，如果要将 200 TB 分层到云层，则性能层聚合至少应为 20 TB 。

> 如果性能层容量大于 70% ，则从云层写入到性能层将被禁用。如果发生这种情况，则直接从云层读取块。

调整云层大小

在考虑规模估算时，充当云层的对象存储应能够执行以下任务：

- 支持读取现有冷数据
- 支持写入新冷数据
- 支持对象删除和碎片整理

拥有成本

。 "FabricPool 经济计算器" 可通过独立 IT 分析机构 Evaluator Group 获得，帮助预测内部和云之间在冷数据存储方面的成本节省。该计算器提供了一个简单的界面，用于确定在性能层上存储不常访问的数据的成本，而不是在数据生命周期的剩余时间将其发送到云层。根据 5 年的计算结果，我们会利用源容量，数据增长，快照容量和冷数据百分比这四个关键因素来确定该时间段内的存储成本。

结论

云之旅因组织，业务单位甚至组织内的业务单位而异。有些选择采用速度较快，而另一些则采用较为保守的方法。无论企业规模大小如何，采用云的速度如何， FabricPool 都能融入云战略，进一步展示了 FlexPod 基础架构的效率和可扩展性优势。

从何处查找追加信息

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：

- FabricPool 最佳实践

  "www.netapp.com/us/media/tr-4598.pdf"

- NetApp 产品文档

  "https://docs.netapp.com"

- TR-4036：《 FlexPod 数据中心技术规格》

  "https://www.netapp.com/us/media/tr-4036.pdf"

采用IBM Cloud Private的FlexPod 数据中心

Sreenivasa Edula、Cisco Thanachit Wichianchai、IBM Jacky Ben-Bassat、IBM全球联盟、NetApp

IBM Cloud Private (ICP)是一个内部平台、用于开发和管理适用于云原生和应用程序现代化用例的容器化应用程序。它是一个基于Kubernetes作为容器编排构建的集成环境、包括一个适用于Docker容器的私有映像存储库、一个管理控制台、一个监控框架、许多基于开源和IBM容器化的应用程序等。将ICP与Cisco和NetApp的融合基础架构FlexPod 相结合、可以简化基础架构的部署和管理。您还可以从提高存储效率、改善数据保护、降低风险以及灵活扩展这种高度可用的企业级基础架构堆栈中受益、以适应新的业务需求以及随时间推移发生的其他变化。

"采用IBM Cloud Private的FlexPod 数据中心"

适用于混合云的FlexPod 数据中心与Cisco CloudCenter和NetApp私有存储—设计

NetApp公司Cisco David Arnette Haseeb Niazi

Cisco Validated Design (CVD)提供经过设计、测试和记录的系统和解决方案、以促进和改进客户部署。这些设计将广泛的技术和产品融入到了一系列解决方案中、这些解决方案是为满足客户的业务需求而开发的、并为客户从设计到部署提供指导。

"适用于混合云的FlexPod 数据中心与Cisco CloudCenter和NetApp私有存储—设计"

适用于多云的FlexPod 数据中心与Cisco CloudCenter和NetApp Data Fabric

NetApp公司Cisco David Arnette Haseeb Niazi

本文档提供了有关为混合云设置FlexPod 数据中心的深入配置和实施准则。以下设计要素将此版本的FlexPod 与先前的型号区分开来：

- 将Cisco CloudCenter与FlexPod Datacenter集成、并将ACI作为私有云
- 将Cisco CloudCenter与Amazon Web Services (AWS)和Microsoft Azure Resource Manager (MS Azure RM)公共云集成
- 在FlexPod 数据中心和公共云之间提供安全连接、以确保虚拟机(VM)之间的流量安全

- 在FlexPod 数据中心和NetApp私有存储(NPS)之间提供安全连接、以传输数据复制流量
- 能够在公共云或私有云中部署应用程序实例、并通过Cisco CloudCenter驱动的流程编排为这些实例提供最新的应用程序数据
- 在此新的混合云模式下设置、验证和突出显示开发和测试环境的操作方面。

"适用于多云的FlexPod 数据中心与Cisco CloudCenter和NetApp Data Fabric"

企业数据库

SAP

基于 FlexPod 的 SAP 简介

FlexPod 平台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（ Cisco UCS ）， Cisco Nexus 系列交换机和 NetApp 存储控制器构建。

FlexPod 是运行 SAP 应用程序的合适平台，此处提供的解决方案可帮助您快速，可靠地部署 SAP HANA ，并采用量身定制的数据中心集成模式。FlexPod 不仅提供了基线配置，而且还可以灵活地调整规模并进行优化，以满足多种不同的使用情形和要求。

适用于SAP解决方案 的FlexPod 数据中心使用光纤通道SAN与Cisco UCS Manager 4.0和NetApp ONTAP 9.7

NetApp公司Cisco Marco Schoen的Pramod Ramamurthy

本文档介绍了在NetApp AFF A400存储上使用NetApp ONTAP 9.7的Cisco和NetApp FlexPod Datacenter、以及采用适用于SAP HANA的第二代Intel Xeon可扩展处理器的Cisco UCS Manager统一软件版本4.1 (1)。

采用NetApp ONTAP 9.7和Cisco UCS统一软件版本4.1 (1)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(Cisco UCS)、Cisco Nexus 9000系列交换机、MDS 9000多层光纤交换机、 以及运行ONTAP 9.7存储操作系统的NetApp AFF A系列存储阵列。

"适用于SAP解决方案 的FlexPod 数据中心使用光纤通道SAN与Cisco UCS Manager 4.0和NetApp ONTAP 9.7"

采用SQL的SAP非HANA白皮书—设计

当前的IT行业正在见证数据中心解决方案的重大转型。近年来、人们对经过预先验证和设计的数据中心解决方案非常感兴趣。在关键领域引入虚拟化技术对这些解决方案的设计原则和架构产生了重大影响。它允许在裸机系统上运行的许多应用程序迁移到新的虚拟化集成解决方案。FlexPod 是一个经过预先验证和精心设计的数据中心解决方案 、旨在满足IT部门快速变化的需求。Cisco和NetApp合作推出了FlexPod 、它使用一流的计算、网络和存储组件作为各种企业工作负载的基础、包括数据库、企业资源规划(ERP)、客户关系管理(CRM)和Web应用程序。

近年来、IT应用程序、尤其是数据库的整合引起了人们的极大关注。过去几年来、Microsoft SQL Server是最广泛采用和部署的数据库平台。SQL Server数据库经常会出现数据库无序增长的情况、从而导致IT面临诸多挑战、例如服务器利用率低下、许可不正确、安全问题、管理问题以及巨大的运营成本。因此、SQL Server数据库很适合整合到一个更强大、更灵活且更具弹性的平台上。本文档讨论了用于部署和整合SQL Server数据库的FlexPod 参考架构。

"采用SQL的SAP非HANA白皮书—设计"

适用于SAP解决方案 的FlexPod 数据中心、采用Cisco UCS第三代网络结构和NetApp AFF A系列

NetApp公司Cisco Marco Schoen的Pramod Ramamurthy

本文档介绍了基于第二代Intel Xeon可扩展处理器支持的Cisco UCS计算系统(Cisco UCS)的Cisco和NetApp FlexPod Datacenter for SAP HANA的部署方法。

Cisco UCS Manager (UCSM) 4.0 (4)可为所有当前的Cisco UCS互联阵列型号(6200、6300、6324和6454)、2200/2300系列IOM、Cisco UCS B系列刀片式服务器和Cisco UCS C系列机架式服务器提供整合支持。采用Cisco UCS统一软件版本4.0 (4D)和NetApp ONTAP 9.6的FlexPod 数据中心是一种基于Cisco UCS、Cisco Nexus 9000系列交换机和NetApp AFF A系列存储阵列构建的预先设计的最佳实践数据中心架构。

"适用于SAP解决方案 的FlexPod 数据中心、采用Cisco UCS第三代网络结构和NetApp AFF A系列"

适用于SAP解决方案 的FlexPod 数据中心使用光纤通道SAN与Cisco UCS Manager 4.0和NetApp ONTAP 9.7—设计

NetApp公司Cisco Marco Schoen的Pramod Ramamurthy

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 提供了一个集成架构、该架构整合了计算、存储和网络设计最佳实践、通过验证集成架构来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。

"适用于SAP解决方案 的FlexPod 数据中心使用光纤通道SAN与Cisco UCS Manager 4.0和NetApp ONTAP 9.7—设计"

采用Cisco ACI、Cisco UCS Manager 4.0和NetApp AFF A系列的适用于SAP解决方案的FlexPod Datacenter—设计

NetApp公司Cisco Marco Schoen的Pramod Ramamurthy

本文档介绍了Cisco ACI集成的FlexPod 解决方案 、它是一种经过验证的方法、用于部署SAP HANA定制的数据中心集成(Data Center Integration、TDI)环境。此经过验证的设计为实施采用Cisco和NetApp最佳实践的SAP HANA提供了准则和框架。

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、以支持包含以下组件的Cisco UCS硬件平台：

- Cisco UCS B系列刀片式服务器和Cisco UCS C系列机架式服务器、可使用Intel Optane Data Center Persistent Memory Module (DCPMM)选项进行配置
- Cisco UCS 6400系列互联阵列
- Cisco Nexus 9000系列叶式和Spine交换机
- NetApp全闪存系列存储阵列

此外、本文档还对Red Hat Enterprise Linux和适用于SAP HANA的SUSE Linux Enterprise Server进行了验证。

"采用Cisco ACI、Cisco UCS Manager 4.0和NetApp AFF A系列的适用于SAP解决方案 的FlexPod Datacenter—设计"

采用Cisco ACI、Cisco UCS Manager 4.0和NetApp AFF A系列的FlexPod Datacenter for SAP—部署

NetApp公司Cisco Marco Schoen的Pramod Ramamurthy

本文档介绍了FlexPod 基础架构上SAP HANA定制的数据中心集成选项的架构和部署过程、该选项包括：

- 由第二代Intel Xeon可扩展处理器支持的Cisco UCS计算系统(Cisco UCS)。
- 利用Cisco Application Centric Infrastructure (ACI)的交换产品。
- NetApp A系列AFF 阵列。

本文档旨在介绍SAP HANA部署的详细配置步骤

"采用Cisco ACI、Cisco UCS Manager 4.0和NetApp AFF A系列的FlexPod Datacenter for SAP—部署"

采用Cisco UCS Manager 4.0和NetApp AFF A系列的适用于SAP解决方案 的FlexPod Datacenter—设计

NetApp公司Cisco Marco Schoen的Pramod Ramamurthy

本文档介绍了Cisco和NetApp FlexPod 解决方案 、这是一种经过验证的部署SAP HANA定制数据中心集成(Data Center Integration、TDI)环境的方法。此经过验证的设计为实施采用Cisco和NetApp最佳实践的SAP HANA提供了准则和框架。

FlexPod 是一款领先的集成基础架构、可支持广泛的企业工作负载和用例。借助此解决方案 、您可以使用量身定制的数据中心集成模式快速、可靠地部署SAP HANA。

"采用Cisco UCS Manager 4.0和NetApp AFF A系列的适用于SAP解决方案 的FlexPod Datacenter—设计"

在采用SLES 12 SP3和RHEL 7.4的Cisco UCS M5服务器上、采用Cisco ACI的FlexPod Datacenter for SAP解决方案

NetApp公司Cisco Marco Schoen的Pramod Ramamurthy

本文档介绍了FlexPod 基础架构上的SAP HANA定制数据中心集成选项的架构和部署流程、该选项由Cisco计算和交换产品组成、这些产品利用了行业领先的软件定义网络解决方案 (SDN) Cisco Application Centric Infrastructure (ACI)以及NetApp A系列AFF 阵列。本文档旨在展示设计原则以及SAP HANA部署的详细配置步骤。

"在采用SLES 12 SP3和RHEL 7.4的Cisco UCS M5服务器上、采用Cisco ACI的FlexPod Datacenter for SAP解决方案"

适用于SAP解决方案 的FlexPod 数据中心、采用基于IP的存储、并使用NetApp AFF A系列和Cisco UCS Manager 3.2

NetApp公司Cisco Ralf Klahr Cisco Marco Schoen的Shailendra Mruthunjaya

本文档中详细介绍的参考架构重点介绍了基于IP的存储解决方案 的故障恢复能力、成本效益和部署简便性。一个能够通过一个接口提供多个协议的存储系统可以为客户提供选择和投资保护、因为它确实是一种一次线架构。解决方案 专为托管可扩展的SAP HANA工作负载而设计。

"适用于SAP解决方案 的FlexPod 数据中心、采用基于IP的存储、并使用NetApp AFF A系列和Cisco UCS Manager 3.2"

适用于SAP解决方案 的FlexPod 数据中心使用光纤通道SAN与Cisco UCS Manager 4.0和NetApp ONTAP 9.7

NetApp公司Cisco Marco Schoen的Pramod Ramamurthy

本文档介绍了在NetApp AFF A400存储上使用NetApp ONTAP 9.7的Cisco和NetApp FlexPod Datacenter、以及采用适用于SAP HANA的第二代Intel Xeon可扩展处理器的Cisco UCS Manager统一软件版本4.1 (1)。

采用NetApp ONTAP 9.7和Cisco UCS统一软件版本4.1 (1)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(Cisco UCS)、Cisco Nexus 9000系列交换机、MDS 9000多层光纤交换机、 以及运行ONTAP 9.7存储操作系统的NetApp AFF A系列存储阵列。

"适用于SAP解决方案 的FlexPod 数据中心使用光纤通道SAN与Cisco UCS Manager 4.0和NetApp ONTAP 9.7"

使用SQL在FlexPod 上部署SAP应用程序服务器

FlexPod 是一款经过预先验证和设计的数据中心解决方案 、专为满足IT部门快速变化的需求而设计。Cisco和NetApp合作推出了FlexPod 、它使用同类最佳的计算、网络和存储组件作为各种企业工作负载的基础、包括数据库、企业资源规划(ERP)、客户关系管理(CRM)和Web应用程序。近年来、IT应用程序、尤其是数据库的整合引起了人们的极大关注。过去几年来、Microsoft SQL Server是最广泛采用和部署的数据库平台。SQL Server数据库经常会出现数据库无序增长的情况、从而导致IT面临诸多挑战、例如服务器利用率低下、许可不正确、安全问题、管理问题以及巨大的运营成本。因此、SQL Server数据库很适合整合到一个更强大、更灵活且更具弹性的平台上。本文档讨论了用于部署和整合SQL Server数据库的FlexPod 参考架构。

"使用SQL在FlexPod 上部署SAP应用程序服务器"

采用Cisco ACI、Cisco UCS Manager 4.0和NetApp AFF A系列的适用于SAP的FlexPod 数据中心

NetApp公司Cisco Marco Schoen的Pramod Ramamurthy

本文档介绍了FlexPod 基础架构上SAP HANA定制的数据中心集成选项的架构和部署过

程、该选项包括：

- 由第二代Intel Xeon可扩展处理器支持的Cisco UCS计算系统(Cisco UCS)。
- 利用Cisco Application Centric Infrastructure (ACI)的交换产品。
- NetApp A系列AFF 阵列。

"采用Cisco ACI、Cisco UCS Manager 4.0和NetApp AFF A系列的适用于SAP的FlexPod 数据中心"

采用Cisco ACI、Cisco UCS Manager 4.0和NetApp AFF A系列的适用于SAP解决方案的FlexPod Datacenter—设计

NetApp公司Cisco Marco Schoen的Pramod Ramamurthy

本文档介绍了Cisco ACI集成的FlexPod 解决方案 、它是一种经过验证的方法、用于部署SAP HANA定制的数据中心集成(Data Center Integration、TDI)环境。此经过验证的设计为实施采用Cisco和NetApp最佳实践的SAP HANA提供了准则和框架。

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、以支持包含以下组件的Cisco UCS硬件平台：

- Cisco UCS B系列刀片式服务器和Cisco UCS C系列机架式服务器、可使用Intel Optane Data Center Persistent Memory Module (DCPMM)选项进行配置
- Cisco UCS 6400系列互联阵列
- Cisco Nexus 9000系列叶式和Spine交换机
- NetApp全闪存系列存储阵列

此外、本文档还对Red Hat Enterprise Linux和适用于SAP HANA的SUSE Linux Enterprise Server进行了验证。

"采用Cisco ACI、Cisco UCS Manager 4.0和NetApp AFF A系列的适用于SAP解决方案 的FlexPod Datacenter—设计"

适用于SAP解决方案 的FlexPod 数据中心、采用Cisco UCS第三代网络结构和NetApp AFF A系列

NetApp公司Cisco Ralf Klahr Cisco Marco Schoen的Shailendra Mruthunjaya

本文档介绍了基于第二代Intel Xeon可扩展处理器支持的Cisco UCS计算系统(Cisco UCS)的Cisco和NetApp FlexPod Datacenter for SAP HANA部署方法。

Cisco UCS Manager (UCSM) 4.0 (4)可为所有当前的Cisco UCS互联阵列型号(6200、6300、6324和6454)、2200/2300系列IOM、Cisco UCS B系列刀片式服务器和Cisco UCS C系列机架式服务器提供整合支持。采用Cisco UCS统一软件版本4.0 (4D)和NetApp ONTAP 9.6的FlexPod 数据中心是一种基于Cisco UCS、Cisco Nexus 9000系列交换机和NetApp AFF A系列存储阵列构建的预先设计的最佳实践数据中心架构。

"适用于SAP解决方案 的FlexPod 数据中心、采用Cisco UCS第三代网络结构和NetApp AFF A系列"

采用Cisco UCS Manager 4.0和NetApp AFF A系列的适用于SAP解决方案 的FlexPod Datacenter—设计

NetApp公司Cisco Marco Schoen的Pramod Ramamurthy

本文档介绍了Cisco和NetApp FlexPod 解决方案 、这是一种经过验证的部署SAP HANA定制数据中心集成(Data Center Integration、TDI)环境的方法。此经过验证的设计为实施采用Cisco和NetApp最佳实践的SAP HANA提供了准则和框架。

FlexPod 是一款领先的集成基础架构、可支持广泛的企业工作负载和用例。借助此解决方案 、您可以使用量身定制的数据中心集成模式快速、可靠地部署SAP HANA。

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、以支持包含以下组件的Cisco UCS硬件平台：

- Cisco UCS B系列刀片式服务器和Cisco UCS C系列机架式服务器、可使用Intel Optane Data Center Persistent Memory Module (DCPMM)选项进行配置
- Cisco UCS 6300系列互联阵列
- Cisco Nexus 9000 系列交换机
- NetApp全闪存系列存储阵列

此外、本文档还对Red Hat Enterprise Linux和适用于SAP HANA的SUSE Linux Enterprise Server进行了验证。

"采用Cisco UCS Manager 4.0和NetApp AFF A系列的适用于SAP解决方案 的FlexPod Datacenter—设计"

Oracle

FlexPod Datacenter在Cisco UCS上使用Oracle 19c RAC数据库、而NetApp AFF 在光纤通道上使用NVMe

Cisco Hardakkumar Vyas公司Tushar Patel

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。本CVD文档介绍了Cisco和NetApp FlexPod 解决方案 、这是一种经过验证的方法、用于部署高可用性Oracle RAC数据库环境。Cisco和NetApp已针对各种数据库工作负载验证了此参考架构、例如Cisco UCS Datacenter实验室中的OLTP(联机事务处理)和数据仓库。本文档显示了所涉及组件的硬件和软件配置以及各种测试的结果。此外、本文档还提供了一个框架、用于在使用Cisco UCS和NetApp存储系统的NVMe/FC上实施Oracle RAC数据库。

"FlexPod Datacenter在Cisco UCS上使用Oracle 19c RAC数据库、而NetApp AFF 在光纤通道上使用NVMe"

FlexPod 数据中心与基于 Cisco UCS 和 NetApp AFF A 系列的 Oracle RAC 数据库

Cisco Hardakkumar Vyas公司Tushar Patel

经过Cisco验证的设计包括设计、测试和记录的系统和解决方案、旨在帮助和改进客户部

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 、它为各种工作负载奠定了基础、并可根据客户需求进行高效的架构设计。FlexPod 解决方案 是一种经验证的方法、用于将Cisco和NetApp技术部署为共享云基础架构。

采用NetApp全闪存AFF 系统的FlexPod 数据中心是一个融合基础架构平台、它将Cisco和NetApp的同类最佳技术整合到一个功能强大的企业级应用程序融合平台中。Cisco和NetApp与Oracle密切合作、为当今企业所需的最苛刻的事务处理和响应时间敏感型数据库提供支持。

此Cisco验证设计(Cisco Validated Design、CVD)介绍了使用FlexPod UCS和NetApp全闪存AFF 存储部署高可用性Oracle RAC数据库环境的参考数据中心架构。本文档显示了所涉及组件的硬件和软件配置以及各种测试的结果。此外、本文档还提供了使用Cisco UCS计算服务器、Cisco互联阵列交换机、Cisco MDS交换机、Cisco Nexus交换机、NetApp AFF 存储和Oracle RAC数据库的实施和最佳实践指导。

"FlexPod 数据中心与基于 Cisco UCS 和 NetApp AFF A 系列的 Oracle RAC 数据库"

基于 **Oracle Linux** 的 **FlexPod Datacenter** 和 **Oracle RAC**

Tushar Patel、Cisco Niranjan Mohmapatra、Cisco John Elliott、NetApp

Cisco Unified Computing System (Cisco UCS)是下一代数据中心平台、可将计算、网络、存储访问和虚拟化整合到一个统一的系统中。Cisco UCS是任务关键型数据库工作负载架构的理想平台。Cisco UCS平台、NetApp存储和Oracle Real Application Cluster (RAC)架构相结合、可以加快部署速度、提高选择灵活性、提高效率并降低风险、从而加快IT转型。此Cisco验证设计(Cisco Validated Design、CVD)重点介绍了一个灵活的多租户高性能、弹性FlexPod 参考架构、该架构采用Oracle 12c RAC数据库。

FlexPod 平台由NetApp和Cisco开发、是一款灵活的集成基础架构解决方案 、可提供经过预先验证的存储、网络和服务器技术。它旨在提高IT对业务需求的响应能力、同时降低整体计算成本。考虑最长正常运行时间和最低风险。FlexPod 组件经过集成和标准化、可帮助您实现及时、可重复、一致的部署。您可以准确地规划每个FlexPod 部署的电源、占地空间、可用容量、性能和成本。

FlexPod 采用最新技术、并高效地简化了数据中心工作负载、从而重新定义了它提供价值的方式：

- 利用具有Flash Pool闪存的NetApp FAS 混合阵列的功能、可以根据您的特定应用程序或环境将精确比例的闪存部署到旋转介质。
- 利用经过预先验证的平台最大限度地减少业务中断、提高IT灵活性、并将部署时间从数月缩短到数周。
- 将管理时间和总拥有成本(TCO)削减50%。
- 满足或超出不断增长的数据中心工作负载硬件性能需求。

"基于 Oracle Linux 的 FlexPod Datacenter 和 Oracle RAC"

FlexPod 数据中心与基于 **Cisco UCS** 和 **NetApp AFF A** 系列的 **Oracle RAC** 数据库

Cisco Hardakkumar Vyas公司Tushar Patel

采用NetApp全闪存AFF 系统的FlexPod 数据中心是一个融合基础架构平台、它将Cisco和NetApp的同类最佳技术整合到一个功能强大的企业级应用程序融合平台中。Cisco

和NetApp与Oracle密切合作、为当今企业所需的最苛刻的事务处理和响应时间敏感型数据库提供支持。

此Cisco验证设计(Cisco Validated Design、CVD)介绍了使用FlexPod UCS和NetApp全闪存AFF 存储部署高可用性Oracle RAC数据库环境的参考数据中心架构。本文档显示了所涉及组件的硬件和软件配置以及各种测试的结果。此外、本文档还提供了使用Cisco UCS计算服务器、Cisco互联阵列交换机、Cisco MDS交换机、Cisco Nexus交换机、NetApp AFF 存储和Oracle RAC数据库的实施和最佳实践指导。

"FlexPod 数据中心与基于 Cisco UCS 和 NetApp AFF A 系列的 Oracle RAC 数据库"

Microsoft SQL Server

适用于 Microsoft SQL Server 2019 和 VMware vSphere 6.7 的 FlexPod Datacenter

NetApp公司Cisco Atul Bhalodia的Cisco Sanjeev Nardurkar Gopu Narasimha Reddy

本文档介绍了使用最新硬件和软件产品的FlexPod 参考架构、并提供了在VMware ESXi虚拟化环境中托管Microsoft SQL Server 2019数据库的部署建议。此解决方案 还使用Cisco工作负载优化管理器(Workload Optimization Manager、CWOM)、该管理器可提供自动化建议、以便为SQL工作负载和基础架构提供最佳且高效的资源利用率。

解决方案 基于Cisco统一计算系统(Cisco UCS)构建、并使用统一软件版本4.1.1 c来支持Cisco UCS硬件平台、包括Cisco UCS B系列刀片式服务器、Cisco UCS 6400互联阵列、Cisco Nexus 9000系列交换机和NetApp AFF系列存储阵列。

"适用于 Microsoft SQL Server 2019 和 VMware vSphere 6.7 的 FlexPod Datacenter"

采用 Microsoft SQL Server 2016 和 VMware vSphere 6.5 的 FlexPod Datacenter

NetApp公司Cisco Sanjev Nardurkar、Cisco David Arnette的Gopu Narasimha Reddy

本文档介绍了使用最新硬件和软件产品的FlexPod 参考架构、并提供了在虚拟化环境中部署Microsoft SQL Server数据库的配置建议。

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、Cisco UCS 6300互联阵列、Cisco Nexus 9000系列交换机和NetApp全闪存系列存储阵列。此外、此解决方案 还包括VMware vSphere 6.5和vSphere 6.5、可提供许多新功能来优化存储利用率并促进私有云的使用。

"采用 Microsoft SQL Server 2016 和 VMware vSphere 6.5 的 FlexPod Datacenter"

在VMware和Hyper-V上运行的Linux VM上运行FlexPod Datacenter和Microsoft SQL Server 2017

NetApp公司Cisco Atul Bhalodia的Cisco Sanjeev Nardurkar Gopu Narasimha Reddy

本文档介绍了使用最新硬件和软件产品的FlexPod 参考架构、并提供了在VMware ESXi和Microsoft Windows Hyper-V虚拟化环境中托管Microsoft SQL Server数据库的部署建议、其中包括Microsoft为SQL Server部署提供的Linux支持。

建议的解决方案 架构基于使用统一软件版本4.0.1c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、Cisco UCS 6300互联阵列、Cisco Nexus 9000系列交换机和NetApp AFF 系列存储阵列。

"在VMware和Hyper-V上运行的Linux VM上运行FlexPod Datacenter和Microsoft SQL Server 2017"

在VMware和Hyper-V上运行的Linux VM上运行FlexPod Datacenter和Microsoft SQL Server 2017

NetApp公司Cisco Atul Bhalodia的Cisco Sanjeev Nardurkar Gopu Narasimha Reddy

本文档介绍了使用最新硬件和软件产品的FlexPod 参考架构、并提供了在VMware ESXi和Microsoft Windows Hyper-V虚拟化环境中托管Microsoft SQL Server数据库的部署建议、其中包括Microsoft为SQL Server部署提供的Linux支持。

建议的解决方案 架构基于使用统一软件版本4.0.1c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、Cisco UCS 6300互联阵列、Cisco Nexus 9000系列交换机和NetApp AFF 系列存储阵列。

"在VMware和Hyper-V上运行的Linux VM上运行FlexPod Datacenter和Microsoft SQL Server 2017"

医疗保健

适用于基因组学的 FlexPod

TR-4911： FlexPod 基因组学

NetApp 公司 JayaKishore Esanakula

在医疗保健和生命科学方面，与基因组学相比，医学领域更重要的领域很少，而基因组学正在迅速成为医生和护士的重要临床工具。基因组学与医学影像和数字病理学相结合，可帮助我们了解患者的基因可能会受到治疗协议的影响。基因组学在医疗保健领域的成功越来越取决于大规模数据互操作性。最终目标是，了解大量基因数据，确定临床相关的相关性和变体，以改进诊断并实现精准医学。基因组学有助于我们了解疾病爆发的起源，疾病的演变以及哪些治疗方法和策略可能会很有效。显然，基因组学具有许多涵盖预防，诊断和治疗的优势。医疗保健组织正在努力应对多种挑战，其中包括：

- 提高护理质量
- 基于价值的维护
- 数据爆炸式增长
- 精确医学
- 大流行病
- 可穿戴设备，远程监控和护理
- 网络安全

标准化的临床途径和临床协议是现代医学的重要组成部分之一。标准化的一个关键方面是护理提供商之间的互操作性，不仅对于医疗记录，而且对于基因组数据。一个大问题是，医疗保健组织是否会放弃对基因组数据的所有权，而不是让患者拥有其个人基因组数据和相关医疗记录？

可互操作的患者数据是实现精准医疗的关键，而精准医疗是近期数据激增背后的推动力之一。精准医疗的目标是提高健康维护，疾病预防，诊断和治疗解决方案的有效性和准确性。

数据增长率呈指数级增长。2021 年 2 月初，美国实验室每周对大约 8， 000 个 COVID-19 型菌种进行了排序。截至 2021 年 4 月，按顺序排列的基因组数量已增加到每周 29， 000 个。每个完全序列化的人类基因组的大小约为 125 GB 。因此，按每周排序 29， 000 个基因组的速率，剩余的总基因组存储每年将超过 180 PB 。许多国家 / 地区已承诺为基因组流行病提供资源，以改进基因组监控并为应对下一波全球健康挑战做好准备。

基因组研究成本的降低正在以前所未有的速度推动基因测试和研究。这三个 PS 处于转折点：计算机电源，数据隐私和医学个性化。到 2025 年，研究人员估计将对 1 亿到 20 亿个人类基因组进行测序。要使基因组学发挥效用并成为一项有价值的主张，基因组学功能必须是护理工作流的无缝组成部分；它应该易于访问，并可在患者就诊期间执行操作。同样重要的是，将患者电子病历数据与患者基因组学数据集成在一起。随着 FlexPod 等一流的融合基础架构的出现，企业可以将其基因组功能融入医生，护士和诊所经理的日常工作流中。有关最新的 FlexPod 平台信息，请参见此 "采用 Cisco UCS X 系列的 FlexPod Datacenter 白皮书"。

对于医生来说，基因组学的真正价值包括精准医学和基于患者基因组数据的个性化治疗计划。过去临床医生和数据科学家之间从未有过这样的协同作用，基因组学也从最近的技术创新以及医疗保健组织与行业技术领导者之间的真正合作中受益。

学术医疗中心和其他医疗保健和生命科学组织正在努力建立基因组科学卓越中心（Center of excellence，COE）。据Charlie Gersbach 博士Greg Crawford 和Duke 大学的 Tim E Reddy 说： " 我们知道，基因不是通过简单的二进制开关打开或关闭的，而是由多个协同工作的基因监管开关造成的。" 他们还确定 " 基因组的这些部分都不是孤立地工作的。基因组是一个非常复杂的网络，它是进化所交织的 " （"ref"）。

10 多年来， NetApp 和 Cisco 一直在努力逐步改进 FlexPod 平台。所有客户反馈都会得到倾听，评估，并与 FlexPod 中的价值流和功能集相关联。正是这一持续的反馈，协作，改进和庆祝活动循环让 FlexPod 在全球范围内成为值得信赖的融合基础架构平台。它经过全面简化和设计，成为医疗保健组织最可靠，最强大，最灵活的平台。

范围

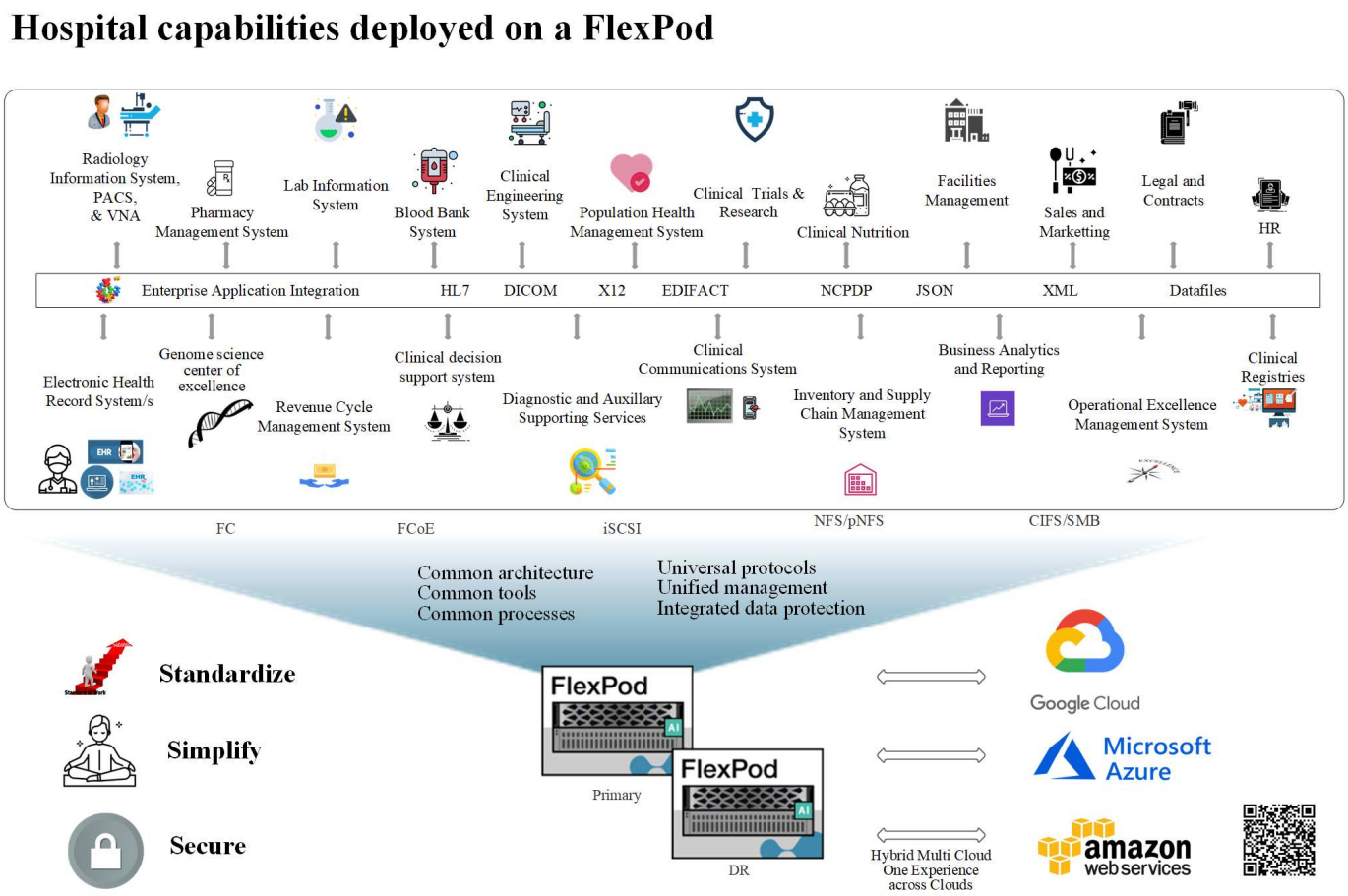
借助 FlexPod 融合基础架构平台，医疗保健组织可以托管一个或多个基因组工作负载以及其他临床和非临床医疗保健应用程序。本技术报告在 FlexPod 平台验证期间使用了一种名为 GATK 的开源行业标准基因组学工具。但是，本文档不会深入探讨基因组学或 GATK 。

audience

本文档面向医疗保健行业的技术主管以及 Cisco 和 NetApp 合作伙伴解决方案工程师和专业服务人员。NetApp 假定读者已很好地了解计算和存储规模估算概念，并在技术上熟悉医疗保健威胁，医疗保健安全，医疗保健 IT 系统， Cisco UCS 和 NetApp 存储系统。

在 **FlexPod** 上部署的医院功能

一家典型的医院拥有多种多样的 IT 系统。大多数此类系统都是从供应商购买的，而很少有系统是由医院内部系统构建的。因此，医院系统必须管理其数据中心的多样化基础架构环境。当医院将其系统统一为 FlexPod 等融合基础架构平台时，企业可以将其数据中心运营标准化。借助 FlexPod ，医疗保健组织可以在同一平台上实施临床和非临床系统，从而统一数据中心运营。



"接下来：在 FlexPod 上部署基因组工作负载的优势。"

在 FlexPod 上部署基因组工作负载的优势

"上一页：简介。"

本节简要列出了在 FlexPod 融合基础架构平台上运行基因组工作负载的优势。我们来快速介绍一下医院的功能。以下业务架构视图显示了一家医院在混合云就绪 FlexPod 融合基础架构平台上部署的功能。

- * 避免医疗保健孤岛。 * 医疗保健孤岛是一个非常值得关注的问题。各个部门往往不是根据自己的选择而是按照演变过程有机地孤立到自己的一组硬件和软件中。例如，放射学，心脏病学， EHR ，基因组学， 分析，收入周期和其他部门最终会获得各自的一套专用软件和硬件。医疗保健组织拥有一组有限的 IT 专业人员来管理其硬件和软件资产。当这组人需要管理一组非常多样化的硬件和软件时，就会出现转折点。供应商为医疗保健组织提供的一系列流程不一致，使异构性变得更加糟糕。
- * 从小规模入手，然后不断增长。 * GATK 工具套件专为 CPU 执行而设计，最适合 FlexPod 等平台。FlexPod 支持网络，计算和存储的独立可扩展性。从小规模入手，随着您的基因组功能和环境增长进行扩展。医疗保健组织无需投资专用平台即可运行基因组工作负载。相反，企业可以利用 FlexPod 等多种平台在同一平台上运行基因组学和非基因组工作负载。例如，如果儿科部门希望实施基因组学功能， IT 领导层可以在现有 FlexPod 实例上配置计算，存储和网络。随着基因组业务部门的发展，医疗保健组织可以根据需要扩展其 FlexPod 平台。
- * 单一控制窗格和无与伦比的灵活性。 * Cisco Intersight 通过将应用程序与基础架构相连接，从裸机服务器和虚拟机管理程序到无服务器应用程序提供可见性和管理，从而显著简化 IT 运营，从而降低成本并降低风险。此统一 SaaS 平台采用统一的开放式 API 设计，可与第三方平台和工具本机集成。此外，它还允许您的

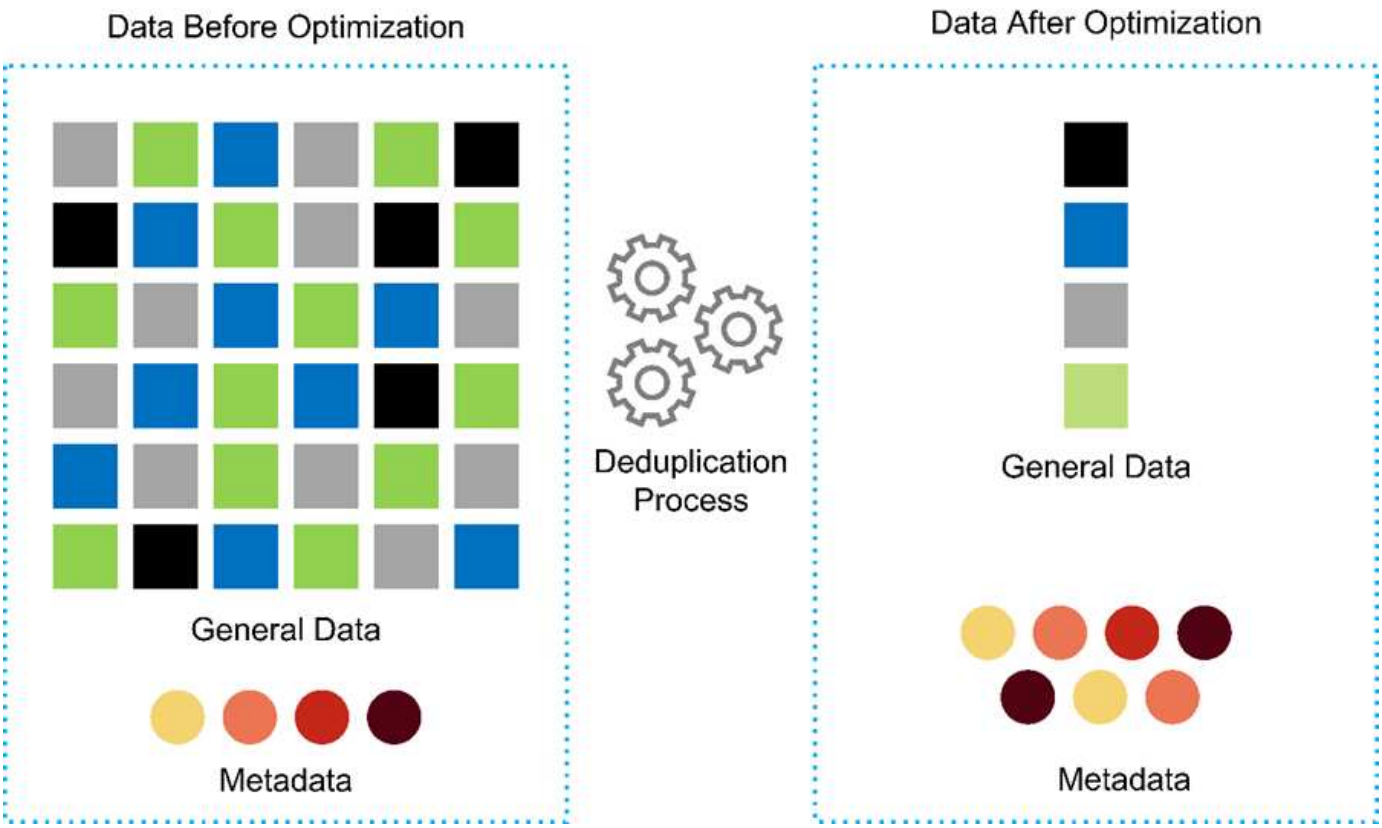
数据中心运营团队在现场或任何位置使用移动应用程序进行管理。

用户可以利用 Intersight 作为管理平台，快速释放环境中的有形价值。Intersight 可以为许多日常手动任务实现自动化，从而消除错误并简化日常操作。此外，借助 Intersight 提供的高级支持功能，采用者可以提前解决问题并加快问题描述解决速度。综合来看，企业在应用程序基础架构上花费的时间和资金远远少于在核心业务开发上花费的时间和资金。

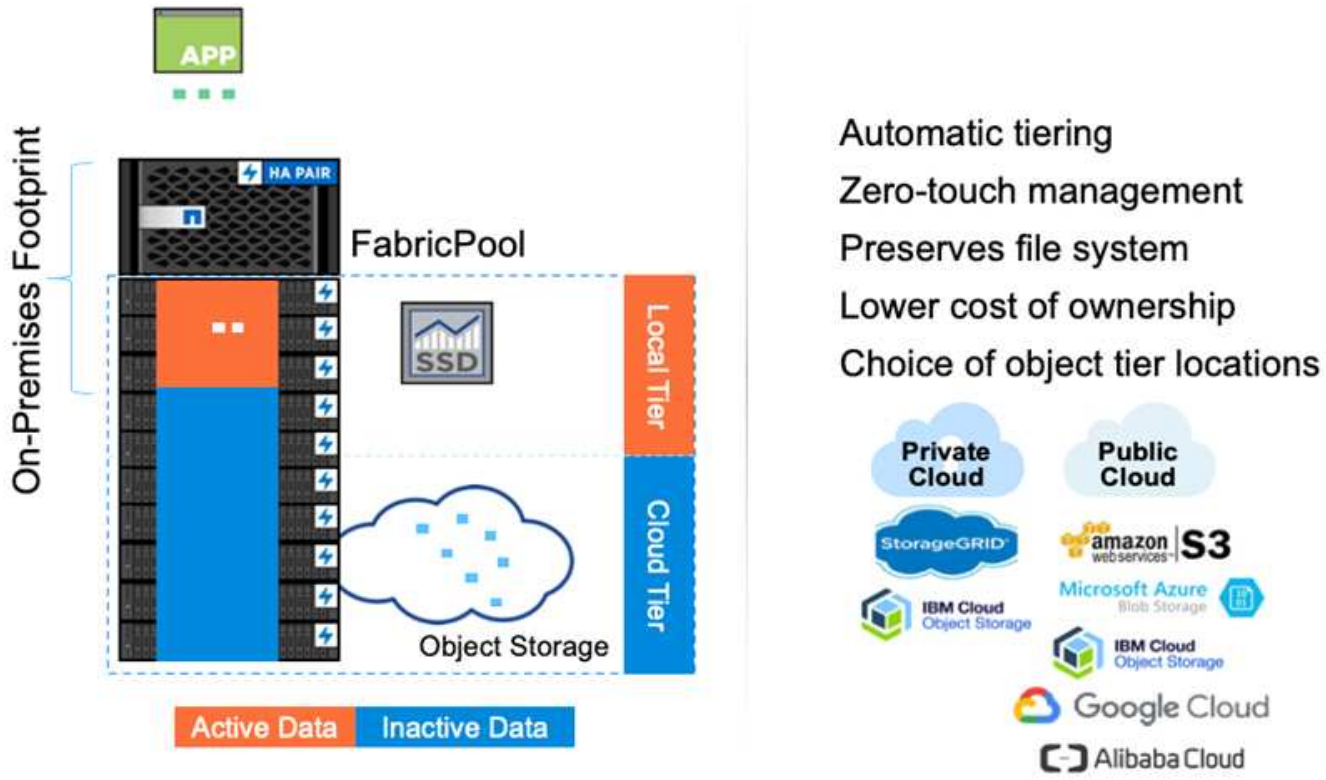
利用 Intersight 管理和 FlexPod 易于扩展的架构，企业可以在一个 FlexPod 平台上运行多个基因组工作负载，从而提高利用率并降低总拥有成本（TCO）。FlexPod 可以灵活地进行规模估算，从小型 FlexPod 快速计划开始，并可扩展到大型 FlexPod 数据中心实施。借助 Cisco Intersight 内置的基于角色的访问控制功能，医疗保健组织可以实施强大的访问控制机制，从而避免需要单独的基础架构堆栈。医疗保健组织内的多个业务部门可以将基因组作为一项关键核心能力。

最终， FlexPod 有助于简化 IT 运营并降低运营成本， IT 基础架构管理员可以将精力集中在帮助临床医生创新的任务上，而不是仅仅为了让他们保持正常运行。

- 经过验证的设计和有保障的结果。 * FlexPod 设计和部署指南经过验证，可以重复使用，其中涵盖了放心部署 FlexPod 所需的全面配置详细信息和行业最佳实践。Cisco 和 NetApp 经验证的设计指南，部署指南和架构可帮助您的医疗保健或生命科学组织从一开始就消除实施经验证且值得信赖的平台时的猜测。借助 FlexPod ，您可以加快部署速度，降低成本，复杂性和风险。FlexPod 经验证的设计和部署指南将 FlexPod 确立为各种基因组工作负载的理想平台。
- * 创新与敏捷性。 * FlexPod 是 Epic ， Cerner ， Meditech 等 EHR 公司以及 Agfa ， GE ，飞利浦等成像系统的理想平台。有关的详细信息，请参见 "史诗般的荣誉卷" 和目标平台架构，请参见 Epic 用户 Web 。运行基因组学 "FlexPod" 让医疗保健组织能够灵活地继续其创新之旅。借助 FlexPod ，实施组织变革自然成为必然。当企业在 FlexPod 平台上实现标准化时，医疗保健 IT 专家可以为创新配置时间，精力和资源，从而实现生态系统所需的灵活性。
- * 数据解放。 * 借助 FlexPod 融合基础架构平台和 NetApp ONTAP 存储系统，可以通过一个平台上的各种规模协议提供和访问基因组数据。采用 NetApp ONTAP 的 FlexPod 提供了一个简单，直观且功能强大的混合云平台。由 NetApp ONTAP 提供支持的 Data Fabric 可跨站点，跨物理边界和跨应用程序将数据集于一体。您的 Data Fabric 专为以数据为中心的环境中的数据驱动型企业而构建。数据在多个位置创建和使用，通常需要利用并与其他位置，应用程序和基础架构共享。因此，您需要采用一致且集成的方式来管理它。FlexPod 可以让您的 IT 团队掌控一切，并简化日益增加的 IT 复杂性。
- * 安全多租户。 * FlexPod 使用符合 FIPS 140-2 的加密模块，因此，企业可以将安全性作为基本要素来实施，而不是事后考虑。无论平台大小如何， FlexPod 都支持企业从一个融合基础架构平台实施安全多租户。采用安全多租户和 QoS 的 FlexPod 有助于分离工作负载并最大程度地提高利用率。这有助于避免资本被锁定到可能未充分利用且需要专业技能集进行管理的专用平台中。
- * 存储效率。 * 基因组学要求底层存储具有行业领先的存储效率功能。您可以利用 NetApp 存储效率功能降低存储成本，例如重复数据删除（实时和按需），数据压缩和数据缩减（"ref"）。NetApp 重复数据删除可在 FlexVol 卷中提供块级重复数据删除。从本质上说，重复数据删除会删除重复的块，从而仅在 FlexVol 卷中存储唯一的块。重复数据删除的粒度较高，并在 FlexVol 卷的活动文件系统上运行。下图简要显示了 NetApp 重复数据删除的工作原理。重复数据删除是应用程序透明的。因此，可以使用它对使用 NetApp 系统的任何应用程序生成的数据进行重复数据删除。您可以将卷重复数据删除作为实时进程和后台进程运行。您可以将其配置为自动运行，计划运行或通过命令行界面， NetApp ONTAP System Manager 或 NetApp Active IQ Unified Manager 手动运行。



- * 实现基因组互操作性。 * ONTAP FlexCache 是一种远程缓存功能，可简化文件分发，减少 WAN 延迟并降低 WAN 带宽成本 "ref"）。基因组变体识别和标注期间的一项关键活动是临床医生之间的协作。即使协作临床医生位于不同地理位置， ONTAP FlexCache 技术也能提高数据吞吐量。鉴于 * 。 bam 文件的典型大小（ 1 GB 到 100 GB ），底层平台必须能够向不同地理位置的临床医生提供文件。采用 ONTAP FlexCache 的 FlexPod 让基因组数据和应用程序真正实现了多站点就绪，让全球各地的研究人员可以无缝协作，实现低延迟和高吞吐量。在多站点环境下运行基因组学应用程序的医疗保健组织可以使用数据网络结构进行横向扩展，以平衡易管理性与成本和速度。
- * 智能使用存储平台。 * 采用 ONTAP 自动分层和 NetApp Fabric Pool 技术的 FlexPod 可简化数据管理。FabricPool 有助于降低存储成本，而不会影响性能，效率，安全性或保护。FabricPool 对企业级应用程序是透明的，它可以降低存储 TCO ，而无需重新构建应用程序基础架构，从而充分利用云效率。FlexPod 可以从 FabricPool 的存储分层功能中受益，从而更高效地利用 ONTAP 闪存存储。有关详细信息，请参见 " 采用 FabricPool 的 FlexPod"。下图简要概述了 FabricPool 及其优势。



- * 更快的变体分析和标注速度。 * FlexPod 平台的部署和实施速度更快。FlexPod 平台可实现大规模数据可用，并提供低延迟和更高吞吐量，从而实现临床医生协作。增强的互操作性有助于创新。医疗保健组织可以并行运行基因组和非基因组工作负载，这意味着组织不需要专门的平台来开始其基因组学之旅。

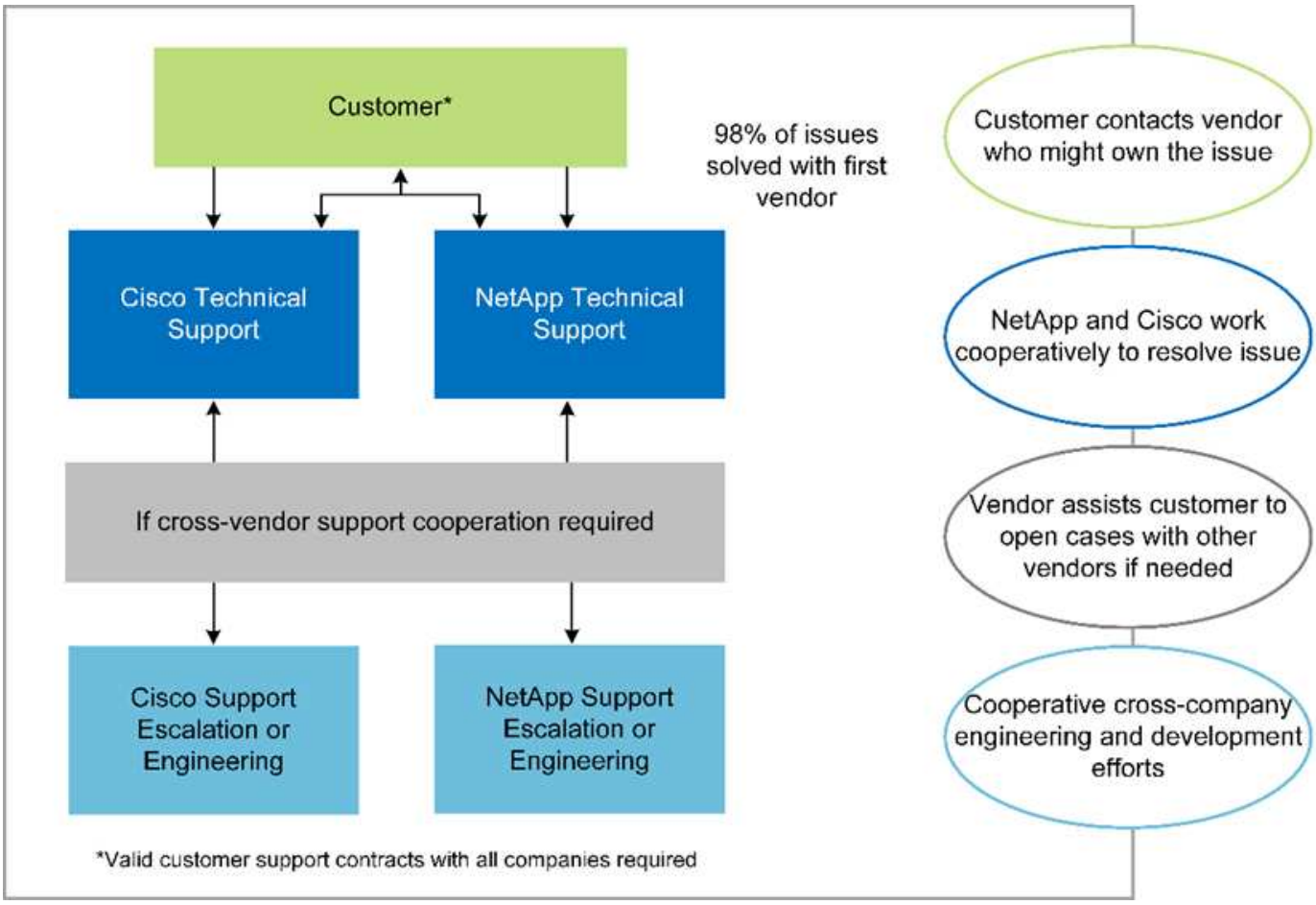
  FlexPod ONTAP 会定期为存储平台添加前沿功能。FlexPod 数据中心是部署 FC-NVMe 以允许需要高性能存储访问的应用程序的最佳共享基础架构基础。随着 FC-NVMe 不断发展，包括高可用性，多路径和额外的操作系统支持， FlexPod 非常适合作为首选平台，可提供支持这些功能所需的可扩展性和可靠性。ONTAP 通过端到端 NVMe 实现更快的 I/O ，从而加快完成基因组分析的速度（ "ref"）。

  按顺序排列的原始基因组数据会产生较大的文件大小，因此，请务必将这些文件提供给变体分析器，以减少从样本收集到变体标注所需的总时间。NVMe （非易失性内存快速）用作存储访问和数据传输协议时，可提供前所未有的吞吐量水平和最快的响应时间。FlexPod 可在通过 PCI Express 总线（ PCIe ）访问闪存存储时部署 NVMe 协议。PCIe 支持实施数万个命令队列，从而提高了并行处理能力和吞吐量。从存储到内存的一个协议可以快速访问数据。

- * 从零到零的灵活性进行临床研究。 * 灵活，可扩展的存储容量和性能使医疗保健研究组织能够以弹性或实时（ JIT ）的方式优化环境。通过将存储与计算和网络基础架构分离，可以在不中断的情况下纵向和横向扩展 FlexPod 平台。使用 Cisco Intersight ，可以使用内置和自定义自动化工作流来管理 FlexPod 平台。借助 Cisco Intersight 工作流，医疗保健组织可以缩短应用程序生命周期管理时间。当学术医疗中心要求将患者数据匿名化并提供给其研究信息学中心和 / 或质量中心时，其 IT 组织可以利用 Cisco Intersight FlexPod 工作流在数秒内（而不是数小时）执行安全数据备份，克隆和还原。借助 NetApp Trident 和 Kubernetes ， IT 组织可以配置新的数据科学家，并在几分钟内（有时甚至几秒钟内）为模型开发提供临床数据。
- * 保护基因组数据。 * NetApp SnapLock 提供了一个专用卷，可在其中存储文件并将其置于不可擦除，不可重写的状态。用户驻留在 FlexVol 卷中的生产数据可以通过 NetApp SnapMirror 或 SnapVault 技术镜像或存储到 SnapLock 卷。在保留期限结束之前，无法删除 SnapLock 卷，卷本身及其托管聚合中的文件。使用 ONTAP FPolicy 软件，企业可以禁止对具有特定扩展名的文件执行操作，从而防止勒索软件攻击。可以为特定文件操作触发 FPolicy 事件。此事件与策略相关联，策略将调用需要使用的引擎。您可以为策略配置一组可能包含勒索软件的文件扩展名。如果具有不允许扩展名的文件尝试执行未经授权的操作，则 FPolicy 会阻

止执行该操作 ("ref"）。

- * FlexPod 合作支持。 * NetApp 和 Cisco 建立了 FlexPod 合作支持，这是一种强大，可扩展且灵活的支持模式，可满足 FlexPod 融合基础架构的独特支持要求。此模式结合了 NetApp 和 Cisco 的经验，资源和技术支持专业知识，可以简化识别和解决 FlexPod 支持问题的流程，而不管问题位于何处。下图概述了 FlexPod 合作支持模式。客户联系可能拥有问题描述的供应商， Cisco 和 NetApp 将合作解决此问题。Cisco 和 NetApp 拥有跨公司工程和开发团队，他们携手解决问题。此支持模式可减少翻译期间的信息丢失，建立信任并减少停机时间。

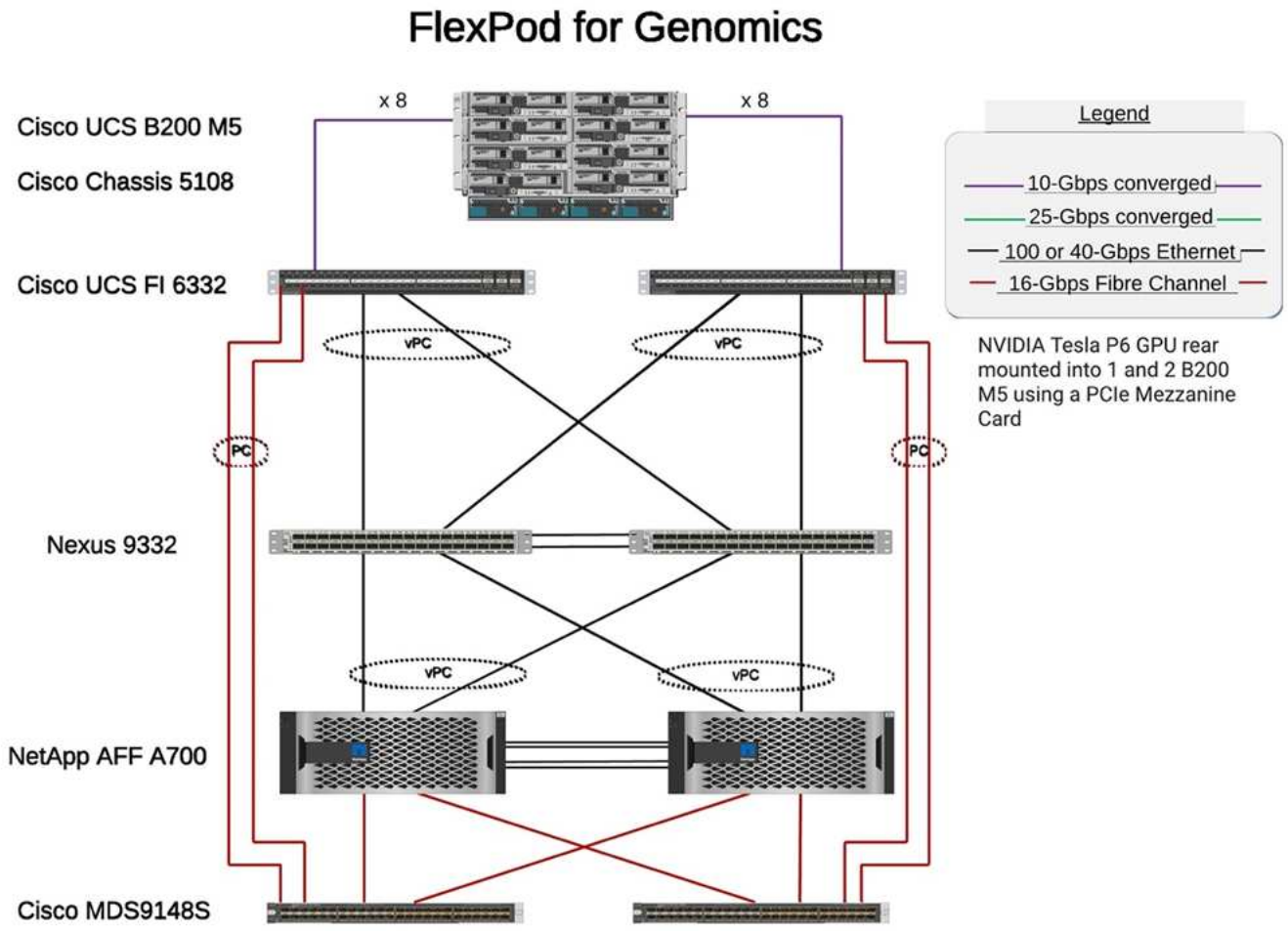


"接下来：解决方案基础架构硬件和软件组件。"

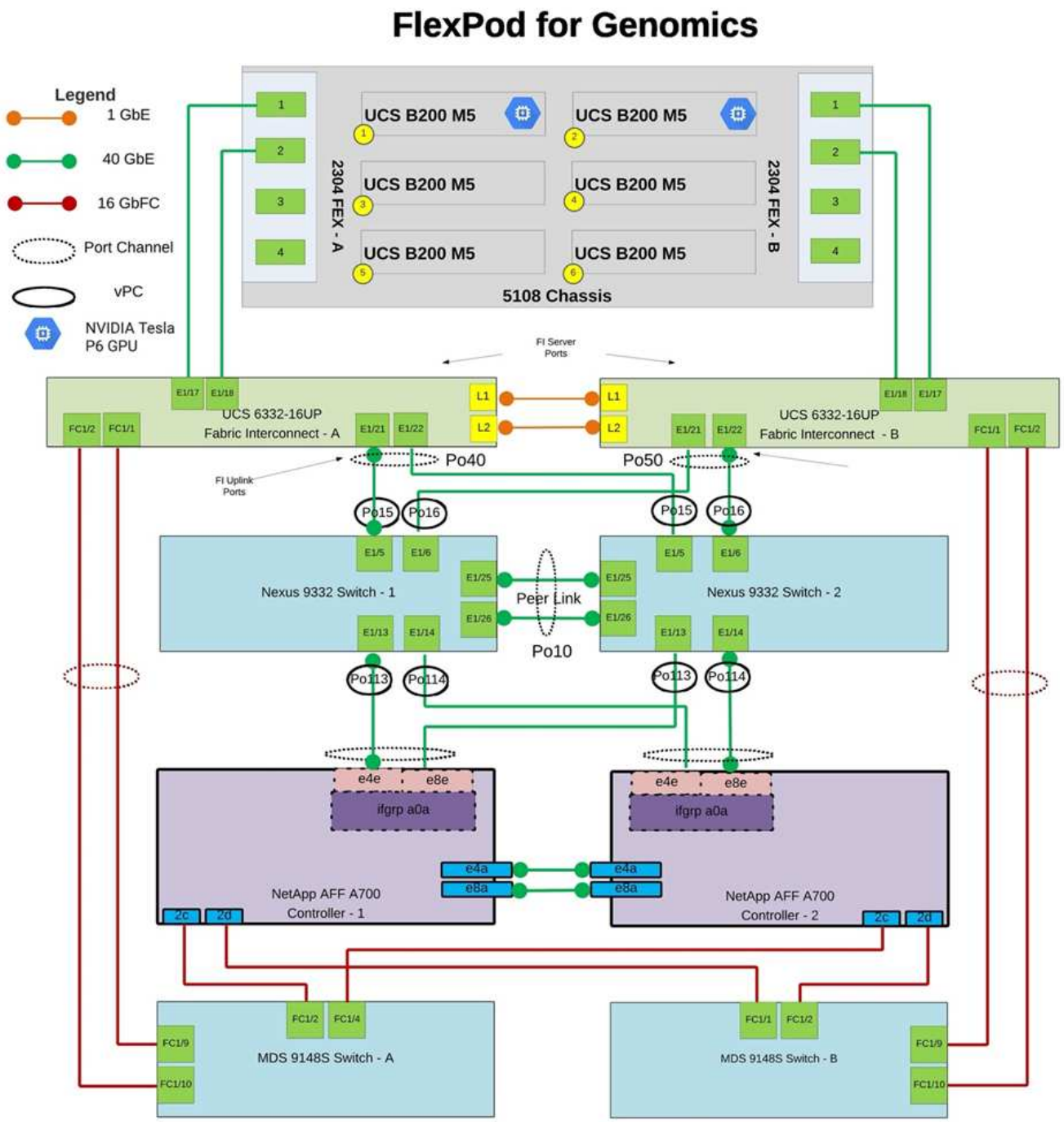
解决方案基础架构硬件和软件组件

"先前版本：在 FlexPod 上部署基因组工作负载的优势。"

下图显示了用于 GATK 设置和验证的 FlexPod 系统。我们使用了 "采用 VMware vSphere 7.0 和 NetApp ONTAP 9.7 的 FlexPod Datacenter Cisco 验证设计（CVD）" 在设置过程中。



下图显示了 FlexPod 布线详细信息。



下表列出了在 FlexPod 上启用 GATK 测试期间使用的硬件组件。下面是 "NetApp 互操作性表工具" （IMT）和 "Cisco 硬件兼容性列表（HCL）"。

层	产品系列	数量和型号	详细信息
计算	Cisco UCS 5108 机箱	1 或 2	
	Cisco UCS 刀片式服务器	6 个 B200 M5	每个都具有 2 个 20 或更多核心， 2.7 GHz 和 128-384 GB RAM

层	产品系列	数量和型号	详细信息
	Cisco UCS 虚拟接口卡（VIC）	Cisco UCS 1440	请参见
	2 个 Cisco UCS 互联阵列	6332	-
网络	Cisco Nexus 交换机	2 个 Cisco Nexus 9332	-
存储网络	用于通过 SMB/CIFS，NFS 或 iSCSI 协议进行存储访问的 IP 网络	与上述相同的网络交换机	-
	通过 FC 进行存储访问	2 个 Cisco MDS 9148S	-
存储	NetApp AFF A700 全闪存存储系统	1 个集群	具有两个节点的集群
	磁盘架	一个 DS224C 或 NS224 磁盘架	已完全填充 24 个驱动器
	SSD	24， 1.2 TB 或更大容量	-

此表列出了基础架构软件。

软件	产品系列	版本或版本	详细信息
各种	Linux	RHEL 8.3	-
	Windows	Windows Server 2012 R2（64 位）	-
	NetApp ONTAP	ONTAP 9.8 或更高版本	-
	Cisco UCS 互联阵列	Cisco UCS Manager 4.1 或更高版本	-
	Cisco 以太网 3000 或 9000 系列交换机	对于 9000 系列，对于 3000 系列，则为 7.0 （3） i7 （7）或更高版本，对于 9.2 （4）或更高版本	-
	Cisco FC： Cisco MDS 9132T	8.4 （1a）或更高版本	-
	虚拟机管理程序	VMware vSphere ESXi 7.0	-
存储	虚拟机管理程序管理系统	VMware vCenter Server 7.0 （vCSA）或更高版本	-
网络	NetApp 虚拟存储控制台（VSC）	VSC 9.7 或更高版本	-
	NetApp SnapCenter	SnapCenter 4.3 或更高版本	-
	Cisco UCS Manager	4.1 （3c）或更高版本	
虚拟机管理程序	ESXi		

软件	产品系列	版本或版本	详细信息
管理	虚拟机管理程序管理系统 VMware vCenter Server 7.0 （ vCSA ）或更高版本		
	NetApp 虚拟存储控制台（ VSC ）	VSC 9.7 或更高版本	
	NetApp SnapCenter	SnapCenter 4.3 或更高版本	
	Cisco UCS Manager	4.1 （ 3c ）或更高版本	

"接下来：基因组学— GATK 设置和执行。"

基因组学— GATK 设置和执行

"先前版本：解决方案基础架构硬件和软件组件。"

根据国家人类基因组研究所（ "NHGRI"），" 基因组学是对一个人的所有基因（基因组）的研究，包括这些基因相互作用以及与人的环境相互作用。"

根据 "NHGRI"" 去氧碳核克利酸（ Deoxyribonucleic acid ， DNA/ 脱氧核素）是一种化合物，其中包含开发和指导几乎所有生物体活动所需的说明。DNA 分子由两个绞合成对的线组成，通常称为双螺旋。 " " 一个生物体的一整套基因称为其基因组。 "

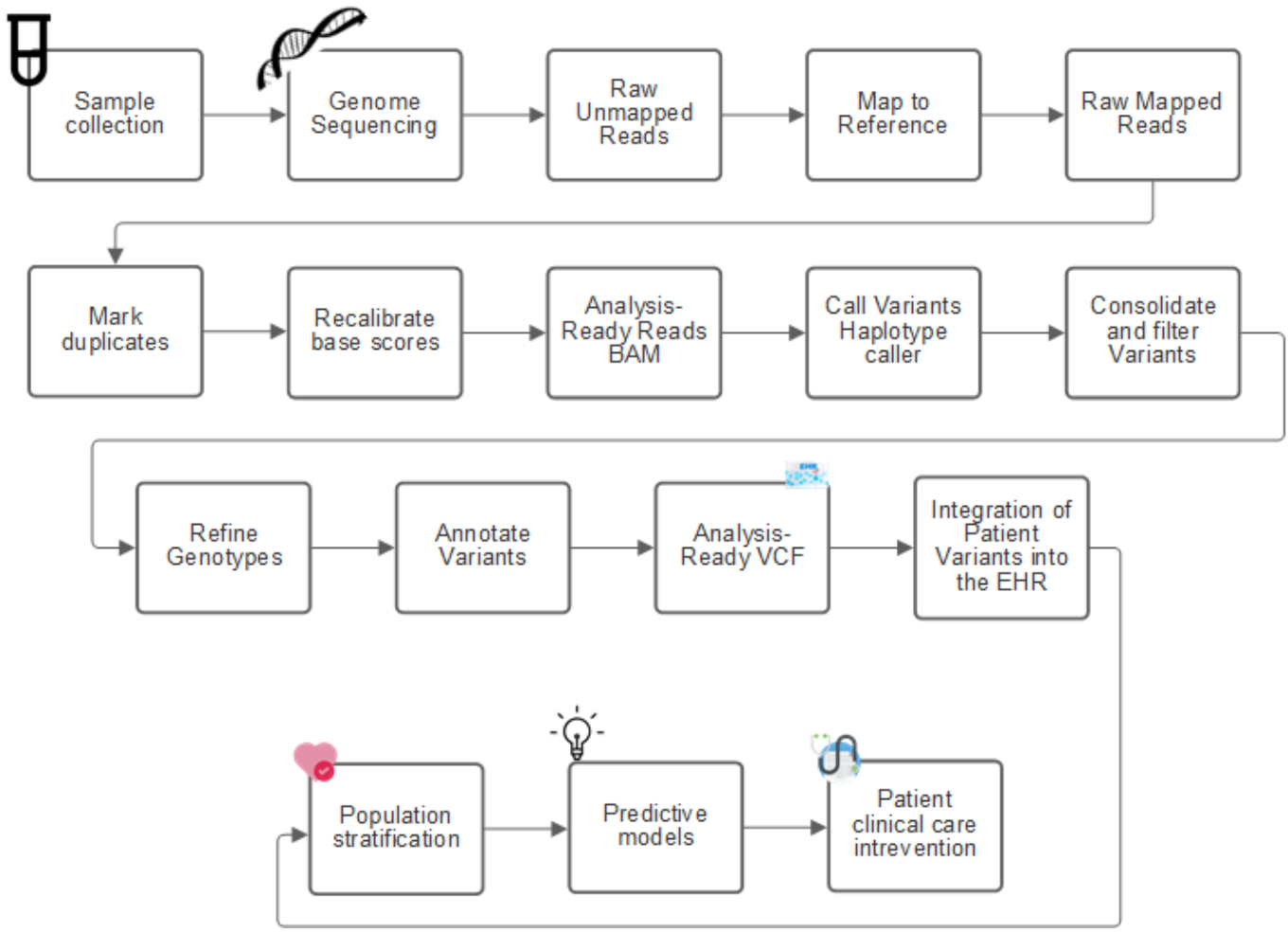
测序是指确定基准在一个 DNA 链中的确切顺序的过程。当今最常见的排序类型之一称为 " 按合成排序 " 。此技术使用荧光信号的辐射来对基准进行排序。研究人员可以使用基因排序来搜索遗传变体以及在某个人仍处于萌芽阶段时可能对疾病的发展或发展起作用的任何变体。

从样本到变体标识，标注和预测

从较高的层面来看，基因组学可以分为以下几个步骤。以下列表并不详尽：

1. 样本收集。
2. "基因组测序" 使用序列发生器生成原始数据。
3. 预处理。例如： "deduplication" 使用 "图标"。
4. 基因组分析。
   a. 映射到参考基因组。
   b. "变体" 通常使用 GATK 和类似工具执行标识和标注。
5. 集成到电子运行状况记录（ EHR ）系统中。
6. "人口分层" 并确定跨地理位置和种族背景的遗传变体。
7. "预测模型" 使用显著的单核退潮多形态。
8. "验证"。

下图显示了从采样到变体标识，标注和预测的过程。



人类基因组项目于 2003 年 4 月完成，该项目对公有域中的人类基因组序列进行了高质量的模拟。这种参考基因组引发了基因组功能研究和开发的爆炸式增长。几乎每一种人类疾病都有其基因特征。直到最近，医生一直在利用基因预测和确定诸如镰状细胞性贫血之类的缺陷，这是由一个基因的变化所导致的某种继承模式引起的。人类基因组项目所提供的数据的宝贵财富导致了基因组功能的当前状态的出现。

基因组学具有一系列广泛的优势。以下是医疗保健和生命科学领域的一小部分优势：

- 更好地在护理点进行诊断
- 预后更好
- 精确医学
- 个性化的治疗计划
- 改善疾病监控
- 减少不利事件
- 改善获得治疗的途径
- 改进了疾病监控
- 有效地参与临床试验，并根据基因型更好地选择患者进行临床试验。

基因组学是一种 "四向 Beast ，" 因为数据集的整个生命周期都有计算需求：采集，存储，分布和分析。

基因组分析工具包（**GATK**）

GATK 是作为中的数据科学平台而开发的 "Broad Institute"。GATK 是一组开源工具，可用于进行基因组分析，尤其是变体发现，标识，标注和基因分型。GATK 的一个优势是，可以将一组工具和 / 或命令链接在一起，形成一个完整的工作流。广义学院要应对的主要挑战如下：

- 了解疾病的根本原因和生物机制。
- 确定可用于基本发生原因 of a disease 的治疗干预措施。
- 了解从各种变体到在人类物理中发挥作用的视觉特征。
- 制定标准和策略 "框架" 用于基因组数据表示，存储，分析，安全性等。
- 实现可互操作的基因组聚合数据库（gnomAD）的标准化和社交化。
- 基于基因组的患者监控，诊断和治疗更加精确。
- 帮助实施能够在症状出现之前很好地预测疾病的工具。
- 创建一个跨学科合作伙伴社区并赋予其能力，帮助解决生物医学领域最棘手，最重要的问题。

GATK 和 Broad Institute 表示，基因组测序应视为病理学实验室的一种协议；每个任务都经过了详细记录，优化，可重现，并在样本和实验中保持一致。下面是 Broad Institute 建议的一组步骤，有关详细信息，请参见 "GATK 网站"。

FlexPod 设置

基因组工作负载验证包括从头开始设置 FlexPod 基础架构平台。FlexPod 平台具有高可用性，可以独立扩展；例如，可以独立扩展网络，存储和计算。我们使用以下经过 Cisco 验证的设计指南作为参考架构文档来设置 FlexPod 环境： "采用 VMware vSphere 7.0 和 NetApp ONTAP 9.7 的 FlexPod Datacenter"。请参见以下 FlexPod 平台设置亮点：

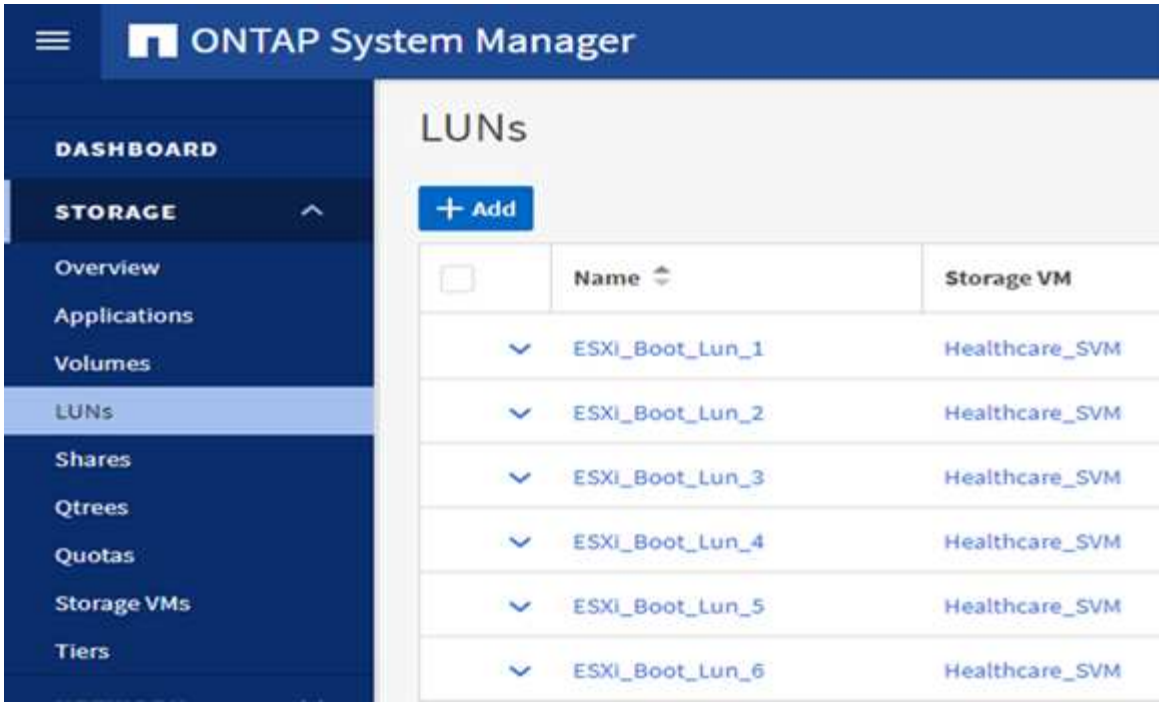
要执行 FlexPod 实验室设置，请完成以下步骤：

1. FlexPod 实验室设置和验证使用以下 IP4 预留和 VLAN 。

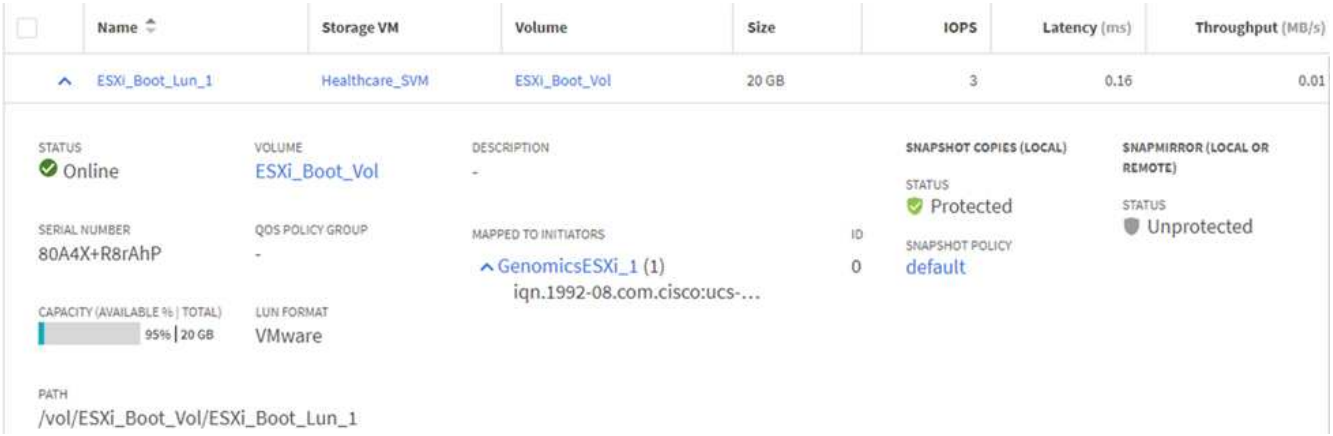
IP Reservations

VLAN	IP Range	Subnet Mask	Purpose
3281	172.21.25 /24	255.255.255.0	IB-MGMT
3282	172.21.26 /24	255.255.255.0	vMotion
3283	172.21.27 /24	255.255.255.0	VM
3284	172.21.28 /24	255.255.255.0	NFS
3285	172.21.29 /24	255.255.255.0	iSCSI-A
3286	172.21.30 /24	255.255.255.0	iSCSI-B

2. 在 ONTAP SVM 上配置基于 iSCSI 的启动 LUN 。

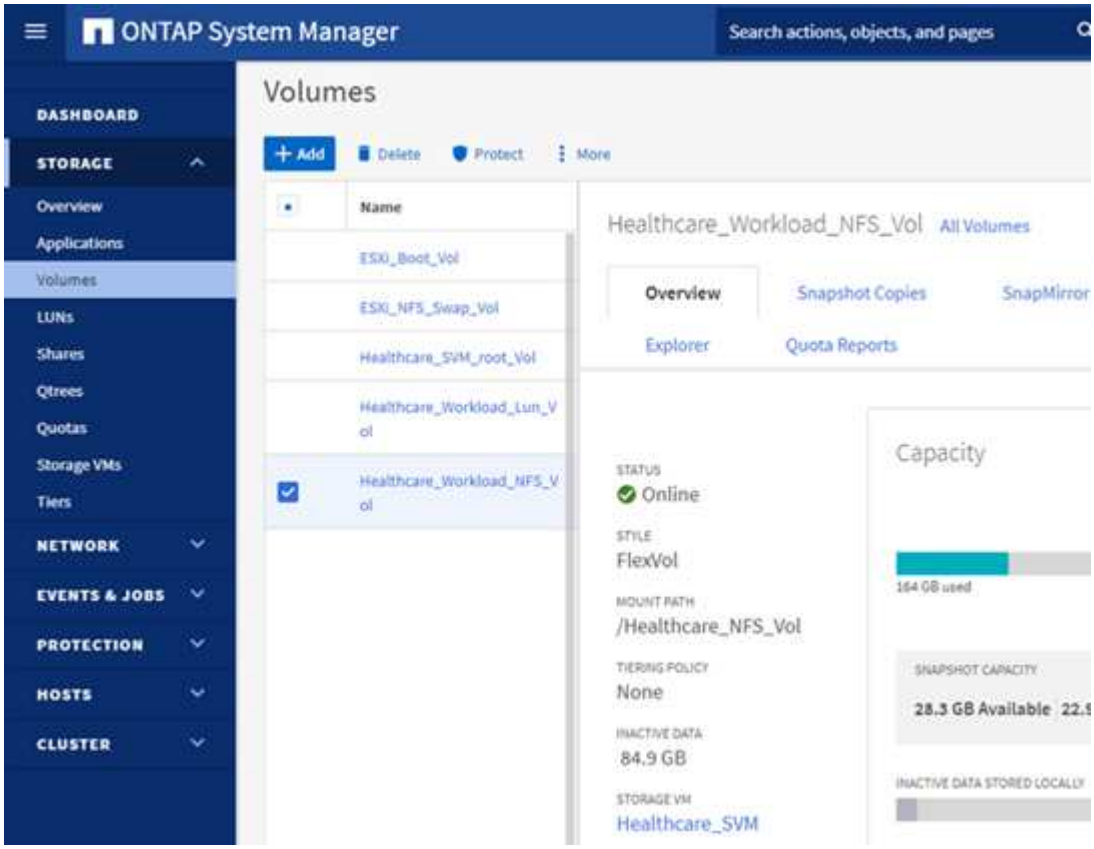


3. 将 LUN 映射到 iSCSI 启动程序组。

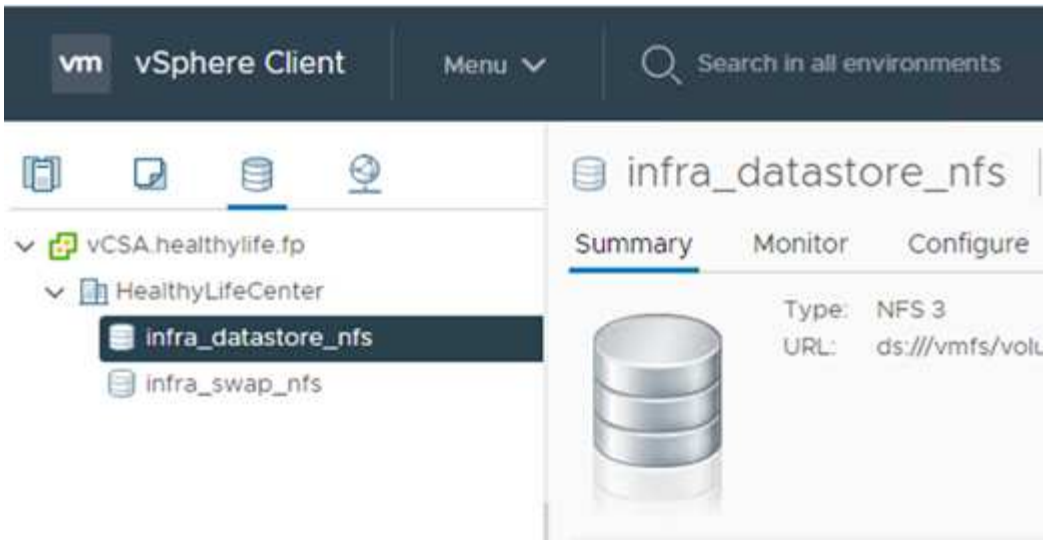


4. 使用 iSCSI 启动安装 vSphere 7.0 。
5. 向 vCenter 注册 ESXi 主机。

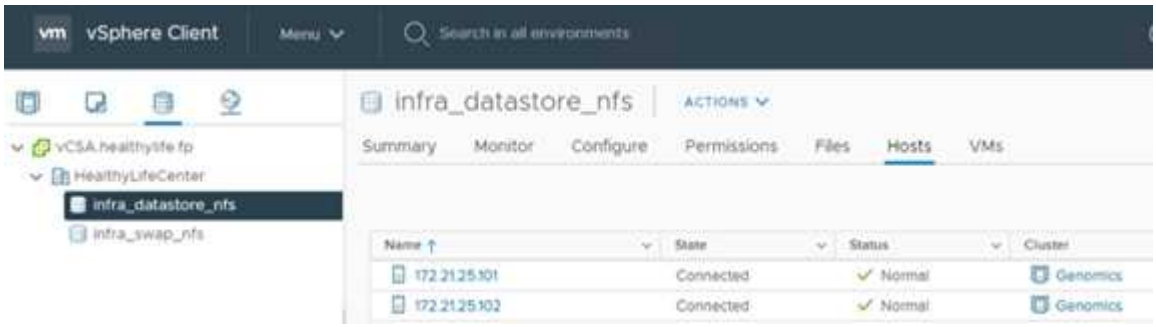
6. 在 ONTAP 存储上配置 NFS 数据存储库 `infra_datastore_nfs` 。



7. 将数据存储库添加到 vCenter 。



8. 使用 vCenter 向 ESXi 主机添加 NFS 数据存储库。



9. 使用 vCenter 创建 Red Hat Enterprise Linux （ RHEL ） 8.3 VM 以运行 GATK 。
10. NFS 数据存储库会提供给虚拟机并挂载在 ` /mnt/genomics` 中，用于存储 GATK 可执行文件，脚本，二进制对齐映射（ BAM ）文件，参考文件，索引文件，词典文件和输出文件，以用于变量调用。

```
[root@genomics1 genomics]# df | grep genomics
/dev/sdb                308587328  5699492 287142812   2% /mnt/genomics
[root@genomics1 genomics]#
```

GATK 设置和执行

在 RedHat Enterprise 8.3 Linux VM 上安装以下前提条件：

- Java 8 或 SDK 1.8 或更高版本
- 从 Broad Institute 下载 GATK 4.2.0.0 "GitHub 站点"。基因组序列数据通常以一系列制表符分隔的 ASCII 列的形式存储。但是， ASCII 需要的存储空间太多。因此，一个新标准会逐渐演变为 BAM （ * 。 bam ）文件。BAM 文件以压缩，索引和二进制形式存储序列数据。我们 "已下载" 一组公开可用的 BAM 文件，用于从执行 GATK "公有域"。我们还下载了索引文件（ * 。 bai ），词典文件（ * 。dict ）和引用数据文件（ * 。FASAA ）公有。

下载后， GATK 工具包将包含一个 JAR 文件和一组支持脚本。

- `gatk-package-4.2.0.0-local.jar` 可执行文件

- `gatk` 脚本文件。

我们下载了一个由父，母和子 * 。 bam 文件组成的系列的 BAM 文件以及相应的索引，词典和参考基因组文件。

克伦威尔引擎

Cromwell 是一款开源引擎，适用于支持工作流管理的科学工作流。可以将 Cromwell 引擎分为两种运行方式 "模式"，服务器模式或单工作流运行模式。可以使用控制 Cromwell 引擎的行为 "Cromwell 引擎配置文件"。

- * 服务器模式。 * 启用 "RESTful" 在 Cromwell 引擎中执行工作流。
- * 运行模式。 * 运行模式最适合在克伦威尔执行单个工作流， "ref" 查看运行模式下的一整套可用选项。

我们使用克伦威尔引擎大规模执行工作流和管道。Cromwell 引擎使用用户友好型 "Workflow 问题描述语言" （ WDL ）编写脚本的语言。此外，还支持第二个工作流脚本编写标准，称为通用工作流语言（ Common Workflow Language ， CWL ）。在本技术报告中，我们使用了 WDL 。WDL 最初是由广泛的基因组分析管道研究所开发的。使用 WDL 工作流可以通过多种策略来实施，其中包括：

- * 线性链。 * 顾名思义，任务 1 的输出将作为输入发送到任务 2 。
- * 多输入 / 输出。 * 这与线性链类似，因为每个任务都可以将多个输出作为输入发送到后续任务。
- * 散点收集。 * 这是最强大的企业应用程序集成（ EAI ）策略之一，尤其是在事件驱动型架构中使用时。每个任务以分离的方式执行，每个任务的输出将整合到最终输出中。

使用 WDL 在独立模式下运行 GATK 的步骤有三个：

1. 使用 `womtool.jar` 验证语法。

```
[root@genomics1 ~]#  java -jar womtool.jar validate ghplo.wdl
```

2. 生成输入 JSON 。

```
[root@genomics1 ~]#  java -jar womtool.jar inputs ghplo.wdl > ghplo.json
```

3. 使用 Cromwell 引擎和 `Cromwell.jar` 运行工作流。

```
[root@genomics1 ~]#  java -jar cromwell.jar run ghplo.wdl --inputs
ghplo.json
```

可以使用多种方法执行 GATK ；本文档将探讨其中三种方法。

使用 **JAR** 文件执行 **GATK**

下面我们来了解一下使用哈普斯特型变量调用程序执行单一变体调用管道的情况。

```
[root@genomics1 ~]#  java -Dsamjdk.use_async_io_read_samtools=false \
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta
```

在这种执行方法中，我们使用 GATK 本地执行 JAR 文件，使用一个 Java 命令调用该 JAR 文件，并将多个参数传递到该命令。

1. 此参数表示我们正在调用 `Hplotypecaller` 变量调用程序管道。
2. ` - 输入` 指定输入 BAM 文件。
3. ` -output` 以变体调用格式（ * 。 vcf ）指定变体输出文件 ("ref"）。
4. 使用 ` -reference` 参数时，我们将传递一个参考基因组。

执行后，可以在部分中找到输出详细信息 "使用 JAR 文件执行 GATK 的输出。"

使用 ./gatk 脚本执行 GATK

GATK 工具套件可使用 ` 。 /gatk` 脚本执行。让我们来看看以下命令：

```
[root@genomics1 execution]# ./gatk \
--java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
```

我们会向命令传递多个参数。

- 此参数表示我们正在调用 `Hplotypecaller` 变量调用程序管道。
- ` -i` 指定输入 BAM 文件。
- ` -O` 以变体调用格式（ * 。 vcf ）指定变体输出文件 ("ref"）。
- 使用 ` -R` 参数时，我们会传递一个参考基因组。

执行后，可以在部分中找到输出详细信息 "016e203cf9beada735f224ab14d0b3af"

我们使用 Cromwell 引擎管理 GATK 执行。我们来检查命令行及其参数。

```
[root@genomics1 genomics]# java -jar cromwell-65.jar \
run /mnt/genomics/GATK/seq/ghplo.wdl  \
--inputs /mnt/genomics/GATK/seq/ghplo.json
```

在此，我们通过传递 `-JAR` 参数来调用 Java 命令，以指示我们要执行 JAR 文件，例如， `Cromwell-65.jar` 。传递的下一个参数（`run` ）表示 Cromwell 引擎正在运行模式，另一个可能的选项是服务器模式。下一个参数为 `* 。 wdll` ，运行模式应使用该参数执行管道。下一个参数是要执行的工作流的一组输入参数。

以下是 `ghplo.wdll` 文件的内容：

```
[root@genomics1 seq]# cat ghplo.wdl
workflow helloHaplotypeCaller {
  call haplotypeCaller
}
task haplotypeCaller {
  File GATK
  File RefFasta
  File RefIndex
  File RefDict
  String sampleName
  File inputBAM
  File bamIndex
  command {
    java -jar ${GATK} \
         HaplotypeCaller \
        -R ${RefFasta} \
        -I ${inputBAM} \
        -O ${sampleName}.raw.indels.snps.vcf
  }
  output {
    File rawVCF = "${sampleName}.raw.indels.snps.vcf"
  }
}
[root@genomics1 seq]#
```

下面是相应的 JSON 文件以及对 Cromwell 引擎的输入。

```
[root@genomics1 seq]# cat ghplo.json
{
"helloHaplotypeCaller.haplotypeCaller.GATK": "/mnt/genomics/GATK/gatk-
4.2.0.0/gatk-package-4.2.0.0-local.jar",
"helloHaplotypeCaller.haplotypeCaller.RefFasta": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta",
"helloHaplotypeCaller.haplotypeCaller.RefIndex": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta.fai",
"helloHaplotypeCaller.haplotypeCaller.RefDict": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.dict",
"helloHaplotypeCaller.haplotypeCaller.sampleName": "fatherbam",
"helloHaplotypeCaller.haplotypeCaller.inputBAM": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bam",
"helloHaplotypeCaller.haplotypeCaller.bamIndex": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bai"
}
[root@genomics1 seq]#
```

请注意， Cromwell 使用内存数据库来执行。执行后，输出日志将显示在一节中 "使用 Cromwell 引擎执行 GATK 的输出。"

有关如何执行 GATK 的一组完整步骤，请参见 "GATK 文档"。

"下一步：使用 JAR 文件执行 GATK 的输出。"

使用 JAR 文件执行 GATK 的输出

"上一篇：基因组学— GATK 设置和执行。"

使用 Jar 文件执行 GATK 会生成以下示例输出。

```
[root@genomics1 execution]# java -Dsamjdk.use_async_io_read_samtools=false
\
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
22:52:58.430 INFO  NativeLibraryLoader - Loading libgkl_compression.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
```

```
local.jar!/com/intel/gkl/native/libgkl_compression.so
Aug 17, 2021 10:52:58 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
22:52:58.541 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
22:52:58.542 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
22:52:58.542 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
22:52:58.542 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v1.8.0_302-b08
22:52:58.542 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021
10:52:58 PM EDT
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
22:52:58.542 INFO  HaplotypeCaller - Picard Version: 2.25.0
22:52:58.542 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
22:52:58.543 INFO  HaplotypeCaller - Deflater: IntelDeflater
22:52:58.543 INFO  HaplotypeCaller - Inflater: IntelInflater
22:52:58.543 INFO  HaplotypeCaller - GCS max retries/reopens: 20
22:52:58.543 INFO  HaplotypeCaller - Requester pays: disabled
22:52:58.543 INFO  HaplotypeCaller - Initializing engine
22:52:58.804 INFO  HaplotypeCaller - Done initializing engine
22:52:58.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
22:52:58.820 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
22:52:58.821 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
22:52:58.854 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
```

```
22:52:58.854 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
running PairHMM
22:52:58.854 INFO  IntelPairHmm - Available threads: 16
22:52:58.854 INFO  IntelPairHmm - Requested threads: 4
22:52:58.854 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
22:52:58.872 INFO  ProgressMeter - Starting traversal
22:52:58.873 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
22:53:00.733 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
22:53:08.873 INFO  ProgressMeter -          20:17538652              0.2
58900         353400.0
22:53:17.681 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
22:53:17.681 INFO  ProgressMeter -          20:63024652              0.3
210522         671592.9
22:53:17.681 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
22:53:17.687 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.010347438
22:53:17.687 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.259172573
22:53:17.687 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.27 sec
22:53:17.687 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 10:53:17 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.32 minutes.
Runtime.totalMemory()=5561122816
[root@genomics1 execution]#
```

请注意，输出文件位于执行后指定的位置。

"fb08e15744e912200b45cf04b5fce2ad"

使用 ./gatk 脚本执行 GATK 的输出

"previous： 使用 JAR 文件执行 GATK 的输出。"

使用 ` 。 /gatk` 脚本执行 GATK 后，生成了以下示例输出。

```
[root@genomics1 gatk-4.2.0.0]# ./gatk --java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
Using GATK jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar
Running:
    java -Dsamjdk.use_async_io_read_samtools=false
-Dsamjdk.use_async_io_write_samtools=true
-Dsamjdk.use_async_io_write_tribble=false -Dsamjdk.compression_level=2
-Xmx4G -jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar
HaplotypeCaller -I /mnt/genomics/GATK/TEST DATA/bam/workshop_1906_2-
germline_bams_father.bam -R /mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta -O /mnt/genomics/GATK/TEST
DATA/variants.vcf
23:29:45.553 INFO  NativeLibraryLoader - Loading libgkl_compression.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_compression.so
Aug 17, 2021 11:29:45 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
23:29:45.686 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.686 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
23:29:45.686 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
23:29:45.687 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
23:29:45.687 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v11.0.12+7-LTS
23:29:45.687 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021 at
11:29:45 PM EDT
23:29:45.687 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller -
```

```
------------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
23:29:45.687 INFO  HaplotypeCaller - Picard Version: 2.25.0
23:29:45.687 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
23:29:45.688 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
23:29:45.688 INFO  HaplotypeCaller - Deflater: IntelDeflater
23:29:45.688 INFO  HaplotypeCaller - Inflater: IntelInflater
23:29:45.688 INFO  HaplotypeCaller - GCS max retries/reopens: 20
23:29:45.688 INFO  HaplotypeCaller - Requester pays: disabled
23:29:45.688 INFO  HaplotypeCaller - Initializing engine
23:29:45.804 INFO  HaplotypeCaller - Done initializing engine
23:29:45.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
23:29:45.818 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
23:29:45.819 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
23:29:45.852 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
23:29:45.852 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
running PairHMM
23:29:45.852 INFO  IntelPairHmm - Available threads: 16
23:29:45.852 INFO  IntelPairHmm - Requested threads: 4
23:29:45.852 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
23:29:45.868 INFO  ProgressMeter - Starting traversal
23:29:45.868 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
23:29:47.772 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
23:29:55.868 INFO  ProgressMeter -          20:18885652              0.2
63390         380340.0
23:30:04.389 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
```

```
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
23:30:04.389 INFO  ProgressMeter -          20:63024652              0.3
210522         681999.9
23:30:04.389 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
23:30:04.395 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.012129203000000002
23:30:04.395 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.267345217
23:30:04.395 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.23 sec
23:30:04.395 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 at 11:30:04 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.31 minutes.
Runtime.totalMemory()=2111832064
[root@genomics1 gatk-4.2.0.0]#
```

请注意，输出文件位于执行后指定的位置。

"下一步：使用 Cromwell 引擎执行 GATK 的输出。"

使用 Cromwell 引擎执行 GATK 的输出

"11fffe01d469840980d9b9a5f45bf9ed"

使用 Cromwell 引擎执行 GATK 后，生成了以下示例输出。

```
[root@genomics1 genomics]# java -jar  cromwell-65.jar run
/mnt/genomics/GATK/seq/ghplo.wdl  --inputs
/mnt/genomics/GATK/seq/ghplo.json
[2021-08-18 17:10:50,78] [info] Running with database db.url =
jdbc:hsqldb:mem:856a1f0d-9a0d-42e5-9199-
5e6c1d0f72dd;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:57,74] [info] Running migration
RenameWorkflowOptionsInMetadata with a read batch size of 100000 and a
write batch size of 100000
[2021-08-18 17:10:57,75] [info] [RenameWorkflowOptionsInMetadata] 100%
[2021-08-18 17:10:57,83] [info] Running with database db.url =
jdbc:hsqldb:mem:6afe0252-2dc9-4e57-8674-
ce63c67aa142;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:58,17] [info] Slf4jLogger started
```

```
[2021-08-18 17:10:58,33] [info] Workflow heartbeat configuration:
{
  "cromwellId" : "cromid-41b7e30",
  "heartbeatInterval" : "2 minutes",
  "ttl" : "10 minutes",
  "failureShutdownDuration" : "5 minutes",
  "writeBatchSize" : 10000,
  "writeThreshold" : 10000
}
[2021-08-18 17:10:58,38] [info] Metadata summary refreshing every 1
second.
[2021-08-18 17:10:58,38] [info] No metadata archiver defined in config
[2021-08-18 17:10:58,38] [info] No metadata deleter defined in config
[2021-08-18 17:10:58,40] [info] KvWriteActor configured to flush with
batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,40] [info] WriteMetadataActor configured to flush
with batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,44] [info] CallCacheWriteActor configured to flush
with batch size 100 and process rate 3 seconds.
[2021-08-18 17:10:58,44] [warn] 'docker.hash-lookup.gcr-api-queries-per-
100-seconds' is being deprecated, use 'docker.hash-lookup.gcr.throttle'
instead (see reference.conf)
[2021-08-18 17:10:58,54] [info] JobExecutionTokenDispenser - Distribution
rate: 50 per 1 seconds.
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Version 65
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Submitting
workflow
[2021-08-18 17:10:58,64] [info] Unspecified type (Unspecified version)
workflow 3e246147-b1a9-41dc-8679-319f81b7701e submitted
[2021-08-18 17:10:58,66] [info] SingleWorkflowRunnerActor: Workflow
submitted 3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,66] [info] 1 new workflows fetched by cromid-41b7e30:
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,67] [info] WorkflowManagerActor: Starting workflow
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] WorkflowManagerActor: Successfully started
WorkflowActor-3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] Retrieved 1 workflows from the
WorkflowStoreActor
[2021-08-18 17:10:58,70] [info] WorkflowStoreHeartbeatWriteActor
configured to flush with batch size 10000 and process rate 2 minutes.
[2021-08-18 17:10:58,76] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Parsing workflow as WDL draft-2
[2021-08-18 17:10:59,34] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Call-to-Backend assignments:
helloHaplotypeCaller.haplotypeCaller -> Local
```

```
[2021-08-18 17:11:00,54] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Starting
helloHaplotypeCaller.haplotypeCaller
[2021-08-18 17:11:01,56] [info] Assigned new job execution tokens to the
following groups: 3e246147: 1
[2021-08-18 17:11:01,70] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: java -jar
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/inputs/-179397211/gatk-package-
4.2.0.0-local.jar \
     HaplotypeCaller \
    -R /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604632695/workshop_1906_2-germline_ref_ref.fasta \
    -I /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604617202/workshop_1906_2-germline_bams_father.bam
\
    -O fatherbam.raw.indels.snps.vcf
[2021-08-18 17:11:01,72] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: executing: /bin/bash
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/execution/script
[2021-08-18 17:11:03,49] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: job id: 26867
[2021-08-18 17:11:03,53] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from -
to WaitingForReturnCode
[2021-08-18 17:11:03,54] [info] Not triggering log of token queue status.
Effective log interval = None
[2021-08-18 17:11:23,65] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from
WaitingForReturnCode to Done
[2021-08-18 17:11:25,04] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Workflow helloHaplotypeCaller complete.
Final Outputs:
{
  "helloHaplotypeCaller.haplotypeCaller.rawVCF": "/mnt/genomics/cromwell-
executions/helloHaplotypeCaller/3e246147-b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
}
[2021-08-18 17:11:28,43] [info] WorkflowManagerActor: Workflow actor for
3e246147-b1a9-41dc-8679-319f81b7701e completed with status 'Succeeded'.
The workflow will be removed from the workflow store.
[2021-08-18 17:11:32,24] [info] SingleWorkflowRunnerActor workflow
finished with status 'Succeeded'.
```

```
{
  "outputs": {
    "helloHaplotypeCaller.haplotypeCaller.rawVCF":
"/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-
41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
  },
  "id": "3e246147-b1a9-41dc-8679-319f81b7701e"
}
[2021-08-18 17:11:33,45] [info] Workflow polling stopped
[2021-08-18 17:11:33,46] [info] 0 workflows released by cromid-41b7e30
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowStoreActor - Timeout
= 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowLogCopyRouter -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down JobExecutionTokenDispenser -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Aborting all running workflows.
[2021-08-18 17:11:33,46] [info] JobExecutionTokenDispenser stopped
[2021-08-18 17:11:33,46] [info] WorkflowStoreActor stopped
[2021-08-18 17:11:33,47] [info] WorkflowLogCopyRouter stopped
[2021-08-18 17:11:33,47] [info] Shutting down WorkflowManagerActor -
Timeout = 3600 seconds
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor: All workflows
finished
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor stopped
[2021-08-18 17:11:33,64] [info] Connection pools shut down
[2021-08-18 17:11:33,64] [info] Shutting down SubWorkflowStoreActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down JobStoreActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down CallCacheWriteActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] SubWorkflowStoreActor stopped
[2021-08-18 17:11:33,64] [info] Shutting down ServiceRegistryActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down DockerHashActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down IoProxy - Timeout = 1800
seconds
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor Shutting down: 0
queued messages to process
[2021-08-18 17:11:33,64] [info] JobStoreActor stopped
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor stopped
[2021-08-18 17:11:33,64] [info] KvWriteActor Shutting down: 0 queued
messages to process
```

```
[2021-08-18 17:11:33,64] [info] IoProxy stopped
[2021-08-18 17:11:33,64] [info] WriteMetadataActor Shutting down: 0 queued
messages to process
[2021-08-18 17:11:33,65] [info] ServiceRegistryActor stopped
[2021-08-18 17:11:33,65] [info] DockerHashActor stopped
[2021-08-18 17:11:33,67] [info] Database closed
[2021-08-18 17:11:33,67] [info] Stream materializer shut down
[2021-08-18 17:11:33,67] [info] WDL HTTP import resolver closed
[root@genomics1 genomics]#
```

"下一步： GPU 设置。"

GPU 设置

"previous ： 使用 Cromwell 引擎执行 GATK 的输出。"

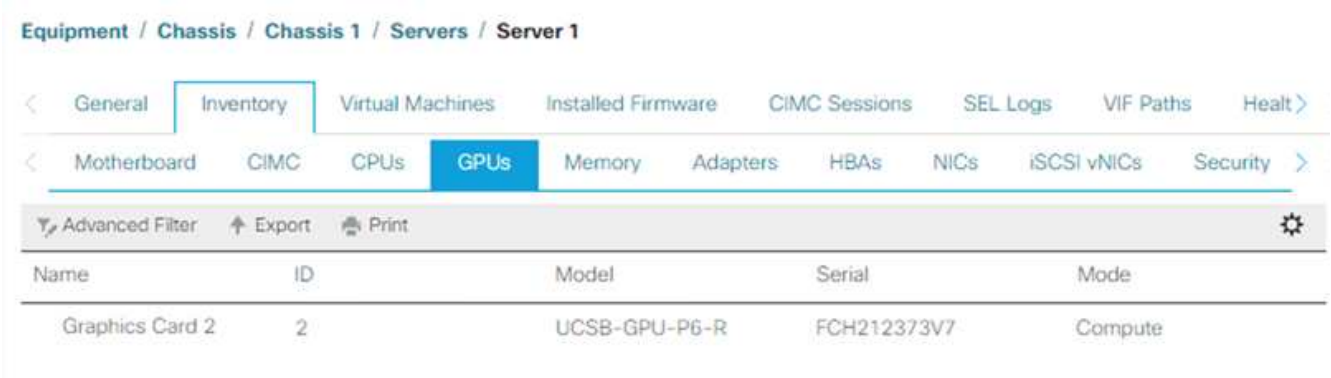
截至发布时， GATK 工具不支持在内部执行基于 GPU 的原生。我们提供了以下设置和指导，帮助读者了解使用 GATK PCIe 夹层卡在后部安装的 NVIDIA Tesla P6 GPU 上使用 FlexPod 的简单程度。

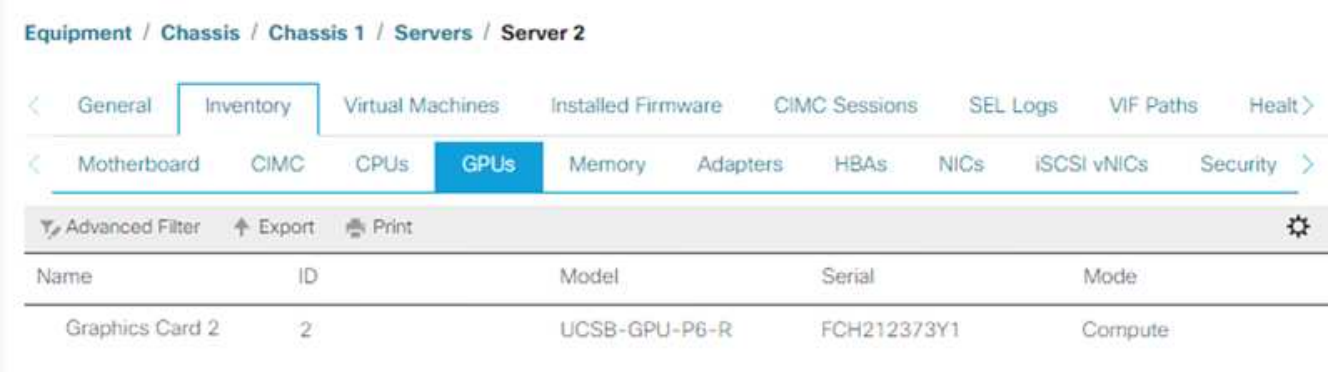
我们使用以下 Cisco 验证设计（ Cisco Validated Design ， CVD ）作为参考架构和最佳实践指南来设置 FlexPod 环境，以便可以运行使用 GPU 的应用程序。

- "适用于 AI/ML 的 FlexPod 数据中心与适用于深度学习的 Cisco UCS 480 ML"

下面是此设置期间的一组要点：

1. 我们在 UCS B200 M5 服务器的夹层插槽中使用了 PCIe NVIDIA Tesla P6 GPU 。





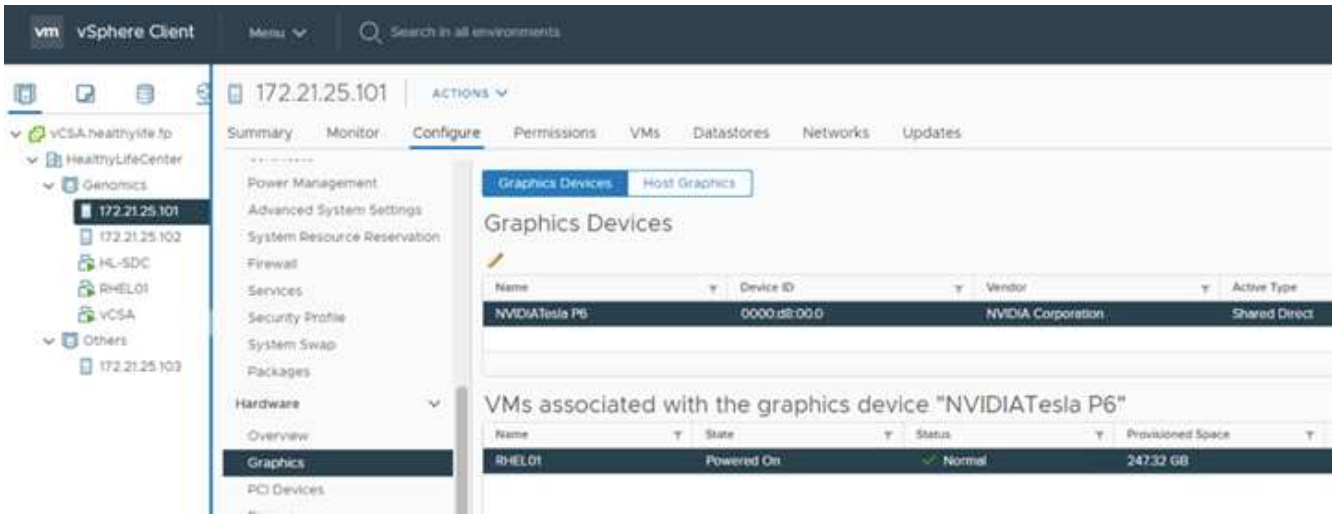
2. 对于此设置，我们已在 NVIDIA 合作伙伴门户上注册，并获得了一个评估许可证（也称为授权），以便能够在计算模式下使用 GPU 。
3. 我们从 NVIDIA 合作伙伴网站下载了所需的 NVIDIA vGPU 软件。
4. 我们从 NVIDIA 合作伙伴网站下载了授权 ` * 。 bin` 文件。
5. 我们安装了一个 NVIDIA vGPU 许可证服务器，并使用从 NVIDIA 合作伙伴站点下载的 ` * 。 bin` 文件将授权添加到许可证服务器。
6. 确保在 NVIDIA 合作伙伴门户上为您的部署选择正确的 NVIDIA vGPU 软件版本。在此设置中，我们使用的驱动程序版本为 460.73.02 。
7. 此命令将安装 "NVIDIA vGPU Manager" 在 ESXi 中。

```
[root@localhost:~] esxcli software vib install -v
/vmfs/volumes/infra_datastore_nfs/nvidia/vib/NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992.vib
Installation Result
Message: Operation finished successfully.
Reboot Required: false
VIBs Installed: NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992
VIBs Removed:
VIBs Skipped:
```

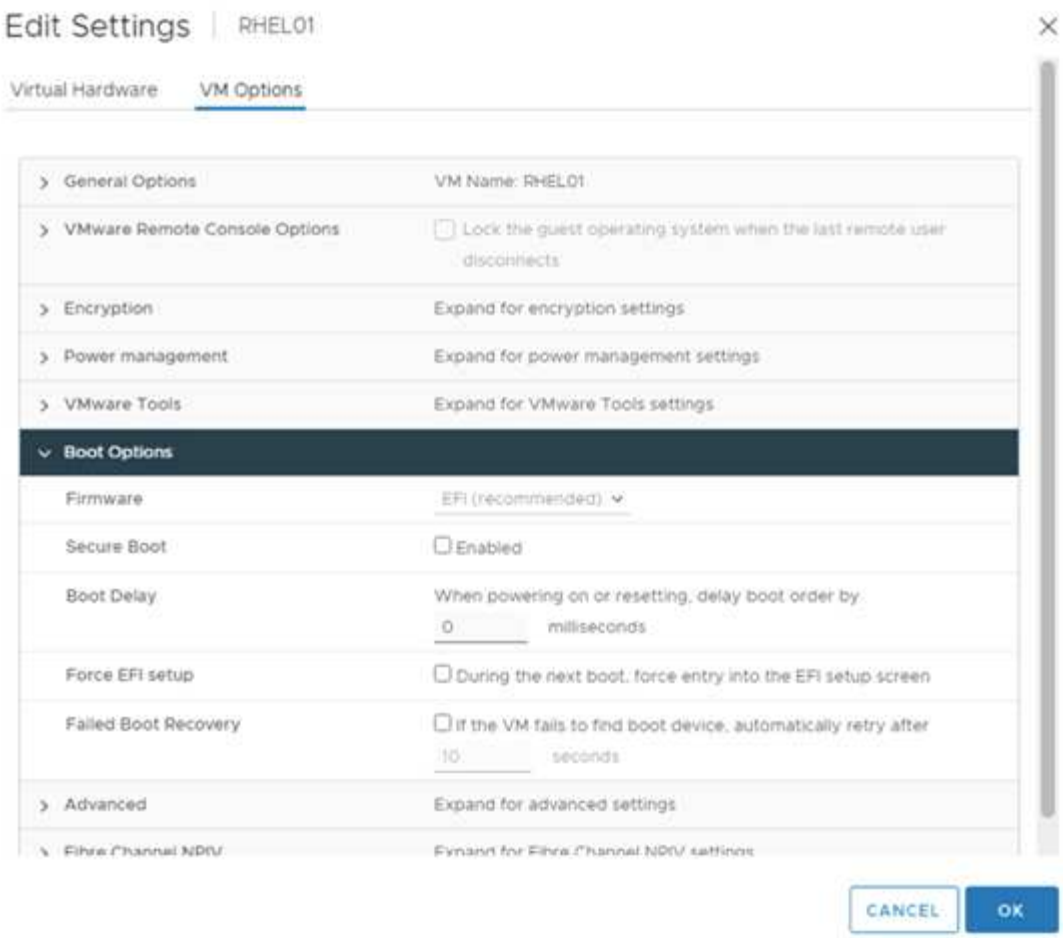
8. 重新启动 ESXi 服务器后，运行以下命令以验证 GPU 的安装并检查其运行状况。

```
[root@localhost:~] nvidia-smi
Wed Aug 18 21:37:19 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.02    Driver Version: 460.73.02    CUDA Version: N/A
|
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+================
======|
|   0  Tesla P6            On   | 00000000:D8:00.0 Off |
0 |
| N/A   35C    P8     9W /  90W |  15208MiB / 15359MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A   2812553    C+G   RHEL01
15168MiB |
+-----------------------------------------------------------------------------
------+
[root@localhost:~]
```

9. 使用 vCenter， "配置" 图形设备设置为 "shared direction" 。



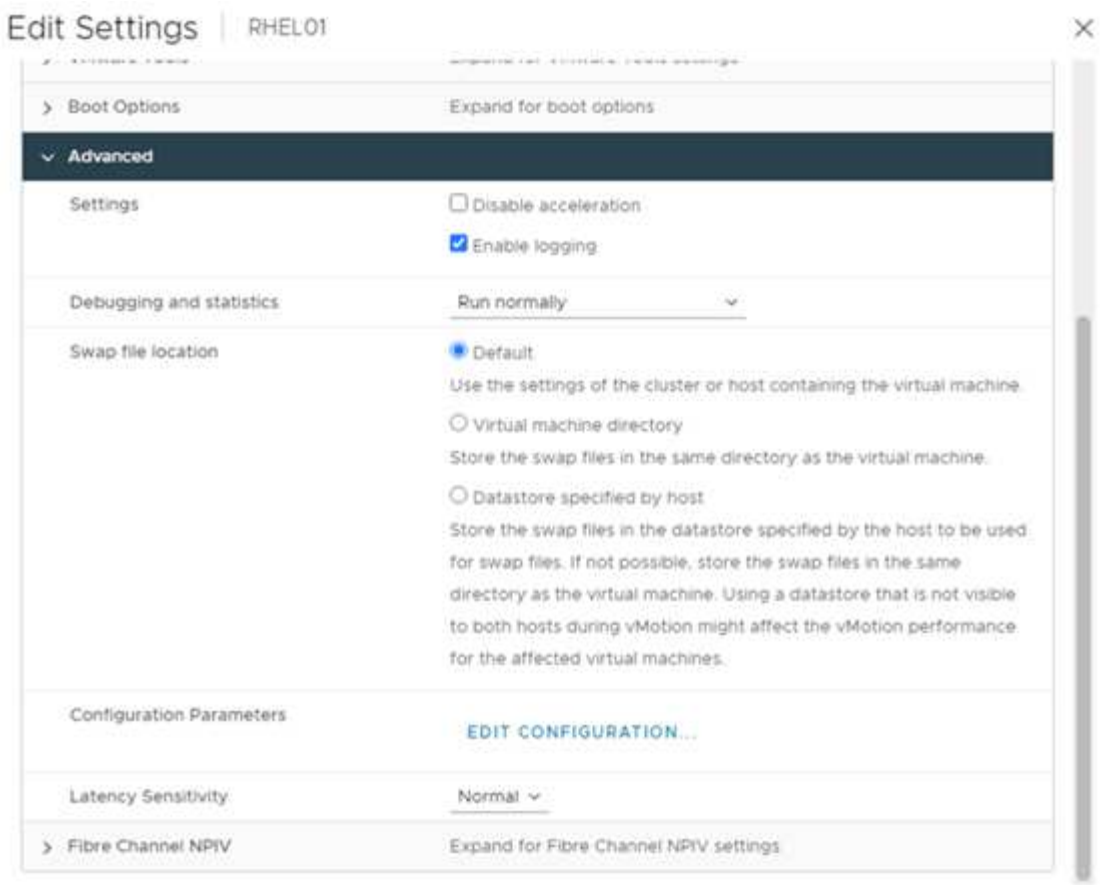
10. 确保已为 RedHat VM 禁用安全启动。
11. 确保 VM 启动选项固件设置为 EFI （"ref"）。

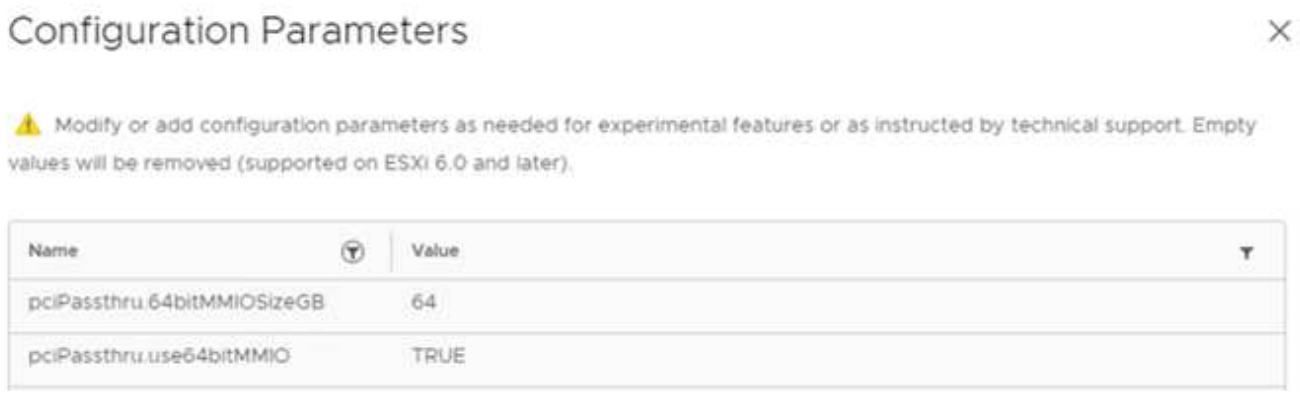


12. 确保已将以下参数添加到 VM 选项高级编辑配置中。`pciPassthru .64bitMMIOSizeGB` 参数的值取决于 GPU 内存和分配给虚拟机的 GPU 数量。例如：

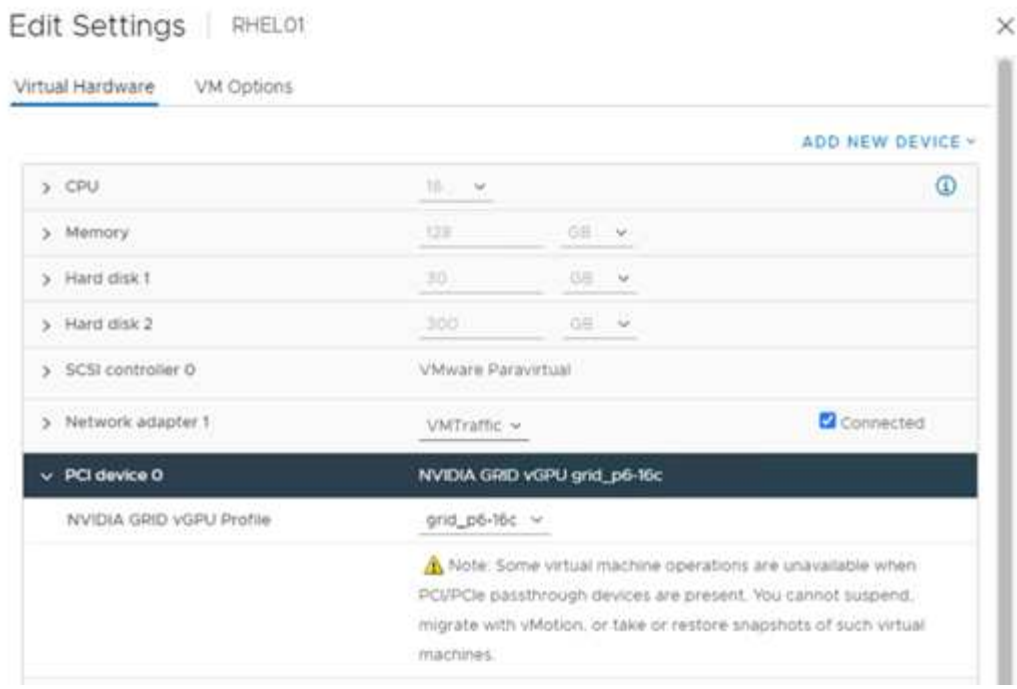
    a. 如果为虚拟机分配了 4 个 32 GB V100 GPU ，则此值应为 128 。

    b. 如果为虚拟机分配了 4 个 16 GB P6 GPU ，则此值应为 64 。





13. 在 vCenter 中将 vGPU 作为新的 PCI 设备添加到虚拟机时，请确保选择 NVIDIA GRID vGPU 作为 PCI 设备类型。
14. 选择适合所用 GPU ， GPU 内存和使用目的的正确 GPU 配置文件：例如，图形与计算。



15. 在 RedHat Linux VM 上，可以运行以下命令来安装 NVIDIA 驱动程序：

```
[root@genomics1 genomics]#sh NVIDIA-Linux-x86_64-460.73.01-grid.run
```

16. 运行以下命令，验证是否报告了正确的 vGPU 配置文件：

```
[root@genomics1 genomics]# nvidia-smi -query-gpu=gpu_name
-format=csv,noheader -id=0 | sed -e 's/ /-/g'
GRID-P6-16C
[root@genomics1 genomics]#
```

17. 重新启动后，验证是否报告了正确的 NVIDIA vGPU 以及驱动程序版本。

```
[root@genomics1 genomics]# nvidia-smi
Wed Aug 18 20:30:56 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.01    Driver Version: 460.73.01    CUDA Version:
11.2     |
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+================
======|
|   0  GRID P6-16C         On   | 00000000:02:02.0 Off |
N/A |
| N/A   N/A    P8    N/A /  N/A |   2205MiB / 16384MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A      8604      G   /usr/libexec/Xorg
13MiB |
+-----------------------------------------------------------------------------
------+
[root@genomics1 genomics]#
```

18. 确保已在 vGPU 网格配置文件中的 VM 上配置许可证服务器 IP 。
    a. 复制模板。

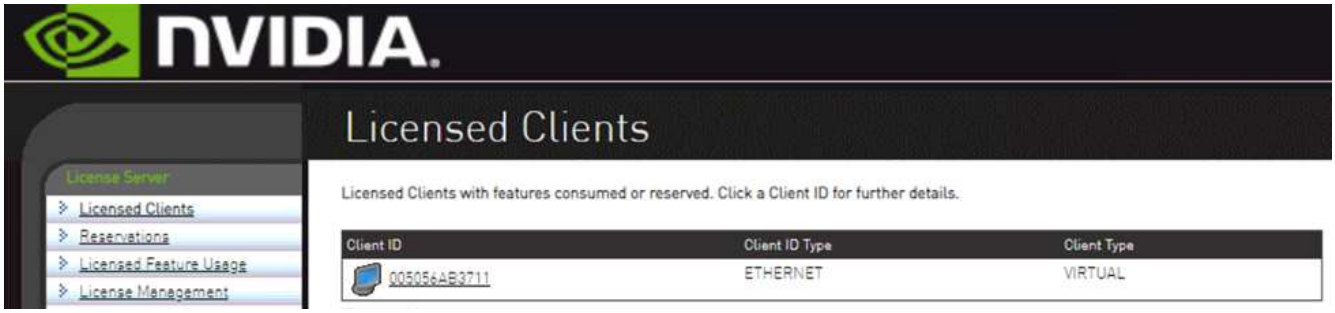
```
[root@genomics1 genomics]# cp /etc/nvidia/gridd.conf.template
/etc/nvidia/gridd.conf
```

b. 编辑文件 ` /etc/nvidia/rid` ，添加许可证服务器 IP 地址，并将功能类型设置为 1 。

```
ServerAddress=192.168.169.10
```

```
FeatureType=1
```

19. 重新启动虚拟机后，您应在许可证服务器中的 " 已许可客户端 " 下看到一个条目，如下所示。



20. 有关下载 GATK 和 Cromwell 软件的详细信息，请参见 " 解决方案设置 " 一节。
21. 在 GATK 可以在内部使用 GPU 之后，工作流问题描述语言为 ` * 。WDL` 具有运行时属性，如下所示。

```
task ValidateBAM {
  input {
    # Command parameters
    File input_bam
    String output_basename
    String? validation_mode
    String gatk_path
    # Runtime parameters
    String docker
    Int machine_mem_gb = 4
    Int addtional_disk_space_gb = 50
  }
  Int disk_size = ceil(size(input_bam, "GB")) + addtional_disk_space_gb
  String output_name = "${output_basename}_${validation_mode}.txt"
  command {
    ${gatk_path} \
      ValidateSamFile \
      --INPUT ${input_bam} \
      --OUTPUT ${output_name} \
      --MODE ${default="SUMMARY" validation_mode}
  }
  runtime {
    gpuCount: 1
    gpuType: "nvidia-tesla-p6"
    docker: docker
    memory: machine_mem_gb + " GB"
    disks: "local-disk " + disk_size + " HDD"
  }
  output {
    File validation_report = "${output_name}"
  }
}
```

"接下来：总结。"

结论

"上一步： GPU 设置。"

全球许多医疗保健组织都将 FlexPod 作为一个通用平台进行了标准化。借助 FlexPod ，您可以放心地部署医疗保健功能。采用 NetApp ONTAP 的 FlexPod 标配，能够即装即用地实施一组行业领先的协议。无论对给定患者运行基因组学的请求来自何处， FlexPod 平台都标配了互操作性，可访问性，可用性和可扩展性。在 FlexPod 平台上实现标准化后，创新文化将具有传染性。

从何处查找追加信息

要了解有关本文档所述信息的更多信息，请查看以下文档和网站：

- 适用于 AI/ML 的 FlexPod 数据中心与适用于深度学习的 Cisco UCS 480 ML

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_480ml_aiml_deployment.pdf"

- 采用 VMware vSphere 7.0 和 NetApp ONTAP 9.7 的 FlexPod Datacenter

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/fp_vmware_vsphere_7_0_ontap_9_7.html"

- ONTAP 9 文档中心

  "http://docs.netapp.com"

- 敏捷高效— FlexPod 如何推动数据中心现代化

  "https://www.flexpod.com/idc-white-paper/"

- 医疗保健领域的人工智能

  "https://www.netapp.com/us/media/na-369.pdf"

- FlexPod for HealthCare 可帮助您轻松实现转型

  "https://flexpod.com/solutions/verticals/healthcare/"

- Cisco 和 NetApp 的 FlexPod

  "https://flexpod.com/"

- 适用于医疗保健的 AI 和分析（ NetApp ）

  "https://www.netapp.com/us/artificial-intelligence/healthcare-ai-analytics/index.aspx"

- 医疗保健智能基础架构选择中的人工智能有助于取得更大成功

  https://www.netapp.com/pdf.html?item=/media/7410-wp-7314.pdf

- 采用 ONTAP 9.8 的 FlexPod 数据中心，适用于 Cisco Intersight 的 ONTAP 存储连接器和 Cisco Intersight 托管模式。

  https://www.netapp.com/pdf.html?item=/media/25001-tr-4883.pdf

- 采用 Red Hat Enterprise Linux OpenStack Platform 的 FlexPod Datacenter

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_openstack_osp6.html"

版本历史记录

version	Date	文档版本历史记录
版本 1.0	2021年11月	初始版本。

《适用于 MEDITECH 的 FlexPod 方向性规模估算指南》

TR-4774： 适用于 MEDITECH 定向规模估算的 FlexPod

Branon Agee， John Duignan， NetApp Mike Brennan， Jon Ebmeir， Cisco

与以下合作伙伴：

本报告为 MEDITECH EHR 应用程序软件环境的 FlexPod 规模估算提供了指导。

目的

可以部署 FlexPod 系统来托管 MEDITECH expanse， 6.x， 5.x 和 Magic 服务。托管 MEDITECH 应用程序层的 FlexPod 服务器为可靠的高性能基础架构提供了一个集成平台。FlexPod 集成平台由经验丰富的 FlexPod 渠道合作伙伴快速部署，并由 Cisco 和 NetApp 技术支持中心提供支持。

规模估算基于 MEDITECH 的硬件配置提案和 MEDITECH 任务文档中的信息。目标是确定计算，网络和存储基础架构组件的最佳大小。

。 "Meditech 工作负载概述" 第节介绍了可在 MEDITECH 环境中找到的计算和存储工作负载类型。

。 "小型，中型和大型架构的技术规格" 第节详细介绍了本节所述不同存储架构的示例材料清单。提供的配置仅供一般参考。请始终根据工作负载使用规模估算器调整系统的大小，并相应地调整配置。

解决方案的整体优势

在 FlexPod 架构基础上运行 MEDITECH 环境可以帮助医疗保健组织提高工作效率并降低资本和运营支出。FlexPod 提供了一个经过严格测试的预先验证的融合基础架构，该基础架构由 Cisco 和 NetApp 的战略合作伙伴关系提供。它经过专门设计和设计，可提供可预测的低延迟系统性能和高可用性。这种方法可以加快 MEDITECH EHR 系统用户的响应速度。

Cisco 和 NetApp 的 FlexPod 解决方案通过高性能，模块化，预先验证，融合，虚拟化， 高效，可扩展且经济高效的平台。采用 MEDITECH 的 FlexPod 数据中心可为医疗保健行业带来以下优势：

- * 模块化架构 * 。FlexPod 可通过针对每个特定工作负载的自定义 FlexPod 系统来满足 MEDITECH 模块化架构的各种需求。所有组件均通过集群模式服务器和存储管理网络结构进行连接，并使用一个统一的管理工具集。
- * 简化操作并降低成本 * 。您可以通过使用更高效，可扩展的共享资源来取代原有平台，从而消除原有平台的成本和复杂性，无论临床医生身在何处，均可为其提供支持。此解决方案可提高资源利用率，从而提高投资回报率（ ROI ）。
- * 加快基础架构部署 * 。FlexPod 数据中心与 MEDITECH 的集成设计使客户可以快速轻松地为现场和远程数据中心启动和运行新的基础架构。

- * 横向扩展架构 * 。您可以将 SAN 和 NAS 从 TB 扩展到数十 PB ，而无需重新配置正在运行的应用程序。
- * 无中断运行 * 。您可以在不中断业务的情况下执行存储维护，硬件生命周期操作和软件升级。
- * 安全多租户 * 。此优势可满足日益增长的虚拟化服务器和共享存储基础架构需求，从而可以安全地多租户处理特定于设施的信息。如果您要托管多个数据库和软件实例，则此优势非常重要。
- * 池化资源优化 * 。这一优势有助于减少物理服务器和存储控制器数量，平衡工作负载需求，提高利用率并同时提高性能。
- * 服务质量（ QoS ）。 * FlexPod 可在整个堆栈上提供服务质量（ QoS ）。行业领先的 QoS 存储策略可在共享环境中提供不同的服务级别。这些策略可以为工作负载提供最佳性能，并有助于隔离和控制失控的应用程序。
- * 存储效率 * 。您可以利用 NetApp 7： 1 存储效率降低存储成本。
- * 灵活性 * 。FlexPod 系统提供行业领先的工作流自动化，编排和管理工具，可以使 IT 更快速地响应业务请求。这些业务请求包括从 MEDITECH 备份和配置更多测试和培训环境到为人口健康管理计划复制分析数据库等。
- * 工作效率 * 。您可以快速部署和扩展此解决方案，以获得最佳临床医生最终用户体验。
- * 数据网络结构 * 。NetApp Data Fabric 架构可以跨站点，跨物理边界和跨应用程序将数据集于一体。NetApp Data Fabric 专为以数据为中心的世界中的数据驱动型企业而构建。数据在多个位置创建和使用，通常与应用程序和基础架构共享。Data Fabric 提供了一种一致且集成的数据管理方式。它还可以让 IT 更好地控制数据，并简化日益增加的 IT 复杂性。

范围

本文档介绍了使用 Cisco UCS 和基于 NetApp ONTAP 的存储的环境。它提供了用于托管 MEDITECH 的示例参考架构。

它不包括：

- 使用 NetApp System Performance Modeler （ SPM ）或其他 NetApp 规模估算工具提供详细的规模估算指南。
- 针对非生产工作负载进行规模估算。

audience

本文档面向 NetApp 和合作伙伴系统工程师以及 NetApp 专业服务人员。NetApp 假定读者已很好地了解计算和存储规模估算概念，并在技术上熟悉 Cisco UCS 和 NetApp 存储系统。

相关文档

以下技术报告和其他文档与本技术报告相关，并构成在 FlexPod 基础架构上对 MEDITECH 进行规模估算，设计和部署所需的一整套文档。

- "TR-4753：《适用于 MEDITECH 的 FlexPod 数据中心部署指南》"
- "TR-4190：《适用于 MEDITECH 环境的 NetApp 规模估算准则》"
- "TR-4319：《适用于 MEDITECH 环境的 NetApp 部署准则》"

要访问其中某些报告，需要 NetApp Field Portal 的登录凭据。

Meditech 工作负载概述

本节介绍在 MEDITECH 环境中可能会发现的计算和存储工作负载类型。

Meditech 和备份工作负载

在为 MEDITECH 环境估算 NetApp 存储系统的规模时，您必须同时考虑 MEDITECH 生产工作负载和备份工作负载。

MEDITECH 主机
MEDITECH 主机是数据库服务器。此主机也称为 MEDITECH 文件服务器（对于 expanse ， 6.x 或 C/S 5.x 平台）或魔力机器（对于魔力平台）。本文档使用术语 MEDITECH 主机来指代 MEDITECH 文件服务器和魔力机器。

以下各节将介绍这两个工作负载的 I/O 特征和性能要求。

Meditech 工作负载

在 MEDITECH 环境中，运行 MEDITECH 软件的多个服务器作为一个称为 MEDITECH 系统的集成系统执行各种任务。有关 MEDITECH 系统的详细信息，请参见 MEDITECH 文档：

- 对于生产型 MEDITECH 环境，请参阅相应的 MEDITECH 文档，以确定在调整 NetApp 存储系统规模时必须包含的 MEDITECH 主机数量和存储容量。
- 对于新的 MEDITECH 环境，请参见硬件配置提案文档。对于现有的 MEDITECH 环境，请参阅硬件评估任务文档。硬件评估任务与 MEDITECH 服务单关联。客户可以向 MEDITECH 申请上述任一文档。

您可以通过添加主机来扩展 MEDITECH 系统，以提高容量和性能。每个主机都需要存储容量来存储其数据库和应用程序文件。每个 MEDITECH 主机可用的存储还必须支持该主机生成的 I/O 。在 MEDITECH 环境中，每个主机都有一个 LUN ，以满足该主机的数据库和应用程序存储要求。您部署的 MEDITECH 类别类型和平台类型决定了每个 MEDITECH 主机的工作负载特征，因此也决定了整个系统的工作负载特征。

MEDITECH 类别

Meditech 会将部署规模与 1 到 6 之间的类别编号关联起来。类别 1 表示最小的 MEDITECH 部署；类别 6 表示最大的部署。与每个类别关联的 MEDITECH 应用程序规范示例包括以下指标：

- 医院床位数
- 每年住院患者数
- 每年门诊患者
- 每年的紧急房间访问量
- 每年的考试
- 每天为患者开处方
- 每天提供门诊处方

有关 MEDITECH 类别的详细信息，请参见 MEDITECH 类别参考表。您可以通过客户或通过 MEDITECH 系统安装程序从 MEDITECH 获取此表。

Meditech 平台

Meditech 有四个平台：

- 贵
- Meditech 6.x
- 客户端 / 服务器 5.x （ C/S 5.x ）
- 魔力

对于 MEDITECH expanse ， 6.x 和 C/S 5.x 平台，每个主机的 I/O 特征均定义为 100% 随机，请求大小为 4 ，000 。对于 MEDITECH 魔力平台，每台主机的 I/O 特征均定义为 100% 随机，请求大小为 8 ， 000 或 16 ，000 。据 MEDITECH 报告，典型的魔力生产部署的请求大小为 8 ， 000 或 16 ， 000 。

读取和写入比率因部署的平台而异。Meditech 会估算读写的平均混合比例，然后将其表示为百分比。Meditech 还会估算特定 MEDITECH 平台上的每个 MEDITECH 主机所需的平均持续 IOPS 值。下表总结了 MEDITECH 提供的平台专用 I/O 特征。

MEDITECH 类别	**Meditech** 平台	平均随机读取 **%**	平均随机写入 **%**	每个 **MEDITECH** 主机的平均持续 **IOPS**
1.	expanse ， 6.x	20	80	750
2-6	贵	20	80	750
	6.x	20	80	750
	C/S 5.x	40	60	600
	魔力	90	10	400

在 MEDITECH 系统中，每个主机的平均 IOPS 级别必须等于上表中定义的 IOPS 值。要根据每个平台确定正确的存储规模估算，请在中所述的规模估算方法中使用上表中指定的 IOPS 值 "小型，中型和大型架构的技术规格" 部分。

Meditech 要求每台主机的平均随机写入延迟保持在 1 毫秒以下。但是，在备份和重新分配作业期间，写入延迟临时增加到 2 毫秒是可以接受的。Meditech 还要求 1 类主机的平均随机读取延迟低于 7 毫秒， 2 类主机的平均随机读取延迟低于 5 毫秒。无论使用哪种 MEDITECH 平台，这些延迟要求都适用于每个主机。

下表总结了在为 MEDITECH 工作负载估算 NetApp 存储规模时必须考虑的 I/O 特征。

参数	**MEDITECH** 类别	贵	**Meditech 6.x**	**C/S 5.x**	魔力
请求大小	1 至 6	4k	4k	4k	8 K 或 16 K
随机 / 顺序		100% 随机	100% 随机	100% 随机	100% 随机
平均持续 IOPS	1.	750	750	不适用	不适用
	2-6	750	750	600	400
读 / 写比率	1 至 6	20% 读取， 80% 写入	20% 读取， 80% 写入	读取率为 40% ，写入率为 60%	读取率为 90% ，写入率为 10%
写入延迟		小于 1 毫秒	小于 1 毫秒	小于 1 毫秒	小于 1 毫秒

参数	MEDITECH 类别	贵	Meditech 6.x	C/S 5.x	魔力
临时峰值写入延迟	1 至 6	小于 2 毫秒	小于 2 毫秒	小于 2 毫秒	小于 2 毫秒
读取延迟	1.	< 7 毫秒	< 7 毫秒	不适用	不适用
	2-6	小于 5 毫秒	小于 5 毫秒	小于 5 毫秒	小于 5 毫秒

3 到 6 类的 Meditech 主机与 2 类具有相同的 I/O 特征。对于 MEDITECH 类别 2 到 6 ，在每个类别中部署的主机数量会有所不同。

NetApp 存储系统的大小应满足前面几节所述的性能要求。除了 MEDITECH 生产工作负载之外， NetApp 存储系统还必须能够在备份操作期间保持这些 MEDITECH 性能目标，如下一节所述。

备份工作负载问题描述

经过 Meditech 认证的备份软件可备份由 MEDITECH 系统中的每个 MEDITECH 主机使用的 LUN 。要使备份处于应用程序一致的状态，备份软件将暂停 MEDITECH 系统并暂停对磁盘的 I/O 请求。在系统处于静默状态时，备份软件会向 NetApp 存储系统发出一条命令，为包含 LUN 的卷创建 NetApp Snapshot 副本。备份软件稍后会使 MEDITECH 系统退出静默状态，从而可以继续向数据库发出生产 I/O 请求。该软件将基于 Snapshot 副本创建 NetApp FlexClone 卷。此卷由备份源使用，而生产 I/O 请求则继续在托管 LUN 的父卷上发出。

备份软件生成的工作负载来自对 FlexClone 卷中 LUN 的顺序读取。此工作负载是指请求大小为 64 ， 000 的 100% 顺序读取工作负载。对于 MEDITECH 生产工作负载，性能标准是保持所需的 IOPS 以及相关的读 / 写延迟级别。但是，对于备份工作负载，需要注意备份操作期间生成的整体数据吞吐量（ MBps ）。Meditech LUN 备份需要在八小时的备份时间内完成，但 NetApp 建议在六小时或更短的时间内完成所有 MEDITECH LUN 的备份。如果要在不到六小时的时间内完成备份，则可以减少 MEDITECH 工作负载计划外增加， NetApp ONTAP 后台操作或数据随时间增长等事件的影响。任何此类事件都可能会导致备份时间过长。无论存储的应用程序数据量如何，备份软件都会为每个 MEDITECH 主机对整个 LUN 执行完整的块级备份。

根据其他相关因素，计算完成此窗口中的备份所需的顺序读取吞吐量：

- 所需的备份持续时间
- LUN 的数量
- 要备份的每个 LUN 的大小

例如，在一个 50 主机的 MEDITECH 环境中，每个主机的 LUN 大小为 200 GB ，在此环境中，要备份的 LUN 总容量为 10 TB 。

要在八小时内备份 10 TB 的数据，需要以下吞吐量：

- = （ 10 x 10^6 ） MB （ 8 x 3 ， 600 ） s
- = 347.2 MBps

但是，为了考虑计划外事件，我们会选择一个 5.5 小时的保守备份窗口，以提供超过建议的 6 小时的余量。

要在八小时内备份 10 TB 的数据，需要以下吞吐量：

- = （ 10 x 10^6 ） MB （ 5.5 x 3 ， 600 ） s
- = 500 Mbps

以 500 Mbps 的吞吐量速率，备份可以在 5.5 小时的时间范围内完成，并且可以在 8 小时的备份要求范围内轻松完成。

下表总结了在估算存储系统规模时要使用的备份工作负载的 I/O 特征。

参数	所有平台
请求大小	64K
随机 / 顺序	100% 顺序
读 / 写比率	100% 读取
平均吞吐量	取决于 MEDITECH 主机的数量和每个 LUN 的大小：备份必须在 8 小时内完成。
所需的备份持续时间	8 小时

适用于 **MEDITECH** 的 **Cisco UCS** 参考架构

基于 FlexPod 的 MEDITECH 的架构基于 MEDITECH ， Cisco 和 NetApp 的指导以及合作伙伴在与各种规模的 MEDITECH 客户合作方面的经验。该架构具有适应性，并会根据客户的数据中心战略应用 MEDITECH 的最佳实践：无论是小型还是大型，集中式，分布式还是多租户。

在部署 MEDITECH 时， Cisco 设计的 Cisco UCS 参考架构直接符合 MEDITECH 的最佳实践。Cisco UCS 提供紧密集成的解决方案，可提供高性能，高可用性，可靠性和可扩展性，支持医生诊疗以及配备数千张床位的医院系统。

小型，中型和大型架构的技术规格

本节将讨论不同大小的存储架构的示例材料清单。

小型，中型和大型架构的材料清单。

FlexPod 设计是一种灵活的基础架构，包含许多不同的组件和软件版本。使用 … "TR-4036： FlexPod 技术规格" 作为汇编有效 FlexPod 配置的指南。下表中的配置是 FlexPod 的最低要求，只是一个示例。可以根据不同环境和使用情形的需要扩展每个产品系列的配置。

对于此规模估算练习， " 小型 " 对应于 3 类 MEDITECH 环境， " 中型 " 对应于 5 类， " 大型 " 对应于 6 类。

	小型	中等	大型
平台	一个 NetApp AFF A220 全闪存存储系统 HA 对	一个 NetApp AFF A220 HA 对	一个 NetApp AFF A300 全闪存存储系统 HA 对
磁盘架	9 TB x 3.8 TB	13 TB x 3.8 TB	19 TB x 3.8 TB
Meditech 数据库大小	3TB-12 TB	17 TB	大于 30 TB
Meditech IOPS	少于 22 ， 000 IOPS	超过 25 ， 000 IOPS	超过 32 ， 000 个 IOPS
总 IOPS	2000 年	27000	35000
原始	34.2 TB	49.4TB	68.4TB
可用容量	18.53 TiB	27.96 TiB	33.82 TiB

	小型	中等	大型
有效容量（2： 1 存储效率）	55.6 TiB	83.89 TiB	101.47 TiB

> 某些客户环境可能会同时运行多个 MEDITECH 生产工作负载，或者 IOPS 要求可能更高。在这种情况下，请与 NetApp 客户团队合作，根据所需的 IOPS 和容量对存储系统进行规模估算。您应该能够确定适合工作负载的平台。例如，有些客户成功地在一个 NetApp AFF A700 全闪存存储系统 HA 对上运行了多个 MEDITECH 环境。

下表显示了 MEDITECH 配置所需的标准软件。

软件	产品系列	版本或版本	详细信息
存储	ONTAP	ONTAP 9.4 常规可用性（GA）	
网络	Cisco UCS 互联阵列	Cisco UCSM 4.x	当前建议版本
	Cisco Nexus 以太网交换机	7.0 （3） i7 （6）	当前建议版本
	Cisco FC： Cisco MDS 9132T	8.3 （2）	当前建议版本
虚拟机管理程序	虚拟机管理程序	VMware vSphere ESXi 6.7	
	虚拟机（VM）	Windows 2016	
管理	虚拟机管理程序管理系统	VMware vCenter Server 6.7 U1 （VCSA）	
	NetApp 虚拟存储控制台（VSC）	VSC 7.0P1	
	NetApp SnapCenter	SnapCenter 4.0	
	Cisco UCS Manager	4.x	

下表显示了一个小型（第 3 类）配置示例—基础架构组件。

层	产品系列	数量和型号	详细信息
计算	Cisco UCS 5108 机箱	1.	最多支持八个半宽刀片式服务器或四个全宽刀片式服务器。随着服务器需求的增长，请添加机箱。
	Cisco 机箱 I/O 模块	2 x 2208	8 GB x 10 GB 上行链路端口
	Cisco UCS 刀片式服务器	4 个 B200 M5	每个系统具有 2 个 14 核，2.6 GHz 或更高时钟速度以及 384 GB BIOS 3.2 （3#）
	Cisco UCS 虚拟接口卡	4 个 UCS 1440	VMware ESXi fNIC FC 驱动程序： 1.6.0.47 VMware ESXi eNIC 以太网驱动程序： 1.0.27.0 （请参见互操作性表：
	2 个 Cisco UCS 互联阵列（FI）	2 个 UCS 6454 FI	第四代互联阵列，支持 10/25/100GB 以太网和 32 Gb FC
网络	Cisco 以太网交换机	2 个 Nexus 9336c-x2	1 GB ， 10 GB ， 25 GB ， 40 GB ， 100 GB
存储网络	用于 BLOB 存储的 IP 网络 Nexus 9k		FI 和 UCS 机箱
	FC： Cisco MDS 9132T		两台 Cisco 9132T 交换机
存储	NetApp AFF A300 全闪存存储系统	1 个 HA 对	适用于所有 MEDITECH 工作负载的双节点集群（文件服务器，映像服务器，SQL Server ， VMware 等）
	DS224C 磁盘架	1 个 DS224C 磁盘架	
	固态驱动器（SSD）	9 个 3.8 TB	

下表显示了中型（5 类）配置示例—基础架构组件

层	产品系列	数量和型号	详细信息
计算	Cisco UCS 5108 机箱	1.	最多支持八个半宽刀片式服务器或四个全宽刀片式服务器。随着服务器需求的增长，请添加机箱。
	Cisco 机箱 I/O 模块	2 x 2208	8 GB x 10 GB 上行链路端口
	Cisco UCS 刀片式服务器	6 个 B200 M5	每个系统具有 2 个 16 核，2.5 GHz/ 或更高时钟速度以及 384 GB 或更多内存 BIOS 3.2 （ 3# ）
	Cisco UCS 虚拟接口卡（ VIC ）	6 个 UCS 1440 VIC	VMware ESXi fNIC FC 驱动程序： 1.6.0.47 VMware ESXi eNIC 以太网驱动程序： 1.0.27.0 （请参见互操作性表：）
	2 个 Cisco UCS 互联阵列（ FI ）	2 个 UCS 6454 FI	第四代互联阵列，支持 10 GB/25 GB/100 GB 以太网和 32 Gb FC
网络	Cisco 以太网交换机	2 个 Nexus 9336c-x2	1 GB ， 10 GB ， 25 GB ， 40 GB ， 100 GB
存储网络	用于 BLOB 存储的 IP 网络 Nexus 9k		
	FC ： Cisco MDS 9132T		两台 Cisco 9132T 交换机
存储	NetApp AFF A220 全闪存存储系统	2 个 HA 对	适用于所有 MEDITECH 工作负载的双节点集群（文件服务器，映像服务器，SQL Server ， VMware 等）
	DS224C 磁盘架	1 个 DS224C 磁盘架	
	SSD	13 个 3.8 TB	

下表显示了一个大型（第 6 类）配置示例—基础架构组件。

层	产品系列	数量和型号	详细信息
计算	Cisco UCS 5108 机箱	1.	
	Cisco 机箱 I/O 模块	2 x 2208	8 个 10 GB 上行链路端口
	Cisco UCS 刀片式服务器	8 个 B200 M5	每个模块具有 2 个 24 核，2.7 GHz 和 768 GB BIOS 3.2 （3#）
	Cisco UCS 虚拟接口卡（VIC）	8 个 UCS 1440 VIC	VMware ESXi fNIC FC 驱动程序： 1.6.0.47 VMware ESXi eNIC 以太网驱动程序： 1.0.27.0 （请查看互操作性表：
	2 个 Cisco UCS 互联阵列（FI）	2 个 UCS 6454 FI	第四代互联阵列，支持 10 GB/25 GB/100 GB 以太网和 32 Gb FC
网络	Cisco 以太网交换机	2 个 Nexus 9336c-x2	2 个 Cisco Nexus 9332PQ1 ， 10 GB ， 25 GB ， 40 GB ， 100 GB
存储网络	用于 BLOB 存储的 IP 网络 N9k		
	FC ： Cisco MDS 9132T		两台 Cisco 9132T 交换机
存储	AFF A300	1 个 HA 对	适用于所有 MEDITECH 工作负载的双节点集群（文件服务器，映像服务器，SQL Server ， VMware 等）
	DS224C 磁盘架	1 个 DS224C 磁盘架	
	SSD	19 个 3.8 TB	

这些配置为规模估算指导提供了一个起点。某些客户环境可能会同时运行多个 MEDITECH 生产工作负载和非 MEDITECH 工作负载，或者它们的 IOP 要求可能更高。您应与 NetApp 客户团队合作，根据所需的 IOPS ，工作负载和容量来估算存储系统的规模，以确定适合为工作负载提供服务的平台。

追加信息

要了解有关本文档所述信息的更多信息，请参见以下文档或网站：

- 采用 FC Cisco 验证设计的 FlexPod 数据中心。

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- 《适用于 MEDITECH 环境的 NetApp 部署准则》。

  "https://fieldportal.netapp.com/content/248456" （需要 NetApp 登录）

- 《适用于 MEDITECH 环境的 NetApp 规模估算准则》。

"www.netapp.com/us/media/tr-4190.pdf"

- 适用于 Epic EHR 部署的 FlexPod 数据中心

  "www.netapp.com/us/media/tr-4693.pdf"

- FlexPod 设计区域

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

- 使用 NetApp AFF， vSphere 6.5U1 和 Cisco UCS Manager 的具有 FC 存储（MDS 交换机）的 FlexPod DC

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- Cisco 医疗保健

  https://www.cisco.com/c/en/us/solutions/industries/healthcare.html?dtid=osscdc000283

致谢

以下人员为本指南的编写和创建做出了贡献。

- NetApp 技术营销工程师布兰登·阿吉
- NetApp 医疗保健部门解决方案架构师 John Duignan
- NetApp 产品经理 Ketan Mota
- Cisco Systems， Inc 技术解决方案架构师 Jon Ebmeier
- Cisco Systems， Inc 产品经理 Mike Brennan

《适用于 MEDITECH 的 FlexPod 数据中心部署指南》

TR-4753：《适用于 MEDITECH 的 FlexPod 数据中心部署指南》

NetApp 公司的 Brandon Agee， John Duignan， Mike Brennan 和 Cisco 公司的 Jon Ebmeier

与以下合作伙伴：

解决方案的整体优势

通过在 FlexPod 架构基础上运行 MEDITECH 环境，您的医疗保健组织有望提高员工工作效率，并减少资本和运营支出。适用于 MEDITECH 的 FlexPod 数据中心提供了医疗保健行业特有的多项优势，包括：

- * 简化操作并降低成本。 * 通过使用更高效且可扩展的共享资源来取代原有平台，从而消除原有平台的成本和复杂性，从而为临床医生提供支持，无论这些平台位于何处。此解决方案可提高资源利用率，从而提高投资回报率（ROI）。

- * 加快基础架构部署速度。 * 无论是现有数据中心还是远程位置，借助经过测试的集成 FlexPod 数据中心设计，您可以在更短的时间内完成新基础架构的启动和运行，而无需费力。
- * 认证存储。 * 采用 MEDITECH 的 NetApp ONTAP 数据管理软件可为您提供经过测试和认证的存储供应商所具有的卓越可靠性。Meditech 不会对其他基础架构组件进行认证。
- * 横向扩展架构。 * 无需重新配置正在运行的应用程序，即可将 SAN 和 NAS 从 TB 扩展到数十 PB 。
- * 无中断运行。 * 在不中断业务的情况下执行存储维护，硬件生命周期操作和 FlexPod 升级。
- * 安全多租户。 * 支持日益增长的虚拟化服务器和存储共享基础架构需求，支持对设施特定信息进行安全多租户，尤其是在您的系统托管多个数据库和软件实例时。
- * 池化资源优化。 * 有助于减少物理服务器和存储控制器数量，负载平衡工作负载需求并提高利用率，同时提高性能。
- * 服务质量（ QoS ）。 * FlexPod 可在整个堆栈上提供 QoS 。行业领先的 QoS 网络，计算和存储策略可在共享环境中实现不同的服务级别。这些策略可以为工作负载提供最佳性能，并有助于隔离和控制失控的应用程序。
- * 存储效率。 * 使用降低存储成本 "NetApp 7： 1 存储效率担保"。
- * 灵活性。 * 借助 FlexPod 系统提供的行业领先的工作流自动化，流程编排和管理工具，您的 IT 团队可以更快速地响应业务请求。这些业务请求包括从 MEDITECH 备份和配置更多测试和培训环境到为人口健康管理计划复制分析数据库等。
- * 提高了工作效率。 * 快速部署和扩展此解决方案，以获得最佳临床医生最终用户体验。
- * NetApp Data Fabric 。 * NetApp Data Fabric 架构可以跨站点，跨物理边界和跨应用程序将数据集于一体。NetApp Data Fabric 专为以数据为中心的世界中的数据驱动型企业而构建。数据是在多个位置创建和使用的，通常您需要利用并与其他位置，应用程序和基础架构共享数据。您需要一种一致且集成的数据管理方式。Data Fabric 提供了一种数据管理方式，可以控制数据并简化日益增加的 IT 复杂性。

FlexPod

适用于 MEDITECH EHR 的新基础架构方法

像您这样的医疗保健提供商组织仍然面临着最大程度地从行业领先的 MEDITECH 电子健康记录（ Electronic Health records ， EHR ）的大量投资中获益的压力。对于任务关键型应用程序，客户在为 MEDITECH 解决方案设计数据中心时，通常会为其数据中心架构确定以下目标：

- MEDITECH 应用程序的高可用性
- 高性能
- 在数据中心轻松实施 MEDITECH
- 灵活性和可扩展性，支持通过新的 MEDITECH 版本或应用程序实现增长
- 成本效益
- 与 MEDITECH 指南和目标平台保持一致
- 易管理性，稳定性和易支持性
- 强大的数据保护，备份，恢复和业务连续性

随着 MEDITECH 用户不断发展，成为负责的医疗保健组织，并根据捆绑式强化报销模式进行调整，在以更高效，更灵活的 IT 交付模式交付所需的 MEDITECH 基础架构时，面临的挑战就会越来越大。

经过预先验证的融合基础架构的价值

由于提供可预测的低延迟系统性能和高可用性的总体要求， MEDITECH 对其客户的硬件要求具有规范性。

FlexPod 是一款经过预先验证，经过严格测试的融合基础架构，由 Cisco 和 NetApp 的战略合作伙伴合作打造。它经过专门设计和设计，可提供可预测的低延迟系统性能和高可用性。这种方法可确保 MEDITECH 合规，并最终为 MEDITECH 系统的用户提供最佳响应时间。

Cisco 和 NetApp 推出的 FlexPod 解决方案采用高性能，模块化，预先验证，融合，虚拟化， 高效，可扩展且经济高效的平台。它提供：

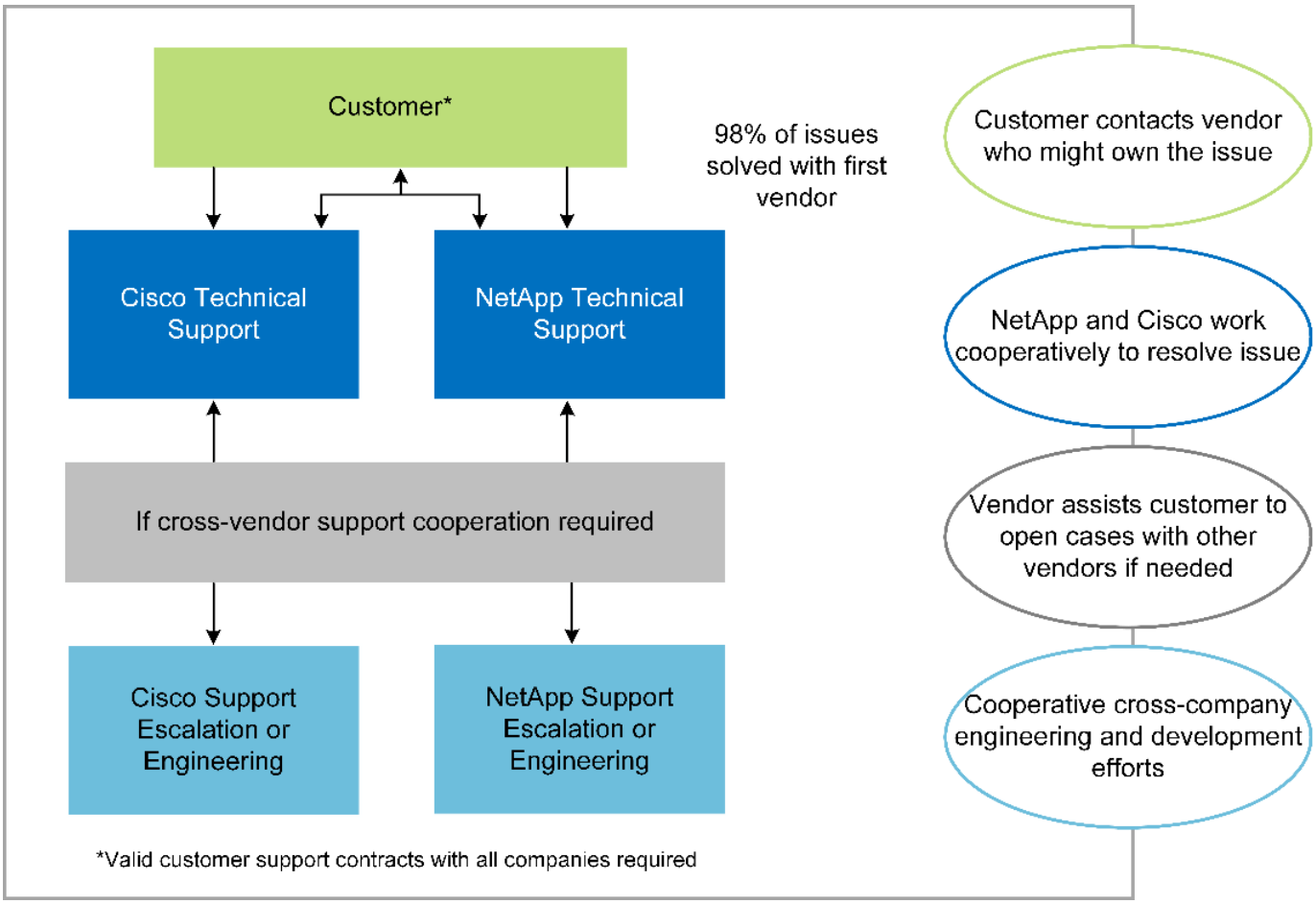
- * 模块化架构。 * FlexPod 可通过针对每个特定工作负载专门配置的 FlexPod 平台来满足 MEDITECH 模块化架构的各种需求。所有组件均通过集群服务器，存储管理网络结构和一个统一的管理工具集进行连接。
- * 融合堆栈各级均采用行业领先的技术。 * Cisco ， NetApp ， VMware 和 Microsoft Windows 在服务器，网络，存储和操作系统的各个类别中均被行业分析师评为第一或第二。
- * 利用标准化，灵活的 IT 保护投资。 * FlexPod 参考架构可预测新产品版本和更新，并持续进行严格的互操作性测试，以适应未来技术的推出。
- * 在广泛的环境中进行成熟的部署。 * FlexPod 已通过广泛的虚拟机管理程序，操作系统，应用程序和基础架构软件的预先测试和联合验证，安装在多个 MEDITECH 客户组织中。

经验证的 **FlexPod** 架构和合作支持

FlexPod 是一款经验证的数据中心解决方案，可提供灵活的共享基础架构，可轻松扩展以满足不断增长的工作负载需求，而不会对性能产生负面影响。通过利用 FlexPod 架构，此解决方案可提供 FlexPod 的全部优势，包括：

- * 性能可满足 MEDITECH 工作负载要求。 * 根据您的 MEDITECH 硬件配置提案要求，可以部署不同的 ONTAP 平台来满足您所需的 I/O 和延迟要求。
- * 可扩展性可轻松适应临床数据增长。 * 可按需动态扩展虚拟机（ VM ），服务器和存储容量，而不受传统限制。
- * 提高了效率。 * 借助融合虚拟化基础架构缩短管理时间并降低 TCO ，这种基础架构更易于管理，更高效地存储数据，同时利用 MEDITECH 软件提高性能。
- * 降低风险。 * 利用基于定义的架构构建的预先验证的平台，最大程度地减少业务中断，消除部署猜测并适应持续的工作负载优化。
- * FlexPod 合作支持。 * NetApp 和 Cisco 建立了合作支持，这是一种强大，可扩展且灵活的支持模式，可满足 FlexPod 融合基础架构的独特支持要求。此模式结合了 NetApp 和 Cisco 的经验，资源和技术支持专业知识，可简化识别和解决 FlexPod 支持问题描述的流程，而无论问题位于何处。借助 FlexPod 合作支持模式，您的 FlexPod 系统可以高效运行并受益于最新技术，您还可以与经验丰富的团队合作，帮助您解决集成问题。

  对于在 FlexPod 融合基础架构上运行业务关键型应用程序（例如 MEDITECH ）的医疗保健组织来说，FlexPod 合作支持尤其重要。下图显示了 FlexPod 合作支持模式。



除了这些优势之外，采用 MEDITECH 解决方案的 FlexPod 数据中心堆栈的每个组件还为 MEDITECH EHR 工作流提供了特定优势。

Cisco Unified Computing System

Cisco Unified Computing System （ Cisco UCS ）是一个自我集成的自我感知系统，由一个管理域组成，该管理域与统一 I/O 基础架构互连。为了使基础架构能够提供最可用的关键患者信息，适用于 MEDITECH 环境的 Cisco UCS 已与 MEDITECH 基础架构建议和最佳实践保持一致。

基于 Cisco UCS 架构的 MEDITECH 的基础是 Cisco UCS 技术，它具有集成的系统管理， Intel Xeon 处理器和服务器虚拟化功能。这些集成技术可解决数据中心挑战，并帮助您实现 MEDITECH 数据中心设计的目标。Cisco UCS 将 LAN ， SAN 和系统管理统一为一个简化的链路，用于机架式服务器，刀片式服务器和 VM 。Cisco UCS 是一种端到端 I/O 架构，它整合了 Cisco Unified Fabric 和 Cisco Fabric Extender Technology （ FEX 技术），可将 Cisco UCS 中的每个组件连接到一个网络结构和一个网络层。

该系统可以部署为一个或多个逻辑单元，这些逻辑单元可整合并扩展到多个刀片式服务器机箱，机架服务器，机架和数据中心。该系统实施了一个彻底简化的架构，消除了在传统刀片式服务器机箱和机架服务器中填充多个冗余设备的情况。在传统系统中，以太网和 FC 适配器以及机箱管理模块等冗余设备会造成多层复杂性。Cisco UCS 由一对冗余的 Cisco UCS 互联阵列（ Fabric Interconnects ， CLI ）组成，可为所有 I/O 流量提供单点管理和单点控制。

Cisco UCS 使用服务配置文件来帮助确保 Cisco UCS 基础架构中的虚拟服务器配置正确。服务配置文件由网络，存储和计算策略组成，这些策略由每个领域的主题专家创建一次。服务配置文件包括有关服务器标识的关键服务器信息，例如 LAN 和 SAN 寻址， I/O 配置，固件版本，启动顺序，网络虚拟 LAN （ VLAN ），物理端口和 QoS 策略。可以在几分钟内动态创建服务配置文件并将其与系统中的任何物理服务器相关联，而无需花费数小时或数天的时间。将服务配置文件与物理服务器关联起来只需执行一项简单的操作，即可在环境中的服务器之间

迁移身份，而无需更改任何物理配置。它有助于为已停用的服务器快速配置更换件。

使用服务配置文件有助于确保服务器在整个企业中的配置一致。如果使用多个 Cisco UCS 管理域，则 Cisco UCS Central 可以使用全局服务配置文件在各个域之间同步配置和策略信息。如果需要在一个域中执行维护，则可以将虚拟基础架构迁移到另一个域。这种方法有助于确保即使单个域脱机，应用程序也能继续以高可用性运行。

为了证明它符合服务器配置要求， Cisco UCS 已在多年的时间里与 MEDITECH 进行了广泛的测试。Cisco UCS 是一个受支持的服务器平台，如 MEDITECH 产品资源系统支持站点所示。

Cisco 网络

Cisco Nexus 交换机和 Cisco MDS 多层控制器可提供企业级连接和 SAN 整合。Cisco 多协议存储网络通过提供以下灵活性和选项降低业务风险： FC ，光纤连接（ Fibre Connection ， Ficon ），以太网 FC （ FCoE ），IP 上 SCSI （ iSCSI ）和 IP 上 FC （ FCIP ）。

Cisco Nexus 交换机可在一个平台中提供最全面的数据中心网络功能集之一。它们可以为数据中心和园区核心提供高性能和高密度。此外，它们还为数据中心聚合，行尾和数据中心互连部署提供了一整套功能，可在一个具有高度弹性的模块化平台中实现。

Cisco UCS 可将计算资源与 Cisco Nexus 交换机和统一 I/O 网络结构相集成，从而识别和处理不同类型的网络流量。此流量包括存储 I/O ，流式桌面流量，管理以及对临床和业务应用程序的访问。您可以获得：

