FlexPod Express

FlexPod

NetApp
October 30, 2025

Tabla de contenidos

FlexPod Express

Guía de diseño de FlexPod Express con Cisco UCS C-Series y la serie AFF C190 de NetApp

Diseño de la arquitectura NVA-1139: FlexPod Express con Cisco UCS C-Series y AFF C190 Series de NetApp

Savita Kumari, NetApp

En colaboración con:[Error: Falta la imagen gráfica]

Las tendencias en el sector señalan una gran transformación de los centros de datos hacia una infraestructura compartida y cloud computing. Además, las organizaciones buscan una solución sencilla y eficaz para oficinas remotas y sucursales que utilicen la tecnología con la que están familiarizados en su centro de datos.

FlexPod Express es una arquitectura de centro de datos prediseñada con las mejores prácticas que se basa en Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus y los sistemas AFF de NetApp. Los componentes de FlexPod Express se asemejan a los homólogos de FlexPod Datacenter, lo que permite sinergias de gestión en un entorno completo de infraestructura TECNOLÓGICA a una escala menor. FlexPod Datacenter y FlexPod Express son plataformas óptimas para virtualización y para sistemas operativos con configuración básica y cargas de trabajo empresariales.

"Siguiente: Resumen del programa."

Resumen del programa

Cartera de infraestructura convergente de FlexPod

Las arquitecturas de referencia de FlexPod se proporcionan como diseños validados por Cisco (CVD) o como arquitecturas verificadas de NetApp (NVA). Se permiten las desviaciones basadas en los requisitos del cliente de un CVD o NVA determinado si dichas variaciones no dan como resultado la puesta en marcha de configuraciones no compatibles.

Como se muestra en la siguiente figura, la cartera de FlexPod incluye las siguientes soluciones: FlexPod Express y FlexPod Datacenter.

- **FlexPod Express** es una solución de gama básica con tecnologías de Cisco y NetApp.
- **FlexPod Datacenter** proporciona una base multiuso óptima para diversas cargas de trabajo y aplicaciones.

[Error: Falta la imagen gráfica]

Programa Arquitectura validada por NetApp

El programa Arquitectura verificada de NetApp ofrece a los clientes una arquitectura verificada para soluciones NetApp. Una solución NVA tiene las siguientes cualidades:

- Ha sido probada a conciencia

- Tiene naturaleza prescriptiva
- Minimiza los riesgos de implementación
- Acelera el plazo de comercialización esta guía detalla el diseño de FlexPod Express con VMware vSphere.

Además, este diseño aprovecha el nuevo sistema AFF C190, que ejecuta el software ONTAP 9.6 de NetApp, los conmutadores Cisco Nexus 31108 y los servidores Cisco UCS C220 M5 como nodos de hipervisor.

Descripción general de la solución

FlexPod Express está diseñado para ejecutar cargas de trabajo de virtualización mixtas. Está pensado para oficinas remotas, sucursales y para pequeñas y medianas empresas. También es perfecto para empresas más grandes que deseen implementar una solución dedicada para un fin específico. Esta nueva solución para FlexPod Express añade nuevas tecnologías, como ONTAP 9.6 de NetApp, el sistema AFF C190 de NetApp y VMware vSphere 6.7U2.

La siguiente figura muestra los componentes de hardware incluidos en la solución FlexPod Express.

[Error: Falta la imagen gráfica]

Público objetivo

Este documento está dirigido a usuarios que desean aprovechar una infraestructura creada para proporcionar eficiencia TECNOLÓGICA y posibilitar la innovación EN tecnología. El público de este documento incluye, sin limitarse a ellos, ingenieros de ventas, consultores de campo, personal de servicios profesionales, gestores DE TECNOLOGÍA, ingenieros de partners y clientes.

Tecnología de soluciones

Esta solución aprovecha las últimas tecnologías de NetApp, Cisco y VMware. Incluye el nuevo sistema AFF C190 de NetApp, que ejecuta el software ONTAP 9.6, los switches Cisco Nexus 31108 duales y los servidores de montaje en rack Cisco UCS C220 M5 que ejecutan VMware vSphere 6.7U2. Esta solución validada, como se muestra en la siguiente figura, utiliza tecnología Ethernet de 10 GB (10 GbE). También se ofrece orientación sobre cómo escalar agregando dos nodos de hipervisor a la vez para que la arquitectura FlexPod Express pueda adaptarse a las cambiantes necesidades empresariales de una organización.

[Error: Falta la imagen gráfica]

"Siguiente: Requisitos tecnológicos."

Requisitos tecnológicos

FlexPod Express requiere una combinación de componentes de hardware y software que depende de la velocidad del hipervisor y de la red seleccionados. Además, FlexPod Express puede establecer los componentes de hardware necesarios para añadir nodos de hipervisor en unidades de dos.

Requisitos de hardware

Independientemente del hipervisor elegido, todas las configuraciones exprés de FlexPod utilizan el mismo hardware. Por lo tanto, aunque cambien los requisitos del negocio, puede utilizar un hipervisor diferente en el mismo hardware de FlexPod Express.

En la siguiente tabla se enumeran los componentes de hardware necesarios para esta configuración exprés de FlexPod e implantar esta solución. Los componentes de hardware que se usan en cualquier implementación de la solución pueden variar en función de las necesidades del cliente.

Hardware subyacente	Cantidad
Clúster de 2 nodos C190 de AFF	1
Servidor Cisco UCS C220 M5	2
Switch Cisco Nexus 31108	2
Tarjeta de interfaz virtual (VIC) Cisco UCS 1457 para el servidor de montaje en rack Cisco UCS C220 M5	2

Requisitos de software

En la siguiente tabla se enumeran los componentes de software necesarios para implementar las arquitecturas de la solución FlexPod Express.

De NetApp	Versión	Detalles
Controladora de gestión integrada de Cisco (CIMC)	4.0.4	Para servidores en rack C220 M5
Cisco NX-OS	7.0(3)I7(6)	Para los switches Cisco Nexus 31108
ONTAP de NetApp	9.6	Para controladoras AFF C190 de NetApp

En la siguiente tabla se muestra el software necesario para todas las implementaciones de VMware vSphere en FlexPod Express.

De NetApp	Versión
Dispositivo VMware vCenter Server	6.7U2
VMware vSphere ESXi	6.7U2
Complemento VAAI de NetApp para ESXi	1.1.2
Consola de almacenamiento virtual de NetApp	9.6

"Siguiente: Opciones de diseño."

