



FlexPod Express

FlexPod

NetApp
October 30, 2025

目录

FlexPod Express	1
采用 Cisco UCS C 系列和 NetApp AFF C190 系列的 FlexPod Express 设计指南	1
NVA-1139-design：采用 Cisco UCS C 系列和 NetApp AFF C190 系列的 FlexPod Express	1
计划摘要	1
技术要求	2
设计选择	3
结论	7
从何处查找追加信息	7
《采用 Cisco UCS C 系列和 NetApp AFF C190 系列的 FlexPod 快速部署指南》	7
NVA-1142-Deploy：采用 Cisco UCS C 系列和 NetApp AFF C190 系列的 FlexPod Express — NVA	7
部署	
解决方案概述	8
技术要求	11
FlexPod 快速布线信息	12
部署过程	15
结论	100
致谢	100
从何处查找追加信息	101
版本历史记录	101
采用 Cisco UCS C 系列和 AFF A220 系列的 FlexPod Express 设计指南	101
NVA-1125-设计：采用 Cisco UCS C 系列和 AFF A220 系列的 FlexPod Express	101
计划摘要	101
解决方案概述	102
技术要求	104
设计选择	105
解决方案验证	110
结论	110
从何处查找追加信息	111
《采用 Cisco UCS C 系列和 AFF A220 系列的 FlexPod 快速部署指南》	111
NVA-1123-Deploy：《采用 VMware vSphere 6.7 的 FlexPod Express 和 NetApp AFF A220	111
部署指南》	
解决方案概述	111
技术要求	114
FlexPod 快速布线信息	115
部署过程	117
结论	190
从何处查找追加信息	190
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 ...	190
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	190
解决方案概述	190
技术要求	194
FlexPod 快速布线信息	194
部署过程	196
结论	300
追加信息	301
适用于采用Cisco UCS Mini和NetApp AFF/FAS的VMware vSphere 7.0的FlexPod Express—NVA—部署 ..	301

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：[错误：缺少图形映像]

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。

[错误：缺少图形映像]

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。

[错误：缺少图形映像]

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。

[错误：缺少图形映像]

"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 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。

[错误：缺少图形映像]

下图显示了通过传统 RJ-45 以太网缆线连接的 10GBASE-T 端口。

[错误：缺少图形映像]



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。

[错误：缺少图形映像]

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。

[错误：缺少图形映像]

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

[错误：缺少图形映像]

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。

[错误：缺少图形映像]

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）和计算资源负载均衡。

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。

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。

[错误：缺少图形映像]

"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"](https://docs.netapp.com/platstor/index.jsp)

- AFF 文档资源页面

["https://www.netapp.com/us/documentation/all-flash-fas.aspx"](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"](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调整。

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。

The FlexPod Portfolio

A prevalidated, flexible platform that features



FlexPod® Express

Remote office or branch office, retail, small and midsize business, and edge



FlexPod Datacenter

Enterprise apps, unified infrastructure, and virtualization

11

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：

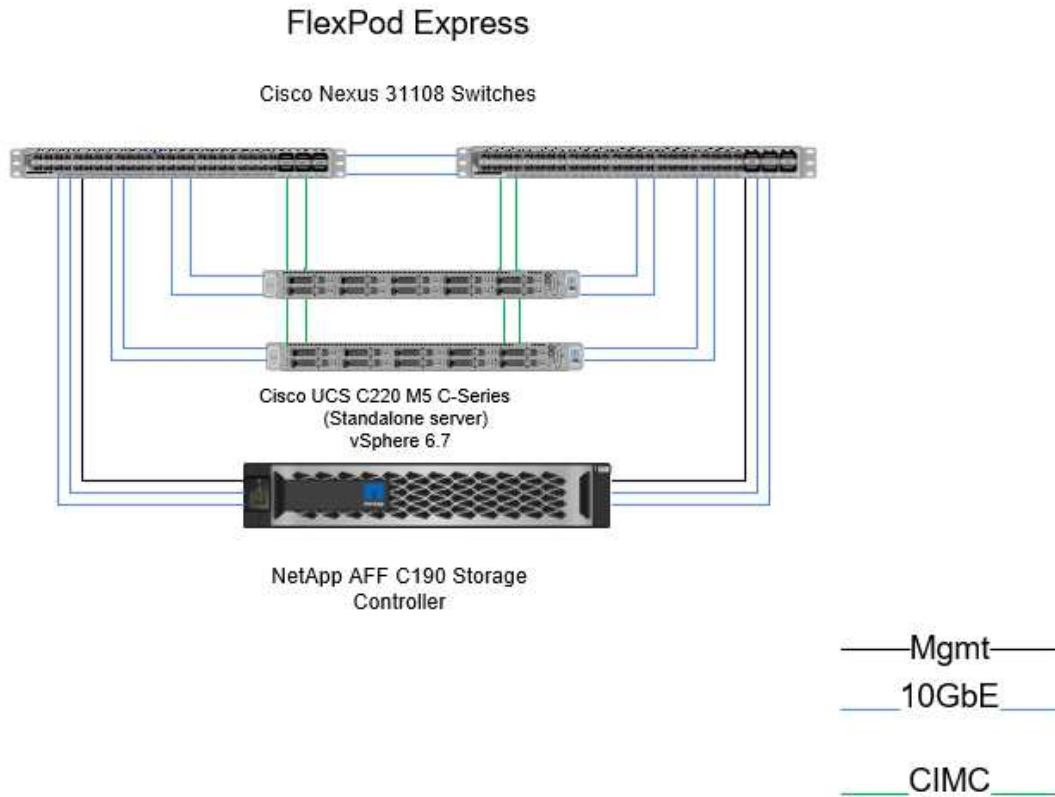
- 经过全面测试
- 规范性
- 最大限度地降低部署风险
- 加快上市速度

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 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

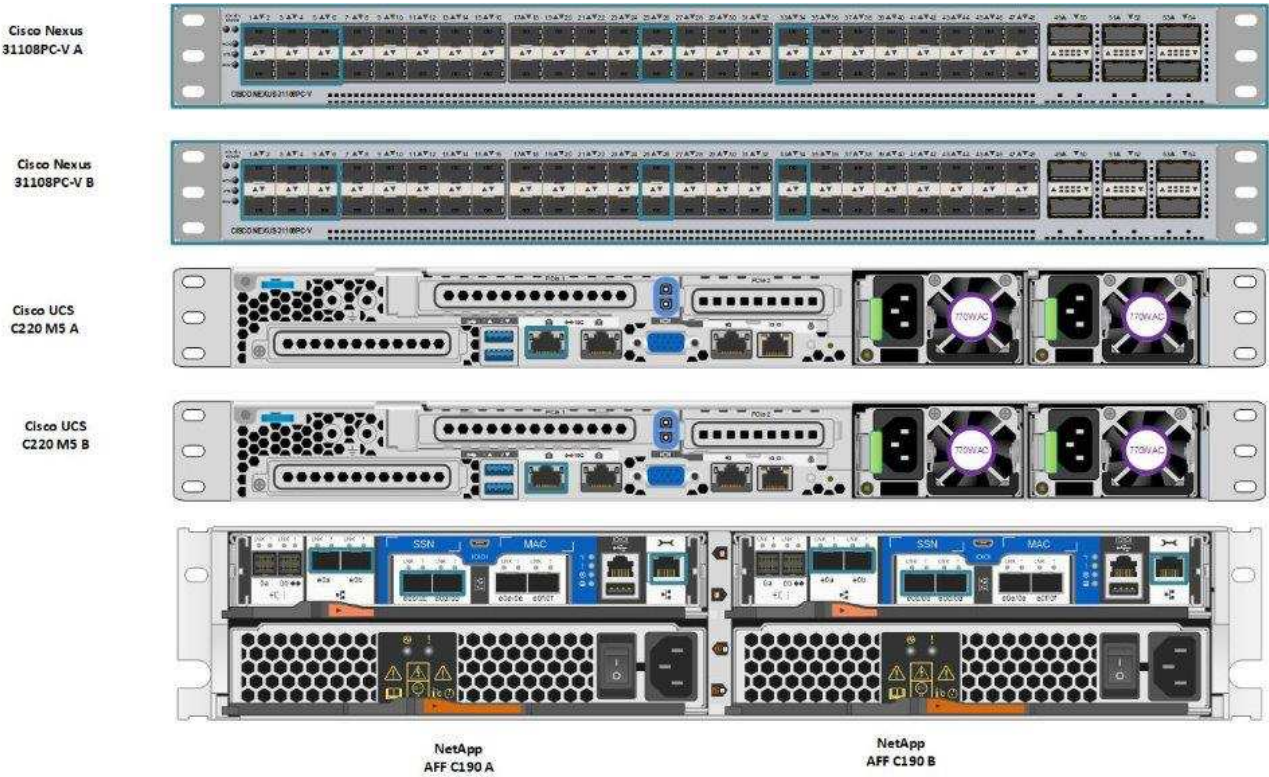
下表列出了在 FlexPod Express 上实施所有 VMware vSphere 所需的软件。

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 xxxxx 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? (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。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 Pol1
    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 Pol2
    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。

Guided Setup to Configure a Cluster

Provide the information required below to configure your cluster:



? AutoSupport ☒

? Proxy URL (Optional)

i Connection is verified after configuring AutoSupport on all nodes.

? Event Notifications

Notify me through:



Email

SMTP Mail Host

Email Addresses

Separate email addresses with a comma...



SNMP

SNMP Trap Host



Syslog

Syslog Server

Submit

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
```

Node	Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin 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,fc
```

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 。



Copyright (c) 2019 Cisco Systems, Inc.

Press <F2> BIOS Setup : <F6> Boot Menu : <F7> Diagnostics
Press <F8> CIMC Setup : <F12> Network Boot
Bios Version : C220M5.4.0.4g.0.0712190011
Platform ID : C220M5

Processor(s) Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz
Total Memory = 64 GB Effective Memory = 64 GB
Memory Operating Speed 2400 Mhz
M.2 SWRAID configuration is not detected. Switching to AHCI mode.

Cisco IMC IPv4 Address : 10.63.172.160
Cisco IMC MAC Address : 70:69:5A:B5:8D:68

Entering CIMC Configuration Utility ...

92

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`

```

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
NIC Properties
NIC mode                               NIC redundancy
Dedicated:      [X]                   None:          [X]
Shared LOM:     [ ]                   Active-standby: [ ]
Cisco Card:     [ ]                   Active-active:  [ ]
  Riser1:       [ ]                   VLAN (Advanced)
  Riser2:       [ ]                   VLAN enabled:   [ ]
  MLom:         [ ]                   VLAN ID:       1
  Shared LOM Ext: [ ]                   Priority:      0
IP (Basic)
IPv4:           [X]                   IPv6:          [ ]
DHCP enabled    [ ]
CIMC IP:        10.63.172.160
Prefix/Subnet:  255.255.255.0
Gateway:        10.63.172.1
Pref DNS Server: 0.0.0.0
Smart Access USB
Enabled         [ ]
*****
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F1>Additional settings

```

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 。

Cisco Integrated Management Controller

[Home](#) / [Compute](#) / [BIOS](#) ★

[BIOS](#)
[Remote Management](#)
[Troubleshooting](#)
[Power Policies](#)
[PID Catalog](#)

[Enter BIOS Setup](#) | [Clear BIOS CMOS](#) | [Restore Manufacturing Custom Settings](#) | [Restore Defaults](#)

[Configure BIOS](#)
[Configure Boot Order](#)
[Configure BIOS Profile](#)

BIOS Properties

Running Version

C220M5.4.0.4g.0.0712190011

UEFI Secure Boot

☐

Actual Boot Mode

Uefi

Configured Boot Mode

▼

Last Configured Boot Order Source

BIOS

Configured One time boot device

▼

Save Changes

▼ Configured Boot Devices

Basic

▶ ☒ Advanced

Actual Boot Devices

UEFI: Built-in EFI Shell (NonPolicyTarget)

UEFI: PXE IP4 Intel(R) Ethernet Controller X550 (NonPolicyTarget)

UEFI: PXE IP4 Intel(R) Ethernet Controller X550 (NonPolicyTarget)

Configure Boot Order

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。

Configure Boot Order

Configured Boot Level: Advanced

Basic

Advanced

Add Boot Device

Add Local HDD

Add PXE Boot

Add SAN Boot

Add iSCSI Boot

Add USB

Add Virtual Media

Add PCHStorage

Add UEFISHELL

Add SD Card

Add NVME

Add Local CDD

Advanced Boot Order Configuration

Selected 1 / Total 3

Enable/Disable

Modify

Delete

Clone

Re-Apply

Move Up

Move Down

	Name	Type	Order	State
<input checked="" type="checkbox"/>	KVM-MAPPED-DVD	VMEDIA	1	Enabled
<input type="checkbox"/>	iSCSI-A	ISCSI	2	Enabled
<input type="checkbox"/>	iSCSI-B	ISCSI	3	Enabled

Save Changes

Reset Values

Close

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 。

BIOS	Remote Management	Troubleshooting	Power Policies	PID Catalog	
I/O	Server Management	Security	Processor	Memory	Power/Performance

Note: Default values are shown in bold.

Reboot Host Immediately: ☒

Intel VT for directed IO:	Enabled ▼
Intel VTD ATS support:	Enabled ▼
LOM Port 1 OptionRom:	Enabled ▼
Pcie Slot 1 OptionRom:	Disabled ▼
MLOM OptionRom:	Enabled ▼
Front NVME 1 OptionRom:	Enabled ▼
MRAID Link Speed:	Auto ▼
PCIe Slot 1 Link Speed:	Auto ▼
Front NVME 1 Link Speed:	Auto ▼
VGA Priority:	Onboard ▼
P-SATA OptionROM:	LSI SW RAID ▼
USB Port Rear:	Enabled ▼
USB Port Internal:	Enabled ▼
IPV6 PXE Support:	Disabled ▼

Legacy USB Support:	Enabled ▼
Intel VTD coherency support:	Disabled ▼
All Onboard LOM Ports:	Enabled ▼
LOM Port 2 OptionRom:	Enabled ▼
Pcie Slot 2 OptionRom:	Disabled ▼
MRAID OptionRom:	Enabled ▼
Front NVME 2 OptionRom:	Enabled ▼
MLOM Link Speed:	Auto ▼
PCIe Slot 2 Link Speed:	Auto ▼
Front NVME 2 Link Speed:	Auto ▼
M.2 SATA OptionROM:	AHCI ▼
USB Port Front:	Enabled ▼
USB Port KVM:	Enabled ▼
USB Port:M.2 Storage:	Enabled ▼

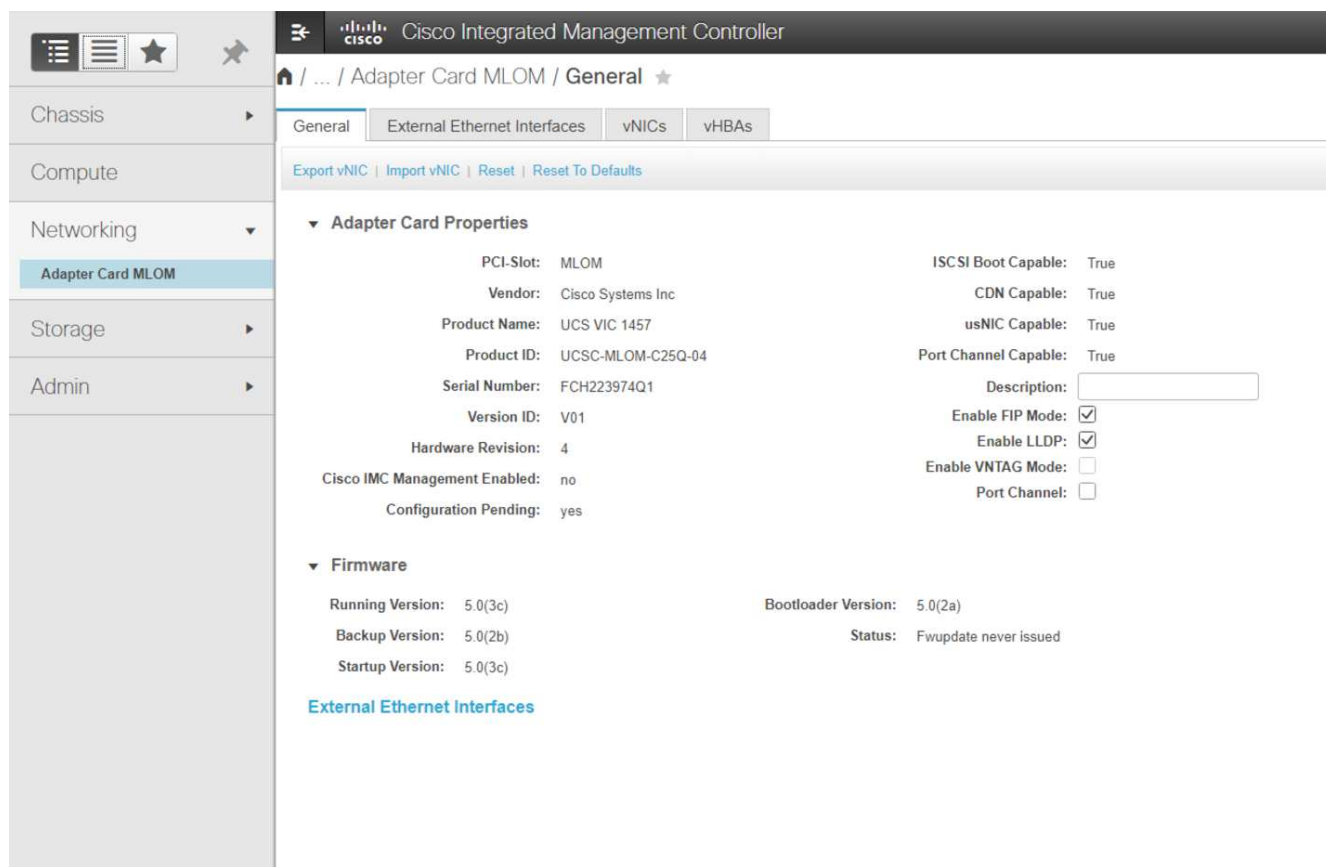
为 iSCSI 启动配置 Cisco VIC1457

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。

▼ General

Name:

CDN:

MTU: (1500 - 9000)

Uplink Port: ▼

MAC Address: ☐ Auto
☒

Class of Service: (0 - 6)

Trust Host CoS: ☐

PCI Order: (0 - 7)

Default VLAN: ☐ None
☒ ?

6. 选择左侧的 vNIC eth1 。

General External Ethernet Interfaces **vNICs** vHBAs

▼ vNICs

- eth0
- eth1**
- eth2
- eth3

► vNIC Properties

▼ iSCSI Boot Properties

► General

▼ Initiator

Name: (0 - 222) chars

IP Address:

Subnet Mask:

Gateway:

Primary DNS:

► Primary Target

► Secondary Target

[Unconfigure iSCSI Boot](#)

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]`

▼ vNICs

- eth0
- eth1**
- eth2
- eth3

► vNIC Properties

▼ iSCSI Boot Properties

► General

▼ Initiator

Name: (0 - 222) chars

IP Address:

Subnet Mask:

Gateway:

Primary DNS:

Initiator Priority:

Secondary DNS:

TCP Timeout: (0 - 255)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

▼ Primary Target

Name: (0 - 222) chars

IP Address:

TCP Port:

Boot LUN: (0 - 65535)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

▼ Secondary Target

Name: (0 - 222) chars

IP Address:

TCP Port:

Boot LUN: (0 - 65535)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

[Unconfigure iSCSI Boot](#)

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]`

Adapter Card MLOM / vNICs

General External Ethernet Interfaces vNICs vHBAs

vNICs

eth0 eth1 eth2 eth3

vNIC Properties

iSCSI Boot Properties

General

Initiator

Name: ign.1992-01.com.cisco.ucsa-02 (0 - 222) chars

IP Address: 172.21.184.110

Subnet Mask: 255.255.255.0

Gateway: 172.21.184.1

Primary DNS:

Initiator Priority: primary

Secondary DNS:

TCP Timeout: 15 (0 - 255)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

Primary Target

Name: ign.1992-08.com.netapp.sn.e42fa6b2d2 (0 - 222) chars

IP Address: 172.21.184.105

TCP Port: 3260

Secondary Target

Name: ign.1992-08.com.netapp.sn.e42fa6b2d2 (0 - 222) chars

IP Address: 172.21.184.106

TCP Port: 3260

Boot LUN: 0 (0 - 65535)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

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：

- 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。

Cisco Integrated Management Controller

Home / ... / Adapter Card MLOM / vNICs

General External Ethernet Interfaces **vNICs** vHBAs

vNIC Properties

General

Name: eth0

CDN: VIC-MLOM-eth0

MTU: 9000 (1500 - 9000)

Uplink Port: 0

MAC Address: ☐ Auto ☒ F8:0F:6F:89:26:CE

Class of Service: 0 (0 - 6)

Trust Host CoS: ☐

PCI Order: 0 (0 - 7)

Default VLAN: ☐ None ☒ 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。

Cisco Integrated Management Controller

Home / ... / Adapter Card MLOM / vNICs

General External Ethernet Interfaces **vNICs** vHBAs

Host Ethernet Interfaces

Selected 0 / Total 4

	Name	CDN	MAC Address	MTU	usNIC	Uplink Port	CoS	VLAN	VLAN Mode	ISCSI Boot	PXE Boot	Channel	Port Profile	Uplink Failover
<input type="checkbox"/>	eth0	VIC-MLO...	F8:0F:6F:89:26:CE	9000	0	0	0	2	TRUNK	disabled	enabled	N/A	N/A	N/A
<input type="checkbox"/>	eth1	VIC-ISC...	F8:0F:6F:89:26:CF	9000	0	1	0	3439	TRUNK	enabled	enabled	N/A	N/A	N/A
<input type="checkbox"/>	eth2	VIC-MLO...	F8:0F:6F:89:26:D0	9000	0	2	0	2	TRUNK	disabled	enabled	N/A	N/A	N/A
<input type="checkbox"/>	eth3	VIC-ISC...	F8:0F:6F:89:26:D1	9000	0	3	0	3440	TRUNK	enabled	enabled	N/A	N/A	N/A



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



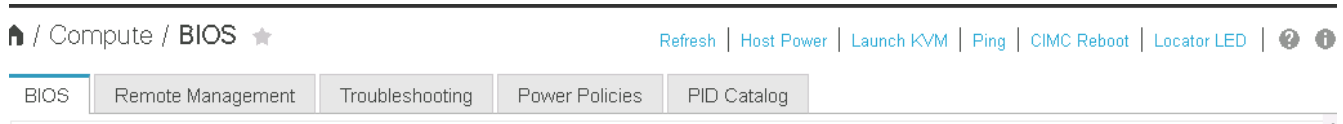
对于添加到集群中的任何其他节点，必须完成此操作步骤。

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。

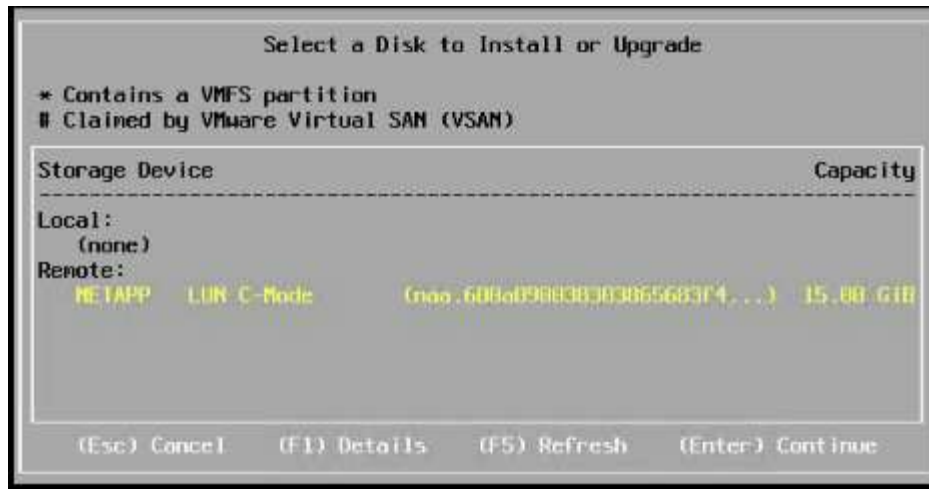
7. 浏览到 VMware ESXi 6.7U2 安装程序 ISO 映像文件，然后单击打开。单击映射设备。
8. 选择电源菜单，然后选择系统重新启动（冷启动）。单击是。

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。

Network Adapters

Select the adapters for this host's default management network connection. Use two or more adapters for fault-tolerance and load-balancing.

Device Name	Hardware Label (MAC Address)	Status
<input type="checkbox"/> vmnic0	LOM Port 1 (...:5a:b5:8d:6e)	Connected
<input type="checkbox"/> vmnic1	LOM Port 2 (...:5a:b5:8d:6f)	Disconnected
<input checked="" type="checkbox"/> vmnic2	VIC-MLOM-eth0 (...:70:6c:cc)	Connected (...)
<input type="checkbox"/> vmnic3	VIC-iSCSI-A (...:3c:70:6c:cd)	Connected (...)
<input checked="" type="checkbox"/> vmnic4	VIC-MLOM-eth2 (...:70:6c:ce)	Connected (...)
<input type="checkbox"/> vmnic5	VIC-iSCSI-B (...:3c:70:6c:cf)	Connected (...)

<D> View Details <Space> Toggle Selected <Enter> OK <Esc> Cancel

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：

- 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。
- 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。

iScsiBootPG-A - Edit Settings

Properties

Security

Traffic shaping

Teaming and fallover

Load balancing

Network failure detection

Notify switches

Failback

Failover order

☒ Override



Active adapters

vmnic3

Standby adapters

Unused adapters

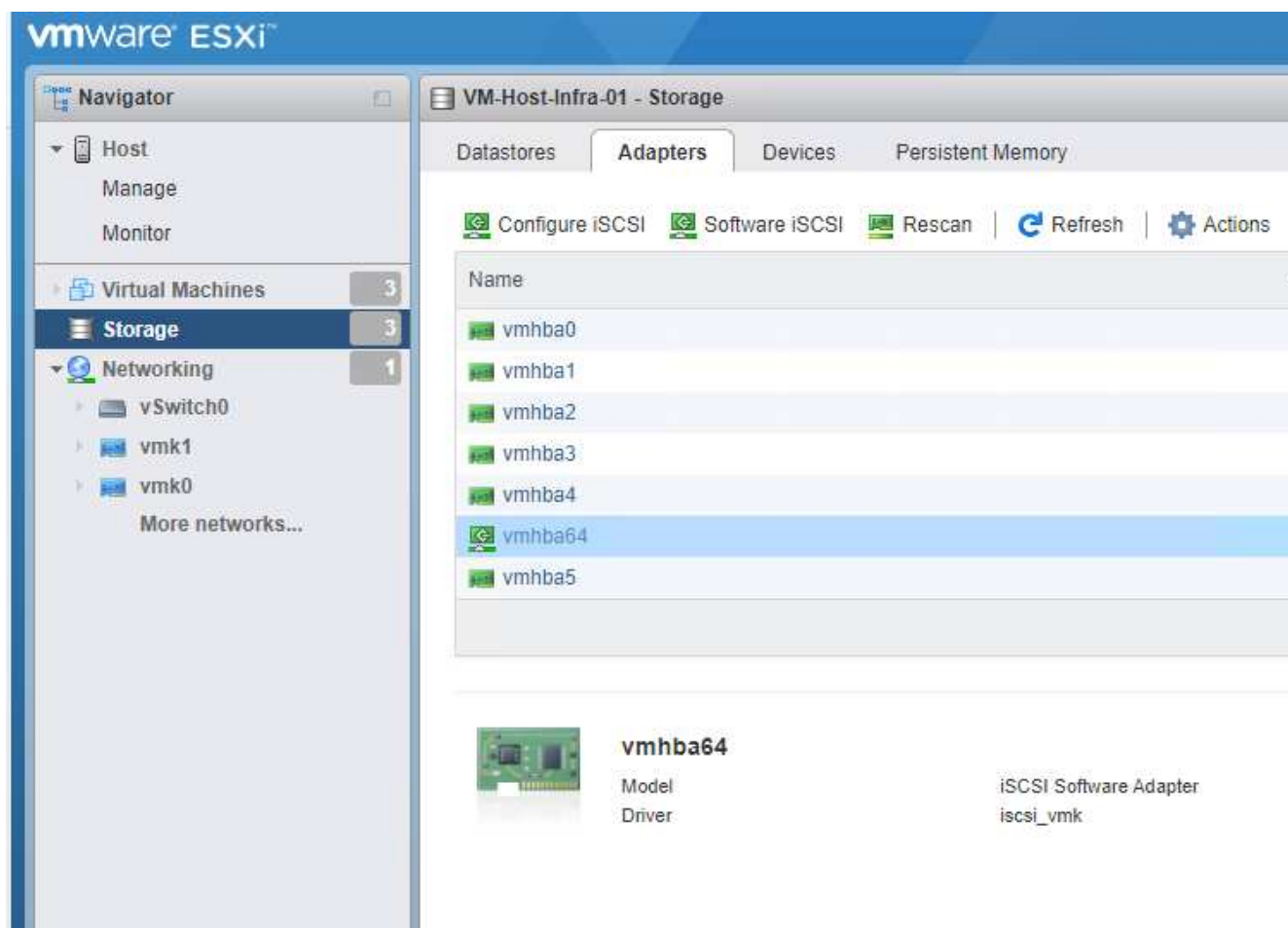
vmnic5

Select active and standby adapters

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。

Configure iSCSI - vmhba64

iSCSI enabled ☐ Disabled ☒ Enabled

▶ Name & alias iqn.1992-01.com.cisco:ucsA-01

▶ CHAP authentication Do not use CHAP

▶ Mutual CHAP authentication Do not use CHAP

▶ Advanced settings Click to expand

Network port bindings No port bindings

Static targets

Add static target Remove static target Edit settings

Target	Address	Port
iqn.1992-08.com.netapp:sn.e42fa6b2d2e011e9a68d00a098f...	172.21.183.105	3260
iqn.1992-08.com.netapp:sn.e42fa6b2d2e011e9a68d00a098f...	172.21.184.106	3260
iqn.1992-08.com.netapp:sn.e42fa6b2d2e011e9a68d00a098f...	172.21.183.106	3260
iqn.1992-08.com.netapp:sn.e42fa6b2d2e011e9a68d00a098f...	172.21.184.105	3260

Dynamic targets

Add dynamic target Remove dynamic target Edit settings

Address	Port
172.21.183.105	3260
172.21.184.105	3260
172.21.183.106	3260
172.21.184.106	3260

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。

Dynamic targets

Add dynamic target Remove dynamic target Edit settings

Address	Port
172.21.183.105	3260
172.21.184.105	3260
172.21.183.106	3260
172.21.184.106	3260



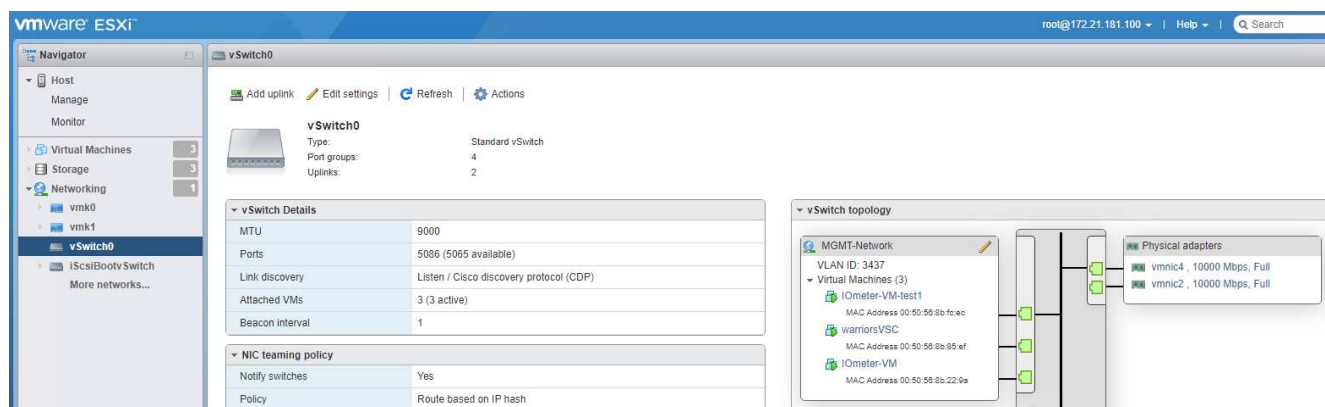
您可以通过在 NetApp 集群上运行 `network interface show` 命令或查看 System Manager 中的 Network Interfaces 选项卡来查找 iSCSI LIF IP 地址。

配置 ESXi 主机

要配置 ESXi 启动，请完成以下步骤：

- 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。



负载均衡的 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

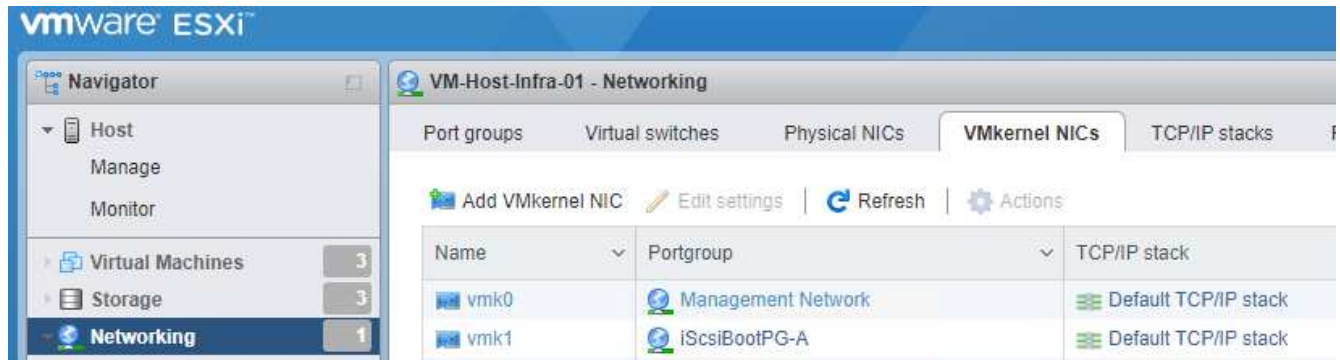
要配置端口组和 VMkernel NIC，请完成以下步骤：

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。

Add VMkernel NIC

Virtual switch	vSwitch0
VLAN ID	3441
MTU	9000
IP version	IPv4 only
▼ IPv4 settings	
Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
Address	172.21.185.63
Subnet mask	255.255.255.0
TCP/IP stack	Default TCP/IP stack
Services	<input checked="" type="checkbox"/> vMotion <input type="checkbox"/> Provisioning <input type="checkbox"/> Fault tolerance logging <input type="checkbox"/> Management <input type="checkbox"/> Replication <input type="checkbox"/> NFC replication

Create Cancel

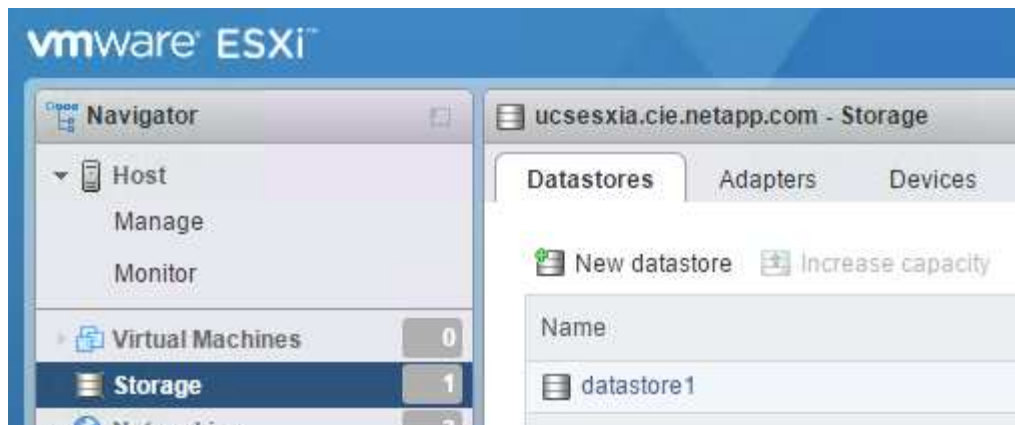


可以通过多种方法配置 ESXi 网络，包括在许可允许的情况下使用 VMware vSphere 分布式交换机。如果需要使用其他网络配置来满足业务需求，FlexPod Express 支持这些配置。

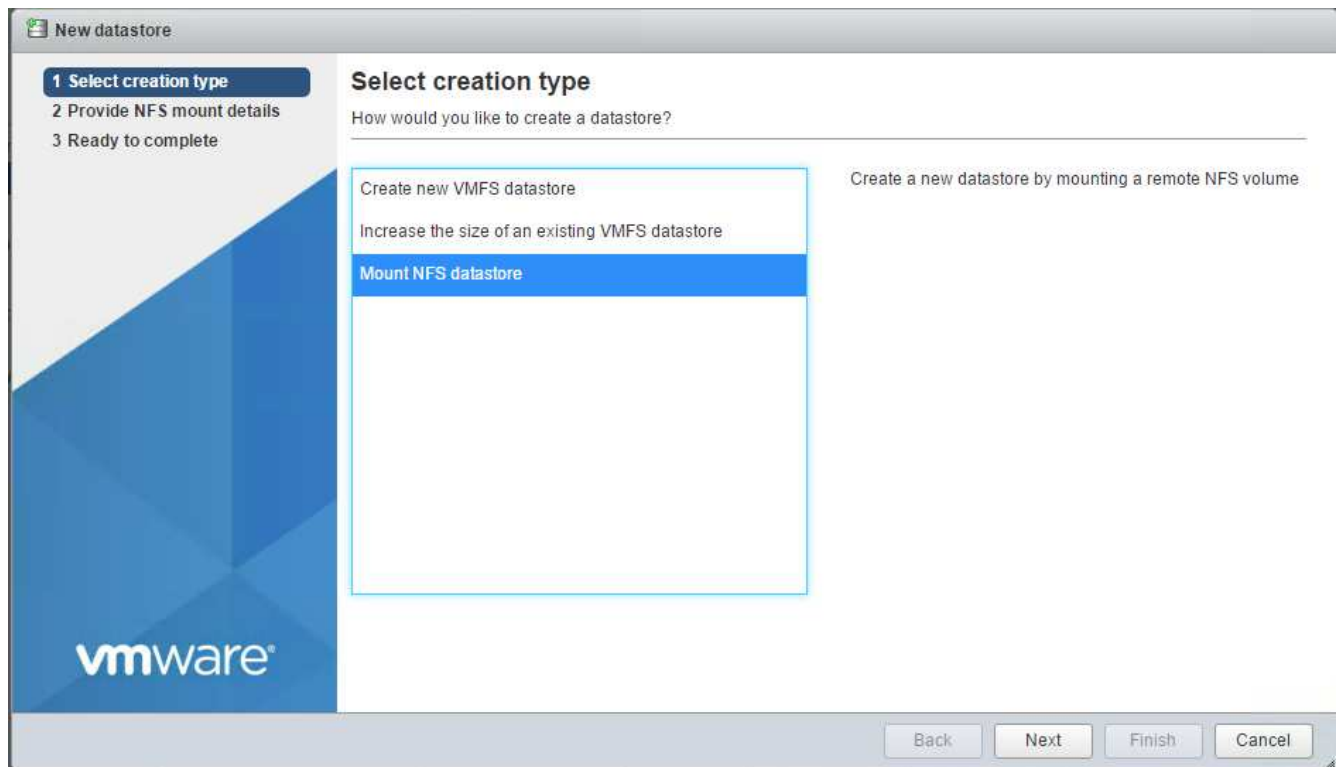
挂载第一个数据存储库

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：

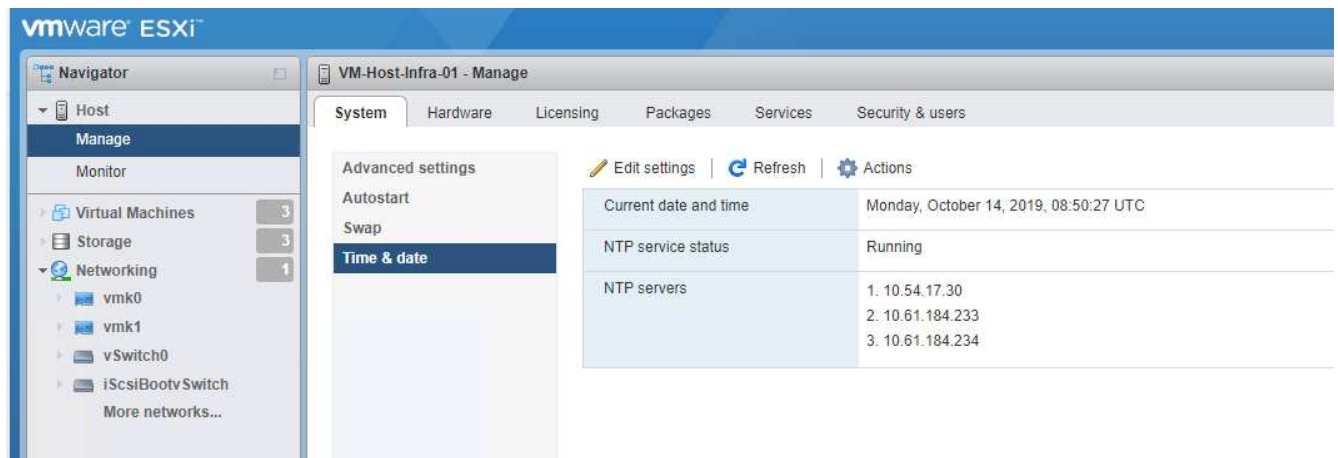
- 名称: `infra_swap`
- NFS 服务器: ``<<var_noda_nfs_lif>>``
- 共享: ``/infra_swap``