- * 基础架构可扩展性。 * 虚拟化，高效的电耗和散热，自动化的云扩展，高密度和高性能都支持高效的数据中心增长。
- * 操作连续性。 * 该设计集成了硬件， NX-OS 软件功能和管理功能，可支持零停机环境。
- * 网络和计算机 QoS 。 * Cisco 在网络，存储和计算网络结构中提供策略驱动型服务级别（ CoS ）和 QoS ，以实现任务关键型应用程序的最佳性能。
- * 传输灵活性。 * 利用经济高效的解决方案逐步采用新的网络技术。

Cisco UCS 与 Cisco Nexus 交换机和 Cisco MDS 多层控制器相结合，可为 MEDITECH 提供最佳的计算，网络和 SAN 连接解决方案。

NetApp ONTAP

运行 ONTAP 软件的 NetApp 存储可降低整体存储成本，同时提供 MEDITECH 工作负载所需的低延迟读写响应时间和 IOPS 。ONTAP 支持全闪存和混合存储配置，可创建满足 MEDITECH 要求的最佳存储平台。NetApp 闪存加速系统已获得 MEDITECH 的验证和认证，可为作为 MEDITECH 客户的您提供性能和响应能力，这是对延迟敏感的 MEDITECH 运营的关键。通过在一个集群中创建多个故障域， NetApp 系统还可以将生产与非生产隔离开来。此外， NetApp 系统还可以为采用 ONTAP QoS 的工作负载提供最低性能保障，从而减少性能问题。

ONTAP 软件的横向扩展架构可以灵活地适应各种 I/O 工作负载。为了提供临床应用程序所需的必要吞吐量和低延迟，同时提供模块化横向扩展架构，全闪存配置通常用于 ONTAP 架构。NetApp AFF 节点可以在同一个横向扩展集群中与混合（ HDD 和闪存）存储节点组合使用，这些存储节点适用于存储高吞吐量的大型数据集。除了经过 MEDITECH 批准的备份解决方案之外，您还可以将 MEDITECH 环境从昂贵的固态驱动器（ SSD ）存储克隆，复制和备份到其他节点上更经济的 HDD 存储。此方法符合或超出了 MEDITECH 对基于 SAN 的克隆和生产池备份的指导原则。

许多 ONTAP 功能在 MEDITECH 环境中特别有用：简化管理，提高可用性和自动化以及减少所需的总存储量。借助这些功能，您可以：

- * 卓越的性能。 * NetApp AFF 解决方案共享统一存储架构， ONTAP 软件，管理界面，丰富的数据服务以及

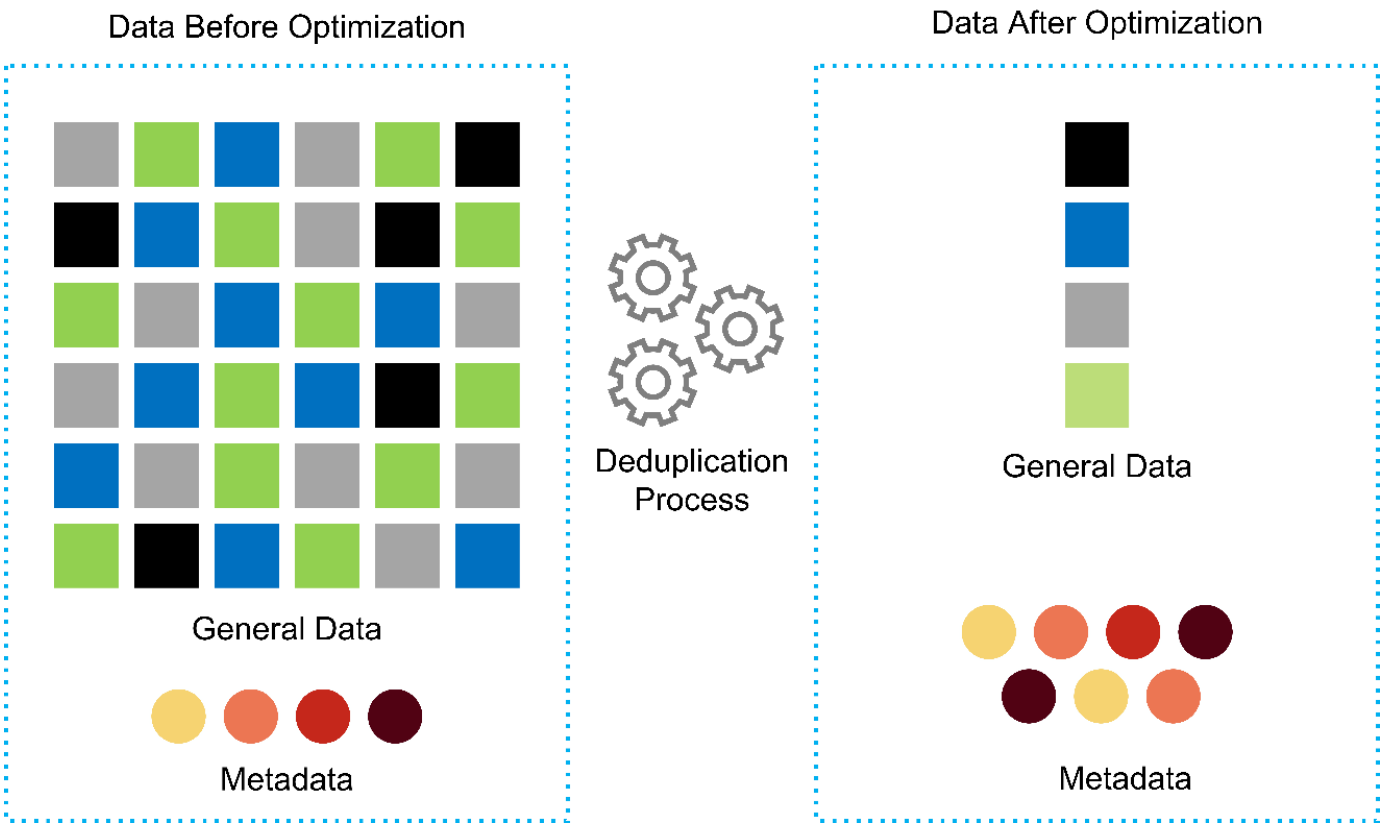
其他 NetApp FAS 产品系列所具有的高级功能集。全闪存介质与 ONTAP 的这种创新组合，通过行业领先的 ONTAP 软件质量，为全闪存存储提供稳定一致的低延迟和高 IOPS 。

- * 存储效率。 * 利用重复数据删除， NetApp FlexClone 数据复制技术，实时压缩，实时数据缩减，精简复制，精简配置， 和聚合重复数据删除。

  NetApp 重复数据删除可在 NetApp FlexVol 卷或数据成分卷中提供块级重复数据删除。从本质上说，重复数据删除会删除重复的块，从而仅在 FlexVol 卷或数据成分卷中存储唯一的块。

  重复数据删除的粒度较高，并且在 FlexVol 卷或数据成分卷的活动文件系统上运行。它是应用程序透明的；因此，您可以使用它对使用 NetApp 系统的任何应用程序生成的数据进行重复数据删除。您可以将卷重复数据删除作为实时进程运行（从 ONTAP 8.3.2 开始）。您也可以将其作为后台进程运行，您可以将其配置为自动运行，计划运行或通过命令行界面， NetApp ONTAP System Manager 或 NetApp Active IQ Unified Manager 手动运行。

  下图显示了 NetApp 重复数据删除在最高级别的工作原理。

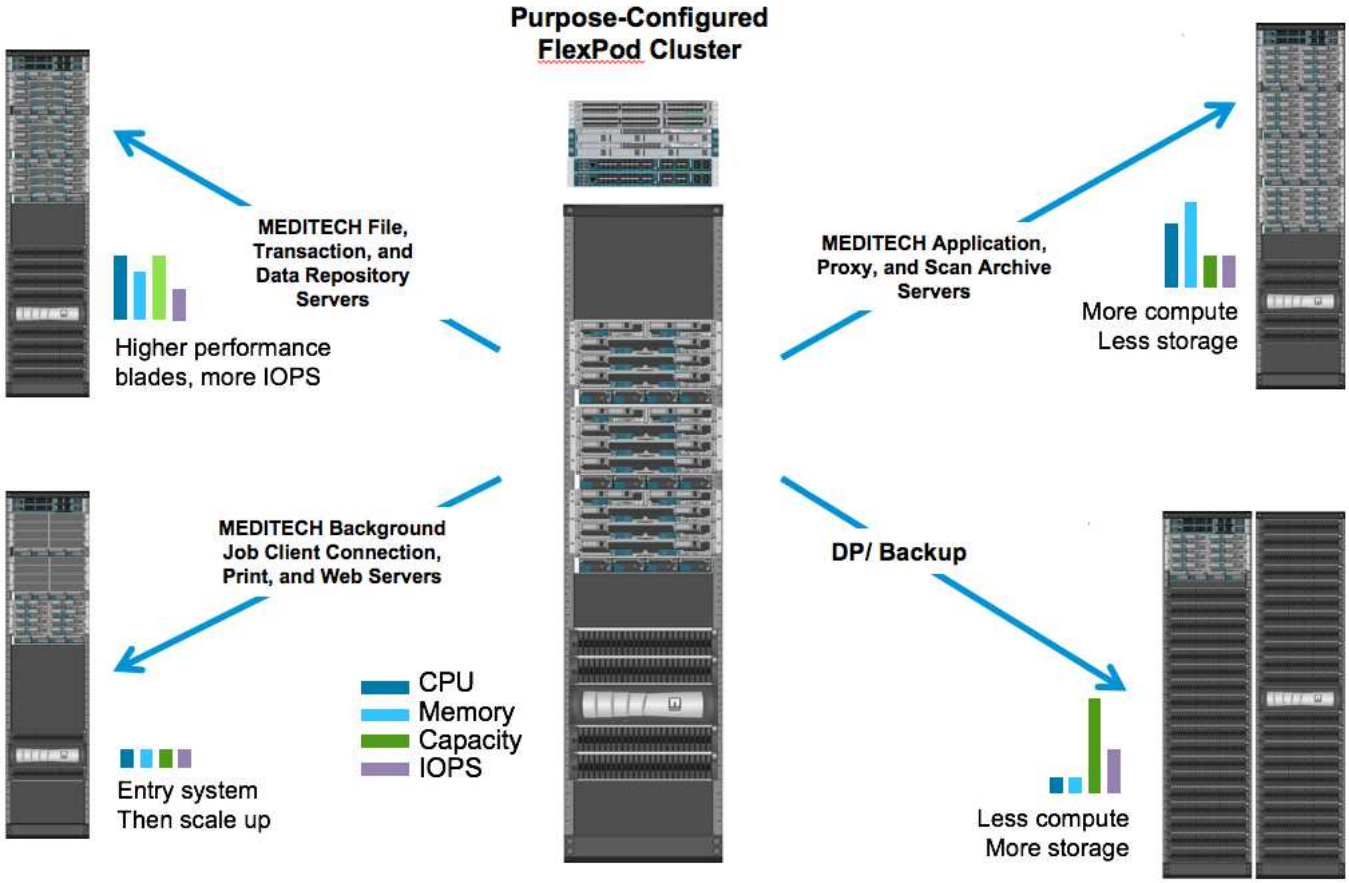


- * 节省空间的克隆。 * 借助 FlexClone 功能，您几乎可以即时创建克隆，以支持备份和测试环境刷新。只有在进行更改后，这些克隆才会占用更多存储。
- * NetApp Snapshot 和 SnapMirror 技术。 * ONTAP 可以为 MEDITECH 主机使用的逻辑单元号（ LUN ）创建节省空间的 Snapshot 副本。对于双站点部署，您可以实施 SnapMirror 软件，以实现更多数据复制和故障恢复能力。
- * 集成数据保护。 * 完整的数据保护和灾难恢复功能可帮助您保护关键数据资产并提供灾难恢复。
- * 无中断运行。 * 您可以执行升级和维护，而无需使数据脱机。
- * QoS 和自适应 QoS （ AQoS ）。 * 存储 QoS 可用于限制潜在的抢占资源的工作负载。更重要的是，QoS 可以保证像 MEDITECH 生产这样的关键工作负载的最低性能。通过限制争用， NetApp QoS 可以减少与性能相关的问题。AQO 可与预定义的策略组结合使用，您可以将这些策略组直接应用于卷。这些策略组

可以自动扩展吞吐量上限或下限到卷大小，从而在卷大小发生变化时保持 IOPS 与 TB 和 GB 的比率。

- * NetApp Data Fabric 。 * NetApp Data Fabric 简化并集成了云和内部环境中的数据管理，加快了数字化转型的步伐。它提供一致且集成的数据管理服务和应用程序，以提高数据可见性和洞察力，实现数据访问和控制以及数据保护和安全性。NetApp 与 Amazon Web Services （AWS ）， Azure ， Google Cloud Platform 和 IBM Cloud Cloud Cloud Cloud Cloud Cloud 相集成，为您提供广泛的选择。

下图显示了适用于 MEDITECH 工作负载的 FlexPod 架构。



MEDITECH 概述

Medical Information Technology ， Inc. （通常称为 MEDITECH ）是一家总部位于马萨诸塞州的软件公司，负责为医疗保健组织提供信息系统。Meditech 提供了一个 EHR 系统，用于存储和组织最新的患者数据，并为临床工作人员提供数据。患者数据包括但不限于人口统计信息，病历，药物，实验室测试结果； 放射学图像；以及年龄，高度和重量等个人信息。

本文档不会介绍 MEDITECH 软件支持的广泛功能。附录 A 提供了有关这些广泛的 MEDITECH 功能集的详细信息。Meditech 应用程序需要多个 VM 来支持这些功能。要部署这些应用程序，请参见 MEDITECH 的建议。

从存储系统角度来看，对于每个部署，所有 MEDITECH 软件系统都需要一个分布式以患者为中心的数据库。Meditech 拥有自己的专有数据库，该数据库使用 Windows 操作系统。

bridgehead 和 Commvault 是两个备份软件应用程序，均已通过 NetApp 和 MEDITECH 的认证。本文档不会介绍这些备份应用程序的部署。

本文档的主要重点是，使 FlexPod 堆栈（服务器和存储）能够满足 MEDITECH 数据库的性能驱动型要求以及 EHR 环境中的备份要求。

专为特定的 MEDITECH 工作负载而设计

Meditech 不会转售服务器，网络或存储硬件，虚拟机管理程序或操作系统； 但是，它对基础架构堆栈的每个组件都有特定的要求。因此， Cisco 和 NetApp 携手测试并支持 FlexPod 数据中心的成功配置，部署和支持，以满足像您这样的客户对 MEDITECH 生产环境的要求。

Meditech 类别

Meditech 会将部署规模与 1 到 6 之间的类别编号关联起来。类别 1 表示最小的 MEDITECH 部署，类别 6 表示最大的 MEDITECH 部署。

有关每个类别中 MEDITECH 主机的 I/O 特征和性能要求的信息，请参见 NetApp "TR-4190： 《适用于 MEDITECH 环境的 NetApp 规模估算准则》"。

Meditech 平台

MEDITECH expanse 平台是该公司 EHR 软件的最新版本。早期的 MEDITECH 平台是客户端 / 服务器 5.x 和魔力平台。本节介绍与 MEDITECH 主机及其存储要求相关的 MEDITECH 平台（适用于 expanse ， 6.x ， C/S 5.x 和 Magic ）。

对于上述所有 MEDITECH 平台，多个服务器运行 MEDITECH 软件并执行各种任务。上图显示了一个典型的 MEDITECH 系统，其中包括用作应用程序数据库服务器的 MEDITECH 主机和其他 MEDITECH 服务器。其他 MEDITECH 服务器的示例包括数据存储库应用程序，扫描和归档应用程序以及后台作业客户端。有关其他 MEDITECH 服务器的完整列表，请参见《硬件配置建议》（对于新部署）和《硬件评估任务》（对于现有部署）文档。您可以通过 MEDITECH 系统集成商或您的 MEDITECH 技术客户经理（ Technical Account Manager ， TAM ）从 MEDITECH 获取这些文档。

MEDITECH 主机

MEDITECH 主机是数据库服务器。此主机也称为 MEDITECH 文件服务器（对于 expanse ， 6.x 或 C/S 5.x 平台）或魔力机器（对于魔力平台）。本文档使用术语 MEDITECH 主机来指代 MEDITECH 文件服务器或魔力机器。

Meditech 主机可以是在 Microsoft Windows Server 操作系统上运行的物理服务器或 VM 。在现场最常见的情况是， MEDITECH 主机部署为在 VMware ESXi 服务器上运行的 Windows VM 。截至本文撰写时， VMware 是 MEDITECH 唯一支持的虚拟机管理程序。MEDITECH 主机将其程序，词典和数据文件存储在 Windows 系统上的 Microsoft Windows 驱动器（例如驱动器 E ）上。

在虚拟环境中， Windows E 驱动器驻留在通过物理兼容模式下的原始设备映射（ Raw Device Mapping ， RDM ）连接到 VM 的 LUN 上。在这种情况下， MEDITECH 不支持将虚拟机磁盘（ VMDK ）文件用作 Windows E 驱动器。

Meditech 主机工作负载 I/O 特征

每个 MEDITECH 主机和整个系统的 I/O 特征取决于您部署的 MEDITECH 平台。所有 MEDITECH 平台（ expanse ， 6.x ， C/S 5.x 和 Magic ）都会生成 100% 随机的工作负载。

MEDITECH expanse 平台产生的工作负载要求最高，因为它的每台主机写入操作和整体 IOPS 百分比最高，其次是 6.x ， C/S 5.x 和魔力平台。

有关 MEDITECH 工作负载说明的更多详细信息，请参见 "TR-4190： 《适用于 MEDITECH 环境的 NetApp 规模估算准则》"。

存储网络

Meditech 要求对 NetApp FAS 或 AFF 系统与所有类别的 MEDITECH 主机之间的数据流量使用 FC 协议。

MEDITECH 主机的存储表示

每个 MEDITECH 主机都使用两个 Windows 驱动器：

- * 驱动器 C.* 此驱动器用于存储 Windows Server 操作系统和 MEDITECH 主机应用程序文件。
- * 驱动器 e* MEDITECH 主机将其程序，词典和数据文件存储在 Windows Server 操作系统的驱动器 E 上。驱动器 E 是使用 FC 协议从 NetApp FAS 或 AFF 系统映射的 LUN 。Meditech 要求使用 FC 协议，以满足 MEDITECH 主机的 IOPS 以及读写延迟要求。

卷和 LUN 命名约定

Meditech 要求对所有 LUN 使用特定的命名约定。

在进行任何存储部署之前，请验证 MEDITECH 硬件配置建议，以确认 LUN 的命名约定。MEDITECH 备份过程依靠卷和 LUN 命名约定来正确标识要备份的特定 LUN 。

全面的管理工具和自动化功能

采用 Cisco UCS Manager 的 Cisco UCS

Cisco 侧重于提供卓越数据中心基础架构的三个关键要素：简化，安全性和可扩展性。Cisco UCS Manager 软件与平台模块化相结合，可提供一个简化，安全且可扩展的桌面虚拟化平台：

- * 简化。 * Cisco UCS 提供了一种全新的行业标准计算方法，并为所有工作负载提供了数据中心基础架构的核心。Cisco UCS 具有许多功能和优势，包括减少所需服务器数量以及减少每台服务器使用的缆线数量。另一项重要功能是能够通过 Cisco UCS 服务配置文件快速部署或重新配置服务器。由于需要管理的服务器和缆线更少，并且服务器和应用程序工作负载配置更简化，因此操作也得到了简化。使用 Cisco UCS Manager 服务配置文件，可以在几分钟内配置多个刀片式服务器和机架式服务器。Cisco UCS 服务配置文件消除了服务器集成操作手册并消除了配置偏差。这种方法可以加快最终用户的工作效率，提高业务灵活性，并允许将 IT 资源分配给其他任务。

  Cisco UCS Manager 可自动执行许多常见且容易出错的数据中心操作，例如配置和配置服务器，网络和存储访问基础架构。此外，具有较大内存占用空间的 Cisco UCS B 系列刀片式服务器和 C 系列机架式服务器还可以提高应用程序用户密度，从而有助于降低服务器基础架构要求。

  通过简化，可以更快，更成功地部署 MEDITECH 基础架构。

- * 安全。 * 虽然虚拟机本身比物理前代产品更安全，但它们带来了新的安全挑战。使用虚拟桌面等通用基础架构的任务关键型 Web 和应用程序服务器现在面临的安全威胁风险更高。现在， VM 间流量已经成为 IT 经理必须考虑的一个重要安全问题，尤其是在 VM 使用 VMware vMotion 在服务器基础架构间移动的动态环境中。

  因此，虚拟化显著增加了对 VM 级别策略和安全性的感知需求，尤其是考虑到 VM 在扩展计算基础架构中的移动性具有动态性和流动性。新虚拟桌面的快速普及进一步增强了虚拟化感知型网络和安全基础架构的重要性。适用于桌面虚拟化的 Cisco 数据中心基础架构（ Cisco UCS ， Cisco MDS 和 Cisco Nexus 系列解决方案）可提供强大的数据中心，网络和桌面安全性，并提供从桌面到虚拟机管理程序的全面安全性。通过对虚拟桌面进行分段，虚拟机感知型策略和管理以及 LAN 和 WAN 基础架构中的网络安全性，增强了安全性。

- * 可扩展。 * 虚拟化解决方案的增长是不可避免的，因此解决方案必须能够随着这种增长进行扩展和可预测

的扩展。Cisco 虚拟化解决方案支持高 VM 密度（每台服务器具有 VM ），更多服务器可通过近乎线性的性能进行扩展。Cisco 数据中心基础架构提供了一个灵活的平台来实现增长并提高业务灵活性。Cisco UCS Manager 服务配置文件允许按需配置主机，并使部署数百台主机与部署数十台主机一样简单。

Cisco UCS 服务器可提供近乎线性的性能和可扩展性。Cisco UCS 实施了获得专利的 Cisco 扩展内存技术，可通过更少的插槽提供较大的内存占用空间（通过双插槽和四插槽服务器可扩展到 1 TB 的内存）。通过使用统一网络结构技术作为组件， Cisco UCS 服务器聚合带宽可扩展到每台服务器高达 80 Gbps ，而北向 Cisco UCS 互联阵列可按线路速率输出 2Tbps 。此功能有助于防止桌面虚拟化 I/O 和内存瓶颈。Cisco UCS 采用基于统一网络结构的高性能，低延迟网络架构，可支持大量虚拟桌面流量，包括高分辨率视频和通信流量。此外，作为 FlexPod 虚拟化解决方案的一部分， ONTAP 还有助于在启动和登录风暴期间保持数据可用性和最佳性能。

Cisco UCS ， Cisco MDS 和 Cisco Nexus 数据中心基础架构设计为增长提供了一个出色的平台。您可以透明地扩展服务器，网络和存储资源，以支持桌面虚拟化，数据中心应用程序和云计算。

VMware vCenter Server

VMware vCenter Server 为管理 MEDITECH 环境提供了一个集中式平台，使您的医疗保健组织可以放心地自动化和交付虚拟基础架构：

- * 部署简单。 * 使用虚拟设备快速轻松地部署 vCenter Server 。
- * 集中控制和可见性。 * 从一个位置管理整个 VMware vSphere 基础架构。
- * 主动式优化。 * 分配和优化资源以实现最高效率。
- * 管理。 * 使用功能强大的插件和工具简化管理并扩展控制。

适用于 VMware vSphere 的 Virtual Storage Console

NetApp 的 Virtual Storage Console （ VSC ）， vSphere API for Storage Awareness （ VASA ） Provider 和 VMware Storage Replication Adapter （ SRA ） for VMware vSphere 构成了一个虚拟设备。此产品套件将 SRA 和 VASA Provider 作为 vCenter Server 的插件，可为使用 NetApp 存储系统的 VMware 环境中的 VM 提供端到端生命周期管理。

VSC ， VASA Provider 和 SRA 虚拟设备可与 VMware vSphere Web Client 平稳集成，并支持您使用 SSO 服务。在具有多个 VMware vCenter Server 实例的环境中，要管理的每个 vCenter Server 实例都必须有自己注册的 VSC 实例。通过 VSC 信息板页面，您可以快速检查数据存储库和 VM 的整体状态。

通过部署 VSC ， VASA Provider 和 SRA 虚拟设备，您可以执行以下任务：

- * 使用 VSC 部署和管理存储以及配置 ESXi 主机。 * 您可以使用 VSC 为 VMware 环境中的存储控制器添加凭据，删除凭据，分配凭据以及设置权限。此外，您还可以管理连接到 NetApp 存储系统的 ESXi 服务器。只需单击几下鼠标，即可为所有主机设置主机超时， NAS 和多路径的建议最佳实践值。您还可以查看存储详细信息并收集诊断信息。
- * 使用 VASA Provider 创建存储功能配置文件并设置警报。 * 启用 VASA Provider 扩展后，适用于 ONTAP 的 VASA Provider 将注册到 VSC 中。您可以创建和使用存储功能配置文件和虚拟数据存储库。您还可以设置警报，以便在卷和聚合的阈值接近全满时向您发出警报。您可以监控 VMDK 以及在虚拟数据存储库上创建的 VM 的性能。
- * 使用 SRA 进行灾难恢复。 * 您可以使用 SRA 在环境中配置受保护站点和恢复站点，以便在发生故障时进行灾难恢复。

NetApp OnCommand Insight 和 ONTAP

NetApp OnCommand Insight 将基础架构管理集成到了 MEDITECH 服务交付链中。这种方法可以使医疗保健组织更好地控制，自动化和分析存储，网络和计算基础架构。它可以优化您当前的基础架构，以获得最大收益，同时简化确定购买内容和购买时间的过程。它还可以降低与复杂技术迁移相关的风险。由于不需要代理，因此安装简单，无中断。系统会持续发现已安装的存储和 SAN 设备，并收集详细信息以全面了解整个存储环境。您可以快速识别滥用，错位，未充分利用或孤立的资产，并回收这些资产以推动未来的扩展。OnCommand Insight 可帮助您：

- * 优化现有资源。 * 利用已建立的最佳实践来识别滥用，未充分利用或孤立的资产，以避免出现问题并满足服务级别要求。
- * 做出更明智的决策。 * 实时数据有助于更快地解决容量问题，从而准确规划未来的购买，避免超支并推迟资本支出。
- * 加速 IT 计划。 * 更好地了解您的虚拟环境，帮助您管理风险，最大限度地减少停机时间并加快云部署速度。

设计

适用于 MEDITECH 的 FlexPod 架构基于 MEDITECH ， Cisco 和 NetApp 的指导以及合作伙伴与各种规模的 MEDITECH 客户合作的经验。该架构具有适应性，并会根据您的数据中心战略，组织规模以及您的系统是集中式系统，分布式系统还是多租户系统，应用 MEDITECH 的最佳实践。

正确的存储架构可通过总 IOPS 大小来确定。性能本身并不是唯一的因素，您可能会根据其他客户需求决定使用更大的节点数。使用 NetApp 存储的优势在于，您可以根据需求的变化轻松无中断地扩展集群。您也可以从集群中无中断删除节点，以重新利用设备或在设备更新期间使用。

以下是 NetApp ONTAP 存储架构的一些优势：

- * 轻松，无中断地纵向扩展和横向扩展。 * 您可以使用 ONTAP 无中断操作升级，添加或删除磁盘和节点。您可以从四个节点开始，然后移至六个节点或无中断升级到更大的控制器。
- * 存储效率。 * 利用重复数据删除， NetApp FlexClone ，实时压缩，实时数据缩减，精简复制， 精简配置和聚合重复数据删除。通过 FlexClone 功能，您几乎可以即时创建克隆，以支持备份和测试环境更新。只有在进行更改后，这些克隆才会占用更多存储。
- * 灾难恢复卷影数据库服务器。 * 灾难恢复卷影数据库服务器是业务连续性策略的一部分（用于支持存储只读功能，并可能配置为存储读 / 写实例）。因此，第三个存储系统的放置和规模估算通常与生产数据库存储系统中的放置和规模估算相同。
- * 数据库一致性（需要考虑一些因素）。 * 如果您使用 NetApp SnapMirror 备份副本来保持业务连续性，请参见 "TR-3446 ：《 SnapMirror 异步概述和最佳实践指南》"。

存储布局

用于 MEDITECH 主机的专用聚合

要满足 MEDITECH 的高性能和高可用性要求，第一步是为 MEDITECH 环境正确设计存储布局，以便将 MEDITECH 主机生产工作负载隔离到专用的高性能存储上。

应在每个存储控制器上配置一个专用聚合，用于存储 MEDITECH 主机的程序，词典和数据文件。为了消除其他工作负载使用相同磁盘并影响性能的可能性，不会从这些聚合配置任何其他存储。

> 为其他 MEDITECH 服务器配置的存储不应放置在 MEDITECH 主机所使用的 LUN 的专用聚合上。您应将其他 MEDITECH 服务器的存储放置在一个单独的聚合上。有关其他 MEDITECH 服务器的存储要求，请参见《硬件配置建议》（针对新部署）和《硬件评估任务》（针对现有部署）文档。您可以通过 MEDITECH 系统集成商或您的 MEDITECH 技术客户经理（ Technical Account Manager ， TAM ）从 MEDITECH 获取这些文档。NetApp 解决方案工程师可以咨询 NetApp MEDITECH 独立软件供应商（ ISV ）团队，以便正确，完整地配置 NetApp 存储规模估算。

将 **MEDITECH** 主机工作负载均匀分布在所有存储控制器上

NetApp FAS 和 AFF 系统部署为一个或多个高可用性对。NetApp 建议您在每个存储控制器之间均匀分布 MEDITECH expanse 和 6.x 工作负载，以便在每个存储控制器上应用计算，网络和缓存资源。

请按照以下准则在每个存储控制器之间均匀分布 MEDITECH 工作负载：

- 如果您知道每个 MEDITECH 主机的 IOPS ，则可以通过确认每个控制器从 MEDITECH 主机提供的 IOPS 数量相似，在所有存储控制器之间均匀分布 MEDITECH expanse 和 6.x 工作负载。
- 如果您不知道每个 MEDITECH 主机的 IOPS ，则仍然可以在所有存储控制器之间均匀分布 MEDITECH expanse 和 6.x 工作负载。要完成此任务，请确认 MEDITECH 主机的聚合容量均匀分布在所有存储控制器上。这样，专用于 MEDITECH 主机的所有数据聚合中的磁盘数量都是相同的。
- 使用相似的磁盘类型和相同的 RAID 组为两个控制器创建存储聚合，以便平均分布工作负载。在创建存储聚合之前，请联系 NetApp 认证集成商。

> 据 MEDITECH 报告， MEDITECH 系统中的两个主机生成的 IOPS 高于其余主机。这两个主机的 LUN 应放置在不同的存储控制器上。在部署系统之前，您应在 MEDITECH 团队的协助下确定这两台主机。

存储放置

MEDITECH 主机的数据库存储

MEDITECH 主机的数据库存储将作为 NetApp FAS 或 AFF 系统中的块设备（即 LUN ）提供。LUN 通常作为 E 驱动器挂载到 Windows 操作系统。

其他存储

MEDITECH 主机操作系统和数据库应用程序通常会在存储上生成大量 IOPS 。如果需要， MEDITECH 主机 VM 及其 VMDK 文件的存储配置会被视为独立于满足 MEDITECH 性能阈值所需的存储。

为其他 MEDITECH 服务器配置的存储不应放置在 MEDITECH 主机使用的 LUN 的专用聚合上。将其他 MEDITECH 服务器的存储置于单独的聚合上。

存储控制器配置

高可用性

要缓解控制器故障的影响并实现存储系统无中断升级，您应在高可用性模式下为存储系统配置高可用性对中的控制器。

在高可用性控制器对配置中，磁盘架应通过多条路径连接到控制器。此连接可防止单路径故障，从而提高存储故障恢复能力，并可在发生控制器故障转移时提高性能一致性。

存储控制器故障转移期间的存储性能

对于在高可用性对中配置了控制器的存储系统，如果发生控制器故障的可能性不大，则配对控制器将接管发生故障的控制器的存储资源和工作负载。请务必咨询客户，以确定发生控制器故障时必须满足的性能要求，并相应地调整系统大小。

硬件辅助接管

NetApp 建议您在两个存储控制器上启用硬件辅助接管功能。

硬件辅助接管旨在最大程度地缩短存储控制器故障转移时间。它使一个控制器的远程 LAN 模块或服务处理器模块能够以比检测信号超时触发器更快的速度向其配对节点通知控制器故障，从而缩短故障转移所需的时间。默认情况下，高可用性配置中的存储控制器会启用硬件辅助接管功能。

有关硬件辅助接管的详细信息，请参见 "ONTAP 9 文档中心"。

Disk type

为了满足 MEDITECH 工作负载的低读取延迟要求， NetApp 建议您对专用于 MEDITECH 主机的 AFF 系统上的聚合使用高性能 SSD 。

NetApp AFF

NetApp 提供高性能 AFF 阵列，以满足需要高吞吐量，具有随机数据访问模式和低延迟要求的 MEDITECH 工作负载的需求。对于 MEDITECH 工作负载，与基于 HDD 的系统相比， AFF 阵列具有性能优势。闪存技术与企业数据管理相结合，可在三个主要方面提供优势：性能，可用性和存储效率。

NetApp 支持工具和服务

NetApp 提供了一整套支持工具和服务。应在 NetApp AFF/FAS 系统上启用和配置 NetApp AutoSupport 工具，以便在发生硬件故障或系统配置不当时回电。致电主页可提醒 NetApp 支持团队及时修复任何问题。NetApp Active IQ 是一款基于 Web 的应用程序，它基于您的 NetApp 系统中的 AutoSupport 信息，可提供预测性和主动式洞察力，帮助提高可用性，效率和性能。

部署和配置

概述

本文档中提供的适用于 FlexPod 部署的 NetApp 存储指南包括：

- 使用 ONTAP 的环境
- 使用 Cisco UCS 刀片式服务器和机架式服务器的环境

本文档不涉及以下内容：

- 详细部署 FlexPod 数据中心环境

  有关详细信息，请参见 "采用 FC Cisco 验证设计的 FlexPod 数据中心" （ CVD ）。

- MEDITECH 软件环境，参考架构和集成最佳实践指南概述。

  有关详细信息，请参见 "TR-4300i ：《适用于 MEDITECH 环境的 NetApp FAS 和全闪存存储系统最佳实践

指南》"（需要 NetApp 登录）。

- 量化性能要求和规模估算指南。

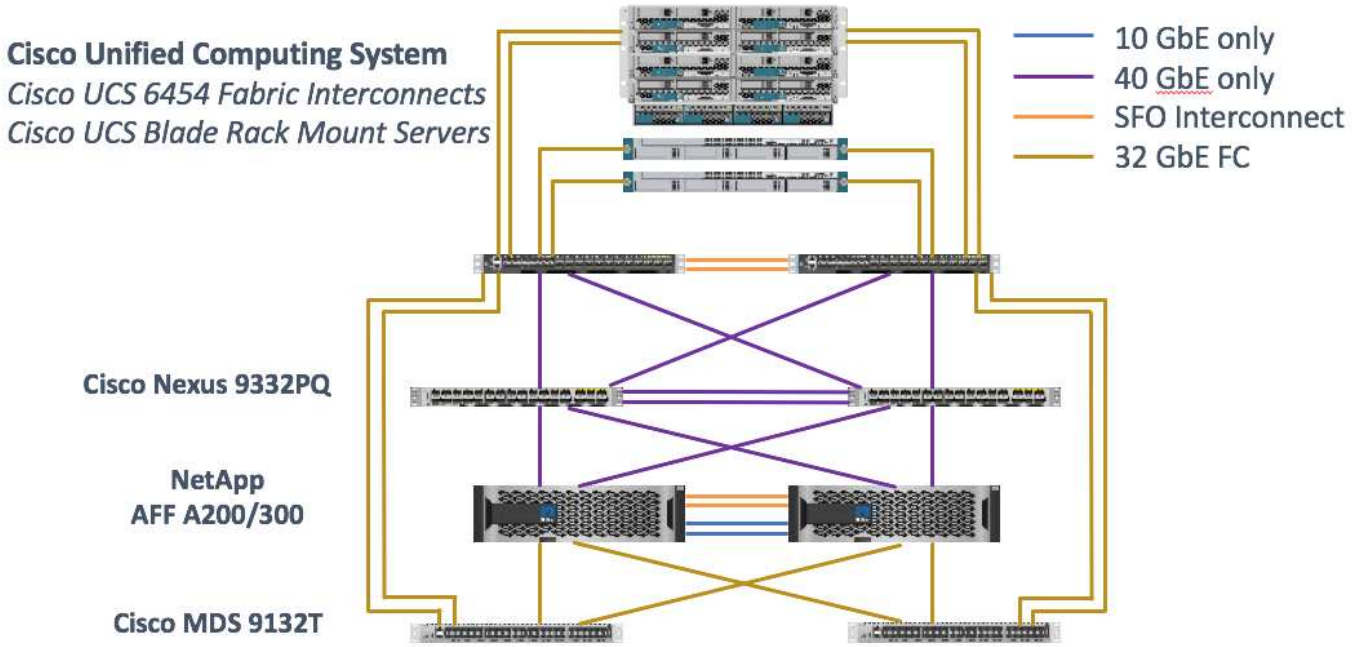
  有关详细信息，请参见 "TR-4190：《适用于 MEDITECH 环境的 NetApp 规模估算准则》"。

- 使用 NetApp SnapMirror 技术满足备份和灾难恢复要求。
- 通用 NetApp 存储部署指南。

本节提供了一个配置示例，其中包含基础架构部署最佳实践，并列出了各种基础架构硬件和软件组件以及您可以使用的版本。

布线图

下图显示了 MEDITECH 部署的 32 Gb FC/40GbE 拓扑图。



请始终使用 "互操作性表工具（IMT）" 验证是否支持所有版本的软件和固件。第节中的表 "Meditech 模块和组件" 列出了解决方案测试中使用的基础架构硬件和软件组件。

"接下来：基础架构配置。"

基础架构配置

网络连接

在配置基础架构之前，必须建立以下网络连接：

- 使用端口通道和虚拟端口通道（Virtual Port Channel， vPC）的链路聚合可在整个环境中使用，从而实现更高带宽和高可用性的设计：
  - VPC 用于 Cisco FI 和 Cisco Nexus 交换机之间。
  - 每个服务器都具有虚拟网络接口卡（Virtual Network Interface Card， vNIC），并可通过冗余连接到

统一网络结构。在 CLI 之间使用 NIC 故障转移来实现冗余。
    - 每个服务器都具有虚拟主机总线适配器（ vHBA ），并与统一网络结构建立冗余连接。
- Cisco UCS FI 会按照建议配置为终端主机模式，以便将 vNIC 动态固定到上行链路交换机。

存储连接

在配置基础架构之前，必须建立以下存储连接：

- 存储端口接口组（ ifgroups ， vPC ）
- 连接到交换机 N9K-A 的 10 Gb 链路
- 连接到交换机 N9K-B 的 10 Gb 链路
- 带内管理（主动 - 被动绑定）：
    - 1 GB 到管理交换机 N9K-A 的链路
    - 1 GB 到管理交换机 N9K-B 的链路
- 通过 Cisco MDS 交换机实现 32 Gb FC 端到端连接；配置了单个启动程序分区
- FC SAN 启动可完全实现无状态计算；服务器从 AFF 存储集群上托管的启动卷中的 LUN 启动
- 所有 MEDITECH 工作负载都托管在 FC LUN 上，这些 LUN 分布在存储控制器节点上

主机软件

必须安装以下软件：

- ESXi 安装在 Cisco UCS 刀片式服务器上
- 已安装并配置 VMware vCenter （已在 vCenter 中注册所有主机）
- 已在 VMware vCenter 中安装并注册 VSC
- 已配置 NetApp 集群

"接下来： Cisco UCS 刀片式服务器和交换机配置。"

Cisco UCS 刀片式服务器和交换机配置

适用于 MEDITECH 的 FlexPod 软件在各个级别均具有容错功能。系统中没有单点故障。为了获得最佳性能， Cisco 建议使用热备用刀片式服务器。

本文档提供了有关为 MEDITECH 软件配置 FlexPod 环境的高级指导。在本节中，我们将简要介绍一些步骤以及一些示例，以准备 FlexPod 配置中的 Cisco UCS 计算平台要素。本指南的前提条件是，按照中的说明对 FlexPod 配置进行机架安装，供电和布线 "使用 VMware vSphere 6.5 Update 1 ， NetApp AFF A 系列和 Cisco UCS Manager 3.2 的采用光纤通道存储的 FlexPod 数据中心"CVD 。

Cisco Nexus 交换机配置

为解决方案部署了一对容错 Cisco Nexus 9300 系列以太网交换机。您应按照中所述为这些交换机布线 "布线图" 部分。Cisco Nexus 配置有助于确保为 MEDITECH 应用程序优化以太网流量。

1. 完成初始设置和许可后，运行以下命令在两台交换机上设置全局配置参数：

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
port-channel load-balance src-dst l4port
ntp server <global-ntp-server-ip> use-vrf management
ntp master 3
ip route 0.0.0.0/0 <ib-mgmt-vlan-gateway>
copy run start
```

2. 使用全局配置模式在每个交换机上为解决方案创建 VLAN：

```
vlan <ib-mgmt-vlan-id>
name IB-MGMT-VLAN
vlan <native-vlan-id>
name Native-VLAN
vlan <vmotion-vlan-id>
name vMotion-VLAN
vlan <vm-traffic-vlan-id>
name VM-Traffic-VLAN
vlan <infra-nfs-vlan-id>
name Infra-NFS-VLAN
exit
copy run start
```

3. 创建网络时间协议（NTP）分发接口，端口通道，端口通道参数和端口说明以进行故障排除 "使用 VMware vSphere 6.5 Update 1， NetApp AFF A 系列和 Cisco UCS Manager 3.2 的采用光纤通道存储的 FlexPod 数据中心"CVD 。

Cisco MDS 9132T 配置

Cisco MDS 9100 系列 FC 交换机可在 NetApp AFF A200 或 AFF A300 控制器与 Cisco UCS 计算网络结构之间提供 32 Gb 冗余 FC 连接。您应按照中所述连接这些缆线 "布线图" 部分。

1. 从每个 MDS 交换机的控制台上，运行以下命令以启用解决方案所需的功能：

```
configure terminal
feature npiv
feature fport-channel-trunk
```

2. 按照中的 FlexPod Cisco MDS 交换机配置部分配置各个端口，端口通道和说明 "采用 FC Cisco 验证设计的 FlexPod 数据中心"。
3. 要为解决方案创建所需的虚拟 SAN （VSAN），请在全局配置模式下完成以下步骤：
   a. 对于 Fabric-A MDS 交换机，运行以下命令：

```
vsan database
vsan <vsan-a-id>
vsan <vsan-a-id> name Fabric-A
exit
zone smart-zoning enable vsan <vsan-a-id>
vsan database
vsan <vsan-a-id> interface fc1/1
vsan <vsan-a-id> interface fc1/2
vsan <vsan-a-id> interface port-channel110
vsan <vsan-a-id> interface port-channel112
```

命令最后两行中的端口通道编号是在使用参考文档配置各个端口，端口通道和说明时创建的。

b. 对于 Fabric-B MDS 交换机，运行以下命令：

```
vsan database
vsan <vsan-b-id>
vsan <vsan-b-id> name Fabric-B
exit
zone smart-zoning enable vsan <vsan-b-id>
vsan database
vsan <vsan-b-id> interface fc1/1
vsan <vsan-b-id> interface fc1/2
vsan <vsan-b-id> interface port-channel111
vsan <vsan-b-id> interface port-channel113
```

命令最后两行中的端口通道编号是在使用参考文档配置各个端口，端口通道和说明时创建的。

4. 对于每个 FC 交换机，请使用参考文档中的详细信息创建设备别名，以便在日常操作中直观地识别每个设备。
5. 最后，使用在步骤 4 中为每个 MDS 交换机创建的设备别名创建 FC 分区，如下所示：
   a. 对于 Fabric-A MDS 交换机，运行以下命令：

```
configure terminal
zone name VM-Host-Infra-01-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-01-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zone name VM-Host-Infra-02-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-02-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zoneset name Fabric-A vsan <vsan-a-id>
member VM-Host-Infra-01-A
member VM-Host-Infra-02-A
exit
zoneset activate name Fabric-A vsan <vsan-a-id>
exit
show zoneset active vsan <vsan-a-id>
```

b. 对于 Fabric-B MDS 交换机，运行以下命令：

```
configure terminal
zone name VM-Host-Infra-01-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-01-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zone name VM-Host-Infra-02-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-02-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zoneset name Fabric-B vsan <vsan-b-id>
member VM-Host-Infra-01-B
member VM-Host-Infra-02-B
exit
zoneset activate name Fabric-B vsan <vsan-b-id>
exit
show zoneset active vsan <vsan-b-id>
```

Cisco UCS 配置指南

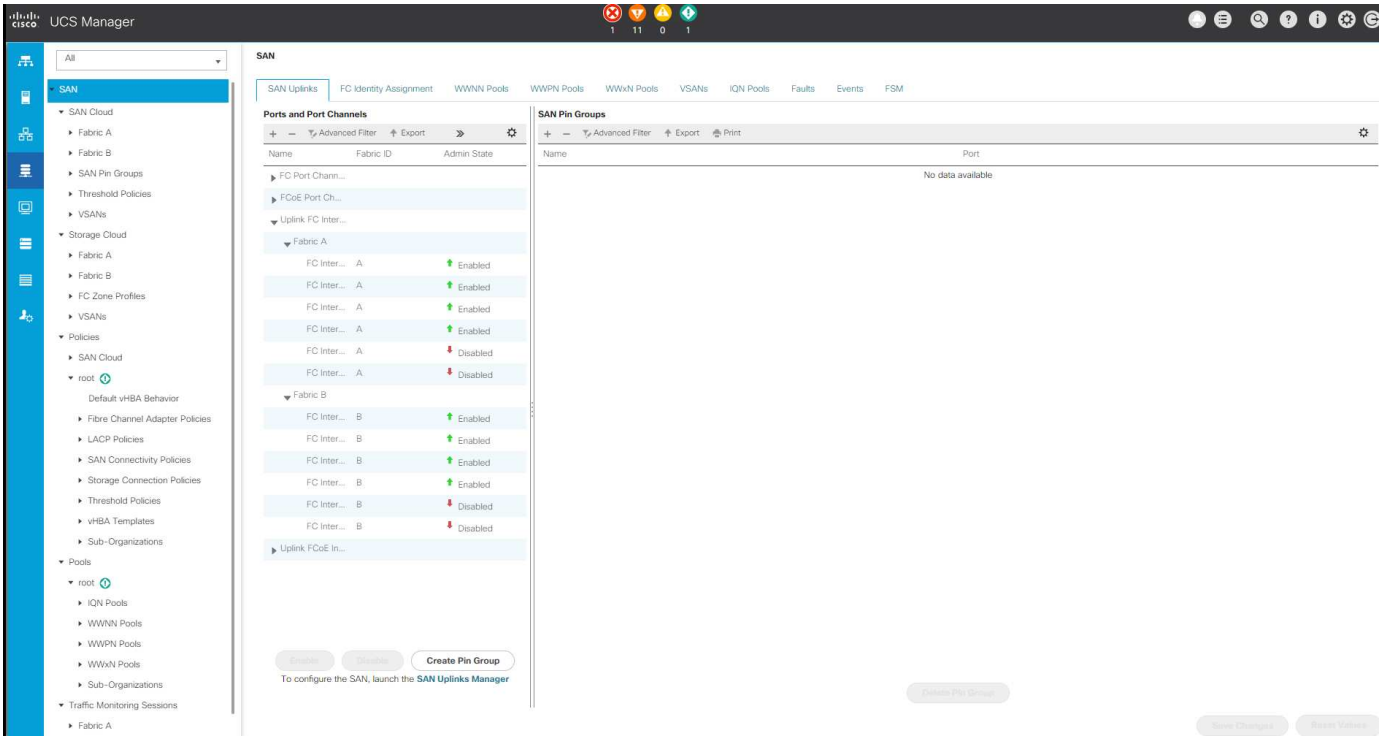
作为 MEDITECH 客户，您可以利用网络，存储和计算领域的主题专家来创建策略和模板，以便根据您的特定需求定制环境。创建这些策略和模板后，可以将这些策略和模板组合到服务配置文件中，以便为 Cisco 刀片式服务

器和机架式服务器提供一致，可重复，可靠且快速的部署。

Cisco UCS 提供了三种管理 Cisco UCS 系统的方法，称为域：

- Cisco UCS Manager HTML5 图形用户界面
- Cisco UCS 命令行界面
- 适用于多域环境的 Cisco UCS Central

下图显示了 Cisco UCS Manager 中 SAN 节点的屏幕截图示例。



在大型部署中，可以构建独立的 Cisco UCS 域，以便在主要的 MEDITECH 功能组件级别实现更强的容错能力。

在具有两个或更多数据中心的高度容错设计中， Cisco UCS Central 在设置全局策略和全局服务配置文件以确保整个企业内主机之间的一致性方面发挥着关键作用。

要设置 Cisco UCS 计算平台，请完成以下过程。在 Cisco UCS 5108 AC 刀片式服务器机箱中安装 Cisco UCS B200 M5 刀片式服务器后，请执行以下步骤。此外，您还必须与中所述的布线要求进行竞争 "布线图" 部分。

1. 将 Cisco UCS Manager 固件升级到 3.2 （ 2f ）或更高版本。
2. 配置域的报告， Cisco 自动通报功能和 NTP 设置。
3. 在每个互联阵列上配置服务器和上行链路端口。
4. 编辑机箱发现策略。
5. 创建用于带外管理的地址池，通用唯一标识符（ UUID ）， MAC 地址，服务器，全球通用节点名称（ WWNN ）和全球通用端口名称（ WWPN ）。
6. 创建以太网和 FC 上行链路端口通道和 VSAN 。
7. 为 SAN 连接，网络控制，服务器池资格认定，电源控制，服务器 BIOS 创建策略 和默认维护。

8. 创建 vNIC 和 vHBA 模板。
9. 创建 vMedia 和 FC 启动策略。
10. 为每个 MEDITECH 平台元素创建服务配置文件模板和服务配置文件。
11. 将服务配置文件与相应的刀片式服务器相关联。

有关为 FlexPod 配置 Cisco UCS 服务配置文件中每个关键要素的详细步骤，请参见 "使用 VMware vSphere 6.5 Update 1 ， NetApp AFF A 系列和 Cisco UCS Manager 3.2 的采用光纤通道存储的 FlexPod 数据中心"CVD 文档。

"下一步： ESXi 配置最佳实践。"

ESXi 配置最佳实践

对于 ESXi 主机端配置，按照运行任何企业数据库工作负载的方式配置 VMware 主机：

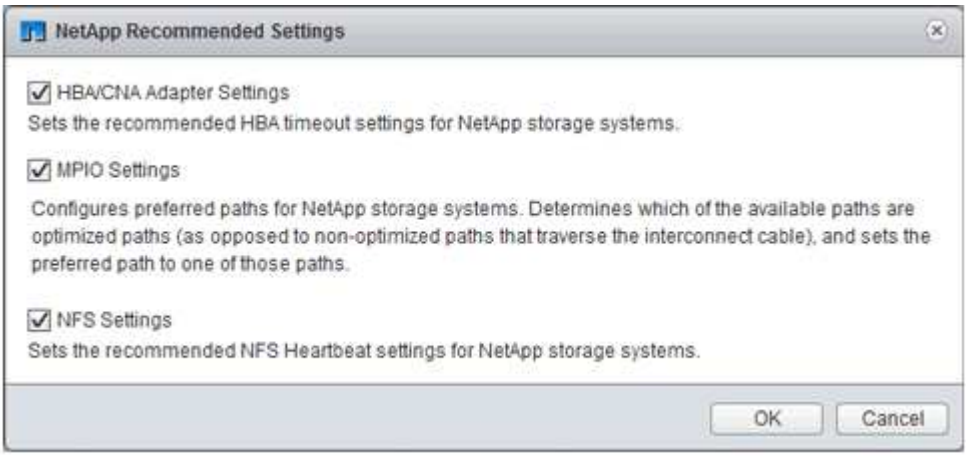
- 适用于 VMware vSphere 的 VSC 会检查并设置最适合 NetApp 存储系统的 ESXi 主机多路径设置和 HBA 超时设置。VSC 设置的值基于 NetApp 的严格内部测试。
- 要获得最佳存储性能，请考虑使用支持 VMware vStorage API - 阵列集成（ VAAI ）的存储硬件。适用于 VAAI 的 NetApp 插件是一个软件库，它集成了 ESXi 主机上安装的 VMware 虚拟磁盘库。通过 VMware VAAI 软件包，可以将某些任务从物理主机卸载到存储阵列。

  您可以在阵列级别执行精简配置和硬件加速等任务，以减少 ESXi 主机上的工作负载。副本卸载功能和空间预留功能可提高 VSC 操作的性能。您可以从 NetApp 支持站点下载此插件安装包并获取此插件的安装说明。

  VSC 可设置 ESXi 主机超时，多路径设置和 HBA 超时设置以及其他值，以实现最佳性能并成功对 NetApp 存储控制器进行故障转移。请按照以下步骤操作：

  a. 从 VMware vSphere Web Client 主页页面中，选择 vCenter > 主机。
  b. 右键单击某个主机，然后选择操作 > NetApp VSC > 设置建议值。
  c. 在 NetApp 建议设置对话框中，选择最适合您的系统的值。

     默认情况下会设置标准建议值。



  a. 单击确定。

"下一步： NetApp 配置。"

NetApp 配置

为 MEDITECH 软件环境部署的 NetApp 存储使用高可用性对配置中的存储控制器。必须通过 FC 协议将存储从两个控制器提供给 MEDITECH 数据库服务器。此配置可提供两个控制器的存储，以便在正常操作期间均匀平衡应用程序负载。

ONTAP 配置

本节介绍使用相关 ONTAP 命令的部署和配置过程示例。重点是展示如何配置存储以实施 NetApp 建议的存储布局，该布局使用高可用性控制器对。ONTAP 的主要优势之一是能够在不影响现有高可用性对的情况下进行横向扩展。

ONTAP 许可证

设置存储控制器后，应用许可证以启用 NetApp 建议的 ONTAP 功能。MEDITECH 工作负载的许可证包括 FC ， CIFS 和 NetApp Snapshot ， SnapRestore ， FlexClone ， 和 SnapMirror 技术。

要配置许可证，请打开 NetApp ONTAP 系统管理器，转至配置许可证，然后添加相应的许可证。

或者，也可以使用命令行界面运行以下命令来添加许可证：

```
license add -license-code <code>
```

AutoSupport 配置

NetApp AutoSupport 工具可通过 HTTPS 向 NetApp 发送摘要支持信息。要配置 AutoSupport ，请运行以下 ONTAP 命令：

```
autosupport modify -node * -state enable
autosupport modify -node * -mail-hosts <mailhost.customer.com>
autosupport modify -node prod1-01 -from prod1-01@customer.com
autosupport modify -node prod1-02 -from prod1-02@customer.com
autosupport modify -node * -to storageadmins@customer.com
autosupport modify -node * -support enable
autosupport modify -node * -transport https
autosupport modify -node * -hostnamesubj true
```

硬件辅助接管配置

在每个节点上，启用硬件辅助接管，以便在发生控制器故障的情况下尽可能地缩短启动接管所需的时间。要配置硬件辅助接管，请完成以下步骤：

1. 将以下 ONTAP 命令运行到 xxx 。

   将配对地址选项设置为 `prod1-01` 的管理端口的 IP 地址。

```
MEDITECH::> storage failover modify -node prod1-01 -hwassist-partner-ip
<prod1-02-mgmt-ip>
```

2. 将以下 ONTAP 命令运行到 xxx：

   将配对地址选项设置为 `cluster1-02` 的管理端口的 IP 地址。

```
MEDITECH::> storage failover modify -node prod1-02 -hwassist-partner-ip
<prod1-01-mgmt-ip>
```

3. 运行以下 ONTAP 命令，在 `prod1-01` 和 `prod1-02` HA 控制器对上启用硬件辅助接管。

```
MEDITECH::> storage failover modify -node prod1-01 -hwassist true
MEDITECH::> storage failover modify -node prod1-02 -hwassist true
```

"下一步：聚合配置。"

聚合配置

NetApp RAID DP

NetApp 建议将 NetApp RAID DP 技术作为 NetApp FAS 或 AFF 系统中所有聚合的 RAID 类型，包括常规 NetApp Flash Pool 聚合。Meditech 文档可能会指定使用 RAID 10 ，但 MEDITECH 已批准使用 RAID DP 。

RAID 组大小和 RAID 组数量

默认 RAID 组大小为 16 。此大小对于特定站点的 MEDITECH 主机的聚合可能是最佳的，也可能不是最佳的。有关 NetApp 建议在 RAID 组中使用的磁盘数量，请参见 "NetApp TR-3838：《存储子系统配置指南》"。

RAID 组大小对于存储扩展非常重要，因为 NetApp 建议您将磁盘添加到一个聚合中，该聚合包含一个或多个与 RAID 组大小相等的磁盘组。RAID 组的数量取决于数据磁盘的数量和 RAID 组的大小。要确定所需的数据磁盘数量，请使用 NetApp System Performance Modeler （ SPM ）规模估算工具。确定数据磁盘数量后，请调整 RAID 组大小，以将奇偶校验磁盘数量降至每个磁盘类型的 RAID 组大小建议范围内。

有关如何在 MEDITECH 环境中使用 SPM 规模估算工具的详细信息，请参见 "NetApp TR-4190：《适用于 MEDITECH 环境的 NetApp 规模估算准则》"。

存储扩展注意事项

扩展包含更多磁盘的聚合时，请添加组中与聚合 RAID 组大小相等的磁盘。遵循此方法有助于在整个聚合中提供性能一致性。

例如，要向 RAID 组大小为 20 的聚合添加存储， NetApp 建议添加的磁盘数为一个或多个 20 磁盘组。因此，您应添加 20 ， 40 ， 60 等磁盘。

扩展聚合后，您可以通过在受影响的卷或聚合上运行重新分配任务来将现有数据条带分布到新磁盘上来提高性能。此操作非常有用，尤其是在现有聚合接近全满时。

您应计划在非生产时间重新分配计划，因为这是一项 CPU 和磁盘密集型任务。

有关在聚合扩展后使用重新分配的详细信息，请参见 "NetApp TR-3929 ：《重新分配最佳实践指南》"。

聚合级 Snapshot 副本

将聚合级别的 NetApp Snapshot 副本预留设置为零并禁用默认聚合 Snapshot 计划。如果可能，请删除任何已存在的聚合级别 Snapshot 副本。

"下一步： Storage Virtual Machine 配置。"

Storage Virtual Machine 配置

本节介绍在 ONTAP 8.3 及更高版本上部署的相关信息。

Storage Virtual Machine （ SVM ）在 ONTAP API 和 ONTAP 命令行界面中也称为 Vserver 。

用于 MEDITECH 主机 LUN 的 SVM

您应为每个 ONTAP 存储集群创建一个专用 SVM ，以便拥有和管理包含 MEDITECH 主机的 LUN 的聚合。

SVM 语言编码设置

NetApp 建议您为所有 SVM 设置语言编码。如果在创建 SVM 时未指定语言编码设置，则使用默认语言编码设置。对于 ONTAP ，默认语言编码设置为 C.UTF-8 。设置语言编码后，您将无法稍后修改带有无限卷的 SVM 的语言。

与 SVM 关联的卷将继承 SVM 语言编码设置，除非您在创建卷时明确指定其他设置。要使某些操作正常运行，您应在站点的所有卷中一致地使用语言编码设置。例如， SnapMirror 要求源和目标 SVM 具有相同的语言编码设置。

"下一步：卷配置。"

卷配置

卷配置

专用于 MEDITECH 主机的 Meditech 卷可以采用厚配置或精简配置。

默认卷级 Snapshot 副本

Snapshot 副本是在备份工作流中创建的。每个 Snapshot 副本可用于在不同时间访问存储在 MEDITECH LUN 中的数据。经 MEDITECH 批准的备份解决方案会基于这些 Snapshot 副本创建精简配置的 FlexClone 卷，以提供 MEDITECH LUN 的时间点副本。MEDITECH 环境与经过批准的备份软件解决方案集成在一起。因此，NetApp 建议您在构成 MEDITECH 生产数据库 LUN 的每个 NetApp FlexVol 卷上禁用默认 Snapshot 副本计划。

- 重要信息： * FlexClone 卷共享父数据卷空间，因此卷必须有足够的空间来容纳 MEDITECH 数据 LUN 和备份服务器创建的 FlexClone 卷。FlexClone 卷占用的空间不像数据卷那样多。但是，如果在短时间内对 MEDITECH LUN 进行了大量删除，则克隆卷可能会增加。

每个聚合的卷数

对于使用 Flash Pool 或 NetApp Flash Cache 缓存的 NetApp FAS 系统， NetApp 建议为每个聚合配置三个或更多卷，这些卷专用于存储 MEDITECH 程序，词典和数据文件。

对于 AFF 系统， NetApp 建议为每个聚合指定四个或更多卷，用于存储 MEDITECH 程序，词典和数据文件。

卷级别重新分配计划

随着时间的推移，存储的数据布局变得不太理想，尤其是当它被诸如 MEDITECH expanse ， 6.x 和 C/S 5.x 平台等写入密集型工作负载使用时。随着时间的推移，这种情况可能会增加顺序读取延迟，从而导致完成备份的时间更长。数据布局或碎片化不良也会影响写入延迟。您可以使用卷级别重新分配来优化磁盘上的数据布局，以改善写入延迟和顺序读取访问。经过改进的存储布局有助于在分配的 8 小时时间内完成备份。

最佳实践
NetApp 建议您至少实施每周卷重新分配计划，以便在分配的维护停机时间或生产站点的非高峰时段运行重新分配操作。 NetApp 强烈建议您在每个控制器上一次对一个卷运行重新分配任务。

有关为生产数据库存储确定适当的卷重新分配计划的详细信息，请参见中的第 3.12 节 "NetApp TR-3929 ：《重新分配最佳实践指南》"。该节还将指导您如何为繁忙站点创建每周重新分配计划。

"下一步： LUN 配置。"

LUN 配置

环境中的 MEDITECH 主机数量决定了在 NetApp FAS 或 AFF 系统中创建的 LUN 数量。硬件配置建议用于指定每个 LUN 的大小。

LUN 配置

专用于 MEDITECH 主机的 Meditech LUN 可以采用厚配置或精简配置。

LUN 操作系统类型

要正确对齐创建的 LUN ，必须正确设置 LUN 的操作系统类型。未对齐的 LUN 会产生不必要的写入操作开销，并且更正错位的 LUN 会产生高昂的成本。

MEDITECH 主机服务器通常使用 VMware vSphere 虚拟机管理程序在虚拟化的 Windows Server 环境中运行。主机服务器也可以在裸机服务器上的 Windows Server 环境中运行。要确定要设置的正确操作系统类型值，请参阅的 "LUN 创建 " 一节 "《集群模式 Data ONTAP 8.3 命令：手册页参考》"。

LUN 大小

要确定每个 MEDITECH 主机的 LUN 大小，请参见 MEDITECH 提供的硬件配置建议（新部署）或硬件评估任务（现有部署）文档。

LUN 显示

Meditech 要求使用 FC 协议将程序，词典和数据文件的存储作为 LUN 提供给 MEDITECH 主机。在 VMware 虚拟环境中， LUN 会提供给托管 MEDITECH 主机的 VMware ESXi 服务器。然后，在物理兼容模式下使用 RDM 将呈现给 VMware ESXi 服务器的每个 LUN 映射到每个 MEDITECH 主机 VM 。

您应使用适当的 LUN 命名约定将 LUN 呈现给 MEDITCH 主机。例如，为了便于管理，您必须将 LUN `MTFS01E` 提供给 MEDITECH 主机 `mt-host-01` 。

在向 MEDITECH 和备份系统安装程序咨询以为 MEDITECH 主机使用的 LUN 设计一致的命名约定时，请参见 MEDITECH 硬件配置提案。

例如， MEDITECH LUN 名称是 `MTFS05E` ，其中：

- `mTFS` 表示 MEDITECH 文件服务器（对于 MEDITECH 主机）。
- `05` 表示主机编号 5 。
- `E` 表示 Windows E 驱动器。

"下一步：启动程序组配置。"

启动程序组配置

使用 FC 作为数据网络协议时，请在每个存储控制器上创建两个启动程序组（ igroup ）。第一个 igroup 包含托管 MEDITECH 主机 VM 的 VMware ESXi 服务器上 FC 主机接口卡的 WWPN （对于 MEDITECH 为 igroup ）。

您必须根据环境设置设置 MEDITECH igroup 操作系统类型。例如：

- 对于 Windows Server 环境中裸机服务器硬件上安装的应用程序，请使用 igroup 操作系统类型 `Windows` 。
- 对于使用 VMware vSphere 虚拟机管理程序进行虚拟化的应用程序，请使用 igroup 操作系统类型 `VMware` 。

> igroup 的操作系统类型可能与 LUN 的操作系统类型不同。例如，对于虚拟化的 MEDITECH 主机，您应将 igroup 操作系统类型设置为 `vmware` 。对于虚拟化 MEDITECH 主机使用的 LUN ，应将操作系统类型设置为 `Windows 2008` 或更高版本 。请使用此设置，因为 MEDITECH 主机操作系统是 Windows Server 2008 R2 64 位企业版。

要确定正确的操作系统类型值，请参见中的 "LUN igroup Create" 和 "LUN Create" 两节 "《集群模式 Data ONTAP 8.2 命令：手册页参考》"。

"下一步： LUN 映射。"

LUN 映射

创建 LUN 时会为 MEDITECH 主机建立 LUN 映射。

Meditech 模块和组件

MEDITECH 应用程序涵盖多个模块和组件。下表列出了这些模块所涵盖的功能。有关追加

信息设置和部署这些模块的信息，请参见 MEDITECH 文档。

功能	Type
连接	• Web 服务器 • 实时应用程序服务器（ Wi — Web 集成） • 测试应用程序服务器（ Wi ） • SAML 身份验证服务器（ Wi ） • SAML 代理服务器（ Wi ） • 数据库服务器
基础架构	• 文件服务器 • 后台作业客户端 • 连接服务器 • 事务服务器
扫描和归档	• 映像服务器
数据存储库	• SQL 服务器
业务和临床分析	• 实时智能服务器（ BCA ） • 测试智能服务器（ BCA ） • 数据库服务器（ BCA ）
家庭护理	• 远程站点解决方案 • 连接 • 基础架构 • 打印 • 现场设备 • 扫描 • 托管站点要求 • 防火墙配置
支持	• 后台作业客户端（ CAL —客户端访问许可证）
用户设备	• 平板电脑 • 固定设备

功能	Type
打印	• 实时网络打印服务器（必需；可能已存在） • 测试网络打印服务器（必需；可能已存在）
第三方要求	• 首款 Databank （ FDB ）医疗知识框架 v4.3

致谢

以下人员为本指南的创建做出了贡献。

- NetApp 技术营销工程师布兰登 · 阿吉
- NetApp 技术营销工程师 Atul Bhalodia
- NetApp 高级产品经理 Ketan Mota
- NetApp 医疗保健解决方案架构师 John Duignan
- Cisco 公司 Jon Ebmeier
- Cisco 公司 Mike Brennan

从何处查找追加信息

要了解有关本文档所述信息的更多信息，请查看以下文档或网站：

FlexPod 设计区域

- "FlexPod 设计区域"
- "使用 NetApp AFF ， vSphere 6.5U1 和 Cisco UCS Manager 的具有 FC 存储（ MDS 交换机）的 FlexPod 数据中心"

NetApp 技术报告

- "TR-3929 ：《重新分配最佳实践指南》"
- "TR-3987 ：适用于 InterSystems Cach 的 Snap Creator Framework 插件"
- "TR-4300i ：《适用于 MEDITECH 环境的 NetApp FAS 和全闪存存储系统最佳实践指南》"
- "TR-4017 ：《 FC SAN 最佳实践》"
- "TR-3446 ：《 SnapMirror 异步概述和最佳实践指南》"

ONTAP 文档

- "NetApp 产品文档"
- "适用于 vSphere 的 Virtual Storage Console （ VSC ）文档"
- "ONTAP 9 文档中心"：
  - "适用于 ESXi 的 FC 快速指南"

- "所有 ONTAP 9.3 文档"：
  - "软件设置指南"
  - "磁盘和聚合高级指南"
  - "《 SAN 管理指南》"
  - "《 SAN 配置指南》"
  - "《适用于 Windows 的 FC 配置快速指南》"
  - "《 FC SAN 优化的 AFF 设置指南》"
  - "《 High-Availability 配置指南》"
  - "《逻辑存储管理指南》"
  - "性能管理高级指南"
  - "《 SMB/CIFS 配置高级指南》"
  - "SMB/CIFS 参考"
  - "数据保护高级指南"
  - "《数据保护磁带备份和恢复指南》"
  - "《 NetApp 加密高级指南》"
  - "《网络管理指南》"
  - "命令：《 ONTAP 9.3 手册页参考》"

《 **Cisco Nexus ， MDS ， Cisco UCS** 和 **Cisco UCS Manager** 指南》

- "Cisco UCS 服务器概述"
- "Cisco UCS 刀片式服务器概述"
- "Cisco UCS B200 M5 产品规格"
- "Cisco UCS Manager 概述"
- "Cisco UCS Manager 3.2 （ 3a ）基础架构捆绑包" （需要 Cisco.com 授权）
- "Cisco Nexus 9300 平台交换机"
- "Cisco MDS 9132T FC 交换机"

适用于医疗成像的 FlexPod

TR-4865： 适用于医疗成像的 FlexPod

NetApp 公司 Jaya Kishore Esanakula 和 Atul Bhalodia

医疗成像占医疗保健组织生成的所有数据的 70% 。随着数字模式的不断发展以及新模式的出现，数据量将继续增加。例如，从模拟病理学向数字病理学的过渡将大幅增加图像大小，这将挑战当前实施的任何数据管理策略。

COVID-19 显然重塑了数字化转型；据最近的一项调查显示 "report"， COVID-19 将数字商务加速了 5 年。问题

解决者推动的技术创新正在从根本上改变我们的日常生活方式。这一技术驱动的变革将彻底改变我们生活中的许多关键方面，包括医疗保健。

医疗保健行业有望在未来几年发生重大变化。COVID 正在加速医疗保健领域的创新，将推动行业发展至少几年。这一变化的核心是，需要在不影响可靠性的情况下提高医疗保健的经济性，可用性和可访问性，从而使医疗保健在处理流行病方面更加灵活。

这一医疗保健变革的基础是一个精心设计的平台。衡量平台的一个关键指标是，平台变更的实施是否容易。速度是新的扩展，数据保护不会受到影响。全球一些最关键的数据正由为临床医生提供支持的临床系统创建和使用。NetApp 已在临床医生需要的地方，内部，云端或混合环境中为患者提供关键数据。混合多云环境是当前 IT 架构最先进的环境。

众所周知，医疗保健是围绕提供商（医生，护士，放射科医生，医疗设备技术人员等）和患者进行的。随着我们将患者和提供商紧密联系在一起，使地理位置成为一个数据点，当提供商和患者需要时，提供底层平台变得更加重要。该平台必须长期高效且经济高效。他们努力降低患者护理成本， "负责的护理组织" （ ACoS ）将通过一个高效的平台来实现。

对于医疗保健组织所使用的健康信息系统，构建与购买问题往往只涉及一个问题解答：购买。这可能是出于许多主观原因。多年的购买决策可以创建异构信息系统。每个系统都有一组特定的部署平台要求。最重要的问题描述是信息系统所需的多种大型存储协议和性能级别，这使得平台标准化和最佳运营效率成为一项重大挑战。医疗保健组织不能专注于任务关键型问题，因为它们的注意力分散在一些琐碎的运营需求上，例如需要多种技能和 SME 保留能力的大型平台上。

这些挑战可分为以下几类：

- 异构存储需求
- 部门孤岛
- IT 运营复杂性
- 云连接
- 网络安全
- 人工智能和深度学习

借助 FlexPod ，您可以从一个平台获得一个支持 FC ， FCoE ， iSCSI ， NFS/pNFS ， SMB/CIFS 等的平台。人员，流程和技术是 FlexPod 设计和构建的基因的一部分。FlexPod 自适应 QoS 可在同一底层 FlexPod 平台上支持多个任务关键型临床系统，从而有助于细分部门孤岛。FlexPod 已通过 FedRAMP 认证和 FIPS 140-2 认证。此外，医疗保健组织还面临着人工智能和深度学习等机会。FlexPod 和 NetApp 解决了这些难题，并在标准平台中的内部环境或混合多云环境中按需提供数据。有关详细信息和一系列客户成功案例，请参见 "FlexPod 医疗保健"。

典型的医学影像信息和 PACS 系统具有以下功能集：

- 接收和注册
- 计划
- 映像
- 记录
- 管理
- 数据交换

- 映像归档
- 为技术人员提供图像查看功能，用于图像采集和读取，并为临床医生提供图像查看功能

在成像方面，医疗保健部门正在努力解决以下临床挑战：

- 更广泛地采用 "自然语言处理" （ NLP ）辅助技术人员和医生执行图像读取。放射部门可以从语音识别到记录报告中受益。NLP 可用于识别患者的记录并将其匿名化，尤其是嵌入在 Dicom 图像中的 Dicom 标记。NLP 功能需要高性能平台以及低延迟响应时间来处理映像。FlexPod QoS 不仅可以提供高性能，还可以为未来的增长提供成熟的容量预测。
- ACoS 和社区健康组织更广泛地采用标准化的临床途径和协议。以往，临床路径一直是一组静态准则，而不是一个用于指导临床决策的集成工作流。随着 NLP 和图像处理的进步，可以将图像中的 Dicom 标记作为事实集成到临床路径中，以推动临床决策。因此，这些流程需要底层基础架构平台和存储系统的高性能，低延迟和高吞吐量。
- 利用卷积神经网络的 ML 模型可以实时实现图像处理功能的自动化，因此需要支持 GPU 的基础架构。FlexPod 提供了内置于同一系统中的 CPU 和 GPU 计算组件，并且 CPU 和 GPU 可以彼此独立扩展。
- 如果在临床最佳实践建议中将 Dicom 标记用作事实，则系统必须以低延迟和高吞吐量执行更多的 Dicom 项目读取。
- 在评估图像时，各组织的放射科医生之间的实时协作要求最终用户计算设备中具有高性能的图形处理能力。NetApp 提供行业领先的 VDI 解决方案，这些解决方案专为高端图形使用情形而设计并经过验证。有关详细信息，请参见 "此处"。
- 在整个 ACO 运行状况组织中，无论映像的记录系统如何，都可以使用一个平台来管理图像和介质，方法是使用医学数字成像和通信等协议（ "Dicom"）和对持续使用 DICOM- 的对象的 Web 访问（ "WADO"）
- 运行状况信息交换（ "HIE"）包括消息中嵌入的图像。
- 移动设备，例如手持式，无线扫描设备（例如，连接到手机的便携手持式超声波扫描仪），需要一个强大的网络基础架构，在边缘，核心和云端都具有 DoD 级别的安全性，可靠性和延迟。 "NetApp 支持的数据网络结构" 为企业大规模提供此功能。
- 较新的模式具有指数级存储需求；例如， CT 和 MRI 对于每个模式都需要几百 MB 的容量，但数字病理学图像（包括整个幻灯片成像）的大小可能只有几 GB 。FlexPod 的设计采用 "性能，可靠性和扩展是基本特征"。

精心设计的医疗成像系统平台是创新的核心。FlexPod 架构提供灵活的计算和存储功能以及行业领先的存储效率。

解决方案的整体优势

通过在 FlexPod 架构基础上运行映像应用程序环境，您的医疗保健组织可以看到员工工作效率的提高以及资本和运营支出的降低。FlexPod 提供经过严格测试，预先验证和融合的产品，经过精心设计和设计，可提供可预测的低延迟系统性能和高可用性。这种方法可为医疗成像系统的用户带来较高的舒适程度，并最终实现最佳的响应时间。

映像系统的不同组件可能需要将数据存储在 SMB/CIFS ， NFS ， ext4 或 NTFS 文件系统中。这一要求意味着基础架构必须通过 NFS ， SMB/CIFS 和 SAN 协议提供数据访问。一个 NetApp 存储系统可以支持 NFS ， SMB/CIFS 和 SAN 协议，因此不再需要传统的协议专用存储系统。

FlexPod 基础架构是一个模块化，融合，虚拟化，可扩展（横向扩展和纵向扩展）且经济高效的平台。借助 FlexPod 平台，您可以独立横向扩展计算，网络和存储，加快应用程序部署速度。模块化架构支持无中断运行，即使在系统横向扩展和升级活动期间也是如此。

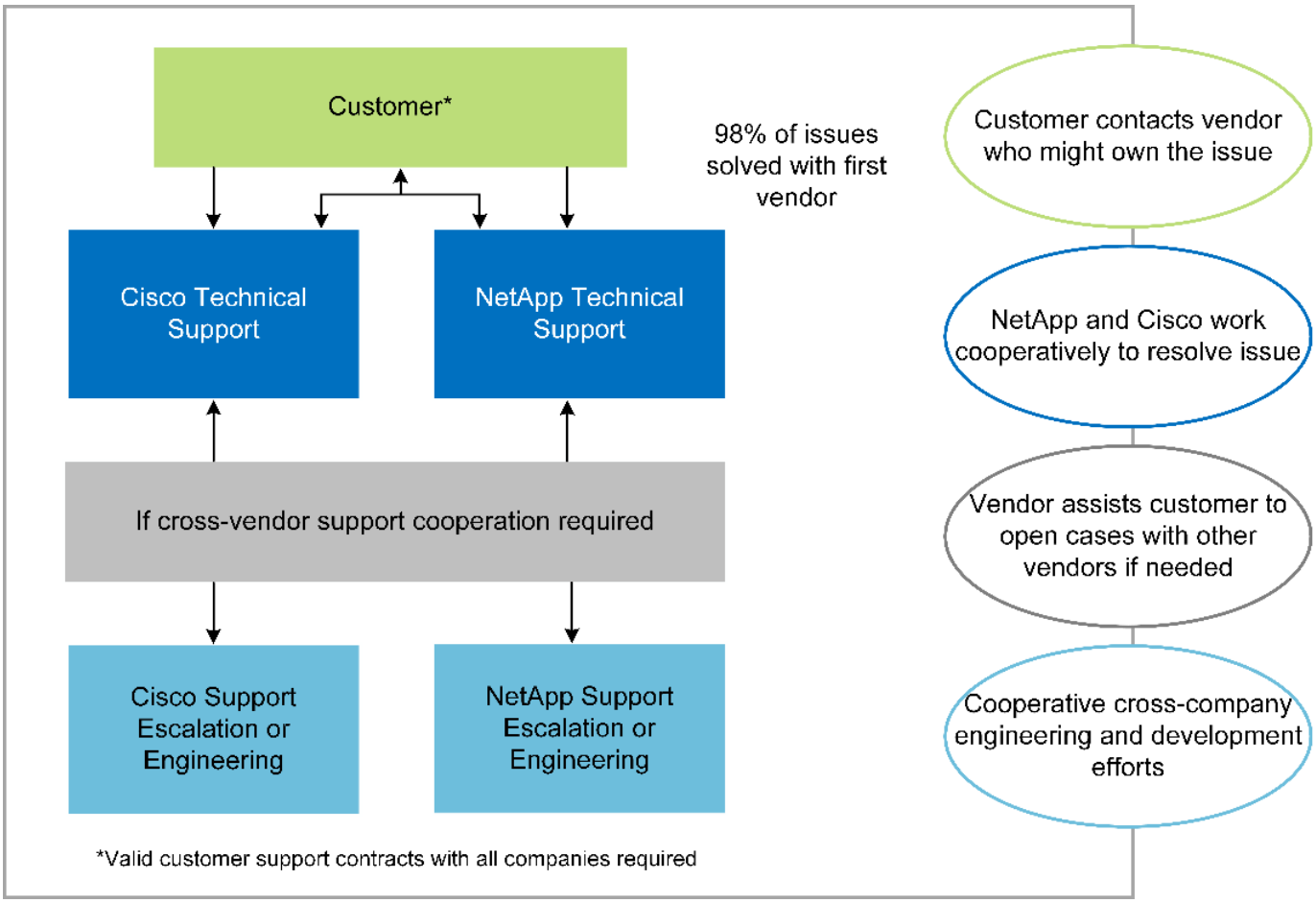
FlexPod 提供了医疗成像行业特有的多项优势：

- * 低延迟系统性能。 * 放射科医生时间是一种高价值资源，高效利用放射科医生的时间至关重要。等待图像或视频加载可能会导致临床医生突发，并可能影响临床医生的效率和患者安全。
- * 模块化架构。 * FlexPod 组件通过集群服务器，存储管理网络结构和综合管理工具集进行连接。随着成像设施的逐年增长以及研究次数的增加，底层基础架构也需要相应地进行扩展。FlexPod 可以独立扩展计算，存储和网络。
- * 更快地部署基础架构。 * 无论位于现有数据中心还是远程位置， FlexPod 数据中心与医疗成像的集成和测试设计都能帮助您以更少的工作量在更短的时间内启动和运行新基础架构。
- * 加速应用程序部署。 * 经过预先验证的架构可减少任何工作负载的实施集成时间和风险， NetApp 技术可自动部署基础架构。无论您是使用解决方案首次推出医疗映像，硬件更新还是扩展，您都可以将更多资源转移到项目的业务价值上。
- * 简化操作并降低成本。 * 您可以将原有专有平台替换为更高效，可扩展的共享资源，以满足工作负载的动态需求，从而消除其成本和复杂性。此解决方案可提高基础架构资源利用率，从而提高投资回报率（ ROI ）。
- * 横向扩展架构。 * 您无需重新配置正在运行的应用程序，即可将 SAN 和 NAS 从 TB 扩展到数十 PB 。
- * 无中断运行。 * 您可以在不中断业务的情况下执行存储维护，硬件生命周期操作和软件升级。
- * 安全多租户。 * 此优势可满足日益增长的虚拟化服务器和存储共享基础架构需求，从而可以安全地多租户特定于设施的信息，尤其是在托管多个数据库和软件实例时。
- * 池化资源优化。 * 此优势可帮助您减少物理服务器和存储控制器数量，负载平衡工作负载需求并提高利用率，同时提高性能。
- * 服务质量（ QoS ）。 * FlexPod 可在整个堆栈上提供 QoS 。这些行业领先的 QoS 存储策略可在共享环境中提供不同的服务级别。这些策略有助于优化工作负载的性能，并有助于隔离和控制失控的应用程序。
- * 使用 QoS 支持存储层 SLA 。 * 您不必为医疗映像环境通常需要的不同存储层部署不同的存储系统。一个存储集群包含多个 NetApp FlexVol 卷，并为不同的层提供特定的 QoS 策略，即可实现这一目的。通过这种方法，可以动态满足特定存储层不断变化的需求来共享存储基础架构。NetApp AFF 可以通过在 FlexVol 卷级别启用 QoS 来支持不同的存储层 SLA ，从而无需为应用程序的不同存储层使用不同的存储系统。
- * 存储效率。 * 医疗映像通常由映像应用程序预先压缩为 jpeg2k 无损压缩，压缩率约为 2.5： 1 。但是，这是特定于映像应用程序和供应商的。在大型成像应用程序环境（大于 1 PB ）中，可以节省 5-10% 的存储空间，您可以利用 NetApp 存储效率功能降低存储成本。与您的映像应用程序供应商和 NetApp 主题专家合作，释放您的医疗映像系统潜在的存储效率。
- * 灵活性。 * 借助 FlexPod 系统提供的行业领先的工作流自动化，流程编排和管理工具，您的 IT 团队可以更快速地响应业务请求。这些业务请求包括医疗映像备份和配置额外的测试和培训环境，以及为人口健康管理计划复制分析数据库等。
- * 工作效率更高。 * 您可以快速部署和扩展此解决方案，以获得最佳临床医生最终用户体验。
- * Data Fabric 。 * 由 NetApp 提供支持的 Data Fabric 可以跨站点，跨物理边界和跨应用程序将数据集于一体。NetApp 支持的 Data Fabric 专为以数据为中心的世界中的数据驱动型企业而构建。数据在多个位置创建和使用，通常需要利用并与其他位置，应用程序和基础架构共享。因此，您需要一种一致且集成的方式来管理它。此解决方案提供了一种数据管理方式，可让您的 IT 团队掌控一切，并简化日益增加的 IT 复杂性。
- * FabricPool 。 * NetApp ONTAP FabricPool 有助于降低存储成本，而不会影响性能，效率，安全性或保护。FabricPool 对企业级应用程序是透明的，它可以降低存储 TCO ，而无需重新构建应用程序基础架构，从而充分利用云效率。FlexPod 可以从 FabricPool 的存储分层功能中受益，从而更高效地利用 ONTAP 闪存存储。有关完整信息，请参见 "采用 FabricPool 的 FlexPod"。
- * FlexPod 安全性。 * 安全性是 FlexPod 的基础。在过去几年中，勒索软件已成为一种日益严重的威胁。勒索软件是一种基于密码病毒的恶意软件，它使用加密技术构建恶意软件。此恶意软件可以使用对称密钥加密和非对称密钥加密来锁定受影响的数据，并要求勒索以提供密钥来对数据进行解密。要了解 FlexPod 如何帮助缓解勒索软件等威胁，请参见 "解决方案到勒索软件"。FlexPod 基础架构组件也是联邦信息处理标准 "（

FIPS ） 140-2" 合规。

- * FlexPod 合作支持。 * NetApp 和 Cisco 建立了 FlexPod 合作支持，这是一种强大，可扩展且灵活的支持模式，可满足 FlexPod 融合基础架构的独特支持要求。此模式结合了 NetApp 和 Cisco 的经验，资源和技术支持专业知识，可简化识别和解决 FlexPod 支持问题描述的流程，而无论问题位于何处。FlexPod 合作支持模式有助于确认您的 FlexPod 系统运行效率高，并受益于最新技术，同时还可以提供经验丰富的团队来帮助解决集成问题。

  如果您的医疗保健组织运行业务关键型应用程序， FlexPod 合作支持就显得尤为重要。下图显示了 FlexPod 合作支持模式的概述。



范围

本文档从技术角度概述了用于托管此医疗成像解决方案的 Cisco 统一计算系统（ Cisco UCS ）和基于 NetApp ONTAP 的 FlexPod 基础架构。

audience

本文档面向医疗保健行业的技术主管以及 Cisco 和 NetApp 合作伙伴解决方案工程师和专业服务人员。NetApp 假定读者已很好地了解计算和存储规模估算概念，并在技术上熟悉医疗成像系统， Cisco UCS 和 NetApp 存储系统。

医学影像应用程序

典型的医疗成像应用程序提供了一套应用程序，这些应用程序共同构成了适合中小型和大型医疗保健组织的企业

级成像解决方案。

该产品套件的核心是以下临床功能：

- 企业映像存储库
- 支持传统图像源，例如放射学和心脏病学。此外，还支持其他护理领域，例如眼科，皮肤科，柱镜检查以及照片和视频等其他医学影像对象。
- "图片归档和通信系统" （ PACS ），这是一种计算机手段，用于取代传统辐射胶片的角色
- 企业级映像供应商中立归档（ VNA ）：
  - 可扩展地整合了 Dicom 和非 Dicom 文档
  - 集中式医疗成像系统
  - 支持企业中多个（ CRS ）之间的文档同步和数据完整性
  - 通过基于规则的专家系统进行文档生命周期管理，利用文档元数据，例如：
  - 设备类型
  - 研究年限
  - 患者年龄（当前和图像采集时）
  - 企业内部和外部单点集成（ HIE ）：
  - 上下文感知文档链接
  - Health Level Seven International （ HL7 ）， Dicom 和 WADO
  - 与存储无关的归档功能
- 与使用了 HL7 和上下文感知链接的其他运行状况信息系统集成：
  - 使 EHRs 能够通过患者图表，成像工作流等实现与患者图像的直接链接。
  - 帮助将患者的纵向护理图像历史记录嵌入到 EHRs 中。
- 放射科技术人员工作流
- 企业级零占用空间查看器，可在任何功能强大的设备上从任意位置查看图像
- 利用可追溯性和实时数据的分析工具：
  - 合规性报告
  - 操作报告
  - 质量控制和质量保证报告

医疗保健组织的规模和平台规模估算

医疗保健组织可以采用基于标准的方法进行广泛分类，从而为 ACO 等计划提供帮助。其中一种分类采用临床集成网络（ CIN ）的概念。如果一组医院相互协作并遵循成熟的标准临床协议和途径来提高护理价值并降低患者成本，则可以称为 CIN 。CIN 中的医院对遵循 CIN 核心值的机上医生实施控制和实践。传统上，集成交付网络（ IDN ）仅限于医院和医生组。一个 CIN 跨越传统的 IDN 边界，一个 CIN 仍可属于一个 ACO 。根据 CIN 的原则，医疗保健组织可以分为小型，中型和大型。

小型医疗保健组织

如果医疗保健机构仅包括一家医院，并设有门诊和住院部门，则该机构规模较小，但不属于 CIN 。医生作为护理人员，在整个护理过程中协调患者护理。这些小型组织通常包括由医生运营的设施。他们可能会或不会将紧急和精神创伤护理作为患者的综合护理。通常，一家小型医疗保健组织每年执行大约 25 万次临床成像研究。成像中心被视为小型医疗保健组织，它们提供成像服务。有些组织还向其他组织提供放射科口授服务。

中型医疗保健组织

如果医疗保健组织包含多个医院系统，并以以下组织为重点，则视为中型组织：

- 成人护理诊所和成人住院医院
- 人力和交付部门
- 儿童护理诊所和儿童住院医院
- 癌症治疗中心
- 成人紧急部门
- 儿童紧急部门
- 家庭医学和初级护理办公室
- 一个成人精神创伤护理中心
- 儿童精神创伤护理中心

在中型医疗保健组织中，医生遵循 CIN 的原则，并作为一个整体运行。医院具有单独的医院，医生和药房计费功能。医院可能与学术研究机构有联系，并进行介入临床研究和试验。一家中型医疗保健组织每年执行多达 500 ， 000 次临床成像研究。

大型医疗保健组织

如果医疗保健组织具备中型医疗保健组织的特征，并向位于多个地理位置的社区提供中型临床功能，则该组织就会被视为大型组织。

大型医疗保健组织通常执行以下功能：

- 设有一个中央办公室来管理整体职能
- 与其他医院合作
- 每年与付款方组织协商费率
- 按州和地区协商付款人费率
- 参与有意义的使用（ MU ）计划
- 使用基于标准的人口健康管理（ PHM ）工具对人口健康组执行高级临床研究
- 每年执行多达 100 万次临床成像研究

一些参与 CIN 的大型医疗保健组织也具有基于 AI 的成像读取功能。这些组织通常每年执行 100 万到 200 万次临床成像研究。

在了解这些规模不同的组织如何转换为规模最佳的 FlexPod 系统之前，您应了解各种 FlexPod 组件以及 FlexPod 系统的不同功能。

FlexPod

Cisco Unified Computing System

Cisco UCS 由一个与统一 I/O 基础架构互连的管理域组成。适用于医疗成像环境的 Cisco UCS 已与 NetApp 医疗成像系统基础架构建议和最佳实践保持一致，以便该基础架构能够提供关键的患者信息并最大限度地提高可用性。

企业级医疗成像的计算基础是 Cisco UCS 技术，它具有集成的系统管理， Intel Xeon 处理器和服务器虚拟化功能。这些集成技术可以解决数据中心的难题，并帮助您通过典型的医疗成像系统实现数据中心设计目标。Cisco UCS 将 LAN ， SAN 和系统管理统一为一个简化的链路，用于连接机架式服务器，刀片式服务器和虚拟机（ VM ）。Cisco UCS 由一对冗余 Cisco UCS 互联阵列组成，可为所有 I/O 流量提供单点管理和单点控制。

Cisco UCS 使用服务配置文件，以便正确一致地配置 Cisco UCS 基础架构中的虚拟服务器。服务配置文件包括有关服务器标识的关键服务器信息，例如 LAN 和 SAN 寻址， I/O 配置，固件版本，启动顺序，网络虚拟 LAN （ VLAN ），物理端口和 QoS 策略。可以在几分钟内动态创建服务配置文件并将其与系统中的任何物理服务器关联，而无需花费数小时或数天的时间。将服务配置文件与物理服务器关联起来是一项简单的操作，可以在环境中的服务器之间迁移身份，而无需更改任何物理配置。此外，它还有助于快速裸机配置故障服务器的更换件。

使用服务配置文件有助于确认服务器在整个企业中的配置是否一致。使用多个 Cisco UCS 管理域时， Cisco UCS Central 可以使用全局服务配置文件在域之间同步配置和策略信息。如果必须在一个域中执行维护，则可以将虚拟基础架构迁移到另一个域。通过这种方法，即使一个域脱机，应用程序也会继续以高可用性运行。

Cisco UCS 是适用于刀片式服务器和机架式服务器计算的下一代解决方案。该系统将低延迟，无损的 40GbE 统一网络结构与企业级 x86 架构服务器集成在一起。该系统是一个集成的可扩展多机箱平台，其中所有资源都属于一个统一的管理域。Cisco UCS 可通过对虚拟化和非虚拟化系统的端到端配置和迁移支持，轻松，可靠，安全地加快新服务的交付。Cisco UCS 提供以下功能：

- 全面的管理
- 彻底简化
- 高性能

Cisco UCS 包含以下组件：

- * 计算。 * 该系统基于全新的计算系统，该系统采用基于 Intel Xeon 可扩展处理器产品系列的机架式服务器和刀片式服务器。
- * 网络。 * 该系统集成到低延迟，无损， 40Gbps 统一网络结构中。这一网络基础整合了 LAN ， SAN 和高性能计算网络，这些网络目前是独立的网络。统一网络结构可减少网络适配器，交换机和缆线的数量，并降低电耗和散热需求，从而降低成本。
- * 虚拟化。 * 系统通过增强虚拟环境的可扩展性，性能和操作控制，充分发挥虚拟化的潜能。Cisco 安全性，策略实施和诊断功能现已扩展到虚拟化环境中，以更好地支持不断变化的业务和 IT 需求。
- * 存储访问。 * 系统可通过统一网络结构对 SAN 存储和 NAS 进行整合访问。它也是软件定义存储的理想系统。通过将一个框架的优势相结合，在一个窗格中管理计算和存储服务器，可以在需要时实施 QoS ，以便在系统中注入 I/O 限制。此外，您的服务器管理员还可以为存储资源预先分配存储访问策略，从而简化存储连接和管理，并有助于提高工作效率。除了外部存储之外，机架和刀片式服务器都具有内部存储，可通过内置硬件 RAID 控制器访问这些存储。通过在 Cisco UCS Manager 中设置存储配置文件和磁盘配置策略，主机操作系统和应用程序数据的存储需求将由用户定义的 RAID 组来满足。因此，可用性高，性能更好。
- * 管理。 * 系统可唯一集成所有系统组件，以便 Cisco UCS Manager 将整个解决方案作为一个实体进行管理。为了管理所有系统配置和操作， Cisco UCS Manager 提供了一个直观的 GUI ，一个 CLI 以及一个基于强大 API 构建的适用于 Microsoft Windows PowerShell 的功能强大的脚本库模块。

Cisco Unified Computing System 将访问层网络和服务器结合使用。这款高性能下一代服务器系统为您的数据中心提供了高度的工作负载灵活性和可扩展性。

Cisco UCS Manager

Cisco UCS Manager 可为 Cisco UCS 中的所有软件和硬件组件提供统一的嵌入式管理。通过使用单连接技术，UCS Manager 可以管理，控制和管理数千个 VM 的多个机箱。通过直观的 GUI ， CLI 或 XML API ，管理员可以使用该软件将整个 Cisco UCS 作为一个逻辑实体进行管理。Cisco UCS Manager 位于一对 Cisco UCS 6300 系列互联阵列上，这些互联阵列使用集群模式主动 - 备用配置来实现高可用性。

Cisco UCS Manager 提供了一个统一的嵌入式管理界面，可将您的服务器，网络和存储集成在一起。Cisco UCS Manager 会执行自动发现，以检测您添加或更改的系统组件的清单，管理和配置这些组件。它提供了一组用于第三方集成的完整 XML API ，并提供了 9 ， 000 个集成点。此外，它还有助于自定义开发，以实现自动化，流程编排，并实现更高水平的系统可见性和控制。

服务配置文件既有利于虚拟化环境，也有利于非虚拟化环境。它们可以提高非虚拟化服务器的移动性，例如在将工作负载从服务器移动到服务器时，或者在使服务器脱机以进行服务或升级时。此外，您还可以将配置文件与虚拟化集群结合使用，以便轻松地将新资源联机，从而完善现有的 VM 移动性。

有关 Cisco UCS Manager 的详细信息，请参见 "Cisco UCS Manager 产品页面"。

Cisco UCS 的差异化优势

Cisco Unified Computing System 正在彻底改变数据中心服务器的管理方式。请参见以下 Cisco UCS 和 Cisco UCS Manager 的独特优势：

- * 嵌入式管理。 * 在 Cisco UCS 中，服务器由互联阵列中的嵌入式固件管理，因此无需任何外部物理或虚拟设备来管理它们。
- * 统一网络结构。 * 在 Cisco UCS 中，从刀片式服务器机箱或机架服务器到互联阵列，一根以太网缆线用于传输 LAN ， SAN 和管理流量。这种融合 I/O 可减少所需的缆线， SFP 和适配器数量，进而降低整个解决方案的资本和运营支出。
- * 自动发现。 * 只需将刀片式服务器插入机箱或将机架服务器连接到互联阵列，即可自动发现和清点计算资源，无需任何管理干预。统一网络结构和自动发现相结合，可实现 Cisco UCS 的线一次架构，在该架构中，可以轻松扩展计算功能，同时保持与 LAN ， SAN 和管理网络的现有外部连接。
- * 基于策略的资源分类。 * 如果 Cisco UCS Manager 发现计算资源，则可以根据您定义的策略将其自动分类到给定资源池。此功能在多租户云计算中非常有用。
- * 机架和刀片式服务器管理相结合。 * Cisco UCS Manager 可以在同一 Cisco UCS 域下管理 B 系列刀片式服务器和 C 系列机架式服务器。此功能以及无状态计算使计算资源真正不受硬件外形因素的限制。
- * 基于模型的管理架构。 * Cisco UCS Manager 架构和管理数据库是基于模型和数据驱动的。通过提供的开放式 XML API 可在管理模式上运行，可以轻松，可扩展地将 Cisco UCS Manager 与其他管理系统集成在一起。
- * 策略，池和模板。 * Cisco UCS Manager 中的管理方法基于定义策略，池和模板，而不是混乱的配置。它支持采用简单，松散耦合的数据驱动方法来管理计算，网络和存储资源。
- 参考完整性松散。 * 在 Cisco UCS Manager 中，服务配置文件，端口配置文件或策略可以引用其他策略或引用完整性松散的其他逻辑资源。在编写转介策略时，不能存在转介策略，但即使其他策略正在引用转介策略，也可以删除该转介策略。通过此功能，不同的主题专家可以彼此独立工作。您可以通过让来自不同领域的不同专家（例如网络，存储，安全，服务器和虚拟化）共同完成一项复杂任务来获得极大的灵活性。
- * 策略解析。 * 在 Cisco UCS Manager 中，您可以创建组织单位层次结构的树结构，以模拟实际租户和组织关系。您可以在组织层次结构的不同级别定义各种策略，池和模板。按名称引用其他策略的策略将在策略匹配最接近的组织层次结构中进行解析。如果在根组织的层次结构中未找到具有特定名称的策略，则会搜索名

为 "defaultion" 的特殊策略。这种策略解决实践可实现易于自动化的管理 API ，并为不同组织的所有者提供极大的灵活性。

- * 服务配置文件和无状态计算。 * 服务配置文件是服务器的逻辑表示，它包含服务器的各种身份和策略。您可以将此逻辑服务器分配给任何物理计算资源，只要它满足资源要求即可。无状态计算支持在几分钟内采购服务器，而在传统服务器管理系统中，这种情况过去需要数天时间。
- * 内置多租户支持。 * 策略，池，模板，松散的引用完整性，组织层次结构中的策略解析以及基于服务配置文件的计算资源方法的组合，使得 Cisco UCS Manager 本质上有利于多租户环境，而这种环境通常在私有云和公有云中运行。
- * 扩展内存。 * 企业级 Cisco UCS B200 M5 刀片式服务器采用半宽刀片式外形，扩展了 Cisco Unified Computing System 产品组合的功能。Cisco UCS B200 M5 可利用最新 Intel Xeon 可扩展处理器 CPU 的强大功能， RAM 高达 3 TB 。此功能可以实现许多部署所需的巨大虚拟机与物理服务器比率，也可以使某些架构支持大数据等大内存操作。
- * 支持虚拟化的网络。 * Cisco Virtual Machine Fabric Extender （ VM-FEX ）技术可使访问网络层能够识别主机虚拟化。如果虚拟网络由网络管理员团队定义的端口配置文件管理，则这种感知可防止虚拟化对计算和网络域造成的影响。VM-FEX 还可以通过在硬件中执行切换来减轻虚拟机管理程序 CPU 的负载，从而使虚拟机管理程序 CPU 能够执行更多与虚拟化相关的任务。为了简化云管理， VM-FEX 技术与 VMware vCenter ， Linux 基于内核的虚拟机（ KVM ）和 Microsoft Hyper-V SR-IOV 完美集成。
- * 简化的 QoS 。 * 尽管 FC 和以太网已在 Cisco UCS 中融合，但对 QoS 和无损以太网的内置支持仍可实现无缝连接。通过在一个 GUI 面板中表示所有系统类，可在 Cisco UCS Manager 中简化网络 QoS 。

Cisco Nexus IP 和 MDS 交换机

Cisco Nexus 交换机和 Cisco MDS 多层控制器为您提供企业级连接和 SAN 整合。Cisco 多协议存储网络可提供以下灵活性和选项，帮助您降低业务风险： FC ，光纤连接（ Fibre Connection ， Ficon ），以太网 FC （ FCoE ）， iSCSI 和 IP FC （ FCIP ）。

Cisco Nexus 交换机可在一个平台中提供最全面的数据中心网络功能集之一。它们可以为数据中心和园区核心提供高性能和高密度。此外，它们还为数据中心聚合，行尾和数据中心互连部署提供了一整套功能，可在一个具有高度弹性的模块化平台中实现。

Cisco UCS 可将计算资源与 Cisco Nexus 交换机和一个统一网络结构集成在一起，用于识别和处理不同类型的网络流量。此流量包括存储 I/O ，流式桌面流量，管理以及对临床和业务应用程序的访问。您可以获得以下功能：

- * 基础架构可扩展性。 * 虚拟化，高效的电耗和散热，自动化的云扩展，高密度和高性能都支持高效的数据中心增长。
- * 操作连续性。 * 该设计集成了硬件， Cisco NX-OS 软件功能和管理功能，可支持零停机环境。
- * 传输灵活性。 * 借助这款经济高效的解决方案，您可以逐步采用新的网络技术。

Cisco UCS 与 Cisco Nexus 交换机和 MDS 多层控制器相结合，可为企业级医疗成像系统提供计算，网络和 SAN 连接解决方案。

NetApp 全闪存存储

运行 ONTAP 软件的 NetApp 存储可降低整体存储成本，同时提供医疗成像系统工作负载所需的低延迟读写响应时间和高 IOPS 。为了创建满足典型医疗成像系统要求的最佳存储系统， ONTAP 同时支持全闪存和混合存储配置。NetApp 闪存存储为像您这样的医疗成像系统客户提供了高性能和响应能力的关键组件，可支持延迟敏感型医疗成像系统操作。通过在一个集群中创建多个故障域， NetApp 技术还可以将生产环境与非生产环境隔离开来。此外， NetApp 还可以通过确保使用 ONTAP 最低 QoS 的工作负载的系统性能不低于某个级别来减少系统的性能问题。

ONTAP 软件的横向扩展架构可以灵活地适应各种 I/O 工作负载。为了提供临床应用程序所需的必要吞吐量和低延迟，并提供模块化横向扩展架构， ONTAP 架构通常使用全闪存配置。NetApp AFF 节点可以与混合（ HDD 和闪存）存储节点组合在同一个横向扩展集群中，适用于存储高吞吐量的大型数据集。您可以将医疗成像系统环境从昂贵的 SSD 存储克隆，复制和备份到其他节点上更经济的 HDD 存储。借助 NetApp 支持云的存储和 NetApp 提供的数据网络结构，您可以备份到内部或云中的对象存储。

对于医学影像， ONTAP 已通过大多数领先的医学影像系统的验证。这意味着它已经过测试，可为医疗成像提供快速可靠的性能。此外，以下功能还可以简化管理，提高可用性和自动化程度，并减少所需的总存储量。

- * 卓越的性能。 * NetApp AFF 解决方案与 NetApp FAS 产品系列的其他产品系列共享相同的统一存储架构， ONTAP 软件，管理界面，丰富的数据服务和高级功能集。全闪存介质与 ONTAP 的这种创新组合，可以为全闪存存储提供稳定一致的低延迟和高 IOPS ，同时还可以使用行业领先的 ONTAP 软件。
- * 存储效率。 * 您可以通过与 NetApp SME 合作来降低总容量需求，以了解此功能如何应用于您的特定医疗成像系统。
- * 节省空间的克隆。 * 借助 FlexClone 功能，您的系统几乎可以即时创建克隆以支持备份和测试环境刷新。只有在进行更改后，这些克隆才会占用额外的存储空间。
- * 集成数据保护。 * 完整的数据保护和灾难恢复功能可帮助您保护关键数据资产并提供灾难恢复。
- * 无中断运行。 * 您可以执行升级和维护，而无需使数据脱机。
- * qos.* 存储 QoS 可帮助您限制潜在的抢占资源的工作负载。更重要的是， QoS 可以为关键工作负载（例如医疗成像系统的生产环境）提供最低性能保证，确保系统性能不会低于特定水平。通过限制争用， NetApp QoS 还可以减少与性能相关的问题。
- * Data Fabric 。 * 为了加速数字化转型， NetApp 提供的 Data Fabric 可简化并集成云和内部环境中的数据管理。它提供一致且集成的数据管理服务和应用程序，可提供卓越的数据可见性和洞察力，数据访问和控制以及数据保护和安全性。NetApp 与 AWS ， Azure ， Google Cloud 和 IBM Cloud 等大型公有云相集成，为您提供广泛的选择。

主机虚拟化— **VMware vSphere**

FlexPod 架构已通过行业领先的虚拟化平台 VMware vSphere 6.x 的验证。VMware ESXi 6.x 用于部署和运行 VM 。vCenter Server 设备 6.x 用于管理 ESXi 主机和 VM 。使用在 Cisco UCS B200 M5 刀片式服务器上运行的多个 ESXi 主机构成 VMware ESXi 集群。VMware ESXi 集群可对所有集群节点中的计算，内存和网络资源进行池化，并为集群上运行的 VM 提供一个弹性平台。VMware ESXi 集群功能， vSphere 高可用性和分布式资源计划程序（ DRS ）都有助于使 vSphere 集群承受故障的能力，并有助于在 VMware ESXi 主机之间分布资源。

NetApp 存储插件和 Cisco UCS 插件与 VMware vCenter 集成在一起，可为您所需的存储和计算资源提供操作工作流。

VMware ESXi 集群和 vCenter Server 为您提供了一个集中式平台，用于在 VM 中部署医疗映像环境。您的医疗保健组织可以放心地实现行业领先虚拟基础架构的所有优势，例如：

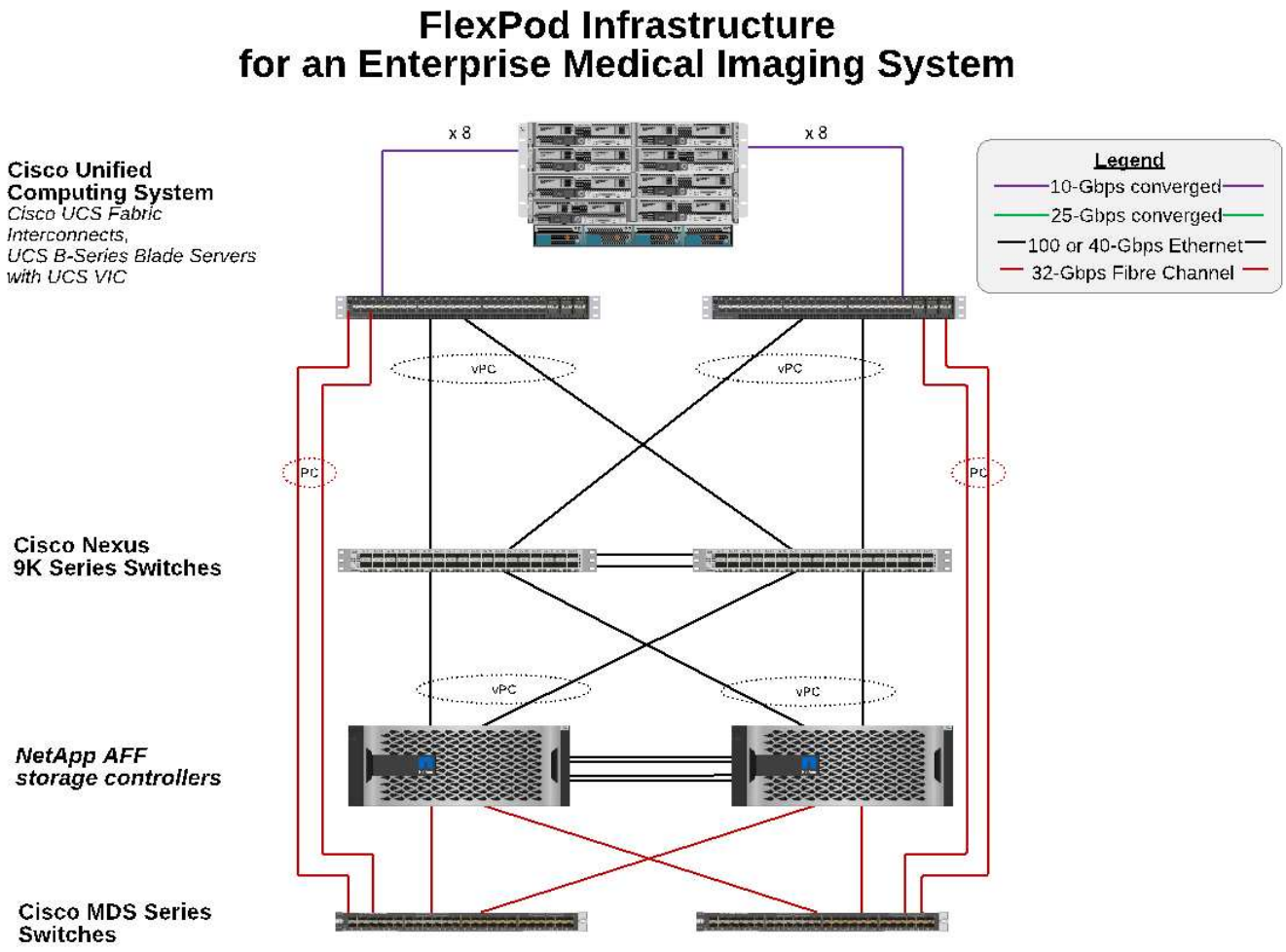
- * 部署简单。 * 使用虚拟设备快速轻松地部署 vCenter Server 。
- * 集中控制和可见性。 * 从一个位置管理整个 vSphere 基础架构。
- * 主动式优化。 * 分配，优化和迁移资源以实现最高效率。
- * 管理。 * 使用功能强大的插件和工具简化管理并扩展控制。

架构

FlexPod 架构旨在在整个计算，网络和存储堆栈中的组件或链路发生故障时提供高可用

性。多个用于客户端访问和存储访问的网络路径可实现负载平衡并优化资源利用率。

下图显示了用于医疗成像系统解决方案部署的 16 Gb FC/40 Gb 以太网（40GbE）拓扑结构。



存储架构

使用本节中的存储架构准则为企业级医疗映像系统配置存储基础架构。

存储层

典型的企业级医疗成像环境由多个不同的存储层组成。每个层都有特定的性能和存储协议要求。NetApp 存储支持各种 RAID 技术；有关详细信息，请参见 "此处"。以下是 NetApp AFF 存储系统如何满足映像系统不同存储层的需求：

- * 性能存储（第 1 层）。 * 此层可为数据库，操作系统驱动器， VMware 虚拟机文件系统（VMFS）数据存储库等提供高性能和高冗余。根据 ONTAP 中的配置，块 I/O 会通过光纤移动到 SSD 的共享存储阵列。最小延迟为 1 毫秒到 3 毫秒，偶尔峰值为 5 毫秒。此存储层通常用于短期存储缓存，通常用于 6 到 12 个月的映像存储，以便快速访问联机的 Dicom 映像。此层可为映像缓存，数据库备份等提供高性能和高冗余。NetApp 全闪存阵列可在持续带宽下提供低于 1 毫秒的延迟，远远低于典型企业级医疗成像环境所需的服务时间。NetApp ONTAP 既支持 RAID-TEC （三重奇偶校验 RAID ，用于承受三个磁盘故障），也支持 RAID DP （双奇偶校验 RAID ，用于承受两个磁盘故障）。

- * 归档存储（第 2 层）。 * 此层用于典型的成本优化文件访问，较大卷的 RAID 5 或 RAID 6 存储以及长期低成本 / 性能归档。NetApp ONTAP 既支持 RAID-TEC （三重奇偶校验 RAID ，用于承受三个磁盘故障），也支持 RAID DP （双奇偶校验 RAID ，用于承受两个磁盘故障）。FlexPod 中的 NetApp FAS 支持通过 NFS/SMB 将应用程序 I/O 映像到 SAS 磁盘阵列。NetApp FAS 系统可在持续带宽下提供 ~10 毫秒的延迟，远远低于企业级医疗成像系统环境中存储层 2 的预期服务时间。

在混合云环境中，基于云的归档可用于使用 S3 或类似协议归档到公有云存储提供商。通过 NetApp SnapMirror 技术，可以将映像数据从全闪存或 FAS 阵列复制到基于磁盘的速度较慢的存储阵列或 Cloud Volumes ONTAP for AWS ， Azure 或 Google Cloud 。

NetApp SnapMirror 可提供行业领先的数据复制功能，通过统一数据复制帮助保护您的医疗映像系统。通过跨平台复制（从闪存到磁盘再到云）简化整个数据网络结构的数据保护管理：

- 在 NetApp 存储系统之间无缝高效地传输数据，以使用相同的目标卷和 I/O 流支持备份和灾难恢复。
- 故障转移到任何二级卷。从二级存储上的任何时间点 Snapshot 进行恢复。
- 利用零数据丢失同步复制（ RPO=0 ）保护最关键的工作负载。
- 减少网络流量。通过高效运营减少存储占用空间。
- 仅传输更改的数据块，以减少网络流量。
- 在传输期间，保持主存储的存储效率优势，包括重复数据删除，数据压缩和数据缩减。
- 利用网络压缩提高实时效率。

有关详细信息，请参见 "此处"。

下表列出了典型医疗成像系统在特定延迟和吞吐量性能特征方面所需的每一层。

存储层	要求	**NetApp** 建议
1.	延迟 1 – 5 毫秒 35 – 500 Mbps 吞吐量	延迟小于 1 毫秒的 AFF 具有两个磁盘架的 AFF A300 高可用性（ HA ）对，可处理高达 ~1.6 GBps 的吞吐量
2.	内部归档	FAS ，延迟长达 30 毫秒
	归档到云	SnapMirror 复制到 Cloud Volumes ONTAP 或使用 NetApp StorageGRID 软件进行备份归档

存储网络连接

FC 网络结构

- FC 网络结构用于从计算到存储的主机操作系统 I/O 。
- 两个 FC 网络结构（阵列 A 和阵列 B ）分别连接到 Cisco UCS 阵列 A 和 UCS 阵列 B 。
- 每个控制器节点上都有一个具有两个 FC 逻辑接口（ LIF ）的 Storage Virtual Machine （ SVM ）。在每个节点上，一个 LIF 连接到阵列 A ，另一个 LIF 连接到阵列 B
- 16 Gbps FC 端到端连接通过 Cisco MDS 交换机实现。一个启动程序，多个目标端口和分区均已配置。
- FC SAN 启动用于创建完全无状态计算。服务器从 AFF 存储集群上托管的启动卷中的 LUN 启动。

用于通过 **iSCSI** ， **NFS** 和 **SMB/CIFS** 进行存储访问的 **IP** 网络

- 每个控制器节点上的 SVM 中有两个 iSCSI LIF 。在每个节点上，一个 LIF 连接到阵列 A ，另一个 LIF 连接到阵列 B
- 每个控制器节点上的 SVM 中有两个 NAS 数据 LIF 。在每个节点上，一个 LIF 连接到阵列 A ，另一个 LIF 连接到阵列 B
- 存储端口接口组（虚拟端口通道 vPC ），用于连接到交换机 N9kA 的 10 Gbps 链路和连接到交换机 N9k-B 的 10 Gbps 链路
- 从 VM 到存储的 ext4 或 NTFS 文件系统中的工作负载：
  - 基于 IP 的 iSCSI 协议。
- NFS 数据存储库中托管的 VM ：
  - VM OS I/O 通过 Nexus 交换机通过多个以太网路径。

带内管理（主动 - 被动绑定）

- 连接到管理交换机 N9kA 的 1 Gbps 链路，连接到管理交换机 N9k-B 的 1 Gbps 链路

备份和恢复

FlexPod 数据中心基于由 NetApp ONTAP 数据管理软件管理的存储阵列构建。ONTAP 软件经过 20 多年的发展，为 VM ， Oracle 数据库， SMB/CIFS 文件共享和 NFS 提供了许多数据管理功能。它还提供保护技术，例如 NetApp Snapshot 技术， SnapMirror 技术和 NetApp FlexClone 数据复制技术。NetApp SnapCenter 软件具有一个服务器和一个 GUI 客户端，可用于对 VM ， SMB/CIFS 文件共享， NFS 以及 Oracle 数据库备份和恢复使用 ONTAP Snapshot ， SnapRestore 和 FlexClone 功能。

NetApp SnapCenter 软件采用 "获得专利" Snapshot 技术，用于在 NetApp 存储卷上瞬时创建整个 VM 或 Oracle 数据库的备份。与 Oracle Recovery Manager （ RMAN ）相比， Snapshot 副本不需要完整的基线备份副本，因为它们不会存储为块的物理副本。创建 Snapshot 副本时， Snapshot 副本会作为指向 ONTAP WAFL 文件系统中存储块的指针进行存储。由于这种紧密的物理关系， Snapshot 副本会与原始数据保持在同一存储阵列上。您还可以在文件级别创建 Snapshot 副本，以便更精细地控制备份。

Snapshot 技术基于写入时重定向技术。它最初仅包含元数据指针，在首次将数据更改为存储块之前不会占用太多空间。如果现有块由 Snapshot 副本锁定，则 ONTAP WAFL 文件系统会将新块作为活动副本写入。这种方法可避免写入时更改技术发生的双写入。

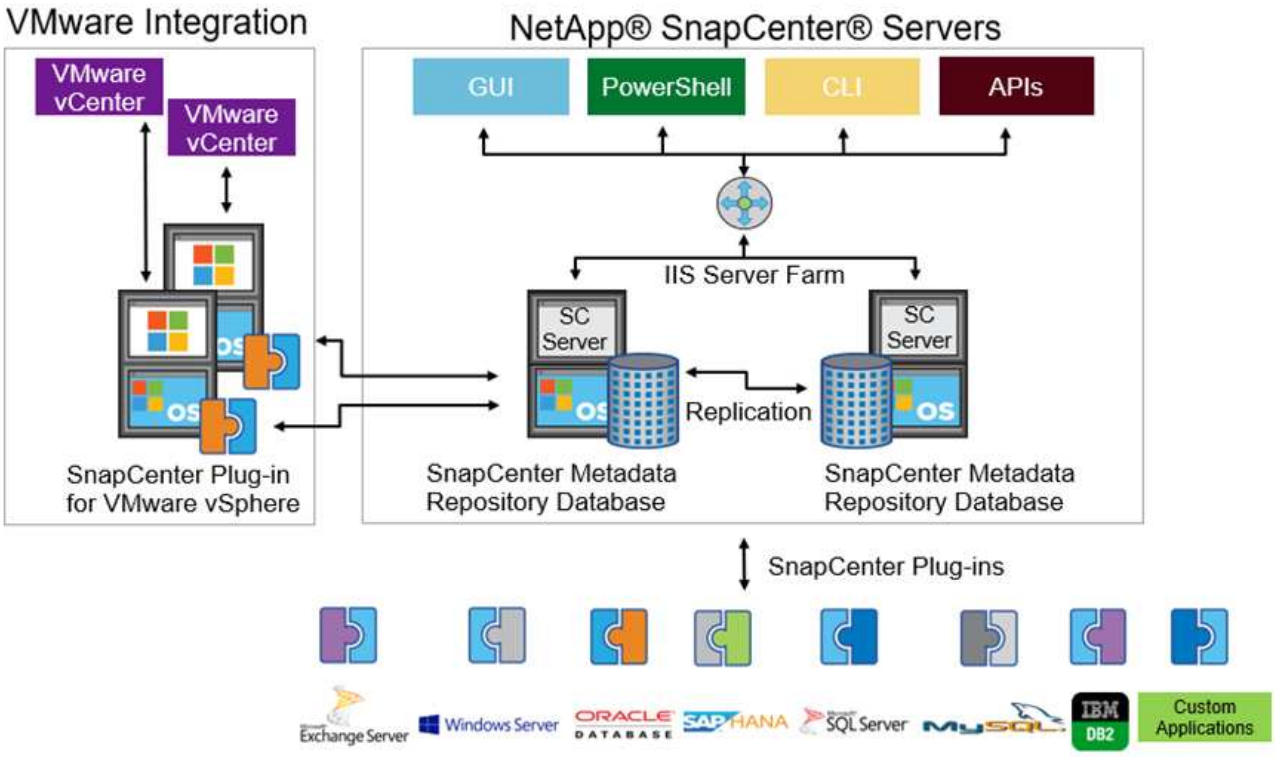
对于 Oracle 数据库备份， Snapshot 副本可节省大量时间。例如，单独使用 RMAN 需要 26 小时才能完成的备份可能需要不到 2 分钟才能使用 SnapCenter 软件完成。

由于数据还原不会复制任何数据块，而是会在创建 Snapshot 副本时将指针翻转到应用程序一致的 Snapshot 块映像，因此 Snapshot 备份副本几乎可以瞬时还原。SnapCenter 克隆会为现有 Snapshot 副本创建一个单独的元数据指针副本，并将新副本挂载到目标主机。此过程速度快，存储效率高。

下表总结了 Oracle RMAN 与 NetApp SnapCenter 软件之间的主要区别。

	备份	还原	克隆	需要完整备份	空间使用量	异地副本
RMAN	速度较慢	速度较慢	速度较慢	是的。	高	是的。
SnapCenter	快速	快速	快速	否	低	是的。

下图显示了 SnapCenter 架构。



全球数千家企业都在使用 NetApp MetroCluster 配置在数据中心内外实现高可用性（ HA ），零数据丢失和无中断运行。MetroCluster 是 ONTAP 软件的一项免费功能，用于在位于不同位置或故障域的两个 ONTAP 集群之间同步镜像数据和配置。MetroCluster 通过自动处理两个目标为应用程序提供持续可用的存储：零恢复点目标（ RPO ），通过同步镜像写入集群的数据。通过镜像配置和自动访问第二个站点的数据实现接近零恢复时间目标（ RTO） MetroCluster 可在两个站点的两个独立集群之间自动镜像数据和配置，从而简化操作。由于存储是在一个集群中配置的，因此它会自动镜像到第二个站点的第二个集群。NetApp SyncMirror 技术可为所有数据提供一个完整副本，并且 RPO 为零。因此，一个站点的工作负载可以随时切换到另一个站点，并继续提供数据而不会丢失数据。有关详细信息，请参见 "此处"。

网络

一对 Cisco Nexus 交换机可为从计算到存储的 IP 流量以及医学影像系统图像查看器的外部客户端提供冗余路径：

- 使用端口通道和 vPC 的链路聚合可在整个系统中使用，从而实现更高带宽和高可用性的设计：
  - VPC 用于 NetApp 存储阵列和 Cisco Nexus 交换机之间。
  - VPC 用于 Cisco UCS 互联阵列和 Cisco Nexus 交换机之间。
  - 每台服务器都具有虚拟网络接口卡（ Virtual Network Interface Card， vNIC ），可通过冗余连接到统一网络结构。在互联阵列之间使用 NIC 故障转移来实现冗余。
  - 每个服务器都具有虚拟主机总线适配器（ vHBA ），并与统一网络结构建立冗余连接。
- Cisco UCS 互联阵列会按照建议配置在终端主机模式下，以便将 vNIC 动态固定到上行链路交换机。
- FC 存储网络由一对 Cisco MDS 交换机提供。

计算— **Cisco Unified Computing System**

通过不同互联阵列连接的两个 Cisco UCS 网络结构提供两个故障域。每个网络结构都连接到两个 IP 网络交换机和不同的 FC 网络交换机。

为了运行 VMware ESXi ，系统会根据 FlexPod 最佳实践为每个 Cisco UCS 刀片式服务器创建相同的服务配置文件。每个服务配置文件应包含以下组件：

- 两个 vNIC （每个网络结构上一个），用于传输 NFS ， SMB/CIFS 以及客户端或管理流量
- 为 vNIC 提供所需的其他 VLAN ，以传输 NFS ， SMB/CIFS 和客户端或管理流量
- 两个 vNIC （每个网络结构上一个），用于传输 iSCSI 流量
- 两个存储 FC HBA （每个网络结构上一个），用于向存储传输 FC 流量
- SAN 启动

虚拟化

VMware ESXi 主机集群运行工作负载 VM 。集群包含在 Cisco UCS 刀片式服务器上运行的 ESXi 实例。

每个 ESXi 主机都包含以下网络组件：

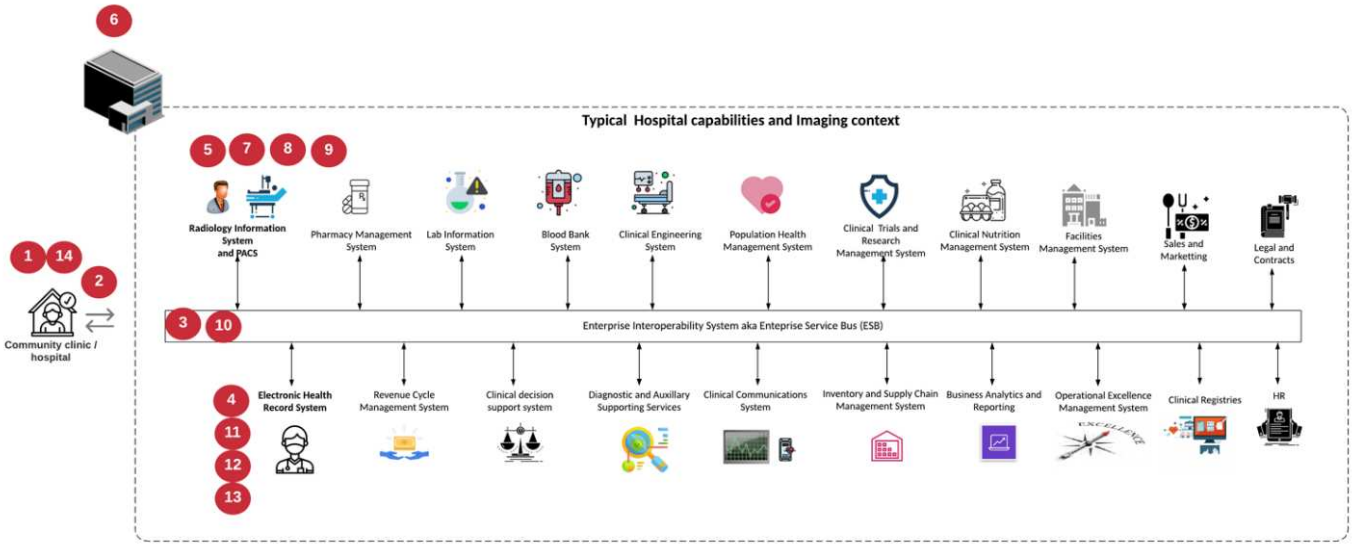
- 通过 FC 或 iSCSI 启动 SAN
- NetApp 存储上的启动 LUN （位于用于启动操作系统的专用 FlexVol 中）
- 两个 vmnic （ Cisco UCS vNIC ），用于 NFS ， SMB/CIFS 或管理流量
- 两个存储 HBA （ Cisco UCS FC vHBA ），用于传输到存储的 FC 流量
- 标准交换机或分布式虚拟交换机（根据需要）
- 工作负载 VM 的 NFS 数据存储库
- 虚拟机的管理，客户端流量网络和存储网络端口组
- 用于管理，客户端流量和存储访问（ NFS ， iSCSI 或 SMB/CIFS ）的网络适配器
- 已启用 VMware DRS
- 为存储的 FC 或 iSCSI 路径启用了原生多路径
- 已关闭虚拟机的 VMware 快照
- 为 VMware 部署的 NetApp SnapCenter 用于 VM 备份

医疗成像系统架构

在医疗保健组织中，医疗成像系统是关键应用程序，可与从患者注册到收入周期计费相关活动的临床工作流完美集成。

下图显示了典型大型医院涉及的各种系统；此图旨在在我们放大典型医疗成像系统的架构组件之前为医疗成像系统提供架构环境。工作流千差万别，并且因医院和使用情形而异。

下图显示了患者，社区诊所和大型医院环境下的医疗成像系统。



1. 患者前往社区诊所时出现症状。在咨询期间，社区医生会发出一个成像指令，该指令将以一条 HL7 顺序消息的形式发送到较大的医院。
2. 社区医生的 EHR 系统会向大型医院发送 "HL7 Order/ORD" 消息。
3. 企业互操作性系统（也称为企业服务总线（ Enterprise Service Bus ， ESB] ）处理订单消息并将订单消息发送到 EHR 系统。
4. EHR 将处理订单消息。如果不存在患者记录，则会创建新的患者记录。
5. EHR 会向医疗成像系统发送成像顺序。
6. 患者致电大医院预约成像。
7. 成像接收和注册台使用放射学信息或类似系统为患者安排成像预约。
8. 患者到达后将进行成像预约，此时将创建图像或视频并将其发送到 PACS 。
9. 放射科医生使用支持高端 /GPU 图形的诊断查看器在 PACS 中读取这些图像并为这些图像添加标注。某些映像系统在映像工作流中内置了人工智能（ AI ）效率提升功能。
10. 图像顺序结果将通过 ESB-发送 到 EHR ，形式为 Order Results HL7 ORU 消息。
11. EHR 会将顺序结果处理到患者的记录中，并将缩略图放置在可识别上下文的链接中以指向实际的 Dicom 图像。如果需要从 EHR 中获取更高分辨率的图像，医生可以启动诊断查看器。
12. 医生会查看该图像并将医生备注输入到患者记录中。医生可以使用临床决策支持系统来改进审核流程，并协助正确诊断患者。
13. 然后， EHR 系统会将订单结果以订单结果消息的形式发送到社区医院。此时，如果社区医院可以接收完整的映像，则该映像将通过 WADO 或 Dicom 发送。
14. 社区医生完成诊断，并为患者提供后续步骤。

典型的医疗成像系统使用 N 层架构。医疗成像系统的核心组件是一个用于托管各种应用程序组件的应用程序服务器。典型的应用程序服务器基于 Java 运行时或 C# .Net CLR- 。大多数企业级医疗成像解决方案都使用 Oracle 数据库服务器， MS SQL Server 或 Sybase 作为主数据库。此外，某些企业医疗成像系统还使用数据库在一个地理区域内加速和缓存内容。某些企业医疗成像系统还会将 MongoDB ， Redis 等 NoSQL 数据库与企业集成服务器结合使用，以便使用这些数据库作为 Dicom 接口和 / 或 API 。

典型的医疗成像系统可为两组不同的用户提供对图像的访问权限：诊断用户 / 放射科医生或订购该图像的临床医生。

放射科医生通常使用支持图形的高端诊断查看器，这些查看器运行在物理或虚拟桌面基础架构中的高端计算和图形工作站上。如果您即将开始虚拟桌面基础架构之旅，可以找到更多信息 "此处"。

当卡特里娜飓风毁坏了路易斯安那州两家主要教学医院时，各级领导者们聚集在一起，构建了一个弹性电子健康记录系统，在创纪录的时间内包含 3000 多个虚拟桌面。有关使用情形参考架构和 FlexPod 参考捆绑包的详细信息，请参见 "此处"。

临床医生主要通过两种方式访问图像：

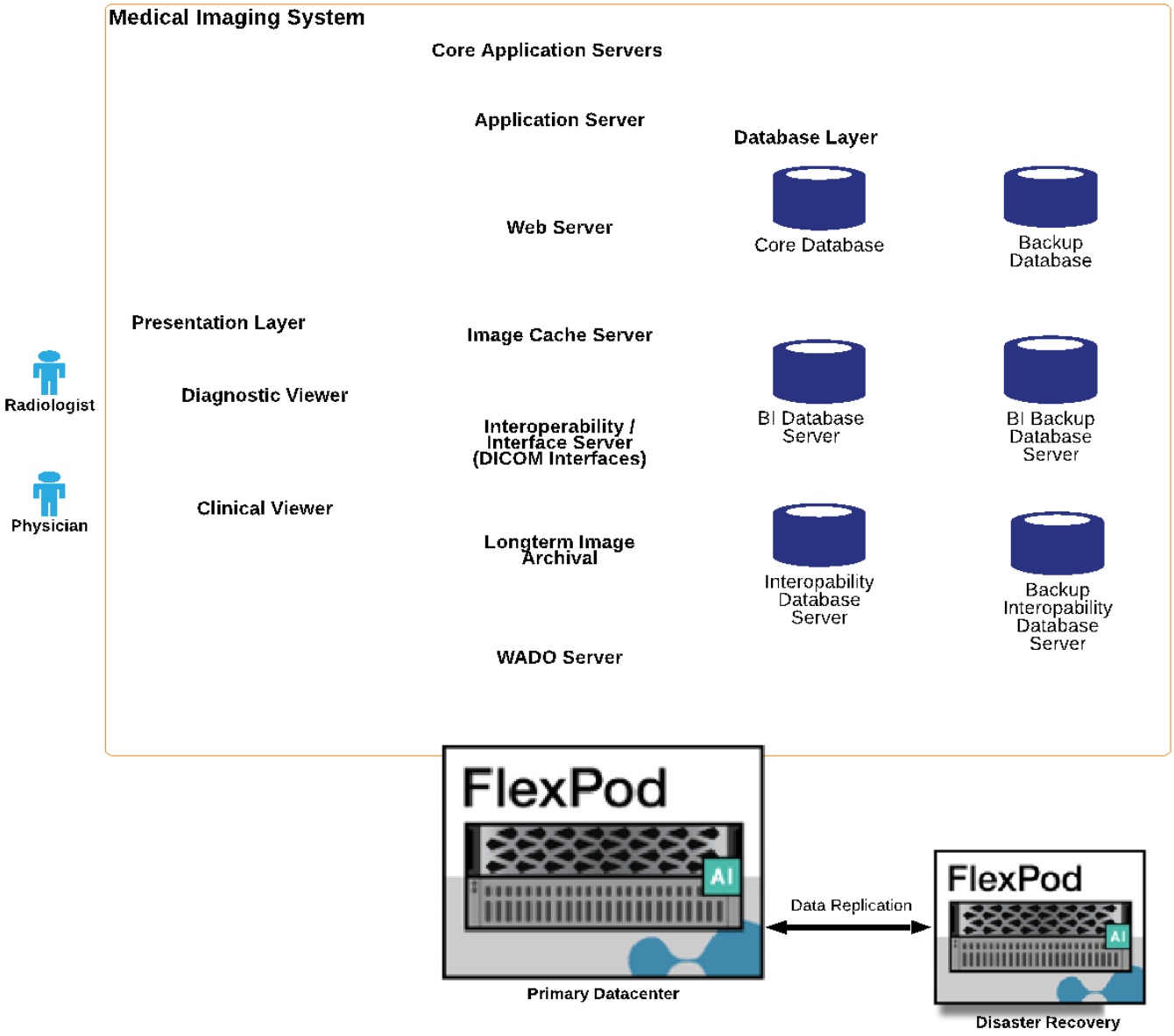
- * 基于 Web 的访问。 * EHR 系统通常使用此功能将 PACS 图像嵌入为上下文感知链接，以链接形式存储到患者的电子病历（ EMR ）中，并可链接到成像工作流，操作步骤工作流，进度注释工作流等。此外，还可以通过基于 Web 的链接通过患者门户访问患者的图像。基于 Web 的访问使用一种称为上下文感知链接的技术模式。上下文感知链接可以是直接指向 Dicom 介质的静态链接 /URI ，也可以是使用自定义宏动态生成的链接 /URI 。
- * 厚客户端。 * 某些企业医疗系统还允许您使用基于厚客户端的方法来查看映像。您可以从患者 EMR 中启动厚客户端，也可以作为独立应用程序启动。

通过医学影像系统，可以访问一个由医生或加入 CIN 的医生参加的社区。典型的医疗成像系统包括一些组件，这些组件可以使您的医疗保健组织内外的其他医疗 IT 系统实现映像互操作性。社区医生可以通过基于 Web 的应用程序访问映像，也可以利用映像交换平台实现映像互操作性。映像交换平台通常使用 WADO 或 Dicom 作为底层映像交换协议。

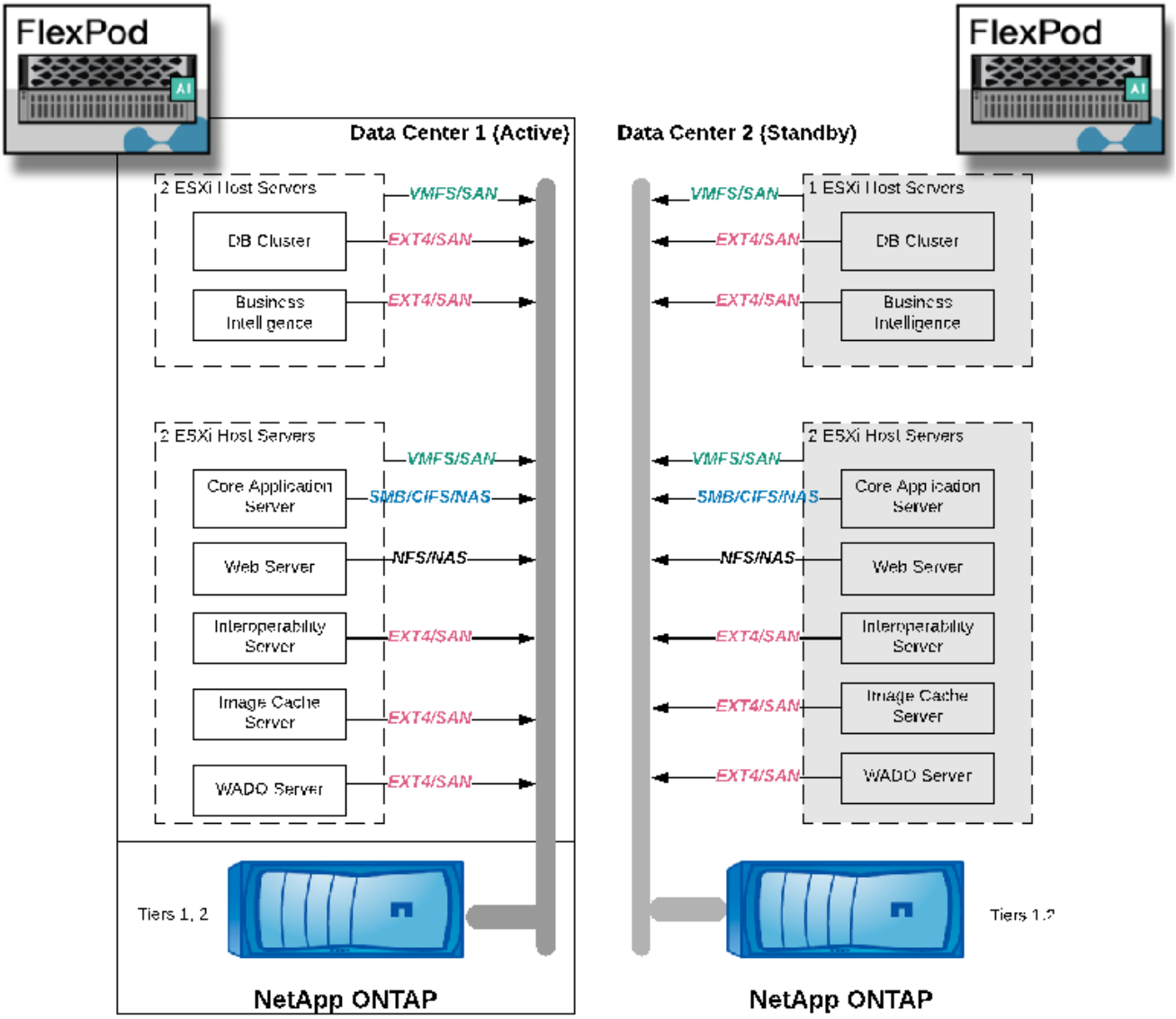
医学影像系统还可以支持需要在课堂上使用 PACS 或影像系统的学术医疗中心。为了支持学术活动，典型的医疗成像系统可以在占用空间较小的情况下拥有 PACS 系统的功能，也可以在仅供教学使用的成像环境中提供此功能。典型的供应商中立归档系统和一些企业级医疗成像系统提供了 "DICOM" 图像标记形态功能，可对用于教学目的的图像进行匿名化处理。标签形态使医疗保健组织能够以供应商中立的方式在不同供应商的医疗影像系统之间交换 Dicom 图像。此外，标记形态化还可以使医疗成像系统在企业范围内对医疗影像实施供应商中立的归档功能。

医疗成像系统正在开始使用 "基于 GPU 的计算功能" 通过预处理图像来增强人类工作流，从而提高效率。典型的企业级医疗成像系统可利用行业领先的 NetApp 存储效率功能。企业级医疗成像系统通常使用 RMAN 执行备份，恢复和还原活动。为了提高性能并缩短创建备份所需的时间，可以使用 Snapshot 技术进行备份操作，并使用 SnapMirror 技术进行复制。

下图显示了分层架构视图中的逻辑应用程序组件。



下图显示了物理应用程序组件。



逻辑应用程序组件要求基础架构支持多种协议和文件系统。NetApp ONTAP 软件支持一组行业领先的协议和文件系统。

下表列出了应用程序组件，存储协议和文件系统要求。

应用程序组件	**SAN/NAS**	文件系统类型	存储层	复制类型
VMware 主机产品数据库	本地	SAN	VMFS	第 1 层
应用程序	VMware 主机产品数据库	代表	SAN	VMFS
第 1 层	应用程序	VMware 主机 prod 应用程序	本地	SAN
VMFS	第 1 层	应用程序	VMware 主机 prod 应用程序	代表
SAN	VMFS	第 1 层	应用程序	核心数据库服务器

应用程序组件	**SAN/NAS**	文件系统类型	存储层	复制类型
SAN	ext4	第 1 层	应用程序	备份数据库服务器
SAN	ext4	第 1 层	无	映像缓存服务器
NAS	SMB/CIFS	第 1 层	无	归档服务器
NAS	SMB/CIFS	第 2 层	应用程序	Web 服务器
NAS	SMB/CIFS	第 1 层	无	WADO 服务器
SAN	NFS	第 1 层	应用程序	业务智能服务器
SAN	NTFS	第 1 层	应用程序	业务智能备份
SAN	NTFS	第 1 层	应用程序	互操作性服务器
SAN	ext4	第 1 层	应用程序	互操作性数据库服务器

解决方案基础架构硬件和软件组件

下表分别列出了医疗成像系统的 FlexPod 基础架构的硬件和软件组件。

层	产品系列	数量和型号	详细信息
计算	Cisco UCS 5108 机箱	1 或 2	根据支持年度研究数量所需的刀片式服务器数量
	Cisco UCS 刀片式服务器	B200 M5	刀片式服务器数量，根据每年的研究次数计算，每个研究中有 2 个或 20 个以上的核心， 2.7 GHz 和 128-384 GB RAM
	Cisco UCS 虚拟接口卡（VIC）	Cisco UCS 1440	请参见
	2 个 Cisco UCS 互联阵列	6454 或更高版本	–
网络	Cisco Nexus 交换机	2 个 Cisco Nexus 3000 系列或 9000 系列	–
存储网络	用于通过 SMB/CIFS ，NFS 或 iSCSI 协议进行存储访问的 IP 网络	与上述相同的网络交换机	–
	通过 FC 进行存储访问	2 个 Cisco MDS 9132T	–
存储	NetApp AFF A400 全闪存存储系统	1 个或多个 HA 对	包含两个或更多节点的集群
	磁盘架	1 个或多个 DS224C 或 NS224 磁盘架	已完全填充 24 个驱动器
	SSD	大于 24 ， 1.2 TB 或更大的容量	–

软件	产品系列	版本或版本	详细信息
企业级医疗成像系统			
	MS SQL 或 Oracle 数据库服务器	按照医疗成像系统供应商的建议	
	没有像 MongoDB Server 这样的 SQL 数据库	按照医疗成像系统供应商的建议	
	应用程序服务器	按照医疗成像系统供应商的建议	
	集成服务器（ MS BizTalk ， MuleSoft ， Rhapsody ， Tibco ）	按照医疗成像系统供应商的建议	
	虚拟机	Linux （ 64 位）	
	虚拟机	Windows Server （ 64 位）	
存储	ONTAP	ONTAP 9.7 或更高版本	
网络	Cisco UCS 互联阵列	Cisco UCS Manager 4.1 或更高版本	
	Cisco 以太网交换机	9.2 （ 3 ） i7 （ 2 ）或更高版本	
	Cisco FC： Cisco MDS 9132T	8.4 （ 2 ）或更高版本	
虚拟机管理程序	虚拟机管理程序	VMware vSphere ESXi 6.7 U2 或更高版本	
管理	虚拟机管理程序管理系统	VMware vCenter Server 6.7 U1 （ vCSA ）或更高版本	
	NetApp 虚拟存储控制台（ VSC ）	VSC 9.7 或更高版本	
	SnapCenter	SnapCenter 4.3 或更高版本	

解决方案规模估算

存储规模估算

本节介绍了研究的数量以及相应的基础架构要求。

下表列出的存储要求假定现有数据为 1 年值加上主系统（第 1 层，第 2 层）研究一年的预计增长。对于前两年之后 3 年的预计增长，还会单独列出其他存储需求。

	小型	中等	大型
年度研究	少于 25 万项研究	25 万– 50 万项研究	50 万到 100 万项研究
第 1 层存储			

	小型	中等	大型
IOPS （平均）	1.5 万– 5 千	5 K 到 15 K	15 K 到 40 K
IOPS （峰值）	5 公里	20 万	65 万
吞吐量	50 – 100 Mbps	50 – 150 MBps	100 – 300 Mbps
容量数据中心 1 （旧数据 1 年，新研究 1 年）	70 TB	140 TB	260 TB
容量数据中心 1 （新研究还需要 4 年时间）	25 TB	45 TB	80 TB
容量数据中心 2 （旧数据 1 年，新研究 1 年）	45 TB	110 TB	165 TB
容量数据中心 2 （新研究还需要 4 年时间）	25 TB	45 TB	80 TB
第 2 层存储			
IOPS （平均）	1k	2k	3 K
容量数据中心 1.	320 TB	800 TB	2000 TB

计算规模估算

下表列出了小型，中型和大型医疗成像系统的计算要求。

	小型	中等	大型
年度研究	少于 25 万项研究	25 万– 50 万项研究	50 万到 100 万项研究
数据中心 1.			
VM 数量	21	27	35
虚拟 CPU （ vCPU ）总数	56	124.	220
总内存要求	225 GB	450 GB	900 GB
物理服务器（刀片式服务器）规格（假设 1 个 vCPU -=1 个核心）	4 个服务器，每个服务器具有 20 个核心和 192 GB RAM	8 个服务器，每个服务器具有 20 个核心和 128 GB RAM	14 个服务器，每个服务器具有 20 个核心和 128 GB RAM
数据中心 2.			
VM 数量	15	17	22.
vCPU 总数	42	72.	140
总内存要求	179 GB	243 GB	513 GB
物理服务器（刀片式服务器）规格（假设 1 个 vCPU = 1 个核心）	3 个服务器，每个服务器具有 20 个核心和 16 GB RAM	6 个服务器，每个服务器具有 20 个核心和 128 GB RAM	8 个服务器，每个服务器具有 24 个核心和 128 GB RAM

网络和 **Cisco UCS** 基础架构规模估算

下表列出了小型，中型和大型医疗成像系统的网络连接和 Cisco UCS 基础架构要求。

	小型	中等	大型
数据中心 1.			
存储节点端口的数量	2 个融合网络适配器（ CNA）； 2 个 FC	2 个 CNA； 2 个 FC	2 个 CNA； 2 个 FC
IP 网络交换机端口（ Cisco Nexus 9000）	48 端口交换机	48 端口交换机	48 端口交换机
FC 交换机（ Cisco MDS）	32 端口交换机	32 端口交换机	48 端口交换机
Cisco UCS 机箱计数	1 x 5108	1 x 5108	2 x 5108
Cisco UCS 互联阵列	2 个 6332	2 个 6332	2 个 6332
数据中心 2.			
Cisco UCS 机箱计数	1 x 5108	1 x 5108	1 x 5108
Cisco UCS 互联阵列	2 个 6332	2 个 6332	2 个 6332
存储节点端口的数量	2 个 CNA； 2 个 FC	2 个 CNA； 2 个 FC	2 个 CNA； 2 个 FC
IP 网络交换机端口（ Cisco Nexus 9000）	48 端口交换机	48 端口交换机	48 端口交换机
FC 交换机（ Cisco MDS）	32 端口交换机	32 端口交换机	48 端口交换机

最佳实践

存储最佳实践

高可用性

NetApp 存储集群设计可在每个级别提供高可用性：

- 集群节点
- 后端存储连接
- RAID TEC ，可承受三个磁盘故障
- 可承受两个磁盘故障的 RAID DP
- 从每个节点物理连接到两个物理网络
- 存储 LUN 和卷的多个数据路径

安全多租户

NetApp Storage Virtual Machine （ SVM ）提供了一个虚拟存储阵列构造，用于分隔安全域，策略和虚拟网络。NetApp 建议您为存储集群上托管数据的每个租户组织创建单独的 SVM 。

NetApp 存储最佳实践

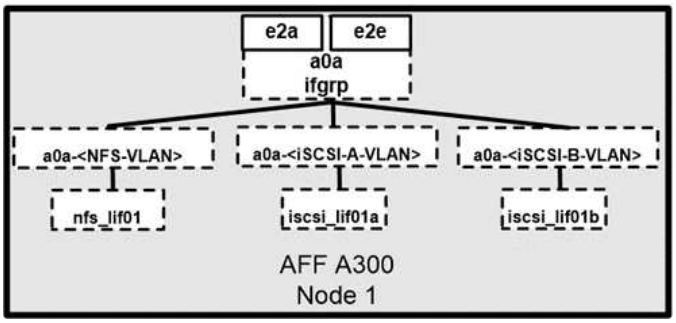
请考虑以下 NetApp 存储最佳实践：

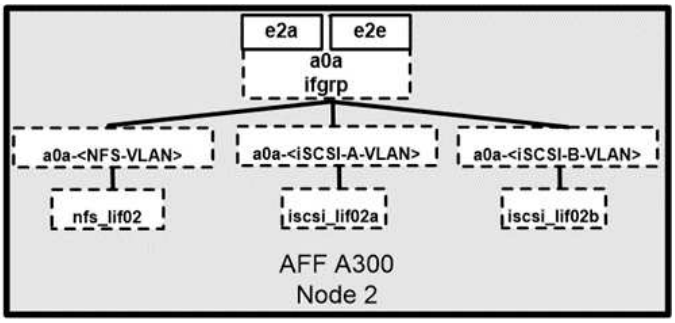
- 始终启用 NetApp AutoSupport 技术，该技术会通过 HTTPS 向 NetApp 发送支持摘要信息。
- 为了最大程度地提高可用性和移动性，请确保为 NetApp ONTAP 集群中每个节点上的每个 SVM 创建一个 LIF 。非对称逻辑单元访问（ Asymmetric Logical Unit Access ， ALUA ）用于解析路径并识别活动优化（ Direct ）路径与活动非优化路径。ALUA 既适用于 FC ，也适用于 FCoE 和 iSCSI 。
- 仅包含 LUN 的卷不需要在内部挂载，也不需要接合路径。
- 如果您在 ESXi 中使用质询握手身份验证协议（ Challenge-Handshake Authentication Protocol ， CHAP ）进行目标身份验证，则还必须在 ONTAP 中对其进行配置。使用命令行界面（`vserver iscsi security create` ）或 NetApp ONTAP 系统管理器（在 "Storage">"SVM">"SVM Settings">"Protocols">"iSCSI" 下编辑启动程序安全性）。

SAN 启动

NetApp 建议您在 FlexPod Datacenter 解决方案中为 Cisco UCS 服务器实施 SAN 启动。通过此步骤，可以通过 NetApp AFF 存储系统安全地保护操作系统，从而提高性能。本解决方案概述的设计使用 iSCSI SAN 启动。

在 iSCSI SAN 启动中，为每个 Cisco UCS 服务器分配两个 iSCSI vNIC （每个 SAN 网络结构一个），以便在通往存储的整个过程中提供冗余连接。此示例中连接到 Cisco Nexus 交换机的存储端口 E2A 和 e2e 将分组在一起，形成一个名为接口组（ ifgrp ）的逻辑端口（在此示例中为 a0a ）。iSCSI VLAN 在 igroup 上创建， iSCSI LIF 在 iSCSI 端口组（在此示例中为 a0a-<iscsi-a-VLAN> ）上创建。iSCSI 启动 LUN 通过 iSCSI LIF 使用 igroup 公开给服务器。此方法仅允许授权服务器访问启动 LUN 。有关端口和 LIF 布局，请参见下图。





与 NAS 网络接口不同， SAN 网络接口未配置为在发生故障期间进行故障转移。相反，如果网络接口不可用，则主机将选择一个新的优化路径来访问可用的网络接口。ALUA 是 NetApp 支持的一种标准，可提供有关 SCSI 目标的信息，从而使主机能够确定最佳存储路径。

存储效率和精简配置

NetApp 在存储效率创新方面一直处于行业领先地位，例如首次针对主工作负载执行重复数据删除，以及通过实时数据缩减增强数据压缩并高效存储小文件和 I/O 。ONTAP 支持实时和后台重复数据删除，以及实时和后台数据压缩。

要在块环境中实现重复数据删除的优势，必须对 LUN 进行精简配置。尽管 VM 管理员仍认为 LUN 占用了已配置的容量，但重复数据删除节省的空间会返回到卷中以用于其他需求。NetApp 建议您将这些 LUN 部署在 FlexVol 卷中，这些卷也采用精简配置，其容量是 LUN 大小的两倍。这样部署 LUN 时， FlexVol 卷仅充当配额。LUN 占用的存储会在 FlexVol 卷及其所属聚合中进行报告。

要最大程度地节省重复数据删除的空间，请考虑计划后台重复数据删除。但是，这些进程在运行时会使用系统资源。因此，理想情况下，您应将其计划在活动较少的时间（例如周末），或者更频繁地运行，以减少要处理的更

改数据量。AFF 系统上的自动后台重复数据删除对前台活动的影响要小得多。后台数据压缩（对于基于硬盘的系统）也会占用资源，因此您应仅考虑性能要求有限的二级工作负载。

Quality of service

运行 ONTAP 软件的系统可以使用 ONTAP 存储服务质量功能来限制吞吐量（以每秒兆位数（ MBps ）为单位），并限制文件， LUN ，卷或整个 SVM 等不同存储对象的 IOPS 。自适应 QoS 用于设置 IOPS 下限（ QoS 最小值）和上限（ QoS 最大值），此上限可根据数据存储库容量和已用空间动态调整。

吞吐量限制可用于在部署之前控制未知工作负载或测试工作负载，以确认它们不会影响其他工作负载。在确定抢占资源的工作负载后，您也可以使用这些限制来对其进行限制。此外，还支持基于 IOPS 的最低服务级别，以便为 ONTAP 中的 SAN 对象提供稳定一致的性能。

对于 NFS 数据存储库，可以将 QoS 策略应用于整个 FlexVol 卷或其中的各个虚拟机磁盘（ Virtual Machine Disk ， VMDK ）文件。对于使用 ONTAP LUN 的 VMFS 数据存储库（ Hyper-V 中的集群共享卷 [CSV] ），您可以将 QoS 策略应用于包含 LUN 的 FlexVol 卷或各个 LUN 。但是，由于 ONTAP 无法识别 VMFS ，因此无法将 QoS 策略应用于单个 VMDK 文件。在 VSC 7.1 或更高版本中使用 VMware 虚拟卷（ VVOL ）时，您可以使用存储功能配置文件在各个 VM 上设置最大 QoS 。

要为 LUN （包括 VMFS 或 CSV ）分配 QoS 策略，您可以从 ONTAP 主页上的存储系统菜单中获取 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 。在使用 ONTAP 工具之一指定 QoS 时，请使用此方法。

您可以为对象设置 QoS 最大吞吐量限制，以 MBps 和 IOPS 为单位。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。将策略应用于多个工作负载时，这些工作负载将共享策略的总限制。不支持嵌套对象（例如，对于卷中的某个文件，不能每个对象都有自己的策略）。QoS 最小值只能以 IOPS 为单位进行设置。

存储布局

本节介绍有关存储上 LUN ，卷和聚合布局的最佳实践。

存储 **LUN**

为了获得最佳性能，管理和备份， NetApp 建议采用以下 LUN 设计最佳实践：

- 创建单独的 LUN 以存储数据库数据和日志文件。
- 为每个实例创建一个单独的 LUN 以存储 Oracle 数据库日志备份。LUN 可以属于同一个卷。
- 为数据库文件和日志文件配置 LUN 并进行精简配置（禁用空间预留选项）。
- 所有映像数据都托管在 FC LUN 中。在分布在不同存储控制器节点所拥有的聚合中的 FlexVol 卷中创建这些 LUN 。

要在存储卷中放置 LUN ，请遵循下一节中的准则。

存储卷

为了获得最佳性能和管理、NetApp建议采用以下卷设计最佳实践：

- 在单独的存储卷上隔离具有I/O密集型查询的数据库。
- 数据文件可以放置在一个LUN或一个卷上、但为了提高吞吐量、建议使用多个卷/LUN。

- 使用多个LUN时、可以通过使用任何受支持的文件系统来实现I/O并行。
- 将数据库文件和事务日志放在不同的卷上、以提高恢复粒度。
- 请考虑使用自动调整大小、Snapshot预留、QoS等卷属性。

聚合

聚合是 NetApp 存储配置的主存储容器，包含一个或多个 RAID 组，这些 RAID 组同时包含数据磁盘和奇偶校验磁盘。

NetApp 使用共享聚合和专用聚合执行各种 I/O 工作负载特征测试，这些聚合的数据文件和事务日志文件是分开的。测试显示，一个包含更多 RAID 组和驱动器（ HDD 或 SSD ）的大型聚合可优化和提高存储性能，并且更便于管理员管理，原因有两个：

- 一个大型聚合可使所有驱动器的 I/O 功能对所有文件可用。
- 一个大型聚合可以最高效地利用磁盘空间。

为了实现有效的灾难恢复， NetApp 建议您将异步副本放置在灾难恢复站点中独立存储集群的聚合上，并使用 SnapMirror 技术复制内容。

为了获得最佳存储性能， NetApp 建议聚合中至少有 10% 的可用空间。

AFF A300 系统（具有两个磁盘架和 24 个驱动器）的存储聚合布局指南包括：

- 保留两个备用驱动器。
- 使用高级磁盘分区功能在每个驱动器上创建三个分区：根分区和数据分区。
- 每个聚合总共使用 20 个数据分区和两个奇偶校验分区。

备份最佳实践

NetApp SnapCenter 用于 VM 和数据库备份。NetApp 建议采用以下备份最佳实践：

- 部署 SnapCenter 以创建用于备份的 Snapshot 副本时，请关闭托管 VM 和应用程序数据的 FlexVol 的 Snapshot 计划。
- 为主机启动 LUN 创建专用 FlexVol 。
- 对具有相同用途的 VM 使用类似或单个备份策略。
- 每个工作负载类型使用类似的或单个备份策略；例如，对所有数据库工作负载使用类似的策略。对数据库，Web 服务器，最终用户虚拟桌面等使用不同的策略。
- 在 SnapCenter 中启用备份验证。
- 配置将备份 Snapshot 副本归档到 NetApp SnapVault 备份解决方案。
- 根据归档计划在主存储上配置备份保留。

基础架构最佳实践

网络最佳实践

NetApp 建议采用以下网络最佳实践：

- 确保您的系统包含用于生产和存储流量的冗余物理 NIC 。
- 为计算和存储之间的 iSCSI ， NFS 和 SMB/CIFS 流量分隔 VLAN 。
- 确保您的系统包含一个专用 VLAN ，用于客户端访问医疗映像系统。

您可以在 FlexPod 基础架构设计和部署指南中找到其他网络最佳实践。

计算最佳实践

NetApp 建议采用以下计算最佳实践：

- 确保每个指定的 vCPU 都由一个物理核心支持。

虚拟化最佳实践

NetApp 建议采用以下虚拟化最佳实践：

- 使用 VMware vSphere 6 或更高版本。
- 将 ESXi 主机服务器 BIOS 和操作系统层设置为 Custom Controlled – High Performance 。
- 在非高峰时段创建备份。

医学影像系统最佳实践

请参见典型医疗成像系统的以下最佳实践和一些要求：

- 请勿过量使用虚拟内存。
- 确保 vCPU 总数等于物理 CPU 数量。
- 如果环境较大，则需要专用 VLAN 。
- 使用专用 HA 集群配置数据库 VM 。
- 确保 VM OS VMDK 托管在快速第 1 层存储中。
- 与医疗映像系统供应商合作，确定准备 VM 模板以快速部署和维护的最佳方法。
- 管理，存储和生产网络需要对数据库进行 LAN 隔离，并为 VMware vMotion 提供隔离的 VLAN 。
- 使用名为的基于存储阵列的 NetApp 复制技术 "SnapMirror" 而不是基于vSphere的复制。
- 使用利用 VMware API 的备份技术；备份时间应在正常生产时间之外。

结论

通过在 FlexPod 上运行医疗影像环境，您的医疗保健组织可以看到员工工作效率的提高以及资本和运营支出的降低。FlexPod 提供经过 Cisco 和 NetApp 战略合作伙伴关系严格测试的预先验证的融合基础架构。它经过专门设计和设计，可提供可预测的低延迟系统性能和高可用性。这种方法可为医疗成像系统的用户提供卓越的用户体验和最佳的响应时间。

医疗成像系统的不同组件需要在 SMB/CIFS ， NFS ， ext4 和 NTFS 文件系统中存储数据。因此，您的基础架构必须通过 NFS ， SMB/CIFS 和 SAN 协议提供数据访问。NetApp 存储系统可从一个存储阵列支持这些协议。

高可用性，存储效率，基于 Snapshot 副本的计划快速备份，快速还原操作，用于灾难恢复的数据复制以及

FlexPod 存储基础架构功能均可提供行业领先的数据存储和管理系统。

追加信息

要了解有关本文档所述信息的更多信息，请查看以下文档和网站：

- 《采用 Cisco UCS 480 ML 的 FlexPod Datacenter for AI/ML 深度学习设计指南》

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_c480m5l_aiml_design.html"

- 采用 VMware vSphere 6.7 U1， Cisco UCS 第四代和 NetApp AFF A 系列的 FlexPod 数据中心基础架构

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_datacenter_vmware_netappaffa.html"

- 《使用 SnapCenter 解决方案备份 FlexPod 数据中心 Oracle 数据库简介》

  "https://www.netapp.com/us/media/sb-3999.pdf"

- FlexPod 数据中心与基于 Cisco UCS 和 NetApp AFF A 系列的 Oracle RAC 数据库

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orc12cr2_affaseries.html"

- 基于 Oracle Linux 的 FlexPod Datacenter 和 Oracle RAC

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orcrac_12c_bm.html"

- 适用于 Microsoft SQL Server 的 FlexPod

  "https://flexpod.com/solutions/use-cases/microsoft-sql-server/"

- Cisco 和 NetApp 的 FlexPod

  "https://flexpod.com/"

- "适用于 MongoDB 的 NetApp 解决方案" 解决方案简介（需要登录到 NetApp ）

  "https://fieldportal.netapp.com/content/734702"

- TR-4700： 适用于 Oracle 数据库的 SnapCenter 插件

  "https://www.netapp.com/us/media/tr-4700.pdf"

- NetApp 产品文档

  "https://www.netapp.com/us/documentation/index.aspx"

- 适用于虚拟桌面基础架构的 FlexPod (VDI) 解决方案

  "https://flexpod.com/solutions/use-cases/virtual-desktop-infrastructure/"

虚拟桌面基础架构

采用Citrix虚拟应用程序和桌面1912 LTSR和VMware vSphere 7的FlexPod 数据中心、最多可容纳6000个席位

NetApp Dre Jackson、NetApp公司Cisco Suresh ThopPay Jeff Nichols

本文档介绍了最多可供6000个最终用户计算用户使用的虚拟桌面基础架构的架构和设计。解决方案 在第五代Cisco UCS B200 M5刀片式服务器上进行虚拟化、可从AFF A400存储阵列通过FC SAN启动VMware vSphere 7.01 Update 1。虚拟桌面采用Citrix Provisioning Server 1912 LTSR和Citrix RDS/Citrix虚拟应用程序和桌面1912 LTSR提供支持、并混合使用RDS托管的共享桌面(6000)、池化和/或非持久托管的虚拟Windows 10桌面(5000)、 和使用Citrix Machine Creation Services (5000)配置的永久性托管虚拟Windows 10桌面、以支持用户群。本文档在适用情况下提供了有关此解决方案 的客户部署的最佳实践建议和规模估算准则。

"采用Citrix虚拟应用程序和应用程序的FlexPod Datacenter；桌面1912 LTSR和VMware vSphere 7、最多可容纳6000个席位"

采用VMware Horizon View 7.10、VMware vSphere 6.7 U2、Cisco UCS Manager 4.0和NetApp ONTAP 9.6的FlexPod 数据中心、最多可容纳7700个席位

NetApp公司Cisco Suresh ThopPay Vadim Lebedev

本文档提供了一个参考架构和设计指南、用于在FlexPod Datacenter上使用Cisco UCS和NetApp AFF A300以及NetApp ONTAP 数据管理软件的5000席位到6000席位桌面工作负载和最终用户计算环境。解决方案 包括基于VMware Horizon服务器的RDS Windows Server 2019会话、VMware Horizon永久性完整克隆Microsoft Windows 10虚拟桌面以及VMware vSphere 6.7U2上的VMware Horizon非永久性即时克隆Microsoft Windows 10虚拟桌面

"采用VMware Horizon View 7.10、VMware vSphere 6.7 U2、Cisco UCS Manager 4.0和NetApp ONTAP 9.6的FlexPod 数据中心、最多可容纳7700个席位"

使用Citrix和NVIDIA实现3D图形可视化—白皮书

本文档介绍了在采用SPECviewperf 13的Cisco UCS C240 M5和B200 M5服务器上使用NVIDIA Tesla P4、P6和P40卡的Citrix XenServer上Citrix XenDesktop的性能。

"使用Citrix和NVIDIA实现3D图形可视化—白皮书"

采用Citrix XenDesktop/XenApp 7.15和VMware vSphere 6.5 Update 1的FlexPod Datacenter、可容纳6000个席位

NetApp公司Cisco Chris Rodrigueev的Vadim Lebedev

本文档提供了一个参考架构、用于使用基于Cisco UCS且采用NetApp全闪存FAS (AFF) A300存储和VMware vSphere ESXi 6.5虚拟机管理程序平台的Citrix XenApp/XenDesktop 7.15来设计虚拟桌面和应用程序。

桌面和应用程序虚拟化的格局正在不断变化。全新的M5高性能Cisco UCS刀片式服务器和Cisco UCS统一网络结构作为FlexPod 成熟的基础架构的一部分、与最新一代的NetApp AFF 存储相结合、形成了一个更紧凑、更强大、更可靠、更高效的平台。

"采用Citrix XenDesktop/XenApp 7.15和VMware vSphere 6.5 Update 1的FlexPod Datacenter、可容纳6000个席位"

采用VMware Horizon View 7.3的FlexPod Datacenter和采用Cisco UCS Manager 3.2的VMware vSphere 6.5 Update 1、可容纳5000个席位

NetApp公司Cisco David Arnette Ramesh Guduru

本文档提供了一个参考架构、设计指南、以及在采用FlexPod UCS和NetApp全闪存FAS (AFF) A300存储的Datacenter上为多达5000个席位的混合工作负载最终用户计算环境进行的部署。解决方案 包括基于VMware Horizon服务器的远程桌面服务器托管会话、VMware Horizon永久性Microsoft Windows 10虚拟桌面以及VMware vSphere 6.5上的VMware Horizon非永久性Microsoft Windows 10即时克隆虚拟桌面。

"采用VMware Horizon View 7.3的FlexPod Datacenter和采用Cisco UCS Manager 3.2的VMware vSphere 6.5 Update 1、可容纳5000个席位"

采用VMware Horizon View 7.10、VMware vSphere 6.7 U2、Cisco UCS Manager 4.0和NetApp ONTAP 9.6的FlexPod 数据中心、最多可容纳7700个席位

NetApp公司Cisco Suresh ThopPay Vadim Lebedev

本文档为采用FlexPod UCS、NetApp AFF A300和NetApp ONTAP 数据管理软件的Datacenter上的5000席位到6000席位桌面工作负载最终用户计算环境提供了参考架构和设计指南。解决方案 包括基于VMware Horizon服务器的RDS Windows Server 2019会话、VMware Horizon永久性、完整克隆的Microsoft Windows 10虚拟桌面以及VMware vSphere 6.7 U2上的VMware Horizon非持久即时克隆Microsoft Windows 10虚拟桌面。

"采用VMware Horizon View 7.10、VMware vSphere 6.7 U2、Cisco UCS Manager 4.0和NetApp ONTAP 9.6的FlexPod 数据中心、最多可容纳7700个席位"

现代应用程序

FlexPod 数据中心、用于将人工智能和机器学习与Cisco UCS 480 ML相结合、用于深度学习—设计

NetApp公司Cisco Arvind Ramakrishnan的Haseeb Niazi

本文档详细介绍了如何将Cisco UCS C480 ML M5平台集成到FlexPod Datacenter解决方案 中、以便在融合基础架构中提供统一的AI和ML功能。通过让客户能够使用人工智能和机器学习功能以及用于管理传统FlexPod 系统的熟悉工具来管理服务器、大大降低了部署深度学习平台的管理开销和成本。此CVD中提供的设计还包括其他Cisco UCS平台、例如具有两个NVIDIA T4 GPU的C220 M5服务器以及配有两个NVIDIA V100 32 Gb PCIe卡的C240 M5服务器、作为处理并发AI和ML工作负载的附加选项。

"FlexPod 数据中心、用于将人工智能和机器学习与Cisco UCS 480 ML相结合、用于深度学习—设计"

使用FlexPod 在Cisco容器平台上部署NetApp Trident CSI插件

本文档提供了在FlexPod 解决方案 中的Cisco容器平台Kubernetes租户集群上部署NetApp Trident容器存储接口(CSI)插件的分步过程。

"使用FlexPod 在Cisco容器平台上部署NetApp Trident CSI插件"

适用于OpenShift容器平台的FlexPod 数据中心4—部署

NetApp公司Cisco Alan Cowles的Haseeb Niazi

Red Hat OpenShift是一款企业级Kubernetes容器平台、用于管理混合云和多云部署。Red Hat OpenShift容器平台提供了混合云、企业容器以及Kubernetes开发和部署所需的一切。它包括企业级Linux操作系统、容器运行时、网络连接、监控、容器注册表、 身份验证和授权解决方案。

将Red Hat OpenShift与FlexPod Datacenter解决方案 相结合、可以简化容器基础架构的部署和管理。客户可以从提高效率、改善数据保护、降低风险以及灵活扩展这种高可用性企业级基础架构堆栈以满足新业务需求中受益。经过预先验证的融合解决方案 方法可帮助企业实现所有应用程序现代化和数字化转型计划所需的速度、灵活性和扩展性。

"适用于OpenShift容器平台的FlexPod 数据中心4—部署"

采用适用于容器管理的Docker企业版的FlexPod 数据中心

来自NetApp Uday Shetty、Docker的Cisco Amit Borulkar、Cisco John George的Muhammad Afzal

Docker是全球领先的软件容器平台、可供开发人员和IT运营人员随时随地构建、交付和运行分布式应用程序。随着微服务架构塑造下一代IT、对整体式应用程序进行大量投资的企

业正在寻找方法、将Docker作为一种策略、用于实现应用程序架构现代化并保持企业竞争力和成本效益。容器化可提供开发人员和IT运营在任何基础架构中构建和部署应用程序所需的灵活性、控制力和可移动性。通过Docker平台、分布式应用程序可以轻松地组成一个轻型应用程序容器、该容器可以动态更改、但不会造成中断。此功能可使应用程序在本地物理机或虚拟机上、数据中心内以及不同云服务提供商的网络上运行的开发、测试和生产环境中均可移植。

"采用适用于容器管理的Docker企业版的FlexPod 数据中心"

适用于OpenShift容器平台4的FlexPod 数据中心—设计

NetApp公司Cisco Alan Cowles的Haseeb Niazi

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 提供了一个集成架构、其中整合了计算、存储和网络设计的最佳实践、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。

"适用于OpenShift容器平台4的FlexPod 数据中心—设计"

FlexPod 数据中心、用于将AI和ML与Cisco UCS 480 ML相结合、用于深度学习—部署

NetApp公司Cisco Arvind Ramakrishnan的Haseeb Niazi

本文档提供了有关将Cisco UCS C480 ML M5平台集成到FlexPod 数据中心解决方案 中的部署详细信息和指导、以便在融合基础架构中提供统一的AI和ML功能。本文档还介绍了Cisco UCS C220和C240平台上的NVIDIA GPU配置。有关此解决方案 中使用的平台和技术的详细设计讨论、请参见 "FlexPod 数据中心、用于将人工智能和机器学习与Cisco UCS 480 ML相结合、用于深度学习设计"。

"FlexPod 数据中心、用于将AI和ML与Cisco UCS 480 ML相结合、用于深度学习—部署"

在Cisco UCS上使用VMware和NVIDIA实现3D图形可视化—白皮书

本文档介绍了在Cisco UCS C240 M5机架式服务器和B200 M5刀片式服务器上使用NVIDIA Tesla P4、P6和P40解决方案 的VMware ESXi虚拟机管理程序和VMware Horizon的性能。

"在Cisco UCS上使用VMware和NVIDIA实现3D图形可视化—白皮书"

使用Citrix和NVIDIA实现3D图形可视化—白皮书

本文档介绍了在采用SPECviewperf 13的Cisco UCS C240 M5和B200 M5服务器上使用NVIDIA Tesla P4、P6和P40卡的Citrix XenServer上Citrix XenDesktop的性能。

"使用Citrix和NVIDIA实现3D图形可视化—白皮书"

FlexPod Express

采用 Cisco UCS C 系列和 NetApp AFF C190 系列的 FlexPod Express 设计指南

NVA-1139-design ： 采用 Cisco UCS C 系列和 NetApp AFF C190 系列的 FlexPod Express

NetApp 公司 Savita Kumari

与以下合作伙伴：

行业趋势表明，数据中心正在向共享基础架构和云计算转型。此外，企业还希望为远程办公室和分支机构提供一个简单有效的解决方案，以使用他们在数据中心熟悉的技术。

FlexPod Express 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（ Cisco UCS ），Cisco Nexus 系列交换机和 NetApp AFF 系统构建。FlexPod Express 的各个组件与 FlexPod 数据中心的对应组件一样，可以在较小规模的整个 IT 基础架构环境中实现管理协作。FlexPod 数据中心和 FlexPod Express 是虚拟化以及裸机操作系统和企业工作负载的最佳平台。

"接下来：计划摘要。"

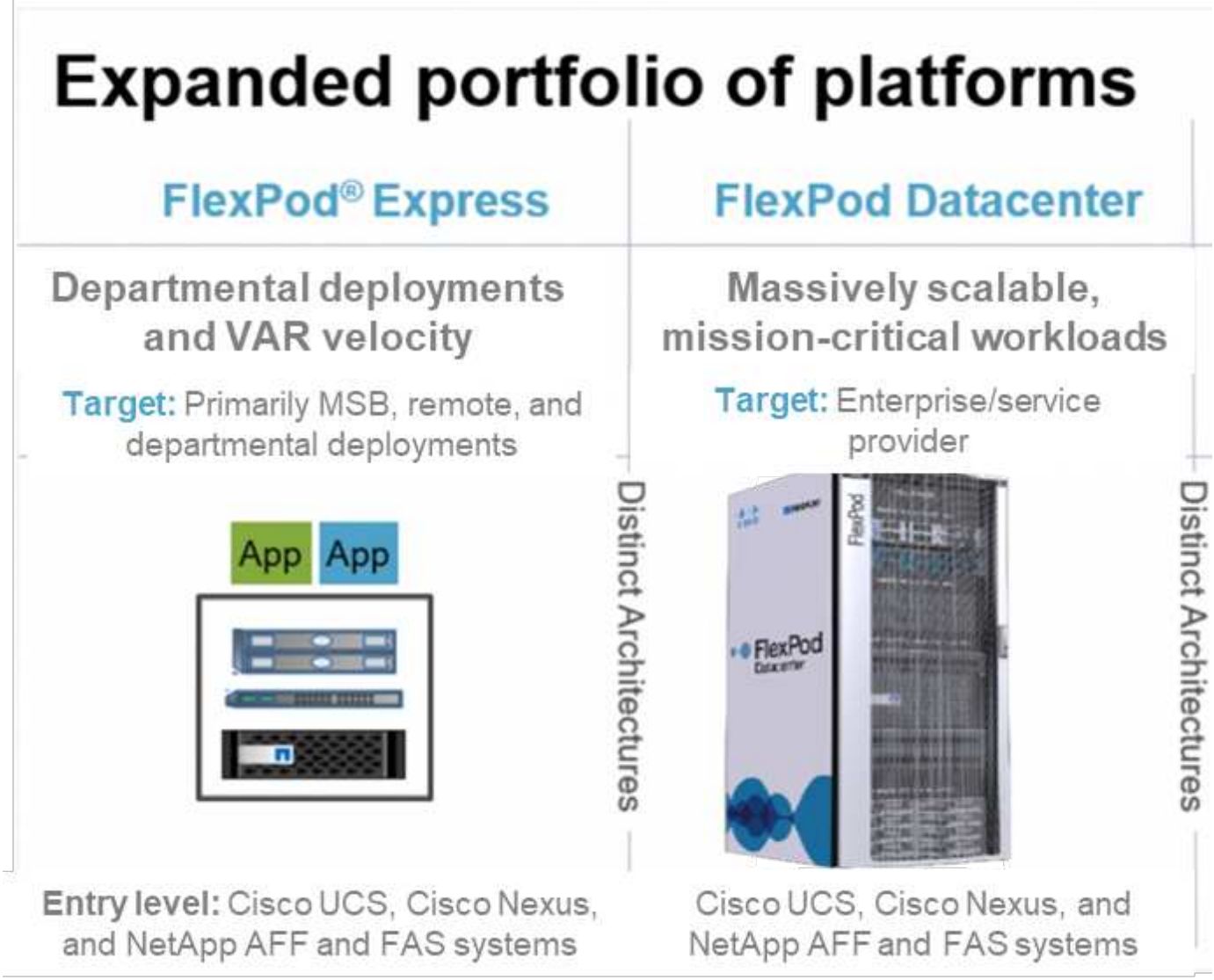
计划摘要

FlexPod 融合基础架构产品组合

FlexPod 参考架构以 Cisco 验证设计（ CVD ）或 NetApp 验证架构（ NVA ）的形式提供。如果给定 CVD 或 NVA 的差异不会导致部署不受支持的配置，则允许根据客户要求进行差异。

如下图所示， FlexPod 产品组合包括以下解决方案： FlexPod Express 和 FlexPod Datacenter 。

- * FlexPod Express* 是一款采用 Cisco 和 NetApp 技术的入门级解决方案。
- FlexPod 数据中心 * 为各种工作负载和应用程序提供了最佳的多用途基础。



经验证的 **NetApp** 架构计划

经验证的 NetApp 架构计划为客户提供经过验证的 NetApp 解决方案架构。NVA 解决方案具有以下特性：

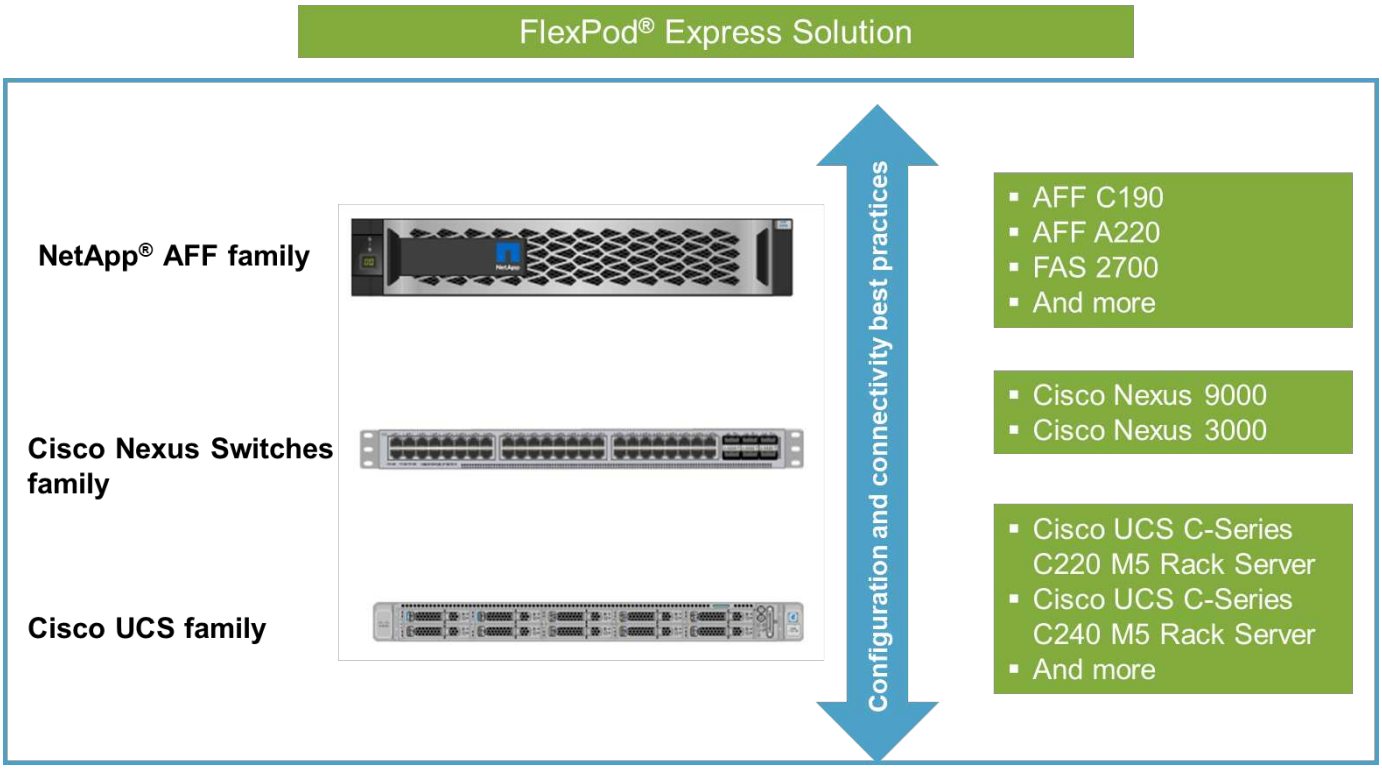
- 经过全面测试
- 具有规范性
- 最大限度地降低部署风险
- 加快上市速度本指南详细介绍了采用 VMware vSphere 的 FlexPod Express 的设计。

此外，此设计还利用全新的 AFF C190 系统作为虚拟机管理程序节点，该系统运行 NetApp ONTAP 9.6 软件，Cisco Nexus 31108 交换机和 Cisco UCS C220 M5 服务器。

解决方案概述

FlexPod Express 专为运行混合虚拟化工作负载而设计。它面向远程办公室和分支机构以及中小型企业。对于希望为特定目的实施专用解决方案的大型企业来说，它也是最佳选择。这款全新的解决方案 for FlexPod Express 新增了 NetApp ONTAP 9.6 ， NetApp AFF C190 系统和 VMware vSphere 6.7U2 等新技术。

下图显示了 FlexPod Express 解决方案中包含的硬件组件。

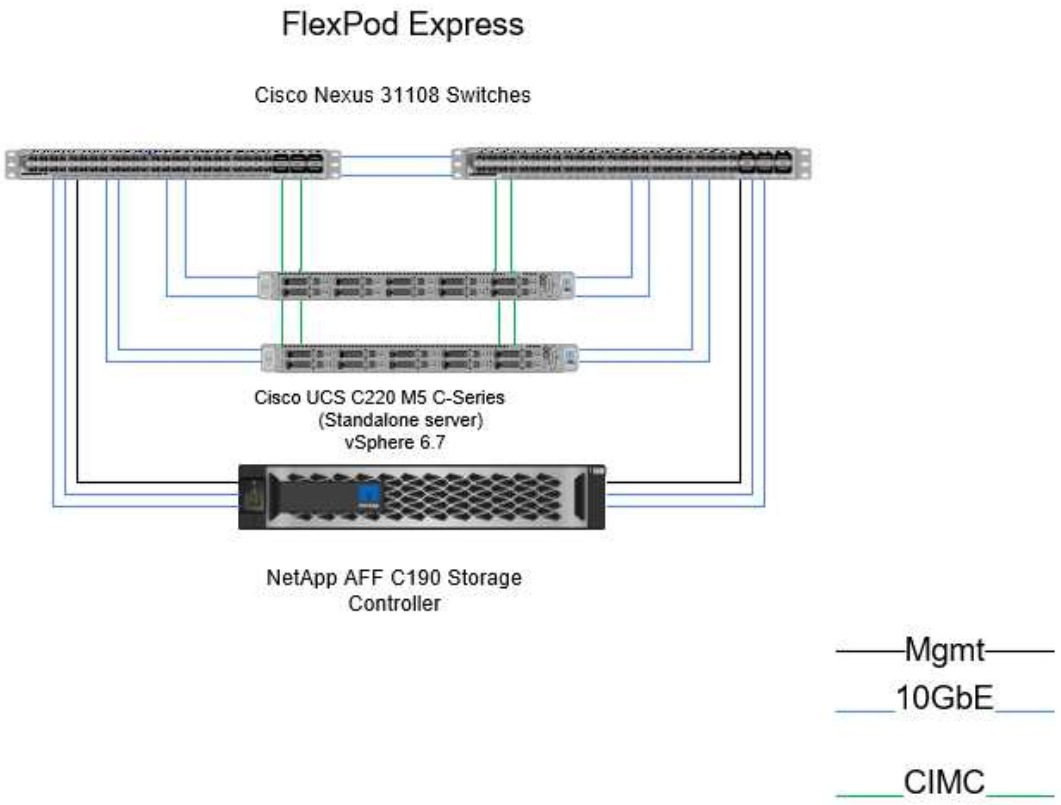


目标受众

本文档面向希望利用专为提高 IT 效率和实现 IT 创新而构建的基础架构的人员。本文档的受众包括但不限于销售工程师，现场顾问，专业服务人员， IT 经理， 合作伙伴工程师和客户。

解决方案技术

此解决方案利用了 NetApp ， Cisco 和 VMware 的最新技术。它采用全新的 NetApp AFF C190 系统，该系统运行 ONTAP 9.6 软件，双 Cisco Nexus 31108 交换机以及运行 VMware vSphere 6.7U2 的 Cisco UCS C220 M5 机架式服务器。下图所示的这一经过验证的解决方案使用万兆以太网（ 10GbE ）技术。此外，还提供了有关如何通过一次添加两个虚拟机管理程序节点进行扩展的指导，以便 FlexPod 快速架构能够适应组织不断变化的业务需求。



"接下来：技术要求。"

技术要求

FlexPod Express 需要硬件和软件组件的组合，具体取决于所选虚拟机管理程序和网络速度。此外， FlexPod Express 还以两个单元的形式列出了向系统添加虚拟机管理程序节点所需的硬件组件。

硬件要求

无论选择何种虚拟机管理程序，所有 FlexPod 快速配置都使用相同的硬件。因此，即使业务需求发生变化，您也可以在同一个 FlexPod Express 硬件上使用不同的虚拟机管理程序。

下表列出了此 FlexPod 快速配置以及实施此解决方案所需的硬件组件。在任何解决方案实施中使用的硬件组件可能会因客户要求而异。

硬件	数量
AFF C190 双节点集群	1.
Cisco UCS C220 M5 服务器	2.
Cisco Nexus 31108 交换机	2.
适用于 Cisco UCS C220 M5 机架式服务器的 Cisco UCS 虚拟接口卡（ VIC ） 1457	2.

软件要求

下表列出了实施 FlexPod Express 解决方案架构所需的软件组件。

软件	**version**	详细信息
Cisco 集成管理控制器（CIMC）	4.0.4	适用于 C220 M5 机架式服务器
Cisco NX-OS	7.0 （3） i7 （6）	适用于 Cisco Nexus 31108 交换机
NetApp ONTAP	9.6	适用于 NetApp AFF C190 控制器

下表列出了在 FlexPod Express 上实施所有 VMware vSphere 所需的软件。

软件	**version**
VMware vCenter Server 设备	6.7U2
VMware vSphere ESXi	6.7U2
适用于 ESXi 的 NetApp VAAI 插件	1.1.2
NetApp 虚拟存储控制台	9.6

"接下来：设计选择。"

设计选择

本节中列出的技术是在架构设计阶段选择的。每个技术在 FlexPod Express 基础架构解决方案中都有一个特定用途。

采用 **ONTAP 9.6** 的 **NetApp AFF C190** 系列

此解决方案利用了两种最新的 NetApp 产品： NetApp AFF C190 系统和 ONTAP 9.6 软件。

AFF C190 系统

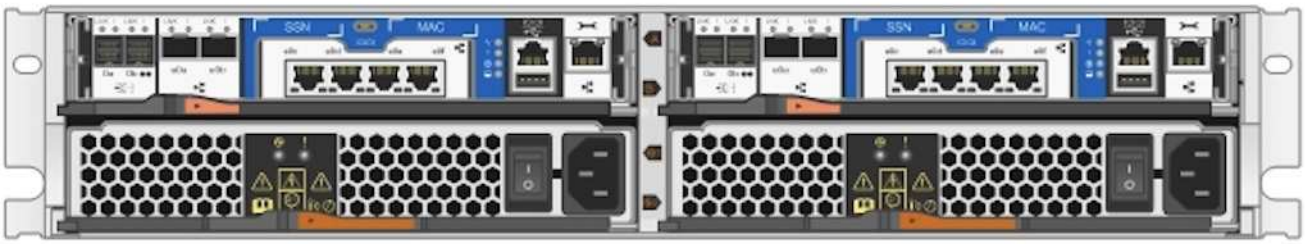
目标群体是希望以经济实惠的价格利用全闪存技术打造现代化 IT 基础架构的客户。AFF C190 系统附带了新的 ONTAP 9.6 和闪存捆绑包许可，这意味着具有以下功能：

- CIFS， NFS， iSCSI 和 FCP
- NetApp SnapMirror 数据复制软件， NetApp SnapVault 备份软件， NetApp SnapRestore 数据恢复软件，NetApp SnapManager 存储管理软件产品套件和 NetApp SnapCenter 软件
- FlexVol 技术
- 重复数据删除，数据压缩和数据缩减
- 精简配置
- 存储 QoS
- NetApp RAID DP 技术
- NetApp Snapshot 技术
- FabricPool

下图显示了主机连接的两个选项。

下图显示了可插入 SFP+ 模块的 UTA 2 端口。

下图显示了通过传统 RJ-45 以太网缆线连接的 10GBASE-T 端口。



对于 10GBASE-T 端口选项，您必须使用基于 10GBASE-T 的上行链路交换机。

AFF C190 系统仅提供 960 GB SSD 。您可以从四个扩展阶段中进行选择：

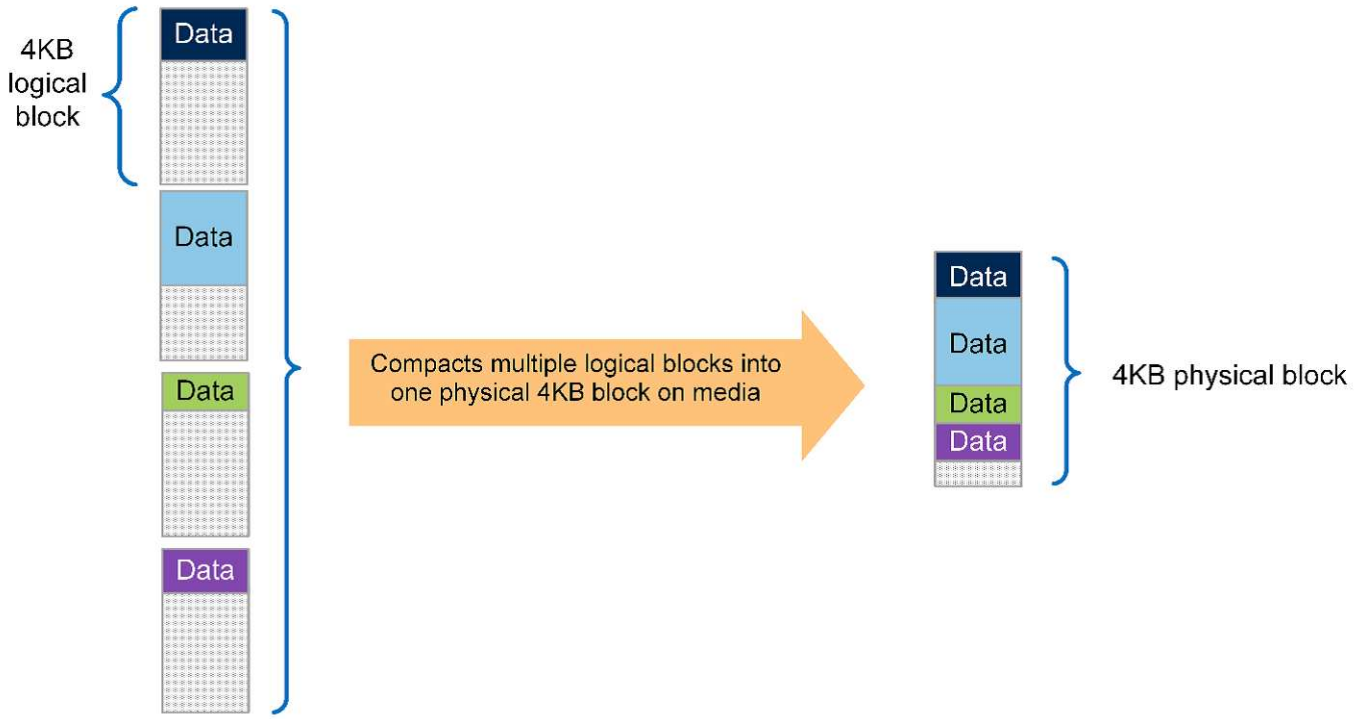
- 8 个 960 GB
- 12 个 960 GB
- 18 个 960 GB
- 24 个 960 GB

有关 AFF C190 硬件系统的完整信息，请参见 "NetApp AFF C190 全闪存阵列页面"。

ONTAP 9.6 软件

NetApp AFF C190 系统使用全新的 ONTAP 9.6 数据管理软件。ONTAP 9.6 是行业领先的企业级数据管理软件。它将更高级别的精简性和灵活性与强大的数据管理功能，存储效率和领先的云集成相结合。

ONTAP 9.6 具有多种非常适合 FlexPod Express 解决方案的功能。最重要的是 NetApp 对存储效率的承诺，存储效率是小型部署最重要的功能之一。ONTAP 9.6 提供了 NetApp 存储效率的标志功能，例如重复数据删除，数据压缩，数据缩减和精简配置。NetApp WAFL 系统始终会写入 4 KB 块；因此，如果这些块未使用分配的 4 KB 空间，则数据缩减会将多个块合并为一个 4 KB 块。下图说明了此过程。



ONTAP 9.6 现在支持为 NVMe 卷提供可选的 512 字节块大小。此功能可与本机使用 512 字节块的 VMware 虚拟机文件系统（ VMFS ）配合使用。您可以保留默认的 4 k 大小，也可以选择设置 512 字节的块大小。

ONTAP 9.6 中的其他增强功能包括：

- * NetApp 聚合加密（ NAE ）。 * NAE 在聚合级别分配密钥，从而对聚合中的所有卷进行加密。此功能允许在聚合级别对卷进行加密和重复数据删除。
- * NetApp ONTAP FlexGroup 卷增强功能 * 。在 ONTAP 9.6 中，您可以轻松重命名 FlexGroup 卷。无需创建要将数据迁移到的新卷。也可以使用 ONTAP 系统管理器或命令行界面减小卷大小。
- * FabricPool 增强功能。 * ONTAP 9.6 增加了对对象存储作为云层的额外支持。此列表还添加了对 Google Cloud 和 Alibaba Cloud Object Storage Service （ OSS ）的支持。FabricPool 支持多个对象存储，包括 AWS S3 ， Azure Blob ， IBM Cloud 对象存储和 NetApp StorageGRID 基于对象的存储软件。
- * SnapMirror 增强功能 * 。在 ONTAP 9.6 中，新的卷复制关系在离开源阵列之前会默认加密，并在 SnapMirror 目标上解密。

Cisco Nexus 3000 系列

Cisco Nexus 31108PC-V 是一款基于 10 Gbps SFP+ 的机架顶部（ ToR ）交换机，具有 48 个 SFP+ 端口和 6 个 QSFP28 端口。每个 SFP+ 端口可以以 100 Mbps ， 10 Gbps 的速率运行，每个 QSFP28 端口可以在原生 100 Gbps 或 40 Gbps 模式或 4 个 10 Gbps 模式下运行，从而提供灵活的迁移选项。此交换机是真正的无 PHY 交换机，针对低延迟和低功耗进行了优化。

Cisco Nexus 31108PC-V 规范包括以下组件：

- 对于 31108PC-V ，交换机容量和转发速率高达 2.2 Tbps
- 48 个 SFP 端口支持 1 和 10 千兆以太网（ 10GbE ）； 6 个 QSFP28 端口支持每个 4 个 10GbE 或 40GbE 或 100GbE

下图显示了 Cisco Nexus 31108PC-V 交换机。

有关 Cisco Nexus 31108PC-V 交换机的详细信息，请参见 "Cisco Nexus 3172PQ ， 3172TQ ， 3172TQ-32T ， 3172PQ-XL 和 3172TQ-XL 交换机产品规格"。

Cisco UCS C 系列

之所以选择 Cisco UCS C 系列机架式服务器来支持 FlexPod Express ，是因为它具有多种配置选项，可以根据 FlexPod Express 部署中的特定要求进行定制。

Cisco UCS C 系列机架式服务器采用行业标准外形规格提供统一计算，以降低 TCO 并提高灵活性。

Cisco UCS C 系列机架式服务器具有以下优势：

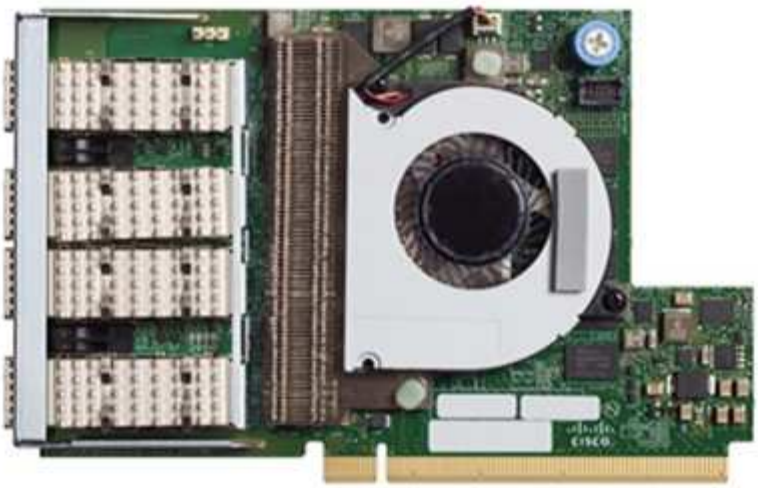
- 与外形规格无关的 Cisco UCS 入门点
- 简化并快速部署应用程序
- 将统一计算创新技术和优势扩展到机架式服务器
- 通过熟悉的机架包装提供独特优势，增加客户的选择

如上图所示， Cisco UCS C220 M5 机架式服务器是业内用途最广泛的通用企业基础架构和应用程序服务器之一。它是一款高密度双插槽机架式服务器，可为包括虚拟化，协作和裸机应用程序在内的各种工作负载提供行业领先的性能和效率。Cisco UCS C 系列机架式服务器可以作为独立服务器部署，也可以作为 Cisco UCS 的一部分部署，以利用 Cisco 基于标准的统一计算创新技术，帮助客户降低 TCO 并提高业务灵活性。

有关 C220 M5 服务器的详细信息，请参见 "Cisco UCS C220 M5 机架式服务器数据表"。

适用于 **C220 M5** 机架式服务器的 **Cisco UCS VIC 1457** 连接

下图所示的 Cisco UCS VIC 1457 适配器是一个四端口小型可插拔（ SFP28 ）模块化主板 LAN （ mLOM ）卡，专为 M5 代 Cisco UCS C 系列服务器而设计。此卡支持 10/25Gbps 以太网或 FCoE 。该卡可以向主机提供符合 PCIe 标准的接口，这些接口可以动态配置为 NIC 或 HBA 。



有关 Cisco UCS VIC 1457 适配器的完整信息，请参见 "Cisco UCS 虚拟接口卡 1400 系列产品规格"。

VMware vSphere 6.7U2

VMware vSphere 6.7U2 是适用于 FlexPod Express 的虚拟机管理程序选项之一。通过 VMware vSphere ，企业可以减少电耗和散热占用空间，同时确认已购买的计算容量已充分利用。此外， VMware vSphere 还支持在 vSphere 主机集群（维护模式下为 VMware Distributed Resource Scheduler 或 VMware DRS-MM ）之间实现硬件故障保护（ VMware 高可用性或 VMware HA ）和计算资源负载平衡。

由于 VMware vSphere 6.7U2 仅重新启动内核，因此客户可以快速启动，从而加载 vSphere ESXi ，而无需重新启动硬件。vSphere 6.7U2 vSphere 客户端（基于 HTML5 的客户端）具有一些新的增强功能，例如具有代码捕获和 API Explore 的开发人员中心。通过代码捕获，您可以在 vSphere 客户端中记录您的操作，以提供简单，可用的代码输出。vSphere 6.7U2 还包含维护模式下的 DRS （ DRS-MM ）等新功能。

VMware vSphere 6.7U2 提供以下功能：

- VMware 正在弃用外部 VMware Platform Services Controller （ PSC ）部署模式。

  从下一个主要 vSphere 版本开始，外部 PSC 将不是可用选项。

- 为备份和还原 vCenter Server 设备提供了新的协议支持。将 NFS 和 SMB 作为受支持的协议选项进行介绍，总共可支持多达 7 个协议（ HTTP ， HTTPS ， FTP ， FTPS ， SCP ， NFS 和 SMB ）。
- 使用内容库时的新增功能。现在，如果为 vCenter Server 配置了增强型链接模式，则可以在内容库之间同步原生 VM 模板。
- 更新到 "客户端插件页面"。
- VMware vSphere Update Manager 还为 vSphere 客户端添加了增强功能。您可以在一个屏幕上执行附加检查合规性和修复操作。

有关 VMware vSphere 6.7 U2 的详细信息，请参见 "VMware vSphere 博客页面"。

有关 VMware vCenter Server 6.7 U2 更新的详细信息，请参见 "发行说明"。

虽然此解决方案已通过 vSphere 6.7U2 的验证，但它支持通过其他组件认证的任何 vSphere 版本 "NetApp 互操作性表工具（ IMT ）"。NetApp 建议您部署下一个版本的 vSphere 以修复其问题并增强其功能。

启动架构

FlexPod 快速启动架构支持的选项包括：

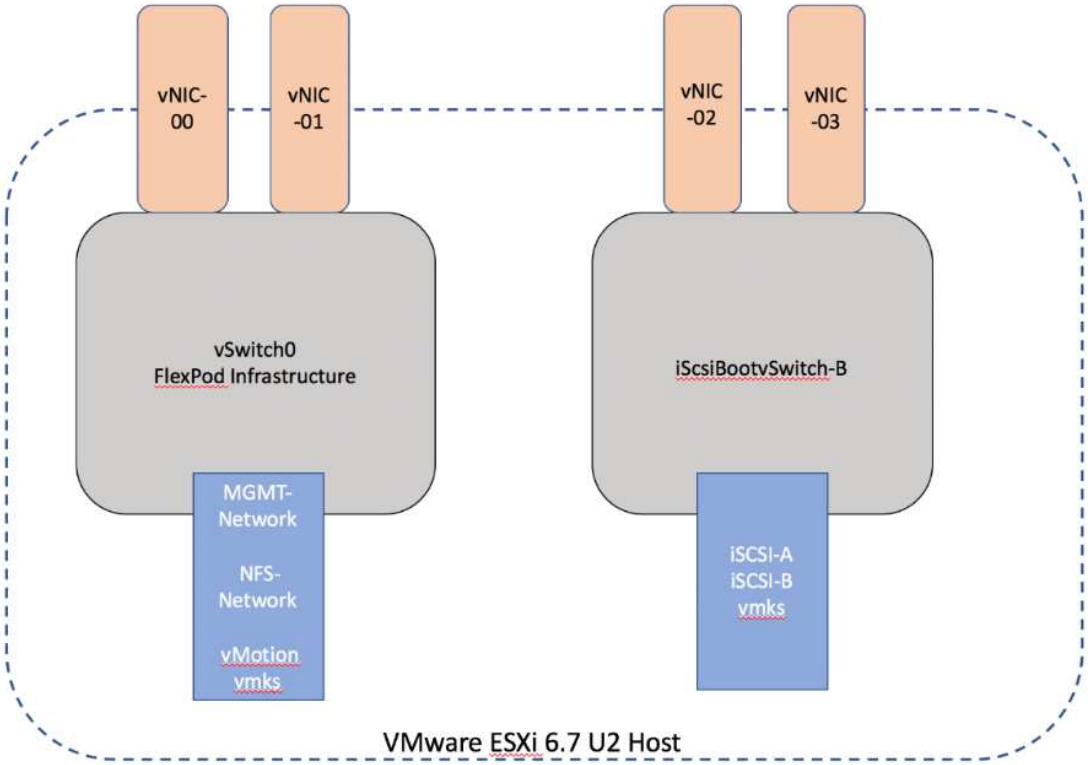
- iSCSI SAN LUN
- Cisco FlexFlash SD 卡
- 本地磁盘

FlexPod 数据中心可从 iSCSI LUN 启动；因此，也可通过对 FlexPod Express 使用 iSCSI 启动来增强解决方案的易管理性。

ESXi 主机虚拟网络接口卡布局

Cisco UCS VIC 1457 具有四个物理端口。此解决方案验证包括使用 ESXi 主机的中的这四个物理端口。如果 NIC 数量较小或较大，则可能具有不同的 vmnic 编号。

在 iSCSI 启动实施中， iSCSI 启动需要单独的虚拟网络接口卡（ Virtual Network Interface Card ， vNIC ）来进行 iSCSI 启动。这些 VNIC 使用相应网络结构的 iSCSI VLAN 作为原生 VLAN ，并连接到 iSCSI 启动 VSwitch ，如下图所示。



"接下来：总结。"

结论

经过 FlexPod 快速验证的设计是一种简单而有效的解决方案，它使用行业领先的组件。通过扩展虚拟机管理程序平台并为其提供选项， FlexPod Express 可以根据特定业务需求进

行定制。FlexPod Express 专为中小型企业，远程办公室和分支机构以及其他需要专用解决方案的企业而设计。

"下一步：从何处查找追加信息。"

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请参见以下文档和网站：

- AFF 和 FAS 系统文档中心

  "https://docs.netapp.com/platstor/index.jsp"

- AFF 文档资源页面

  "https://www.netapp.com/us/documentation/all-flash-fas.aspx"

- 《使用 VMware vSphere 6.7 和 NetApp AFF C190 的 FlexPod 快速部署指南》（正在进行中）
- NetApp 文档

  "https://docs.netapp.com"

《采用 Cisco UCS C 系列和 NetApp AFF C190 系列的 FlexPod 快速部署指南》

NVA-1142-Deploy：采用 Cisco UCS C 系列和 NetApp AFF C190 系列的 FlexPod Express — NVA 部署

NetApp 公司 Savita Kumari

行业趋势表明，数据中心正在向共享基础架构和云计算进行大规模转型。此外，企业还希望为使用数据中心所熟悉的技术的远程办公室和分支机构提供一个简单有效的解决方案。

FlexPod ® Express 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（ Cisco UCS ），Cisco Nexus 系列交换机和 NetApp ® 存储技术构建。FlexPod 快速系统中的组件与 FlexPod 数据中心的对应组件一样，可以在较小规模的整个 IT 基础架构环境中实现管理协作。FlexPod 数据中心和 FlexPod Express 是虚拟化以及裸机操作系统和企业工作负载的最佳平台。

FlexPod 数据中心和 FlexPod Express 提供基线配置，并可灵活调整规模和进行优化，以满足多种不同的使用情形和要求。现有的 FlexPod 数据中心客户可以使用他们习惯使用的工具来管理其 FlexPod 快速系统。新的 FlexPod Express 客户可以随着环境的增长轻松过渡到管理 FlexPod 数据中心。

FlexPod Express 是远程办公室和分支机构以及中小型企业的最佳基础架构基础。对于希望为专用工作负载提供基础架构的客户来说，它也是最佳解决方案。

FlexPod Express 提供了一个易于管理的基础架构，几乎适合任何工作负载。

解决方案概述

此 FlexPod Express 解决方案是 FlexPod 融合基础架构计划的一部分。

FlexPod 融合基础架构计划

FlexPod 参考架构以 Cisco 验证设计（CVD）或 NetApp 验证架构（NVA）的形式提供。如果给定 CVD 或 NVA 不会产生不受支持的配置，则允许根据客户要求进行差异。

FlexPod 计划包括两个解决方案： FlexPod Express 和 FlexPod Datacenter 。

- * FlexPod Express* 为客户提供了采用 Cisco 和 NetApp 技术的入门级解决方案。
- * FlexPod Datacenter 。 * 为各种工作负载和应用程序提供最佳的多用途基础。

经验证的 **NetApp** 架构计划

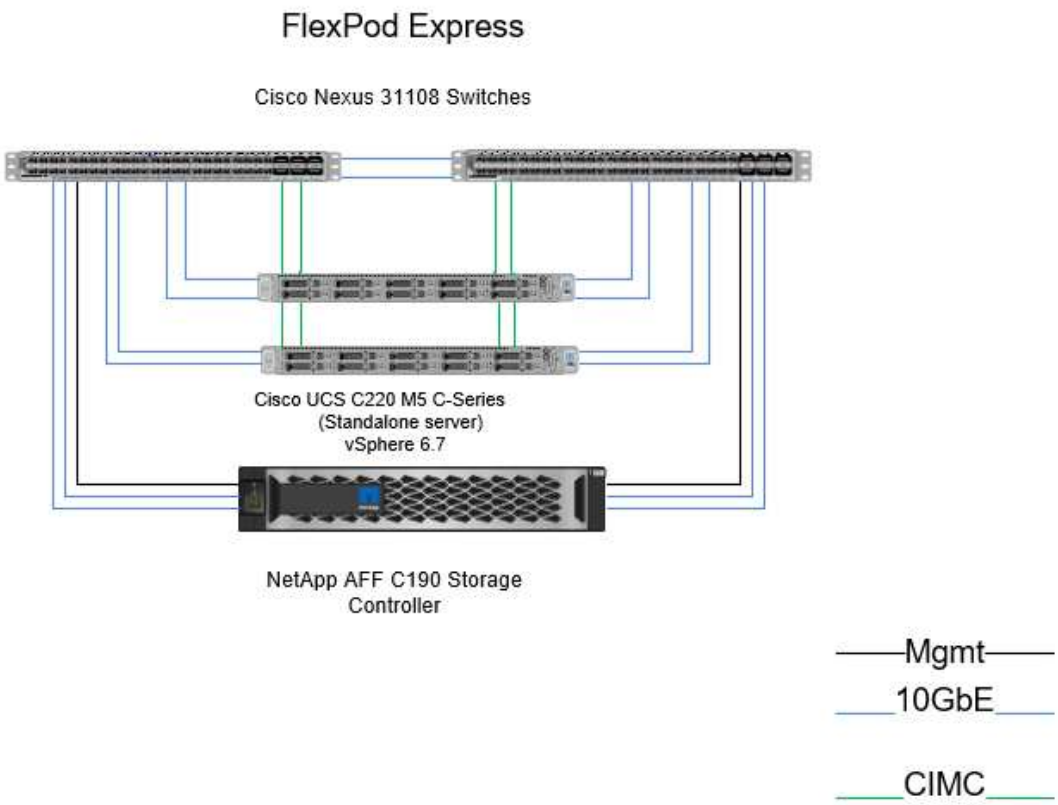
经验证的 NetApp 架构计划为客户提供经过验证的 NetApp 解决方案架构。经验证的 NetApp 架构可提供具有以下品质的 NetApp 解决方案架构：

- 经过全面测试
- 规范性
- 最大限度地降低部署风险
- 加快上市速度

本指南详细介绍了采用 VMware vSphere 的 FlexPod Express 的设计。此外，此设计还使用全新的 AFF C190 系统（运行 NetApp ONTAP ® 9.6 ）， Cisco Nexus 31108 和 Cisco UCS C 系列 C220 M5 服务器作为虚拟机管理程序节点。

解决方案技术

此解决方案利用了 NetApp ， Cisco 和 VMware 的最新技术。此解决方案采用运行 ONTAP 9.6 的全新 NetApp AFF C190 ，双 Cisco Nexus 31108 交换机和运行 VMware vSphere 6.7U2 的 Cisco UCS C220 M5 机架式服务器。此经过验证的解决方案采用 10GbE 技术。此外，还提供了有关如何通过一次添加两个虚拟机管理程序节点来扩展计算容量的指导，以使 FlexPod 快速架构能够适应组织不断变化的业务需求。



要高效使用 VIC 1457 上的四个物理 10GbE 端口，请在每个服务器与顶部机架交换机之间另外创建两条链路。

使用情形摘要

FlexPod Express 解决方案可应用于多种使用情形，包括以下情形：

- 远程办公室或分支机构
- 中小型企业
- 需要经济高效的专用解决方案的环境

FlexPod Express 最适合虚拟化和混合工作负载。虽然此解决方案已通过 vSphere 6.7U2 的验证，但它支持任何经 NetApp 互操作性表工具认证可与其他组件配合使用的 vSphere 版本。NetApp 建议部署 vSphere 6.7U2 ，因为它具有以下修复和增强功能：

- 为备份和还原 vCenter Server 设备提供了新的协议支持，包括 HTTP ， HTTPS ， FTP ， FTPS ， SCP ， NFS 和 SMB 。
- 利用内容库时新增功能。现在，如果为 vCenter Server 配置了增强型链接模式，则可以在内容库之间同步原生 VM 模板。
- 更新了客户端插件页面。
- 在 vSphere Update Manager （ VUM ）和 vSphere 客户端中增加了增强功能。现在，您可以在一个屏幕上执行连接，检查合规性和修复操作。

有关此主题的详细信息，请参见 "vSphere 6.7U2 页面" 和 "《 vCenter Server 6.7U2 发行说明》"。

技术要求

FlexPod 快速系统需要硬件和软件组件的组合。FlexPod Express 还介绍了以两个单位向系统添加虚拟机管理程序节点所需的硬件组件。

硬件要求

无论选择何种虚拟机管理程序，所有 FlexPod 快速配置都使用相同的硬件。因此，即使业务需求发生变化，您也可以在同一个 FlexPod Express 硬件上使用不同的虚拟机管理程序。

下表列出了 FlexPod 快速配置和实施所需的硬件组件。在任何解决方案实施中使用的硬件组件可能会因客户要求而异。

硬件	数量
AFF C190 双节点集群	1.
Cisco C220 M5 服务器	2.
Cisco Nexus 31108PC-V 交换机	2.
适用于 Cisco UCS C220 M5 机架式服务器的 Cisco UCS 虚拟接口卡（ VIC ） 1457	2.

下表列出了实施 10GbE 所需的硬件以及基本配置。

硬件	数量
Cisco UCS C220 M5 服务器	2.
Cisco VIC 1457	2.

软件要求

下表列出了实施 FlexPod 快速解决方案架构所需的软件组件。

软件	**version**	详细信息
Cisco 集成管理控制器（CIMC）	4.0.4	适用于 Cisco UCS C220 M5 机架式服务器
Cisco nenic 驱动程序	1.0.29	适用于 VIC 1457 接口卡
Cisco NX-OS	7.0 （3） i7 （6）	适用于 Cisco Nexus 31108PC-V 交换机
NetApp ONTAP	9.6	适用于 AFF C190 控制器

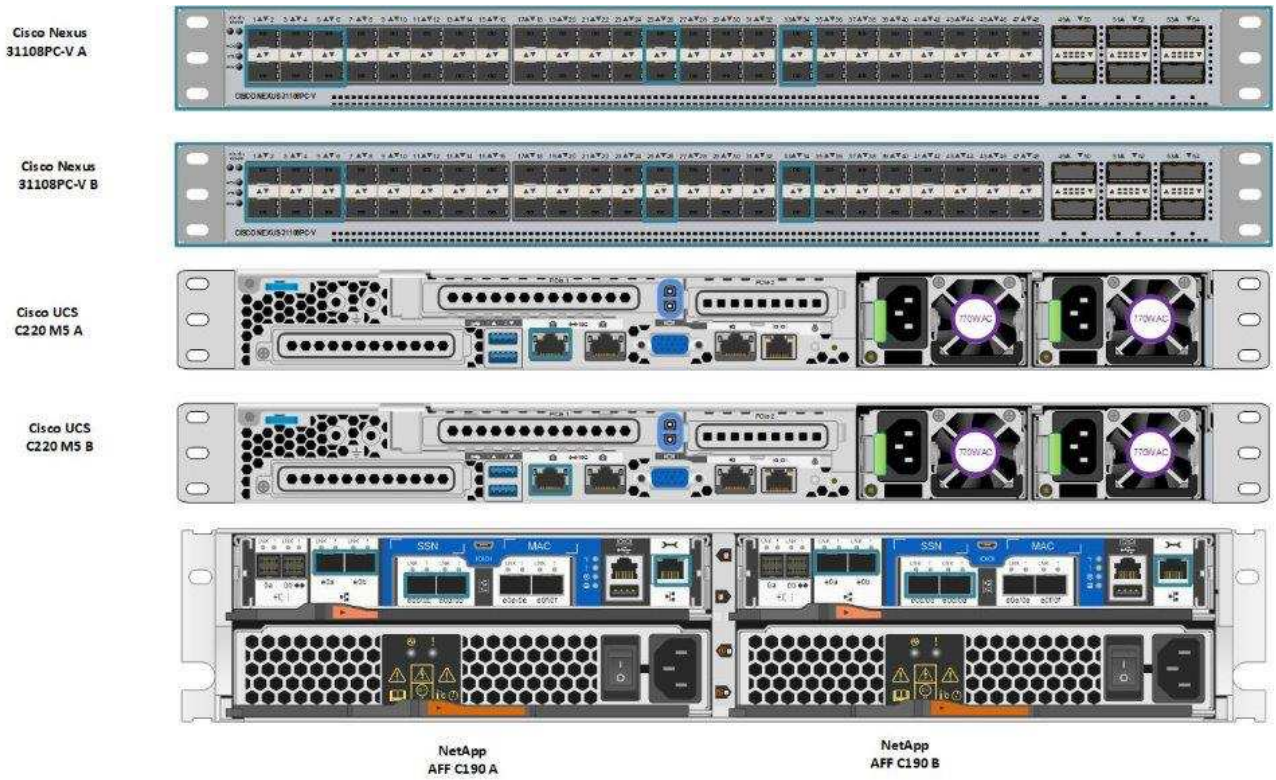
下表列出了在 FlexPod Express 上实施所有 VMware vSphere 所需的软件。

软件	**version**
VMware vCenter Server 设备	6.7U2
VMware vSphere ESXi 虚拟机管理程序	6.7U2
适用于 ESXi 的 NetApp VAAI 插件	1.1.2
NetApp VSC	9.6

FlexPod 快速布线信息

此参考验证已按照下图和表所示进行布线。

此图显示了参考验证布线。



下表列出了 Cisco Nexus 交换机 31108PC-V-A 的布线信息

本地设备	本地端口	远程设备	远程端口
Cisco Nexus 交换机 31108PC-V A	Eth1/1	NetApp AFF C190 存储控制器 A	e0c
	eth1/2	NetApp AFF C190 存储控制器 B	e0c
	Eth1/3	Cisco UCS C220 C 系列独立服务器 A	MLOM0
	Eth1/4	Cisco UCS C220 C 系列独立服务器 B	MLOM0
	eth1/5	Cisco UCS C220 C 系列独立服务器 A	MLOM1
	eth1/6.	Cisco UCS C220 C 系列独立服务器 B	MLOM1
	eth1/25	Cisco Nexus 交换机 31108PC-V B	eth1/25
	eth1/26.	Cisco Nexus 交换机 31108PC-V B	eth1/26.
	eth1/33	NetApp AFF C190 存储控制器 A	e0M
	eth1/34	Cisco UCS C220 C 系列独立服务器 A	CIMC （FEX135/1/25）

此表列出了 Cisco Nexus 交换机 31108PC-V- B 的布线信息

本地设备	本地端口	远程设备	远程端口
Cisco Nexus 交换机 31108PC-V B	Eth1/1	NetApp AFF C190 存储控制器 A	e0d
	eth1/2	NetApp AFF C190 存储控制器 B	e0d
	Eth1/3	Cisco UCS C220 C 系列独立服务器 A	MLOM2
	Eth1/4	Cisco UCS C220 C 系列独立服务器 B	MLOM2
	eth1/5	Cisco UCS C220 C 系列独立服务器 A	MLOM3
	eth1/6.	Cisco UCS C220 C 系列独立服务器 B	MLOM3
	eth1/25	Cisco Nexus 交换机 31108 A	eth1/25
	eth1/26.	Cisco Nexus 交换机 31108 A	eth1/26.
	eth1/33	NetApp AFF C190 存储控制器 B	e0M
	eth1/34	Cisco UCS C220 C 系列独立服务器 B	CIMC （FEX135/1/26）

下表列出了 NetApp AFF C190 存储控制器 A 的布线信息

本地设备	本地端口	远程设备	远程端口
NetApp AFF C190 存储控制器 A	e0a	NetApp AFF C190 存储控制器 B	e0a
	e0b	NetApp AFF C190 存储控制器 B	e0b
	e0c	Cisco Nexus 交换机 31108PC-V A	Eth1/1
	e0d	Cisco Nexus 交换机 31108PC-V B	Eth1/1
	e0M	Cisco Nexus 交换机 31108PC-V A	eth1/33

下表列出了 NetApp AFF C190 存储控制器 B 的布线信息

本地设备	本地端口	远程设备	远程端口
NetApp AFF C190 存储控制器 B	e0a	NetApp AFF C190 存储控制器 A	e0a
	e0b	NetApp AFF C190 存储控制器 A	e0b
	e0c	Cisco Nexus 交换机 31108PC-V A	eth1/2
	e0d	Cisco Nexus 交换机 31108PC-V B	eth1/2
	e0M	Cisco Nexus 交换机 31108PC-V B	eth1/33

部署过程

概述

本文档详细介绍了如何配置完全冗余，高可用性的 FlexPod Express 系统。为了反映这种冗余，在每个步骤中配置的组件称为组件 A 或组件 B例如，控制器 A 和控制器 B 可识别本文档中配置的两个 NetApp 存储控制器。交换机 A 和交换机 B 可识别一对 Cisco Nexus 交换机。

此外，本文档还介绍配置多个 Cisco UCS 主机的步骤，这些主机按顺序标识为服务器 A ，服务器 B 等。

要指示您应在步骤中包含与您的环境相关的信息，请在命令结构中显示 ` <<text>>` 。请参见以下 `vlan create` 命令示例：