Opciones de diseño

Las tecnologías enumeradas en esta sección se han elegido durante la fase de diseño de la arquitectura. Cada tecnología cumple un propósito específico en la solución de infraestructura Express de FlexPod.

Serie AFF C190 de NetApp con ONTAP 9.6

Esta solución aprovecha dos de los productos más recientes de NetApp: El sistema AFF C190 de NetApp y el software ONTAP 9.6.

Sistema C190 de AFF

El grupo objetivo son los clientes que quieren modernizar su infraestructura TECNOLÓGICA con tecnología all-flash a un precio asequible. El sistema AFF C190 incluye el nuevo ONTAP 9.6 y las licencias de paquetes flash, lo que significa que las siguientes funciones están integradas:

- CIFS, NFS, iSCSI y FCP
- Software de replicación de datos SnapMirror de NetApp, software de backup SnapVault de NetApp, software de recuperación de datos SnapRestore de NetApp, suite de productos de software de gestión del almacenamiento SnapManager de NetApp y software SnapCenter de NetApp
- Tecnología FlexVol
- Deduplicación, compresión y compactación
- Aprovisionamiento ligero
- Calidad de servicio del almacenamiento
- Tecnología RAID DP de NetApp
- Tecnología Snapshot de NetApp
- FabricPool

Las siguientes figuras muestran las dos opciones para la conectividad de host.

La siguiente figura ilustra los puertos UTA 2 donde se puede insertar el módulo SFP+.

[Error: Falta la imagen gráfica]

En la siguiente figura se muestran los puertos 10GBASE-T para la conexión a través de cables Ethernet RJ-45 convencionales.

[Error: Falta la imagen gráfica]

Para la opción de puerto 10GBASE-T, debe tener un switch de enlace ascendente basado en 10GBASE-T.

El sistema C190 de AFF se ofrece exclusivamente con SSD de 960 GB. Puede elegir entre cuatro fases de expansión:

- 8x 960 GB
- 12x 960 GB
- 18x 960 GB
- 24x 960 GB

Para obtener toda la información sobre el sistema de hardware C190 de AFF, consulte "Página de la cabina all-flash C190 de AFF de NetApp".

Software ONTAP 9.6

Los sistemas AFF C190 de NetApp utilizan el nuevo software de gestión de datos ONTAP 9.6. ONTAP 9.6 es el software de gestión de datos empresariales líder del sector. Combina nuevos niveles de simplicidad y flexibilidad con potentes funcionalidades de gestión de datos, eficiencias de almacenamiento e integración del cloud líder.

ONTAP 9.6 cuenta con varias funciones que resultan adecuadas para la solución FlexPod Express. Lo más importante es el compromiso de NetApp con la eficiencia del almacenamiento, que puede ser una de las funciones más importantes para implementaciones pequeñas. Las características distintivas de la eficiencia del almacenamiento de NetApp, como la deduplicación, la compresión, la compactación y el thin provisioning, están disponibles en ONTAP 9.6. El sistema WAFL de NetApp siempre escribe bloques de 4 KB; por tanto, la compactación combina varios bloques en un bloque de 4 KB cuando los bloques no utilizan el espacio asignado de 4 KB. La siguiente figura ilustra este proceso.

[Error: Falta la imagen gráfica]

ONTAP 9.6 ahora admite un tamaño de bloque de 512 bytes opcional para volúmenes NVMe. Esta funcionalidad funciona bien con el sistema de archivos de máquina virtual (VMFS) de VMware, que utiliza de forma nativa un bloque de 512 bytes. Puede permanecer con el tamaño predeterminado de 4K o, opcionalmente, establecer el tamaño de bloque de 512 bytes.

Entre otras mejoras de las funciones de ONTAP 9.6 se incluyen:

- **Cifrado de agregados de NetApp (NAE).** NAE asigna claves a nivel de agregado, con lo que se cifran todos los volúmenes del agregado. Esta función permite cifrar y deduplicar los volúmenes en el nivel de agregado.
- **Mejora de volumen de ONTAP FlexGroup de NetApp**. En ONTAP 9.6, se puede cambiar fácilmente el nombre de un volumen de FlexGroup. No es necesario crear un nuevo volumen al que migrar los datos. El tamaño del volumen también se puede reducir mediante System Manager o CLI de ONTAP.
- **Mejora de FabricPool.** ONTAP 9.6 añadió compatibilidad adicional para almacenes de objetos como niveles de nube. También se añadió compatibilidad con Google Cloud y Alibaba Cloud Object Storage Service (OSS). FabricPool admite varios almacenes de objetos, incluidos AWS S3, Azure Blob, el almacenamiento de objetos IBM Cloud y el software de almacenamiento basado en objetos StorageGRID de NetApp.
- **Mejora de SnapMirror.** en ONTAP 9.6, una nueva relación de replicación de volúmenes se cifra de forma predeterminada antes de salir de la matriz de origen y se descifra en el destino de SnapMirror.

Serie Nexus 3000 de Cisco

El Cisco Nexus 31108PC-V es un switch de superior rack (Tor) basado en 10 Gbps SFP+ con 48 puertos SFP+ y 6 puertos QSFP28. Cada puerto SFP+ puede funcionar en 100 Mbps, 10 Gbps y cada puerto QSFP28 puede funcionar en modo nativo de 100 Gbps o 40 Gbps o en modo 4x 10 Gbps, lo que ofrece opciones flexibles de migración. Este conmutador es un verdadero conmutador sin PHY optimizado para una baja latencia y bajo consumo de energía.

La especificación Cisco Nexus 31108PC-V incluye los siguientes componentes:

- Capacidad de conmutación de 2,16 Tbps y velocidad de reenvío de hasta 1,2 Tbps para 31108PC-V.
- 48 puertos SFP admiten 1 y 10 Gigabit Ethernet (10GbE); los seis puertos QSFP28 admiten 4 x 10 GbE o 40 GbE cada uno o 100 GbE

La siguiente figura muestra el switch Cisco Nexus 31108PC-V.

[Error: Falta la imagen gráfica]

Para obtener más información sobre los switches Cisco Nexus 31108PC-V, consulte "Hoja de datos de los conmutadores Cisco Nexus 3172PQ, 3172TQ, 3172PQ-32T, 3172PQ-XL y 3172TQ-XL".

Cisco UCS C-Series

Se eligió el servidor en rack Cisco UCS C-Series para FlexPod Express porque sus numerosas opciones de configuración permiten adaptarse a requisitos específicos en una puesta en marcha de FlexPod Express.

Los servidores de montaje en rack Cisco UCS C-Series ofrecen informática unificada en un factor de forma estándar del sector para reducir el TCO y aumentar la agilidad.