- 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：

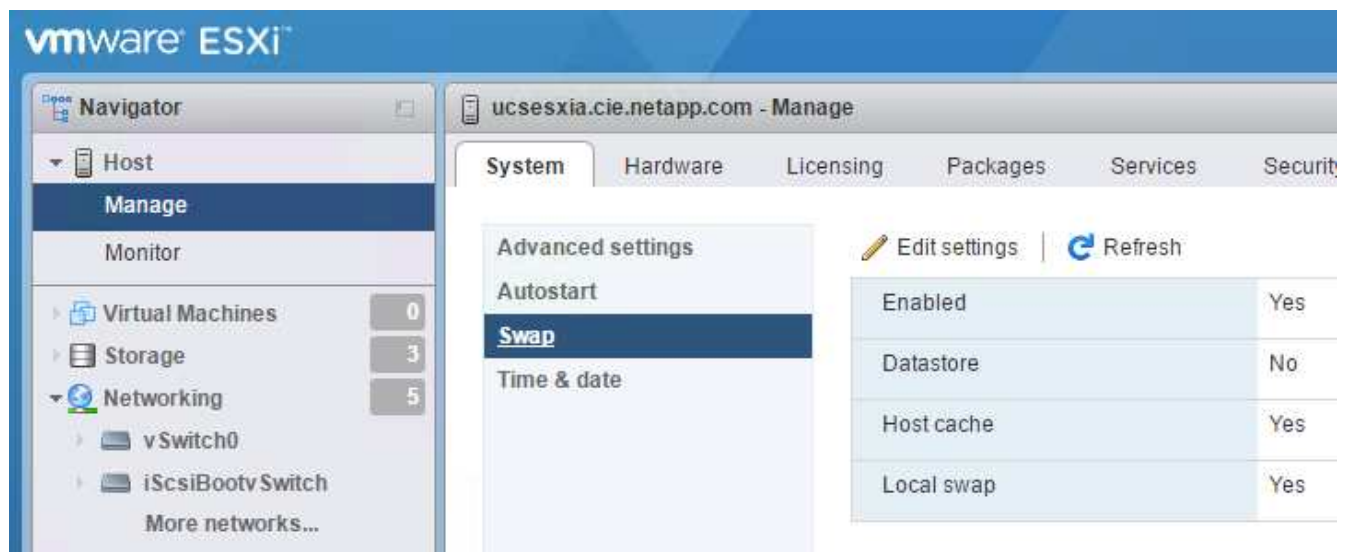
1. 单击左侧导航窗格中的管理。在右窗格中选择 System，然后单击 Time & Date。
2. 选择使用网络时间协议（启用 NTP 客户端）。
3. 选择 Start 和 Stop with Host 作为 NTP 服务启动策略。
4. 输入 `<<var_ntf>>` 作为 NTP 服务器。您可以设置多个 NTP 服务器。
5. 单击保存。



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。

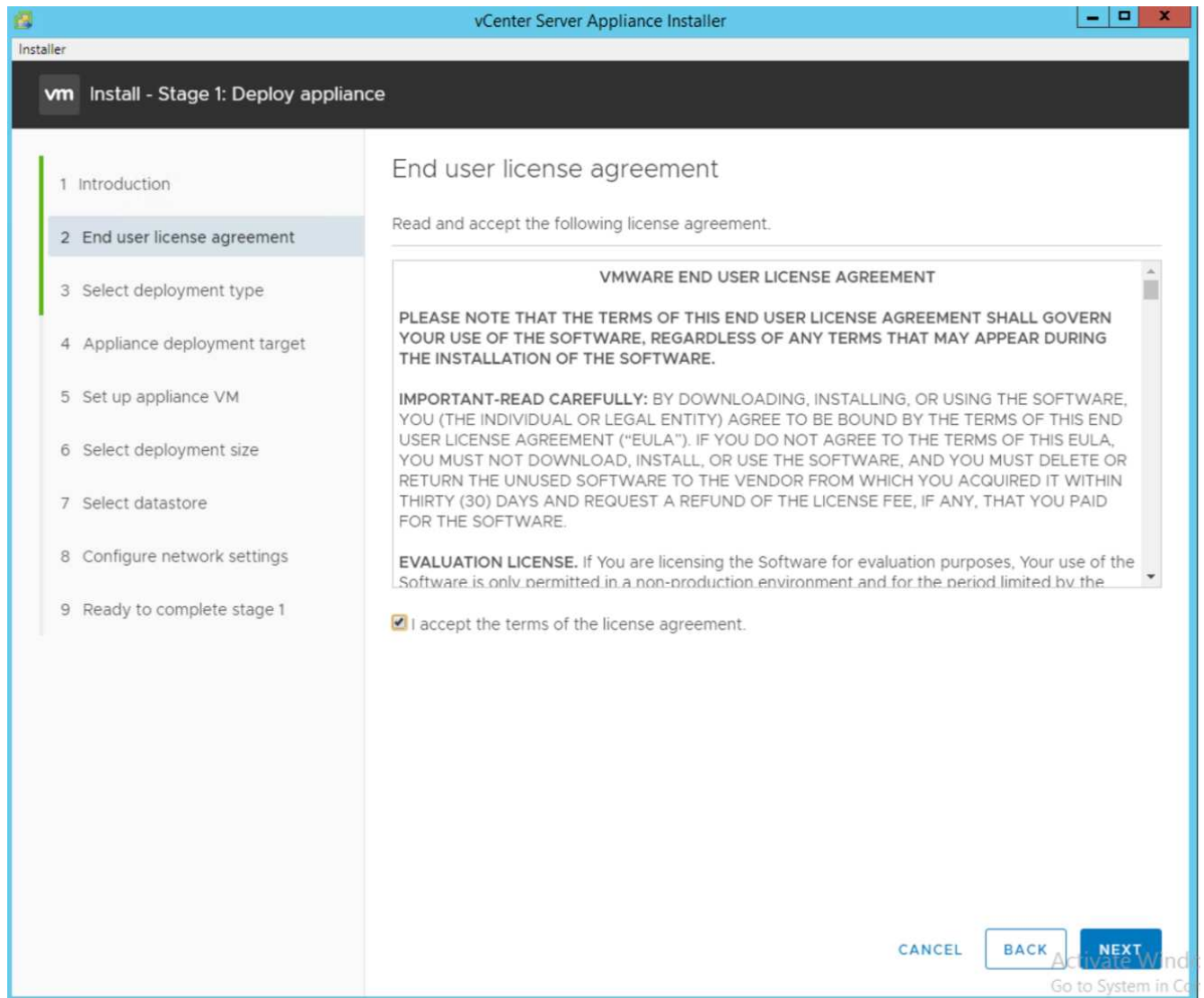


FlexPod Express 使用 VMware vCenter Server 设备（VCSA）。

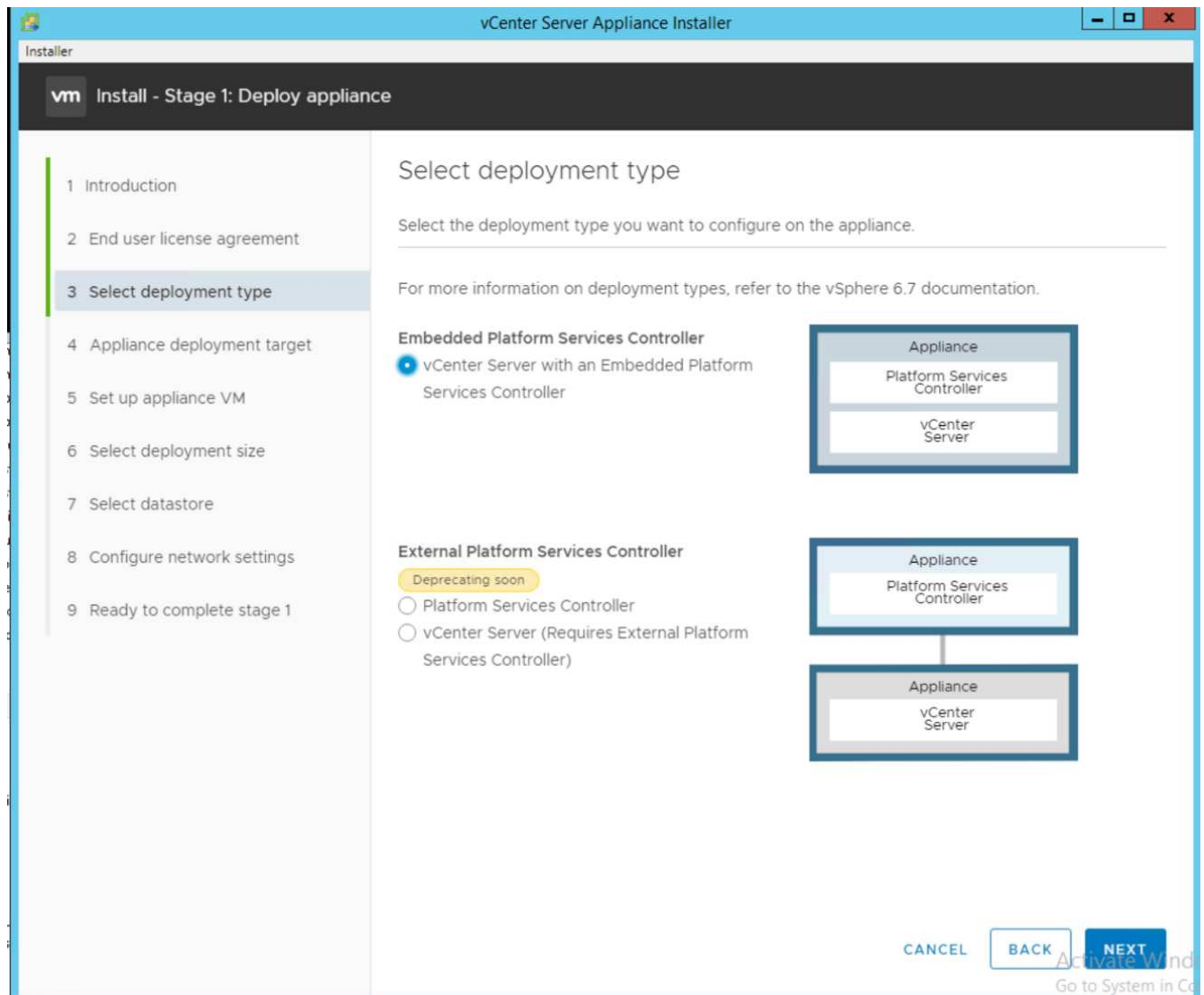
下载 VMware vCenter Server 设备

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。

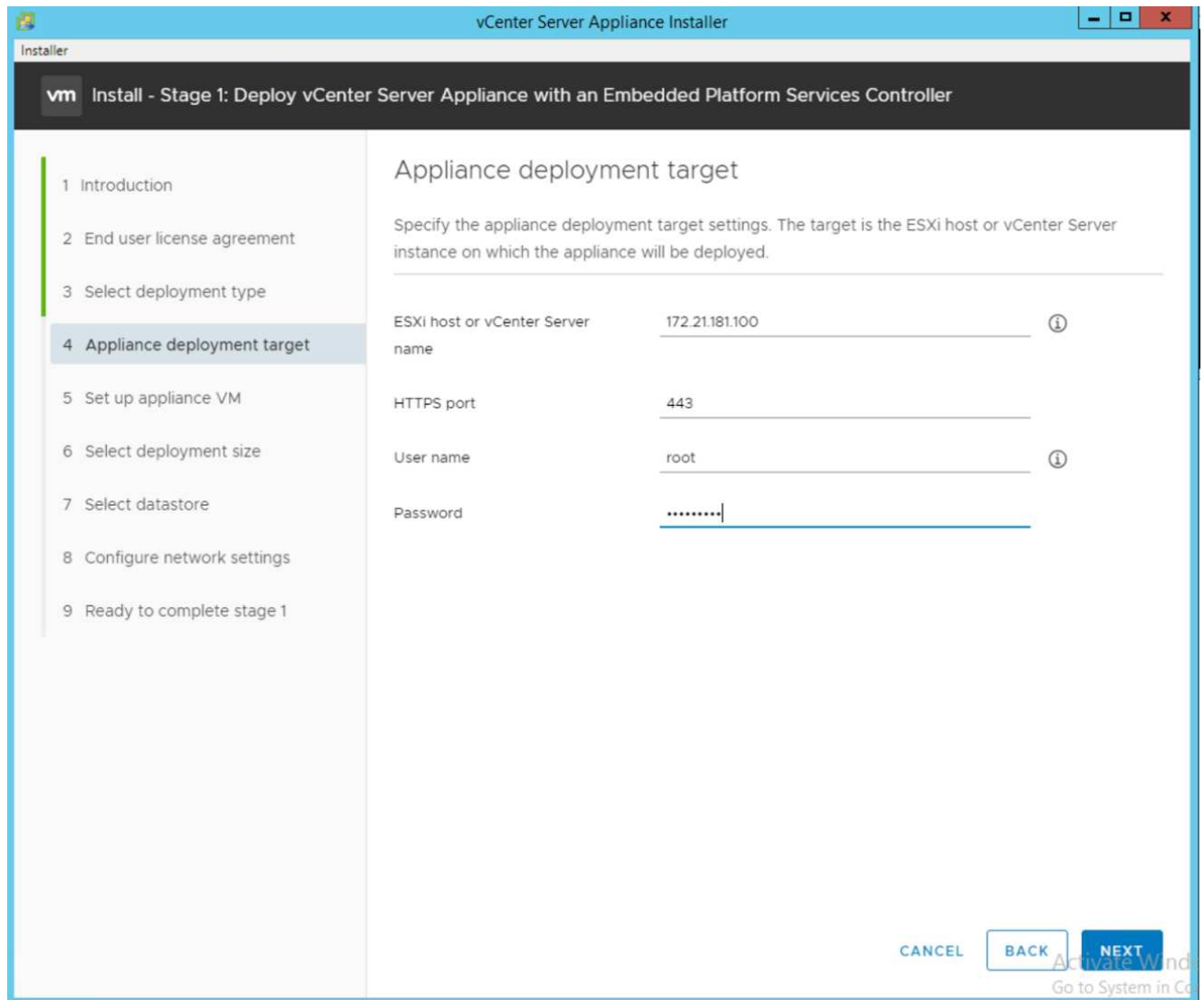


8. 选择 Embedded Platform Services Controller 作为部署类型。

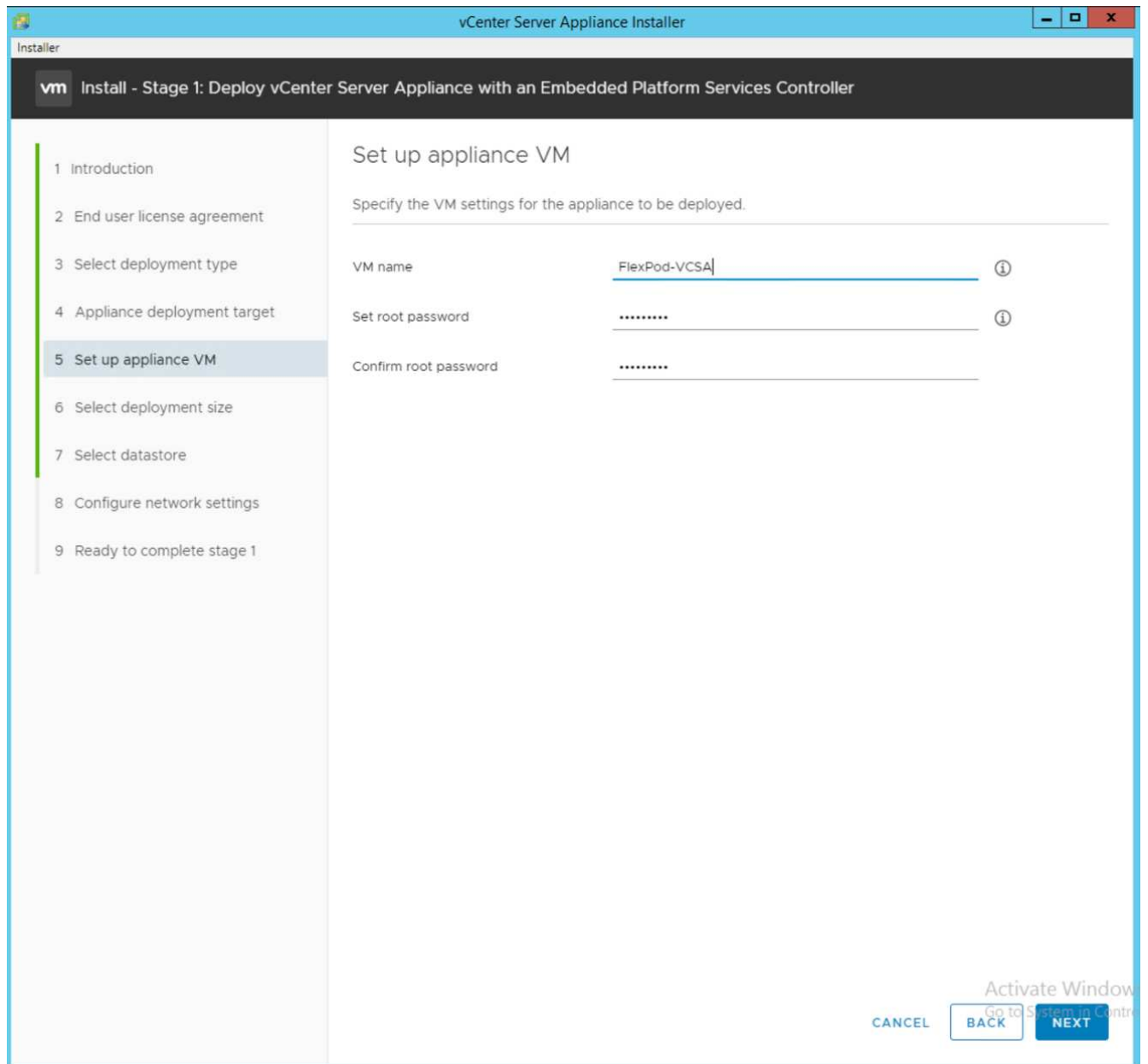


如果需要，还支持在 FlexPod Express 解决方案中部署外部平台服务控制器。

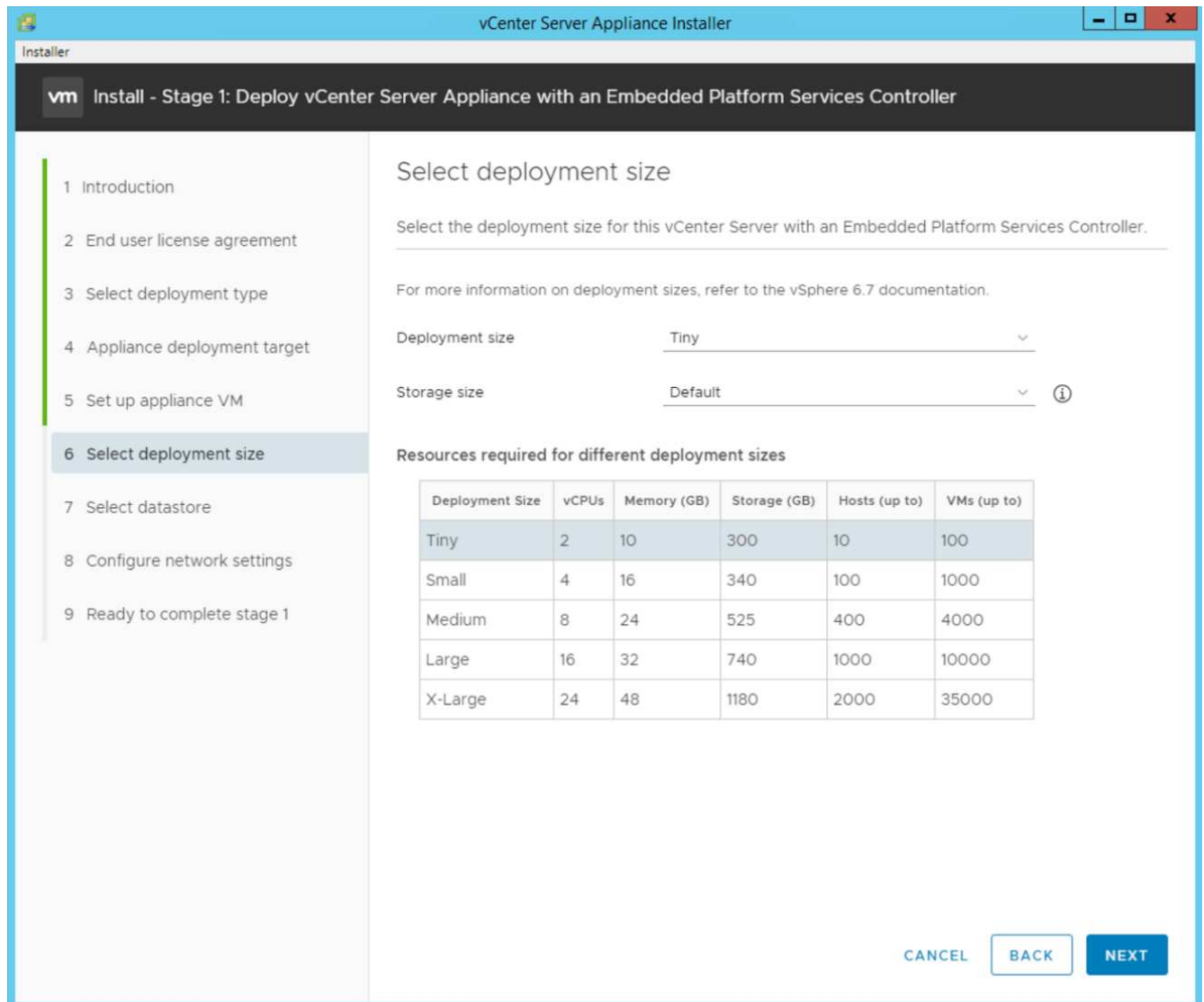
9. 在设备部署目标中，输入已部署的 ESXi 主机的 IP 地址， root 用户名和 root 密码。



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。

Installer

vCenter Server Appliance Installer

vm Install - Stage 1: Deploy vCenter Server Appliance with an Embedded Platform Services Controller

- 1 Introduction
- 2 End user license agreement
- 3 Select deployment type
- 4 Appliance deployment target
- 5 Set up appliance VM
- 6 Select deployment size
- 7 Select datastore
- 8 Configure network settings**
- 9 Ready to complete stage 1

Configure network settings

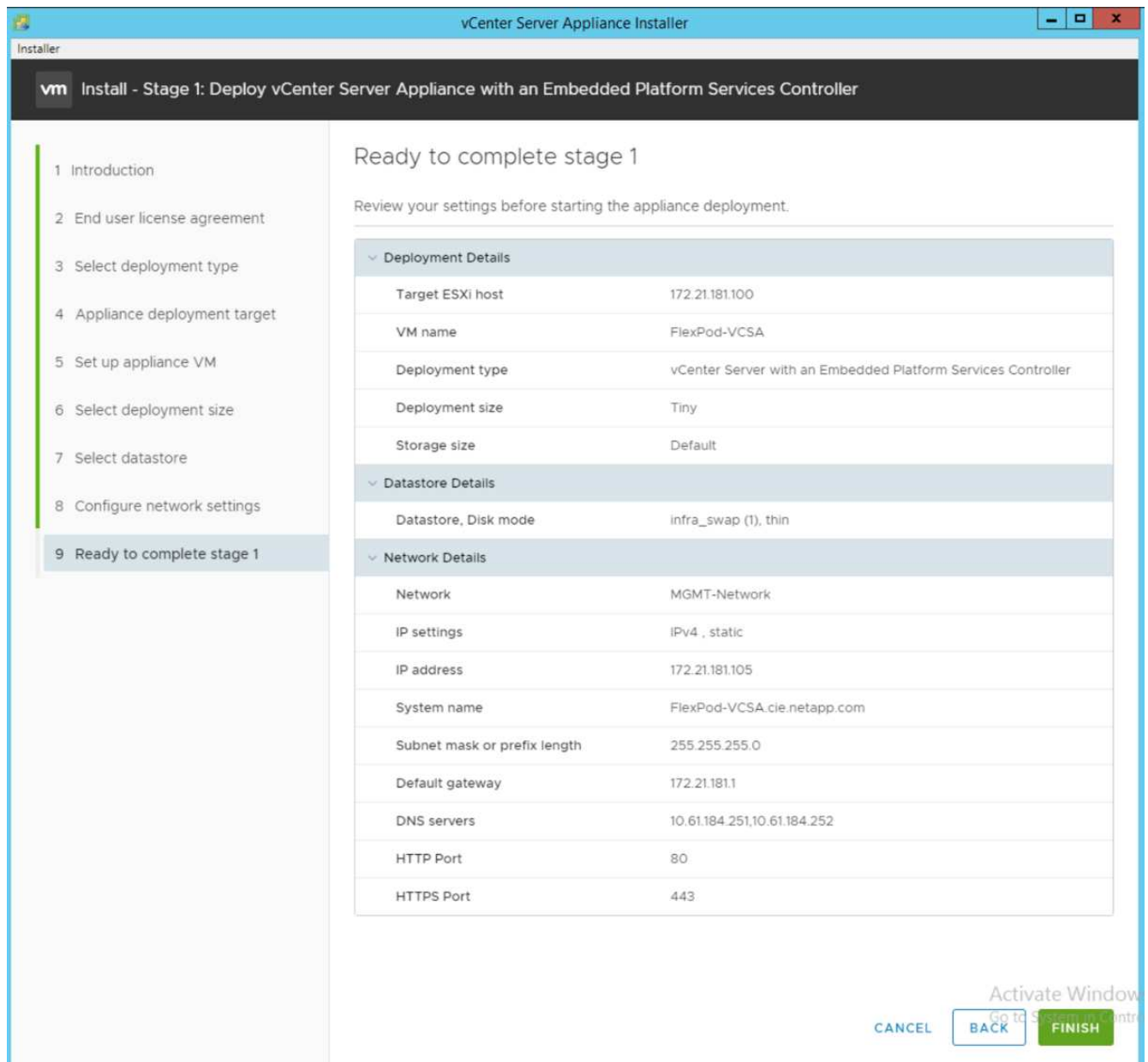
Configure network settings for this appliance

Network	MGMT-Network	ⓘ
IP version	IPv4	
IP assignment	static	
FQDN	FlexPod-VCSA.cie.netapp.com	ⓘ
IP address	172.21.181.105	
Subnet mask or prefix length	255.255.255.0	ⓘ
Default gateway	172.21.181.1	
DNS servers	10.61.184.251,10.61.184.252	
Common Ports		
HTTP	80	
HTTPS	443	

CANCEL BACK NEXT

Activate Windows
Go to System in Control

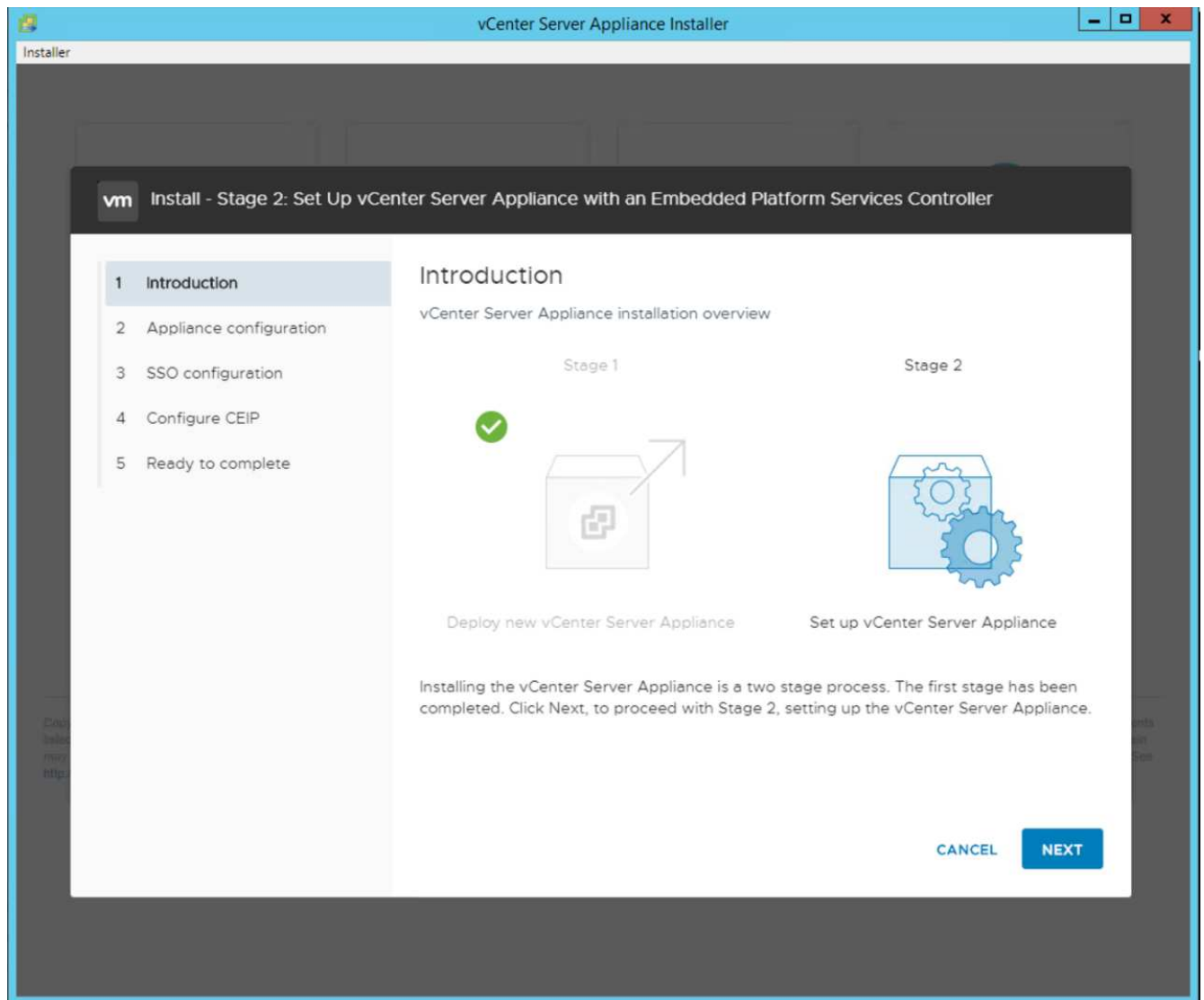
15. 开始部署设备之前，请查看第 1 阶段的设置。



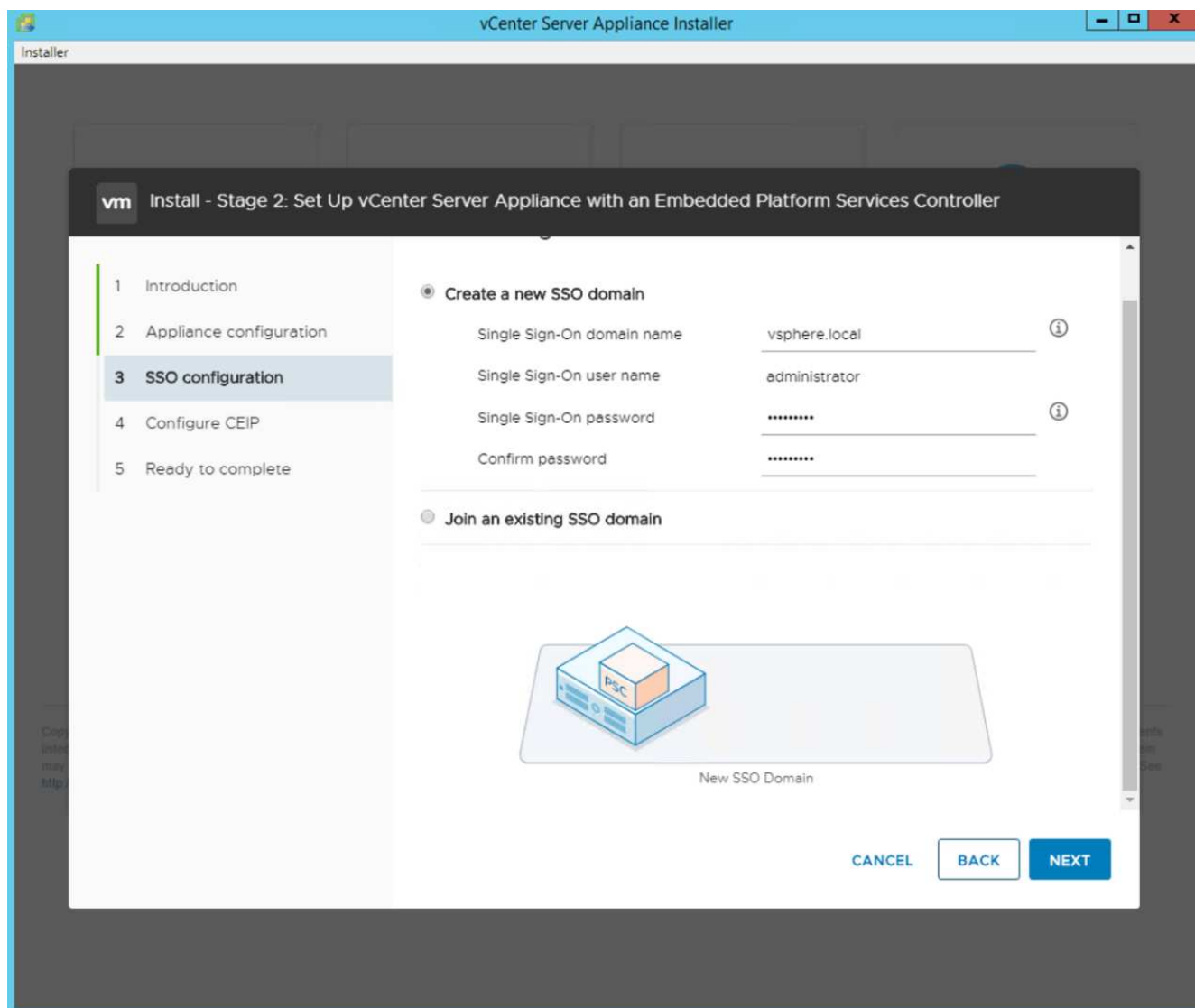
此时将安装 VCSA。此过程需要几分钟时间。

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。

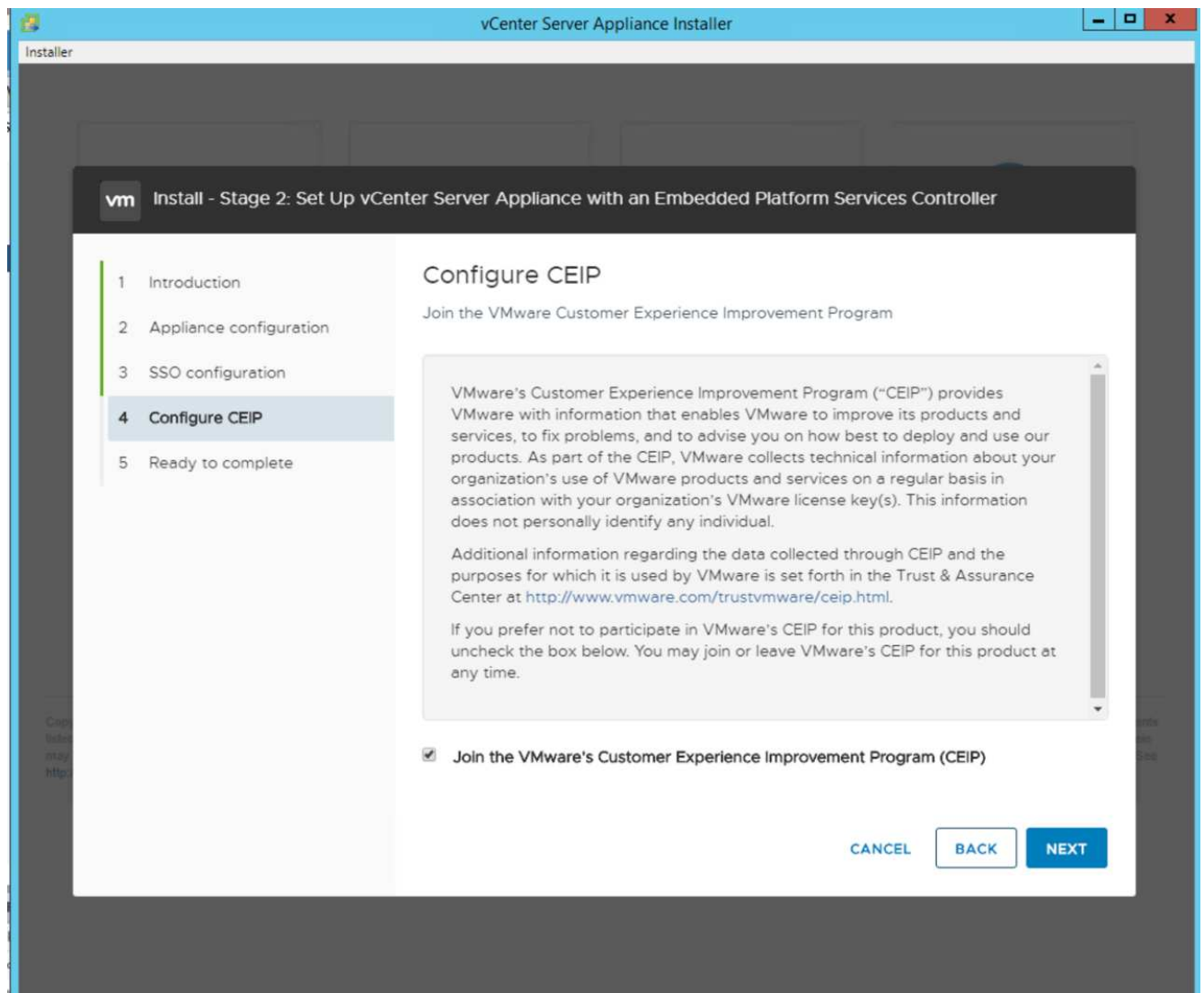


18. 输入 `<<var_ntp_id>>` 作为 NTP 服务器地址。您可以输入多个 NTP IP 地址。
19. 如果您计划使用 vCenter Server 高可用性（HA），请确保已启用 SSH 访问。
20. 配置 SSO 域名，密码和站点名称。单击下一步。