```
Controller01> network port vlan create -node <<var_nodeA>> -vlan-name
<<var_vlan-name>>
```

通过本文档，您可以完全配置 FlexPod 快速环境。在此过程中，您需要通过多个步骤插入客户专用的命名约定， IP 地址和虚拟局域网（ VLAN ）方案。下表介绍了部署所需的 VLAN ，如本指南所述。此表可根据特定站点变量填写，并用于实施文档配置步骤。

> 如果使用单独的带内和带外管理 VLAN ，则必须在它们之间创建第 3 层路由。在此验证中，使用了一个通用管理 VLAN 。

VLAN name	**VLAN** 用途	**VLAN ID**	
管理 VLAN	用于管理接口的 VLAN	3437	vSwitch0
NFS VLAN	用于 NFS 流量的 VLAN	3438	vSwitch0
VMware vMotion VLAN	为将虚拟机（ VM ）从一台物理主机移动到另一台物理主机而指定的 VLAN	3441	vSwitch0

VLAN name	VLAN 用途	VLAN ID	
VM 流量 VLAN	用于 VM 应用程序流量的 VLAN	3442	vSwitch0
iSCSI-A-VLAN	网络结构 A 上用于 iSCSI 流量的 VLAN	3439	iScsiBootvSwitch
iSCSI-B-VLAN	网络结构 B 上用于 iSCSI 流量的 VLAN	3440	iScsiBootvSwitch
原生 VLAN	将未标记的帧分配到的 VLAN	2.	

在整个 FlexPod Express 配置过程中都需要 VLAN 编号。这些 VLAN 称为 `<<var_xxxx_vlan>>`，其中 `xxxx` 是 VLAN 的用途（例如 iSCSI-A）。

在此验证中创建了两个 vSwitch 。

下表列出了解决方案 vSwitch 。

vSwitch 名称	活动适配器	端口	MTU	负载平衡
vSwitch0	vmnic2， vmnic4	默认值（120）	9000	基于 IP 哈希的路由
iScsiBootvSwitch	vmnic3， vmnic5	默认值（120）	9000	基于源虚拟端口 ID 的路由。

> 负载平衡的 IP 哈希方法需要使用具有静态（模式开启）端口通道的 SRC/DST-IP EtherChannel 为底层物理交换机进行正确配置。如果由于交换机配置不当而导致连接间歇性中断，请暂时关闭 Cisco 交换机上两个关联上行链路端口之一，以便在对端口通道设置进行故障排除时恢复与 ESXi 管理 vmkernel 端口的通信。

下表列出了已创建的 VMware VM 。

VM 问题描述	主机名
VMware vCenter Server	FlexPod-VCSA
Virtual Storage Console	FlexPod-VSC

部署 Cisco Nexus 31108PC-V

本节详细介绍了 FlexPod Express 环境中使用的 Cisco Nexus 331108PC-V 交换机配置。

Cisco Nexus 31108PC-V 交换机的初始设置

以下过程介绍了如何配置 Cisco Nexus 交换机以在基础 FlexPod Express 环境中使用。

> 此操作步骤假定您使用的是运行 NX-OS 软件版本 7.0 （3） i7 （6）的 Cisco Nexus 31108PC-V 。

1. 首次启动并连接到交换机的控制台端口后， Cisco NX-OS 设置将自动启动。此初始配置可解决基本设置，例如交换机名称， mgmt0 接口配置和安全 Shell （SSH）设置。

2. FlexPod 快速管理网络可以通过多种方式进行配置。31108PC-V 交换机上的 mgmt0 接口可以连接到现有管理网络，也可以采用背对背配置连接 31108PC-V 交换机的 mgmt0 接口。但是，此链路不能用于外部管理访问，例如 SSH 流量。

> 在本部署指南中， FlexPod Express Cisco Nexus 31108PC-V 交换机连接到现有管理网络。

3. 要配置 Cisco Nexus 31108PC-V 交换机，请启动交换机并按照屏幕上的提示进行操作，如此处所示，对这两台交换机进行初始设置，并将相应的值替换为交换机特定信息。

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 31108PC-V-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]: <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: <enter>
```

4. 然后，您将看到配置摘要，系统会询问您是否要对其进行编辑。如果配置正确，请输入 `n` 。

```
Would you like to edit the configuration? (y
es/no) [n]: n
```

5. 然后，系统会询问您是否要使用此配置并保存它。如果是，请输入 `y` 。

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. 对 Cisco Nexus 交换机 B 重复此操作步骤

启用高级功能

要提供其他配置选项，必须在 Cisco NX-OS 中启用某些高级功能。要在 Cisco Nexus 交换机 A 和交换机 B 上启用相应功能，请使用命令（ config t ）进入配置模式并运行以下命令：

```
feature interface-vlan
feature lacp
feature vpc
```

> 默认端口通道负载平衡哈希使用源 IP 地址和目标 IP 地址来确定端口通道中各个接口之间的负载平衡算法。除了源 IP 地址和目标 IP 地址之外，还可以为哈希算法提供更多输入，从而在端口通道的各个成员之间实现更好的分布。出于同样的原因， NetApp 强烈建议将源和目标 TCP 端口添加到哈希算法中。

在配置模式（ config t ）下，输入以下命令，在 Cisco Nexus 交换机 A 和交换机 B 上设置全局端口通道负载平衡配置：

```
port-channel load-balance src-dst ip-l4port
```

配置全局生成树

Cisco Nexus 平台使用一种新的保护功能，称为网桥保证。如果设备不再运行生成树算法，则网桥保证有助于防止单向链路或其他软件故障继续转发数据流量。根据平台的不同，可以将端口置于多种状态之一，包括网络或边缘状态。

NetApp 建议设置网桥保证，以便默认情况下将所有端口都视为网络端口。此设置强制网络管理员查看每个端口的配置。此外，它还会显示最常见的配置错误，例如未标识的边缘端口或未启用网桥保证功能的邻居。此外，生成树块中的端口较多而不是太少会更安全，这样就可以使用默认端口状态来增强网络的整体稳定性。

添加服务器，存储和上行链路交换机时，请密切关注生成树的状态，尤其是在它们不支持网桥保证的情况下。在这种情况下，您可能需要更改端口类型才能使端口处于活动状态。

默认情况下，作为另一层保护，在边缘端口上启用网桥协议数据单元（ BPDU ）保护。为了防止网络中出现环路，如果在此接口上看到来自另一个交换机的 BPDU ，则此功能将关闭此端口。

在配置模式（ config t ）下，运行以下命令以配置 Cisco Nexus 交换机 A 和交换机 B 上的默认生成树选项，包

括默认端口类型和 BPDU 保护：

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
ntp server <<var_ntp_ip>> use-vrf management
ntp master 3
```

定义 VLAN

在配置具有不同 VLAN 的各个端口之前，必须在交换机上定义第 2 层 VLAN 。此外，最好对 VLAN 进行命名，以便将来进行故障排除。

在配置模式（ config t ）下，运行以下命令来定义和描述 Cisco Nexus 交换机 A 和交换机 B 上的第 2 层 VLAN ：

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

配置访问和管理端口说明

与为第 2 层 VLAN 分配名称一样，为所有接口设置说明有助于配置和故障排除。

在每个交换机的配置模式（ config t ）中，为 FlexPod 快速大型配置输入以下端口说明：

Cisco Nexus 交换机 A

```
int eth1/1
  description AFF C190-A e0c
int eth1/2
  description AFF C190-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0 vSwitch0
int eth1/4
  description UCS-Server-B: MLOM port 0 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 1 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 1 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-B 1/25
int eth1/26
  description vPC peer-link 31108PC-V-B 1/26
int eth1/33
  description AFF C190-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Cisco Nexus 交换机 B

```
int eth1/1
  description AFF C190-A e0d
int eth1/2
  description AFF C190-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 2 vSwitch0
int eth1/4
description UCS-Server-B: MLOM port 2 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 3 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 3 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-A 1/25
int eth1/26
  description vPC peer-link 31108PC-V-A 1/26
int eth1/33
  description AFF C190-B e0M
int eth1/34
  description UCS Server B: CIMC
```

配置服务器和存储管理接口

服务器和存储的管理接口通常仅使用一个 VLAN 。因此，请将管理接口端口配置为访问端口。为每个交换机定义管理 VLAN ，并将生成树端口类型更改为边缘。

在配置模式（ config t ）下，输入以下命令为服务器和存储的管理接口配置端口设置：

Cisco Nexus 交换机 A

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus 交换机 B

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

执行虚拟端口通道全局配置

通过虚拟端口通道（ vPC ），物理连接到两个不同 Cisco Nexus 交换机的链路可以显示为连接到第三个设备的单端口通道。第三个设备可以是交换机，服务器或任何其他网络设备。vPC 可以提供第 2 层多路径功能，通过增加带宽，在节点之间启用多个并行路径以及存在备用路径的负载平衡流量，您可以创建冗余。

vPC 具有以下优势：

- 允许单个设备在两个上游设备之间使用端口通道
- 消除生成树协议阻止的端口
- 提供无环路拓扑
- 使用所有可用的上行链路带宽
- 在链路或设备发生故障时提供快速融合
- 提供链路级别故障恢复能力
- 帮助提供高可用性

要使 vPC 功能正常运行，需要在两个 Cisco Nexus 交换机之间进行一些初始设置。如果使用背对背 mgmt0 配置，请使用接口上定义的地址，并使用 `ping` ` [switch_A/B_mgmt0_IP_addr]vRF` management 命令验证它们是否可以通信。

在配置模式（ config t ）下，运行以下命令为两台交换机配置 vPC 全局配置：

Cisco Nexus 交换机 A

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf
management
peer-switch
peer-gateway
auto-recovery
delay restore 150
ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Cisco Nexus 交换机 B

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  delay-restore 150
   ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

配置存储端口通道

NetApp 存储控制器允许使用链路聚合控制协议（ Link Aggregation Control Protocol ， LACP ）与网络建立主动 - 主动连接。最好使用 LACP ，因为它会在交换机之间添加协商和日志记录功能。由于网络是为 vPC 设置的，因此，通过这种方法，您可以将主动 - 主动连接从存储连接到不同的物理交换机。每个控制器与每个交换机之间都有两条链路。但是，所有四个链路都属于同一个 vPC 和接口组（ ifgrp ）。

在配置模式（ config t ）下，对每个交换机运行以下命令，为连接到 NetApp AFF 控制器的端口配置各个接口以及生成的端口通道配置。

1. 在交换机 A 和交换机 B 上运行以下命令，为存储控制器 A 配置端口通道：

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. 在交换机 A 和交换机 B 上运行以下命令，为存储控制器 B 配置端口通道：

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```

配置服务器连接

Cisco UCS 服务器具有一个四端口虚拟接口卡 VIC1457 ，用于数据流量以及使用 iSCSI 启动 ESXi 操作系统。这些接口配置为相互故障转移，可在单链路之外提供额外冗余。通过将这些链路分布在多个交换机上，即使在交换机完全发生故障时，服务器也能正常运行。

在配置模式（ config t ）下，运行以下命令，为连接到每个服务器的接口配置端口设置。

Cisco Nexus 交换机 A： Cisco UCS Server-A 和 Cisco UCS Server-B 配置

```
int eth1/5
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

Cisco Nexus 交换机 B： Cisco UCS Server-A 和 Cisco UCS Server-B 配置

```
int eth1/6
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

配置服务器端口通道

在交换机 A 和交换机 B 上运行以下命令，为 Server-A 配置端口通道：

```
int eth1/3
  channel-group 13 mode active
int Po13
  description vPC to Server-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 13
  no shut
```

在交换机 A 和交换机 B 上运行以下命令，为 Server-B 配置端口通道：

```
int eth1/4
  channel-group 14 mode active
int Po14
  description vPC to Server-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 14
  no shut
```

> 此解决方案验证使用的 MTU 为 9000 。但是，您可以根据应用程序要求为 MTU 配置不同的值。在整个 FlexPod 解决方案中设置相同的 MTU 值非常重要。组件之间的 MTU 配置不正确会导致数据包被丢弃，需要重新传输这些数据包，从而影响解决方案的整体性能。

> 要通过添加更多 Cisco UCS 服务器来扩展解决方案，请使用交换机 A 和 B 上新添加的服务器所插入的交换机端口运行上述命令

通过上行链路连接到现有网络基础架构

根据可用的网络基础架构，可以使用多种方法和功能来上行链路连接 FlexPod 环境。如果存在现有的 Cisco Nexus 环境， NetApp 建议使用 vPC 通过上行链路将 FlexPod 环境中的 Cisco Nexus 31108 交换机连接到基础架构中。对于 10GbE 基础架构解决方案，上行链路可以是 10GbE 上行链路，如果需要，上行链路可以是 1GbE 基础架构解决方案。可以使用上述过程创建到现有环境的上行链路 vPC 。配置完成后，请务必运行 copy start 在每个交换机上保存配置。

"下一步：NetApp存储部署操作步骤 (第1部分)。"

NetApp 存储部署操作步骤（第 **1** 部分）

本节介绍 NetApp AFF 存储部署操作步骤。

安装 **NetApp** 存储控制器 **AFF C190** 系列

NetApp Hardware Universe

NetApp Hardware Universe （ HWU ）应用程序可为任何特定 ONTAP 版本提供受支持的硬件和软件组件。它提供了 ONTAP 软件当前支持的所有 NetApp 存储设备的配置信息。此外，还提供了一个组件兼容性表。

确认要安装的 ONTAP 版本支持您要使用的硬件和软件组件：

访问 "HWU" 应用程序以查看系统配置指南。单击控制器选项卡以查看不同版本的 ONTAP 软件与符合所需规格的 NetApp 存储设备之间的兼容性。

或者，要按存储设备比较组件，请单击比较存储系统。

控制器 **AFF190** 系列的前提条件
要规划存储系统的物理位置，请参见 NetApp Hardware Universe 。请参见以下部分： • 电气要求 • 支持的电源线 • 板载端口和缆线

存储控制器

按照 AFF 中控制器的物理安装过程进行操作 "C190" 文档。

NetApp ONTAP 9.6

配置工作表

在运行设置脚本之前，请填写产品手册中的配置工作表。配置工作表可从《 ONTAP 9.6 软件设置指南》中获取。

> 此系统在双节点无交换机集群配置中设置。

下表提供了 ONTAP 9.6 的安装和配置信息。

集群详细信息	集群详细信息值
集群节点 A IP 地址	<<var_nodeA_mgmt_ip>>
集群节点 A 网络掩码	<<var_nodeA_mgmt_mask>>
集群节点 A 网关	<<var_nodeA_mgmt_gateway>>
集群节点 A 名称	<<var_nodeA>>
集群节点 B IP 地址	<<var_nodeB_mgmt_ip>>
集群节点 B 网络掩码	<<var_nodeB_mgmt_mask>>
集群节点 B 网关	<<var_nodeB_mgmt_gateway>>
集群节点 B 名称	<<var_nodeB>>
ONTAP 9.6 URL	<<var_url_boot_software>>
集群的名称	<<var_clustername>>
集群管理 IP 地址	<<var_clustermgmt_ip>>
集群 B 网关	<<var_clustermgmt_gateway>>
集群 B 网络掩码	<<var_clustermgmt_mask>>
域名	<<var_domain_name>>
DNS 服务器 IP （您可以输入多个）	<var_dns_server_ip

集群详细信息	集群详细信息值
NTP 服务器 IP （您可以输入多个）	<<var_ntp_server_ip>>

配置节点 **A**

要配置节点 A ，请完成以下步骤：

1. 连接到存储系统控制台端口。您应看到 Loader-A 提示符。但是，如果存储系统处于重新启动循环中，请在看到以下消息时按 Ctrl-C 退出自动启动循环：

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

   允许系统启动。

   ```
   autoboot
   ```

2. 按 Ctrl-C 进入启动菜单。

   > 如果 ONTAP 9.6 不是要启动的软件版本，请继续执行以下步骤以安装新软件。如果要启动的版本是 ONTAP 9.6 ，请选择选项 8 和 y 以重新启动节点。然后，继续执行步骤 14 。

3. 要安装新软件，请选择选项 7 。
4. 输入 y 执行升级。
5. 为要用于下载的网络端口选择 e0M 。
6. 输入 y 立即重新启动。
7. 在相应位置输入 e0M 的 IP 地址，网络掩码和默认网关。

   ```
   <<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
   ```

8. 输入可在其中找到软件的 URL 。

   > 此 Web 服务器必须可执行 Ping 操作。

   ```
   <<var_url_boot_software>>
   ```

9. 按 Enter 输入用户名，表示无用户名。
10. 输入 y 将新安装的软件设置为后续重新启动所使用的默认软件。
11. 输入 y 重新启动节点。

> 安装新软件时，系统可能会对 BIOS 和适配器卡执行固件升级，从而导致重新启动，并可能在 Loader-A 提示符处停止。如果发生这些操作，系统可能会与此操作步骤有所偏差。

12. 按 Ctrl-C 进入启动菜单。
13. 选择选项 4 以清除配置并初始化所有磁盘。
14. 输入 y 将磁盘置零，重置配置并安装新的文件系统。
15. 输入 y 擦除磁盘上的所有数据。

> 根聚合的初始化和创建可能需要 90 分钟或更长时间才能完成，具体取决于所连接磁盘的数量和类型。初始化完成后，存储系统将重新启动。请注意， SSD 初始化所需的时间要少得多。您可以在节点 A 的磁盘置零时继续进行节点 B 配置。

在节点 A 初始化期间，开始配置节点 B

配置节点 **B**

要配置节点 B ，请完成以下步骤：

1. 连接到存储系统控制台端口。您应看到 Loader-A 提示符。但是，如果存储系统处于重新启动循环中，请在看到以下消息时按 Ctrl-C 退出自动启动循环：

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. 按 Ctrl-C 进入启动菜单。

```
autoboot
```

3. 出现提示时，按 Ctrl-C 。

> 如果 ONTAP 9.6 不是要启动的软件版本，请继续执行以下步骤以安装新软件。如果要启动的版本是 ONTAP 9.6 ，请选择选项 8 和 y 以重新启动节点。然后，继续执行步骤 14 。

4. 要安装新软件，请选择选项 7.A
5. 输入 y 执行升级。
6. 为要用于下载的网络端口选择 e0M 。
7. 输入 y 立即重新启动。
8. 在相应位置输入 e0M 的 IP 地址，网络掩码和默认网关。

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. 输入可在其中找到软件的 URL 。

此 Web 服务器必须可执行 Ping 操作。

```
<<var_url_boot_software>>
```

10. 按 Enter 输入用户名，表示无用户名。
11. 输入 y 将新安装的软件设置为后续重新启动所使用的默认软件。
12. 输入 y 重新启动节点。

安装新软件时，系统可能会对 BIOS 和适配器卡执行固件升级，从而导致重新启动，并可能在 Loader-A 提示符处停止。如果发生这些操作，系统可能会与此操作步骤有所偏差。

13. 按 Ctrl-C 进入启动菜单。
14. 选择选项 4 以清除配置并初始化所有磁盘。
15. 输入 y 将磁盘置零，重置配置并安装新的文件系统。
16. 输入 y 擦除磁盘上的所有数据。

根聚合的初始化和创建可能需要 90 分钟或更长时间才能完成，具体取决于所连接磁盘的数量和类型。初始化完成后，存储系统将重新启动。请注意， SSD 初始化所需的时间要少得多。

继续执行节点 **A** 配置和集群配置

从连接到存储控制器 A （节点 A ）控制台端口的控制台端口程序中，运行节点设置脚本。首次在节点上启动 ONTAP 9.6 时，将显示此脚本。

在 ONTAP 9.6 中，节点和集群设置操作步骤略有更改。现在，集群设置向导用于配置集群中的第一个节点，而 NetApp ONTAP 系统管理器（以前称为 OnCommand ® System Manager ）用于配置集群。

1. 按照提示设置节点 A

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. 导航到节点管理接口的 IP 地址。

> 也可以使用命令行界面执行集群设置。本文档介绍如何使用 System Manager 引导式设置进行集群设置。

3. 单击引导式设置以配置集群。
4. 输入 ` <<var_clustername>>` 作为集群名称，并为要配置的每个节点输入 ` <<var_nodeA>>` 和 ` <<var_nodeB>>` 。输入要用于存储系统的密码。选择无交换机集群作为集群类型。输入集群基本许可证。
5. 您还可以输入集群， NFS 和 iSCSI 的功能许可证。
6. 此时将显示一条状态消息，指出正在创建集群。此状态消息会循环显示多个状态。此过程需要几分钟时间。
7. 配置网络。
   a. 取消选择 IP 地址范围选项。
   b. 在集群管理 IP 地址字段中输入 ` [var_clustermgmt_ip]` ，在网络掩码字段中输入 `

[var_clustermgmt_mask]` ，在网关字段中输入 ` [var_clustermgmt_gateway]` 。使用… 选择端口字段中的选择器以选择节点 A 的 e0M

c. 节点 A 的节点管理 IP 已填充。为节点 B 输入 ` <<var_nodeA_mgmt_ip>>`

d. 在 DNS 域名字段中输入 ` <<var_domain_name>>` 。在 DNS Server IP Address 字段中输入 ` <<var_dns_server_ip>>` 。

> 您可以输入多个 DNS 服务器 IP 地址。

e. 在 Primary NTP Server 字段中输入 `10.63.172.162` 。

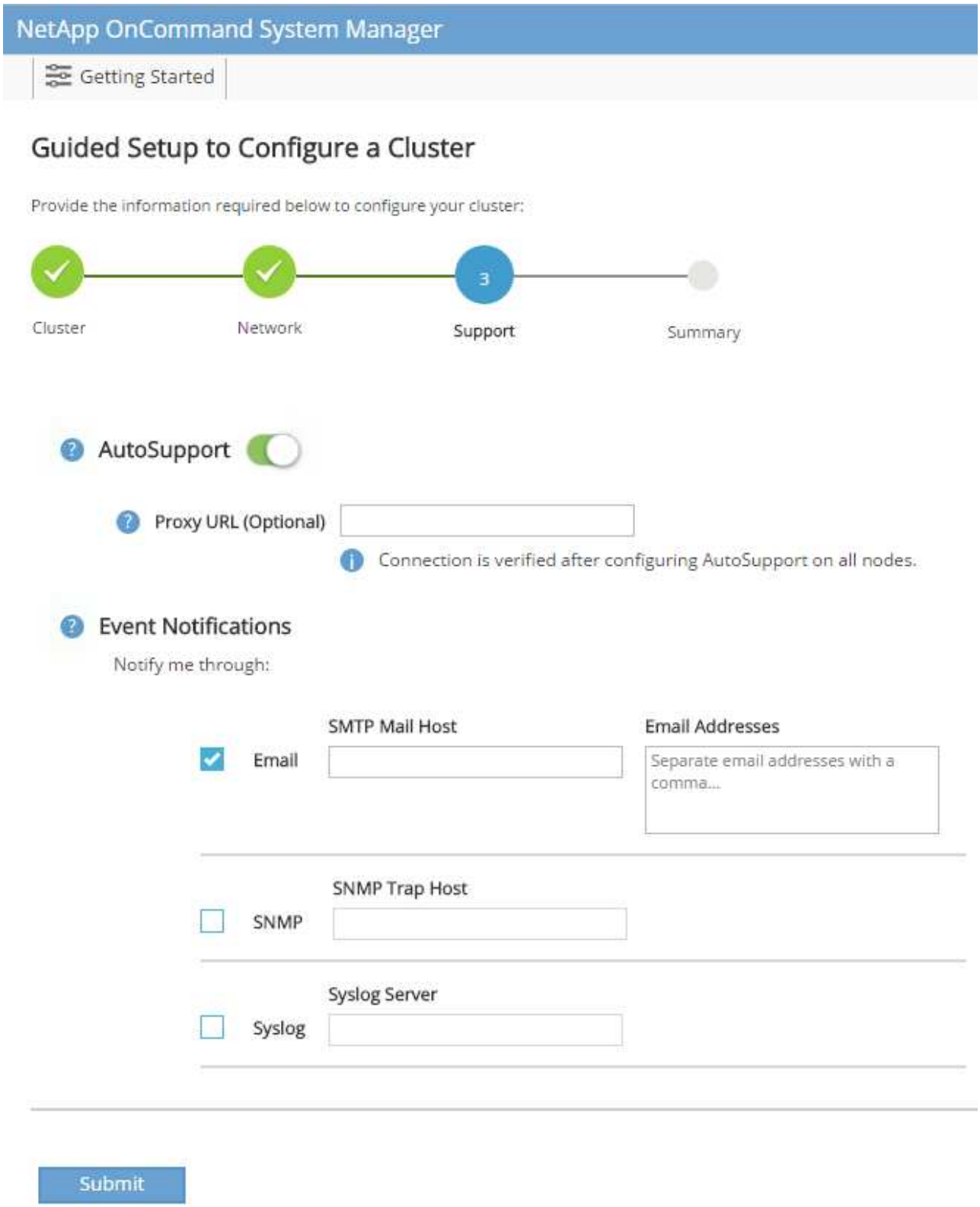
> 您也可以输入备用 NTP 服务器。IP 地址 `10.63.172.162` from ` <<var_ntp_server_ip>>` 是 Nexus Mgmt IP 。

8. 配置支持信息。

a. 如果您的环境需要代理来访问 AutoSupport ，请在代理 URL 中输入 URL 。

b. 输入事件通知的 SMTP 邮件主机和电子邮件地址。

> 您必须至少设置事件通知方法，然后才能继续操作。您可以选择任何方法。



当系统指示集群配置已完成时，单击管理集群以配置存储。

继续存储集群配置

配置存储节点和基础集群后，您可以继续配置存储集群。

将所有备用磁盘置零

要将集群中的所有备用磁盘置零，请运行以下命令：

```
disk zerospares
```

设置板载 **UTA2** 端口特性

1. 运行 `ucadmin show` 命令，验证端口的当前模式和当前类型。

```
AFF C190::> ucadmin show
                       Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF C190_A     0c       cna       target     -        -          online
AFF C190_A     0d       cna       target     -        -          online
AFF C190_A     0e       cna       target     -        -          online
AFF C190_A     0f       cna       target     -        -          online
AFF C190_B     0c       cna       target     -        -          online
AFF C190_B     0d       cna       target     -        -          online
AFF C190_B     0e       cna       target     -        -          online
AFF C190_B     0f       cna       target     -        -          online
8 entries were displayed.
```

2. 验证正在使用的端口的当前模式是否为 CNA ，以及当前类型是否设置为目标。如果不是，请使用以下命令更改端口个性化设置：

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

> 要运行上一个命令，端口必须处于脱机状态。要使端口脱机，请运行以下命令：

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

> 如果更改了端口属性，则必须重新启动每个节点，此更改才能生效。

重命名管理逻辑接口

要重命名管理逻辑接口（ LIF ），请完成以下步骤：

1. 显示当前管理 LIF 名称。

```
network interface show -vserver <<clustername>>
```

2. 重命名集群管理 LIF 。

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_cluster_mgmt_lif_1 -newname cluster_mgmt
```

3. 重命名节点 B 管理 LIF 。

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF C190_B_1 -newname AFF C190-02_mgmt1
```

在集群管理上设置自动还原

在集群管理界面上设置 auto-revert 参数。

```
network interface modify -vserver <<clustername>> -lif cluster_mgmt -auto-
revert true
```

设置服务处理器网络接口

要为每个节点上的服务处理器分配静态 IPv4 地址，请运行以下命令：

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

服务处理器 IP 地址应与节点管理 IP 地址位于同一子网中。

在 **ONTAP** 中启用存储故障转移

要确认已启用存储故障转移，请在故障转移对中运行以下命令：

1. 验证存储故障转移的状态。

```
storage failover show
```

> ` [var_nodeA]` 和 ` [var_nodeB]` 都必须能够执行接管。如果节点可以执行接管，请转至步骤 3 。

2. 在两个节点之一上启用故障转移。

```
storage failover modify -node <<var_nodeA>> -enabled true
```

> 在一个节点上启用故障转移后，这两个节点都可以进行故障转移。

3. 验证双节点集群的 HA 状态。

> 此步骤不适用于具有两个以上节点的集群。

```
cluster ha show
```

4. 如果配置了高可用性，请转至步骤 6 。如果配置了高可用性，则在发出命令时会显示以下消息：

```
High Availability Configured: true
```

5. 仅为双节点集群启用 HA 模式。

> 请勿对具有两个以上节点的集群运行此命令，因为它会导致故障转移出现问题。

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. 验证是否已正确配置硬件辅助，并根据需要修改配对 IP 地址。

```
storage failover hwassist show
```

> 消息 **保持活动状态：错误：** 表示其中一个控制器未从其配对控制器收到 hwassist 保持活动警报，表示未配置硬件辅助。运行以下命令以配置硬件辅助。

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

在 ONTAP 中创建巨型帧 MTU 广播域

要创建 MTU 为 9000 的数据广播域，请运行以下命令：

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

从默认广播域中删除数据端口

10GbE 数据端口用于 iSCSI/NFS 流量，这些端口应从默认域中删除。不使用端口 e0e 和 e0f ，也应从默认域中删除。

要从广播域中删除端口，请运行以下命令：

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

禁用 UTA2 端口上的流量控制

NetApp 最佳实践是，在连接到外部设备的所有 UTA2 端口上禁用流量控制。要禁用流量控制，请运行以下命令：

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```

在 **ONTAP** 中配置接口组 **LACP**

此类型的接口组需要两个或更多以太网接口以及一个支持 LACP 的交换机。确保已根据本指南第 5.1 节中的步骤对其进行配置。

在集群提示符处，完成以下步骤：

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

在 ONTAP 中配置巨型帧

要将 ONTAP 网络端口配置为使用巨型帧（ MTU 通常为 9， 000 字节），请从集群 Shell 运行以下命令：

```
AFF C190::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF C190::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

在 ONTAP 中创建 VLAN

要在 ONTAP 中创建 VLAN，请完成以下步骤：

1. 创建 NFS VLAN 端口并将其添加到数据广播域。

   ```
   network port vlan create -node <<var_nodeA>> -vlan-name a0a-
   <<var_nfs_vlan_id>>
   network port vlan create -node <<var_nodeB>> -vlan-name a0a-
   <<var_nfs_vlan_id>>
   broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
   <<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
   <<var_nfs_vlan_id>>
   ```

2. 创建 iSCSI VLAN 端口并将其添加到数据广播域。

```
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. 创建 MGMT-VLAN 端口。

```
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

在 **ONTAP** 中创建数据聚合

在 ONTAP 设置过程中，将创建一个包含根卷的聚合。要创建其他聚合，请确定聚合名称，要创建聚合的节点及其包含的磁盘数。

要创建聚合，请运行以下命令：

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

> 在配置中至少保留一个磁盘（选择最大的磁盘）作为备用磁盘。最佳做法是，每个磁盘类型和大小至少有一个备用磁盘。

> 从五个磁盘开始；您可以在需要额外存储时向聚合添加磁盘。

> 在磁盘置零完成之前，无法创建聚合。运行 `aggr show` 命令以显示聚合创建状态。在 aggr1_nodeA 联机之前，请勿继续操作。

在 ONTAP 中配置时区

要配置时间同步并设置集群上的时区，请运行以下命令：

```
timezone <<var_timezone>>
```

> 例如，在美国东部，时区为 America/New_York 。开始键入时区名称后，按 Tab 键查看可用选项。

在 ONTAP 中配置 SNMP

要配置 SNMP ，请完成以下步骤：

1. 配置 SNMP 基本信息，例如位置和联系人。轮询时，此信息在 SNMP 中显示为 `sysLocation` 和 `sysContact` 变量。

   ```
   snmp contact <<var_snmp_contact>>
   snmp location "<<var_snmp_location>>"
   snmp init 1
   options snmp.enable on
   ```

2. 配置 SNMP 陷阱以发送到远程主机。

   ```
   snmp traphost add <<var_snmp_server_fqdn>>
   ```

在 ONTAP 中配置 SNMPv1

要配置 SNMPv1 ，请设置名为社区的共享机密纯文本密码。

```
snmp community add ro <<var_snmp_community>>
```

> 请谨慎使用 `snmp community delete all` 命令。如果社区字符串用于其他监控产品，则此命令会将其删除。

在 ONTAP 中配置 SNMPv3

SNMPv3 要求您定义并配置用户进行身份验证。要配置 SNMPv3 ，请完成以下步骤：

1. 运行 `security snmpusers` 命令以查看引擎 ID 。
2. 创建名为 `snmpv3user` 的用户。

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. 输入权威实体的引擎 ID ，然后选择 MD5 作为身份验证协议。
4. 出现提示时，输入身份验证协议的最小长度为八个字符的密码。
5. 选择 DES 作为隐私协议。
6. 出现提示时，输入隐私协议的最小长度为八个字符的密码。

在 ONTAP 中配置 AutoSupport HTTPS

NetApp AutoSupport 工具通过 HTTPS 向 NetApp 发送支持摘要信息。要配置 AutoSupport ，请运行以下命令：

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

创建 Storage Virtual Machine

要创建基础架构 Storage Virtual Machine （ SVM ），请完成以下步骤：

1. 运行 `vserver create` 命令。

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. 将数据聚合添加到 NetApp VSC 的 infra-sVM 聚合列表中。

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. 从 SVM 中删除未使用的存储协议，而不使用 NFS 和 iSCSI 。

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. 在 infra-sVM SVM 中启用并运行 NFS 协议。

```
nfs create -vserver Infra-SVM -udp disabled
```

5. 打开 NetApp NFS VAAI 插件的 `SVM vStorage` 参数。然后，验证是否已配置 NFS 。

```
vserver nfs modify -vserver Infra-SVM -vstorage enabled
vserver nfs show
```

> 在命令行中，命令以 `vserver` 为前缀，因为 SVM 以前称为 Vserver 。

在 ONTAP 中配置 NFSv3

下表列出了完成此配置所需的信息。

详细信息	详细信息值
ESXi 主机 A NFS IP 地址	<<var_esxi_HostA_NFS_IP>>
ESXi 主机 B NFS IP 地址	<<var_esxi_HostB_NFS_IP>>

要在 SVM 上配置 NFS ，请运行以下命令：

1. 在默认导出策略中为每个 ESXi 主机创建一个规则。
2. 为要创建的每个 ESXi 主机分配一个规则。每个主机都有自己的规则索引。第一个 ESXi 主机的规则索引为 1 ，第二个 ESXi 主机的规则索引为 2 ，依此类推。

```
vserver export-policy rule create -vserver Infra-SVM -policyname default
-ruleindex 1 -protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys -rwrule sys -superuser sys -allow-suid false
vserver export-policy rule create -vserver Infra-SVM -policyname default
-ruleindex 2 -protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys -rwrule sys -superuser sys -allow-suid false
vserver export-policy rule show
```

3. 将导出策略分配给基础架构 SVM 根卷。

```
volume modify -vserver Infra-SVM -volume rootvol -policy default
```

> 如果您选择在设置 vSphere 后安装导出策略，则 NetApp VSC 会自动处理导出策略。如果不安装此服务器，则必须在添加其他 Cisco UCS C 系列服务器时创建导出策略规则。

在 ONTAP 中创建 iSCSI 服务

要在 SVM 上创建 iSCSI 服务，请运行以下命令。此命令还会启动 iSCSI 服务并为 SVM 设置 iSCSI IQN 。验证是否已配置 iSCSI 。

```
iscsi create -vserver Infra-SVM
iscsi show
```

在 ONTAP 中创建 SVM 根卷的负载共享镜像

要在 ONTAP 中为 SVM 根卷创建负载共享镜像，请完成以下步骤：

1. 在每个节点上创建一个卷作为基础架构 SVM 根卷的负载共享镜像。

```
volume create -vserver Infra_Vserver -volume rootvol_m01 -aggregate
aggr1_nodeA -size 1GB -type DP
volume create -vserver Infra_Vserver -volume rootvol_m02 -aggregate
aggr1_nodeB -size 1GB -type DP
```

2. 创建作业计划，以便每 15 分钟更新一次根卷镜像关系。

```
job schedule interval create -name 15min -minutes 15
```

3. 创建镜像关系。

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. 初始化镜像关系并验证它是否已创建。

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

在 ONTAP 中配置 HTTPS 访问

要配置对存储控制器的安全访问，请完成以下步骤：

1. 提高访问证书命令的权限级别。

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. 通常，已有自签名证书。运行以下命令以验证证书：

```
security certificate show
```

3. 对于所示的每个 SVM ，证书公用名应与 SVM 的 DNS FQDN 匹配。四个默认证书应被删除，并替换为自签

名证书或证书颁发机构提供的证书。

> 最好在创建证书之前删除已过期的证书。运行 `security certificate delete` 命令删除已过期的证书。在以下命令中，使用 Tab completion 选择并删除每个默认证书。

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. 要生成并安装自签名证书，请一次性运行以下命令。为 infra-sVM 和集群 SVM 生成服务器证书。同样，请使用 Tab completion 帮助完成这些命令。

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 3650 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. 要获取以下步骤中所需参数的值，请运行 security certificate show 命令。
6. 使用 ` – server-enabled true` 和 ` – client-enabled false` 参数启用刚刚创建的每个证书。同样，请使用 Tab 补全。

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. 配置并启用 SSL 和 HTTPS 访问以及禁用 HTTP 访问。

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

> 其中某些命令通常会返回一条错误消息，指出此条目不存在。

8. 还原到管理员权限级别并创建设置，以使 SVM 可供 Web 使用。

```
set -privilege admin
vserver services web modify -name spi -vserver * -enabled true
```

在 ONTAP 中创建 NetApp FlexVol 卷

要创建 NetApp FlexVol ® 卷，请输入卷名称，大小及其所在的聚合。创建两个 VMware 数据存储库卷和一个服务器启动卷。

```
volume create -vserver Infra-SVM -volume infra_datastore -aggregate
aggr1_nodeB -size 500GB -state online -policy default -junction-path
/infra_datastore -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
-efficiency-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

在 ONTAP 中创建 LUN

要创建两个启动 LUN ，请运行以下命令：

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

> 添加额外的 Cisco UCS C 系列服务器时，必须创建额外的启动 LUN 。

在 ONTAP 中创建 iSCSI LIF

下表列出了完成此配置所需的信息。

详细信息	详细信息值
存储节点 A iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
存储节点 A iSCSI LIF01A 网络掩码	<<var_nodeA_iscsi_lif01a_mask>>
存储节点 A iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
存储节点 A iSCSI LIF01B 网络掩码	<<var_nodeA_iscsi_lif01b_mask>>
存储节点 B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
存储节点 B iSCSI LIF01A 网络掩码	<<var_nodeB_iscsi_lif01a_mask>>

详细信息	详细信息值
存储节点 B iSCSI LIF01B	<<var_nodeB_iscsi_lif01b_ip>>
存储节点 B iSCSI LIF01B 网络掩码	<<var_nodeB_iscsi_lif01b_mask>>

创建四个 iSCSI LIF ，每个节点两个。

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false
network interface show
```

在 **ONTAP** 中创建 **NFS LIF**

下表列出了完成此配置所需的信息。

详细信息	详细信息值
存储节点 A NFS LIF 01 IP	<<var_nodeA_nfs_lif_01_ip>>
存储节点 A NFS LIF 01 网络掩码	<<var_nodeA_nfs_lif_01_mask>>
存储节点 B NFS LIF 02 IP	<<var_nodeB_nfs_lif_02_ip>>
存储节点 B NFS LIF 02 网络掩码	<<var_nodeB_nfs_lif_02_mask>>

创建 NFS LIF 。

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up -failover-policy broadcast-
domain-wide -firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up -failover-policy broadcast-
domain-wide -firewall-policy data -auto-revert true
network interface show
```

添加基础架构 **SVM** 管理员

下表列出了添加 SVM 管理员所需的信息。

详细信息	详细信息值
Vsmgmt IP	<<var_svm_mgmt_ip>>
Vsmgmt 网络掩码	<<var_svm_mgmt_mask>>
Vsmgmt 默认网关	<<var_svm_mgmt_gateway>>

要将基础架构 SVM 管理员和 SVM 管理逻辑接口添加到管理网络，请完成以下步骤：

1. 运行以下命令：

```
network interface create -vserver Infra-SVM -lif vsmgmt -role data
-data-protocol none -home-node <<var_nodeB>> -home-port  e0M -address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
-failover-policy broadcast-domain-wide -firewall-policy mgmt -auto-
revert true
```

> 此处的 SVM 管理 IP 应与存储集群管理 IP 位于同一子网中。

2. 创建一个默认路由，以使 SVM 管理接口能够访问外部环境。

```
network route create -vserver Infra-SVM -destination 0.0.0.0/0 -gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. 为 SVM vsadmin 用户设置密码并解除锁定此用户。

```
security login password -username vsadmin -vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock -username vsadmin -vserver Infra-SVM
```

"接下来：部署Cisco UCS C系列机架式服务器。"

部署 **Cisco UCS C** 系列机架式服务器

本节详细介绍了用于配置 Cisco UCS C 系列独立机架服务器以在 FlexPod 快速配置中使用的操作步骤。

对 **CIMC** 执行初始 **Cisco UCS C** 系列独立服务器设置

完成以下步骤以初始设置 Cisco UCS C 系列独立服务器的 CIMC 接口。

下表列出了为每个 Cisco UCS C 系列独立服务器配置 CIMC 所需的信息。

详细信息	详细信息值
CIMC IP 地址	<<CMC_IP>>
CIMC 子网掩码	\<<CIMC 网络掩码
CIMC 默认网关	<<CIMC 网关 >>

此验证中使用的 CIMC 版本为 CIMC 4.0.4 （ 4 ）。

所有服务器

1. 将 Cisco 键盘，视频和鼠标（ KVM ）转换器（随服务器提供）连接到服务器正面的 KVM 端口。将 VGA 显示器和 USB 键盘插入相应的 KVM 转换器端口。

   打开服务器电源，在系统提示您输入 CIMC 配置时按 F8 。

2. 在 CIMC 配置实用程序中，设置以下选项：

   a. 网络接口卡（ Network Interface Card ， NIC ）模式：

      专用 ` X`

   b. IP （基本）：

      IPv4 ： ` X`

      已启用 DHCP ： ` [ ]`

      CIMC IP ： ` [CIMC IP ]`

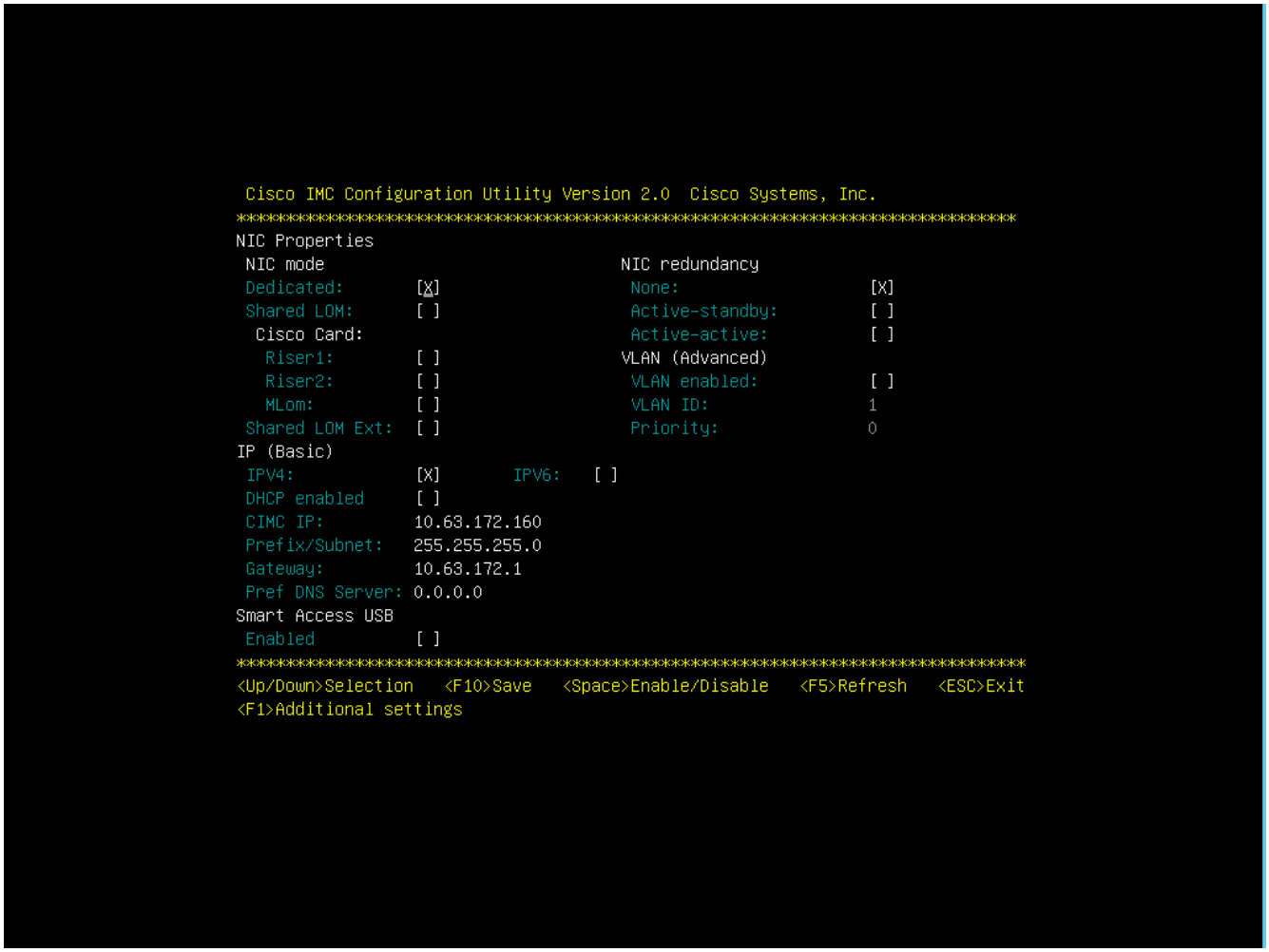
      前缀 / 子网： ` <<CIMC _netmask>>`

      网关： ` [CIMC 网关 ]`

   c. VLAN （高级）：保持清除状态以禁用 VLAN 标记。

      NIC 冗余

      无： ` X`



3. 按 F1 可查看其他设置：

   a. 通用属性：

      主机名：`<<ESXi_host_name>>`

      动态 DNS：`[ ]`

      出厂默认设置：保持清除状态。

   b. 默认用户（基本）：

      默认密码：`<<admin_password>>`

      重新输入密码：`<<admin_password>>`

      端口属性：使用默认值。

   端口配置文件：保持清除状态。

4. 按 F10 保存 CIMC 接口配置。
5. 保存配置后，按 Esc 退出。

配置 **Cisco UCS C** 系列服务器 **iSCSI** 启动

在此 FlexPod 快速配置中， VIC1457 用于 iSCSI 启动。

下表列出了配置 iSCSI 启动所需的信息。

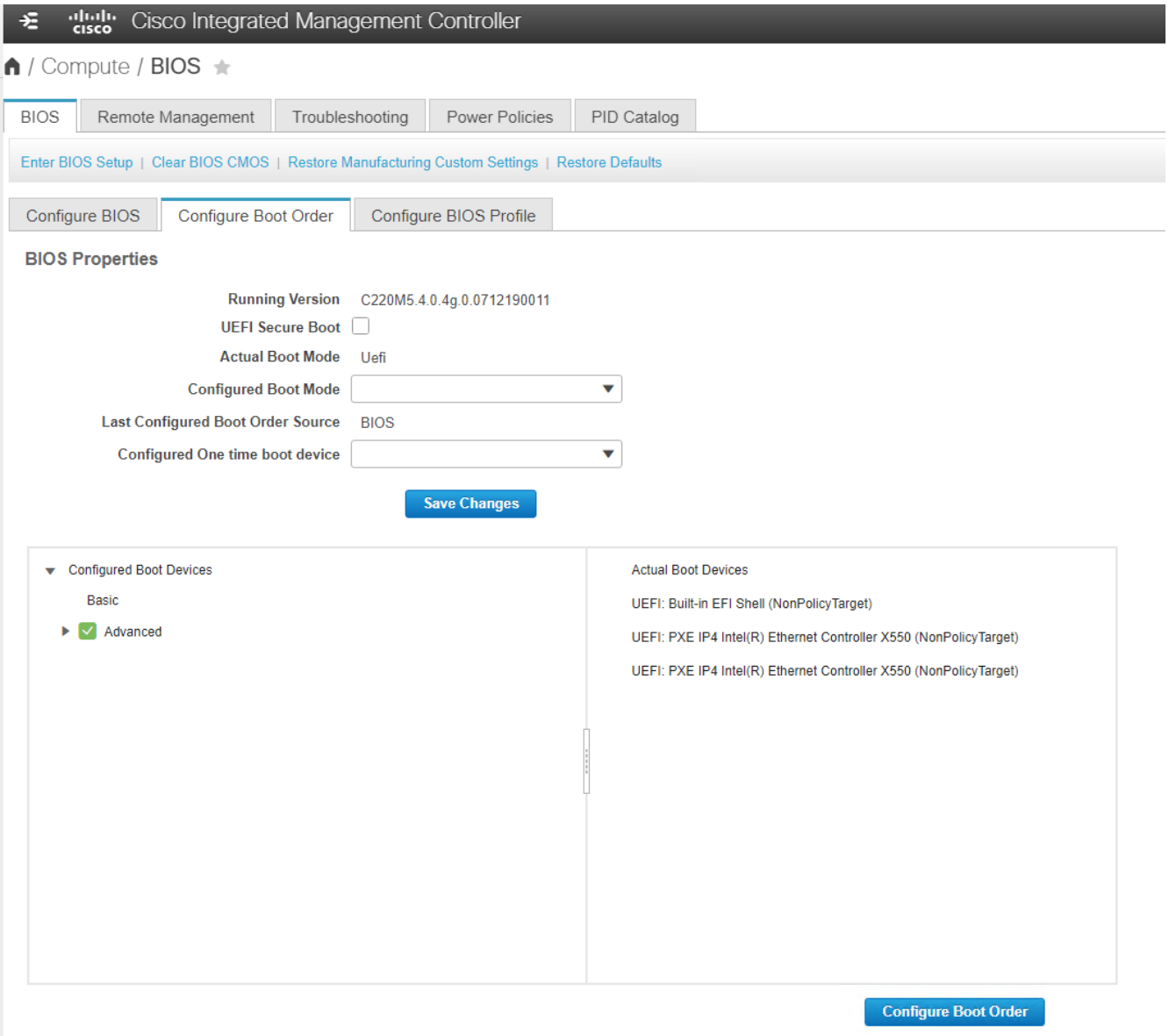
> 斜体表示每个 ESXi 主机唯一的变量。

详细信息	详细信息值
ESXi 主机启动程序 A 名称	<<var_UCS_initiator_name_A>>
ESXi 主机 iSCSI-A IP	<<var_esxi_host_iscsiA_IP>>
ESXi 主机 iSCSI-A 网络掩码	<<var_esxi_host_iscsiA_mask>>
ESXi 主机 iSCSI 是默认网关	<<var_esxi_host_iscsiA_gateway>>
ESXi 主机启动程序 B 名称	<<var_UCS_initiator_name_B>>
ESXi 主机 iSCSI-B IP	<<var_esxi_host_iscsiB_ip>>
ESXi 主机 iSCSI-B 网络掩码	<<var_esxi_host_iscsiB_mask>>
ESXi 主机 iSCSI-B 网关	<<var_esxi_host_iscsiB_gateway>>
IP 地址 iscsi_lif01a	<<var_iscsi_lif01a>>
IP 地址 iscsi_lif02a	<<var_iscsi_lif02a>>
IP 地址 iscsi_lif01b	<<var_iscsi_lif01b>>
IP 地址 iscsi_lif02b	<<var_iscsi_lif02b>>
infra_sVM IQN	<<var_svm_IQN>>

启动顺序配置

要设置启动顺序配置，请完成以下步骤：

1. 在 CIMC 界面浏览器窗口中，单击 Compute 选项卡并选择 BIOS 。
2. 单击 Configure Boot Order ，然后单击 OK 。



3. 单击 "Add Boot Device" 下的设备并转到 "Advanced （高级） " 选项卡，配置以下设备：

   a. 添加虚拟介质：

      名称： KVM-CD-DVD

      子类型： KVM 映射的 DVD

      状态：已启用

      顺序： 1

   b. 添加 iSCSI 启动：

      名称： iscsi-A

      状态：已启用

      顺序： 2

插槽： MLOM

端口： 1

c. 单击 Add iSCSI Boot ：

名称： iSCSI-B

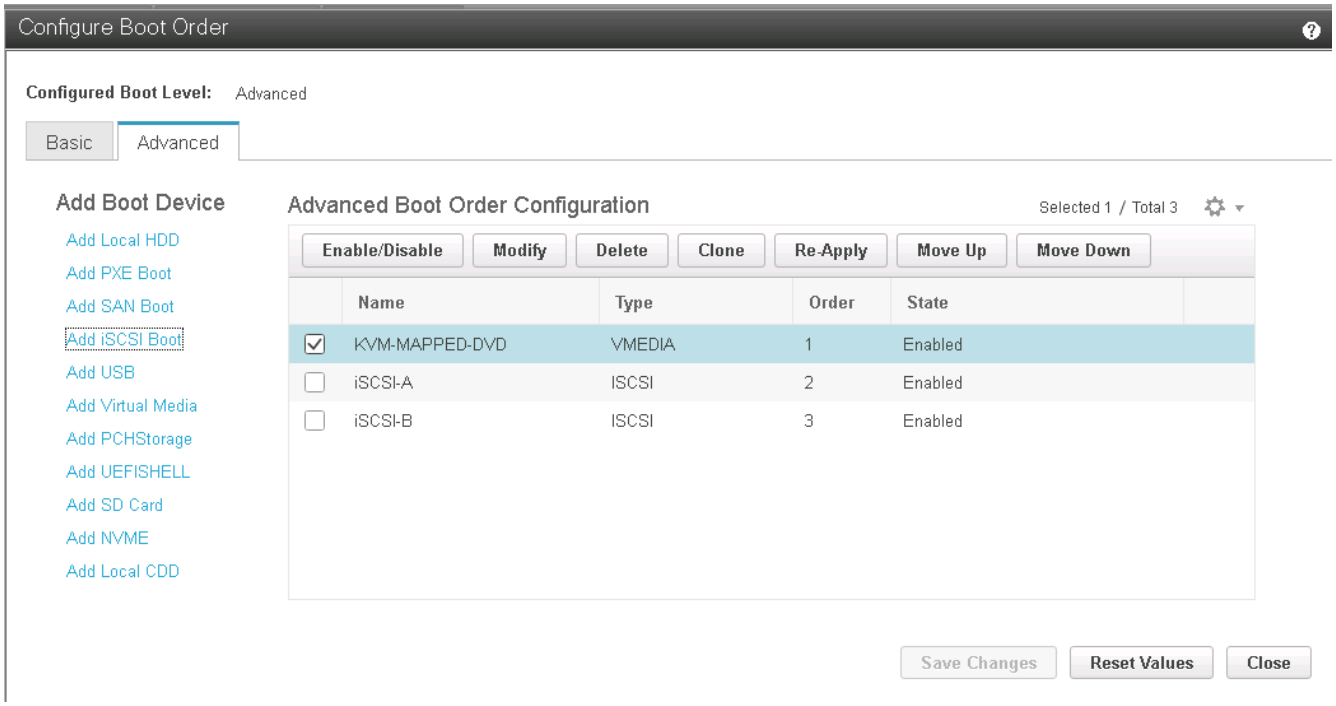
状态：已启用

顺序： 3

插槽： MLOM

端口： 3

4. 单击添加设备。
5. 单击保存更改，然后单击关闭。

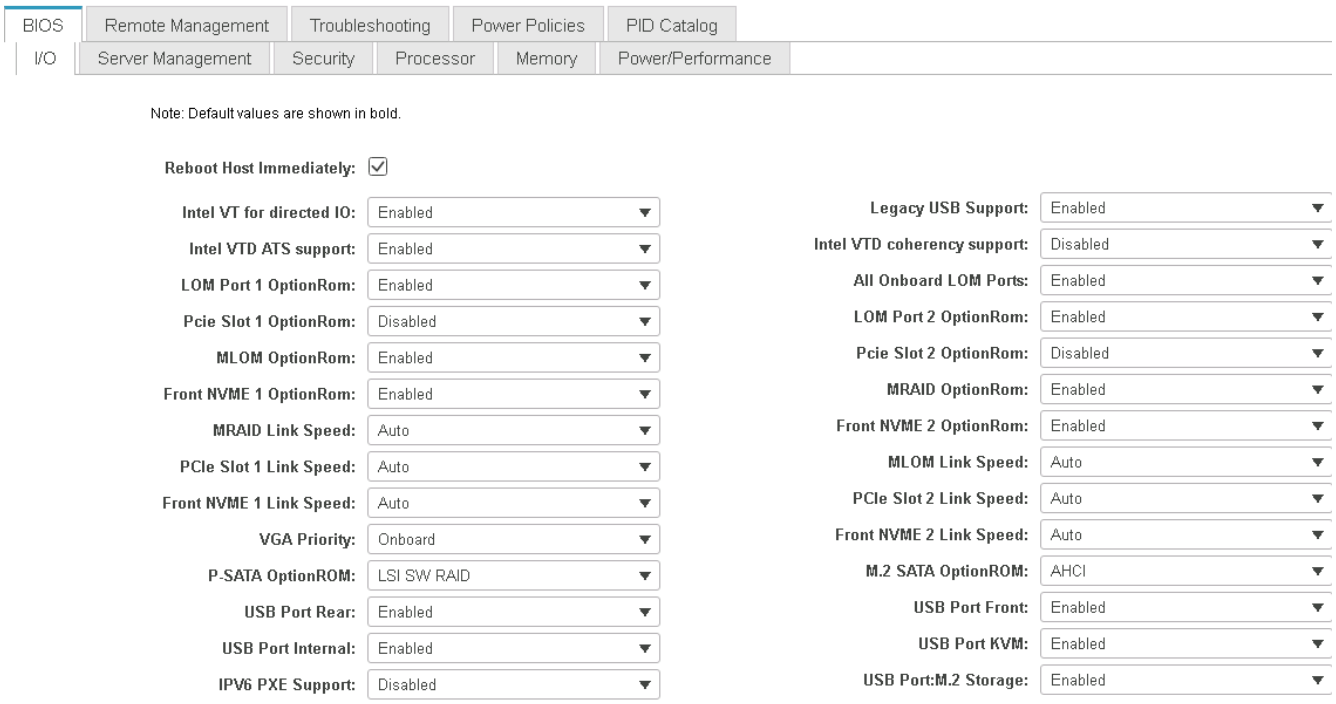


6. 重新启动服务器以使用新的启动顺序启动。

禁用 **RAID** 控制器（如果存在）

如果 C 系列服务器包含 RAID 控制器，请完成以下步骤。从 SAN 启动配置不需要 RAID 控制器。您也可以从服务器中物理删除 RAID 控制器。

1. 在 Compute 选项卡下，单击 CIMC 左侧导航窗格中的 BIOS 。
2. 选择 Configure BIOS 。
3. 向下滚动到 PCIe 插槽： HBA 选项 ROM 。
4. 如果尚未禁用此值，请将其设置为 disabled 。

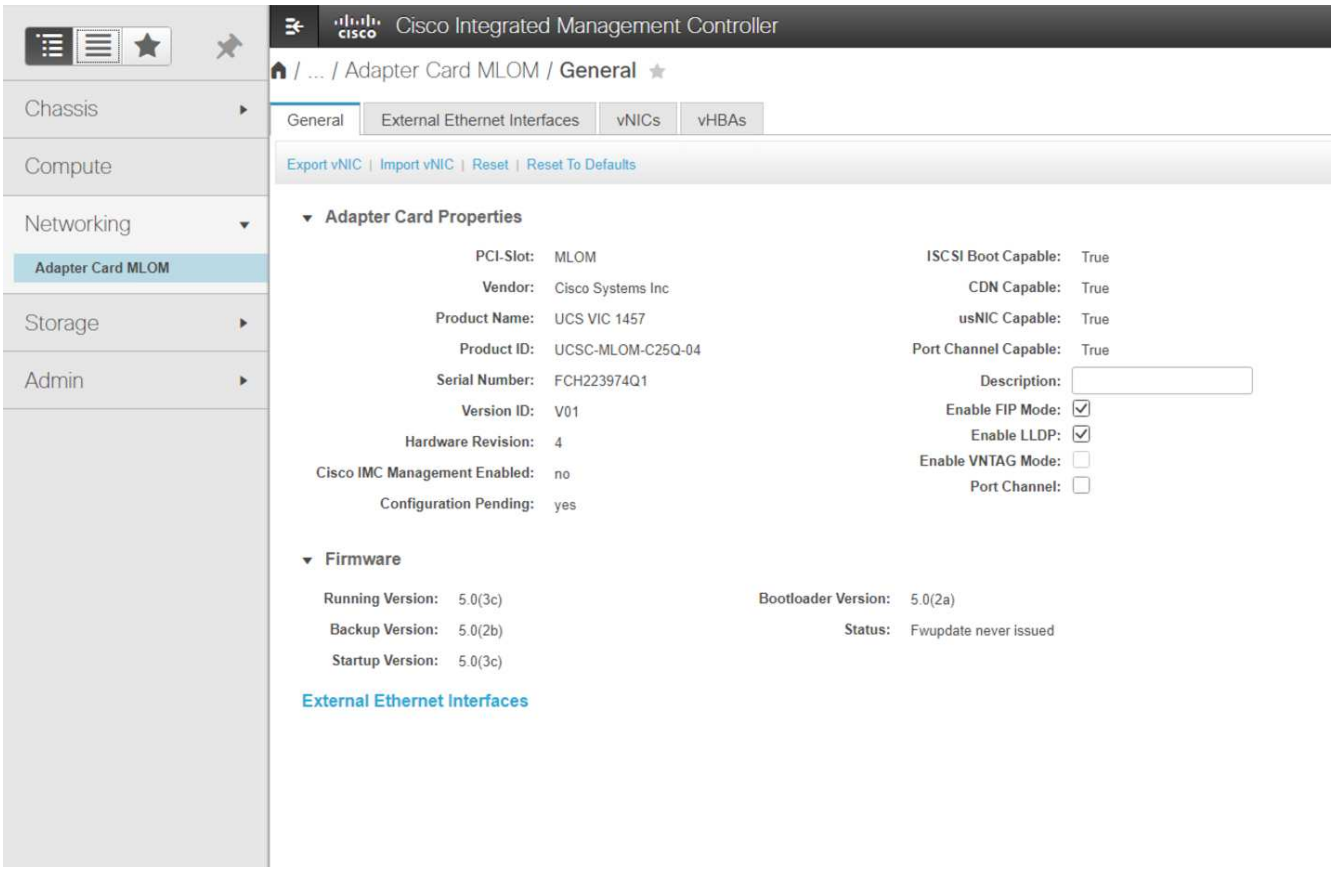


为 **iSCSI** 启动配置 **Cisco VIC1457**

以下配置步骤适用于用于 iSCSI 启动的 Cisco VIC 1457 。

> 必须先关闭端口 0 ， 1 ， 2 和 3 之间的默认端口通道，然后才能配置四个单独的端口。如果端口通道未关闭，则 VIC 1457 仅显示两个端口。完成以下步骤以在 CIMC 上启用端口通道：

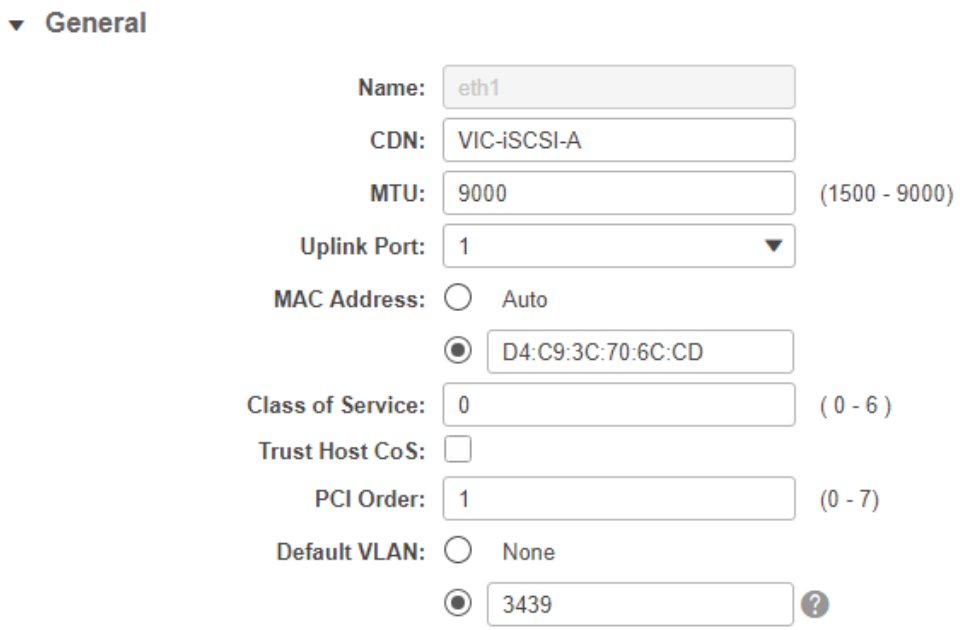
1. 在网络连接选项卡下，单击适配器卡 MLOM 。
2. 在常规选项卡下，取消选中端口通道。
3. 保存更改并重新启动 CIMC 。



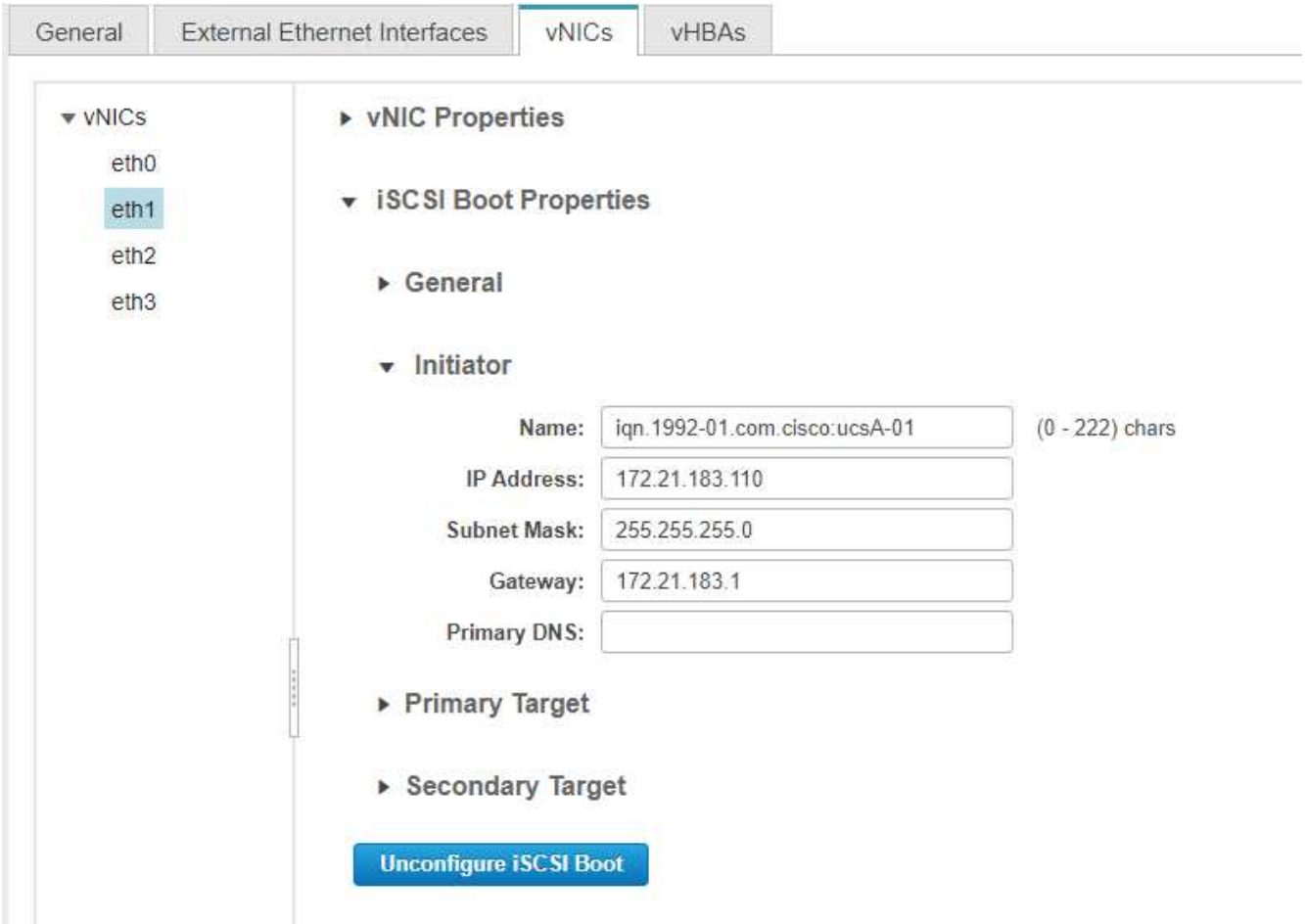
创建 **iSCSI vNIC**

要创建 iSCSI vNIC ，请完成以下步骤：

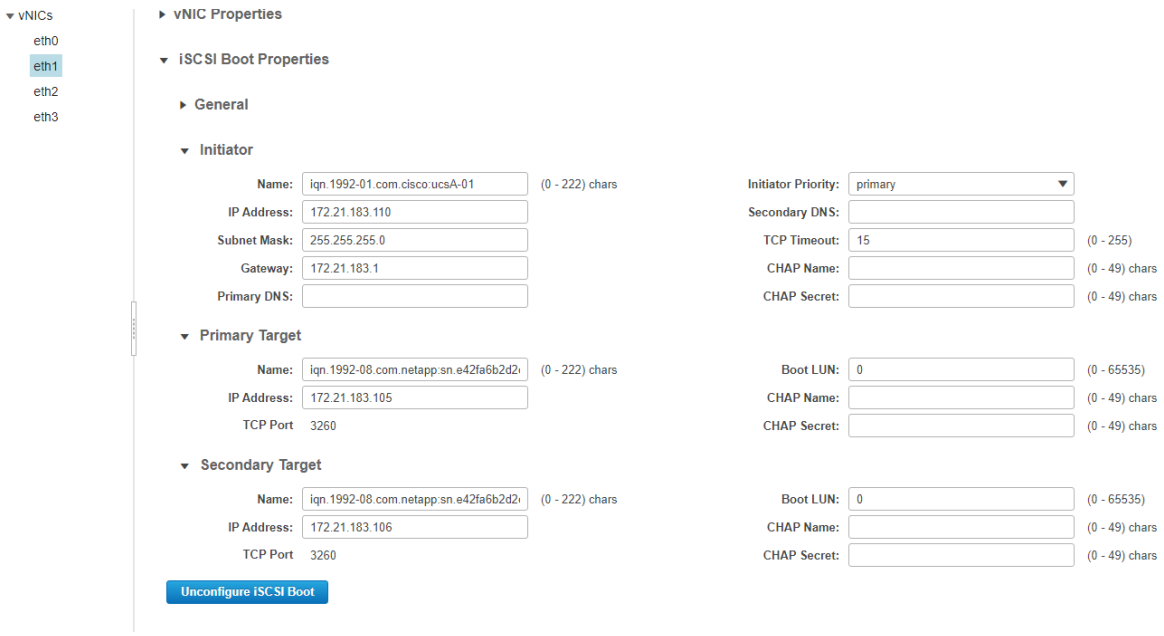
1. 在网络连接选项卡下，单击适配器卡 MLOM 。
2. 单击添加 vNIC 以创建 vNIC 。
3. 在 Add vNIC 部分中，输入以下设置：
   - 名称： eth1
   - CDN 名称： iscsi-vNIC-A
   - MTU ： 9000
   - 默认 VLAN ： ` <<var_iscsi_vlan_A>>`
   - VLAN 模式：中继
   - Enable PXE boot ： check
4. 单击添加 vNIC ，然后单击确定。
5. 重复此过程以添加第二个 vNIC ：
   - 将 vNIC 命名为 eth3 。
   - CDN 名称： iscsi-vNIC-B
   - 输入 ` <<var_iscsi_vlan_b>>` 作为 VLAN 。
   - 将上行链路端口设置为 3 。



6. 选择左侧的 vNIC eth1 。



7. 在 "iSCSI 启动属性 " 下，输入启动程序详细信息：
    - 名称： ` <<var_UCSA_initiator_name_A>>`
    - IP 地址： ` [var_esxi_HostA_iscsiA_IP]`
    - 子网掩码： ` [var_esxi_HostA_iscsiA_mask]`
    - 网关： ` [var_esxi_HostA_iscsiA_gateway]`



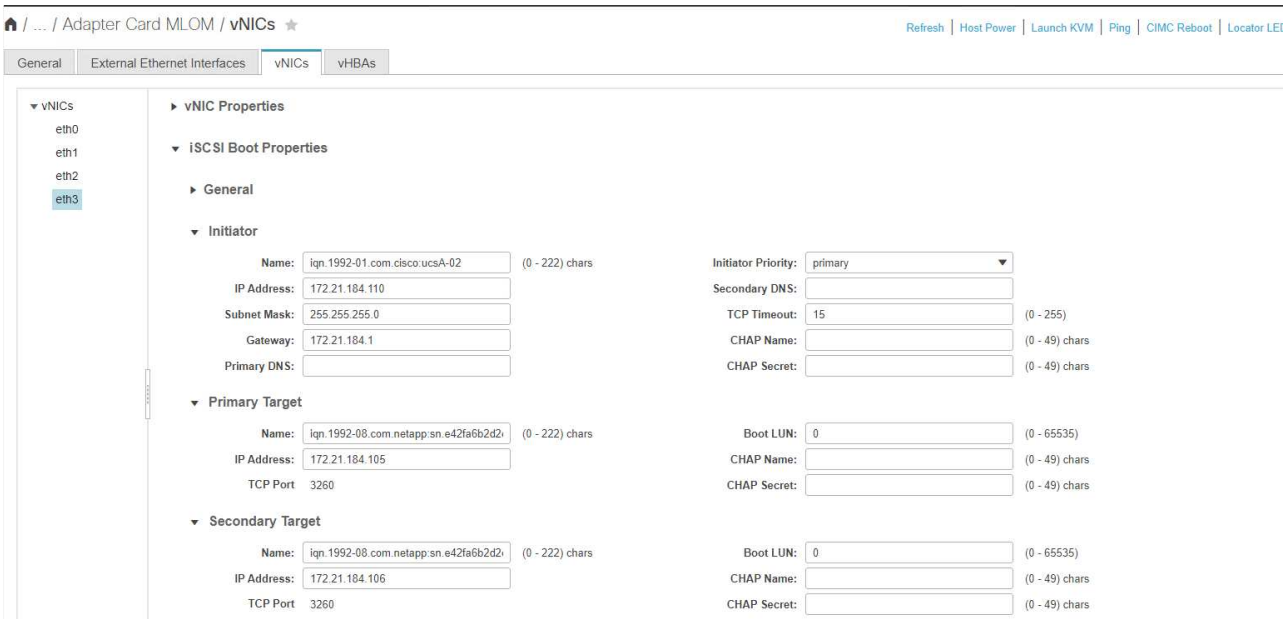
8. 输入主目标详细信息：
    - 名称： infra-svm 的 IQN 编号
    - IP address ： iSCSI_lif01a 的 IP 地址
    - 启动 LUN ： 0
9. 输入二级目标详细信息：
    - 名称： infra-svm 的 IQN 编号
    - IP address ： iSCSI_lif02a 的 IP 地址
    - 启动 LUN ： 0

> 您可以运行 `vserver iscsi show` 命令来获取存储 IQN 编号。

> 请务必记录每个 vNIC 的 IQN 名称。您需要在后续步骤中使用它们。此外，启动程序的 IQN 名称对于每个服务器和 iSCSI vNIC 都必须是唯一的。

10. 单击 Save Changes 。
11. 选择 vNIC eth3 ，然后单击主机以太网接口部分顶部的 iSCSI 启动按钮。
12. 重复此过程以配置 eth3 。
13. 输入启动程序详细信息：

- 名称： ` <<var_UCSA_initiator_name_b>>`
- IP 地址： ` [var_esxi_HostB_iscsib_ip]`
- 子网掩码： ` [var_esxi_HostB_iscsib_mask]`
- 网关： ` [var_esxi_HostB_iscsib_gateway]`



14. 输入主目标详细信息：
    - 名称： infra-svm 的 IQN 编号
    - IP address ： iSCSI_lif01b 的 IP 地址
    - 启动 LUN ： 0
15. 输入二级目标详细信息：
    - 名称： infra-svm 的 IQN 编号
    - IP address ： iSCSI_lif02b 的 IP 地址
    - 启动 LUN ： 0

> 您可以使用 `vserver iscsi show` 命令获取存储 IQN 编号。

> 请务必记录每个 vNIC 的 IQN 名称。您需要在后续步骤中使用它们。

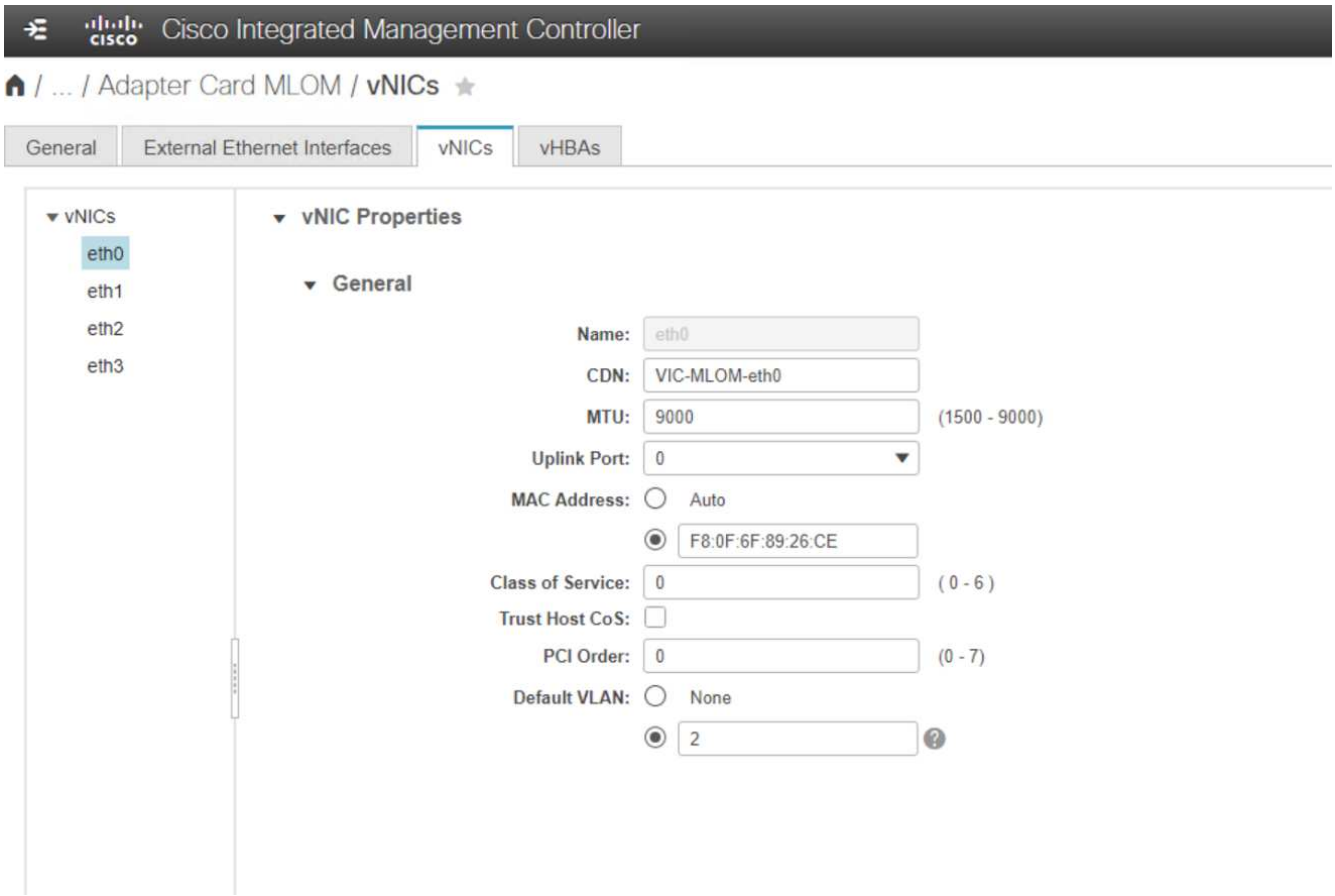
16. 单击 Save Changes 。
17. 重复此过程为 Cisco UCS 服务器 B 配置 iSCSI 启动

为 **ESXi** 配置 **vNIC**

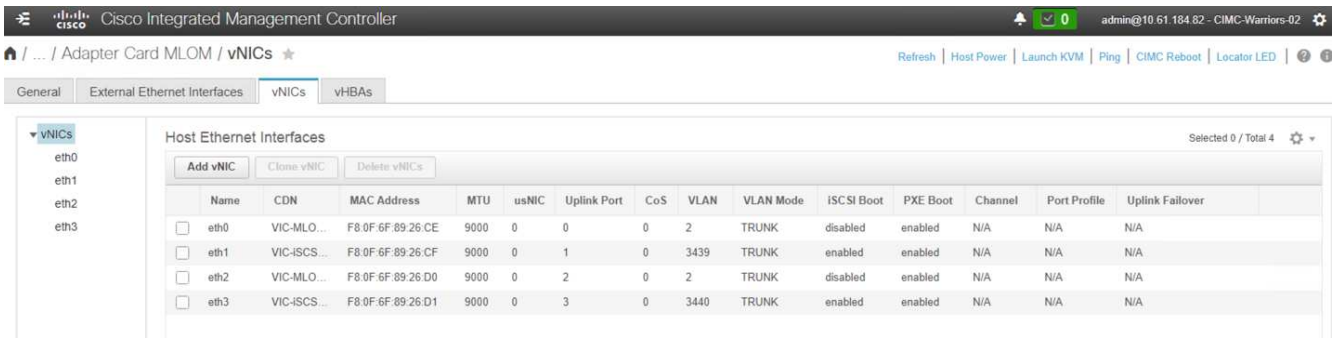
要为 ESXi 配置 vNIC ，请完成以下步骤：

1. 在 CIMC 界面浏览器窗口中，单击清单，然后单击右窗格上的 Cisco VIC 适配器。

2. 在 Networking > Adapter Card MLOM 下，选择 vNIC 选项卡，然后选择下方的 vNIC 。
3. 选择 eth0 并单击属性。
4. 将 MTU 设置为 9000 。单击 Save Changes 。
5. 将 VLAN 设置为原生 VLAN 2 。



6. 对 eth1 重复步骤 3 和 4 ，验证 eth1 的上行链路端口是否设置为 1 。



> 必须对添加到环境中的每个初始 Cisco UCS 服务器节点和每个额外的 Cisco UCS 服务器节点重复此操作步骤。

"下一步：NetApp AFF 存储部署操作步骤 (第2部分)。"

NetApp AFF 存储部署操作步骤（第 2 部分）

设置 **ONTAP SAN** 启动存储

创建 iSCSI igroup

在此步骤中，您需要使用服务器配置中的 iSCSI 启动程序 IQN 。

要创建 igroup ，请从集群管理节点 SSH 连接运行以下命令。要查看此步骤中创建的三个 igroup ，请运行 `igroup show` 命令。

```
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-A -protocol iscsi
-ostype vmware -initiator <<var_vm_host_infra_a_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-B -protocol iscsi
-ostype vmware -initiator <<var_vm_host_infra_b_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

添加其他 Cisco UCS C 系列服务器时，必须完成此步骤。

将启动 **LUN** 映射到 **igroup**

```
To map boot LUNs to igroups, run the following commands from the cluster
management SSH connection:
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -igroup
VM-Host-Infra-A -lun-id 0
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -igroup
VM-Host-Infra-B -lun-id 0
```

添加其他 Cisco UCS C 系列服务器时，必须完成此步骤。

"下一步：VMware vSphere 6.7U2部署操作步骤。"

VMware vSphere 6.7U2 部署操作步骤

本节详细介绍了在 FlexPod 快速配置中安装 VMware ESXi 6.7U2 的过程。下面的部署过程已进行自定义，以包括前面几节所述的环境变量。

在此类环境中安装 VMware ESXi 的方法有多种。此操作步骤使用适用于 Cisco UCS C 系列服务器的 CIMC 界面的虚拟 KVM 控制台和虚拟介质功能，将远程安装介质映射到每个服务器。

必须为 Cisco UCS 服务器 A 和 Cisco UCS 服务器 B 完成此操作步骤

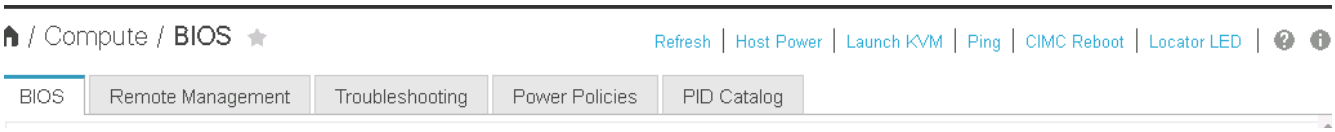
对于添加到集群中的任何其他节点，必须完成此操作步骤。

登录到 Cisco UCS C 系列独立服务器的 CIMC 界面

以下步骤详细介绍了登录到 Cisco UCS C 系列独立服务器的 CIMC 界面的方法。您必须登录到 CIMC 界面才能运行虚拟 KVM ，管理员可以通过远程介质开始安装操作系统。

所有主机

1. 导航到 Web 浏览器，然后输入 Cisco UCS C 系列的 CIMC 接口的 IP 地址。此步骤将启动 CIMC GUI 应用程序。
2. 使用管理员用户名和凭据登录到 CIMC UI 。
3. 在主菜单中，选择服务器选项卡。
4. 单击 Launch KVM Console 。



5. 从虚拟 KVM 控制台中，选择 Virtual Media 选项卡。
6. 选择映射 CD/DVD 。

> 您可能需要先单击激活虚拟设备。如果出现提示，请选择 Accept this session 。

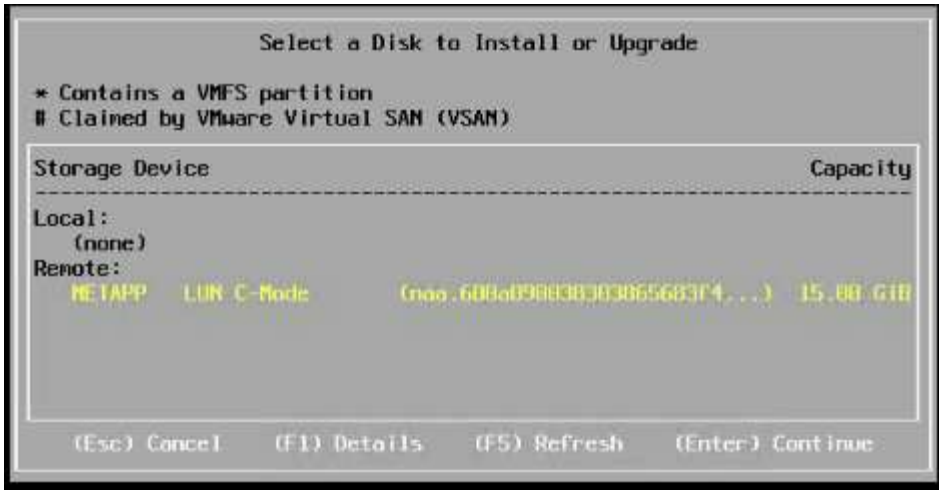
7. 浏览到 VMware ESXi 6.7U2 安装程序 ISO 映像文件，然后单击打开。单击映射设备。
8. 选择电源菜单，然后选择系统重新启动（冷启动）。单击是。

安装 VMware ESXi

以下步骤介绍了如何在每台主机上安装 VMware ESXi 。

下载 **ESXi 6.7U2 Cisco** 自定义映像

1. 导航到 "VMware vSphere 下载页面" 用于自定义 ISO 。
2. 单击适用于 ESXi 6.7U2 安装 CD 的 Cisco 自定义映像旁边的转至下载。
3. 下载适用于 ESXi 6.7U2 安装 CD （ ISO ）的 Cisco 自定义映像。
4. 系统启动时，计算机会检测是否存在 VMware ESXi 安装介质。
5. 从显示的菜单中选择 VMware ESXi 安装程序。安装程序将加载，可能需要几分钟时间。
6. 安装程序加载完毕后，按 Enter 继续安装。
7. 阅读最终用户许可协议后，接受该协议并按 F11 继续安装。
8. 选择先前设置为 ESXi 安装磁盘的 NetApp LUN ，然后按 Enter 继续安装。



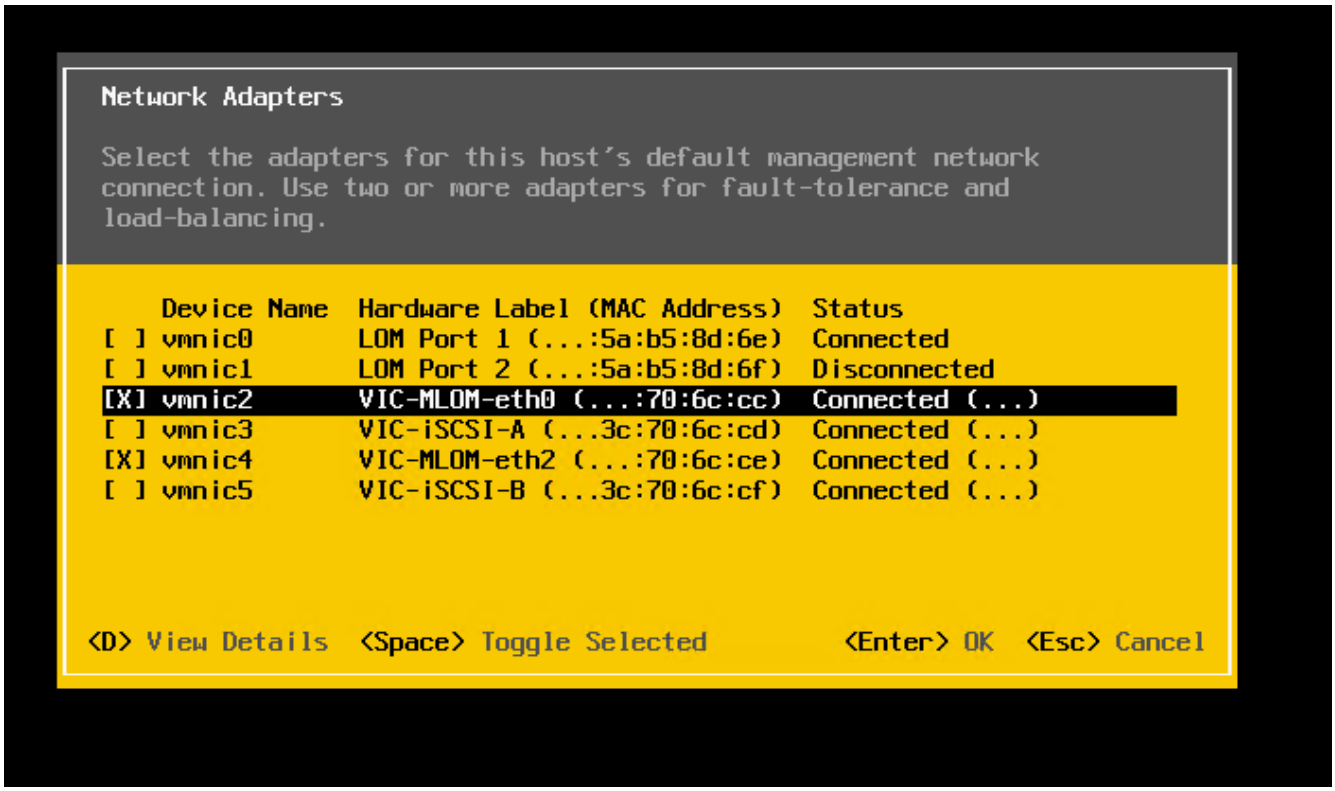
9. 选择适当的键盘布局，然后按 Enter 键。
10. 输入并确认根密码，然后按 Enter 键。
11. 安装程序会警告您已删除卷上的现有分区。按 F11 继续安装。安装 ESXi 后，服务器将重新启动。

设置 **VMware ESXi** 主机管理网络

以下步骤介绍了如何为每个 VMware ESXi 主机添加管理网络。

所有主机

1. 服务器完成重新启动后，按 F2 输入选项以自定义系统。
2. 使用 root 作为登录名登录，并使用先前在安装过程中输入的 root 密码登录。
3. 选择配置管理网络选项。
4. 选择网络适配器，然后按 Enter 键。
5. 为 vSwitch0 选择所需的端口。按 Enter 键。
6. 在 CIMC 中选择与 eth0 和 eth1 对应的端口。



7. 选择 VLAN （可选）并按 Enter 键。
8. 输入 VLAN ID ` <<mgmt_vlan_id>>` 。按 Enter 键。
9. 从配置管理网络菜单中，选择 IPv4 配置以配置管理接口的 IP 地址。按 Enter 键。
10. 使用箭头键选中设置静态 IPv4 地址，然后使用空格键选择此选项。
11. 输入用于管理 VMware ESXi 主机 ` 的 IP 地址 <<ESXi_host_mgmt_ip>>` 。
12. 输入 VMware ESXi 主机的子网掩码 ` <<ESXi_host_mgmt_netmask>>` 。
13. 输入 VMware ESXi 主机的默认网关 ` <<ESXi_host_mgmt_gateway>>` 。
14. 按 Enter 接受对 IP 配置所做的更改。
15. 进入 IPv6 配置菜单。
16. 使用空格键取消选择启用 IPv6 （需要重新启动）选项以禁用 IPv6 。按 Enter 键。
17. 进入菜单配置 DNS 设置。
18. 由于 IP 地址是手动分配的，因此还必须手动输入 DNS 信息。
19. 输入主 DNS 服务器的 IP 地址 ` <<nameserver_ip>>` 。
20. （可选）输入辅 DNS 服务器的 IP 地址。
21. 输入 VMware ESXi 主机名的 FQDN： ` <<ESXi_host_FQDN>>` 。
22. 按 Enter 接受对 DNS 配置所做的更改。
23. 按 Esc 退出配置管理网络子菜单。
24. 按 Y 确认更改并重新启动服务器。
25. 选择 Troubleshooting Options ，然后选择 Enable ESXi Shell and SSH 。

在根据客户的安全策略进行验证后，可以禁用这些故障排除选项。

26. 按两次 Esc 可返回到主控制台屏幕。
27. 从屏幕顶部的 CIMC 宏 > 静态宏 > Alt-F 下拉菜单中单击 Alt-F1 。
28. 使用 ESXi 主机的正确凭据登录。
29. 在提示符处，按顺序输入以下 esxcli 命令列表以启用网络连接。

```
esxcli network vswitch standard policy failover set -v vSwitch0 -a
vmnic2,vmnic4 -l iphash
```

配置 **ESXi** 主机

使用下表中的信息配置每个 ESXi 主机。

详细信息	详细信息值
ESXi 主机名	<<ESXi_host_FQDN>>
ESXi 主机管理 IP	<<ESXi_host_mgmt_ip>>
ESXi 主机管理掩码	<<ESXi_host_mgmt_netmask>>
ESXi 主机管理网关	<<ESXi_host_mgmt_gateway>>
ESXi 主机 NFS IP	<<ESXi_host_nfs_ip>>
ESXi 主机 NFS 掩码	<<ESXi_host_nfs_netmask>>
ESXi 主机 NFS 网关	<<ESXi_host_nfs_gateway>>
ESXi 主机 vMotion IP	<<ESXi_host_vMotion_IP>>
ESXi 主机 vMotion 掩码	<<ESXi_host_vMotion_netmask>>
ESXi 主机 vMotion 网关	<<ESXi_host_vMotion_gateway>>
ESXi 主机 iSCSI-A IP	<<ESXi_host_iscsi-A_IP>>
ESXi 主机 iSCSI-A 掩码	<<ESXi_host_iscsi-a_netmask>>
ESXi 主机 iSCSI-A 网关	<<ESXi_host_iscsi-a_gateway>>
ESXi 主机 iSCSI-B IP	<<ESXi_host_iscsi-B_ip>>
ESXi 主机 iSCSI-B 掩码	<<ESXi_host_iscsi-B_netmask>>
ESXi 主机 iSCSI-B 网关	<<ESXi_host_scsi-B_gateway>>

登录到 **ESXi** 主机

要登录到 ESXi 主机，请完成以下步骤：

1. 在 Web 浏览器中打开主机的管理 IP 地址。
2. 使用 root 帐户和您在安装过程中指定的密码登录到 ESXi 主机。

3. 阅读有关 VMware 客户体验改进计划的声明。选择正确的响应后，单击确定。

配置 **iSCSI** 启动

要配置 iSCSI 启动，请完成以下步骤：

1. 选择左侧的 Networking 。
2. 在右侧，选择 Virtual Switches 选项卡。

3. 单击 iScsiBootvSwitch 。
4. 选择编辑设置。
5. 将 MTU 更改为 9000 ，然后单击保存。
6. 将 iSCSIBootPG 端口重命名为 iSCSIBootPG-A

> 在此配置中， vmnic3 和 vmnic5 用于 iSCSI 启动。如果 ESXi 主机中有其他 NIC ，则可能具有不同的 vmnic 编号。要确认用于 iSCSI 启动的 NIC ，请将 CIMC 中 iSCSI vNIC 上的 MAC 地址与 ESXi 中的 vmnic 进行匹配。

7. 在中间窗格中，选择 VMkernel NIC 选项卡。
8. 选择添加 VMkernel NIC 。
   a. 指定 iScsiBootPG-B 的新端口组名称
   b. 为虚拟交换机选择 iScsiBootvSwitch 。
   c. 输入 ` <<iscsib_vlan_id>>` 作为 VLAN ID 。
   d. 将 MTU 更改为 9000 。
   e. 展开 IPv4 设置。
   f. 选择静态配置。
   g. 为地址输入 ` <<var_hosta_iscsib_ip>>` 。

h. 为子网掩码输入 ` <<var_hosta_iscsib_mask>>` 。

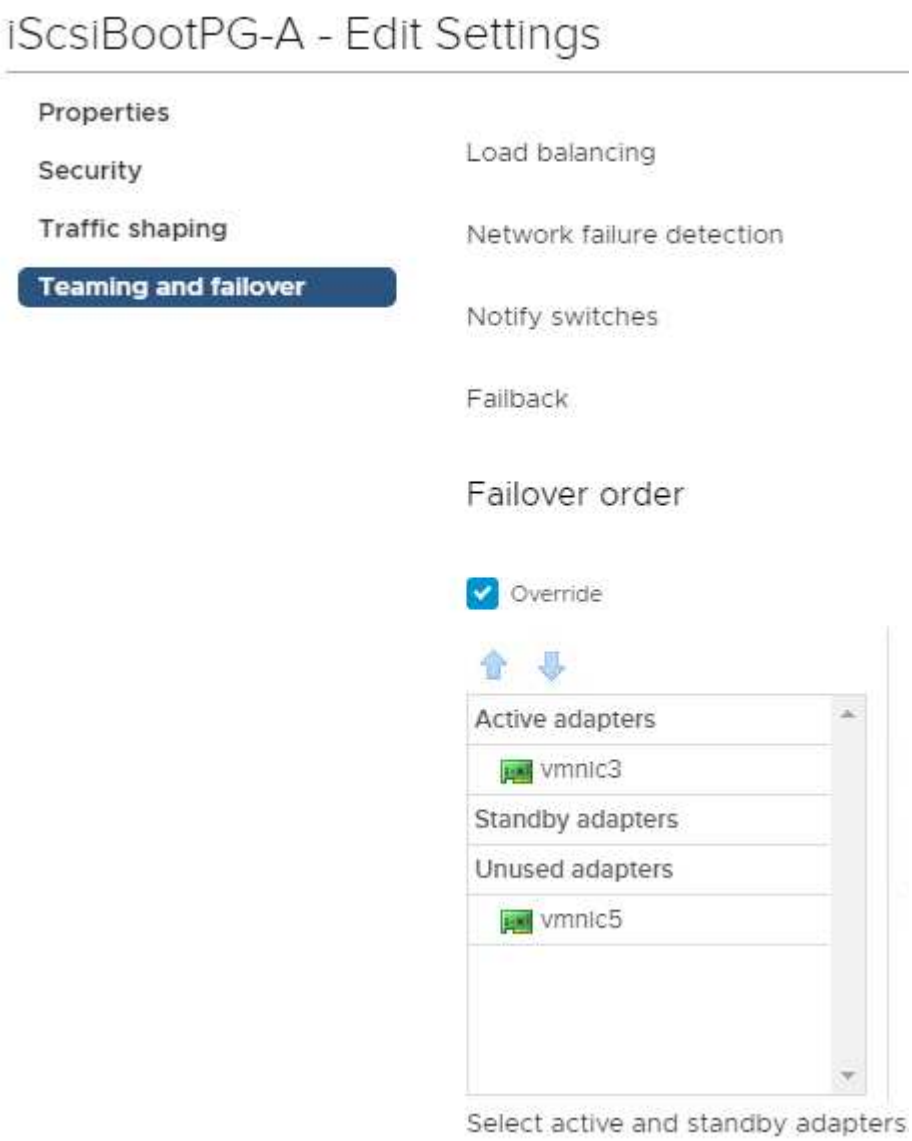
i. 单击创建。

> 在 iScsiBootPG-A 上将 MTU 设置为 9000

9. 要设置故障转移，请完成以下步骤：

   a. 单击 "iSCSIBootPG-A">" 分层和故障转移 ">" 故障转移顺序 ">"vmnic3" 上的编辑设置。vmnic3 应为活动状态， vmnic5 应为未使用状态。

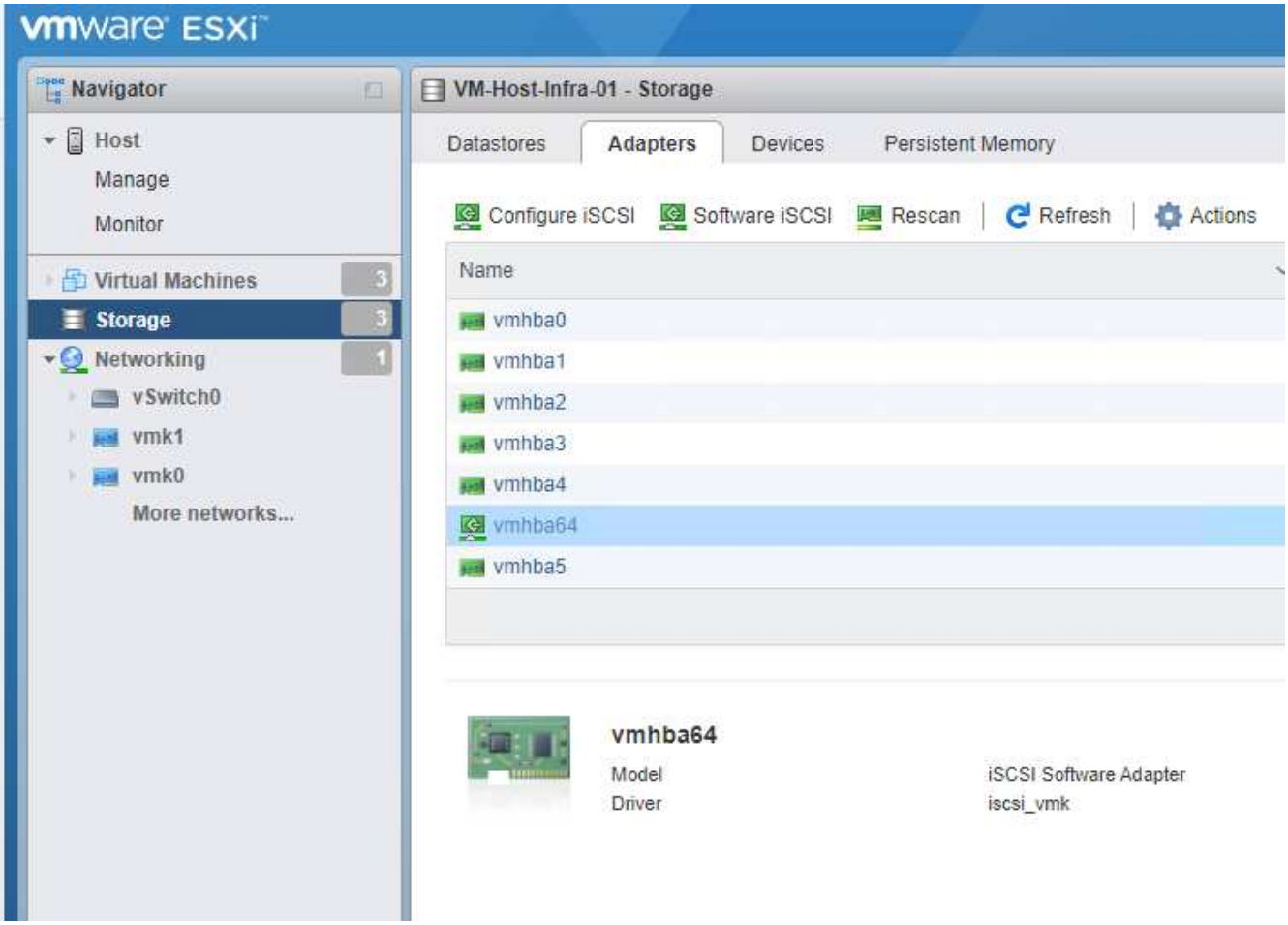
   b. 单击 "iSCSIBootPG-B 上的编辑设置 ">" 绑定和故障转移 ">" 故障转移顺序 ">"vmnic5" 。vmnic5 应为活动状态， vmnic3 应为未使用状态。



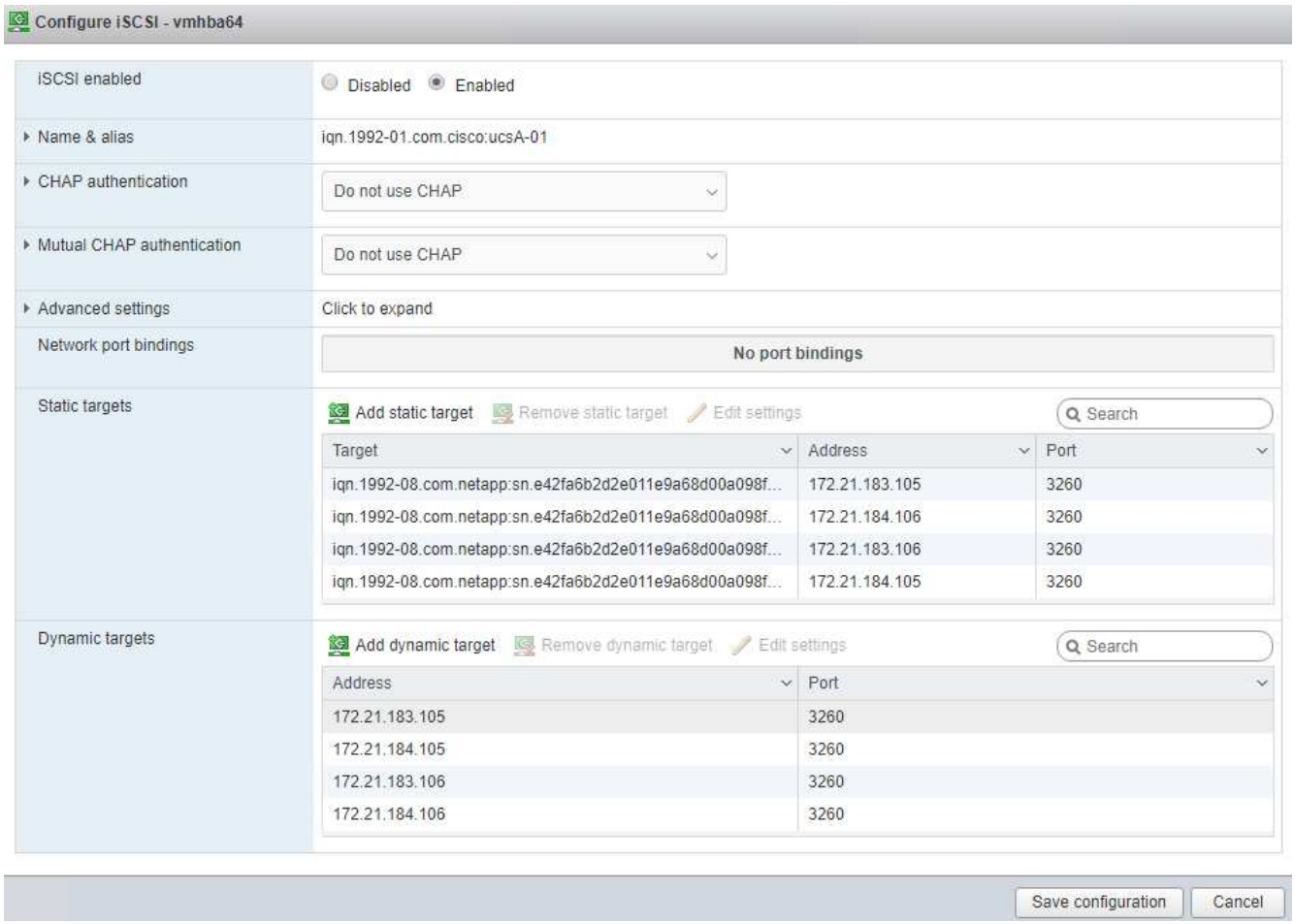
配置 **iSCSI** 多路径

要在 ESXi 主机上设置 iSCSI 多路径，请完成以下步骤：

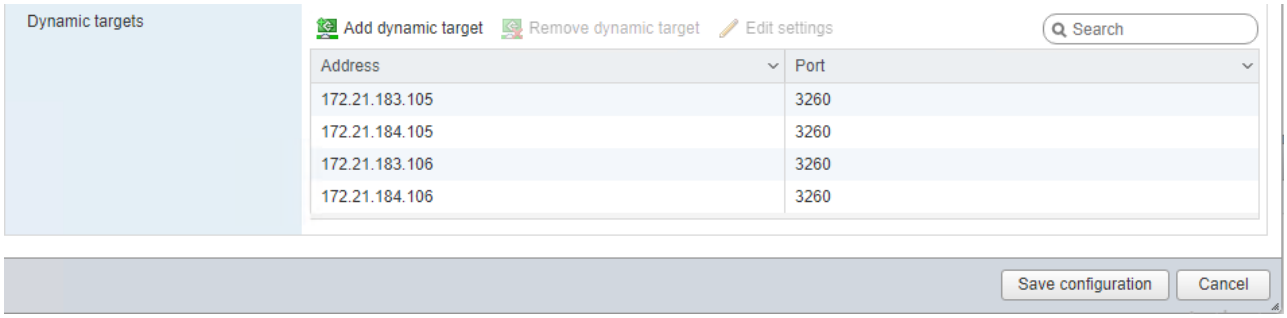
1. 在左侧导航窗格中选择存储。单击适配器。
2. 选择 iSCSI 软件适配器，然后单击配置 iSCSI 。



3. 在动态目标下，单击添加动态目标。



4. 输入 IP 地址 `iscsi_lif01a` 。
   a. 对 IP 地址 `iscsi_lif01b` ， `iscsi_lif02a` 和 `iscsi_lif02b` 重复上述步骤。
   b. 单击保存配置。



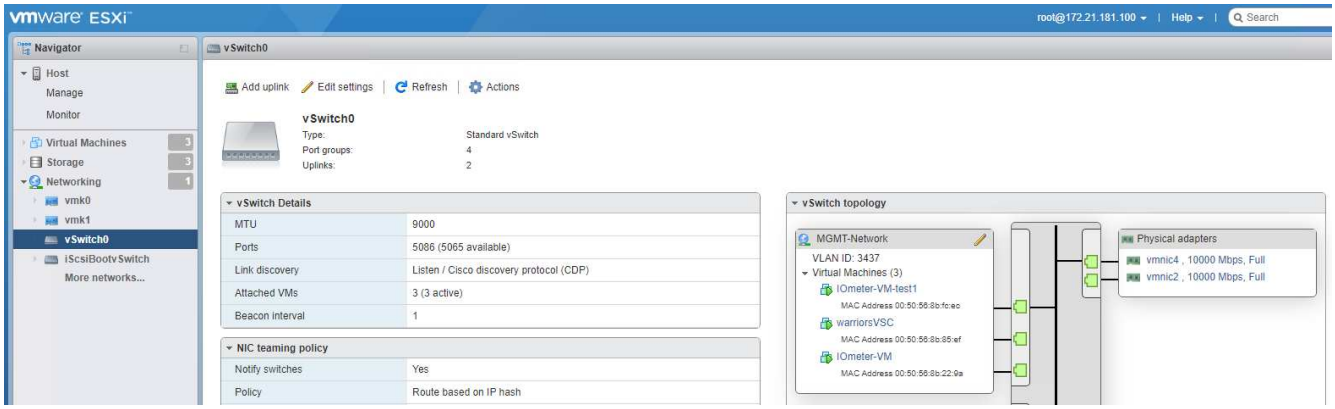
> 您可以通过在 NetApp 集群上运行 network interface show 命令或查看 System Manager 中的 Network Interfaces 选项卡来查找 iSCSI LIF IP 地址。

配置 **ESXi** 主机

要配置 ESXi 启动，请完成以下步骤：

1. 在左侧导航窗格中，选择网络。

2. 选择 vSwitch0 。



3. 选择编辑设置。
4. 将 MTU 更改为 9000 。
5. 展开 NIC 绑定并验证 vmnic2 和 vmnic4 是否均已设置为 active ， NIC 绑定和故障转移是否已设置为基于 IP 哈希的路由。

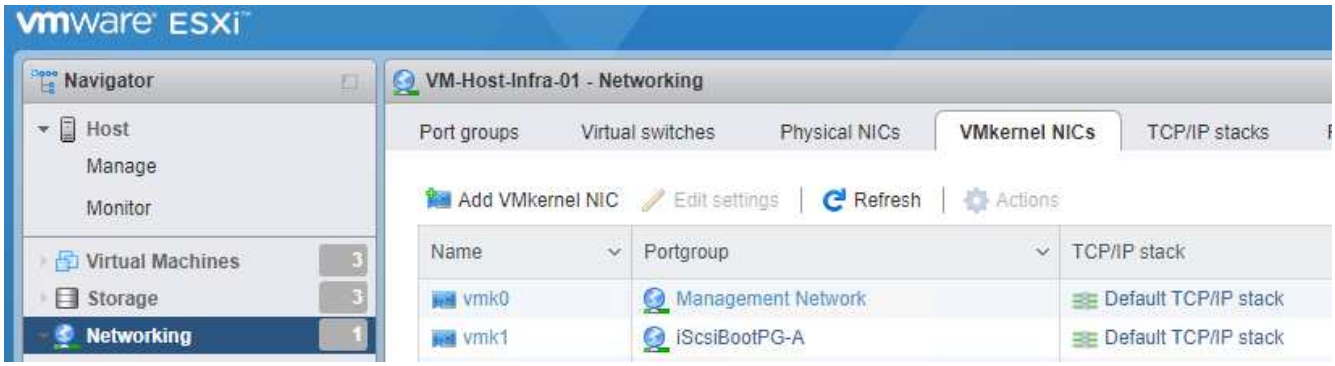
> 负载平衡的 IP 哈希方法要求使用具有静态（模式开启）端口通道的 SRC/DST-IP EtherChannel 正确配置底层物理交换机。由于交换机可能配置不当，您可能会遇到间歇性连接。如果是，请暂时关闭 Cisco 交换机上两个关联上行链路端口之一，以便在对端口通道设置进行故障排除时恢复与 ESXi 管理 vmkernel 端口的通信。

配置端口组和 **VMkernel NIC**

要配置端口组和 VMkernel NIC ，请完成以下步骤：

1. 在左侧导航窗格中，选择网络。
2. 右键单击端口组选项卡。

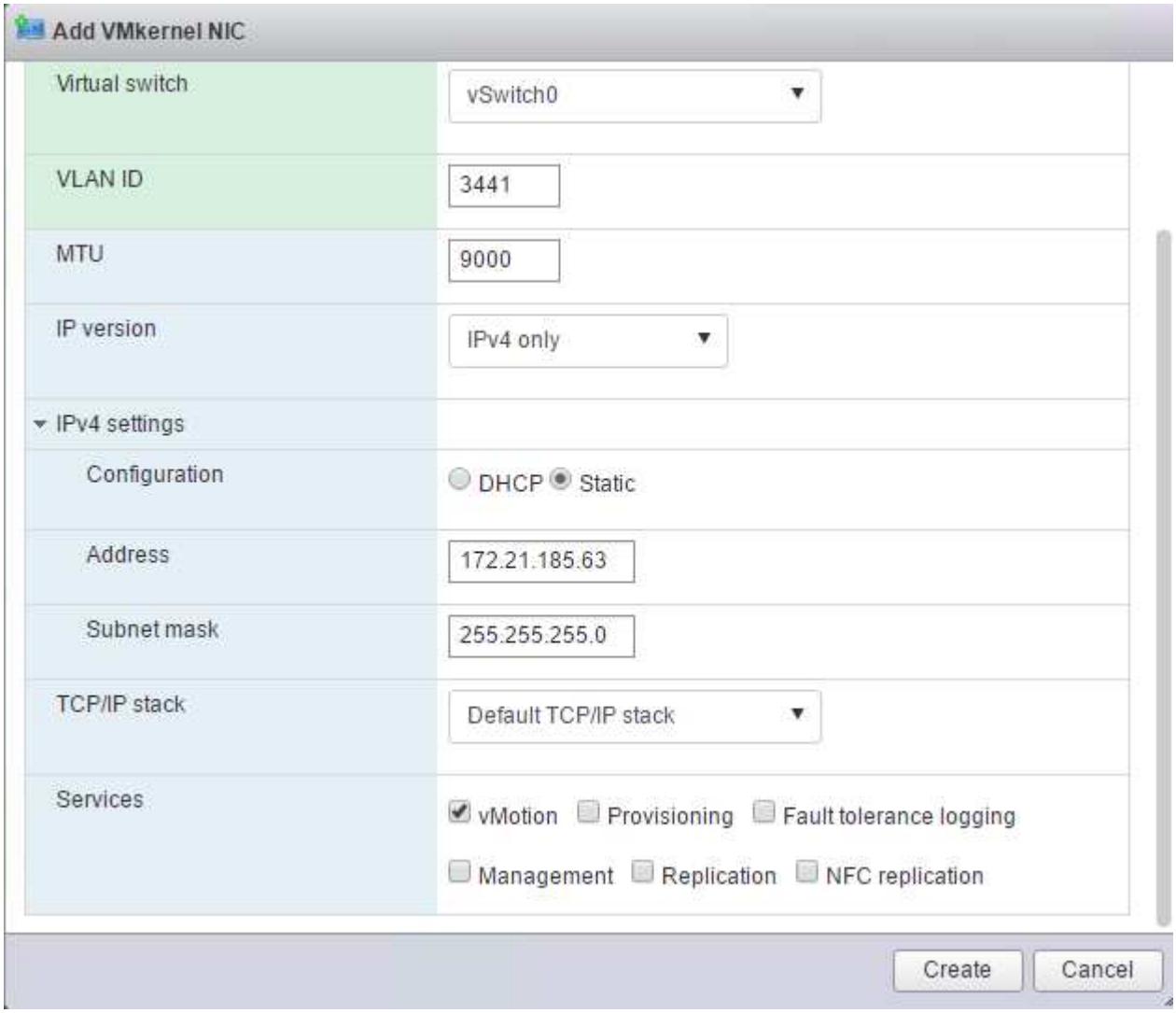
3. 右键单击 VM Network ，然后选择 Edit 。将 VLAN ID 更改为 ` <<var_vm_traffic _vlan>>` 。
4. 单击添加端口组。
   a. 将端口组命名为 MGMT-Network 。
   b. 输入 ` <<mgmt_vlan>>` 作为 VLAN ID 。
   c. 确保已选择 vSwitch0 。
   d. 单击保存。
5. 单击 VMkernel NIC 选项卡。