Los servidores de montaje en rack Cisco UCS C-Series ofrecen las siguientes ventajas:

- Un punto de entrada independiente del factor de forma en Cisco UCS
- Puesta en marcha de aplicaciones simplificada y rápida
- Ampliación de las innovaciones y ventajas de la informática unificada a los servidores en rack
- Mayor elección para el cliente gracias a sus ventajas únicas en un paquete de rack conocido

[Error: Falta la imagen gráfica]

El servidor de montaje en rack Cisco UCS C220 M5, mostrado en la figura anterior, se encuentra entre la infraestructura empresarial y los servidores de aplicaciones más versátiles y generales del sector. Se trata de un servidor en rack de dos sockets de alta densidad que ofrece un rendimiento y una eficiencia líderes en el sector para una amplia gama de cargas de trabajo, incluidas aplicaciones de virtualización, colaboración y con configuración básica. Los servidores en rack Cisco UCS C-Series se pueden implementar como servidores independientes o como parte de Cisco UCS para aprovechar las innovaciones informáticas unificadas basadas en estándares de Cisco que ayudan a reducir el coste total de propiedad de los clientes y a aumentar la agilidad empresarial.

Para obtener más información sobre los servidores C220 M5, consulte "Hoja de datos del servidor en rack Cisco UCS C220 M5".

Conectividad Cisco UCS VIC 1457 para servidores C220 M5

El adaptador Cisco UCS VIC 1457 mostrado en la siguiente figura es una LAN modular de factor de forma pequeño y conectable (SFP28) de cuatro puertos en la tarjeta madre (mLOM) diseñada para la generación M5 de servidores Cisco UCS C-Series. La tarjeta admite Ethernet o FCoE de 10 Gbps. La tarjeta puede presentar interfaces compatibles con los estándares PCIe al host y pueden configurarse dinámicamente como NIC o HBA.

[Error: Falta la imagen gráfica]

Para obtener toda la información sobre el adaptador Cisco UCS VIC 1457, consulte "Especificaciones técnicas de la serie 1400 de tarjeta de interfaz virtual Cisco UCS".

VMware vSphere 6.7U2

VMware vSphere 6.7U2 es una de las opciones de hipervisor para utilizar con FlexPod Express. VMware vSphere permite a las organizaciones reducir su huella de potencia y refrigeración a la vez que confirman que la capacidad de computación adquirida se ha aprovechado al máximo. Además, VMware vSphere permite la protección contra fallos de hardware (alta disponibilidad de VMware o ha de VMware) y el equilibrio de carga de recursos informáticos en un clúster de hosts vSphere (planificador de recursos distribuidos de VMware en modo de mantenimiento o DRS-MM de VMware).

Dado que reinicia únicamente el kernel, VMware vSphere 6.7U2 permite a los clientes efectuar un arranque rápido, cargando vSphere ESXi sin reiniciar el hardware. El cliente vSphere 6.7U2 vSphere (cliente basado en HTML5) tiene algunas mejoras nuevas como Developer Center con Code Capture y API Explore. Con Code

Capture, puede registrar sus acciones en vSphere Client para proporcionar una salida de código simple y utilizable. VSphere 6.7U2 también contiene nuevas funciones como DRS en modo de mantenimiento (DRS-MM).

VMware vSphere 6.7U2 ofrece las siguientes funciones:

- VMware utiliza el modelo de puesta en marcha externo de VMware Platform Services Controller (PSC).

> A partir de la siguiente versión principal de vSphere, PSC externo no será una opción disponible.

- Nueva compatibilidad de protocolos para realizar backups y restaurar un dispositivo de vCenter Server. Introducción de NFS y SMB como opciones de protocolo admitidas, hasta un total de 7 (HTTP, HTTPS, FTP, FTPS, SCP, NFS y SMB) al configurar una instancia de vCenter Server para operaciones de backup o restauración basadas en archivos.
- Nuevo funcionalmente al utilizar la biblioteca de contenido. La sincronización de una plantilla de máquina virtual nativa entre bibliotecas de contenido ahora está disponible cuando vCenter Server está configurado para el modo vinculado mejorado.
- Actualice a la "Página de complementos de cliente".
- VMware vSphere Update Manager también añade mejoras al cliente vSphere. Puede realizar el cumplimiento de la comprobación de asociación y solucionar acciones desde una sola pantalla.

Para obtener más información sobre VMware vSphere 6.7 U2, consulte "Página del blog de VMware vSphere".

Para obtener más información sobre las actualizaciones de VMware vCenter Server 6.7 U2, consulte "Notas de la versión".

> Aunque esta solución se validó con vSphere 6.7U2, admite cualquier versión de vSphere calificada con los otros componentes del "Herramienta de matriz de interoperabilidad de NetApp (IMT)". NetApp recomienda poner en marcha la siguiente versión de vSphere para sus correcciones y funciones mejoradas.

Arquitectura de arranque

Entre las opciones admitidas para la arquitectura de arranque Express de FlexPod se incluyen las siguientes:

- LUN SAN iSCSI
- Tarjeta SD Cisco FlexFlash
- Disco local

El centro de datos FlexPod se arranca desde LUN de iSCSI; por tanto, la administración de la solución se mejora mediante el uso también del arranque iSCSI para FlexPod Express.

Distribución de la tarjeta de interfaz de red virtual del host ESXi

Cisco UCS VIC 1457 tiene cuatro puertos físicos. Esta validación de solución incluye estos cuatro puertos físicos en el uso del host ESXi. Si tiene un número menor o mayor de NIC, puede tener diferentes números VMNIC.

En una implementación de arranque iSCSI, el arranque iSCSI requiere tarjetas de interfaz de red virtual (vNIC) independientes para el arranque iSCSI. Estos vNIC utilizan la VLAN iSCSI de la estructura adecuada como VLAN nativa y están conectados a los vSwitch de arranque iSCSI, como se muestra en la siguiente figura.

[Error: Falta la imagen gráfica]

"Siguiente: Conclusión."

Conclusión

El diseño validado FlexPod Express es una solución sencilla y efectiva que utiliza componentes líderes en el sector. Al escalar y proporcionar opciones para la plataforma del hipervisor, FlexPod Express se puede adaptar a las necesidades específicas del negocio. FlexPod Express se ha diseñado para pequeñas y medianas empresas, oficinas remotas y sucursales, y otras empresas que requieren soluciones dedicadas.

"Siguiente: Dónde encontrar información adicional."