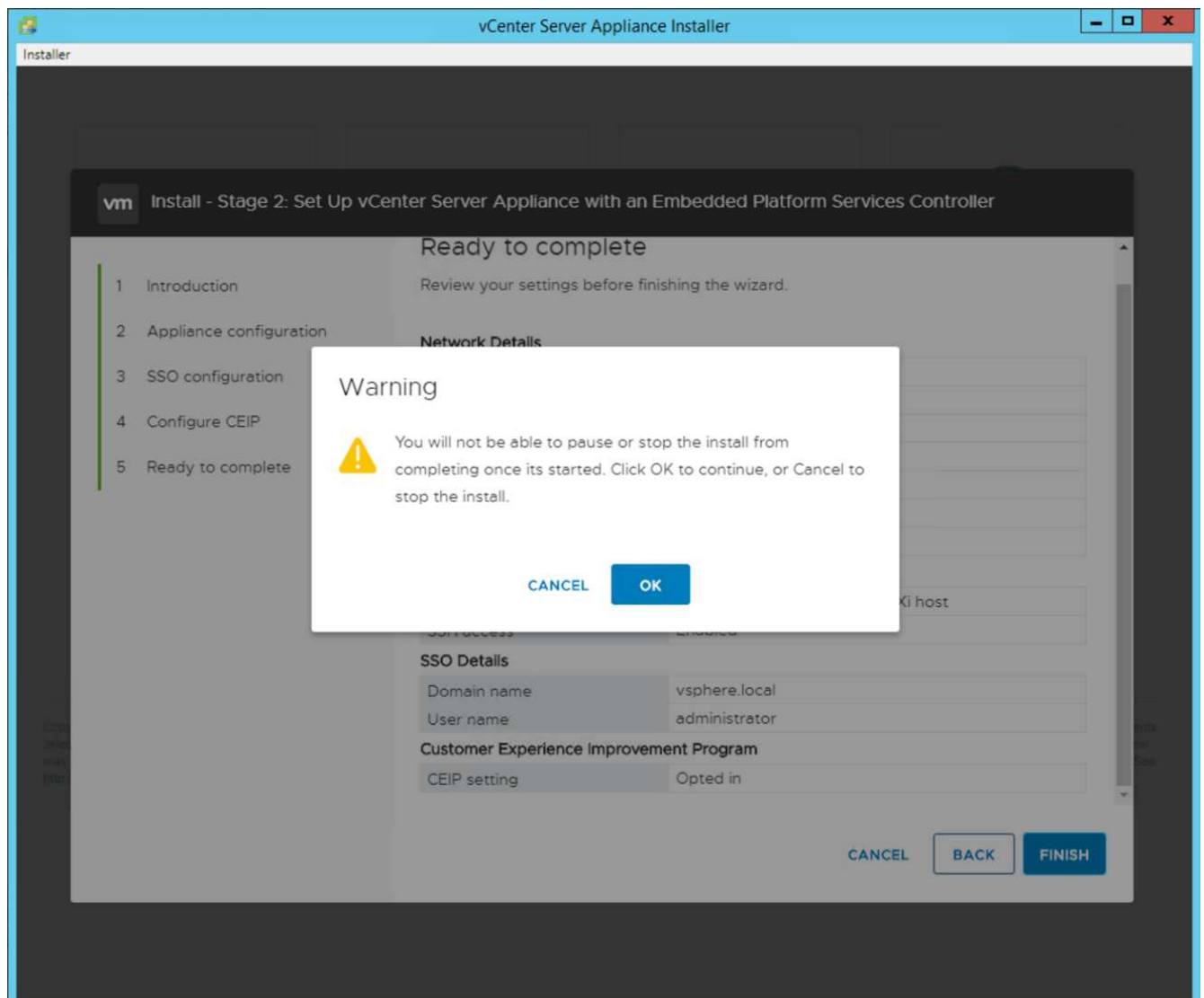


请记住这些值以供参考，特别是当您与 `vsphere.local` 域名有所偏差时。

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

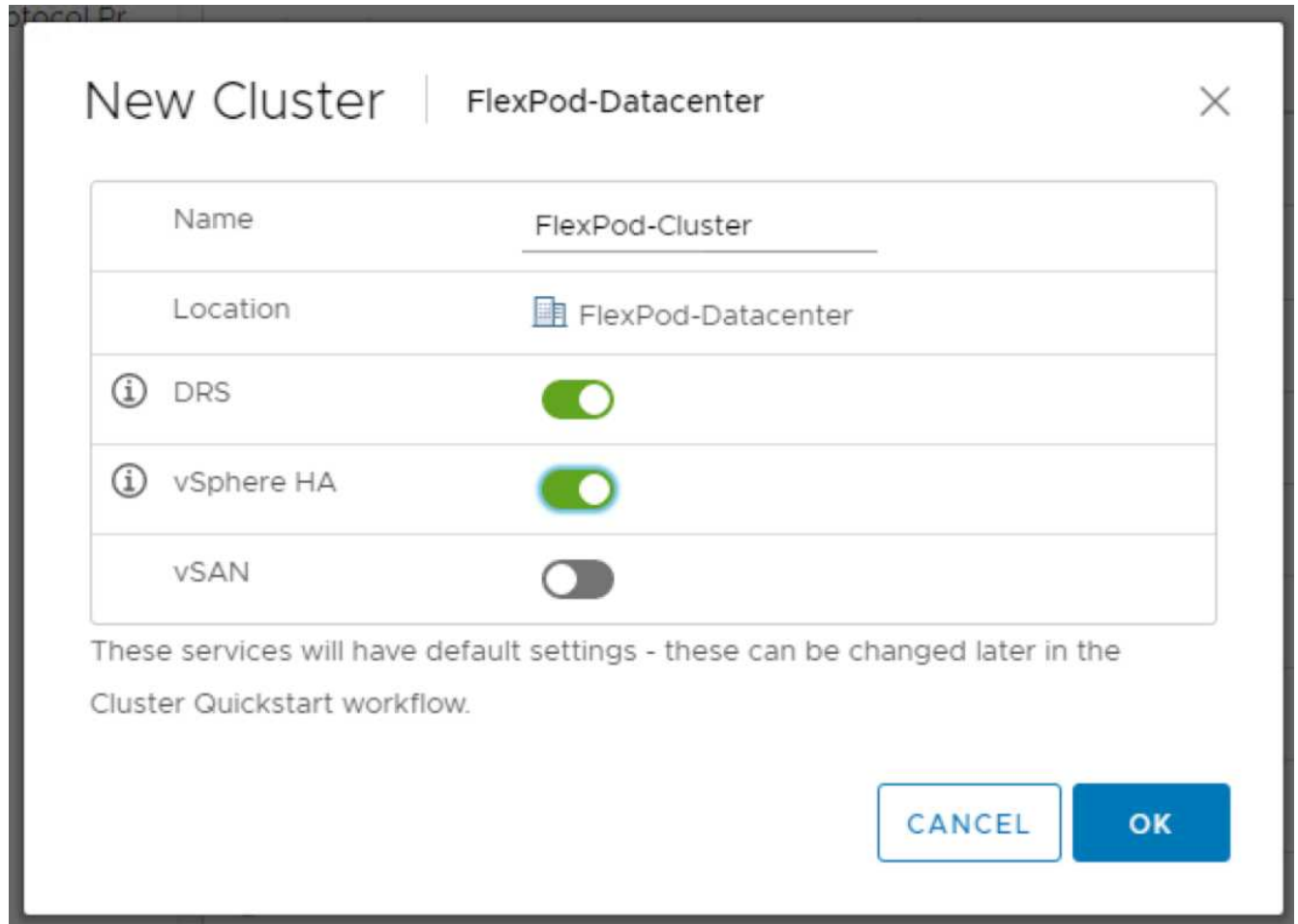
要配置 VMware vCenter Server 6.7 和 vSphere 集群，请完成以下步骤：

1. 导航到 `[https://<<FQDN 或 vCenter 的 IP >/vsphere-client/`。](https://<<FQDN 或 vCenter 的 IP >/vsphere-client/)
2. 单击 Launch vSphere Client。
3. 使用用户名 mailto: administrator@vsphere.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。



New Cluster | FlexPod-Datacenter

Name	FlexPod-Cluster
Location	 FlexPod-Datacenter
 DRS	<input checked="" type="checkbox"/>
 vSphere HA	<input checked="" type="checkbox"/>
vSAN	<input type="checkbox"/>

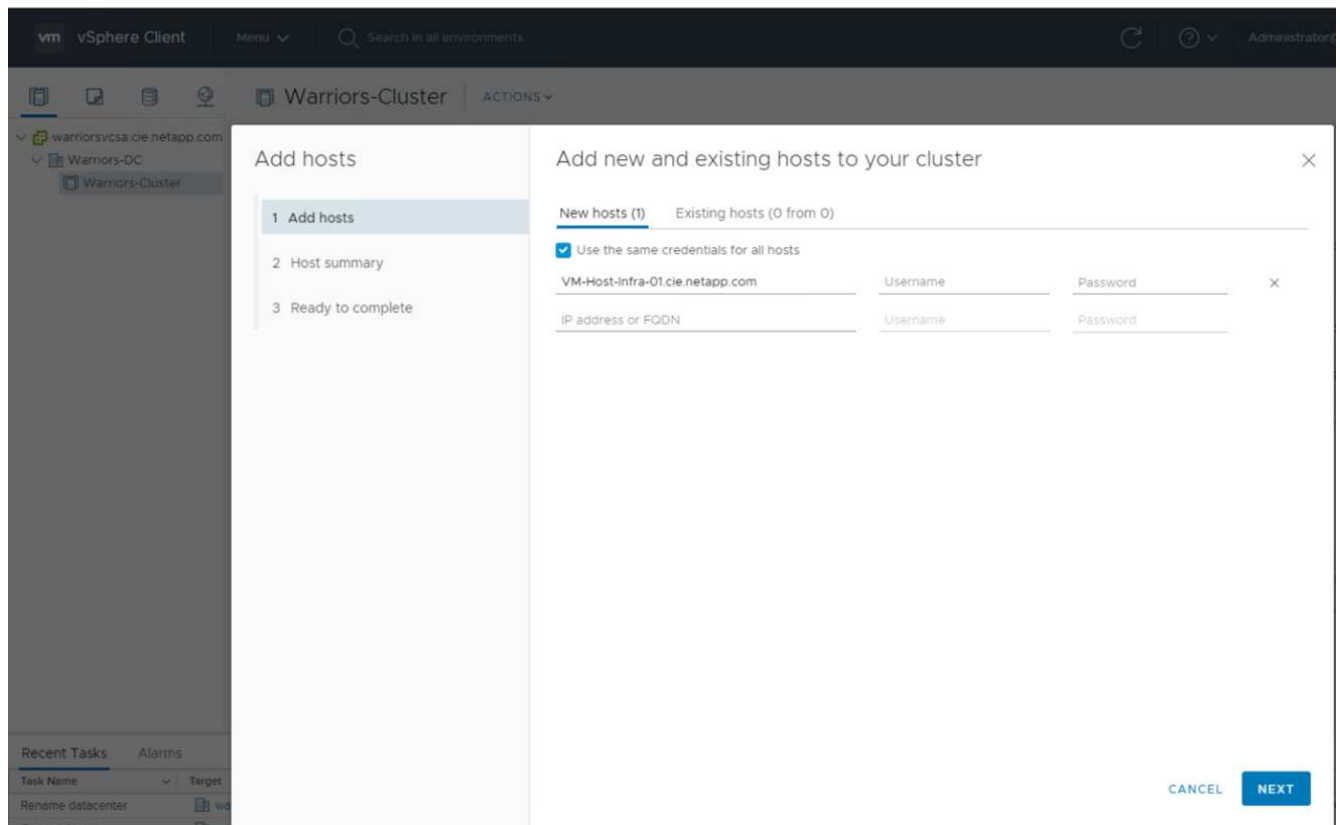
These services will have default settings - these can be changed later in the Cluster Quickstart workflow.

CANCEL **OK**

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。

← → ↻ ⚠ Not secure | 172.21.181.105:5480/ui/services

vm Appliance Management
 Mon 10-28-2019 06:51 AM UTC

Summary
 Monitor
 Access
 Networking
 Firewall
 Time
 Services
 Update
 Administration
 Syslog
 Backup

RESTART START STOP

	Name
<input type="radio"/>	vSAN health Service
<input type="radio"/>	VMware vSphere Web Client
<input type="radio"/>	VMware vSphere Update Manager
<input type="radio"/>	VMware vSphere Profile-Driven Storage Service
<input checked="" type="radio"/>	VMware vSphere ESXi Dump Collector
<input type="radio"/>	VMware vSphere Client
<input type="radio"/>	VMware vSphere Authentication Proxy
<input type="radio"/>	VMware vService Manager
<input type="radio"/>	VMware vSAN Data Protection Service
<input type="radio"/>	VMware vCenter-Services
<input type="radio"/>	VMware vCenter Server
<input type="radio"/>	VMware vCenter High Availability
<input type="radio"/>	VMware Topology Service

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。

```
root@VM-Host-Infra-01:~] esxcli system coredump network set -i 172.21.181.105 -
vmk0 -o 6500
root@VM-Host-Infra-01:~]
root@VM-Host-Infra-01:~] esxcli system coredump network set --enable=true
root@VM-Host-Infra-01:~] esxcli system coredump network check
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。"

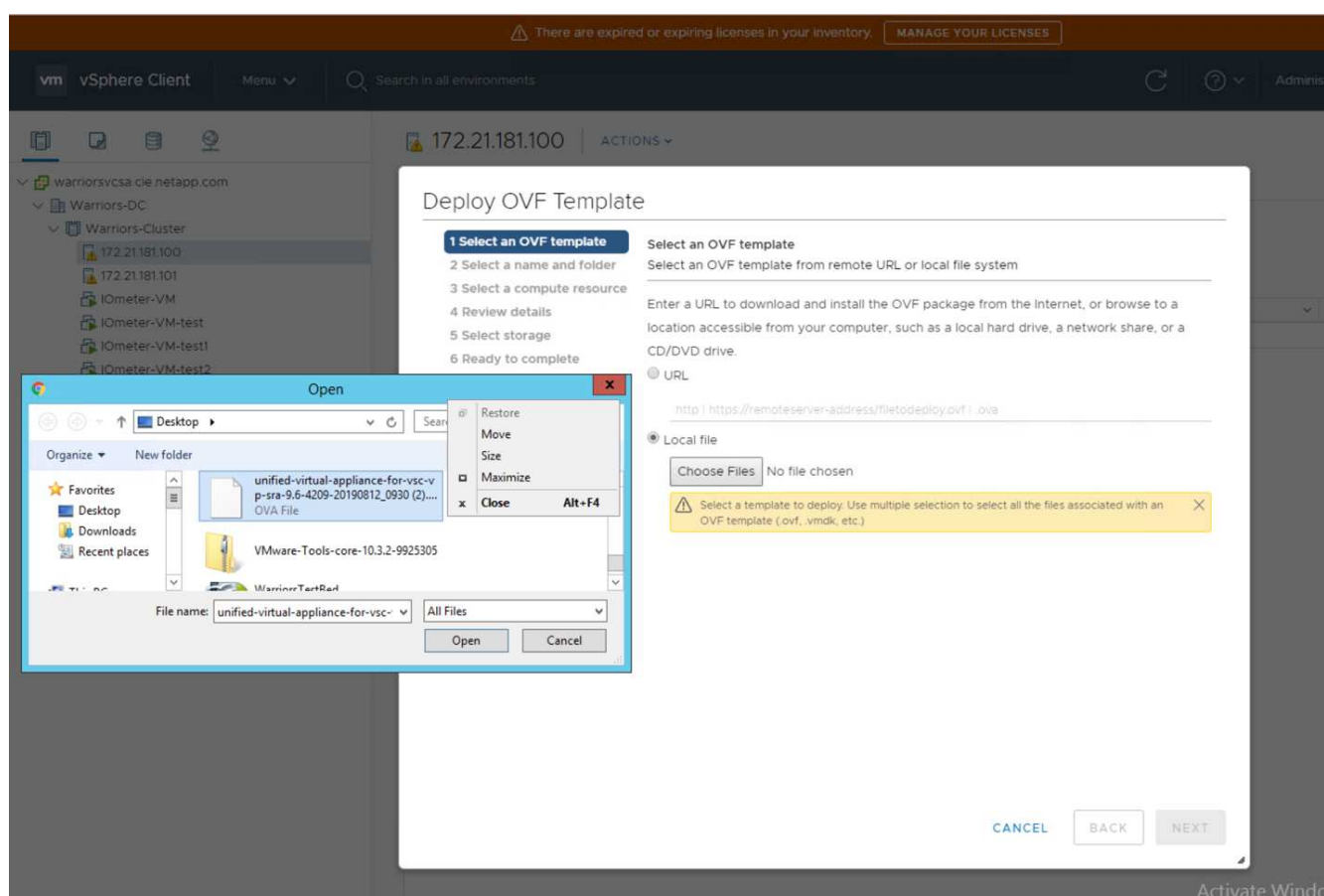
NetApp Virtual Storage Console 9.6 部署过程

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。

Deploy OVF Template

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

Select a name and folder

Specify a unique name and target location

Virtual machine name: FlexPod-VSC

Select a location for the virtual machine.

- ▼ warriorsvcsa.cie.netapp.com
 - > FlexPod-Datacenter

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。

Deploy OVF Template

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

Review details

Verify the template details.

Publisher	No certificate present
Product	Virtual Appliance - NetApp VSC, VASA Provider and SRA for ONTAP
Version	See appliance for version
Vendor	NetApp Inc.
Description	Virtual Appliance - NetApp VSC, VASA Provider, and SRA virtual appliance for NetApp storage systems. For more information or support please visit http://www.netapp.com/
Download size	1.0 GB
Size on disk	2.1 GB (thin provisioned)
	53.0 GB (thick provisioned)

CANCEL

BACK

NEXT

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。

Deploy OVF Template

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

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thin Provision

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type
infra_datastore	75 GB	360 KB	75 GB	NF
infra_datastore1	475 GB	639.9 GB	276.86 GB	NF
infra_swap (1)	100 GB	4.98 GB	95.02 GB	NF

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

8. 在 Select Networks 中，选择一个目标网络，然后单击 Next。

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

✓ 3 Select a compute resource

✓ 4 Review details

✓ 5 License agreements

✓ 6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	MGMT-Network

1 items

IP Allocation Settings

IP allocation:

Static - Manual

IP protocol:

IPv4

CANCEL

BACK

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。

Deploy OVF Template

✓ 1 Select an OVF template

✓ 2 Select a name and folder

✓ 3 Select a compute resource

✓ 4 Review details

✓ 5 License agreements

✓ 6 Select storage

✓ 7 Select networks

✓ 8 Customize template

9 Ready to complete

vCenter Server Address (*)

Specify the IP address/hostname of an existing vCenter to register to.

172.21.181.105

Port (*)

Specify the HTTPS port of an existing vCenter to register to.

443

Username (*)

Specify the username of an existing vCenter to register to.

administrator@vsphere.local

Password (*)

Specify the password of an existing vCenter to register to.

Password

Confirm Password

.....

.....

Network Properties

8 settings

Host Name

Specify the hostname for the appliance. (Leave blank if DHCP is desired)

CANCEL

BACK

NEXT

- 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。
- 启动 NetApp-VSC VM 并打开 VM 控制台。
- 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

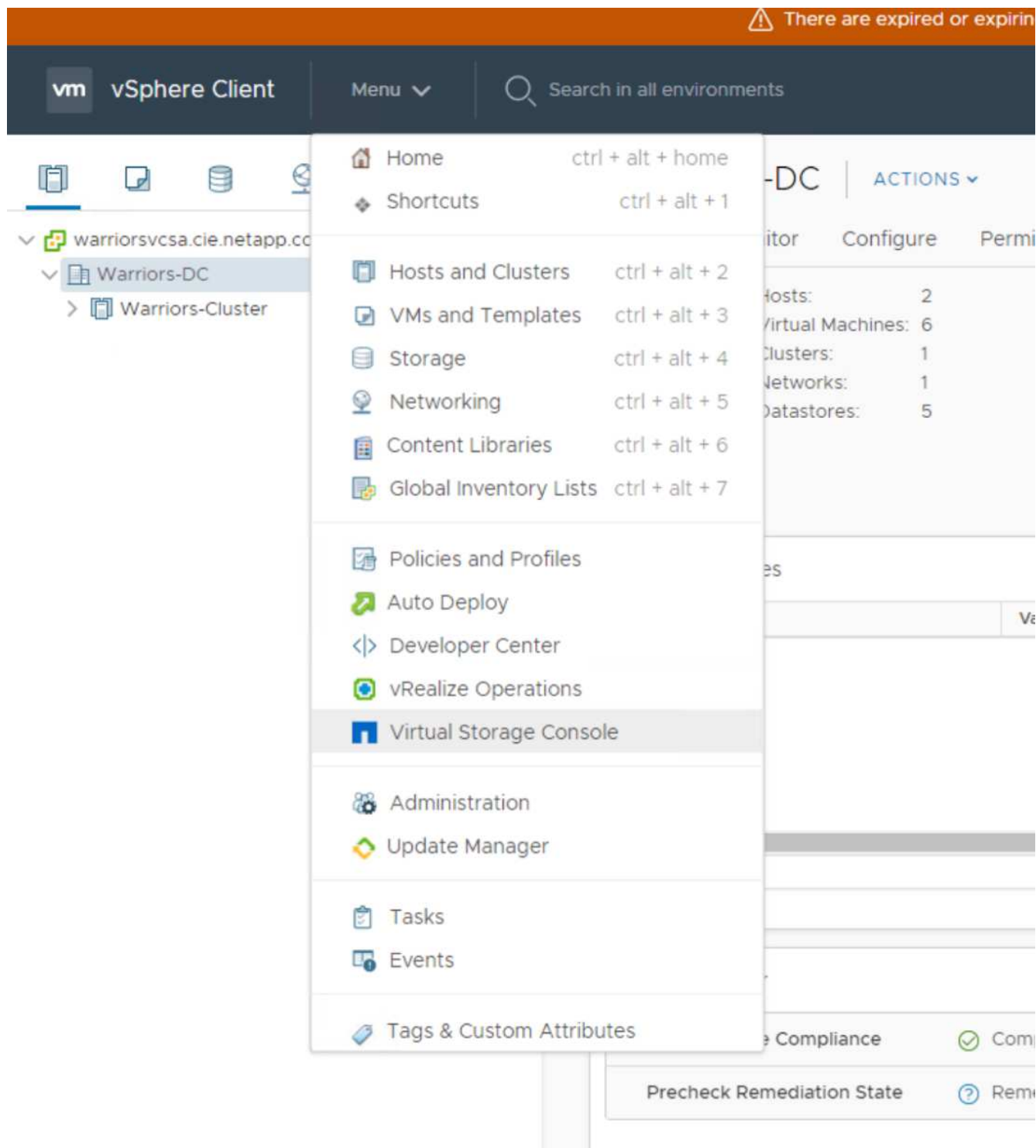
Click on "Install VMware Tools" pop-up box on the vSphere Web Client.

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。

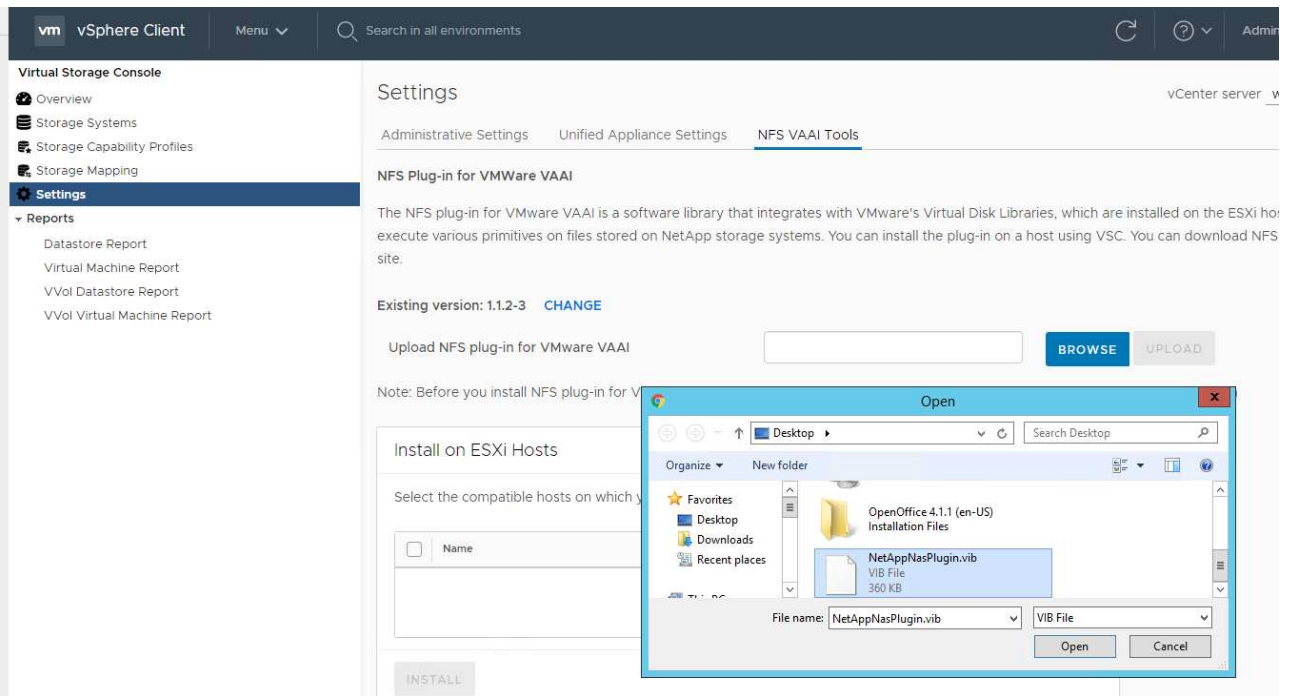


下载并安装 **NetApp NFS VAAI** 插件

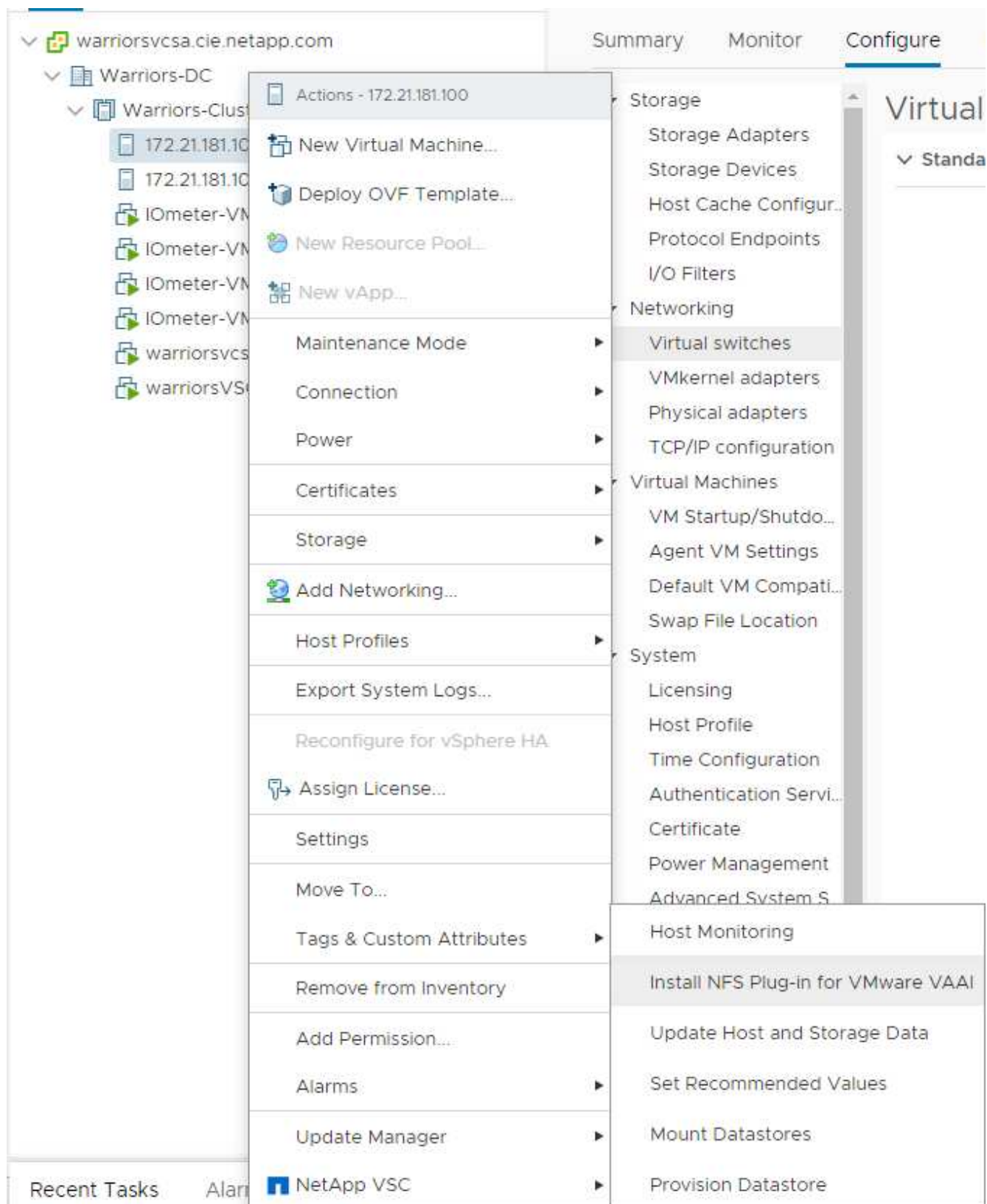
要下载并安装 NetApp NFS VAAI 插件，请完成以下步骤：

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。



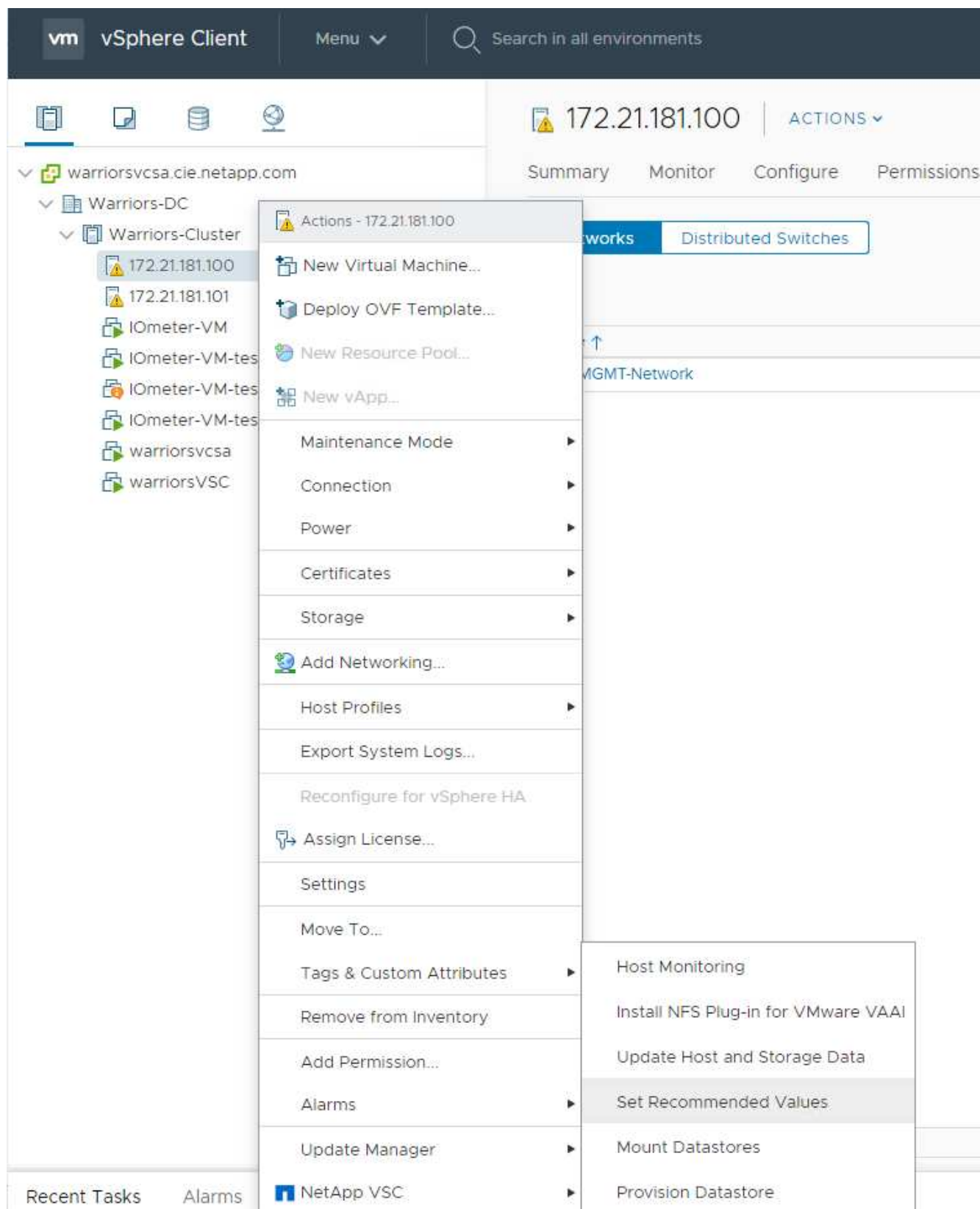
3. 单击上传将此插件传输到 vCenter 。
4. 选择主机，然后选择 NetApp VSC > 安装适用于 VMware VAAI 的 NFS 插件。



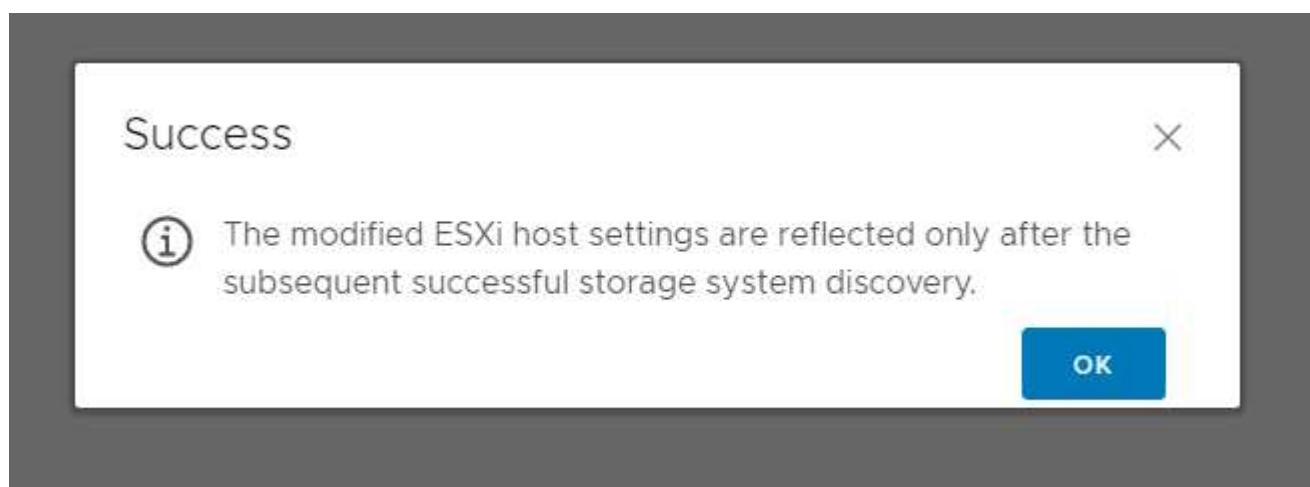
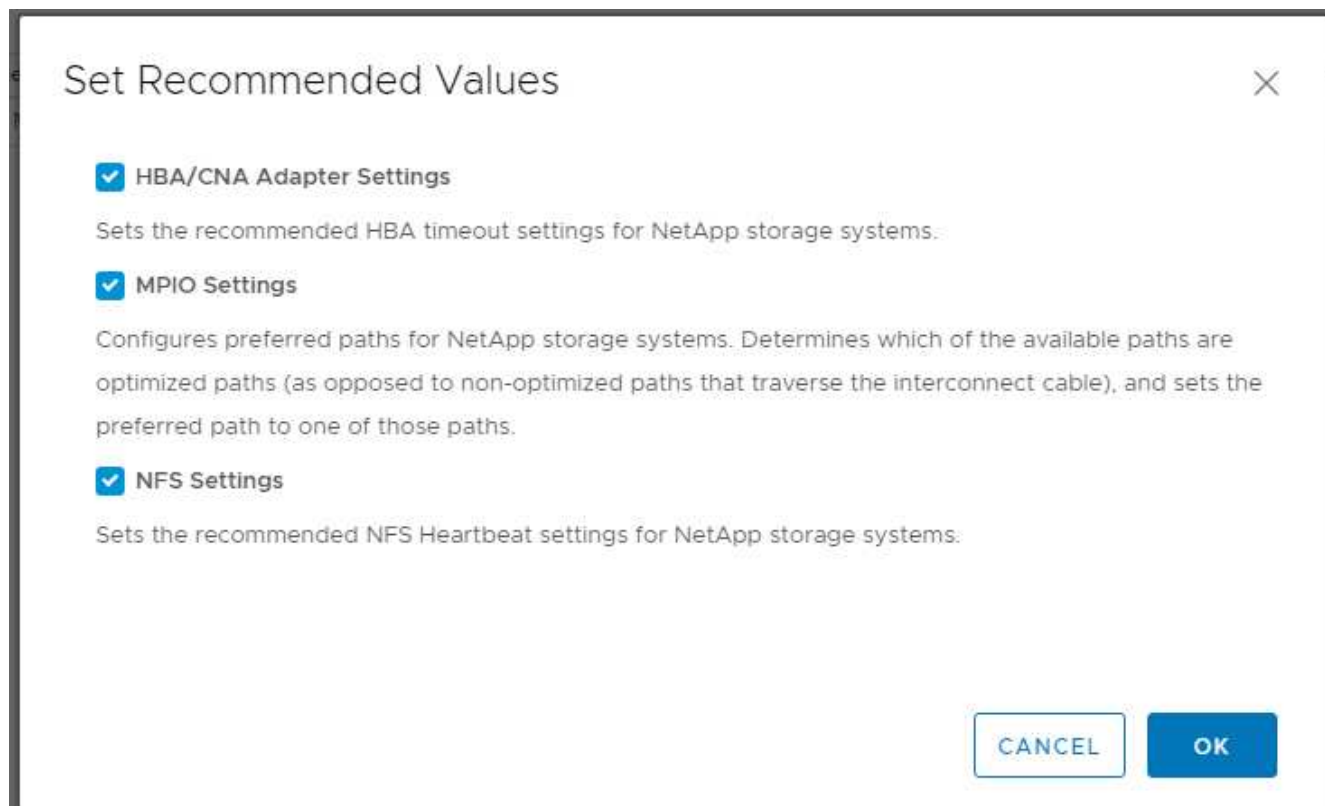
对 **ESXi** 主机使用最佳存储设置

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](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"](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。"](#)

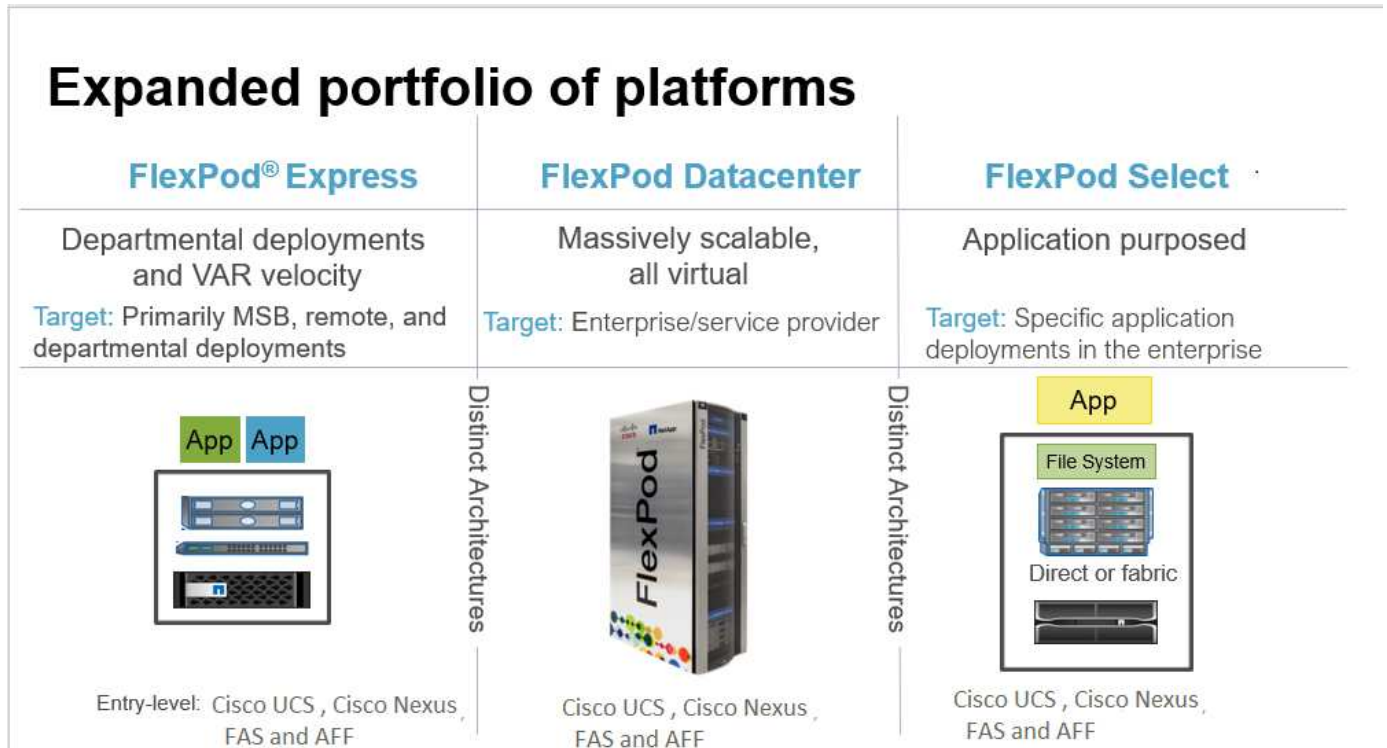
计划摘要

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。

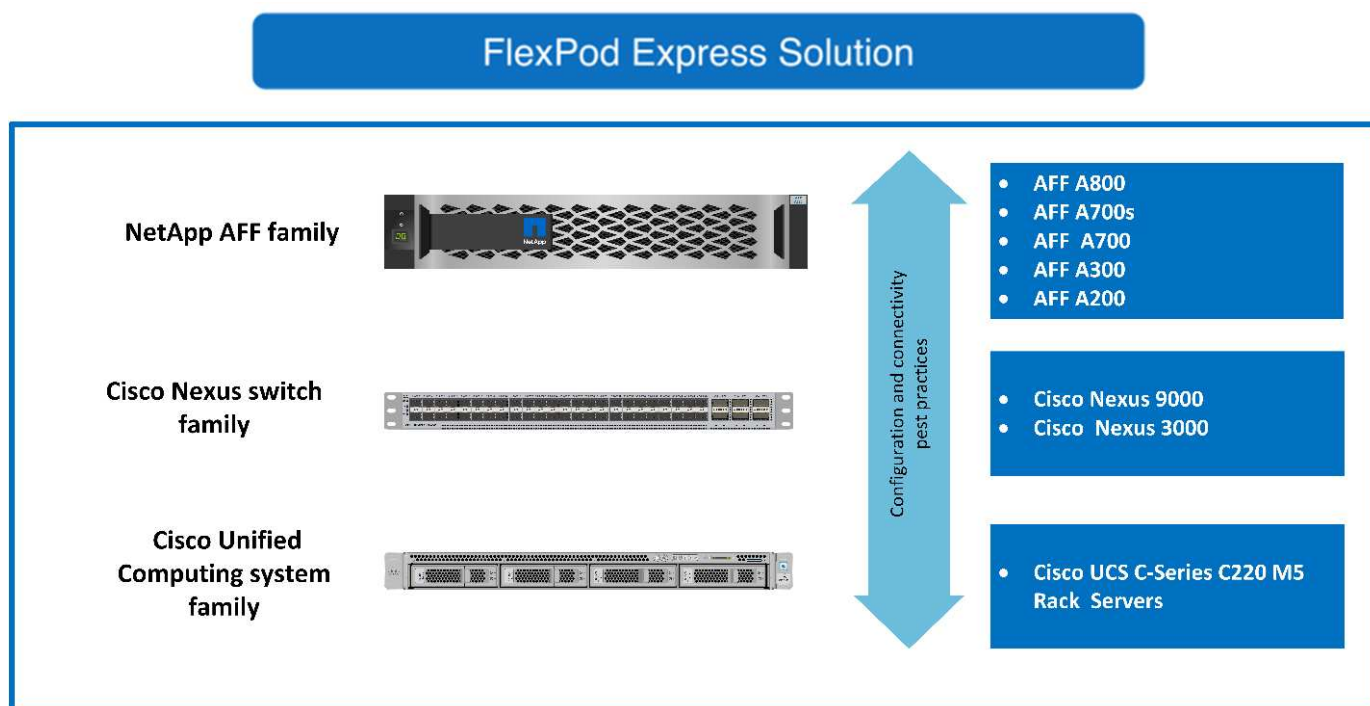
尽管本文档已针对 AFF A220 进行了验证，但此解决方案也支持 FAS2700 。

"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。



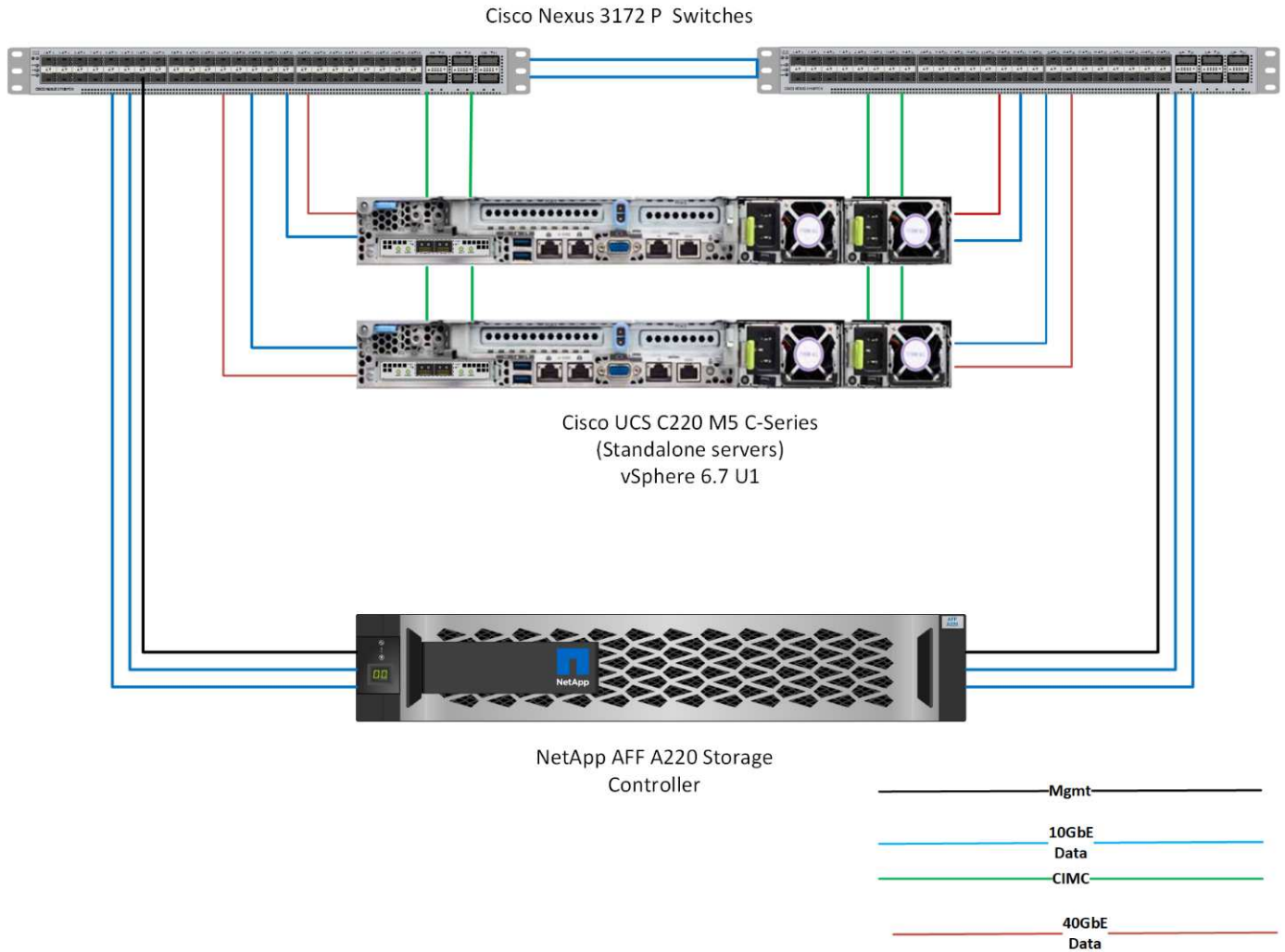
目标受众

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。

FlexPod Express



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

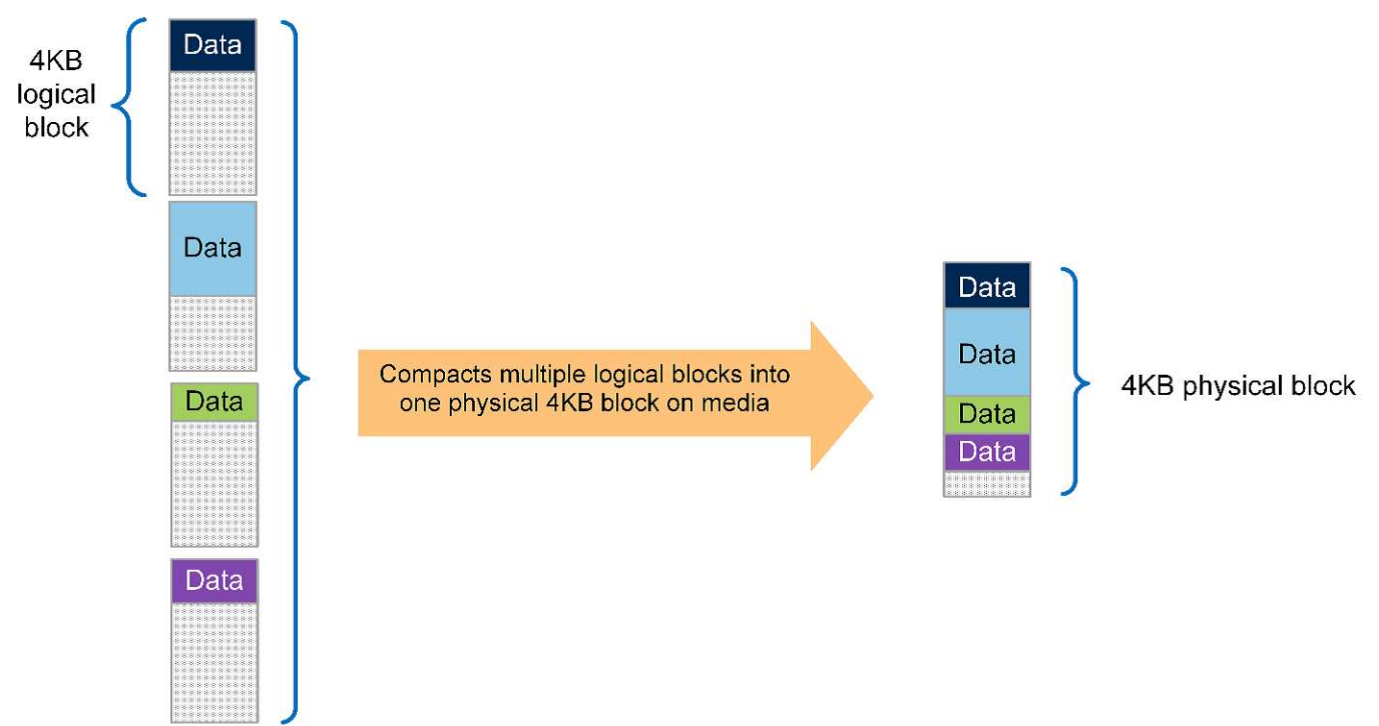
有关 AFF A220 硬件系统的详细信息，请参见 "[AFF A 系列主页](#)"。

ONTAP 9.4 软件

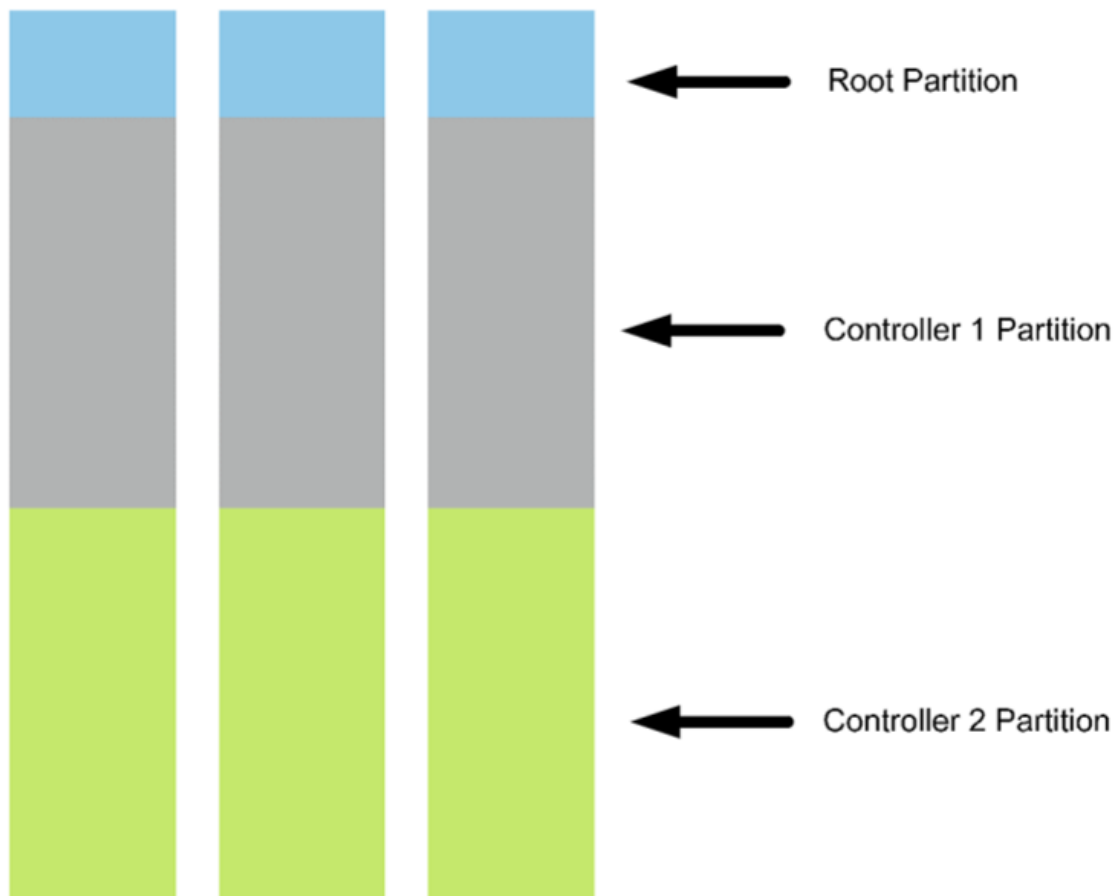
NetApp AFF A220 系统使用新的 ONTAP 9.4 软件。ONTAP 9.4 是行业领先的企业级数据管理软件。它将更高

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"](#)。此外，请参见NetApp ["ONTAP 9 文档中心"](#)，它已更新为包括ONTAP 9.4。

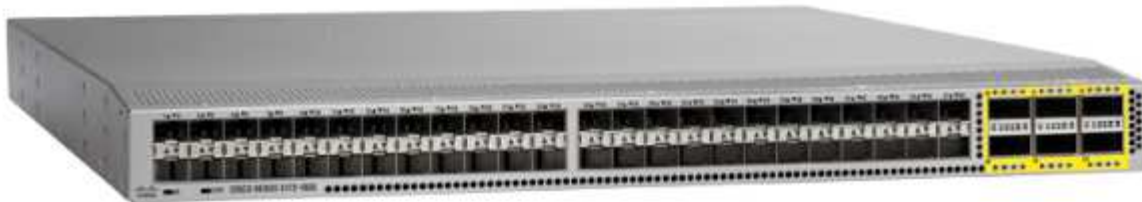
Cisco Nexus 3000 系列

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"](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"](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

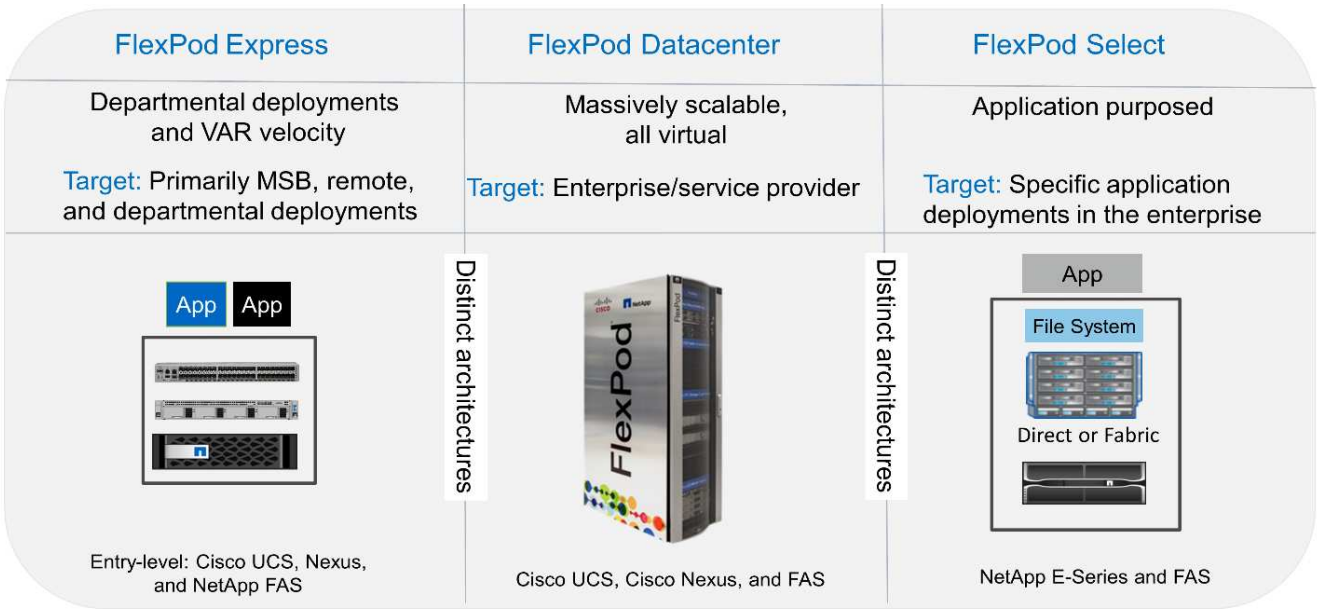
此 FlexPod Express 解决方案是 FlexPod 融合基础架构计划的一部分。

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调整。

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：

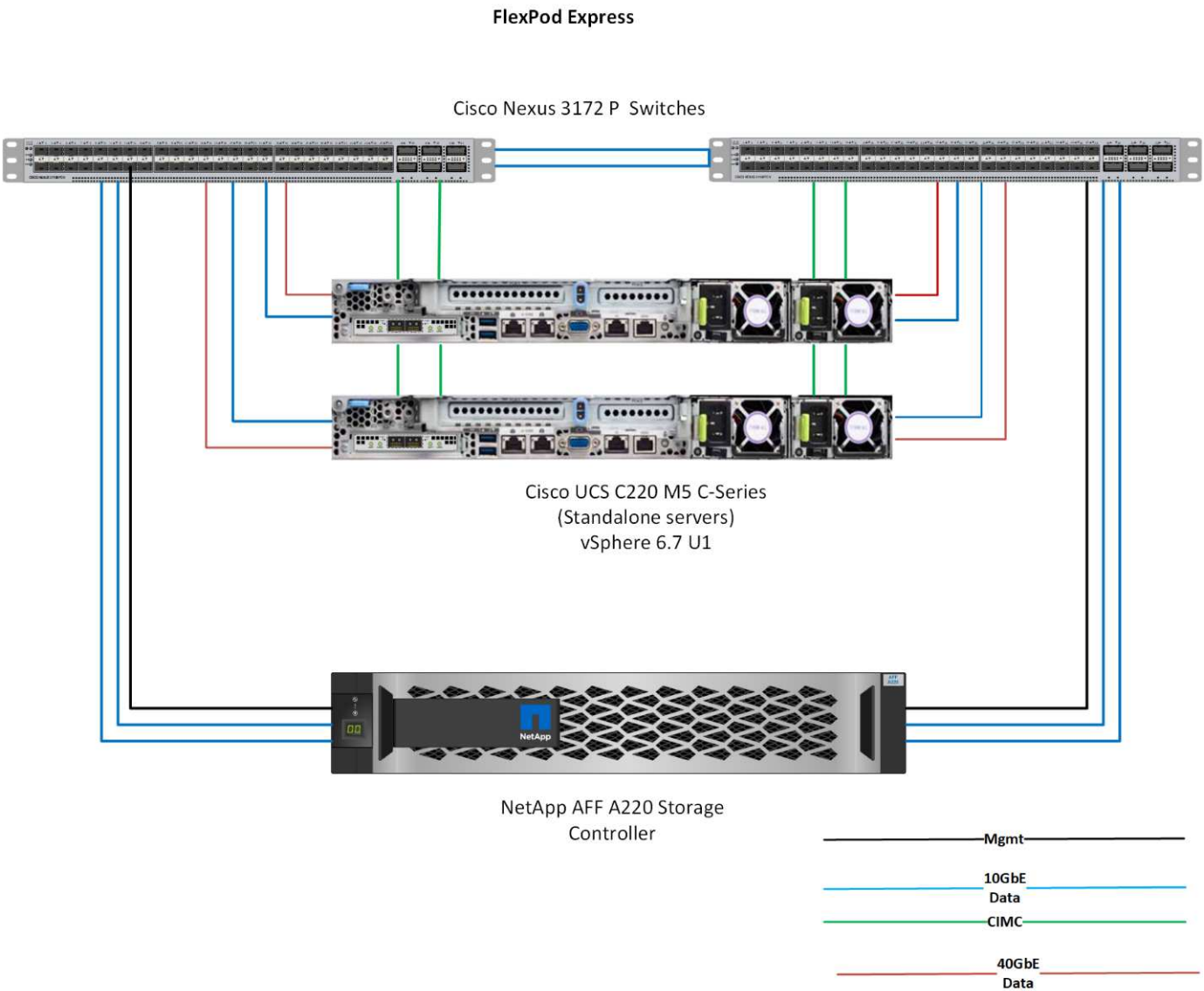
- 经过全面测试
- 具有规范性
- 最大限度地降低部署风险
- 加快上市速度

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。

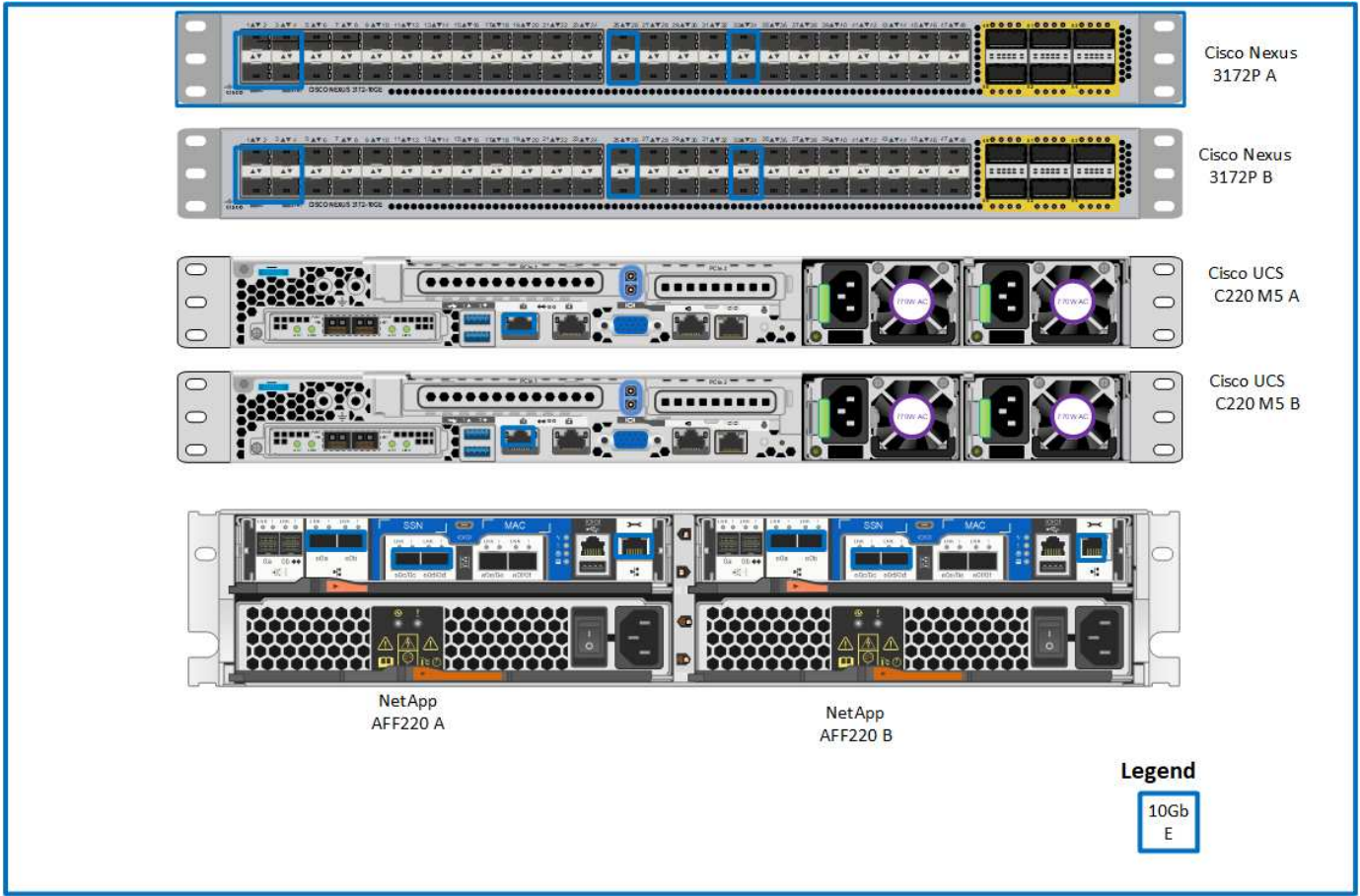
软件	version	详细信息
Cisco 集成管理控制器（CIMC）	3.1（3g）	适用于 Cisco UCS C220 M5 机架式服务器
Cisco nenic 驱动程序	1.0.25.0	适用于 VIC 1387 接口卡
Cisco NX-OS	nxos.7.0.3.17.5.bin	适用于 Cisco Nexus 3172P 交换机
NetApp ONTAP	9.4	适用于 AFF A220 控制器

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 xxxxx 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

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 Pol1
    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 Pol2
    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。

- 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>>
```