6. 选择添加 VMkernel NIC 。
   a. 选择 New Port Group 。
   b. 将端口组命名为 nfs-Network 。
   c. 输入 ` <<NFS_VLAN_id>>` 作为 VLAN ID 。
   d. 将 MTU 更改为 9000 。
   e. 展开 IPv4 设置。
   f. 选择静态配置。
   g. 为地址输入 ` <<var_hosta_nfs_ip>>` 。
   h. 为子网掩码输入 ` <<var_hosta_nfs_mask>>` 。
   i. 单击创建。
7. 重复此过程以创建 vMotion VMkernel 端口。
8. 选择添加 VMkernel NIC 。
   a. 选择 New Port Group 。
   b. 将端口组命名为 vMotion 。
   c. 输入 ` <<vmotion_vlan_id>>` 作为 VLAN ID 。
   d. 将 MTU 更改为 9000 。
   e. 展开 IPv4 设置。
   f. 选择静态配置。
   g. 为地址输入 ` <<var_hosta_vmotion_ip>>` 。

h. 输入 ` <<var_hosta_vmotion_mask>>` 作为子网掩码。

i. 确保在 IPv4 设置后选中 vMotion 复选框。

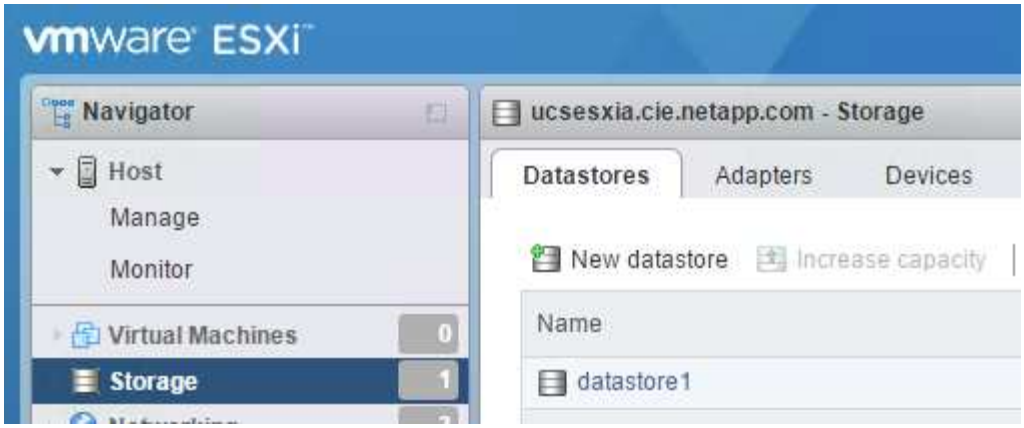


> 可以通过多种方法配置 ESXi 网络，包括在许可允许的情况下使用 VMware vSphere 分布式交换机。如果需要使用其他网络配置来满足业务需求， FlexPod Express 支持这些配置。

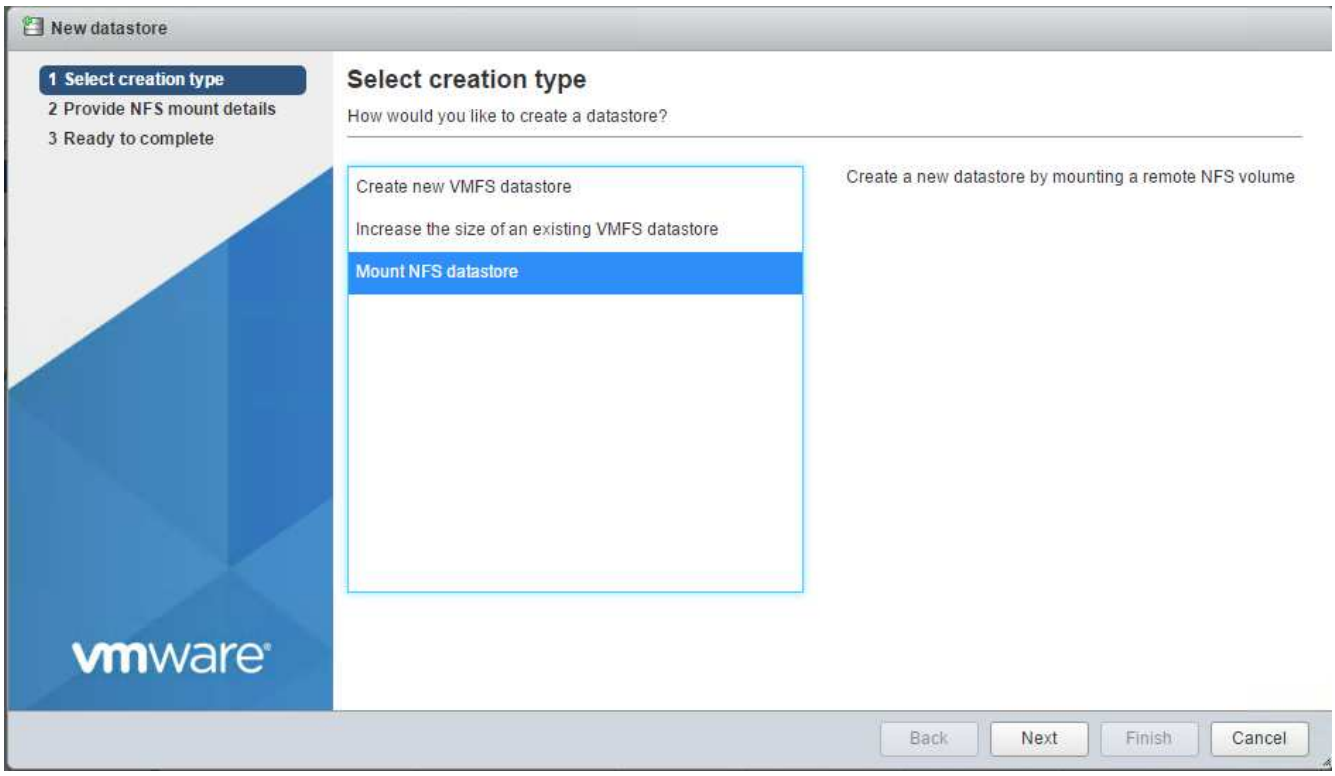
挂载第一个数据存储库

要挂载的第一个数据存储库是 VM 的 `infra_datastore` 数据存储库和 VM 交换文件的 `infra_swap` 数据存储库。

1. 单击左侧导航窗格中的存储，然后单击新建数据存储库。



2. 选择挂载 NFS 数据存储库。



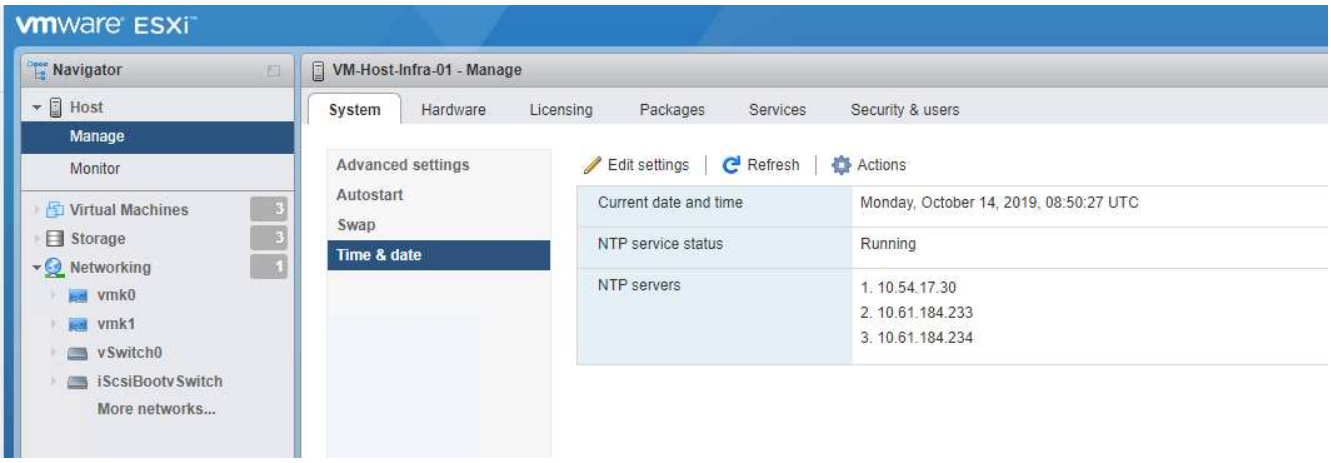
3. 在提供 NFS 挂载详细信息页面中输入以下信息：
   - 名称： `infra_datastore`
   - NFS 服务器： `<<var_noda_nfs_lif>>`
   - 共享： `/infra_datastore`
   - 确保已选择 NFS 3 。
4. 单击完成。您可以在 " 近期任务 " 窗格中看到任务正在完成。
5. 重复此过程以挂载 `infra_swap` 数据存储库：
   - 名称： `infra_swap`
   - NFS 服务器： `<<var_noda_nfs_lif>>`
   - 共享： `/infra_swap`

- 确保已选择 NFS 3 。

配置 **NTP**

要为 ESXi 主机配置 NTP ，请完成以下步骤：

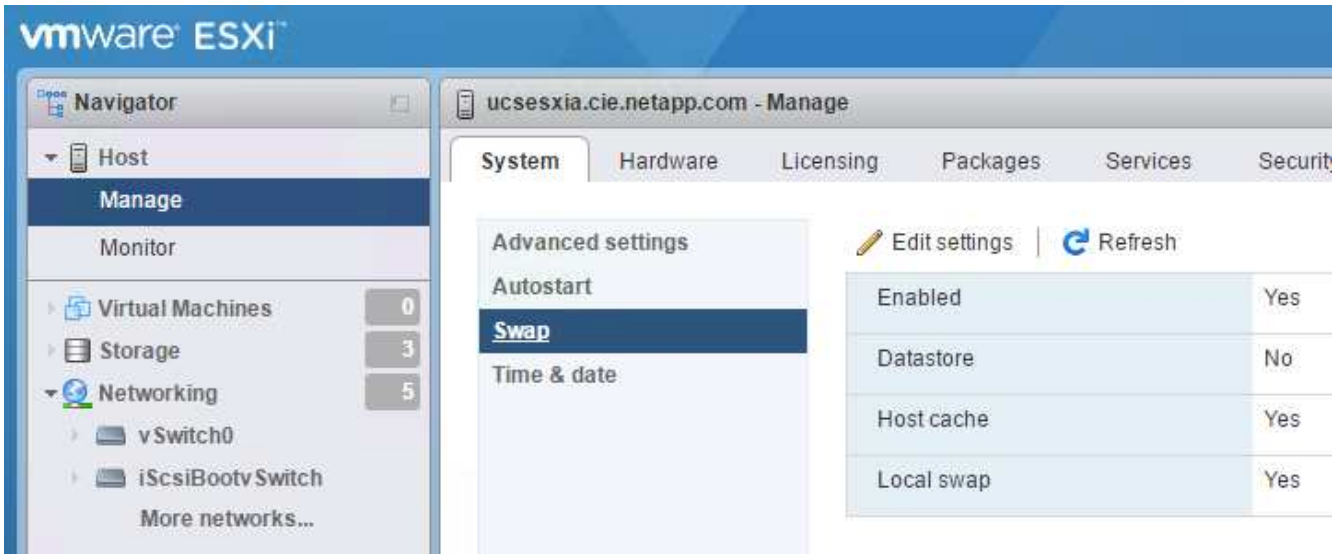
1. 单击左侧导航窗格中的管理。在右窗格中选择 System ，然后单击 Time & Date 。
2. 选择使用网络时间协议（启用 NTP 客户端）。
3. 选择 Start 和 Stop with Host 作为 NTP 服务启动策略。
4. 输入 ` <<var_ntf>>` 作为 NTP 服务器。您可以设置多个 NTP 服务器。
5. 单击保存。



移动 **VM** 交换文件位置

以下步骤提供了有关移动 VM 交换文件位置的详细信息。

1. 单击左侧导航窗格中的管理。在右窗格中选择 system ，然后单击 Swap 。



2. 单击编辑设置。从数据存储库选项中选择 `infra_swap` 。

3. 单击保存。

"下一步：VMware vCenter Server 6.7U2安装操作步骤。"

VMware vCenter Server 6.7U2 安装操作步骤

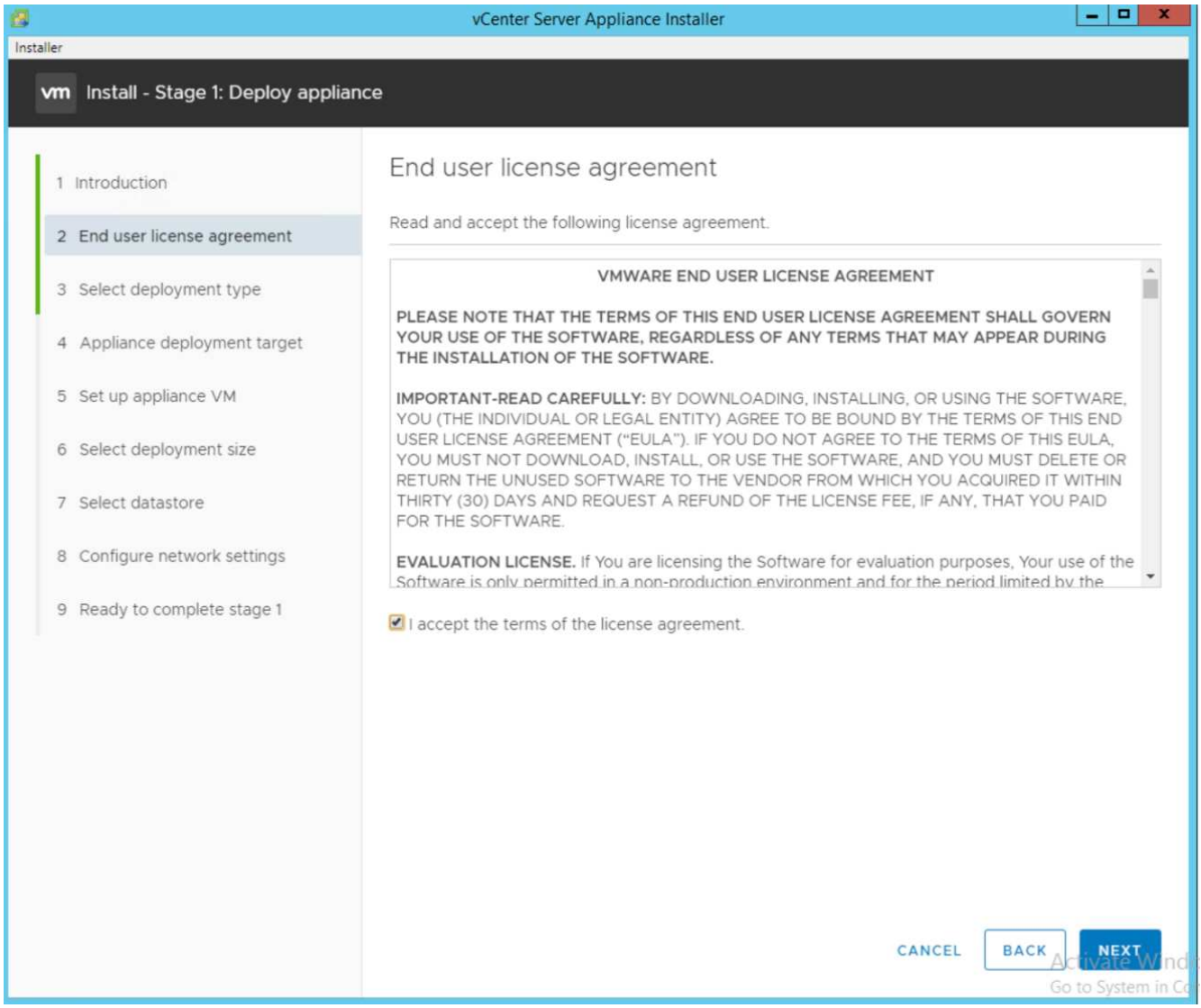
本节详细介绍了在 FlexPod 快速配置中安装 VMware vCenter Server 6.7 的过程。

FlexPod Express 使用 VMware vCenter Server 设备（VCSA）。

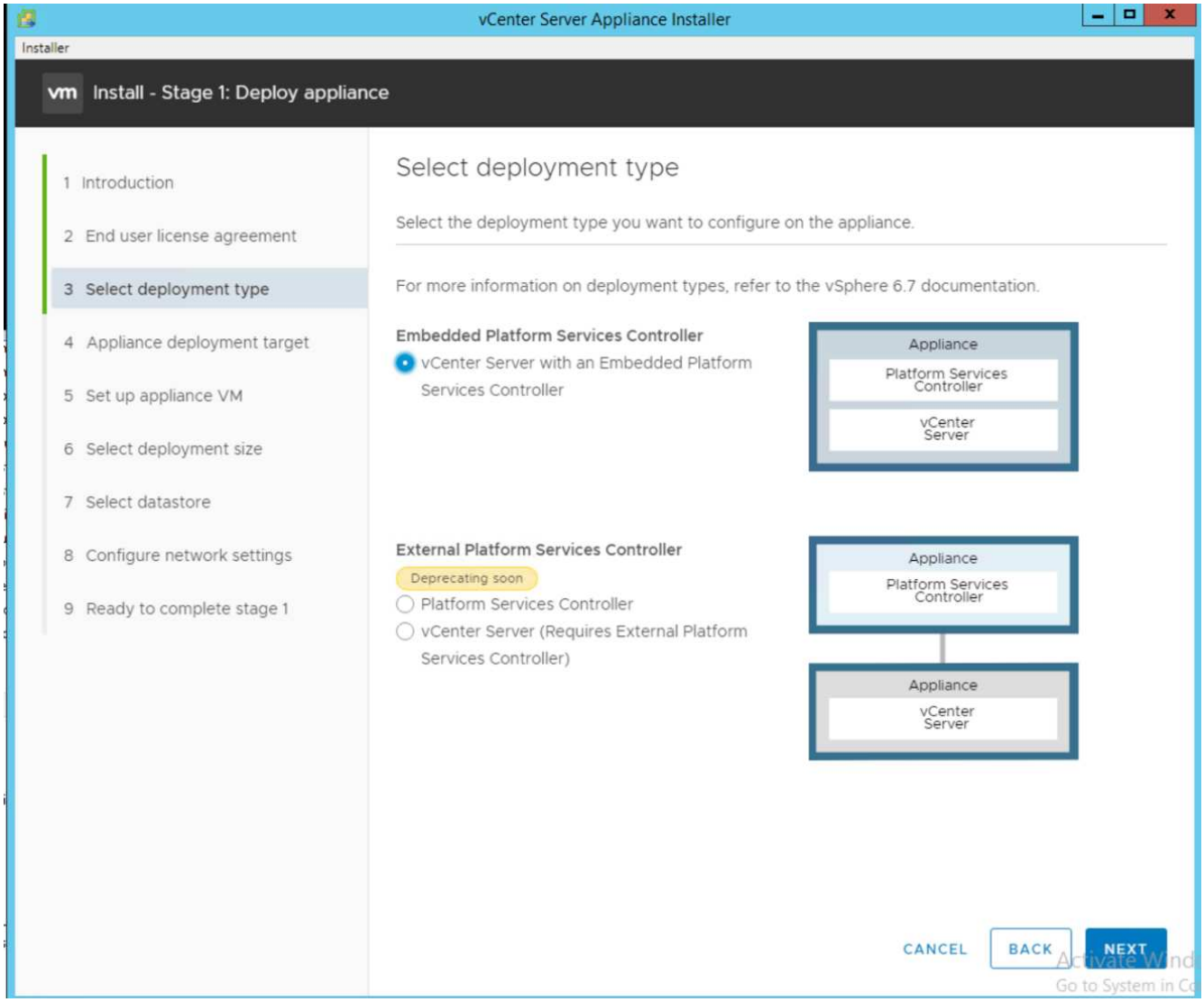
下载 **VMware vCenter Server** 设备

要下载 VMware vCenter Server Appliance （VCSA），请完成以下步骤：

1. 下载 VCSA。在管理 ESXi 主机时，单击获取 vCenter Server 图标以访问下载链接。
2. 从 VMware 站点下载 VCSA。
3. 虽然支持安装 Microsoft Windows vCenter Server，但 VMware 建议在新部署中使用 VCSA。
4. 挂载 ISO 映像。
5. 导航到 vcsa - ui-installer > win32 目录。双击 `installer.exe`。
6. 单击安装。
7. 单击简介页面上的下一步。

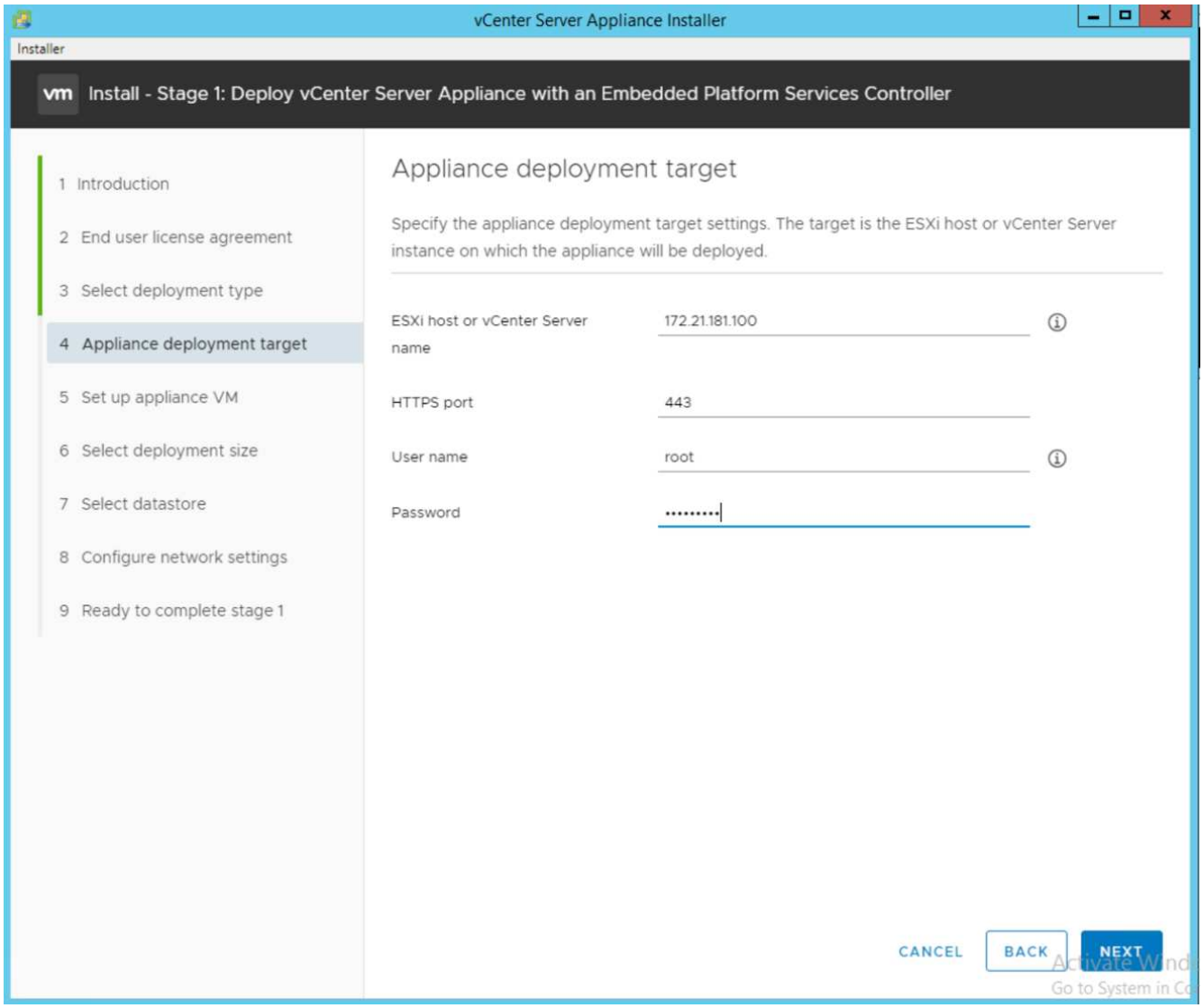


8. 选择 Embedded Platform Services Controller 作为部署类型。

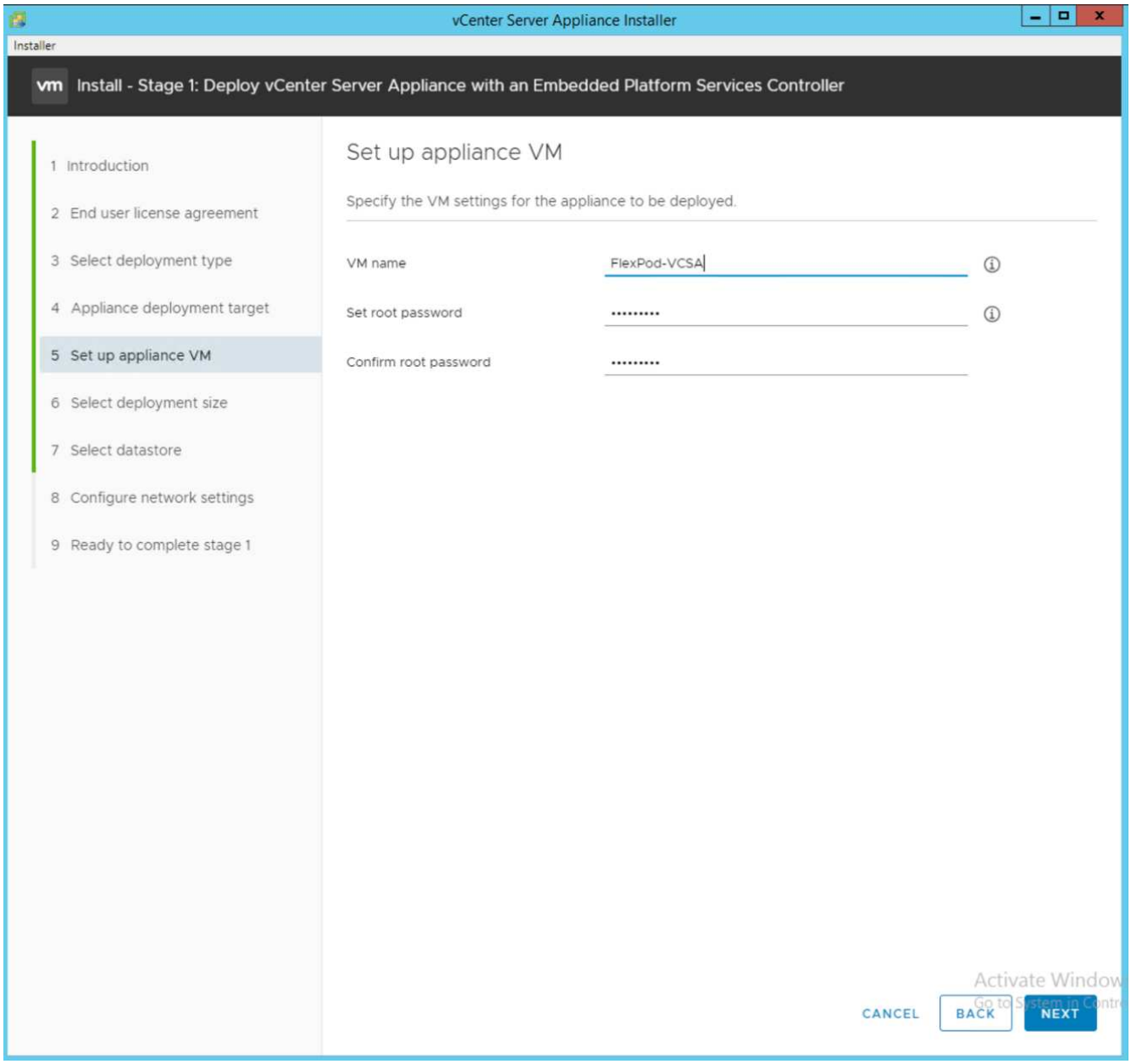


如果需要，还支持在 FlexPod Express 解决方案中部署外部平台服务控制器。

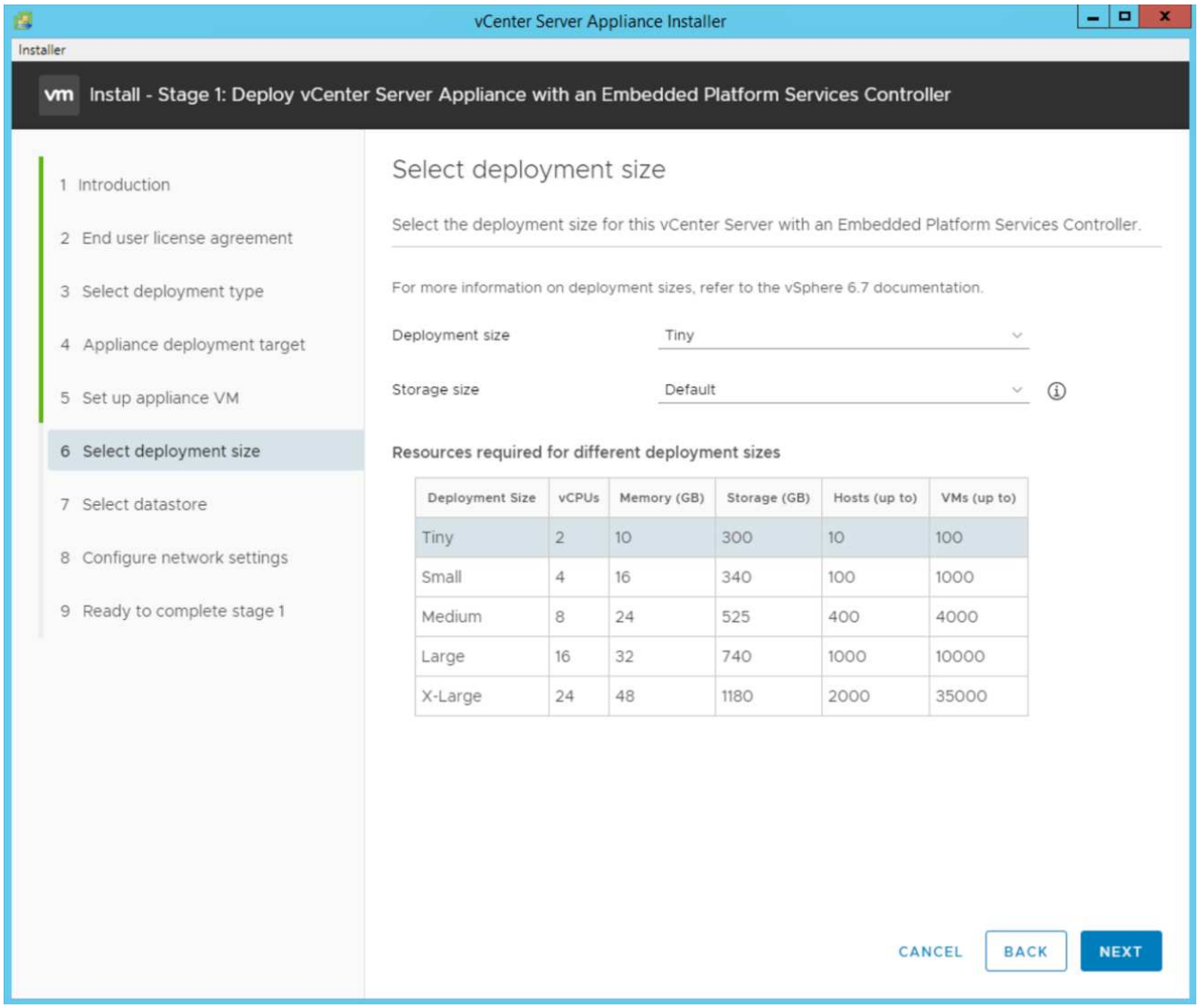
9. 在设备部署目标中，输入已部署的 ESXi 主机的 IP 地址， root 用户名和 root 密码。



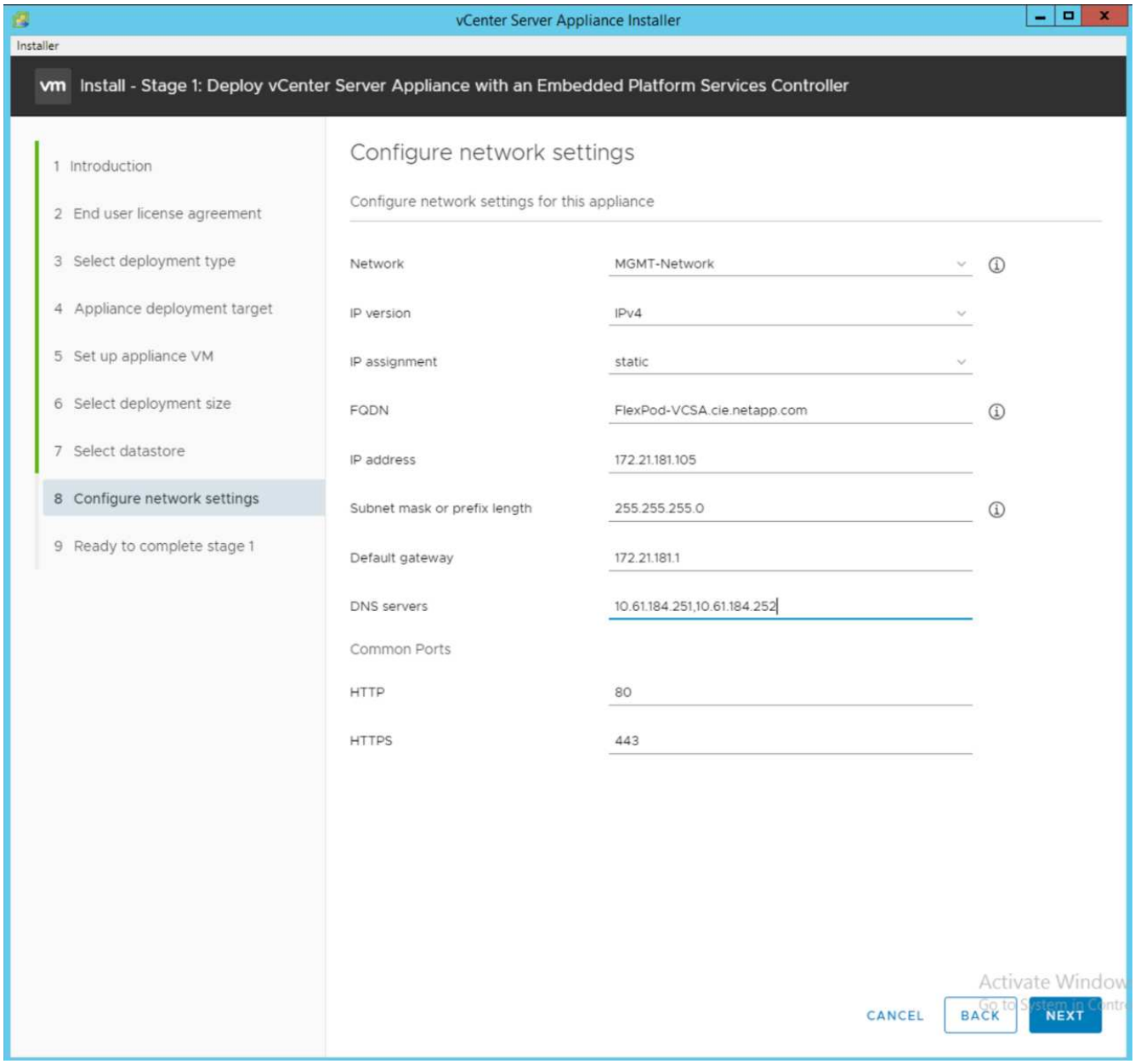
10. 输入 vCSA 作为要用于 VCSA 的虚拟机名称和根密码，以设置设备虚拟机。



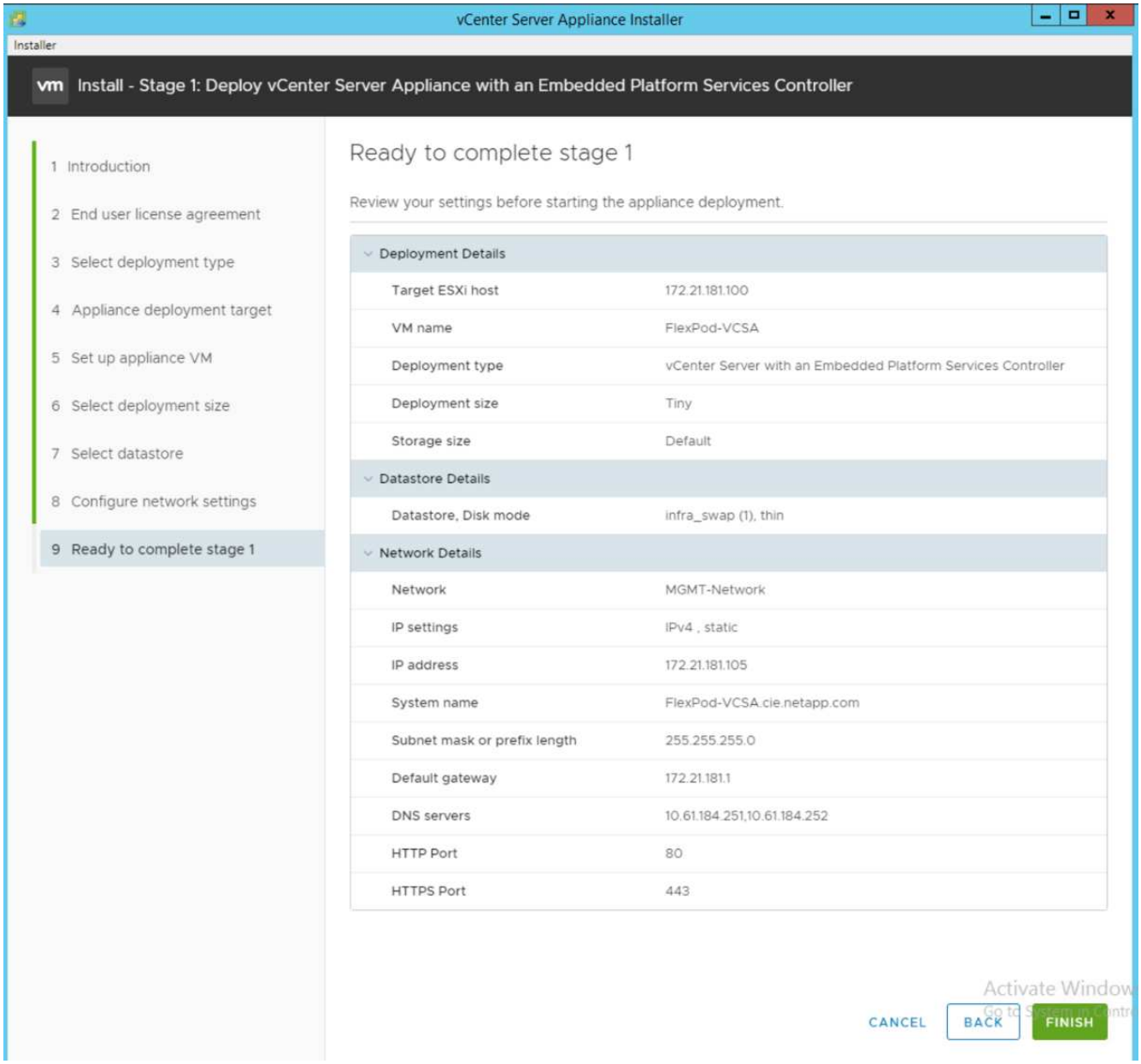
11. 选择最适合您环境的部署规模。单击下一步。



12. 选择 `infra_datastore` 数据存储库。单击下一步。
13. 在 Configure network settings 页面中输入以下信息，然后单击 Next 。
    a. 选择 MGMT-Network for Network 。
    b. 输入要用于 VCSA 的 FQDN 或 IP 。
    c. 输入要使用的 IP 地址。
    d. 输入要使用的子网掩码。
    e. 输入默认网关。
    f. 输入 DNS 服务器。
14. 在准备完成阶段 1 页面上，验证您输入的设置是否正确。单击完成。

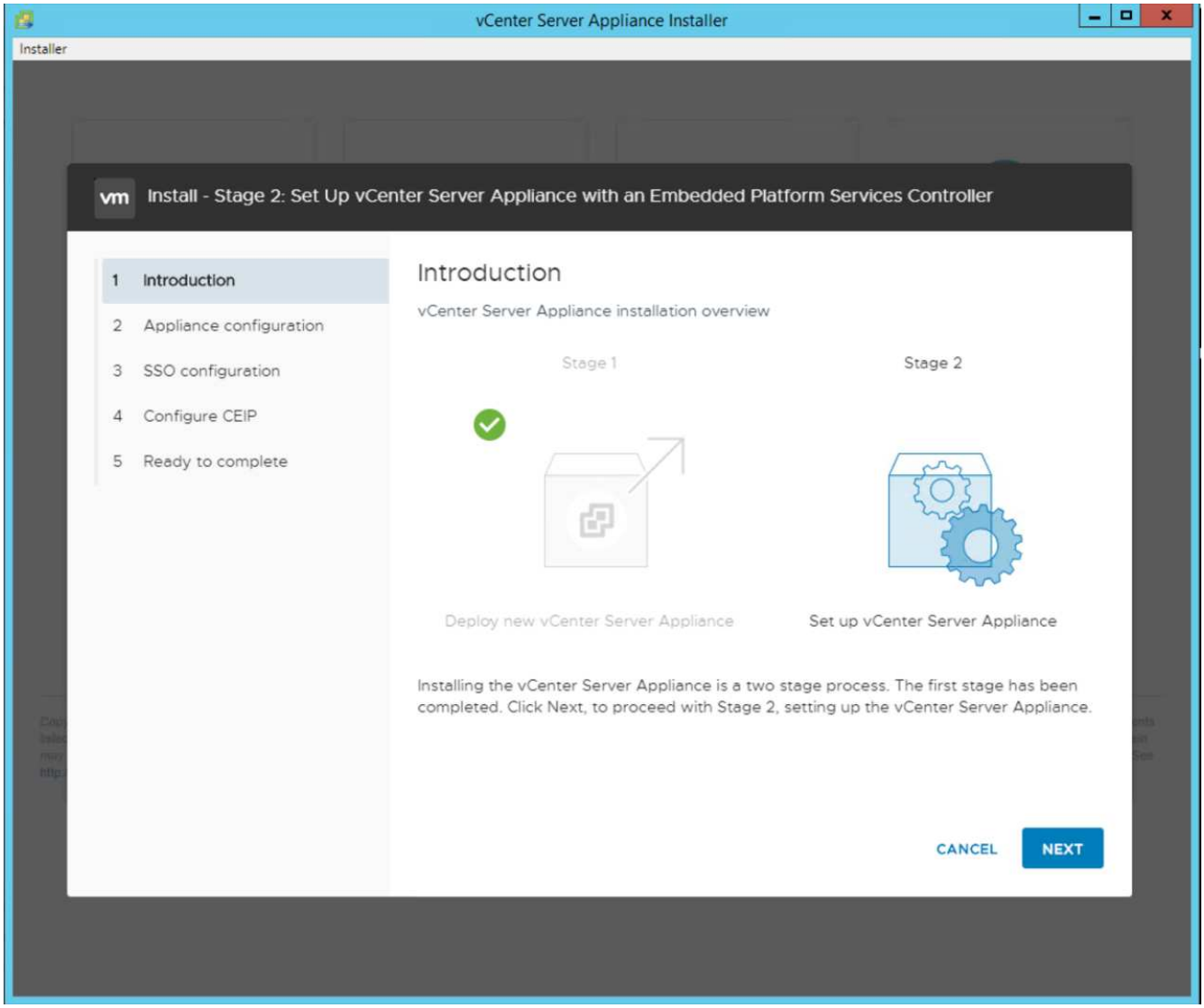


15. 开始部署设备之前，请查看第 1 阶段的设置。

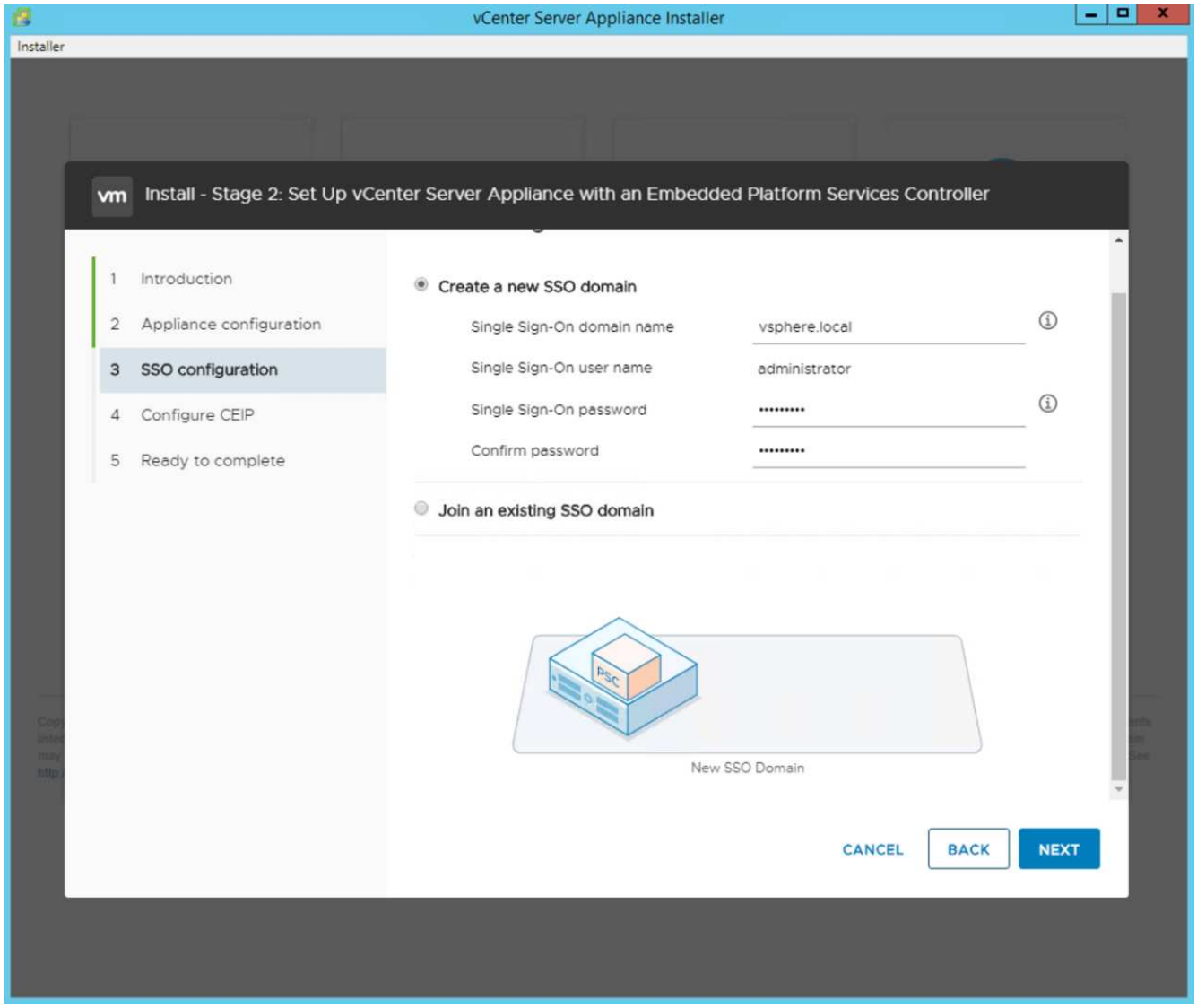


此时将安装 VCSA 。此过程需要几分钟时间。

16. 阶段 1 完成后，将显示一条消息，指出已完成。单击 Continue 以开始第 2 阶段配置。
17. 在第 2 阶段简介页面上，单击下一步。

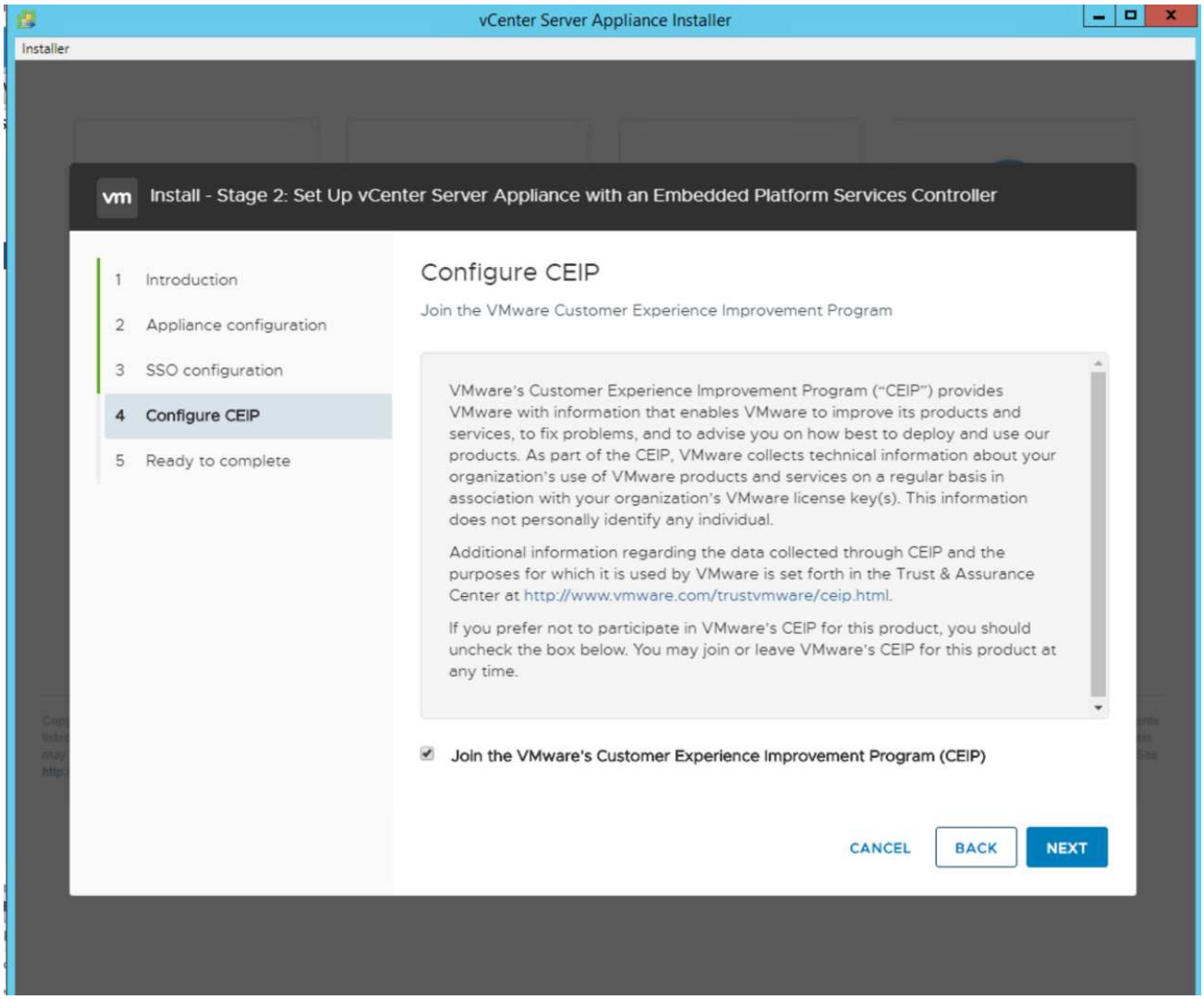


18. 输入 ` <<var_ntp_id>>` 作为 NTP 服务器地址。您可以输入多个 NTP IP 地址。
19. 如果您计划使用 vCenter Server 高可用性（HA），请确保已启用 SSH 访问。
20. 配置 SSO 域名，密码和站点名称。单击下一步。

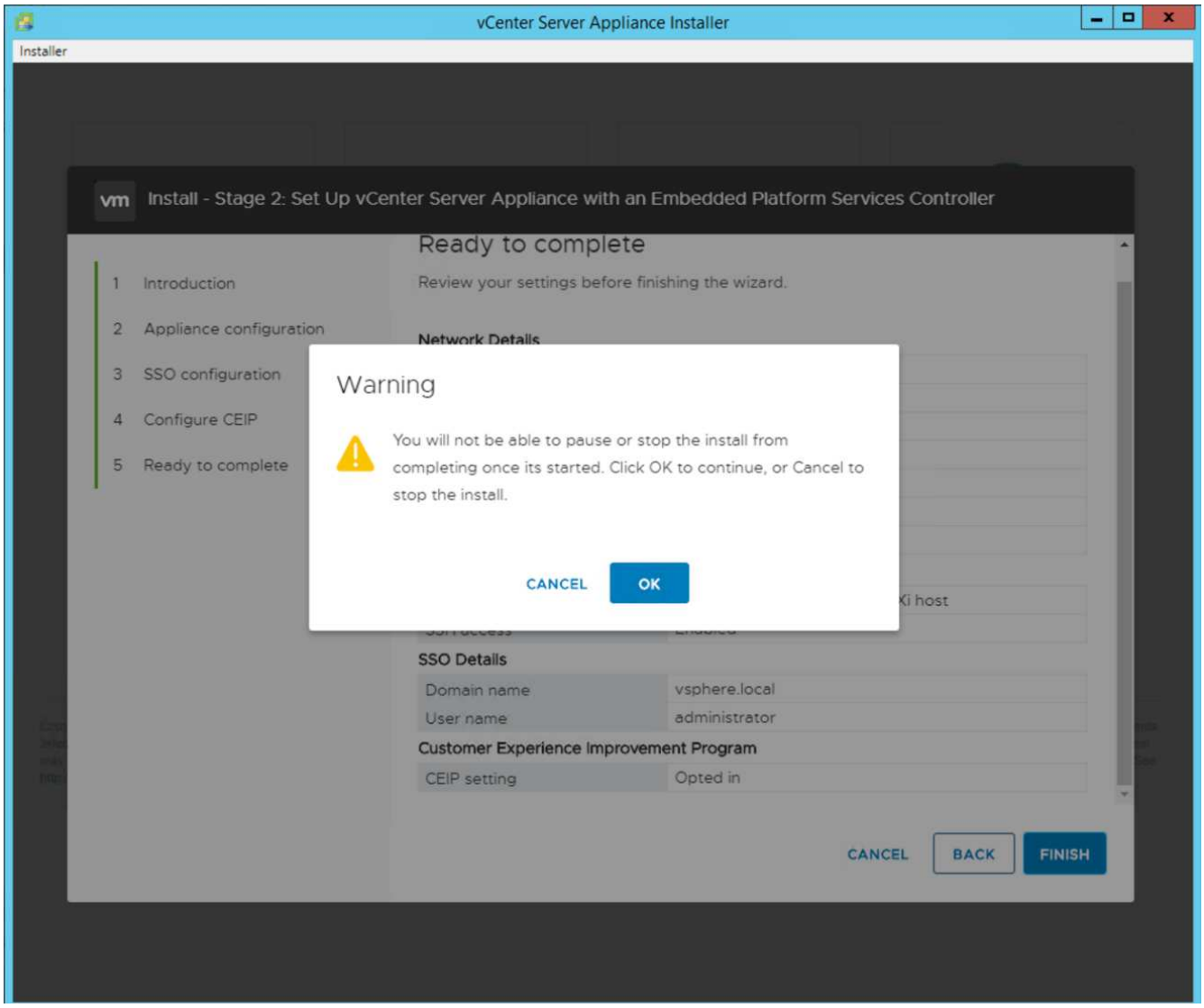


请记下这些值以供参考，特别是当您与 `vsphere.local` 域名有所偏差时。

21. 如果需要，请加入 VMware 客户体验计划。单击下一步。



22. 查看设置摘要。单击完成或使用返回按钮编辑设置。
23. 此时将显示一条消息，指出在安装开始后，您将无法暂停或停止安装完成。单击确定继续。



设备设置将继续。这需要几分钟时间。

此时将显示一条消息，指示设置已成功。

24. 安装程序提供的用于访问 vCenter Server 的链接可单击。

"下一步：VMware vCenter Server 6.7U2和vSphere集群配置。"

VMware vCenter Server 6.7U2 和 vSphere 集群配置

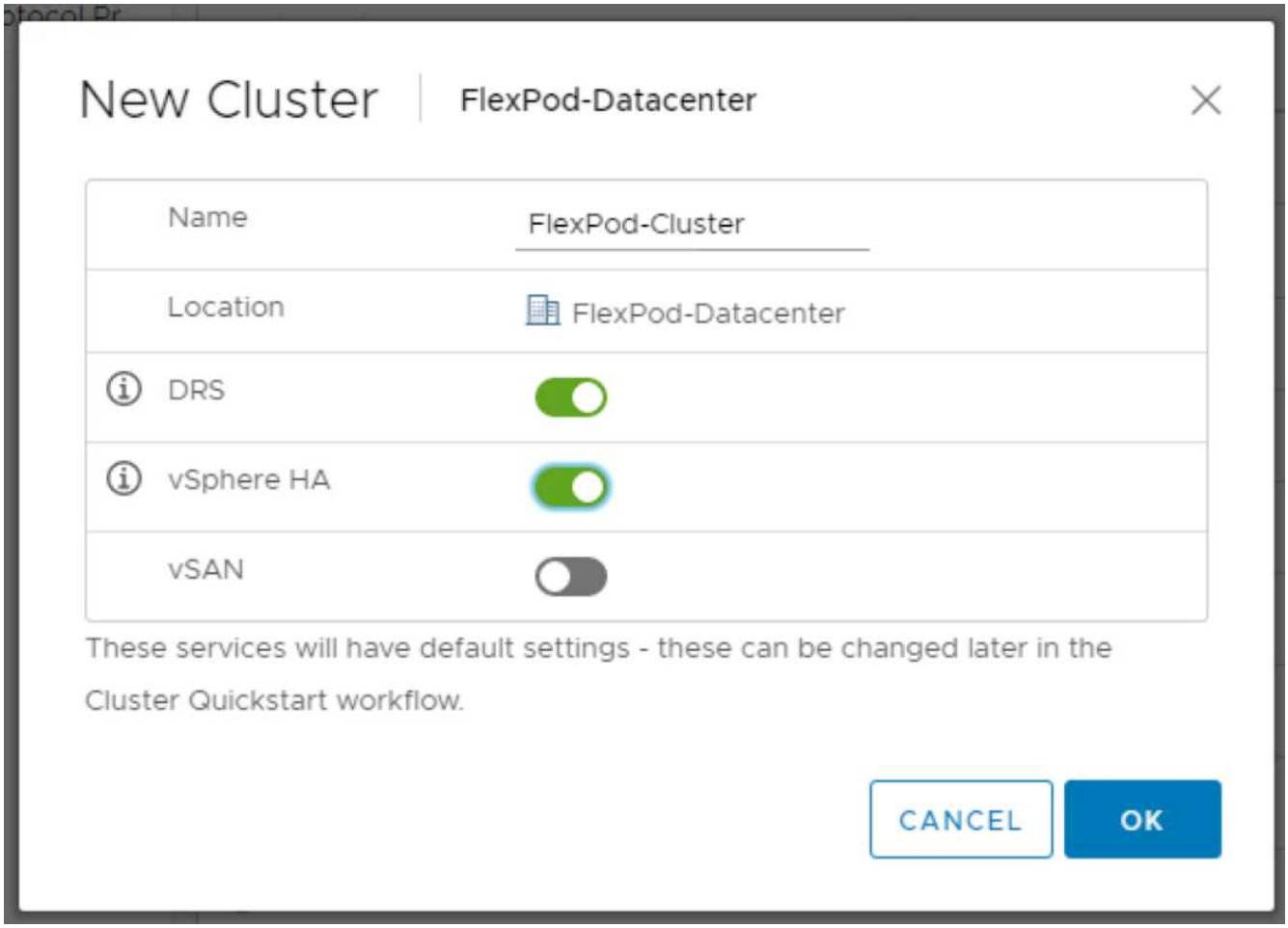
要配置 VMware vCenter Server 6.7 和 vSphere 集群，请完成以下步骤：

1. 导航到 ` https://\<<FQDN 或 vCenter 的 IP >/vsphere-client/` 。
2. 单击 Launch vSphere Client 。
3. 使用用户名 mailto： administrator@vspehre.local[管理员^]@vsphere.local 以及您在 VCSA 设置过程中输入的 SSO 密码登录。
4. 右键单击 vCenter 名称并选择新建数据中心。
5. 输入数据中心的名称，然后单击确定。

创建 **vSphere** 集群

要创建 vSphere 集群，请完成以下步骤：

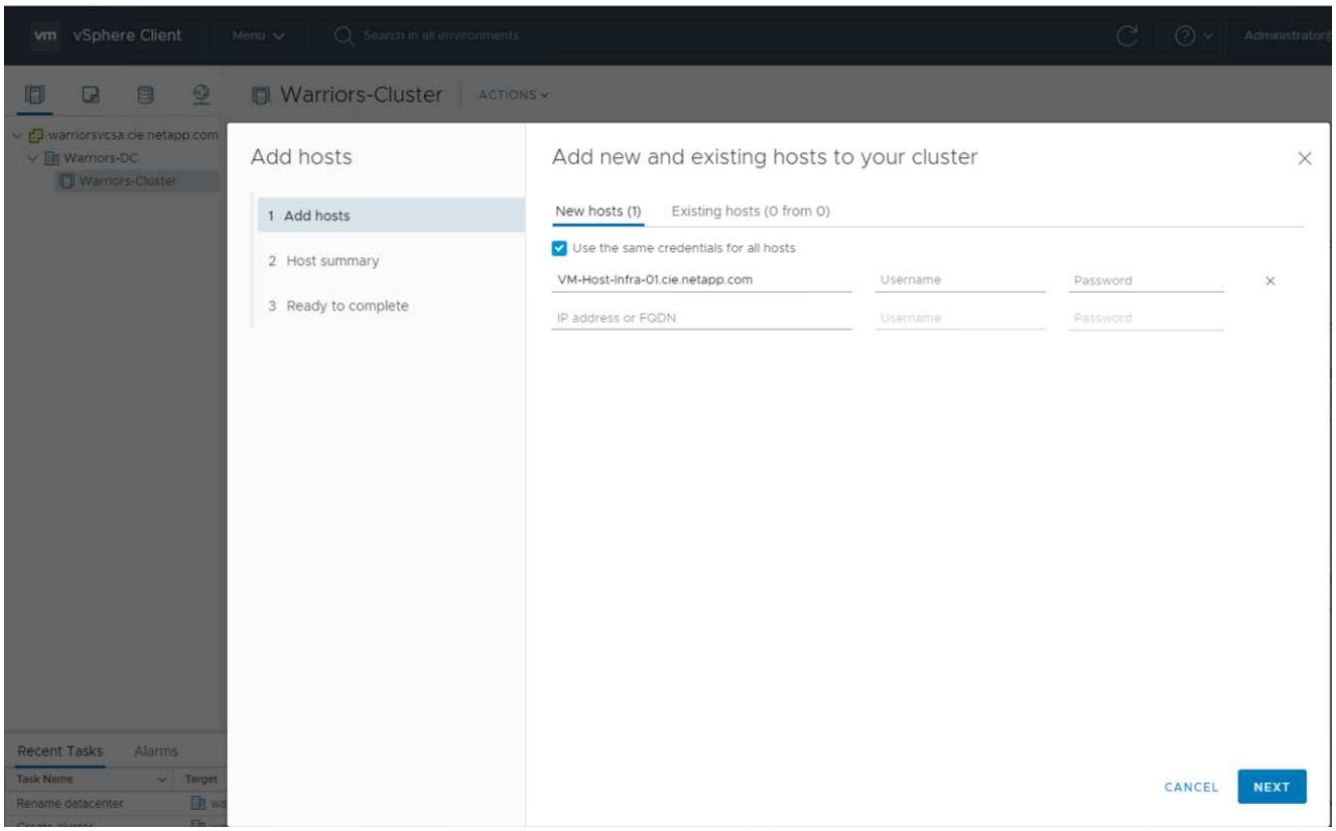
1. 右键单击新创建的数据中心，然后选择 New Cluster 。
2. 输入集群的名称。
3. 选中复选框以启用灾难恢复和 vSphere HA 。
4. 单击确定。



将 **ESXi** 主机添加到集群中

要将 ESXi 主机添加到集群，请完成以下步骤：

1. 右键单击集群并选择添加主机。



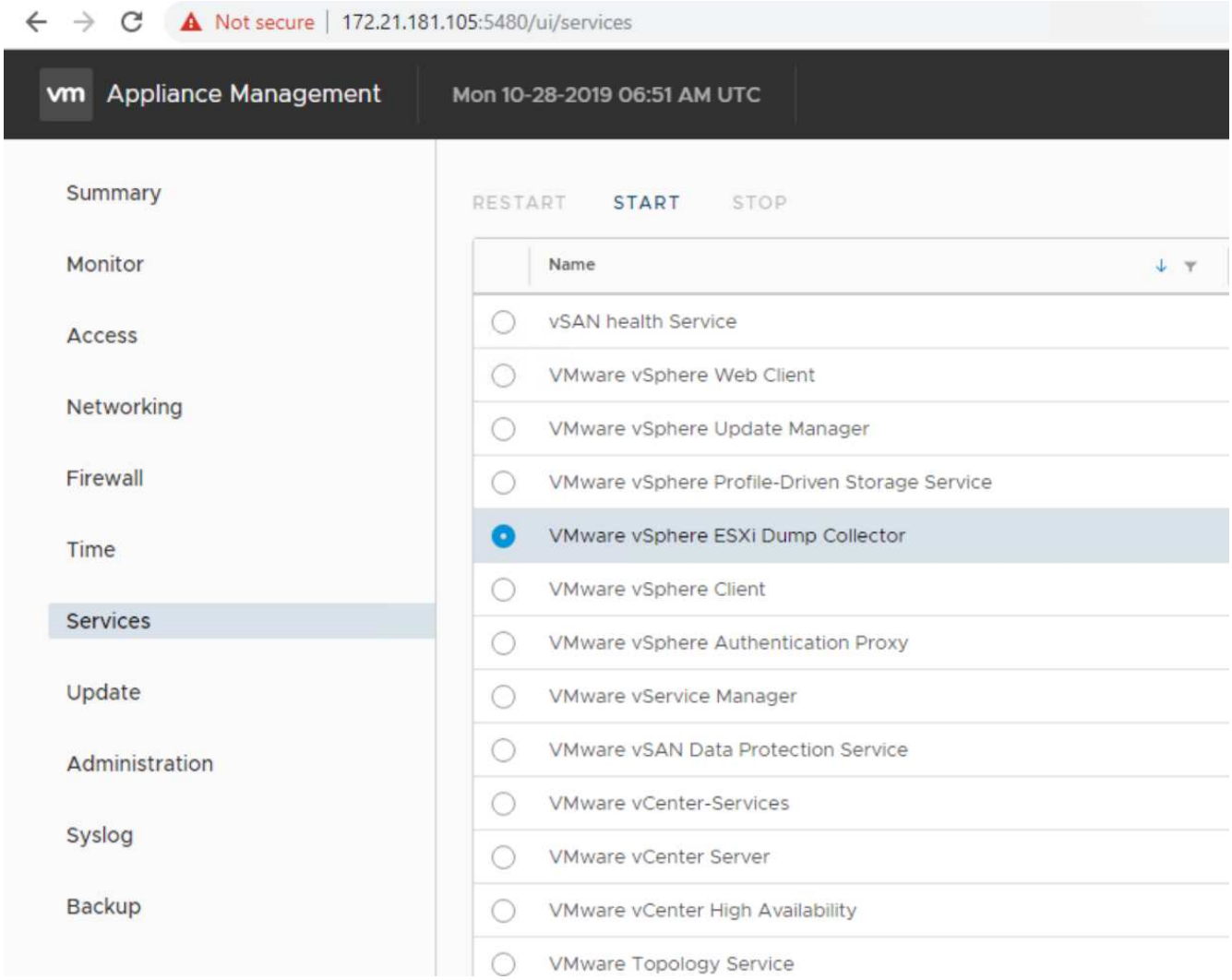
2. 要将 ESXi 主机添加到集群，请完成以下步骤：
   a. 输入主机的 IP 或 FQDN 。单击下一步。
   b. 输入 root 用户名和密码。单击下一步。
   c. 单击是将主机的证书替换为由 VMware 证书服务器签名的证书。
   d. 单击主机摘要页面上的下一步。
   e. 单击绿色 + 图标向 vSphere 主机添加许可证。
3. 如果需要，可以稍后完成此步骤。
   a. 单击下一步以使锁定模式保持禁用状态。
   b. 单击 VM 位置页面上的下一步。
   c. 查看即将完成页面。使用 " 返回 " 按钮进行任何更改或选择 " 完成 " 。
4. 对 Cisco UCS 主机 B 重复步骤 1 和 2

> 对于添加到 FlexPod 快速配置中的任何其他主机，必须完成此过程。

在 **ESXi** 主机上配置核心转储

要在 ESXi 主机上配置核心转储，请完成以下步骤：

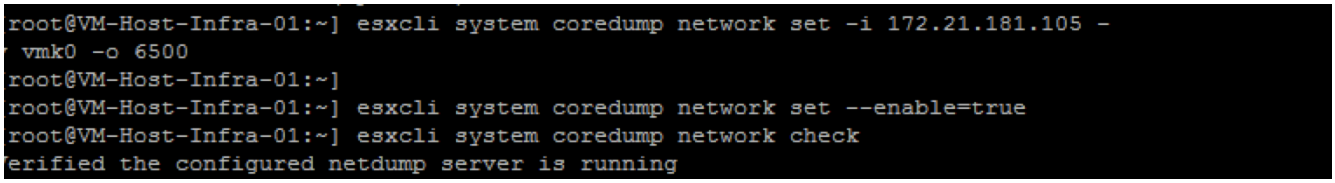
1. 登录到 https： // "vCenter" ip： 5480/ ，输入 root 作为用户名，然后输入 root 密码。
2. 单击服务并选择 VMware vSphere ESXi 转储收集器。
3. 启动 VMware vSphere ESXi 转储收集器服务。



4. 使用 SSH 连接到管理 IP ESXi 主机，输入 root 作为用户名，然后输入 root 密码。
5. 运行以下命令：

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

6. 输入最后一个命令后，将显示消息 `Verified the configured netdump server is running`。



对于添加到 FlexPod Express 中的任何其他主机，必须完成此过程。

此验证中的 `IP_address_of_core_dump_collector` 是 vCenter IP 。

"下一步：NetApp Virtual Storage Console 9.6部署过程。"

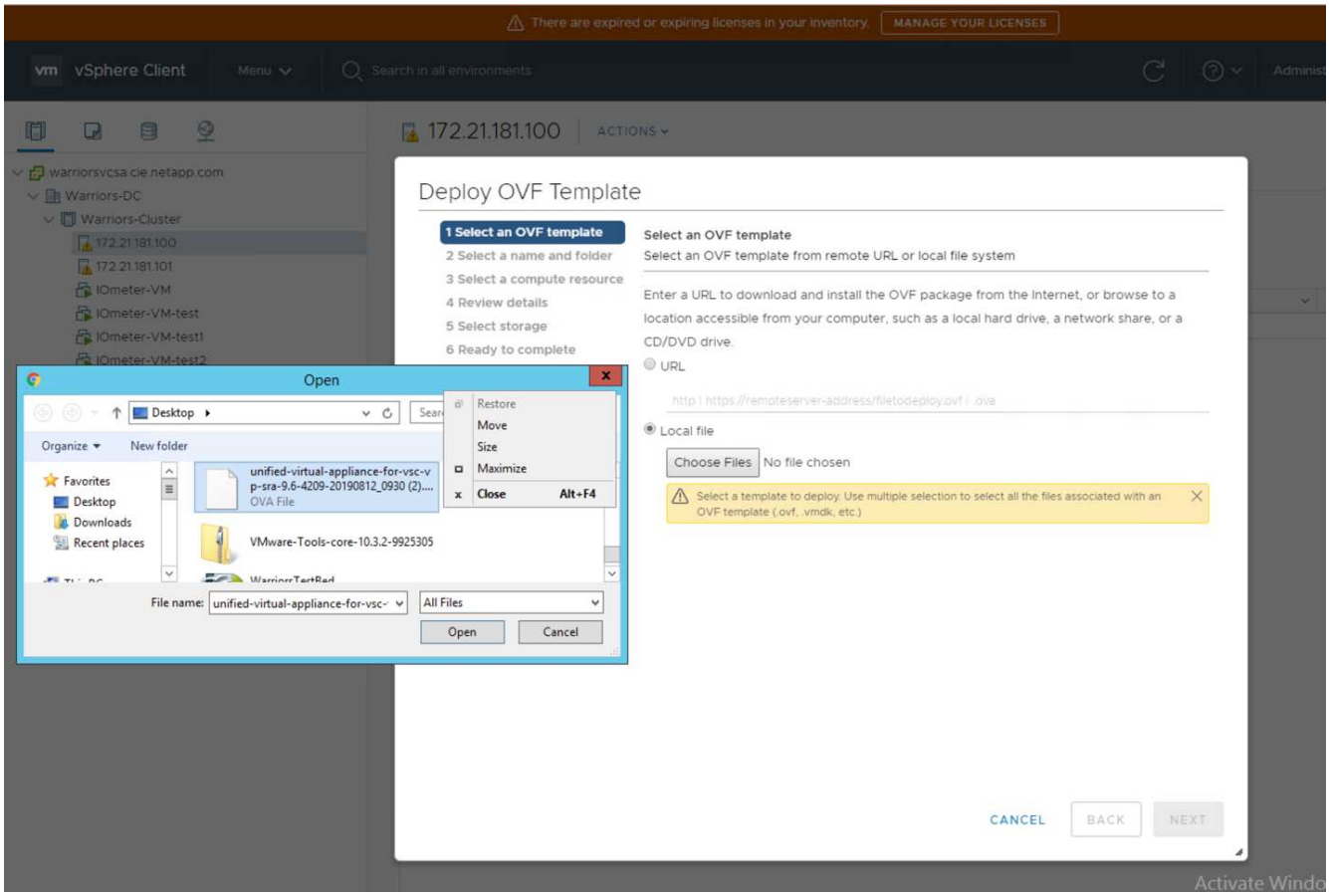
NetApp Virtual Storage Console 9.6 部署过程

本节介绍 NetApp 虚拟存储控制台（ VSC ）的部署过程。

安装 Virtual Storage Console 9.6

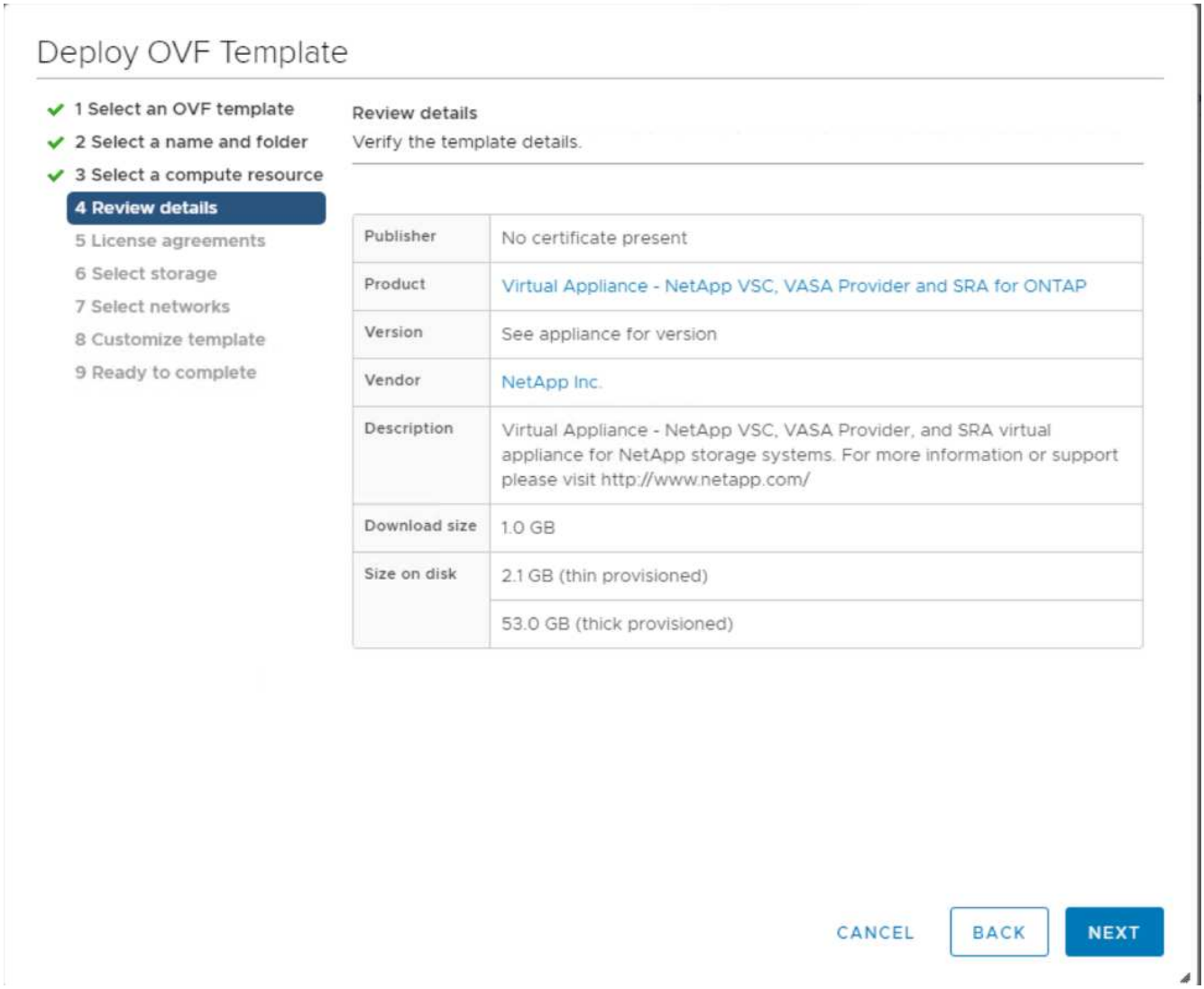
要使用开放式虚拟化格式（ OVF ）部署安装 VSC 9.6 软件，请执行以下步骤：

1. 转至 vSphere Web Client > 主机集群 > 部署 OVF 模板。
2. 浏览到从 NetApp 支持站点下载的 VSC OVF 文件。

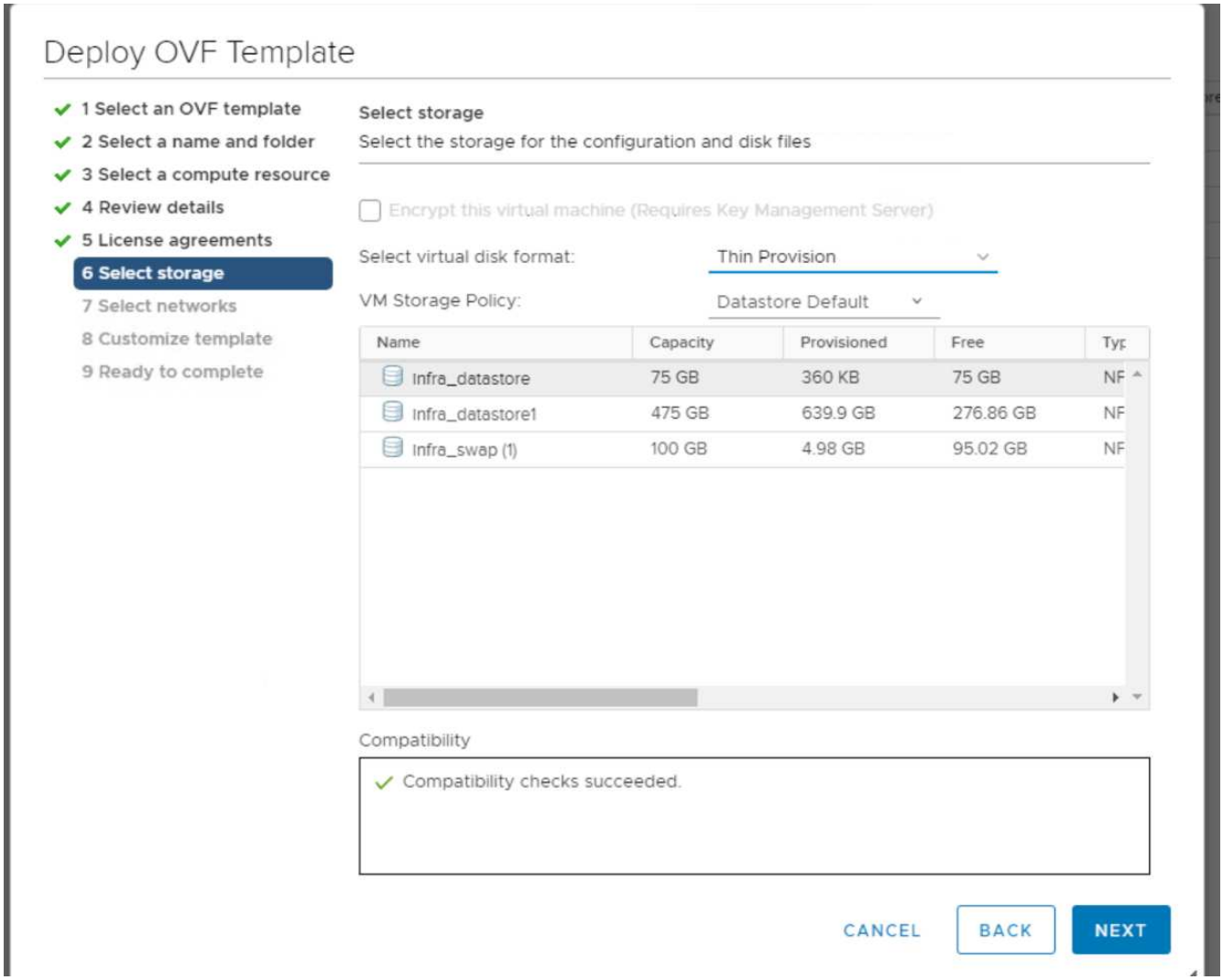


3. 输入 VM 名称并选择要部署的数据中心或文件夹。单击下一步。

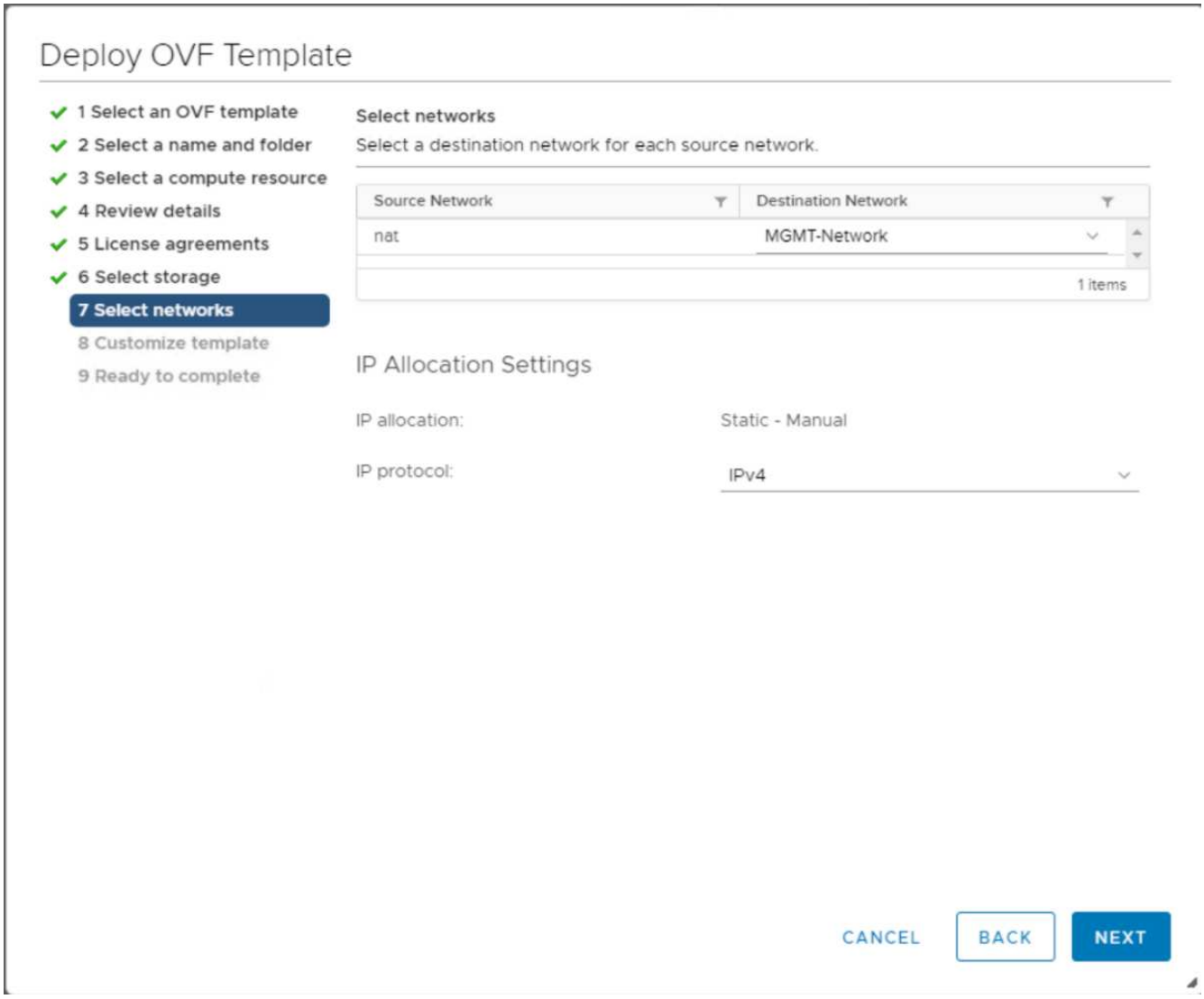
4. 选择 FlexPod-Cluster ESXi 集群，然后单击下一步。
5. 查看详细信息，然后单击下一步。



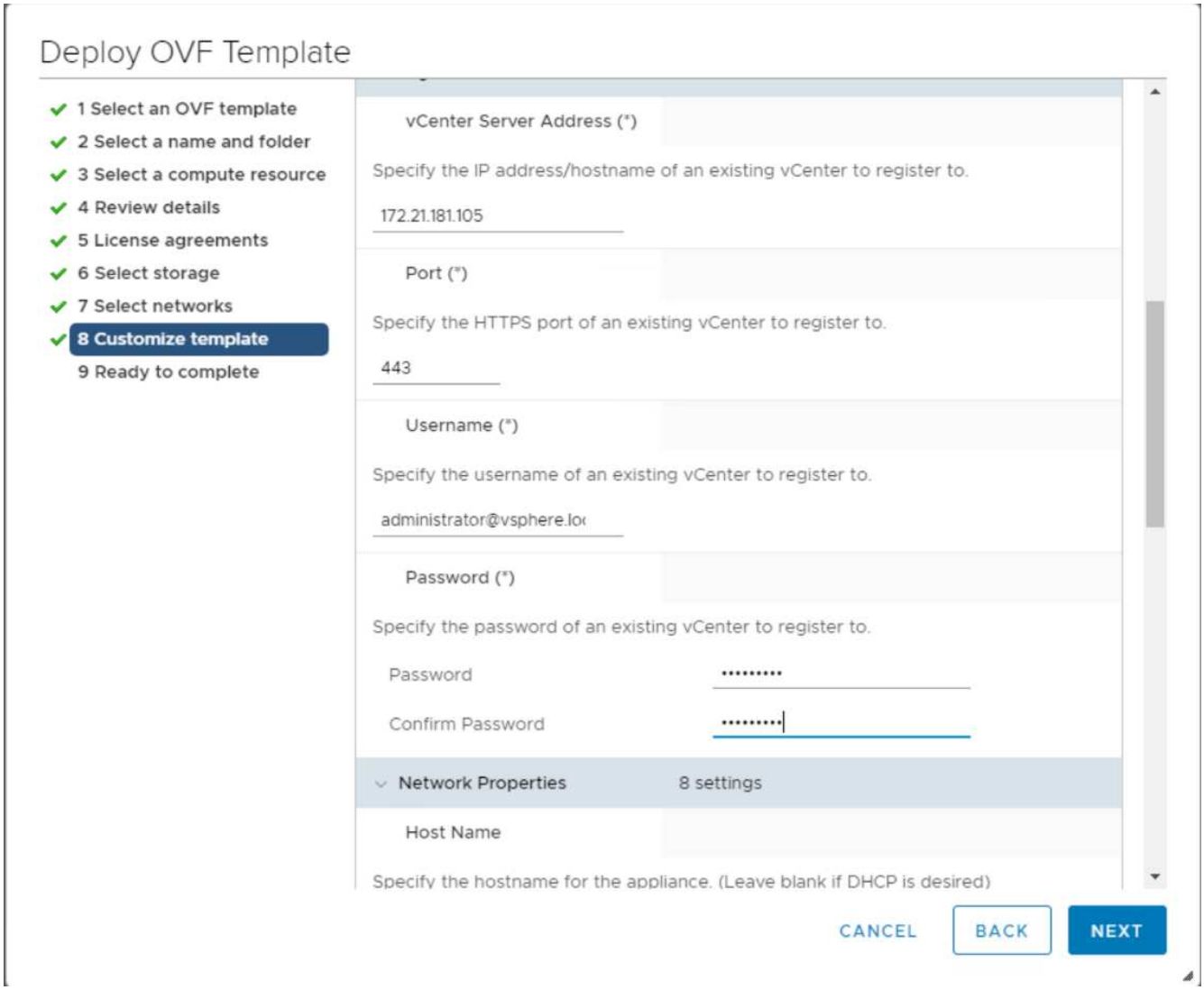
6. 单击 Accept 以接受许可证，然后单击 Next 。
7. 选择精简配置虚拟磁盘格式和一个 NFS 数据存储库。单击下一步。



8. 在 Select Networks 中，选择一个目标网络，然后单击 Next 。



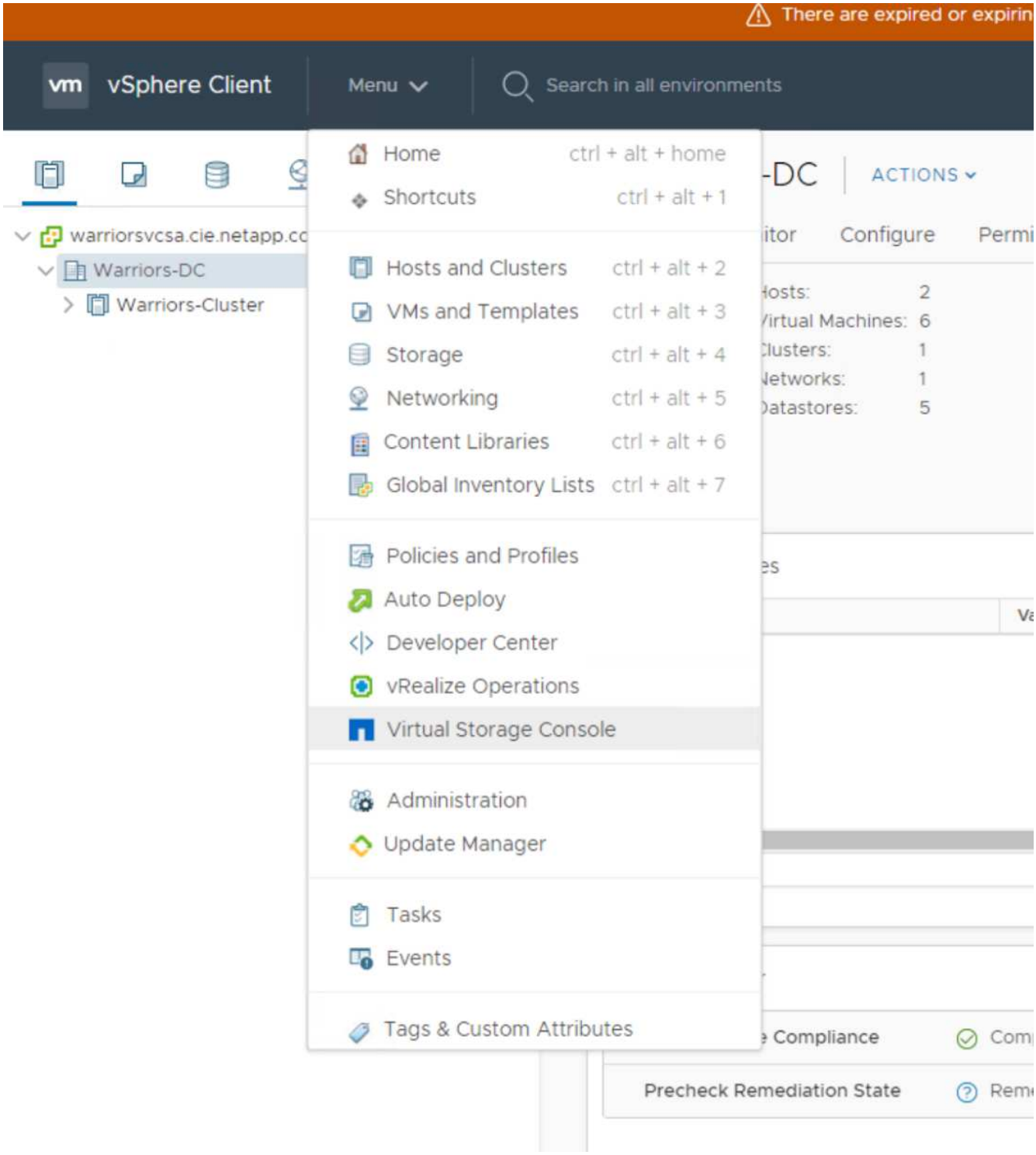
9. 在自定义模板中，输入 VSC 管理员密码， vCenter 名称或 IP 地址以及其他配置详细信息，然后单击下一步。



10. 查看输入的配置详细信息，然后单击完成以完成 NetApp-VSC VM 的部署。
11. 启动 NetApp-VSC VM 并打开 VM 控制台。
12. 在 NetApp-VSC VM 启动过程中，您会看到安装 VMware Tools 的提示。在 vCenter 中，选择 NetApp-VSC VM > 子操作系统 > 安装 VMware Tools 。

```
Booting VSC, VASA Provider, and SRA virtual appliance...Please wait...
VMware Tools OVF vCenter configuration not found.
VMware Tools OVF vCenter configuration not found.
VMware Tools OVF vCenter configuration not found.

VMware Tools installation


Before you can continue the VSC, VASA Provider, and SRA virtual appliance
installation, you must install the VMware Tools:

  1.  Select VM > Guest OS > Install VMware Tools.

                    OR

      Click on "Install VMware Tools" pop-up box on the vSphere Web Client.

  2.  Follow the prompts provided by the VMware Tools wizard.

Once you click on mount, the installation process will automatically continue.
```

13. 在 OVF 模板自定义期间提供了网络配置和 vCenter 注册信息。因此，在运行 NetApp-VSC 虚拟机后， VSC ， vSphere API for Storage Awareness （ VASA ）和 VMware Storage Replication Adapter （ SRA ）将注册到 vCenter 中。
14. 从 vCenter Client 中注销并重新登录。从主页菜单中，确认已安装 NetApp VSC 。



下载并安装 **NetApp NFS VAAI** 插件

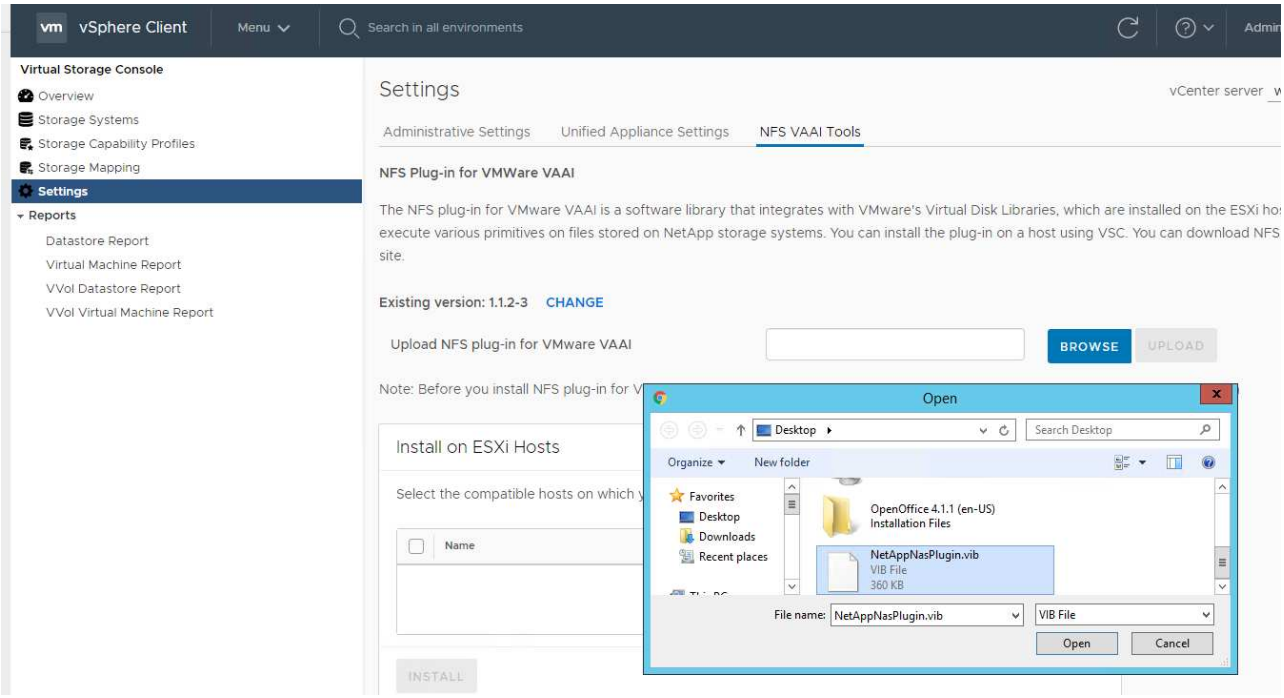
要下载并安装 NetApp NFS VAAI 插件，请完成以下步骤：

1. 下载适用于 VMware 的 NetApp NFS 插件 1.1.2 ` 。从 NFS 插件下载页面下载 VIB` 文件，并将其保存到本地计算机或管理主机。
2. 下载适用于 VMware VAAI 的 NetApp NFS 插件：
   a. 转至 "软件下载页面"。

b. 向下滚动并单击适用于 VMware VAAI 的 NetApp NFS 插件。

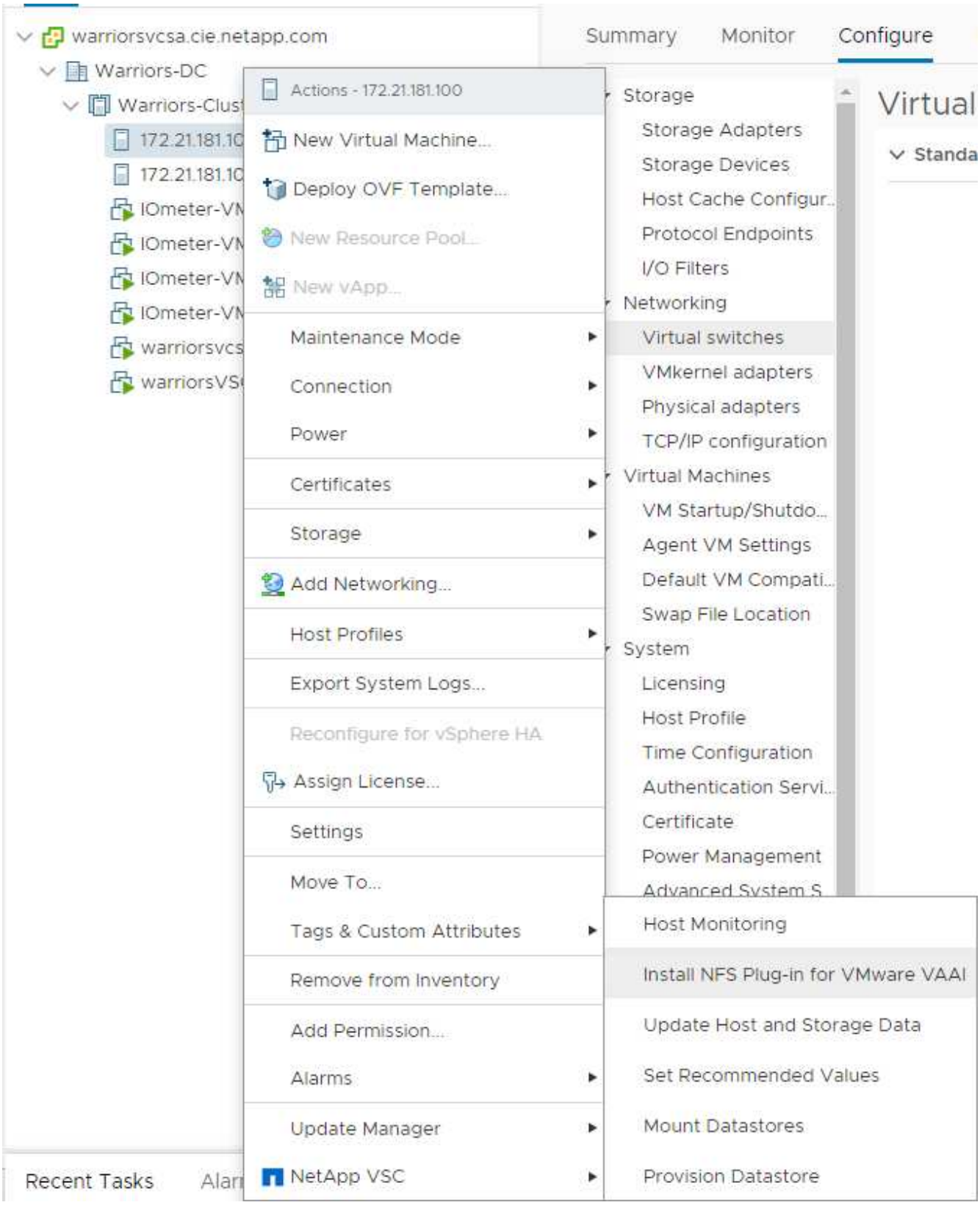
c. 从 vSphere Web Client 的主页屏幕中，选择 Virtual Storage Console 。

d. 在 Virtual Storage Console > 设置 > NFS VAAI 工具下，选择选择选择文件并浏览到下载插件的存储位置，以上传 NFS 插件。



3. 单击上传将此插件传输到 vCenter 。

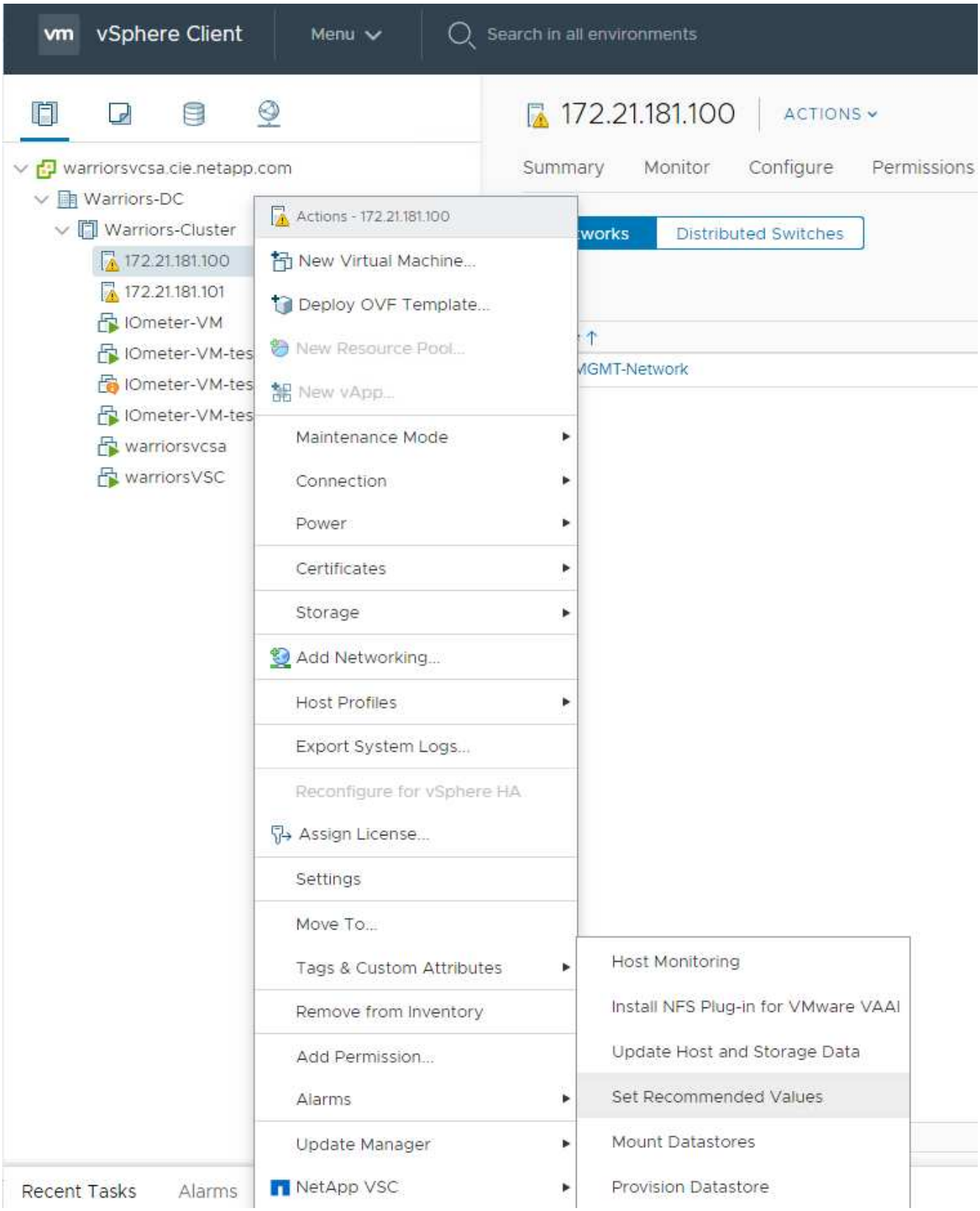
4. 选择主机，然后选择 NetApp VSC > 安装适用于 VMware VAAI 的 NFS 插件。



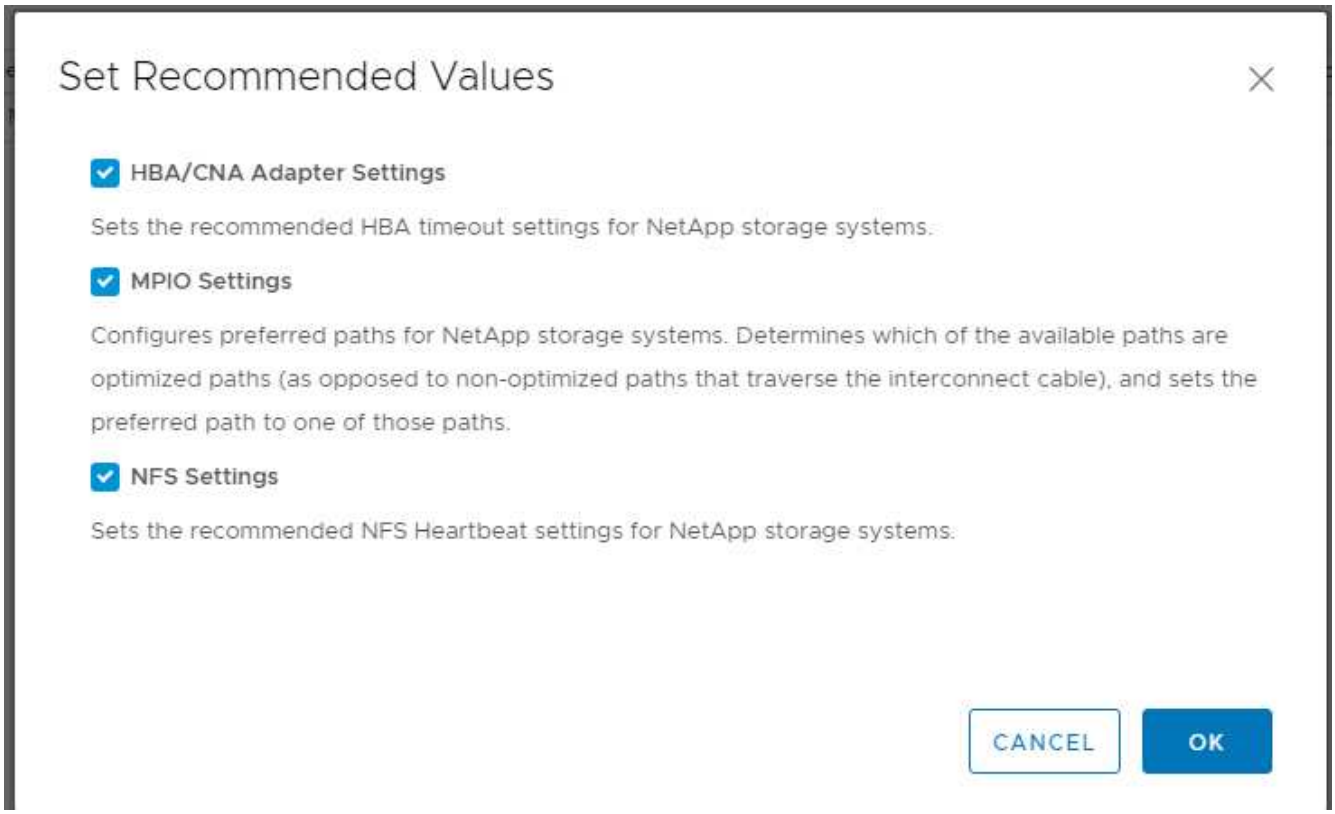
对 **ESXi** 主机使用最佳存储设置

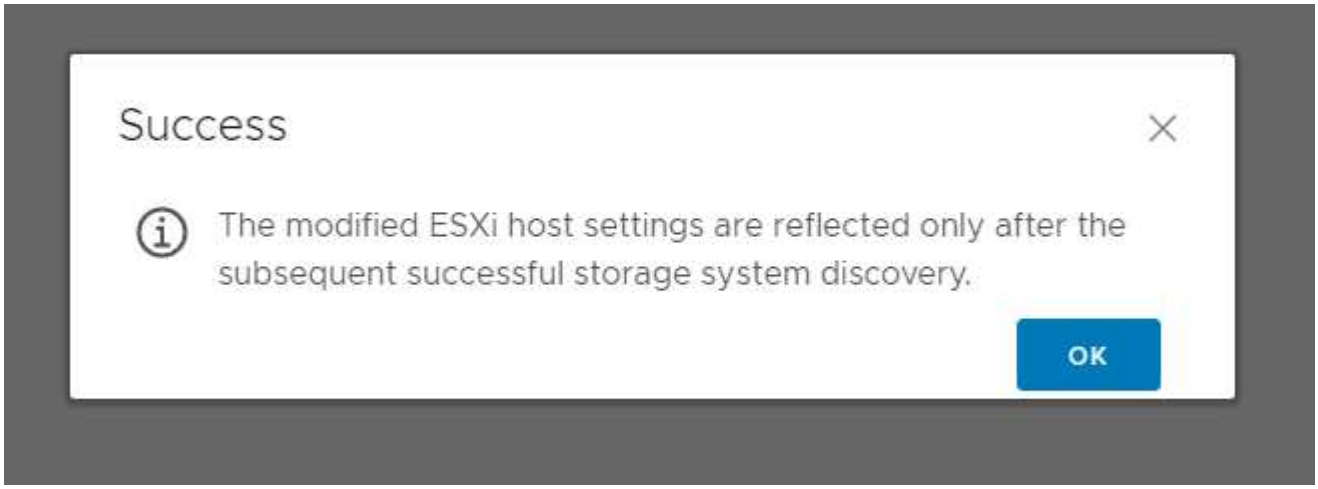
VSC 可为连接到 NetApp 存储控制器的所有 ESXi 主机自动配置与存储相关的设置。要使用这些设置，请完成以下步骤：

1. 在主页屏幕中，选择 vCenter > 主机和集群。对于每个 ESXi 主机，右键单击并选择 NetApp VSC > 设置建议值。



2. 检查要应用于选定 vSphere 主机的设置。单击确定以应用设置。





3. 应用这些设置后，重新启动 ESXi 主机。

结论

FlexPod Express 通过提供经过验证的设计，使用行业领先的组件，提供了一个简单而有效的解决方案。通过添加组件进行扩展，可以根据特定业务需求定制 FlexPod Express 。FlexPod Express 专为中小型企业， ROBO 以及其他需要专用解决方案的企业而设计。

致谢

作者谨向 John George 表示感谢，感谢他对这一设计的支持和贡献。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请参见以下文档和 / 或网站：

NetApp 产品文档

http://docs。 "NetApp".com

FlexPod 快速指南

NVA-1139-design ： 采用 Cisco UCS C 系列和 NetApp AFF C190 系列的 FlexPod Express

"https://www.netapp.com/us/media/nva-1139-design.pdf"

版本历史记录

version	Date	文档版本历史记录
版本 1.0	2019年11月	初始版本。

采用 Cisco UCS C 系列和 AFF A220 系列的 FlexPod Express 设计指南

NVA-1125- 设计：采用 Cisco UCS C 系列和 AFF A220 系列的 FlexPod Express

NetApp 公司 Savita Kumari 与以下组织合作：

行业趋势表明，数据中心正在向共享基础架构和云计算转型。此外，企业还寻求为远程办公室和分支机构提供简单有效的解决方案，利用他们在数据中心熟悉的技术。

FlexPod Express 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（ Cisco UCS ），Cisco Nexus 系列交换机和 NetApp AFF 构建。FlexPod Express 中的组件与 FlexPod 数据中心的对应组件一样，可以在较小规模的整个 IT 基础架构环境中实现管理协作。FlexPod 数据中心和 FlexPod Express 是虚拟化以及裸机操作系统和企业工作负载的最佳平台。

"接下来：计划摘要。"

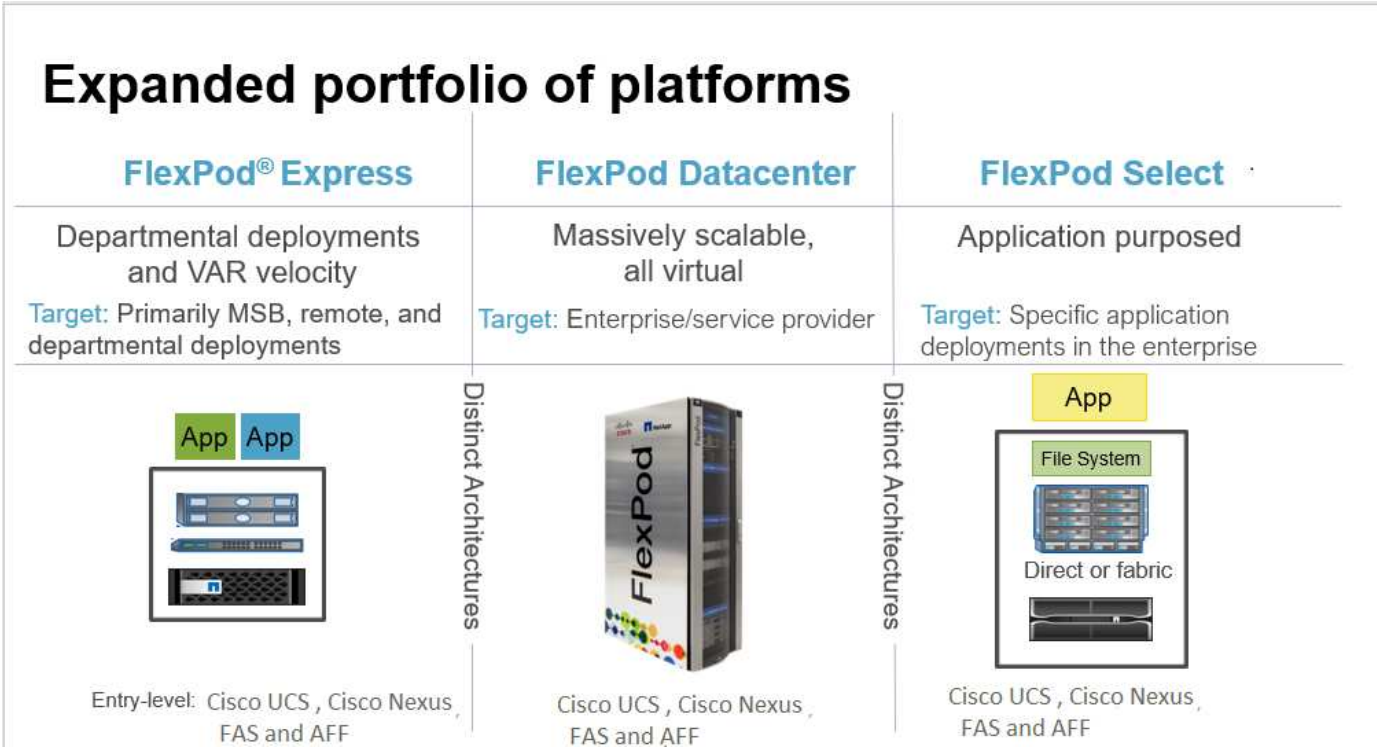
计划摘要

FlexPod 融合基础架构产品组合

FlexPod 参考架构以 Cisco 验证设计（ CVD ）或 NetApp 验证架构（ NVA ）的形式提供。如果变化不会导致部署不受支持的配置，则允许根据客户要求从给定 CVD 或 NVA 进行差异。

如下图所示， FlexPod 产品组合包括三个解决方案： FlexPod Express ， FlexPod Datacenter 和 FlexPod Select ：

- * FlexPod Express* 提供了一个由 Cisco 和 NetApp 技术组成的入门级解决方案。
- * FlexPod Datacenter 。 * 为各种工作负载和应用程序提供最佳的多用途基础。
- * FlexPod Select* 整合了 FlexPod 数据中心的最佳功能，并根据给定应用程序量身定制基础架构。



经验证的 **NetApp** 架构计划

NVA 计划为客户提供经过验证的 NetApp 解决方案架构。NVA 表示 NetApp 解决方案具有以下特性：

- 经过全面测试
- 具有规范性
- 最大限度地降低部署风险
- 加快上市速度

本指南详细介绍了采用 VMware vSphere 的 FlexPod Express 的设计。此外，此设计还利用全新的 AFF A220 系统作为虚拟机管理程序节点，该系统运行 NetApp ONTAP 9.4 软件， Cisco Nexus 3172P 交换机和 Cisco UCS C220 M5 服务器。

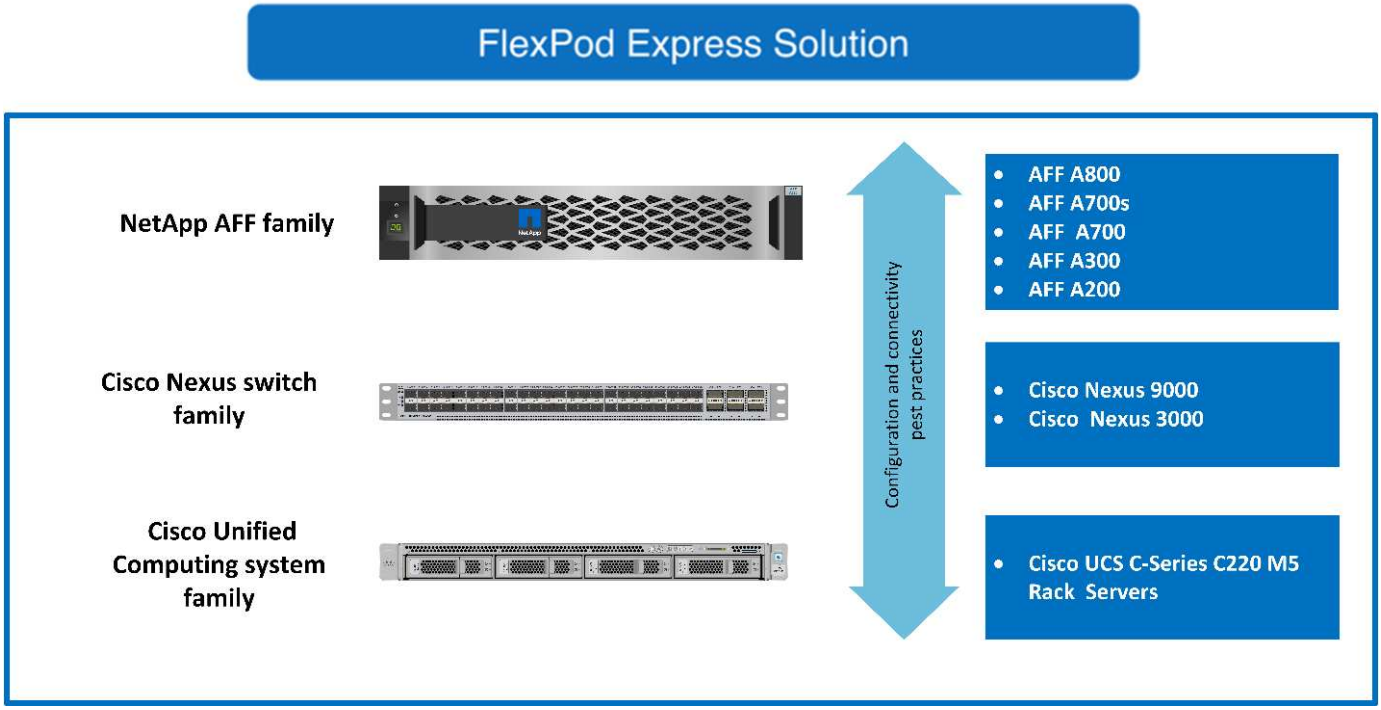
尽管本文档已针对 AFF A220 进行了验证，但此解决方案也支持 FAS2700 。

"接下来：解决方案概述。"

解决方案概述

FlexPod Express 专为运行混合虚拟化工作负载而设计。它面向远程办公室和分支机构以及中小型企业。它也是希望专用解决方案的大型企业的最佳选择。这款全新的解决方案 for FlexPod Express 新增了 NetApp ONTAP 9.4 ， NetApp AFF A220 和 VMware vSphere 6.7 等新技术。

下图显示了 FlexPod Express 解决方案中包含的硬件组件。

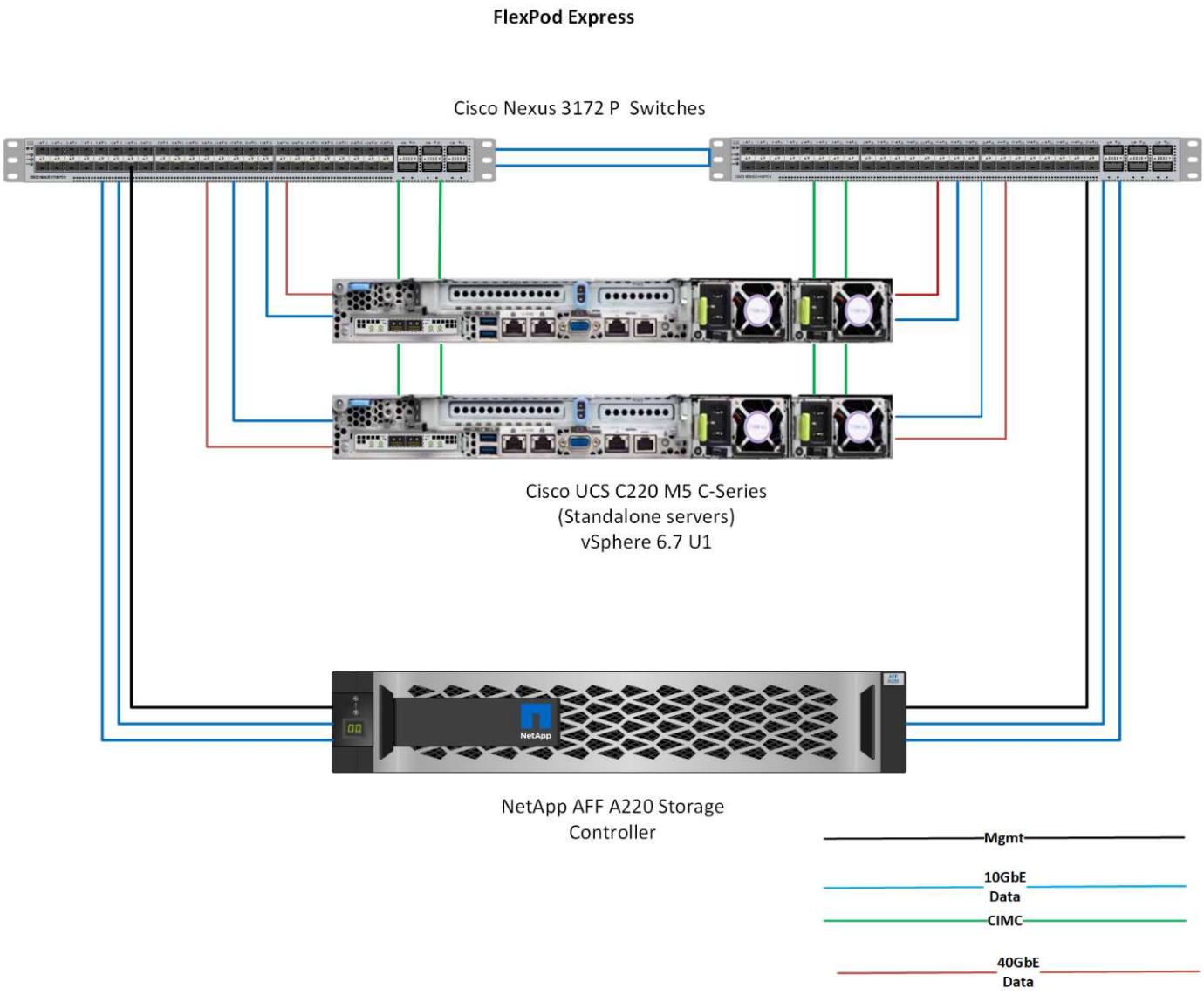


目标受众

本文档面向希望利用专为提高 IT 效率和实现 IT 创新而构建的基础架构的用户。本文档的受众包括但不限于销售工程师，现场顾问，专业服务人员， IT 经理， 合作伙伴工程师和客户。

解决方案技术

此解决方案利用了 NetApp ， Cisco 和 VMware 的最新技术。此解决方案采用全新的 NetApp AFF A220 系统，该系统运行 ONTAP 9.4 软件，双 Cisco Nexus 3172P 交换机以及运行 VMware vSphere 6.7 的 Cisco UCS C220 M5 机架式服务器。此经过验证的解决方案采用万兆以太网（ 10GbE ）技术。下图概述了相关信息。此外，还提供了有关如何通过一次添加两个虚拟机管理程序节点进行扩展的指导，以便 FlexPod 快速架构能够适应组织不断变化的业务需求。



40GbE 未经过验证，但它是受支持的基础架构。

"接下来：技术要求。"

技术要求

FlexPod Express 需要硬件和软件组件的组合，具体取决于所选虚拟机管理程序和网络速度。此外， FlexPod Express 还以两个单元的形式列出了向系统添加虚拟机管理程序节点所需的硬件组件。

硬件要求

无论选择何种虚拟机管理程序，所有 FlexPod 快速配置都使用相同的硬件。因此，即使业务需求发生变化，任何虚拟机管理程序都可以在同一个 FlexPod Express 硬件上运行。

下表列出了所有 FlexPod 快速配置以及实施解决方案所需的硬件组件。在任何特定解决方案实施中使用的硬件组件可能会因客户要求而异。

硬件	数量
AFF A220 双节点集群	1.
Cisco UCS C220 M5 服务器	2.
Cisco Nexus 3172P 交换机	2.
适用于 Cisco UCS C220 M5 机架式服务器的 Cisco UCS 虚拟接口卡（VIC） 1387	2.
Cisco CVR-QSFP-SFP10G 适配器	4.

软件要求

下表列出了实施 FlexPod Express 解决方案架构所需的软件组件。

下表列出了基本 FlexPod 快速实施的软件要求。

软件	**version**	详细信息
Cisco 集成管理控制器（CIMC）	3.1.3	适用于 C220 M5 机架式服务器
Cisco NX-OS	nxos.7.0.3.I7.5.bin	适用于 Cisco Nexus 3172P 交换机
NetApp ONTAP	9.4	适用于 AFF A220 控制器

下表列出了在 FlexPod Express 上实施所有 VMware vSphere 所需的软件。

软件	**version**
VMware vCenter Server 设备	6， 7.
VMware vSphere ESXi	6， 7.
适用于 ESXi 的 NetApp VAAI 插件	1.1.2

"接下来：设计选择。"

设计选择

在设计此设计的架构过程中，我们选择了以下技术。每个技术在 FlexPod Express 基础架构解决方案中都有一个特定用途。

采用 **ONTAP 9.4** 的 **NetApp AFF A220** 系列

此解决方案利用两种最新的 NetApp 产品： NetApp AFF A220 和 ONTAP 9.4 软件。

AFF A220 系统

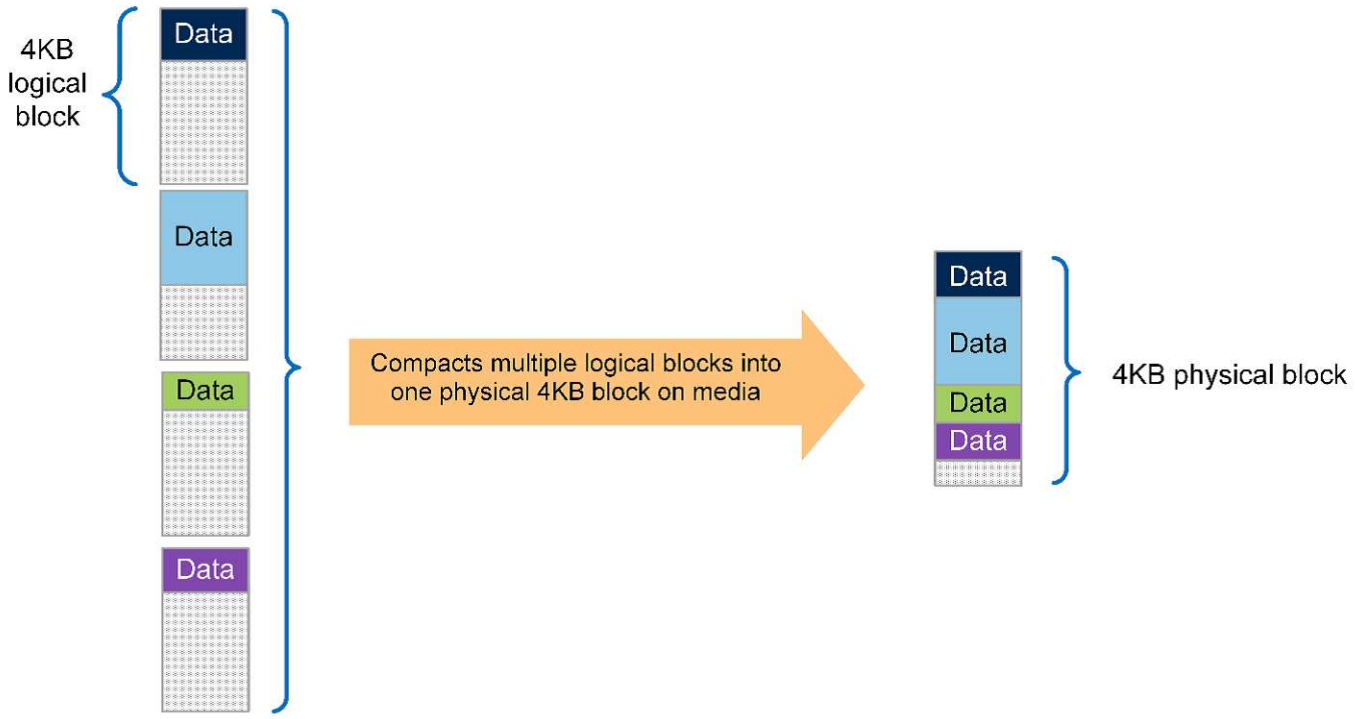
有关 AFF A220 硬件系统的详细信息，请参见 "AFF A 系列主页"。

ONTAP 9.4 软件

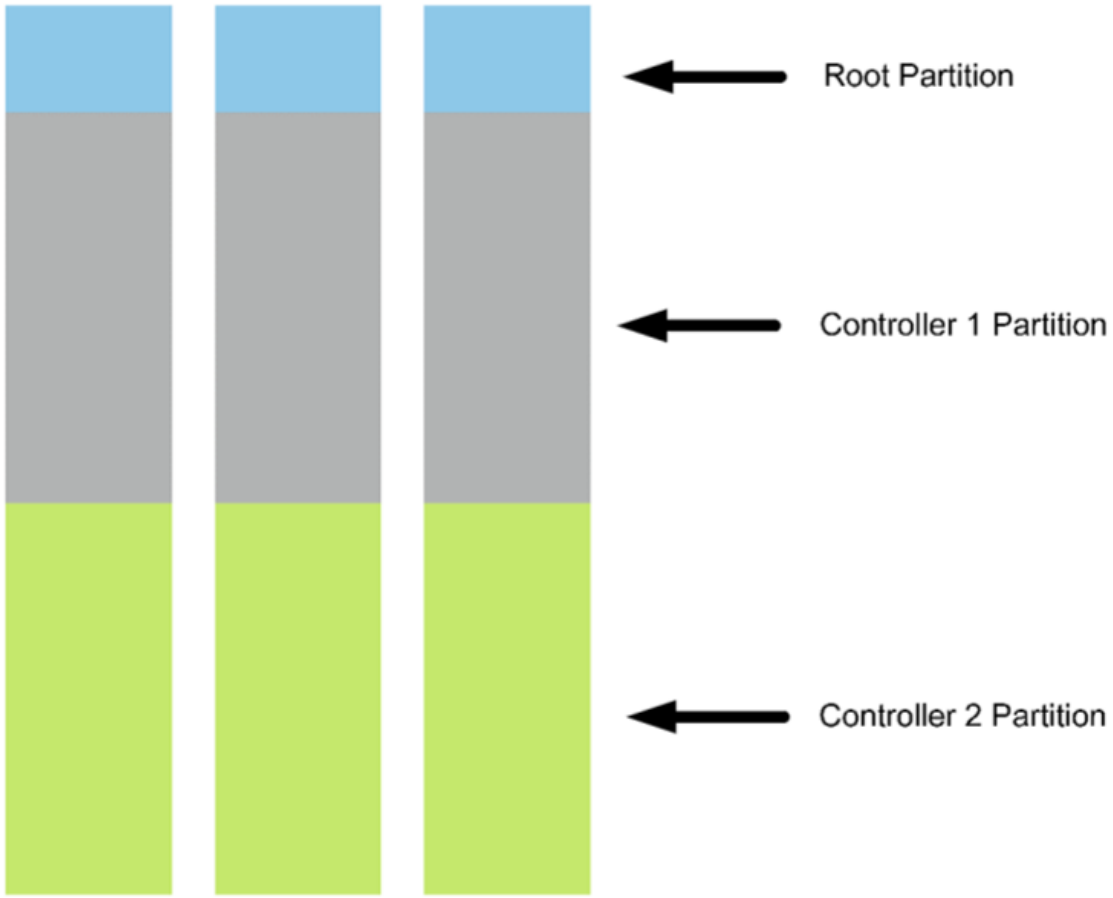
NetApp AFF A220 系统使用新的 ONTAP 9.4 软件。ONTAP 9.4 是行业领先的企业级数据管理软件。它将更高

级别的精简性和灵活性与强大的数据管理功能，存储效率和领先的云集成相结合。

ONTAP 9.4 具有多种非常适合 FlexPod Express 解决方案的功能。最重要的是 NetApp 对存储效率的承诺，存储效率是小型部署最重要的功能之一。ONTAP 9.4 新增了重复数据删除，数据压缩和精简配置等 NetApp 存储效率功能，并增加了数据缩减功能。由于 NetApp WAFL 系统始终写入 4 KB 块，因此，如果这些块未使用分配的 4 KB 空间，则数据缩减功能会将多个块合并到一个 4 KB 块中。下图说明了此过程。



此外，还可以在 AFF A220 系统上利用根数据分区功能。通过此分区，可以在系统中的磁盘之间对根聚合和两个数据聚合进行条带化。因此，双节点 AFF A220 集群中的两个控制器均可利用聚合中所有磁盘的性能。请参见下图。



这些只是 FlexPod Express 解决方案的几项主要功能。有关 ONTAP 9.4 的其他特性和功能的详细信息，请参见 "ONTAP 9 数据管理软件产品规格"。另请参见 NetApp "ONTAP 9 文档中心"，已更新为包括 ONTAP 9.4 。

Cisco Nexus 3000 系列

Cisco Nexus 3172P 是一款功能强大且经济高效的交换机，可提供 1/10/40/100Gbps 的交换。Cisco Nexus 3172PQ 交换机属于统一网络结构系列，是一款紧凑型单机架单元（ 1RU ）交换机，适用于机架顶部数据中心部署。（请参见下图。） 它可在 1RU 中提供多达 72 个 1/10GbE 端口，或在 1RU 中提供 48 个 1/10GbE 端口以及 6 个 40GbE 端口。为了最大程度地提高物理层灵活性，它还支持 1/10/40Gbps 。

由于所有各种 Cisco Nexus 系列型号都运行相同的底层操作系统 NX-OS ，因此 FlexPod Express 和 FlexPod Datacenter 解决方案支持多个 Cisco Nexus 型号。

性能规格包括：

- 所有端口上的线速流量吞吐量（第 2 层和第 3 层）
- 可配置的最大传输单元（ MTU ），最多 9216 字节（巨型帧）

有关 Cisco Nexus 3172 交换机的详细信息，请参见 "Cisco Nexus 3172PQ， 3172TQ， 3172TQ-32T，3172PQ-XL 和 3172TQ-XL 交换机数据表"。

Cisco UCS C 系列

之所以选择 Cisco UCS C 系列机架式服务器来支持 FlexPod Express，是因为它具有多种配置选项，可以根据 FlexPod Express 部署中的特定要求进行定制。

Cisco UCS C 系列机架式服务器采用行业标准外形规格提供统一计算，以降低 TCO 并提高灵活性。

Cisco UCS C 系列机架式服务器具有以下优势：

- 与外形规格无关的 Cisco UCS 入门点
- 简化并快速部署应用程序
- 将统一计算创新技术和优势扩展到机架式服务器
- 通过熟悉的机架包装提供独特优势，增加客户的选择

Cisco UCS C220 M5 机架式服务器（如上图所示）是业内用途最广泛的通用企业基础架构和应用程序服务器之一。它是一款高密度双插槽机架式服务器，可为包括虚拟化，协作和裸机应用程序在内的各种工作负载提供行业领先的性能和效率。Cisco UCS C 系列机架式服务器可以作为独立服务器部署，也可以作为 Cisco UCS 的一部分部署，以利用 Cisco 基于标准的统一计算创新技术，帮助客户降低 TCO 并提高业务灵活性。

有关 C220 M5 服务器的详细信息，请参见 "Cisco UCS C220 M5 机架式服务器数据表"。

C220 M5 机架式服务器的连接选项

C220 M5 机架式服务器的连接选项如下：

- * Cisco UCS VIC 1387*

  Cisco UCS VIC 1387 （如下图所示）采用模块化主板上 LAN （ mLOM ）外形规格，可提供双端口增强型 QSF+40GbE 和以太网 FC （ FCoE ）。可以使用 mLOM 插槽安装 Cisco VIC，而无需使用外设组件互连快速（ Peripheral Component Interconnect Express， PCIe ）插槽，从而提高 I/O 可扩展性。

有关 Cisco UCS VIC 1387 适配器的详细信息，请参见 "Cisco UCS 虚拟接口卡 1387" 数据表。

- * CVR-QSFP-SFP10G 适配器 *

  Cisco QSA 模块可将 QSFP 端口转换为 SFP 或 SFP+ 端口。借助此适配器，客户可以灵活地使用任何 SFP+ 或 SFP 模块或缆线连接到网络另一端的低速度端口。这种灵活性可以最大限度地利用高密度 40GbE QSFP 平台，经济高效地过渡到 40GbE 。此适配器支持所有 SFP+ 光纤和缆线连接，并支持多个 1GbE SFP 模块。由于此项目已通过使用 10GbE 连接进行验证，并且所使用的 VIC 1387 为 40GbE ，因此使用 CVR-QSFP-SFP10G 适配器（下图中）进行转换。

VMware vSphere 6.7

VMware vSphere 6.7 是一个适用于 FlexPod Express 的虚拟机管理程序选项。通过 VMware vSphere ，企业可以减少电耗和散热占用空间，同时确认已购买的计算容量已充分利用。此外， VMware vSphere 还支持在 vSphere 主机集群（ VMware Distributed Resource Scheduler 或 VMware DRS ）之间进行硬件故障保护（ VMware High Availability 或 VMware HA ）和计算资源负载平衡。

由于 VMware vSphere 6.7 只会重新启动内核，因此客户可以通过它 " 快速启动 " 来加载 vSphere ESXi ，而无需重新启动硬件。此功能仅适用于快速启动白名单上的平台和驱动程序。vSphere 6.7 扩展了 vSphere Client 的功能， vSphere Client 可执行大约 90% 的 vSphere Web Client 功能。

在 vSphere 6.7 中， VMware 扩展了此功能，使客户能够按虚拟机（ VM ）而非主机设置增强型 vMotion 兼容

性（ EVC ）。在 vSphere 6.7 中， VMware 还公开了可用于创建即时克隆的 API 。

以下是 vSphere 6.7 U1 的一些功能：

- 功能全面的基于 Web 的 HTML5 vSphere Client
- 适用于 NVIDIA GRID vGPU VM 的 VMotion 。支持 Intel FPGA 。
- vCenter Server Converge Tool 可从外部 PSC 迁移到内部 PC 。
- vSAN 增强功能（ HCI 更新）。
- 增强的内容库。

有关 vSphere 6.7 U1 的详细信息，请参见 "vCenter Server 6.7 Update 1 中的新增功能"。虽然此解决方案已通过 vSphere 6.7 的验证，但它支持任何经 NetApp 互操作性表工具认证可与其他组件配合使用的 vSphere 版本。NetApp 建议部署 vSphere 6.7U1 以修复其问题并增强其功能。

启动架构

以下是 FlexPod 快速启动架构支持的选项：

- iSCSI SAN LUN
- Cisco FlexFlash SD 卡
- 本地磁盘

由于 FlexPod 数据中心是从 iSCSI LUN 启动的，因此通过对 FlexPod Express 使用 iSCSI 启动来增强解决方案的易管理性。

"接下来：解决方案验证。"

解决方案验证

Cisco 和 NetApp 设计并构建了 FlexPod Express ，作为客户的首要基础架构平台。由于 FlexPod Express 采用行业领先的组件设计，因此客户可以信赖它作为基础架构的基础。为了符合 FlexPod 产品组合的基本原则， FlexPod 快速架构已通过 Cisco 和 NetApp 数据中心架构师和工程师的全面测试。从冗余和可用性到每项功能，整个 FlexPod 快速架构都经过验证，可以为客户树立信心，并在设计过程中建立信任。

VMware vSphere 6.7 已在 FlexPod 快速基础架构组件上进行了验证。此验证包括虚拟机管理程序的 10GbE 上行链路连接选项。

"接下来：总结。"

结论

FlexPod Express 通过提供经过验证的设计，使用行业领先的组件，提供了一个简单而有效的解决方案。通过扩展虚拟机管理程序平台并为其提供选项， FlexPod Express 可以根据特定业务需求进行定制。FlexPod Express 在设计时考虑到了中小型企业，远程办公室和分支机构以及其他需要专用解决方案的企业。

"下一步：从何处查找追加信息。"

从何处查找追加信息

要了解有关本文档所述信息的更多信息，请参见以下文档和网站：

- NetApp 文档

  "https://docs.netapp.com"

- 《使用 VMware vSphere 6.7 的 FlexPod Express 和 NetApp AFF A220 部署指南》

  "https://www.netapp.com/us/media/nva-1123-deploy.pdf"

《采用 Cisco UCS C 系列和 AFF A220 系列的 FlexPod 快速部署指南》

NVA-1123-Deploy：《采用 VMware vSphere 6.7 的 FlexPod Express 和 NetApp AFF A220 部署指南》

NetApp 公司 Savita Kumari

与以下合作伙伴：

行业趋势表明，数据中心正在向共享基础架构和云计算转型。此外，企业还寻求为远程办公室和分支机构提供简单有效的解决方案，并利用他们在数据中心中熟悉的技术。

FlexPod Express 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（Cisco UCS），Cisco Nexus 系列交换机和 NetApp 存储技术构建。FlexPod 快速系统中的组件与 FlexPod 数据中心的对应组件一样，可以在较小规模的整个 IT 基础架构环境中实现管理协作。FlexPod 数据中心和 FlexPod Express 是虚拟化以及裸机操作系统和企业工作负载的最佳平台。

FlexPod 数据中心和 FlexPod Express 提供基线配置，并可灵活调整规模和进行优化，以满足多种不同的使用情形和要求。现有的 FlexPod 数据中心客户可以使用他们习惯使用的工具来管理其 FlexPod 快速系统。新的 FlexPod Express 客户可以随着环境的增长轻松适应 FlexPod 数据中心的管理。

FlexPod Express 是远程办公室和分支机构以及中小型企业的最佳基础架构基础。对于希望为专用工作负载提供基础架构的客户来说，它也是最佳解决方案。

FlexPod Express 提供了一个易于管理的基础架构，几乎适合任何工作负载。

解决方案概述

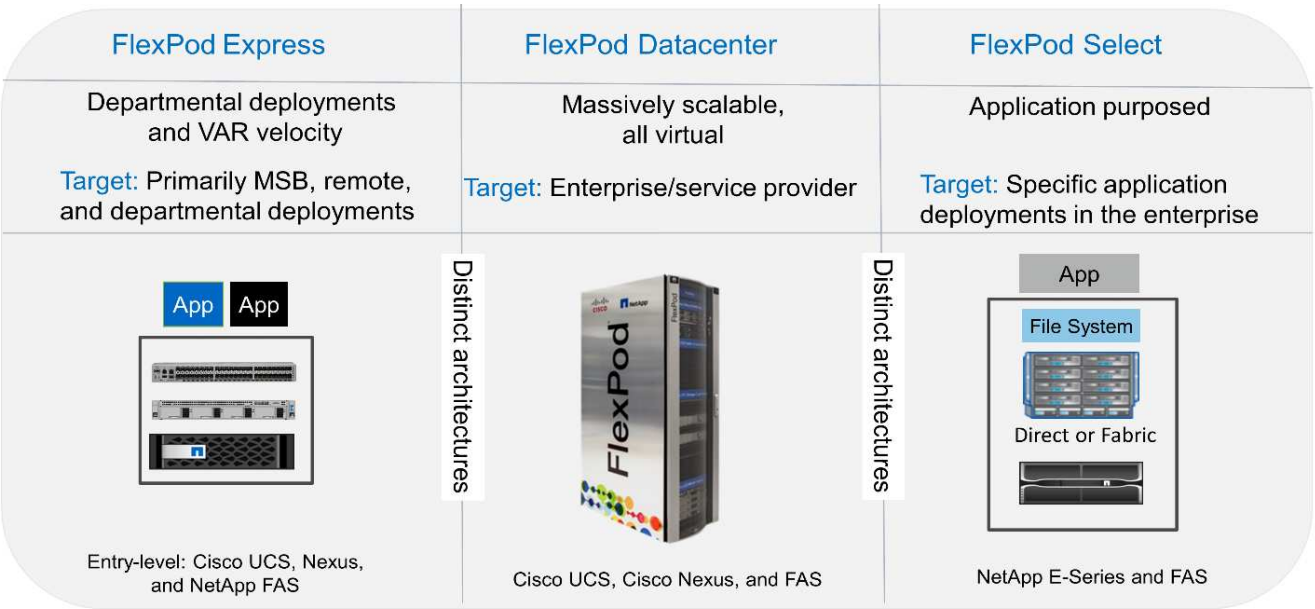
此 FlexPod Express 解决方案是 FlexPod 融合基础架构计划的一部分。

FlexPod 融合基础架构计划

FlexPod 参考架构以 Cisco 验证设计（CVD）或 NetApp 验证架构（NVA）的形式提供。如果给定 CVD 或 NVA 不会产生不受支持的配置，则允许根据客户要求进行差异。

如下图所示， FlexPod 计划包括三个解决方案： FlexPod Express， FlexPod Datacenter 和 FlexPod Select：

- * FlexPod Express* 为客户提供了采用 Cisco 和 NetApp 技术的入门级解决方案。
- * FlexPod Datacenter 。 * 为各种工作负载和应用程序提供最佳的多用途基础。
- * FlexPod Select* 整合了 FlexPod 数据中心的最佳功能，并根据给定应用程序量身定制基础架构。



经验证的 **NetApp** 架构计划

经验证的 NetApp 架构计划为客户提供经过验证的 NetApp 解决方案架构。经验证的 NetApp 架构可提供具有以下品质的 NetApp 解决方案架构：

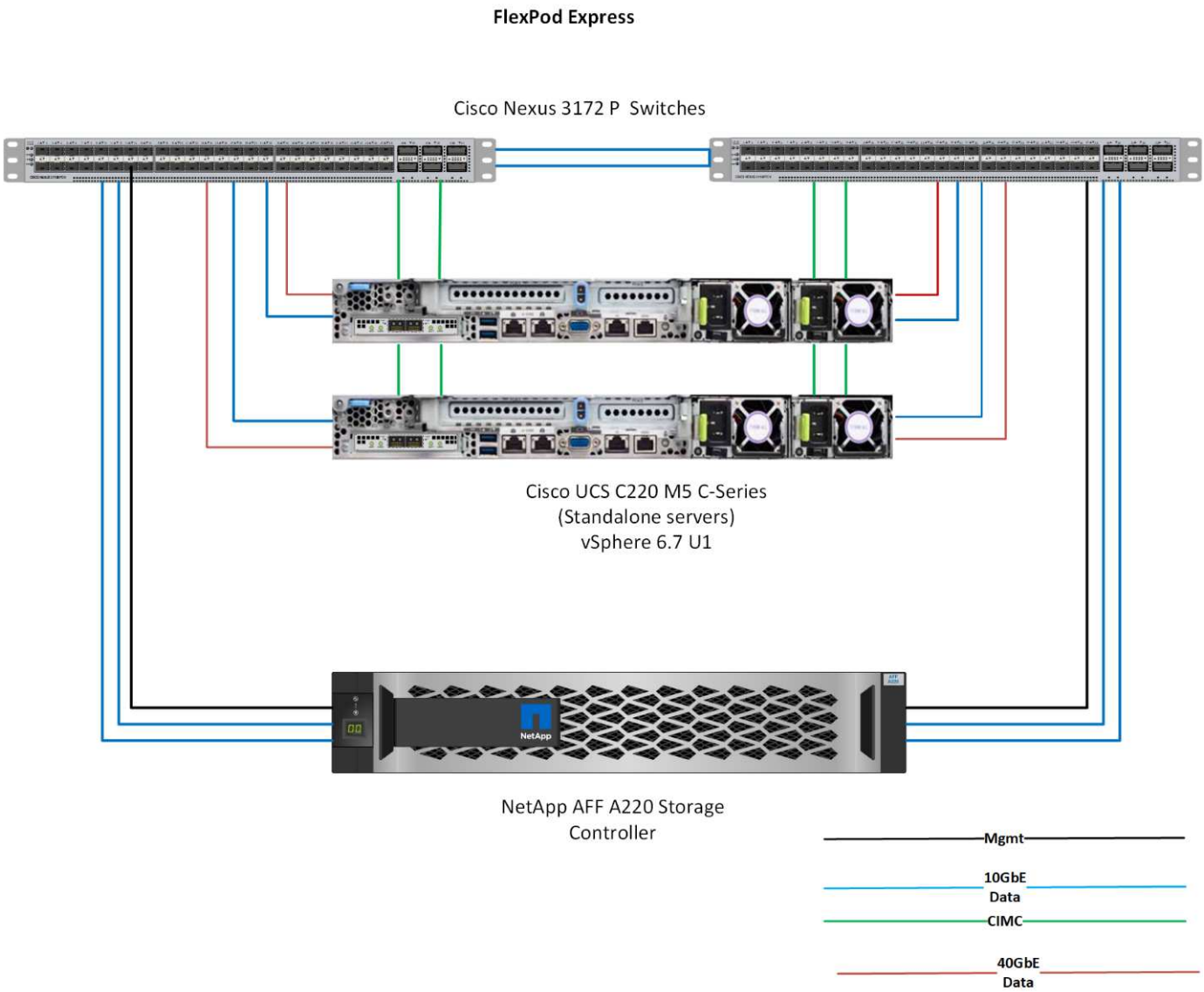
- 经过全面测试
- 具有规范性
- 最大限度地降低部署风险
- 加快上市速度

本指南详细介绍了采用 VMware vSphere 的 FlexPod Express 的设计。此外，此设计还使用全新的 AFF A220 系统（运行 NetApp ONTAP 9.4）， Cisco Nexus 3172P 和 Cisco UCS C 系列 C220 M5 服务器作为虚拟机管理程序节点。

解决方案技术

此解决方案利用了 NetApp， Cisco 和 VMware 的最新技术。此解决方案采用运行 ONTAP 9.4 的全新 NetApp AFF A220，双 Cisco Nexus 3172P 交换机以及运行 VMware vSphere 6.7 的 Cisco UCS C220 M5 机架式服务器。此经过验证的解决方案采用 10GbE 技术。此外，还提供了有关如何通过一次添加两个虚拟机管理程序节点来扩展计算容量的指导，以使 FlexPod 快速架构能够适应组织不断变化的业务需求。

下图显示了采用 VMware vSphere 10GbE 架构的 FlexPod Express 。



此验证使用 10GbE 连接和一个 40GbE Cisco UCS VIC 1387 。要实现 10GbE 连接，请使用 CVR-QSFP-SFP10G 适配器。

使用情形摘要

FlexPod Express 解决方案可应用于多种使用情形，包括以下情形：

- 远程办公室或分支机构
- 中小型企业

- 需要经济高效的专用解决方案的环境

FlexPod Express 最适合虚拟化和混合工作负载。

> 虽然此解决方案已通过 vSphere 6.7 的验证，但它支持任何经 NetApp 互操作性表工具认证可与其他组件配合使用的 vSphere 版本。NetApp 建议部署 vSphere 6.7U1 以修复其问题并增强其功能。

以下是 vSphere 6.7 U1 的一些功能：

- 功能全面的基于 Web 的 HTML5 vSphere 客户端
- 适用于 NVIDIA GRID vGPU VM 的 VMotion 。支持 Intel FPGA
- vCenter Server Converge Tool 可从外部 PSC 迁移到内部 PC
- vSAN 增强功能（ HCI 更新）
- 增强的内容库

有关 vSphere 6.7 U1 的详细信息，请参见 "vCenter Server 6.7 Update 1 中的新增功能"。

技术要求

FlexPod 快速系统需要硬件和软件组件的组合。FlexPod Express 还介绍了以两个单位向系统添加虚拟机管理程序节点所需的硬件组件。

硬件要求

无论选择何种虚拟机管理程序，所有 FlexPod 快速配置都使用相同的硬件。因此，即使业务需求发生变化，任何虚拟机管理程序都可以在同一个 FlexPod Express 硬件上运行。

下表列出了所有 FlexPod 快速配置所需的硬件组件。

硬件	数量
AFF A220 HA 对	1.
Cisco C220 M5 服务器	2.
Cisco Nexus 3172P 交换机	2.
适用于 C220 M5 服务器的 Cisco UCS 虚拟接口卡（ VIC ） 1387	2.
CVR-QSFP-SFP10G 适配器	4.

下表列出了实施 10GbE 所需的硬件以及基本配置。

硬件	数量
Cisco UCS C220 M5 服务器	2.
Cisco VIC 1387	2.
CVR-QSFP-SFP10G 适配器	4.