Dónde encontrar información adicional

Para obtener más información sobre la información descrita en este documento, consulte los siguientes documentos y sitios web:

- Centro de documentación de los sistemas AFF y FAS

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

- Recursos de documentación de AFF

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

- Guía de puesta en marcha de FlexPod Express con VMware vSphere 6.7 y AFF C190 de NetApp (en curso)
- Documentación de NetApp

  "https://docs.netapp.com"

Guía de puesta en marcha de FlexPod Express con Cisco UCS C-Series y la serie AFF C190 de NetApp

NVA-1142-PUESTA en MARCHA: FlexPod Express con Cisco UCS C-Series y AFF C190 Series de NetApp: Puesta en marcha NVA

Savita Kumari, NetApp

Las tendencias del sector indican que se está produciendo una gran transformación de los centros de datos hacia la infraestructura compartida y el cloud computing. Además, las organizaciones buscan una solución sencilla y eficaz para oficinas remotas y sucursales que utilicen la tecnología con la que estén familiarizados en su centro de datos.

FlexPod® Express es una arquitectura de centro de datos diseñada previamente y basada en el Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus y las tecnologías de almacenamiento de

NetApp®. Los componentes de un sistema FlexPod Express se asemejan a los del centro de datos FlexPod, lo que permite sinergias de gestión en todo el entorno de infraestructura DE TI a una escala menor. FlexPod Datacenter y FlexPod Express son plataformas óptimas para virtualización y para sistemas operativos con configuración básica y cargas de trabajo empresariales.

El centro de datos de FlexPod y FlexPod Express proporcionan una configuración básica y cuentan con la flexibilidad necesaria para ajustar su tamaño y optimizarse con el objetivo de acomodar distintos casos de uso y requisitos. Los clientes existentes de FlexPod Datacenter pueden gestionar su sistema FlexPod Express con las herramientas a las que están acostumbrados. Los nuevos clientes de FlexPod Express pueden realizar fácilmente la transición a la gestión del centro de datos FlexPod a medida que crece su entorno.

FlexPod Express es una base de infraestructura óptima para oficinas remotas y sucursales y para pequeñas y medianas empresas. También es una solución óptima para los clientes que desean proporcionar infraestructura para cargas de trabajo dedicadas.

FlexPod Express proporciona una infraestructura fácil de gestionar que es adecuada para casi cualquier carga de trabajo.

Descripción general de la solución

Esta solución FlexPod Express forma parte del programa de infraestructura convergente de FlexPod.

Programa de infraestructura convergente FlexPod

Las arquitecturas de referencia FlexPod se proporcionan como diseños validados por Cisco (CVD) o como arquitecturas verificadas por NetApp (NVA). Se permiten las desviaciones basadas en los requisitos de los clientes de un CVD o NVA determinado si estas variaciones no crean una configuración incompatible.

El programa FlexPod incluye dos soluciones: FlexPod Express y FlexPod Datacenter.

- **FlexPod Express.** ofrece a los clientes una solución de gama básica con tecnologías de Cisco y NetApp.
- **FlexPod Datacenter.** proporciona una base multiuso óptima para diversas cargas de trabajo y aplicaciones.

Programa Arquitectura validada por NetApp

El programa Arquitectura verificada de NetApp ofrece a los clientes una arquitectura verificada para soluciones NetApp. Una arquitectura verificada de NetApp ofrece una arquitectura de solución de NetApp con las siguientes cualidades:

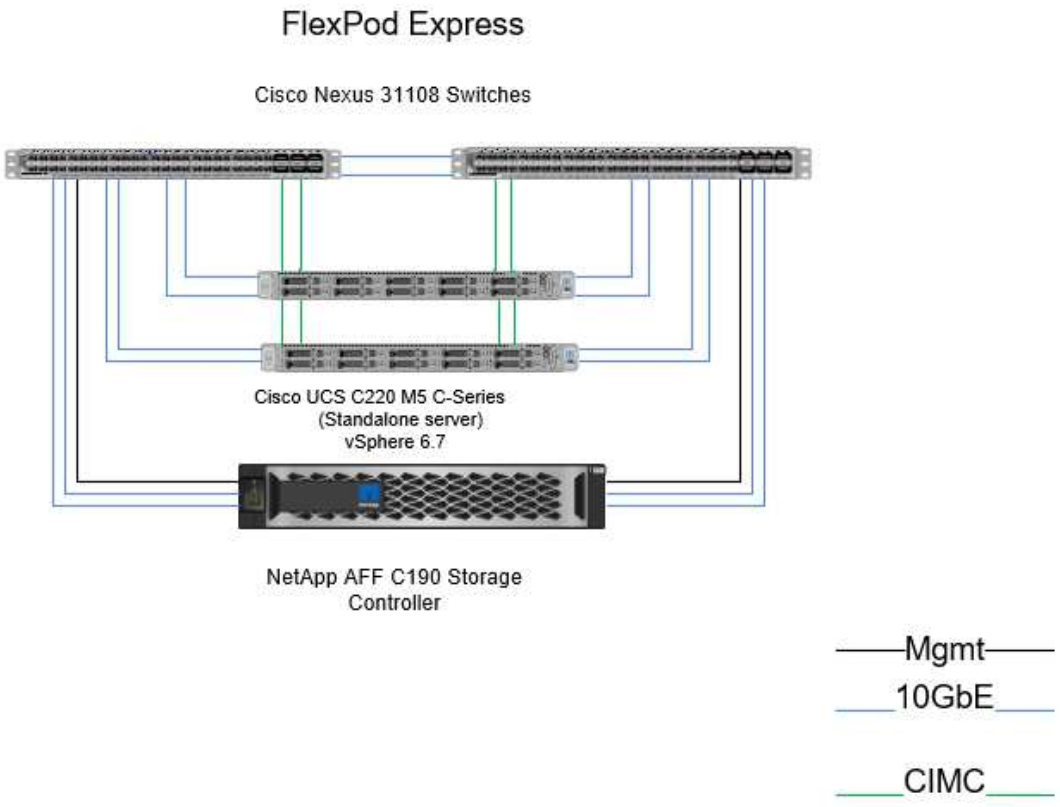
- Completamente probado
- Naturaleza prescriptiva
- Riesgos mínimos en la implementación
- Plazos de comercialización reducidos

Esta guía detalla el diseño de FlexPod Express con VMware vSphere. Además, este diseño utiliza el nuevo sistema AFF C190 (que ejecuta ONTAP® 9.6 de NetApp), los servidores Cisco Nexus 31108 y Cisco UCS C-Series C220 M5 como nodos de hipervisor.