- 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>>
```

- 按 Enter 输入用户名，表示无用户名。
- 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。
- 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。

- 按 Ctrl-C 进入启动菜单。
- 选择选项 4 以清除配置并初始化所有磁盘。
- 输入 `y` 将磁盘置零，重置配置并安装新的文件系统。
- 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。

- 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。

Guided Setup to Configure a Cluster

Provide the information required below to configure your cluster:

The interface shows a progress bar with four steps: 1. Cluster (active), 2. Network, 3. Support, and 4. Summary.

Cluster Name [Text Field]

Nodes
 ⓘ Not sure all nodes have been discovered? Refresh

Diagram showing two nodes connected by an HA-PAR link. Each node is labeled FAS2650 and 621630000092. Each node has a green checkmark and a text field.

Cluster Configuration: ☐ Switched Cluster ☐ Switchless Cluster

ⓘ Username admin

Password [Text Field]

Confirm Password [Text Field]

Cluster Base License (Optional) [Text Field]

ⓘ For any queries related to licenses, contact mysupport.netapp.com

Feature Licenses (Optional) [Text Field: Enter comma separated license keys...]

ⓘ Cluster Base License is mandatory to add Feature Licenses.

Submit

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。

Guided Setup to Configure a Cluster

Provide the information required below to configure your cluster:



? AutoSupport ☒

? Proxy URL (Optional)

i Connection is verified after configuring AutoSupport on all nodes.

? Event Notifications

Notify me through:



Email

SMTP Mail Host

Email Addresses

Separate email addresses with a comma...



SNMP

SNMP Trap Host



Syslog

Syslog Server

Submit

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。

```
AFF A220::> ucadmin show
```

Node	Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin 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 vservers 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,fc
```

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
```

- 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
```

- 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
```

- 要获取以下步骤中所需参数的值，请运行 `security certificate show` 命令。
- 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
```

- 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。

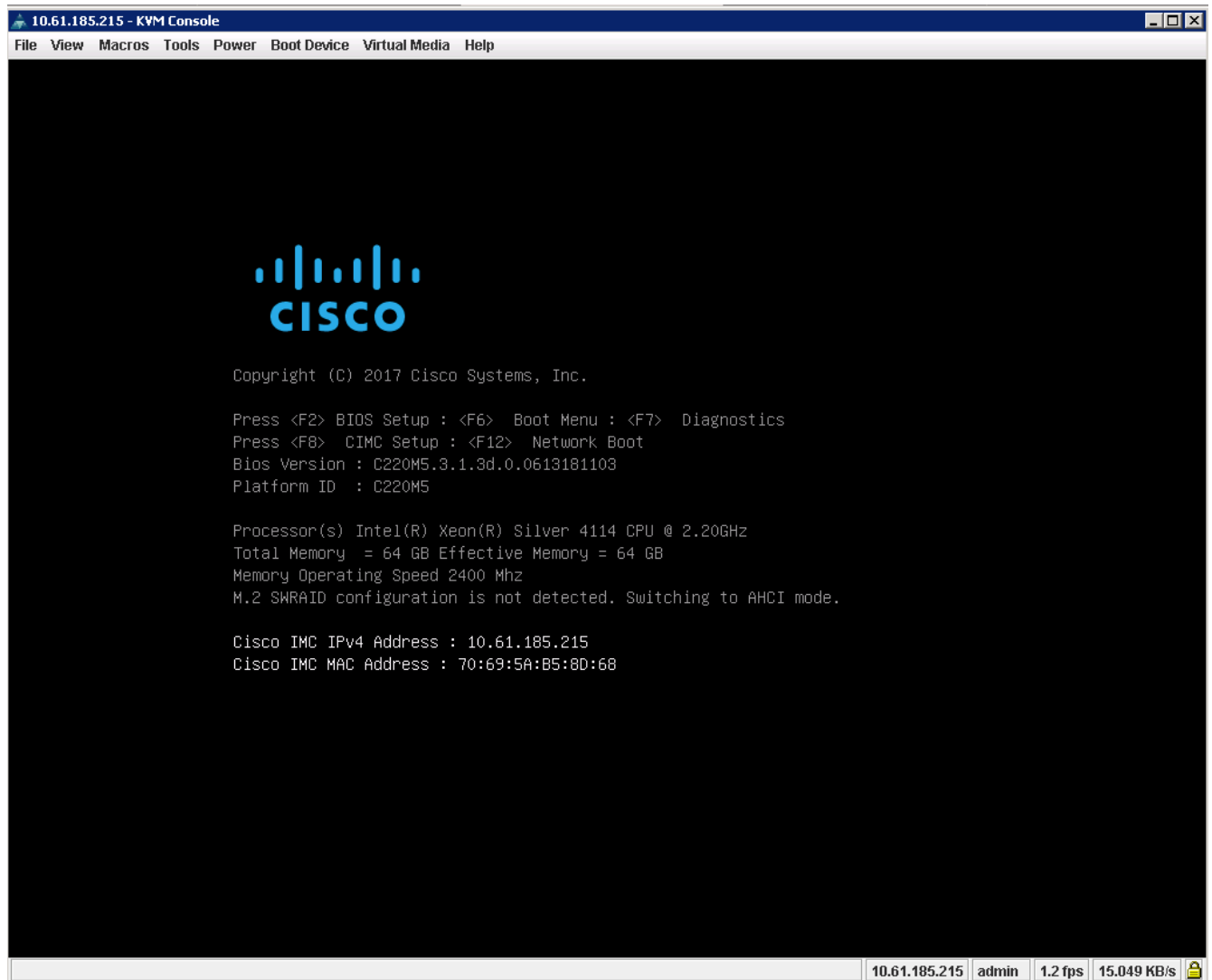
详细信息	详细信息值
CIMC IP 地址	<<CMC_IP>>
CIMC 子网掩码	<<CIMC 网络掩码 >>
CIMC 默认网关	<<CIMC 网关 >>



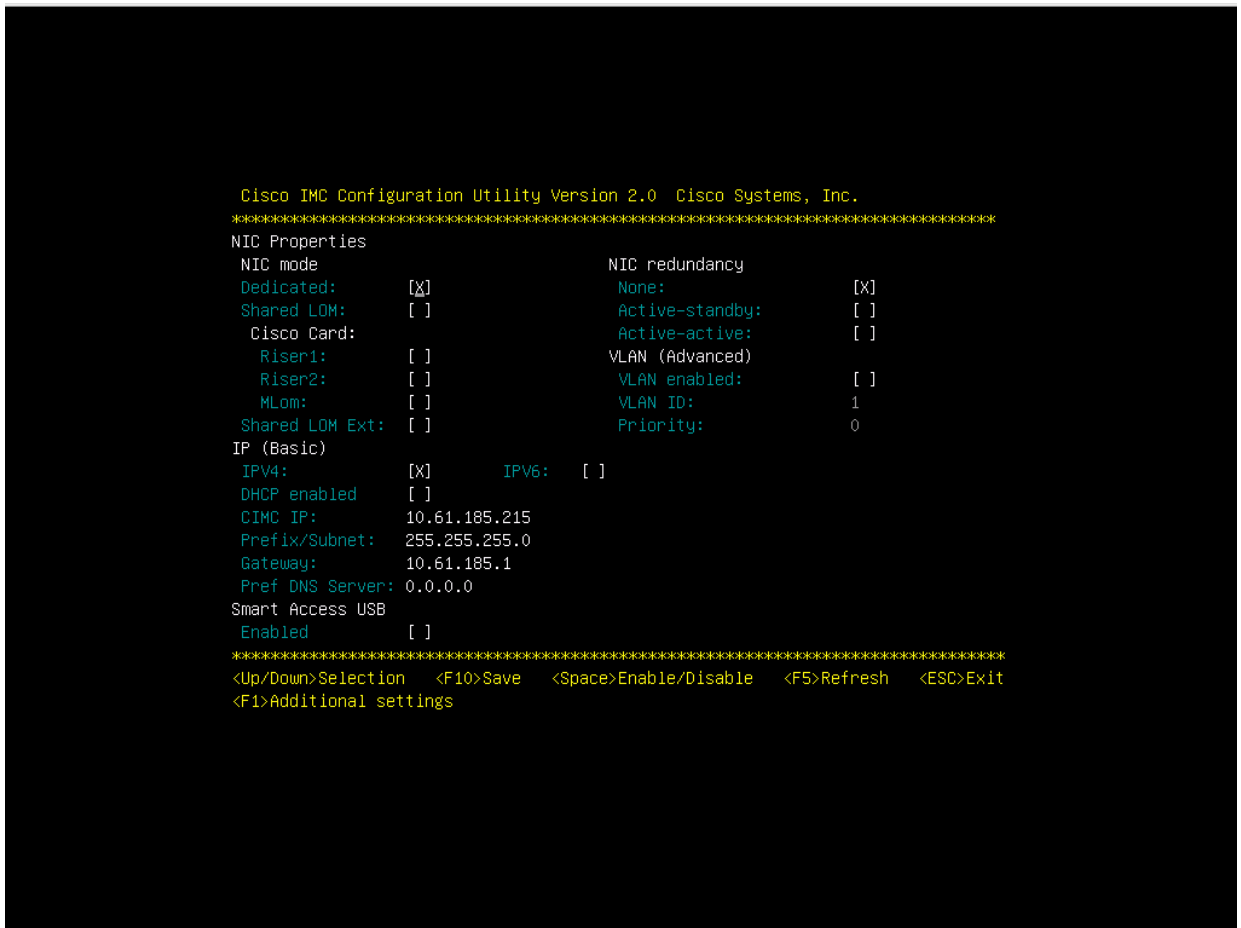
此验证中使用的 CIMC 版本为 CIMC 3.1.3 （g）。

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。


```
Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
Common Properties
  Hostname:      CIMC-Tiger-02
  Dynamic DNS:   [X]
  DDNS Domain:
FactoryDefaults
  Factory Default:      [ ]
Default User(Basic)
  Default password:      -
  Reenter password:
Port Properties
  Auto Negotiation:      [X]
                                Admin Mode      Operation Mode
  Speed[1000/100/10Mbps]:      Auto              1000
  Duplex mode[half/full]:      Auto              full
Port Profiles
  Reset:                  [ ]
  Name:
*****
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F2>PreviousPageettings
```

- 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。

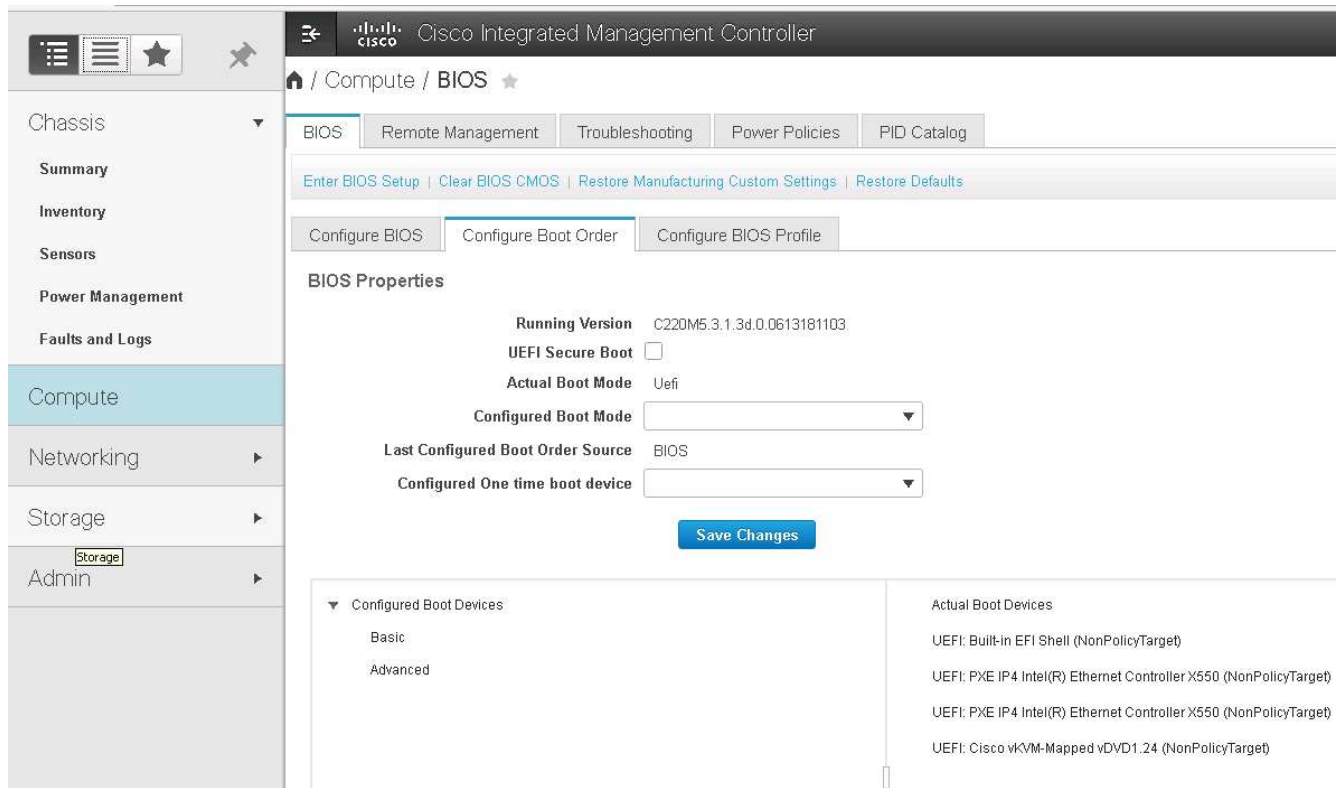
详细信息	详细信息值
ESXi 主机启动程序 A 名称	<<var_UCS_initiator_name_A>>
ESXi 主机 iSCSI-A IP	<<var_esxi_host_iscsiA_IP>>
ESXi 主机 iSCSI-A 网络掩码	<<var_esxi_host_iscsiA_mask>>
ESXi 主机 iSCSI 是默认网关	<<var_esxi_host_iscsiA_gateway>>
ESXi 主机启动程序 B 名称	<<var_UCS_initiator_name_B>>
ESXi 主机 iSCSI-B IP	<<var_esxi_host_iscsiB_ip>>
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。

Configure Boot Order

Configured Boot Level: Advanced

Basic Advanced

Add Boot Device

- Add Local HDD
- Add PXE Boot
- Add SAN Boot
- Add iSCSI Boot
- Add USB
- Add Virtual Media
- Add PCHStorage
- Add UEFISHELL
- Add SD Card
- Add NVME
- Add Local CDD

Advanced Boot Order Configuration

Selected 1 / Total 3

Enable/Disable	Name	Type	Order	State
<input checked="" type="checkbox"/>	KVM-MAPPED-DVD	VMEDIA	1	Enabled
<input type="checkbox"/>	iSCSI-A	ISCSI	2	Enabled
<input type="checkbox"/>	iSCSI-B	ISCSI	3	Enabled

Save Changes Reset Values Close

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。

- 单击 CIMC 左侧导航窗格中的 BIOS。
- 选择 Configure BIOS。
- 向下滚动到 PCIe 插槽：HBA 选项 ROM。
- 如果尚未禁用此值，请将其设置为 disabled。

BIOS	Remote Management	Troubleshooting	Power Policies	PID Catalog	
I/O	Server Management	Security	Processor	Memory	Power/Performance

Note: Default values are shown in bold.

Reboot Host Immediately: ☒

Intel VT for directed IO: Enabled ▼

Intel VTD ATS support: Enabled ▼

LOM Port 1 OptionRom: Enabled ▼

Pcie Slot 1 OptionRom: Disabled ▼

MLOM OptionRom: Enabled ▼

Front NVME 1 OptionRom: Enabled ▼

MRAID Link Speed: Auto ▼

PCIe Slot 1 Link Speed: Auto ▼

Front NVME 1 Link Speed: Auto ▼

VGA Priority: Onboard ▼

P-SATA OptionROM: LSI SW RAID ▼

USB Port Rear: Enabled ▼

USB Port Internal: Enabled ▼

IPV6 PXE Support: Disabled ▼

Legacy USB Support: Enabled ▼

Intel VTD coherency support: Disabled ▼

All Onboard LOM Ports: Enabled ▼

LOM Port 2 OptionRom: Enabled ▼

Pcie Slot 2 OptionRom: Disabled ▼

MRAID OptionRom: Enabled ▼

Front NVME 2 OptionRom: Enabled ▼

MLOM Link Speed: Auto ▼

PCIe Slot 2 Link Speed: Auto ▼

Front NVME 2 Link Speed: Auto ▼

M.2 SATA OptionROM: AHCI ▼

USB Port Front: Enabled ▼

USB Port KVM: Enabled ▼

USB Port:M.2 Storage: Enabled ▼

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

▼ vNIC Properties

▼ General

Name: iscsi-vNIC-A

CDN: VIC-MLOM-iscsi-vNIC-A

MTU: 9000 (1500 - 9000)

Uplink Port: 0 ▼

MAC Address: ☐ Auto ☒ 70:69:5A:C0:98:ED

Class of Service: 0 (0 - 6)

Trust Host CoS: ☒

PCI Order: 4 (0 - 5)

Default VLAN: ☐ None ☒ 3439

VLAN Mode: Trunk ▼

Rate Limit: ☒ OFF ☐ ?