软件要求

下表列出了实施 FlexPod 快速解决方案架构所需的软件组件。

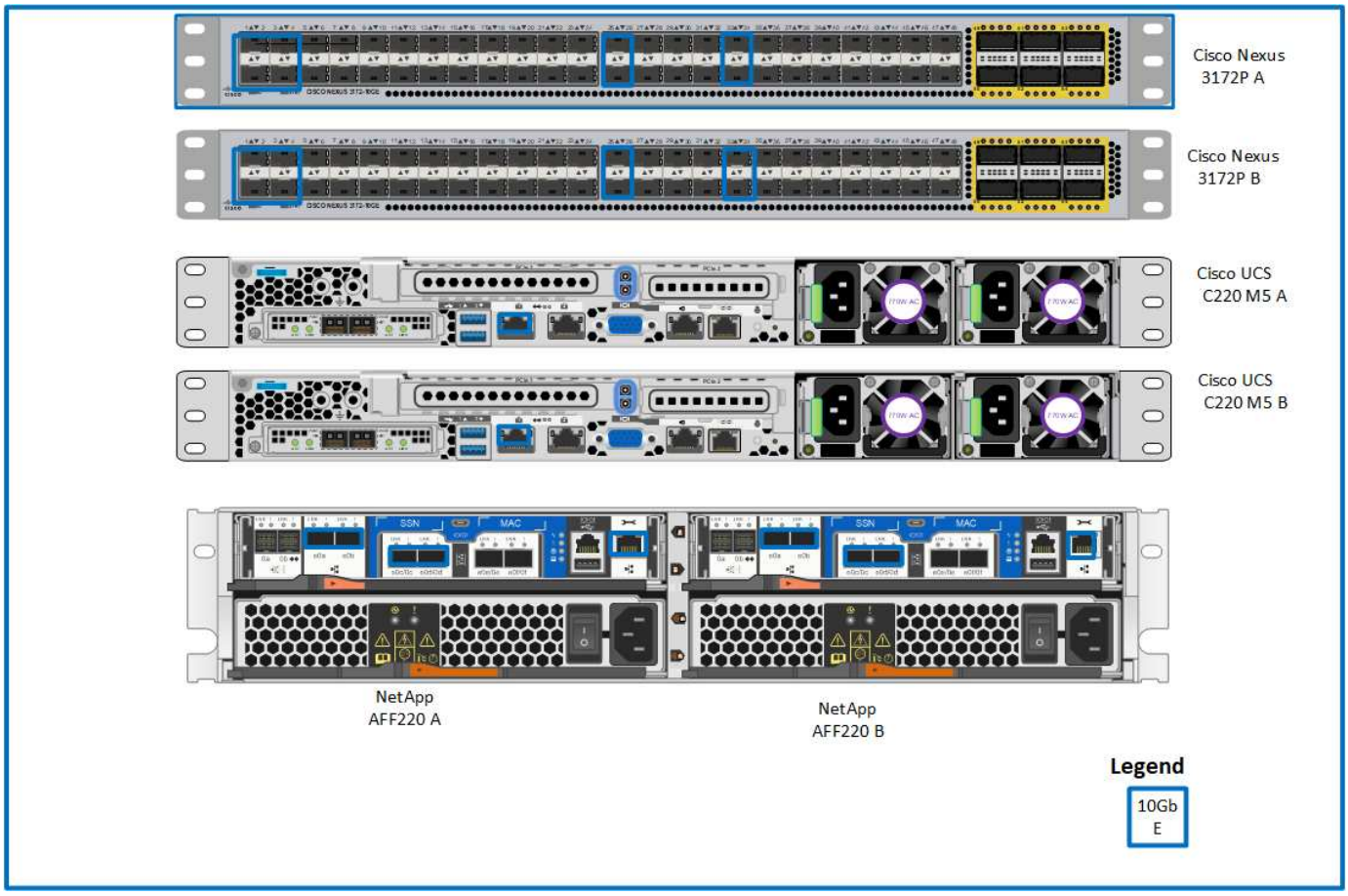
软件	**version**	详细信息
Cisco 集成管理控制器（CIMC）	3.1 （3g）	适用于 Cisco UCS C220 M5 机架式服务器
Cisco nenic 驱动程序	1.0.25.0	适用于 VIC 1387 接口卡
Cisco NX-OS	nxos.7.0.3.I7.5.bin	适用于 Cisco Nexus 3172P 交换机
NetApp ONTAP	9.4	适用于 AFF A220 控制器

下表列出了在 FlexPod Express 上实施所有 VMware vSphere 所需的软件。

软件	**version**
VMware vCenter Server 设备	6， 7.
VMware vSphere ESXi 虚拟机管理程序	6， 7.
适用于 ESXi 的 NetApp VAAI 插件	1.1.2

FlexPod 快速布线信息

下图显示了参考验证布线。



下表显示了 Cisco Nexus 交换机 3172P A 的布线信息

本地设备	本地端口	远程设备	远程端口
Cisco Nexus 交换机 3172P A	Eth1/1	NetApp AFF A220 存储控制器 A	e0c
	eth1/2	NetApp AFF A220 存储控制器 B	e0c
	Eth1/3	Cisco UCS C220 C 系列独立服务器 A	采用 CVR-QSFP-SFP10G 适配器的 MLOM1
	Eth1/4	Cisco UCS C220 C 系列独立服务器 B	采用 CVR-QSFP-SFP10G 适配器的 MLOM1
	eth1/25	Cisco Nexus 交换机 3172P B	eth1/25
	eth1/26.	Cisco Nexus 交换机 3172P B	eth1/26.
	eth1/33	NetApp AFF A220 存储控制器 A	e0M
	eth1/34	Cisco UCS C220 C 系列独立服务器 A	CIMC

下表显示了 Cisco Nexus 交换机 3172P B 的布线信息

本地设备	本地端口	远程设备	远程端口
Cisco Nexus 交换机 3172P B	Eth1/1	NetApp AFF A220 存储控制器 A	e0d
	eth1/2	NetApp AFF A220 存储控制器 B	e0d
	Eth1/3	Cisco UCS C220 C 系列独立服务器 A	采用 CVR-QSFP-SFP10G 适配器的 MLOM2
	Eth1/4	Cisco UCS C220 C 系列独立服务器 B	采用 CVR-QSFP-SFP10G 适配器的 MLOM2
	eth1/25	Cisco Nexus 交换机 3172P A	eth1/25
	eth1/26.	Cisco Nexus 交换机 3172P A	eth1/26.
	eth1/33	NetApp AFF A220 存储控制器 B	e0M
	eth1/34	Cisco UCS C220 C 系列独立服务器 B	CIMC

下表显示了 NetApp AFF A220 存储控制器 A 的布线信息

本地设备	本地端口	远程设备	远程端口
NetApp AFF A220 存储控制器 A	e0a	NetApp AFF A220 存储控制器 B	e0a
	e0b	NetApp AFF A220 存储控制器 B	e0b
	e0c	Cisco Nexus 交换机 3172P A	Eth1/1
	e0d	Cisco Nexus 交换机 3172P B	Eth1/1
	e0M	Cisco Nexus 交换机 3172P A	eth1/33

下表显示了 NetApp AFF A220 存储控制器 B 的布线信息

本地设备	本地端口	远程设备	远程端口
NetApp AFF A220 存储控制器 B	e0a	NetApp AFF A220 存储控制器 A	e0a
	e0b	NetApp AFF A220 存储控制器 A	e0b
	e0c	Cisco Nexus 交换机 3172P A	eth1/2
	e0d	Cisco Nexus 交换机 3172P B	eth1/2
	e0M	Cisco Nexus 交换机 3172P B	eth1/33

部署过程

本文档详细介绍了如何配置完全冗余，高可用性的 FlexPod Express 系统。为了反映这种冗余，在每个步骤中配置的组件称为组件 A 或组件 B例如，控制器 A 和控制器 B 可识别本文档中配置的两个 NetApp 存储控制器。交换机 A 和交换机 B 可识别一对 Cisco Nexus 交换机。

此外，本文档还介绍配置多个 Cisco UCS 主机的步骤，这些主机按顺序标识为服务器 A ，服务器 B 等。

要指示您应在步骤中包含与您的环境相关的信息，请在命令结构中显示 ` <<text>>` 。请参见以下 `vlan create` 命令示例：

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

通过本文档，您可以完全配置 FlexPod 快速环境。在此过程中，您需要通过多个步骤插入客户专用的命名约定， IP 地址和虚拟局域网（ VLAN ）方案。下表介绍了部署所需的 VLAN ，如本指南所述。此表可根据特定站点变量填写，并用于实施文档配置步骤。

> 如果使用单独的带内和带外管理 VLAN ，则必须在它们之间创建第 3 层路由。在此验证中，使用了一个通用管理 VLAN 。

AN 名称	**VLAN** 用途	用于验证本文档的 **ID**
管理 VLAN	用于管理接口的 VLAN	3437
原生 VLAN	将未标记的帧分配到的 VLAN	2.
NFS VLAN	用于 NFS 流量的 VLAN	3438
VMware vMotion VLAN	为将虚拟机从一台物理主机移动到另一台物理主机而指定的 VLAN	3441
虚拟机流量 VLAN	虚拟机应用程序流量的 VLAN	3442
iSCSI-A-VLAN	网络结构 A 上用于 iSCSI 流量的 VLAN	3439
iSCSI-B-VLAN	网络结构 B 上用于 iSCSI 流量的 VLAN	3440

在整个 FlexPod Express 配置过程中都需要 VLAN 编号。这些 VLAN 称为 ` <<var_xxxx_vlan>>` ，其中 `xxxx` 是 VLAN 的用途（例如 iSCSI-A ）。

下表列出了创建的 VMware 虚拟机。

虚拟机问题描述	主机名
VMware vCenter Server	

Cisco Nexus 3172P 部署操作步骤

以下部分详细介绍了 FlexPod Express 环境中使用的 Cisco Nexus 3172P 交换机配置。

Cisco Nexus 3172P 交换机的初始设置

以下过程介绍了如何配置 Cisco Nexus 交换机以在基础 FlexPod Express 环境中使用。

> 此操作步骤假定您使用的是运行 NX-OS 软件版本 7.0 （ 3 ） i7 （ 5 ）的 Cisco Nexus 3172P 。

1. 首次启动并连接到交换机的控制台端口后， Cisco NX-OS 设置将自动启动。此初始配置可解决基本设置，例如交换机名称， mgmt0 接口配置和安全 Shell （ SSH ）设置。
2. FlexPod 快速管理网络可以通过多种方式进行配置。3172P 交换机上的 mgmt0 接口可以连接到现有管理网络，也可以采用背对背配置连接 3172P 交换机的 mgmt0 接口。但是，此链路不能用于外部管理访问，例如 SSH 流量。

   在本部署指南中， FlexPod Express Cisco Nexus 3172P 交换机连接到现有管理网络。

3. 要配置 Cisco Nexus 3172P 交换机，请启动交换机并按照屏幕上的提示进行操作，如此处所示，对这两台交换机进行初始设置，并将相应的值替换为交换机特定信息。

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 3172P-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]:  <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:  <enter>
```

4. 然后，您将看到配置摘要，系统会询问您是否要对其进行编辑。如果配置正确，请输入 `n`。

```
Would you like to edit the configuration? (yes/no) [n]: n
```

5. 然后，系统会询问您是否要使用此配置并保存它。如果是，请输入 `y`。

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. 对 Cisco Nexus 交换机 B 重复此操作步骤

启用高级功能

要提供其他配置选项，必须在 Cisco NX-OS 中启用某些高级功能。

> 只有在使用本文档中所述的背对背 `mgmt0` 选项时，才需要 `interface-vlan` 功能。通过此功能，您可以为接口 VLAN （交换机虚拟接口）分配 IP 地址，从而可以与交换机进行带内管理通信（例如通过 SSH ）。

1. 要在 Cisco Nexus 交换机 A 和交换机 B 上启用相应功能，请使用命令 ` （ config t ）` 进入配置模式，然后运行以下命令：

```
feature interface-vlan
feature lacp
feature vpc
```

   默认端口通道负载平衡哈希使用源 IP 地址和目标 IP 地址来确定端口通道中各个接口之间的负载平衡算法。除了源 IP 地址和目标 IP 地址之外，还可以为哈希算法提供更多输入，从而在端口通道的各个成员之间实现更好的分布。出于同样的原因， NetApp 强烈建议将源和目标 TCP 端口添加到哈希算法中。

2. 在配置模式（`config t`）下，输入以下命令以设置 Cisco Nexus 交换机 A 和交换机 B 上的全局端口通道负载平衡配置：

```
port-channel load-balance src-dst ip-l4port
```

执行全局生成树配置

Cisco Nexus 平台使用一种新的保护功能，称为网桥保证。如果设备不再运行生成树算法，则网桥保证有助于防止单向链路或其他软件故障继续转发数据流量。根据平台的不同，可以将端口置于多种状态之一，包括网络或边缘状态。

NetApp 建议设置网桥保证，以便默认情况下将所有端口都视为网络端口。此设置强制网络管理员查看每个端口的配置。此外，它还会显示最常见的配置错误，例如未标识的边缘端口或未启用网桥保证功能的邻居。此外，生成树块中的端口较多而不是太少会更安全，这样就可以使用默认端口状态来增强网络的整体稳定性。

添加服务器，存储和上行链路交换机时，请密切关注生成树的状态，尤其是在它们不支持网桥保证的情况下。在这种情况下，您可能需要更改端口类型才能使端口处于活动状态。

默认情况下，作为另一层保护，在边缘端口上启用网桥协议数据单元（ BPDU ）保护。为了防止网络中出现环路，如果在此接口上看到来自另一个交换机的 BPDU ，则此功能将关闭此端口。

在配置模式（`config t`）下，运行以下命令以配置 Cisco Nexus 交换机 A 和交换机 B 上的默认生成树选项，包括默认端口类型和 BPDU 保护：

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

定义 VLAN

在配置具有不同 VLAN 的各个端口之前，必须在交换机上定义第 2 层 VLAN 。此外，最好对 VLAN 进行命名，以便将来进行故障排除。

在配置模式（`config t`）下，运行以下命令来定义和描述 Cisco Nexus 交换机 A 和交换机 B 上的第 2 层 VLAN：

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

配置访问和管理端口说明

与为第 2 层 VLAN 分配名称一样，为所有接口设置说明有助于配置和故障排除。

在每个交换机的配置模式（`config t`）中，输入 FlexPod 快速大型配置的以下端口说明：

Cisco Nexus 交换机 A

```
int eth1/1
  description AFF A220-A e0c
int eth1/2
  description AFF A220-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0
int eth1/4
  description UCS-Server-B: MLOM port 0
int eth1/25
  description vPC peer-link 3172P-B 1/25
int eth1/26
  description vPC peer-link 3172P-B 1/26
int eth1/33
  description AFF A220-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Cisco Nexus 交换机 B

```
int eth1/1
  description AFF A220-A e0d
int eth1/2
  description AFF A220-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 1
int eth1/4
  description UCS-Server-B: MLOM port 1
int eth1/25
  description vPC peer-link 3172P-A 1/25
int eth1/26
  description vPC peer-link 3172P-A 1/26
int eth1/33
  description AFF A220-B e0M
int eth1/34
  description UCS Server B: CIMC
```

配置服务器和存储管理接口

服务器和存储的管理接口通常仅使用一个 VLAN 。因此，请将管理接口端口配置为访问端口。为每个交换机定义管理 VLAN ，并将生成树端口类型更改为边缘。

在配置模式（`config t`）下，输入以下命令为服务器和存储的管理接口配置端口设置：

Cisco Nexus 交换机 A

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus 交换机 B

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

执行虚拟端口通道全局配置

通过虚拟端口通道（ vPC ），物理连接到两个不同 Cisco Nexus 交换机的链路可以显示为连接到第三个设备的单端口通道。第三个设备可以是交换机，服务器或任何其他网络设备。vPC 可以提供第 2 层多路径功能，通过增加带宽，在节点之间启用多个并行路径以及存在备用路径的负载平衡流量，您可以创建冗余。

vPC 具有以下优势：

- 允许单个设备在两个上游设备之间使用端口通道
- 消除生成树协议阻止的端口
- 提供无环路拓扑
- 使用所有可用的上行链路带宽
- 在链路或设备发生故障时提供快速融合
- 提供链路级别故障恢复能力
- 帮助提供高可用性

要使 vPC 功能正常运行，需要在两个 Cisco Nexus 交换机之间进行一些初始设置。如果使用背对背 mgmt0 配置，请使用接口上定义的地址，并使用 ping ` 验证它们是否可以通信[switch_A/B_mgmt0_ip_addr]vRF` 管理命令。

在配置模式（`config t`）下，运行以下命令为两台交换机配置 vPC 全局配置：

Cisco Nexus 交换机 A

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Cisco Nexus 交换机 B

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25- 26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

配置存储端口通道

NetApp 存储控制器允许使用链路聚合控制协议（ Link Aggregation Control Protocol ， LACP ）与网络建立主动 - 主动连接。最好使用 LACP ，因为它会在交换机之间添加协商和日志记录功能。由于网络是为 vPC 设置的，因此，通过这种方法，您可以将主动 - 主动连接从存储连接到不同的物理交换机。每个控制器与每个交换机之间都有两条链路。但是，所有四个链路都属于同一个 vPC 和接口组（ IFGRP ）。

在配置模式（`config t`）下，对每个交换机运行以下命令，为连接到 NetApp AFF 控制器的端口配置各个接口以及生成的端口通道配置。

1. 在交换机 A 和交换机 B 上运行以下命令，为存储控制器 A 配置端口通道：

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. 在交换机 A 和交换机 B 上运行以下命令，为存储控制器 B 配置端口通道

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```

> 在此解决方案验证中，使用的 MTU 为 9000 。但是，根据应用程序要求，您可以配置适当的 MTU 值。在整个 FlexPod 解决方案中设置相同的 MTU 值非常重要。组件之间的 MTU 配置不正确将导致数据包和这些数据包被丢弃。

配置服务器连接

Cisco UCS 服务器具有一个双端口虚拟接口卡 VIC1387 ，用于数据流量以及使用 iSCSI 启动 ESXi 操作系统。这些接口配置为相互故障转移，可在单链路之外提供额外冗余。通过将这些链路分布在多个交换机上，即使在交换机完全发生故障时，服务器也能正常运行。

在配置模式（`config t`）下，运行以下命令，为连接到每个服务器的接口配置端口设置。

Cisco Nexus 交换机 A： Cisco UCS Server-A 和 Cisco UCS Server-B 配置

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu9216
  no shut
exit
copy run start
```

Cisco Nexus 交换机 B： Cisco UCS Server-A 和 Cisco UCS Server-B 配置

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

在此解决方案验证中，使用的 MTU 为 9000 。但是，根据应用程序要求，您可以配置适当的 MTU 值。在整个 FlexPod 解决方案中设置相同的 MTU 值非常重要。组件之间的 MTU 配置不正确将导致数据包被丢弃，需要重新传输这些数据包。这将影响解决方案的整体性能。

要通过添加更多 Cisco UCS 服务器来扩展解决方案，请使用交换机 A 和 B 上新添加的服务器所插入的交换机端口运行上述命令

通过上行链路连接到现有网络基础架构

根据可用的网络基础架构，可以使用多种方法和功能来上行链路连接 FlexPod 环境。如果存在现有的 Cisco Nexus 环境， NetApp 建议使用 vPC 通过上行链路将 FlexPod 环境中的 Cisco Nexus 3172P 交换机连接到基础架构中。对于 10GbE 基础架构解决方案，上行链路可以是 10GbE 上行链路，如果需要，上行链路可以是 1GbE 基础架构解决方案。可以使用上述过程创建到现有环境的上行链路 vPC 。配置完成后，请务必运行 copy run start 在每个交换机上保存配置。

"下一步： NetApp 存储部署操作步骤（第 1 部分）"

NetApp 存储部署操作步骤（第 1 部分）

本节介绍 NetApp AFF 存储部署操作步骤。

NetApp 存储控制器 AFF2 xx 系列安装

NetApp Hardware Universe

NetApp Hardware Universe （ HWU ）应用程序可为任何特定 ONTAP 版本提供受支持的硬件和软件组件。它提供了 ONTAP 软件当前支持的所有 NetApp 存储设备的配置信息。此外，还提供了一个组件兼容性表。

确认要安装的 ONTAP 版本支持您要使用的硬件和软件组件：

1. 访问 "HWU" 应用程序以查看系统配置指南。单击控制器选项卡以查看不同版本的 ONTAP 软件与符合所需规格的 NetApp 存储设备之间的兼容性。
2. 或者，要按存储设备比较组件，请单击比较存储系统。

控制器 **AFFXX** 系列的前提条件
要规划存储系统的物理位置，请参见 NetApp Hardware Universe 。请参阅以下部分：电气要求，支持的电源线以及板载端口和缆线。

存储控制器

按照中控制器的物理安装过程进行操作 "AFF A220 文档"。

NetApp ONTAP 9.4

配置工作表

在运行设置脚本之前，请填写产品手册中的配置工作表。中提供了配置工作表 "《 ONTAP 9.4 软件设置指南》"。

> 此系统在双节点无交换机集群配置中设置。

下表显示了 ONTAP 9.4 的安装和配置信息。

集群详细信息	集群详细信息值
集群节点 A IP 地址	<<var_nodeA_mgmt_ip>>
集群节点 A 网络掩码	<<var_nodeA_mgmt_mask>>
集群节点 A 网关	<<var_nodeA_mgmt_gateway>>
集群节点 A 名称	<<var_nodeA>>
集群节点 B IP 地址	<<var_nodeB_mgmt_ip>>
集群节点 B 网络掩码	<<var_nodeB_mgmt_mask>>
集群节点 B 网关	<<var_nodeB_mgmt_gateway>>
集群节点 B 名称	<<var_nodeB>>

集群详细信息	集群详细信息值
ONTAP 9.4 URL	<<var_url_boot_software>>
集群的名称	<<var_clustername>>
集群管理 IP 地址	<<var_clustermgmt_ip>>
集群 B 网关	<<var_clustermgmt_gateway>>
集群 B 网络掩码	<<var_clustermgmt_mask>>
域名	<<var_domain_name>>
DNS 服务器 IP （您可以输入多个）	<<var_dns_server_ip>>
NTP 服务器 IP （您可以输入多个）	<<var_ntp_server_ip>>

配置节点 **A**

要配置节点 A ，请完成以下步骤：

1. 连接到存储系统控制台端口。您应看到 Loader-A 提示符。但是，如果存储系统处于重新启动循环中，请在看到以下消息时按 Ctrl-C 退出自动启动循环：

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. 允许系统启动。

```
autoboot
```

3. 按 Ctrl-C 进入启动菜单。

   如果 ONTAP 9.4 不是要启动的软件版本，请继续执行以下步骤以安装新软件。如果要启动的是 ONTAP 9.4 版本，请选择选项 8 和 y 以重新启动节点。然后，继续执行步骤 14 。

4. 要安装新软件，请选择选项 `7` 。
5. 输入 `y` 执行升级。
6. 为要用于下载的网络端口选择 `e0M` 。
7. 输入 `y` 立即重新启动。
8. 在相应位置输入 e0M 的 IP 地址，网络掩码和默认网关。

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. 输入可在其中找到软件的 URL 。

   ⓘ 此 Web 服务器必须可执行 Ping 操作。

```
<<var_url_boot_software>>
```

10. 按 Enter 输入用户名，表示无用户名。
11. 输入 `y` 将新安装的软件设置为后续重新启动所使用的默认软件。
12. 输入 `y` 以重新启动节点。

    安装新软件时，系统可能会对 BIOS 和适配器卡执行固件升级，从而导致重新启动，并可能在 Loader-A 提示符处停止。如果发生这些操作，系统可能会与此操作步骤有所偏差。

13. 按 Ctrl-C 进入启动菜单。
14. 为 Clean Configuration 和 Initialize All Disks 选择选项 `4` 。
15. 输入 `y` 将磁盘置零，重置配置并安装新的文件系统。
16. 输入 `y` 以擦除磁盘上的所有数据。

    根聚合的初始化和创建可能需要 90 分钟或更长时间才能完成，具体取决于所连接磁盘的数量和类型。初始化完成后，存储系统将重新启动。请注意， SSD 初始化所需的时间要少得多。您可以在节点 A 的磁盘置零时继续进行节点 B 配置。

17. 在节点 A 初始化期间，开始配置节点 B

配置节点 **B**

要配置节点 B ，请完成以下步骤：

1. 连接到存储系统控制台端口。您应看到 Loader-A 提示符。但是，如果存储系统处于重新启动循环中，请在看到以下消息时按 Ctrl-C 退出自动启动循环：

    ```
    Starting AUTOBOOT press Ctrl-C to abort…
    ```

2. 按 Ctrl-C 进入启动菜单。

    ```
    autoboot
    ```

3. 出现提示时，按 Ctrl-C 。

    如果 ONTAP 9.4 不是要启动的软件版本，请继续执行以下步骤以安装新软件。如果要启动的是 ONTAP 9.4 版本，请选择选项 8 和 y 以重新启动节点。然后，继续执行步骤 14 。

4. 要安装新软件，请选择选项 7 。
5. 输入 `y` 执行升级。
6. 为要用于下载的网络端口选择 `e0M` 。
7. 输入 `y` 立即重新启动。

8. 在相应位置输入 e0M 的 IP 地址，网络掩码和默认网关。

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. 输入可在其中找到软件的 URL 。

> 此 Web 服务器必须可执行 Ping 操作。

```
<<var_url_boot_software>>
```

10. 按 Enter 输入用户名，表示无用户名。
11. 输入 `y` 将新安装的软件设置为后续重新启动所使用的默认软件。
12. 输入 `y` 以重新启动节点。

    安装新软件时，系统可能会对 BIOS 和适配器卡执行固件升级，从而导致重新启动，并可能在 Loader-A 提示符处停止。如果发生这些操作，系统可能会与此操作步骤有所偏差。

13. 按 Ctrl-C 进入启动菜单。
14. 选择选项 4 以清除配置并初始化所有磁盘。
15. 输入 `y` 将磁盘置零，重置配置并安装新的文件系统。
16. 输入 `y` 以擦除磁盘上的所有数据。

    根聚合的初始化和创建可能需要 90 分钟或更长时间才能完成，具体取决于所连接磁盘的数量和类型。初始化完成后，存储系统将重新启动。请注意， SSD 初始化所需的时间要少得多。

继续执行节点 **A** 配置和集群配置

从连接到存储控制器 A （节点 A ）控制台端口的控制台端口程序中，运行节点设置脚本。首次在节点上启动 ONTAP 9.4 时，将显示此脚本。

> 在 ONTAP 9.4 中，节点和集群设置操作步骤略有变化。现在，集群设置向导用于配置集群中的第一个节点，而 System Manager 用于配置集群。

1. 按照提示设置节点 A

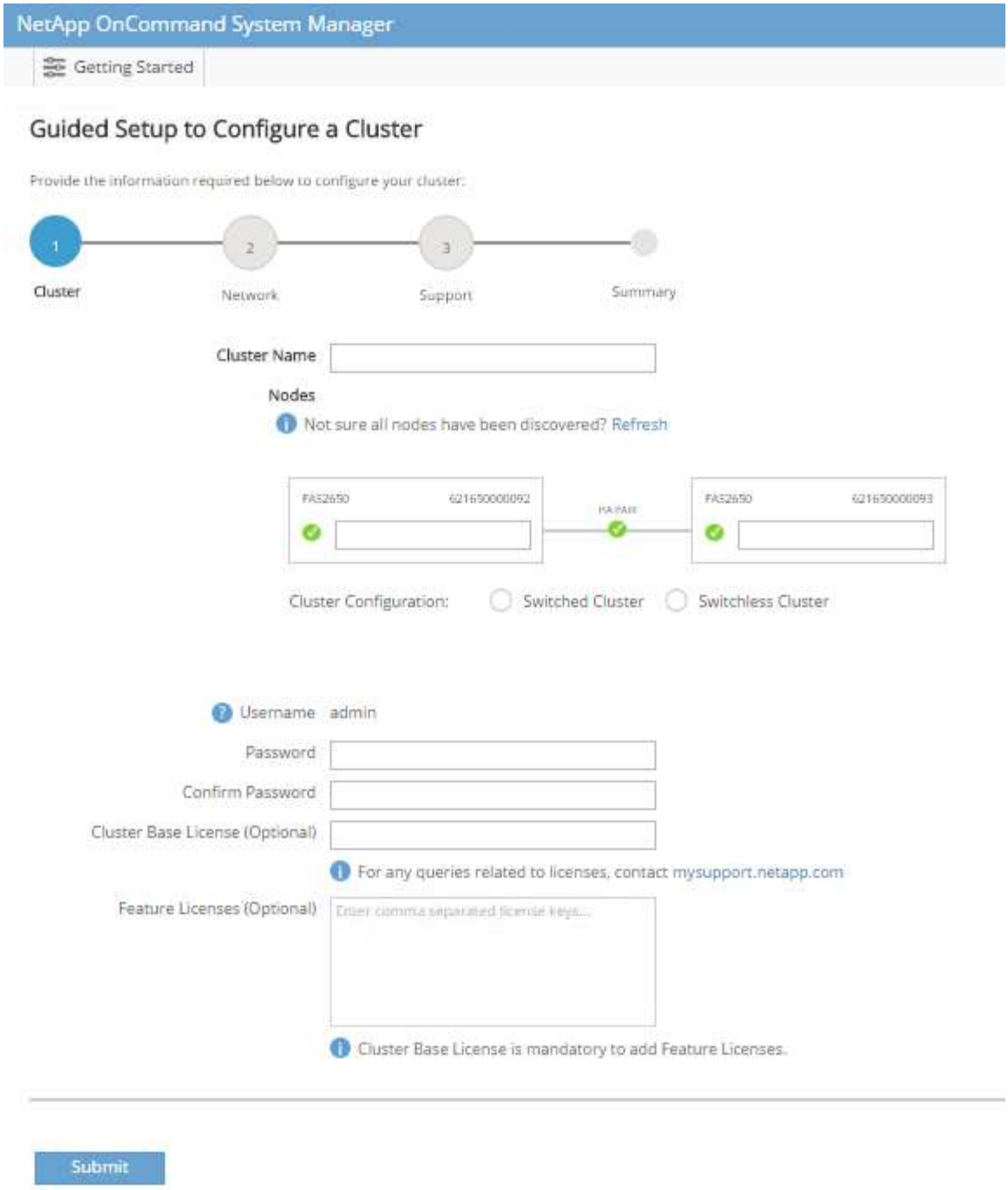
```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. 导航到节点管理接口的 IP 地址。

   也可以使用命令行界面执行集群设置。本文档介绍如何使用 NetApp System Manager 引导式设置进行集群设置。

3. 单击引导式设置以配置集群。

4. 输入 ` <<var_clustername>>` 作为集群名称，并为要配置的每个节点输入 ` <<var_nodeA>>` 和 ` <<var_nodeB>>` 。输入要用于存储系统的密码。选择无交换机集群作为集群类型。输入集群基本许可证。



5. 您还可以输入集群， NFS 和 iSCSI 的功能许可证。
6. 此时将显示一条状态消息，指出正在创建集群。此状态消息会循环显示多个状态。此过程需要几分钟时间。
7. 配置网络。
   a. 取消选择 IP 地址范围选项。
   b. 在集群管理 IP 地址字段中输入 `[var_clustermgmt_ip]` ，在网络掩码字段中输入 `[var_clustermgmt_mask]` ，在网关字段中输入 `[var_clustermgmt_gateway]` 。使用… 选择端口字段中的选择器以选择节点 A 的 e0M
   c. 节点 A 的节点管理 IP 已填充。为节点 B 输入 `<<var_nodeA_mgmt_ip>>`
   d. 在 DNS 域名字段中输入 `<<var_domain_name>>` 。在 DNS Server IP Address 字段中输入 `

<<var_dns_server_ip>>` 。

您可以输入多个 DNS 服务器 IP 地址。

e. 在主 NTP 服务器字段中输入 ` <<var_ntp_server_ip>>` 。

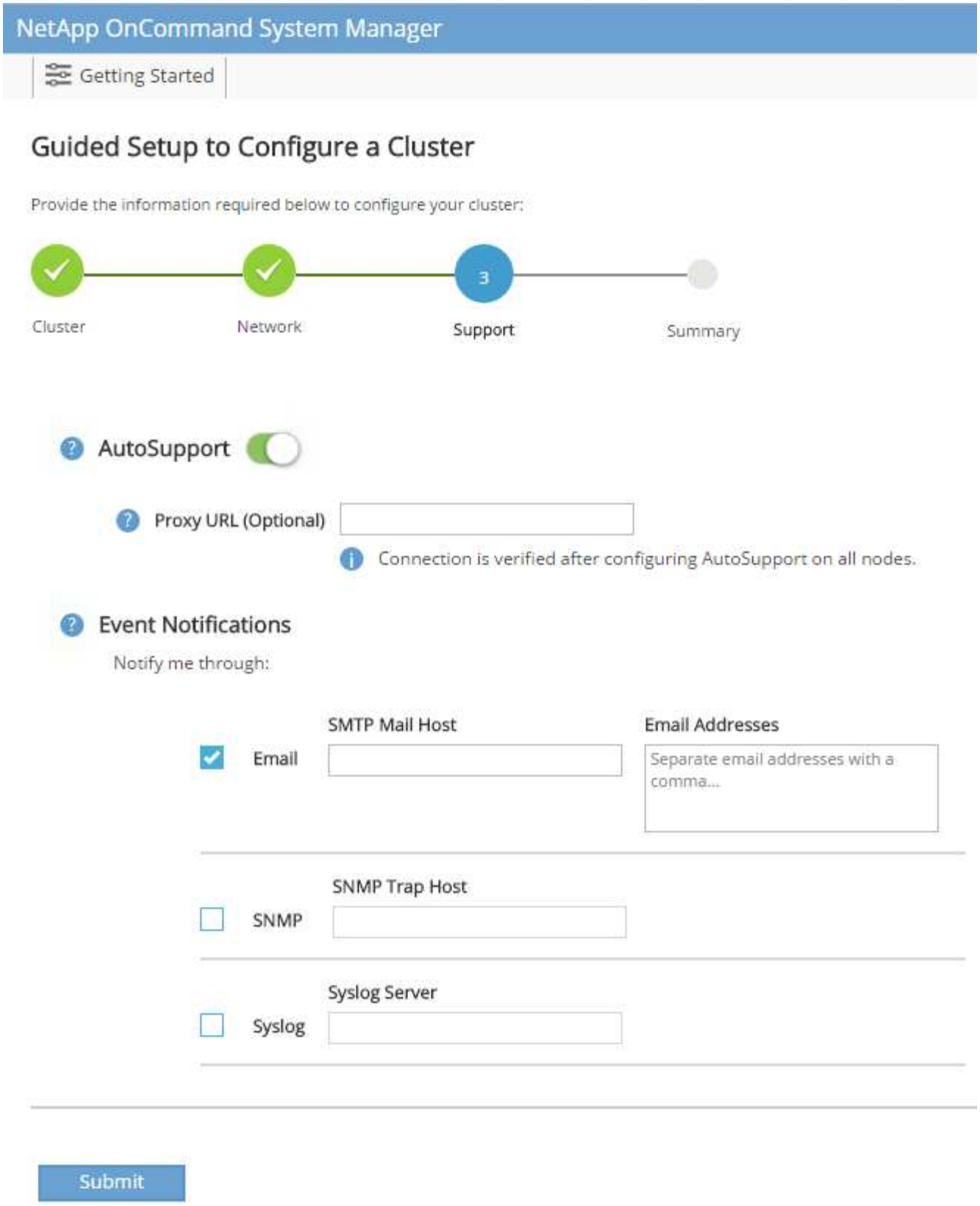
您也可以输入备用 NTP 服务器。

8. 配置支持信息。

a. 如果您的环境需要代理来访问 AutoSupport ，请在代理 URL 中输入 URL 。

b. 输入事件通知的 SMTP 邮件主机和电子邮件地址。

您必须至少设置事件通知方法，然后才能继续操作。您可以选择任何方法。



9. 当指示集群配置已完成时，单击 Manage Your Cluster 以配置存储。

配置存储节点和基础集群后，您可以继续配置存储集群。

将所有备用磁盘置零

要将集群中的所有备用磁盘置零，请运行以下命令：

```
disk zerospares
```

设置板载 UTA2 端口个性化设置

1. 运行 `ucadmin show` 命令，验证端口的当前模式和当前类型。

```
AFF A220::> ucadmin show
                       Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF A220_A     0c       fc       target     -        -          online
AFF A220_A     0d       fc       target     -        -          online
AFF A220_A     0e       fc       target     -        -          online
AFF A220_A     0f       fc       target     -        -          online
AFF A220_B     0c       fc       target     -        -          online
AFF A220_B     0d       fc       target     -        -          online
AFF A220_B     0e       fc       target     -        -          online
AFF A220_B     0f       fc       target     -        -          online
8 entries were displayed.
```

2. 验证正在使用的端口的当前模式是否为 `CNA` ，当前类型是否设置为 **目标** 。如果不是，请使用以下命令更改端口个性化设置：

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

要运行上一个命令，端口必须处于脱机状态。要使端口脱机，请运行以下命令：

```
`network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down`
```

> 如果更改了端口属性，则必须重新启动每个节点，此更改才能生效。

重命名管理逻辑接口（**LIF**）

要重命名管理 LIF，请完成以下步骤：

1. 显示当前管理 LIF 名称。

```
network interface show -vserver <<clustername>>
```

2. 重命名集群管理 LIF。

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_cluster_mgmt_lif_1 -newname cluster_mgmt
```

3. 重命名节点 B 管理 LIF。

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF A220_B_1 -newname AFF A220-02_mgmt1
```

在集群管理上设置自动还原

在集群管理界面上设置 `auto-revert` 参数。

```
network interface modify -vserver <<clustername>> -lif cluster_mgmt -auto-
revert true
```

设置服务处理器网络接口

要为每个节点上的服务处理器分配静态 IPv4 地址，请运行以下命令：

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

服务处理器 IP 地址应与节点管理 IP 地址位于同一子网中。

在 **ONTAP** 中启用存储故障转移

要确认已启用存储故障转移，请在故障转移对中运行以下命令：

1. 验证存储故障转移的状态。

```
storage failover show
```

` [var_nodeA]` 和 ` [var_nodeB]` 都必须能够执行接管。如果节点可以执行接管，请转至步骤 3 。

2. 在两个节点之一上启用故障转移。

```
storage failover modify -node <<var_nodeA>> -enabled true
```

在一个节点上启用故障转移后，这两个节点都可以进行故障转移。

3. 验证双节点集群的 HA 状态。

此步骤不适用于具有两个以上节点的集群。

```
cluster ha show
```

4. 如果配置了高可用性，请转至步骤 6 。如果配置了高可用性，则在发出命令时会显示以下消息：

```
High Availability Configured: true
```

5. 仅为双节点集群启用 HA 模式。

> 请勿对具有两个以上节点的集群运行此命令，因为它会导致故障转移出现问题。

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. 验证是否已正确配置硬件辅助，并根据需要修改配对 IP 地址。

```
storage failover hwassist show
```

消息 保活状态：错误：未收到配对节点发出的 `hwassist` 保活警报 表示未配置硬件协助。运行以下命令以配置硬件辅助。

```
storage failover modify -hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify -hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

在 **ONTAP** 中创建巨型帧 **MTU** 广播域

要创建 MTU 为 9000 的数据广播域，请运行以下命令：

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

从默认广播域中删除数据端口

10GbE 数据端口用于 iSCSI/NFS 流量，这些端口应从默认域中删除。不使用端口 e0e 和 e0f ，也应从默认域中删除。

要从广播域中删除端口，请运行以下命令：

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

禁用 **UTA2** 端口上的流量控制

NetApp 最佳实践是，在连接到外部设备的所有 UTA2 端口上禁用流量控制。要禁用流量控制，请运行以下命令：

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```

在 ONTAP 中配置 IFGRP LACP

此类型的接口组需要两个或更多以太网接口以及一个支持 LACP 的交换机。确保交换机配置正确。

在集群提示符处，完成以下步骤。

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

在 **NetApp ONTAP** 中配置巨型帧

要将 ONTAP 网络端口配置为使用巨型帧（ MTU 通常为 9， 000 字节），请从集群 Shell 运行以下命令：

```
AFF A220::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

在 **ONTAP** 中创建 **VLAN**

要在 ONTAP 中创建 VLAN，请完成以下步骤：

1. 创建 NFS VLAN 端口并将其添加到数据广播域。

   ```
   network port vlan create -node <<var_nodeA>> -vlan-name a0a-
   <<var_nfs_vlan_id>>
   network port vlan create -node <<var_nodeB>> -vlan-name a0a-
   <<var_nfs_vlan_id>>
   broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
   <<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
   <<var_nfs_vlan_id>>
   ```

2. 创建 iSCSI VLAN 端口并将其添加到数据广播域。

```
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. 创建 MGMT-VLAN 端口。

```
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

在 **ONTAP** 中创建聚合

在 ONTAP 设置过程中，将创建一个包含根卷的聚合。要创建其他聚合，请确定聚合名称，要创建聚合的节点及其包含的磁盘数。

要创建聚合，请运行以下命令：

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

在配置中至少保留一个磁盘（选择最大的磁盘）作为备用磁盘。最佳做法是，每个磁盘类型和大小至少有一个备用磁盘。

从五个磁盘开始；您可以在需要额外存储时向聚合添加磁盘。

在磁盘置零完成之前，无法创建聚合。运行 `aggr show` 命令以显示聚合创建状态。在 `aggr1` _`nodeA` 联机之前，请勿继续操作。

在 ONTAP 中配置时区

要配置时间同步并设置集群上的时区，请运行以下命令：

```
timezone <<var_timezone>>
```

> 例如，在美国东部，时区为 `America/New York`。开始键入时区名称后，按 Tab 键查看可用选项。

在 ONTAP 中配置 SNMP

要配置 SNMP ，请完成以下步骤：

1. 配置 SNMP 基本信息，例如位置和联系人。轮询时，此信息在 SNMP 中显示为 `sysLocation` 和 `sysContact` 变量。

   ```
   snmp contact <<var_snmp_contact>>
   snmp location "<<var_snmp_location>>"
   snmp init 1
   options snmp.enable on
   ```

2. 配置 SNMP 陷阱以发送到远程主机。

   ```
   snmp traphost add <<var_snmp_server_fqdn>>
   ```

在 ONTAP 中配置 SNMPv1

要配置 SNMPv1 ，请设置名为社区的共享机密纯文本密码。

```
snmp community add ro <<var_snmp_community>>
```

> 请谨慎使用 `snmp community delete all` 命令。如果社区字符串用于其他监控产品，则此命令会将其删除。

在 ONTAP 中配置 SNMPv3

SNMPv3 要求您定义并配置用户进行身份验证。要配置 SNMPv3 ，请完成以下步骤：

1. 运行 `security snmpusers` 命令以查看引擎 ID 。
2. 创建名为 `snmpv3user` 的用户。

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. 输入权威实体的引擎 ID ，然后选择 `mD5` 作为身份验证协议。
4. 出现提示时，输入身份验证协议的最小长度为八个字符的密码。
5. 选择 `des` 作为隐私协议。
6. 出现提示时，输入隐私协议的最小长度为八个字符的密码。

在 ONTAP 中配置 AutoSupport HTTPS

NetApp AutoSupport 工具通过 HTTPS 向 NetApp 发送支持摘要信息。要配置 AutoSupport ，请运行以下命令：

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

创建 Storage Virtual Machine

要创建基础架构 Storage Virtual Machine （ SVM ），请完成以下步骤：

1. 运行 `vserver create` 命令。

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. 将数据聚合添加到 NetApp VSC 的 infra-sVM 聚合列表中。

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. 从 SVM 中删除未使用的存储协议，而不使用 NFS 和 iSCSI 。

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. 在 infra-sVM SVM 中启用并运行 NFS 协议。

```
`nfs create -vserver Infra-SVM -udp disabled`
```

5. 打开 NetApp NFS VAAI 插件的 `SVM vStorage` 参数。然后，验证是否已配置 NFS 。

```
`vserver nfs modify -vserver Infra-SVM -vstorage enabled`
`vserver nfs show `
```

命令行中的命令前面带有 `vserver` ，因为 Storage Virtual Machine 以前称为服务器。

在 ONTAP 中配置 NFSv3

下表列出了完成此配置所需的信息。

详细信息	详细信息值
ESXi 主机 A NFS IP 地址	<<var_esxi_HostA_NFS_IP>>
ESXi 主机 B NFS IP 地址	<<var_esxi_HostB_NFS_IP>>

要在 SVM 上配置 NFS ，请运行以下命令：

1. 在默认导出策略中为每个 ESXi 主机创建一个规则。
2. 为要创建的每个 ESXi 主机分配一个规则。每个主机都有自己的规则索引。第一个 ESXi 主机的规则索引为 1 ，第二个 ESXi 主机的规则索引为 2 ，依此类推。

```
vserver export-policy rule create -vserver Infra-SVM -policyname default
-ruleindex 1 -protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys -rwrule sys -superuser sys -allow-suid false
vserver export-policy rule create -vserver Infra-SVM -policyname default
-ruleindex 2 -protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys -rwrule sys -superuser sys -allow-suid false
vserver export-policy rule show
```

3. 将导出策略分配给基础架构 SVM 根卷。

```
volume modify -vserver Infra-SVM -volume rootvol -policy default
```

如果您选择在设置 vSphere 后安装导出策略，则 NetApp VSC 会自动处理导出策略。如果不安装此服务器，则必须在添加其他 Cisco UCS C 系列服务器时创建导出策略规则。

在 ONTAP 中创建 iSCSI 服务

要创建 iSCSI 服务，请完成以下步骤：

1. 在 SVM 上创建 iSCSI 服务。此命令还会启动 iSCSI 服务并为 SVM 设置 iSCSI IQN 。验证是否已配置 iSCSI 。

```
iscsi create -vserver Infra-SVM
iscsi show
```

在 **ONTAP** 中创建 **SVM** 根卷的负载共享镜像

1. 在每个节点上创建一个卷作为基础架构 SVM 根卷的负载共享镜像。

```
volume create -vserver Infra_Vserver -volume rootvol_m01 -aggregate
aggr1_nodeA -size 1GB -type DP
volume create -vserver Infra_Vserver -volume rootvol_m02 -aggregate
aggr1_nodeB -size 1GB -type DP
```

2. 创建作业计划，以便每 15 分钟更新一次根卷镜像关系。

```
job schedule interval create -name 15min -minutes 15
```

3. 创建镜像关系。

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. 初始化镜像关系并验证它是否已创建。

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

在 **ONTAP** 中配置 **HTTPS** 访问

要配置对存储控制器的安全访问，请完成以下步骤：

1. 提高访问证书命令的权限级别。

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. 通常，已有自签名证书。运行以下命令以验证证书：

```
security certificate show
```

3. 对于所示的每个 SVM ，证书公用名应与 SVM 的 DNS FQDN 匹配。四个默认证书应被删除，并替换为自签名证书或证书颁发机构提供的证书。

   最好在创建证书之前删除已过期的证书。运行 `security certificate delete` 命令删除已过期的证书。在以下命令中，使用 Tab completion 选择并删除每个默认证书。

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. 要生成并安装自签名证书，请一次性运行以下命令。为 infra-sVM 和集群 SVM 生成服务器证书。同样，请使用 Tab completion 帮助完成这些命令。

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm. netapp.com
-type  server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. 要获取以下步骤中所需参数的值，请运行 `security certificate show` 命令。
6. 使用 ` – server-enabled true` 和 ` – client-enabled false` 参数启用刚刚创建的每个证书。同样，请使用 Tab 补全。

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. 配置并启用 SSL 和 HTTPS 访问以及禁用 HTTP 访问。

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be
         interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

其中某些命令通常会返回一条错误消息，指出此条目不存在。

8. 还原到管理员权限级别并创建设置以允许 Web 使用 SVM 。

```
set -privilege admin
vserver services web modify -name spi|ontapi|compat -vserver * -enabled
true
```

在 ONTAP 中创建 NetApp FlexVol 卷

要创建 NetApp FlexVol 卷，请输入卷名称，大小及其所在的聚合。创建两个 VMware 数据存储库卷和一个服务器启动卷。

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB -state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

在 ONTAP 中启用重复数据删除

要在相应的卷上启用重复数据删除，请运行以下命令：

```
volume efficiency on -vserver Infra-SVM -volume infra_datastore_1
volume efficiency on -vserver Infra-SVM -volume esxi_boot
```

在 ONTAP 中创建 LUN

要创建两个启动 LUN ，请运行以下命令：

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

添加额外的 Cisco UCS C 系列服务器时，必须创建额外的启动 LUN 。

在 ONTAP 中创建 iSCSI LIF

下表列出了完成此配置所需的信息。

详细信息	详细信息值
存储节点 A iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
存储节点 A iSCSI LIF01A 网络掩码	<<var_nodeA_iscsi_lif01a_mask>>
存储节点 A iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
存储节点 A iSCSI LIF01B 网络掩码	<<var_nodeA_iscsi_lif01b_mask>>
存储节点 B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
存储节点 B iSCSI LIF01A 网络掩码	<<var_nodeB_iscsi_lif01a_mask>>
存储节点 B iSCSI LIF01B	<<var_nodeB_iscsi_lif01b_ip>>
存储节点 B iSCSI LIF01B 网络掩码	<<var_nodeB_iscsi_lif01b_mask>>

1. 创建四个 iSCSI LIF ，每个节点两个。

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

在 ONTAP 中创建 NFS LIF

下表列出了完成此配置所需的信息。

详细信息	详细信息值
存储节点 A NFS LIF 01 IP	<<var_nodeA_nfs_lif_01_ip>>
存储节点 A NFS LIF 01 网络掩码	<<var_nodeA_nfs_lif_01_mask>>
存储节点 B NFS LIF 02 IP	<<var_nodeB_nfs_lif_02_ip>>
存储节点 B NFS LIF 02 网络掩码	<<var_nodeB_nfs_lif_02_mask>>

1. 创建 NFS LIF 。

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up -failover-policy broadcast-
domain-wide -firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up -failover-policy broadcast-
domain-wide -firewall-policy data -auto-revert true
network interface show
```

添加基础架构 **SVM** 管理员

下表列出了完成此配置所需的信息。

详细信息	详细信息值
Vsmgmt IP	<<var_svm_mgmt_ip>>
Vsmgmt 网络掩码	<<var_svm_mgmt_mask>>
Vsmgmt 默认网关	<<var_svm_mgmt_gateway>>

要将基础架构 SVM 管理员和 SVM 管理逻辑接口添加到管理网络，请完成以下步骤：

1. 运行以下命令：

```
network interface create -vserver Infra-SVM -lif vsmgmt -role data
-data-protocol none -home-node <<var_nodeB>> -home-port  e0M -address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
-failover-policy broadcast-domain-wide -firewall-policy mgmt -auto-
revert true
```

> 此处的 SVM 管理 IP 应与存储集群管理 IP 位于同一子网中。

2. 创建一个默认路由，以使 SVM 管理接口能够访问外部环境。

```
network route create -vserver Infra-SVM -destination 0.0.0.0/0 -gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. 为 SVM vsadmin 用户设置密码并解除锁定此用户。

```
security login password -username vsadmin -vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock -username vsadmin -vserver Infra-SVM
```

"接下来： Cisco UCS C 系列机架式服务器部署操作步骤"

Cisco UCS C 系列机架式服务器部署操作步骤

下一节详细介绍了用于配置 Cisco UCS C 系列独立机架服务器以在 FlexPod 快速配置中使用的操作步骤。

对 **Cisco** 集成管理服务器执行初始 **Cisco UCS C** 系列独立服务器设置

完成以下步骤以初始设置 Cisco UCS C 系列独立服务器的 CIMC 接口。

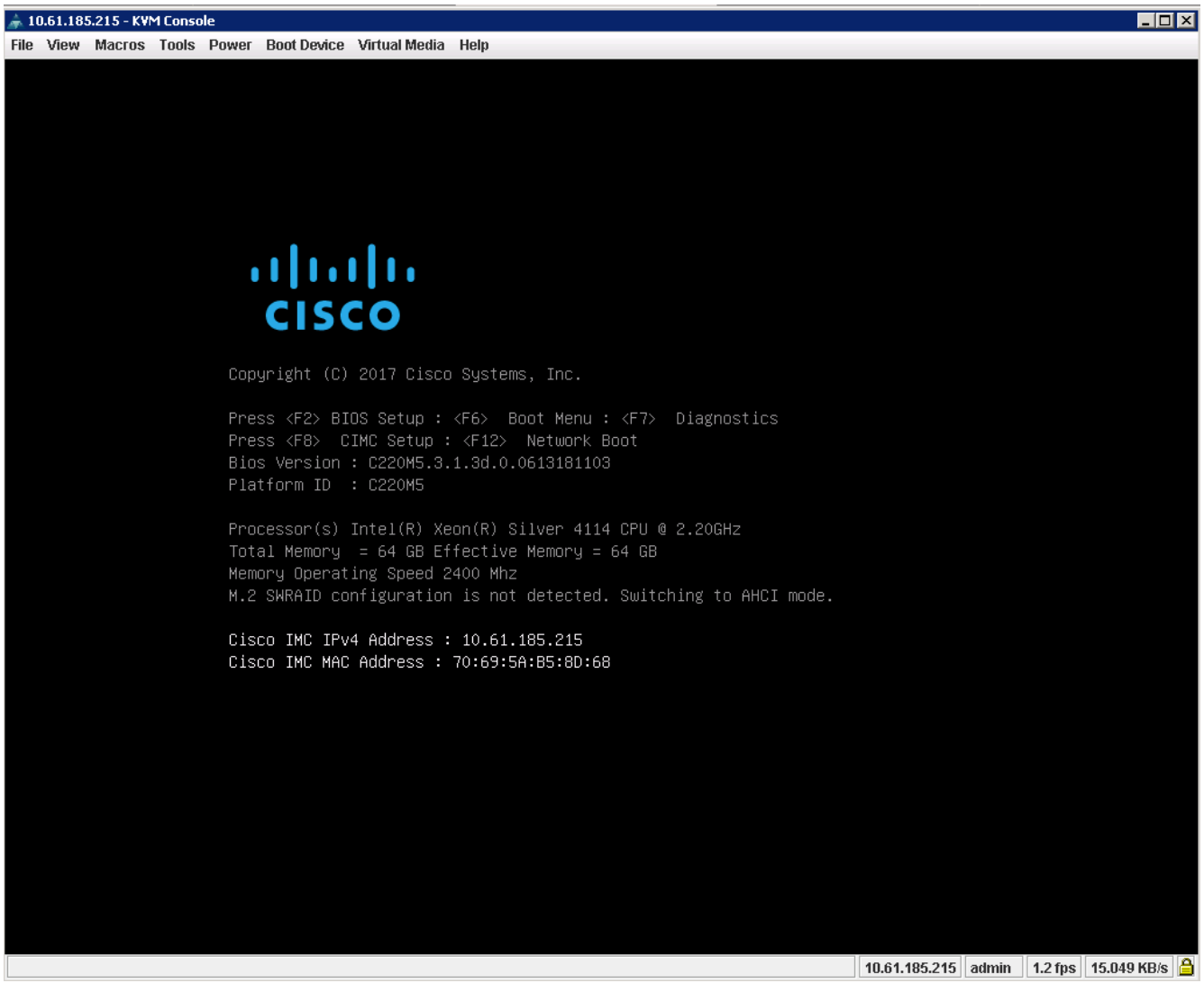
下表列出了为每个 Cisco UCS C 系列独立服务器配置 CIMC 所需的信息。

详细信息	详细信息值
CIMC IP 地址	<<CMC_IP>>
CIMC 子网掩码	<<CIMC 网络掩码 >>
CIMC 默认网关	<<CIMC 网关 >>

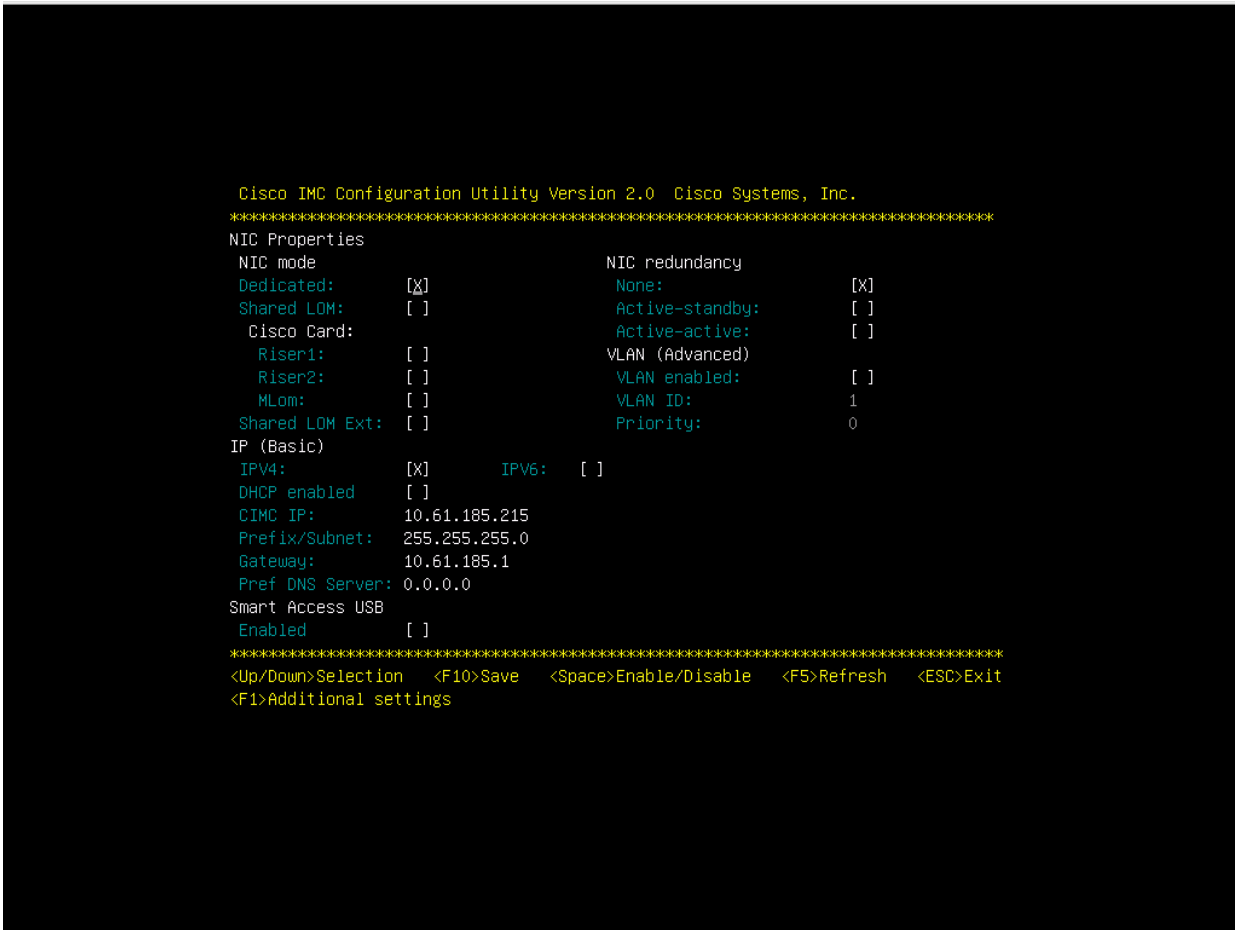
此验证中使用的 CIMC 版本为 CIMC 3.1.3 （ g ）。

所有服务器

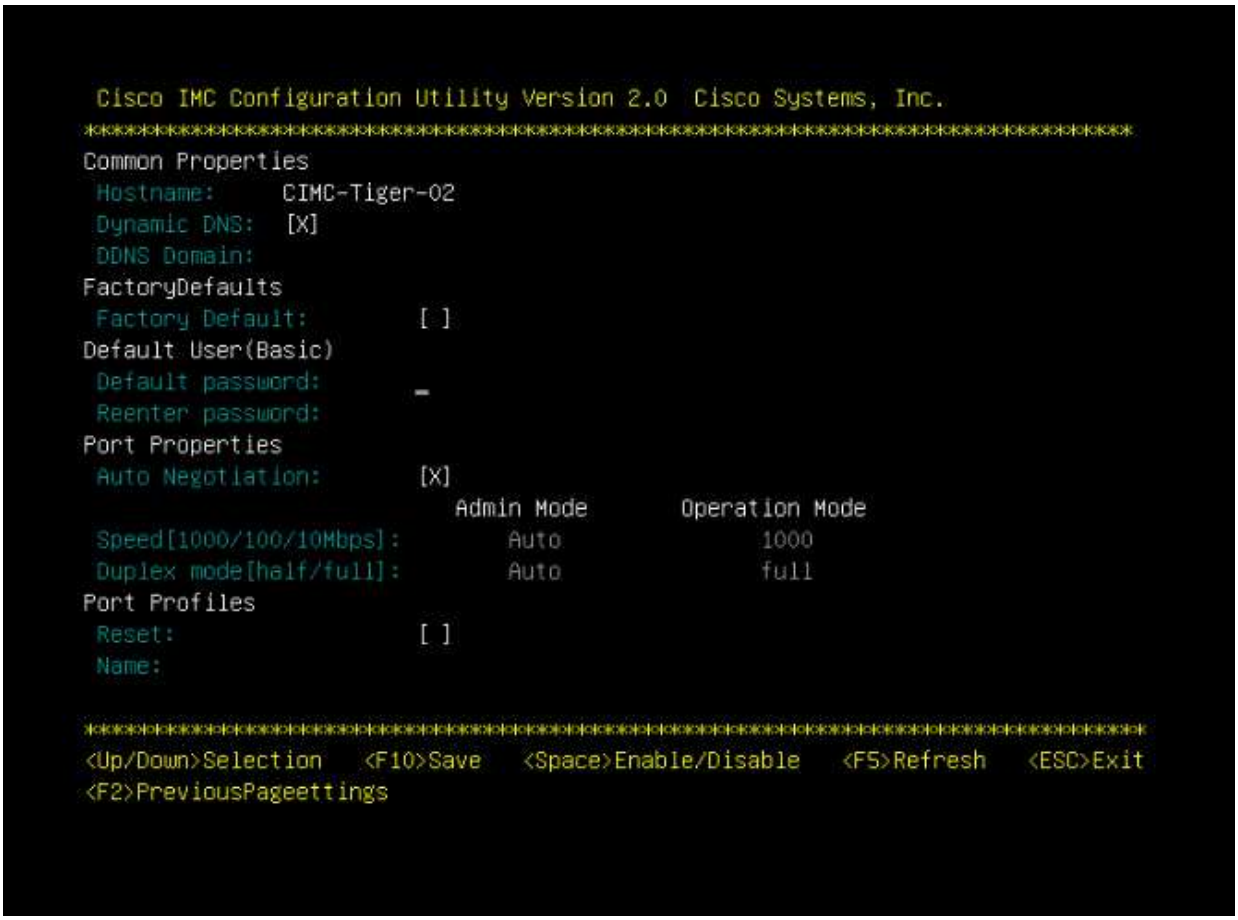
1. 将 Cisco 键盘，视频和鼠标（ KVM ）转换器（随服务器提供）连接到服务器正面的 KVM 端口。将 VGA 显示器和 USB 键盘插入相应的 KVM 转换器端口。
2. 打开服务器电源，在系统提示您输入 CIMC 配置时按 F8 。



3. 在 CIMC 配置实用程序中，设置以下选项：
   - 网络接口卡（ Network Interface Card ， NIC ）模式：
     - 专用 "X"
   - IP （基本）：
     - IPv4： [x]
     - 已启用 DHCP： [ ]
     - CIMC IP： [CIMC IP]
     - 前缀 / 子网： [CIMC _netmask]
     - 网关： [CIMC 网关]
   - VLAN （高级）：保持清除状态以禁用 VLAN 标记。
     - NIC 冗余
     - 无： [x]



4. 按 F1 可查看其他设置。
   - 通用属性：
     - 主机名： [ESXi_host_name]
     - 动态 DNS ： [ ]
     - 出厂默认设置：保持清除状态。
   - 默认用户（基本）：
     - 默认密码： [admin_password]
     - 重新输入密码： [admin_password]
     - 端口属性：使用默认值。
     - 端口配置文件：保持清除状态。



5. 按 F10 保存 CIMC 接口配置。
6. 保存配置后，按 Esc 退出。

配置 Cisco UCS C 系列服务器 iSCSI 启动

在此 FlexPod 快速配置中， VIC1387 用于 iSCSI 启动。

下表列出了配置 iSCSI 启动所需的信息。

> 斜体表示每个 ESXi 主机唯一的变量。

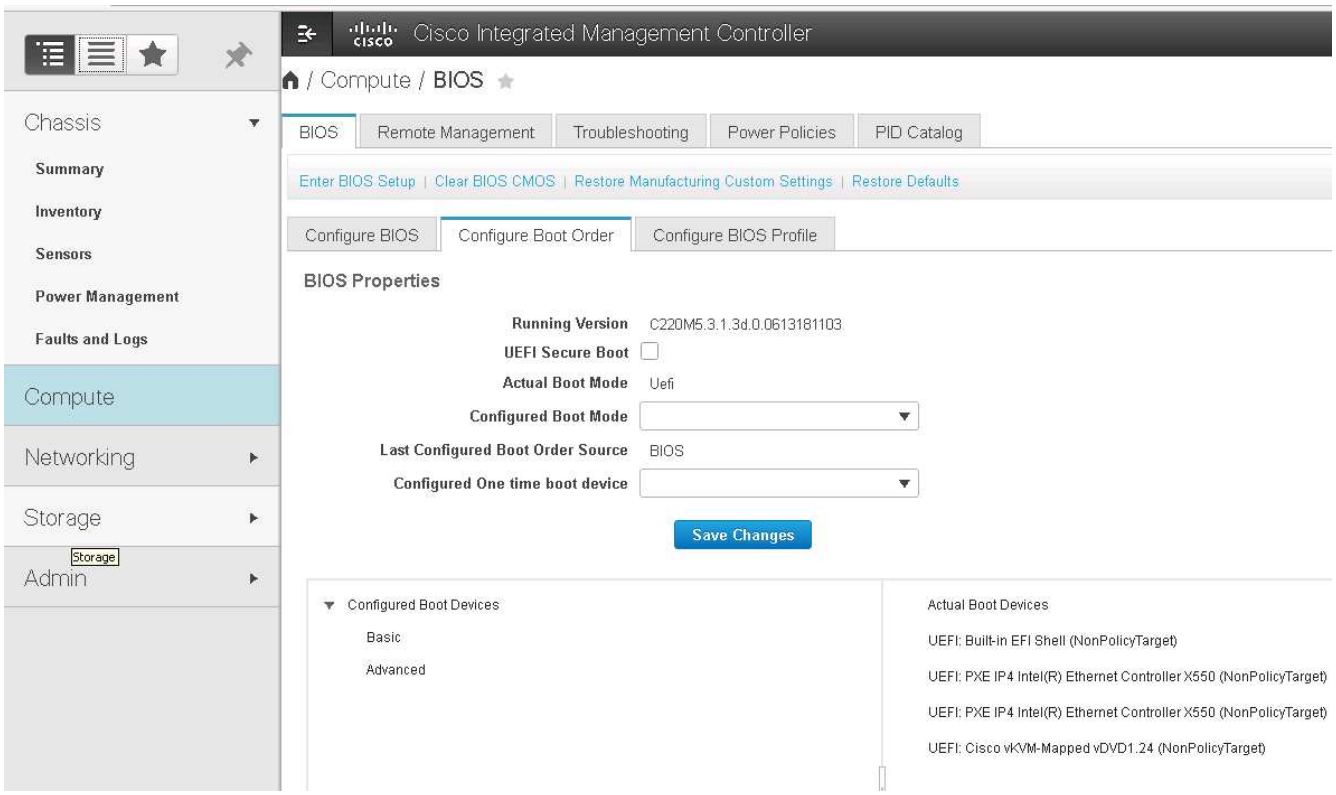
详细信息	详细信息值
ESXi 主机启动程序 A 名称	<<var_UCS_initiator_name_A>>
ESXi 主机 iSCSI-A IP	<<var_esxi_host_iscsiA_IP>>
ESXi 主机 iSCSI-A 网络掩码	<<var_esxi_host_iscsiA_mask>>
ESXi 主机 iSCSI 是默认网关	<<var_esxi_host_iscsiA_gateway>>
ESXi 主机启动程序 B 名称	<<var_UCS_initiator_name_B>>
ESXi 主机 iSCSI-B IP	<<var_esxi_host_iscsiB_ip>>
ESXi 主机 iSCSI-B 网络掩码	<<var_esxi_host_iscsiB_mask>>
ESXi 主机 iSCSI-B 网关	<<var_esxi_host_iscsiB_gateway>>

详细信息	详细信息值
IP 地址 iscsi_lif01a	
IP 地址 iscsi_lif02a	
IP 地址 iscsi_lif01b	
IP 地址 iscsi_lif02b	
infra_sVM IQN	

启动顺序配置

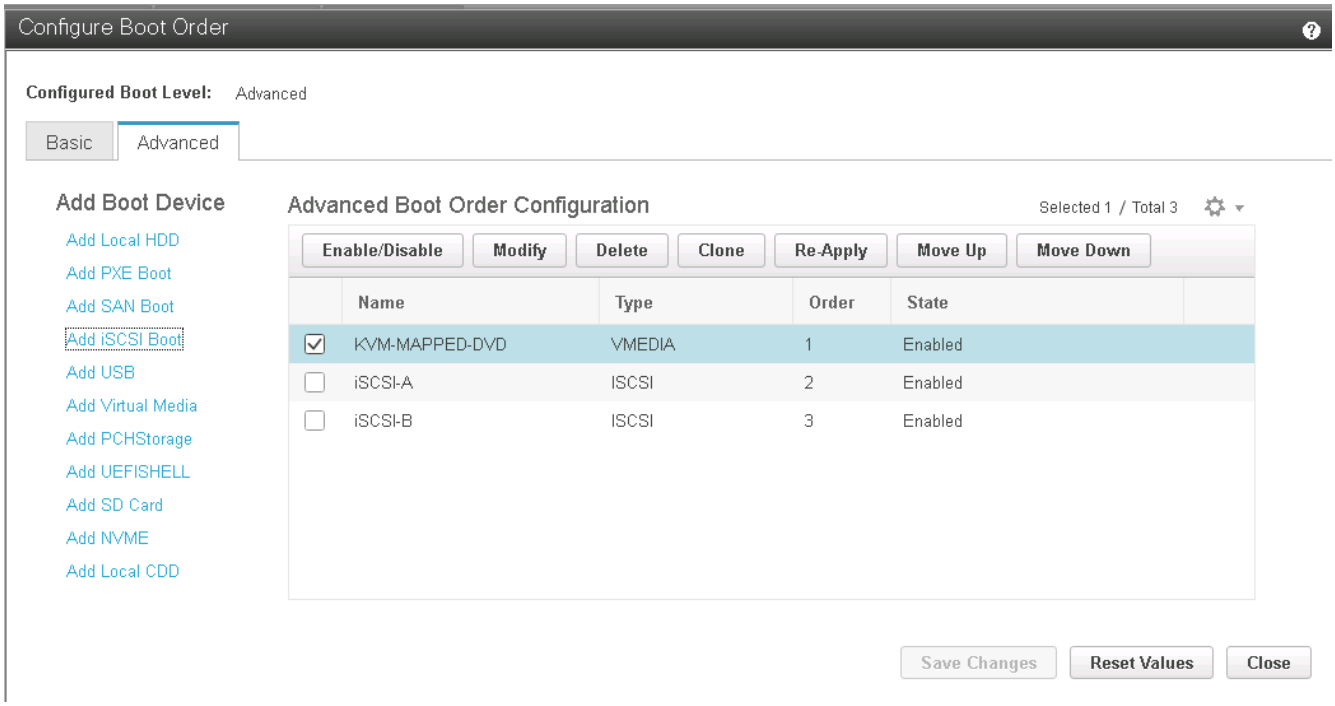
要设置启动顺序配置，请完成以下步骤：

1. 在 CIMC 界面浏览器窗口中，单击 Server 选项卡并选择 BIOS 。
2. 单击 Configure Boot Order ，然后单击 OK 。



3. 通过单击添加启动设备下的设备并转到高级选项卡来配置以下设备。
   - 添加虚拟介质
     - 名称： KVM-CD-DVD
     - 子类型： KVM 映射的 DVD
     - 状态：已启用
     - 顺序： 1
   - 添加 iSCSI 启动。
     - 名称： iscsi-A

    - 状态：已启用
    - 顺序： 2
    - 插槽： MLOM
    - 端口： 0
  - 单击添加 iSCSI 启动。
    - 名称： iSCSI-B
    - 状态：已启用
    - 顺序： 3
    - 插槽： MLOM
    - 端口： 1
4. 单击添加设备。
5. 单击保存更改，然后单击关闭。

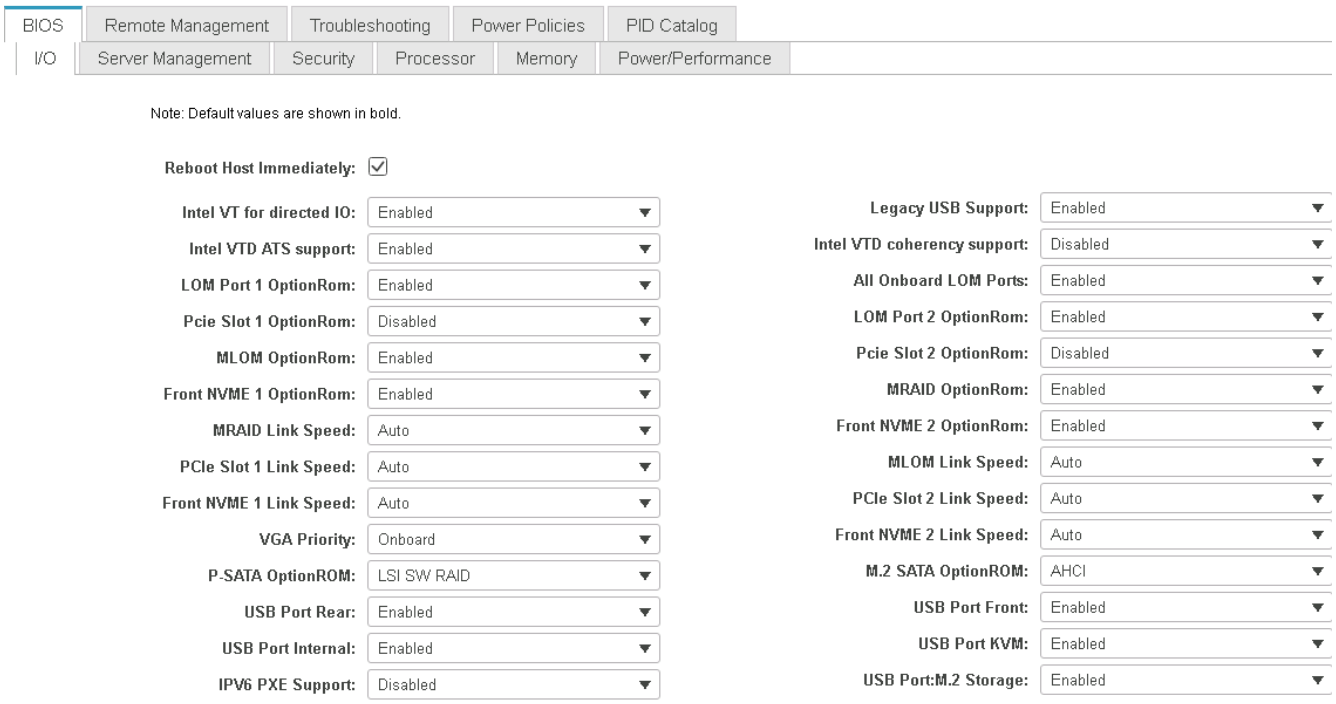


6. 重新启动服务器以使用新的启动顺序启动。

禁用 RAID 控制器（如果存在）

如果 C 系列服务器包含 RAID 控制器，请完成以下步骤。从 SAN 启动配置不需要 RAID 控制器。您也可以从服务器中物理删除 RAID 控制器。

1. 单击 CIMC 左侧导航窗格中的 BIOS 。
2. 选择 Configure BIOS 。
3. 向下滚动到 PCIe 插槽： HBA 选项 ROM 。
4. 如果尚未禁用此值，请将其设置为 disabled 。



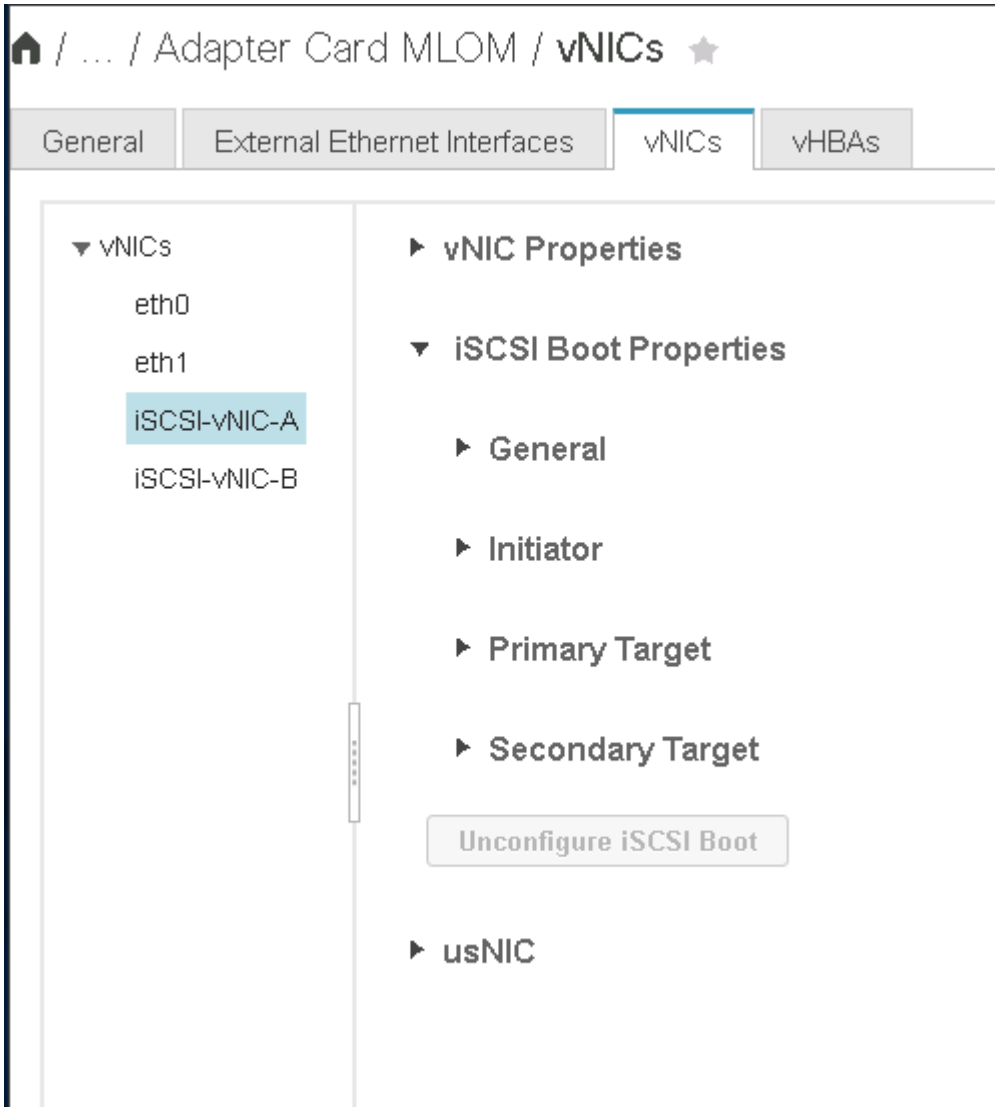
为 **iSCSI** 启动配置 **Cisco VIC1387**

以下配置步骤适用于用于 iSCSI 启动的 Cisco VIC 1387 。

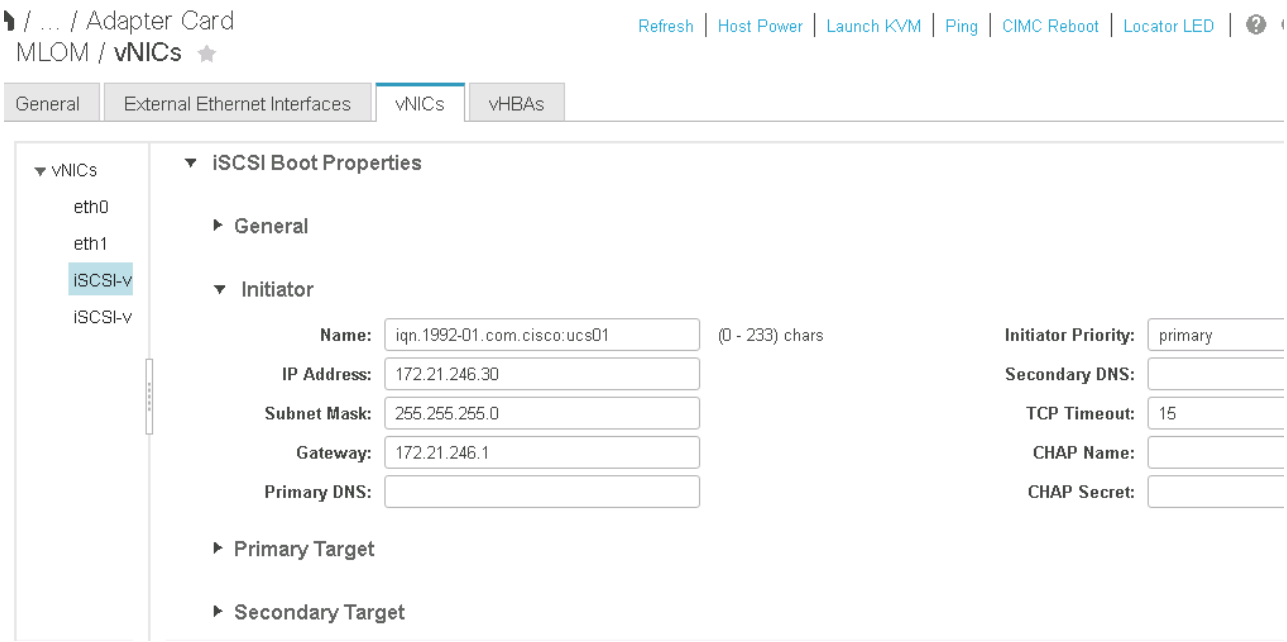
创建 **iSCSI vNIC**

1. 单击添加以创建 vNIC 。
2. 在 Add vNIC 部分中，输入以下设置：
   - 名称： iscsi-vNIC-A
   - MTU： 9000
   - 默认 VLAN： `<<var_iscsi_vlan_A>>`
   - VLAN 模式：中继
   - Enable PXE boot： check

3. 单击添加 vNIC ，然后单击确定。
4. 重复此过程以添加另一个 vNIC 。
   a. 将 vNIC 命名为 `iscsi-vNIC-B` 。
   b. 输入 ` <<var_iscsi_vlan_b>>` 作为 VLAN 。
   c. 将上行链路端口设置为 `1` 。
5. 选择左侧的 vNIC `iscsi-vNIC-A` 。



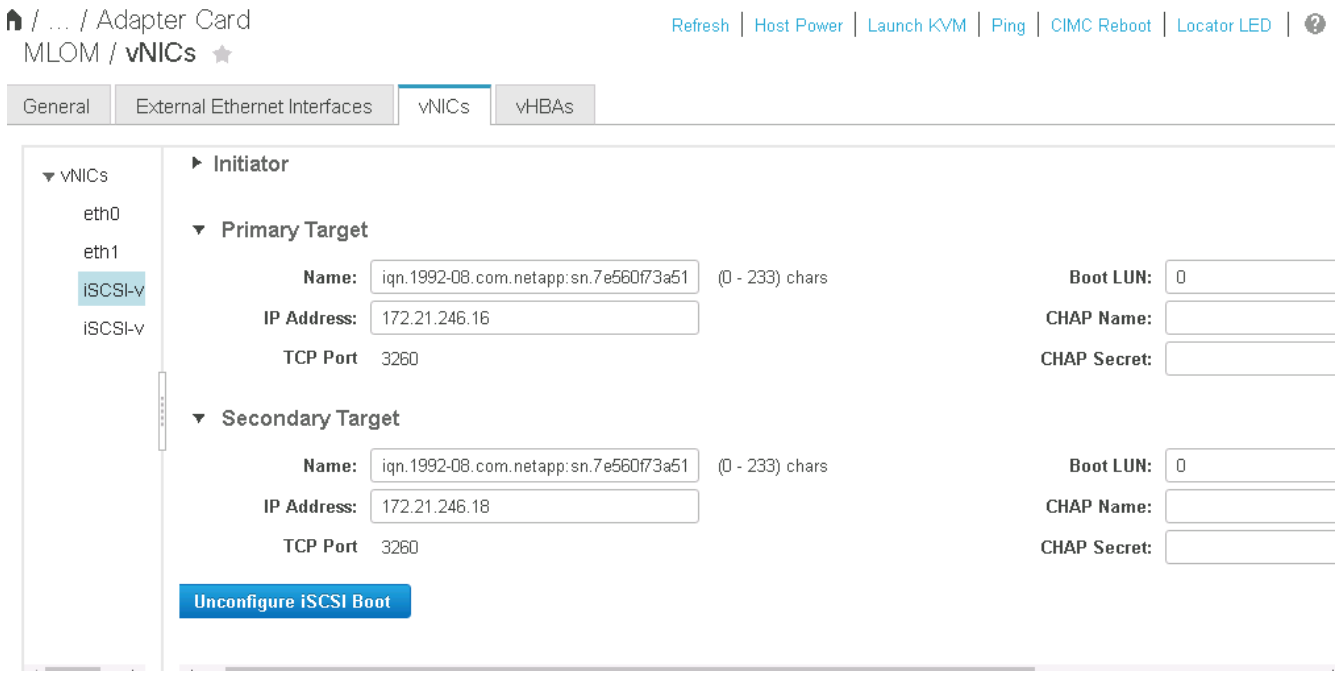
6. 在 "iSCSI 启动属性 " 下，输入启动程序详细信息：
   - 名称： [var_UCSA_initiator_name_A]
   - IP 地址： [var_esxi_HostA_iscsiA_IP]
   - 子网掩码： [var_esxi_HostA_iscsiA_mask]
   - 网关： [var_esxi_HostA_iscsiA_gateway]



7. 输入主目标详细信息。
   - 名称： infra-svm 的 IQN 编号
   - IP 地址： IP 地址 `iscsi_lif01a`
   - 启动 LUN ： 0
8. 输入二级目标详细信息。
   - 名称： infra-svm 的 IQN 编号
   - IP 地址： IP 地址 `iscsi_lif02a`
   - 启动 LUN ： 0

   您可以运行 `vserver iscsi show` 命令来获取存储 IQN 编号。

   请务必记录每个 vNIC 的 IQN 名称。您需要在后续步骤中使用它们。



9. 单击 Configure iSCSI 。
10. 选择 vNIC `iscsi-vNIC- B` ，然后单击主机以太网接口部分顶部的 iSCSI 启动按钮。
11. 重复此过程以配置 `iscsi-vNIC-B` 。
12. 输入启动程序详细信息。
    - 名称： `<<var_UCSA_initiator_name_b>>`
    - IP 地址： `[var_esxi_HostB_iscsib_ip]`
    - 子网掩码： `[var_esxi_HostB_iscsib_mask]`
    - 网关： `[var_esxi_HostB_iscsib_gateway]`
13. 输入主目标详细信息。
    - 名称： infra-svm 的 IQN 编号
    - IP 地址： IP 地址 `iscsi_lif01b`
    - 启动 LUN ： 0
14. 输入二级目标详细信息。
    - 名称： infra-svm 的 IQN 编号
    - IP 地址： IP 地址 `iscsi_lif02b`
    - 启动 LUN ： 0

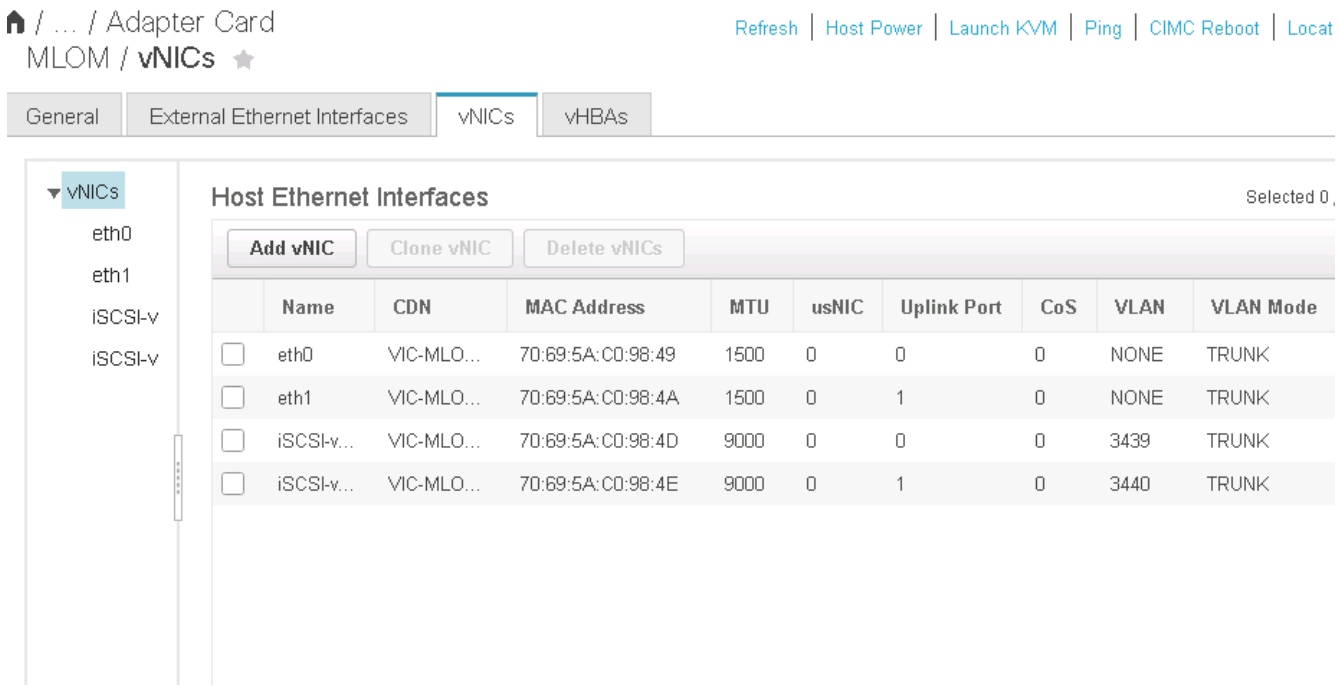
    您可以使用 `vserver iscsi show` 命令获取存储 IQN 编号。

    请务必记录每个 vNIC 的 IQN 名称。您需要在后续步骤中使用它们。

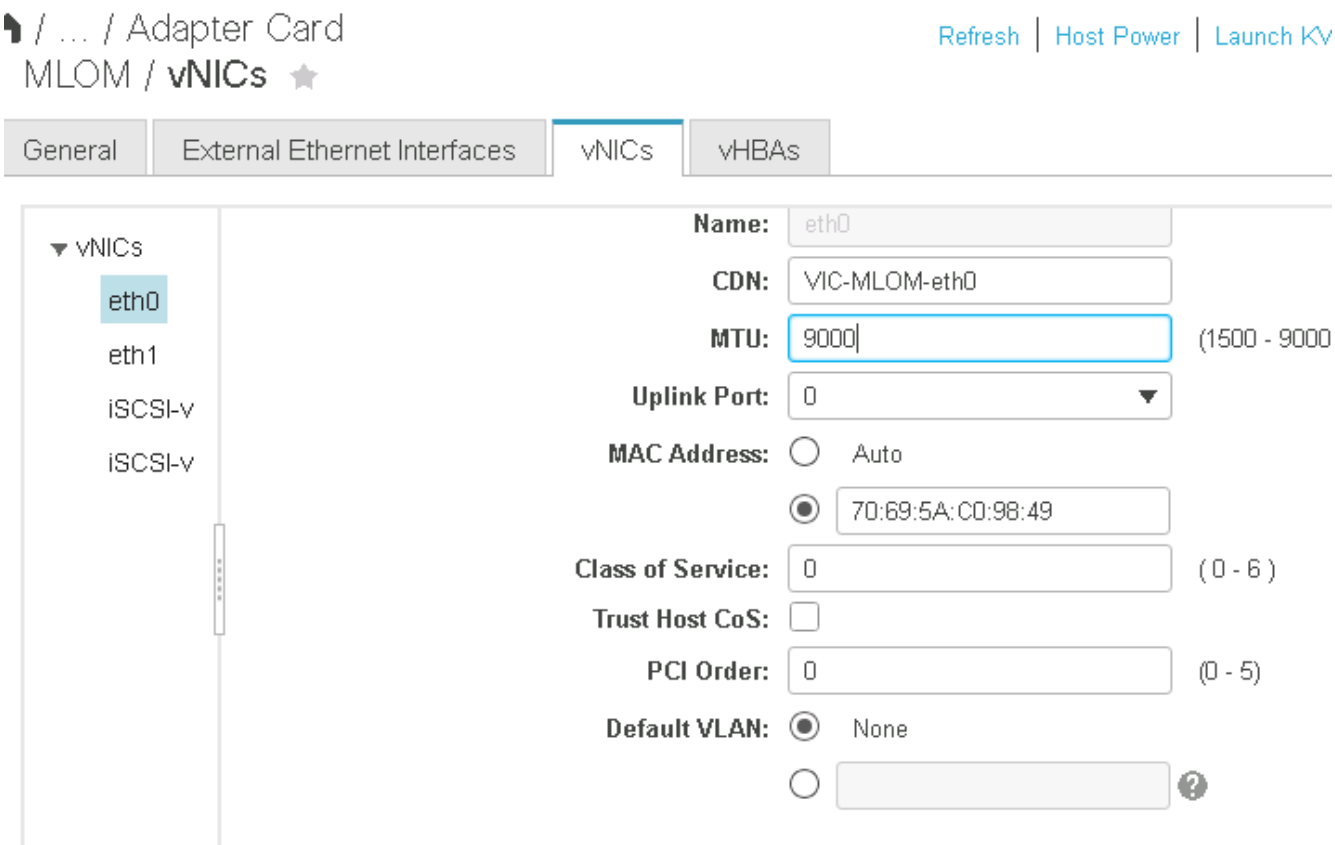
15. 单击 Configure iSCSI 。
16. 重复此过程为 Cisco UCS 服务器 B 配置 iSCSI 启动

为 ESXi 配置 vNIC

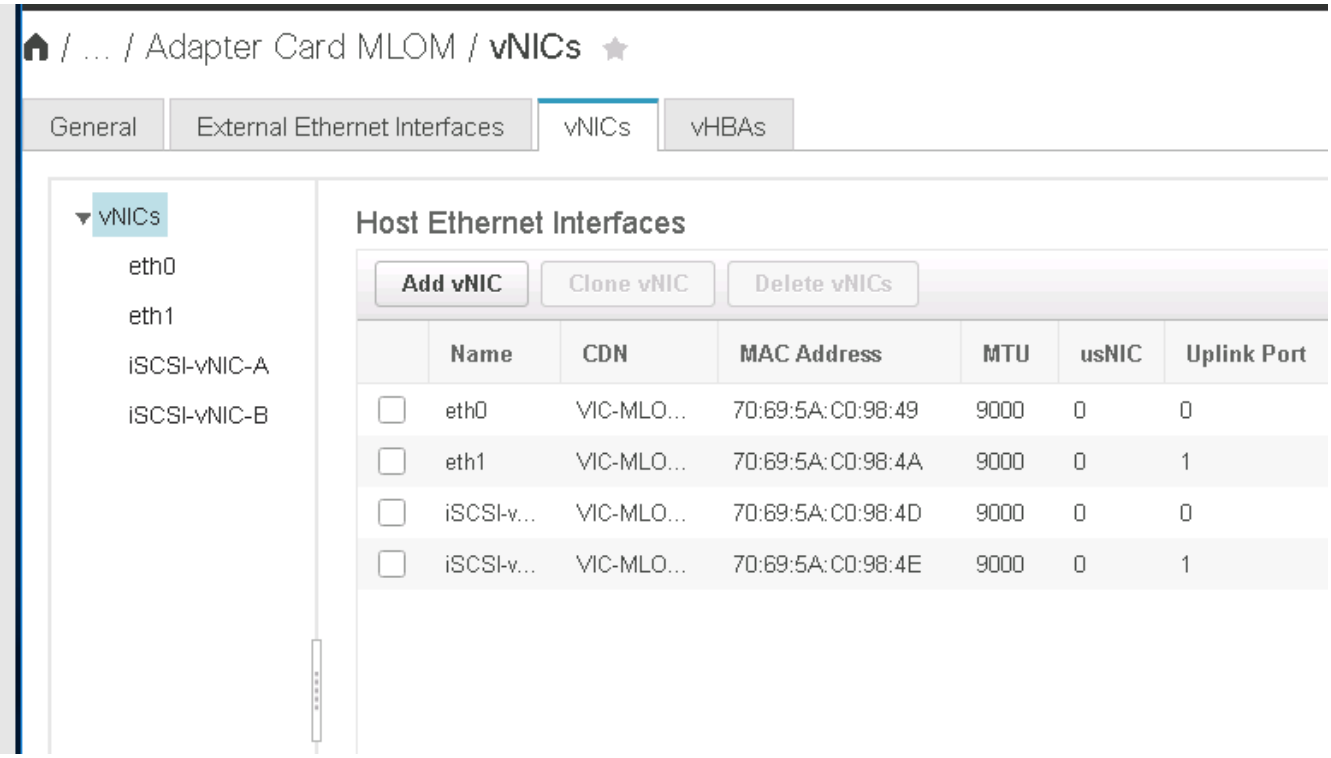
1. 在 CIMC 界面浏览器窗口中，单击清单，然后单击右窗格上的 Cisco VIC 适配器。
2. 在 Adapter Cards 下，选择 Cisco UCS VIC 1387 ，然后选择下面的 vNIC 。



3. 选择 eth0 并单击属性。
4. 将 MTU 设置为 9000 。单击 Save Changes 。



5. 对 eth1 重复步骤 3 和 4 ，验证 eth1 的上行链路端口是否设置为 `1` 。



必须对添加到环境中的每个初始 Cisco UCS 服务器节点和每个额外的 Cisco UCS 服务器节点重复此操作步骤。

"下一步： NetApp AFF 存储部署操作步骤（第 2 部分）"

NetApp AFF 存储部署操作步骤（第 2 部分）

ONTAP SAN 启动存储设置

创建 iSCSI igroup

要创建 igroup ，请完成以下步骤：

在此步骤中，您需要使用服务器配置中的 iSCSI 启动程序 IQN 。

1. 从集群管理节点 SSH 连接中，运行以下命令。要查看在此步骤中创建的三个 igroup ，请运行 igroup show 命令。

```
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-A -protocol iscsi
-ostype vmware -initiator <<var_vm_host_infra_a_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-B -protocol iscsi
-ostype vmware -initiator <<var_vm_host_infra_b_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

> 添加其他 Cisco UCS C 系列服务器时，必须完成此步骤。

将启动 LUN 映射到 igroup

要将启动 LUN 映射到 igroup ，请从集群管理 SSH 连接运行以下命令：

```
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra- A -igroup
VM-Host-Infra- A -lun-id 0
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra- B -igroup
VM-Host-Infra- B -lun-id 0
```

> 添加其他 Cisco UCS C 系列服务器时，必须完成此步骤。

"接下来： VMware vSphere 6.7 部署操作步骤。"

VMware vSphere 6.7 部署操作步骤

本节详细介绍了在 FlexPod 快速配置中安装 VMware ESXi 6.7 的过程。下面的部署过程已进行自定义，以包括前面几节所述的环境变量。

在此类环境中安装 VMware ESXi 的方法有多种。此操作步骤使用适用于 Cisco UCS C 系列服务器的 CIMC 界面的虚拟 KVM 控制台和虚拟介质功能，将远程安装介质映射到每个服务器。

必须为 Cisco UCS 服务器 A 和 Cisco UCS 服务器 B 完成此操作步骤

对于添加到集群中的任何其他节点，必须完成此操作步骤。

登录到 Cisco UCS C 系列独立服务器的 CIMC 界面

以下步骤详细介绍了登录到 Cisco UCS C 系列独立服务器的 CIMC 界面的方法。您必须登录到 CIMC 界面才能运行虚拟 KVM ，管理员可以通过远程介质开始安装操作系统。

所有主机

1. 导航到 Web 浏览器，然后输入 Cisco UCS C 系列的 CIMC 接口的 IP 地址。此步骤将启动 CIMC GUI 应用程序。
2. 使用管理员用户名和凭据登录到 CIMC UI 。
3. 在主菜单中，选择服务器选项卡。
4. 单击 Launch KVM Console 。

5. 从虚拟 KVM 控制台中，选择 Virtual Media 选项卡。
6. 选择映射 CD/DVD 。

   您可能需要先单击激活虚拟设备。如果出现提示，请选择 Accept this session 。

7. 浏览到 VMware ESXi 6.7 安装程序 ISO 映像文件，然后单击打开。单击映射设备。
8. 选择电源菜单，然后选择系统重新启动（冷启动）。单击是。

安装 VMware ESXi

以下步骤介绍了如何在每台主机上安装 VMware ESXi 。

下载 ESXi 6.7 Cisco 自定义映像

1. 导航到 "VMware vSphere 下载页面" 用于自定义 ISO 。
2. 单击适用于 ESXi 6.7 GA 的 Cisco 自定义映像安装 CD 旁边的转至下载。
3. 下载适用于 ESXi 6.7 GA 的 Cisco 自定义映像安装 CD （ ISO ）。

所有主机

1. 系统启动时，计算机会检测是否存在 VMware ESXi 安装介质。
2. 从显示的菜单中选择 VMware ESXi 安装程序。

   安装程序将加载。这需要几分钟时间。

3. 安装程序加载完毕后，按 Enter 继续安装。
4. 阅读最终用户许可协议后，接受该协议并按 F11 继续安装。
5. 选择先前设置为 ESXi 安装磁盘的 NetApp LUN ，然后按 Enter 继续安装。

6. 选择适当的键盘布局，然后按 Enter 键。
7. 输入并确认根密码，然后按 Enter 键。
8. 安装程序会警告您已删除卷上的现有分区。按 F11 继续安装。安装 ESXi 后，服务器将重新启动。

设置 **VMware ESXi** 主机管理网络

以下步骤介绍了如何为每个 VMware ESXi 主机添加管理网络。

所有主机

1. 服务器完成重新启动后，按 F2 输入选项以自定义系统。
2. 使用 root 作为登录名登录，并使用先前在安装过程中输入的 root 密码登录。
3. 选择配置管理网络选项。
4. 选择网络适配器，然后按 Enter 键。
5. 为 vSwitch0 选择所需的端口。按 Enter 键。

> 在 CIMC 中选择与 eth0 和 eth1 对应的端口。

6. 选择 VLAN （可选）并按 Enter 键。
7. 输入 VLAN ID ` <<mgmt_vlan_id>>` 。按 Enter 键。
8. 从配置管理网络菜单中，选择 IPv4 配置以配置管理接口的 IP 地址。按 Enter 键。
9. 使用箭头键选中设置静态 IPv4 地址，然后使用空格键选择此选项。
10. 输入用于管理 VMware ESXi 主机 ` 的 IP 地址 <<ESXi_host_mgmt_ip>>` 。
11. 输入 VMware ESXi 主机的子网掩码 ` <<ESXi_host_mgmt_netmask>> 。`
12. 输入 VMware ESXi 主机的默认网关 ` <<ESXi_host_mgmt_gateway>>` 。
13. 按 Enter 接受对 IP 配置所做的更改。
14. 进入 IPv6 配置菜单。
15. 使用空格键取消选择启用 IPv6 （需要重新启动）选项以禁用 IPv6 。按 Enter 键。
16. 进入菜单配置 DNS 设置。
17. 由于 IP 地址是手动分配的，因此还必须手动输入 DNS 信息。
18. 输入主 DNS 服务器的 IP 地址 `[nameserver_ip]` 。
19. （可选）输入辅 DNS 服务器的 IP 地址。
20. 输入 VMware ESXi 主机名的 FQDN： `[esxi_host_fqdn]` 。
21. 按 Enter 接受对 DNS 配置所做的更改。
22. 按 Esc 退出配置管理网络子菜单。
23. 按 Y 确认更改并重新启动服务器。
24. 按 Esc 退出 VMware 控制台。

配置 **ESXi** 主机

您需要下表中的信息来配置每个 ESXi 主机。

详细信息	价值
ESXi 主机名	

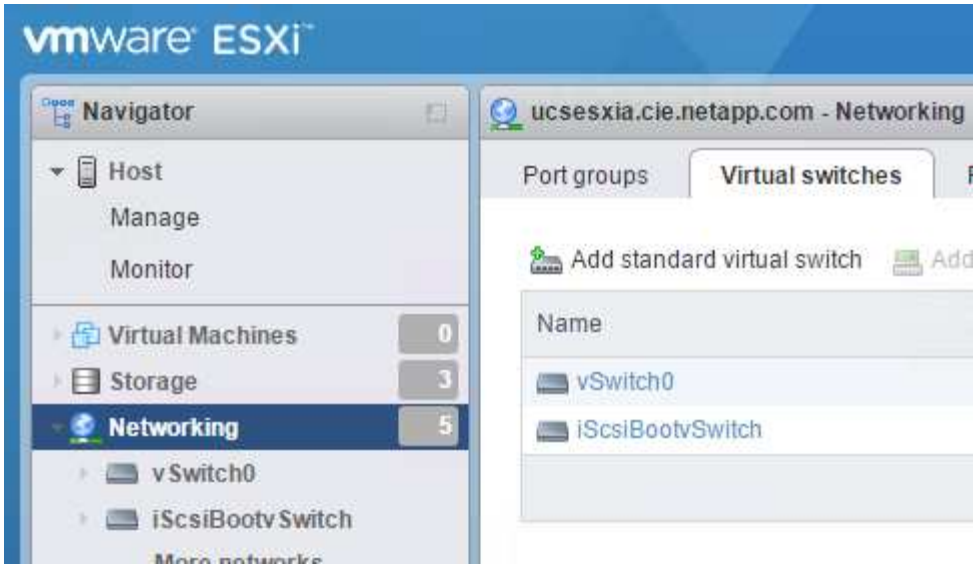
详细信息	价值
ESXi 主机管理 IP	
ESXi 主机管理掩码	
ESXi 主机管理网关	
ESXi 主机 NFS IP	
ESXi 主机 NFS 掩码	
ESXi 主机 NFS 网关	
ESXi 主机 vMotion IP	
ESXi 主机 vMotion 掩码	
ESXi 主机 vMotion 网关	
ESXi 主机 iSCSI-A IP	
ESXi 主机 iSCSI-A 掩码	
ESXi 主机 iSCSI-A 网关	
ESXi 主机 iSCSI-B IP	
ESXi 主机 iSCSI-B 掩码	
ESXi 主机 iSCSI-B 网关	

登录到 **ESXi** 主机

1. 在 Web 浏览器中打开主机的管理 IP 地址。
2. 使用 root 帐户和您在安装过程中指定的密码登录到 ESXi 主机。
3. 阅读有关 VMware 客户体验改进计划的声明。选择正确的响应后，单击确定。

配置 **iSCSI** 启动

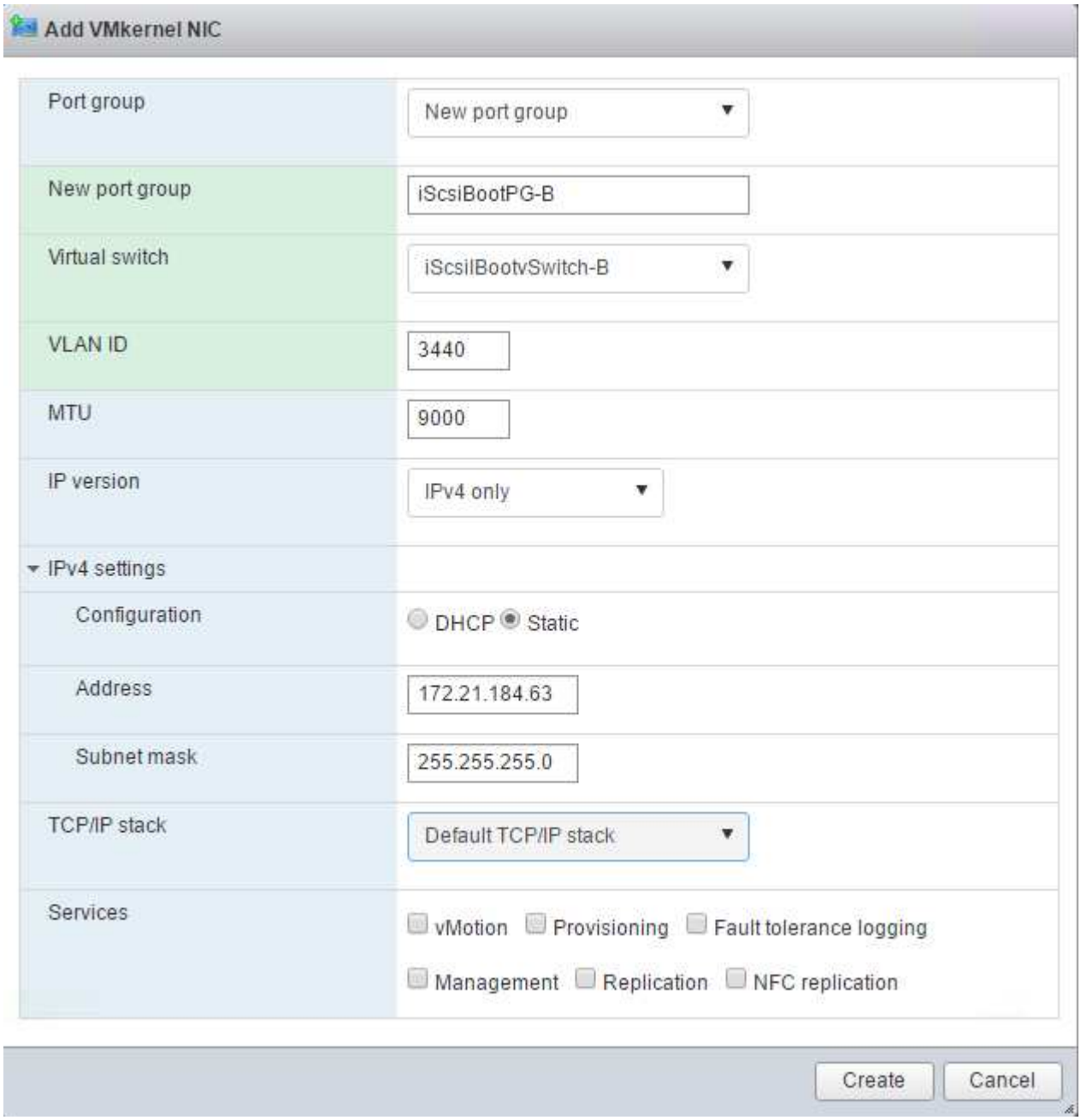
1. 选择左侧的 Networking 。
2. 在右侧，选择 Virtual Switches 选项卡。



3. 单击 iScsiBootvSwitch 。
4. 选择编辑设置。
5. 将 MTU 更改为 9000 ，然后单击保存。
6. 单击左侧导航窗格中的 Networking 以返回到 Virtual Switches 选项卡。
7. 单击添加标准虚拟交换机。
8. 请提供 vSwitch 名称 `iScsiBootvSwitch B` 。
   - 将 MTU 设置为 9000 。
   - 从上行链路 1 选项中选择 vmnic3 。
   - 单击添加。

> 在此配置中， vmnic2 和 vmnic3 用于 iSCSI 启动。如果 ESXi 主机中有其他 NIC ，则可能具有不同的 vmnic 编号。要确认用于 iSCSI 启动的 NIC ，请将 CIMC 中 iSCSI vNIC 上的 MAC 地址与 ESXi 中的 vmnic 进行匹配。

9. 在中间窗格中，选择 VMkernel NIC 选项卡。
10. 选择添加 VMkernel NIC 。
    - 指定新端口组名称 `iScsiBootPG-B` 。
    - 为虚拟交换机选择 iScsiBootvSwitch B 。
    - 输入 ` <<iscsib_vlan_id>>` 作为 VLAN ID 。
    - 将 MTU 更改为 9000 。
    - 展开 IPv4 设置。
    - 选择静态配置。
    - 为地址输入 ` <<var_hosta_iscsib_ip>>` 。
    - 为子网掩码输入 ` <<var_hosta_iscsib_mask>>` 。
    - 单击创建。

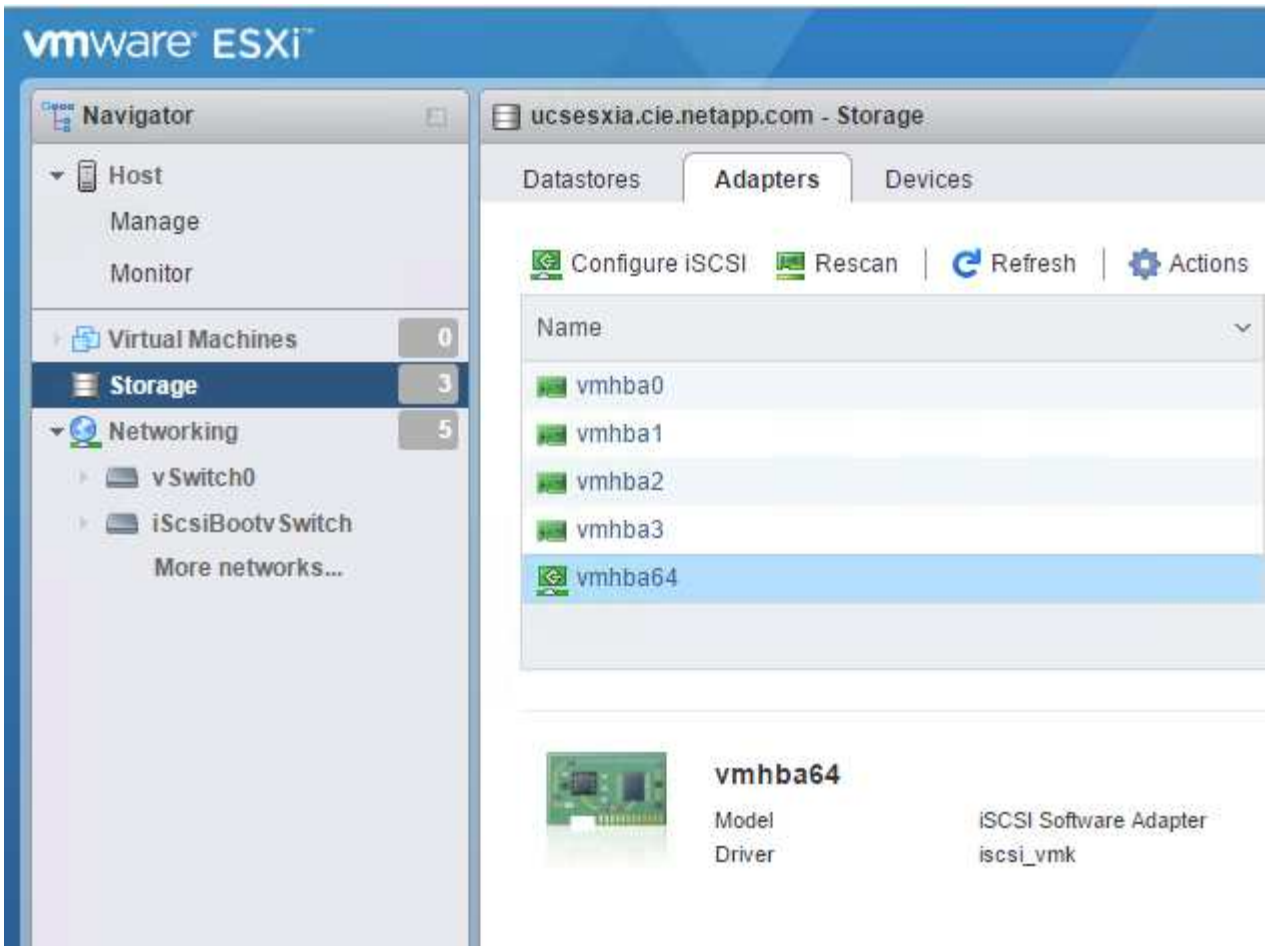


在 `iScsiBootPg- A` 上将 MTU 设置为 9000

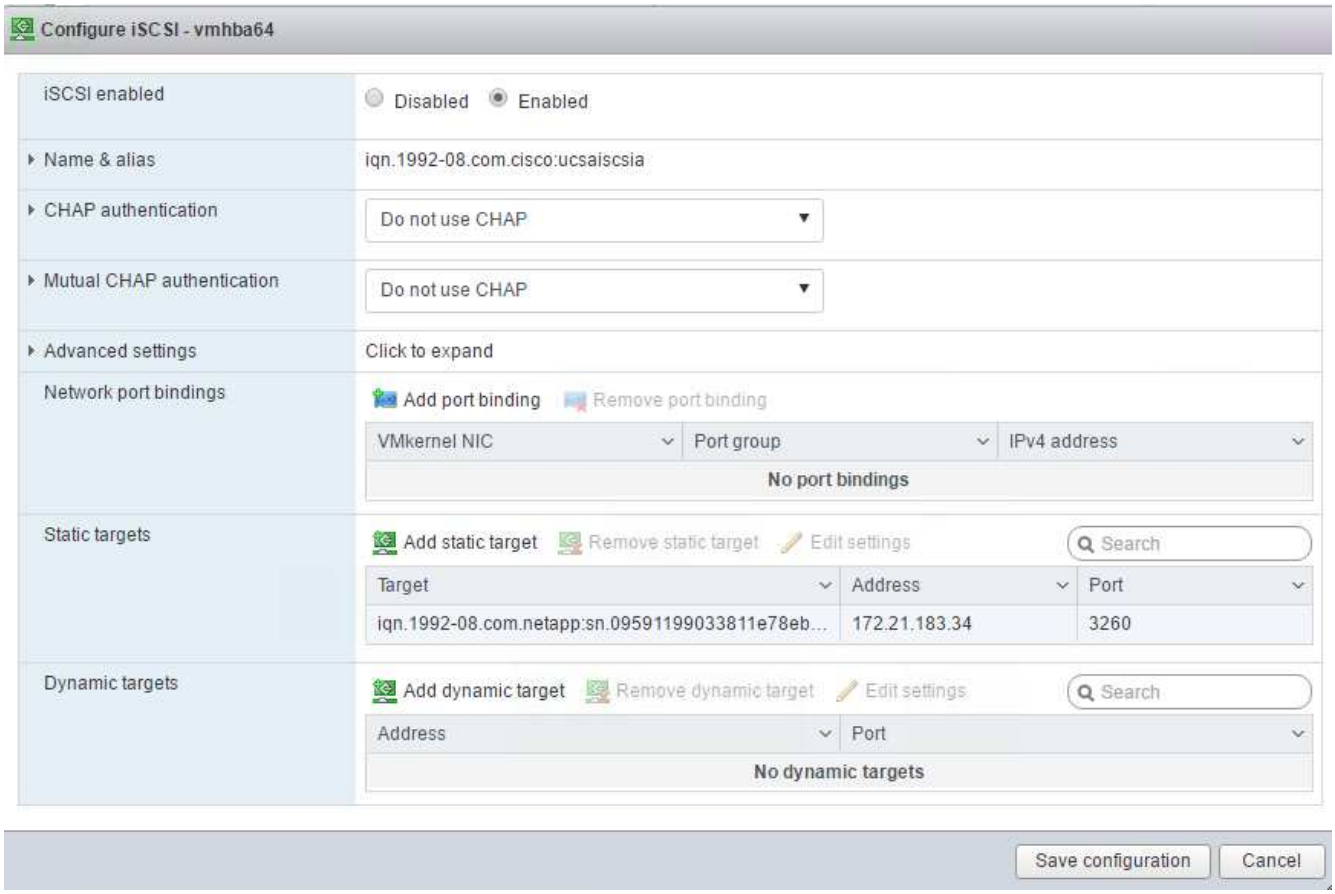
配置 **iSCSI** 多路径

要在 ESXi 主机上设置 iSCSI 多路径，请完成以下步骤：

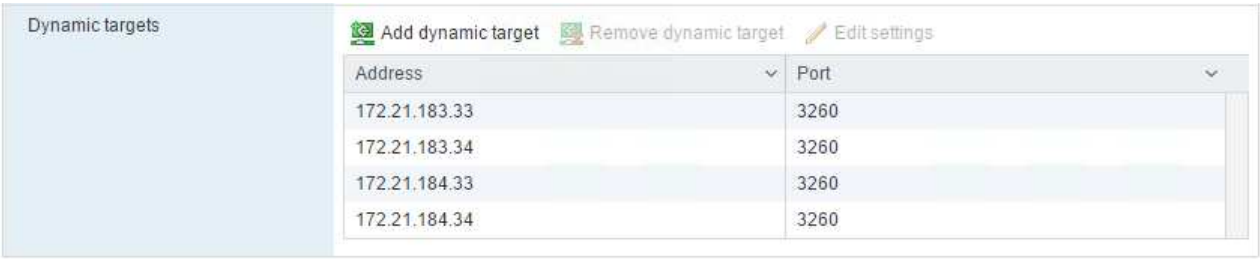
1. 在左侧导航窗格中选择存储。单击适配器。
2. 选择 iSCSI 软件适配器，然后单击配置 iSCSI 。



3. 在动态目标下，单击添加动态目标。



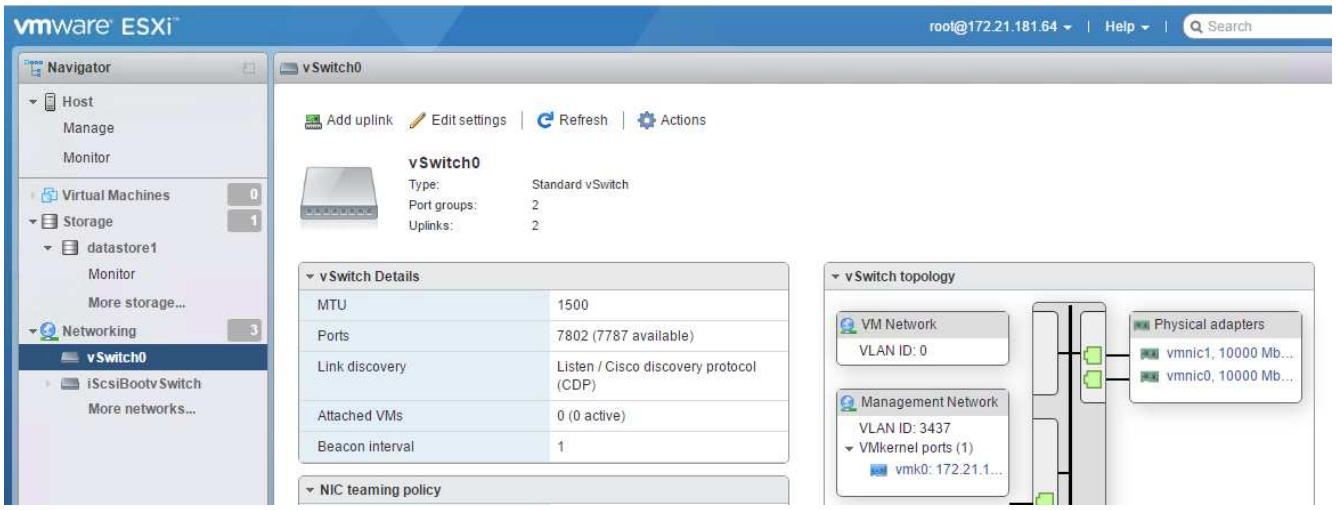
4. 输入 IP 地址 `iscsi_lif01a` 。
   - 对 IP 地址 `iscsi_lif01b` ， `iscsi_lif02a` 和 `iscsi_lif02b` 重复上述步骤。
   - 单击保存配置。



> 您可以通过在 NetApp 集群上运行 `network interface show `命令或查看 OnCommand 系统管理器中的网络接口选项卡来查找 iSCSI LIF IP 地址。

配置 **ESXi** 主机

1. 在左侧导航窗格中，选择网络。
2. 选择 vSwitch0 。



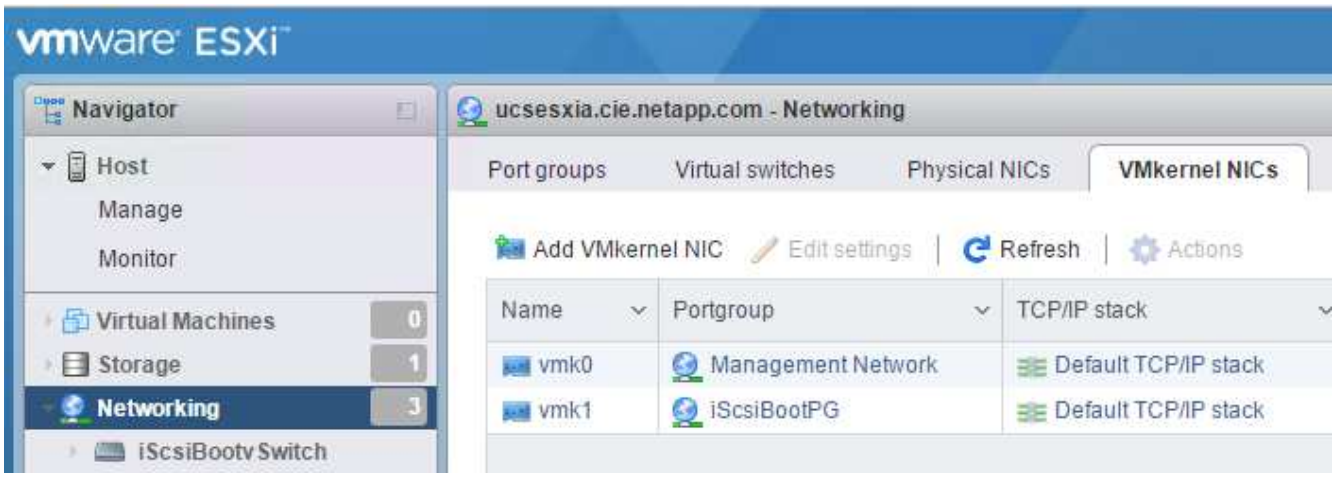
3. 选择编辑设置。
4. 将 MTU 更改为 9000 。
5. 展开 NIC 绑定并验证 vmnic0 和 vmnic1 是否都设置为 active 。

配置端口组和 **VMkernel NIC**

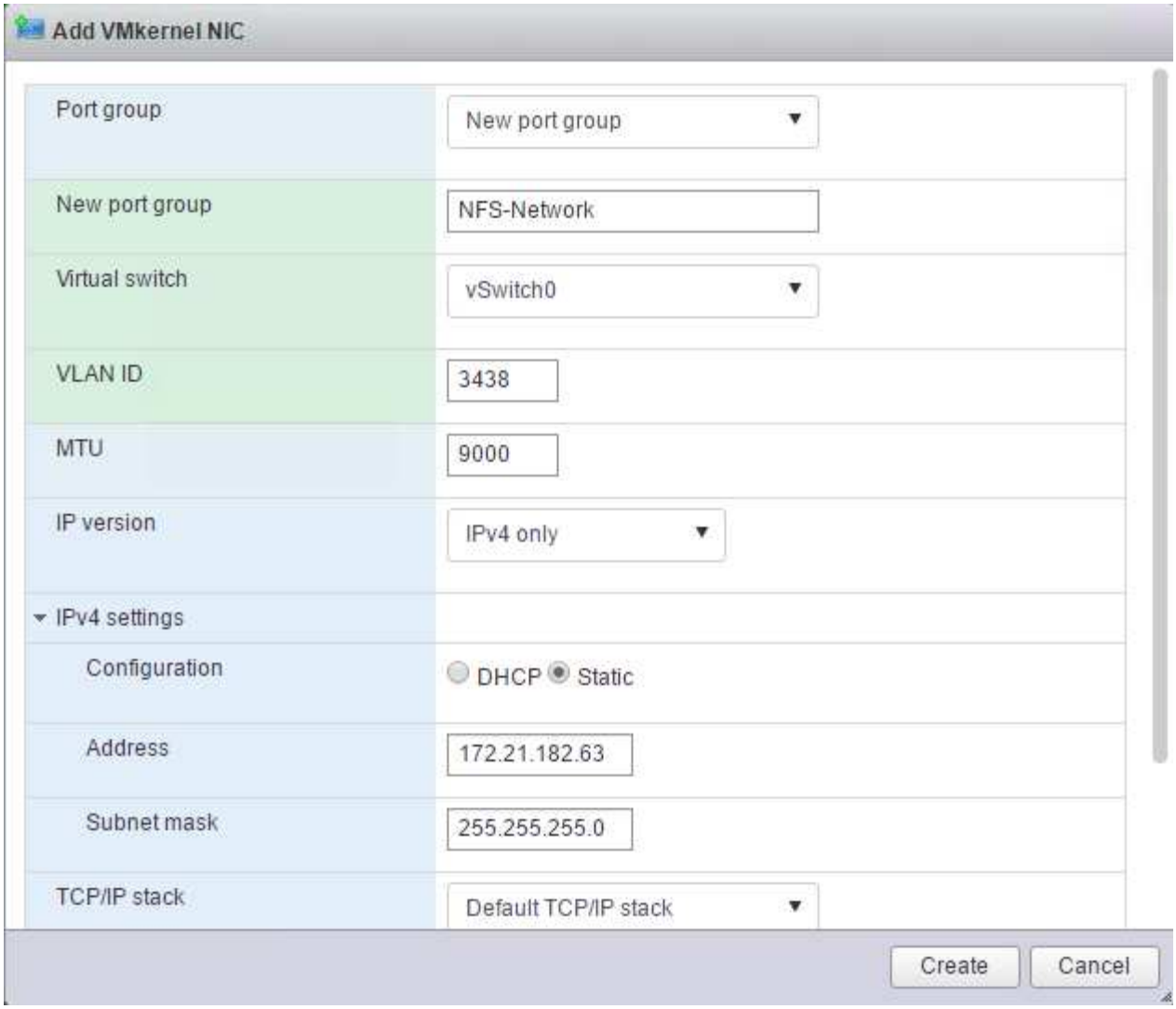
1. 在左侧导航窗格中，选择网络。
2. 右键单击端口组选项卡。

3. 右键单击 VM Network ，然后选择 Edit 。将 VLAN ID 更改为 ` <<var_vm_traffic _vlan>>` 。
4. 单击添加端口组。
   - 将端口组命名为 `MGMT-Network` 。
   - 输入 ` <<mgmt_vlan>>` 作为 VLAN ID 。
   - 确保已选择 vSwitch0 。
   - 单击添加。

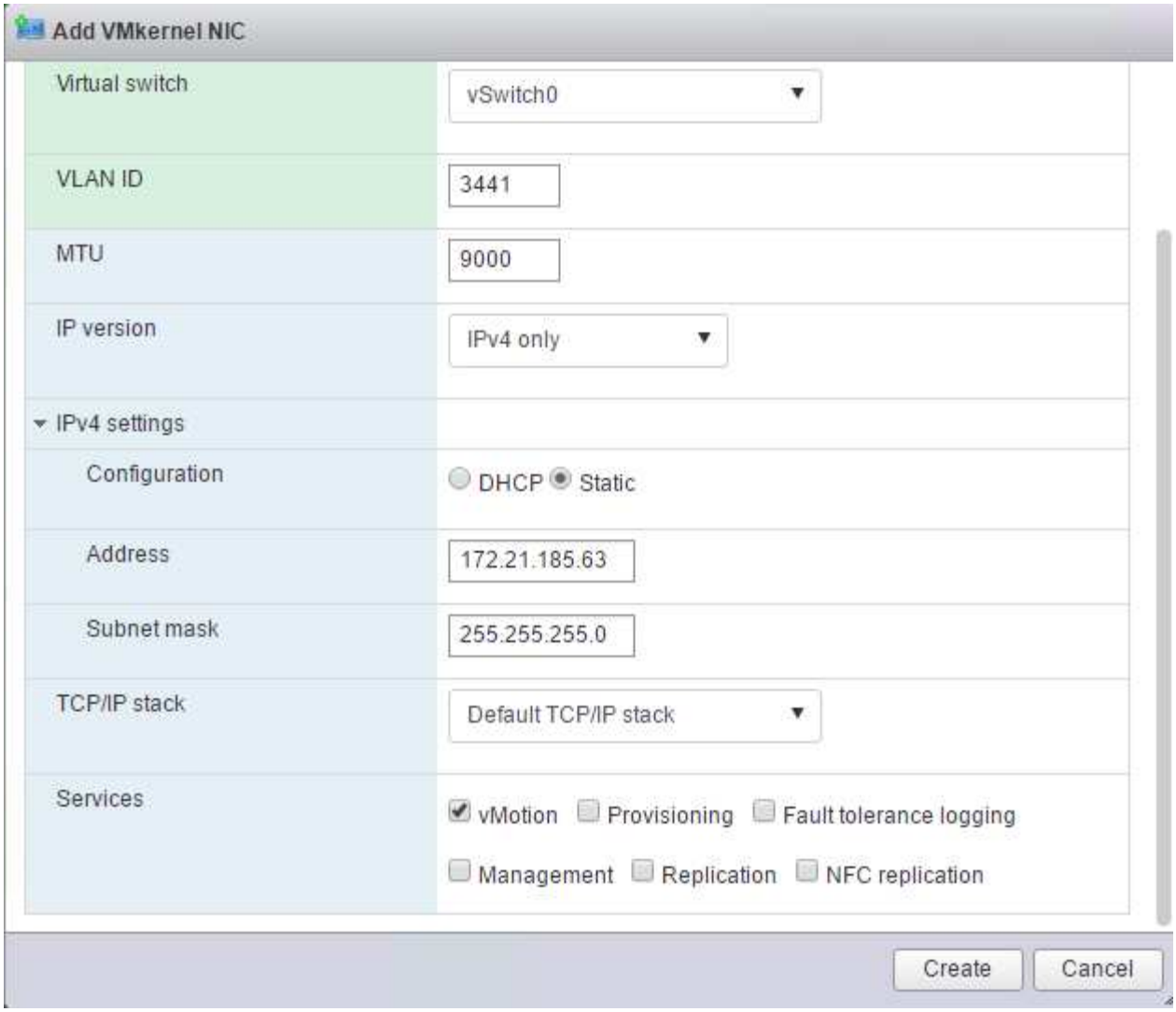
5. 单击 VMkernel NIC 选项卡。



6. 选择添加 VMkernel NIC 。
   - 选择 New Port Group 。
   - 将端口组命名为 `NFS-Network` 。
   - 输入 ` <<NFS_VLAN_id>>` 作为 VLAN ID 。
   - 将 MTU 更改为 9000 。
   - 展开 IPv4 设置。
   - 选择静态配置。
   - 为地址输入 ` <<var_hosta_nfs_ip>>` 。
   - 为子网掩码输入 ` <<var_hosta_nfs_mask>>` 。
   - 单击创建。



7. 重复此过程以创建 vMotion VMkernel 端口。
8. 选择添加 VMkernel NIC 。
    a. 选择 New Port Group 。
    b. 将端口组命名为 vMotion 。
    c. 输入 ` <<vmotion_vlan_id>>` 作为 VLAN ID 。
    d. 将 MTU 更改为 9000 。
    e. 展开 IPv4 设置。
    f. 选择静态配置。
    g. 为地址输入 ` <<var_hosta_vmotion_ip>>` 。
    h. 输入 ` <<var_hosta_vmotion_mask>>` 作为子网掩码。
    i. 确保在 IPv4 设置后选中 vMotion 复选框。

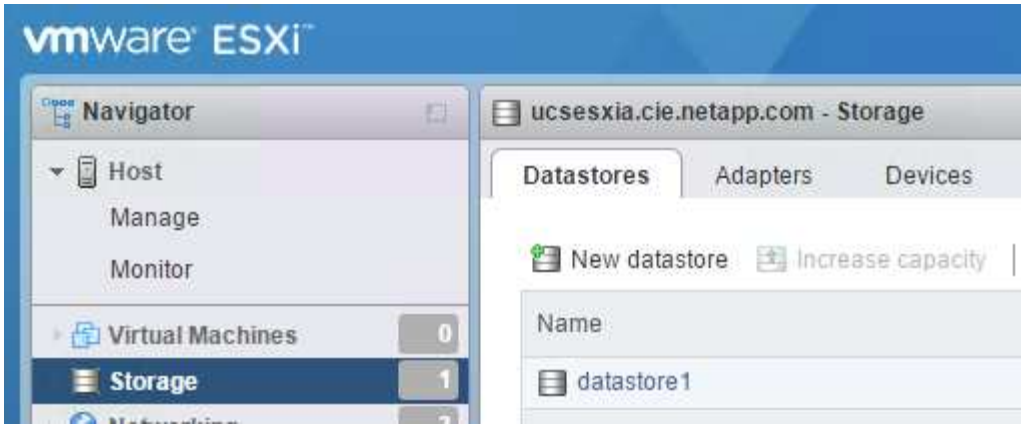


可以通过多种方法配置 ESXi 网络，包括在许可允许的情况下使用 VMware vSphere 分布式交换机。如果需要使用其他网络配置来满足业务需求， FlexPod Express 支持这些配置。

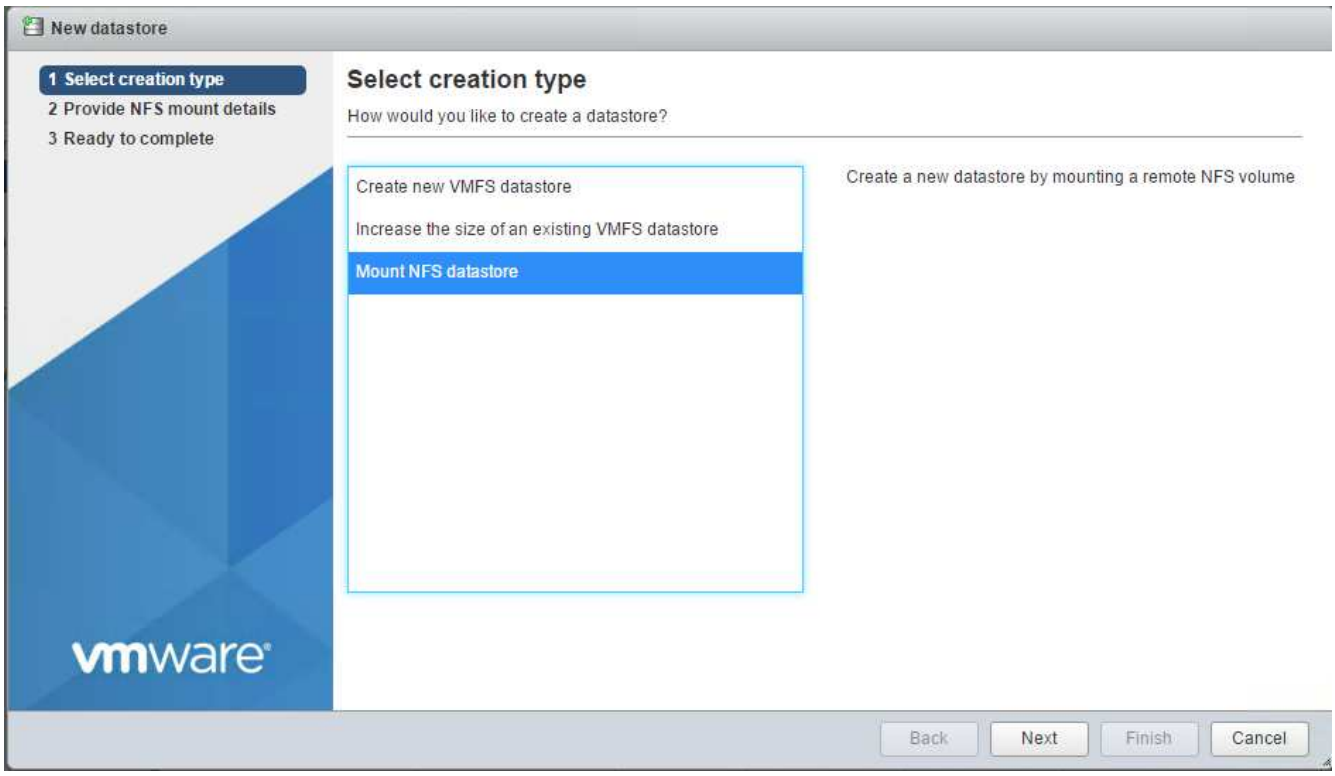
首先挂载数据存储库

要挂载的第一个数据存储库是虚拟机的 infra_datastore_1 数据存储库和虚拟机交换文件的 infra_swap 数据存储库。

1. 单击左侧导航窗格中的存储，然后单击新建数据存储库。



2. 选择挂载 NFS 数据存储库。



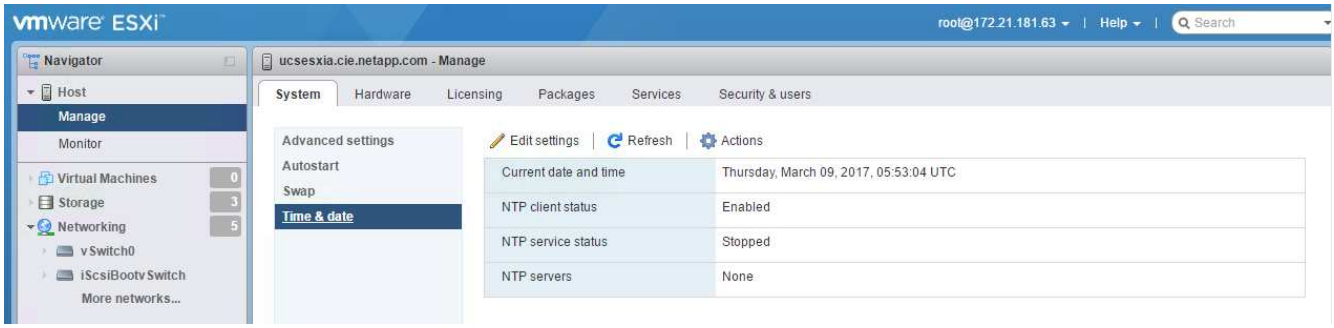
3. 接下来，在提供 NFS 挂载详细信息页面中输入以下信息：
   - 名称： `infra_datastore_1`
   - NFS 服务器：` <<var_noda_nfs_lif>>`
   - 共享： /infra_datastore_1
   - 确保已选择 NFS 3 。
4. 单击完成。您可以在 " 近期任务 " 窗格中看到任务正在完成。
5. 重复此过程挂载 infra_swap 数据存储库：
   - 名称： `infra_swap`
   - NFS 服务器：` <<var_noda_nfs_lif>>`
   - 共享：` /infra_swap`

- 确保已选择 NFS 3 。

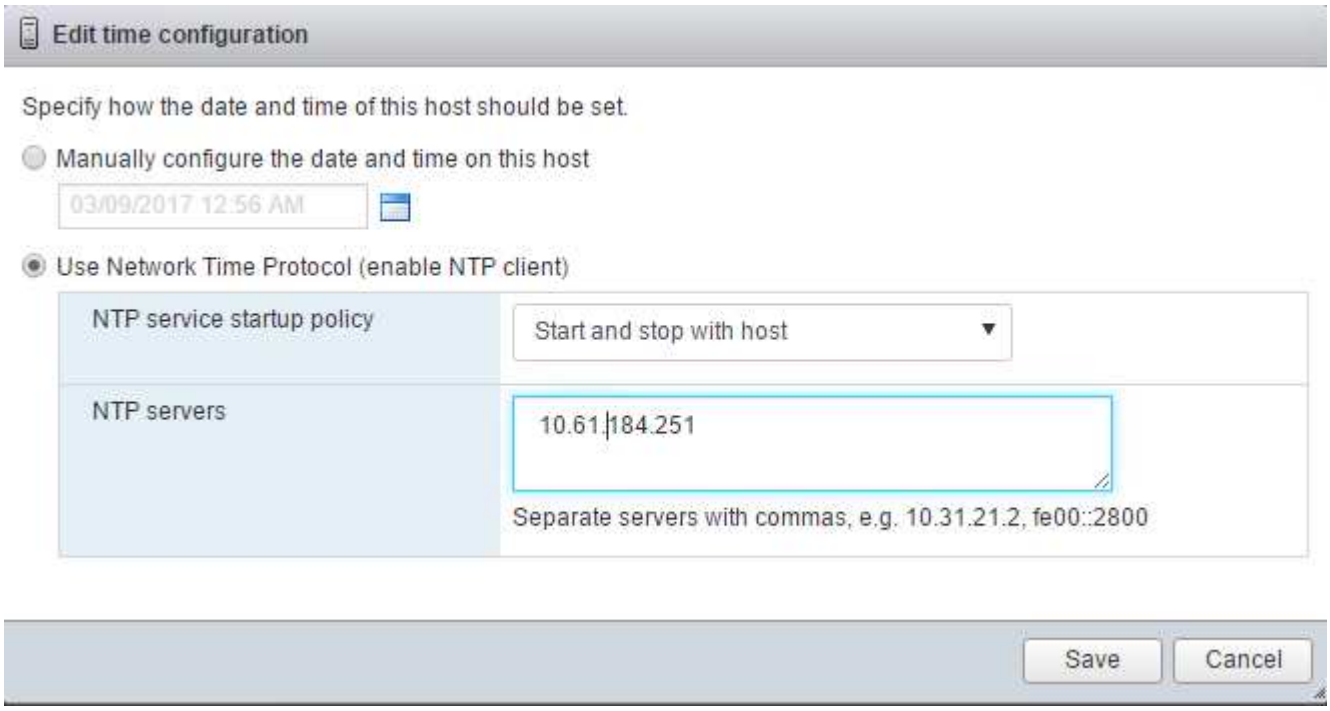
配置 **NTP**

要为 ESXi 主机配置 NTP ，请完成以下步骤：

1. 单击左侧导航窗格中的管理。在右窗格中选择 System ，然后单击 Time & Date 。



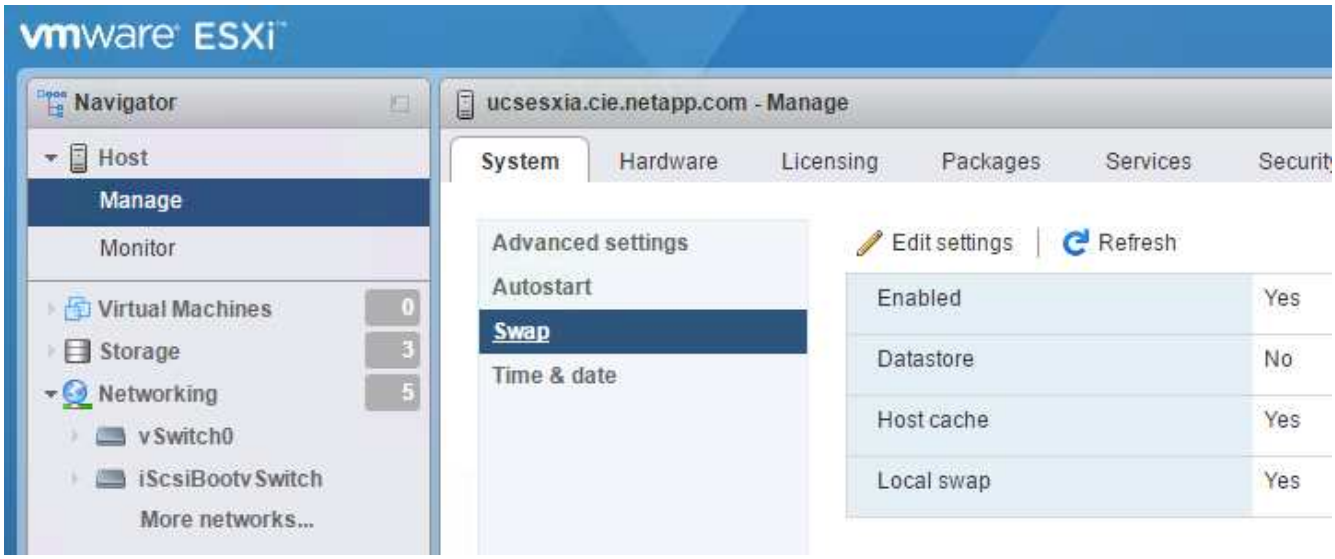
2. 选择使用网络时间协议（启用 NTP 客户端）。
3. 选择 Start 和 Stop with Host 作为 NTP 服务启动策略。
4. 输入 ` <<var_ntf>>` 作为 NTP 服务器。您可以设置多个 NTP 服务器。
5. 单击保存。



移动虚拟机交换文件的位置

以下步骤提供了有关移动虚拟机交换文件位置的详细信息。

1. 单击左侧导航窗格中的管理。在右窗格中选择 system ，然后单击 Swap 。



2. 单击编辑设置。从数据存储库选项中选择 infra_swap 。

3. 单击保存。

安装适用于 **VMware VAAI** 的 **NetApp NFS** 插件 **1.0.20**

要安装适用于 VMware VAAI 的 NetApp NFS 插件 1.0.20 ，请完成以下步骤。

1. 输入以下命令以验证是否已启用 VAAI ：

```
esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
```

如果启用了 VAAI ，则这些命令将生成以下输出：

```
~ #  esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
~ # esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
```

2. 如果未启用 VAAI ，请输入以下命令以启用 VAAI ：

```
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedInit
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
```

这些命令将生成以下输出：

```
~ # esxcfg-advcfg -s 1 /Data Mover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
~ #  esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
```

3. 下载适用于 VMware VAAI 的 NetApp NFS 插件：
   a. 转至 "软件下载页面"。
   b. 向下滚动并单击适用于 VMware VAAI 的 NetApp NFS 插件。
   c. 选择 ESXi 平台。
   d. 下载最新插件的脱机软件包（ .zip ）或联机软件包（ .vib ）。
4. 使用 ESX 命令行界面在 ESXi 主机上安装此插件。
5. 重新启动 ESXi 主机。

```
[root@vm-host-infra-04:~] ls /vmfs/volumes/datastore1/NetAppNasPlugin.vib
/vmfs/volumes/datastore1/NetAppNasPlugin.vib
[root@vm-host-infra-04:~] esxcli software vib install -v /vmfs/volumes/datastore1/NetAppNasPlugin.vib
Installation Result
   Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.
   Reboot Required: true
   VIBs Installed: NetApp_bootbank_NetAppNasPlugin_1.1.2-3
   VIBs Removed:
   VIBs Skipped:
[root@vm-host-infra-04:~]
```

"接下来：安装 VMware vCenter Server 6.7"

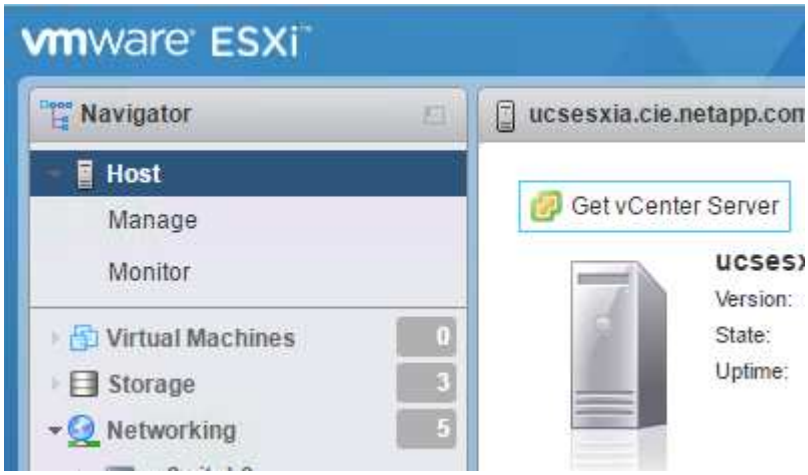
安装 **VMware vCenter Server 6.7**

本节详细介绍了在 FlexPod 快速配置中安装 VMware vCenter Server 6.7 的过程。

> FlexPod Express 使用 VMware vCenter Server 设备（ VCSA ）。

下载 **VMware vCenter Server** 设备

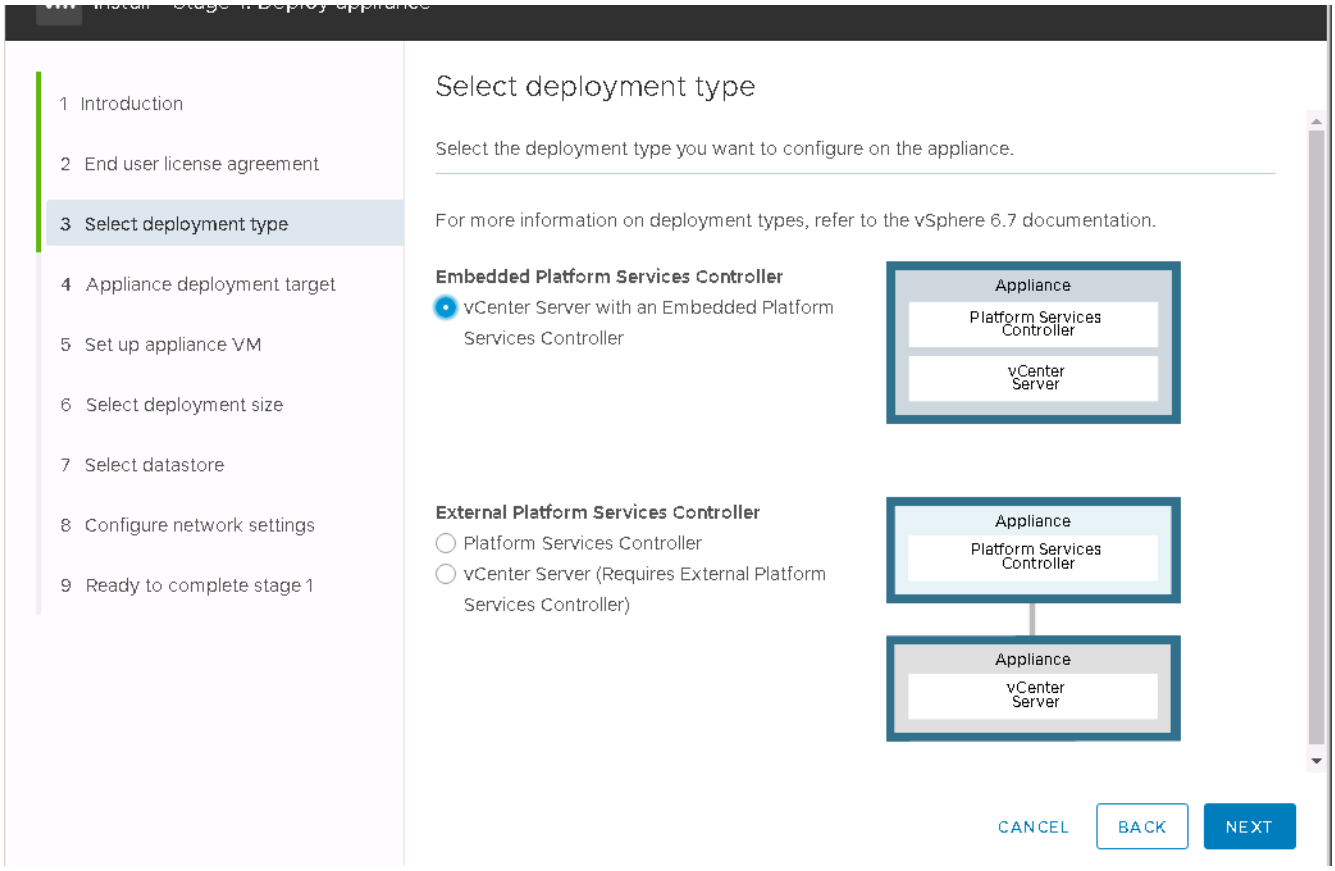
1. 下载 VCSA 。在管理 ESXi 主机时，单击获取 vCenter Server 图标以访问下载链接。



2. 从 VMware 站点下载 VCSA 。

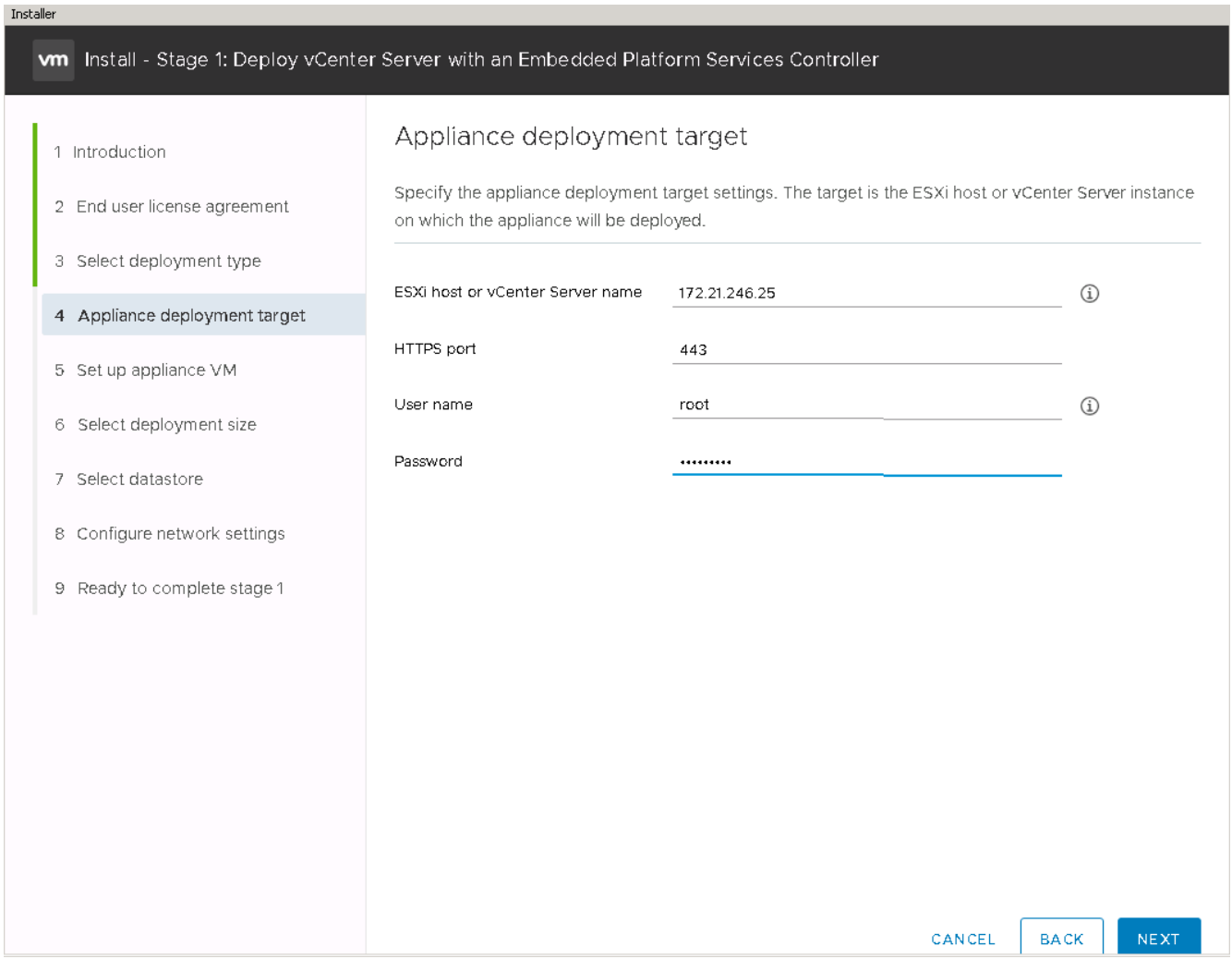
> 虽然支持安装 Microsoft Windows vCenter Server ，但 VMware 建议在新部署中使用 VCSA 。

3. 挂载 ISO 映像。
4. 导航到 vcsa-ui-installer>win32 目录。双击 installer.exe 。
5. 单击安装。
6. 单击简介页面上的下一步。
7. 接受最终用户许可协议。
8. 选择 Embedded Platform Services Controller 作为部署类型。

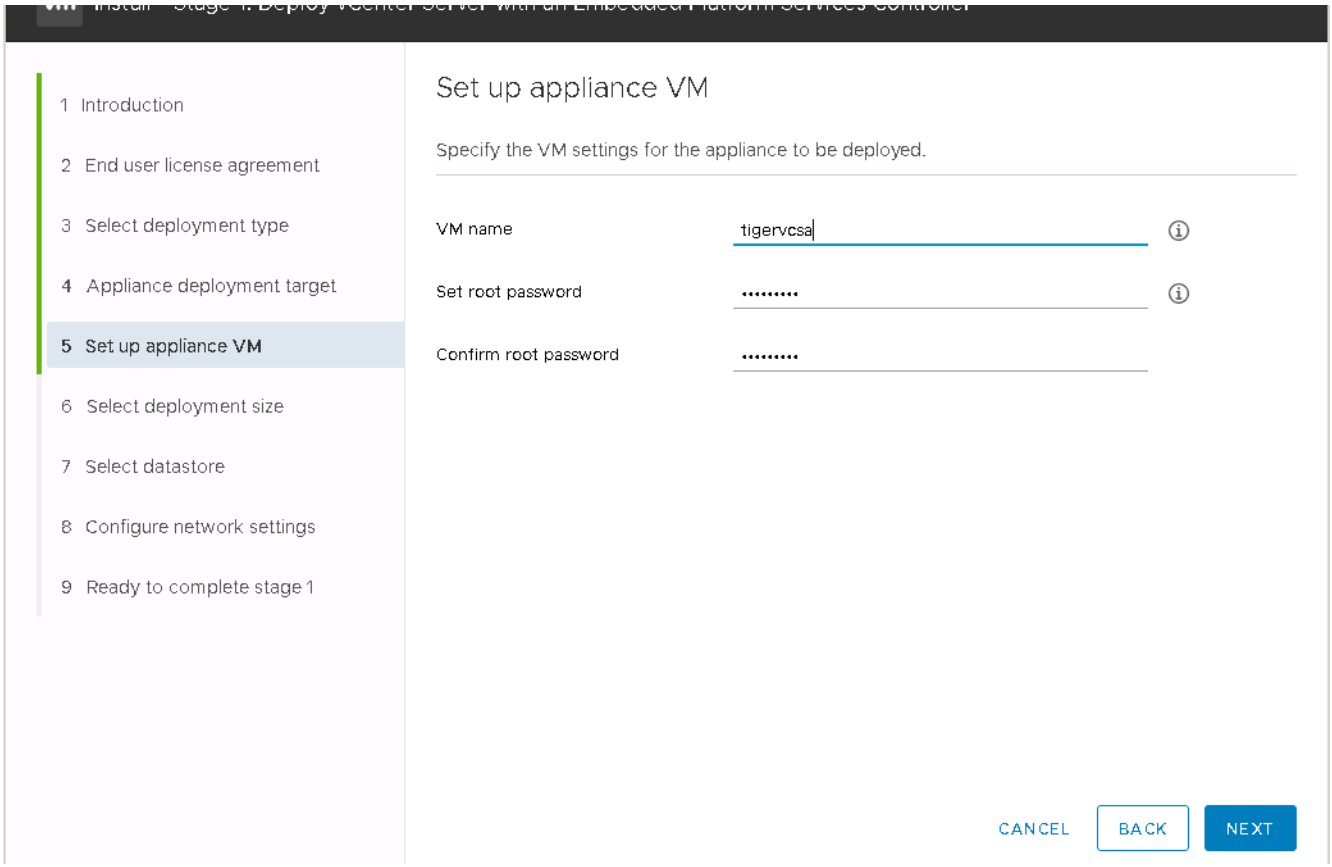


> 如果需要，还支持在 FlexPod Express 解决方案中部署外部平台服务控制器。

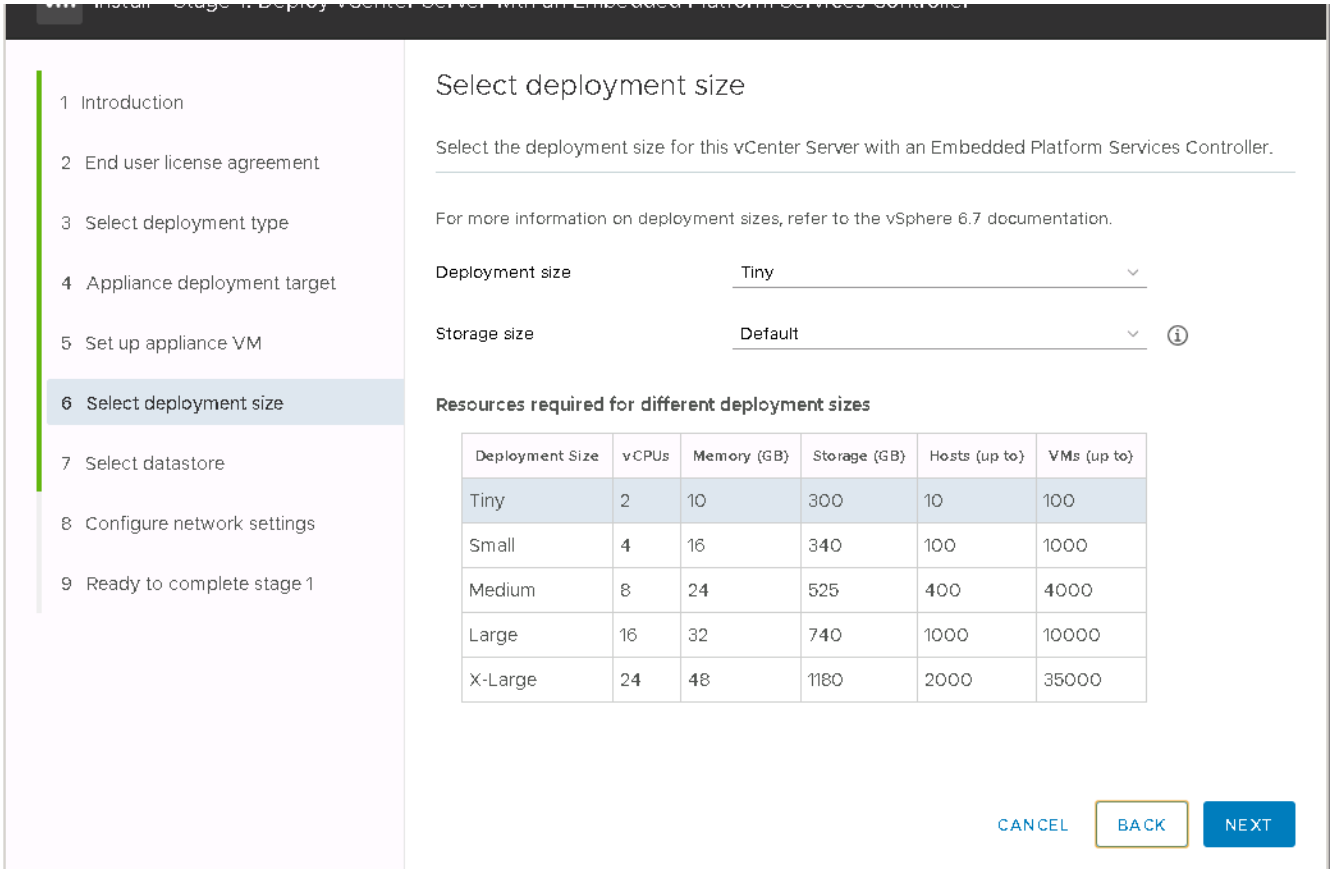
9. 在设备部署目标中，输入已部署的 ESXi 主机的 IP 地址以及 root 用户名和 root 密码。



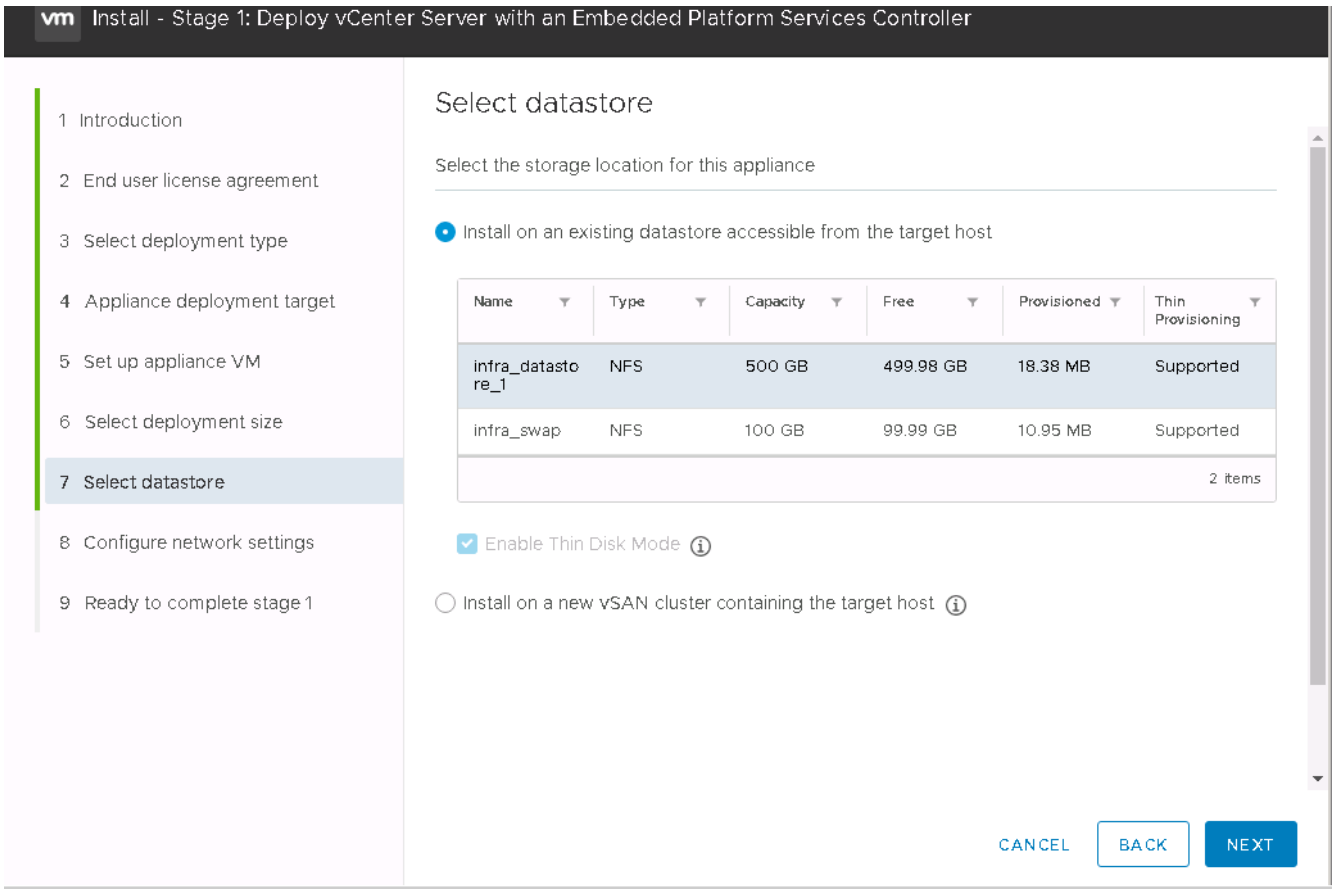
10. 输入 `vCSA` 作为要用于 VCSA 的 VM 名称和根密码，以设置设备 VM 。



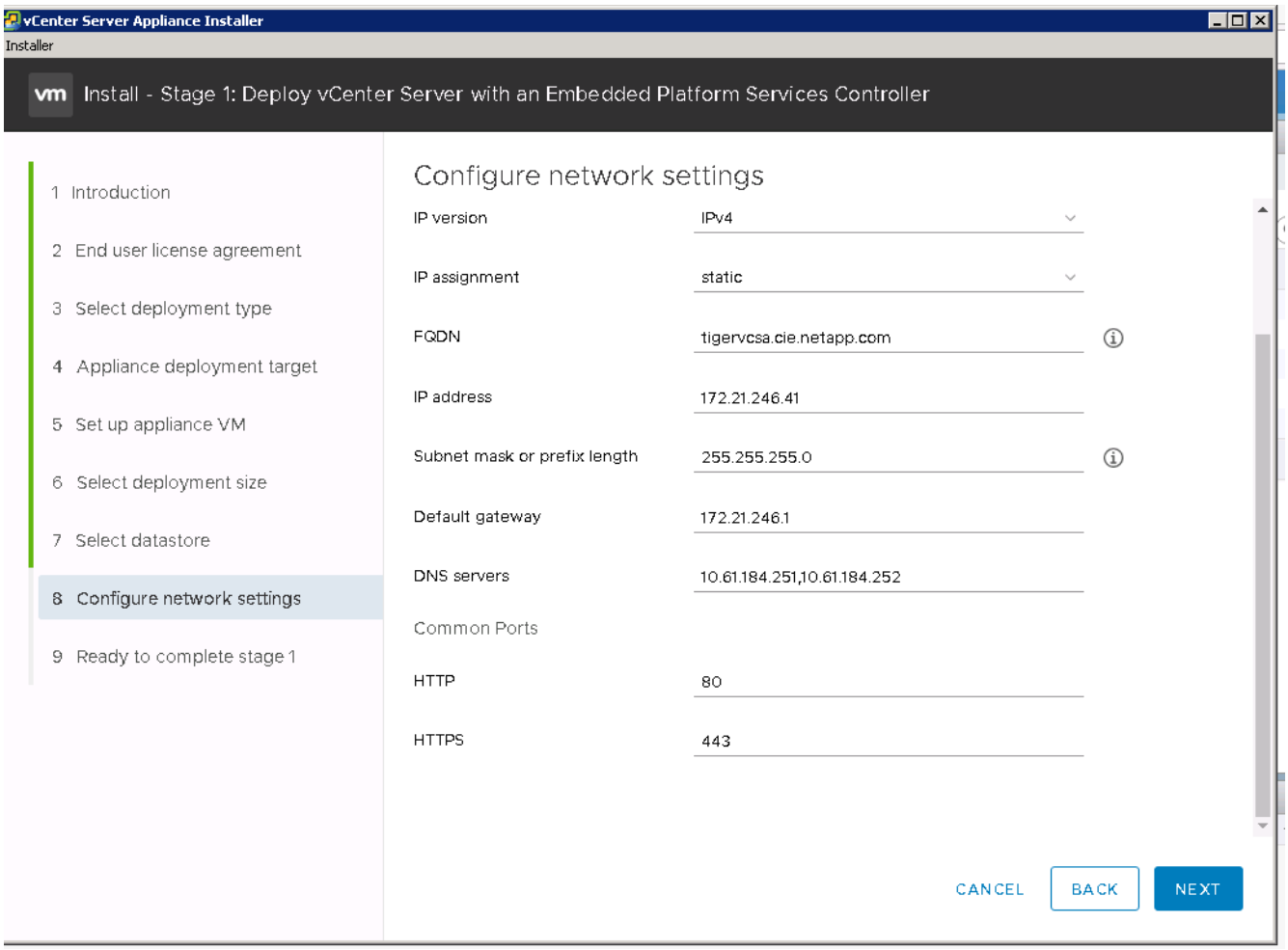
11. 选择最适合您环境的部署规模。单击下一步。



12. 选择 infra_datastore_1 数据存储库。单击下一步。

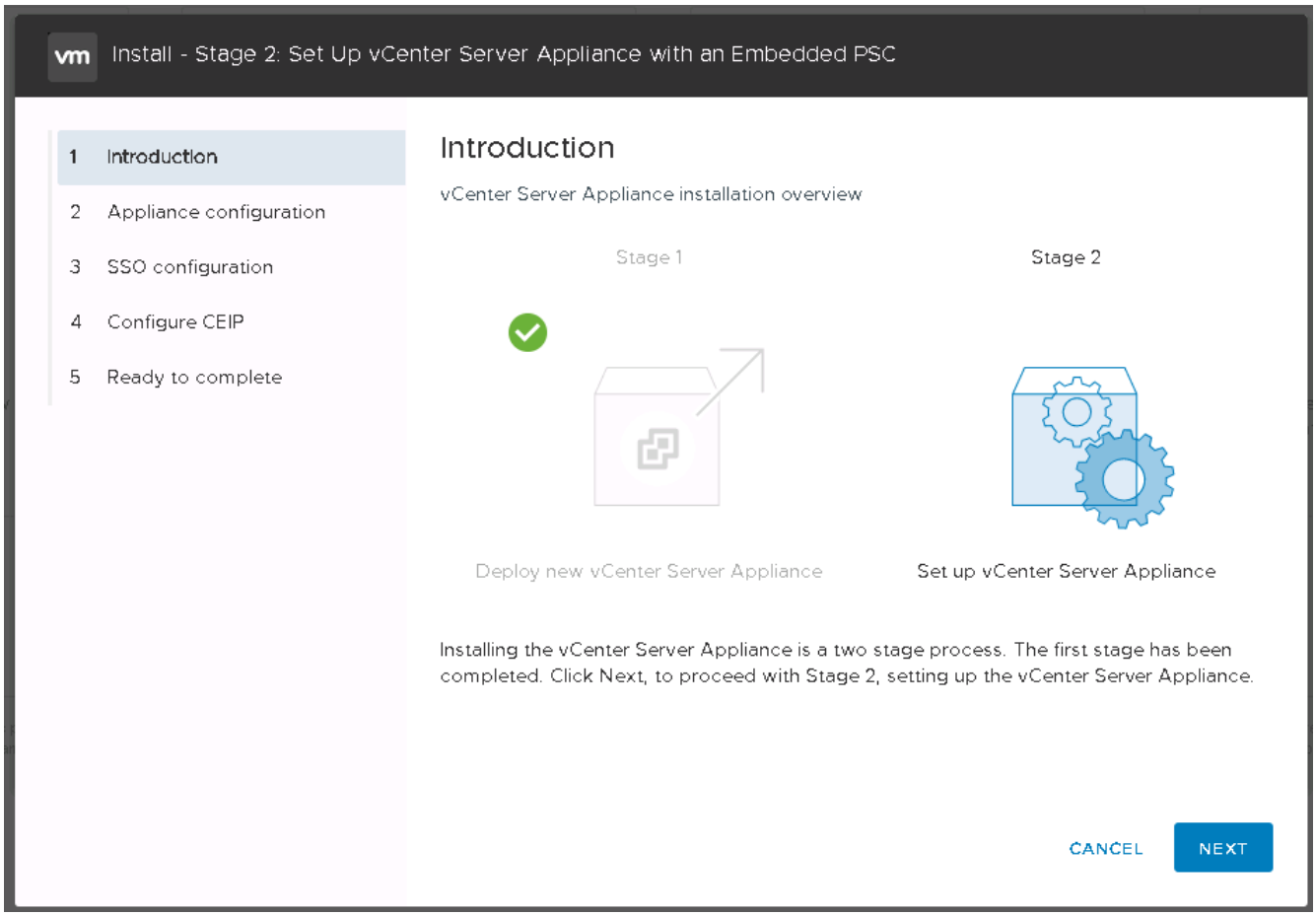


13. 在 Configure network settings 页面中输入以下信息，然后单击 Next 。
    a. 选择 MGMT-Network for Network 。
    b. 输入要用于 VCSA 的 FQDN 或 IP 。
    c. 输入要使用的 IP 地址。
    d. 输入要使用的子网掩码。
    e. 输入默认网关。
    f. 输入 DNS 服务器。
14. 在准备完成阶段 1 页面上，验证您输入的设置是否正确。单击完成。



此时将安装 VCSA 。此过程需要几分钟时间。

15. 阶段 1 完成后，将显示一条消息，指出已完成。单击 Continue 以开始第 2 阶段配置。
16. 在第 2 阶段简介页面上，单击下一步。



17. 输入 ` <<var_ntp_id>>` 作为 NTP 服务器地址。您可以输入多个 NTP IP 地址。

    如果您计划使用 vCenter Server 高可用性（HA），请确保已启用 SSH 访问。

18. 配置 SSO 域名，密码和站点名称。单击下一步。

    请记下这些值以供参考，特别是当您与 vsphere.local 域名有所偏差时。

19. 如果需要，请加入 VMware 客户体验计划。单击下一步。
20. 查看设置摘要。单击完成或使用返回按钮编辑设置。
21. 此时将显示一条消息，指出在安装开始后，您将无法暂停或停止安装完成。单击确定继续。

    设备设置将继续。这需要几分钟时间。

    此时将显示一条消息，指示设置已成功。

    安装程序提供的用于访问 vCenter Server 的链接可单击。

"接下来：配置 VMware vCenter Server 6.7 和 vSphere 集群。"

配置 **VMware vCenter Server 6.7** 和 **vSphere** 集群

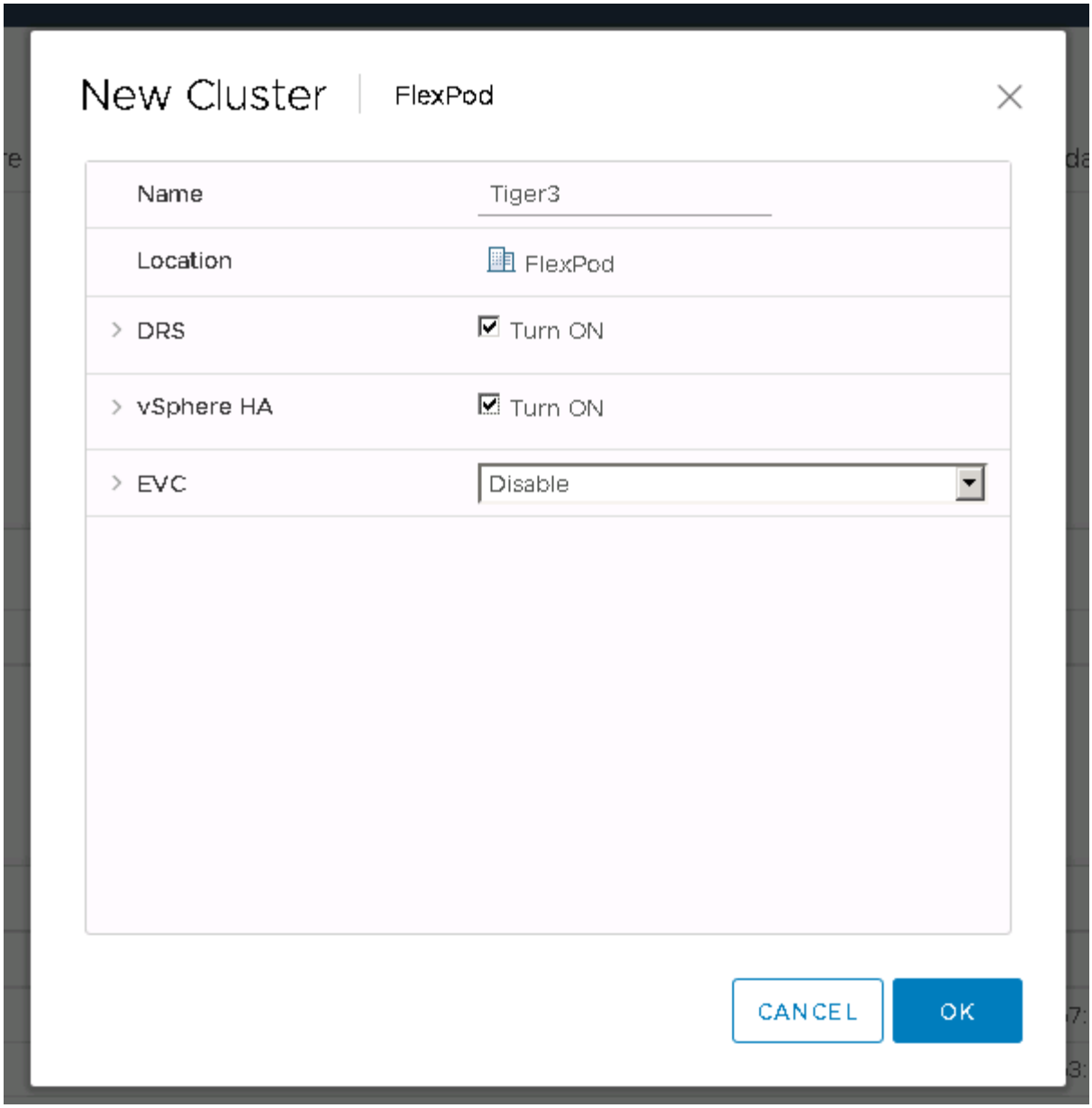
要配置 VMware vCenter Server 6.7 和 vSphere 集群，请完成以下步骤：

1. 导航到 https://\<<FQDN 或 vCenter 的 IP >/vsphere-client/ 。
2. 单击 Launch vSphere Client 。
3. 使用用户名 mailto： administrator@vspehre.local[administrator@vsphere.local^] 和您在 VCSA 设置过程中输入的 SSO 密码登录。
4. 右键单击 vCenter 名称并选择新建数据中心。
5. 输入数据中心的名称，然后单击确定。

创建 **vSphere** 集群

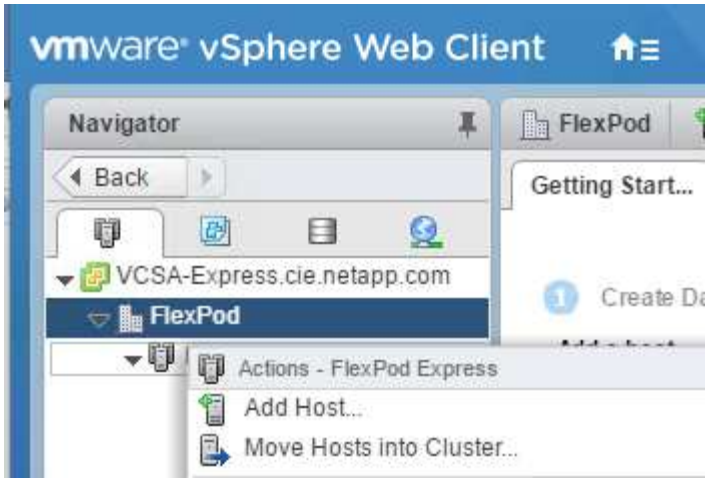
要创建 vSphere 集群，请完成以下步骤：

1. 右键单击新创建的数据中心，然后选择 New Cluster 。
2. 输入集群的名称。
3. 选中复选框以启用灾难恢复和 vSphere HA 。
4. 单击确定。



将 **ESXi** 主机添加到集群

1. 右键单击集群并选择添加主机。



2. 要将 ESXi 主机添加到集群，请完成以下步骤：
   a. 输入主机的 IP 或 FQDN 。单击下一步。
   b. 输入 root 用户名和密码。单击下一步。
   c. 单击是将主机的证书替换为由 VMware 证书服务器签名的证书。
   d. 单击主机摘要页面上的下一步。
   e. 单击绿色 + 图标向 vSphere 主机添加许可证。

      ⓘ 如果需要，可以稍后完成此步骤。

   f. 单击下一步以使锁定模式保持禁用状态。
   g. 单击 VM 位置页面上的下一步。
   h. 查看即将完成页面。使用 " 返回 " 按钮进行任何更改或选择 " 完成 " 。
3. 对 Cisco UCS 主机 B 重复步骤 1 和 2对于添加到 FlexPod 快速配置中的任何其他主机，必须完成此过程。

在 ESXi 主机上配置核心转储

1. 使用 SSH 连接到管理 IP ESXi 主机，输入 root 作为用户名，然后输入 root 密码。
2. 运行以下命令：

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

3. 输入最后一个命令后，将显示消息 `Verified the configured netdump server is running` 。

对于添加到 FlexPod Express 中的任何其他主机，必须完成此过程。

结论

FlexPod Express 通过提供经过验证的设计，使用行业领先的组件，提供了一个简单而有效的解决方案。通过添加其他组件进行扩展， FlexPod Express 可以根据特定业务需求进行定制。FlexPod Express 在设计时考虑到了中小型企业， ROBO 以及其他需要专用解决方案的企业。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请参见以下文档和 / 或网站：

- NetApp 产品文档

  "http://docs.netapp.com"

- 《采用 VMware vSphere 6.7 的 FlexPod Express 和 NetApp AFF A220 设计指南》

  "https://www.netapp.com/us/media/nva-1125-design.pdf"

采用 VMware vSphere 6.7U1 的 FlexPod Express 以及采用基于 IP 的直连存储的 NetApp AFF A220

NVA-1131-Deploy： 采用 VMware vSphere 6.7U1 的 FlexPod Express 以及采用基于 IP 的直连存储的 NetApp AFF A220

NetApp 公司 Sree Lakshmi Lan

行业趋势表明，数据中心正在向共享基础架构和云计算转型。此外，企业还寻求为远程办公室和分支机构提供简单有效的解决方案，并利用他们在数据中心中熟悉的技术。

FlexPod Express 是一种预先设计的最佳实践架构，基于 Cisco 统一计算系统（ Cisco UCS ）， Cisco Nexus 系列交换机和 NetApp 存储技术构建。FlexPod 快速系统中的组件与 FlexPod 数据中心的对应组件一样，可以在较小规模的整个 IT 基础架构环境中实现管理协作。FlexPod 数据中心和 FlexPod Express 是虚拟化以及裸机操作系统和企业工作负载的最佳平台。

FlexPod 数据中心和 FlexPod Express 提供基线配置，并可对多功能性进行规模估算和优化，以满足多种不同的使用情形和要求。现有的 FlexPod 数据中心客户可以使用他们习惯使用的工具来管理其 FlexPod 快速系统。新的 FlexPod Express 客户可以随着环境的增长轻松适应 FlexPod 数据中心的管理。

FlexPod Express 是远程办公室和分支机构（ ROBO ）以及中小型企业的最佳基础架构基础。对于希望为专用工作负载提供基础架构的客户来说，它也是最佳解决方案。

FlexPod Express 提供了一个易于管理的基础架构，几乎适合任何工作负载。

解决方案概述

此 FlexPod Express 解决方案是 FlexPod 融合基础架构计划的一部分。

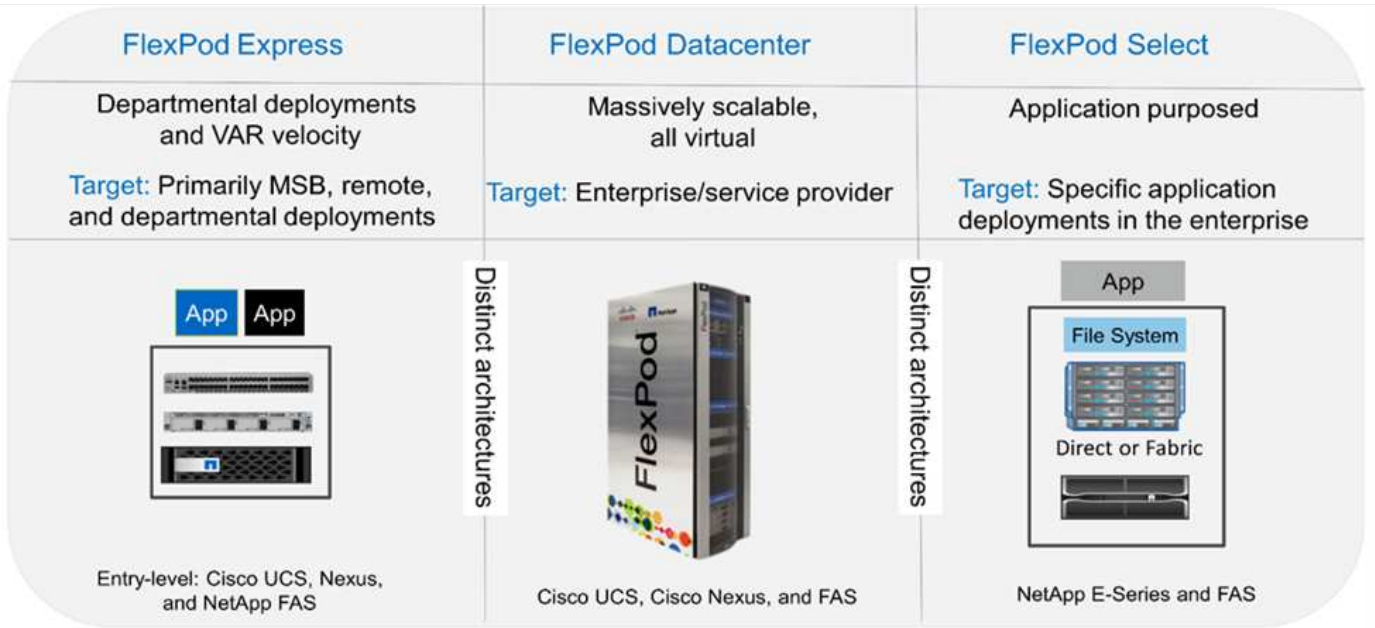
FlexPod 融合基础架构计划

FlexPod 参考架构以 Cisco 验证设计（CVD）或 NetApp 验证架构（NVA）的形式提供。如果给定 CVD 或 NVA 不会产生不受支持的配置，则允许根据客户要求进行差异。

如下图所示， FlexPod 计划包括三个解决方案： FlexPod Express ， FlexPod Datacenter 和 FlexPod Select：

- * FlexPod Express* 为客户提供了采用 Cisco 和 NetApp 技术的入门级解决方案。
- FlexPod 数据中心 * 为各种工作负载和应用程序提供了最佳的多用途基础。
- * FlexPod Select* 整合了 FlexPod 数据中心的最佳功能，并根据给定应用程序量身定制基础架构。

下图显示了解决方案的技术组件。



经验证的 **NetApp** 架构计划

NVA 计划为客户提供经过验证的 NetApp 解决方案架构。NVA 可提供具有以下特性的 NetApp 解决方案架构：

- 经过全面测试
- 具有规范性
- 最大限度地降低部署风险
- 加快上市速度

本指南详细介绍了采用直连 NetApp 存储的 FlexPod Express 的设计。以下各节列出了用于设计此解决方案的组件。

硬件组件

- NetApp AFF A220
- Cisco UCS Mini
- Cisco UCS B200 M5

- Cisco UCS VIC 1440/1480 。
- Cisco Nexus 3000 系列交换机

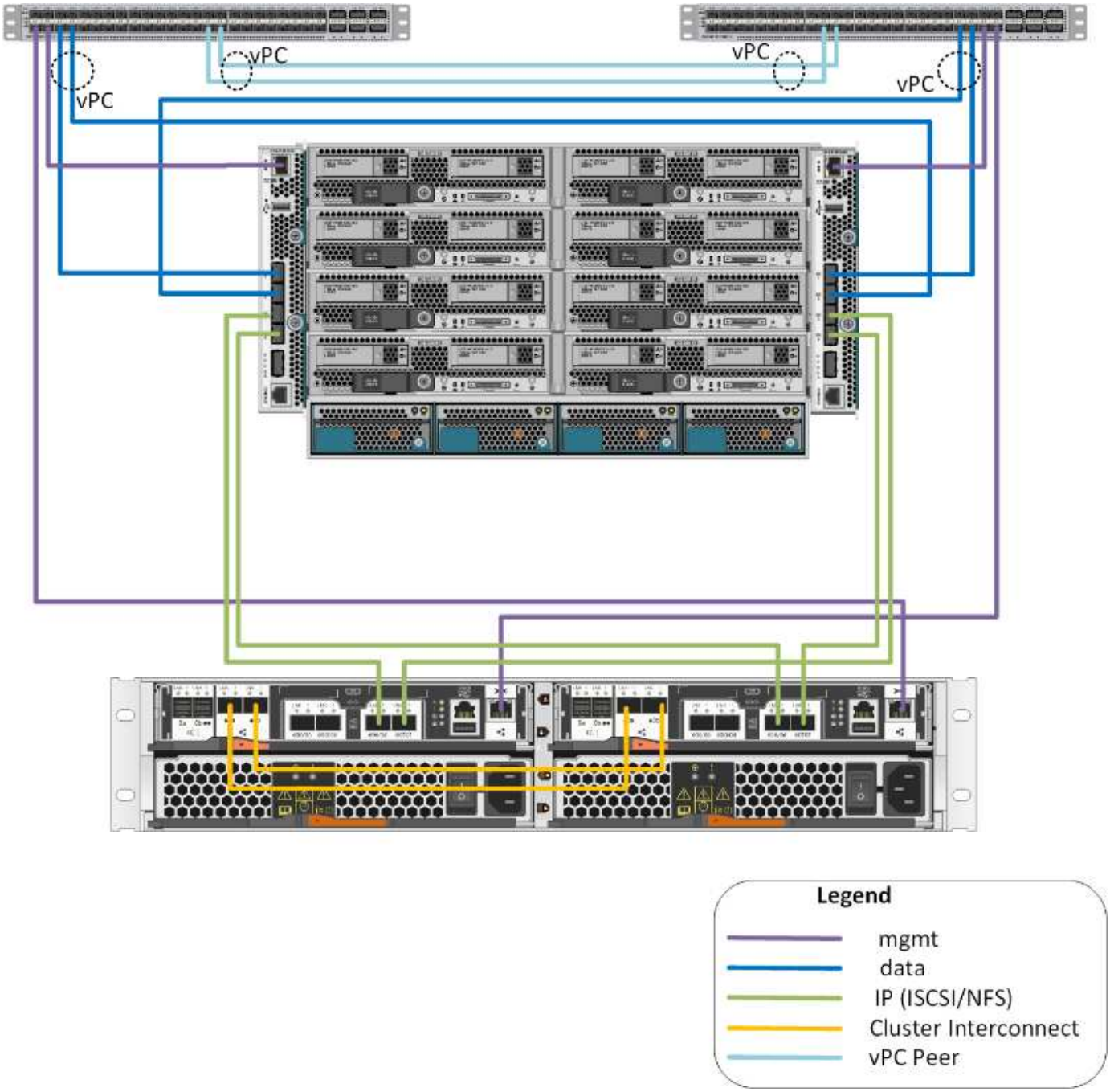
软件组件

- NetApp ONTAP 9.5.
- VMware vSphere 6.7U1
- Cisco UCS Manager 4.0 （ 1b ）
- Cisco NXOS 固件 7.0 （ 3 ） I6 （ 1 ）

解决方案技术

此解决方案利用了 NetApp ， Cisco 和 VMware 的最新技术。它采用运行 ONTAP 9.5 的全新 NetApp AFF A220 ，双 Cisco Nexus 31108PCV 交换机以及运行 VMware vSphere 6.7U1 的 Cisco UCS B200 M5 服务器。此经过验证的解决方案使用基于 10GbE 技术的直连 IP 存储。

下图展示了采用 VMware vSphere 6.7U1 基于 IP 的 Direct Connect 架构的 FlexPod Express 。



使用情形摘要

FlexPod Express 解决方案可应用于多种使用情形，包括以下情形：

- 自动运行
- 中小型企业
- 需要经济高效的专用解决方案的环境

FlexPod Express 最适合虚拟化和混合工作负载。

技术要求

FlexPod 快速系统需要硬件和软件组件的组合。FlexPod Express 还介绍了以两个单位向系统添加虚拟机管理程序节点所需的硬件组件。

硬件要求

无论选择何种虚拟机管理程序，所有 FlexPod 快速配置都使用相同的硬件。因此，即使业务需求发生变化，任何虚拟机管理程序都可以在同一个 FlexPod Express 硬件上运行。

下表列出了所有 FlexPod 快速配置所需的硬件组件。

硬件	数量
AFF A220 HA 对	1.
Cisco UCS B200 M5 服务器	2.
Cisco Nexus 31108PCV 交换机	2.
适用于 Cisco UCS B200 M5 服务器的 Cisco UCS 虚拟接口卡（ VIC ） 1440	2.
具有两个集成 UCS-FI-M-6324 互联阵列的 Cisco UCS Mini	1.

软件要求

下表列出了实施 FlexPod 快速解决方案架构所需的软件组件。

软件	**version**	详细信息
Cisco UCS Manager	4.0 （ 1b ）	适用于 Cisco UCS 互联阵列 FI-6324UP
Cisco 刀片式服务器软件	4.0 （ 1b ）	适用于 Cisco UCS B200 M5 服务器
Cisco nenic 驱动程序	1.0.25.0	适用于 Cisco VIC 1440 接口卡
Cisco NX-OS	7.0 （ 3 ） I6 （ 1 ）	适用于 Cisco Nexus 31108PCV 交换机
NetApp ONTAP	9.5	适用于 AFF A220 控制器

下表列出了在 FlexPod Express 上实施所有 VMware vSphere 所需的软件。

软件	**version**
VMware vCenter Server 设备	6.7U1
VMware vSphere ESXi 虚拟机管理程序	6.7U1

FlexPod 快速布线信息

下表介绍了参考验证布线。

下表列出了 Cisco Nexus 交换机 31108PCV A 的布线信息

本地设备	本地端口	远程设备	远程端口
Cisco Nexus 交换机 31108PCV A	Eth1/1	NetApp AFF A220 存储控制器 A	e0M
	eth1/2	Cisco UCS-Mini FI-A	mgmt0
	Eth1/3	Cisco UCS-Mini FI-A	Eth1/1
	ETH 1/4	Cisco UCS-迷你 FI-B	Eth1/1
	ETH 1/13	Cisco NX 31108PCV B	ETH 1/13
	ETH 1/14	Cisco NX 31108PCV B	ETH 1/14

下表列出了 Cisco Nexus 交换机 31108PCV B 的布线信息

本地设备	本地端口	远程设备	远程端口
Cisco Nexus 交换机 31108PCV B	Eth1/1	NetApp AFF A220 存储控制器 B	e0M
	eth1/2	Cisco UCS-迷你 FI-B	mgmt0
	Eth1/3	Cisco UCS-Mini FI-A	eth1/2
	ETH 1/4	Cisco UCS-迷你 FI-B	eth1/2
	ETH 1/13	Cisco NX 31108PCV A	ETH 1/13
	ETH 1/14	Cisco NX 31108PCV A	ETH 1/14

下表列出了 NetApp AFF A220 存储控制器 A 的布线信息

本地设备	本地端口	远程设备	远程端口
NetApp AFF A220 存储控制器 A	e0a	NetApp AFF A220 存储控制器 B	e0a
	e0b	NetApp AFF A220 存储控制器 B	e0b
	e0e	Cisco UCS-Mini FI-A	Eth1/3
	e0f	Cisco UCS-迷你 FI-B	Eth1/3
	e0M	Cisco NX 31108PCV A	Eth1/1

下表列出了 NetApp AFF A220 存储控制器 B 的布线信息

本地设备	本地端口	远程设备	远程端口
NetApp AFF A220 存储控制器 B	e0a	NetApp AFF A220 存储控制器 B	e0a
	e0b	NetApp AFF A220 存储控制器 B	e0b
	e0e	Cisco UCS-Mini FI-A	Eth1/4
	e0f	Cisco UCS-迷你 FI-B	Eth1/4
	e0M	Cisco NX 31108PCV B	Eth1/1

下表列出了 Cisco UCS 互联阵列 A 的布线信息

本地设备	本地端口	远程设备	远程端口
Cisco UCS 互联阵列 A	Eth1/1	Cisco NX 31108PCV A	Eth1/3
	eth1/2	Cisco NX 31108PCV B	Eth1/3
	Eth1/3	NetApp AFF A220 存储控制器 A	e0e
	Eth1/4	NetApp AFF A220 存储控制器 B	e0e
	mgmt0	Cisco NX 31108PCV A	eth1/2

下表列出了 Cisco UCS 互联阵列 B 的布线信息

本地设备	本地端口	远程设备	远程端口
Cisco UCS 互联阵列 B	Eth1/1	Cisco NX 31108PCV A	Eth1/4
	eth1/2	Cisco NX 31108PCV B	Eth1/4
	Eth1/3	NetApp AFF A220 存储控制器 A	e0f
	Eth1/4	NetApp AFF A220 存储控制器 B	e0f
	mgmt0	Cisco NX 31108PCV B	eth1/2

部署过程

本文档详细介绍了如何配置完全冗余，高可用性的 FlexPod Express 系统。为了反映这种冗余，在每个步骤中配置的组件称为组件 A 或组件 B例如，控制器 A 和控制器 B 可识别本文档中配置的两个 NetApp 存储控制器。交换机 A 和交换机 B 可识别一对 Cisco Nexus 交换机。互联阵列 A 和互联阵列 B 是两个集成 Nexus 互联阵列。

此外，本文档还介绍配置多个 Cisco UCS 主机的步骤，这些主机按顺序标识为服务器 A ，服务器 B 等。

要指示您应在步骤中包含与您的环境相关的信息，请在命令结构中显示 `<<text>>` 。请参见以下 `vlan create` 命令示例：

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

通过本文档，您可以完全配置 FlexPod 快速环境。在此过程中，您需要通过多个步骤插入客户专用的命名约定， IP 地址和虚拟局域网（ VLAN ）方案。下表介绍了部署所需的 VLAN ，如本指南所述。此表可根据特定站点变量填写，并用于实施文档配置步骤。

> 如果使用单独的带内和带外管理 VLAN ，则必须在它们之间创建第 3 层路由。在此验证中，使用了一个通用管理 VLAN 。

VLAN name	**VLAN** 用途	用于验证本文档的 **ID**
管理 VLAN	用于管理接口的 VLAN	18
原生 VLAN	将未标记的帧分配到的 VLAN	2.
NFS VLAN	用于 NFS 流量的 VLAN	104
VMware vMotion VLAN	为将虚拟机（ VM ）从一台物理主机移动到另一台物理主机而指定的 VLAN	103.
VM 流量 VLAN	用于 VM 应用程序流量的 VLAN	102.
iSCSI-A-VLAN	网络结构 A 上用于 iSCSI 流量的 VLAN	124.
iSCSI-B-VLAN	网络结构 B 上用于 iSCSI 流量的 VLAN	125.

在整个 FlexPod Express 配置过程中都需要 VLAN 编号。这些 VLAN 称为 `<<var_xxxx_vlan>>` ，其中 `xxxx` 是 VLAN 的用途（例如 iSCSI-A ）。

下表列出了创建的 VMware VM 。

VM 问题描述	主机名
VMware vCenter Server	Seahawks-vcsa.cie.netapp.com

Cisco Nexus 31108PCV 部署操作步骤

本节详细介绍了在 FlexPod Express 环境中使用的 Cisco Nexus 31308PCV 交换机配置。

Cisco Nexus 31108PCV 交换机的初始设置

此过程介绍如何配置 Cisco Nexus 交换机以在基础 FlexPod Express 环境中使用。

> 此操作步骤假定您使用的是运行 NX-OS 软件版本 7.0 （ 3 ） I6 （ 1 ）的 Cisco Nexus 31108PCV 。

1. 首次启动并连接到交换机的控制台端口后， Cisco NX-OS 设置将自动启动。此初始配置可解决基本设置，例如交换机名称， mgmt0 接口配置和安全 Shell （ SSH ）设置。
2. FlexPod 快速管理网络可以通过多种方式进行配置。31108PCV 交换机上的 mgmt0 接口可以连接到现有管

理网络，也可以采用背对背配置连接 31108PCV 交换机的 mgmt0 接口。但是，此链路不能用于外部管理访问，例如 SSH 流量。

在本部署指南中， FlexPod Express Cisco Nexus 31108PCV 交换机连接到现有管理网络。

3. 要配置 Cisco Nexus 31108PCV 交换机，请启动交换机并按照屏幕上的提示进行操作，如此处所示，对这两个交换机进行初始设置，并将相应的值替换为交换机特定信息。