Tecnología de soluciones

Esta solución aprovecha las últimas tecnologías de NetApp, Cisco y VMware. Esta solución incluye el nuevo

sistema AFF C190 de NetApp con ONTAP 9.6, switches Cisco Nexus 31108 duales y servidores de rack Cisco UCS C220 M5 con VMware vSphere 6.7U2. Esta solución validada usa tecnología 10 GbE. También se ofrece orientación sobre cómo escalar la capacidad de computación mediante la adición de dos nodos de hipervisor a la vez para que la arquitectura FlexPod Express pueda adaptarse a las cambiantes necesidades empresariales de una organización.



Para utilizar los cuatro puertos físicos de 10 GbE del VIC 1457 de manera eficiente, crear dos enlaces adicionales desde cada servidor hasta los switches de bastidor superior.

Resumen de casos de uso

La solución FlexPod Express puede aplicarse a varios casos prácticos, incluidos los siguientes:

- Oficinas remotas o filiales
- Pequeñas y medianas empresas
- Entornos que requieren una solución dedicada y rentable

FlexPod Express está indicado para cargas de trabajo virtualizadas y mixtas. Aunque esta solución se validó con vSphere 6.7U2, es compatible con cualquier versión de vSphere cualificada con el resto de componentes de la herramienta de matriz de interoperabilidad de NetApp. NetApp recomienda implementar vSphere 6.7U2 debido a sus correcciones y funciones mejoradas, como:

- Nueva compatibilidad de protocolos para backup y restauración de un dispositivo servidor vCenter, incluidos HTTP, HTTPS, FTP, FTPS, SCP, NFS Y SMB.

- Nuevo funcionalmente al utilizar la biblioteca de contenido. La sincronización de plantillas de equipos virtuales nativas entre bibliotecas de contenido ahora está disponible cuando vCenter Server está configurado para el modo vinculado mejorado.
- Una página actualizada del complemento de cliente.
- Se han añadido mejoras en vSphere Update Manager (VUM) y el cliente de vSphere. Ahora puede realizar las acciones de adjuntar, comprobar y solucionar, todas desde una sola pantalla.

Para obtener más información sobre este tema, consulte "Página vSphere 6.7U2" y la "Notas de la versión de vCenter Server 6.7U2".

Requisitos tecnológicos

Un sistema FlexPod Express requiere una combinación de componentes de hardware y software. FlexPod Express también describe los componentes de hardware necesarios para añadir nodos de hipervisor al sistema en unidades de dos.

Requisitos de hardware

Independientemente del hipervisor elegido, todas las configuraciones exprés de FlexPod utilizan el mismo hardware. Por lo tanto, aunque cambien los requisitos del negocio, puede utilizar un hipervisor diferente en el mismo hardware de FlexPod Express.

En la siguiente tabla se enumeran los componentes de hardware necesarios para la configuración e implementación de FlexPod Express. Los componentes de hardware que se usan en cualquier implementación de la solución pueden variar en función de las necesidades del cliente.

Hardware subyacente	Cantidad
Clúster de dos nodos C190 de AFF	1
Servidor Cisco C220 M5	2
Switch Cisco Nexus 31108PC-V	2
Tarjeta de interfaz virtual (VIC) Cisco UCS 1457 para el servidor de montaje en rack Cisco UCS C220 M5	2

Esta tabla enumera el hardware necesario además de la configuración base para implementar 10 GbE.

Hardware subyacente	Cantidad
Servidor Cisco UCS C220 M5	2
Cisco VIC 1457	2

Requisitos de software

En la siguiente tabla se enumeran los componentes de software necesarios para implementar las arquitecturas de las soluciones Express de FlexPod.

De NetApp	Versión	Detalles
Controladora de gestión integrada de Cisco (CIMC)	4.0.4	Para los servidores en rack Cisco UCS C220 M5

De NetApp	Versión	Detalles
Controlador nenic de Cisco	1.0.0.29	Para tarjetas de interfaz VIC 1457
Cisco NX-OS	7.0(3)I7(6)	Para switches Cisco Nexus 31108PC-V.
ONTAP de NetApp	9.6	Para controladoras C190 de AFF

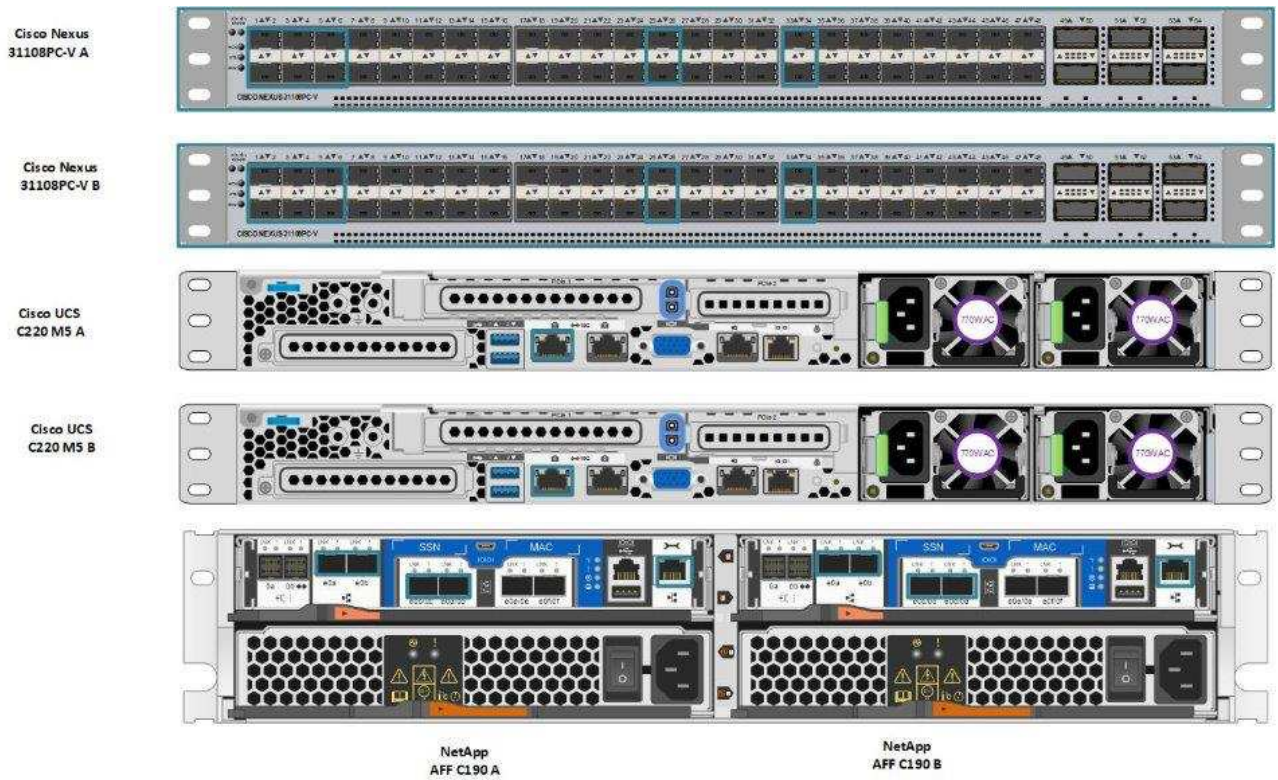
En esta tabla, se enumera el software necesario para todas las implementaciones de VMware vSphere en FlexPod Express.