Channel Number: N/A (1 - 1000)

PCI Link: 0 (0 - 1)

Enable NVGRE: ☐

Enable VXLAN: ☐

Advanced Filter: ☐

Port Profile: N/A ▼

Enable PXE Boot: ☒

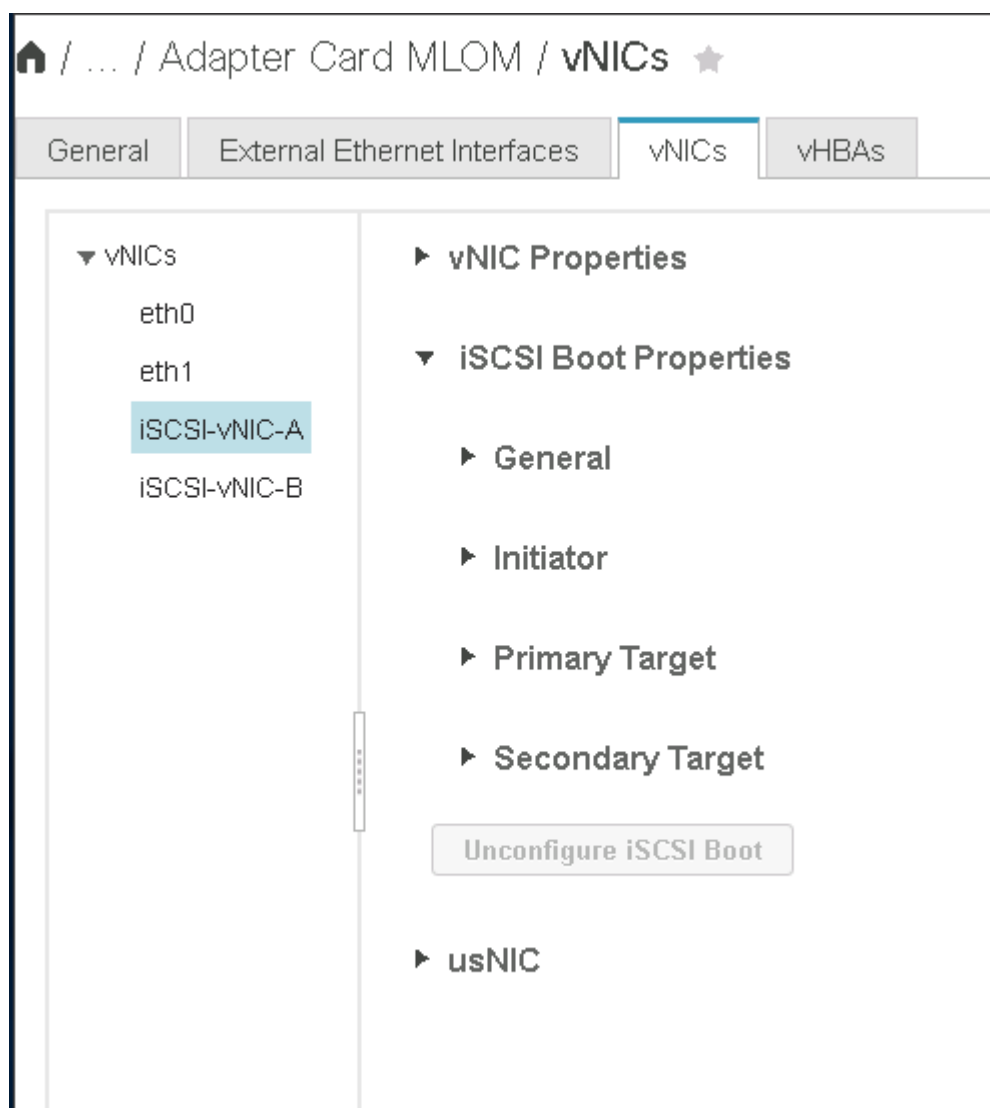
Enable VMQ: ☐

Enable aRFS: ☐

Enable Uplink Failover: ☐

Failback Timeout: N/A (0 - 600)

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]`

▼ vNICs

eth0

eth1

ISCSI-v

ISCSI-v

▼ iSCSI Boot Properties

► General

▼ Initiator

Name: (0 - 233) chars

IP Address:

Subnet Mask:

Gateway:

Primary DNS:

► Initiator Priority:

Secondary DNS:

TCP Timeout:

CHAP Name:

CHAP Secret:

► Primary Target

► Secondary Target

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。

General
External Ethernet Interfaces
vNICs
vHBAs

vNICs
eth0
eth1
iscsi-v
iscsi-v

Initiator

Primary Target

Name: iqn.1992-08.com.netapp:sn.7e560f73a51 (0 - 233) chars
IP Address: 172.21.246.16
TCP Port: 3260

Boot LUN: 0
CHAP Name:
CHAP Secret:

Secondary Target

Name: iqn.1992-08.com.netapp:sn.7e560f73a51 (0 - 233) chars
IP Address: 172.21.246.18
TCP Port: 3260

Boot LUN: 0
CHAP Name:
CHAP Secret:

Unconfigure iSCSI Boot

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 。

🏠 / ... / Adapter Card

MLOM / vNICs ⭐

Refresh | Host Power | Launch KVM | Ping | CIMC Reboot | Locat

General | External Ethernet Interfaces | vNICs | vHBAs

▼ vNICs

eth0

eth1

ISCSI-v

ISCSI-v

Host Ethernet Interfaces

Selected 0

Add vNIC | Clone vNIC | Delete vNICs

	Name	CDN	MAC Address	MTU	usNIC	Uplink Port	CoS	VLAN	VLAN Mode
<input type="checkbox"/>	eth0	VIC-MLO...	70:69:5A:C0:98:49	1500	0	0	0	NONE	TRUNK
<input type="checkbox"/>	eth1	VIC-MLO...	70:69:5A:C0:98:4A	1500	0	1	0	NONE	TRUNK
<input type="checkbox"/>	iSCSI-v...	VIC-MLO...	70:69:5A:C0:98:4D	9000	0	0	0	3439	TRUNK
<input type="checkbox"/>	iSCSI-v...	VIC-MLO...	70:69:5A:C0:98:4E	9000	0	1	0	3440	TRUNK

- 3. 选择 eth0 并单击属性。
- 4. 将 MTU 设置为 9000 。单击 Save Changes 。

General
External Ethernet Interfaces
vNICs
vHBAs

▼ vNICs

eth0

eth1

ISCSI-v

ISCSI-v

Name: eth0
CDN: VIC-MLOM-eth0
MTU: 9000 (1500 - 9000)
Uplink Port: 0
MAC Address: ☐ Auto ☒ 70:69:5A:C0:98:49
Class of Service: 0 (0 - 6)
Trust Host CoS: ☐
PCI Order: 0 (0 - 5)
Default VLAN: ☒ None ☐ ?

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。

Home / ... / Adapter Card MLOM / vNICs ★

General
External Ethernet Interfaces
vNICs
vHBAs

▼ vNICs

eth0

eth1

ISCSI-vNIC-A

ISCSI-vNIC-B

Host Ethernet Interfaces

Add vNIC
Clone vNIC
Delete vNICs

	Name	CDN	MAC Address	MTU	usNIC	Uplink Port
<input type="checkbox"/>	eth0	VIC-MLO...	70:69:5A:C0:98:49	9000	0	0
<input type="checkbox"/>	eth1	VIC-MLO...	70:69:5A:C0:98:4A	9000	0	1
<input type="checkbox"/>	iSCSI-v...	VIC-MLO...	70:69:5A:C0:98:4D	9000	0	0
<input type="checkbox"/>	iSCSI-v...	VIC-MLO...	70:69:5A:C0:98:4E	9000	0	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

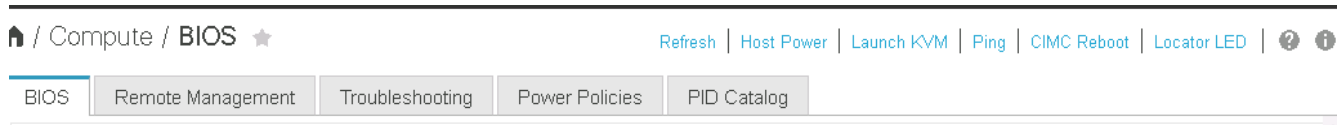
对于添加到集群中的任何其他节点，必须完成此操作步骤。

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

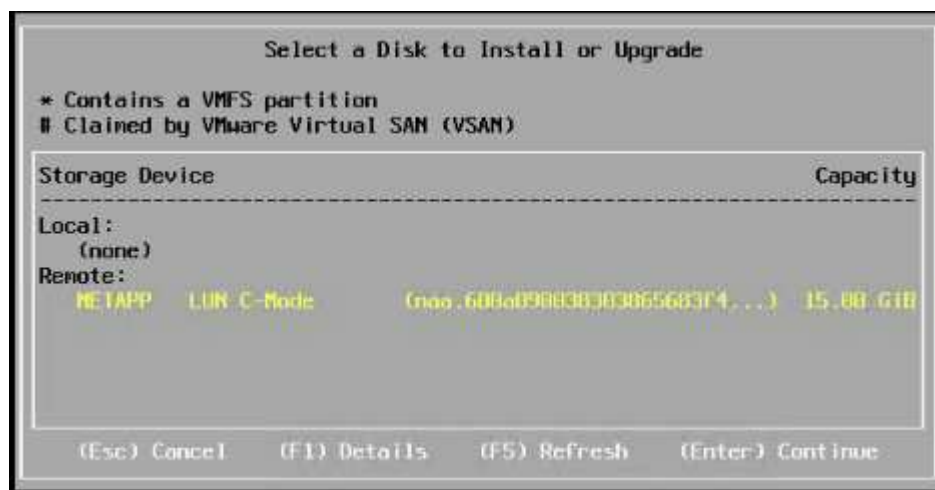
1. 导航到 "[VMware vSphere 下载页面](#)" 用于自定义 ISO。
2. 单击适用于 ESXi 6.7 GA 的 Cisco 自定义映像安装 CD 旁边的转至下载。
3. 下载适用于 ESXi 6.7 GA 的 Cisco 自定义映像安装 CD（ISO）。

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

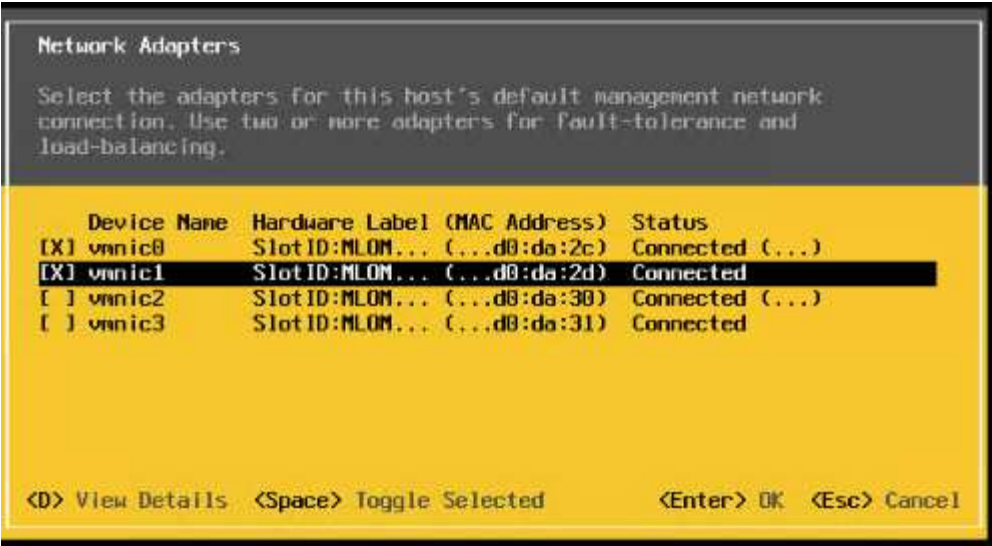
以下步骤介绍了如何为每个 VMware ESXi 主机添加管理网络。

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。

Add VMkernel NIC

Port group	New port group ▼
New port group	iScsiBootPG-B
Virtual switch	iScsiIBootvSwitch-B ▼
VLAN ID	3440
MTU	9000
IP version	IPv4 only ▼
▼ IPv4 settings	
Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
Address	172.21.184.63
Subnet mask	255.255.255.0
TCP/IP stack	Default TCP/IP stack ▼
Services	<input type="checkbox"/> vMotion <input type="checkbox"/> Provisioning <input type="checkbox"/> Fault tolerance logging <input type="checkbox"/> Management <input type="checkbox"/> Replication <input type="checkbox"/> NFC replication

Create Cancel

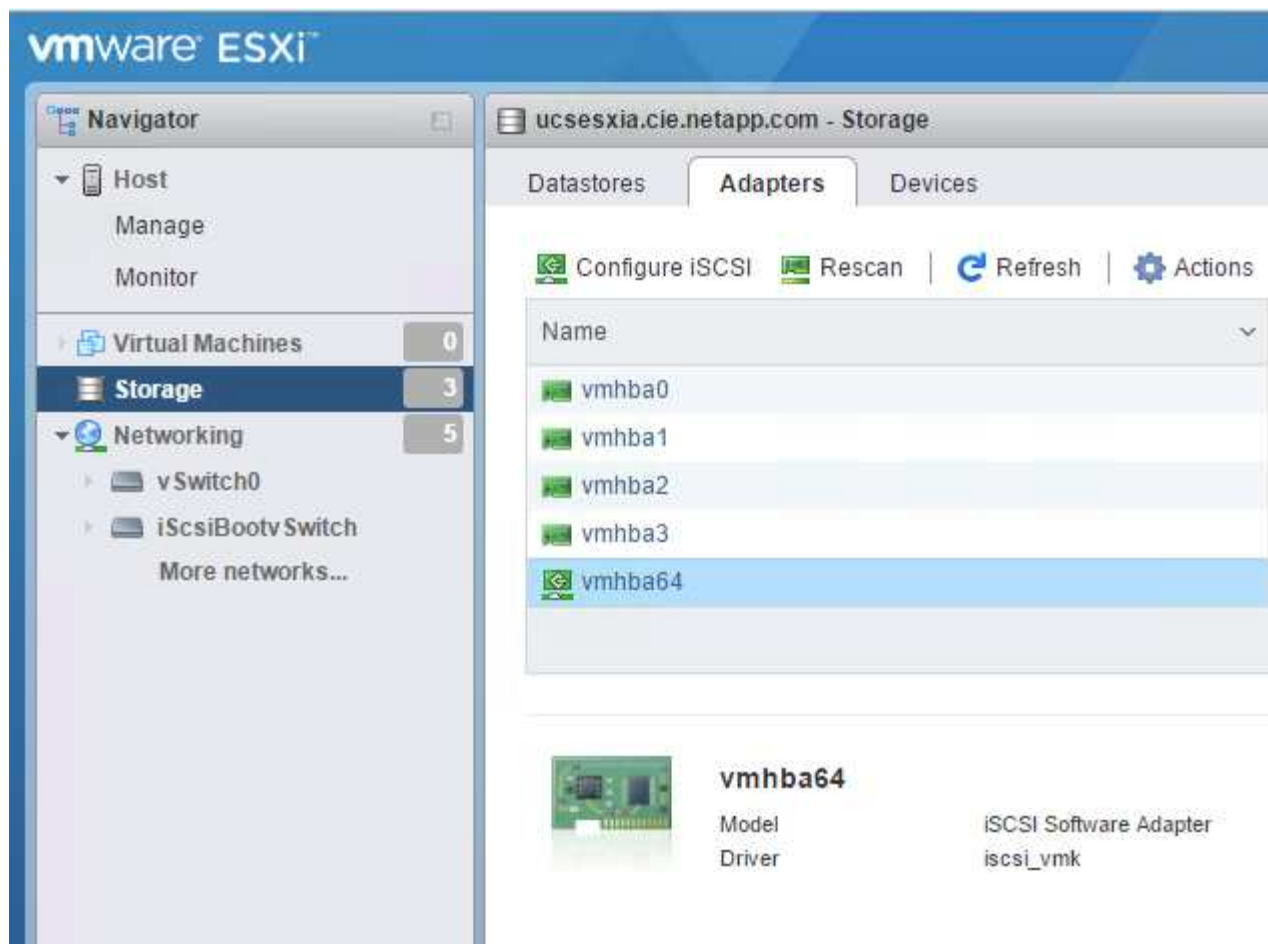


在 iScsiBootPg- A 上将 MTU 设置为 9000

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。

Configure iSCSI - vmhba64

iSCSI enabled	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled								
▶ Name & alias	iqn.1992-08.com.cisco:ucsaiscsia								
▶ CHAP authentication	Do not use CHAP ▼								
▶ Mutual CHAP authentication	Do not use CHAP ▼								
▶ Advanced settings	Click to expand								
Network port bindings	<div> Add port binding Remove port binding </div> <table border="1"> <thead> <tr> <th>VMkernel NIC</th> <th>Port group</th> <th>IPv4 address</th> </tr> </thead> <tbody> <tr> <td colspan="3">No port bindings</td> </tr> </tbody> </table>			VMkernel NIC	Port group	IPv4 address	No port bindings		
VMkernel NIC	Port group	IPv4 address							
No port bindings									
Static targets	<div> Add static target Remove static target Edit settings <input type="text" value="Search"/> </div> <table border="1"> <thead> <tr> <th>Target</th> <th>Address</th> <th>Port</th> </tr> </thead> <tbody> <tr> <td>iqn.1992-08.com.netapp:sn.09591199033811e78eb...</td> <td>172.21.183.34</td> <td>3260</td> </tr> </tbody> </table>			Target	Address	Port	iqn.1992-08.com.netapp:sn.09591199033811e78eb...	172.21.183.34	3260
Target	Address	Port							
iqn.1992-08.com.netapp:sn.09591199033811e78eb...	172.21.183.34	3260							
Dynamic targets	<div> Add dynamic target Remove dynamic target Edit settings <input type="text" value="Search"/> </div> <table border="1"> <thead> <tr> <th>Address</th> <th>Port</th> </tr> </thead> <tbody> <tr> <td colspan="2">No dynamic targets</td> </tr> </tbody> </table>			Address	Port	No dynamic targets			
Address	Port								
No dynamic targets									

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。

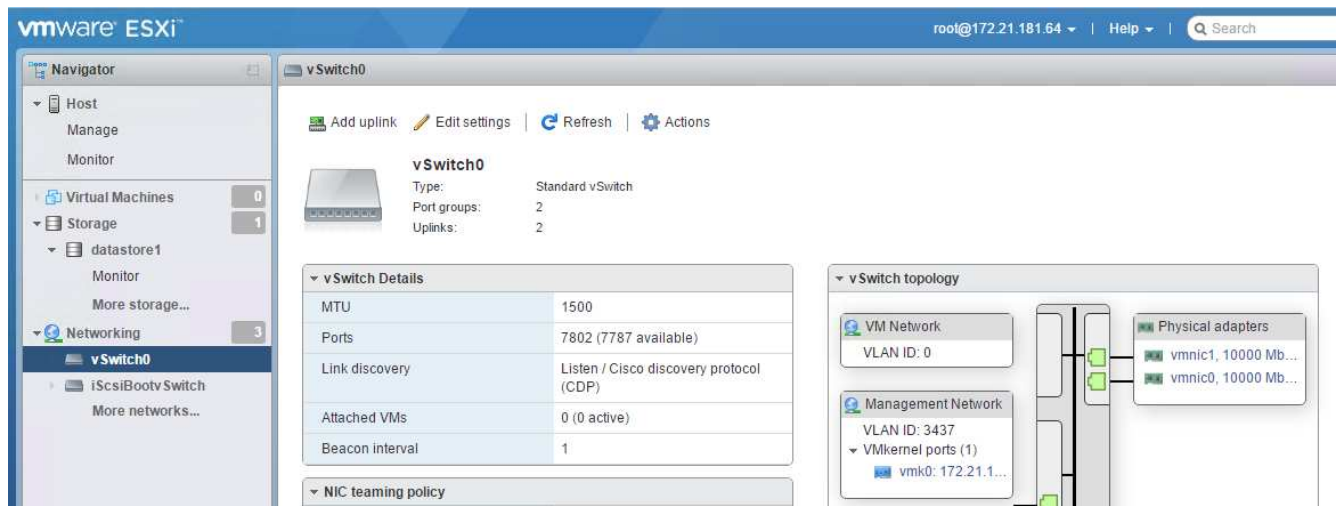
Dynamic targets	Add dynamic target Remove dynamic target Edit settings
Address	Port
172.21.183.33	3260
172.21.183.34	3260
172.21.184.33	3260
172.21.184.34	3260



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 。

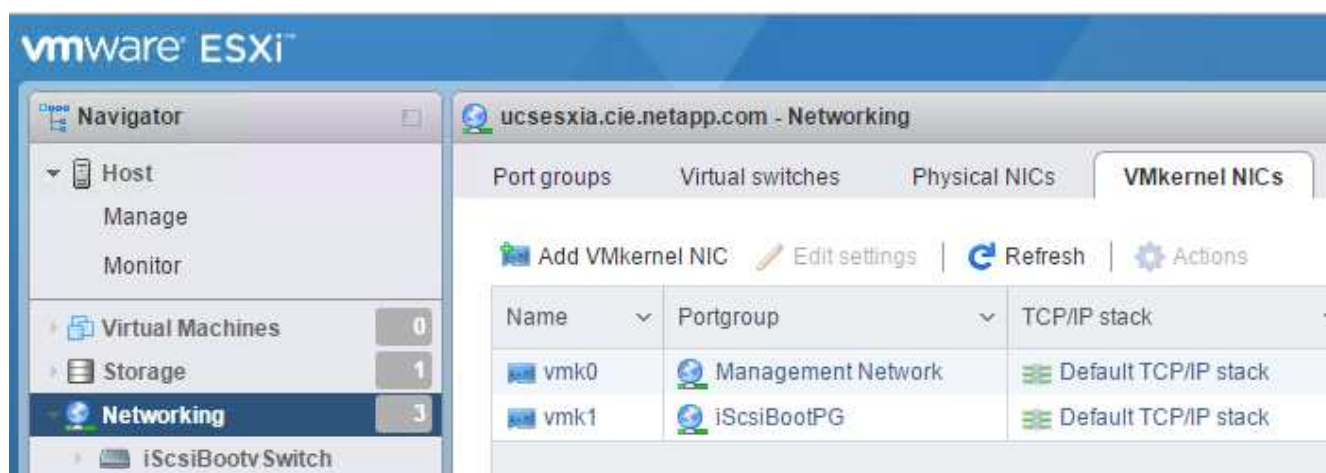
配置端口组和 VMkernel NIC

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。

Port group	New port group ▼
New port group	NFS-Network
Virtual switch	vSwitch0 ▼
VLAN ID	3438
MTU	9000
IP version	IPv4 only ▼
▼ IPv4 settings	
Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
Address	172.21.182.63
Subnet mask	255.255.255.0
TCP/IP stack	Default TCP/IP stack ▼

Create Cancel

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。

Virtual switch	vSwitch0
VLAN ID	3441
MTU	9000
IP version	IPv4 only
▼ IPv4 settings	
Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
Address	172.21.185.63
Subnet mask	255.255.255.0
TCP/IP stack	Default TCP/IP stack
Services	<input checked="" type="checkbox"/> vMotion <input type="checkbox"/> Provisioning <input type="checkbox"/> Fault tolerance logging <input type="checkbox"/> Management <input type="checkbox"/> Replication <input type="checkbox"/> NFC replication

Create Cancel

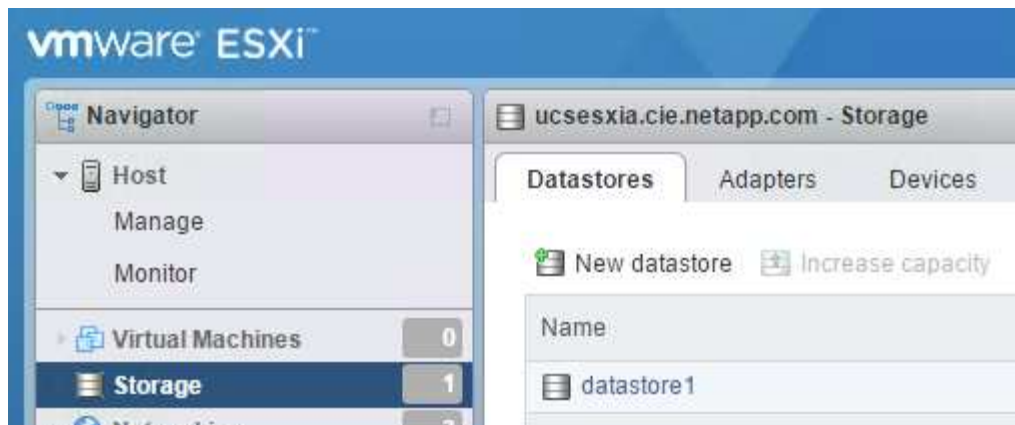


可以通过多种方法配置 ESXi 网络，包括在许可允许的情况下使用 VMware vSphere 分布式交换机。如果需要其他网络配置来满足业务需求，FlexPod Express 支持这些配置。

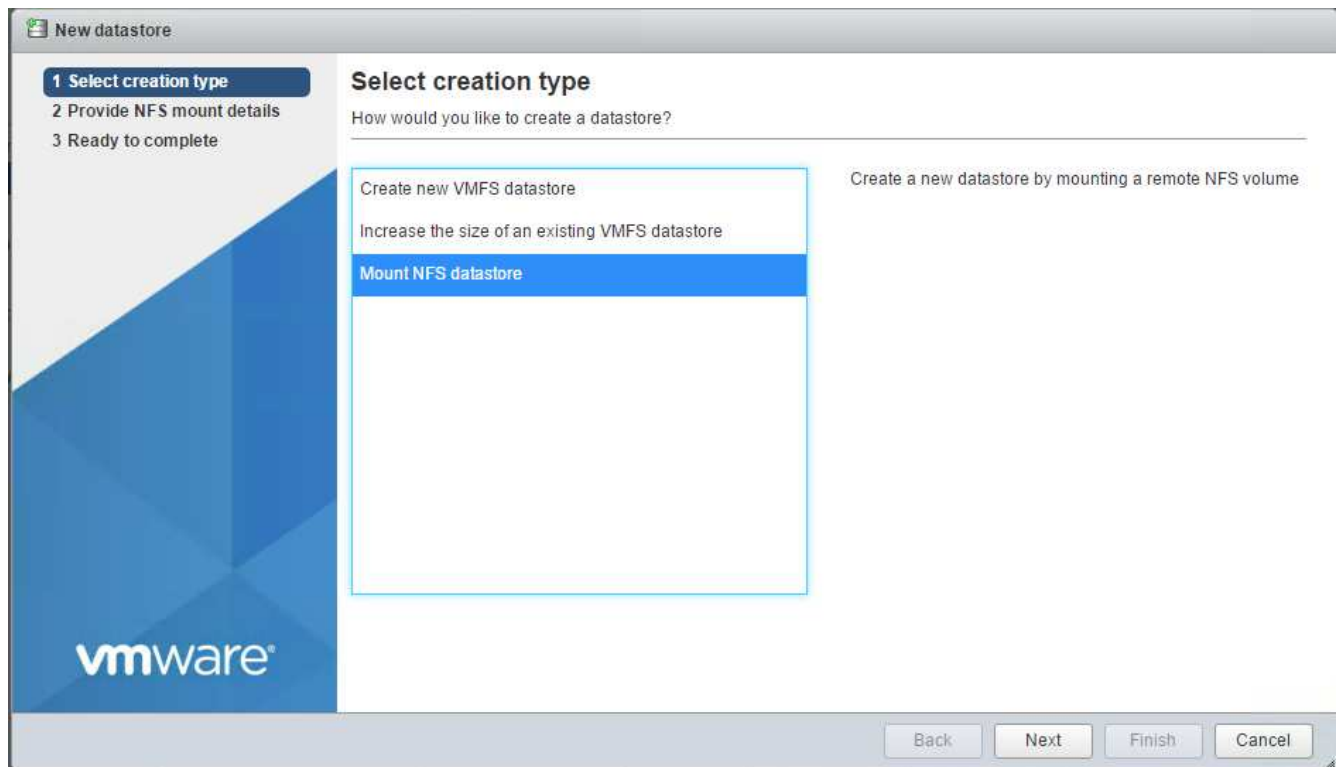
首先挂载数据存储库

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：

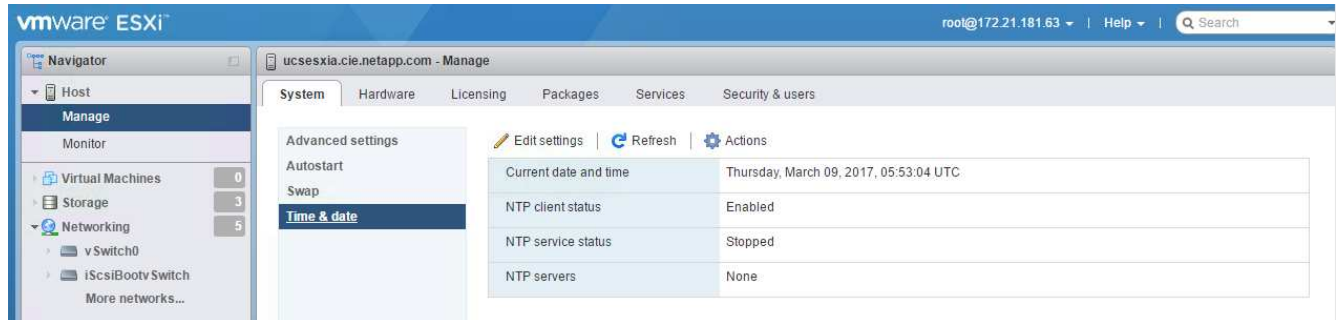
- 名称：infra_swap
- NFS 服务器：`<<var_noda_nfs_lif>>`
- 共享：`/infra_swap`

- 确保已选择 NFS 3。

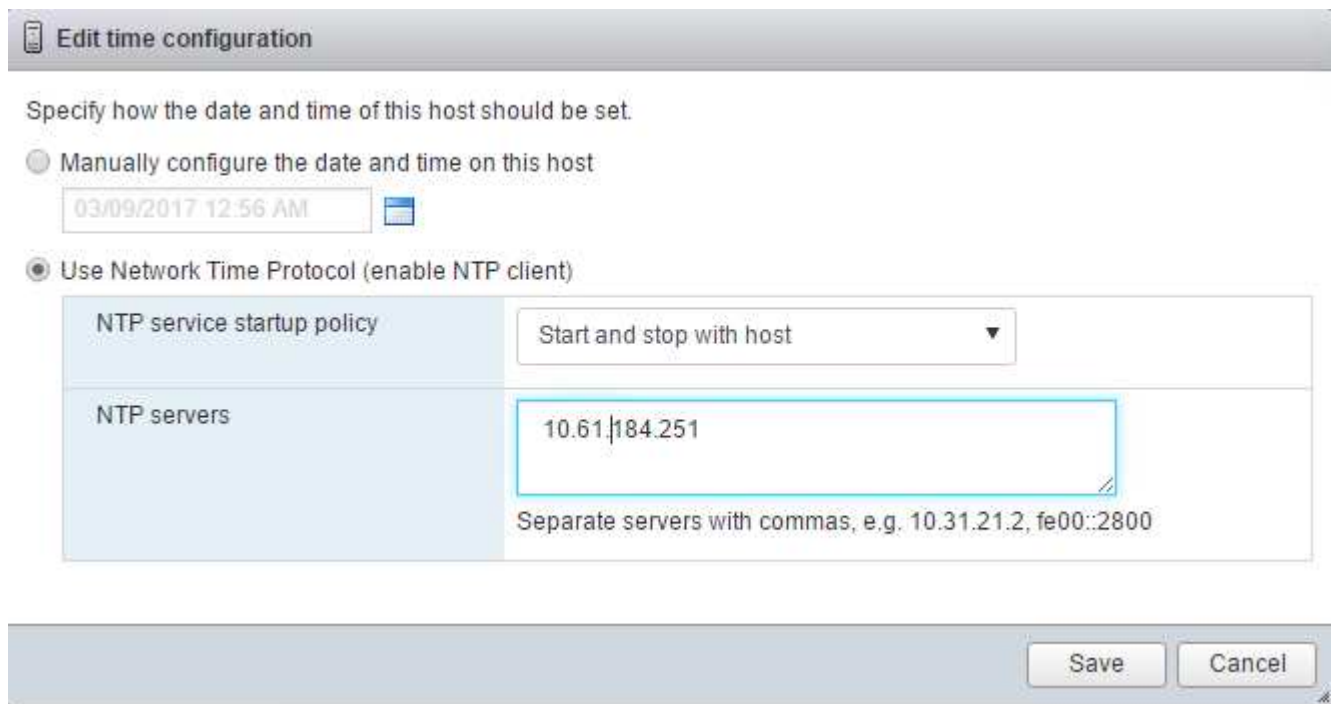
配置 NTP

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。



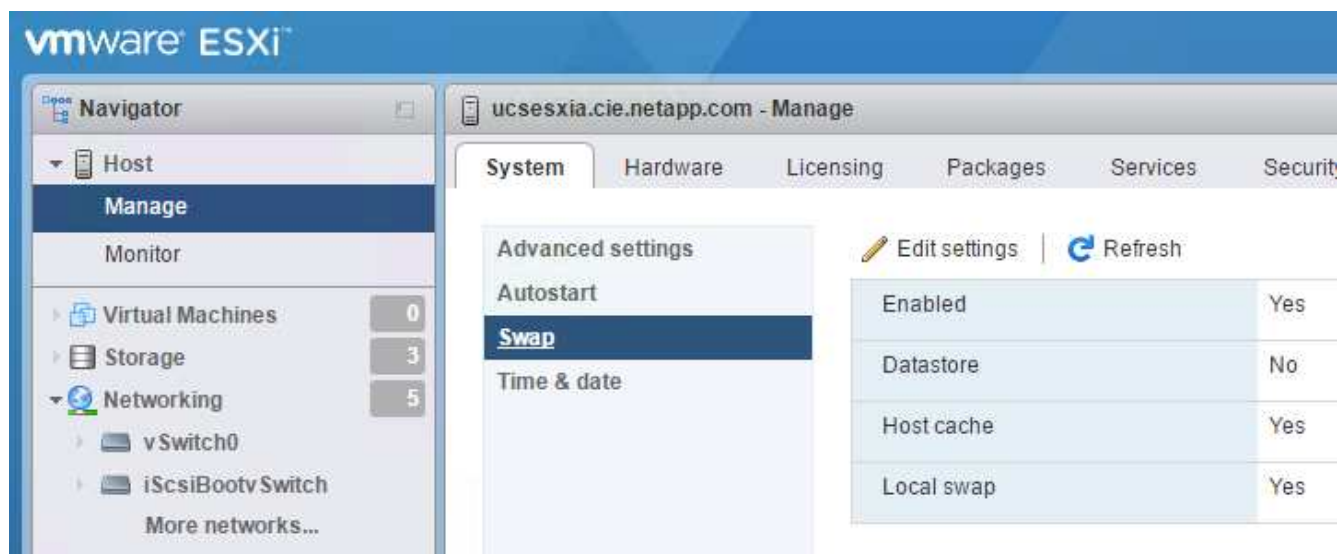
2. 选择使用网络时间协议（启用 NTP 客户端）。
3. 选择 Start 和 Stop with Host 作为 NTP 服务启动策略。
4. 输入 `<<var_ntf>>` 作为 NTP 服务器。您可以设置多个 NTP 服务器。
5. 单击保存。