```
This setup utility will guide you through the basic configuration of the
system. Setup configures only enough connectivity for management of the
system.
```

```
*Note: setup is mainly used for configuring the system initially, when
no configuration is present. So setup always assumes system defaults and
not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip
the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
Create another login account (yes/no) [n]: n
Configure read-only SNMP community string (yes/no) [n]: n
Configure read-write SNMP community string (yes/no) [n]: n
Enter the switch name : 31108PCV-A
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
Configure the default gateway? (yes/no) [y]: y
IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
Configure advanced IP options? (yes/no) [n]: n
Enable the telnet service? (yes/no) [n]: n
Enable the ssh service? (yes/no) [y]: y
Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
Number of rsa key bits <1024-2048> [1024]: <enter>
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address : <<var_ntp_ip>>
Configure default interface layer (L3/L2) [L2]: <enter>
Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]:
<enter>
```

4. 此时将显示配置摘要，系统会询问您是否要编辑此配置。如果配置正确，请输入 `n` 。

```
Would you like to edit the configuration? (yes/no) [n]: no
```

5. 然后，系统会询问您是否要使用此配置并保存它。如果是，请输入 `y` 。

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. 对 Cisco Nexus 交换机 B 重复步骤 1 到 5

启用高级功能

要提供其他配置选项，必须在 Cisco NX-OS 中启用某些高级功能。

1. 要在 Cisco Nexus 交换机 A 和交换机 B 上启用相应功能，请使用命令 `（config t）` 进入配置模式，然后运行以下命令：

```
feature interface-vlan
feature lacp
feature vpc
```

> 默认端口通道负载平衡哈希使用源 IP 地址和目标 IP 地址来确定端口通道中各个接口之间的负载平衡算法。除了源 IP 地址和目标 IP 地址之外，还可以为哈希算法提供更多输入，从而在端口通道的各个成员之间实现更好的分布。出于同样的原因， NetApp 强烈建议将源和目标 TCP 端口添加到哈希算法中。

2. 从配置模式 `（config t）` 中，运行以下命令，在 Cisco Nexus 交换机 A 和交换机 B 上设置全局端口通道负载平衡配置：

```
port-channel load-balance src-dst ip-l4port
```

执行全局生成树配置

Cisco Nexus 平台使用一种新的保护功能，称为网桥保证。如果设备不再运行生成树算法，则网桥保证有助于防止单向链路或其他软件故障继续转发数据流量。根据平台的不同，可以将端口置于多种状态之一，包括网络或边缘状态。

NetApp 建议设置网桥保证，以便默认情况下将所有端口都视为网络端口。此设置强制网络管理员查看每个端口的配置。此外，它还会显示最常见的配置错误，例如未标识的边缘端口或未启用网桥保证功能的邻居。此外，生成树块中的端口较多而不是太少会更安全，这样就可以使用默认端口状态来增强网络的整体稳定性。

添加服务器，存储和上行链路交换机时，请密切关注生成树的状态，尤其是在它们不支持网桥保证的情况下。在这种情况下，您可能需要更改端口类型才能使端口处于活动状态。

默认情况下，作为另一层保护，在边缘端口上启用网桥协议数据单元（ BPDU ）保护。为了防止网络中出现环路，如果在此接口上看到来自另一个交换机的 BPDU ，则此功能将关闭此端口。

在配置模式（`config t`）下，运行以下命令以配置 Cisco Nexus 交换机 A 和交换机 B 上的默认生成树选项，包括默认端口类型和 BPDU 保护：

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

定义 VLAN

在配置具有不同 VLAN 的各个端口之前，必须在交换机上定义第 2 层 VLAN 。此外，最好对 VLAN 进行命名，以便将来进行故障排除。

在配置模式（`config t`）下，运行以下命令来定义和描述 Cisco Nexus 交换机 A 和交换机 B 上的第 2 层 VLAN：

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

配置访问和管理端口说明

与为第 2 层 VLAN 分配名称一样，为所有接口设置说明有助于配置和故障排除。

在每个交换机的配置模式（`config t`）中，输入 FlexPod 快速大型配置的以下端口说明：

Cisco Nexus 交换机 A

```
int eth1/1
  description AFF A220-A e0M
int eth1/2
  description Cisco UCS FI-A mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/1
int eth1/4
  description Cisco UCS FI-B eth1/1
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

Cisco Nexus 交换机 B

```
int eth1/1
  description AFF A220-B e0M
int eth1/2
  description Cisco UCS FI-B mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/2
int eth1/4
  description Cisco UCS FI-B eth1/2
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

配置服务器和存储管理接口

服务器和存储的管理接口通常仅使用一个 VLAN 。因此，请将管理接口端口配置为访问端口。为每个交换机定义管理 VLAN ，并将生成树端口类型更改为边缘。

在配置模式（`config t`）下，运行以下命令为服务器和存储的管理接口配置端口设置：

Cisco Nexus 交换机 A

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus 交换机 B

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

添加 **NTP** 分发接口

Cisco Nexus 交换机 A

在全局配置模式下，执行以下命令。

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-a-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-b-ntp-ip> use-vrf default
```

Cisco Nexus 交换机 B

在全局配置模式下，执行以下命令。

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch- b-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-a-ntp-ip> use-vrf default
```

执行虚拟端口通道全局配置

通过虚拟端口通道（ vPC ），物理连接到两个不同 Cisco Nexus 交换机的链路可以显示为连接到第三个设备的单端口通道。第三个设备可以是交换机，服务器或任何其他网络设备。vPC 可以提供第 2 层多路径功能，通过增加带宽，在节点之间启用多个并行路径以及存在备用路径的负载平衡流量，您可以创建冗余。

vPC 具有以下优势：

- 允许单个设备在两个上游设备之间使用端口通道
- 消除生成树协议阻止的端口
- 提供无环路拓扑
- 使用所有可用的上行链路带宽
- 在链路或设备发生故障时提供快速融合
- 提供链路级别故障恢复能力

- 帮助提供高可用性

要使 vPC 功能正常运行，需要在两个 Cisco Nexus 交换机之间进行一些初始设置。如果使用背对背 mgmt0 配置，请使用接口上定义的地址，并使用 ping ` [switch_A/B_mgmt0_IP_addr]vrf` management 命令验证它们是否可以通信。

在配置模式（`config t`）下，运行以下命令为两台交换机配置 vPC 全局配置：

Cisco Nexus 交换机 A

```
vpc domain 1
 role priority 10
peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10description vPC peer-link
switchport
switchport mode trunkswitchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
  channel-group 14 mode active
copy run start
```

Cisco Nexus 交换机 B

```
vpc domain 1
peer-switch
role priority 20
peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10
description vPC peer-link
switchport
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
```

```
  channel-group 14 mode active
copy run start
```

> 在此解决方案验证中，使用的最大传输单元（ MTU ）为 9000 。但是，根据应用程序要求，您可以配置适当的 MTU 值。在整个 FlexPod 解决方案中设置相同的 MTU 值非常重要。组件之间的 MTU 配置不正确会导致数据包被丢弃。

通过上行链路连接到现有网络基础架构

根据可用的网络基础架构，可以使用多种方法和功能来上行链路连接 FlexPod 环境。如果存在现有的 Cisco Nexus 环境， NetApp 建议使用 vPC 通过上行链路将 FlexPod 环境中的 Cisco Nexus 31108PVC 交换机连接到基础架构中。对于 10GbE 基础架构解决方案，上行链路可以是 10GbE 上行链路，如果需要，上行链路可以是 1GbE 基础架构解决方案。可以使用上述过程创建到现有环境的上行链路 vPC 。配置完成后，请务必运行 copy run start 在每个交换机上保存配置。

NetApp 存储部署操作步骤（第 1 部分）

本节介绍 NetApp AFF 存储部署操作步骤。

NetApp 存储控制器 AFFxx 系列安装

NetApp Hardware Universe

。 "NetApp Hardware Universe" （ HWU ）应用程序可为任何特定的 ONTAP 版本提供受支持的硬件和软件组件。它提供了 ONTAP 软件当前支持的所有 NetApp 存储设备的配置信息。此外，还提供了一个组件兼容性表。

确认要安装的 ONTAP 版本支持您要使用的硬件和软件组件：

1. 访问 "HWU" 应用程序以查看系统配置指南。选择比较存储系统选项卡以查看不同版本的 ONTAP 软件与符合所需规格的 NetApp 存储设备之间的兼容性。
2. 或者，要按存储设备比较组件，请单击比较存储系统。

控制器 AFFXX 系列的前提条件
要规划存储系统的物理位置，请参见以下各节：电气要求支持的电源线板载端口和缆线

存储控制器

按照中控制器的物理安装过程进行操作 "AFF A220 文档"。

NetApp ONTAP 9.5

配置工作表

在运行设置脚本之前，请填写产品手册中的配置工作表。中提供了配置工作表 "《 ONTAP 9.5 软件设置指南》"（可在中使用 "ONTAP 9 文档中心"）。下表显示了 ONTAP 9.5 的安装和配置信息。

> 此系统在双节点无交换机集群配置中设置。

集群详细信息	集群详细信息值
集群节点 A IP 地址	<<var_nodeA_mgmt_ip>>
集群节点 A 网络掩码	<<var_nodeA_mgmt_mask>>
集群节点 A 网关	<<var_nodeA_mgmt_gateway>>
集群节点 A 名称	<<var_nodeA>>
集群节点 B IP 地址	<<var_nodeB_mgmt_ip>>
集群节点 B 网络掩码	<<var_nodeB_mgmt_mask>>
集群节点 B 网关	<<var_nodeB_mgmt_gateway>>
集群节点 B 名称	<<var_nodeB>>
ONTAP 9.5 URL	<<var_url_boot_software>>
集群的名称	<<var_clustername>>
集群管理 IP 地址	<<var_clustermgmt_ip>>
集群 B 网关	<<var_clustermgmt_gateway>>
集群 B 网络掩码	<<var_clustermgmt_mask>>
域名	<<var_domain_name>>
DNS 服务器 IP （您可以输入多个）	<<var_dns_server_ip>>
NTP 服务器 A IP	<< switch-A-NTP-IP >>
NTP 服务器 B IP	<< switch-b-ntp-ip >>

配置节点 **A**

要配置节点 A ，请完成以下步骤：

1. 连接到存储系统控制台端口。您应看到 Loader-A 提示符。但是，如果存储系统处于重新启动循环中，请在看到以下消息时按 Ctrl- C 退出自动启动循环：

   ```
   Starting AUTOBOOT press Ctrl-C to abort...
   ```

2. 允许系统启动。

   ```
   autoboot
   ```

3. 按 Ctrl- C 进入启动菜单。

   如果是 ONTAP 9 。5 不是要启动的软件版本，请继续执行以下步骤以安装新软件。如果是 ONTAP 9 。5 是要启动的版本，请选择选项 8 和 y 以重新启动节点。然后，继续执行步骤 14 。

4. 要安装新软件，请选择选项 `7` 。

5. 输入 `y` 执行升级。

6. 为要用于下载的网络端口选择 `e0M` 。
7. 输入 `y` 立即重新启动。
8. 在相应位置输入 e0M 的 IP 地址，网络掩码和默认网关。

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. 输入可在其中找到软件的 URL 。

   此 Web 服务器必须可执行 Ping 操作。

10. 按 Enter 输入用户名，表示无用户名。
11. 输入 `y` 将新安装的软件设置为后续重新启动所使用的默认软件。
12. 输入 `y` 以重新启动节点。

    安装新软件时，系统可能会对 BIOS 和适配器卡执行固件升级，从而导致重新启动，并可能在 Loader-A 提示符处停止。如果发生这些操作，系统可能会与此操作步骤有所偏差。

13. 按 Ctrl- C 进入启动菜单。
14. 为 Clean Configuration 和 Initialize All Disks 选择选项 `4` 。
15. 输入 `y` 将磁盘置零，重置配置并安装新的文件系统。
16. 输入 `y` 以擦除磁盘上的所有数据。

    根聚合的初始化和创建可能需要 90 分钟或更长时间才能完成，具体取决于所连接磁盘的数量和类型。初始化完成后，存储系统将重新启动。请注意， SSD 初始化所需的时间要少得多。您可以在节点 A 的磁盘置零时继续进行节点 B 配置。

17. 在节点 A 初始化期间，开始配置节点 B

配置节点 **B**

要配置节点 B ，请完成以下步骤：

1. 连接到存储系统控制台端口。您应看到 Loader-A 提示符。但是，如果存储系统处于重新启动循环中，请在看到以下消息时按 Ctrl-C 退出自动启动循环：

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. 按 Ctrl-C 进入启动菜单。

```
autoboot
```

3. 出现提示时，按 Ctrl-C 。

如果是 ONTAP 9 。5 不是要启动的软件版本，请继续执行以下步骤以安装新软件。如果要启动的是 ONTAP 9.4 版本，请选择选项 8 和 y 以重新启动节点。然后，继续执行步骤 14 。

4. 要安装新软件，请选择选项 7 。
5. 输入 `y` 执行升级。
6. 为要用于下载的网络端口选择 `e0M` 。
7. 输入 `y` 立即重新启动。
8. 在相应位置输入 e0M 的 IP 地址，网络掩码和默认网关。

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. 输入可在其中找到软件的 URL 。

   此 Web 服务器必须可执行 Ping 操作。

```
<<var_url_boot_software>>
```

10. 按 Enter 输入用户名，表示无用户名
11. 输入 `y` 将新安装的软件设置为后续重新启动所使用的默认软件。
12. 输入 `y` 以重新启动节点。

    安装新软件时，系统可能会对 BIOS 和适配器卡执行固件升级，从而导致重新启动，并可能在 Loader-A 提示符处停止。如果发生这些操作，系统可能会与此操作步骤有所偏差。

13. 按 Ctrl-C 进入启动菜单。
14. 选择选项 4 以清除配置并初始化所有磁盘。
15. 输入 `y` 将磁盘置零，重置配置并安装新的文件系统。
16. 输入 `y` 以擦除磁盘上的所有数据。

    根聚合的初始化和创建可能需要 90 分钟或更长时间才能完成，具体取决于所连接磁盘的数量和类型。初始化完成后，存储系统将重新启动。请注意， SSD 初始化所需的时间要少得多。

继续节点 **A** 配置和集群配置

从连接到存储控制器 A （节点 A ）控制台端口的控制台端口程序中，运行节点设置脚本。首次在节点上启动 ONTAP 9.5 时，将显示此脚本。

在 ONTAP 9.5 中，节点和集群设置操作步骤略有更改。现在，集群设置向导用于配置集群中的第一个节点，而 System Manager 用于配置集群。

1. 按照提示设置节点 A

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. 导航到节点管理接口的 IP 地址。

> 也可以使用命令行界面执行集群设置。本文档介绍如何使用 NetApp System Manager 引导式设置进行集群设置。

3. 单击引导式设置以配置集群。
4. 输入 `<<var_clustername>>` 作为集群名称，并为要配置的每个节点输入 `<<var_nodeA>>` 和 `<<var_nodeB>>` 。输入要用于存储系统的密码。选择无交换机集群作为集群类型。输入集群基本许可证。
5. 您还可以输入集群， NFS 和 iSCSI 的功能许可证。
6. 此时将显示一条状态消息，指出正在创建集群。此状态消息会循环显示多个状态。此过程需要几分钟时间。
7. 配置网络。
   a. 取消选择 IP 地址范围选项。
   b. 在集群管理 IP 地址字段中输入 `[var_clustermgmt_ip]` ，在网络掩码字段中输入 `[var_clustermgmt_mask]` ，在网关字段中输入 `[var_clustermgmt_gateway]` 。使用端口字段中的 …

选择器选择节点 A 的 e0M

c. 节点 A 的节点管理 IP 已填充。为节点 B 输入 ` <<var_nodeA_mgmt_ip>>`

d. 在 DNS 域名字段中输入 ` <<var_domain_name>>` 。在 DNS Server IP Address 字段中输入 ` <<var_dns_server_ip>>` 。

   您可以输入多个 DNS 服务器 IP 地址。

e. 在 Primary NTP Server 字段中输入 ` <<switch-A-NTP-IP>>` 。

   您也可以输入备用 NTP 服务器 ` <<switch- b-ntp-ip>>` 。

8. 配置支持信息。

   a. 如果您的环境需要代理来访问 AutoSupport ，请在代理 URL 中输入 URL 。

   b. 输入事件通知的 SMTP 邮件主机和电子邮件地址。

      您必须至少设置事件通知方法，然后才能继续操作。您可以选择任何方法。

9. 当指示集群配置已完成时，单击 Manage Your Cluster 以配置存储。

继续存储集群配置

配置存储节点和基础集群后，您可以继续配置存储集群。

将所有备用磁盘置零

要将集群中的所有备用磁盘置零，请运行以下命令：

```
disk zerospares
```

设置板载 **UTA2** 端口个性化设置

1. 运行 `ucadmin show` 命令，验证端口的当前模式和当前类型。

```
AFFA220-Clus::> ucadmin show
                       Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFFA220-Clus-01
              0c       cna      target     -        -          offline
AFFA220-Clus-01
              0d       cna      target     -        -          offline
AFFA220-Clus-01
              0e       cna      target     -        -          offline
AFFA220-Clus-01
              0f       cna      target     -        -          offline
AFFA220-Clus-02
              0c       cna      target     -        -          offline
AFFA220-Clus-02
              0d       cna      target     -        -          offline
AFFA220-Clus-02
              0e       cna      target     -        -          offline
AFFA220-Clus-02
              0f       cna      target     -        -          offline
8 entries were displayed.
```

2. 验证正在使用的端口的当前模式是否为 `CNA` ，当前类型是否设置为 **目标** 。如果不是，请运行以下命令来更改端口属性：

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

要运行上一个命令，端口必须处于脱机状态。要使端口脱机，请运行以下命令：

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

> 如果更改了端口属性，则必须重新启动每个节点，此更改才能生效。

启用 **Cisco** 发现协议

要在 NetApp 存储控制器上启用 Cisco 发现协议（ CDP ），请运行以下命令：

```
node run -node * options cdpd.enable on
```

在所有以太网端口上启用链路层发现协议

运行以下命令，以便在存储交换机和网络交换机之间交换链路层发现协议（Link -Layer Discovery Protocol，LLDP）邻居信息。此命令将在集群中所有节点的所有端口上启用 LLDP 。

```
node run * options lldp.enable on
```

重命名管理逻辑接口

要重命名管理逻辑接口（LIF），请完成以下步骤：

1. 显示当前管理 LIF 名称。

   ```
   network interface show -vserver <<clustername>>
   ```

2. 重命名集群管理 LIF 。

   ```
   network interface rename -vserver <<clustername>> -lif
   cluster_setup_cluster_mgmt_lif_1 -newname cluster_mgmt
   ```

3. 重命名节点 B 管理 LIF 。

   ```
   network interface rename -vserver <<clustername>> -lif
   cluster_setup_node_mgmt_lif_AFF A220_A_1 - newname AFF A220-01_mgmt1
   ```

在集群管理上设置自动还原

在集群管理界面上设置 `auto-revert` 参数。

```
network interface modify -vserver <<clustername>> -lif cluster_mgmt -auto-
revert true
```

设置服务处理器网络接口

要为每个节点上的服务处理器分配静态 IPv4 地址，请运行以下命令：

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

服务处理器 IP 地址应与节点管理 IP 地址位于同一子网中。

在 **ONTAP** 中启用存储故障转移

要确认已启用存储故障转移，请在故障转移对中运行以下命令：

1. 验证存储故障转移的状态。

   ```
   storage failover show
   ```

   ` [var_nodeA]` 和 ` [var_nodeB]` 都必须能够执行接管。如果节点可以执行接管，请转至步骤 3 。

2. 在两个节点之一上启用故障转移。

   ```
   storage failover modify -node <<var_nodeA>> -enabled true
   ```

3. 验证双节点集群的 HA 状态。

   此步骤不适用于具有两个以上节点的集群。

   ```
   cluster ha show
   ```

4. 如果配置了高可用性，请转至步骤 6 。如果配置了高可用性，则在发出命令时会显示以下消息：

   ```
   High Availability Configured: true
   ```

5. 仅为双节点集群启用 HA 模式。

   请勿对具有两个以上节点的集群运行此命令，因为它会导致故障转移出现问题。

   ```
   cluster ha modify -configured true
   Do you want to continue? {y|n}: y
   ```

6. 验证是否已正确配置硬件辅助，并根据需要修改配对 IP 地址。

```
storage failover hwassist show
```

消息 保活状态：错误：未收到配对节点发出的 `hwassist` 保活警报 表示未配置硬件协助。运行以下命令以配置硬件辅助。

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

在 **ONTAP** 中创建巨型帧 **MTU** 广播域

要创建 MTU 为 9000 的数据广播域，请运行以下命令：

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

从默认广播域中删除数据端口

10GbE 数据端口用于 iSCSI/NFS 流量，这些端口应从默认域中删除。不使用端口 e0e 和 e0f ，也应从默认域中删除。

要从广播域中删除端口，请运行以下命令：

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

禁用 **UTA2** 端口上的流量控制

NetApp 最佳实践是，在连接到外部设备的所有 UTA2 端口上禁用流量控制。要禁用流量控制，请运行以下命令：

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
```

与 ONTAP 的 Cisco UCS Mini 直接连接不支持 LACP 。

在 **NetApp ONTAP** 中配置巨型帧

要将 ONTAP 网络端口配置为使用巨型帧（ MTU 通常为 9， 000 字节），请从集群 Shell 运行以下命令：

```
AFF A220::> network port modify -node node_A -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_A -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
```

在 **ONTAP** 中创建 **VLAN**

要在 ONTAP 中创建 VLAN ，请完成以下步骤：

1. 创建 NFS VLAN 端口并将其添加到数据广播域。

```
network port vlan create -node <<var_nodeA>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create -node <<var_nodeA>> -vlan-name e0f-
<<var_nfs_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0f-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>: e0e- <<var_nfs_vlan_id>>, <<var_nodeB>>: e0e-
<<var_nfs_vlan_id>> , <<var_nodeA>>:e0f- <<var_nfs_vlan_id>>,
<<var_nodeB>>:e0f-<<var_nfs_vlan_id>>
```

2. 创建 iSCSI VLAN 端口并将其添加到数据广播域。

```
network port vlan create -node <<var_nodeA>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeA>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>: e0e- <<var_iscsi_vlan_A_id>>,<<var_nodeB>>: e0e-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>: e0f- <<var_iscsi_vlan_B_id>>,<<var_nodeB>>: e0f-
<<var_iscsi_vlan_B_id>>
```

3. 创建 MGMT-VLAN 端口。

```
network port vlan create -node <<var_nodeA>> -vlan-name e0m-
<<mgmt_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0m-
<<mgmt_vlan_id>>
```

在 **ONTAP** 中创建聚合

在 ONTAP 设置过程中，将创建一个包含根卷的聚合。要创建其他聚合，请确定聚合名称，要创建聚合的节点及其包含的磁盘数。

要创建聚合，请运行以下命令：

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

在配置中至少保留一个磁盘（选择最大的磁盘）作为备用磁盘。最佳做法是，每个磁盘类型和大小至少有一个备用磁盘。

从五个磁盘开始；您可以在需要额外存储时向聚合添加磁盘。

在磁盘置零完成之前，无法创建聚合。运行 `aggr show` 命令以显示聚合创建状态。在 `aggr1_nodeA` 联机之前，请勿继续操作。

在 ONTAP 中配置时区

要配置时间同步并设置集群上的时区，请运行以下命令：

```
timezone <<var_timezone>>
```

> 例如，在美国东部，时区为 `America/New_York` 。开始键入时区名称后，按 Tab 键查看可用选项。

在 ONTAP 中配置 SNMP

要配置 SNMP ，请完成以下步骤：

1. 配置 SNMP 基本信息，例如位置和联系人。轮询时，此信息在 SNMP 中显示为 `sysLocation` 和 `sysContact` 变量。

   ```
   snmp contact <<var_snmp_contact>>
   snmp location "<<var_snmp_location>>"
   snmp init 1
   options snmp.enable on
   ```

2. 配置 SNMP 陷阱以发送到远程主机。

   ```
   snmp traphost add <<var_snmp_server_fqdn>>
   ```

在 ONTAP 中配置 SNMPv1

要配置 SNMPv1 ，请设置名为社区的共享机密纯文本密码。

```
snmp community add ro <<var_snmp_community>>
```

> 请谨慎使用 `snmp community delete all` 命令。如果社区字符串用于其他监控产品，则此命令会将其删除。

在 ONTAP 中配置 SNMPv3

SNMPv3 要求您定义并配置用户进行身份验证。要配置 SNMPv3 ，请完成以下步骤：

1. 运行 `security snmpusers` 命令以查看引擎 ID 。
2. 创建名为 `snmpv3user` 的用户。

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. 输入权威实体的引擎 ID ，然后选择 `mD5` 作为身份验证协议。
4. 出现提示时，输入身份验证协议的最小长度为八个字符的密码。
5. 选择 `des` 作为隐私协议。
6. 出现提示时，输入隐私协议的最小长度为八个字符的密码。

在 ONTAP 中配置 AutoSupport HTTPS

NetApp AutoSupport 工具通过 HTTPS 向 NetApp 发送支持摘要信息。要配置 AutoSupport ，请运行以下命令：

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

创建 Storage Virtual Machine

要创建基础架构 Storage Virtual Machine （ SVM ），请完成以下步骤：

1. 运行 `vserver create` 命令。

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume- security-style unix
```

2. 将数据聚合添加到 NetApp VSC 的 infra-sVM 聚合列表中。

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. 从 SVM 中删除未使用的存储协议，而不使用 NFS 和 iSCSI 。

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. 在 infra-sVM SVM 中启用并运行 NFS 协议。

```
nfs create -vserver Infra-SVM -udp disabled
```

5. 打开 NetApp NFS VAAI 插件的 `SVM vStorage` 参数。然后，验证是否已配置 NFS 。

```
vserver nfs modify -vserver Infra-SVM -vstorage enabled
vserver nfs show
```

> 在命令行中，命令以 `vserver` 为前缀，因为 SVM 以前称为服务器

在 **ONTAP** 中配置 **NFSv3**

下表列出了完成此配置所需的信息。

详细信息	详细信息值
ESXi 主机 A NFS IP 地址	<<var_esxi_HostA_NFS_IP>>
ESXi 主机 B NFS IP 地址	<<var_esxi_HostB_NFS_IP>>

要在 SVM 上配置 NFS ，请运行以下命令：

1. 在默认导出策略中为每个 ESXi 主机创建一个规则。
2. 为要创建的每个 ESXi 主机分配一个规则。每个主机都有自己的规则索引。第一个 ESXi 主机的规则索引为 1 ，第二个 ESXi 主机的规则索引为 2 ，依此类推。

```
vserver export-policy rule create -vserver Infra-SVM -policyname default
-ruleindex 1 -protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys -rwrule sys -superuser sys -allow-suid falsevserver export-
policy rule create -vserver Infra-SVM -policyname default -ruleindex 2
-protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>> -rorule sys -rwrule
sys -superuser sys -allow-suid false
vserver export-policy rule show
```

3. 将导出策略分配给基础架构 SVM 根卷。

```
volume modify -vserver Infra-SVM -volume rootvol -policy default
```

> 如果您选择在设置 vSphere 后安装导出策略，则 NetApp VSC 会自动处理导出策略。如果不安装此服务器，则必须在添加其他 Cisco UCS B 系列服务器时创建导出策略规则。

在 **ONTAP** 中创建 **iSCSI** 服务

要创建 iSCSI 服务，请完成以下步骤：

1. 在 SVM 上创建 iSCSI 服务。此命令还会启动 iSCSI 服务并为 SVM 设置 iSCSI 限定名称（ IQN ）。验证是否已配置 iSCSI 。

```
iscsi create -vserver Infra-SVM
iscsi show
```

在 ONTAP 中创建 SVM 根卷的负载共享镜像

要在 ONTAP 中为 SVM 根卷创建负载共享镜像，请完成以下步骤：

1. 在每个节点上创建一个卷作为基础架构 SVM 根卷的负载共享镜像。

```
volume create -vserver Infra_Vserver -volume rootvol_m01 -aggregate
aggr1_nodeA -size 1GB -type DPvolume create -vserver Infra_Vserver
-volume rootvol_m02 -aggregate aggr1_nodeB -size 1GB -type DP
```

2. 创建作业计划，以便每 15 分钟更新一次根卷镜像关系。

```
job schedule interval create -name 15min -minutes 15
```

3. 创建镜像关系。

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. 初始化镜像关系并验证它是否已创建。

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol snapmirror
show
```

在 ONTAP 中配置 HTTPS 访问

要配置对存储控制器的安全访问，请完成以下步骤：

1. 提高访问证书命令的权限级别。

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. 通常，已有自签名证书。运行以下命令以验证证书：

```
security certificate show
```

3. 对于所示的每个 SVM ，证书公用名应与 SVM 的 DNS 完全限定域名（ FQDN ）匹配。四个默认证书应被删除，并替换为自签名证书或证书颁发机构提供的证书。

   最好在创建证书之前删除已过期的证书。运行 `security certificate delete` 命令删除已过期的证书。在以下命令中，使用 Tab completion 选择并删除每个默认证书。

```
security certificate delete [TAB] ...
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM - type server -serial 552429A6
```

4. 要生成并安装自签名证书，请一次性运行以下命令。为 infra-sVM 和集群 SVM 生成服务器证书。同样，请使用 Tab completion 帮助完成这些命令。

```
security certificate create [TAB] ...
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 - country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email- addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. 要获取以下步骤中所需参数的值，请运行 `security certificate show` 命令。
6. 使用 ` – server-enabled true` 和 ` – client-enabled false` 参数启用刚刚创建的每个证书。同样，请使用 Tab 补全。

```
security ssl modify [TAB] ...
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. 配置并启用 SSL 和 HTTPS 访问以及禁用 HTTP 访问。

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
System services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

> 其中某些命令通常会返回一条错误消息，指出此条目不存在。

8. 还原到管理员权限级别并创建设置以允许 Web 使用 SVM 。

```
set -privilege admin
vserver services web modify -name spi|ontapi|compat -vserver * -enabled
true
```

在 ONTAP 中创建 NetApp FlexVol 卷

要创建 NetApp FlexVol ® 卷，请输入卷名称，大小及其所在的聚合。创建两个 VMware 数据存储库卷和一个服务器启动卷。

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB - state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent- snapshot-space 0
volume create -vserver Infra-SVM -volume infra_datastore_2 -aggregate
aggr1_nodeB -size 500GB - state online -policy default -junction-path
/infra_datastore_2 -space-guarantee none -percent- snapshot-space 0
```

```
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -juntion-path /infra_swap -space
-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

在 ONTAP 中启用重复数据删除

要每天在相应卷上启用一次重复数据删除，请运行以下命令：

```
volume efficiency modify -vserver Infra-SVM -volume esxi_boot -schedule
sun-sat@0
volume efficiency modify -vserver Infra-SVM -volume infra_datastore_1
-schedule sun-sat@0
volume efficiency modify -vserver Infra-SVM -volume infra_datastore_2
-schedule sun-sat@0
```

在 ONTAP 中创建 LUN

要创建两个启动逻辑单元号（ LUN ），请运行以下命令：

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware - space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware - space-reserve disabled
```

添加额外的 Cisco UCS C 系列服务器时，必须创建额外的启动 LUN 。

在 **ONTAP** 中创建 **iSCSI LIF**

下表列出了完成此配置所需的信息。

详细信息	详细信息值
存储节点 A iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
存储节点 A iSCSI LIF01A 网络掩码	<<var_nodeA_iscsi_lif01a_mask>>
存储节点 A iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
存储节点 A iSCSI LIF01B 网络掩码	<<var_nodeA_iscsi_lif01b_mask>>
存储节点 B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
存储节点 B iSCSI LIF01A 网络掩码	<<var_nodeB_iscsi_lif01a_mask>>
存储节点 B iSCSI LIF01B	<<var_nodeB_iscsi_lif01b_ip>>
存储节点 B iSCSI LIF01B 网络掩码	<<var_nodeB_iscsi_lif01b_mask>>

1. 创建四个 iSCSI LIF ，每个节点两个。

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

在 **ONTAP** 中创建 **NFS LIF**

下表列出了完成此配置所需的信息。

详细信息	详细信息值
存储节点 A NFS LIF 01 A IP	<<var_nodeA_nfs_lif_01_A_IP>>
存储节点 A NFS LIF 01 网络掩码	<<var_nodeA_nfs_lif_01_A_mask>>
存储节点 A NFS LIF 01 b IP	<<var_nodeA_nfs_lif_01_b_ip>>
存储节点 A NFS LIF 01 b 网络掩码	<<var_nodeA_nfs_lif_01_b_mask>>
存储节点 B NFS LIF 02 A IP	<<var_nodeB_nfs_lif_02_A_IP>>
存储节点 B NFS LIF 02 A 网络掩码	<<var_nodeB_nfs_lif_02_A_mask>>
存储节点 B NFS LIF 02 b IP	<<var_nodeB_nfs_lif_02_b_ip>>
存储节点 B NFS LIF 02 b 网络掩码	<<var_nodeB_nfs_lif_02_b_mask>>

1. 创建 NFS LIF 。

```
network interface create -vserver Infra-SVM -lif nfs_lif01_a -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0e-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_a_ip>> - netmask <<
var_nodeA_nfs_lif_01_a_mask>> -status-admin up -failover-policy
broadcast-domain-wide - firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif01_b -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0f-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_b_ip>> - netmask <<
var_nodeA_nfs_lif_01_b_mask>> -status-admin up -failover-policy
broadcast-domain-wide - firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_a -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0e-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_a_ip>> - netmask <<
var_nodeB_nfs_lif_02_a_mask>> -status-admin up -failover-policy
broadcast-domain-wide - firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_b -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0f-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_b_ip>> - netmask <<
var_nodeB_nfs_lif_02_b_mask>> -status-admin up -failover-policy
broadcast-domain-wide - firewall-policy data -auto-revert true
network interface show
```

添加基础架构 **SVM** 管理员

下表列出了完成此配置所需的信息。

详细信息	详细信息值
Vsmgmt IP	<<var_svm_mgmt_ip>>
Vsmgmt 网络掩码	<<var_svm_mgmt_mask>>
Vsmgmt 默认网关	<<var_svm_mgmt_gateway>>

要将基础架构 SVM 管理员和 SVM 管理 LIF 添加到管理网络，请完成以下步骤：

1. 运行以下命令：

```
network interface create -vserver Infra-SVM -lif vsmgmt -role data
-data-protocol none -home-node <<var_nodeB>> -home-port e0M -address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> - status-admin up
-failover-policy broadcast-domain-wide -firewall-policy mgmt -auto-
revert true
```

> 此处的 SVM 管理 IP 应与存储集群管理 IP 位于同一子网中。

2. 创建一个默认路由，以使 SVM 管理接口能够访问外部环境。

```
network route create -vserver Infra-SVM -destination 0.0.0.0/0 -gateway
<<var_svm_mgmt_gateway>> network route show
```

3. 为 SVM `vsadmin` 用户设置密码并解除锁定此用户。

```
security login password -username vsadmin -vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock -username vsadmin -vserver
```

Cisco UCS 服务器配置

FlexPod Cisco UCS 基础

对 FlexPod 环境中的 Cisco UCS 6324 互联阵列执行初始设置。

本节详细介绍了使用 FlexPod UCS Manger 配置 Cisco UCS 以在 Cisco ROBO 环境中使用的过程。

Cisco UCS 互联阵列 6324 A

Cisco UCS 使用访问层网络和服务器。这款高性能下一代服务器系统为数据中心提供了高度工作负载灵活性和可扩展性。

Cisco UCS Manager 4.0 （ 1b ）支持 6324 互联阵列，该互联阵列可将互联阵列集成到 Cisco UCS 机箱中，并为较小的部署环境提供集成解决方案。Cisco UCS Mini 可简化系统管理，并为低规模部署节省成本。

硬件和软件组件支持 Cisco 的统一网络结构，该网络结构可通过一个融合网络适配器运行多种类型的数据中心流量。

初始系统设置

首次访问 Cisco UCS 域中的互联阵列时，设置向导会提示您提供配置系统所需的以下信息：

- 安装方法（ GUI 或 CLI ）
- 设置模式（从完整系统备份或初始设置还原）
- 系统配置类型（独立或集群配置）
- 系统名称
- 管理员密码
- 管理端口 IPv4 地址和子网掩码或 IPv6 地址和前缀
- 默认网关 IPv4 或 IPv6 地址
- DNS 服务器 IPv4 或 IPv6 地址
- 默认域名

下表列出了在互联阵列 A 上完成 Cisco UCS 初始配置所需的信息

详细信息	详细信息 / 值
系统名称	<<var_UCS_clustername>>
管理员密码	<<var_password>>
管理 IP 地址：互联阵列 A	<<var_UCSA_mgmt_IP>>
管理网络掩码：互联阵列 A	<<var_UCSA_mgmt_mask>>
默认网关：互联阵列 A	<<var_UCSA_mgmt_gateway>>
集群 IP 地址	<<var_UCS_cluster_IP>>
DNS 服务器 IP 地址	<<var_nameserver_ip>>
域名	<<var_domain_name>>

要配置要在 FlexPod 环境中使用的 Cisco UCS ，请完成以下步骤：

1. 连接到第一个 Cisco UCS 6324 互联阵列 A 上的控制台端口

```
Enter the configuration method. (console/gui) ? console

  Enter the setup mode; setup newly or restore from backup.
(setup/restore) ? setup

  You have chosen to setup a new Fabric interconnect. Continue? (y/n): y

  Enforce strong password? (y/n) [y]: Enter

  Enter the password for "admin":<<var_password>>
  Confirm the password for "admin":<<var_password>>

  Is this Fabric interconnect part of a cluster(select 'no' for
standalone)? (yes/no) [n]: yes

  Enter the switch fabric (A/B) []: A

  Enter the system name: <<var_ucs_clustername>>

  Physical Switch Mgmt0 IP address : <<var_ucsa_mgmt_ip>>

  Physical Switch Mgmt0 IPv4 netmask : <<var_ucsa_mgmt_mask>>

  IPv4 address of the default gateway : <<var_ucsa_mgmt_gateway>>

  Cluster IPv4 address : <<var_ucs_cluster_ip>>

  Configure the DNS Server IP address? (yes/no) [n]: y

       DNS IP address : <<var_nameserver_ip>>

  Configure the default domain name? (yes/no) [n]: y
Default domain name: <<var_domain_name>>

  Join centralized management environment (UCS Central)? (yes/no) [n]:
no

 NOTE: Cluster IP will be configured only after both Fabric
Interconnects are initialized. UCSM will be functional only after peer
FI is configured in clustering mode.

  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. 查看控制台上显示的设置。如果正确，请使用问题解答 `yes` 应用并保存配置。
3. 等待登录提示符，确认配置已保存。

下表列出了在互联阵列 B 上完成 Cisco UCS 初始配置所需的信息

详细信息	详细信息 / 值
系统名称	<<var_UCS_clustername>>
管理员密码	<<var_password>>
管理 IP 地址 FI B	<<var_UCSB_mgmt_ip>>
管理网络掩码— FI B	<<var_UCSB_mgmt_mask>>
默认网关 FI B	<<var_UCSB_mgmt_gateway>>
集群 IP 地址	<<var_UCS_cluster_IP>>
DNS 服务器 IP 地址	<<var_nameserver_ip>>
域名	<<var_domain_name>>

1. 连接到第二个 Cisco UCS 6324 互联阵列 B 上的控制台端口

```
 Enter the configuration method. (console/gui) ? console

  Installer has detected the presence of a peer Fabric interconnect.
This Fabric interconnect will be added to the cluster. Continue (y/n) ?
y

  Enter the admin password of the peer Fabric
interconnect:<<var_password>>
    Connecting to peer Fabric interconnect... done
    Retrieving config from peer Fabric interconnect... done
    Peer Fabric interconnect Mgmt0 IPv4 Address: <<var_ucsb_mgmt_ip>>
    Peer Fabric interconnect Mgmt0 IPv4 Netmask: <<var_ucsb_mgmt_mask>>
    Cluster IPv4 address: <<var_ucs_cluster_address>>

    Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric
Interconnect Mgmt0 IPv4 Address

  Physical Switch Mgmt0 IP address : <<var_ucsb_mgmt_ip>>


  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. 等待登录提示确认配置已保存。

登录到 **Cisco UCS Manager** 。

要登录到 Cisco Unified Computing System （ UCS ）环境，请完成以下步骤：

1. 打开 Web 浏览器并导航到 Cisco UCS 互联阵列集群地址。

   在配置第二个互联阵列后，您可能需要至少等待 5 分钟才能启动 Cisco UCS Manager 。

2. 单击 Launch UCS Manager 链接以启动 Cisco UCS Manager 。
3. 接受所需的安全证书。
4. 出现提示时，输入 admin 作为用户名，然后输入管理员密码。
5. 单击 Login 以登录到 Cisco UCS Manager 。

Cisco UCS Manager 软件版本 **4.0** （ **1b** ）

本文档假设使用的是 Cisco UCS Manager 软件 4.0 （ 1b ）版。要升级 Cisco UCS Manager 软件和 Cisco UCS 6324 互联阵列软件，请参见 "《 Cisco UCS Manager 安装和升级指南》。"

配置 **Cisco UCS** 自动通报

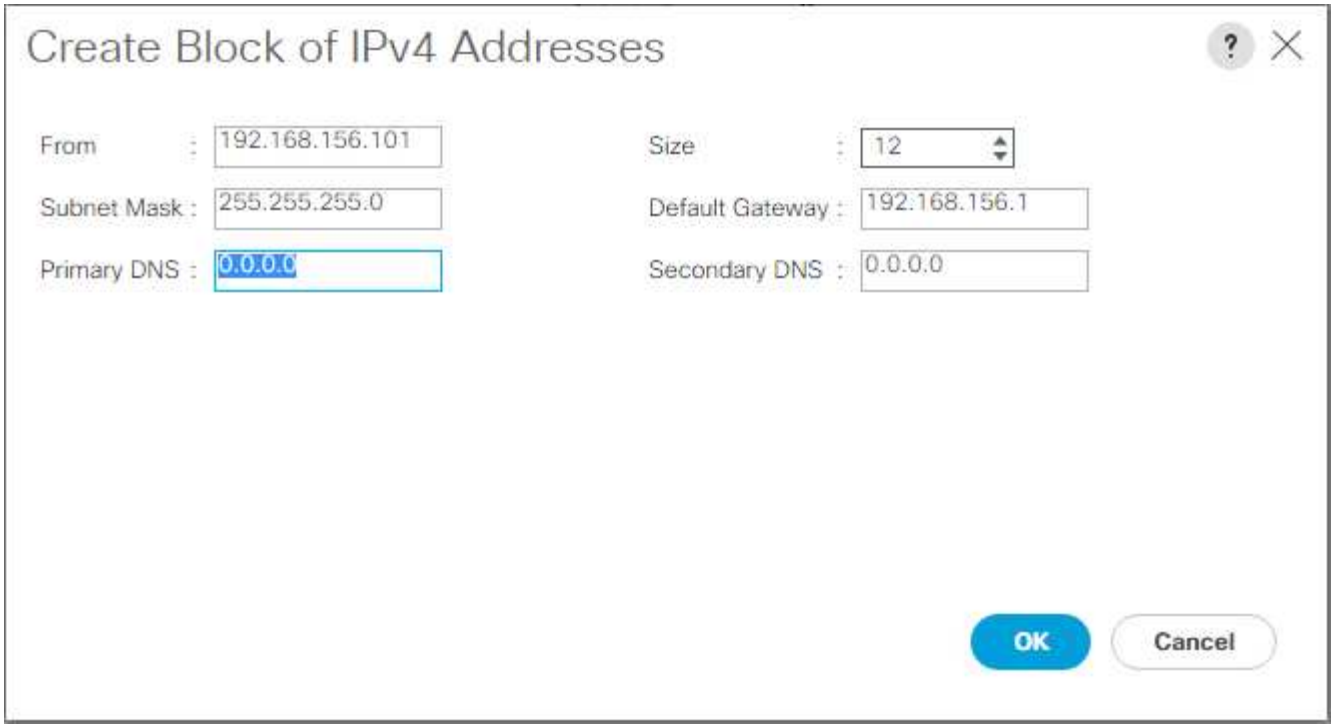
Cisco 强烈建议您在 Cisco UCS Manager 中配置自动通报。配置自动通报可加快解决支持案例的速度。要配置自动通报，请完成以下步骤：

1. 在 Cisco UCS Manager 中，单击左侧的 Admin 。
2. 选择 All > Communication Management > Call Home 。
3. 将 "State" 更改为 "On" 。
4. 根据您的管理首选项填写所有字段，然后单击 Save Changes 和 OK 完成自动通报配置。

添加用于访问键盘，视频和鼠标的 **IP** 地址块

要在 Cisco UCS 环境中为带内服务器键盘，视频，鼠标（ KVM ）访问创建一个 IP 地址块，请完成以下步骤：

1. 在 Cisco UCS Manager 中，单击左侧的 LAN 。
2. 展开 Pools > root > IP Pools 。
3. 右键单击 IP Pool ext-mgmt 并选择 Create Block of IPv4 addresses 。
4. 输入块的起始 IP 地址，所需的 IP 地址数以及子网掩码和网关信息。



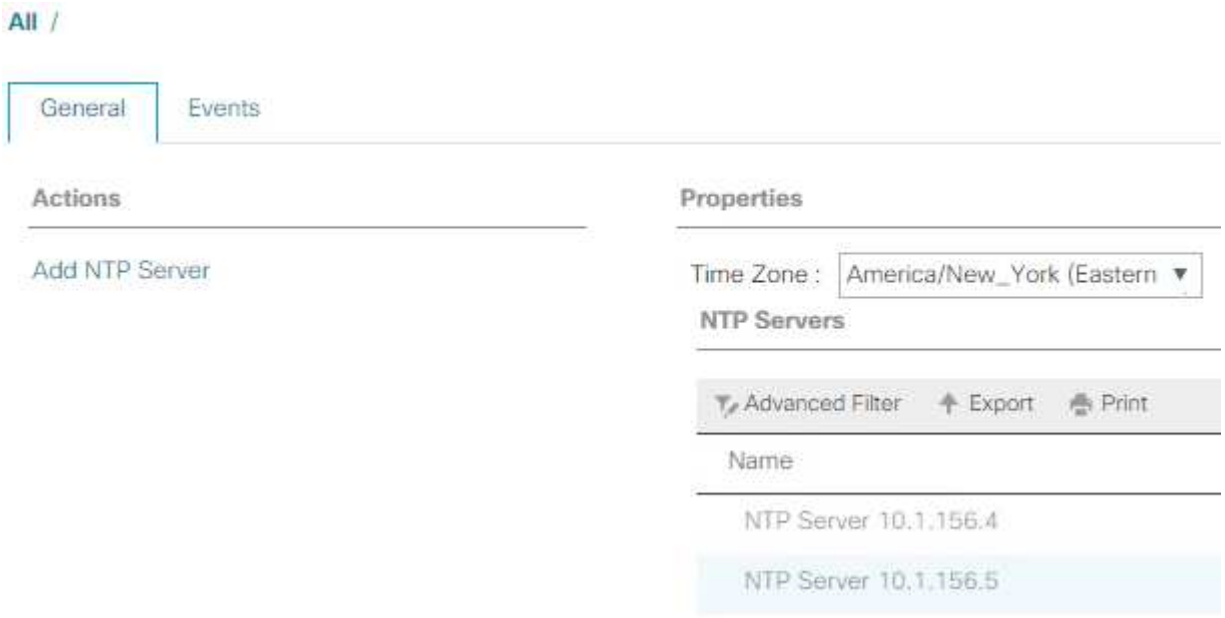
5. 单击确定以创建块。
6. 单击确认消息中的确定。

将 **Cisco UCS** 同步到 **NTP**

要将 Cisco UCS 环境与 Nexus 交换机中的 NTP 服务器同步，请完成以下步骤：

1. 在 Cisco UCS Manager 中，单击左侧的 Admin 。
2. 展开全部 > 时区管理。
3. 选择时区。
4. 在属性窗格的时区菜单中，选择相应的时区。
5. 单击 Save Changes ，然后单击 OK 。
6. 单击添加 NTP 服务器。
7. 输入 ` <switch-A-NTP-IP> 或 <Nexus a-mgmt-IP>` ，然后单击 OK 。单击确定。

8. 单击添加 NTP 服务器。
9. 输入 ` <switch-b-ntp-ip>` 或 `<Nexus B-mgmt-ip>` ，然后单击 OK 。单击确认后的确定。



编辑机箱发现策略

设置发现策略可简化添加 Cisco UCS B 系列机箱和其他阵列扩展器的过程，以进一步实现 Cisco UCS C 系列连接。要修改机箱发现策略，请完成以下步骤：

1. 在 Cisco UCS Manager 中，单击左侧的设备，然后在第二个列表中选择设备。
2. 在右侧窗格中，选择策略选项卡。
3. 在全局策略下，设置机箱 /FEX 发现策略以匹配机箱或阵列扩展器（ FEX ）与互联阵列之间连接的最小上行链路端口数。
4. 将链路分组首选项设置为端口通道。如果要设置的环境包含大量多播流量，请将 " 多播硬件哈希 " 设置设置为 " 已启用 " 。
5. 单击 Save Changes 。
6. 单击确定。

启用服务器，上行链路和存储端口

要启用服务器和上行链路端口，请完成以下步骤：

1. 在 Cisco UCS Manager 的导航窗格中，选择设备选项卡。
2. 展开设备 > 互联阵列 > 互联阵列 A > 固定模块。
3. 展开以太网端口。
4. 选择连接到 Cisco Nexus 31108 交换机的端口 1 和 2 ，右键单击，然后选择配置为上行链路端口。
5. 单击是确认上行链路端口，然后单击确定。
6. 选择连接到 NetApp 存储控制器的端口 3 和 4 ，右键单击，然后选择配置为设备端口。
7. 单击是确认设备端口。
8. 在配置为设备端口窗口中，单击确定。
9. 单击确定进行确认。
10. 在左窗格中，选择互联阵列 A 下的固定模块
11. 在以太网端口选项卡的 If role 列中，确认端口配置正确。如果在可扩展性端口上配置了任何端口 C 系列服务器，请单击该端口以验证该端口的端口连接。

Equipment / Fabric Interconnects / Fabric Interconnect A (subordinate) / Fixed Module

General | Ethernet Ports | FC Ports | Faults | Events

Advanced Filter | Export | Print | All | Unconfigured | Network | Server | FCoE Uplink | Unified Uplink | Appliance Storage | FCoE Storage | Unified Storage | Monitor

Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer
1	0	1	00:DE:FB:30:36:88	Network	Physical	Up	Enabled	
1	0	2	00:DE:FB:30:36:89	Network	Physical	Up	Enabled	
1	0	3	00:DE:FB:30:36:8A	Appliance Storage	Physical	Up	Enabled	
1	0	4	00:DE:FB:30:36:8B	Appliance Storage	Physical	Up	Enabled	
1	5	1	00:DE:FB:30:36:8C	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	2	00:DE:FB:30:36:8D	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	3	00:DE:FB:30:36:8E	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	4	00:DE:FB:30:36:8F	Unconfigured	Physical	Sfp Not Present	Disabled	

12. 展开设备 > 互联阵列 > 互联阵列 B > 固定模块。
13. 展开以太网端口。
14. 选择连接到 Cisco Nexus 31108 交换机的以太网端口 1 和 2 ，右键单击，然后选择配置为上行链路端口。
15. 单击是确认上行链路端口，然后单击确定。
16. 选择连接到 NetApp 存储控制器的端口 3 和 4 ，右键单击，然后选择配置为设备端口。
17. 单击是确认设备端口。
18. 在配置为设备端口窗口中，单击确定。
19. 单击确定进行确认。

20. 在左窗格中，选择互联阵列 B 下的固定模块
21. 在以太网端口选项卡的 If role 列中，确认端口配置正确。如果在可扩展性端口上配置了任何端口 C 系列服务器，请单击它以验证该端口的端口连接。

Equipment / Fabric Interconnects / Fabric Interconnect B (primar... / Fixed Module / Ethernet Ports

Ethernet Ports

Advanced Filter | Export | Print | All | Unconfigured | Network | Server | FCoE Uplink | Unified Uplink | Appliance Storage | FCoE Storage | Unified Storage | Monitor

Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer
1	0	1	00:DE:FB:30:3A:C8	Network	Physical	Up	Enabled	
1	0	2	00:DE:FB:30:3A:C9	Network	Physical	Up	Enabled	
1	0	3	00:DE:FB:30:3A:CA	Appliance Storage	Physical	Up	Enabled	
1	0	4	00:DE:FB:30:3A:CB	Appliance Storage	Physical	Up	Enabled	
1	5	1	00:DE:FB:30:3A:CC	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	2	00:DE:FB:30:3A:CD	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	3	00:DE:FB:30:3A:CE	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	4	00:DE:FB:30:3A:CF	Unconfigured	Physical	Sfp Not Present	Disabled	

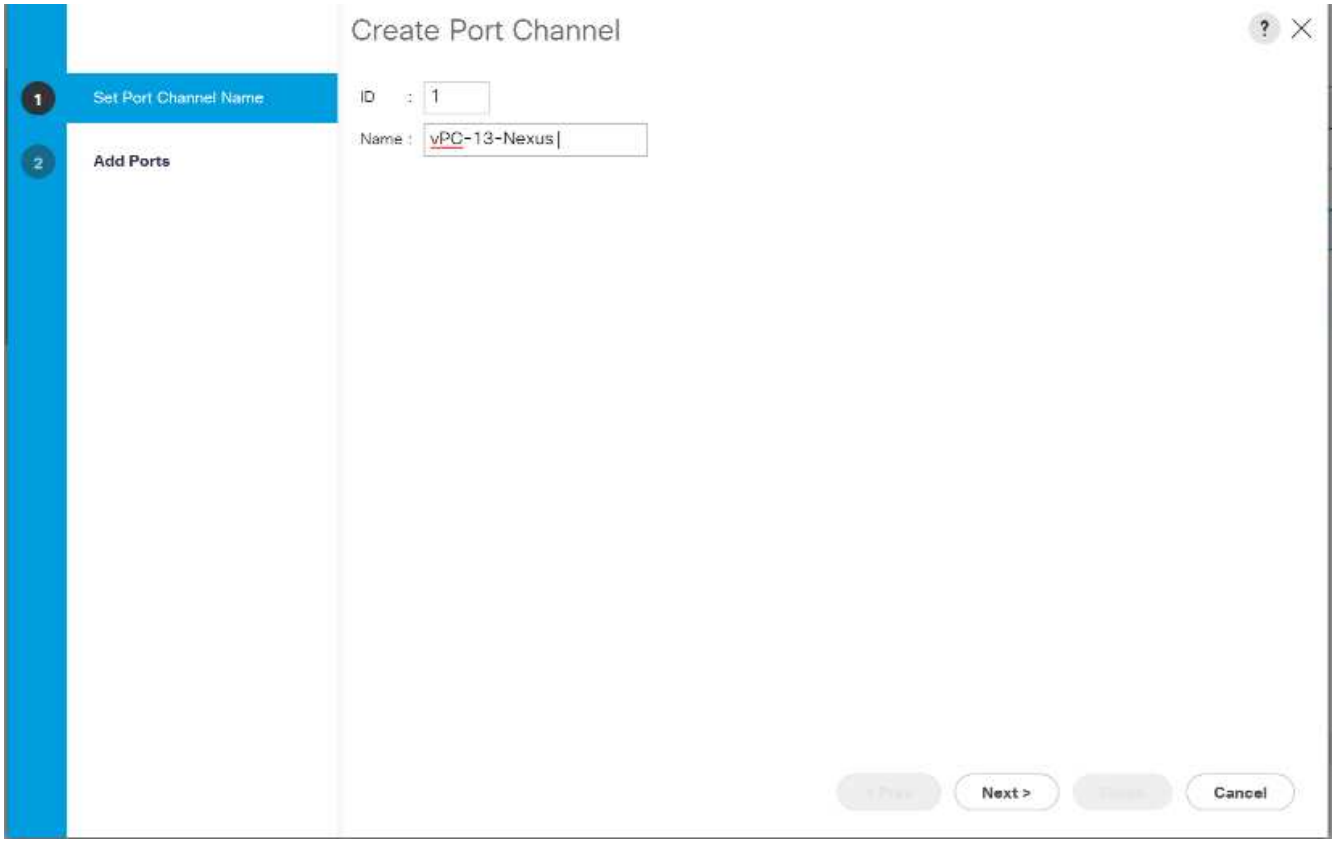
创建到 **Cisco Nexus 31108** 交换机的上行链路端口通道

要在 Cisco UCS 环境中配置所需的端口通道，请完成以下步骤：

1. 在 Cisco UCS Manager 中，选择导航窗格中的 LAN 选项卡。

> 在此操作步骤中，将创建两个端口通道：一个从阵列 A 到两个 Cisco Nexus 31108 交换机，另一个从阵列 B 到两个 Cisco Nexus 31108 交换机。如果使用的是标准交换机，请相应地修改此操作步骤。如果在互联阵列上使用 1 Gb 以太网（1GbE）交换机和 GLC-T SFP，则互联阵列中以太网端口 1/1 和 1/2 的接口速度必须设置为 1 Gbps 。

2. 在 "LAN">"LAN Cloud " 下，展开 "Fabric A 树 " 。
3. 右键单击端口通道。
4. 选择创建端口通道。
5. 输入 13 作为端口通道的唯一 ID 。
6. 输入 vPC-13-Nexus 作为端口通道的名称。
7. 单击下一步。



8. 选择要添加到端口通道的以下端口：
   a. 插槽 ID 1 和端口 1
   b. 插槽 ID 1 和端口 2
9. 单击 >> 将端口添加到端口通道。
10. 单击完成以创建端口通道。单击确定。
11. 在端口通道下，选择新创建的端口通道。

    端口通道的整体状态应为 " 已启动 " 。

12. 在导航窗格中的 "LAN">"LAN Cloud" 下，展开 Fabric B 树。
13. 右键单击端口通道。
14. 选择创建端口通道。
15. 输入 14 作为端口通道的唯一 ID 。
16. 输入 vPC-14-Nexus 作为端口通道的名称。单击下一步。
17. 选择要添加到端口通道的以下端口：
    a. 插槽 ID 1 和端口 1
    b. 插槽 ID 1 和端口 2
18. 单击 >> 将端口添加到端口通道。
19. 单击完成以创建端口通道。单击确定。
20. 在端口通道下，选择新创建的端口通道。

21. 端口通道的整体状态应为 " 已启动 " 。

创建组织（可选）

组织用于组织资源并限制对 IT 组织内各个组的访问，从而实现计算资源的多租户。

> 尽管本文档不假定使用组织，但本操作步骤提供了有关创建组织的说明。

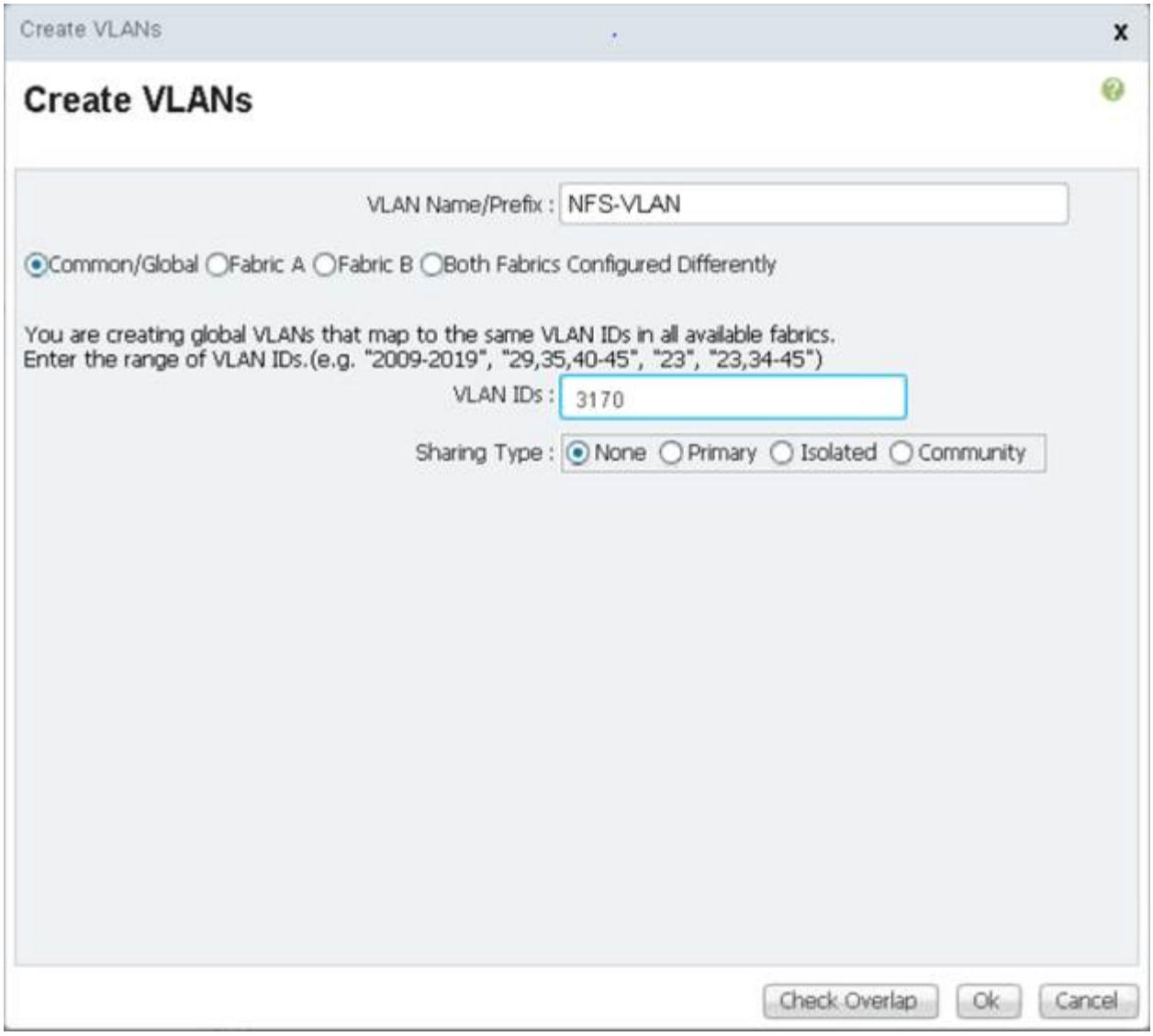
要在 Cisco UCS 环境中配置组织，请完成以下步骤：

1. 在 Cisco UCS Manager 中，从窗口顶部工具栏的 " 新建 " 菜单中选择 " 创建组织 " 。
2. 输入组织名称。
3. 可选：输入组织的问题描述。单击确定。
4. 单击确认消息中的确定。

配置存储设备端口和存储 **VLAN**

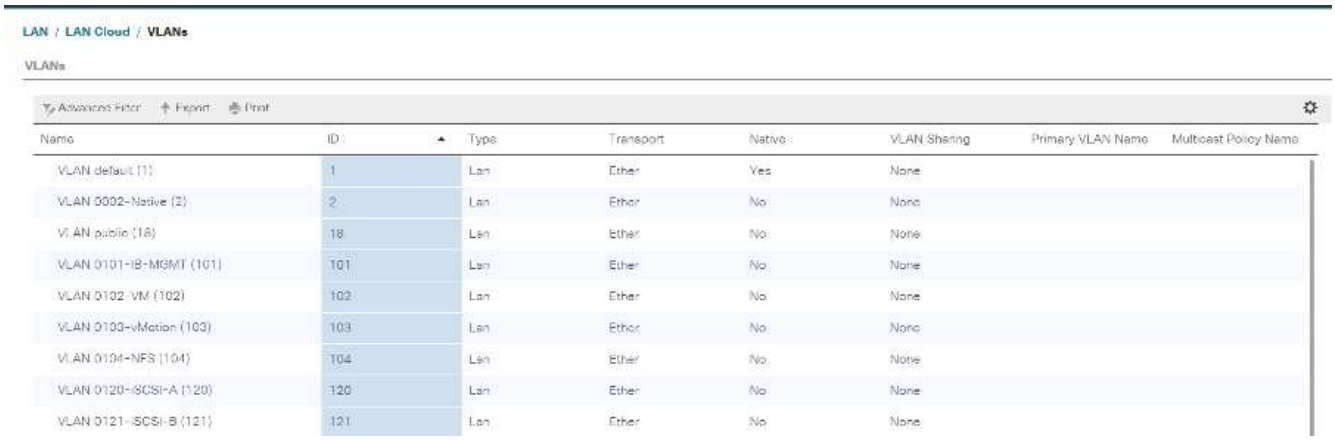
要配置存储设备端口和存储 VLAN ，请完成以下步骤：

1. 在 Cisco UCS Manager 中，选择 LAN 选项卡。
2. 扩展设备云。
3. 右键单击设备云下的 VLAN 。
4. 选择 Create VLAN 。
5. 输入 nfs-vlan 作为基础架构 NFS VLAN 的名称。
6. 保持选中通用 / 全局。
7. 输入 ` <<var_nfs_vlan_id>>` 作为 VLAN ID 。
8. 将 "Sharing Type" 设置为 "None" 。

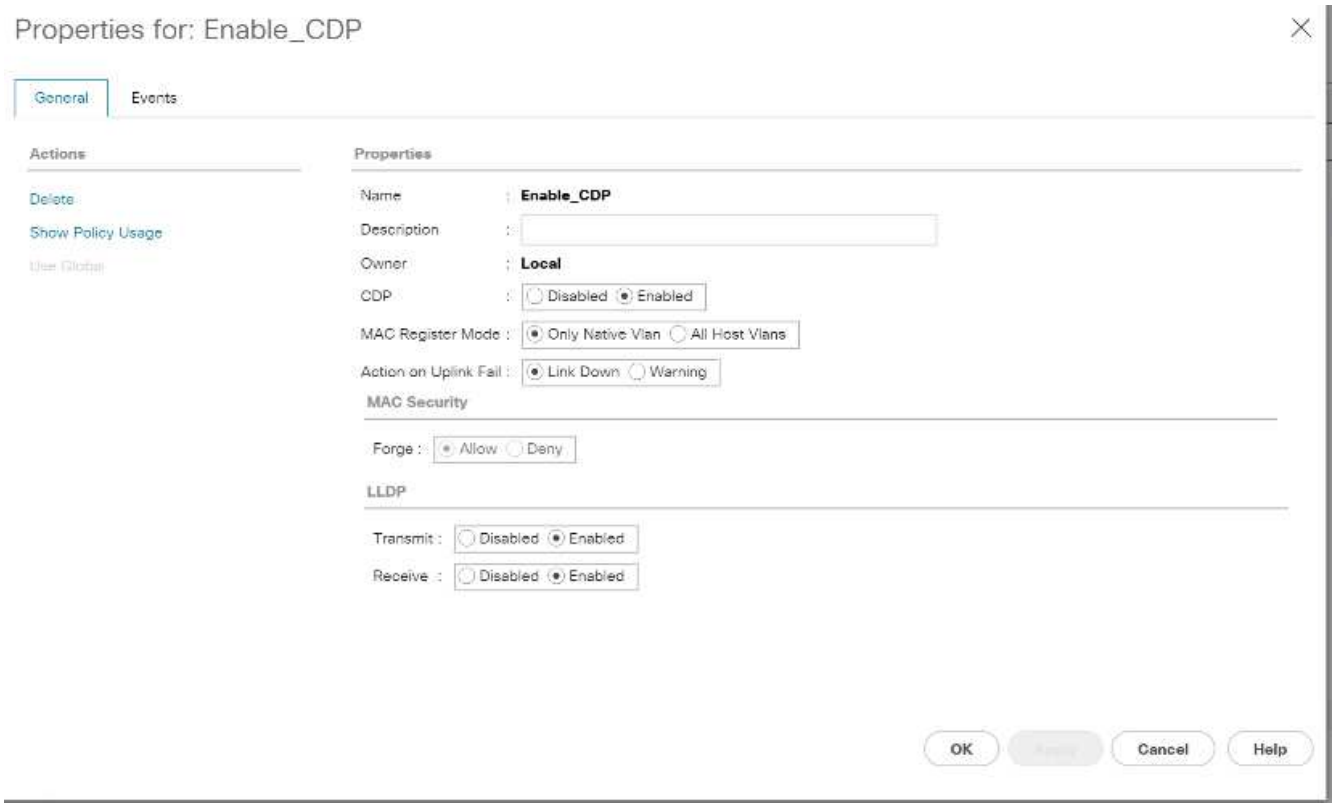


9. 单击确定，然后再次单击确定以创建 VLAN 。
10. 右键单击设备云下的 VLAN 。
11. 选择 Create VLAN 。
12. 输入 iSCSI-A-VLAN 作为基础架构 iSCSI 阵列 A VLAN 的名称。
13. 保持选中通用 / 全局。
14. 输入 ` <<var_iscsi-A_VLAN_id>>` 作为 VLAN ID 。
15. 单击确定，然后再次单击确定以创建 VLAN 。
16. 右键单击设备云下的 VLAN 。
17. 选择 Create VLAN 。
18. 输入 iscsi-B-VLAN 作为基础架构 iSCSI 阵列 B VLAN 的名称。
19. 保持选中通用 / 全局。
20. 输入 ` <<var_iscsi-b_vlan_id>>` 作为 VLAN ID 。
21. 单击确定，然后再次单击确定以创建 VLAN 。

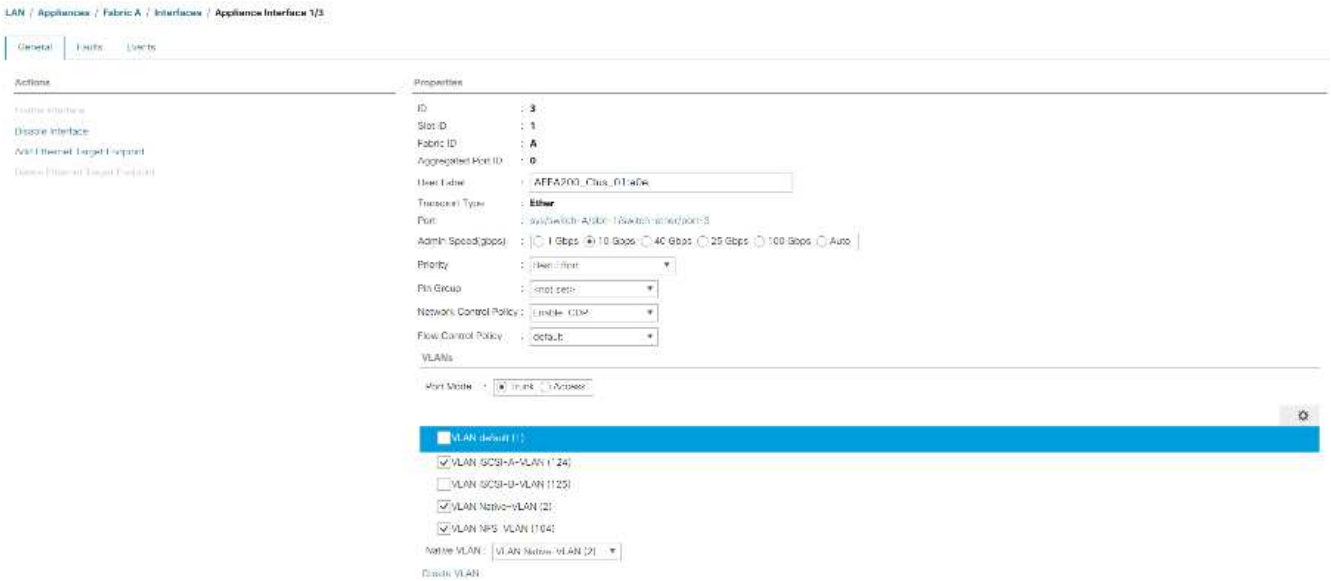
22. 右键单击设备云下的 VLAN 。
23. 选择 Create VLAN 。
24. 输入 Native-VLAN 作为原生 VLAN 的名称。
25. 保持选中通用 / 全局。
26. 输入 ` <<var_native_vlan_id>>` 作为 VLAN ID 。
27. 单击确定，然后再次单击确定以创建 VLAN 。



28. 在导航窗格中的 "LAN">"Policies" 下，展开 "Applies" ，然后右键单击 "Network Control Policies" 。
29. 选择创建网络控制策略。
30. 将此策略命名为 `Enable_CDP_LLDP` ，然后选择 CDP 旁边的 Enabled 。
31. 启用 LLDP 的传输和接收功能。

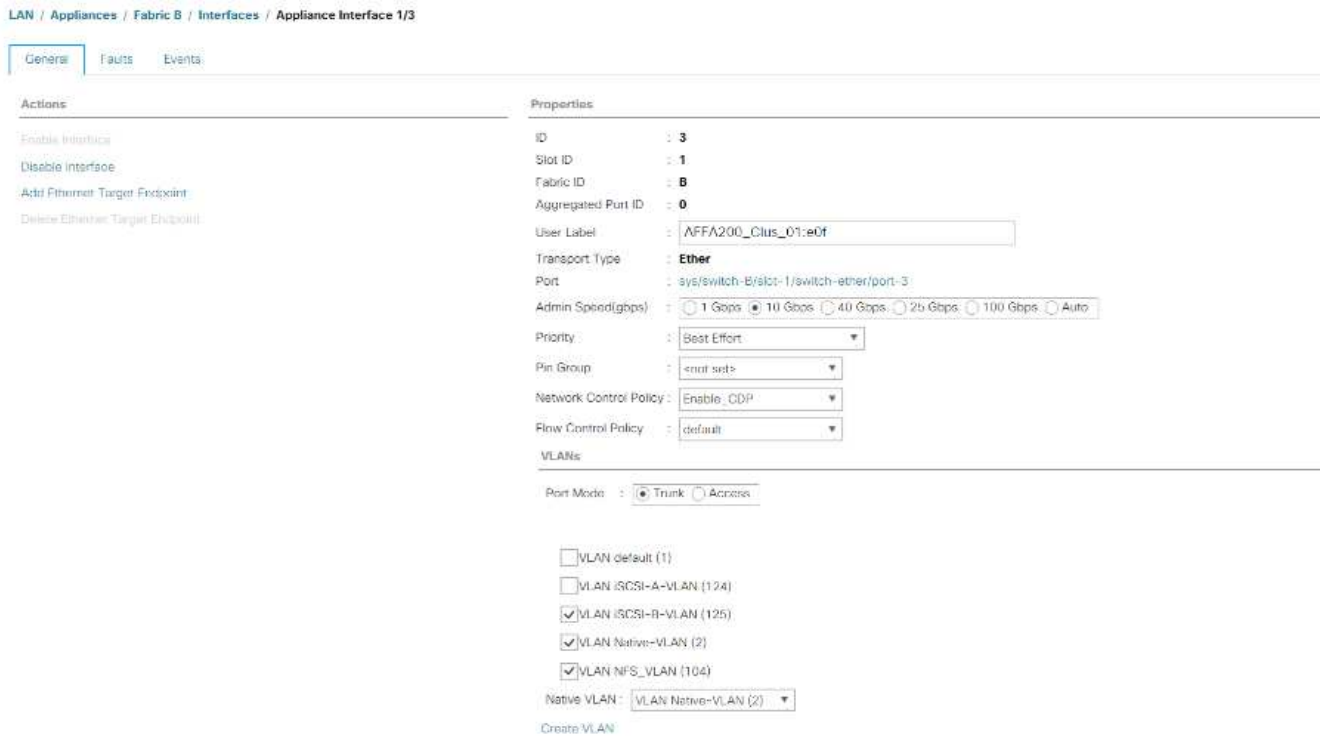


32. 单击确定，然后再次单击确定以创建策略。
33. 在导航窗格中的 "LAN">"Appliances Cloud" 下，展开结构 A 树。
34. 展开接口。
35. 选择设备接口 1/3 。
36. 在用户标签字段中，输入指示存储控制器端口的信息，例如 ` <storage_controller_01_name>： e0e` 。单击 Save Changes and OK 。
37. 选择 Enable_CDP Network Control Policy ，然后选择 Save Changes and OK 。
38. 在 VLAN 下，选择 iSCSI-A-VLAN ， NFS VLAN 和原生 VLAN 。将本机 VLAN 设置为原生 VLAN 。清除默认 VLAN 选择。
39. 单击 Save Changes and OK 。



40. 在 Fabric A 下选择设备接口 1/4
41. 在用户标签字段中，输入指示存储控制器端口的信息，例如 ` <storage_controller_02_name>： e0e` 。单击 Save Changes and OK 。
42. 选择 Enable_CDP Network Control Policy ，然后选择 Save Changes and OK 。
43. 在 VLAN 下，选择 iSCSI-A-VLAN ， NFS VLAN 和原生 VLAN 。
44. 将本机 VLAN 设置为原生 VLAN 。
45. 清除默认 VLAN 选择。
46. 单击 Save Changes and OK 。
47. 在导航窗格中的 "LAN">"Appliances Cloud" 下，展开 Fabric B 树。
48. 展开接口。
49. 选择设备接口 1/3 。
50. 在用户标签字段中，输入指示存储控制器端口的信息，例如 ` <storage_controller_01_name>： e0f` 。单击 Save Changes and OK 。

51. 选择 Enable_CDP Network Control Policy ，然后选择 Save Changes and OK 。
52. 在 VLAN 下，选择 iSCSI-B-VLAN ， NFS VLAN 和原生 VLAN 。将本机 VLAN 设置为原生 VLAN 。取消选择默认 VLAN 。

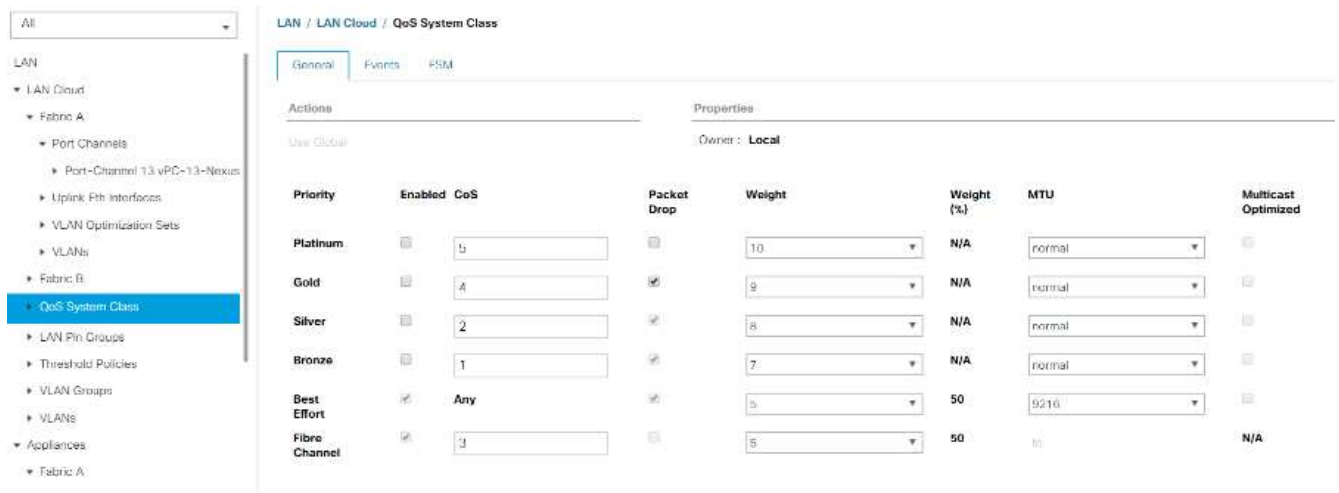


53. 单击 Save Changes and OK 。
54. 在 Fabric B 下选择设备接口 1/4
55. 在用户标签字段中，输入指示存储控制器端口的信息，例如 ` <storage_controller_02_name>： e0f` 。单击 Save Changes and OK 。
56. 选择 Enable_CDP Network Control Policy ，然后选择 Save Changes and OK 。
57. 在 VLAN 下，选择 iSCSI-B-VLAN ， NFS VLAN 和原生 VLAN 。将本机 VLAN 设置为原生 VLAN 。取消选择默认 VLAN 。
58. 单击 Save Changes and OK 。

在 **Cisco UCS** 网络结构中设置巨型帧

要在 Cisco UCS 网络结构中配置巨型帧并启用服务质量，请完成以下步骤：

1. 在 Cisco UCS Manager 的导航窗格中，单击 LAN 选项卡。
2. 选择 LAN > LAN Cloud > QoS 系统类。
3. 在右侧窗格中，单击常规选项卡。
4. 在尽力服务行的 MTU 列下的框中输入 9216 。



5. 单击 Save Changes 。
6. 单击确定。

确认 **Cisco UCS** 机箱

要确认所有 Cisco UCS 机箱，请完成以下步骤：

1. 在 Cisco UCS Manager 中，选择设备选项卡，然后展开右侧的设备选项卡。
2. 展开设备 > 机箱。
3. 在机箱 1 的操作中，选择确认机箱。
4. 单击确定，然后单击确定完成对机箱的确认。
5. 单击关闭以关闭属性窗口。

加载 **Cisco UCS 4.0** （ **1b** ）固件映像

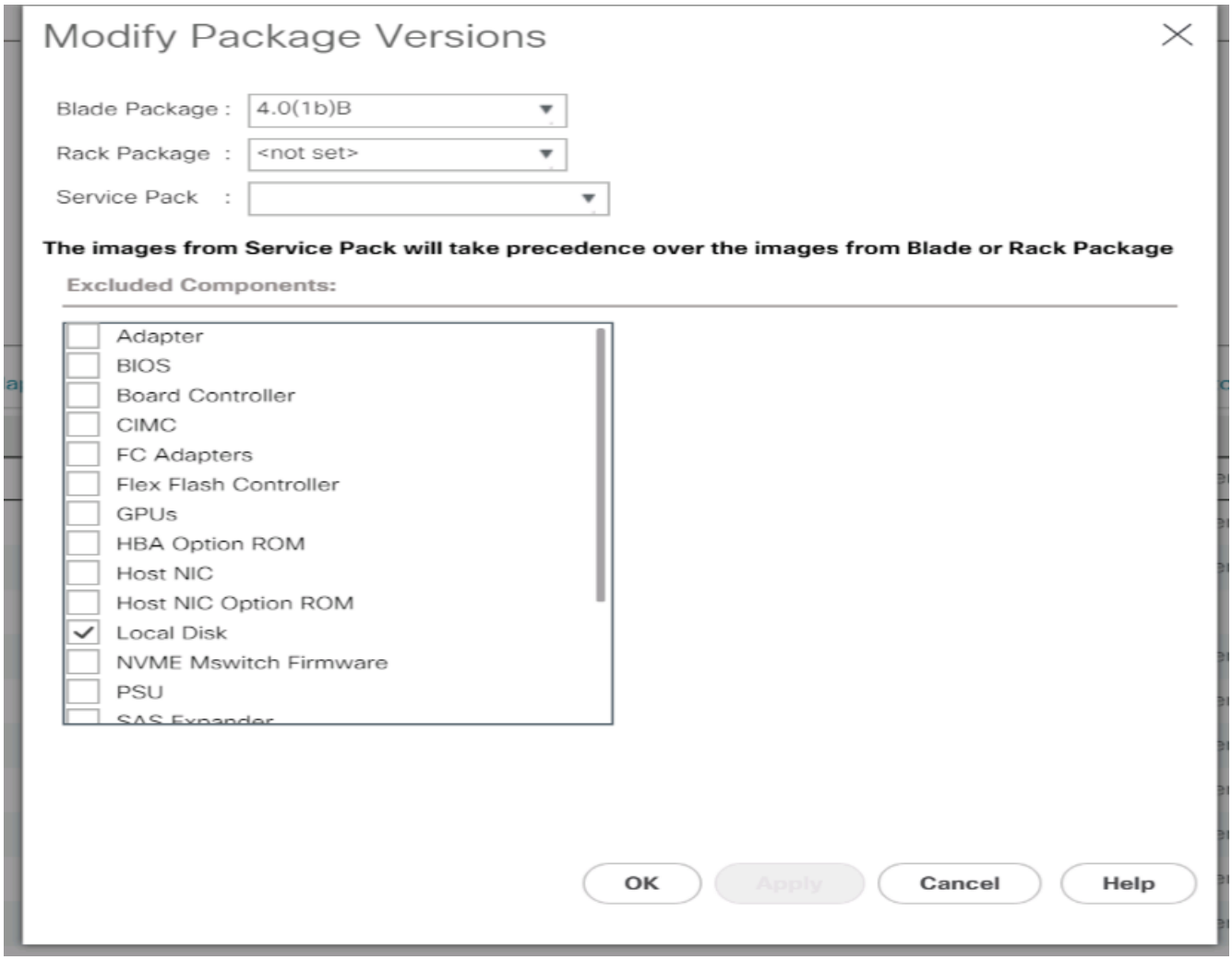
要将 Cisco UCS Manager 软件和 Cisco UCS 互联阵列软件升级到 4.0 （ 1b ）版，请参见 "《 Cisco UCS Manager 安装和升级指南》"。

创建主机固件包

通过固件管理策略，管理员可以为给定服务器配置选择相应的软件包。这些策略通常包括适配器， BIOS ，板载控制器， FC 适配器，主机总线适配器（ HBA ）选项 ROM 以及存储控制器属性的软件包。

要在 Cisco UCS 环境中为给定服务器配置创建固件管理策略，请完成以下步骤：

1. 在 Cisco UCS Manager 中，单击左侧的服务器。
2. 选择策略 > root 。
3. 展开主机固件包。
4. 选择默认。
5. 在操作窗格中，选择修改软件包版本。
6. 为两个刀片式服务器软件包选择版本 4.0 （ 1b ）。



7. 再次单击确定，然后单击确定以修改主机固件包。

创建 **MAC** 地址池

要为 Cisco UCS 环境配置所需的 MAC 地址池，请完成以下步骤：

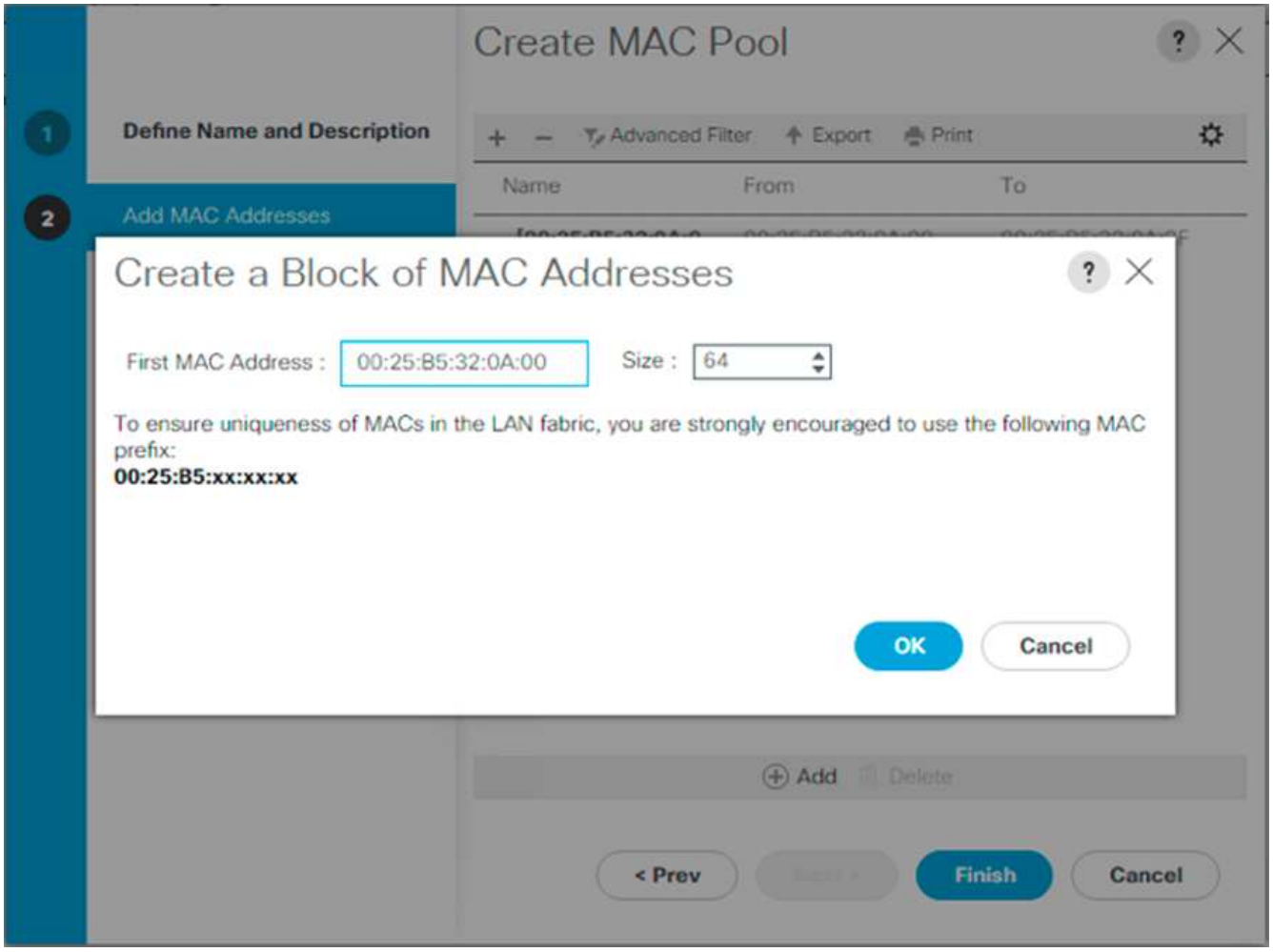
1. 在 Cisco UCS Manager 中，单击左侧的 LAN 。
2. 选择 Pools > root 。

   在此操作步骤中，将创建两个 MAC 地址池，每个交换网络结构一个。

3. 右键单击根组织下的 MAC Pools 。
4. 选择创建 MAC 池以创建 MAC 地址池。
5. 输入 MAC-Pool-A 作为 MAC 池的名称。
6. 可选：输入 MAC 池的问题描述。
7. 选择顺序作为分配顺序的选项。单击下一步。
8. 单击添加。
9. 指定起始 MAC 地址。

> 对于 FlexPod 解决方案，建议将 0A 放置在起始 MAC 地址的倒数第二个八位字节中，以便将所有 MAC 地址标识为阵列 A 地址。在我们的示例中，我们还采用了一个示例，即嵌入 Cisco UCS 域名信息，并将其提供 00： 25： B5： 32： 0a： 00 作为我们的第一个 MAC 地址。

10. 为 MAC 地址池指定一个足以支持可用刀片或服务器资源的大小。单击确定。



11. 单击完成。
12. 在确认消息中，单击确定。
13. 右键单击根组织下的 MAC Pools 。
14. 选择创建 MAC 池以创建 MAC 地址池。
15. 输入 MAC-Pool-B 作为 MAC 池的名称。
16. 可选：输入 MAC 池的问题描述。
17. 选择顺序作为分配顺序的选项。单击下一步。
18. 单击添加。
19. 指定起始 MAC 地址。

> 对于 FlexPod 解决方案，建议将 0B 放置在起始 MAC 地址的最后一个八位字节旁边，以便将此池中的所有 MAC 地址标识为网络结构 B 地址。我们再次在此示例中进行了后续操作，并嵌入了 Cisco UCS 域名信息，使我们的第一个 MAC 地址为 00： 25： B5： 32： 0B： 00 。

20. 为 MAC 地址池指定一个足以支持可用刀片或服务器资源的大小。单击确定。
21. 单击完成。
22. 在确认消息中，单击确定。

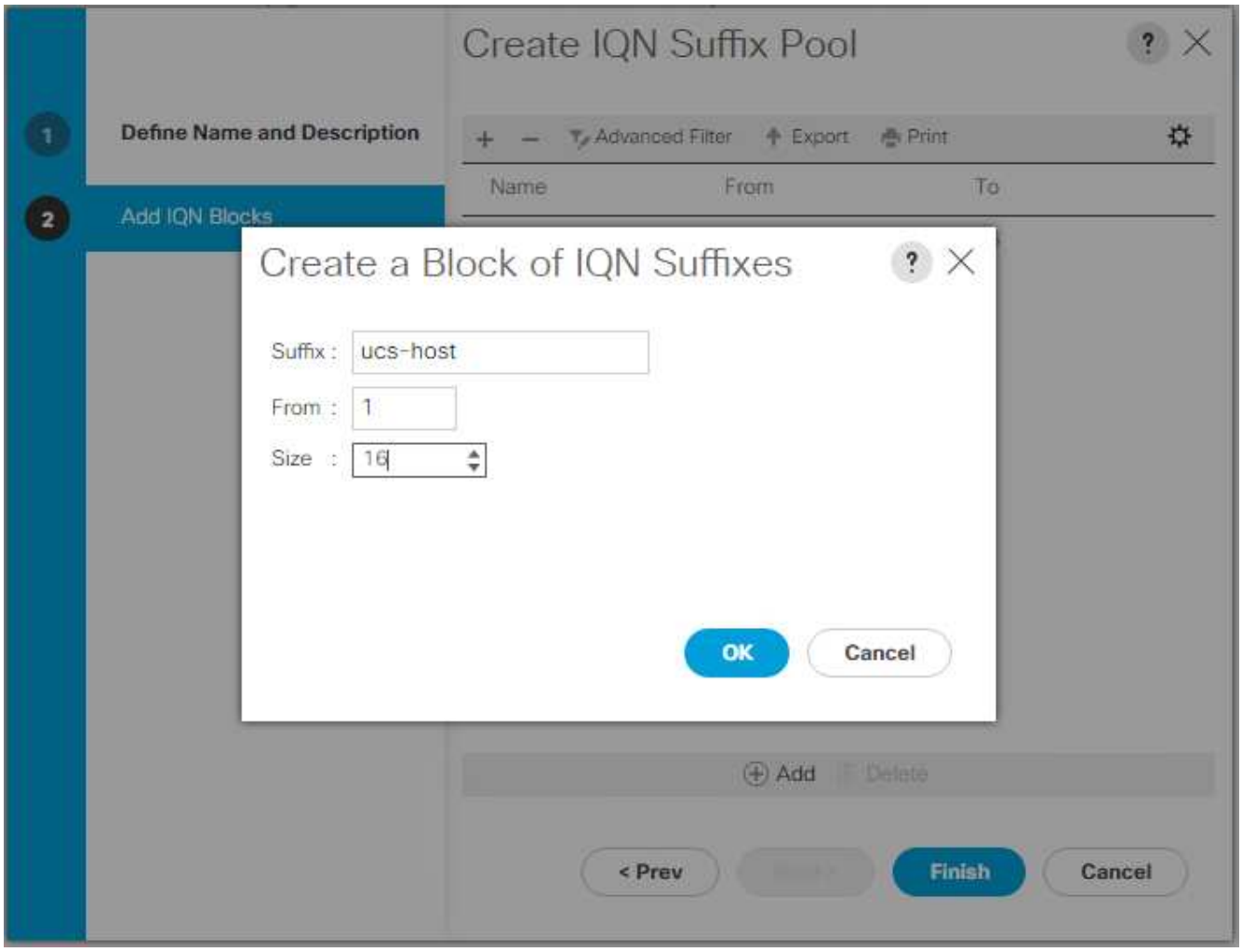
创建 **iSCSI IQN** 池

要为 Cisco UCS 环境配置所需的 IQN 池，请完成以下步骤：

1. 在 Cisco UCS Manager 中，单击左侧的 SAN 。
2. 选择 Pools > root 。
3. 右键单击 IQN Pools 。
4. 选择创建 IQN 后缀池以创建 IQN 池。
5. 输入 IQN-Pool 作为 IQN 池的名称。
6. 可选：输入 IQN 池的问题描述。
7. 输入 `iqn.1992-08.com.cisco` 作为前缀。
8. 为分配顺序选择顺序。单击下一步。
9. 单击添加。
10. 输入 `UCS-host` 作为后缀。

> 如果正在使用多个 Cisco UCS 域，则可能需要使用更具体的 IQN 后缀。

11. 在发件人字段中输入 1 。
12. 指定足以支持可用服务器资源的 IQN 块大小。单击确定。



13. 单击完成。

创建 **iSCSI** 启动程序 **IP** 地址池

要为 Cisco UCS 环境配置所需的 IP 池 iSCSI 启动，请完成以下步骤：

1. 在 Cisco UCS Manager 中，单击左侧的 LAN 。
2. 选择 Pools > root 。
3. 右键单击 IP Pools 。
4. 选择创建 IP 池。
5. 输入 iscsi-ip-pool-A 作为 IP 池的名称。
6. 可选：输入 IP 池的问题描述。
7. 为分配顺序选择顺序。单击下一步。
8. 单击添加以添加 IP 地址块。
9. 在发件人字段中，输入要分配为 iSCSI IP 地址的范围的开头。
10. 将大小设置为足够的地址以容纳服务器。单击确定。
11. 单击下一步。

12. 单击完成。
13. 右键单击 IP Pools 。
14. 选择创建 IP 池。
15. 输入 iscsi-ip-pool-B 作为 IP 池的名称。
16. 可选：输入 IP 池的问题描述。
17. 为分配顺序选择顺序。单击下一步。
18. 单击添加以添加 IP 地址块。
19. 在发件人字段中，输入要分配为 iSCSI IP 地址的范围的开头。
20. 将大小设置为足够的地址以容纳服务器。单击确定。
21. 单击下一步。
22. 单击完成。

创建 **UUID** 后缀池

要为 Cisco UCS 环境配置所需的通用唯一标识符（ UUID ）后缀池，请完成以下步骤：

1. 在 Cisco UCS Manager 中，单击左侧的服务器。
2. 选择 Pools > root 。
3. 右键单击 UUID 后缀池。
4. 选择创建 UUID 后缀池。
5. 输入 UUID-Pool 作为 UUID 后缀池的名称。
6. 可选：输入 UUID 后缀池的问题描述。
7. 将前缀保留在 derived 选项处。
8. 为分配顺序选择顺序。
9. 单击下一步。
10. 单击添加以添加 UUID 块。
11. 将发件人字段保持默认设置。
12. 为 UUID 块指定一个足以支持可用刀片式服务器或服务器资源的大小。单击确定。
13. 单击完成。
14. 单击确定。

创建服务器池

要为 Cisco UCS 环境配置所需的服务器池，请完成以下步骤：

请考虑创建唯一的服务器池，以实现环境所需的粒度。

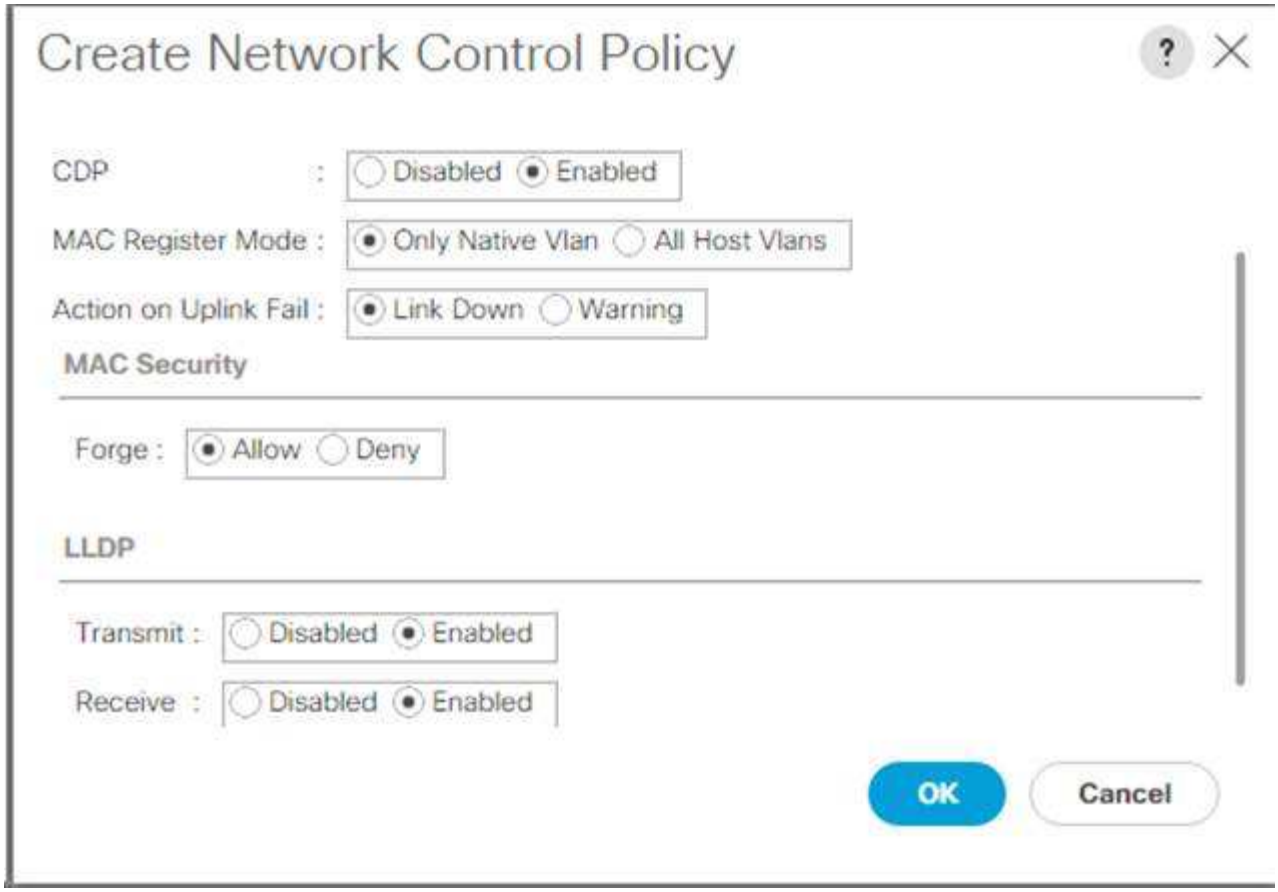
1. 在 Cisco UCS Manager 中，单击左侧的服务器。
2. 选择 Pools > root 。

3. 右键单击 Server Pools 。
4. 选择创建服务器池。
5. 输入 `Infra-Pool `作为服务器池的名称。
6. 可选：输入服务器池的问题描述。单击下一步。
7. 选择要用于 VMware 管理集群的两个（或更多）服务器，然后单击 >> 将其添加到 `Infra-Pool `s服务器池中。
8. 单击完成。
9. 单击确定。

为 **Cisco** 发现协议和链路层发现协议创建网络控制策略

要为 Cisco 发现协议（ CDP ）和链路层发现协议（ LLDP ）创建网络控制策略，请完成以下步骤：

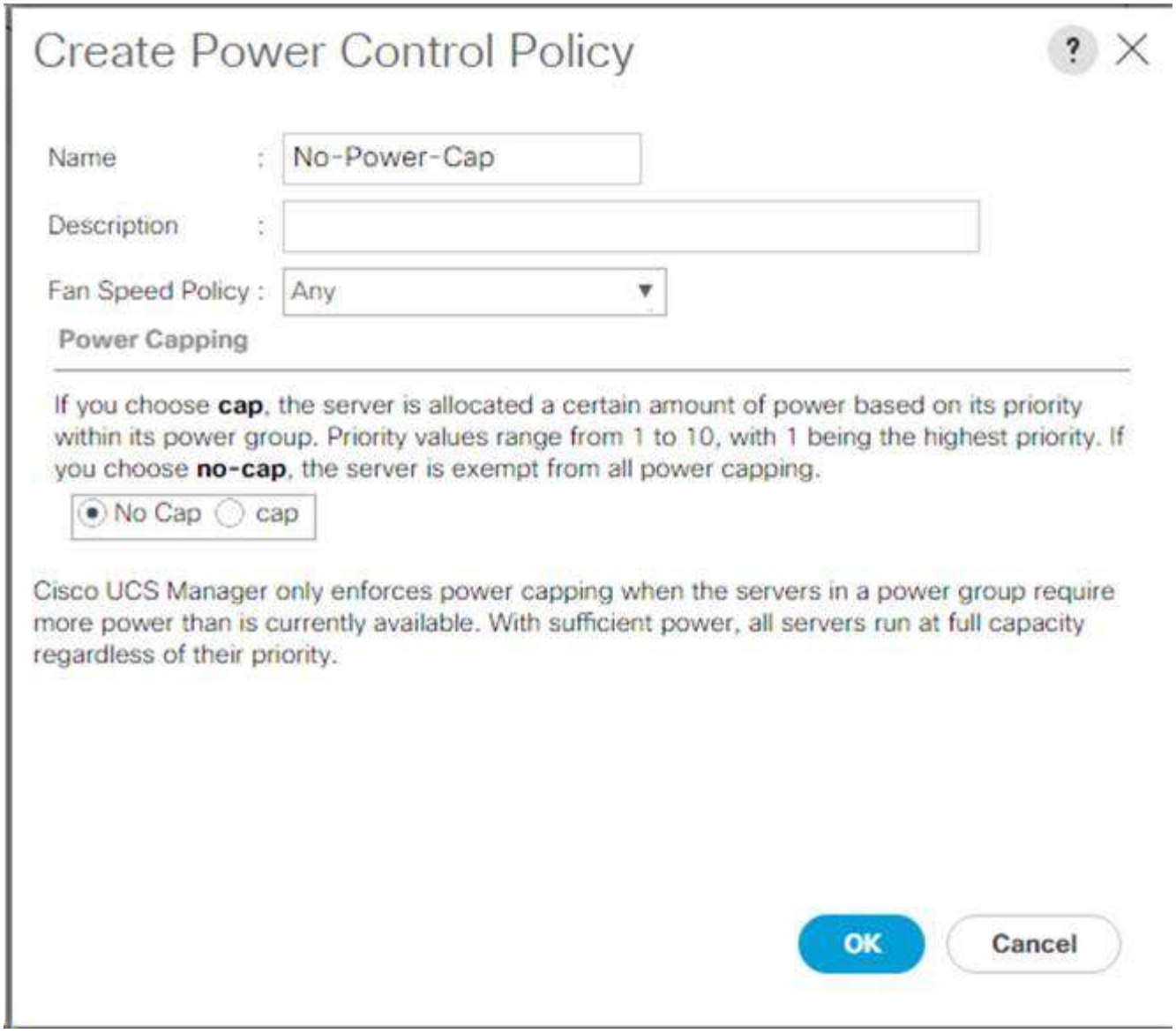
1. 在 Cisco UCS Manager 中，单击左侧的 LAN 。
2. 选择策略 > root 。
3. 右键单击网络控制策略。
4. 选择创建网络控制策略。
5. 输入 Enable-CDP-LLDP 策略名称。
6. 对于 CDP ，选择 Enabled 选项。
7. 对于 LLDP ，向下滚动并为传输和接收选择已启用。
8. 单击确定以创建网络控制策略。单击确定。



创建电源控制策略

要为 Cisco UCS 环境创建电源控制策略，请完成以下步骤：

1. 在 Cisco UCS Manager 中，单击左侧的服务器选项卡。
2. 选择策略 > root 。
3. 右键单击电源控制策略。
4. 选择 Create Power Control Policy 。
5. 输入 No-Power-Cap 作为电源控制策略名称。
6. 将电源上限设置更改为无上限。
7. 单击确定以创建电源控制策略。单击确定。



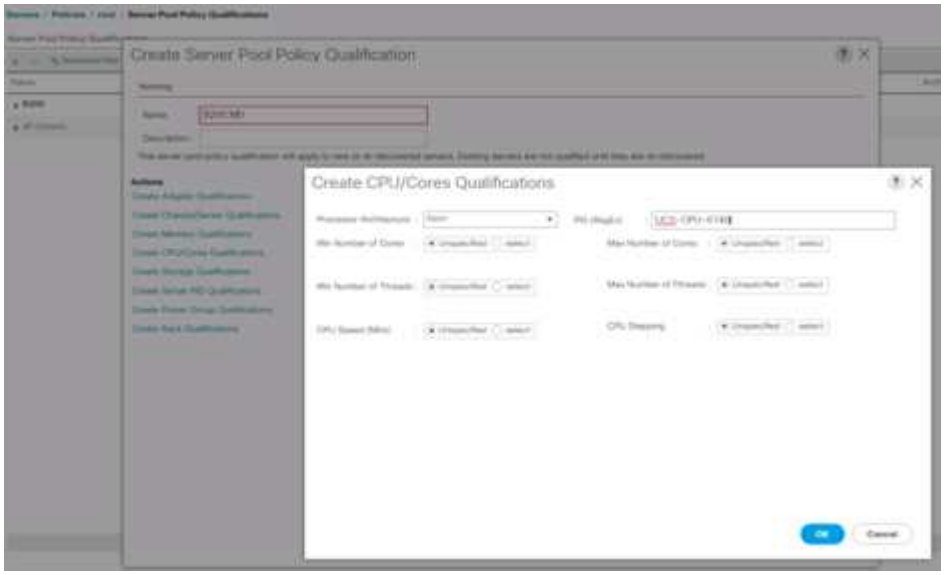
创建服务器池限定策略（可选）

要为 Cisco UCS 环境创建可选的服务器池限定策略，请完成以下步骤：

> 此示例将为采用 Intel E2660 v4 Xeon Broadwell 处理器的 Cisco UCS B 系列服务器创建一个策略。

1. 在 Cisco UCS Manager 中，单击左侧的服务器。
2. 选择策略 > root 。
3. 选择服务器池策略限制条件。
4. 选择创建服务器池策略限制条件或添加。
5. 将策略命名为 Intel 。
6. 选择创建 CPU/ 核心限制条件。
7. 选择 Xeon 作为处理器 / 架构。

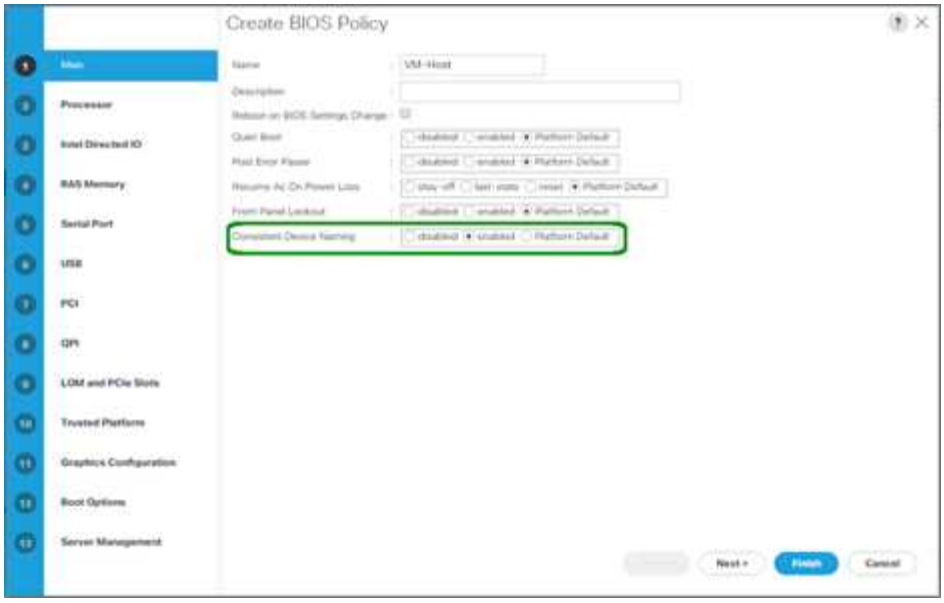
8. 输入 ` <UCS-CPU- PID>` 作为进程 ID （ PID ）。
9. 单击确定以创建 CPU/ 核心资格认定。
10. 单击确定创建策略，然后单击确定进行确认。



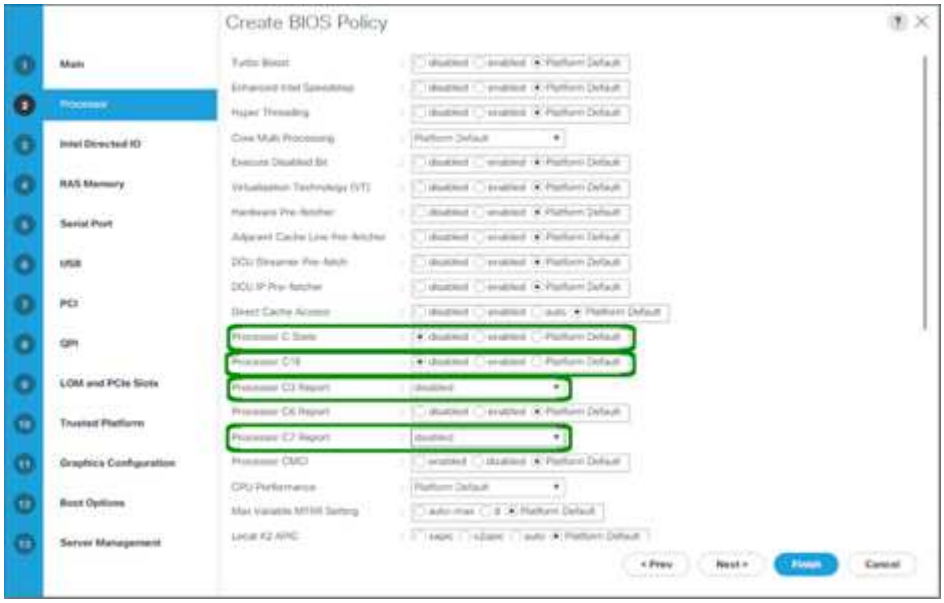
创建服务器 **BIOS** 策略

要为 Cisco UCS 环境创建服务器 BIOS 策略，请完成以下步骤：

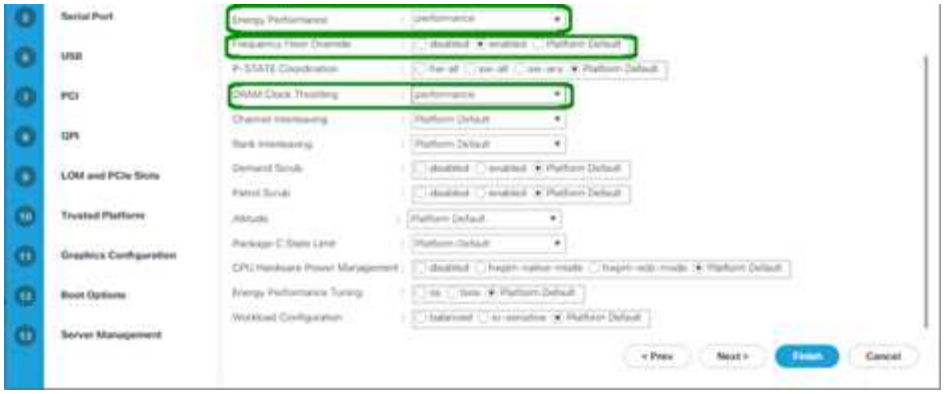
1. 在 Cisco UCS Manager 中，单击左侧的服务器。
2. 选择策略 > root 。
3. 右键单击 BIOS 策略。
4. 选择 Create BIOS Policy 。
5. 输入 VM-Host 作为 BIOS 策略名称。
6. 将 Quiet Boot 设置更改为 disabled 。
7. 将一致设备命名更改为已启用。



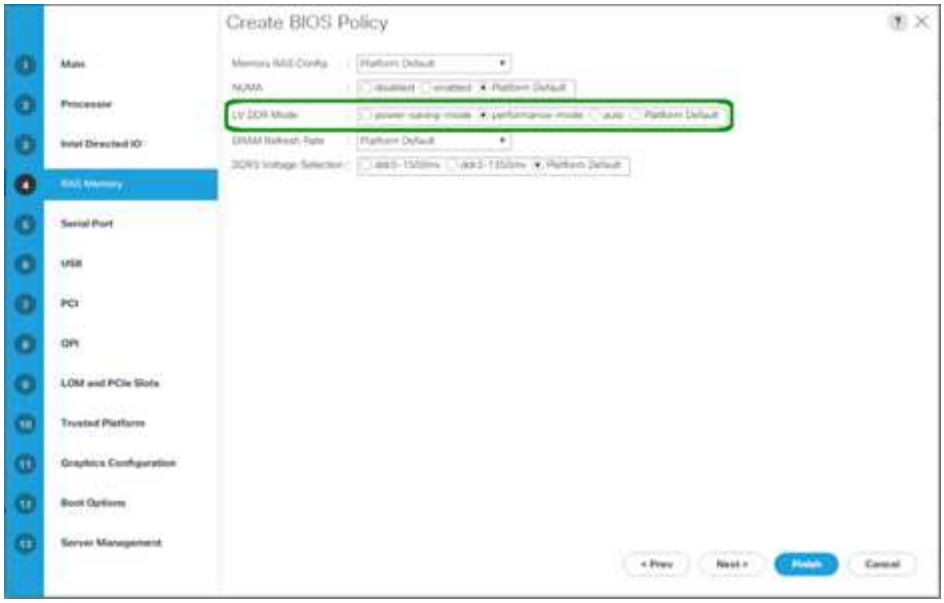
8. 选择处理器选项卡并设置以下参数：
   - 处理器 C 状态：已禁用
   - 处理器 C1E ：已禁用
   - 处理器 C3 报告：已禁用
   - 处理器 C7 报告：已禁用



9. 向下滚动到其余处理器选项并设置以下参数：
   - 能源性能：性能
   - 频率下限覆盖：已启用
   - DRAM 时钟限制：性能



10. 单击 RAS 内存并设置以下参数：
    - LV DDR Mode ： 性能模式

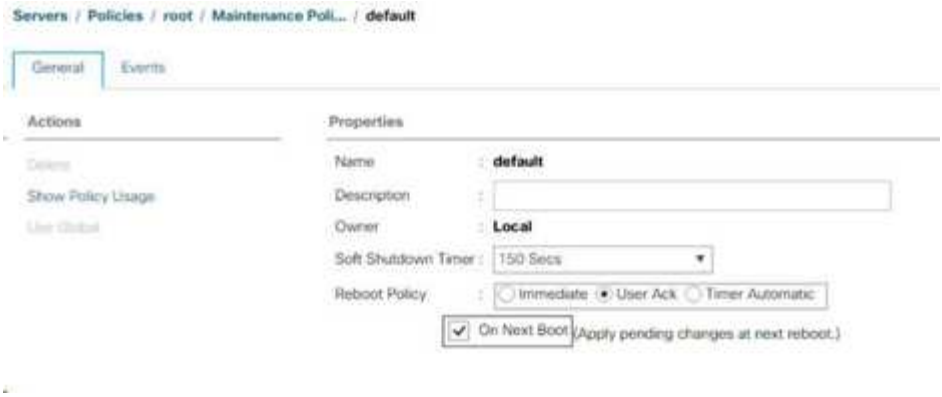


11. 单击完成以创建 BIOS 策略。
12. 单击确定。

更新默认维护策略

要更新默认维护策略，请完成以下步骤：

1. 在 Cisco UCS Manager 中，单击左侧的服务器。
2. 选择策略 > root 。
3. 选择维护策略 > 默认。
4. 将重新启动策略更改为 User Ack 。
5. 选择下次启动可将维护窗口委派给服务器管理员。



6. 单击 Save Changes 。
7. 单击确定接受更改。

创建 **vNIC** 模板

要为 Cisco UCS 环境创建多个虚拟网络接口卡（ Virtual Network Interface Card ， vNIC ）模板，请完成本节中所述的过程。

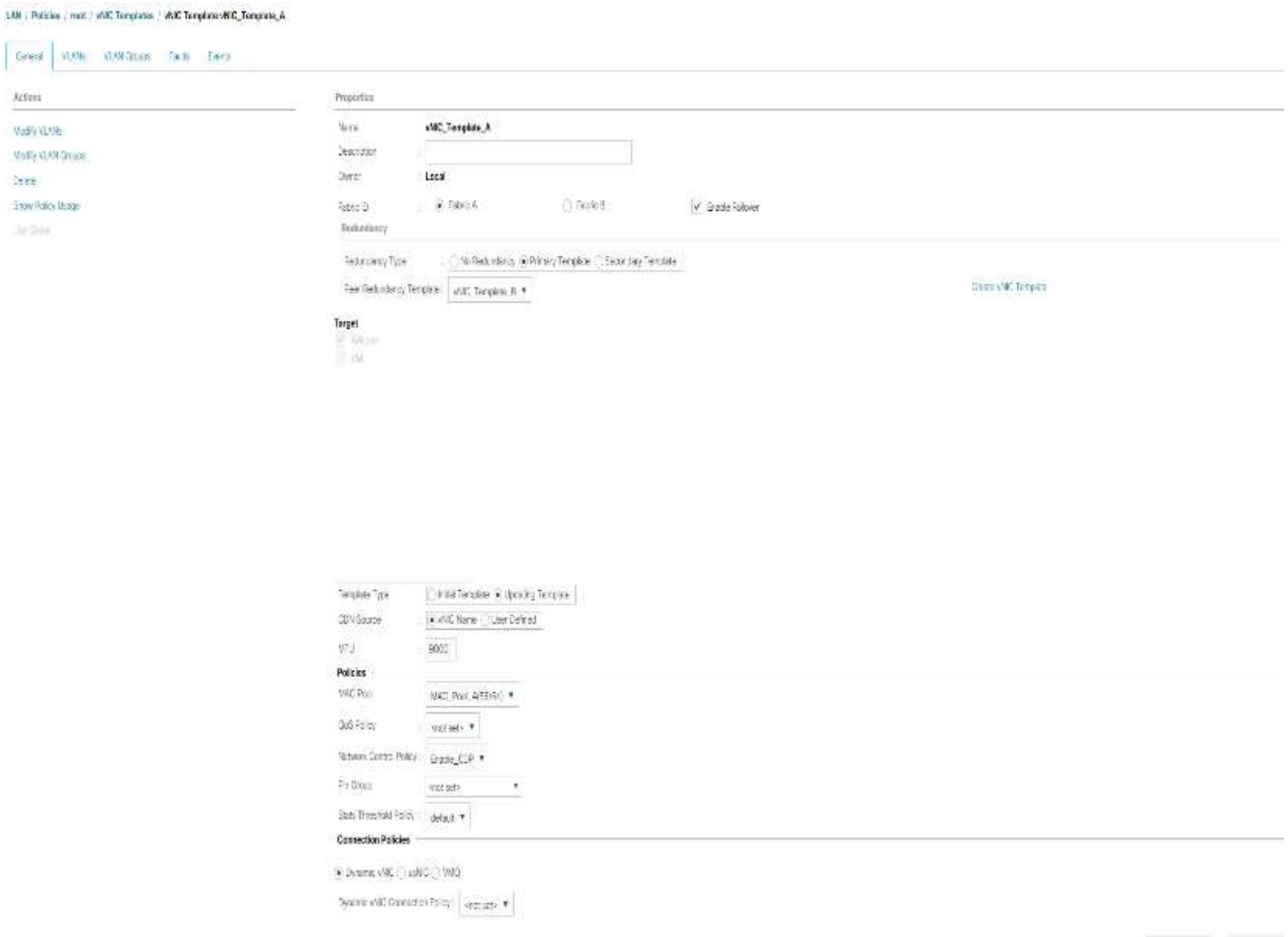
> 总共创建了四个 vNIC 模板。

创建基础架构 **vNIC**

要创建基础架构 vNIC ，请完成以下步骤：

1. 在 Cisco UCS Manager 中，单击左侧的 LAN 。
2. 选择策略 > root 。
3. 右键单击 vNIC 模板。
4. 选择 Create vNIC Template 。
5. 输入 `Site-XX-vNIC_A` 作为 vNIC 模板名称。
6. 选择 Updating-template 作为模板类型。
7. 对于 Fabric ID ，请选择 Fabric A
8. 确保未选中启用故障转移选项。
9. 选择 "Primary Template" 作为 "Redundancy Type" 。
10. 保持对等冗余模板设置为 ` < 未设置 >` 。
11. 在目标下，确保仅选择适配器选项。
12. 将 `native-vlan` 设置为原生 VLAN 。
13. 为 CDN 源选择 vNIC 名称。
14. 对于 MTU ，输入 9000 。
15. 在允许的 VLAN 下，选择 `Native-VLAN` ， `Site-XX-IB-Mgmt` ， `Site-XX-NFS` ， `Site-XX-VM-Traffic` ， 和 Site-XX-vMotion 。使用 Ctrl 键进行多次选择。
16. 单击选择。这些 VLAN 现在应显示在选定 VLAN 下。

17. 在 MAC Pool 列表中，选择 `MAC_Pool_A` 。
18. 在网络控制策略列表中，选择 Pool-A
19. 在网络控制策略列表中，选择 Enable-CDP-LLDP 。
20. 单击确定以创建 vNIC 模板。
21. 单击确定。

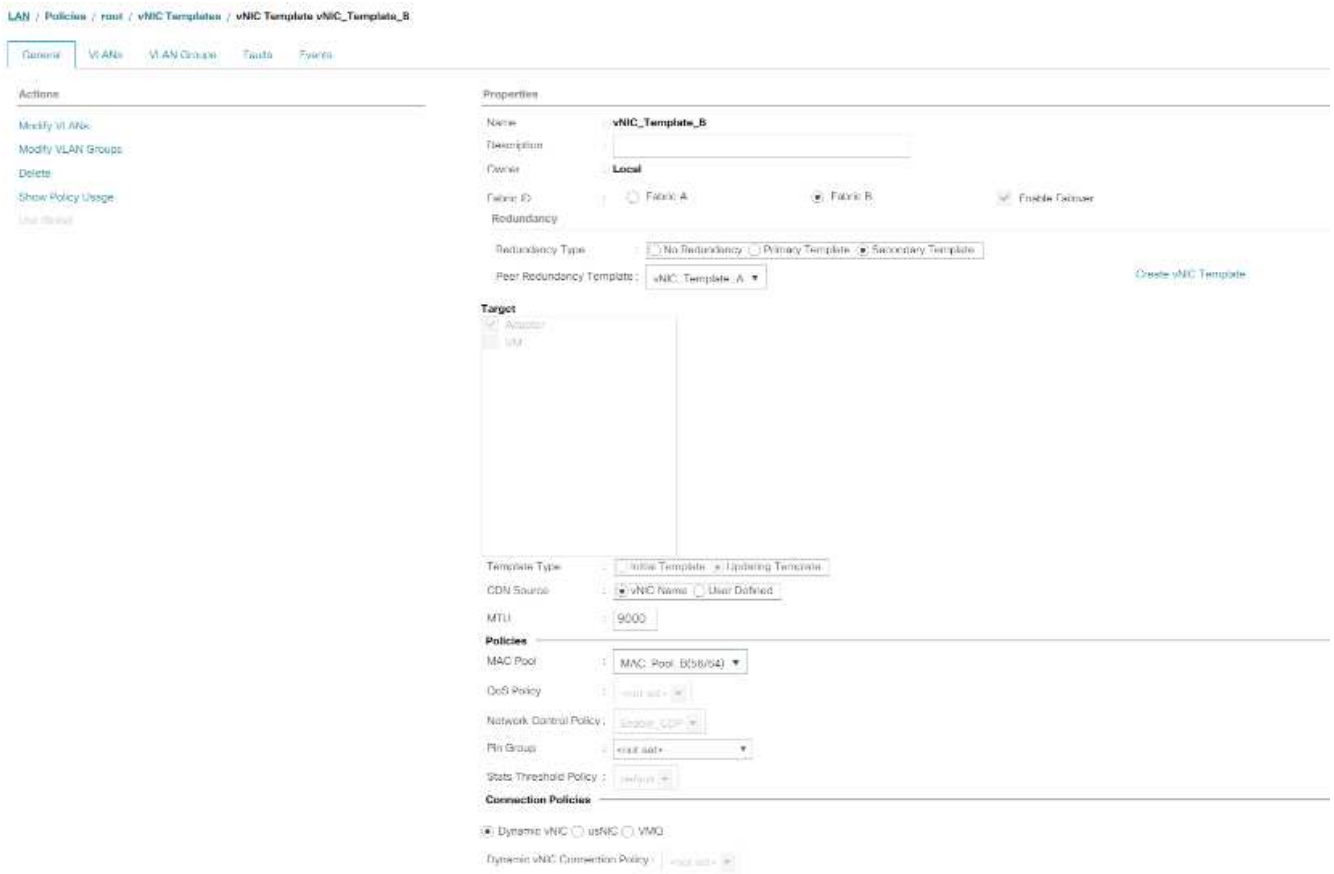


要创建二级冗余模板 Infra-B ，请完成以下步骤：

1. 在 Cisco UCS Manager 中，单击左侧的 LAN 。
2. 选择策略 > root 。
3. 右键单击 vNIC 模板。
4. 选择 Create vNIC Template 。
5. 输入 `Site-XX-vNIC_B `作为 vNIC 模板名称。
6. 选择 Updating-template 作为模板类型。
7. 对于 Fabric ID ，请选择 Fabric B
8. 选择启用故障转移选项。

> 选择故障转移是一个关键步骤，可通过在硬件级别处理链路故障转移来缩短故障转移时间，并防止虚拟交换机未检测到任何可能的 NIC 故障。

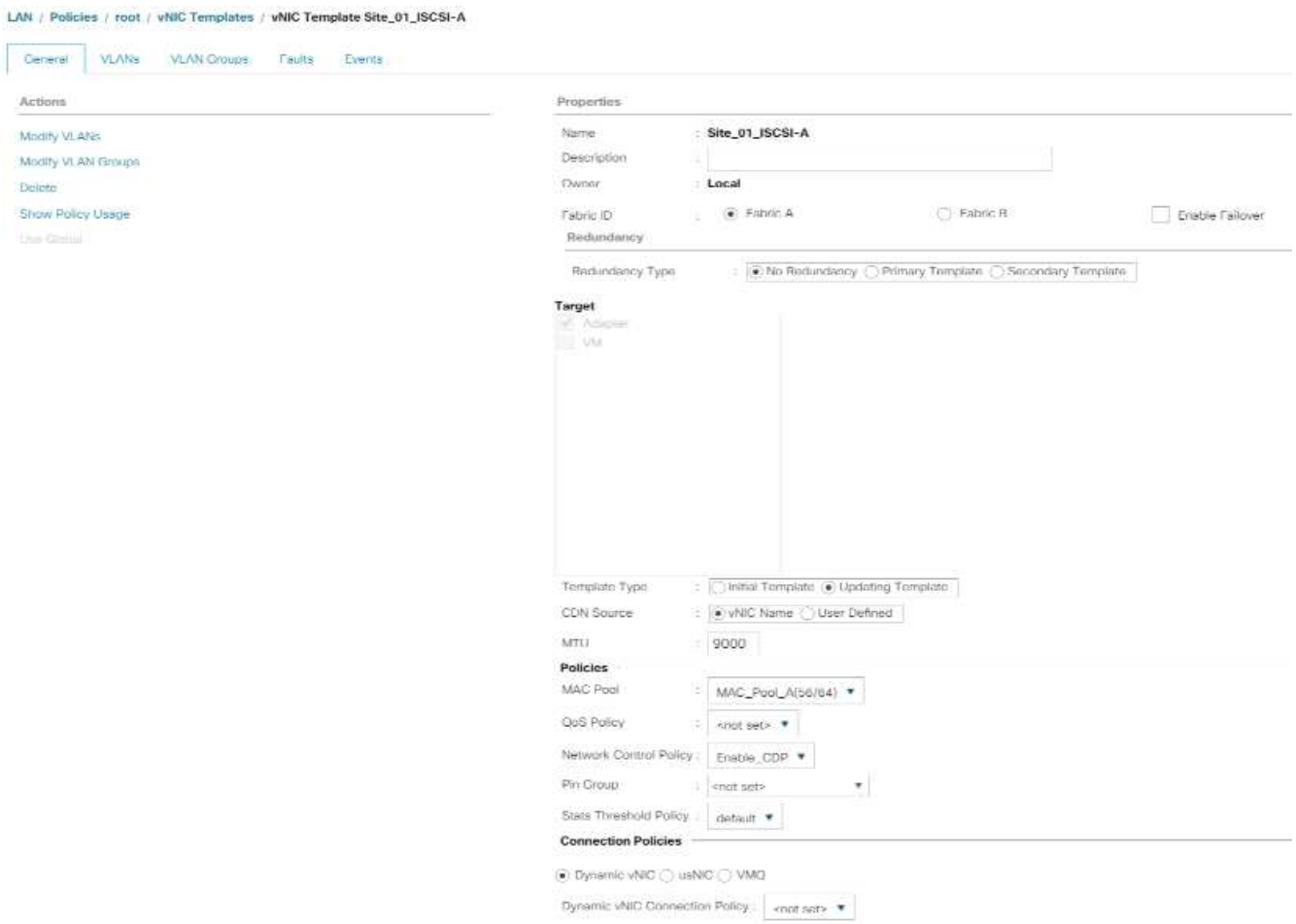
9. 选择 "Primary Template" 作为 "Redundancy Type" 。
10. 保持对等冗余模板设置为 `vNIC_Template_A` 。
11. 在目标下，确保仅选择适配器选项。
12. 将 `native-vlan` 设置为原生 VLAN 。
13. 为 CDN 源选择 vNIC 名称。
14. 对于 MTU ，输入 `9000` 。
15. 在允许的 VLAN 下，选择 `Native-VLAN` ， `Site-XX-IB-Mgmt` ， `Site-XX-NFS` ， `Site-XX-VM-Traffic` ， 和 Site-XX-vMotion 。使用 Ctrl 键进行多次选择。
16. 单击选择。这些 VLAN 现在应显示在选定 VLAN 下。
17. 在 MAC Pool 列表中，选择 `MAC_Pool_B` 。
18. 在网络控制策略列表中，选择 Pool-B
19. 在网络控制策略列表中，选择 Enable-CDP-LLDP 。
20. 单击确定以创建 vNIC 模板。
21. 单击确定。



创建 **iSCSI vNIC**

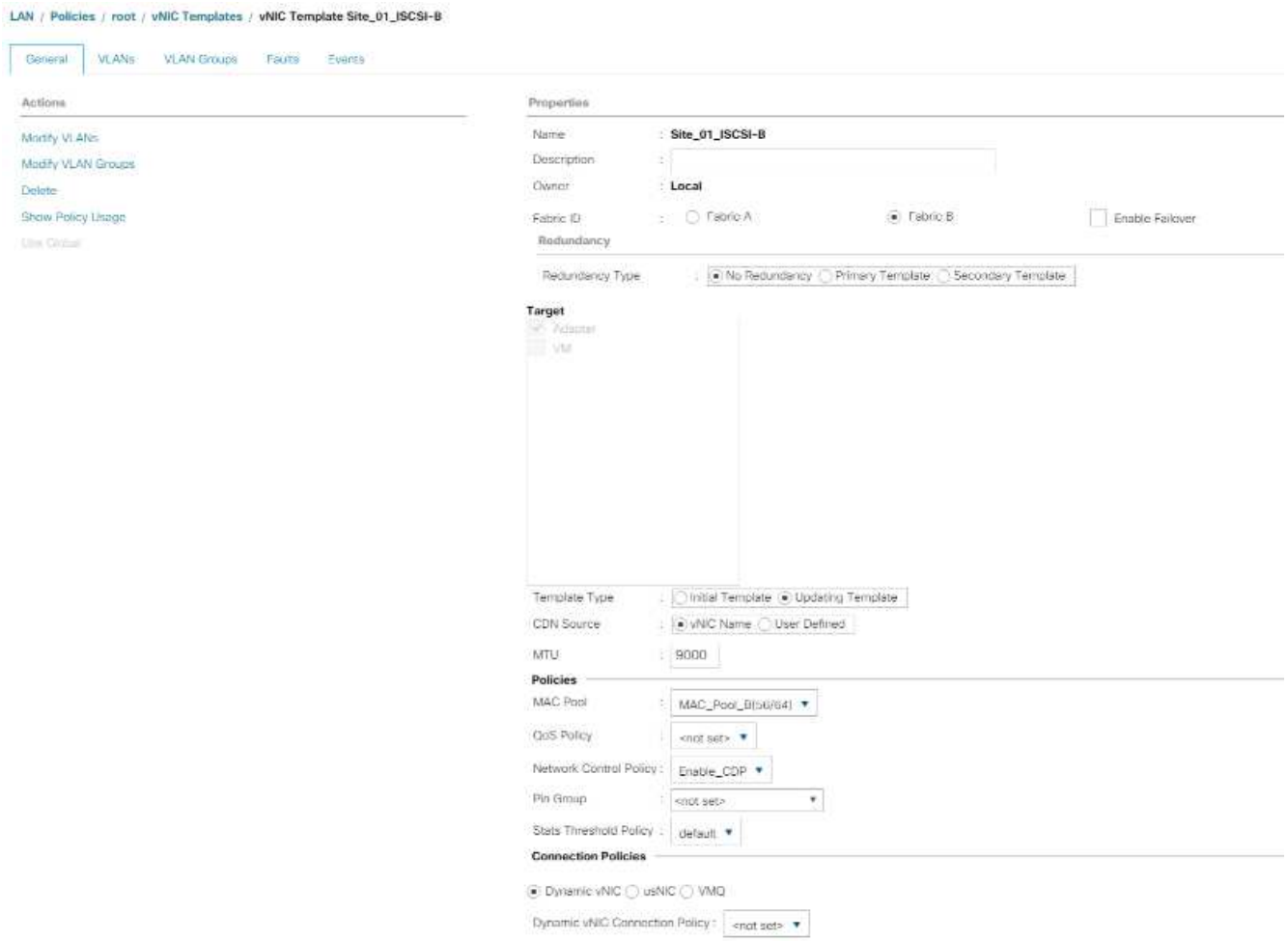
要创建 iSCSI vNIC ，请完成以下步骤：

1. 选择左侧的 LAN 。
2. 选择策略 > root 。
3. 右键单击 vNIC 模板。
4. 选择 Create vNIC Template 。
5. 输入 `Site- 01-iscsi_a` 作为 vNIC 模板名称。
6. 选择 Fabric A请勿选择启用故障转移选项。
7. 将 "Redundancy Type" 设置为 "No Redundancy" 。
8. 在目标下，确保仅选择适配器选项。
9. 选择更新模板类型的模板。
10. 在 VLAN 下，仅选择 Site-01-iSCSI_A_VLAN 。
11. 选择 Site- 01-iSCSI_A_VLAN 作为原生 VLAN 。
12. 保留为 CDN 源设置的 vNIC 名称。
13. 在 MTU 下，输入 9000 。
14. 从 MAC Pool 列表中，选择 MAC-Pool-A
15. 从网络控制策略列表中，选择 Enable-CDP-LLDP 。
16. 单击确定完成 vNIC 模板的创建。
17. 单击确定。



18. 选择左侧的 LAN 。
19. 选择策略 > root 。
20. 右键单击 vNIC 模板。
21. 选择 Create vNIC Template 。
22. 输入 `Site- 01-iscsi_B` 作为 vNIC 模板名称。
23. 选择 Fabric B请勿选择启用故障转移选项。
24. 将 "Redundancy Type" 设置为 "No Redundancy" 。
25. 在目标下，确保仅选择适配器选项。
26. 选择更新模板类型的模板。
27. 在 VLAN 下，仅选择 `Site- 01-iSCSI_B_VLAN` 。
28. 选择 `Site- 01-iSCSI_B_VLAN` 作为原生 VLAN 。
29. 保留为 CDN 源设置的 vNIC 名称。
30. 在 MTU 下，输入 9000 。
31. 从 MAC Pool 列表中，选择 `Mac-pool-B` 。
32. 从网络控制策略列表中，选择 `Enable-CDP-LLDP` 。

33. 单击确定完成 vNIC 模板的创建。
34. 单击确定。



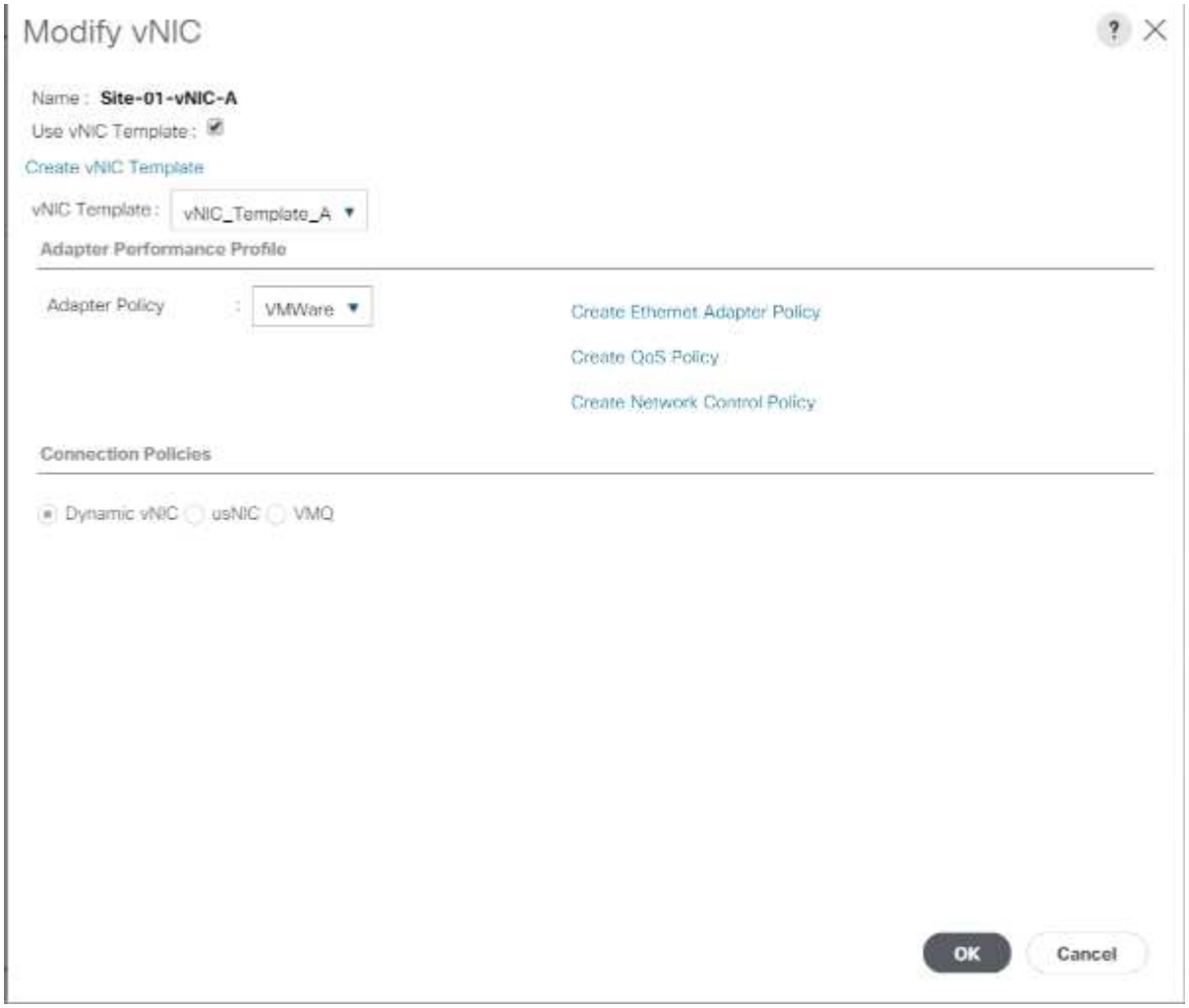
为 **iSCSI** 启动创建 **LAN** 连接策略

此操作步骤适用场景是一种 Cisco UCS 环境，其中两个 iSCSI LIF 位于集群节点 1 上（`iscsi_lif01a` 和 `iscsi_lif01b`），两个 iSCSI LIF 位于集群节点 2 上（`iscsi_lif02a` 和 `iscsi_lif02b`）。此外，假设 A LIF 连接到阵列 A （ Cisco UCS 6324 A ）， B LIF 连接到阵列 B （ Cisco UCS 6324 B ）。

要配置所需的基础架构 LAN 连接策略，请完成以下步骤：

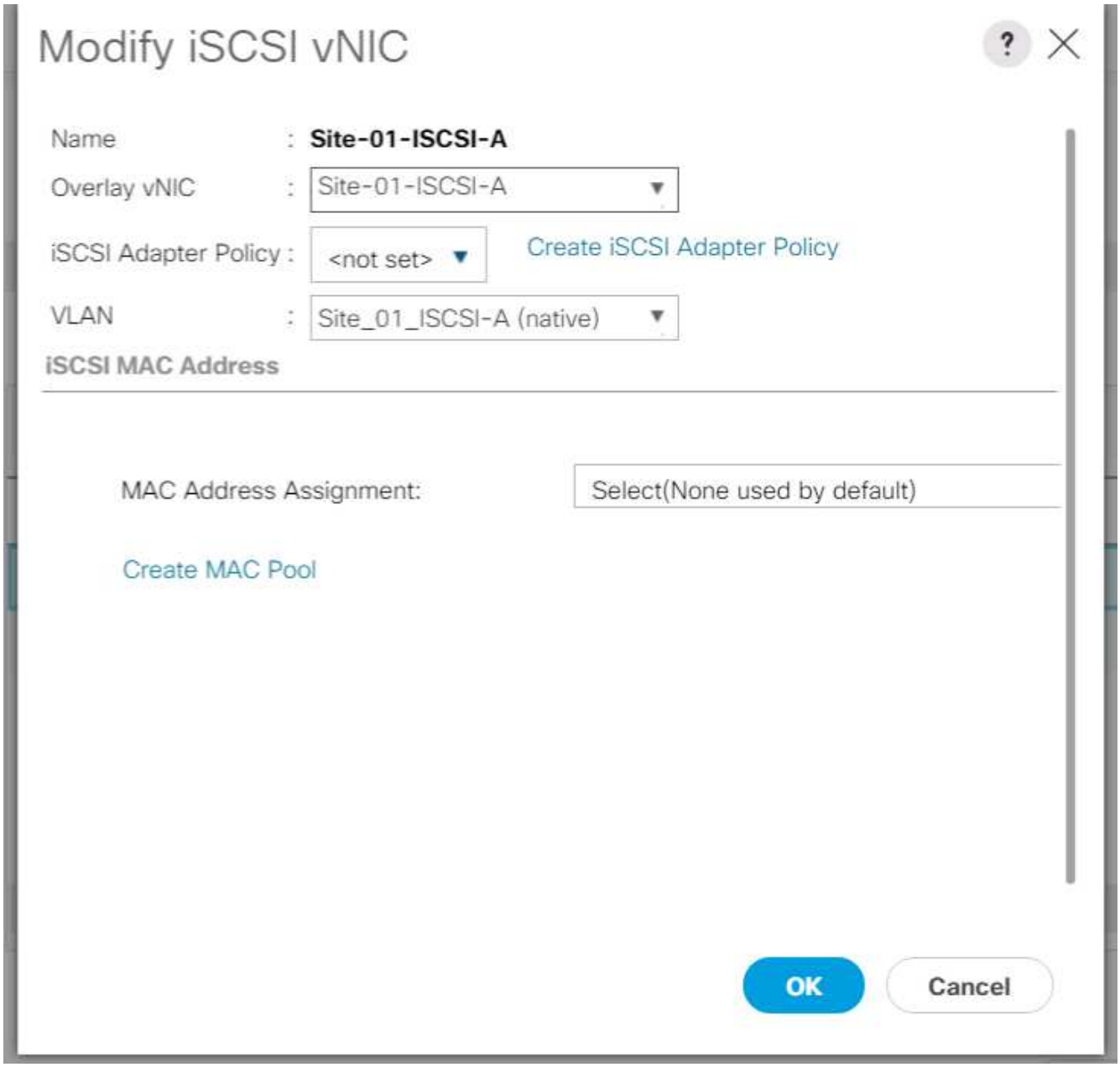
1. 在 Cisco UCS Manager 中，单击左侧的 LAN 。
2. 选择 "LAN">"Policies">"root" 。
3. 右键单击 LAN 连接策略。
4. 选择 Create LAN Connectivity Policy 。
5. 输入 `Site-XX-Fabric-A` 作为策略名称。
6. 单击上部的添加选项以添加 vNIC 。
7. 在 Create vNIC 对话框中，输入 `Site-01-vNIC-A` 作为 vNIC 的名称。

8. 选择使用 vNIC 模板选项。
9. 在 vNIC 模板列表中，选择 `vNIC_Template_A` 。
10. 从适配器策略下拉列表中，选择 VMware 。
11. 单击确定将此 vNIC 添加到策略中。

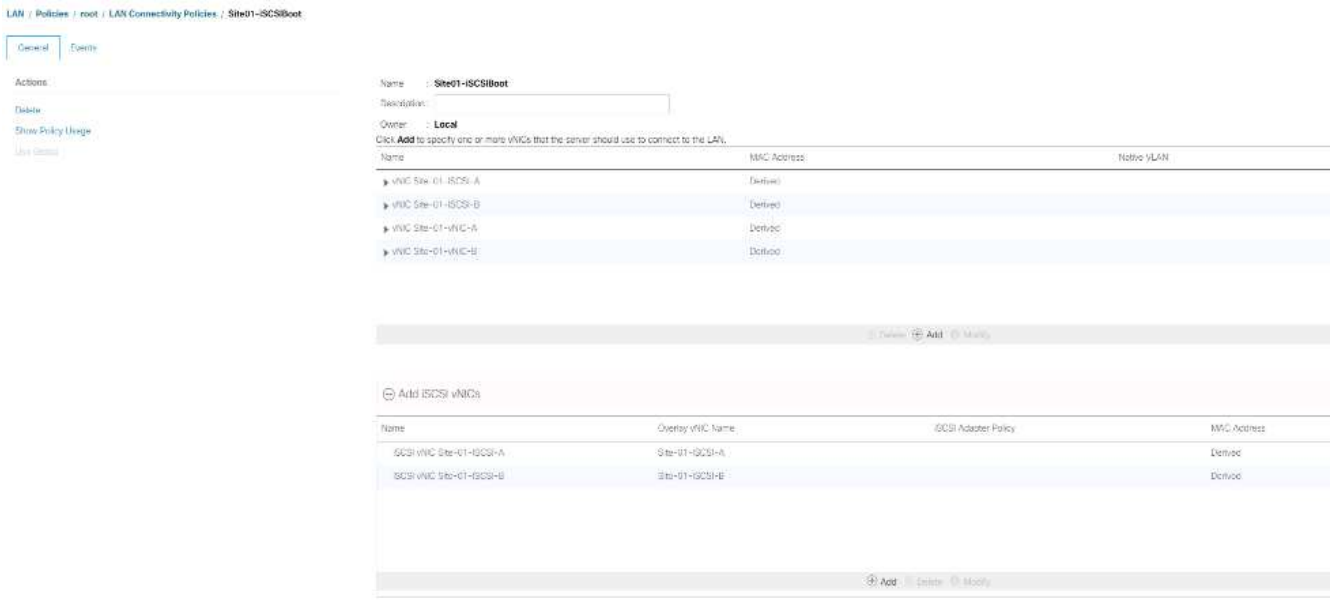


12. 单击上部的添加选项以添加 vNIC 。
13. 在 Create vNIC 对话框中，输入 `Site-01-vNIC-B` 作为 vNIC 的名称。
14. 选择使用 vNIC 模板选项。
15. 在 vNIC 模板列表中，选择 `vNIC_Template_B` 。
16. 从适配器策略下拉列表中，选择 VMware 。
17. 单击确定将此 vNIC 添加到策略中。
18. 单击上部的添加选项以添加 vNIC 。
19. 在 Create vNIC 对话框中，输入 `Site-01- iscsi-a` 作为 vNIC 的名称。
20. 选择使用 vNIC 模板选项。
21. 在 vNIC 模板列表中，选择 `Site-01-iscsi-a` 。

22. 从适配器策略下拉列表中，选择 VMware 。
23. 单击确定将此 vNIC 添加到策略中。
24. 单击上部的添加选项以添加 vNIC 。
25. 在 Create vNIC 对话框中，输入 `Site-01-iscsi-B` 作为 vNIC 的名称。
26. 选择使用 vNIC 模板选项。
27. 在 vNIC 模板列表中，选择 `Site-01-iscsi-B` 。
28. 从适配器策略下拉列表中，选择 VMware 。
29. 单击确定将此 vNIC 添加到策略中。
30. 展开添加 iSCSI vNIC 选项。
31. 单击 Add iSCSI vNIC 空间中下部的 Add 选项以添加 iSCSI vNIC 。
32. 在 Create iSCSI vNIC 对话框中，输入 `Site-01-iscsi-a` 作为 vNIC 的名称。
33. 选择 Overlay vNIC `Site-01-iscsi-a` 。
34. 将 iSCSI 适配器策略选项保留为未设置。
35. 选择 VLAN `Site-01-iscsi-Site-A` （原生）。
36. 选择无（默认使用）作为 MAC 地址分配。
37. 单击确定将 iSCSI vNIC 添加到策略中。



38. 单击 Add iSCSI vNIC 空间中下部的 Add 选项以添加 iSCSI vNIC 。
39. 在 Create iSCSI vNIC 对话框中，输入 `Site-01-iscsi-B` 作为 vNIC 的名称。
40. 选择 Overlay vNIC 作为 Site-01-iSCSI-B
41. 将 iSCSI 适配器策略选项保留为未设置。
42. 选择 VLAN `Site-01-iscsi-Site-B` （原生）。
43. 选择无（默认使用）作为 MAC 地址分配。
44. 单击确定将 iSCSI vNIC 添加到策略中。
45. 单击 Save Changes 。



为 **VMware ESXi 6.7U1** 安装启动创建 **vMedia** 策略

在 NetApp Data ONTAP 设置步骤中，需要使用 HTTP Web 服务器来托管 NetApp Data ONTAP 和 VMware 软件。此处创建的 vMedia 策略映射了 VMware ESXi 6 。7U1 ISO 连接到 Cisco UCS 服务器，以便启动 ESXi 安装。要创建此策略，请完成以下步骤：

1. 在 Cisco UCS Manager 中，选择左侧的 Servers 。
2. 选择策略 > root 。
3. 选择 vMedia 策略。
4. 单击添加以创建新的 vMedia 策略。
5. 将策略命名为 esxia-6.7U1-HTTP 。
6. 在问题描述字段中输入适用于 ESXi 6.7U1 的挂载 ISO 。
7. 对于挂载失败时重试，请选择是。
8. 单击添加。
9. 将挂载的 ESXI-6.7U1-HTTP 命名为。
10. 选择客户尽职调查设备类型。
11. 选择 HTTP 协议。
12. 输入 Web 服务器的 IP 地址。

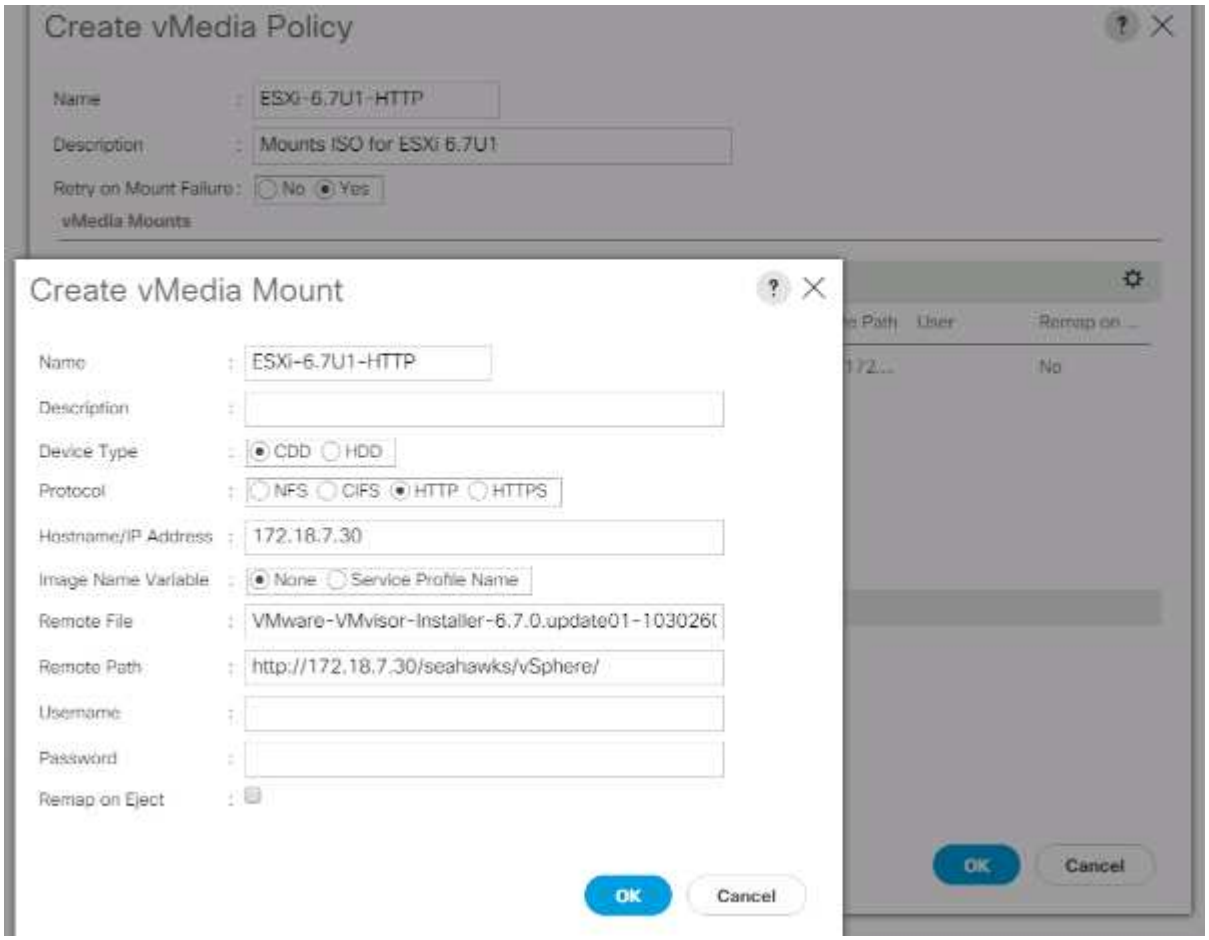
    > 先前未将 DNS 服务器 IP 输入到 KVM IP 中，因此，需要输入 Web 服务器的 IP ，而不是主机名。

13. 输入 `vmware-vmvis-Installer-6.7.0.Update01-10302608.x86_64` 作为远程文件名称。

    此 VMware ESXi 6.7U1 ISO 可从下载 "VMware 下载"。

14. 在远程路径字段中输入 ISO 文件的 Web 服务器路径。
15. 单击确定创建 vMedia 挂载。
16. 再次单击确定，然后单击确定以完成 vMedia 策略的创建。

    对于添加到 Cisco UCS 环境中的任何新服务器，可以使用 vMedia 服务配置文件模板安装 ESXi 主机。首次启动时，主机将启动到 ESXi 安装程序中，因为 SAN 挂载的磁盘为空。安装 ESXi 后，只要启动磁盘可访问，就不会引用 vMedia 。



创建 **iSCSI** 启动策略

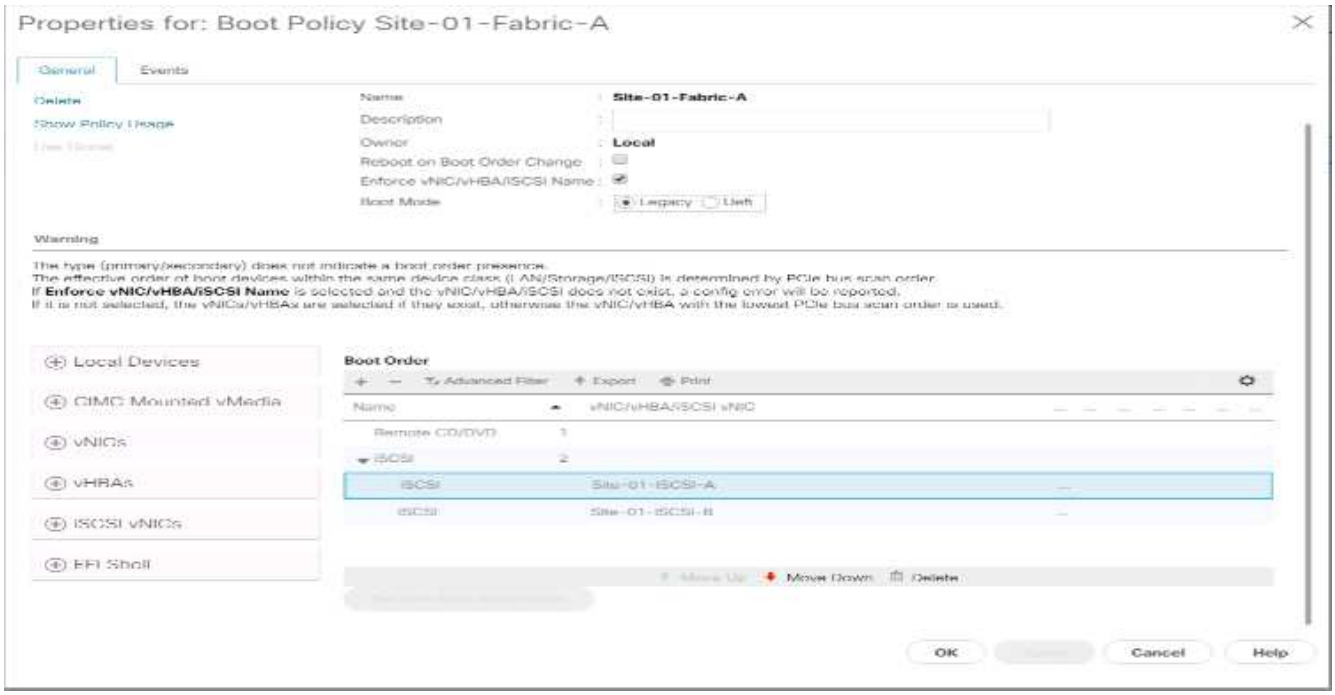
本节中的操作步骤用于适用场景一种 Cisco UCS 环境，其中两个 iSCSI 逻辑接口（ LIF ）位于集群节点 1 上（`iscsi_lif01a` 和 `iscsi_lif01b` ），两个 iSCSI LIF 位于集群节点 2 上（`iscsi_lif02a` 和 `iscsi_lif02b` ）。此外，还假定 A LIF 连接到阵列 A （ Cisco UCS 互联阵列 A ）， B LIF 连接到阵列 B （ Cisco UCS 互联阵列 B ）。

> 在此操作步骤中配置了一个启动策略。此策略会将主目标配置为 `iscsi_lif01a` 。

要为 Cisco UCS 环境创建启动策略，请完成以下步骤：

1. 在 Cisco UCS Manager 中，单击左侧的服务器。
2. 选择策略 > root 。
3. 右键单击启动策略。

4. 选择 Create Boot Policy 。
5. 输入 `Site-01-Fabric-A` 作为启动策略的名称。
6. 可选：输入启动策略的问题描述。
7. 保持清除 " 更改启动顺序后重新启动 " 选项。
8. 启动模式为传统模式。
9. 展开本地设备下拉菜单，然后选择添加远程 CD/DVD 。
10. 展开 iSCSI vNIC 下拉菜单，然后选择添加 iSCSI 启动。
11. 在添加 iSCSI 启动对话框中，输入 `Site-01-iscsi-A` 。单击确定。
12. 选择添加 iSCSI 启动。
13. 在添加 iSCSI 启动对话框中，输入 `Site-01-iscsi-B` 。单击确定。
14. 单击确定创建策略。



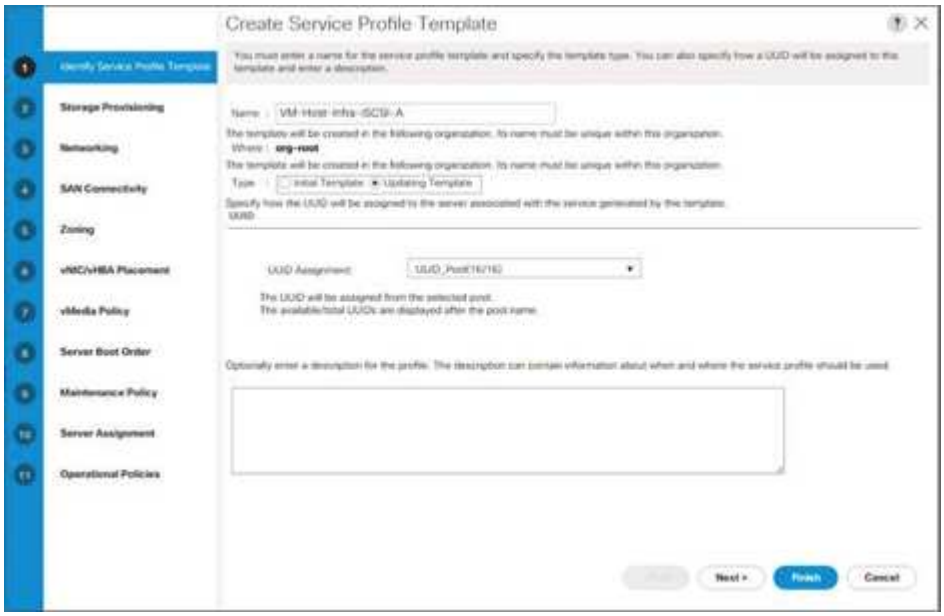
创建服务配置文件模板

在此操作步骤中，为基础架构 ESXi 主机创建了一个用于阵列 A 启动的服务配置文件模板。

要创建服务配置文件模板，请完成以下步骤：

1. 在 Cisco UCS Manager 中，单击左侧的服务器。
2. 选择服务配置文件模板 > 根。
3. 右键单击 root 。
4. 选择创建服务配置文件模板以打开创建服务配置文件模板向导。
5. 输入 `VM-Host-Infra-iscsi-A` 作为服务配置文件模板的名称。此服务配置文件模板已配置为从网络结构 A 上的存储节点 1 启动

6. 选择更新模板选项。
7. 在 UUID 下，选择 `UID_Pool` 作为 UUID 池。单击下一步。



配置存储配置

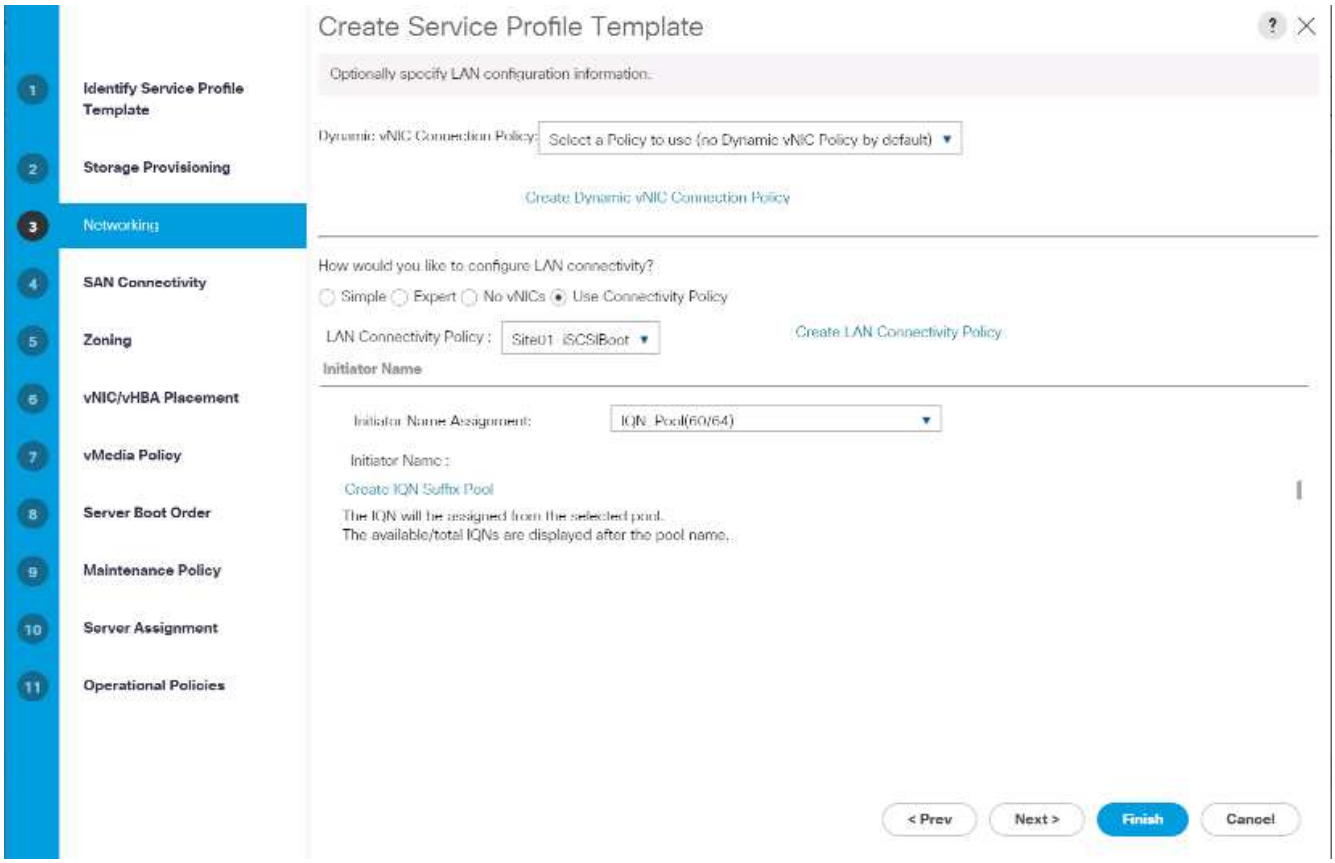
要配置存储配置，请完成以下步骤：

1. 如果您的服务器没有物理磁盘，请单击本地磁盘配置策略并选择 SAN 启动本地存储策略。否则，请选择默认的本地存储策略。
2. 单击下一步。

配置网络选项

要配置网络选项，请完成以下步骤：

1. 保留动态 vNIC 连接策略的默认设置。
2. 选择使用连接策略选项以配置 LAN 连接。
3. 从 LAN 连接策略下拉菜单中选择 iSCSI-Boot 。
4. 在启动程序名称分配中选择 `IQN_Pool` 。单击下一步。



配置 **SAN** 连接

要配置 SAN 连接，请完成以下步骤：

1. 对于 vHBA ，为 How would you like to Configure SAN Connectivity ？ 选项
2. 单击下一步。

配置分区

要配置分区，只需单击下一步即可。

配置 **vNIC/HBA** 放置

要配置 vNIC/HBA 放置，请完成以下步骤：

1. 从选择放置下拉列表中，将放置策略保留为让系统执行放置。
2. 单击下一步。

配置 **vMedia** 策略

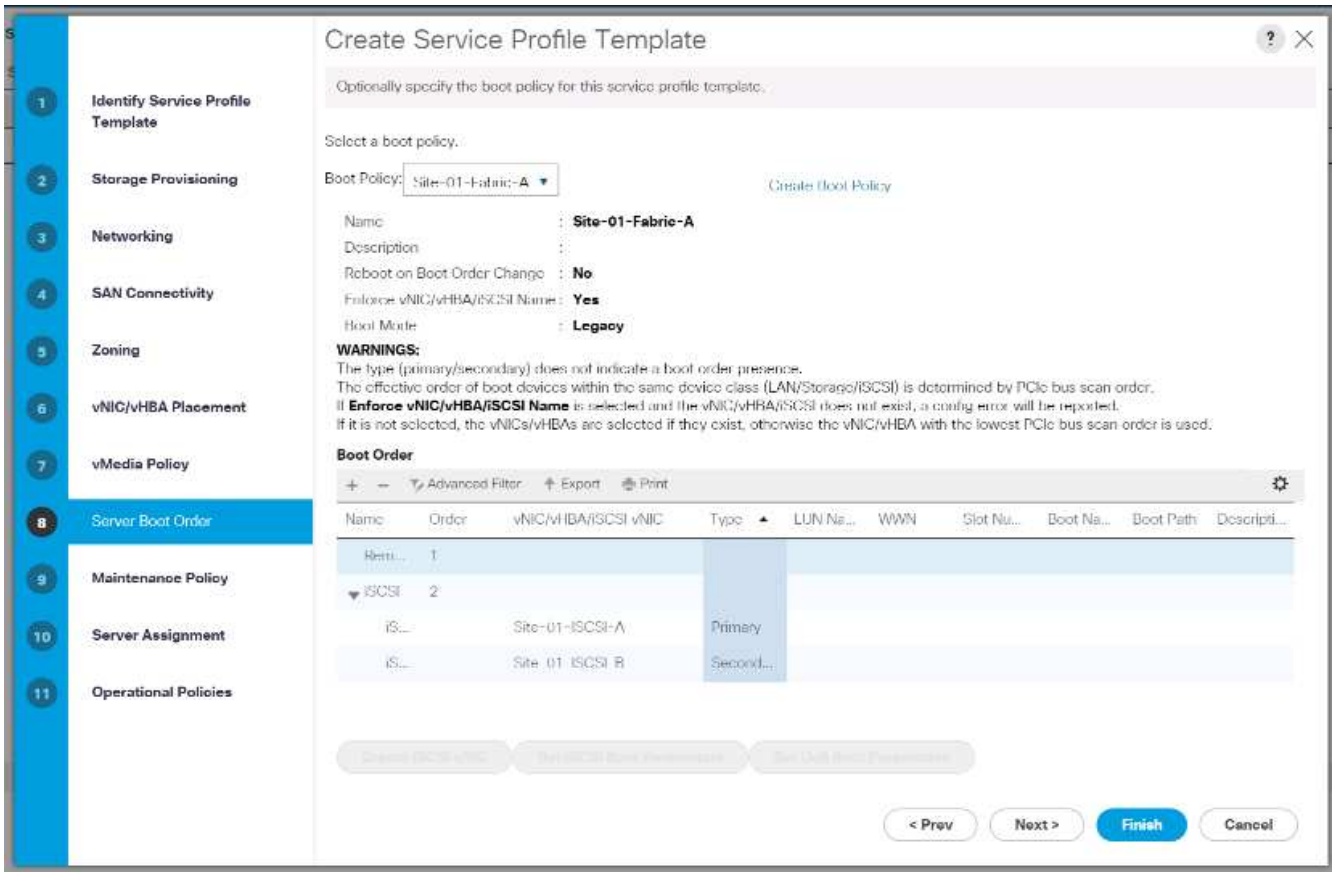
要配置 vMedia 策略，请完成以下步骤：

1. 请勿选择 vMedia 策略。
2. 单击下一步。

配置服务器启动顺序

要配置服务器启动顺序，请完成以下步骤：

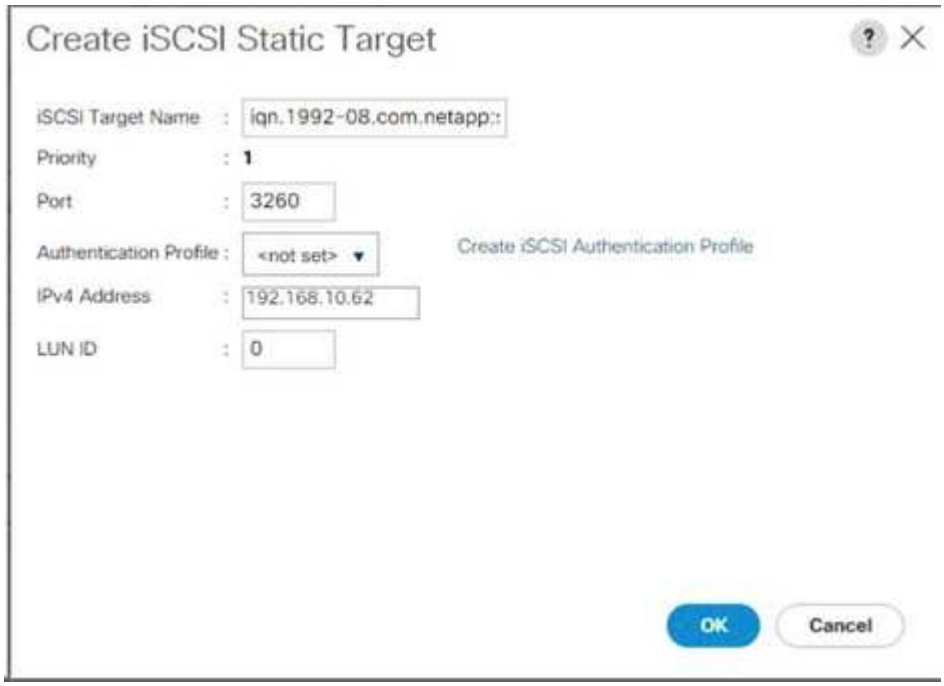
1. 为 Boot Policy 选择 `Boot-Fabric-A` 。



2. 在 Boor 顺序中，选择 `Site-01- iscsi-a` 。
3. 单击设置 iSCSI 启动参数。
4. 在设置 iSCSI 启动参数对话框中，将身份验证配置文件选项保留为未设置，除非您已为您的环境单独创建相应的配置文件。
5. 保持 "Initiator Name Assignment" 对话框未设置为使用上述步骤中定义的单个服务配置文件启动程序名称。
6. 将 `iSCSI_IP_Pool_A` 设置为启动程序 IP 地址策略。
7. 选择 iSCSI 静态目标接口选项。
8. 单击添加。
9. 输入 iSCSI 目标名称。要获取 Infra-SVM 的 iSCSI 目标名称，请登录到存储集群管理界面并运行 `iscsi show` 命令。

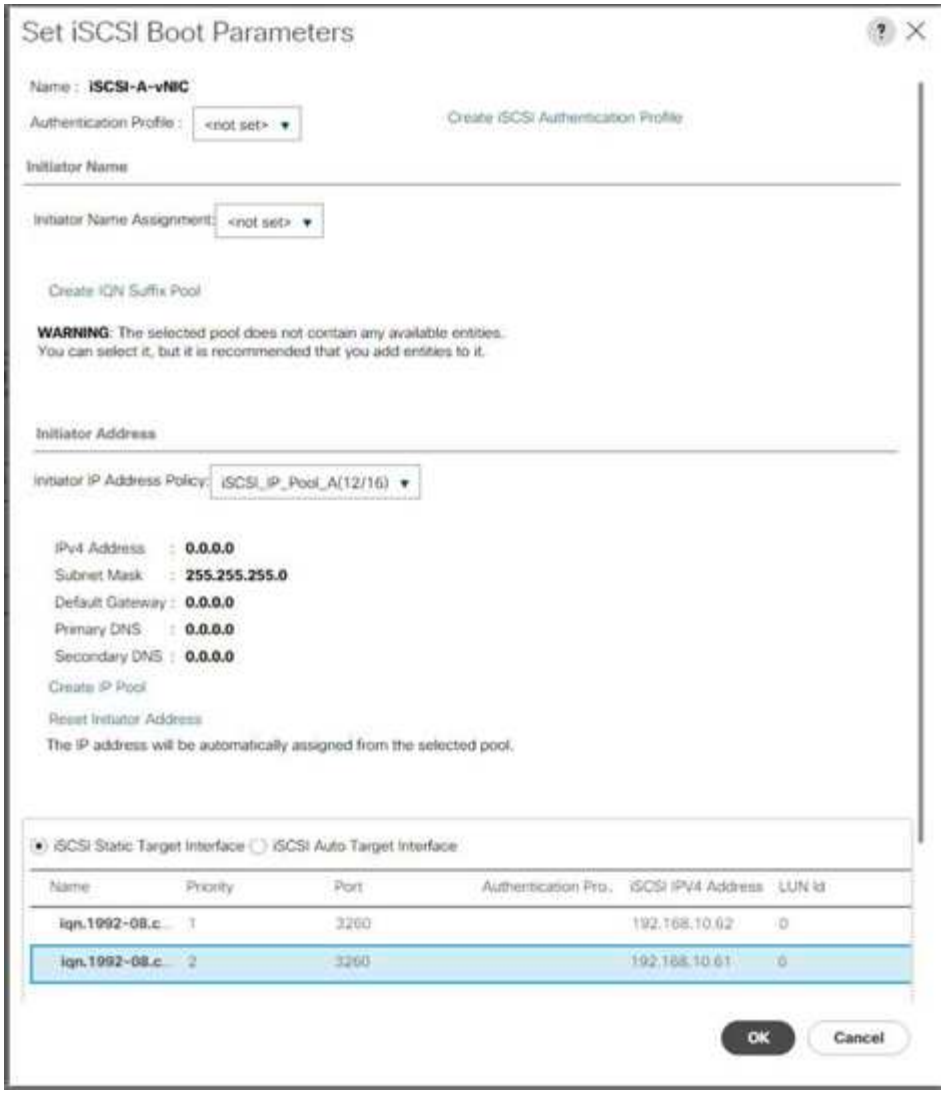
```
bb04-aff300::> iscsi show
          Target                          Target                    Status
Vserver   Name                            Alias                     Admin
--------- ------------------------------- ------------------------- ------
Infra-SVM iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                          Infra-SVM                 up
```

10. 在 "IPv4 Address" 字段中输入 IP 地址 `iscsi_lif_02a` 。



11. 单击确定以添加 iSCSI 静态目标。
12. 单击添加。
13. 输入 iSCSI 目标名称。
14. 在 "IPv4 Address" 字段中输入 IP 地址 `iscsi_lif_01a` 。

15. 单击确定以添加 iSCSI 静态目标。



目标 IP 首先放在存储节点 02 IP 上，其次放在存储节点 01 IP 上。此配置假定启动 LUN 位于节点 01 上。如果使用了此操作步骤中的顺序，则主机将使用节点 01 的路径启动。

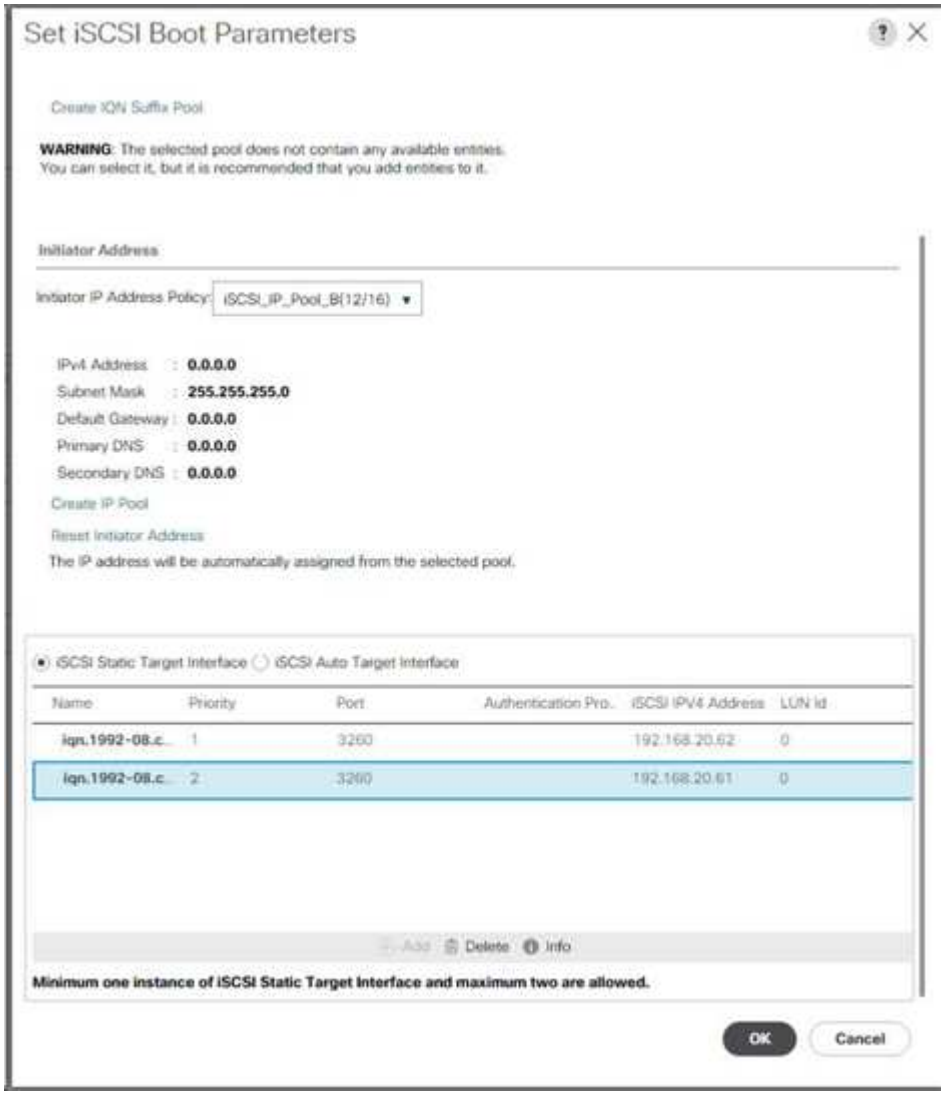
16. 在启动顺序中，选择 iSCSI-B-vNIC 。
17. 单击设置 iSCSI 启动参数。
18. 在设置 iSCSI 启动参数对话框中，将身份验证配置文件选项保留为未设置，除非您已独立创建适合您的环境的配置文件。
19. 保持 "Initiator Name Assignment" 对话框未设置为使用上述步骤中定义的单个服务配置文件启动程序名称。
20. 将 `iscsi_ip_pool_B` 设置为启动程序 IP 地址策略。
21. 选择 iSCSI 静态目标接口选项。
22. 单击添加。
23. 输入 iSCSI 目标名称。要获取 Infra-SVM 的 iSCSI 目标名称，请登录到存储集群管理界面并运行 `iscsi show` 命令。