De NetApp	Versión
Dispositivo VMware vCenter Server	6.7U2
Hipervisor ESXi de VMware vSphere	6.7U2
Complemento VAAI de NetApp para ESXi	1.1.2
VSC de NetApp	9.6

Información sobre el cableado exprés de FlexPod

Esta validación de referencia se cablea como se muestra en las siguientes figuras y tablas.

En esta figura, se muestra el cableado de validación de referencia.



En la siguiente tabla se muestra la información de cableado del switch Cisco Nexus 31108PC-V-A.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Switch Cisco Nexus 31108PC-V A	Eth1/1	La controladora De almacenamiento C190 de AFF de NetApp	e0c
	Eth1/2	Controladora de almacenamiento AFF C190 de NetApp B.	e0c
	Eth1/3	El servidor A independiente Cisco UCS C220 C-Series	MLOM0
	Eth1/4	Servidor B independiente Cisco UCS C220 C-Series	MLOM0
	Eth1/5	El servidor A independiente Cisco UCS C220 C-Series	MLOM1
	Eth1/6	Servidor B independiente Cisco UCS C220 C-Series	MLOM1
	Eth1/25	Switch Cisco Nexus 31108PC-V B	Eth1/25
	Eth1/26	Switch Cisco Nexus 31108PC-V B	Eth1/26
	Eth1/33	La controladora De almacenamiento C190 de AFF de NetApp	E0M
	Eth1/34	El servidor A independiente Cisco UCS C220 C-Series	CIMC (FEX135/1/25)

Esta tabla enumera la información de cableado del switch Cisco Nexus 31108PC-V- B.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Switch Cisco Nexus 31108PC-V B	Eth1/1	La controladora De almacenamiento C190 de AFF de NetApp	e0d
	Eth1/2	Controladora de almacenamiento AFF C190 de NetApp B.	e0d
	Eth1/3	El servidor A independiente Cisco UCS C220 C-Series	MLOM2
	Eth1/4	Servidor B independiente Cisco UCS C220 C-Series	MLOM2
	Eth1/5	El servidor A independiente Cisco UCS C220 C-Series	MLOM3
	Eth1/6	Servidor B independiente Cisco UCS C220 C-Series	MLOM3
	Eth1/25	Switch Cisco Nexus 31108 a	Eth1/25
	Eth1/26	Switch Cisco Nexus 31108 a	Eth1/26
	Eth1/33	Controladora de almacenamiento AFF C190 de NetApp B.	E0M
	Eth1/34	Servidor B independiente Cisco UCS C220 C-Series	CIMC (FEX135/1/26)

Esta tabla enumera la información de cableado de la controladora de almacenamiento AFF C190 de NetApp

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
La controladora De almacenamiento C190 de AFF de NetApp	e0a	Controladora de almacenamiento AFF C190 de NetApp B.	e0a
	e0b	Controladora de almacenamiento AFF C190 de NetApp B.	e0b
	e0c	Switch Cisco Nexus 31108PC-V A	Eth1/1
	e0d	Switch Cisco Nexus 31108PC-V B	Eth1/1
	E0M	Switch Cisco Nexus 31108PC-V A	Eth1/33

Esta tabla enumera la información de cableado de la controladora de almacenamiento AFF C190 de NetApp B.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Controladora de almacenamiento AFF C190 de NetApp B.	e0a	La controladora De almacenamiento C190 de AFF de NetApp	e0a
	e0b	La controladora De almacenamiento C190 de AFF de NetApp	e0b
	e0c	Switch Cisco Nexus 31108PC-V A	Eth1/2
	e0d	Switch Cisco Nexus 31108PC-V B	Eth1/2
	E0M	Switch Cisco Nexus 31108PC-V B	Eth1/33

Procedimientos de implantación

Descripción general

Este documento proporciona detalles para configurar un sistema FlexPod Express completamente redundante y de alta disponibilidad. Para reflejar esta redundancia, los componentes que se configuran en cada paso se denominan componente A o componente B. Por ejemplo, la controladora A y la controladora B identifican las dos controladoras de almacenamiento de NetApp que se aprovisionan en este documento. El switch A y el switch B identifican un par de switches Cisco Nexus.

Además, en este documento se describen los pasos para aprovisionar varios hosts de Cisco UCS, que se identifican secuencialmente como servidor A, servidor B, etc.

Para indicar que debe incluir la información pertinente a su entorno en un paso, `<<text>>` aparece como parte de la estructura de comandos. Consulte el siguiente ejemplo de `vlan create` comando:

```
Controller01> network port vlan create –node <<var_nodeA>> -vlan-name
<<var_vlan-name>>
```

Este documento permite configurar completamente el entorno de FlexPod Express. En este proceso, varios pasos requieren que inserte convenciones de nomenclatura específicas del cliente, direcciones IP y esquemas de red de área local virtual (VLAN). En la siguiente tabla se describen las VLAN necesarias para la implementación, tal y como se describe en esta guía. Esta tabla se puede completar en función de las variables específicas del sitio y se puede utilizar para implementar los pasos de configuración del documento.

Si se utilizan VLAN de gestión fuera de banda y en banda independientes, debe crear una ruta de capa- 3 entre ellas. Para esta validación, se utilizó una VLAN de gestión común.