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:
```

"接下来：安装 VMware vCenter Server 6.7"

安装 VMware vCenter Server 6.7

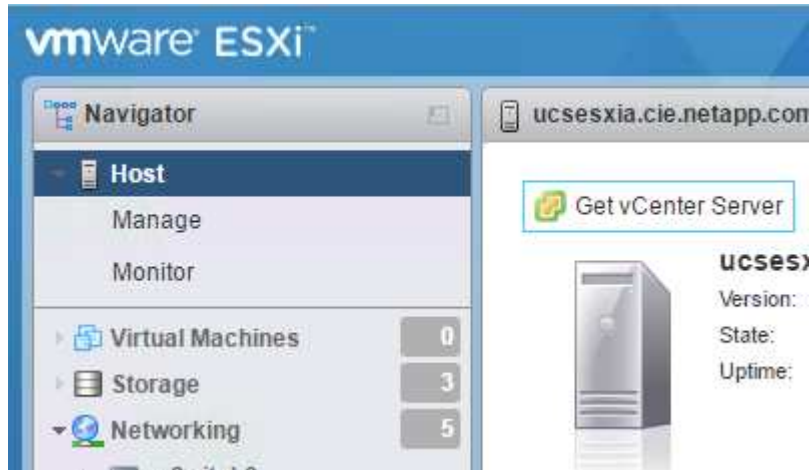
本节详细介绍了在 FlexPod 快速配置中安装 VMware vCenter Server 6.7 的过程。



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。

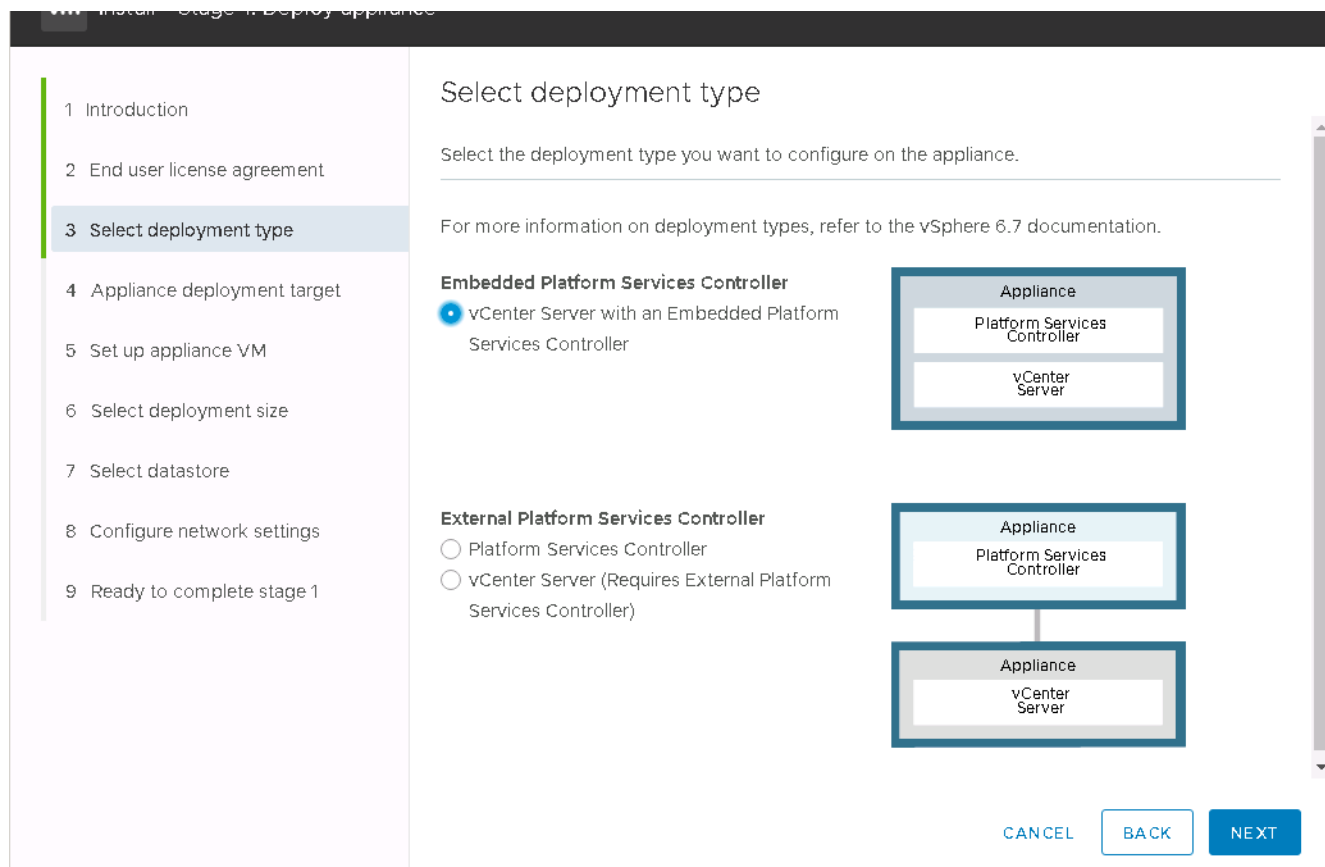


2. 从 VMware 站点下载 VCSA。



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。

Installer

vm Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

1 Introduction

2 End user license agreement

3 Select deployment type

4 Appliance deployment target

5 Set up appliance VM

6 Select deployment size

7 Select datastore

8 Configure network settings

9 Ready to complete stage 1

Appliance deployment target

Specify the appliance deployment target settings. The target is the ESXi host or vCenter Server instance on which the appliance will be deployed.

ESXi host or vCenter Server name	172.21.246.25	i
HTTPS port	443	
User name	root	i
Password	*****	

CANCEL

BACK

NEXT

10. 输入 vCSA 作为要用于 VCSA 的 VM 名称和根密码，以设置设备 VM。

12. 选择 infra_datastore_1 数据存储库。单击下一步。

vm Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

1 Introduction
2 End user license agreement
3 Select deployment type
4 Appliance deployment target
5 Set up appliance VM
6 Select deployment size
7 Select datastore
8 Configure network settings
9 Ready to complete stage 1

Select datastore

Select the storage location for this appliance

☒ Install on an existing datastore accessible from the target host

Name	Type	Capacity	Free	Provisioned	Thin Provisioning
infra_datastore_1	NFS	500 GB	499.98 GB	18.38 MB	Supported
infra_swap	NFS	100 GB	99.99 GB	10.95 MB	Supported

2 items

☒ Enable Thin Disk Mode ⓘ

☐ Install on a new vSAN cluster containing the target host ⓘ

CANCEL BACK NEXT

13. 在 Configure network settings 页面中输入以下信息，然后单击 Next 。

- 选择 MGMT-Network for Network 。
- 输入要用于 VCSA 的 FQDN 或 IP 。
- 输入要使用的 IP 地址。
- 输入要使用的子网掩码。
- 输入默认网关。
- 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。

vCenter Server Appliance Installer

Installer

vm Install - Stage 1: Deploy vCenter Server with an Embedded Platform Services Controller

1 Introduction

2 End user license agreement

3 Select deployment type

4 Appliance deployment target

5 Set up appliance VM

6 Select deployment size

7 Select datastore

8 Configure network settings

9 Ready to complete stage 1

Configure network settings

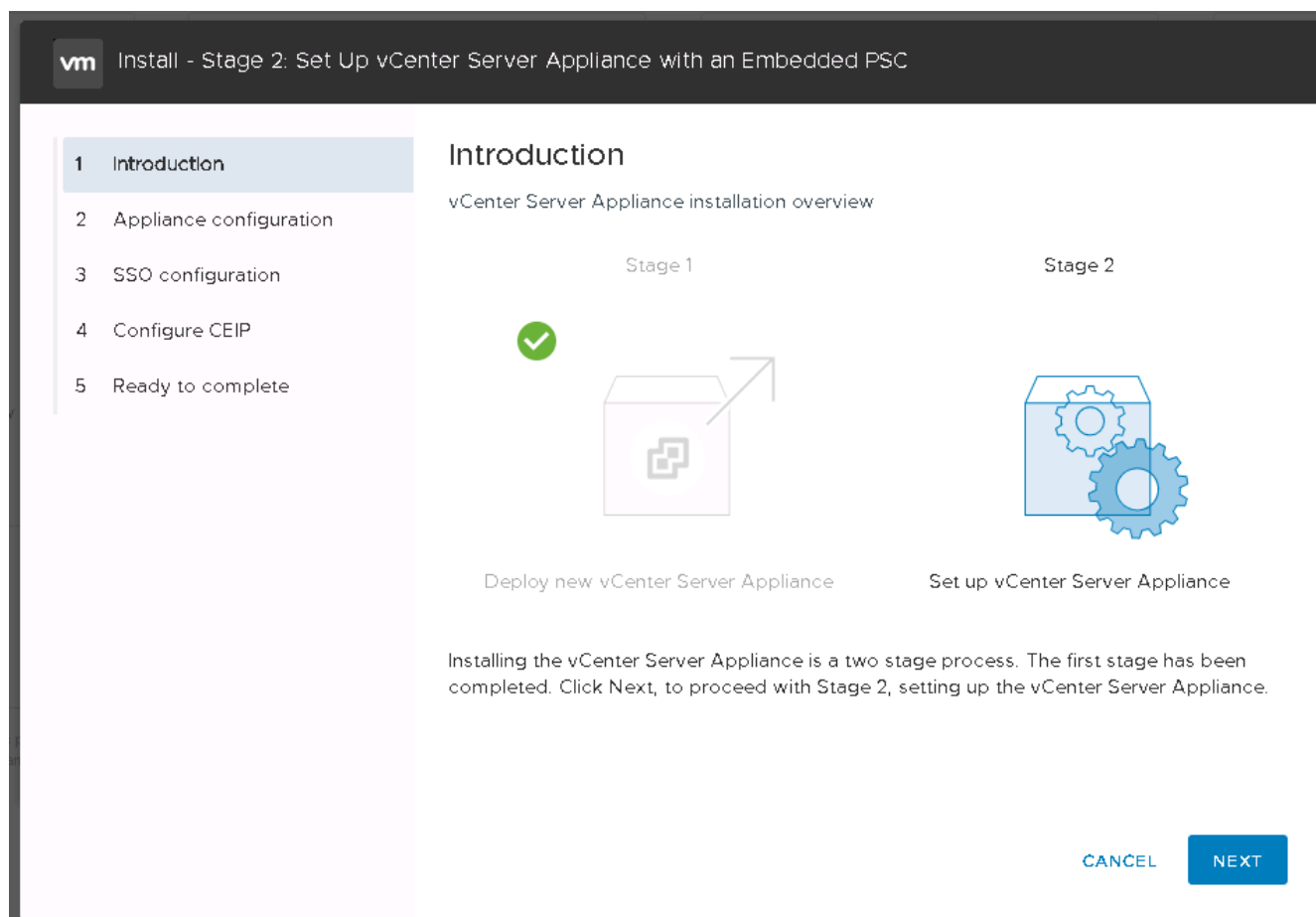
IP version	IPv4	
IP assignment	static	
FQDN	tigervcsa.cle.netapp.com	i
IP address	172.21.246.41	
Subnet mask or prefix length	255.255.255.0	i
Default gateway	172.21.246.1	
DNS servers	10.61.184.251,10.61.184.252	
Common Ports		
HTTP	80	
HTTPS	443	

CANCEL BACK NEXT

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。

请记住这些值以供参考，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@vsphere.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。

New Cluster | FlexPod

Name

Tiger3

Location

FlexPod

> DRS

☒ Turn ON

> vSphere HA

☒ Turn ON

> EVC

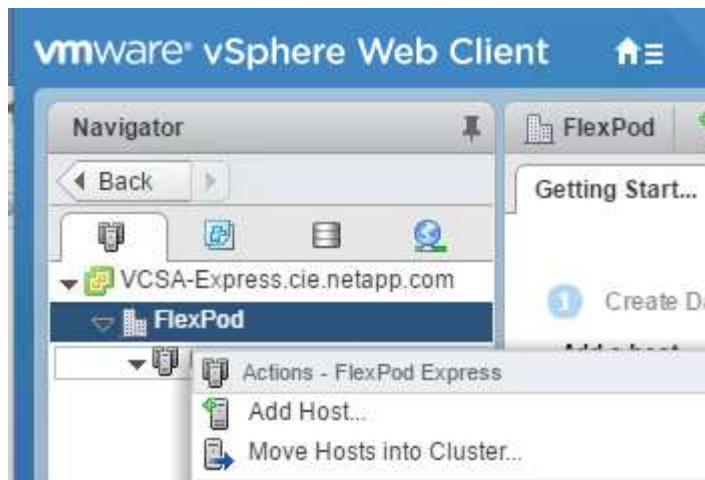
Disable

CANCEL

OK

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"](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"](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的熟悉的技术。

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。

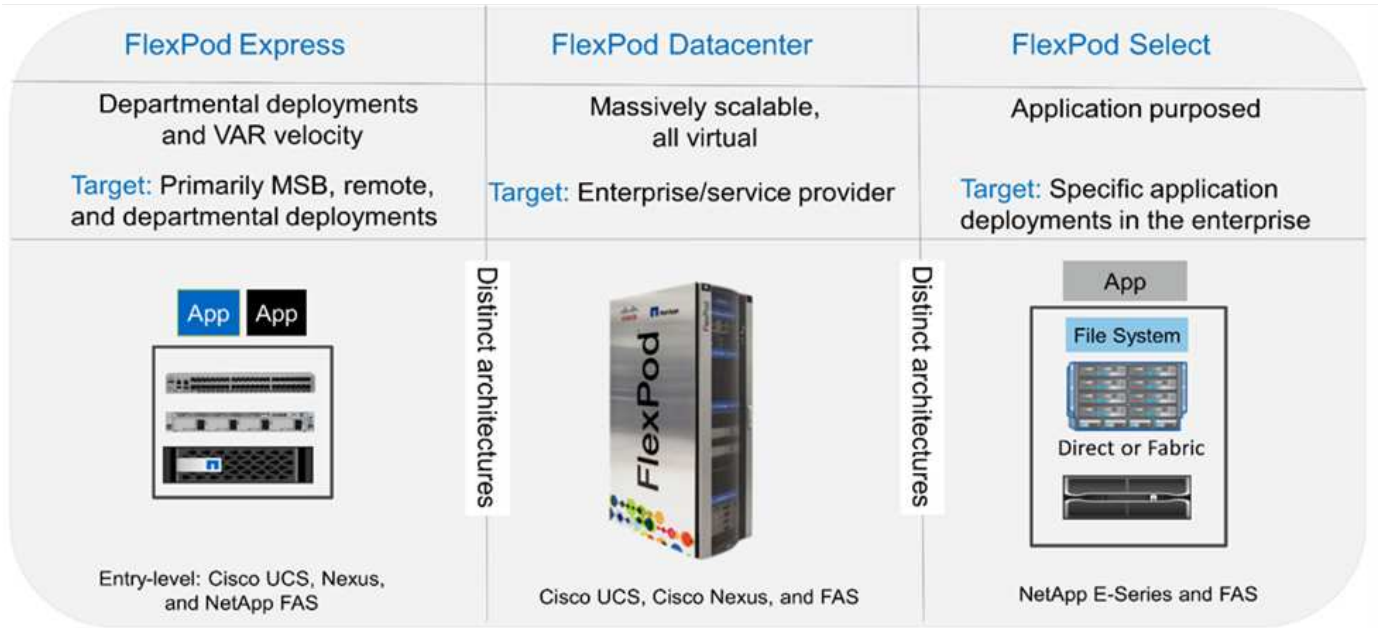
FlexPod 融合基础架构计划

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

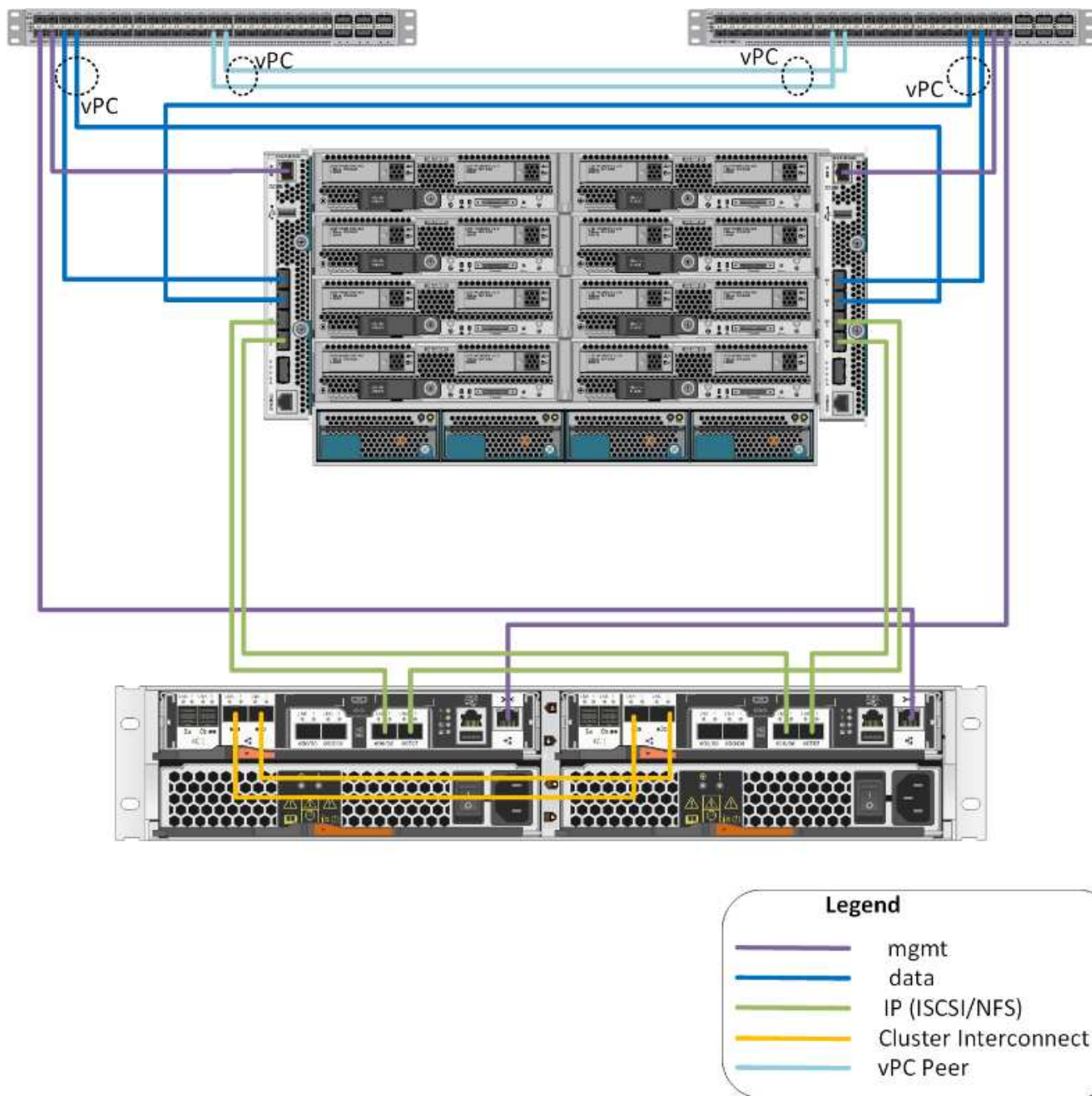
软件组件

- 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 xxxxx 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

```

```

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
```

Node	Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin 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 vservers 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,fc
```

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 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 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
```

- 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
```

- 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
```

- 要获取以下步骤中所需参数的值，请运行 `security certificate show` 命令。
- 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
```

- 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 -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 Manager 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。

Create Block of IPv4 Addresses

From :	192.168.156.101	Size :	12
Subnet Mask :	255.255.255.0	Default Gateway :	192.168.156.1
Primary DNS :	0.0.0.0	Secondary DNS :	0.0.0.0

OK Cancel

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。

Add NTP Server

?
X

NTP Server :

OK

Cancel

- 单击添加 NTP 服务器。
- 输入 `<switch-b-ntp-ip>` 或 <Nexus B-mgmt-ip>，然后单击 OK。单击确认后的确定。

All /

General

Events

Actions

Add NTP Server

Properties

Time Zone :
America/New_York (Eastern ▼)

NTP Servers

Advanced Filter
Export
Print

Name

NTP Server 10.1.156.4

NTP Server 10.1.156.5

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：

- 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。
- 在右侧窗格中，选择策略选项卡。
- 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。
- 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"。
- 单击 Save Changes。
- 单击确定。

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。

- 在左窗格中，选择互联阵列 B 下的固定模块
- 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
☒ FCoF Uplink
☒ Unified Uplink
☒ Appliance Storage
☒ FCoF 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

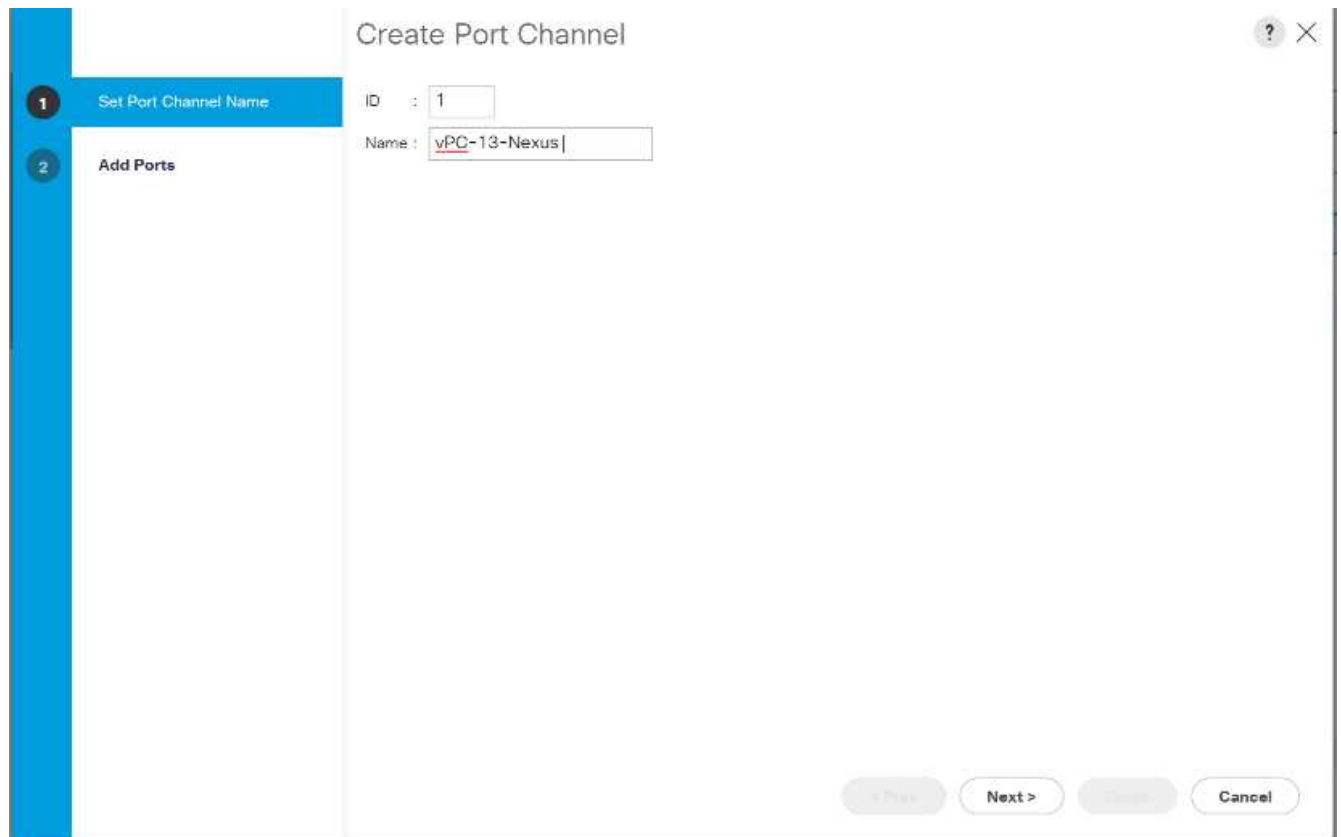
要在 Cisco UCS 环境中配置所需的端口通道，请完成以下步骤：

- 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。

- 在 "LAN">"LAN Cloud " 下，展开 "Fabric A 树 "。
- 右键单击端口通道。
- 选择创建端口通道。
- 输入 13 作为端口通道的唯一 ID 。
- 输入 vPC-13-Nexus 作为端口通道的名称。
- 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" 。

Create VLANs

VLAN Name/Prefix : NFS-VLAN

☒ Common/Global ☐ Fabric A ☐ Fabric B ☐ Both Fabrics Configured Differently

You are creating global VLANs that map to the same VLAN IDs in all available fabrics.
Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs : 3170

Sharing Type : ☒ None ☐ Primary ☐ Isolated ☐ Community

Check Overlap Ok Cancel

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 。

LAN / LAN Cloud / VLANs

VLANs

Advanced Filter Export Print

Name	ID	Type	Transport	Native	VLAN Sharing	Primary VLAN Name	Multicast Policy Name
VLAN default (1)	1	Lan	Ether	Yes	None		
VLAN 0002-Native (2)	2	Lan	Ether	No	None		
VLAN public (18)	18	Lan	Ether	No	None		
VLAN 0101-IB-MGMT (101)	101	Lan	Ether	No	None		
VLAN 0102-VM (102)	102	Lan	Ether	No	None		
VLAN 0103-vMotion (103)	103	Lan	Ether	No	None		
VLAN 0104-NFS (104)	104	Lan	Ether	No	None		
VLAN 0120-SCSI-A (120)	120	Lan	Ether	No	None		
VLAN 0121-SCSI-B (121)	121	Lan	Ether	No	None		

- 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。

Properties for: Enable_CDP

General Events

Actions

Delete

Show Policy Usage

Use Global

Properties

Name : Enable_CDP

Description :

Owner : Local

CDP : ☐ Disabled ☒ Enabled

MAC Register Mode : ☒ Only Native Vlan ☐ All Host Vlans

Action on Uplink Fail : ☒ Link Down ☐ Warning

MAC Security

Forge : ☒ Allow ☐ Deny

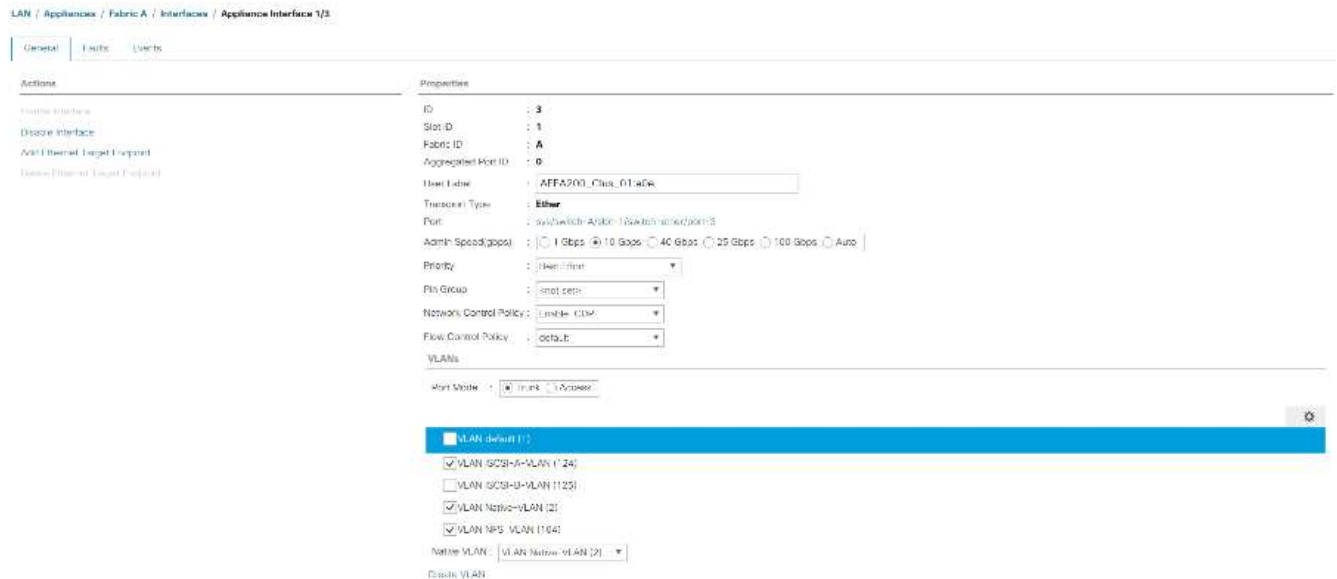
LLDP

Transmit : ☐ Disabled ☒ Enabled

Receive : ☐ Disabled ☒ Enabled

OK Apply Cancel Help

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 ``：`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 ``：`e0f`。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 ``：`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 。

LAN / Appliances / Fabric B / Interfaces / Appliance Interface 1/3

General Faults Events

Actions

- Enable Interface
- Disable Interface
- Add Ethernet Target Endpoint
- Delete Ethernet Target Endpoint

Properties

ID : 3

Slot ID : 1

Fabric ID : B

Aggregated Port ID : 0

User Label : AFFA200_Clus_01:e0f

Transport Type : Ether

Port : sys/switch-B/slot-1/switch-ether/port-3

Admin Speed(gbps) : ☐ 1 Gbps ☒ 10 Gbps ☐ 40 Gbps ☐ 25 Gbps ☐ 100 Gbps ☐ Auto

Priority : Best Effort

Pin Group : <not set>

Network Control Policy : Enable_CDP

Flow Control Policy : default

VLANs

Port Mode : ☒ Trunk ☐ Access

☐ VLAN default (1)

☐ VLAN iSCSI-A-VLAN (124)

☒ VLAN iSCSI-B-VLAN (125)

☒ VLAN Native-VLAN (2)

☒ VLAN NFS_VLAN (104)

Native VLAN : VLAN Native-VLAN (2)

Create 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 。

All

LAN

LAN Cloud

Fabric A

Port Channels

Port-Channel 13 vPC-13-Nexus

Uplink Fth Interfaces

VLAN Optimization Sets

VLANs

Fabric B

QoS System Class

LAN Pin Groups

Threshold Policies

VLAN Groups

VLANs

Appliances

Fabric A

LAN / LAN Cloud / QoS System Class

General

Events

ESM

Actions

Properties

Use Global

Owner: Local

Priority	Enabled	CoS	Packet Drop	Weight	Weight (%)	MTU	Multicast Optimized
Platinum	<input type="checkbox"/>	5	<input type="checkbox"/>	10	N/A	normal	<input type="checkbox"/>
Gold	<input type="checkbox"/>	4	<input checked="" type="checkbox"/>	9	N/A	normal	<input type="checkbox"/>
Silver	<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	8	N/A	normal	<input type="checkbox"/>
Bronze	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	7	N/A	normal	<input type="checkbox"/>
Best Effort	<input checked="" type="checkbox"/>	Any	<input checked="" type="checkbox"/>	5	50	9210	<input type="checkbox"/>
Fibre Channel	<input checked="" type="checkbox"/>	3	<input type="checkbox"/>	5	50	10	N/A

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

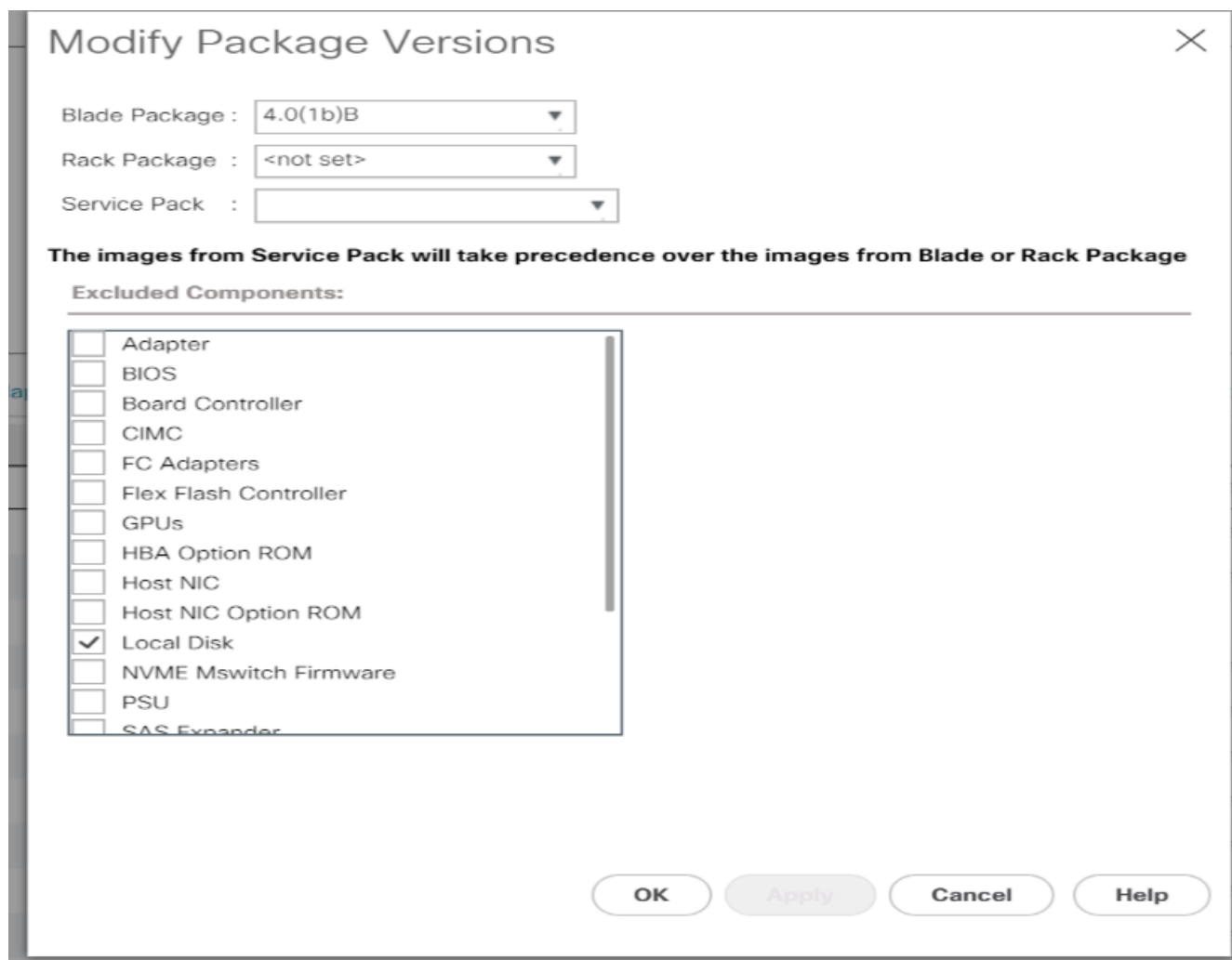
要将 Cisco UCS Manager 软件和 Cisco UCS 互联阵列软件升级到 4.0 （1b）版，请参见 "《[Cisco UCS Manager 安装和升级指南](#)》"。

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。

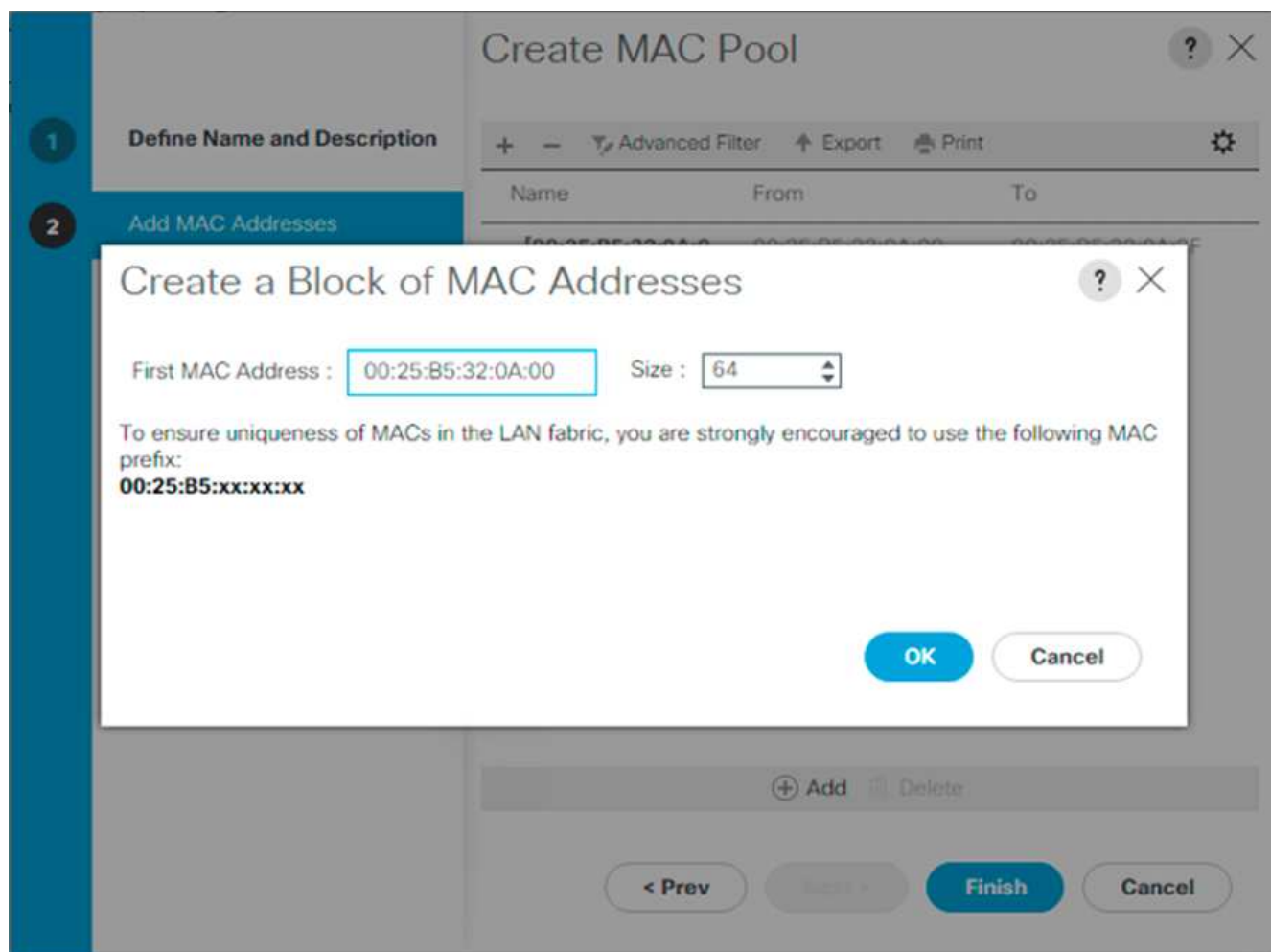
在此操作步骤中，将创建两个 MAC 地址池，每个交换网络结构一个。

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

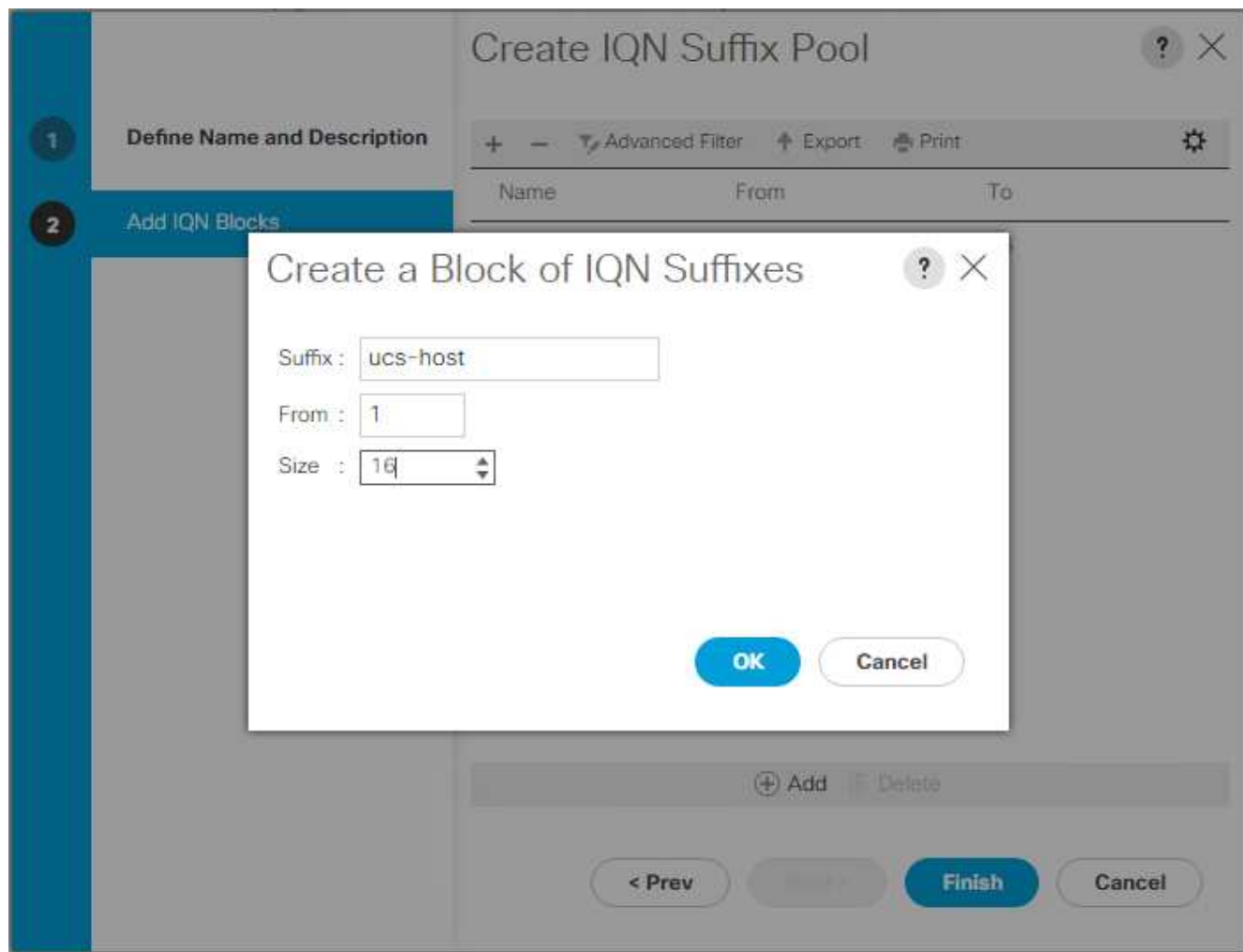
要为 Cisco UCS 环境配置所需的 IQN 池，请完成以下步骤：

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` 的服务器池中。
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。

Create Network Control Policy

CDP : ☐ Disabled ☒ Enabled

MAC Register Mode : ☒ Only Native Vlan ☐ All Host Vlans

Action on Uplink Fail : ☒ Link Down ☐ Warning

MAC Security

Forge : ☒ Allow ☐ Deny

LLDP

Transmit : ☐ Disabled ☒ Enabled

Receive : ☐ Disabled ☒ Enabled

OK

Cancel

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。

Create Power Control Policy

?

×

Name

:

No-Power-Cap

Description

:

Fan Speed Policy

:

Any

▼

Power Capping

If you choose **cap**, the server is allocated a certain amount of power based on its priority within its power group. Priority values range from 1 to 10, with 1 being the highest priority. If you choose **no-cap**, the server is exempt from all power capping.

☒ No Cap

☐ cap

Cisco UCS Manager only enforces power capping when the servers in a power group require more power than is currently available. With sufficient power, all servers run at full capacity regardless of their priority.

OK

Cancel

创建服务器池限定策略（可选）

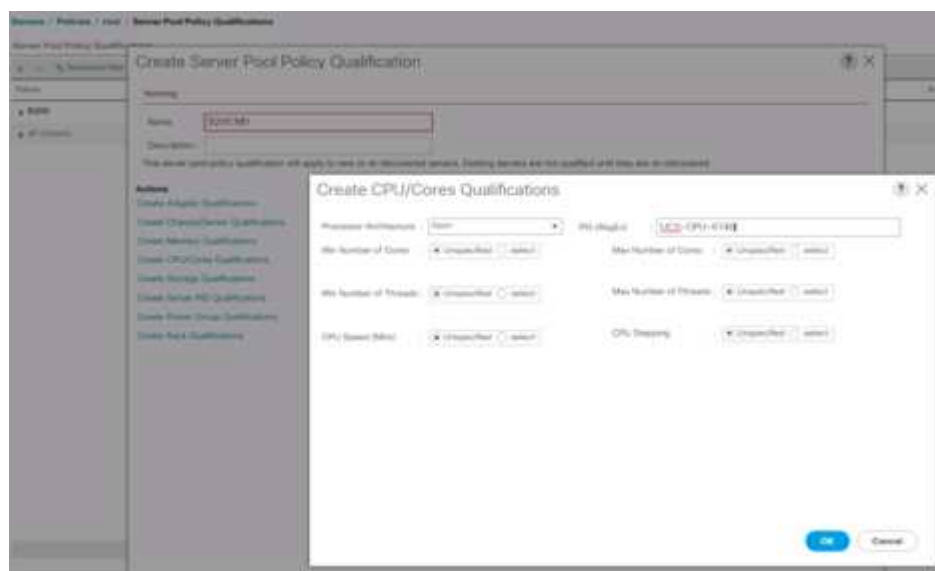
要为 Cisco UCS 环境创建可选的服务器池限定策略，请完成以下步骤：



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。

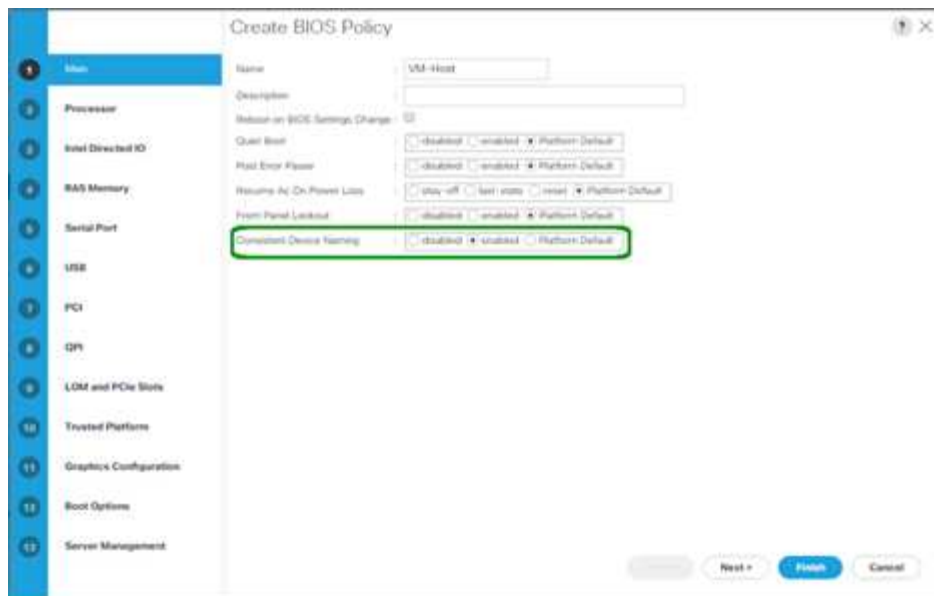
8. 输入 ``<UCS-CPU- PID>`` 作为进程 ID （PID）。
9. 单击确定以创建 CPU/ 核心资格认定。
10. 单击确定创建策略，然后单击确定进行确认。



创建服务器 BIOS 策略

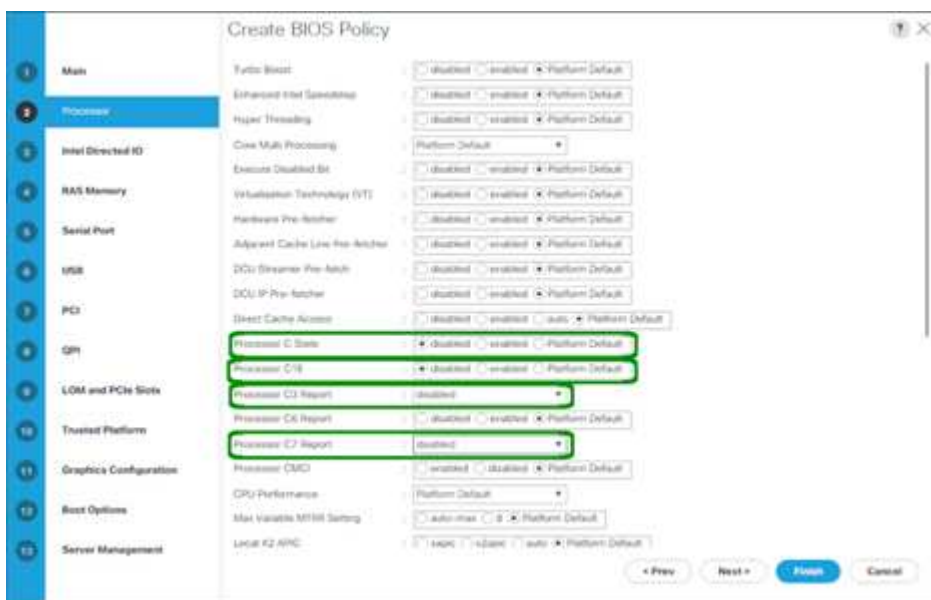
要为 Cisco UCS 环境创建服务器 BIOS 策略，请完成以下步骤：

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。

Servers / Policies / root / Maintenance Poli... / default

General Events

Actions

Cancel

Show Policy Usage

Use Global

Properties

Name : default

Description :

Owner : Local

Soft Shutdown Timer : 150 Secs

Reboot Policy : ☐ Immediate ☒ User Ack ☐ Timer Automatic

☒ On Next Boot (Apply pending changes at next reboot.)

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。



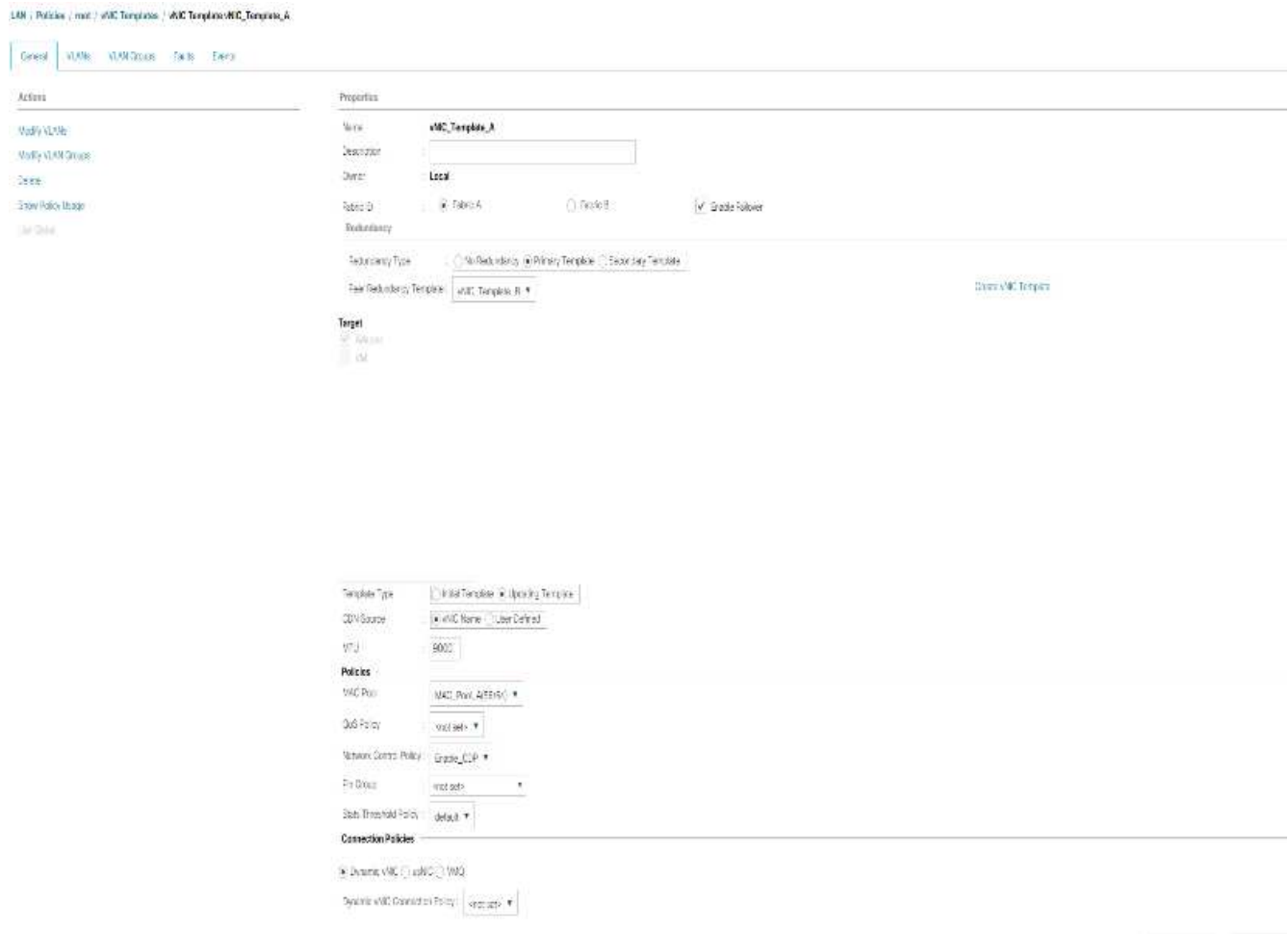
总共创建了四个 vNIC 模板。

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。

LAN / Policies / vNIC Templates / vNIC Template vNIC_Template_B

Current VLANs VLAN Groups Tags Profiles

Actions

- Modify VLANs
- Modify VLAN Groups
- Delete
- Show Policy Usage
- Use Default

Properties

Name: vNIC_Template_B

Description:

Owner: Local

Fabric ID: ☐ Fabric A ☒ Fabric B ☐ Enable Fabric

Redundancy

Redundancy Type: ☐ No Redundancy ☐ Primary Template ☒ Secondary Template

Peer Redundancy Template: vNIC_Template_A [Create vNIC Template](#)

Target

☒ Adapter ☐ VM

Template Type: ☐ New Template ☒ Updating Template

CDN Source: ☒ vNIC Name ☐ User Defined

MTU: 9000

Policies

MAC Pool: MAC_Pool_B(8/64)

QoS Policy: ☐ [Add](#)

Network Control Policy: ☐ [Add](#)

Pin Group: ☐ [Add](#)

Stats Threshold Policy: ☐ [Add](#)

Connection Policies

☒ Dynamic vNIC ☐ vNIC ☐ VMQ

Dynamic vNIC Connection Policy: ☐ [Add](#)

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。

LAN / Policies / root / vNIC Templates / vNIC Template Site_01_ISCSI-A

General VLANs VLAN Groups Faults Events

Actions

- Modify VLANs
- Modify VLAN Groups
- Delete
- Show Policy Usage
- Use Global

Properties

Name : Site_01_ISCSI-A

Description :

Owner : Local

Fabric ID : ☒ Fabric A ☐ Fabric B ☐ Enable Failover

Redundancy

Redundancy Type : ☒ No Redundancy ☐ Primary Template ☐ Secondary Template

Target

☒ Adapter ☐ VM

Template Type : ☐ Initial Template ☒ Updating Template

CDN Source : ☒ vNIC Name ☐ User Defined

MTU : 9000

Policies

MAC Pool : MAC_Pool_A(56/64)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

Dynamic vNIC Connection Policy : <not set>

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。

LAN / Policies / root / vNIC Templates / vNIC Template Site_01_ISCSI-B

GeneralVLANsVLAN GroupsFaultsEvents

Actions

Modify VLANs

Modify VLAN Groups

Delete

Show Policy Usage

Use Circular

Properties

Name : Site_01_ISCSI-B

Description :

Owner : Local

Fabric ID : ☐ Fabric A ☒ Fabric B ☐ Enable Failover

Redundancy

Redundancy Type : ☒ No Redundancy ☐ Primary Template ☐ Secondary Template

Target

Podster

vmt

Template Type : ☐ Initial Template ☒ Updating Template

CDN Source : ☒ vNIC Name ☐ User Defined

MTU : 9000

Policies

MAC Pool : MAC_Pool_B[50/64]

CoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

Dynamic vNIC Connection Policy : <not set>

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。

Modify vNIC

Name: **Site-01-vNIC-A**

Use vNIC Template: ☒

[Create vNIC Template](#)

vNIC Template: vNIC_Template_A ▼

Adapter Performance Profile

Adapter Policy: VMWare ▼

[Create Ethernet Adapter Policy](#)

[Create QoS Policy](#)

[Create Network Control Policy](#)

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

OK **Cancel**

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。

Modify iSCSI vNIC ? ×

Name : **Site-01-ISCSI-A**

Overlay vNIC :

iSCSI Adapter Policy : [Create iSCSI Adapter Policy](#)

VLAN :

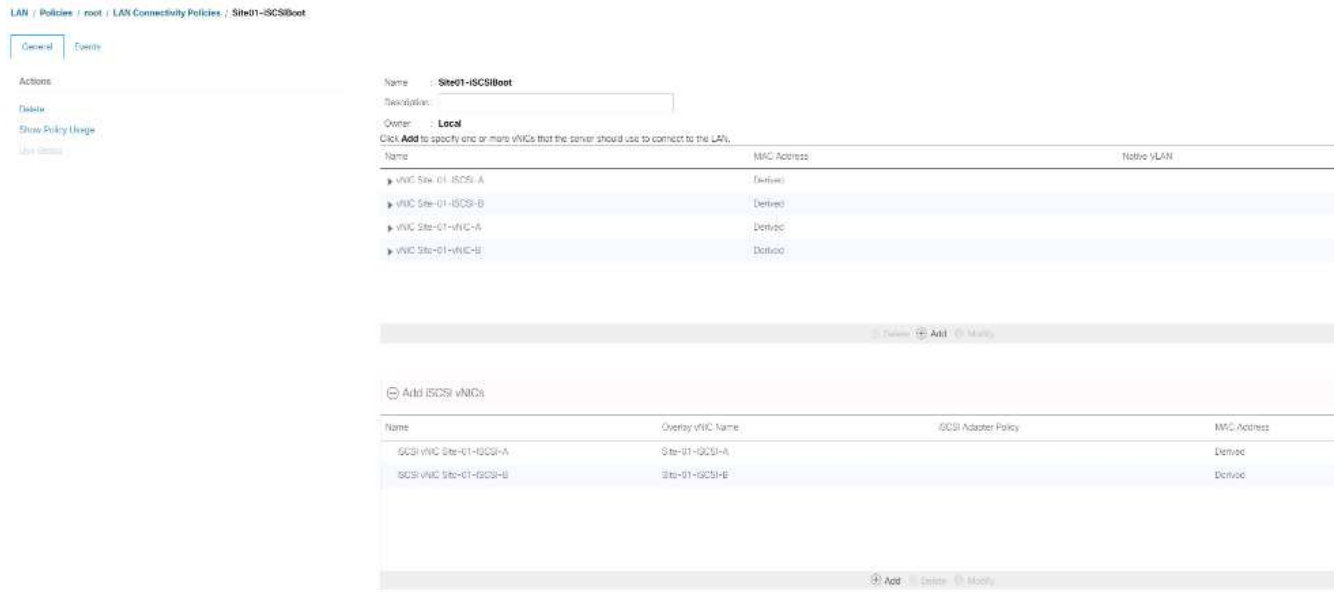
iSCSI MAC Address

MAC Address Assignment:

[Create MAC Pool](#)

OK **Cancel**

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。



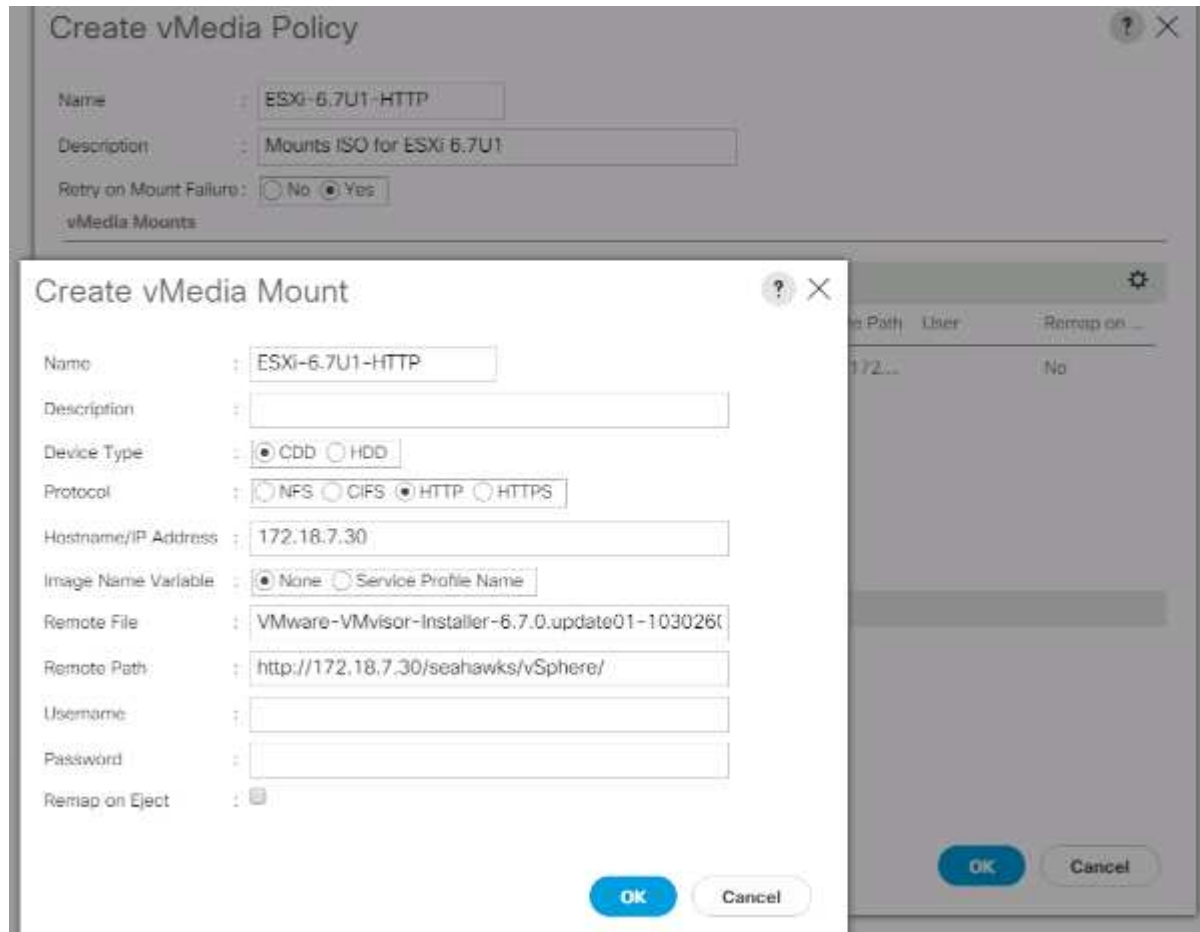
先前未将 DNS 服务器 IP 输入到 KVM IP 中，因此，需要输入 Web 服务器的 IP，而不是主机名。

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。

Create Service Profile Template

You must enter a name for the service profile template and specify the template type. You can also specify how a UUID will be assigned to the template and enter a description.

Name:

The template will be created in the following organization. Its name must be unique within this organization.
Where: **org-root**

The template will be created in the following organization. Its name must be unique within this organization.
Type: ☒ **Updating Template**

Specify how the UUID will be assigned to the server associated with the service generated by the template.
UUID:

UUID Assignment:

The UUID will be assigned from the selected pool.
The available/total UUIDs are displayed after the pool name.

Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used.

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。

Create Service Profile Template

Optionally specify LAN configuration information.

Dynamic vNIC Connection Policy: Select a Policy to use (no Dynamic vNIC Policy by default) ▼

Create Dynamic vNIC Connection Policy

How would you like to configure LAN connectivity?

☐ Simple
 ☐ Expert
 ☐ No vNICs
 ☒ Use Connectivity Policy

LAN Connectivity Policy: Site01 - iSCSIBoot ▼ Create LAN Connectivity Policy

Initiator Name

Initiator Name Assignment: IQN Pool(60/64) ▼

Initiator Name:

Create IQN Suffix Pool

The IQN will be assigned from the selected pool.

The available/total IQNs are displayed after the pool name.

< Prev Next > Finish Cancel

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

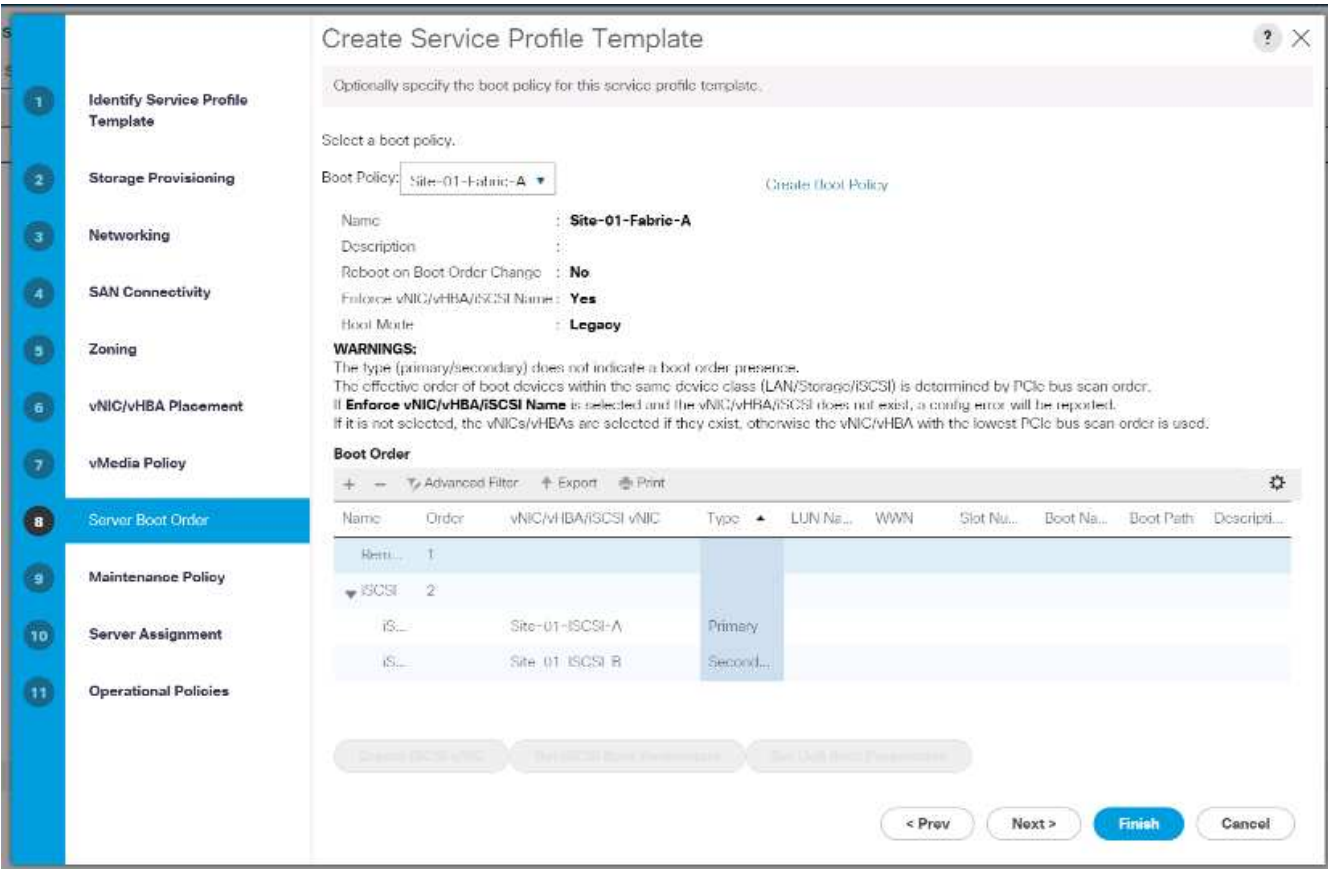
要配置 vMedia 策略，请完成以下步骤：

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：

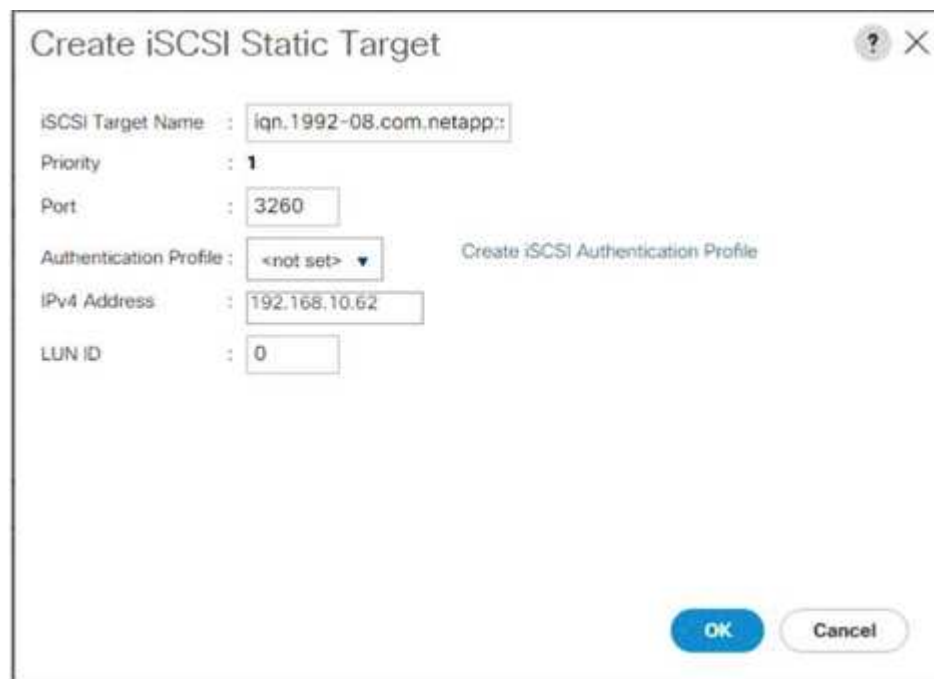
- 1. 为 Boot Policy 选择 Boot-Fabric-A。



- 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.b5acab9ef1c811a68d9d00a098a9fec2:vs.3
                        Infra-SVM                up
```