```
bb04-aff300::> iscsi show
           Target                          Target                      Status
Vserver    Name                            Alias                       Admin
---------- ------------------------------- --------------------------- ------
Infra-SVM  iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                           Infra-SVM                   up
```

24. 在 "IPv4 Address" 字段中输入 IP 地址 `iscsi_lif_02B` 。

25. 单击确定以添加 iSCSI 静态目标。
26. 单击添加。
27. 输入 iSCSI 目标名称。
28. 在 "IPv4 Address" 字段中输入 IP 地址 `iscsi_lif_01B` 。

29. 单击确定以添加 iSCSI 静态目标。

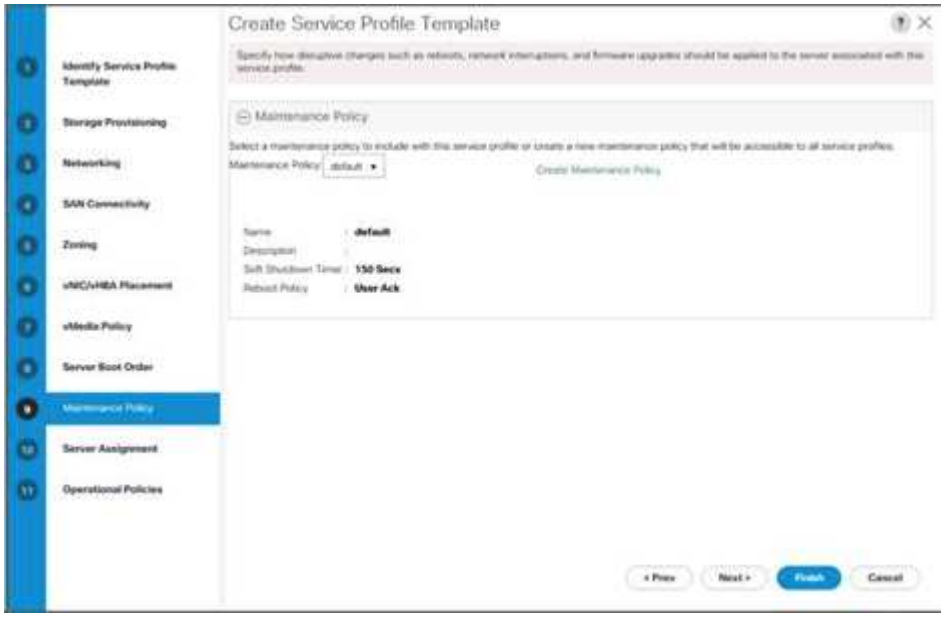


30. 单击下一步。

配置维护策略

要配置维护策略，请完成以下步骤：

1. 将维护策略更改为默认值。

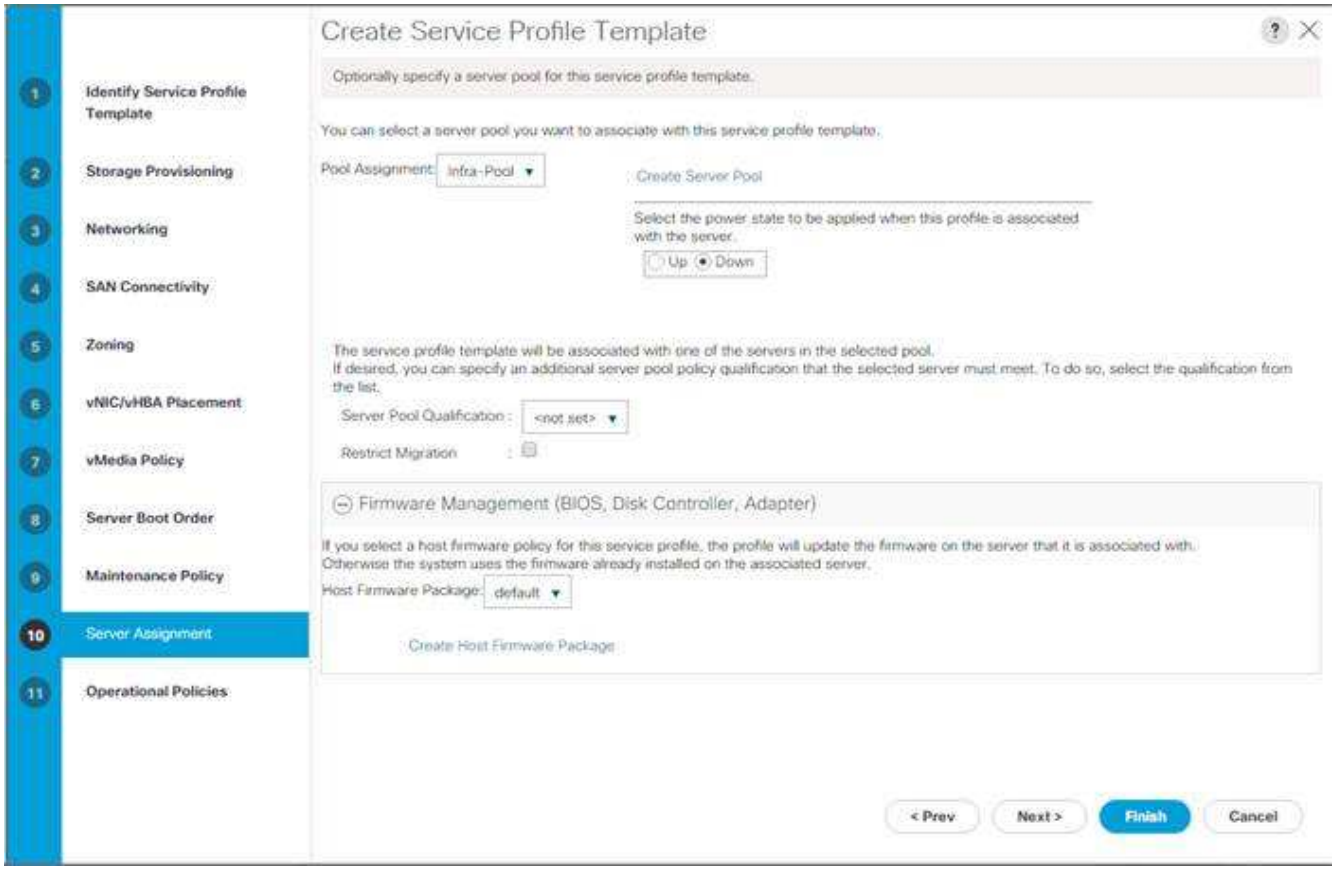


2. 单击下一步。

配置服务器分配

要配置服务器分配，请完成以下步骤：

1. 在 Pool Assignment 列表中，选择 Infra-Pool 。
2. 选择 down 作为配置文件与服务器关联时要应用的电源状态。
3. 展开页面底部的 Firmware Management ，然后选择默认策略。

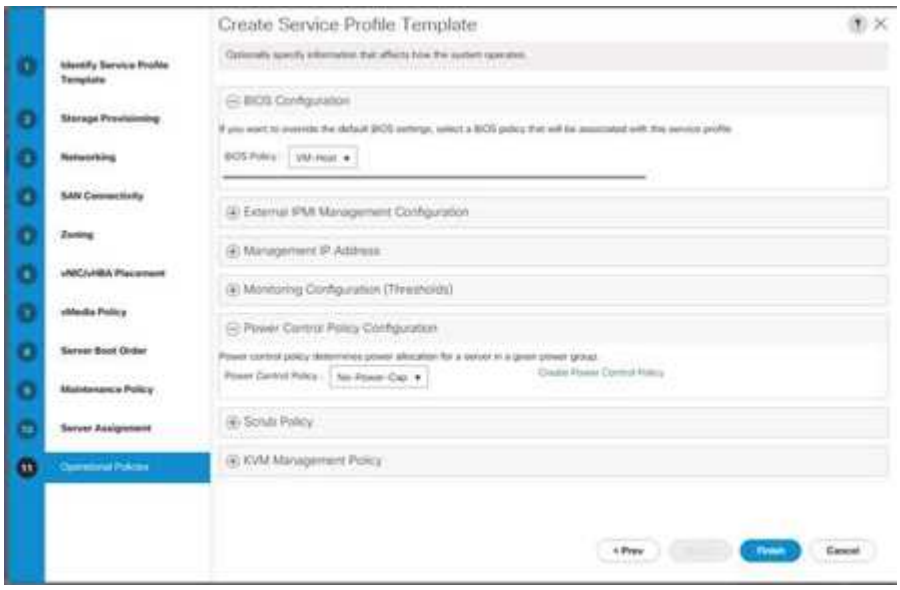


4. 单击下一步。

配置操作策略

要配置操作策略，请完成以下步骤：

1. 从 BIOS 策略下拉列表中，选择 VM-Host 。
2. 展开电源控制策略配置，然后从电源控制策略下拉列表中选择 No-Power-Cap 。



3. 单击完成以创建服务配置文件模板。
4. 单击确认消息中的确定。

创建启用了 **vMedia** 的服务配置文件模板

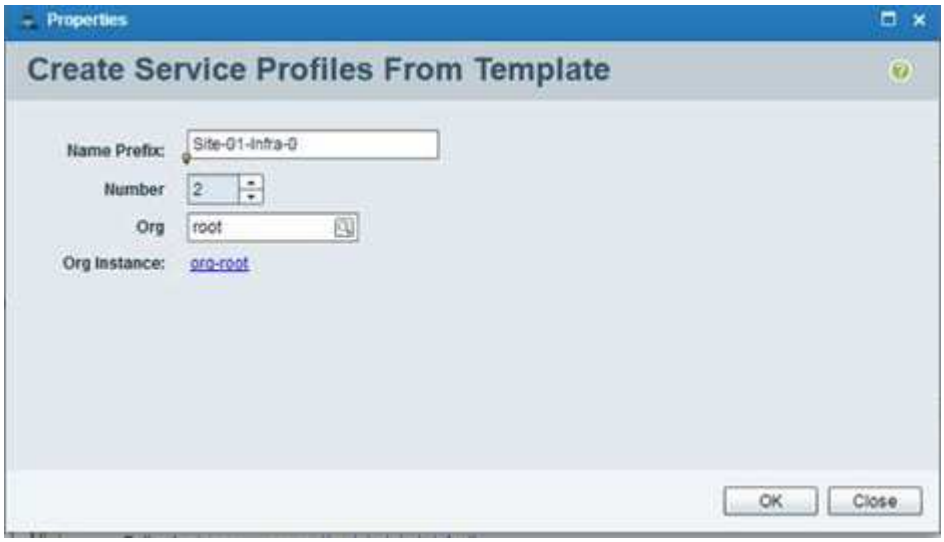
要在启用了 vMedia 的情况下创建服务配置文件模板，请完成以下步骤：

1. 连接到 UCS Manager ，然后单击左侧的服务器。
2. 选择服务配置文件模板 > 根 > 服务模板 VM-Host-Infra-iSCSI-A
3. 右键单击 VM-Host-Infra-iSCSI-A ，然后选择 Create a Clone 。
4. 将克隆命名为 `VM-Host-Infra-iSCSI-A-VM` 。
5. 选择新创建的 VM-Host-Infra-iSCSI-A-VM ，然后选择右侧的 vMedia Policy 选项卡。
6. 单击修改 vMedia 策略。
7. 选择 ESXI-6 。7U1-HTTP vMedia Policy ，然后单击确定。
8. 单击确定进行确认。

创建服务配置文件

要使用服务配置文件模板创建服务配置文件，请完成以下步骤：

1. 连接到 Cisco UCS Manager ，然后单击左侧的服务器。
2. 展开服务器 > 服务配置文件模板 > 根 > 服务模板 < 名称 > 。
3. 在操作中，单击从模板创建服务配置文件并完成以下步骤：
   a. 输入 `Site- 01-Infra-0` 作为命名前缀。
   b. 输入 `2` 作为要创建的实例数。
   c. 选择 root 作为组织。
   d. 单击确定以创建服务配置文件。



4. 单击确认消息中的确定。

5. 验证是否已创建服务配置文件 `Site-01-Infra-01` 和 `Site-01-Infra-02` 。

> 服务配置文件会自动与分配的服务器池中的服务器相关联。

存储配置第 2 部分：启动 LUN 和启动程序组

ONTAP 启动存储设置

创建启动程序组

要创建启动程序组（ igroup ），请完成以下步骤：

1. 从集群管理节点 SSH 连接运行以下命令：

```
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-01 -protocol
iscsi -ostype vmware -initiator <vm-host-infra-01-iqn>
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-02 -protocol
iscsi -ostype vmware -initiator <vm-host-infra-02-iqn>
igroup create -vserver Infra-SVM -igroup MGMT-Hosts -protocol iscsi
-ostype vmware -initiator <vm-host-infra-01-iqn>, <vm-host-infra-02-iqn>
```

> 使用表 1 和表 2 中列出的值获取 IQN 信息。

2. 要查看刚刚创建的三个 igroup ，请运行 `igroup show` 命令。

将启动 **LUN** 映射到 **igroup**

要将启动 LUN 映射到 igroup ，请完成以下步骤：

1. 在存储集群管理 SSH 连接中，运行以下命令：

```
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra- A
-igroup VM-Host-Infra-01 -lun-id 0lun map -vserver Infra-SVM -volume
esxi_boot -lun VM-Host-Infra- B -igroup VM-Host-Infra-02 -lun-id 0
```

VMware vSphere 6.7U1 部署操作步骤

本节详细介绍了在 FlexPod 快速配置中安装 VMware ESXi 6.7U1 的过程。完成这些过程后，将配置两个已启动的 ESXi 主机。

可以通过多种方法在 VMware 环境中安装 ESXi 。这些过程主要介绍如何使用 Cisco UCS Manager 中的内置 KVM 控制台和虚拟介质功能将远程安装介质映射到各个服务器并连接到其启动 LUN 。

下载适用于 **ESXi 6.7U1** 的 **Cisco** 自定义映像

如果尚未下载 VMware ESXi 自定义映像，请完成以下步骤以完成下载：

1. 单击以下链接： https://my.vmware.com/group/vmware/details?downloadGroup=OEM-ESXI67U1-CISCO&productId=742[VMware vSphere Hypervisor （ESXi） 6.7U1 。^
2. 您需要上的用户 ID 和密码 "vmware.com" 下载此软件。
3. 下载 `.ISO` 文件。

Cisco UCS Manager

通过 Cisco UCS IP KVM ，管理员可以通过远程介质开始安装操作系统。要运行 IP KVM ，必须登录到 Cisco UCS 环境。

要登录到 Cisco UCS 环境，请完成以下步骤：

1. 打开 Web 浏览器并输入 Cisco UCS 集群地址的 IP 地址。此步骤将启动 Cisco UCS Manager 应用程序。
2. 单击 HTML 下的 Launch UCS Manager 链接以启动 HTML 5 UCS Manager GUI 。
3. 如果系统提示您接受安全证书，请根据需要接受。
4. 出现提示时，输入 `admin` 作为用户名，然后输入管理密码。
5. 要登录到 Cisco UCS Manager ，请单击 Login 。
6. 从主菜单中，单击左侧的服务器。
7. 选择服务器 > 服务配置文件 > 根 > `VM-Host-Infra-01` 。
8. 右键单击 `VM-Host-Infra-01` 并选择 KVM 控制台。
9. 按照提示启动基于 Java 的 KVM 控制台。
10. 选择服务器 > 服务配置文件 > 根 > `VM-Host-Infra-02` 。
11. 右键单击 `VM-Host-Infra-02` 。并选择 KVM 控制台。
12. 按照提示启动基于 Java 的 KVM 控制台。

设置 **VMware ESXi** 安装

ESXi 托管 VM-Host-Infra-01 和 VM-Host- Infra-02

要为安装操作系统准备服务器，请在每个 ESXi 主机上完成以下步骤：

1. 在 KVM 窗口中，单击虚拟介质。
2. 单击激活虚拟设备。
3. 如果系统提示接受未加密的 KVM 会话，请根据需要接受。
4. 单击 Virtual Media 并选择 Map CD/DVD 。
5. 浏览到 ESXi 安装程序 ISO 映像文件，然后单击打开。
6. 单击映射设备。
7. 单击 KVM 选项卡以监控服务器启动。

- 安装 ESXi*

ESXi 主机 VM-Host-Infra-01 和 VM-Host-Infra-02

要将 VMware ESXi 安装到主机的 iSCSI 可启动 LUN ，请在每个主机上完成以下步骤：

1. 选择 Boot Server 并单击 OK 以启动服务器。然后再次单击确定。
2. 重新启动时，计算机会检测是否存在 ESXi 安装介质。从显示的启动菜单中选择 ESXi 安装程序。
3. 安装程序加载完毕后，按 Enter 继续安装。
4. 阅读并接受最终用户许可协议（ EULA ）。按 F11 接受并继续。
5. 选择先前设置为 ESXi 安装磁盘的 LUN ，然后按 Enter 继续安装。
6. 选择适当的键盘布局，然后按 Enter 键。
7. 输入并确认根密码，然后按 Enter 键。
8. 安装程序会发出警告，指出选定磁盘将重新分区。按 F11 继续安装。
9. 安装完成后，选择 Virtual Media 选项卡并清除 ESXi 安装介质旁边的 P 标记。单击是。

   ⓘ 必须取消映射 ESXi 安装映像，以确保服务器重新启动到 ESXi 而不是安装程序。

10. 安装完成后，按 Enter 重新启动服务器。
11. 在 Cisco UCS Manager 中，将当前服务配置文件绑定到非 vMedia 服务配置文件模板，以防止通过 HTTP 挂载 ESXi 安装 ISO 。

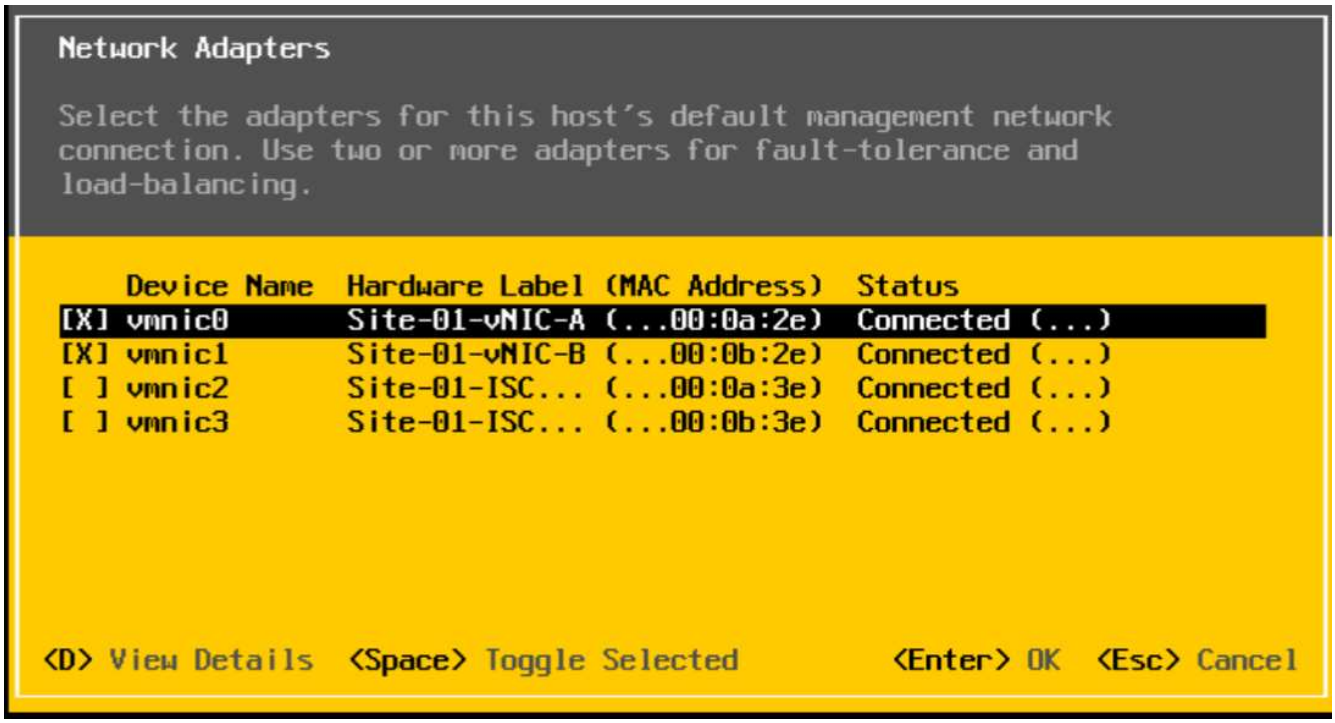
为 **ESXi** 主机设置管理网络

要管理每个 VMware 主机，必须为该主机添加管理网络。要为 VMware 主机添加管理网络，请在每个 ESXi 主机上完成以下步骤：

ESXi 主机 VM-Host-Infra-01 和 VM-Host-Infra-02

要为每个 ESXi 主机配置对管理网络的访问权限，请完成以下步骤：

1. 服务器完成重新启动后，按 F2 自定义系统。
2. 以 `root` 身份登录，输入相应的密码，然后按 Enter 登录。
3. 选择 Troubleshooting Options ，然后按 Enter 键。
4. 选择 "Enable ESXi Shell （启用 ESXi Shell ） "，然后按 Enter 键。
5. 选择 Enable SSH ，然后按 Enter 键。
6. 按 Esc 退出 Troubleshooting Options 菜单。
7. 选择 Configure Management Network 选项，然后按 Enter 键。
8. 选择网络适配器，然后按 Enter 键。
9. 验证硬件标签字段中的数字是否与设备名称字段中的数字匹配。
10. 按 Enter 键。



11. 选择 VLAN （可选）选项，然后按 Enter 键。
12. 输入 ` <IB-mgmt-vlan-id>` 并按 Enter 键。
13. 选择 IPv4 Configuration ，然后按 Enter 键。
14. 使用空格键选择设置静态 IPv4 地址和网络配置选项。
15. 输入用于管理第一台 ESXi 主机的 IP 地址。
16. 输入第一台 ESXi 主机的子网掩码。
17. 输入第一台 ESXi 主机的默认网关。
18. 按 Enter 接受对 IP 配置所做的更改。
19. 选择 DNS Configuration 选项并按 Enter 键。

    由于 IP 地址是手动分配的，因此还必须手动输入 DNS 信息。

20. 输入主 DNS 服务器的 IP 地址。
21. 可选：输入二级 DNS 服务器的 IP 地址。
22. 输入第一个 ESXi 主机的 FQDN 。
23. 按 Enter 接受对 DNS 配置所做的更改。
24. 按 Esc 退出配置管理网络菜单。
25. 选择 Test Management Network 以验证管理网络是否设置正确，然后按 Enter 键。
26. 按 Enter 键运行测试，测试完成后再次按 Enter 键，如果出现故障，请查看环境。
27. 再次选择 Configure Management Network ，然后按 Enter 键。
28. 选择 IPv6 配置选项，然后按 Enter 键。
29. 使用空格键选择 Disable IPv6 （ restart required ），然后按 Enter 键。

30. 按 Esc 退出配置管理网络子菜单。
31. 按 Y 确认更改并重新启动 ESXi 主机。

重置 **VMware ESXi** 主机 **VMkernel** 端口 **vmk0 MAC** 地址（可选）

ESXi 主机 VM-Host-Infra-01 和 VM-Host-Infra-02

默认情况下，管理 VMkernel 端口 vmk0 的 MAC 地址与其所在以太网端口的 MAC 地址相同。如果将 ESXi 主机的启动 LUN 重新映射到具有不同 MAC 地址的其他服务器，则会发生 MAC 地址冲突，因为 vmk0 会保留分配的 MAC 地址，除非重置 ESXi 系统配置。要将 vmk0 的 MAC 地址重置为 VMware 分配的随机 MAC 地址，请完成以下步骤：

1. 在 ESXi 控制台菜单主屏幕中，按 Ctrl-Alt-F1 可访问 VMware 控制台命令行界面。在 UCSM KVM 中， Ctrl-Alt-F1 将显示在静态宏列表中。
2. 以 root 用户身份登录。
3. 键入 `esxcfg-vmknic - l` 可获取接口 vmk0 的详细列表。vmk0 应属于管理网络端口组。记下 vmk0 的 IP 地址和网络掩码。
4. 要删除 vmk0 ，请输入以下命令：

```
esxcfg-vmknic –d “Management Network”
```

5. 要使用随机 MAC 地址重新添加 vmk0 ，请输入以下命令：

```
esxcfg-vmknic –a –i <vmk0-ip> -n <vmk0-netmask> “Management Network””.
```

6. 验证是否已使用随机 MAC 地址重新添加 vmk0

```
esxcfg-vmknic –l
```

7. 键入 `exit` 退出命令行界面。
8. 按 Ctrl-Alt-F2 返回到 ESXi 控制台菜单界面。

使用 **VMware** 主机客户端登录到 **VMware ESXi** 主机

ESXi 主机 VM-Host-Infra-01

要使用 VMware Host Client 登录到 VM-Host-Infra-01 ESXi 主机，请完成以下步骤：

1. 在管理工作站上打开 Web 浏览器，然后导航到 `VM-Host-Infra-01` 管理 IP 地址。
2. 单击 Open the VMware Host Client 。
3. 输入 `root` 作为用户名。
4. 输入 root 密码。

5. 单击 Login 进行连接。
6. 重复此过程以在单独的浏览器选项卡或窗口中登录到 `VM-Host-Infra-02` 。

为 **Cisco** 虚拟接口卡（ **VIC** ）安装 **VMware** 驱动程序

将以下 VMware VIC 驱动程序的脱机捆绑包下载并解压缩到管理工作站：

- Nenic 驱动程序 1.0.25.0 版

ESXi 主机 **VM-Host-Infra-01** 和 **VM-Host-Infra-02**

要在 ESXi 主机 VM-Host-Infra-01 和 VM-Host-Infra-02 上安装 VMware VIC 驱动程序，请完成以下步骤：

1. 从每个主机客户端中，选择存储。
2. 右键单击 datastore1 并选择浏览。
3. 在数据存储库浏览器中，单击上传。
4. 导航到已下载 VIC 驱动程序的保存位置，然后选择 VMW-ESX-6.7.0-nenic-1.0.25.0-offline_bundle-11271332.zip 。
5. 在数据存储库浏览器中，单击上传。
6. 单击打开将文件上传到 datastore1 。
7. 确保已将此文件上传到两个 ESXi 主机。
8. 如果尚未将每个主机置于维护模式，请将其置于维护模式。
9. 通过 ssh 从 Shell 连接或 putty 终端连接到每个 ESXi 主机。
10. 使用 root 密码以 root 用户身份登录。
11. 在每个主机上运行以下命令：

```
esxcli software vib update -d /vmfs/volumes/datastore1/VMW-ESX-6.7.0-
nenic-1.0.25.0-offline_bundle-11271332.zip
reboot
```

12. 重新启动完成后，登录到每个主机上的主机客户端并退出维护模式。

设置 **VMkernel** 端口和虚拟交换机

ESXi 主机 VM-Host-Infra-01 和 VM-Host-Infra-02

要在 ESXi 主机上设置 VMkernel 端口和虚拟交换机，请完成以下步骤：

1. 在 Host Client 中，选择左侧的 Networking 。
2. 在中间窗格中，选择虚拟交换机选项卡。
3. 选择 vSwitch0 。
4. 选择编辑设置。

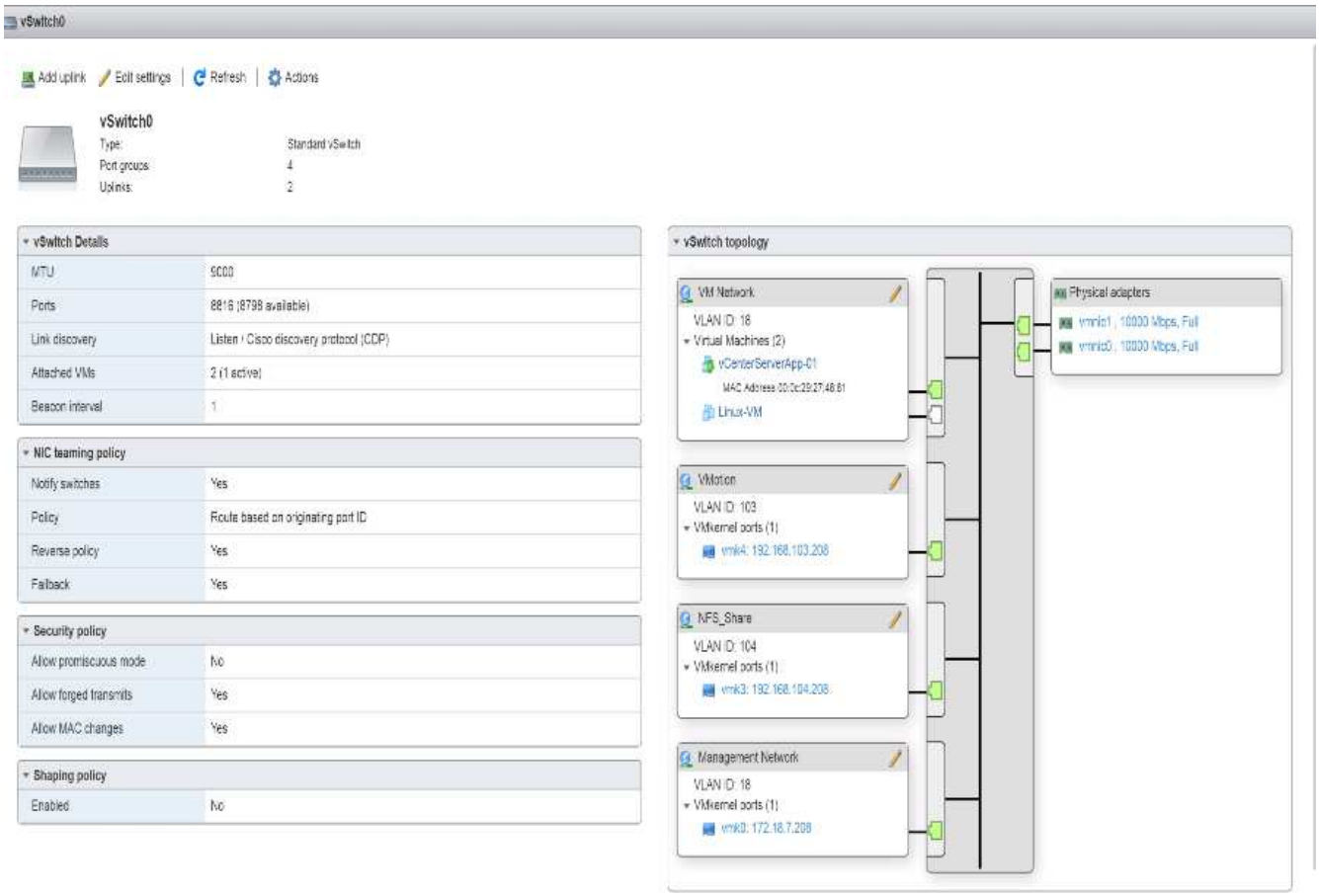
5. 将 MTU 更改为 9000 。
6. 展开 NIC 绑定。
7. 在故障转移顺序部分中，选择 vmnic1 并单击标记为活动。
8. 验证 vmnic1 现在的状态是否为 "Active" 。
9. 单击保存。
10. 选择左侧的 Networking 。
11. 在中间窗格中，选择虚拟交换机选项卡。
12. 选择 iScsiBootvSwitch 。
13. 选择编辑设置。
14. 将 MTU 更改为 9000
15. 单击保存。
16. 选择 VMkernel NIC 选项卡。
17. 选择 vmk1 iScsiBootPG 。
18. 选择编辑设置。
19. 将 MTU 更改为 9000 。
20. 展开 IPv4 设置并将 IP 地址更改为 UCS iscsi-ip-pool-A 以外的地址

> 为了避免在重新分配 Cisco UCS iSCSI IP 池地址时发生 IP 地址冲突，建议对 iSCSI VMkernel 端口使用同一子网中的不同 IP 地址。

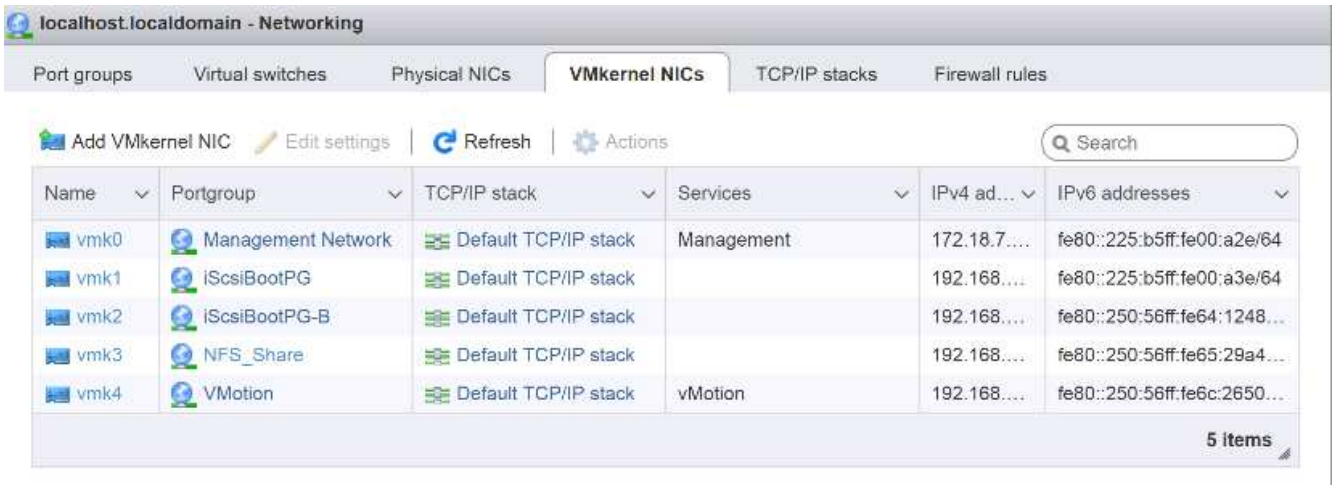
21. 单击保存。
22. 选择虚拟交换机选项卡。
23. 选择添加标准虚拟交换机。
24. 请为 vSwitch 名称提供 `iScciBootVSwitch-B` 。
25. 将 MTU 设置为 9000 。
26. 从上行链路 1 下拉菜单中选择 vmnic3 。
27. 单击添加。
28. 在中间窗格中，选择 VMkernel NIC 选项卡。
29. 选择添加 VMkernel NIC
30. 指定 iScsiBootPG-B 的新端口组名称
31. 为虚拟交换机选择 iScciBootvSwitch B 。
32. 将 MTU 设置为 9000 。请勿输入 VLAN ID 。
33. 为 IPv4 设置选择 Static ，然后展开选项以在配置中提供地址和子网掩码。

> 为了避免 IP 地址冲突，如果应重新分配 Cisco UCS iSCSI IP 池地址，建议对 iSCSI VMkernel 端口使用同一子网中的不同 IP 地址。

34. 单击创建。
35. 在左侧，选择 Networking ，然后选择 Port Groups 选项卡。
36. 在中间窗格中，右键单击 VM Network ，然后选择 Remove 。
37. 单击删除完成端口组的删除。
38. 在中间窗格中，选择添加端口组。
39. 为端口组管理网络命名，并在 VLAN ID 字段中输入 ` <IB-mgmt-vlan-id>` ，并确保已选择虚拟交换机 vSwitch0 。
40. 单击添加以完成对 IB-Mgmt 网络的编辑。
41. 在顶部，选择 VMkernel NIC 选项卡。
42. 单击添加 VMkernel NIC 。
43. 对于新端口组，输入 vMotion 。
44. 对于虚拟交换机，选择 vSwitch0 selected 。
45. 输入 ` <vmotion-vlan-id>` 作为 VLAN ID 。
46. 将 MTU 更改为 9000 。
47. 选择静态 IPv4 设置并展开 IPv4 设置。
48. 输入 ESXi 主机 vMotion IP 地址和网络掩码。
49. 选择 vMotion 堆栈 TCP/IP 堆栈。
50. 在 Services 下选择 vMotion 。
51. 单击创建。
52. 单击添加 VMkernel NIC 。
53. 对于新端口组，输入 nfs_share 。
54. 对于虚拟交换机，选择 vSwitch0 selected 。
55. 输入 ` <infra-nfs-vlan-id>` 作为 VLAN ID
56. 将 MTU 更改为 9000 。
57. 选择静态 IPv4 设置并展开 IPv4 设置。
58. 输入 ESXi 主机基础架构 NFS IP 地址和网络掩码。
59. 请勿选择任何服务。
60. 单击创建。
61. 选择 Virtual Switches 选项卡，然后选择 vSwitch0 。vSwitch0 VMkernel NIC 的属性应类似于以下示例：



62. 选择 VMkernel NIC 选项卡以确认已配置的虚拟适配器。列出的适配器应类似于以下示例：



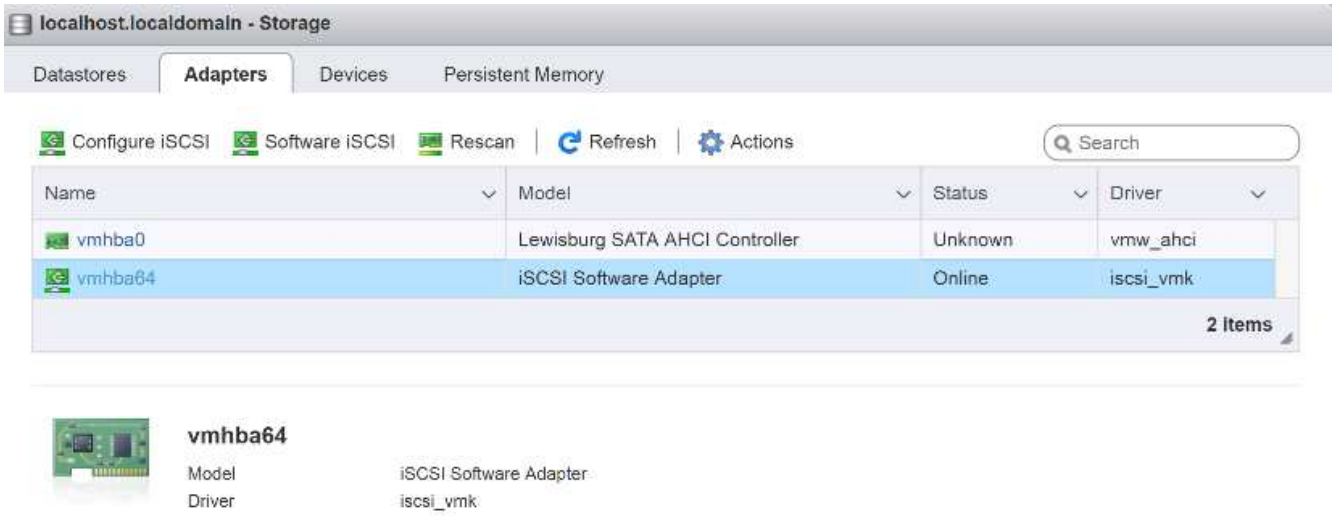
设置 **iSCSI** 多路径

ESXi 主机 VM-Host-Infra-01 和 VM-Host-Infra-02

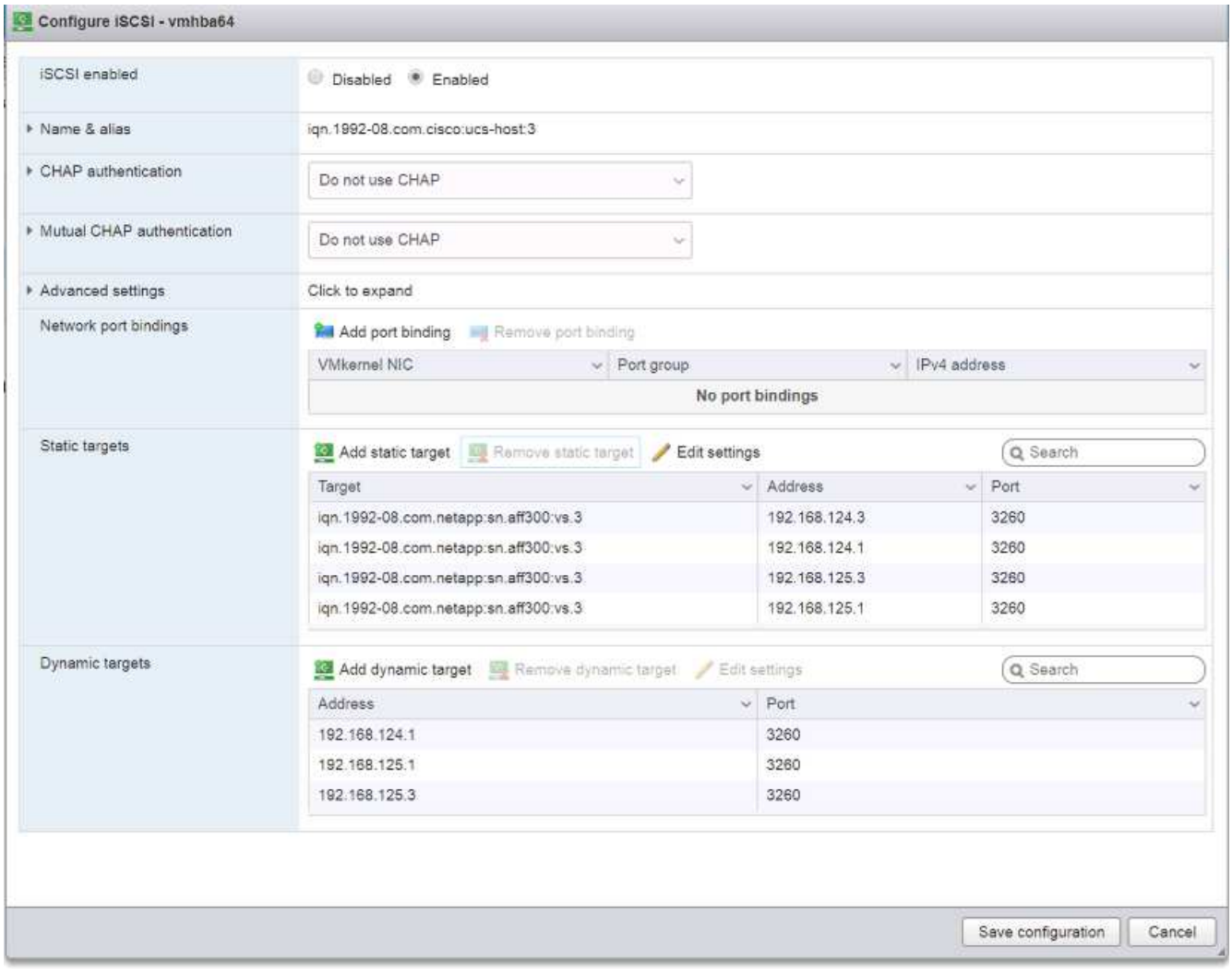
要在 ESXi 主机 VM-Host-Infra-01 和 VM-Host-Infra-02 上设置 iSCSI 多路径，请完成以下步骤：

1. 从每个主机客户端中，选择左侧的存储。
2. 在中间窗格中，单击适配器。

3. 选择 iSCSI 软件适配器，然后单击配置 iSCSI 。



4. 在动态目标下，单击添加动态目标。
5. 输入 IP 地址 `iscsi_lif01a` 。
6. 重复输入以下 IP 地址： `iscsi_lif01b` ， `iscsi_lif02a` 和 `iscsi_lif02b` 。
7. 单击保存配置。



要获取所有 `iscsi_lif` IP 地址，请登录到 NetApp 存储集群管理界面并运行 `network interface show` 命令。

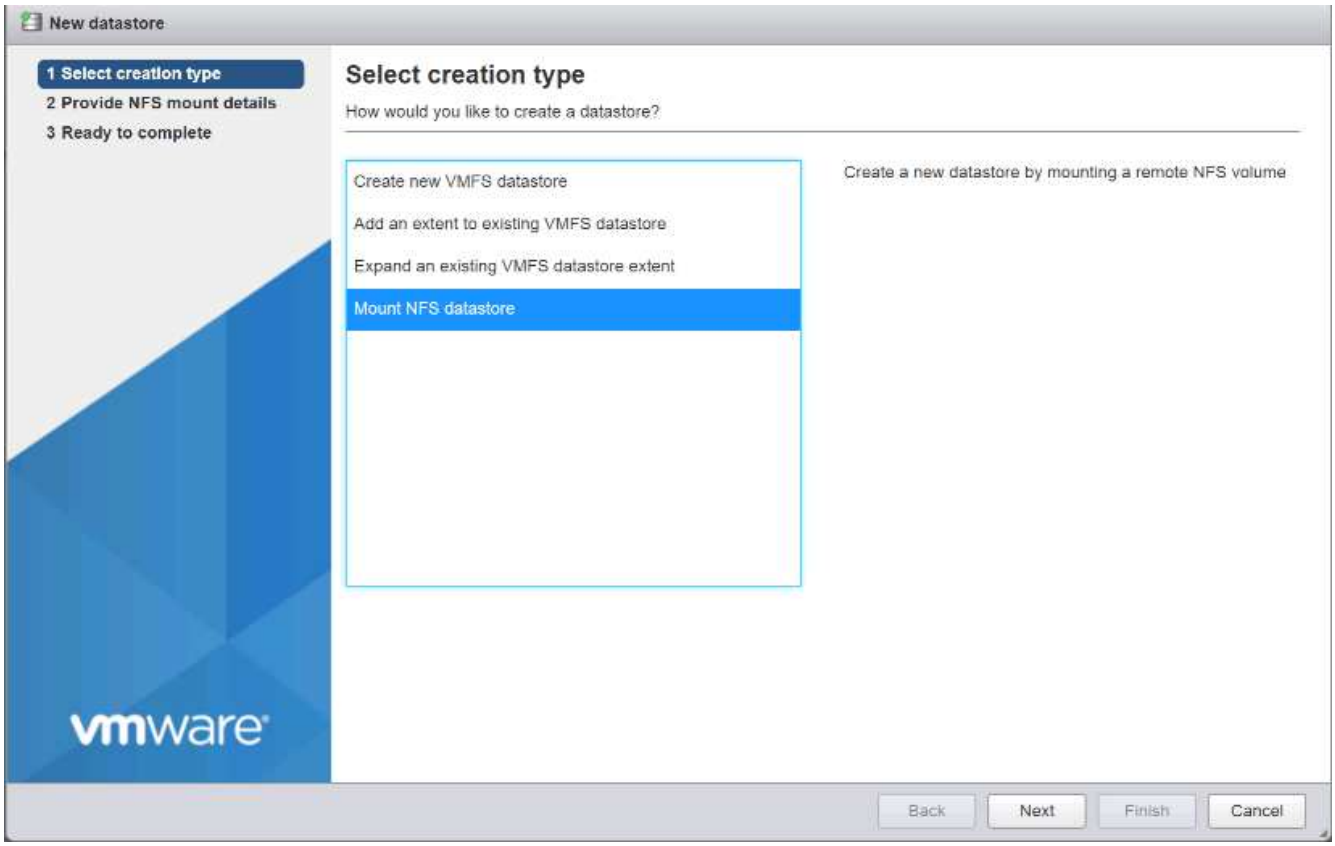
> 主机会自动重新扫描存储适配器，并且目标会添加到静态目标。

挂载所需的数据存储库

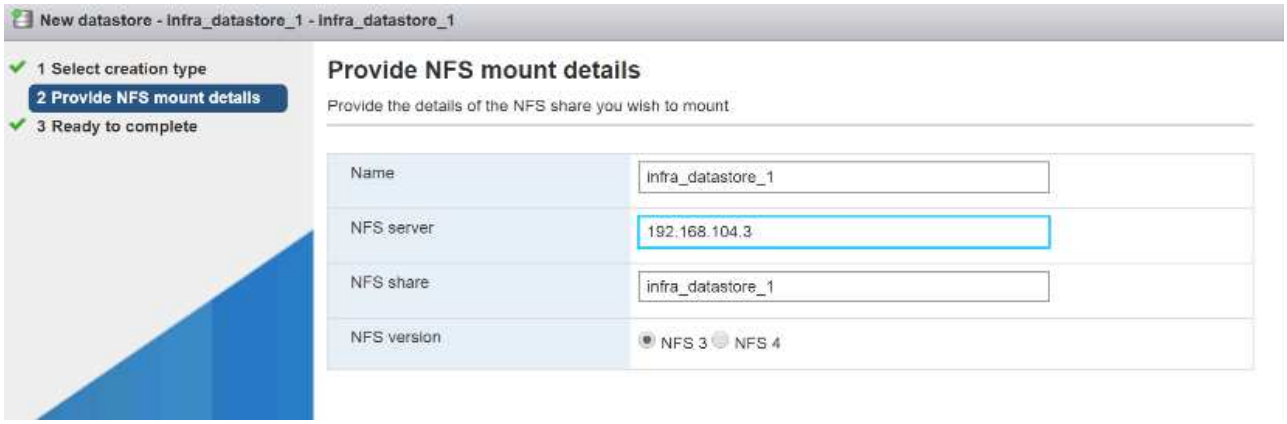
ESXi 主机 VM-Host-Infra-01 和 VM-Host-Infra-02

要挂载所需的数据存储库，请在每个 ESXi 主机上完成以下步骤：

1. 从 Host Client 中，选择左侧的 Storage 。
2. 在中间窗格中，选择数据存储库。
3. 在中间窗格中，选择新建数据存储库以添加新数据存储库。
4. 在新建数据存储库对话框中，选择挂载 NFS 数据存储库，然后单击下一步。



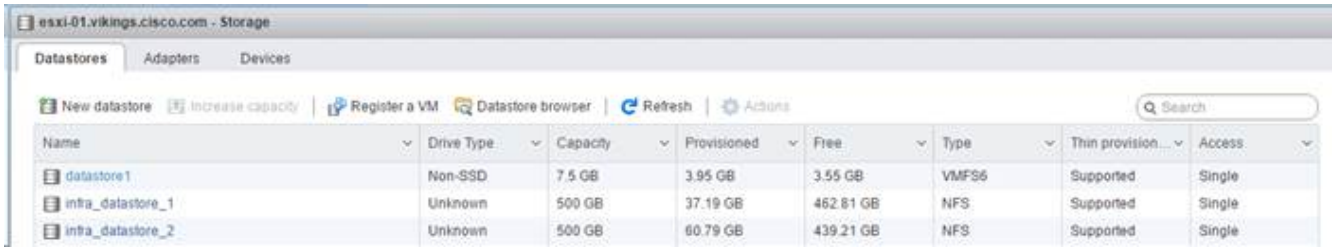
5. 在提供 NFS 挂载详细信息页面上，完成以下步骤：
   a. 输入 `infra_datastore_1` 作为数据存储库名称。
   b. 输入 NFS 服务器的 `nfs_lif01_a` LIF 的 IP 地址。
   c. 为 NFS 共享输入 ` /infra_datastore_1` 。
   d. 将 NFS 版本设置为 NFS 3 。
   e. 单击下一步。



6. 单击完成。此时，数据存储库应显示在数据存储库列表中。
7. 在中间窗格中，选择新建数据存储库以添加新数据存储库。
8. 在新建数据存储库对话框中，选择挂载 NFS 数据存储库，然后单击下一步。
9. 在提供 NFS 挂载详细信息页面上，完成以下步骤：

a. 输入 `infra_datastore_2` 作为数据存储库名称。
b. 输入 NFS 服务器的 `nfs_lif02_a` LIF 的 IP 地址。
c. 为 NFS 共享输入 ` /infra_datastore_2` 。
d. 将 NFS 版本设置为 NFS 3 。
e. 单击下一步。

10. 单击完成。此时，数据存储库应显示在数据存储库列表中。



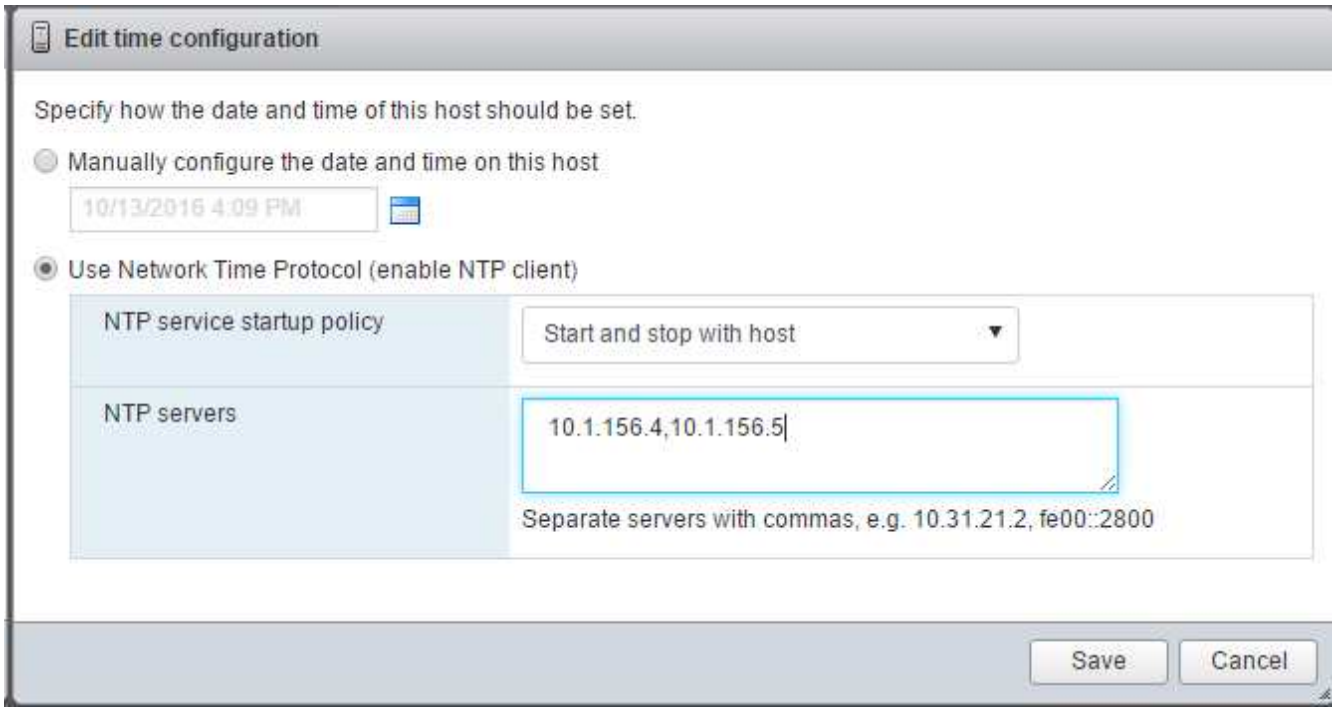
11. 在两台 ESXi 主机上挂载两个数据存储库。

在 **ESXi** 主机上配置 **NTP**

ESXi 主机 VM-Host-Infra-01 和 VM-Host-Infra-02

要在 ESXi 主机上配置 NTP ，请在每个主机上完成以下步骤：

1. 在 Host Client 中，选择左侧的 Manage 。
2. 在中间窗格中，选择时间和日期选项卡。
3. 单击编辑设置。
4. 确保已选择使用网络时间协议（启用 NTP 客户端）。
5. 使用下拉菜单选择 Start 和 Stop with Host 。
6. 在 NTP 服务器框中输入两个 Nexus 交换机 NTP 地址，并用逗号分隔。



7. 单击保存以保存配置更改。
8. 选择操作 > NTP 服务 > 启动。
9. 验证 NTP 服务现在是否正在运行，并且时钟现在设置为大致正确的时间

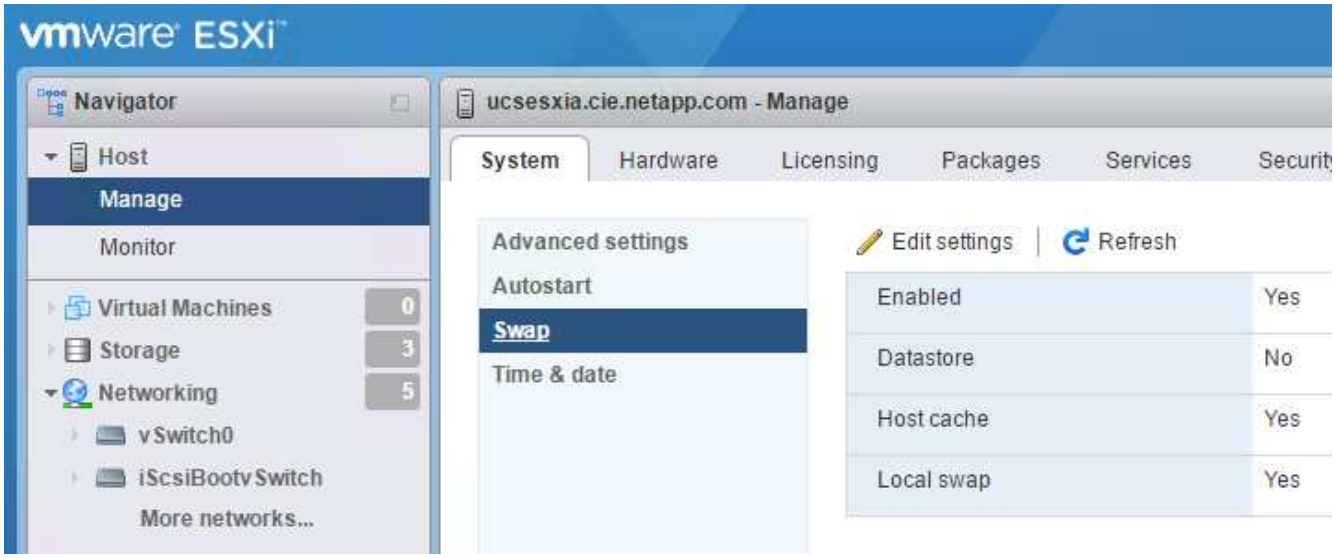
> NTP 服务器时间可能与主机时间略有不同。

配置 **ESXi** 主机交换

ESXi 主机 VM-Host-Infra-01 和 VM-Host-Infra-02

要在 ESXi 主机上配置主机交换，请在每个主机上执行以下步骤：

1. 单击左侧导航窗格中的管理。在右窗格中选择 System ，然后单击 Swap 。



2. 单击编辑设置。从数据存储库选项中选择 `infra_swap` 。

3. 单击保存。

安装适用于 **VMware VAAI** 的 **NetApp NFS** 插件 **1.1.2**

安装 NetApp NFS 插件 1.1.2 对于 VMware VAAI ，请完成以下步骤。

1. 下载适用于 VMware VAAI 的 NetApp NFS 插件：
   a. 转至 "NetApp 软件下载页面"。
   b. 向下滚动并单击适用于 VMware VAAI 的 NetApp NFS 插件。
   c. 选择 ESXi 平台。
   d. 下载最新插件的脱机软件包（ .zip ）或联机软件包（ .vib ）。
2. 适用于 VMware VAAI 的 NetApp NFS 插件正在等待通过 ONTAP 9.5 获得 IMT 认证，互操作性详细信息将很快发布到 NetApp IMT 中。
3. 使用 ESX 命令行界面在 ESXi 主机上安装此插件。
4. 重新启动 ESXi 主机。

安装 **VMware vCenter Server 6.7**

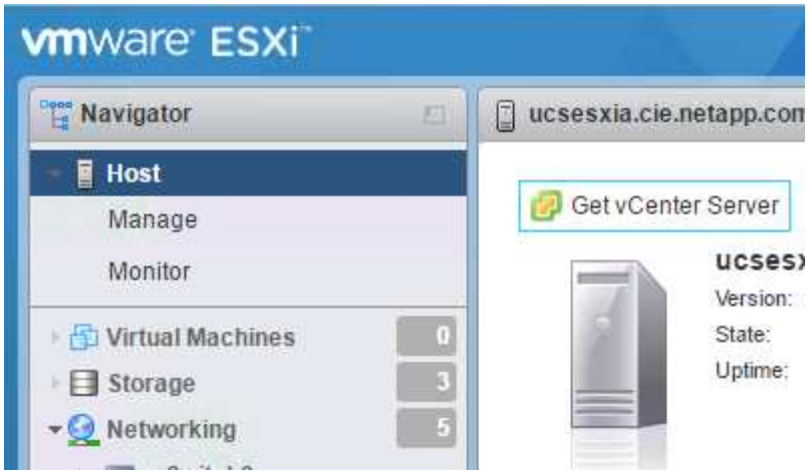
本节详细介绍了在 FlexPod 快速配置中安装 VMware vCenter Server 6.7 的过程。

> FlexPod Express 使用 VMware vCenter Server 设备（ VCSA ）。

安装 **VMware vCenter Server** 设备

要安装 VCSA ，请完成以下步骤：

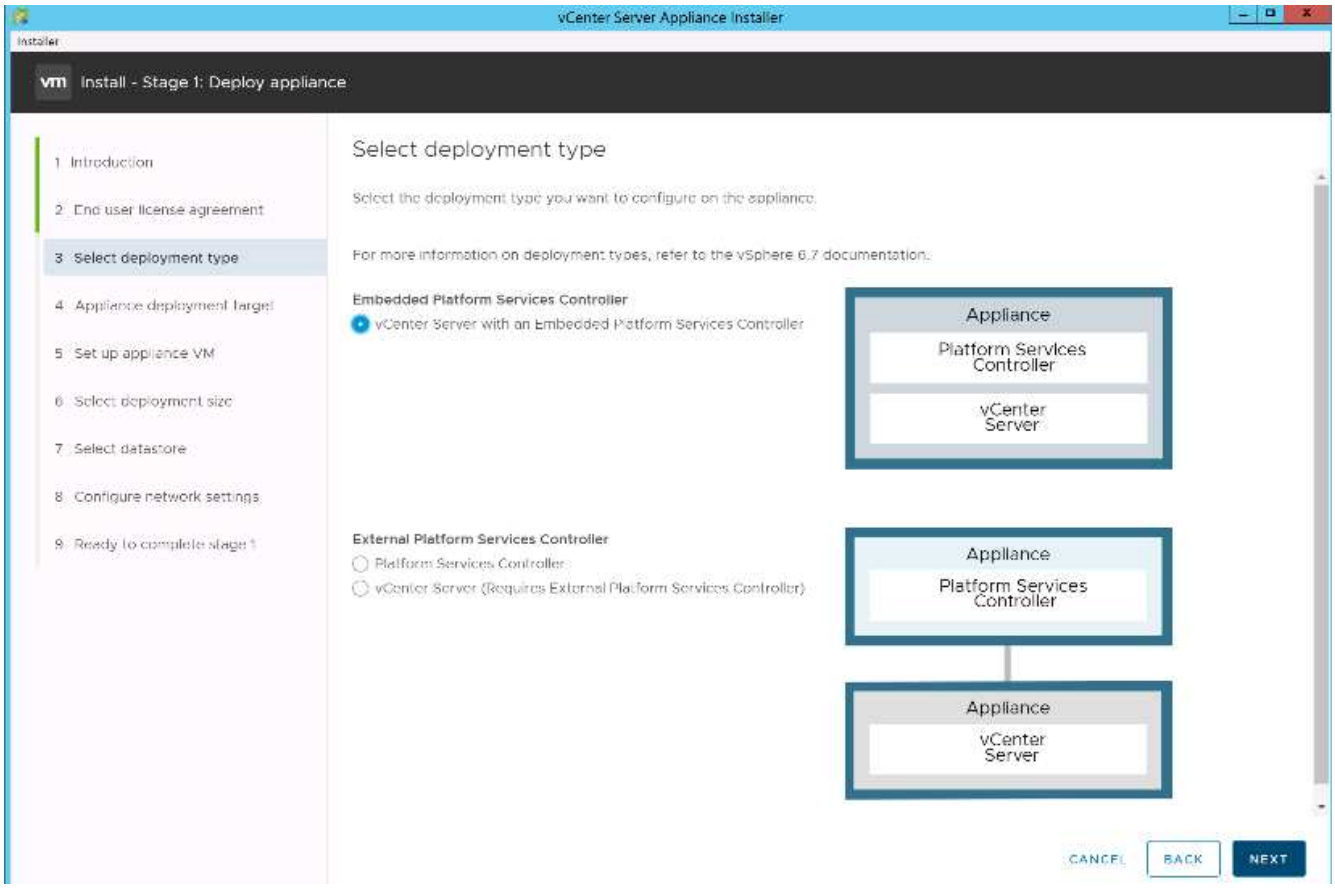
1. 下载 VCSA 。在管理 ESXi 主机时，单击获取 vCenter Server 图标以访问下载链接。



2. 从 VMware 站点下载 VCSA 。

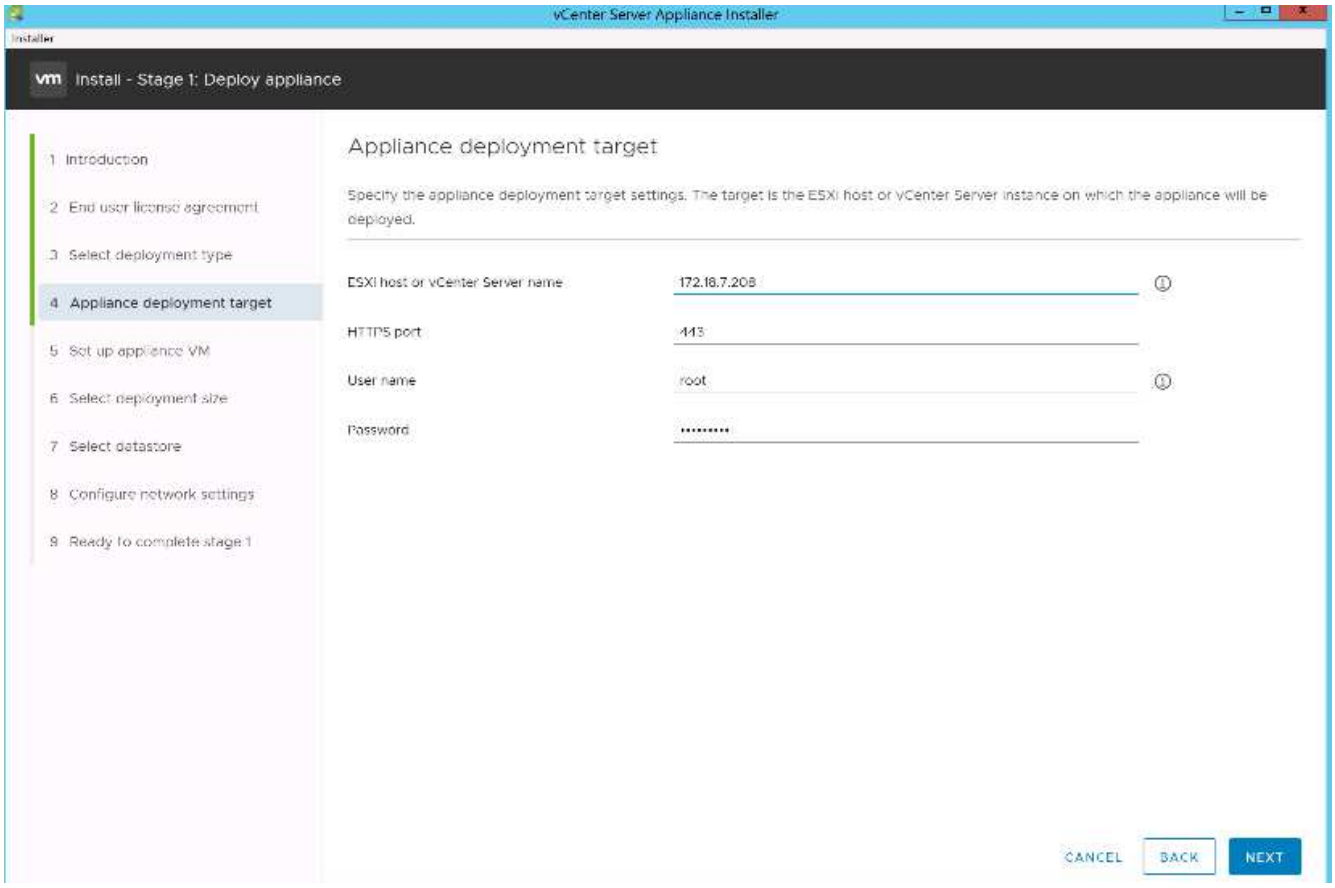
> 虽然支持安装 Microsoft Windows vCenter Server ，但 VMware 建议在新部署中使用 VCSA 。

3. 挂载 ISO 映像。
4. 导航到 `vcsa-ui-installer` > `win32` 目录。双击 `installer.exe` 。
5. 单击安装。
6. 单击简介页面上的下一步。
7. 接受 EULA 。
8. 选择 Embedded Platform Services Controller 作为部署类型。

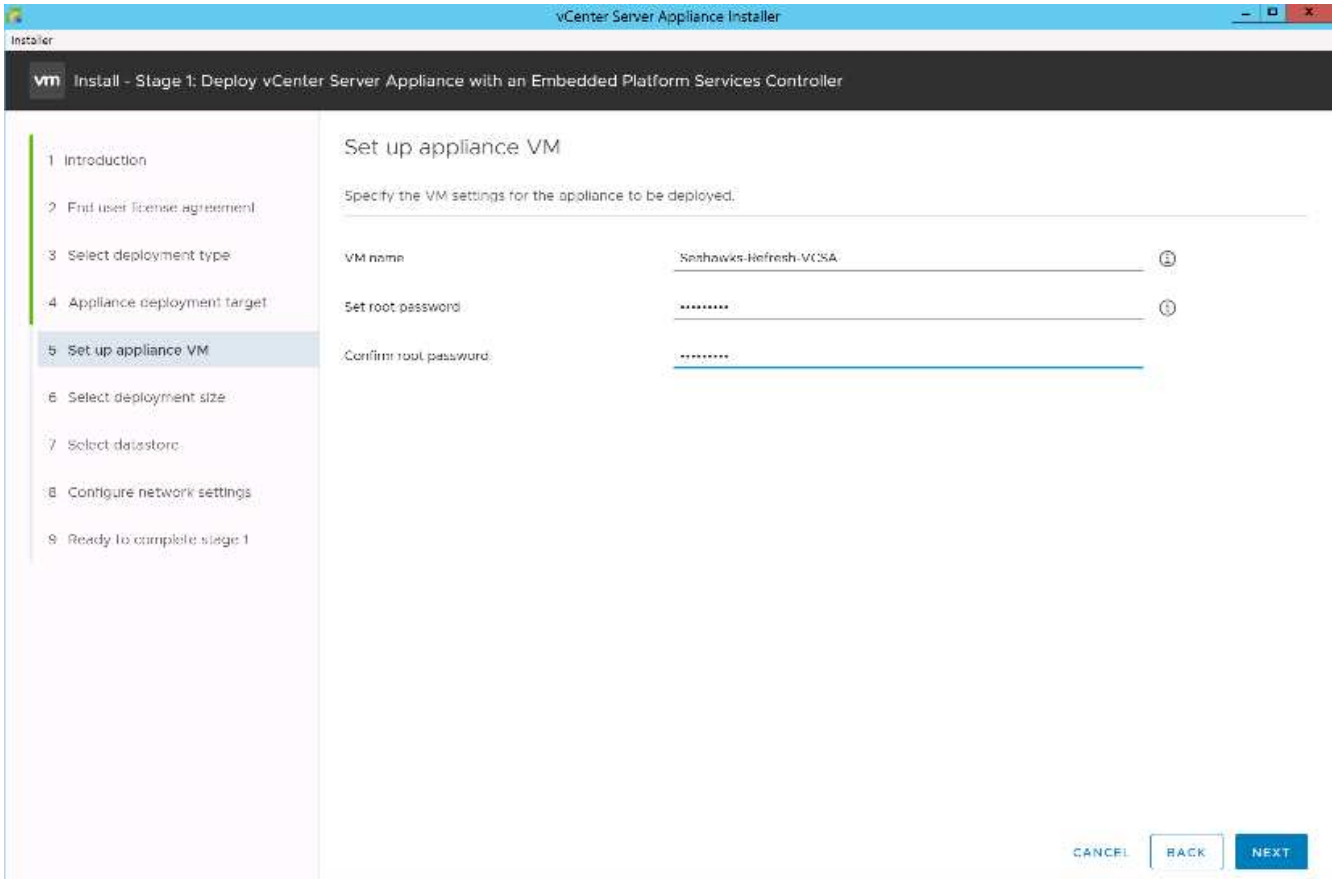


如果需要，还支持在 FlexPod Express 解决方案中部署外部平台服务控制器。

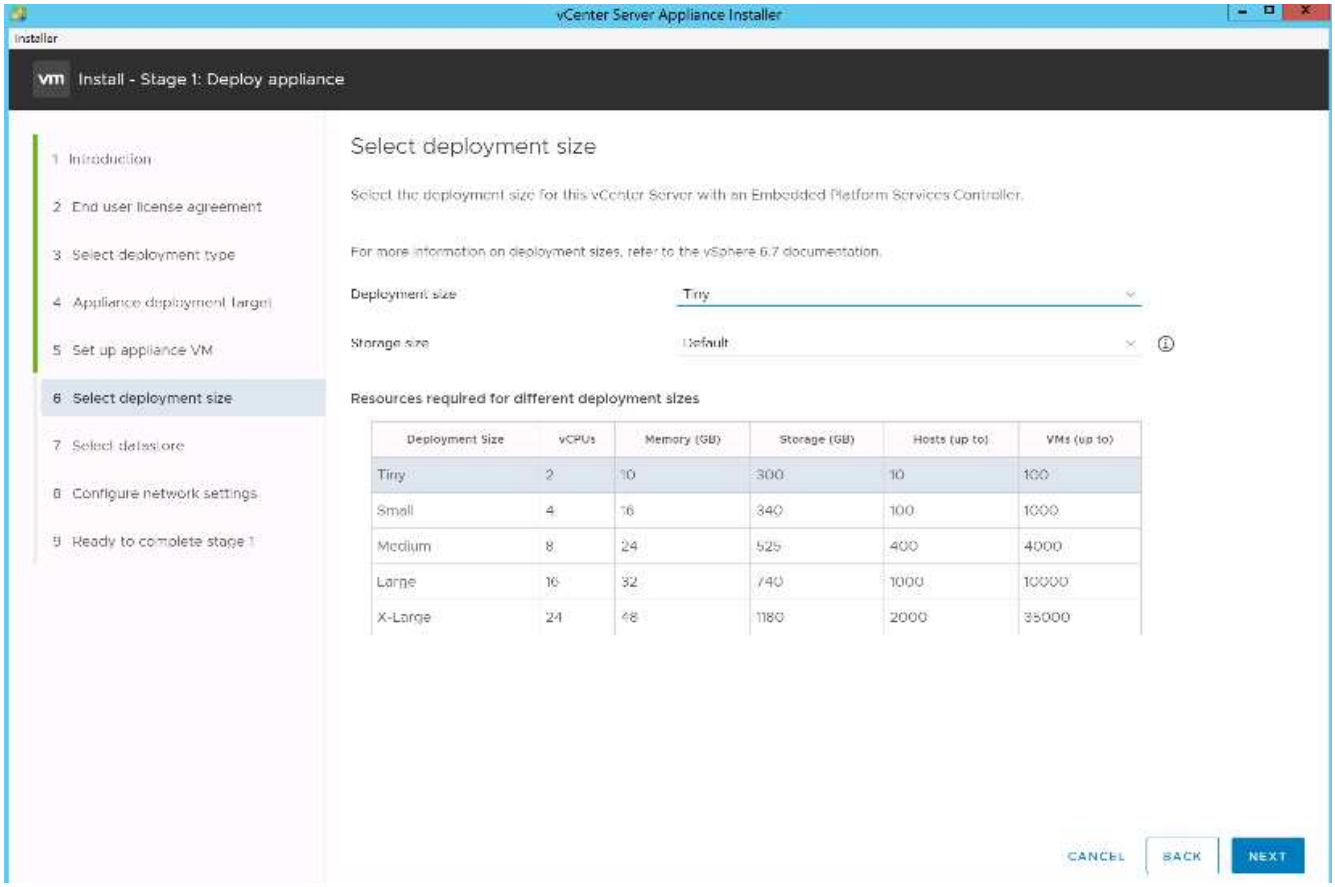
9. 在设备部署目标页面上，输入已部署的 ESXi 主机的 IP 地址， root 用户名和 root 密码。单击下一步。



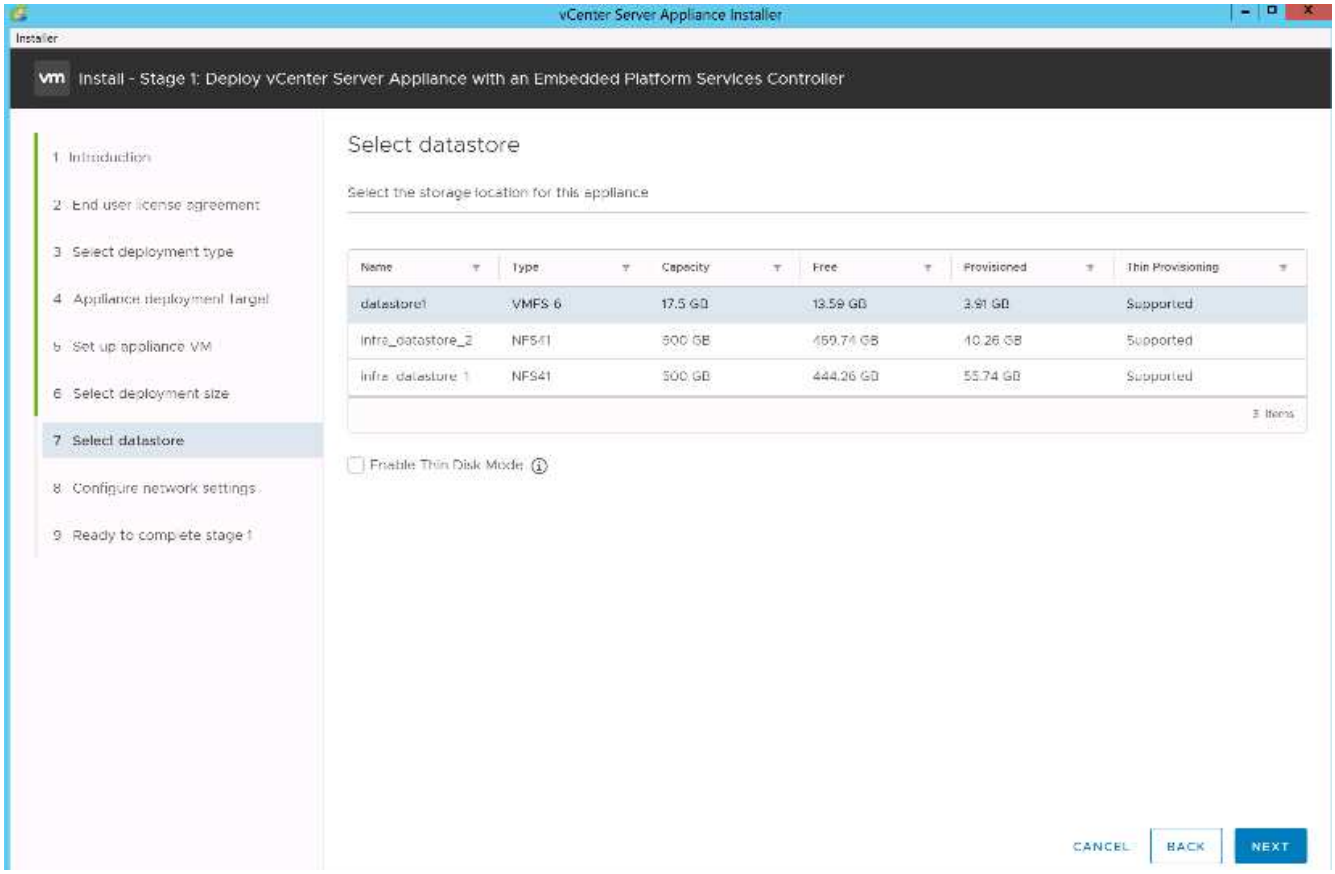
10. 输入 vCSA 作为 VM 名称以及要用于 VCSA 的根密码，以设置设备 VM 。单击下一步。



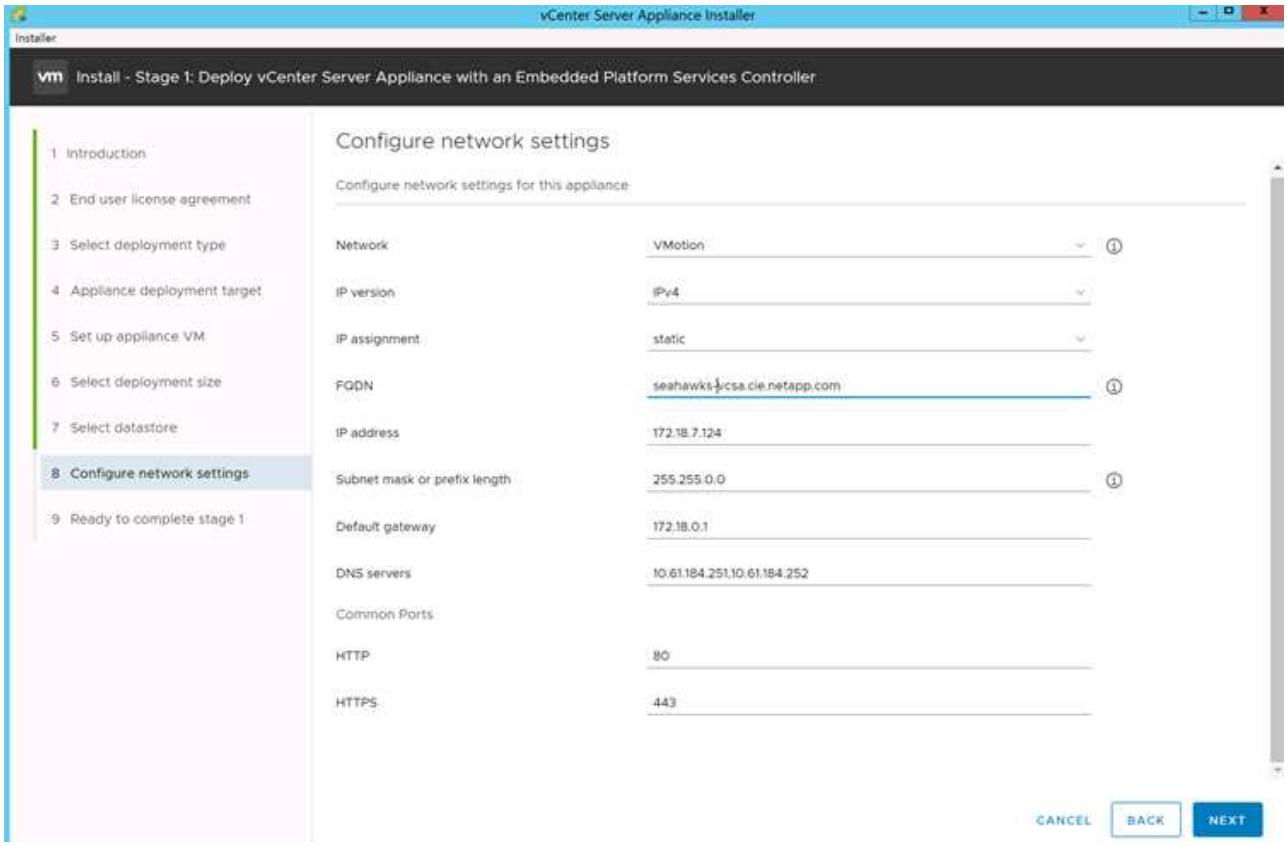
11. 选择最适合您环境的部署规模。单击下一步。



12. 选择 `infra_datastore_1` 数据存储库。单击下一步。



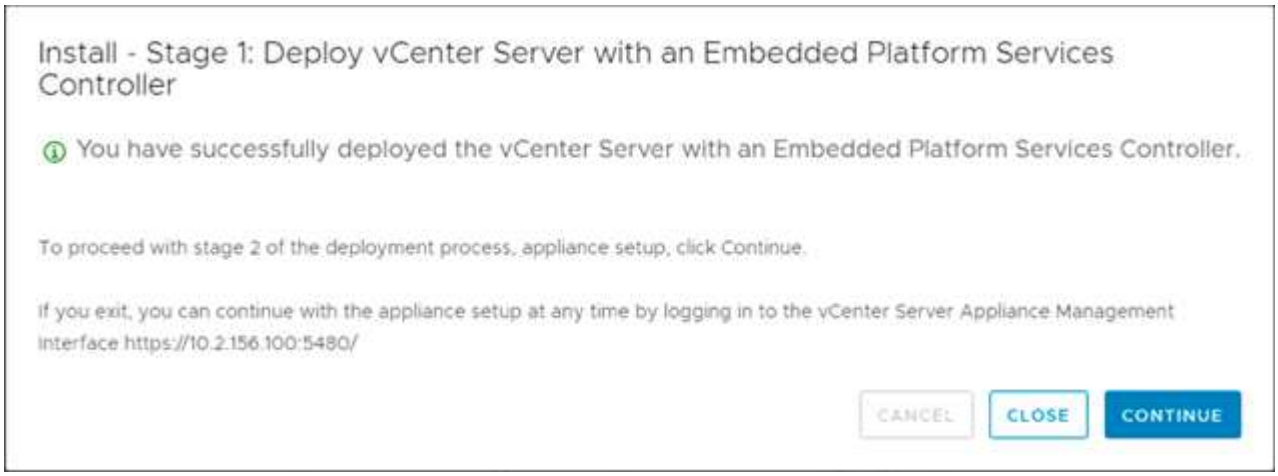
13. 在配置网络设置页面上输入以下信息，然后单击下一步。
    a. 选择 MGMT-Network 作为您的网络。
    b. 输入要用于 VCSA 的 FQDN 或 IP 。
    c. 输入要使用的 IP 地址。
    d. 输入要使用的子网掩码。
    e. 输入默认网关。
    f. 输入 DNS 服务器。



14. 在准备完成阶段 1 页面上，验证您输入的设置是否正确。单击完成。

    此时将安装 VCSA 。此过程需要几分钟时间。

15. 阶段 1 完成后，将显示一条消息，指出已完成。单击 Continue 以开始第 2 阶段配置。



16. 在第 2 阶段简介页面上，单击下一步。
17. 输入 ` <<var_ntp_id>>` 作为 NTP 服务器地址。您可以输入多个 NTP IP 地址。

    如果您计划使用 vCenter Server 高可用性，请确保已启用 SSH 访问。

18. 配置 SSO 域名，密码和站点名称。单击下一步。

请记下这些值以供参考，特别是当您与 `vsphere.local` 域名有所偏差时。

19. 如果需要，请加入 VMware 客户体验计划。单击下一步。
20. 查看设置摘要。单击完成或使用返回按钮编辑设置。
21. 此时将显示一条消息，指出在安装开始后，您无法暂停或停止安装完成。单击确定继续。

    设备设置将继续。这需要几分钟时间。

    此时将显示一条消息，指示设置已成功。

    > 安装程序提供的用于访问 vCenter Server 的链接可单击。

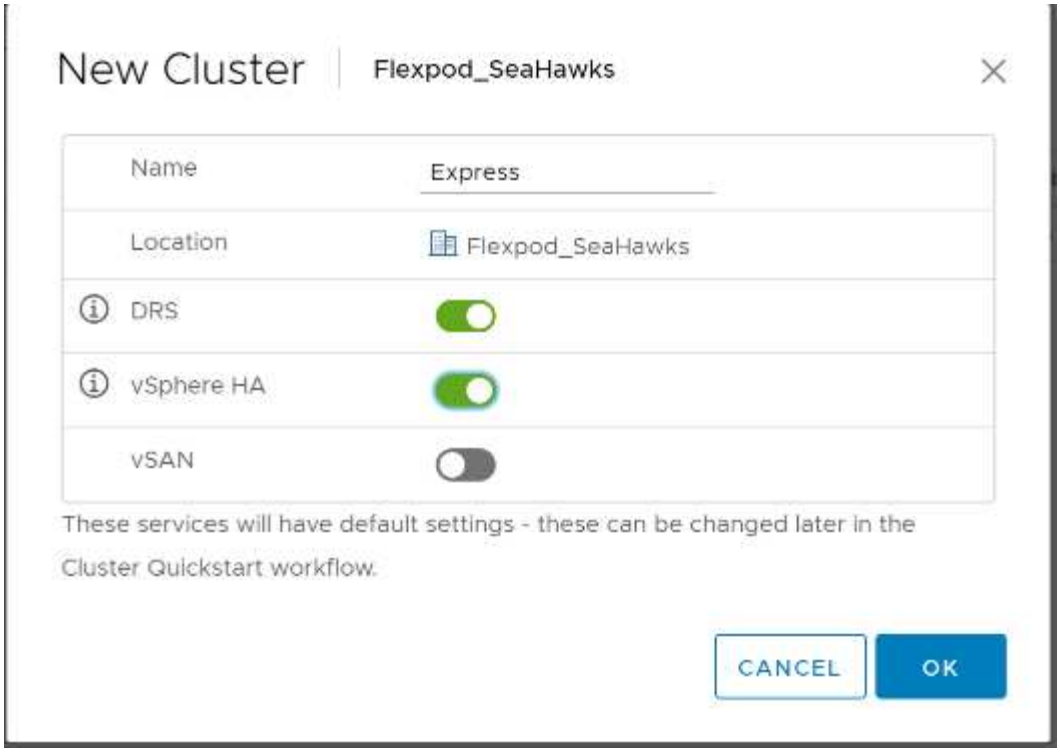
配置 **VMware vCenter Server 6.7** 和 **vSphere** 集群

要配置 VMware vCenter Server 6.7 和 vSphere 集群，请完成以下步骤：

1. 导航到 https://\<<FQDN 或 vCenter 的 IP >/vsphere-client/ 。
2. 单击 Launch vSphere Client 。
3. 使用用户名 administrator@vsphere.local 和您在 VCSA 设置过程中输入的 SSO 密码登录。
4. 右键单击 vCenter 名称并选择新建数据中心。
5. 输入数据中心的名称，然后单击确定。
    - 创建 vSphere 集群。 *

要创建 vSphere 集群，请完成以下步骤：

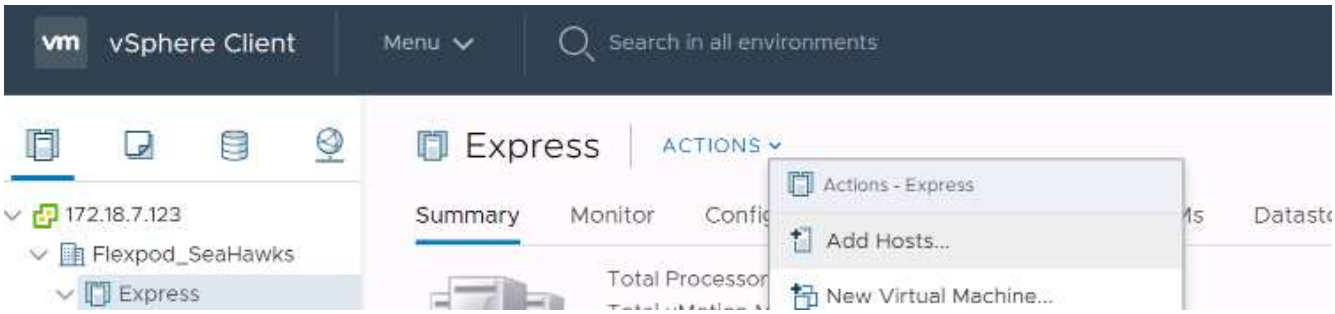
1. 右键单击新创建的数据中心，然后选择 New Cluster 。
2. 输入集群的名称。
3. 选择并启用 DRS 和 vSphere HA 选项。
4. 单击确定。



- 将 ESXi 主机添加到集群 *

要将 ESXi 主机添加到集群，请完成以下步骤：

1. 在集群的操作菜单中选择添加主机。



2. 要将 ESXi 主机添加到集群，请完成以下步骤：
   a. 输入主机的 IP 或 FQDN 。单击下一步。
   b. 输入 root 用户名和密码。单击下一步。
   c. 单击是将主机的证书替换为由 VMware 证书服务器签名的证书。
   d. 单击主机摘要页面上的下一步。
   e. 单击绿色 + 图标向 vSphere 主机添加许可证。

      ⓘ 如果需要，可以稍后完成此步骤。

   f. 单击下一步以使锁定模式保持禁用状态。
   g. 单击 VM 位置页面上的下一步。

h. 查看即将完成页面。使用 " 返回 " 按钮进行任何更改或选择 " 完成 " 。

3. 对 Cisco UCS 主机 B 重复步骤 1 和 2

   对于添加到 FlexPod 快速配置中的任何其他主机，必须完成此过程。

在 **ESXi** 主机上配置核心转储

为 iSCSI 启动的主机设置 ESXi 转储收集器

需要配置使用 VMware iSCSI 软件启动程序通过 iSCSI 启动的 ESXi 主机，以便对 vCenter 中的 ESXi 转储收集器执行核心转储。默认情况下， vCenter 设备不会启用转储收集器。此操作步骤应在 vCenter 部署部分结束时运行。要设置 ESXi 转储收集器，请执行以下步骤：

1. 以 mailto： administrator@vsphere.local[administrator@vsphere.local^] 的身份登录到 vSphere Web Client ，然后选择主页。
2. 在中间窗格中，单击系统配置。
3. 在左窗格中，选择服务。
4. 在服务下，单击 VMware vSphere ESXi 转储收集器。
5. 在中间窗格中，单击绿色的开始图标以启动服务。
6. 在操作菜单中，单击编辑启动类型。
7. 选择自动。
8. 单击确定。
9. 使用 ssh 作为 root 连接到每个 ESXi 主机。
10. 运行以下命令：

```
esxcli system coredump network set -v vmk0 -j <vcenter-ip>
esxcli system coredump network set -e true
esxcli system coredump network check
```

    运行最后一个命令后，将显示消息 `Verified the configured netdump server is running` 。

    对于添加到 FlexPod Express 中的任何其他主机，必须完成此过程。

结论

FlexPod Express 通过提供经过验证的设计，使用行业领先的组件，提供了一个简单而有效的解决方案。通过添加其他组件进行扩展， FlexPod Express 可以根据特定业务需求进行定制。FlexPod Express 在设计时考虑到了中小型企业， ROBO 以及其他需要专用解决方案的企业。

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：

- NVA-1130-design ：采用 VMware vSphere 6.7U1 的 FlexPod Express 和采用基于 IP 的直连存储 NVA 设计的 NetApp AFF A220

  "https://www.netapp.com/us/media/nva-1130-design.pdf"

- AFF 和 FAS 系统文档中心

  "http://docs.netapp.com/platstor/index.jsp"

- ONTAP 9 文档中心

  "http://docs.netapp.com/ontap-9/index.jsp"

- NetApp 产品文档

  "https://docs.netapp.com"

适用于采用Cisco UCS Mini和NetApp AFF/FAS的VMware vSphere 7.0的FlexPod Express—NVA—部署

NetApp 公司 Jyh-shing Chen

采用Cisco UCS Mini和NetApp AFF/FAS解决方案 的适用于VMware vSphere 7.0的FlexPod Express利用具有B200 M5刀片式服务器的Cisco UCS Mini、Cisco UCS 6324机箱内置互联阵列、Cisco Nexus 31108PC-V交换机或其他兼容交换机以及NetApp AFF A220、C190或FAS2700系列控制器HA对、 运行NetApp ONTAP 9.7数据管理软件。本NetApp经验证的架构(NVA)部署文档详细介绍了配置基础架构组件、部署VMware vSphere 7.0以及相关工具以创建基于FlexPod Express的高可靠性和高可用性虚拟基础架构所需的步骤。

"适用于采用Cisco UCS Mini和NetApp AFF/FAS的VMware vSphere 7.0的FlexPod Express—NVA—部署"

FlexPod 和安全性

FlexPod ，《勒索软件解决方案》

TR-4802： FlexPod ，《勒索软件解决方案》

NetApp 公司 Arvind Ramakrishnan

与以下合作伙伴：

要了解勒索软件，必须首先了解有关加密的几个要点。加密方法可以使用共享密钥（对称密钥加密）或一对密钥（非对称密钥加密）对数据进行加密。其中一个密钥是广泛可用的公有密钥，另一个密钥是未公开的私钥。

勒索软件是一种基于密码学的恶意软件，即使用加密技术构建恶意软件。此恶意软件可以使用对称密钥加密和非对称密钥加密来锁定受影响的数据，并要求勒索以提供密钥来对受影响的数据进行解密。

勒索软件的工作原理是什么？

以下步骤介绍勒索软件如何使用加密技术对受害者的数据进行加密，而不会为受害者提供任何解密或恢复范围：

1. 与非对称密钥加密一样，攻击者会生成密钥对。生成的公有密钥将放置在该恶意软件中，然后释放该恶意软件。
2. 恶意软件进入受影响用户的计算机或系统后，它会使用伪数字生成器（ Pseudorandom Number Generator ， PRG ）或任何其他可行的随机数字生成算法生成一个随机对称密钥。
3. 恶意软件使用此对称密钥对受影响的数据进行加密。它最终会使用恶意软件中嵌入的攻击者的公有密钥对对称密钥进行加密。此步骤的输出是加密对称密钥的非对称密文和受影响数据的对称密文。
4. 恶意软件会将受害者的数据以及用于加密数据的对称密钥置零（擦除），从而无法进行恢复。
5. 现在，系统会向受影响的用户显示对称密钥的非对称密钥文本以及为获取用于加密数据的对称密钥而必须支付的勒索金额。
6. 受害者支付勒索费用，并与攻击者共享非对称密码短文。攻击者使用其私钥对密码短文进行解密，从而导致出现对称密钥。
7. 攻击者与受影响的用户共享此对称密钥，此密钥可用于对所有数据进行解密，从而从攻击中恢复。

挑战

个人和组织在遭受勒索软件攻击时面临以下挑战：

- 最重要的挑战是， IT 会立即影响组织或个人的工作效率。恢复正常状态需要一些时间，因为所有重要文件都必须重新获取，并且系统必须安全。
- 它可能会导致数据泄露，其中包含属于客户或客户的敏感机密信息，并导致组织显然希望避免的危机情况。
- 数据很有可能落入不当之手或被彻底擦除，从而导致无法返回，可能对组织和个人造成灾难性后果。

- 支付完勒索后，无法保证攻击者将提供密钥来还原数据。
- 目前无法保证攻击者在支付了勒索之后仍不会广播敏感数据。
- 在大型企业中，识别导致勒索软件攻击的漏洞是一项繁琐的任务，确保所有系统的安全需要付出大量的努力。

谁面临风险?

任何人都可能受到勒索软件的攻击，包括个人和大型组织。如果组织未实施定义明确的安全措施和实践，则更容易受到此类攻击。攻击对大型组织的影响可能比个人承受的影响要大几倍。

勒索软件大约占所有恶意软件攻击的 28% 。换言之，每四个恶意软件事件中就有一个以上是勒索软件攻击。勒索软件可以自动和不分青红皂白地通过互联网传播，一旦发生安全问题，它就可以进入受影响的系统并继续传播到其他已连接的系统。攻击者往往会将目标锁定在执行大量文件共享，拥有大量敏感和关键数据或未充分防范攻击的人员或组织。

攻击者往往关注以下潜在目标：

- 大学和学生社区
- 政府部门和机构
- 医院
- 银行

这并不是详尽的目标列表。如果您不属于这些类别之一，则您将无法认为自己不会受到攻击。

勒索软件如何进入系统或传播?

勒索软件可以通过多种方式进入系统或传播到其他系统。在当今世界，几乎所有系统都通过互联网， LAN ， WAN 等相互连接。在这些系统之间生成和交换的数据量只会增加。

勒索软件的一些最常见传播方式包括我们每天用于共享或访问数据的方法：

- email
- P2P 网络
- 文件下载
- 社交网络
- 移动设备
- 连接到不安全的公有网络
- 访问 Web URL

数据丢失的后果

数据丢失的后果或影响可能会比企业预期的范围更广。根据停机持续时间或组织无法访问其数据的时间段，这些影响可能会有所不同。攻击持续时间越长，对组织收入，品牌和声誉的影响就越大。企业还可能面临法律问题和生产率急剧下降。

随着这些问题持续存在，它们开始放大，并可能最终改变组织的文化，具体取决于组织如何应对攻击。在当今世界，信息迅速传播，有关组织的负面新闻可能会对其声誉造成发生原因永久损害。企业可能会因数据丢失而面临

巨大的处罚，最终可能导致业务关闭。

财务影响

据最近的一份报告称 "McAfee 报告"网络犯罪造成的全球成本约为 6000 亿美元，约占全球 GDP 的 0.8% 。与全球互联网经济增长 4.2 万亿美元相比，这一金额相当于对增长征收 14% 的税。

勒索软件在这一财务成本中占很大比例。2018 年，勒索软件攻击所产生的成本约为 80 亿美元—预计 2019 年将达到 115 亿美元。

什么是解决方案?

只有通过实施主动式灾难恢复计划，才能在最短停机时间内从勒索软件攻击中恢复。拥有从攻击中恢复的能力是不错的，但完全防止攻击是理想之选。

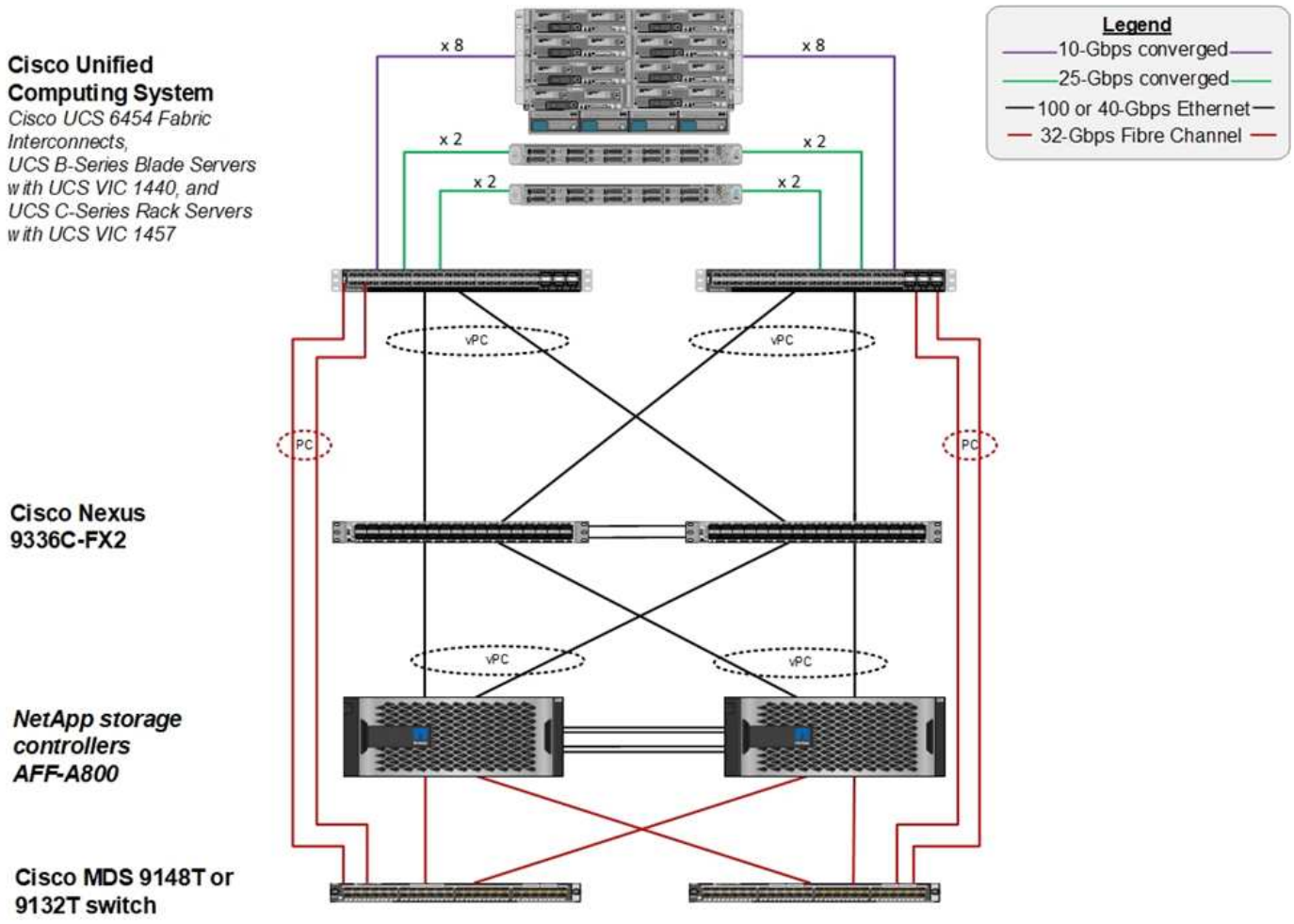
尽管为了防止攻击，您必须查看和修复几个方面，但允许您防止或从攻击中恢复的核心组件是数据中心。

数据中心的设计及其为保护网络，计算和存储端点提供的功能对于构建安全的日常运营环境起着至关重要的作用。本文档介绍了 FlexPod 混合云基础架构的功能如何帮助在发生攻击时快速恢复数据，以及如何帮助全面防止攻击。

FlexPod 概述

FlexPod 是一种经过预先设计，集成和验证的架构，可将 Cisco 统一计算系统（ Cisco UCS ）服务器， Cisco Nexus 系列交换机， Cisco MDS 光纤交换机和 NetApp 存储阵列组合到一个灵活的架构中。FlexPod 解决方案旨在实现高可用性，不会出现单点故障，同时保持成本效益和设计灵活性，以支持各种工作负载。FlexPod 设计可以支持不同的虚拟机管理程序和裸机服务器，也可以根据客户工作负载要求进行规模估算和优化。

下图展示了 FlexPod 架构，并清楚地突出了堆栈所有层的高可用性。存储，网络和计算等基础架构组件的配置方式使操作可以在其中一个组件发生故障时瞬时故障转移到正常运行的配对节点。



FlexPod 系统的一个主要优势是，它经过预先设计，集成和验证，可用于多个工作负载。每项解决方案验证都会发布详细的设计和部署指南。这些文档介绍了工作负载要在 FlexPod 上无缝运行所必须采用的最佳实践。这些解决方案采用同类最佳的计算，网络和存储产品以及一系列侧重于整个基础架构安全性和强化的功能。

"IBM 的 X-Force 威胁情报索引" 声明： " 由于人类错误，三分之二的记录受到破坏，包括配置不当的云基础架构在历史上的 424%" 。

借助 FlexPod 系统，您可以通过 Ansible 攻略手册使用自动化来避免配置不当基础架构，这些攻略手册会根据 Cisco 验证设计（ CVD ）和 NetApp 验证架构（ NVA ）中介绍的最佳实践对基础架构执行端到端设置。

勒索软件保护措施

本节介绍 NetApp ONTAP 数据管理软件以及适用于 Cisco UCS 和 Cisco Nexus 的工具的主要功能，您可以使用这些功能有效地保护和抵御勒索软件攻击。

存储： **NetApp ONTAP**

ONTAP 软件提供了许多对数据保护有用的功能，其中大多数功能对于拥有 ONTAP 系统的客户是免费的。您可以随时使用以下功能来保护数据免受攻击：

- * NetApp Snapshot 技术。 * Snapshot 副本是卷的只读映像，用于捕获文件系统在某一时间点的状态。这些副本有助于保护数据，而不会影响系统性能，同时也不会占用大量存储空间。NetApp 建议您创建 Snapshot 副本创建计划。您还应保持较长的保留时间，因为某些恶意软件可能会休眠，然后在感染后数周或数月重新

激活。发生攻击时，可以使用感染前创建的 Snapshot 副本回滚卷。

- * NetApp SnapRestore 技术。 * SnapRestore 数据恢复软件对于从数据损坏中恢复或仅还原文件内容非常有用。SnapRestore 不会还原卷的属性；它比管理员通过将文件从 Snapshot 副本复制到活动文件系统来实现的速度快得多。如果必须尽快恢复多个文件，则恢复数据的速度会很有用。在发生攻击时，这种高效的恢复过程有助于快速恢复业务联机。
- * NetApp SnapCenter 技术。 * SnapCenter 软件使用基于 NetApp 存储的备份和复制功能来提供应用程序一致的数据保护。该软件可与企业级应用程序集成，并提供特定于应用程序和数据库的工作流，以满足应用程序，数据库和虚拟基础架构管理员的需求。SnapCenter 提供了一个易于使用的企业平台，用于在应用程序，数据库和文件系统之间安全地协调和管理数据保护。它能够提供应用程序一致的数据保护，这在数据恢复期间至关重要，因为它可以轻松地将应用程序更快地还原到一致的状态。
- * NetApp SnapLock 技术。 * SnapLock 提供了一个特殊用途卷，可在其中存储文件并将其提交到不可擦除，不可重写的状态。驻留在 FlexVol 卷中的用户生产数据可以分别通过 NetApp SnapMirror 或 SnapVault 技术镜像或存储到 SnapLock 卷。在保留期限结束之前，无法删除 SnapLock 卷，卷本身及其托管聚合中的文件。
- * NetApp FPolicy 技术。 * 使用 FPolicy 软件禁止对具有特定扩展名的文件执行操作，以防止受到攻击。可以为特定文件操作触发 FPolicy 事件。此事件与策略相关联，策略将调用需要使用的引擎。您可以为策略配置一组可能包含勒索软件的文件扩展名。如果具有不允许扩展名的文件尝试执行未经授权的操作，则 FPolicy 会阻止执行该操作。

网络： **Cisco Nexus**

Cisco NX OS 软件支持可增强网络异常检测和安全性的网络流功能。网络流可捕获网络上每个对话的元数据，通信所涉及的各方，正在使用的协议以及事务持续时间。对信息进行汇总和分析后，可以深入了解正常行为。

通过收集的数据，还可以确定可疑的活动模式，例如恶意软件在网络中传播，否则可能会被忽视。

网络流使用流为网络监控提供统计信息。流量是指到达源接口（或 VLAN ）且密钥值相同的单向数据包流。密钥是指数据包中某个字段的标识值。您可以使用流记录创建流，以便为流定义唯一密钥。您可以使用流量导出器将网络流为流收集的数据导出到远程网络流收集器，例如 Cisco Stealthwatch 。Stealthwatch 使用此信息持续监控网络，并在发生勒索软件爆发时提供实时威胁检测和意外事件响应取证。

计算： **Cisco UCS**

Cisco UCS 是 FlexPod 架构中的计算端点。您可以使用多种 Cisco 产品来帮助在操作系统级别保护堆栈的这一层。

您可以在计算或应用程序层实施以下关键产品：

- * 适用于端点的 Cisco 高级恶意软件保护（ AMP ）。 * 此解决方案在 Microsoft Windows 和 Linux 操作系统上受支持，集成了预防，检测和响应功能。此安全软件可防止违规行为，在入口点阻止恶意软件，并持续监控和分析文件和流程活动，以快速检测，控制和修复可能规避前线防护的威胁。

  AMP 的恶意活动保护（ MAP ）组件持续监控所有端点活动，并提供运行时检测和阻止端点上正在运行的程序的异常行为。例如，如果端点行为表明存在勒索软件，则会终止违规流程，从而阻止端点加密并阻止攻击。

- * 通过 Cisco 高级恶意软件保护实现电子邮件安全。 * 电子邮件已成为传播恶意软件和实施网络攻击的主要工具。平均而言，一天内会交换大约 1000 亿封电子邮件，这为攻击者提供了一个极好的渗透载体，可以渗透到用户的系统中。因此，抵御这种攻击是绝对必要的。

  AMP 可分析电子邮件中隐藏在恶意附件中的威胁，例如零日攻击和窃取恶意软件。此外，它还利用行业领先的 URL 智能来打击恶意链路。它可以为用户提供高级保护，防止他们遭受鱼叉式网络攻击，勒索软件和

其他复杂攻击。

- * 下一代入侵防护系统（NGIP）。 * Cisco Firepower NGIP 可以部署为数据中心中的物理设备，也可以部署为 VMware 上的虚拟设备（NGIPSv for VMware）。这种高效的入侵防护系统可提供可靠的性能和较低的总拥有成本。威胁保护可以通过可选的订阅许可证进行扩展，以提供 AMP ，应用程序可见性和控制以及 URL 筛选功能。虚拟化的 NGIP 可检查虚拟机（VM）之间的流量，并在资源有限的站点上更轻松地部署和管理 NGIP 解决方案，从而增强对物理和虚拟资产的保护。

保护和恢复 **FlexPod** 上的数据

本节介绍在发生攻击时如何恢复最终用户的数据，以及如何使用 FlexPod 系统防止攻击。

测试台概述

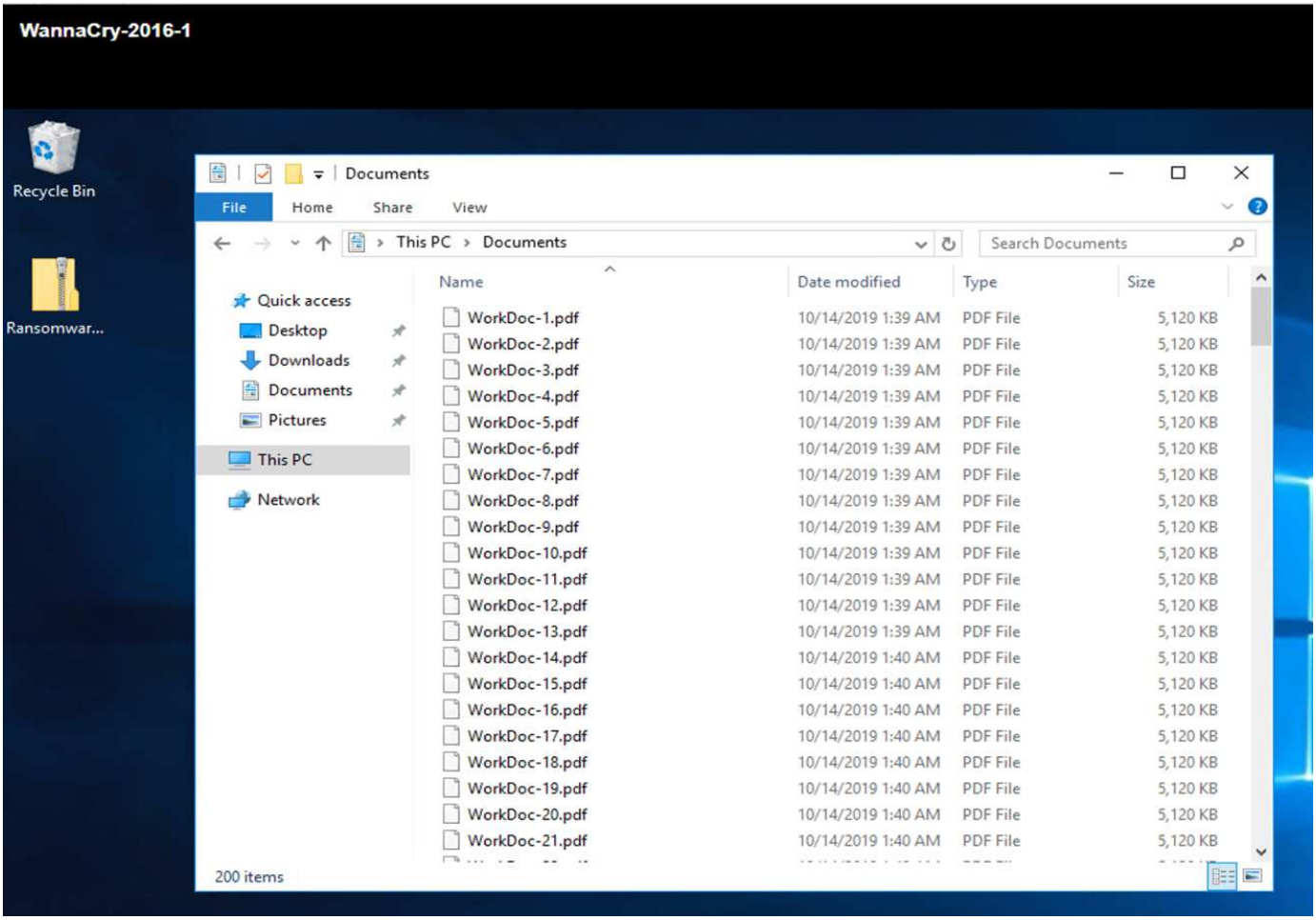
为了展示 FlexPod 的检测，修复和预防，我们根据编写本文档时提供的最新平台 CVD 中指定的准则构建了一个测试台： "采用 VMware vSphere 6.7 U1， Cisco UCS 第四代和 NetApp AFF A 系列 CVD 的 FlexPod 数据中心"。

在 VMware vSphere 基础架构中部署了一个 Windows 2016 VM ，该 VM 通过 NetApp ONTAP 软件提供 CIFS 共享。然后，在 CIFS 共享上配置了 NetApp FPolicy ，以防止执行具有特定扩展类型的文件。此外，还部署了 NetApp SnapCenter 软件来管理基础架构中 VM 的 Snapshot 副本，以提供应用程序一致的 Snapshot 副本。

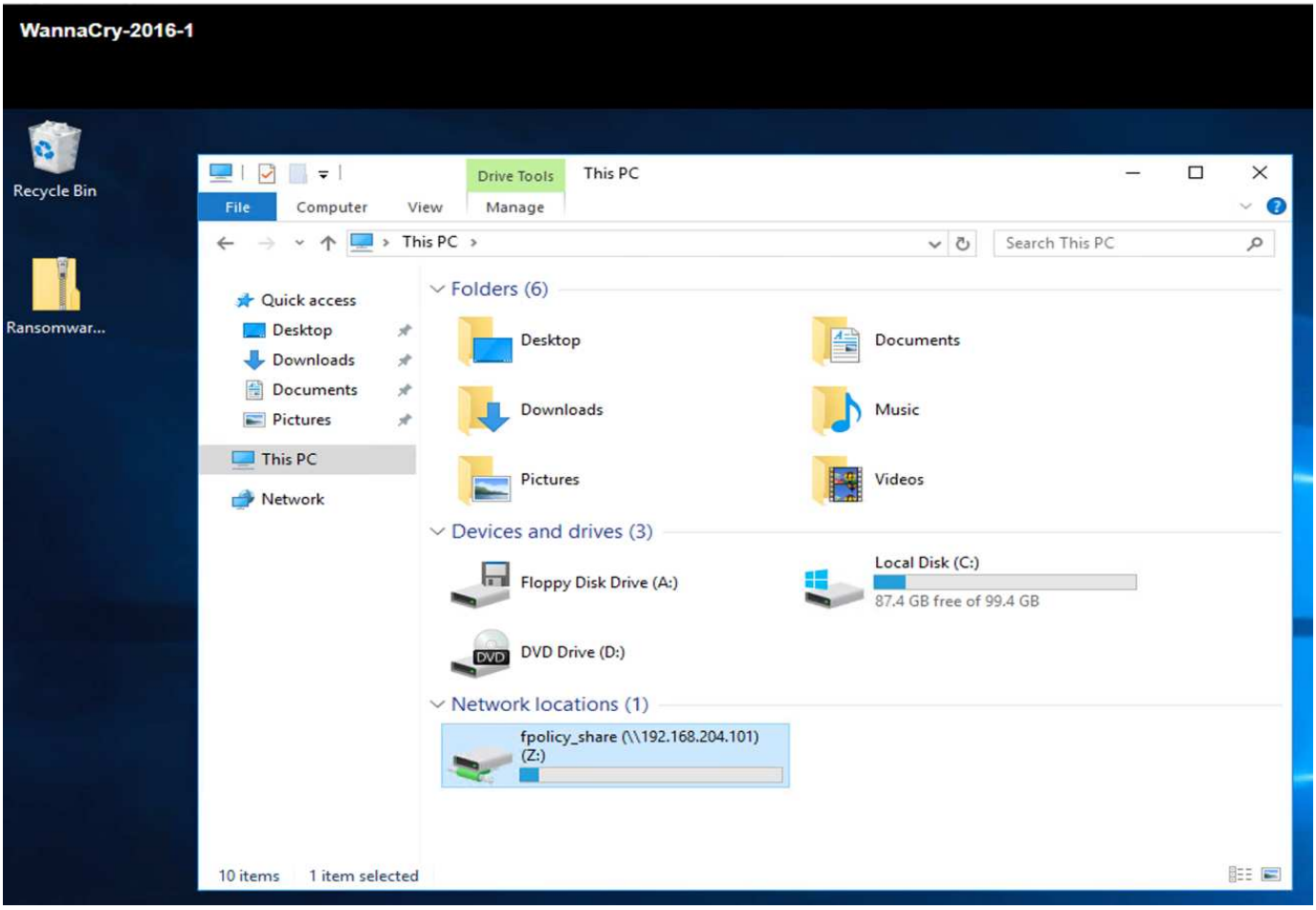
发生攻击前的虚拟机状态及其文件

本节显示了在对虚拟机进行攻击之前文件的状态以及映射到该虚拟机的 CIFS 共享。

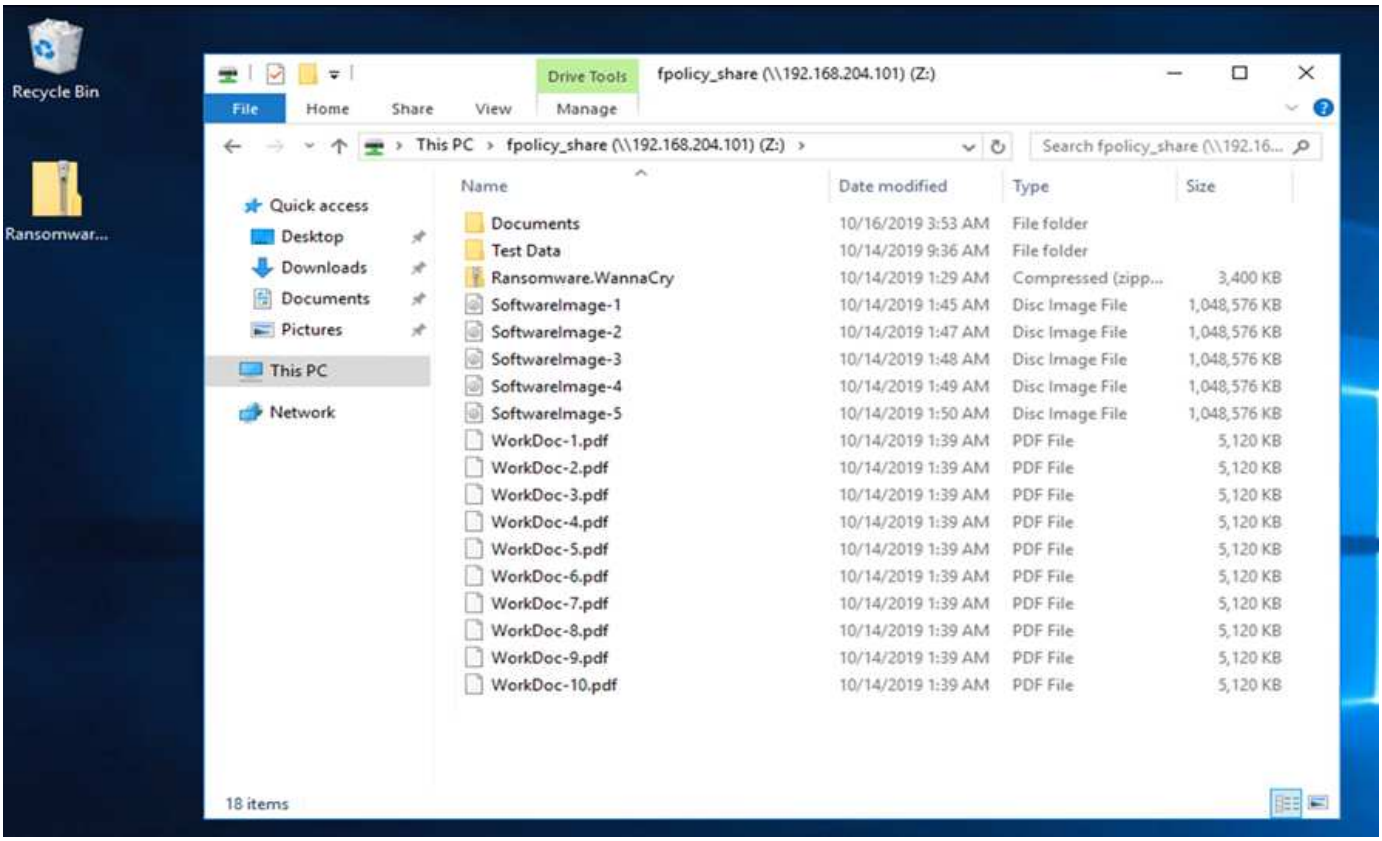
VM 的 Documents 文件夹包含一组 PDF 文件，这些文件尚未被 WannaCry 恶意软件加密。



以下屏幕截图显示了映射到虚拟机的 CIFS 共享。



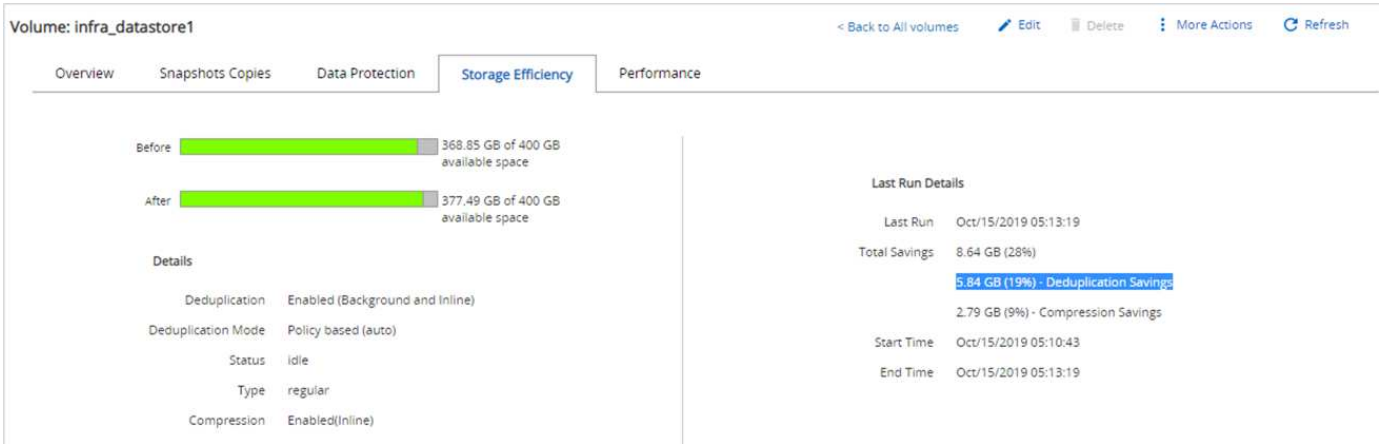
以下屏幕截图显示了 CIFS 共享 `fpolicy_share` 上尚未被 WannaCry 恶意软件加密的文件。



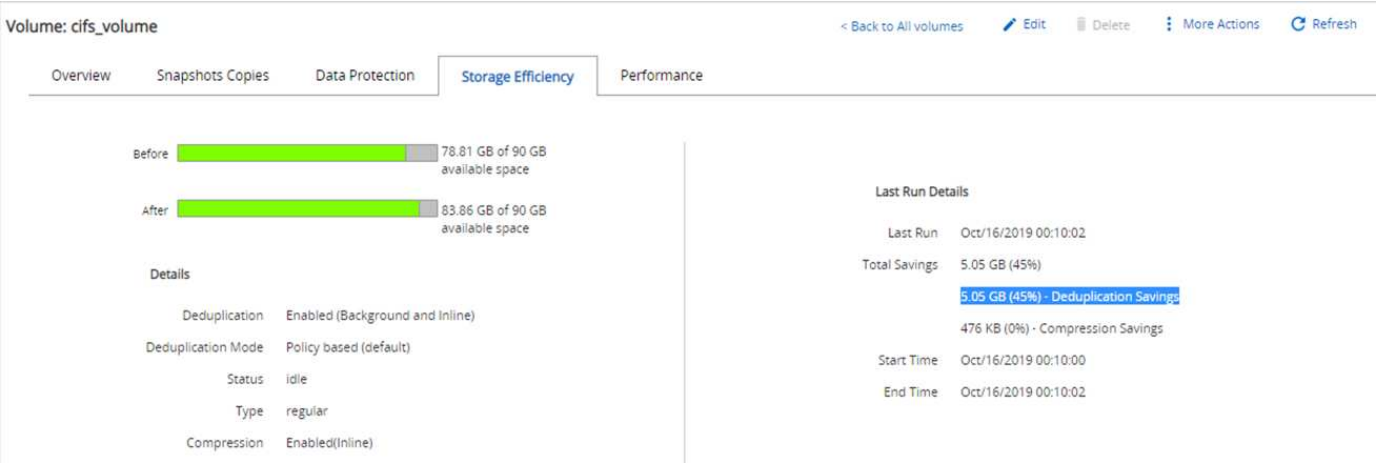
攻击前的重复数据删除和 **Snapshot** 信息

在检测阶段，系统会指示并参考 Snapshot 副本在攻击之前的存储效率详细信息和大小。

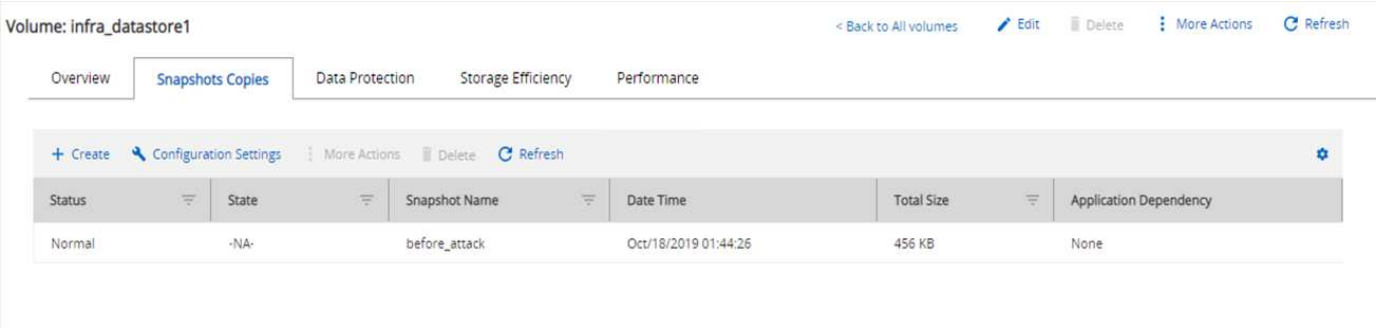
通过对托管 VM 的卷执行重复数据删除，存储节省了 19% 。



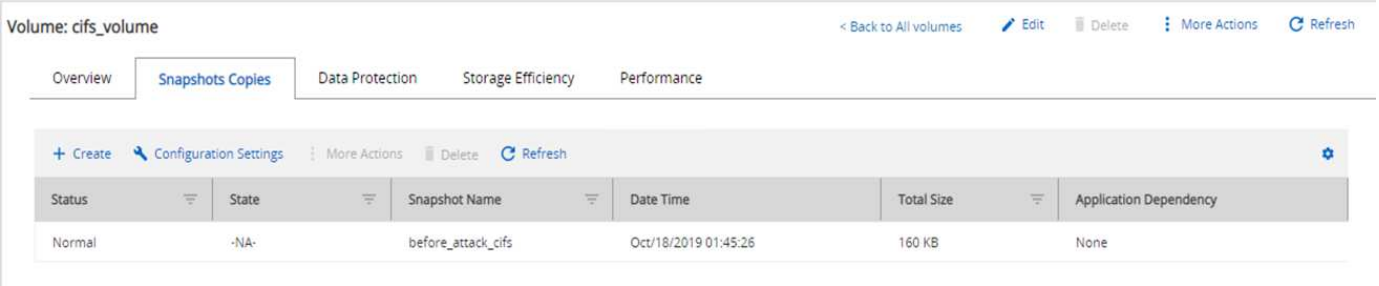
通过对 CIFS 共享 `fpolicy_share` 执行重复数据删除，存储节省了 45% 。



对于托管 VM 的卷，观察到 Snapshot 副本大小为 456 KB 。



对于 CIFS 共享 `fpolicy_share` ，观察到的 Snapshot 副本大小为 160 KB 。



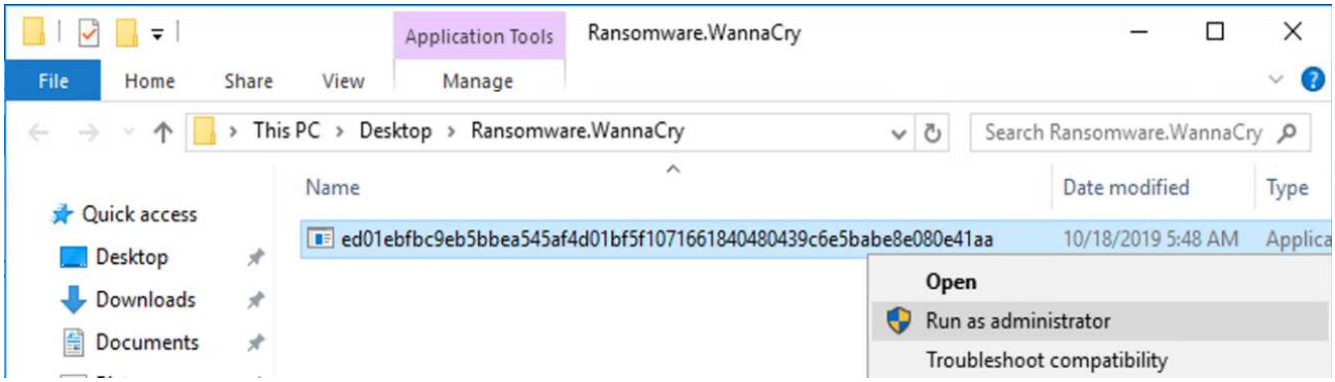
VM 和 CIFS 共享上的 WannaCry 感染

在本节中，我们将介绍 WannaCry 恶意软件是如何引入 FlexPod 环境的，以及随后观察到的系统更改。

以下步骤说明了 WannaCry 恶意软件二进制文件是如何引入 VM 的：

1. 已提取受保护的恶意软件。

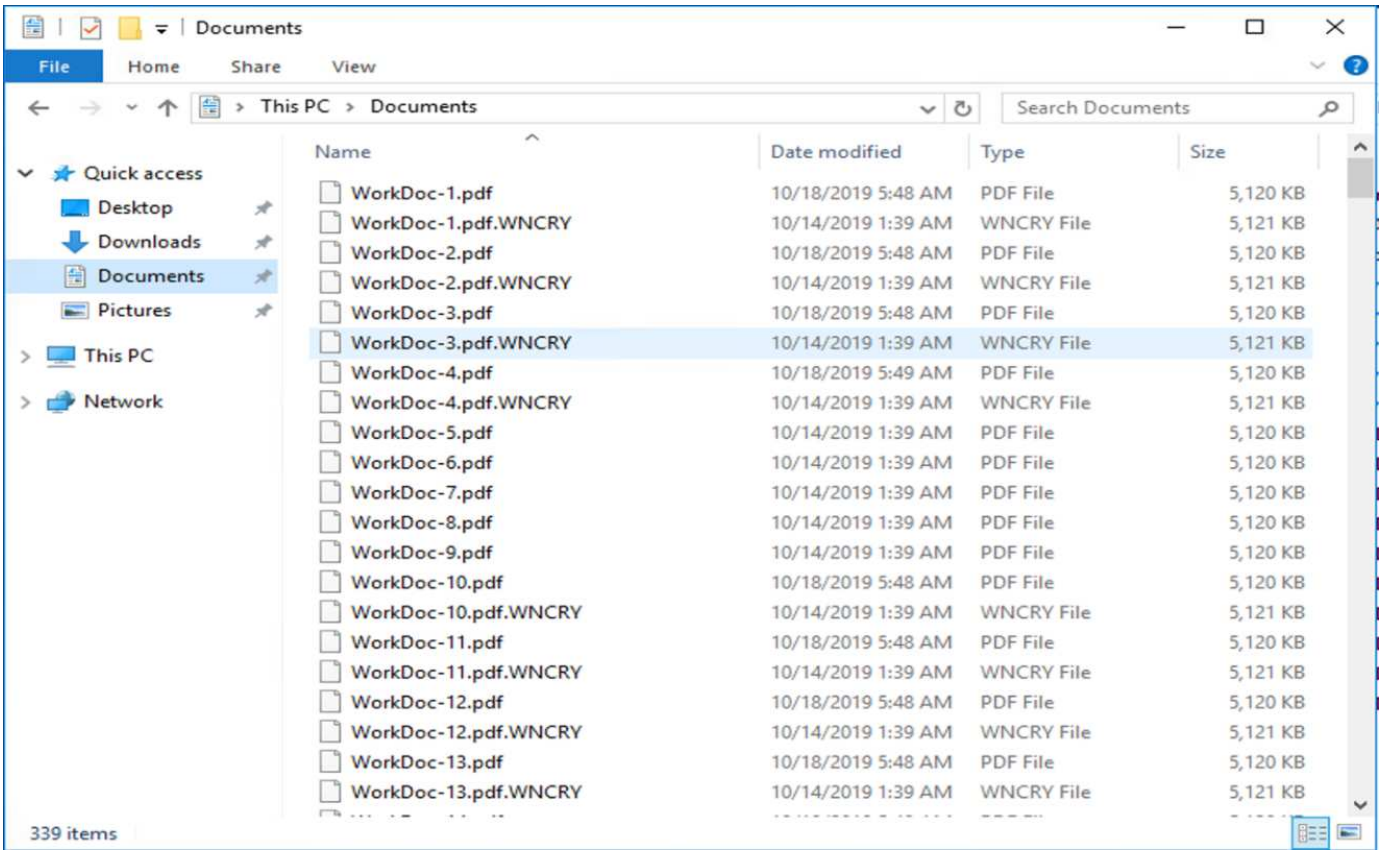
2. 已执行二进制文件。



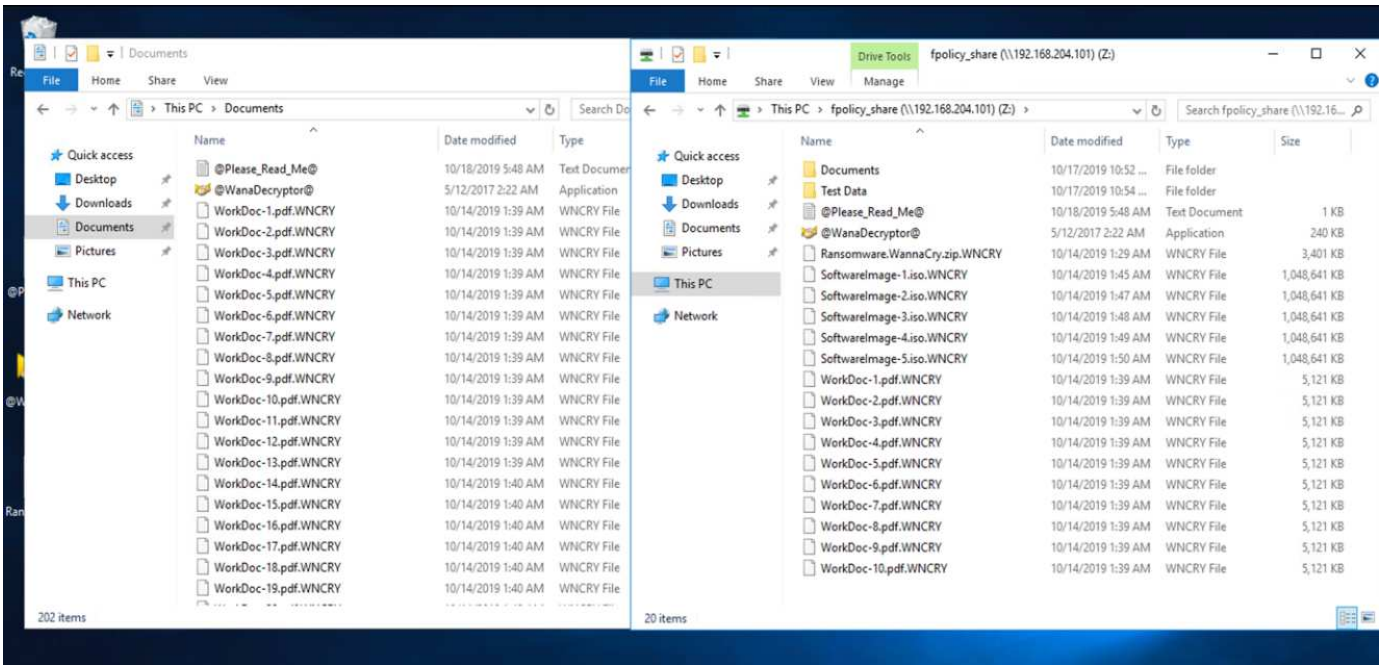
案例 **1**： **WannaCry** 对 **VM** 和映射的 **CIFS** 共享中的文件系统进行加密

本地文件系统和映射的 CIFS 共享已被 WannaCry 恶意软件加密。

恶意软件开始对具有 WNCRY 扩展名的文件进行加密。



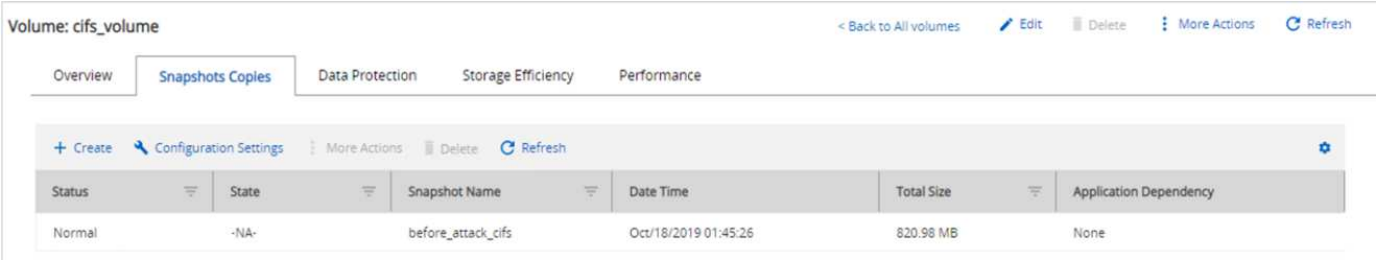
恶意软件会对本地 VM 和映射共享中的所有文件进行加密。



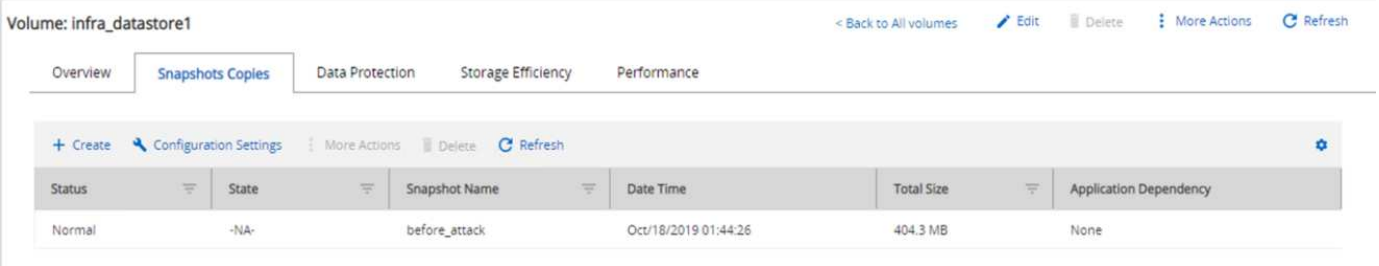
检测

从恶意软件开始对文件进行加密的那一刻起，它就触发了 Snapshot 副本大小的指数级增长以及存储效率百分比的指数级下降。

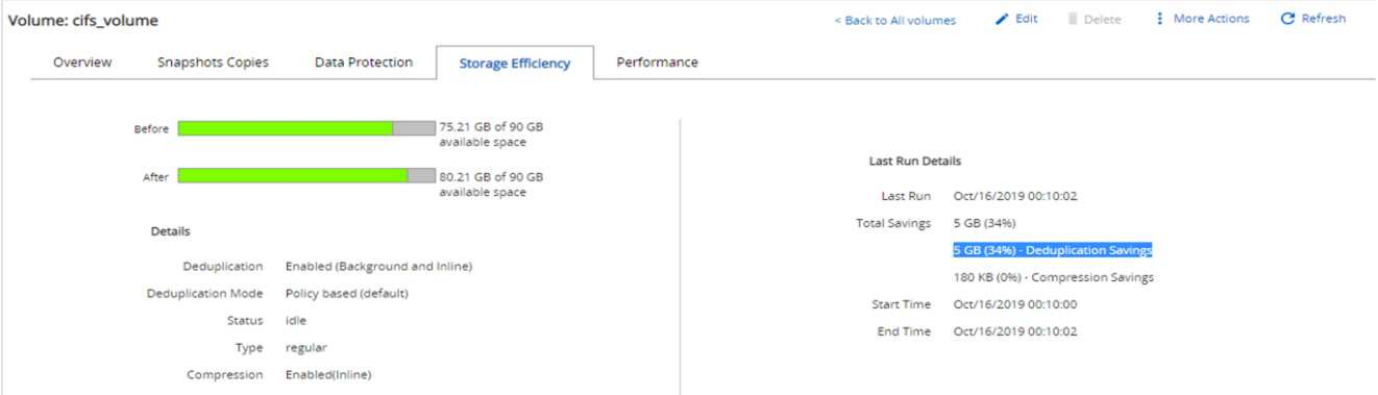
我们检测到，在攻击期间，托管 CIFS 共享的卷的 Snapshot 大小大幅增加到 820.98MB 。



我们检测到托管 VM 的卷的 Snapshot 副本大小增加到了 404.3MB 。



托管 CIFS 共享的卷的存储效率降低到 34% 。



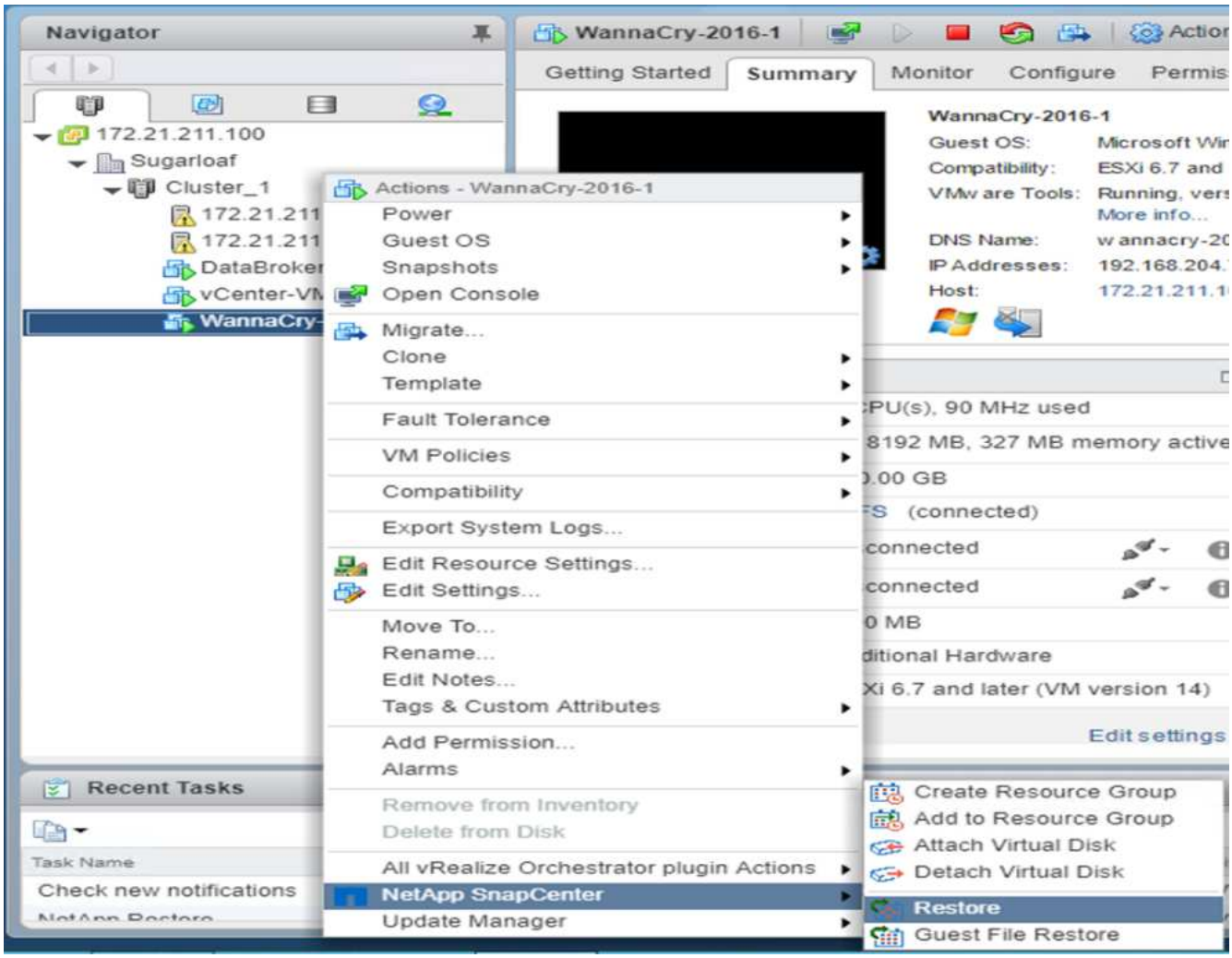
修复

在受到攻击之前使用全新 Snapshot 副本创建功能还原虚拟机和映射的 CIFS 共享。

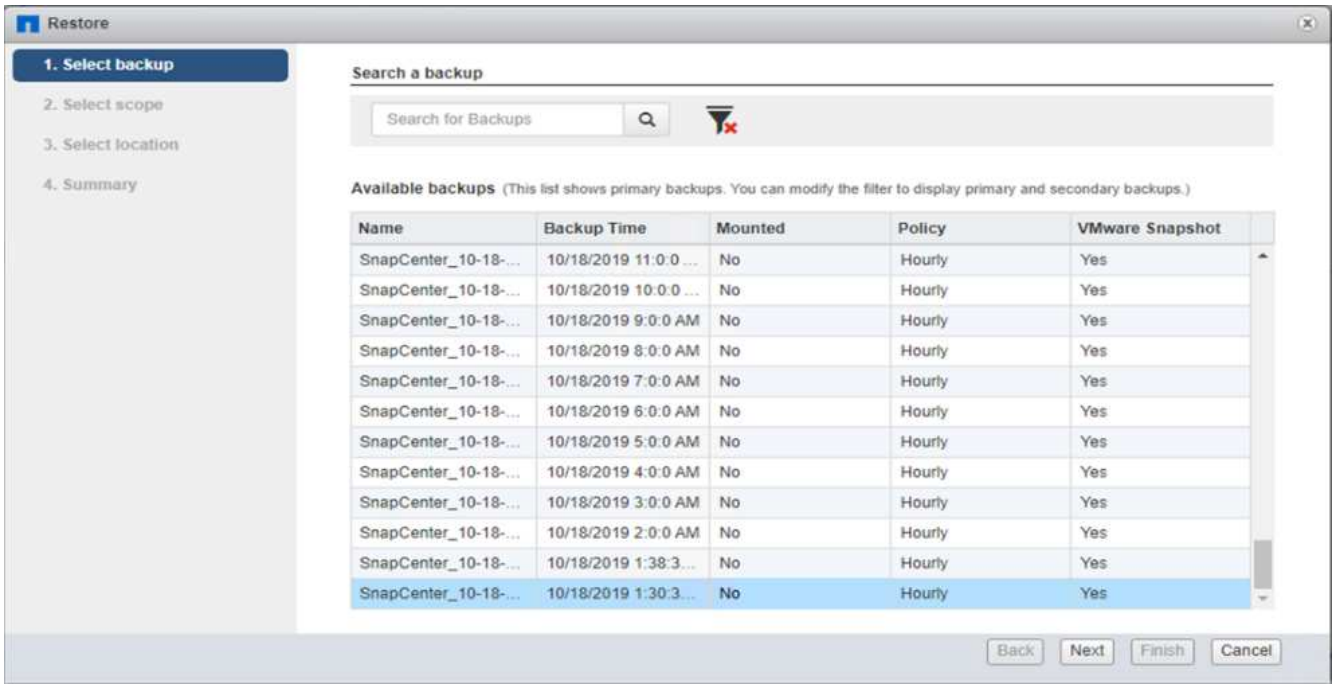
- 还原 VM*

要还原虚拟机，请完成以下步骤：

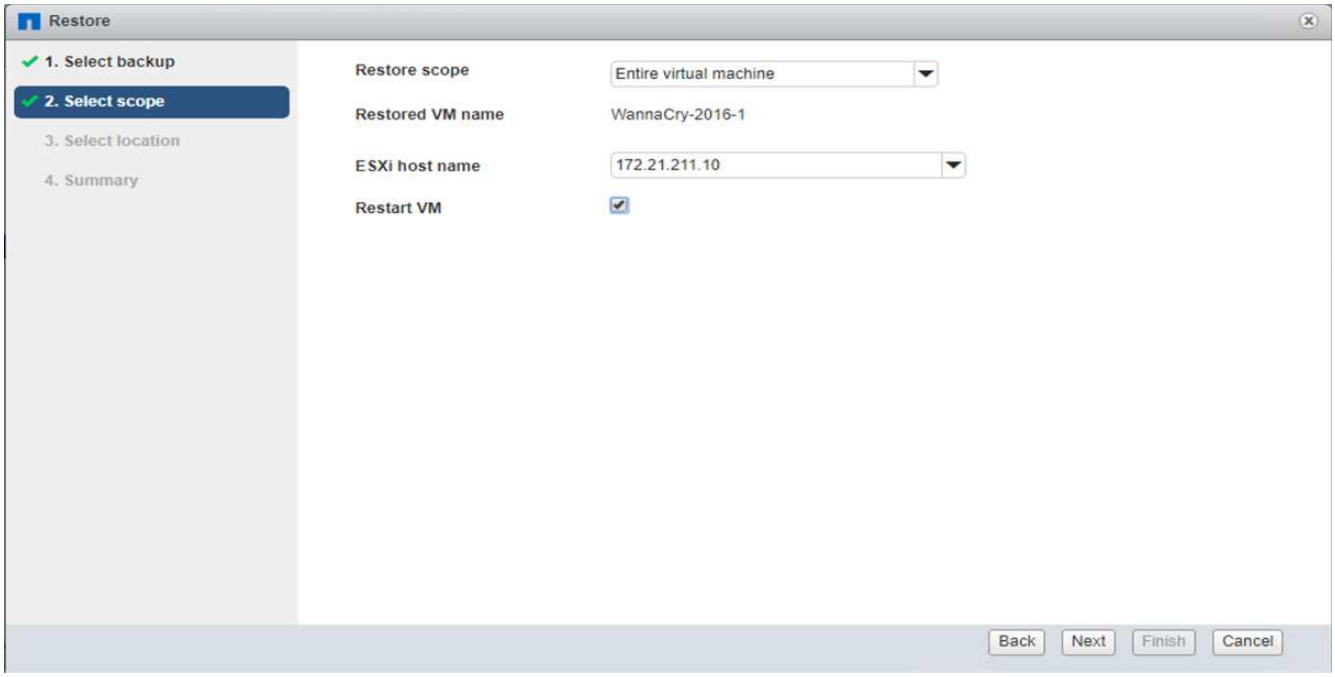
1. 使用您使用 SnapCenter 创建的 Snapshot 副本还原虚拟机。



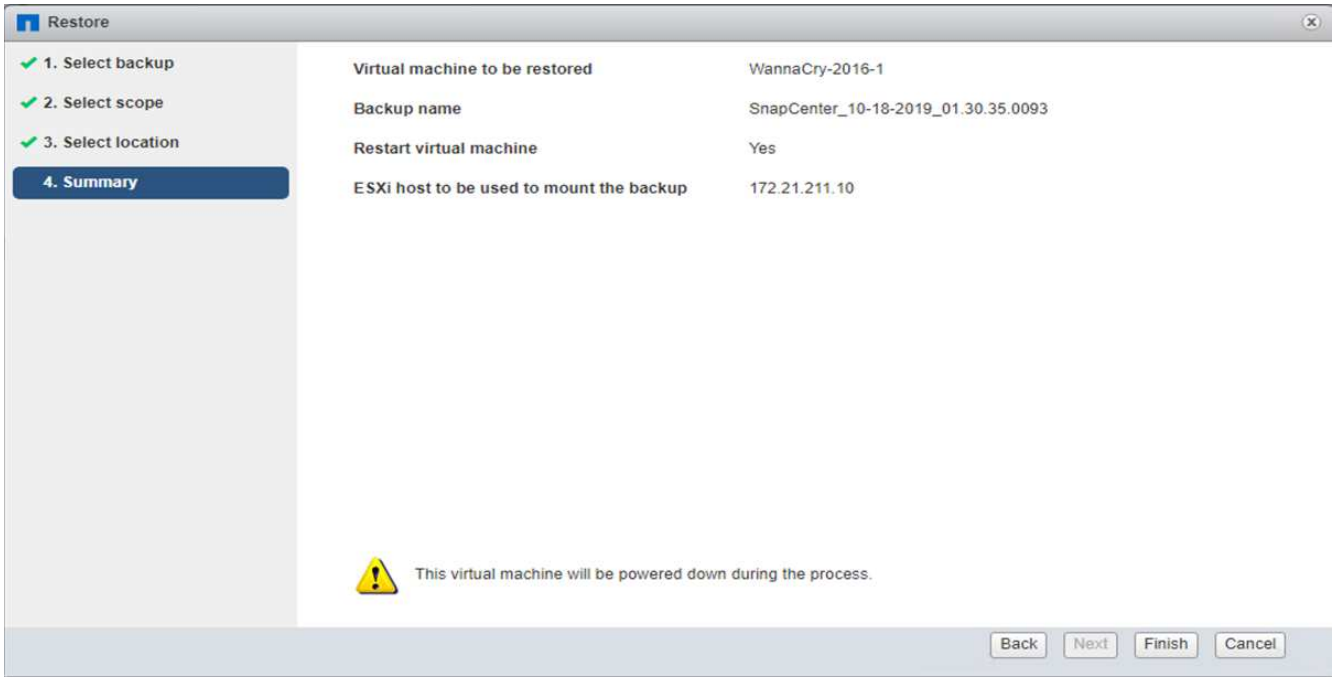
2. 选择所需的 VMware 一致 Snapshot 副本进行还原。



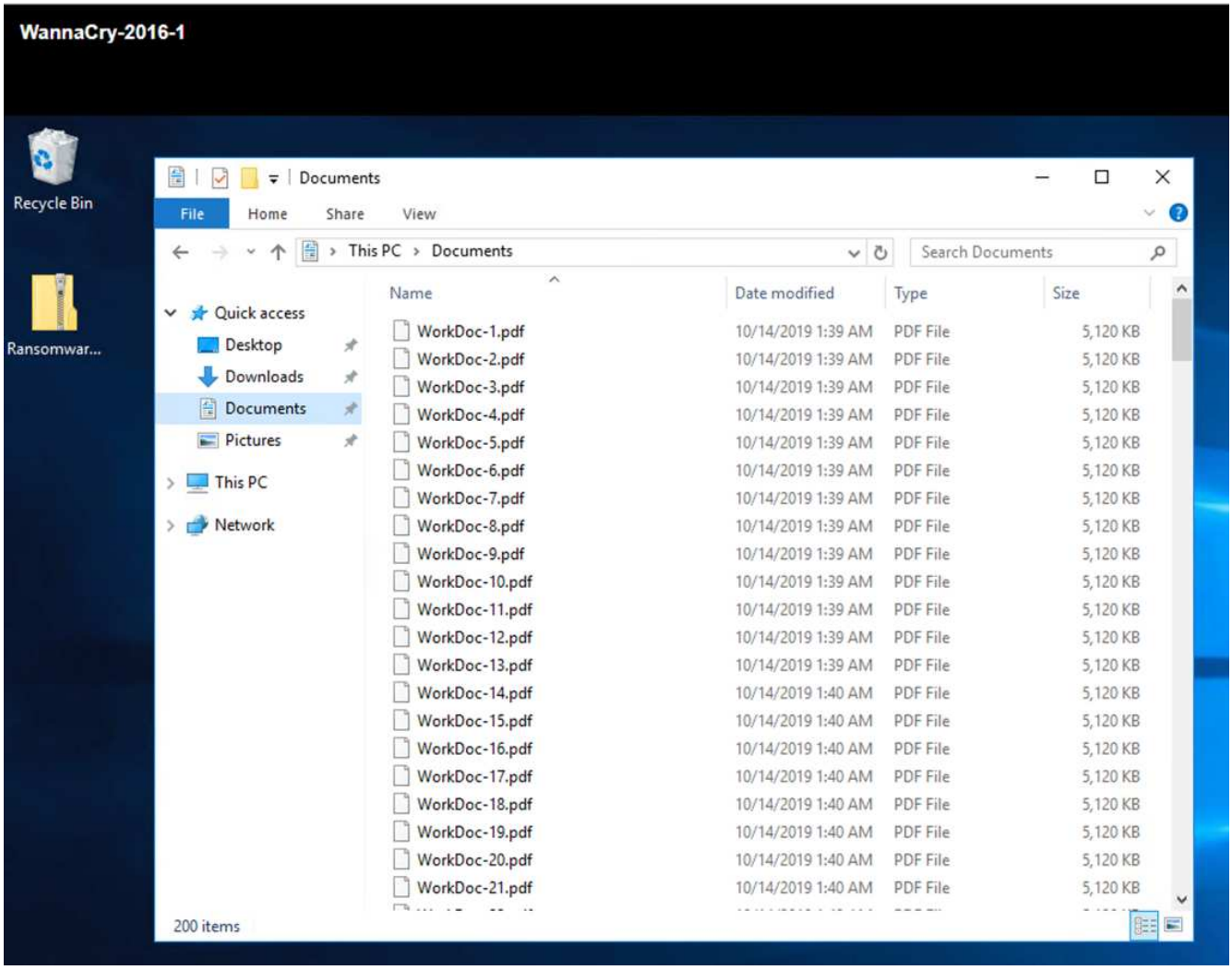
3. 此时将还原并重新启动整个 VM 。



4. 单击完成以启动还原过程。



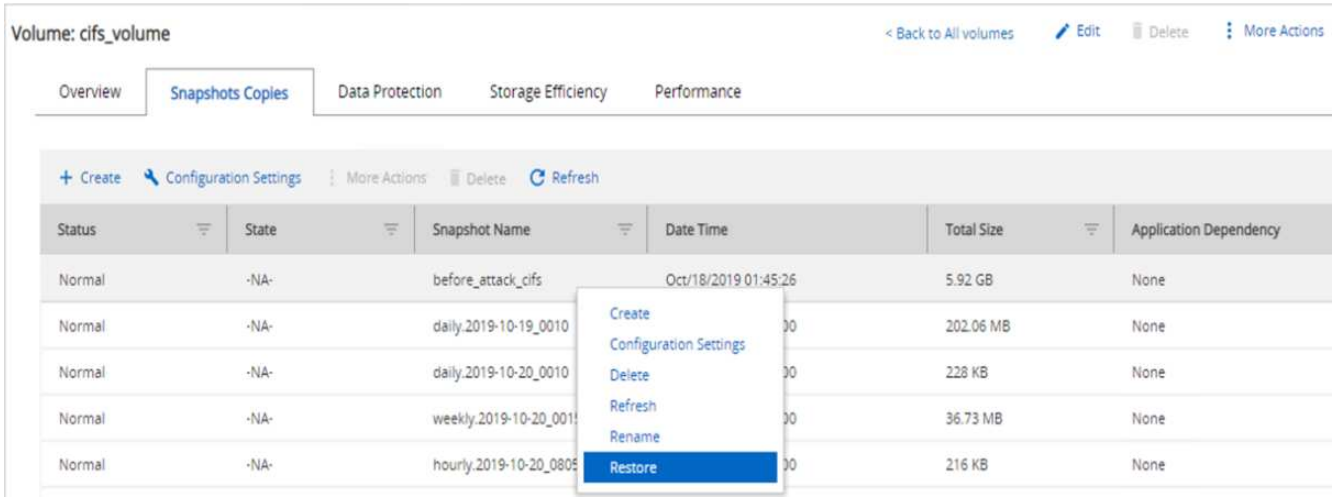
5. 虚拟机及其文件将会还原。



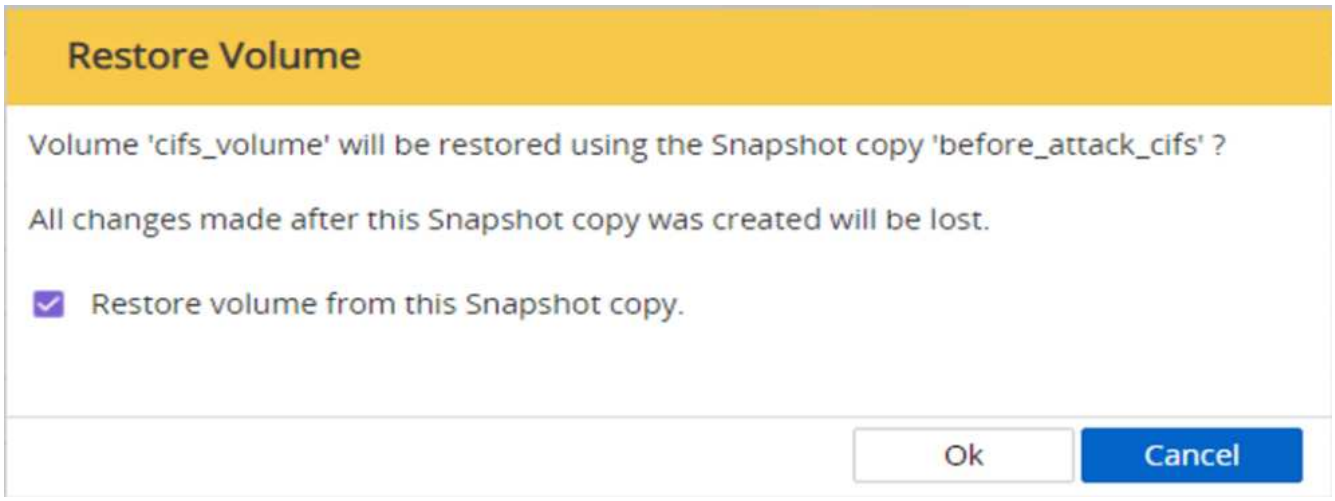
- 还原 CIFS 共享 *

要还原 CIFS 共享，请完成以下步骤：

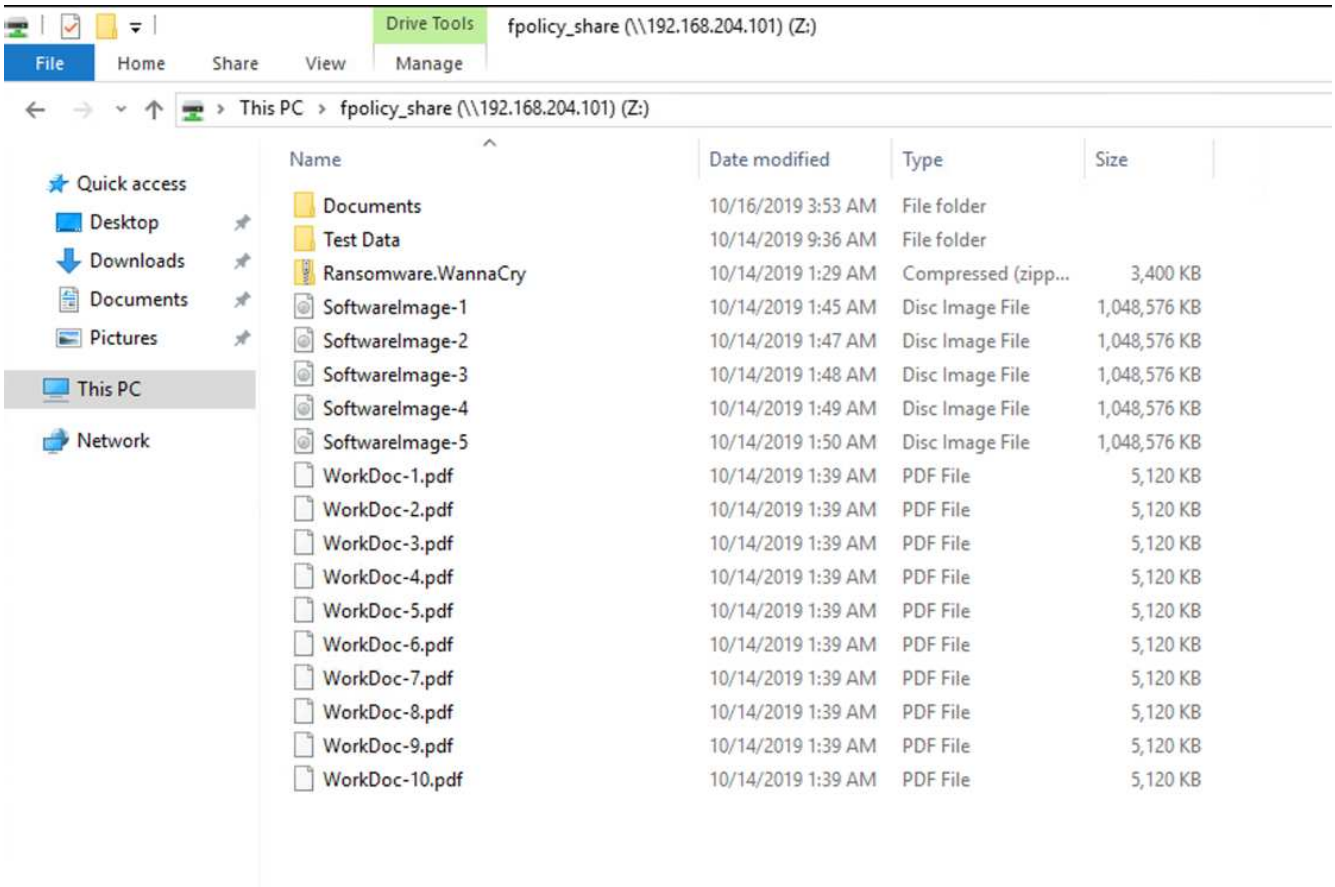
1. 使用攻击前创建的卷的 Snapshot 副本还原共享。



2. 单击确定以启动还原操作。



3. 还原后查看 CIFS 共享。



案例 **2**： **WannaCry** 对虚拟机中的文件系统进行加密，并尝试对通过 **FPolicy** 保护的映射 **CIFS** 共享进行加密

预防

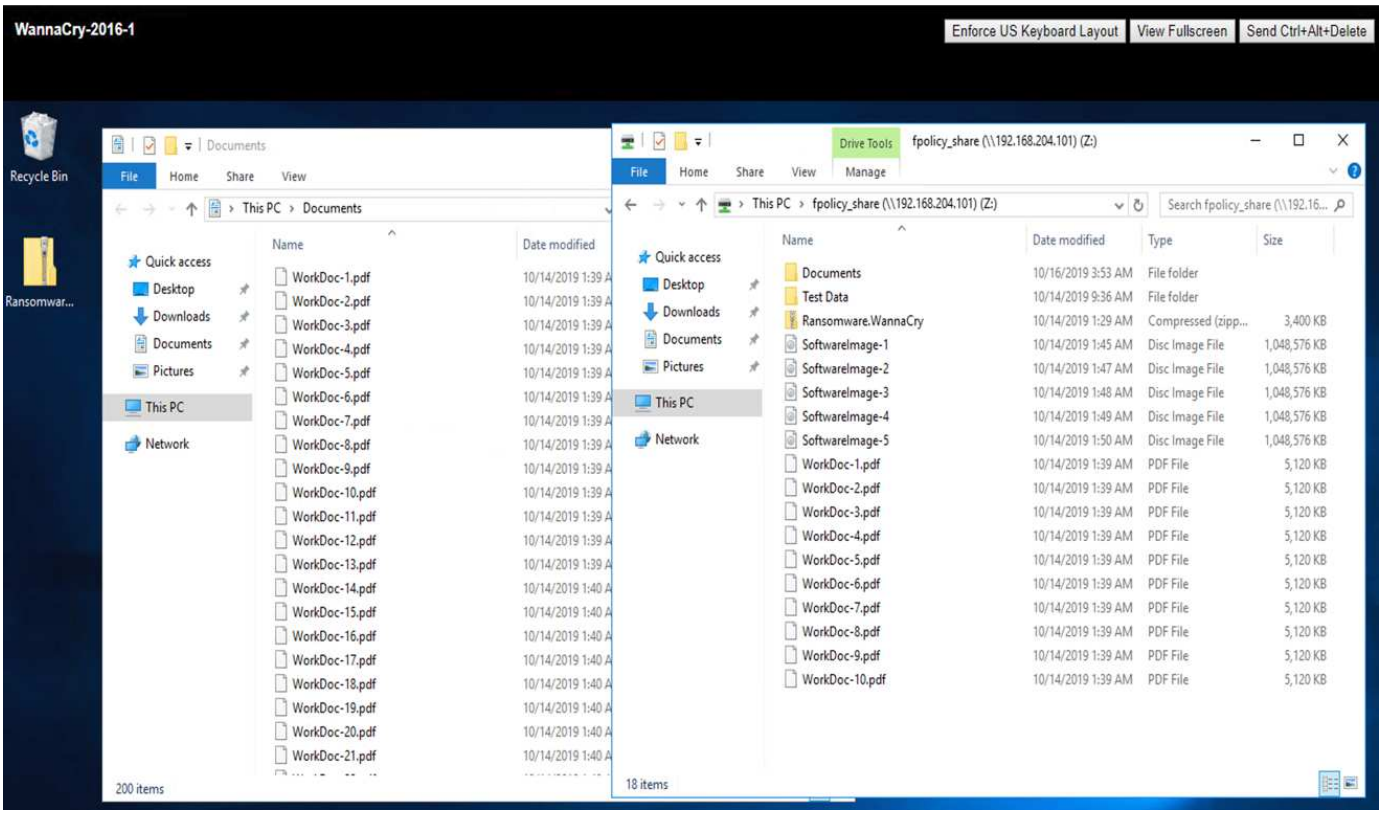
- 配置 FPolicy*

要在 CIFS 共享上配置 FPolicy ，请在 ONTAP 集群上运行以下命令：

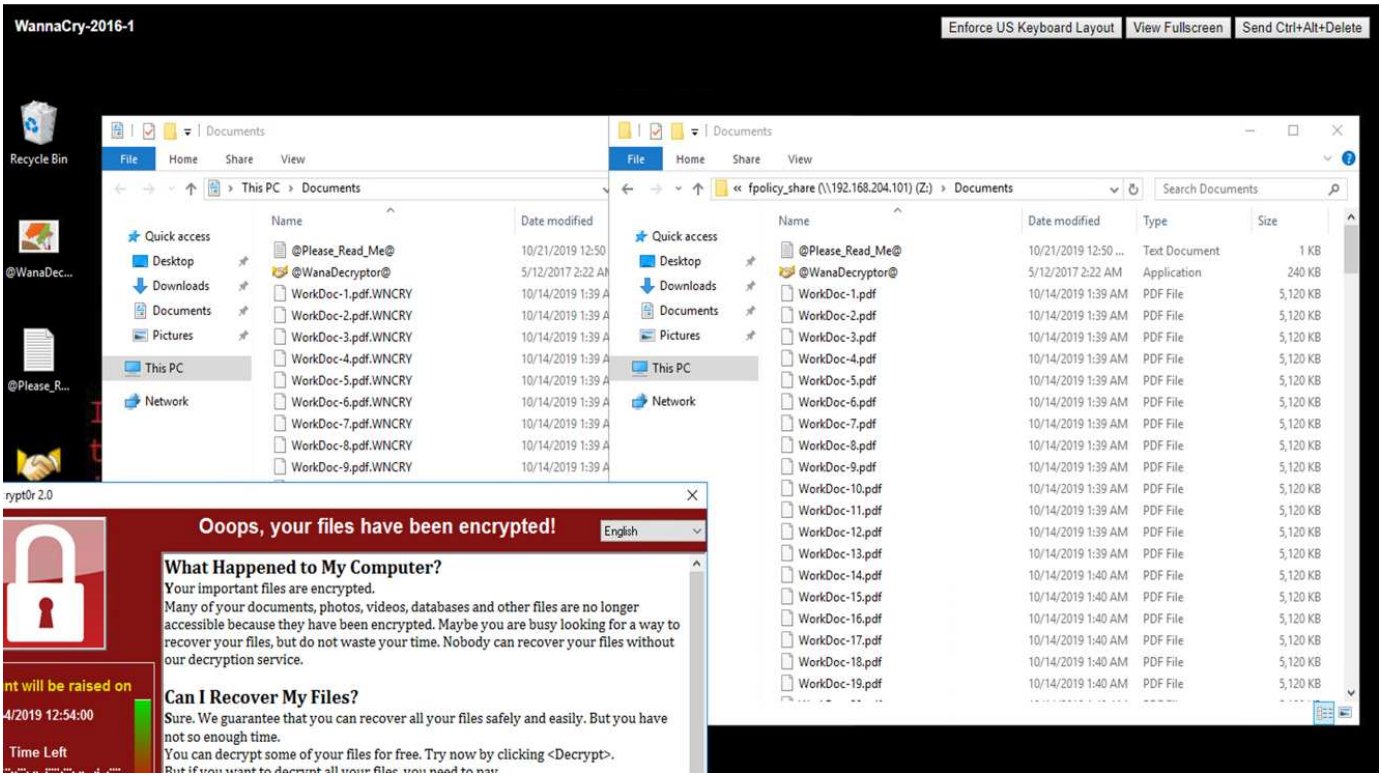
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -vserver infra_svm -policy-name
Ransomware_policy -shares-to-include fpolicy_share -file-extensions-to
-include WNCRY,Locky,ad4c
vserver fpolicy enable -vserver infra_svm -policy-name Ransomware_policy
-sequence-number 1
```