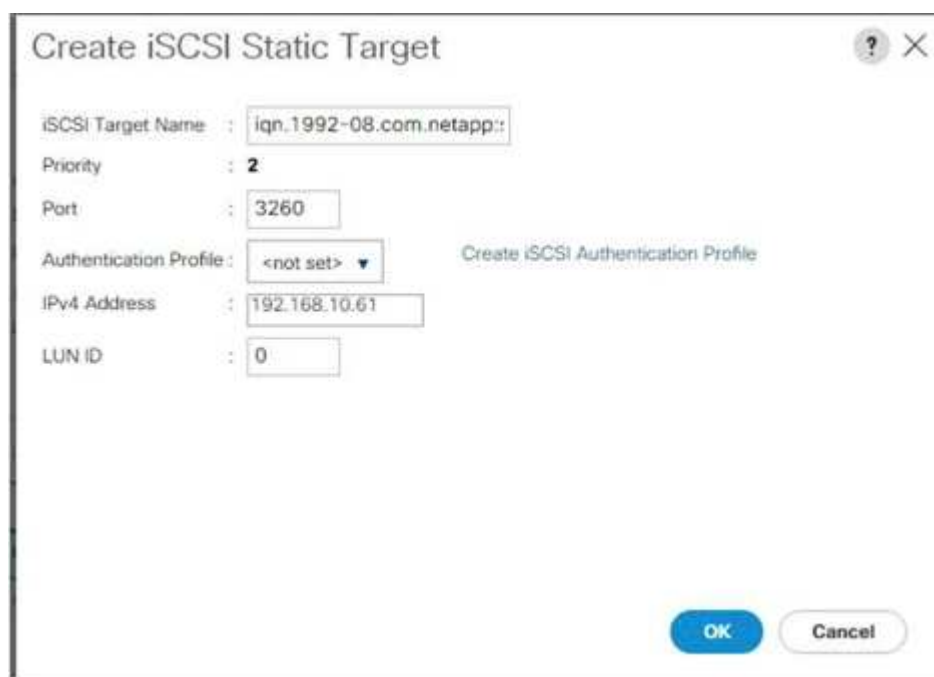
- 10. 在 "IPv4 Address" 字段中输入 IP 地址 `iscsi_lif_02a`。



The dialog box is titled "Create iSCSI Static Target" and contains the following fields and controls:

- iSCSI Target Name:
- Priority:
- Port:
- Authentication Profile: [Create iSCSI Authentication Profile](#)
- IPv4 Address:
- LUN ID:
- Buttons:

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`。



The dialog box is titled "Create iSCSI Static Target" and contains the following fields and controls:

- iSCSI Target Name:
- Priority:
- Port:
- Authentication Profile: [Create iSCSI Authentication Profile](#)
- IPv4 Address:
- LUN ID:
- Buttons:

15. 单击确定以添加 iSCSI 静态目标。

Set iSCSI Boot Parameters

Name : **iSCSI-A-vNIC**

Authentication Profile : <not set> [Create iSCSI Authentication Profile](#)

Initiator Name

Initiator Name Assignment: <not set>

[Create IQN Suffix Pool](#)

WARNING: The selected pool does not contain any available entities. You can select it, but it is recommended that you add entities to it.

Initiator Address

Initiator IP Address Policy: iSCSI_IP_Pool_A(12/16)

IPv4 Address : 0.0.0.0
 Subnet Mask : 255.255.255.0
 Default Gateway : 0.0.0.0
 Primary DNS : 0.0.0.0
 Secondary DNS : 0.0.0.0

[Create IP Pool](#)
[Reset Initiator Address](#)
 The IP address will be automatically assigned from the selected pool.

☒ iSCSI Static Target Interface ☐ iSCSI Auto Target Interface

Name	Priority	Port	Authentication Pro.	iSCSI IPv4 Address	LUN id
iqn.1992-08.c...	1	3260		192.168.10.62	0
iqn.1992-08.c...	2	3260		192.168.10.61	0

OK **Cancel**



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
```

Vserver	Target Name	Target Alias	Status 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`。

Create iSCSI Static Target ? ×

iSCSI Target Name :

Priority :

Port :

Authentication Profile : [Create iSCSI Authentication Profile](#)

IPv4 Address :

LUN ID :

29. 单击确定以添加 iSCSI 静态目标。

Set iSCSI Boot Parameters ? ×

[Create IQN Suffix Pool](#)

WARNING: The selected pool does not contain any available entities. You can select it, but it is recommended that you add entities to it.

[Initiator Address](#)

Initiator IP Address Policy:

IPv4 Address :

Subnet Mask :

Default Gateway :

Primary DNS :

Secondary DNS :

[Create IP Pool](#)

[Reset Initiator Address](#)

The IP address will be automatically assigned from the selected pool.

☒ iSCSI Static Target Interface ☐ iSCSI Auto Target Interface

Name	Priority	Port	Authentication Pro.	iSCSI IPv4 Address	LUN Id
iqn.1992-08.c...	1	3260		192.168.20.62	0
iqn.1992-08.c...	2	3260		192.168.20.61	0

[Add](#) [Delete](#) [Info](#)

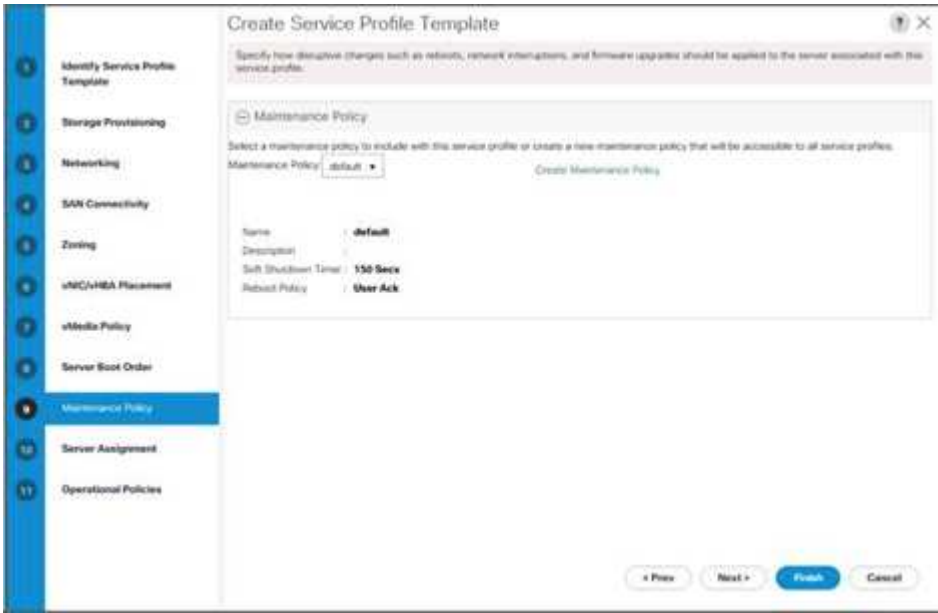
Minimum one instance of iSCSI Static Target Interface and maximum two are allowed.

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。

Create Service Profile Template

Optionally specify a server pool for this service profile template.

You can select a server pool you want to associate with this service profile template.

Pool Assignment: [Create Server Pool](#)

Select the power state to be applied when this profile is associated with the server.

☐ Up ☒ Down

The service profile template will be associated with one of the servers in the selected pool. If desired, you can specify an additional server pool policy qualification that the selected server must meet. To do so, select the qualification from the list.

Server Pool Qualification:

Restrict Migration: ☐

Firmware Management (BIOS, Disk Controller, Adapter)

If you select a host firmware policy for this service profile, the profile will update the firmware on the server that it is associated with. Otherwise the system uses the firmware already installed on the associated server.

Host Firmware Package: [Create Host Firmware Package](#)

< Prev Next > **Finish** Cancel

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。

Create Service Profile Template

Optionally specify information that affects how the system operates.

BIOS Configuration

If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile.

BIOS Policy:

External IP Management Configuration

Management IP Address

Monitoring Configuration (Thresholds)

Power Control Policy Configuration

Power control policy determines power allocation for a server in a given power group.

Power Control Policy: [Create Power Control Policy](#)

SCSI Policy

KVM Management Policy

< Prev Next > **Finish** Cancel

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](https://my.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。

Network Adapters

Select the adapters for this host's default management network connection. Use two or more adapters for fault-tolerance and load-balancing.

	Device Name	Hardware Label (MAC Address)	Status
[X]	vmnic0	Site-01-vNIC-A (...00:0a:2e)	Connected (...)
[X]	vmnic1	Site-01-vNIC-B (...00:0b:2e)	Connected (...)
[]	vmnic2	Site-01-ISC... (...00:0a:3e)	Connected (...)
[]	vmnic3	Site-01-ISC... (...00:0b:3e)	Connected (...)

<D> View Details <Space> Toggle Selected

<Enter> OK <Esc> Cancel

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



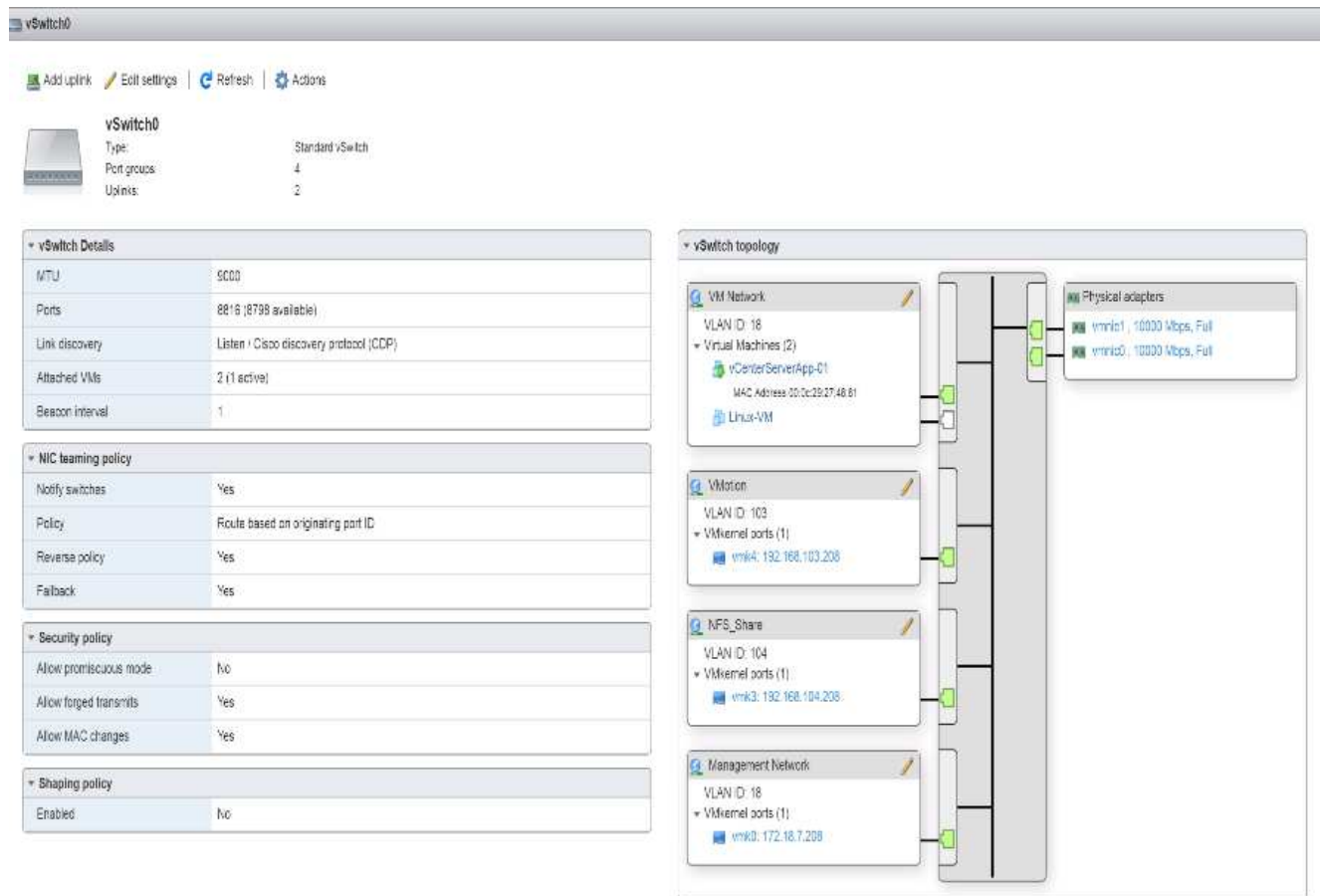
为了避免在重新分配 Cisco UCS iSCSI IP 池地址时发生 IP 地址冲突，建议对 iSCSI VMkernel 端口使用同一子网中的不同 IP 地址。

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 iScsiBootVSwitch-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 iScsiBootvSwitch B 。
32. 将 MTU 设置为 9000 。
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：



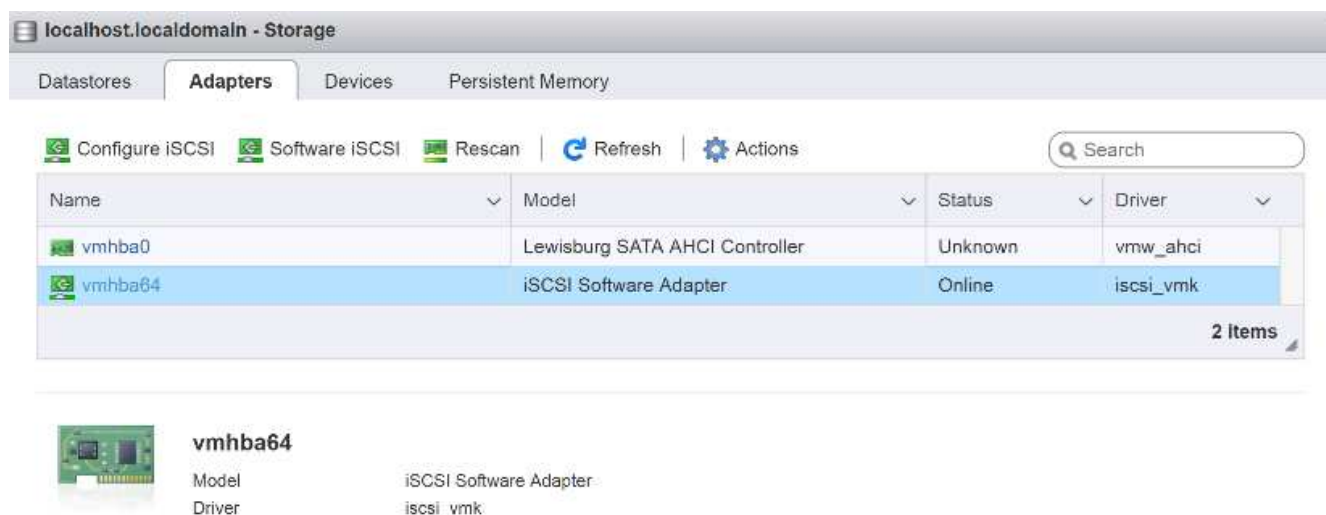
设置 iSCSI 多路径

ESXi 主机 VM-Host-Infra-01 和 VM-Host-Infra-02

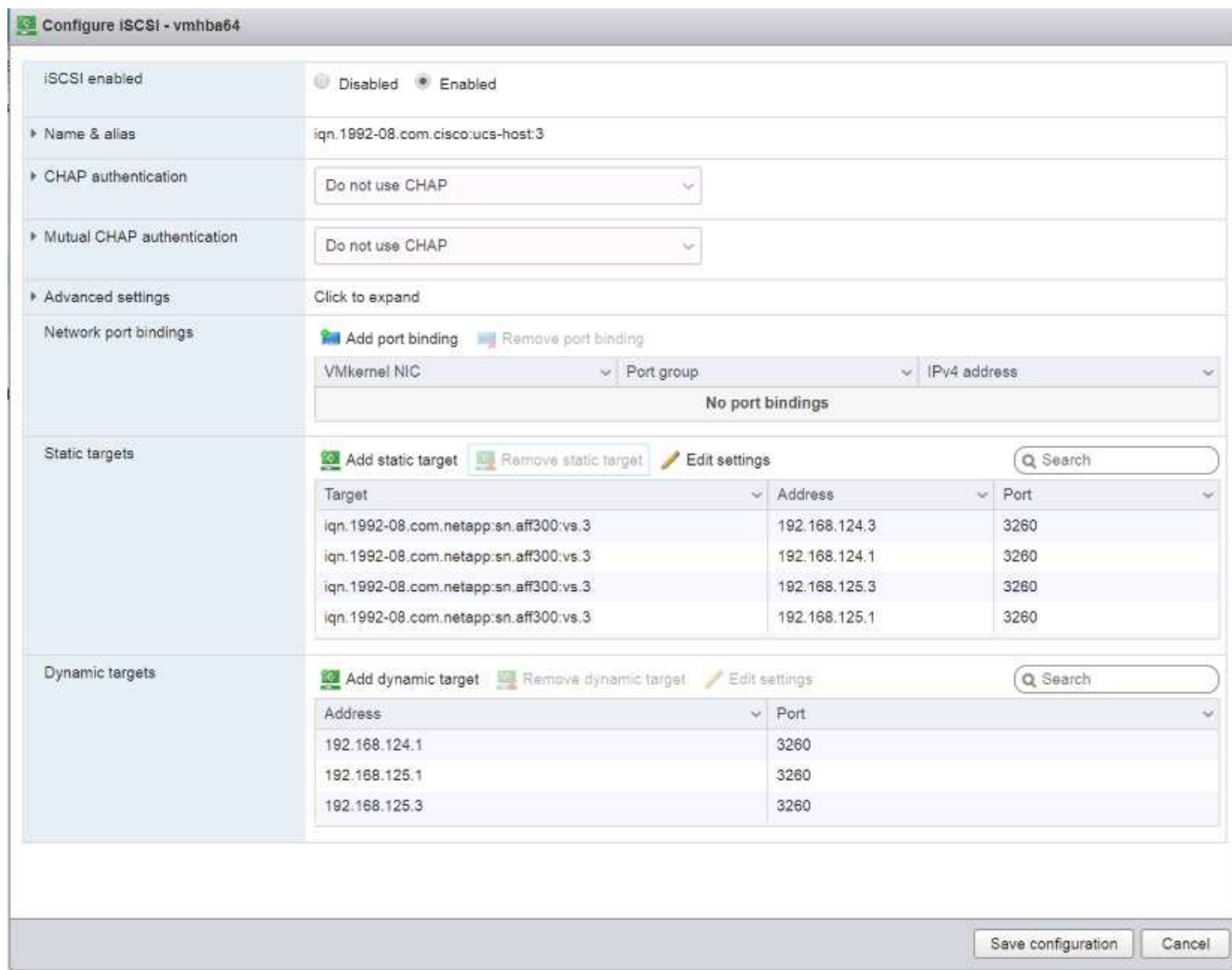
要在 ESXi 主机 VM-Host-Infra-01 和 VM-Host-Infra-02 上设置 iSCSI 多路径，请完成以下步骤：

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。



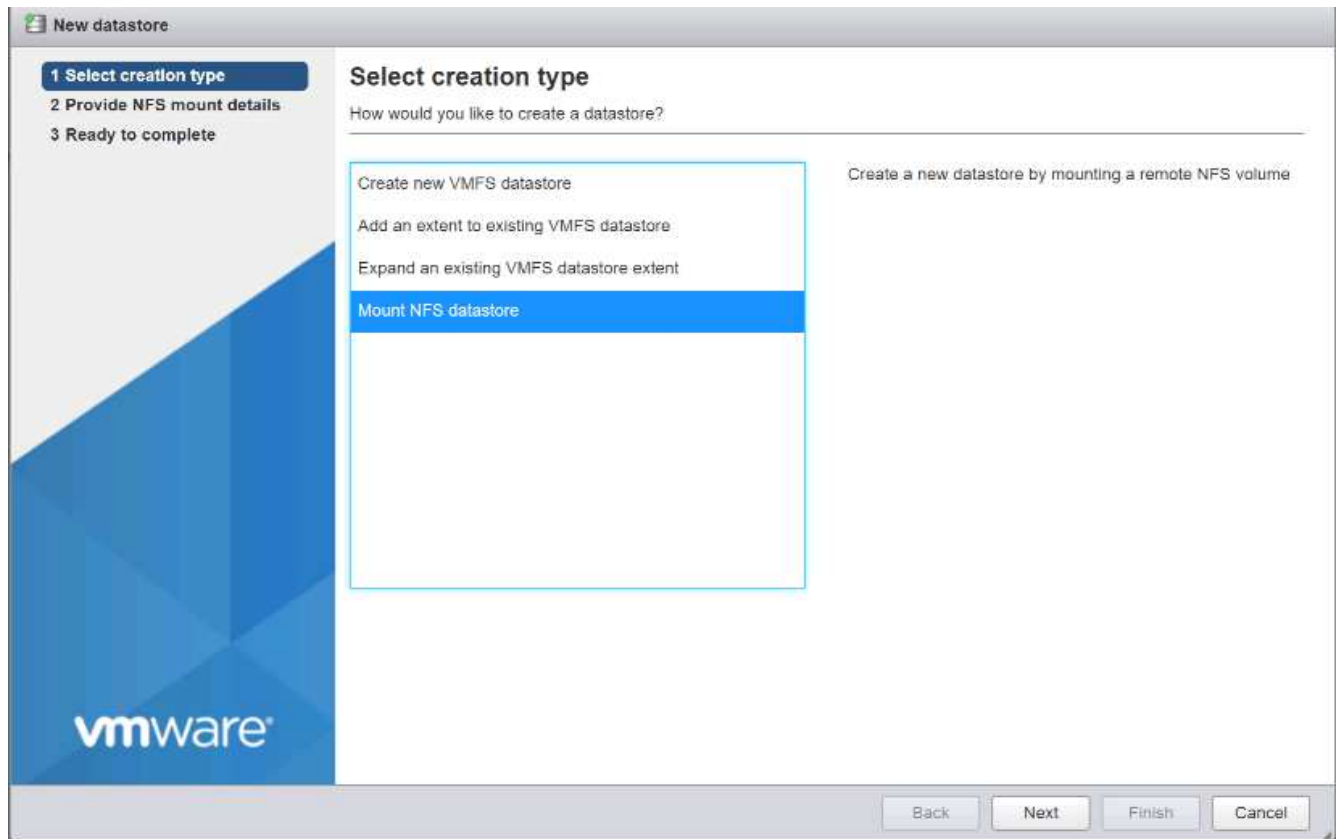
主机自动重新扫描存储适配器，并且目标会添加到静态目标。

挂载所需的数据存储库

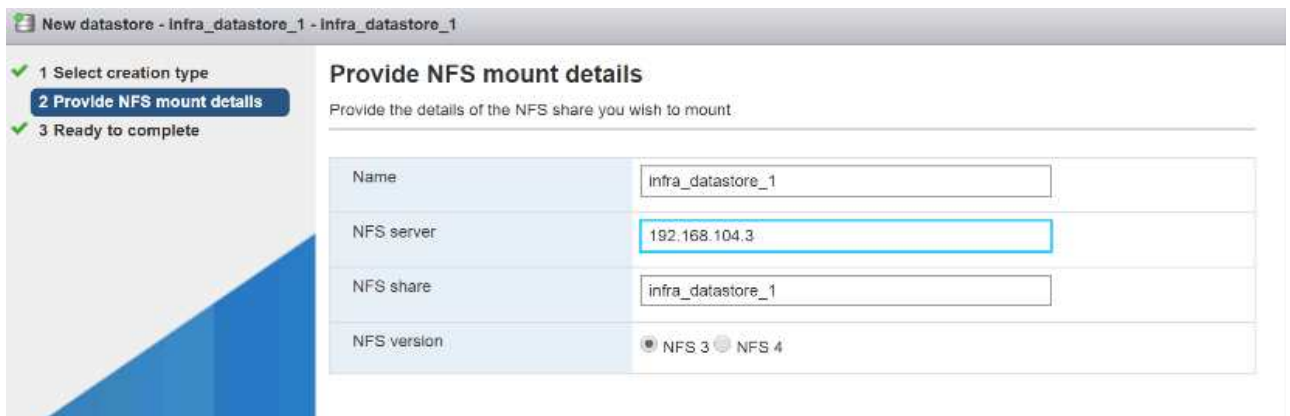
ESXi 主机 VM-Host-Infra-01 和 VM-Host-Infra-02

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。

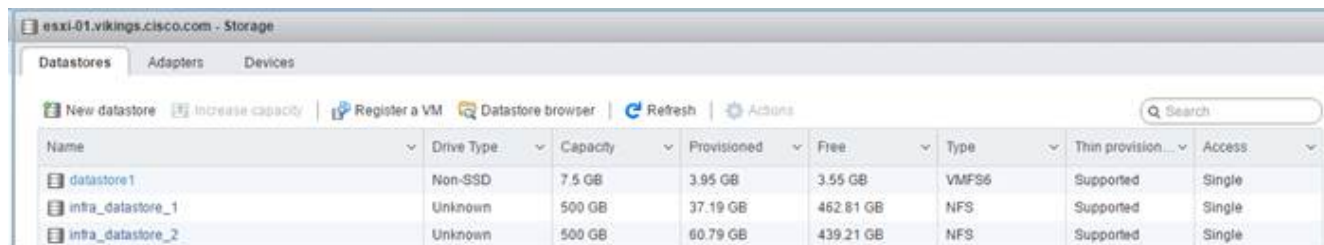


5. 在提供 NFS 挂载详细信息页面上，完成以下步骤：
 - a. 输入 `infra_datastore_1` 作为数据存储库名称。
 - b. 输入 NFS 服务器的 `nfs_lif01_a` LIF 的 IP 地址。
 - c. 为 NFS 共享输入 `/infra_datastore_1`。
 - d. 将 NFS 版本设置为 NFS 3。
 - e. 单击下一步。



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。



Name	Drive Type	Capacity	Provisioned	Free	Type	Thin provision...	Access
datastore1	Non-SSD	7.5 GB	3.95 GB	3.55 GB	VMFS5	Supported	Single
infra_datastore_1	Unknown	500 GB	37.19 GB	462.81 GB	NFS	Supported	Single
infra_datastore_2	Unknown	500 GB	60.79 GB	439.21 GB	NFS	Supported	Single

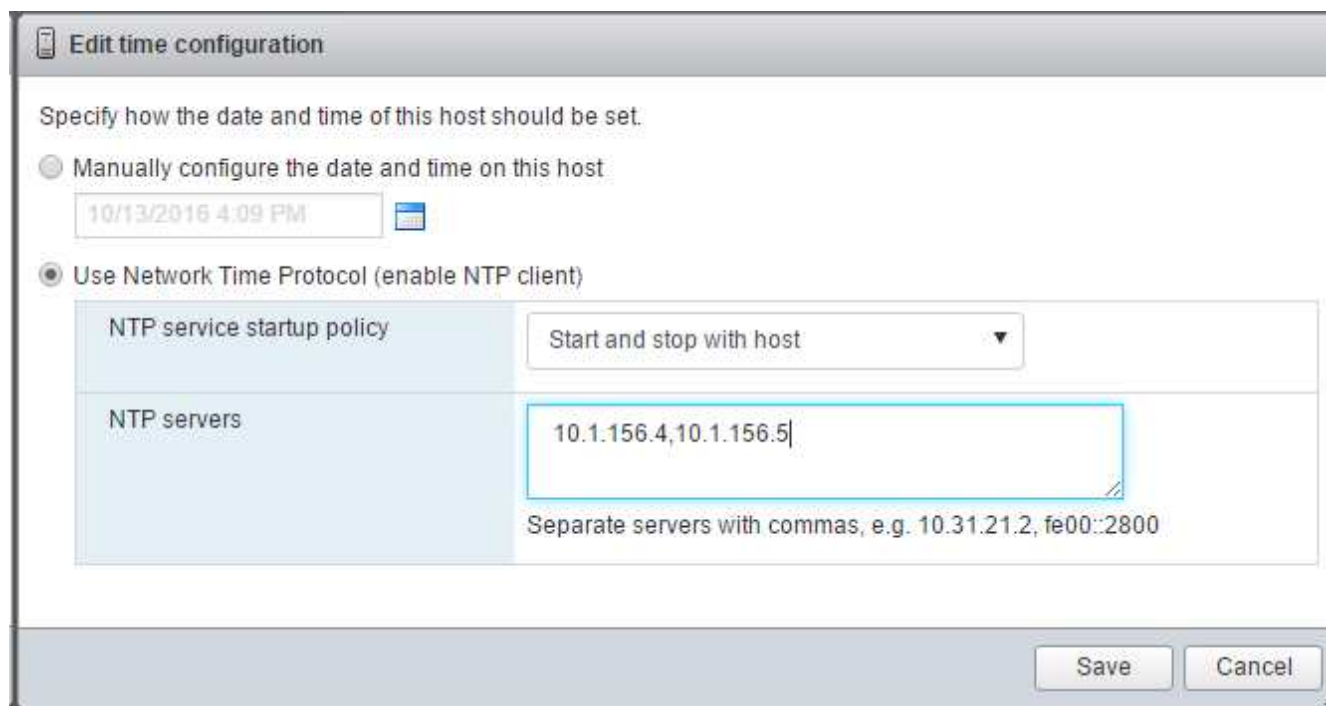
11. 在两台 ESXi 主机上挂载两个数据存储库。

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



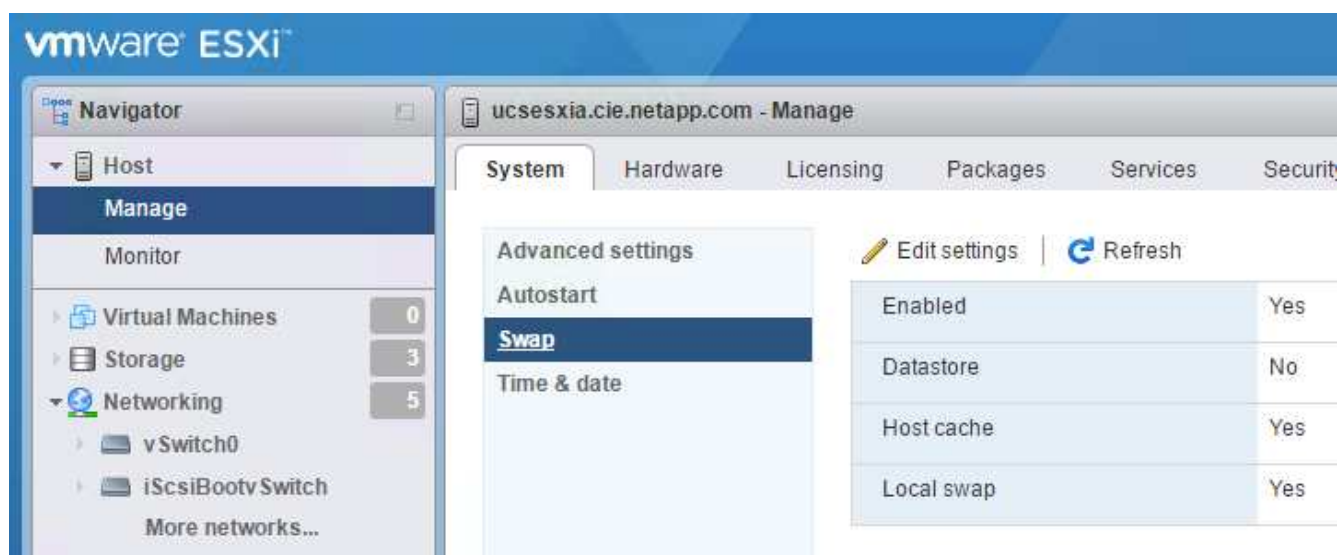
NTP 服务器时间可能与主机时间略有不同。

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。

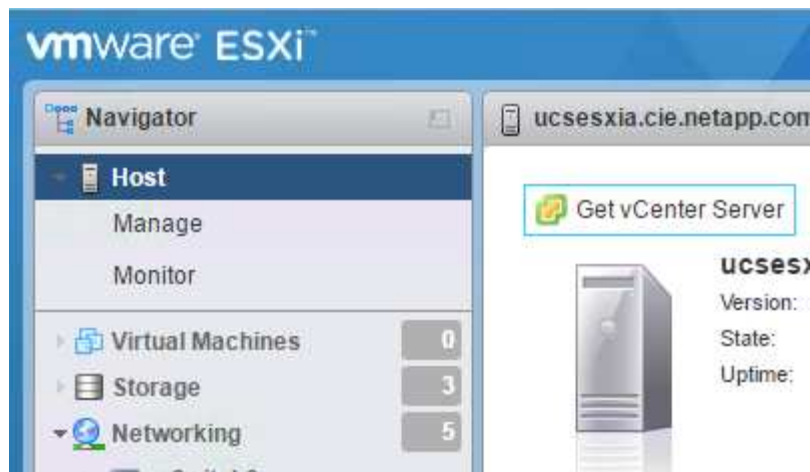


FlexPod Express 使用 VMware vCenter Server 设备（VCSA）。

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。

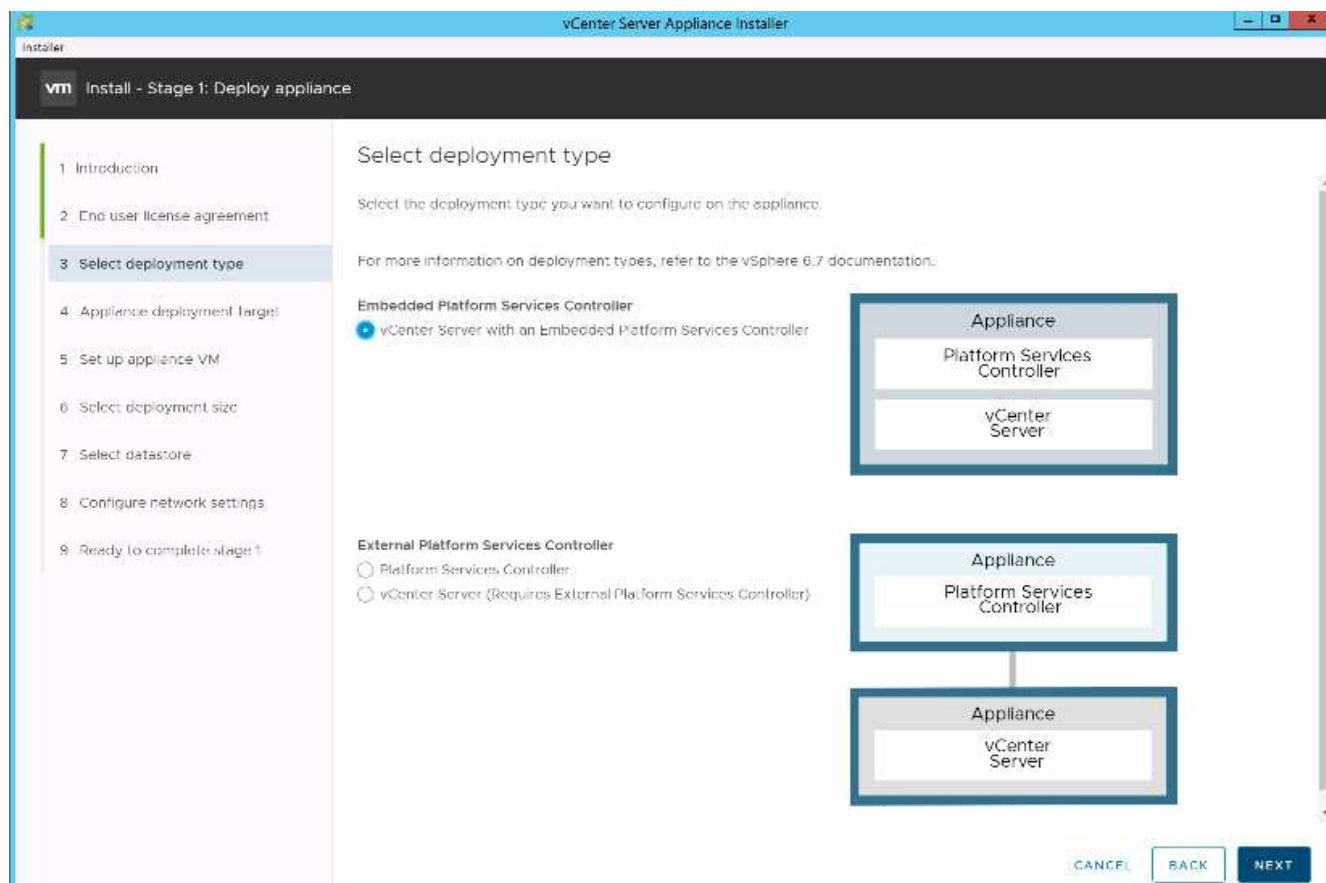
4. 导航到 `vcsa-ui-installer > win32` 目录。双击 `installer.exe`。

5. 单击安装。

6. 单击简介页面上的下一步。

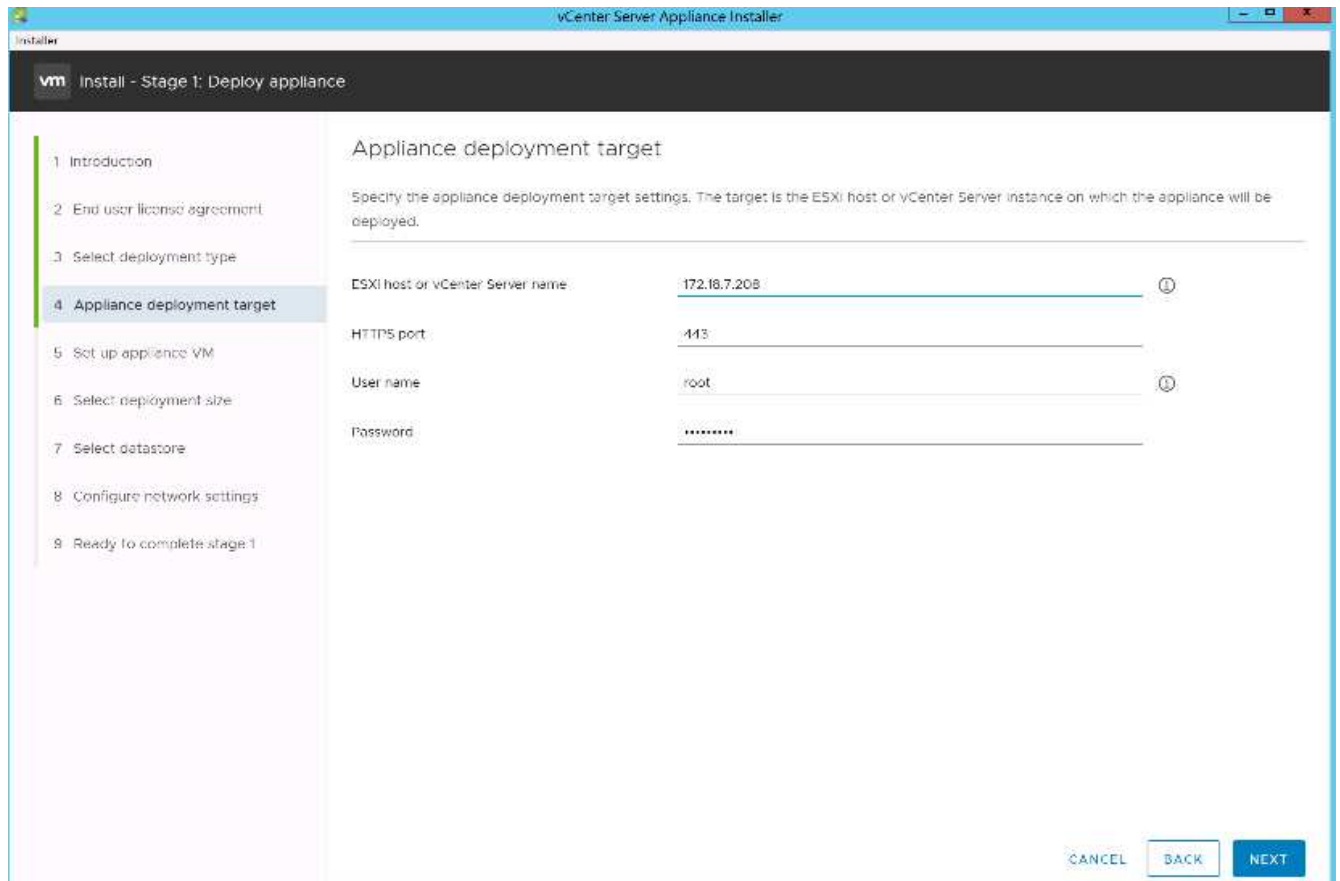
7. 接受 EULA。

8. 选择 Embedded Platform Services Controller 作为部署类型。

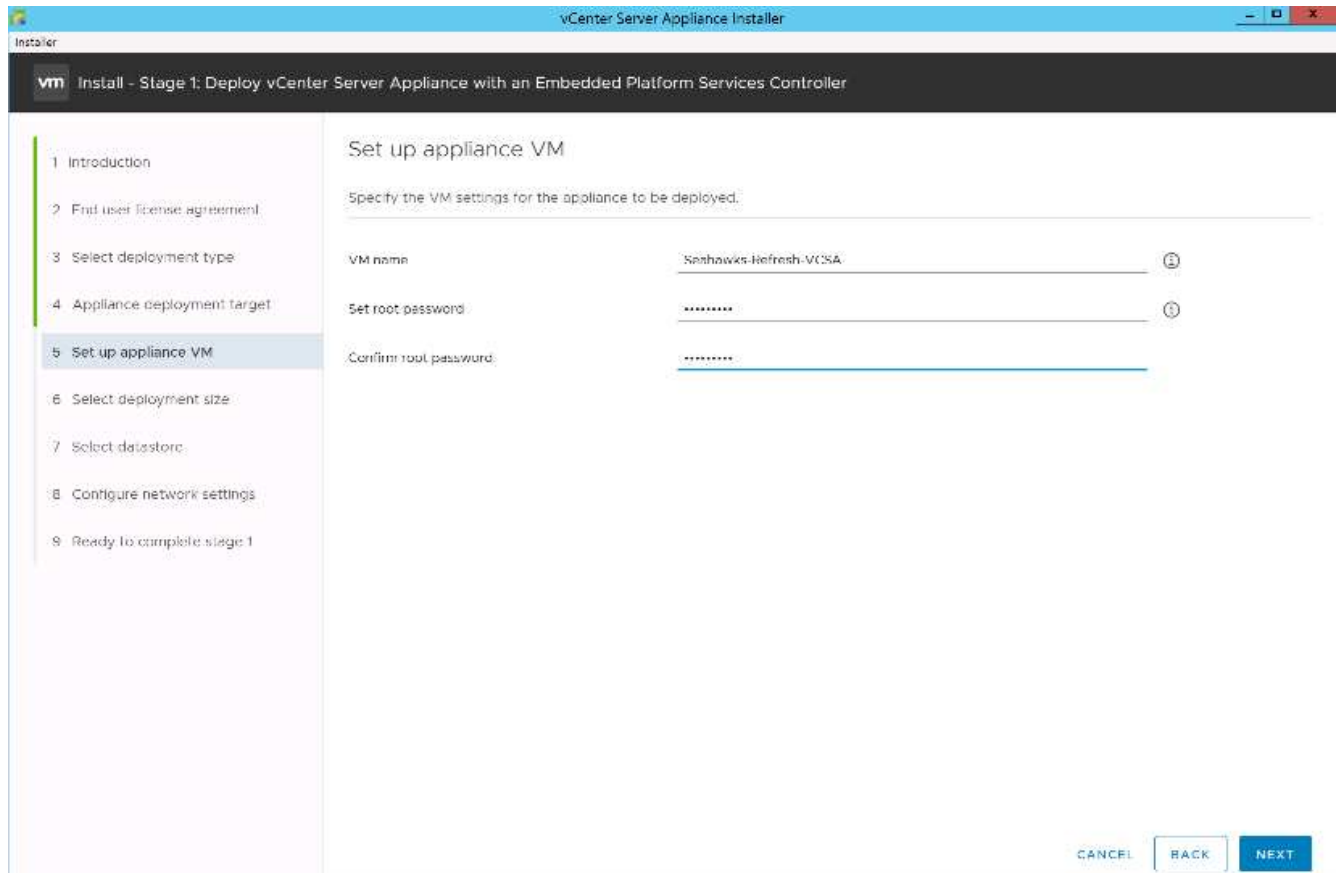


如果需要，还支持在 FlexPod Express 解决方案中部署外部平台服务控制器。

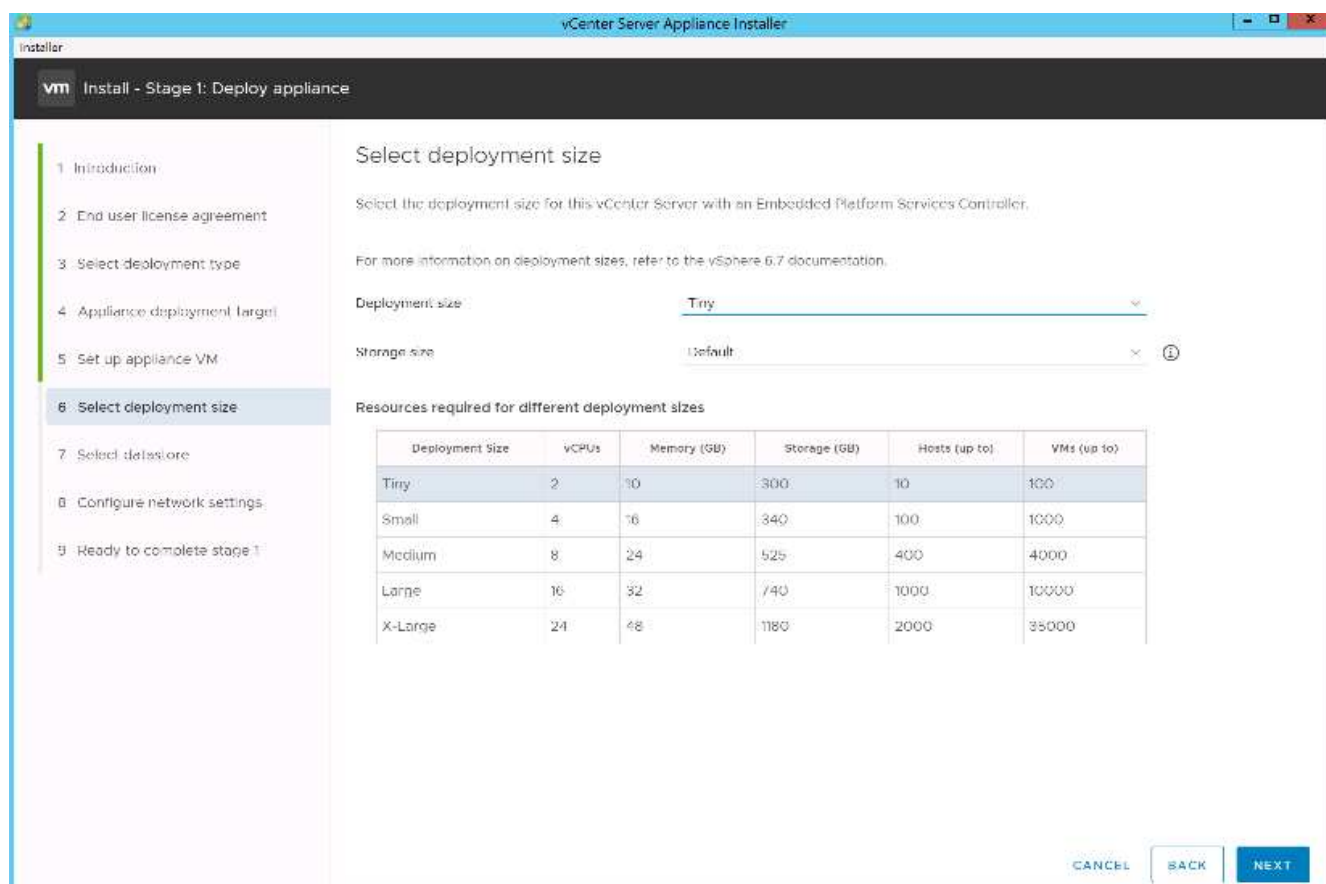
9. 在设备部署目标页面上，输入已部署的 ESXi 主机的 IP 地址，root 用户名和 root 密码。单击下一步。



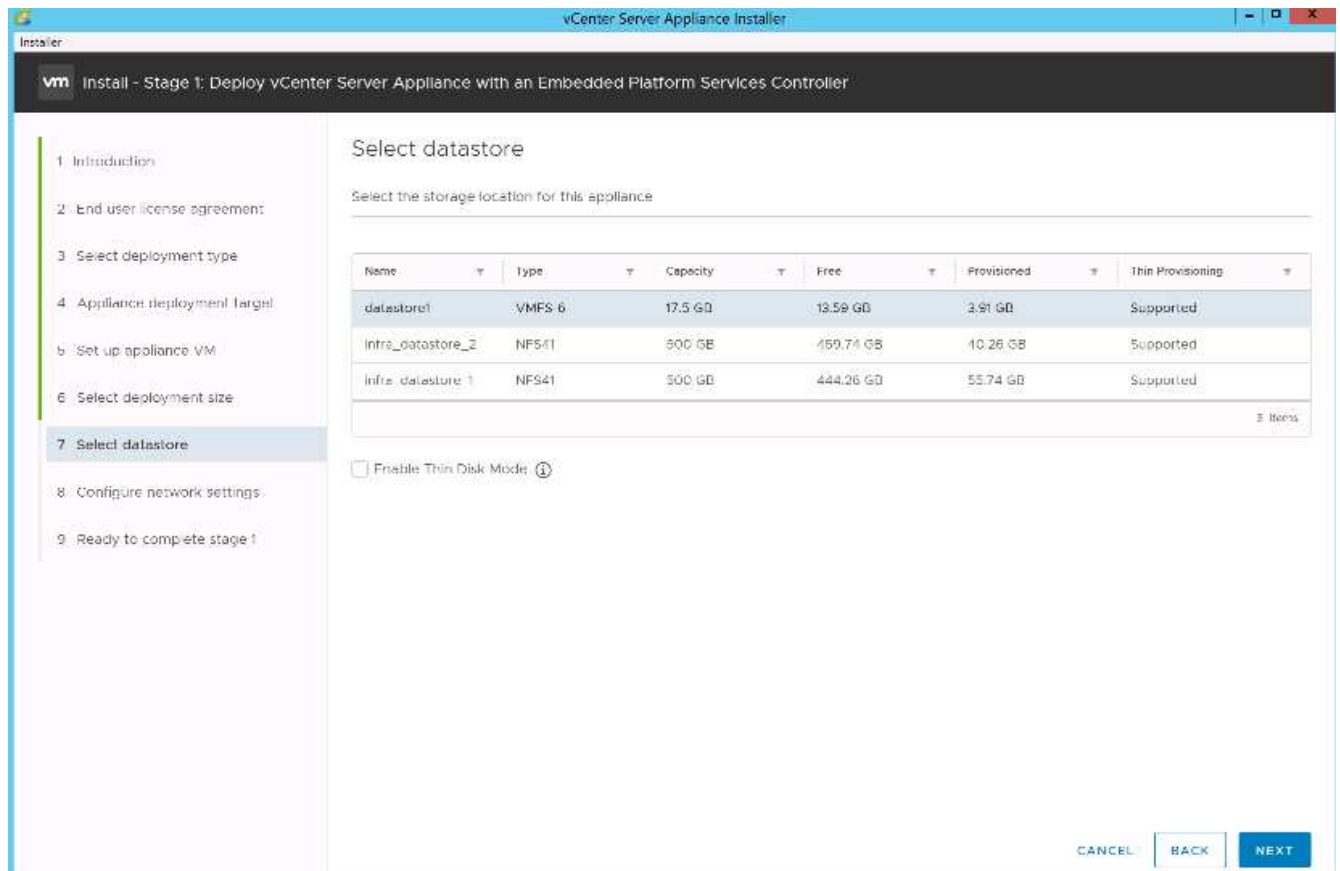
10. 输入 vCSA 作为 VM 名称以及要用于 VCSA 的根密码，以设置设备 VM。单击下一步。



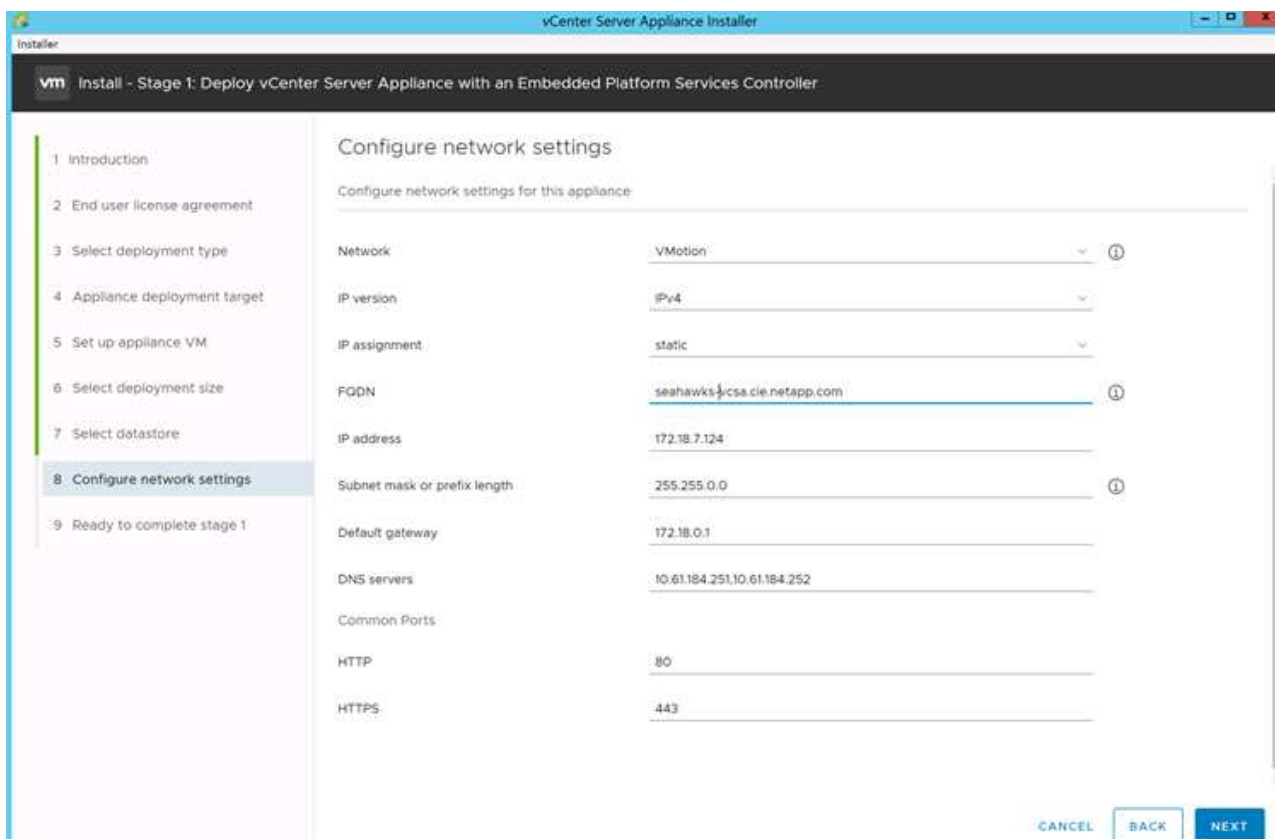
11. 选择最适合您环境的部署规模。单击下一步。



12. 选择 `infra_datastore_1` 数据存储库。单击下一步。



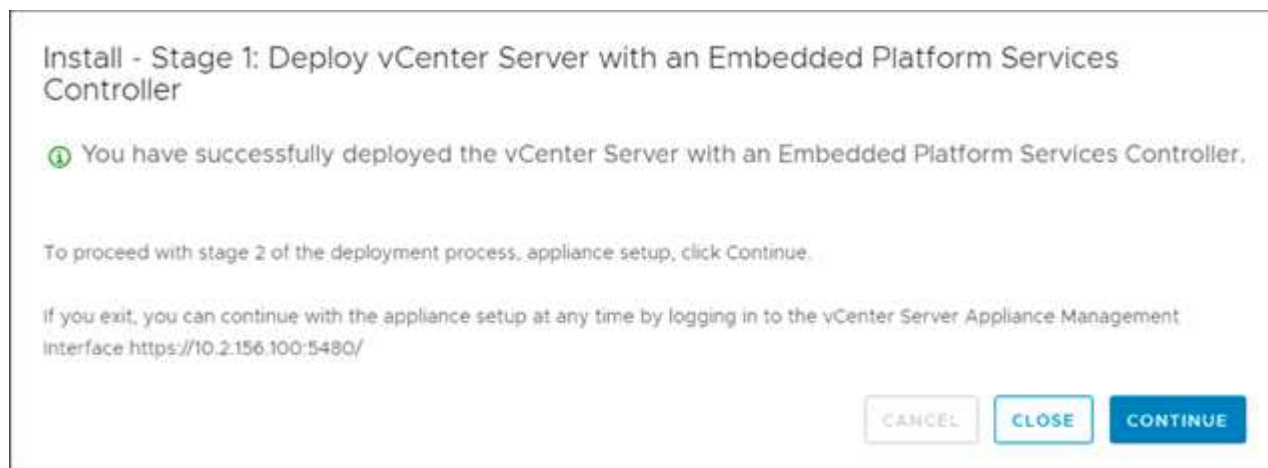
13. 在配置网络设置页面上输入以下信息，然后单击下一步。
 - a. 选择 MGMT-Network 作为您的网络。
 - b. 输入要用于 VCSA 的 FQDN 或 IP 。
 - c. 输入要使用的 IP 地址。
 - d. 输入要使用的子网掩码。
 - e. 输入默认网关。
 - f. 输入 DNS 服务器。



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。

请记住这些值以供参考，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。

New Cluster	
Name	Express
Location	Flexpod_SeaHawks
DRS	<input checked="" type="checkbox"/>
vSphere HA	<input checked="" type="checkbox"/>
vSAN	<input type="checkbox"/>

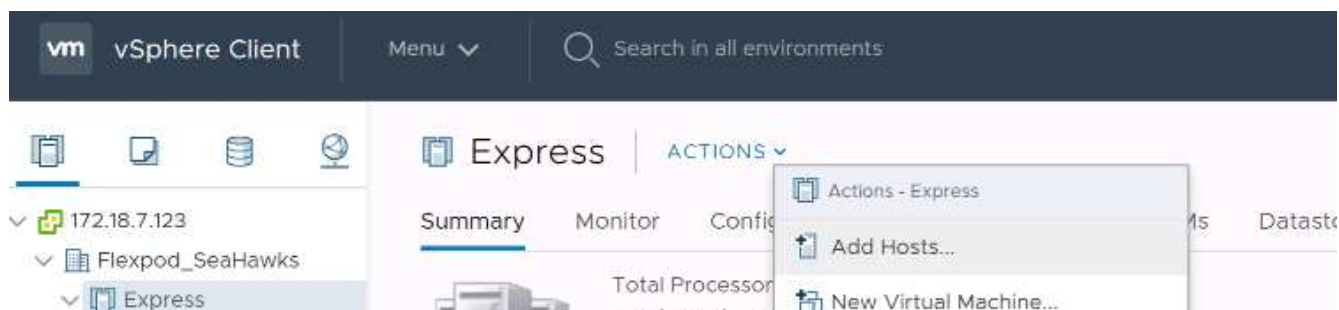
These services will have default settings - these can be changed later in the Cluster Quickstart workflow.

CANCEL OK

- 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"](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"](http://docs.netapp.com/platstor/index.jsp)

- ONTAP 9 文档中心

["http://docs.netapp.com/ontap-9/index.jsp"](http://docs.netapp.com/ontap-9/index.jsp)

- NetApp 产品文档

["https://docs.netapp.com"](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"](#)

版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

商标信息

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