使用此策略时，不允许使用扩展名为 WNCRY， Locky 和 ad4c 的文件执行文件操作 create， rename， write 或 open 。

查看文件在攻击前的状态—它们未加密且位于一个干净的系统中。



虚拟机上的文件已加密。WannaCry 恶意软件会尝试对 CIFS 共享中的文件进行加密，但 FPolicy 会防止其影响这些文件。



继续开展业务运营，无需支付任何费用

本文档中介绍的 NetApp 功能可帮助您在攻击发生后几分钟内还原数据，并从一开始就防止攻击，以便您可以无阻碍地继续开展业务运营。

可以设置 Snapshot 副本计划以满足所需的恢复点目标（RPO）。基于 Snapshot 副本的还原操作非常快速；因此，可以实现极低的恢复时间目标（RTO）。

最重要的是，您不必因攻击而支付任何勒索，您可以快速恢复正常运营。

结论

勒索软件是有组织犯罪的产物，攻击者不会按照道德标准行事。即使在收到勒索之后，他们也可以避免提供解密密钥。受害者不仅会丢失数据，还会损失大量资金，并将面临与生产数据丢失相关的后果。

根据 A "《福布斯》文章"只有 19% 的勒索软件受害者在支付了勒索之后才会获得数据。因此，作者建议在发生攻击时不要支付勒索，因为这样做会增强攻击者对其业务模式的信心。

数据备份和还原操作是勒索软件恢复的重要组成部分。因此，必须将它们作为业务规划的一个组成部分。实施这些操作的预算应用于，以便在发生攻击时恢复功能不会受到任何影响。

关键在于在此过程中选择正确的技术合作伙伴， FlexPod 可在纯闪存 FAS 系统中提供本机所需的大多数功能，而无需额外费用。

致谢

作者谨感谢以下人员为编写本文档提供的支持：

- NetApp 公司的 JORGE Gomez Navarrete
- NetApp 公司 Ganesh Kamath

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：

- NetApp Snapshot 软件

  "https://www.netapp.com/us/products/platform-os/snapshot.aspx"

- SnapCenter 备份管理

  "https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx"

- SnapLock 数据合规性

  "https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx"

- NetApp 产品文档

  "https://www.netapp.com/us/documentation/index.aspx"

- Cisco 高级恶意软件保护（AMP）

  "https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html"

- Cisco Stealthwatch

  "https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html"

适用于医疗保健的 FIPS 140-2 安全合规 FlexPod 解决方案

TR-4892： 适用于医疗保健的 FIPS 140-2 安全合规 FlexPod 解决方案

NetApp Cisco 公司 John McAbel 的 JayaKishore Esanakula

《经济和临床健康健康信息技术法案》（HITECH）要求对经联邦信息处理标准（FIPS） 140-2 验证的电子受保护健康信息（ePHI）进行加密。要获得 " 提升互操作性计划 "（以前称为 " 有意义的使用奖励计划 "）认证，运行状况信息技术（HIT）应用程序和软件必须符合 FIPS 140-2 的要求。符合条件的提供商和医院必须使用符合 FIPS 140-2 （1 级）标准的命中率来获得医疗保健和医疗辅助奖励，并避免从医疗保健和医疗辅助中心（CMS）获得报销处罚。FIPS 140-2 认证加密算法符合作为技术保障的要求 "安全规则" 《健康信息可移植性和责任法案》（HIPAA）。

FIPS 140-2 属于美国为硬件，软件和固件中的加密模块设置安全要求以保护敏感信息的政府标准。美国要求遵守本标准政府机构， IT 也经常用于金融服务和医疗保健等受监管行业。本技术报告有助于读者深入了解 FIPS 140-2 安全标准。它还有助于受众了解医疗保健组织面临的各种威胁。最后，该技术报告有助于了解在 FlexPod 融合基础架构上部署符合 FIPS 140-2 标准的 FlexPod 系统如何帮助保护医疗保健资产的安全。

范围

本文档对基于 Cisco Unified Computing System （Cisco UCS）， Cisco Nexus， Cisco MDS 和 NetApp ONTAP 的 FlexPod 基础架构进行了技术概述，用于托管一个或多个需要 FIPS 140-2 安全合规性的医疗保健 IT 应用程序或解决方案。

audience

本文档面向医疗保健行业的技术主管以及 Cisco 和 NetApp 合作伙伴解决方案工程师和专业服务人员。NetApp 假定读者已很好地了解计算和存储规模估算概念，并在技术上熟悉医疗保健威胁，医疗保健安全，医疗保健 IT 系统， Cisco UCS 和 NetApp 存储系统。

"接下来：医疗保健领域的网络安全威胁。"

医疗保健领域的网络安全威胁

"上一页：简介。"

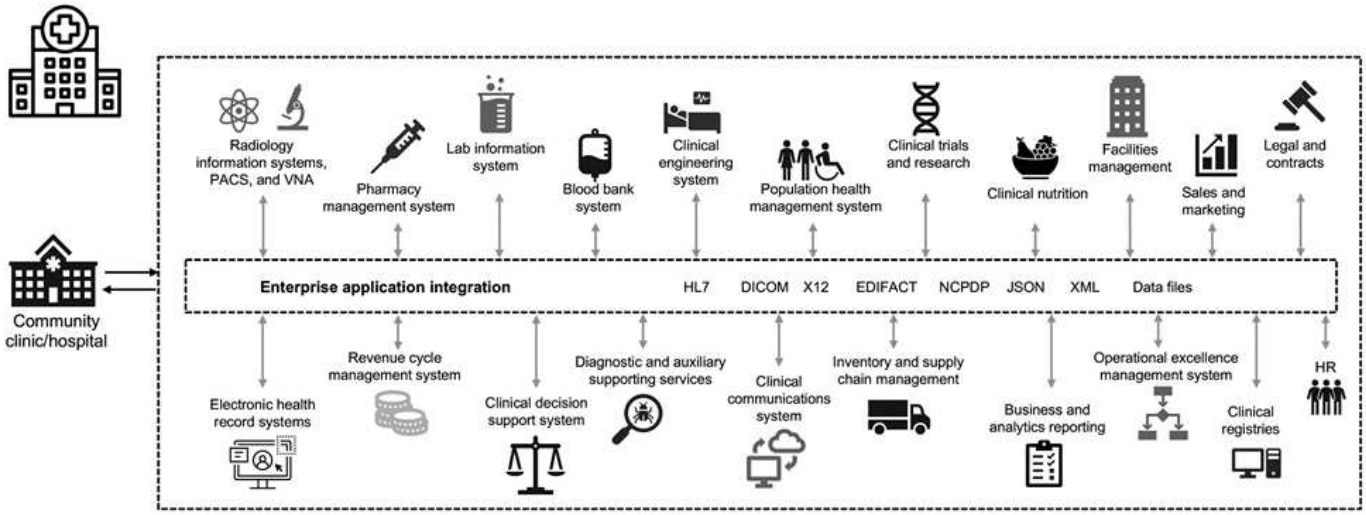
每一个问题都带来了新的机会， COVID 大流行病就是一个例子。根据 A "report" 根据健康和人类服务部门（HHS）网络安全计划， COVID 的响应导致勒索软件攻击数量增加。截至 2020 年 3 月第三周，注册的新互联网域有 6， 000 个。超过 50% 的域托管恶意软件。2020 年，勒索软件攻击造成了近 50% 的医疗保健数据违规，影响到超过 630 家医疗保健组织和大约 2， 900 万份医疗保健记录。19 个泄漏点 / 站点的勒索行为增加了一倍。在 2020 年，医疗保健行业的数据泄露次数高达 24.5% 。

恶意代理通过销售受保护健康信息（Phi）或威胁销毁或公开该信息，试图破坏该信息的安全性和隐私。通常会进行有针对性的大规模广播尝试，以获取对 ePHI 的未授权访问。在 2020 年下半年，大约 75% 的公开患者记录是由于业务伙伴受到影响。

以下医疗保健组织被恶意代理作为目标：

- 医院系统
- 生命科学实验室
- 研究实验室
- 恢复设施
- 社区医院和诊所

构成医疗保健组织的应用程序的多样性是不可否认的，并且日益复杂。信息安全办公室面临着为大量 IT 系统和资产提供监管的挑战。下图显示了典型医院系统的临床功能。



患者数据是此图的核心。患者数据的丢失以及与敏感医疗状况相关的侮辱是非常真实的。其他敏感问题包括社会排斥，勒索，特征描述，容易受到有针对性的营销，被利用的风险，以及在支付者的特权之外对医疗信息可能承担的财务责任。

医疗保健面临的威胁具有多层面性质，而且具有多种影响。全球政府已制定各种条款来确保 ePHI 的安全。医疗保健所面临的不利影响和不断变化的性质使医疗保健组织难以抵御所有威胁。

下面列出了医疗保健领域中发现的常见威胁：

- 勒索软件攻击
- 丢失或被盗包含敏感信息的设备或数据
- 网络钓鱼攻击
- 攻击连接的医疗设备，可能会影响患者安全
- 电子邮件网络钓鱼攻击
- 设备或数据丢失或被盗
- 远程桌面协议损坏
- 软件漏洞

医疗保健组织在法律和监管环境中运营，这种环境与数字生态系统一样复杂。此环境包括但不限于以下内容：

- 美国国家医疗保健技术协调办公室（美国国家协调办公室） ONC 认证电子医疗保健信息技术互操作性标准
- 享受医疗保健和儿童健康保险计划重新授权法案（ MACRA ） / 有意义的使用
- 根据食品和药物管理局（ FDA ）承担的多项义务
- 联合委员会的资格鉴定过程
- HIPAA 要求
- 高科技要求
- 付款人可接受的最低风险标准
- 规定隐私和安全规则
- 通过国家卫生机构等机构将联邦信息安全现代化法案要求纳入联邦合同和研究拨款中

- 支付卡行业数据安全标准（ PCI-DSS ）
- 《药物滥用和精神健康服务管理（ SAMHSA ）要求》
- 用于财务处理的《格雷姆 - 里奇 - 比利雷法案》
- 与向附属组织提供服务相关的《 Stark 法律》
- 《家庭教育权利和隐私法》（ FERPA ）适用于参与高等教育的机构
- 《遗传信息不歧视法》（ GINA-GINESE ）
- 欧盟新的《一般数据保护条例》（ GDPR ）

安全架构标准正在快速发展，以防止恶意行为者影响医疗保健信息系统。其中一项标准是 FIPS 140-2 ，该标准由美国国家标准与技术协会（ NIST ）定义。FIPS 出版物 140-2 详细介绍了美国加密模块的政府要求。安全要求涵盖与安全设计和实施加密模块相关的区域，可应用于命中。定义完善的加密边界可以简化安全管理，同时保持最新的加密模块。这些边界有助于防止恶意攻击者容易利用弱密码模块。它们还有助于防止在管理标准加密模块时出现人为错误。

NIST 与通信安全机构（ CSE ）共同制定了加密模块验证计划（ CMVP ），用于对 FIPS 140-2 验证级别的加密模块进行认证。联邦组织需要使用 FIPS 140-2 认证模块在空闲和移动时保护敏感或有价值的数据。由于 ePHI 能够成功保护敏感或有价值的信息，因此许多医疗保健系统都选择使用 FIPS 140-2 加密模块对 ePHI 进行加密，这超出了法律规定的最低安全级别。

利用和实施 FlexPod FIPS 140-2 功能只需数小时（而不是数天）。无论规模大小，大多数医疗保健组织都可以获得 FIPS 合规性。通过明确定义的加密边界以及详细记录的简单实施步骤，符合 FIPS 140-2 的 FlexPod 架构可以为基础架构奠定坚实的安全基础，并可通过简单的增强功能进一步增强对安全威胁的保护。

"接下来： FIPS 140-2 概述。"

FIPS 140-2 概述

"上一篇：医疗保健领域的网络安全威胁。"

"FIPS 140-2" 指定在保护计算机和电信系统中敏感信息的安全系统中使用的加密模块的安全要求。加密模块应为一组硬件，软件，固件或两者的组合。FIPS 适用场景 加密边界内包含的加密算法，密钥生成和密钥管理器。请务必了解， FIPS 140-2 专门适用于加密模块，而不是产品，架构，数据或生态系统。本文档后面的关键术语中定义的加密模块是实施批准的安全功能的特定组件（无论是硬件，软件和 / 或固件）。此外， FIPS 140-2 还指定了四个级别。经过批准的加密算法适用于所有级别。每个安全级别的关键要素和要求包括：

- * 安全级别 1*
  - 指定加密模块的基本安全要求（至少需要一个经过批准的算法或安全功能）。
  - 除了生产级组件的基本要求之外， 1 级不需要任何指定的物理安全机制。
- * 安全级别 2*
  - 通过使用不受篡改的解决方案（例如，覆盖层或密封，可拆卸盖板或加密模块的门锁）添加篡改证据要求，增强了物理安全机制。
  - 至少需要基于角色的访问控制（ Role-Based Access Control ， RBAC ），在此控制中，加密模块对操作员或管理员的授权进行身份验证，以承担特定角色并执行一组相应的功能。

- * 安全级别 3*
  - 基于 2 级的防篡改要求构建，并尝试防止进一步访问加密模块中的关键安全参数（ CSP ）。
  - 第 3 级所需的物理安全机制旨在检测和响应物理访问尝试或对加密模块的任何使用或修改的可能性较高。示例可能包括：打开加密模块上的可拆卸盖时，强磁盘机箱，防拆检测以及将所有纯文本 CSP 置零的响应电路。
  - 需要基于身份的身份验证机制来增强级别 2 中指定的 RBAC 机制的安全性。加密模块对操作员身份进行身份验证，并验证操作员是否有权使用某个角色并执行该角色的功能。
- * 安全级别 4*
  - FIPS 140-2 中最高级别的安全性。
  - 在物理上不受保护的环境中执行操作的最有用级别。
  - 在这一级别，物理安全机制旨在为加密模块提供全面保护，并负责检测和响应任何未经授权的物理访问尝试。
  - 加密模块的渗透或暴露应具有很高的检测概率，并导致所有不安全或纯文本 CSP 立即置零。

"下一步：控制平面与数据平面。"

控制平面与数据平面

"先前版本： FIPS 140-2 概述。"

在实施 FIPS 140-2 策略时，了解要保护的内容非常重要。这可以轻松细分为两个区域：控制平面和数据平面。控制面板是指影响 FlexPod 系统中组件的控制和操作的方面：例如，对 NetApp 存储控制器， Cisco Nexus 交换机和 Cisco UCS 服务器的管理访问。通过限制管理员可用于连接到设备和进行更改的协议和加密网络算法，可以在这一层提供保护。数据平面是指 FlexPod 系统中的实际信息，例如 PHI 。通过对空闲数据进行加密以及对 FIPS 再次进行加密来保护此数据，从而确保使用的加密模块符合标准。

"接下来： FlexPod Cisco UCS 计算和 FIPS 140-2 。"

FlexPod Cisco UCS 计算和 FIPS 140-2

"上一步：控制平面与数据平面。"

FlexPod 架构可以使用符合 FIPS 140-2 的 Cisco UCS 服务器进行设计。根据美国SNIST ， Cisco UCS 服务器可以在 FIPS 140-2 1 级合规模式下运行。有关符合 FIPS 的 Cisco 组件的完整列表，请参见 "Cisco 的 FIPS 140 页面"。Cisco UCS Manager 已通过 FIPS 140-2 验证。

Cisco UCS 和互联阵列

Cisco UCS Manager 可通过 Cisco 互联阵列（ Fabric Interconnects ， FI ）进行部署和运行。

有关 Cisco UCS 以及如何启用 FIPS 的详细信息，请参见 "Cisco UCS Manager 文档"。

要在每个网络结构 A 和 B 上的 Cisco 互联阵列上启用 FIPS 模式，请运行以下命令：

```
fp-health-fabric-A# connect local-mgmt
fp-health-fabric-A(local-mgmt)# enable fips-mode
FIPS mode is enabled
```

> 要在 Cisco UCS Manager 3.2 （3）版之前的版本上将集群中的 FI 替换为 FI，请在将替代 FI 添加到集群之前，先在现有 FI 上禁用 FIPS 模式（disable `FIPS-mode`）。集群形成后，在 Cisco UCS Manager 启动过程中， FIPS 模式将自动启用。

Cisco 提供了可在计算或应用程序层实施的以下关键产品：

- * 适用于端点的 Cisco 高级恶意软件保护（AMP）。 * 此解决方案 在 Microsoft Windows 和 Linux 操作系统上受支持，集成了预防，检测和响应功能。此安全软件可防止违规行为，在入口点阻止恶意软件，并持续监控和分析文件和流程活动，以快速检测，控制和修复可能规避前线防护的威胁。AMP 的恶意活动保护（MAP）组件持续监控所有端点活动，并提供运行时检测和阻止端点上正在运行的程序的异常行为。例如，如果端点行为表明存在勒索软件，则会终止违规流程，从而阻止端点加密并阻止攻击。
- * 电子邮件安全性的 AMP 。 * 电子邮件已成为传播恶意软件和实施网络攻击的主要工具。平均而言，一天内会交换大约 1000 亿封电子邮件，这为攻击者提供了一个极好的渗透载体，可以渗透到用户的系统中。因此，抵御这种攻击是绝对必要的。AMP 可分析电子邮件中隐藏在恶意附件中的威胁，例如零日攻击和窃取恶意软件。此外，它还利用行业领先的 URL 智能来打击恶意链路。它可以为用户提供高级保护，防止他们遭受鱼叉式网络攻击，勒索软件和其他复杂攻击。
- * 下一代入侵防护系统（NGIP）。 * Cisco Firepower NGIP 可以部署为数据中心的物理设备，也可以部署为 VMware 的虚拟设备（NGIPSv for VMware）。这种高效的入侵防护系统可提供可靠的性能和较低的总拥有成本。威胁保护可以通过可选的订阅许可证进行扩展，以提供 AMP ，应用程序可见性和控制以及 URL 筛选功能。虚拟化的 NGIP 可检查虚拟机（VM）之间的流量，并使在资源有限的站点上部署和管理 NGIP 解决方案变得更加轻松，从而增强对物理和虚拟资产的保护。

"接下来： FlexPod Cisco 网络和 FIPS 140-2 。"

FlexPod Cisco 网络和 FIPS 140-2

"先前版本： FlexPod Cisco UCS 计算和 FIPS 140-2 。"

Cisco MDS

使用软件 8.4.x 的 Cisco MDS 9000 系列平台为 "符合 FIPS 140-2"。Cisco MDS 可为 SNMPv3 和 SSH 实施加密模块和以下服务。

- 支持每个服务的会话建立
- 支持每个服务密钥派生功能的所有底层加密算法
- 每个服务的哈希
- 为每个服务提供对称加密

在启用 FIPS 模式之前，请在 MDS 交换机上完成以下任务：

1. 使密码长度至少为八个字符。
2. 禁用 Telnet 。用户应仅使用 SSH 登录。

3. 禁用通过 RADIUS/TACACS+ 进行远程身份验证。只能对交换机本地的用户进行身份验证。
4. 禁用 SNMP v1 和 v2 。交换机上为 SNMPv3 配置的任何现有用户帐户只能配置 SHA 以进行身份验证，并配置 AES/3DES 以保证隐私。
5. 禁用 VRRP 。
6. 删除具有用于身份验证的 MD5 或用于加密的 DES 的所有 ike 策略。修改策略，使其使用 SHA 进行身份验证，并使用 3DES/AES 进行加密。
7. 删除所有 SSH 服务器 RSA1 密钥对。

要启用 FIPS 模式并在 MDS 交换机上显示 FIPS 状态，请完成以下步骤：

1. 显示 FIPS 状态。

```
MDSSwitch# show fips status
FIPS mode is disabled
MDSSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. 设置 2048 位 SSH 密钥。

```
MDSSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
MDSSwitch(config)# no ssh key
MDSSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
MDSSwitch(config)# ssh key
dsa   rsa
MDSSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. 启用 FIPS 模式。

```
MDSSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
```

4. 显示 FIPS 状态。

```
MDSSwitch(config)# show fips status
FIPS mode is enabled
MDSSwitch(config)# feature ssh
MDSSwitch(config)# show feature | grep ssh
sshServer            1        enabled
```

5. 将配置保存到正在运行的配置中。

```
MDSSwitch(config)# copy ru st
[##########################################] 100%
exitCopy complete.
MDSSwitch(config)# exit
```

6. 重新启动 MDS 交换机

```
MDSSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

7. 显示 FIPS 状态。

```
Switch(config)# fips mode enable
Switch(config)# show fips status
```

有关详细信息，请参见 "启用 FIPS 模式"。

Cisco Nexus

Cisco Nexus 9000 系列交换机（ 9.3 版） "符合 FIPS 140-2"。Cisco Nexus 为 SNMPv3 和 SSH 实施加密模块和以下服务。

- 支持每个服务的会话建立
- 支持每个服务密钥派生功能的所有底层加密算法

- 每个服务的哈希
- 为每个服务提供对称加密

在启用 FIPS 模式之前，请在 Cisco Nexus 交换机上完成以下任务：

1. 禁用 Telnet 。用户应仅使用安全 Shell （ SSH ）登录。
2. 禁用 SNMPv1 和 v2 。设备上已配置 SNMPv3 的任何现有用户帐户只能配置 SHA 进行身份验证，并配置 AES/3DES 以保证隐私。
3. 删除所有 SSH 服务器 RSA1 密钥对。
4. 启用 HMAC-SHA1 消息完整性检查（ Message Integrity Checking ，麦克风），以便在 Cisco TrustSec 安全关联协议（ SAP ）协商期间使用。要执行此操作，请在 `CTS-manual` 或 `CTS-dot1x` 模式中输入 SAP hash-orolor `HMAC-SHA-1` 命令。

要在 Nexus 交换机上启用 FIPS 模式，请完成以下步骤：

1. 设置 2048 位 SSH 密钥。

```
NexusSwitch# show fips status
FIPS mode is disabled
NexusSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. 设置 2048 位 SSH 密钥。

```
NexusSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
NexusSwitch(config)# no ssh key
NexusSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
NexusSwitch(config)# ssh key
dsa   rsa
NexusSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. 启用 FIPS 模式。

```
NexusSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
Show fips status
NexusSwitch(config)# show fips status
FIPS mode is enabled
NexusSwitch(config)# feature ssh
NexusSwitch(config)# show feature | grep ssh
sshServer            1        enabled
Save configuration to the running configuration
NexusSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
NexusSwitch(config)# exit
```

4. 重新启动 Nexus 交换机。

```
NexusSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

5. 显示 FIPS 状态。

```
NexusSwitch(config)# fips mode enable
NexusSwitch(config)# show fips status
```

此外， Cisco NX OS 软件还支持可增强网络异常检测和安全性的网络流功能。网络流可捕获网络上每个对话的元数据，通信所涉及的各方，正在使用的协议以及事务持续时间。对信息进行汇总和分析后，可以深入了解正常行为。通过收集的数据，还可以确定可疑的活动模式，例如恶意软件在网络中传播，否则可能会被忽视。网络流使用流为网络监控提供统计信息。流量是指到达源接口（或 VLAN ）且密钥值相同的单向数据包流。密钥是指数据包中某个字段的标识值。您可以使用流记录创建流，以便为流定义唯一密钥。您可以使用流量导出器将网络流为流收集的数据导出到远程网络流收集器，例如 Cisco Stealthwatch 。Stealthwatch 使用此信息持续监控网络，并在发生勒索软件爆发时提供实时威胁检测和意外事件响应取证。

"接下来： FlexPod NetApp ONTAP 存储和 FIPS 140-2 。"

FlexPod NetApp ONTAP 存储和 FIPS 140-2

"先前版本： FlexPod Cisco 网络和 FIPS 140-2 。"

NetApp 提供各种硬件，软件和服务，其中可以包括根据标准验证的加密模块的各种组件。因此， NetApp 使用多种方法在控制平面和数据平面上实现 FIPS 140-2 合规性：

- NetApp 提供的加密模块已通过传输中数据加密和空闲数据加密的 1 级验证。
- NetApp 收购的硬件和软件模块均已通过这些组件供应商的 FIPS 140-2 验证。例如， NetApp 存储加密解决方案 利用经过 FIPS 级别 2 验证的驱动器。
- NetApp 产品可以使用符合标准的经验证模块，即使该产品或功能不在验证范围内也是如此。例如， NetApp 卷加密（ NVE ）符合 FIPS 140-2 标准。虽然未单独进行验证，但它会利用经过 1 级验证的 NetApp 加密模块。要了解您的 ONTAP 版本的合规性详情，请联系您的 FlexPod SME 。
- NetApp 加密模块已通过 FIPS 140-2 1 级验证 *
- NetApp 加密安全模块（ NetApp Cryptographic Security Module ， NCSM ）已通过 FIPS 140-2 1 级验证。
- NetApp 自加密驱动器已通过 FIPS 140-2 2 级认证 *

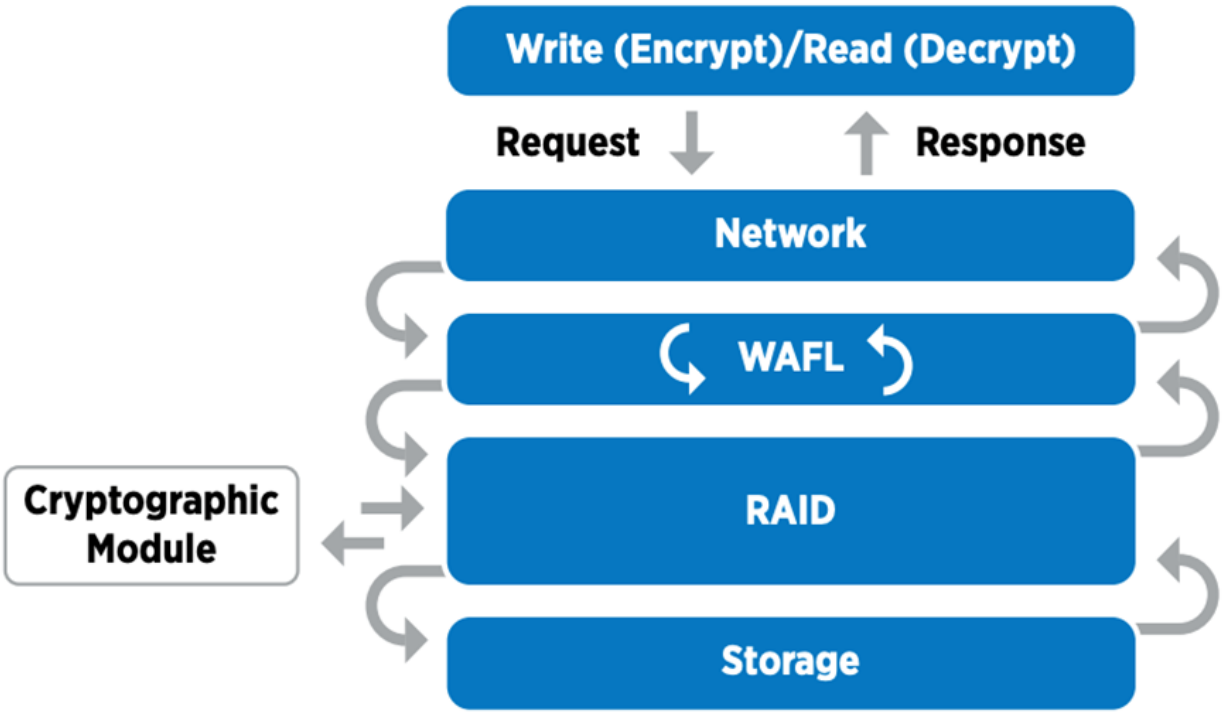
NetApp 购买的自加密驱动器（ SED ）已经过原始设备制造商（ OEM ）的 FIPS 140-2 验证；需要这些驱动器的客户必须在订购时指定这些驱动器。驱动器在级别 2 进行验证。以下 NetApp 产品可以利用经验证的 SED ：

- AFF A 系列和 FAS 存储系统
- E 系列和 EF 系列存储系统
- NetApp 聚合加密和 NetApp 卷加密 *

NVE 和 NetApp 聚合加密（聚合加密， NAE ）技术分别在卷和聚合级别加密数据，使解决方案 与物理驱动器无关。

NVE 是一种基于软件的空闲数据加密解决方案 ，从 ONTAP 9.1 开始提供，自 ONTAP 9.2 起已符合 FIPS 140-2 标准。通过 NVE ， ONTAP 可以对每个卷的数据进行精细加密。ONTAP 9.6 附带的 NAE 是 NVE 的一种增长；它允许 ONTAP 对每个卷的数据进行加密，并且这些卷可以在聚合中共享密钥。NVE 和 NAE 都使用 AES 256 位加密。数据也可以存储在没有 SED 的磁盘上。通过 NVE 和 NAE ，即使启用了加密，您也可以使用存储效率功能。纯应用程序层加密会使存储效率的所有优势失败。使用 NVE 和 NAE 可以保持存储效率，因为数据通过 NetApp WAFL 从网络传入 RAID 层，而 RAID 层决定了数据是否应加密。为了提高存储效率，您可以将聚合重复数据删除与 NAE 结合使用。NVE 卷和 NAE 卷可以同时位于同一 NAE 聚合上。NAE 聚合不支持未加密的卷。

此过程的工作原理如下：对数据进行加密后，它会发送到经过 FIPS 140-2 1 级验证的加密模块。加密模块对数据进行加密并将其发送回 RAID 层。然后，加密数据将发送到磁盘。因此，结合使用 NVE 和 NAE 时，数据在传输到磁盘的过程中已加密。读取操作遵循反向路径。换言之，数据离开磁盘时会进行加密，发送到 RAID ，并通过加密模块进行解密，然后再发送到堆栈的其余部分，如下图所示。



NVE 使用经过 FIPS 140-2 1 级验证的软件加密模块。

有关 NVE 的详细信息，请参见 "NVE 产品规格"。

NVE 可保护云中的数据。Cloud Volumes ONTAP 和 Azure NetApp Files 能够提供 FIPS 140-2 合规的空闲数据加密。

从 ONTAP 9.7 开始，如果您拥有 NVE 许可证以及板载或外部密钥管理，则新创建的聚合和卷会默认加密。从 ONTAP 9.6 开始，您可以使用聚合级别的加密为要加密的卷的所属聚合分配密钥。默认情况下，您在聚合中创建的卷会进行加密。对卷进行加密时，您可以覆盖默认值。

ONTAP NAE 命令行界面命令

在运行以下命令行界面命令之前，请确保集群具有所需的 NVE 许可证。

要创建聚合并对其进行加密，请运行以下命令（在 ONTAP 9.6 及更高版本的集群命令行界面上运行时）：

```
fp-health::> storage aggregate create -aggregate aggregatename -encrypt
-with-aggr-key true
```

要将非 NAE 聚合转换为 NAE 聚合，请运行以下命令（在 ONTAP 9.6 及更高版本的集群命令行界面上运行时）：

```
fp-health::> storage aggregate modify -aggregate aggregatename  -node
svmname -encrypt-with-aggr-key true
```

要将 NAE 聚合转换为非 NAE 聚合，请运行以下命令（在 ONTAP 9.6 及更高版本的集群命令行界面上运行时）：

```
fp-health::> storage aggregate modify -aggregate aggregatename -node
svmname -encrypt-with-aggr-key false
```

ONTAP NVE 命令行界面命令

从 ONTAP 9.6 开始，您可以使用聚合级别的加密为要加密的卷的所属聚合分配密钥。默认情况下，您在聚合中创建的卷会进行加密。

要在启用了 NAE 的聚合上创建卷，请运行以下命令（在 ONTAP 9.6 及更高版本的集群命令行界面上运行时）：

```
fp-health::> volume create -vserver svmname -volume volumename -aggregate
aggregatename -encrypt true
```

要在不移动卷的情况下对现有卷进行 " 原位 " 加密，请运行以下命令（在 ONTAP 9.6 及更高版本的集群命令行界面上运行时）：

```
fp-health::> volume encryption conversion start -vserver svmname -volume
volumename
```

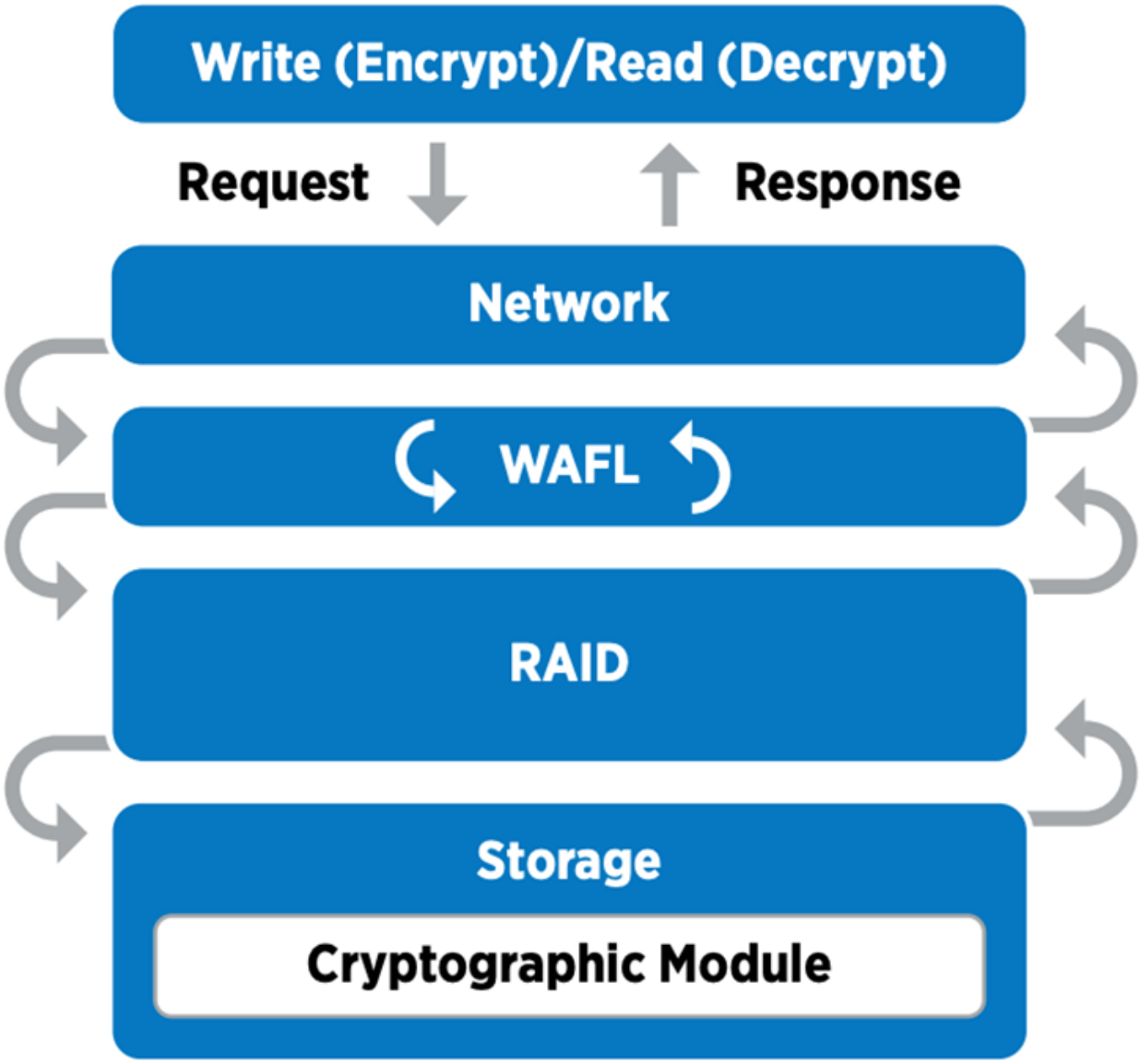
要验证是否已为卷启用加密，请运行以下命令行界面命令：

```
fp-health::> volume show -is-encrypted true
```

NSE

NSE 使用 SED 通过硬件加速机制执行数据加密。

NSE 配置为使用 FIPS 140-2 2 级自加密驱动器，通过 AES 256 位透明磁盘加密来保护空闲数据，从而有利于合规性和备用磁盘返回。驱动器在内部执行所有数据加密操作，如下图所示，包括生成加密密钥。为了防止未经授权访问数据，存储系统必须使用首次使用驱动器时建立的身份验证密钥向驱动器进行身份验证。



NSE 会在每个驱动器上使用硬件加密，此加密已通过 FIPS 140-2 2 级别 2 验证。

有关 NSE 的详细信息，请参见 "NSE 产品规格"。

密钥管理

FIPS 140-2 标准适用场景 边界定义的加密模块，如下图所示。

2.1.1 Cryptographic Boundary

The logical cryptographic boundary of the CryptoMod module is the cryptomod_fips.ko component of ONTAP OS kernel. The logical boundary is depicted in the block diagram below. The Approved DRBG is used to supply the module's cryptographic keys. The physical boundary for the module is the enclosure of the NetApp controller.

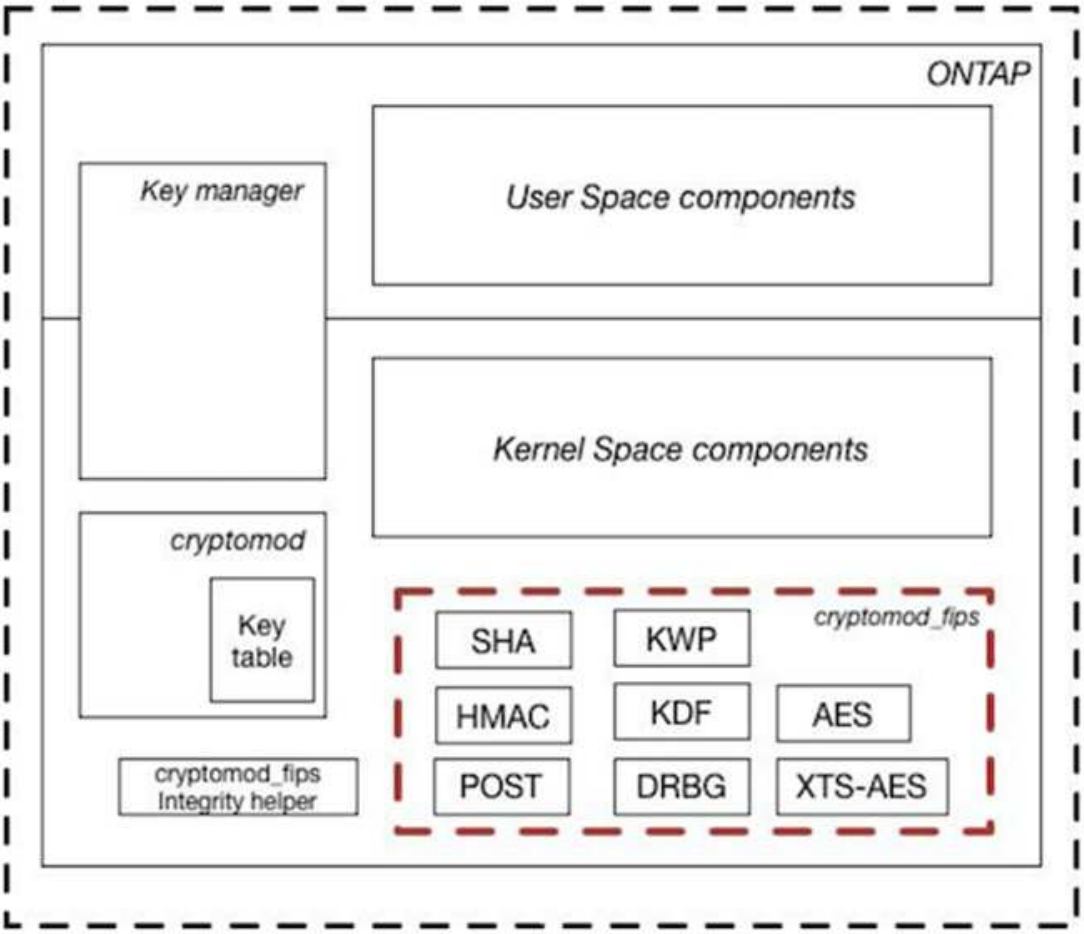


Figure 1 - Block Diagram

密钥管理器会跟踪 ONTAP 使用的所有加密密钥。NSE SED 使用密钥管理器为 NSE SED 设置身份验证密钥。使用密钥管理器时， NVE 和 NAE 解决方案 的组合由软件加密模块，加密密钥和密钥管理器组成。对于每个卷， NVE 使用唯一的 XTS-AES 256 数据加密密钥，该密钥由密钥管理器存储。用于数据卷的密钥对于该集群中的数据卷是唯一的，它是在创建加密卷时生成的。同样， NAE 卷在每个聚合中使用唯一的 XTS-AES 256 数据加密密钥，密钥管理器也会存储这些密钥。创建加密聚合时会生成 NAE 密钥。ONTAP 不会对密钥执行重新生成，重复使用或以纯文本格式显示—它们由密钥管理器存储和保护。

支持外部密钥管理器

从 ONTAP 9.3 开始， NVE 和 NSE 解决方案均支持外部密钥管理器。FIPS 140-2 标准适用场景 —特定供应商实施中使用的加密模块。大多数情况下， FlexPod 和 ONTAP 客户会使用以下经过验证（根据 "NetApp 互操作性表"）密钥管理器：

- Gemalto 或 SafeNet ，网址为
- Vormetric （ Thales ）
- IBM SKLM

- Utimaco （原 MicroFocus ， HPE ）

NSE 和 NVMe SED 身份验证密钥可使用行业标准 OASIS 密钥管理互操作性协议（ KMIP ）备份到外部密钥管理器。只有存储系统，驱动器和密钥管理器才能访问此密钥，如果将此驱动器移至安全域之外，则无法解锁，从而防止数据泄露。外部密钥管理器还存储 NVE 卷加密密钥和 NAE 聚合加密密钥。如果控制器和磁盘已移动，并且无法再访问外部密钥管理器，则 NVE 和 NAE 卷将无法访问，并且无法解密。

以下示例命令会将两个密钥管理服务器添加到 Storage Virtual Machine （ SVM ） `svmname1` 的外部密钥管理器所使用的服务器列表中。

```
fp-health::> security key-manager external add-servers -vserver svmname1
-key-servers 10.0.0.20:15690, 10.0.0.21:15691
```

在多租户情形中使用 FlexPod 数据中心时， ONTAP 会在 SVM 级别为用户提供租户隔离，以确保安全。

要验证外部密钥管理器列表，请运行以下命令行界面命令：

```
fp-health::> security key-manager external show
```

将加密结合使用实现双重加密（分层防护）

如果您需要隔离对数据的访问并确保数据始终受到保护，则 NSE SED 可以与网络或网络结构级加密结合使用。如果管理员忘记配置或错误配置更高级别的加密，则 NSE SED 就像一个后备站。对于两个不同的加密层，您可以将 NSE SED 与 NVE 和 NAE 结合使用。

NetApp ONTAP 集群范围控制面板 FIPS 模式

NetApp ONTAP 数据管理软件具有 FIPS 模式配置，可为客户实例化更高的安全性级别。此 FIPS 模式仅对控制平面进行适用场景 。根据 FIPS 140-2 的关键要素启用 FIPS 模式后，传输层安全 v1 （ Transport Layer Security v1 ， TLSv1 ）和 SSLv3 将被禁用，只有 TLS v1.1 和 TLS v1.2 保持启用状态。

> FIPS 模式下的 ONTAP 集群范围控制窗格符合 FIPS 140-2 1 级标准。集群范围的 FIPS 模式使用 NCSM 提供的基于软件的加密模块。

集群范围控制平面的 FIPS 140-2 合规模式可保护 ONTAP 的所有控制接口。默认情况下，仅 FIPS 140-2 模式处于禁用状态；但是，您可以通过将 `security config modify` 命令的 `is-fips-enabled` 参数设置为 `true` 来启用此模式。

要在 ONTAP 集群上启用 FIPS 模式，请运行以下命令：

```
fp-health::> security config modify -interface SSL -is-fips-enabled true
```

启用 SSL FIPS 模式后，从 ONTAP 到外部客户端或 ONTAP 外部服务器组件的 SSL 通信将对 SSL 使用 FIPS 兼容加密。

要显示整个集群的 FIPS 状态，请运行以下命令：

```
fp-health::> set advanced
fp-health::*> security config modify -interface SSL -is-fips-enabled true
```

"接下来： FlexPod 融合基础架构的解决方案 优势。"

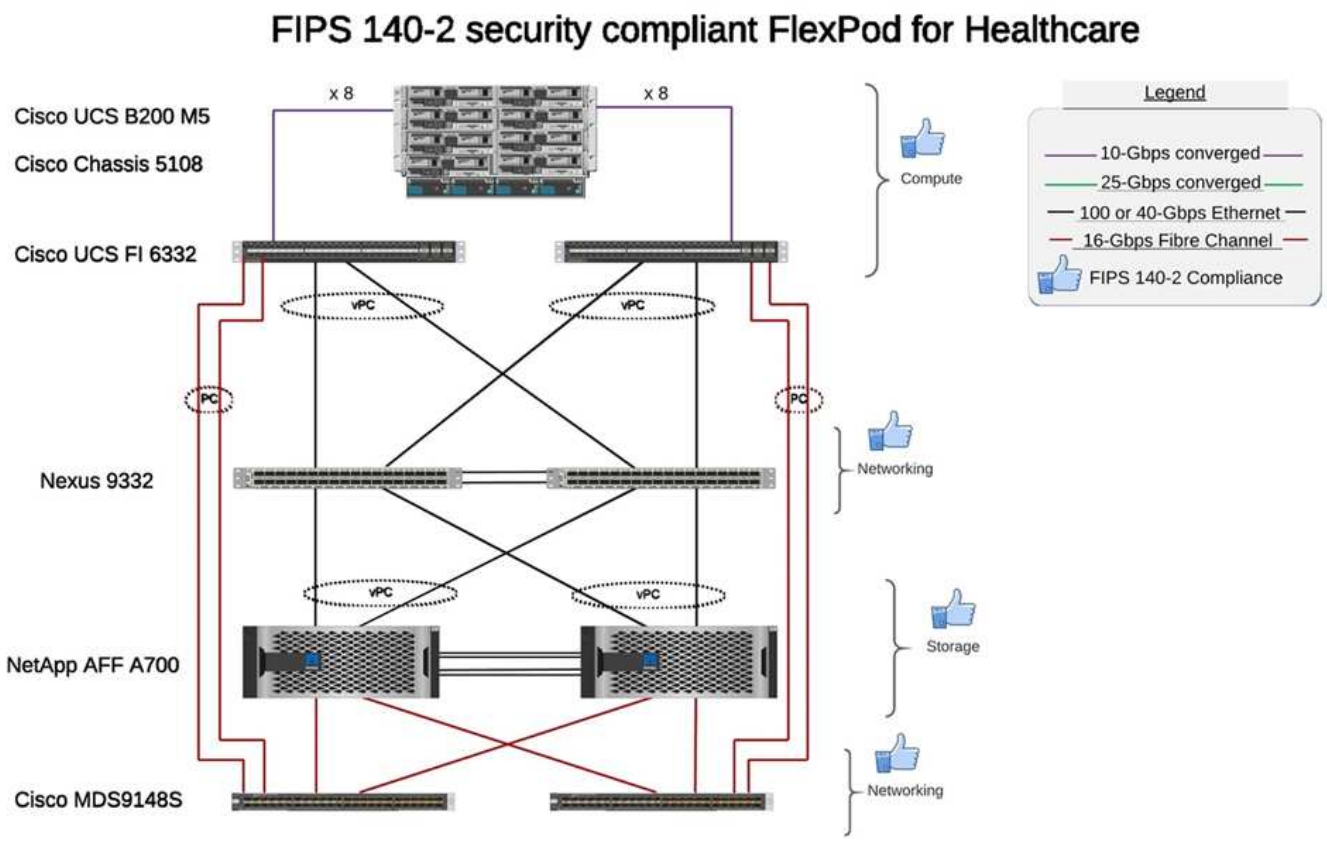
FlexPod 融合基础架构的解决方案 优势

"先前版本： FlexPod NetApp ONTAP 存储和 FIPS 140-2 。"

医疗保健组织拥有多个任务关键型系统。其中两个最关键的系统是电子健康记录（ EHR ）系统和医学影像系统。为了演示 FlexPod 系统上的 FIPS 设置，我们在 FlexPod 系统上使用了开源 EHR 和开源图片归档和通信系统（ PACS ）系统进行实验室设置和工作负载验证。有关 EHR 功能， EHR 逻辑应用程序组件以及在 FlexPod 系统上实施 EHR 系统时如何获益的完整列表，请参见 "TR-4881： 适用于电子健康记录系统的 FlexPod"。有关医疗成像系统功能，逻辑应用程序组件以及在 FlexPod 上实施医疗成像系统时如何受益的完整列表，请参见 "TR-4865： 适用于医疗成像的 FlexPod"。

在 FIPS 设置和工作负载验证期间，我们会运用典型医疗保健组织的工作负载特征。例如，我们采用了开源 EHR 系统，其中包括真实的患者数据访问和更改场景。此外，我们还在 `* 中执行了医疗成像工作负载，其中包括医学数字成像和通信（ Dicom ）对象。dcm` 文件格式。包含元数据的 Dicom 对象存储在文件和块存储中。此外，我们还从虚拟化 RedHat Enterprise Linux （ RHEL ）服务器中实施了多路径功能。我们会将 Dicom 对象存储在 NFS 上，使用 iSCSI 挂载 LUN 以及使用 FC 挂载 LUN 。在 FIPS 设置和验证期间，我们发现 FlexPod 融合基础架构超出了我们的预期，并且性能无缝。

下图显示了用于 FIPS 设置和验证的 FlexPod 系统。我们利用了 "采用 VMware vSphere 7.0 和 NetApp ONTAP 9.7 的 FlexPod Datacenter Cisco 验证设计（ CVD ）" 在设置过程中。



解决方案基础架构硬件和软件组件

以下两个图分别列出了在 FlexPod 上启用 FIPS 测试期间使用的硬件和软件组件。这些表中的建议仅为示例；您应与 NetApp SME 合作，确保这些组件适合您的组织。此外，请确保中支持这些组件和版本 "NetApp 互操作性表工具" （ IMT ）和 "Cisco 硬件兼容性列表（ HCL ）"。

层	产品系列	数量和型号	详细信息
计算	Cisco UCS 5108 机箱	1 或 2	
	Cisco UCS 刀片式服务器	3 个 B200 M5	每个都具有 2 个 20 或更多核心， 2.7 GHz 和 128-384 GB RAM
	Cisco UCS 虚拟接口卡（ VIC ）	Cisco UCS 1440	请参见
	2 个 Cisco UCS 互联阵列	6332	-
网络	Cisco Nexus 交换机	2 个 Cisco Nexus 9332	-
存储网络	用于通过 SMB/CIFS ，NFS 或 iSCSI 协议进行存储访问的 IP 网络	与上述相同的网络交换机	-
	通过 FC 进行存储访问	2 个 Cisco MDS 9148S	-
存储	NetApp AFF A700 全闪存存储系统	1 个集群	具有两个节点的集群

层	产品系列	数量和型号	详细信息
	磁盘架	一个 DS224C 或 NS224 磁盘架	已完全填充 24 个驱动器
	SSD	大于 24 ， 1.2 TB 或更大的容量	-

软件	产品系列	版本或版本	详细信息
各种	Linux	RHEL 7.X	-
	Windows	Windows Server 2012 R2 （64 位）	-
	NetApp ONTAP	ONTAP 9.7 或更高版本	-
	Cisco UCS 互联阵列	Cisco UCS Manager 4.1 或更高版本	-
	Cisco 以太网 3000 或 9000 系列交换机	对于 9000 系列，对于 3000 系列，则为 7.0 （3） i7 （7）或更高版本，对于 9.2 （4）或更高版本	-
	Cisco FC： Cisco MDS 9132T	8.4 （1a）或更高版本	-
	虚拟机管理程序	VMware vSphere ESXi 6.7 U2 或更高版本	-
存储	虚拟机管理程序管理系统	VMware vCenter Server 6.7 U3 （vCSA）或更高版本	-
网络	NetApp 虚拟存储控制台（VSC）	VSC 9.7 或更高版本	-
	NetApp SnapCenter	SnapCenter 4.3 或更高版本	-
	Cisco UCS Manager	4.1 （1c）或更高版本	
虚拟机管理程序	ESXi		
管理	虚拟机管理程序管理系统 VMware vCenter Server 6.7 U3 （vCSA）或更高版本		
	NetApp 虚拟存储控制台（VSC）	VSC 9.7 或更高版本	
	NetApp SnapCenter	SnapCenter 4.3 或更高版本	
	Cisco UCS Manager	4.1 （1c）或更高版本	

"接下来：其他 FlexPod 安全注意事项。"

其他 FlexPod 安全注意事项

"上一篇： FlexPod 融合基础架构的解决方案 优势。"

FlexPod 基础架构是一个模块化，融合，可选择虚拟化，可扩展（横向扩展和纵向扩展）以及经济高效的平台。借助 FlexPod 平台，您可以独立横向扩展计算，网络和存储，加快应用程序部署速度。模块化架构支持无中断运行，即使在系统横向扩展和升级活动期间也是如此。

HIT 系统的不同组件要求将数据存储在 SMB/CIFS ， NFS ， ext4 和 NTFS 文件系统中。这一要求意味着基础架构必须通过 NFS ， CIFS 和 SAN 协议提供数据访问。一个 NetApp 存储系统可以支持所有这些协议，因此不再需要采用传统的协议专用存储系统。此外，一个 NetApp 存储系统还可以支持多个命中工作负载，例如 EHRs ， PACS 或 VNA ，基因组学， VDI 等。 具有有保障且可配置的性能级别。

在 FlexPod 系统中部署时， Hit 可提供医疗保健行业特有的多项优势。下面列出了这些优势的高级问题描述：

- * FlexPod 安全性 * 。安全性是 FlexPod 系统的基础。在过去几年中，勒索软件已成为一种威胁。勒索软件是一种基于密码学的恶意软件，它使用加密技术构建恶意软件。此恶意软件可以使用对称密钥加密和非对称密钥加密来锁定受影响的数据，并要求勒索以提供密钥来对数据进行解密。要了解 FlexPod 解决方案 如何帮助缓解勒索软件等威胁，请参见 "TR-4802： 《从解决方案 到勒索软件》"。FlexPod 基础架构组件也是 "符合 FIPS 140-2"。
- * Cisco Intersight 。 * Cisco Intersight 是一款基于云的创新型管理即服务平台，可为全堆栈 FlexPod 管理和编排提供单一管理平台。Intersight 平台使用符合 FIPS 140-2 安全标准的加密模块。该平台的带外管理架构使其超出了某些标准或审计范围，例如 HIPAA 。网络上任何可识别的个人运行状况信息都不会发送到 Intersight 门户。
- * NetApp FPolicy 技术。 * NetApp FPolicy （名称文件策略的演变）是一个文件访问通知框架，用于通过 NFS 或 SMB/CIFS 协议监控和管理文件访问。这项技术已成为 ONTAP 数据管理软件的一部分已有十多年来的发展，它有助于检测勒索软件。此零信任引擎提供的安全措施超出了访问控制列表（ ACL ）中的权限范围。FPolicy 有两种操作模式：原生 和外部：
  - 原生 模式同时提供了文件扩展名的黑名单和白名单功能。
  - 外部模式与原生 模式具有相同的功能，但它还与在 ONTAP 系统外部运行的 FPolicy 服务器以及安全信息和事件管理（ Security Information and Event Management ，）系统集成。有关如何打击勒索软件的详细信息，请参见 "《与勒索软件作斗争》： 第三部分— ONTAP FPolicy ，另一款功能强大的原生 （也称为免费）工具" 博客
- * 空闲数据 * 。ONTAP 9 及更高版本提供了三种符合 FIPS 140-2 标准的空闲数据加密解决方案：
  - NSE 是一种使用自加密驱动器的硬件解决方案 。
  - NVE 是一种软件解决方案，用于对任何驱动器类型上的任何数据卷进行加密，其中每个卷都有一个唯一的密钥。
  - NAE 是一种软件解决方案，用于对任何驱动器类型上的任何数据卷进行加密，其中每个聚合都使用唯一的密钥启用数据卷。

> 从 ONTAP 9.7 开始，如果已安装名为 VE 的 NetApp NVE 许可证包，则默认情况下会启用 NAE 和 NVE 。

- * 数据正在传输 * 。从 ONTAP 9.8 开始，互联网协议安全（ Internet Protocol Security ， IPsec ）为客户端与 ONTAP SVM 之间的所有 IP 流量提供端到端加密支持。所有 IP 流量的 IPsec 数据加密包括 NFS ， iSCSI 和 SMB/CIFS 协议。IPsec 为 iSCSI 流量提供了唯一的传输加密选项。

- * 跨混合多云数据网络结构的端到端数据加密 * 。现在，使用 NSE 或 NVE 等空闲数据加密技术以及集群对等加密（ Cluster peering Encryption ， CPE ）传输数据复制流量的客户可以通过升级到 ONTAP 9.8 或更高版本并使用 IPsec 在混合多云数据网络结构中的客户端和存储之间使用端到端加密。从 ONTAP 9 开始，您可以为集群范围的控制面板接口启用 FIPS 140-2 合规模式。默认情况下，仅 FIPS 140-2 模式处于禁用状态。从 ONTAP 9.6 开始， CPe 为 ONTAP 数据复制功能（例如 NetApp SnapMirror ， NetApp SnapVault 和 NetApp FlexCache 技术）提供 TLS 1.2 AES-256 GCM 加密支持。加密可通过两个集群对等方之间的预共享密钥（ PSk ）进行设置。
- * 安全多租户 * 。支持日益增长的虚拟化服务器和存储共享基础架构需求，从而可以安全地多租户特定于设施的信息，尤其是在托管多个数据库和软件实例时。

"接下来：总结。"

结论

"先前版本：其他 FlexPod 安全注意事项。"

通过在 FlexPod 平台上运行医疗保健应用程序，支持 FIPS 140-2 的平台可以更好地保护您的医疗保健组织。FlexPod 可为计算，网络和存储等每个组件提供多层保护。FlexPod 数据保护功能可保护空闲或传输中的数据，并在需要时确保备份安全，随时准备就绪。

利用 FlexPod 预先验证的设计避免人为错误，这些设计经过 Cisco 和 NetApp 战略合作伙伴关系严格测试的融合基础架构。FlexPod 系统经过精心设计和设计，即使在计算，网络和存储层启用了 FIPS 140-2 ，也能以极低的影响提供可预测的低延迟系统性能和高可用性。这种方法可为您的 HIT 系统用户提供卓越的用户体验和最佳的响应时间。

"下一步：确认，版本历史记录以及在何处查找追加信息 。"

声明，版本历史记录以及在何处查找追加信息

"上一篇：结论。"

要了解有关本文档所述信息的更多信息，请查看以下文档和网站：

- 《 Cisco MDS 9000 系列 NX-OS 安全配置指南》

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_fips.html#task_1188151

- Cisco Nexus 9000 系列 NX-OS 安全配置指南 9.3 （ x ）版

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x/m-configuring-fips.html

- NetApp 和联邦信息处理标准（ FIPS ）出版物 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- FIPS 140-2

  https://fieldportal.netapp.com/content/902303

- 《 NetApp ONTAP 9 加固指南》

  https://www.netapp.com/us/media/tr-4569.pdf

- 《 NetApp 加密高级指南》

  https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html

- NVE 和 NAE 产品规格

  https://www.netapp.com/us/media/ds-3899.pdf

- NSE 产品规格

  https://www.netapp.com/us/media/ds-3213-en.pdf

- ONTAP 9 文档中心

  http://docs.netapp.com

- NetApp 和联邦信息处理标准（ FIPS ）出版物 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- Cisco 和 FIPS 140-2 合规性

  https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html

- NetApp 加密安全模块

  https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2648.pdf

- 适用于大中型医疗保健组织的网络安全实践

  https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

- Cisco 和加密模块验证计划（ CMVP ）

  https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=cisco&CertificateStatus=Active&ValidationYear=0

- NetApp 存储加密， NVMe 自加密驱动器， NetApp 卷加密和 NetApp 聚合加密

  https://www.netapp.com/pdf.html?item=/media/17073-ds-3898.pdf

- NetApp 卷加密和 NetApp 聚合加密

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- NetApp 存储加密

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- 适用于电子健康记录系统的 FlexPod

  https://www.netapp.com/pdf.html?item=/media/22199-tr-4881.pdf

- Data Now ： 利用云互联闪存技术提高 Epic EHR 环境的性能

  https://www.netapp.com/media/10809-cloud-connected-flash-wp.pdf

- 适用于 Epic EHR 基础架构的 FlexPod 数据中心

  https://www.netapp.com/pdf.html?item=/media/17061-ds-3683.pdf

- 《适用于 Epic EHR 的 FlexPod 数据中心部署指南》

  https://www.netapp.com/media/10658-tr-4693.pdf

- 适用于 MEDITECH 软件的 FlexPod 数据中心基础架构

  https://www.netapp.com/media/8552-flexpod-for-meditech-software.pdf

- FlexPod 标准扩展到了 MEDITECH 软件

  https://blog.netapp.com/the-flexpod-standard-extends-to-meditech-software/

- 《适用于 MEDITECH 的 FlexPod 方向性规模估算指南》

  https://www.netapp.com/pdf.html?item=/media/12429-tr4774.pdf

- 用于医学影像的 FlexPod

  https://www.netapp.com/media/19793-tr-4865.pdf

- 医疗保健领域的人工智能

  https://www.netapp.com/us/media/na-369.pdf

- FlexPod for HealthCare 可帮助您轻松实现转型

  https://flexpod.com/solutions/verticals/healthcare/

- Cisco 和 NetApp 的 FlexPod

  https://flexpod.com/

致谢

- NetApp 技术营销工程师 Abhinav Singh
- NetApp 解决方案 医疗保健（ Epic ）架构师 Brian O ' Marhony
- NetApp 追求业务开发经理 Brian Pruitt
- NetApp 高级解决方案架构师 Arvind Ramakrishnan
- NetApp 公司 FlexPod 全球现场首席技术官 Michael Hommer

版本历史记录

version	Date	文档版本历史记录
版本 1.0	2021年4月	初始版本。

Cisco Intersight与NetApp ONTAP 存储

《Cisco Intersight与NetApp存储快速入门指南》

与以下合作伙伴：

简介

NetApp 和 Cisco 合作提供 Cisco Intersight ，这是 FlexPod 生态系统的单一窗格视图。这种简化的集成为 FlexPod 基础架构和 FlexPod 解决方案中的所有组件创建了一个统一的管理平台。您可以通过 Cisco Intersight 监控 NetApp 存储， Cisco 计算和 VMware 清单。它还允许您编排或自动化工作流，以便同时完成存储和虚拟化任务。

相关信息

要了解更多信息，请参见以下文档和网站：

"TR 4883： 采用 ONTAP 9.8 的 FlexPod 数据中心，适用于 Cisco Intersight 的 ONTAP 存储连接器和 Cisco Intersight 托管模式"

"Cisco Intersight帮助中心"

"Cisco Intersight 入门概述"

"《 Intersight 设备安装和升级指南》"

新增功能

本节列出了 Cisco Intersight 与 NetApp ONTAP 存储的新增特性和功能。

2024年1月

- 使用参考工作流的NetApp存储编排现在可通过在GitHub中下载 "FlexPod Intersight工作流存储库"。有关GitHub中新参考工作流的详细信息、请参见 "用例 2： 使用参考工作流编排 NetApp 存储"。

2023年11月

- 已在用户界面的"Inventory"部分下添加NVMe命名区页面。

2023年8月

> 需要升级到NetApp Active IQ Unified Manager 9.13GA、以确保与最新版本的兼容性和完整功能。

- 改进了"新建NetApp智能LUN "任务、以明确指示可用于创建新启动程序组或选择现有启动程序组的选择选

项。现在、当用户选中用于创建新启动程序组的框时、用于选择现有启动程序组的参数不再可用。如果用户取消选中此框以创建新启动程序组、则现有启动程序组参数将变为可用。

- 增强了"New NetApp LUN Map"(新建LUN映射)和"Remove NetApp LUN Map"(删除LUN映射)任务。此时、LUN和启动程序组之间的新关系已更新。执行任务时、LUN和启动程序组的UI清单会立即更新。
- 现在、"Checks"页面将在用户首次登录时正确加载、不再需要刷新。

2023年7月

> 需要升级到NetApp Active IQ Unified Manager 9.13GA、以确保与最新版本的兼容性和完整功能。

- 已更新NetApp存储任务的名称。有关重命名任务的完整列表、请参见用例3使用无设计器表单的自定义工作流。
- 已将NFS接口IP地址添加为"新建NetApp NAS智能卷"任务的输出。
- 检查选项卡中添加了ASUP传输是否为HTTPS的检查。
- 现在、所有层的正确层类型都将正确显示在层用户界面下。
- 现在、所有合规许可证都将正确显示在许可证页面下。
- 现在、不带或不带主目录的CIFS共享的准确值将显示在共享页面上。
- 现在、已为LUN页面上的已映射列启用排序和筛选。
- 现在、通过排序和筛选、可以在NTP服务器页面上启用已启用身份验证列。
- 向"检查"选项卡添加了新检查以及以下相应类别。
  - 安全性
  - 防反防兰森
  - 可用性
  - 其他
- 在"Inventory (清单)"详细信息视图下、报告"Now Used (现在已用)"容量、而不是"Physical Used

2023年6月

> 需要升级到NetApp Active IQ Unified Manager 9.13RC1、以确保与最新版本的兼容性和完整功能。

- 已更新NetApp存储任务的名称。请参见 "使用案例 3 使用无设计人员表单的自定义工作流" 有关已重命名任务的完整列表。

2023年4月

- 在用户界面的"Inventory"部分的"Policies"页面下添加了"Protection Policies"(SnapMirror)和"Snapshot Policies"选项卡。
- 已在用户界面的"Inventory"部分下添加NFS客户端页面。
- 在用户界面的"Storage VMs"页面的"Inventory"部分下添加了"Protected "列。

- 修改了数据精简信息的报告和显示方式。
- 在用户界面的"Inventory"部分的"Tier"页面下添加了"Local Tier"和"Cloud Tier"选项卡。
- 现在、节点列会显示在用户界面的"Inventory"部分的"Ports"页面下的"Name"列后面。

2023年1月

> 要确保与最新版本的兼容性和完整功能、需要升级到NetApp Active IQ Unified Manager 9.12 GA。有关与此版本相关的已知问题列表、请参见 [已知问题]。

- 现在、在执行兼容性检查时、可以通过目视互操作性检查来区分UCSM和IMM固件模式。
- 对于ONTAP 9.7、保护关系不会显示在Intersight中。此问题描述 已在ONTAP 9.8RC1中修复。

2022年8月

> 要确保与最新版本的兼容性和完整功能、需要升级到NetApp Active IQ Unified Manager 9.11 GA。有关与此版本相关的已知问题列表、请参见 [已知问题]。

- 已更新集群可用容量计算以匹配System Manager
- 已更新集群常规页面、以隐藏性能指标摘要、直到填充性能数据为止
- 修复了偶尔导致页面挂起的集群常规页面UI问题描述
- 已将CIFS共享、CIFS服务、qtree和SVM SnapMirror策略添加到后端清单。
- 已将共享和qtree添加到逻辑清单部分下的UI导航菜单中
- 已从选定Storage VM中将共享添加为选项卡
- 如果Storage VM已启用CIFS、则会在Storage VM的常规选项卡上添加CIFS服务信息
- 添加了一个集群检查页面、可用于使用户验证NetApp存储系统的配置是否符合最佳实践

2022年7月

- 容量小工具中现在提供了改进的集群数据精简率视觉效果
- 已将FC接口选项卡添加到网络接口页面
- 现在、使用通用的"新存储卷"任务创建新卷会将卷空间保证设置为none、并将Snapshot预留百分比设置为0%
- 现在、编辑Snapshot策略任务下的注释字段为可选字段、不再是必需字段
- 提高了UI清单和流程编排的一致性
- 集群容量下的可见容量信息现在与System Manager一致
- 已在新建Storage Virtual Machine任务下添加复选框、用于在创建新管理界面时显示所有参数以提高可用性
- 移动的协议与客户端以下的协议匹配、现在与System Manager保持一致
- 导出策略常规页面现在显示访问协议
- 现在、已有条件地记录igroup删除

- 在新存储NAS数据接口和新存储iSCSI数据接口下为NAS添加了"故障转移策略"和"自动恢复"参数
- 现在、如果未连接任何其他卷、"回滚新存储NAS智能卷"任务将删除导出策略
- 对智能卷和智能LUN任务进行了增强

2022 年 4 月

> 为了确保与未来版本兼容并提供完整的功能，建议您将 NetApp Active IQ Unified Manager 升级到 9.10P1 版。

- 已将广播域添加到以太网端口详细信息页面
- 在用户界面中将聚合和 SVM 的术语 " 聚合 " 更改为 " 层 "
- 已将术语 " 集群状态 " 更改为 " 阵列状态 "
- MTU 筛选器现在适用于 < ， > ， = ， ⇐ ， >= 字符
- 已将网络接口页面添加到集群清单
- 已将 AutoSupport 添加到集群清单
- 已将 `cdpd.enable` 选项添加到节点
- 已为 CDP 邻居添加对象
- 在 Cisco Intersight 中添加了 NetApp 工作流存储任务。请参见 "使用案例 3 使用无设计人员表单的自定义工作流" 有关 NetApp 存储任务的完整列表。

2022 年 1 月

- 为 NetApp Active IQ Unified Manager 9.10 或更高版本添加了基于事件的 Intersight 警报。

> 为了确保与未来版本兼容并提供完整的功能，建议您将 NetApp Active IQ Unified Manager 升级到 9.10 版。

- 显式设置 Storage Virtual Machine 的每个已启用协议（ true 或 false ）
- 已将 clusterHealthStatus 状态 ok-on-suppressed 映射为 OK
- 已将 " 运行状况 " 列重命名为 " 集群 " 列表页面下的 " 集群状态 " 列
- 如果集群已关闭或无法访问，则显示存储阵列 " 无法访问 "
- 已将 " 集群常规 " 页面下的 " 运行状况 " 列重命名为 " 阵列状态 " 列
- 现在， SVM 具有一个 " 卷 " 选项卡，用于显示 SVM 的所有卷
- 卷具有 Snapshot Capacity 部分
- 许可证现在可以正确显示

2021年10月

- 更新了 Cisco Intersight 中可用的 NetApp 存储任务列表。请参见 "使用案例 3 使用无设计人员表单的自定义工作流" 有关 NetApp 存储任务的完整列表。

- 已在集群列表页面下添加运行状况列。
- 现在，已在选定集群的 " 常规 " 页面下提供扩展的详细信息。
- 现在可以通过导航窗格访问 NTP 服务器表。
- 添加了一个新的传感器选项卡，其中包含 Storage Virtual Machine 的常规页面。
- VLAN 和链路聚合组摘要现在可在端口常规页面下查看。
- 在卷总容量表下添加的总数据容量列。
- 在 " 平均卷统计信息 "， " 平均 LUN 统计信息 "， " 平均聚合统计信息 "， " 平均 Storage VM 统计信息 " 和 " 平均节点统计信息 " 表下添加了 " 延迟 "， "IOPS" 和 " 吞吐量 " 列

> 以上性能指标仅适用于通过 NetApp Active IQ Unified Manager 9.9 或更高版本监控的存储阵列。

已知问题

- 如果您使用的是AIQUM 9.11或更早版本、则存储列表页面上显示的值与存储常规页面上的容量条形图之间会出现差异。要解决此问题描述 、请升级到AIQUM 9.12或更高版本、以确保显示的容量值的准确性。
- 如果您使用的是AIQUM 9.11或更早版本、则通过"集成系统"页面下的"互操作性"选项卡执行的任何检查都无法准确区分IMM和UCSM Cisco组件。要解决此问题描述 问题、请升级到AIQUM 9.12以确保正确识别所有组件。
- 为了确保在数据收集过程中不会影响可忽略存储清单数据、必须从Active IQ Unified Manager (AIQUM)中删除任何不受支持的ONTAP 集群(即ONTAP 9.7P1以下的版本)。
- 要成功完成FlexPod 集成系统互操作性查询、所有声称的目标要求AIQUM的最低版本为9.11。
- 如果使用FQDN将ONTAP 集群添加到AIQUM、则不会填充"存储清单检查"页面。用户必须使用IP地址将ONTAP 集群添加到AIQUM。

要求

验证您是否满足NetApp ONTAP存储与Cisco Intersight集成的硬件、软件和许可要求。

硬件和软件要求

这些是实施解决方案所需的最低硬件和软件组件。在任何特定解决方案实施中使用的组件可能会因客户要求而异。

组件	需求详细信息
NetApp ONTAP	ONTAP 9.7P1 及更高版本
NetApp Active IQ Unified Manager	需要最新版本的NetApp Active IQ Unified Manager (当前为9.14RC1)
NetApp 存储阵列	ONTAP 9.7P1及更高版本支持所有ONTAP ASA、AFF和FAS存储阵列
虚拟化虚拟机管理程序	vSphere 7.0及更高版本

请参见 "Cisco Intersight支持的系统" 以满足 Cisco UCS 计算组件和 UCSM 版本的最低要求。

Cisco Intersight 许可要求

思科Intersight提供基础架构服务和Cloud Orchestrator服务等服务、用于管理、自动化和优化物理存储(NetApp存储)。您可以使用这些服务来管理Cisco UCS服务器和Cisco HyperFlex系统。基础架构服务和Cloud Orchestrator服务采用基于订阅的许可模式、并具有多个层。您可以为选定订阅期限选择所需的Cisco UCS Server卷层。

许可模式

Cisco Intersight基础架构服务许可模式已得到简化，现在提供以下两层：

- *Cisco Intersight Infrastructure Services Essentials *- Essentials许可证层提供服务器管理，包括全局运行状况监控功能、清单、通过Cisco TAC-集成提供主动式支持、多因素身份验证，以及提供SDK和API访问。
- **Cisco Intersight**基础架构服务优势-优势许可证层提供高级服务器管理，具有扩展的可见性、生态系统集成、Cisco和第三方硬件和软件的自动化以及多域解决方案。

有关各个许可层所涵盖功能的详细信息，请访问 "基础架构服务许可证"。

开始之前

要从 Cisco Intersight 监控和编排 NetApp 存储，您需要在 vCenter 环境中安装 NetApp Active IQ Unified Manager 和 Cisco Intersight Assist 虚拟设备。

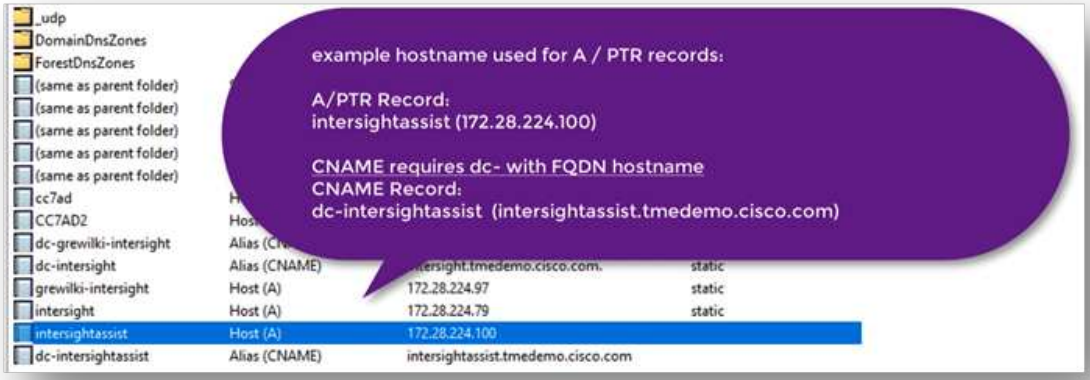
安装或升级 NetApp Active IQ Unified Manager

安装或升级到Active IQ Unified Manager (需要最新版本、当前为9.14RC1)(如果尚未安装或升级)。有关说明，请转至 "NetApp Active IQ Unified Manager 文档"。

安装 Cisco Intersight Assist 虚拟设备

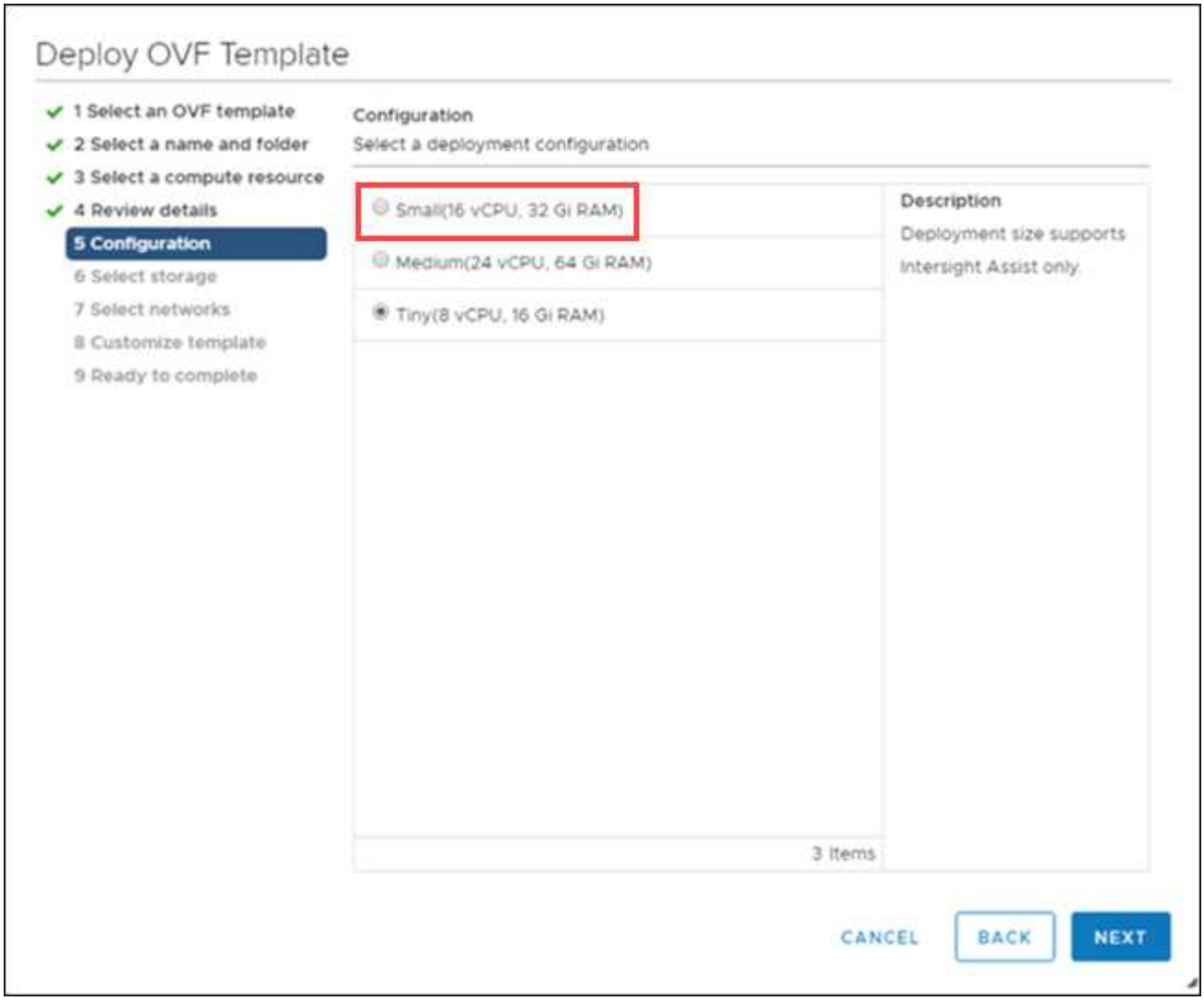
确保满足 "Cisco Intersight Virtual Appliance 许可，系统和网络要求"。

- 步骤 *
  1. 创建 Cisco Intersight 帐户。请访问 "https://intersight.com/" 以创建 Intersight 帐户。要创建 Cisco Intersight 帐户，您必须具有有效的 Cisco ID 。
  2. 从以下位置下载 Intersight 虚拟设备： "software.cisco.com"。有关详细信息，请转到 "《 Intersight 设备安装和升级指南》"。
  3. 部署 OVA 。部署 OVA 需要使用 DNS 和 NTP 。
     a. 在部署 OVA 之前，使用 A/PTR 和 CNAME 别名记录配置 DNS 。请参见以下示例。



b. 根据您对 Intersight Virtual Appliance 的 OVA 部署要求，选择适当的配置大小（小型，小型或中型）。

- 提示： * 对于包含大量存储对象的双节点 ONTAP 集群， NetApp 建议您使用小型（ 16 个 vCPU ， 32 Gi RAM ）选项。



a. 在 * 自定义模板 * 页面上，自定义 OVF 模板的部署属性。本地用户使用管理员密码： admin （WebUI/CLI/ssh ）。

b. 单击 * 下一步 * 。

   1. 部署后 Intersight Assist 设备。

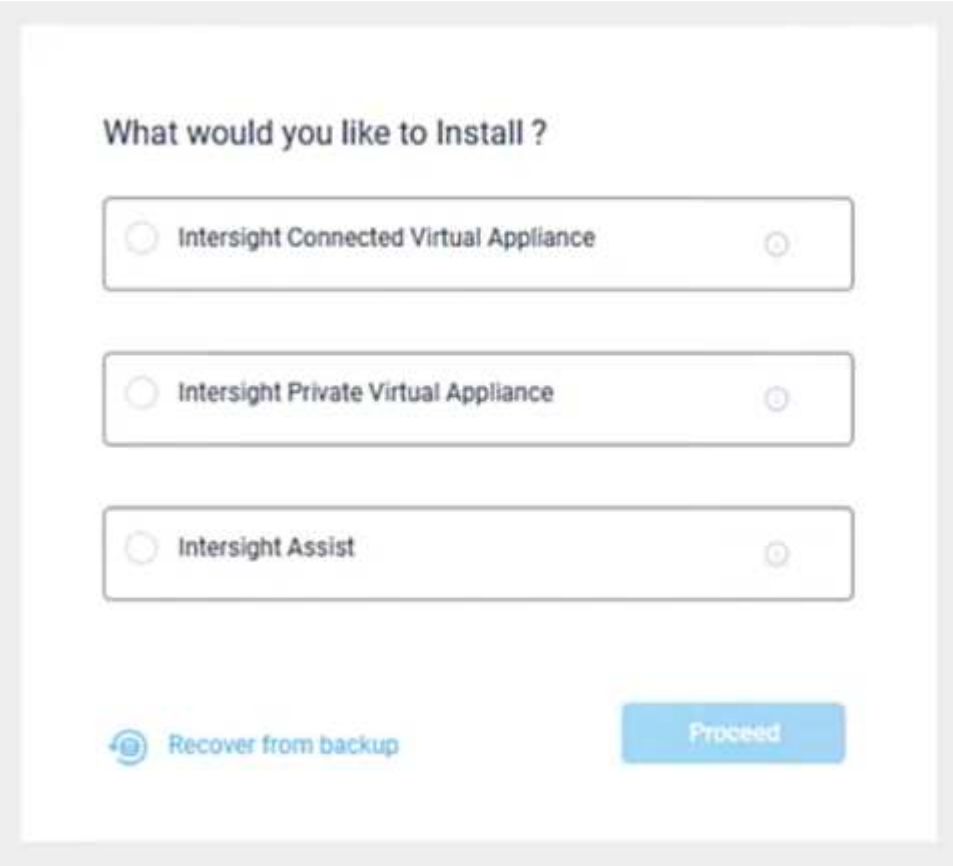
c. 导航到 https://FQDN-of-your-appliance 完成设备的安装后设置。

   安装过程将自动开始。安装可能需要长达一小时，具体取决于 Intersight.com 的带宽。在虚拟机启动后，安全站点也可能需要几秒钟的时间才能正常运行。

d. 在部署后过程中、选择以下选项：

   - * Intersight Assist 。 * 通过此部署， SaaS 模式可以连接到 Cisco Intersight 。

     选择Intersight Assist时、请记下设备ID和款项申请代码、然后再继续操作。



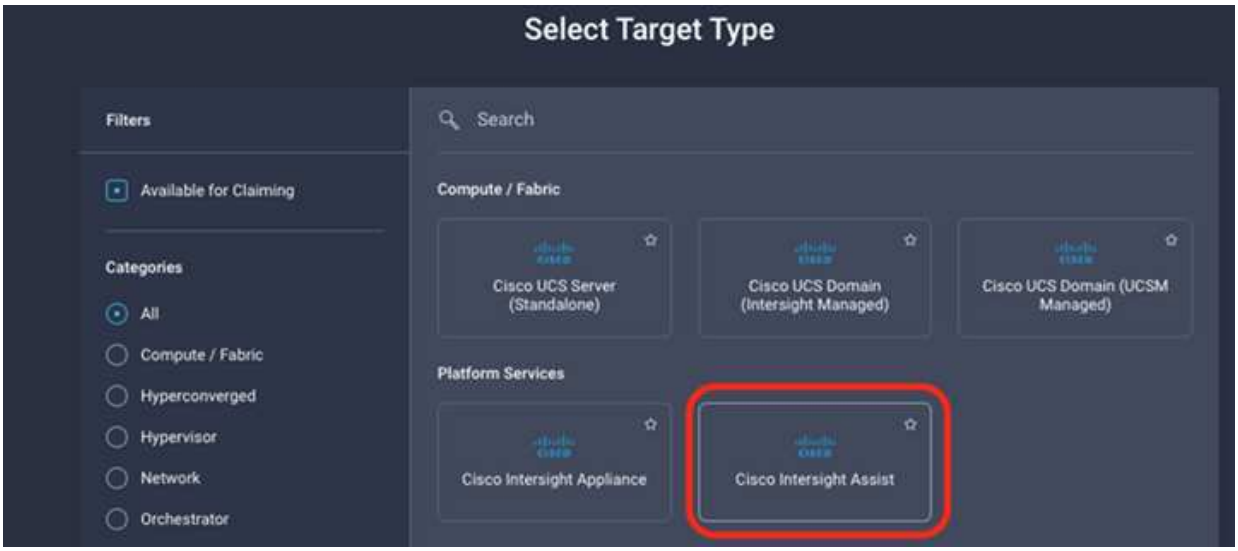
a. 单击 * 继续 * 。

b. 选择*中间视辅助*并完成以下步骤：

   i. 导航到您的 SaaS Intersight 帐户，网址为 "https://intersight.com"。

   ii. 单击 * 目标 * ， * Cisco Intersight Assist * ，然后单击 * 启动 * 。

   iii. 通过从新部署的 Intersight Assist 虚拟设备复制并粘贴设备 ID 和声明代码，申请 * Cisco Intersight assist* 设备。



iv. 返回到 * Cisco Intersight assist* 设备，然后单击 * 继续。 * 您可能需要刷新浏览器。

下载和安装过程将开始。二进制文件将从 Intersight Cloud 传输到您的内部设备。完成时间因您访问 Intersight Cloud 的带宽而异。

为IMT 服务配置AIQ UM代理服务器

如果您使用的代理服务器具有适用于Cisco Intersight的AIQ UM和NetApp ONTAP 存储、则必须通过命令行界面(CLI)配置此设置、以利用互操作性表工具服务(IMT)。IMT 服务位于*集成系统*页面的*互操作性*选项卡下。您必须使用Active IQ Unified Manager 虚拟机(OVA)诊断Shell配置AIQ UM代理服务器设置。

> 有关如何访问AIQ UM Diag Shell的信息、请参见 "如何访问Active IQ Unified Manager 虚拟机(OVA) DIAG Shell"

- 步骤 *

1. 登录到AIQ UM终端并运行以下命令以登录到um。

```
um cli login -u <um maintenance user name>
```

- 示例 *

```
um cli login -u admin
```

1. 运行以下命令、设置`IMT_proxy_host`和`IMT_proxy_port`。

> IMT 代理是一种与AutoSupport (ASUP)代理配置不同的配置。

```
um option set imt.https.proxy.host=<IMT_PROXY_HOST>
um option set imt.https.proxy.port=<IMT_PROXY_PORT>
```

- 示例 *

```
um option set imt.https.proxy.host=example-proxy.cls.eng.com
um option set imt.https.proxy.port=8200
```

> IMT 代理服务器配置不支持身份验证。

1. 通过以下命令查看IMT 代理详细信息以验证`proxy_host`和`proxy_port`设置。

```
um option list |grep imt
```

声明目标

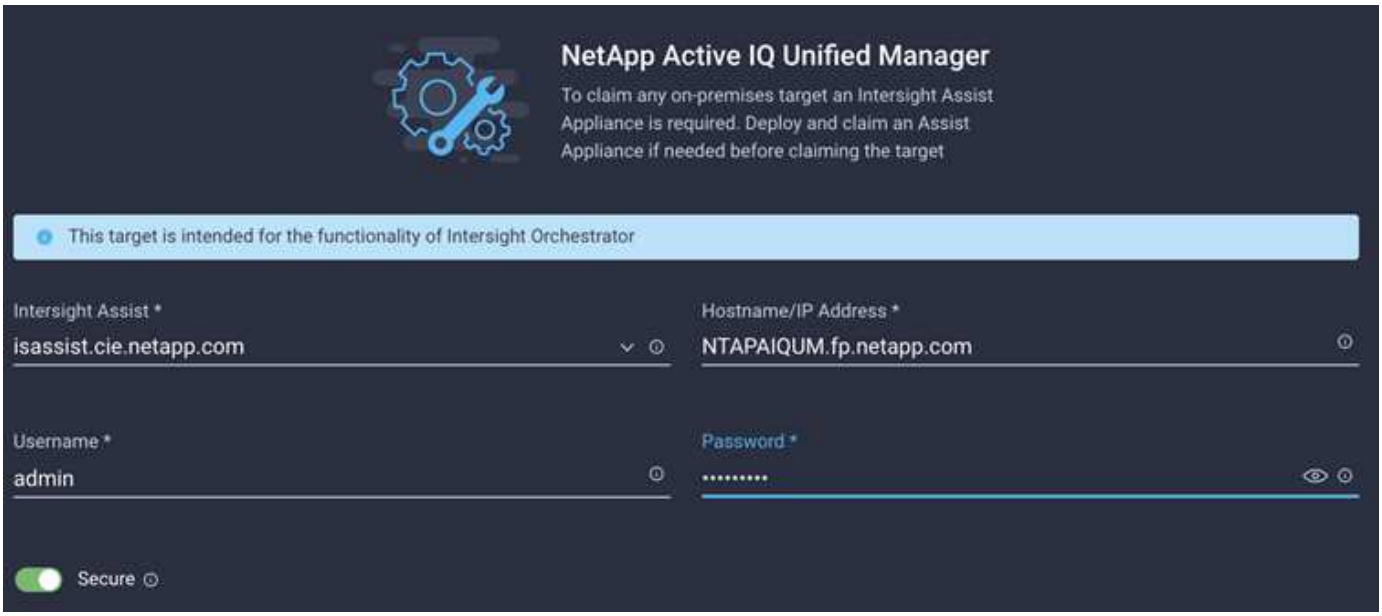
安装 Cisco Intersight Assist 后，您可以申请 NetApp 存储和虚拟化设备。返回到 "Intersight Targets* " 页面，然后添加 vCenter 和 NetApp Active IQ Unified Manager 目标。有关申请流程的详细信息，请观看视频 "通过 Cisco Intersight Assist 申请目标。"

> 确保已启用 NetApp Active IQ Unified Manager （AIQ UM） API 网关。

在NetApp IQ Unified Manager中、导航到*设置>常规>功能设置*。

以下示例显示了从 Cisco Intersight 声明的 NetApp AIQ UM 目标。

声明 NetApp AIQ UM 目标时，由 Active IQ Unified Manager 管理的所有集群都会自动添加到 Intersight 中。

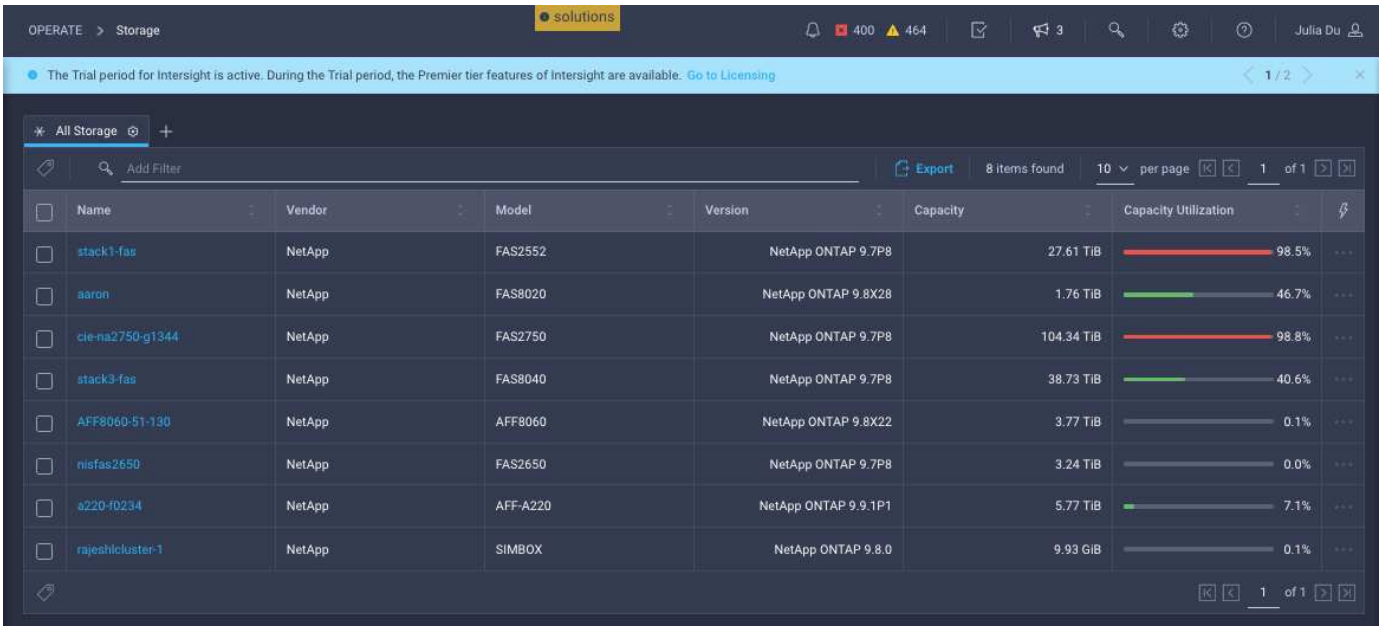


从 Cisco Intersight 监控 NetApp 存储

声明目标后，如果您拥有优势层许可证，则 NetApp 存储小工具，存储清单和虚拟化选项卡将变为可用。如果您拥有 Premier 层许可证，则可以使用业务流程选项卡。

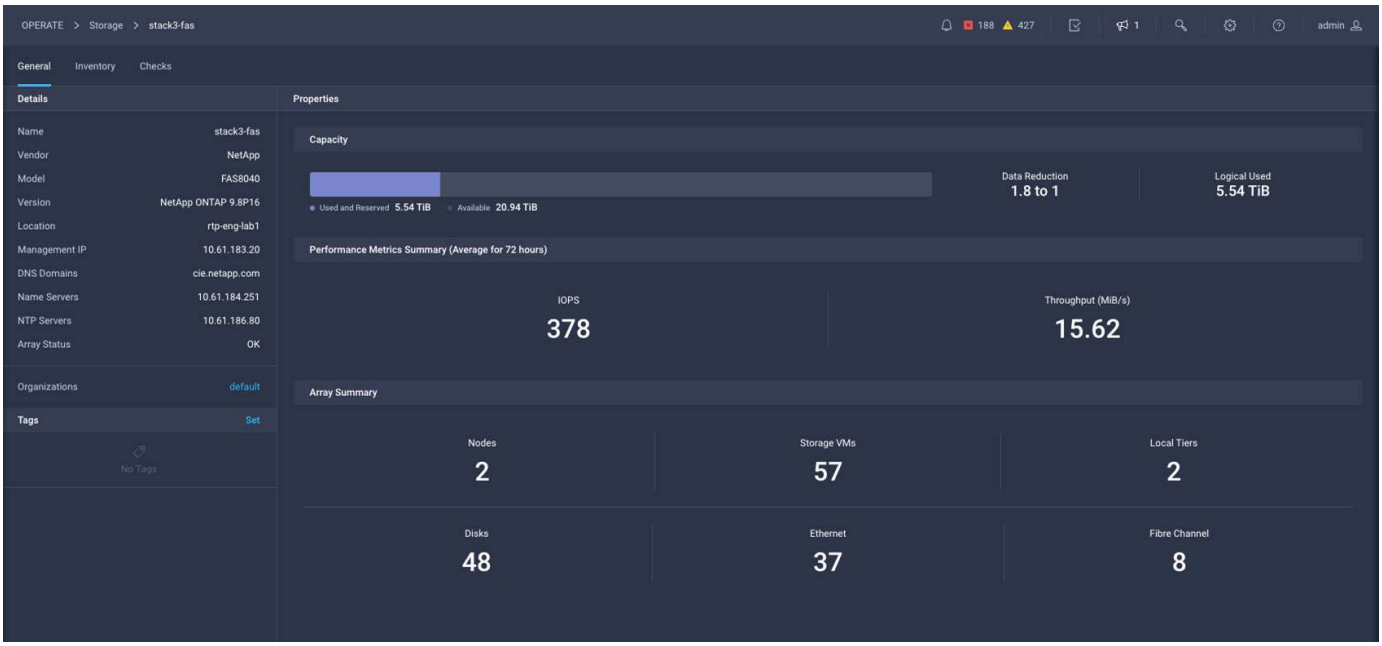
存储清单概述

以下屏幕截图显示了 * 操作 > 存储 * 屏幕。



以下屏幕截图显示了存储集群概述。

只有在通过 NetApp Active IQ Unified Manager 9.9 或更高版本监控存储阵列时，才会显示以下性能指标摘要信息。



存储小工具

要查看存储小工具，请导航到 * 监控 > 信息板 > 查看 NetApp 存储小工具 * 。

- 以下屏幕截图显示了 "Storage Version Summary" 小工具。

- 此屏幕截图显示了按容量利用率排列的前 5 个存储阵列小工具。

Top 5 Storage Arrays by Capacity Utilization

#	Name	Vendor	Capacity	Utilization
1	Warriors_Controller	NetApp	13.83 TiB	89.4%
2	stack3-fas	NetApp	8.95 TiB	66.2%
3	aaron	NetApp	4.71 TiB	44.1%
4	aff-a400	NetApp	40.62 TiB	0.2%

- 此屏幕截图显示了按容量利用率排列的前 5 个存储卷小工具。

Top 5 Storage Volumes by Capacity Utilization

#	Name	Vendor	Capacity	Utilization
1	test_1_vol	NetApp	10.31 GiB	98.6%
2	test_lun_vol	NetApp	10.31 GiB	97.9%
3	vmware_server_1	NetApp	50.00 GiB	95.0%
4	vmware_server_2	NetApp	50.00 GiB	82.3%
5	VM_Datastore_vol	NetApp	150.00 GiB	67.0%

用例

以下是从 Cisco Intersight 监控和编排 NetApp 存储的几个用例示例。

用例 1 ： 监控 NetApp 存储清单和小工具

如果 NetApp 存储环境在 Cisco Intersight 中可用，您可以从存储清单中详细监控 NetApp 存储对象，并从存储小工具中获取概览。

1. 部署 Intersight Assist OVA （ vCenter 环境中的 OnPrem 任务）。
2. 在 Intersight Assist 中添加 NetApp AIQ UM 设备。
3. 转到 * 存储 * 并浏览 NetApp 存储清单。
4. 将适用于 NetApp 存储的 * 小工具 * 添加到 * 监控信息板 * 中。

   这是一个 "链接。" 观看 Cisco Intersight 提供的 NetApp ONTAP 存储监控功能视频。

用例2：使用参考工作流的NetApp存储流程编排

如果NetApp存储和vCenter环境可在Cisco Intersight中使用、则可以通过使用GitHub中提供的端到端参考工作流"FlexPod Intersight工作流存储库"。

参考工作流包括存储和虚拟化任务。存储库的README文件提供了执行工作流所需的前提条件、指向有用资源(包括有关如何导入工作流的文档)的链接以及每个参考工作流的文档链接。

每个工作流在存储库中都有一个文件夹、其中包含两个文件：

- 要下载并导入Intersight的JSON文件、
- 一个文档文件、提供工作流中的任务视图、工作流输入以及工作流执行示例。

执行以下操作以导入和使用参考工作流：

1. 部署 Intersight Assist OVA （ vCenter 环境中的 OnPrem 任务）。
2. 在 Intersight Assist 中添加 NetApp AIQ UM 设备。
3. 通过 Intersight Assist 将 vCenter 目标添加到 Intersight 。
4. 从FlexPod-Intersight工作流存储库下载参考工作流的JSON文件。
5. 将工作流导入Intersight、然后执行工作流。

下面是GitHub FlexPod-Intersight工作流存储库中提供的工作流列表：

- 将启动程序添加到NetApp启动程序组
- NetApp卷的新导出策略
- 使用NetApp智能卷新建NAS数据存储库
- 新的NetApp FC数据接口
- 新建NetApp启动程序组

- 新的NetApp iSCSI数据接口
- 新的NetApp NAS数据接口
- 新建NetApp Storage Virtual Machine
- 使用NetApp智能LUN的新VMFS数据存储库
- 从NetApp启动程序组中删除启动程序
- 使用NetApp智能卷删除NAS数据存储库
- 删除NetApp导出策略
- 删除NetApp启动程序组
- 使用NetApp智能LUN删除VMFS数据存储库
- 使用NetApp智能卷更新NAS数据存储库
- 使用NetApp智能LUN更新VMFS数据存储库

用例 3： 使用无设计人员表单的自定义工作流

如果 NetApp 存储和 vCenter 环境在 Cisco Intersight 中可用，则可以使用 NetApp 存储和虚拟化任务构建自定义工作流。

1. 部署 Intersight Assist OVA （ vCenter 环境中的 OnPrem 任务）
2. 在 Intersight Assist 中添加 NetApp AIQ UM 设备。
3. 通过 Intersight Assist 将 vCenter 目标添加到 Intersight 。
4. 导航到 Intersight 中的 * 流程编排 * 选项卡。
5. 选择 * 创建工作流 * 。
6. 将存储和虚拟化任务添加到工作流中。

   以下是 Cisco Intersight 提供的 NetApp 存储任务：

   - 将ACL添加到NetApp CIFS共享
   - 将客户端匹配项添加到NetApp导出策略规则
   - 将导出策略添加到NetApp卷
   - 将启动程序添加到NetApp启动程序组
   - 将规则添加到NetApp导出策略
   - 将计划添加到NetApp快照策略
   - 确认NetApp许可证状态
   - 确认NetApp Storage Virtual Machine FCP协议状态
   - 编辑Storage Virtual Machine的NetApp聚合
   - 编辑NetApp异步SnapMirror策略
   - 编辑NetApp CIFS共享ACL权限
   - 编辑NetApp导出策略规则

- 编辑NetApp快照策略
- 编辑NetApp快照策略计划
- 编辑NetApp卷安全模式
- 编辑NetApp卷快照策略
- 启用NetApp CIFS服务
- 展开NetApp LUN
- 新增NetApp异步SnapMirror策略
- 新的NetApp CIFS服务器
- 新建NetApp CIFS共享
- 查找NetApp启动程序组LUN映射
- 按ID查找NetApp LUN
- 按ID查找NetApp卷
- 新建NetApp导出策略
- 新的NetApp FC数据接口
- 新建NetApp启动程序组
- 新的NetApp iSCSI数据接口
- 为SVM根卷提供了新的NetApp负载共享镜像
- 新建NetApp LUN
- 新建NetApp LUN映射
- 新的NetApp NAS数据接口
- 新建NetApp NAS智能卷
- 新建NetApp智能LUN
- 为卷创建了新的NetApp SnapMirror关系
- 新建NetApp快照策略
- 新建NetApp Storage Virtual Machine
- 新建NetApp卷
- 新建NetApp卷快照
- 为NetApp Storage Virtual Machine注册DNS
- 从NetApp CIFS共享中删除ACL
- 从NetApp导出策略规则中删除客户端匹配项
- 从NetApp卷中删除导出策略
- 从NetApp启动程序组中删除启动程序
- 删除NetApp CIFS服务器
- 删除NetApp CIFS共享

- 删除NetApp导出策略
- 删除NetApp FC数据接口
- 删除NetApp启动程序组
- 删除NetApp IP接口
- 删除SVM根卷的NetApp负载共享镜像
- 删除NetApp LUN
- 删除NetApp LUN映射
- 删除NetApp NAS智能卷
- 删除NetApp智能LUN
- 删除卷的NetApp SnapMirror关系
- 删除NetApp SnapMirror策略
- 删除NetApp快照策略
- 删除NetApp Storage Virtual Machine
- 删除NetApp卷
- 删除NetApp卷快照
- 从NetApp导出策略中删除规则
- 从NetApp快照策略中删除计划
- 重命名NetApp卷快照
- 更新SVM根卷的NetApp负载共享镜像
- 更新NetApp卷容量

要了解有关使用 NetApp 存储和虚拟化任务自定义工作流的更多信息，请观看视频 "Cisco Intersight 中的 NetApp ONTAP 存储编排"。

基础架构

采用 Cisco UCSM， VMware vSphere 7.0 和 NetApp ONTAP 9 的适用于 FlexPod 的端到端 NVMe

TR-4914：采用 Cisco UCSM， VMware vSphere 7.0 和 NetApp ONTAP 9 的适用于 FlexPod 的端到端 NVMe

NetApp 公司 Chris Schmitt 和 Kamini Singh

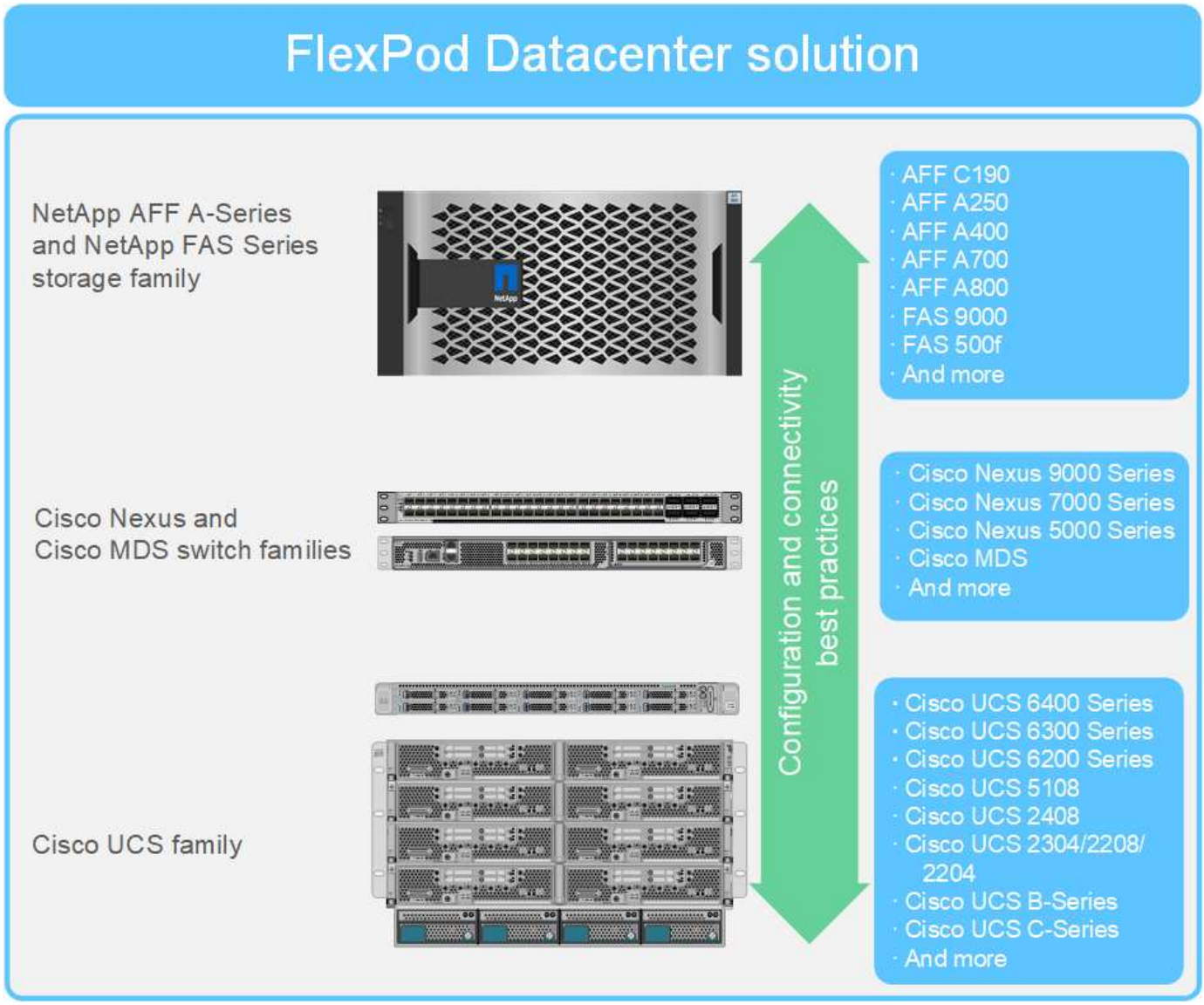
与以下合作伙伴：

NVMe 数据存储标准是一项新兴的核心技术，通过为当前和未来的内存技术提供极高的带宽和极低的延迟存储访问，正在转变企业数据存储访问和传输。NVMe 将 SCSI 命令集替换为 NVMe 命令集。

NVMe 可与非易失性闪存驱动器，多核 CPU 和 GB 内存配合使用。它还利用了自 20 世纪 70 年代以来计算机科学领域的重大进步，实现了简化的命令集，可以更高效地解析和处理数据。端到端 NVMe 架构还使数据中心管理员能够重新思考他们可以在多大程度上推动虚拟化和容器化环境，以及面向事务的数据库可以支持的可扩展性。

FlexPod 是一种最佳实践数据中心架构，其中包括 Cisco 统一计算系统（ Cisco UCS ）， Cisco Nexus 交换机， Cisco MDS 交换机和 NetApp AFF 系统。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一个出色的平台。FlexPod 可以纵向扩展以提高性能和容量（根据需要单独添加计算，网络或存储资源），也可以横向扩展以适应需要多个一致部署的环境（例如部署更多 FlexPod 堆栈）。

下图显示了 FlexPod 组件系列。



FlexPod 是推出 FC-NVMe 的理想平台。支持此功能的方法包括：在现有 Cisco UCS B200 M5 或 M6 服务器或 Cisco UCS C 系列 M5 或 M6 机架式服务器中添加 Cisco UCS VIC 1400 系列和端口扩展器；以及简单，无中断地升级到 Cisco UCS 系统 Cisco MDS 32Gbps 交换机； 和 NetApp AFF 存储阵列。安装支持的硬件和软件后， FC-NVMe 的配置与 FCP 配置类似。

NetApp ONTAP 9.5 及更高版本可提供完整的 FC-NVMe 解决方案。通过对 AFF A300 ， AFF A400 ， AFF A700 ， AFF A700s 和 AFF A800 阵列进行无中断 ONTAP 软件更新，这些设备可以支持端到端 NVMe 存储堆栈。因此，具有第六代主机总线适配器（ HBA ）和 NVMe 驱动程序支持的服务器可以使用原生 NVMe 与这些阵列进行通信。

目标

此解决方案简要概述了基于 FlexPod 的 VMware vSphere 7 的 FC-NVMe 性能。经验证，解决方案可成功传递 FC-NVMe 流量，并为具有各种数据块大小的 FC-NVMe 捕获了性能度量指标。

解决方案的优势

适用于 FlexPod 的端到端 NVMe 可为客户提供卓越的价值，并具有以下解决方案优势：

- NVMe 依赖于 PCIe ，这是一种高速，高带宽的硬件协议，比 SCSI ， SAS 和 SATA 等旧标准速度要快得多。Cisco UCS 服务器和 NetApp 存储阵列之间的高带宽，超低延迟连接，适用于大多数要求苛刻的应用程序。
- FC-NVMe 解决方案无损，可满足下一代应用程序的可扩展性要求。这些新技术包括人工智能（ AI ），机器学习（ ML ），深度学习（ DL ），实时分析和其他任务关键型应用程序。
- 通过高效利用整个堆栈中的所有资源降低 IT 成本。
- 显著缩短响应时间并提升应用程序性能，这与提高 IOPS 和吞吐量并降低延迟相对应。对于现有工作负载，解决方案可将性能提高 ~60% ，并将延迟降低 ~50% 。
- FC-NVMe 是一种简化的协议，具有出色的队列功能，尤其是在每秒 I/O 操作数（ IOPS ；即事务数更多）和并行活动数较多的情况下。
- 为 FlexPod 组件（例如 Cisco UCS ， Cisco MDS 和 NetApp AFF 存储阵列）提供无中断软件升级。无需修改应用程序。

"下一步：测试方法。"

测试方法

"上一页：简介。"

本节简要概述了 FC-NVMe on FlexPod 验证测试。其中包括测试环境 / 配置以及针对使用 VMware vSphere 7 的 FlexPod 的 FC-NVMe 执行工作负载测试所采用的测试计划。

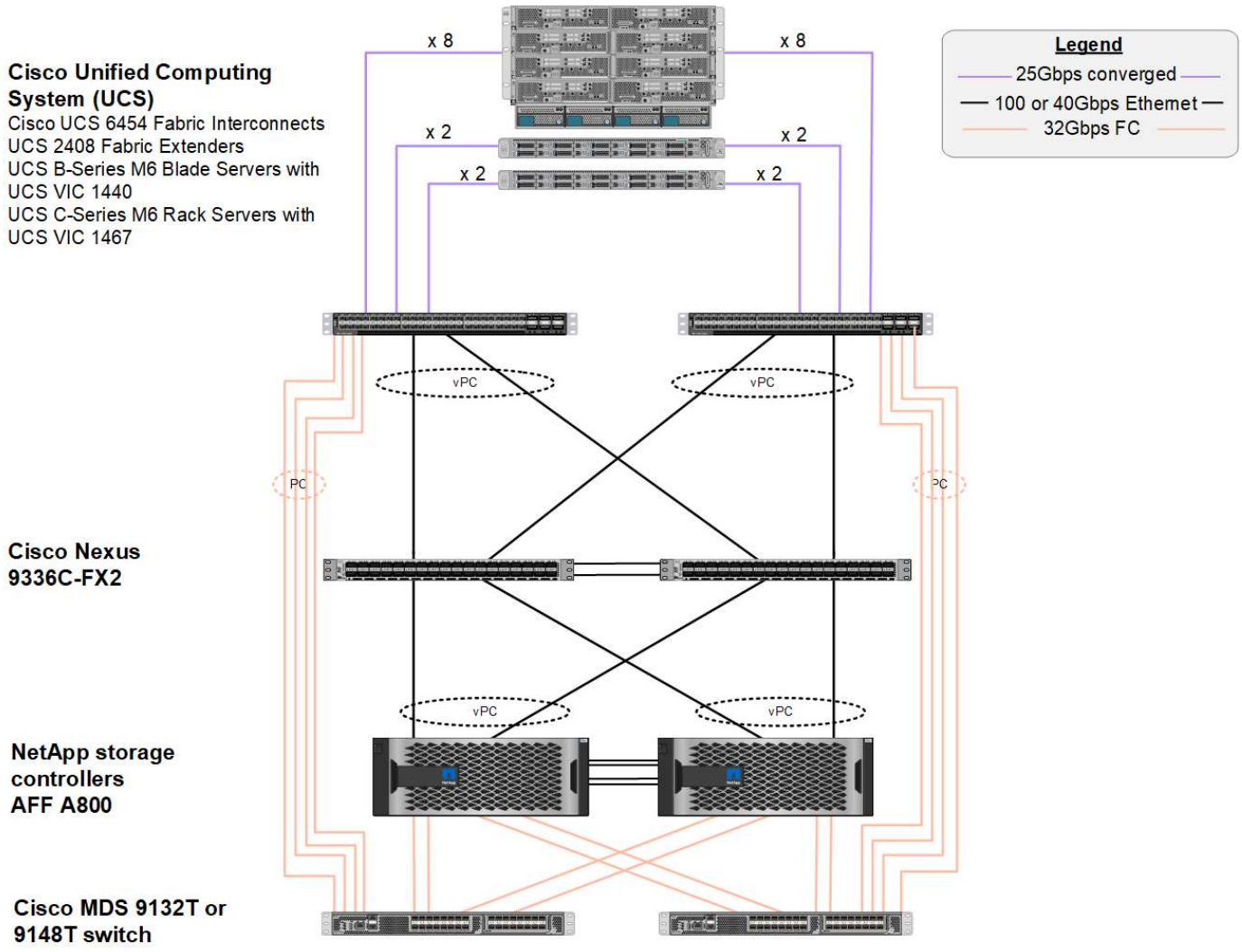
测试环境

Cisco Nexus 9000 系列交换机支持两种操作模式：

- NX-OS 独立模式，使用 Cisco NX-OS 软件
- ACI 网络结构模式，使用 Cisco Application Centric Infrastructure （ Cisco ACI ）平台

在独立模式下，交换机的性能与典型的 Cisco Nexus 交换机类似，端口密度更高，延迟低，连接速度更低。

采用 NX-OS 的 FlexPod 在计算层，网络层和存储层中设计为完全冗余。从设备或流量路径的角度来看，不存在单点故障。下图显示了此 FC-NVMe 验证中使用的最新 FlexPod 设计的各个要素的连接。



从 FC SAN 角度来看，此设计使用最新的第四代 Cisco UCS 6454 互联阵列以及在服务器中具有端口扩展器的 Cisco UCS VIC 1400 平台。Cisco UCS 机箱中的 Cisco UCS B200 M6 刀片式服务器使用 Cisco UCS VIC 1440 ，并将端口扩展器连接到 Cisco UCS 2408 阵列扩展器 IOM ，并且每个以太网光纤通道（ FCoE ）虚拟主机总线适配器（ vHBA ）的速度均为 40 Gbps 。由 Cisco UCS 管理的 Cisco UCS C220 M5 机架式服务器使用 Cisco UCS VIC 1457 ，每个互联阵列具有两个 25 Gbps 接口。每个 C220 M5 FCoE vHBA 的速度均为 50 Gbps 。

互联阵列可通过 32 Gbps SAN 端口通道连接到最新一代的 Cisco MDS 9148T 或 9132T FC 交换机。Cisco MDS 交换机与 NetApp AFF A800 存储集群之间的连接也是 32 Gbps FC 。此配置支持 32 Gbps FC ，光纤通道协议（ FCP ）以及存储集群与 Cisco UCS 之间的 FC-NVMe 存储。在此验证中，每个存储控制器使用四个 FC 连接。在每个存储控制器上，四个 FC 端口同时用于 FCP 和 FC-NVMe 协议。

Cisco Nexus 交换机与最新一代 NetApp AFF A800 存储集群之间的连接速度也为 100 Gbps ，存储控制器上具有端口通道，交换机上具有 VPC 。NetApp AFF A800 存储控制器在高速外设连接接口快速（ Peripheral Connect Interface Express ， PCIe ）总线上配备了 NVMe 磁盘。

此验证中使用的 FlexPod 实施基于 "采用 UCS 托管模式的 FlexPod Datacenter ，采用 Cisco UCS 4.2 （ 1 ）， VMware vSphere 7.0U2 和 NetApp ONTAP 9.9"。

经验证的硬件和软件

下表列出了解决方案验证过程中使用的硬件和软件版本。请注意， Cisco 和 NetApp 具有互操作性表，应参考这

些表来确定是否支持任何特定的 FlexPod 实施。有关详细信息，请参见以下资源：

- "NetApp 互操作性表工具"
- "Cisco UCS 硬件和软件互操作性工具"

层	Device	图像	注释
计算	• 两个 Cisco UCS 6454 互联阵列 • 一个 Cisco UCS 5108 刀片式服务器机箱，带有两个 Cisco UCS 2408 I/O 模块 • 四个 Cisco UCS B200 M6 刀片式服务器，每个刀片式服务器具有一个 Cisco UCS VIC 1440 适配器和端口扩展卡	4.2 版（1f）	包括 Cisco UCS Manager ， Cisco UCS VIC 1440 和端口扩展器
CPU	两个 Intel Xeon Gold 6330 CPU ，主频为 2.0 GHz ，具有 42 MB 第 3 层缓存，每个 CPU 28 个核心	–	–
内存	1024 GB （16 个 64 GB DIMM ，运行速率为 3200 MHz）	–	–
网络	两台 Cisco Nexus 9336C-x2 交换机，采用 NX-OS 独立模式	版本 9.3 （8）	–
存储网络	两个 Cisco MDS 9132T 32 Gbps 32 端口 FC 交换机	版本 8.4 （2c）	支持 FC-NVMe SAN 分析
存储	两个 NetApp AFF A800 存储控制器，具有 24 个 1.8 TB NVMe SSD	NetApp ONTAP 9.9.1.1 P1	–
软件	Cisco UCS Manager	4.2 版（1f）	–
	VMware vSphere	7.0U2	–
	VMware ESXi	7.0.2	–
	VMware ESXi 原生光纤通道 NIC 驱动程序（NFNIC）	5.0.12	在 VMware 上支持 FC-NVMe
	VMware ESXi 原生以太网 NIC 驱动程序（NENIC）	1.0.35.0	–
测试工具	光纤	3.19	–

测试计划

我们制定了一个性能测试计划，用于使用综合工作负载在 FlexPod 上验证 NVMe 。通过此工作负载，我们可以执行 8 KB 随机读取和写入以及 64 KB 读取和写入。我们使用 VMware ESXi 主机对 AFF A800 存储运行测试用例。

我们使用 FIO 这一开源合成 I/O 工具来生成综合工作负载，该工具可用于性能测量。

为了完成性能测试，我们对存储和服务器执行了几个配置步骤。以下是实施的详细步骤：

1. 在存储方面，我们创建了四个 Storage Virtual Machine （ SVM ，以前称为 Vserver ），每个 SVM 八个卷，每个卷一个命名空间。我们创建了 1 TB 卷和 960 GB 命名空间。我们为每个 SVM 创建了四个 LIF ，并为每个 SVM 创建了一个子系统。SVM LIF 均匀分布在集群上的八个可用 FC 端口之间。
2. 在服务器端，我们在每个 ESXi 主机上创建了一个虚拟机（ VM ），总共四个 VM 。我们在服务器上安装了 FIO 以运行综合工作负载。
3. 配置存储和 VM 后，我们可以从 ESXi 主机连接到存储命名空间。这样，我们就可以根据命名空间创建数据存储库，然后根据这些数据存储库创建虚拟机磁盘（ Virtual Machine Disk ， VMDK ）。

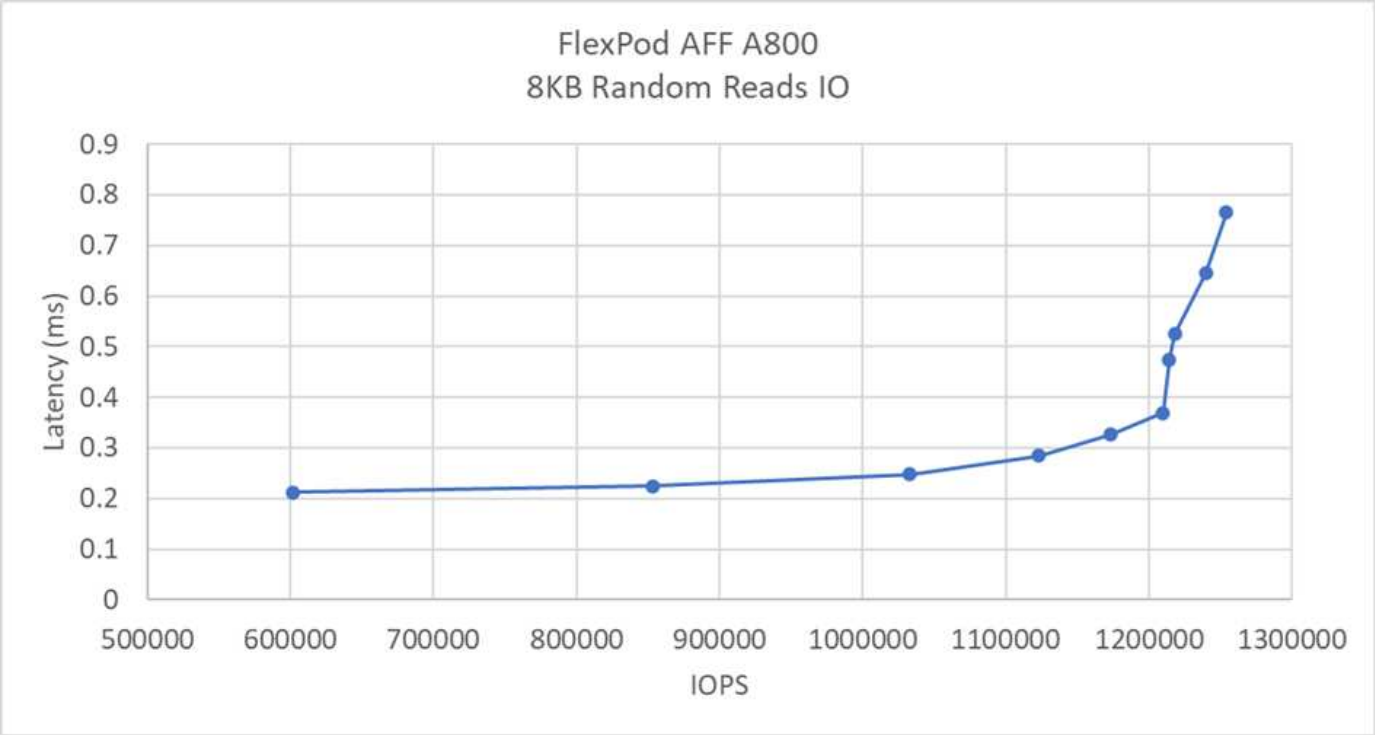
"接下来：测试结果。"

测试结果

"上一篇：测试方法。"

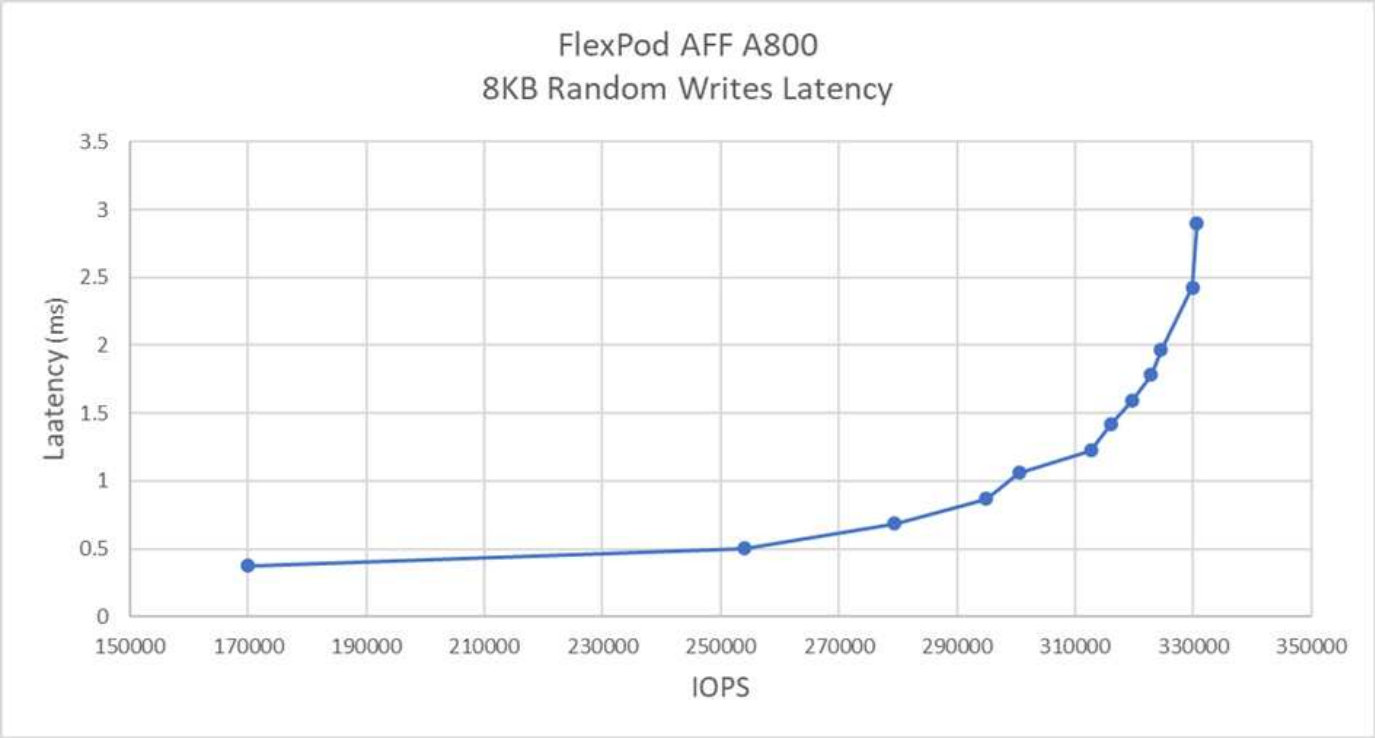
测试包括运行 FIO 工作负载，以测量 FC-NVMe 在 IOPS 和延迟方面的性能。

下图显示了我们在使用 8 KB 块大小运行 100% 随机读取工作负载时的结果。



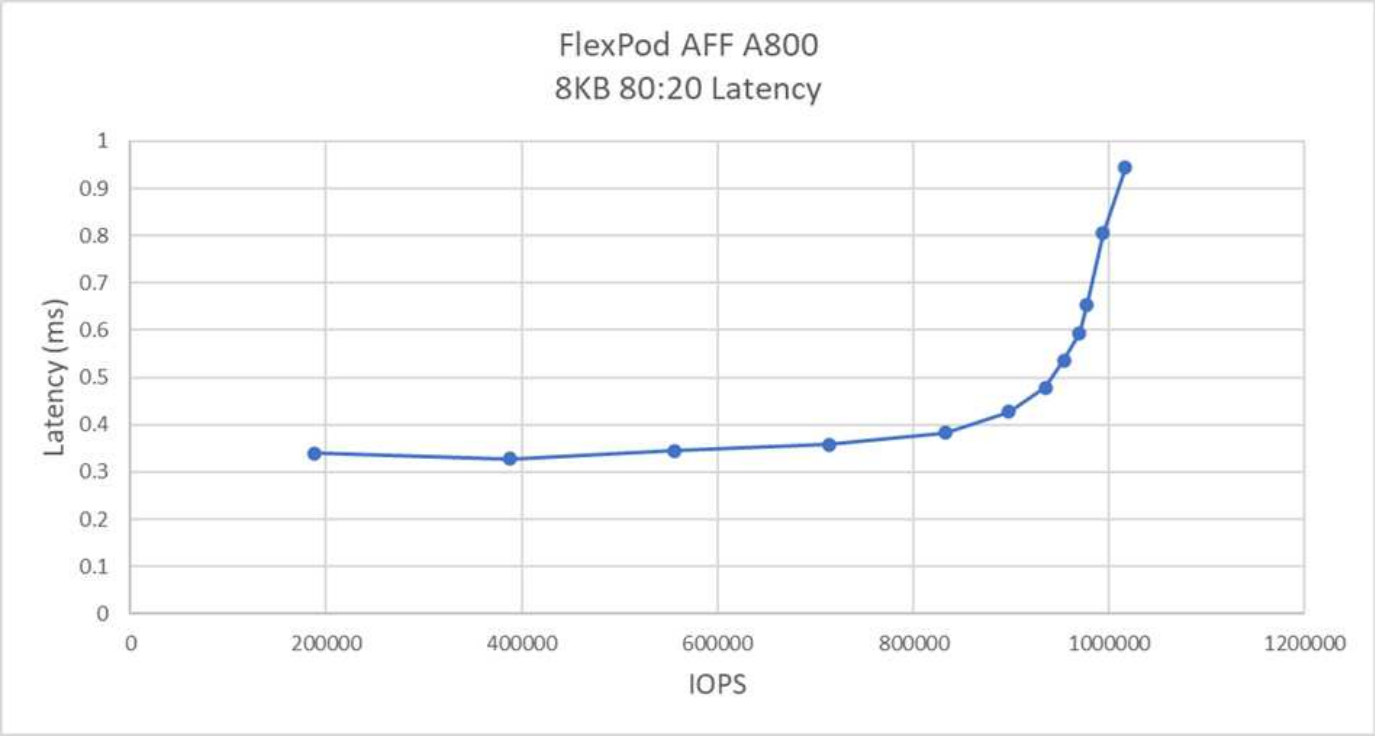
在我们的测试中，我们发现系统实现了超过 120 万次 IOPS ，而服务器端延迟仅保持在 0.35 毫秒以下。

下图显示了我们在使用 8 KB 块大小运行 100% 随机写入工作负载时的结果。



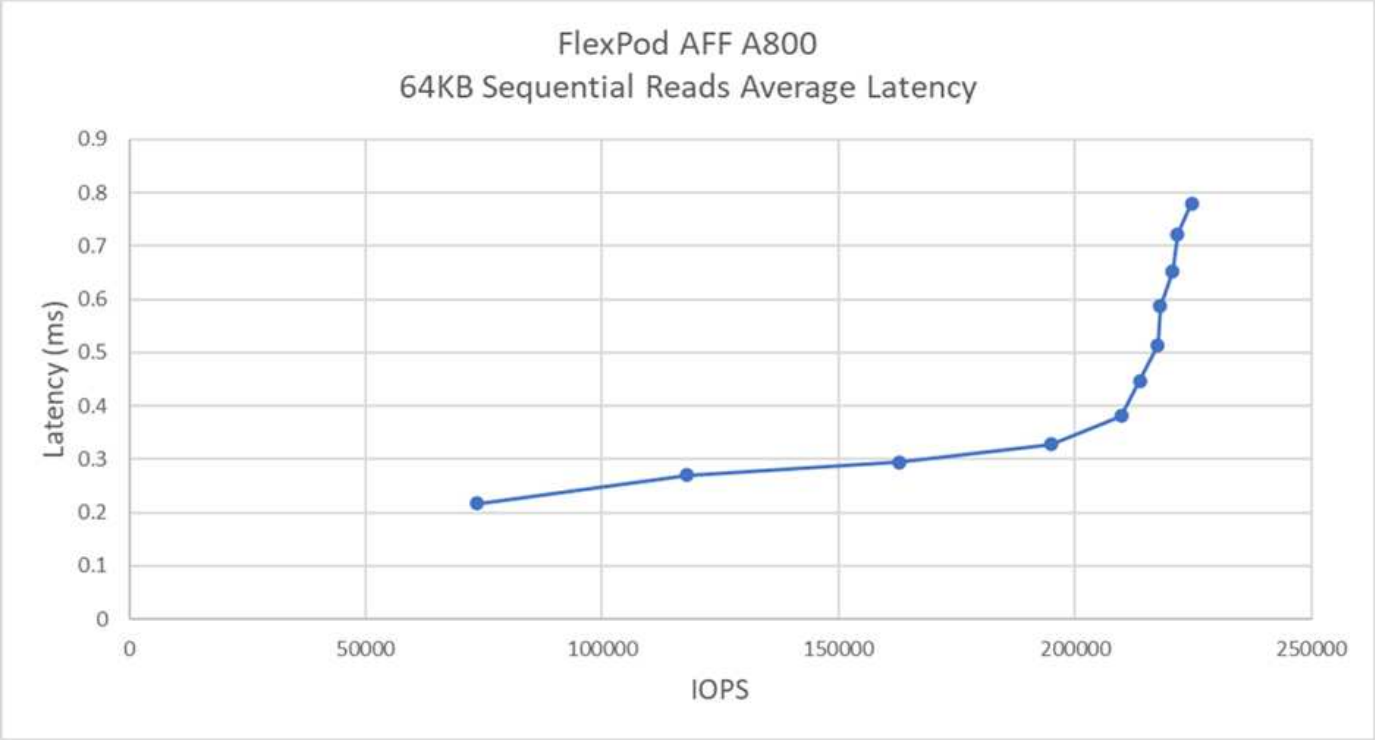
在我们的测试中，我们发现系统实现了接近 30 万次的 IOPS ，同时服务器端延迟仅保持在 1 毫秒以下。

对于随机读取率为 80% ，写入率为 20% 的 8 KB 块大小，我们观察到以下结果：



在我们的测试中，我们发现系统实现了超过 100 万次的 IOPS ，同时服务器端延迟仅保持在 1 毫秒以下。

对于 64 KB 块大小和 100% 顺序读取，我们观察到以下结果：



在我们的测试中，我们发现该系统实现了大约 25 万次 IOPS ，而服务器端延迟仅保持在 1 毫秒以下。

对于 64 KB 块大小和 100% 顺序写入，我们观察到以下结果：

在我们的测试中，我们发现该系统可实现约 120 ， 000 次 IOPS ，而服务器端延迟保持在 1 毫秒以下。

"接下来：总结。"

结论

"上一步：测试结果。"

对于延迟不到 1 毫秒的顺序读取工作负载，此解决方案的观察吞吐量为 14 GBps 和 220 K IOPS 。对于随机读取工作负载，吞吐量达到了 9.5 GBps 和 1.25 万次 IOPS 。FlexPod 通过 FC-NVMe 提供这种性能的能力可以满足任何任务关键型应用程序的需求。

采用 VMware vSphere 7.0 U2 的 FlexPod 数据中心是为各种 IT 工作负载部署 FC-NVMe 的最佳共享基础架构基础，可为需要此功能的应用程序提供高性能存储访问。随着 FC-NVMe 不断发展，包括高可用性，多路径和额外的操作系统支持， FlexPod 非常适合作为首选平台，可提供支持这些功能所需的可扩展性和可靠性。

借助 FlexPod ， Cisco 和 NetApp 创建了一个灵活且可扩展的平台，可用于多种使用情形和应用程序。借助 FC-NVMe ， FlexPod 新增了另一项功能，可帮助企业高效地支持在同一共享基础架构中同时运行的业务关键型应用程序。借助 FlexPod 的灵活性和可扩展性，客户还可以从规模合适的基础架构入手，并随着不断变化的业务需求进行扩展和适应。

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：

- Cisco Unified Computing System （ UCS ）

  "http://www.cisco.com/en/US/products/ps10265/index.html"

- Cisco UCS 6400 系列互联阵列数据表

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/datasheet-c78-741116.html"

- Cisco UCS 5100 系列刀片式服务器机箱

  "http://www.cisco.com/en/US/products/ps10279/index.html"

- Cisco UCS B 系列刀片式服务器

  "http://www.cisco.com/en/US/partner/products/ps10280/index.html"

- Cisco UCS C 系列机架式服务器

  "http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html"

- Cisco Unified Computing System 适配器

  "http://www.cisco.com/en/US/products/ps10277/prod_module_series_home.html"

- Cisco UCS Manager

  "http://www.cisco.com/en/US/products/ps10281/index.html"

- Cisco Nexus 9000 系列交换机

  "http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html"

- Cisco MDS 9000 多层光纤交换机

  "http://www.cisco.com/c/en/us/products/storage-networking/mds-9000-series-multilayer-switches/index.html"

- Cisco MDS 9132T 32 Gbps 32 端口光纤通道交换机

  "https://www.cisco.com/c/en/us/products/collateral/storage-networking/mds-9100-series-multilayer-fabric-switches/datasheet-c78-739613.html"

- NetApp ONTAP 9.

  "http://www.netapp.com/us/products/platform-os/ontap/index.aspx"

- NetApp AFF A 系列

  "http://www.netapp.com/us/products/storage-systems/all-flash-array/aff-a-series.aspx"

- VMware vSphere

  "https://www.vmware.com/products/vsphere"

- VMware vCenter Server

  "http://www.vmware.com/products/vcenter-server/overview.html"

- 现代 SAN 的最佳实践

  "https://www.netapp.com/us/media/tr-4080.pdf"

- 推出适用于 FlexPod 的端到端 NVMe

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/whitepaper-c11-741907.html"

互操作性表

- NetApp 互操作性表工具

  "http://support.netapp.com/matrix/"

- Cisco UCS 硬件兼容性列表

  "https://ucshcltool.cloudapps.cisco.com/public/"

- VMware 兼容性指南

  "http://www.vmware.com/resources/compatibility"

致谢

作者谨向 Cisco 的 John George， NetApp 的 Scott Lane 和 Bobby Oommen 表示感谢，感谢他们在项目执行期间提供的帮助和指导。

法律声明

法律声明提供对版权声明、商标、专利等的访问。

版权

http://www.netapp.com/us/legal/copyright.aspx

商标

NetApp 、 NetApp 徽标和 NetApp 商标页面上列出的标记是 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。

http://www.netapp.com/us/legal/netapptmlist.aspx

专利

有关 NetApp 拥有的专利的最新列表，请访问：

https://www.netapp.com/us/media/patents-page.pdf

隐私政策

https://www.netapp.com/us/legal/privacypolicy/index.aspx