Nombre de la VLAN	Propósito de VLAN	ID DE VLAN	
VLAN de gestión	VLAN para interfaces de gestión	3437	VSwitch0
VLAN NFS	VLAN para tráfico NFS	3438	VSwitch0
VLAN de VMware vMotion	VLAN designada para mover máquinas virtuales (VM) de un host físico a otro	3441	VSwitch0
VLAN de tráfico de la máquina virtual	VLAN para tráfico de aplicaciones de equipos virtuales	3442	VSwitch0
ISCSI-A-VLAN	VLAN para tráfico iSCSI en la estructura A	3439	IScsiBootvSwitch
ISCSI-B-VLAN	VLAN para tráfico iSCSI en la estructura B	3440	IScsiBootvSwitch
VLAN nativa	VLAN a la que se asignan tramas no etiquetadas	2	

Los números VLAN son necesarios en toda la configuración de FlexPod Express. Las VLAN se denominan `<<var_xxxx_vlan>>`, donde `xxxx` Es la finalidad de la VLAN (como iSCSI-A).

En esta validación se han creado dos vSwitch.

En la siguiente tabla se enumeran los vSwitch de la solución.

Nombre de vSwitch	Adaptadores activos	Puertos	MTU	Balanceo de carga
VSwitch0	Vmnic2, vmnic4	predeterminado (120)	9000	Ruta basada en hash IP
IScsiBootvSwitch	Vmnic3, vmnic5	predeterminado (120)	9000	Ruta basada en el identificador de puerto virtual de origen.

El método hash IP del equilibrio de carga requiere la configuración adecuada para el conmutador físico subyacente mediante SRC-DST-IP EtherChannel con un puerto-canal estático (modo activado). En caso de que se produzca una conectividad intermitente debido a una posible configuración incorrecta del switch, cierre temporalmente uno de los dos puertos de enlace ascendente asociados en el switch de Cisco para restaurar la comunicación con el puerto vmkernel de gestión de ESXi mientras se solucionan los problemas de la configuración del canal de puertos.

La siguiente tabla enumera las máquinas virtuales de VMware que se crean.

Descripción de la máquina virtual	Nombre de host
Servidor VMware vCenter	FlexPod-VCSA

Descripción de la máquina virtual	Nombre de host
Consola de almacenamiento virtual	FlexPod VSC

Ponga en marcha Cisco Nexus 31108PC-V

En esta sección se detalla la configuración del switch Cisco Nexus 331108PC-V utilizada en un entorno FlexPod Express.

Configuración inicial del switch Cisco Nexus 31108PC-V.

Los siguientes procedimientos describen cómo configurar los switches Cisco Nexus para su uso en un entorno FlexPod Express básico.

> En este procedimiento se asume que está utilizando un Cisco Nexus 31108PC-V con el software NX-OS versión 7.0(3)I7(6).

1. Tras el arranque y la conexión iniciales al puerto de la consola del switch, se inicia automáticamente la configuración de Cisco NX-OS. Esta configuración inicial trata los valores básicos, como el nombre del switch, la configuración de la interfaz mgmt0 y la configuración de Secure Shell (SSH).
2. La red de gestión del sistema FlexPod Express se puede configurar de varias maneras. Las interfaces mgmt0 de los conmutadores 31108PC-V se pueden conectar a una red de administración existente, o bien las interfaces mgmt0 de los conmutadores 31108PC-V se pueden conectar en una configuración posterior. Sin embargo, este enlace no se puede utilizar para el acceso de gestión externo, como tráfico SSH.

   > En esta guía de puesta en marcha, los switches Cisco Nexus 31108PC-V de FlexPod Express están conectados a una red de gestión existente.

3. Para configurar los switches Cisco Nexus 31108PC-V, encienda el switch y siga las indicaciones que aparecen en pantalla, como se muestra aquí para la configuración inicial de ambos switches, sustituyendo los valores adecuados para la información específica del conmutador.

```
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. A continuación, verá un resumen de la configuración y se le preguntará si desea editarla. Si la configuración es correcta, introduzca `n`.

```
Would you like to edit the configuration? (y
es/no) [n]: n
```

5. A continuación, se le preguntará si desea utilizar esta configuración y guardarla. Si es así, introduzca `y`.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Repita este procedimiento para el switch Cisco Nexus B.

Habilite las funciones avanzadas

Determinadas características avanzadas deben estar habilitadas en Cisco NX-OS para proporcionar opciones de configuración adicionales. Para activar las funciones adecuadas en los switches a y B de Cisco Nexus, entre en el modo de configuración mediante el comando (config t) y ejecute los siguientes comandos:

```
feature interface-vlan
feature lacp
feature vpc
```

> El hash de equilibrio de carga del canal de puerto predeterminado utiliza las direcciones IP de origen y destino para determinar el algoritmo de equilibrio de carga en las interfaces del canal de puerto. Puede lograr una mejor distribución entre los miembros del canal de puerto proporcionando más entradas al algoritmo hash más allá de las direcciones IP de origen y destino. Por el mismo motivo, NetApp recomienda encarecidamente añadir los puertos TCP de origen y destino al algoritmo hash.

En el modo de configuración (config t), introduzca los siguientes comandos para establecer la configuración global del equilibrio de carga del canal de puertos en el switch A y el switch B de Cisco Nexus:

```
port-channel load-balance src-dst ip-l4port
```

Configurar árbol de expansión global

La plataforma Cisco Nexus utiliza una nueva función de protección llamada garantía de puente. La garantía de puente ayuda a proteger contra un enlace unidireccional u otro error de software con un dispositivo que continúa redirectando el tráfico de datos cuando ya no ejecuta el algoritmo de árbol expansivo. Los puertos se pueden colocar en uno de varios estados, incluyendo la red o el borde, dependiendo de la plataforma.

NetApp recomienda establecer la garantía de puente para que todos los puertos se consideren puertos de red de forma predeterminada. Este ajuste obliga al administrador de red a revisar la configuración de cada puerto. También revela los errores de configuración más comunes, como puertos de borde no identificados o un vecino que no tiene activada la función de garantía de puente. Además, es más seguro tener el bloque de árbol expansivo muchos puertos en lugar de muy pocos, lo que permite que el estado de puerto predeterminado mejore la estabilidad general de la red.

Preste especial atención al estado de árbol de expansión al agregar servidores, almacenamiento y switches ascendentes, especialmente si no admiten la garantía de puente. En estos casos, es posible que deba cambiar el tipo de puerto para que los puertos estén activos.

El protector de unidad de datos de protocolo puente (BPDU) está habilitado de forma predeterminada en puertos periféricos como otra capa de protección. Para evitar bucles en la red, esta característica cierra el puerto si se ven BPDU de otro switch en esta interfaz.

En el modo de configuración (config t), ejecute los siguientes comandos para configurar las opciones predeterminadas de árbol de expansión, incluidos el tipo de puerto predeterminado y el protector BPDU, en el conmutador A Cisco Nexus y el conmutador B:

```
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
```

Defina las VLAN

Antes de configurar puertos individuales con VLAN diferentes, se deben definir las VLAN de capa 2 en el switch. También se recomienda nombrar las VLAN para que la solución de problemas sea sencilla en el futuro.

En el modo de configuración (config t), ejecute los siguientes comandos para definir y describir las VLAN de capa 2 en el switch A de Cisco Nexus y el switch B:

```
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
```

Configurar el acceso y las descripciones de los puertos de gestión

Como es el caso con la asignación de nombres a las VLAN de capa 2, las descripciones de configuración de todas las interfaces pueden ayudar tanto al aprovisionamiento como a la resolución de problemas.

Desde el modo de configuración (config t) de cada uno de los switches, introduzca las siguientes descripciones de puertos para la configuración grande de FlexPod Express:

Switch Cisco Nexus 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
```

Switch Cisco Nexus 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
```

Configurar las interfaces de gestión de almacenamiento y servidores

Las interfaces de gestión para el servidor y el almacenamiento suelen utilizar una sola VLAN. Por lo tanto, configure los puertos de la interfaz de gestión como puertos de acceso. Defina la VLAN de administración para cada switch y cambie el tipo de puerto de árbol expansivo a EDGE.

En el modo de configuración (config t), introduzca los siguientes comandos para configurar los ajustes del puerto para las interfaces de gestión tanto de los servidores como del almacenamiento:

Switch Cisco Nexus a

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Switch Cisco Nexus B

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Realizar la configuración global del canal de puerto virtual

Un canal de puerto virtual (VPC) permite que los enlaces que están conectados físicamente a dos switches de Cisco Nexus diferentes aparezcan como un único canal de puerto a un tercer dispositivo. El tercer dispositivo puede ser un conmutador, un servidor o cualquier otro dispositivo de red. Un VPC puede proporcionar una multivía de nivel 2, que le permite crear redundancia aumentando el ancho de banda, habilitando varias rutas paralelas entre los nodos y el tráfico de equilibrio de carga donde haya rutas alternativas.

Un VPC proporciona las siguientes ventajas:

- Permitir que un único dispositivo utilice un canal de puerto a través de dos dispositivos de subida
- Eliminar puertos bloqueados con protocolo de árbol expansivo
- Proporciona una topología sin bucles
- Utilizando todo el ancho de banda disponible de enlace ascendente
- Proporcionar convergencia rápida si el enlace o un dispositivo falla
- Resiliencia a nivel de enlace
- Contribuir a proporcionar una alta disponibilidad

La función VPC requiere alguna configuración inicial entre los dos switches de Cisco Nexus para que funcionen correctamente. Si utiliza la configuración de Mgmt0 de fondo a fondo, utilice las direcciones

definidas en las interfaces y compruebe que se pueden comunicar mediante el `ping <<switch_A/B_mgmt0_ip_addr>>vrf` comando de gestión.

En el modo de configuración (config t), ejecute los siguientes comandos para configurar la configuración global de VPC para ambos switches:

Switch Cisco Nexus 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
```

Switch Cisco Nexus 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
```

Configure los canales del puerto de almacenamiento

Las controladoras de almacenamiento de NetApp permiten una conexión activa-activa a la red mediante el protocolo de control de agregación de enlaces (LACP). El uso de LACP es preferido porque añade negociación y registro entre los switches. Debido a que la red está configurada para VPC, este enfoque permite disponer de conexiones activo-activo del almacenamiento para separar los switches físicos. Cada controladora tiene dos enlaces a cada uno de los switches. Sin embargo, los cuatro enlaces forman parte del mismo VPC y grupo de interfaces (ifgrp).

En el modo de configuración (config t), ejecute los siguientes comandos en cada uno de los switches para configurar las interfaces individuales y la configuración de canal de puerto resultante para los puertos conectados a la controladora AFF de NetApp.

1. Ejecute los siguientes comandos en el switch A y en el switch B a para configurar los canales de puertos de la controladora De almacenamiento A:

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. Ejecute los siguientes comandos en el switch A y en el switch B a para configurar los canales de puertos de la controladora de almacenamiento B:

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```

Configure las conexiones del servidor

Los servidores Cisco UCS tienen una tarjeta de interfaz virtual de cuatro puertos, VIC1457, que se utiliza para el tráfico de datos y el arranque del sistema operativo ESXi mediante iSCSI. Estas interfaces se configuran para que se conmutan al nodo de respaldo entre sí, lo que proporciona redundancia adicional más allá de un solo enlace. Al distribuir estos enlaces a través de varios switches, el servidor puede sobrevivir incluso a un fallo completo del switch.

Desde el modo de configuración (config t), ejecute los siguientes comandos para configurar los ajustes de puerto para las interfaces conectadas a cada servidor.

Switch Cisco Nexus A: Configuración de Cisco UCS Server-A y Cisco UCS Server-B.

```
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 Switch B: Configuración de Cisco UCS Server-A y Cisco UCS Server-B.

```
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
```

Configure los canales del puerto del servidor

Ejecute los siguientes comandos en el switch A y el switch B para configurar los canales de puertos para el servidor A:

```
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
```

Ejecute los siguientes comandos en el switch A y el switch B para configurar los canales de puerto para el servidor B:

```
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
```

Se utilizó una MTU de 9000 en esta validación de solución. Sin embargo, puede configurar un valor diferente para el MTU apropiado para los requisitos de sus aplicaciones. Es importante establecer el mismo valor de MTU en la solución de FlexPod. Una configuración de MTU incorrecta entre componentes provoca que se descartan los paquetes y estos paquetes deberán transmitirse de nuevo, lo que afecta al rendimiento general de la solución.

Para escalar la solución añadiendo servidores Cisco UCS adicionales, ejecute los comandos anteriores con los puertos del switch a los que se han conectado los servidores recién añadidos en los switches A y B.

Enlace ascendente a una infraestructura de red existente

En función de la infraestructura de red disponible, se pueden utilizar varios métodos y funciones para elevar el entorno FlexPod. Si existe un entorno Cisco Nexus existente, NetApp recomienda utilizar PCs para elevar los

switches Cisco Nexus 31108 incluidos en el entorno FlexPod a la infraestructura. Los enlaces ascendentes pueden ser enlaces de subida de 10 GbE para una solución de infraestructura de 10 GbE o 1 GbE para una solución de infraestructura de 1 GbE si fuera necesario. Los procedimientos descritos anteriormente se pueden utilizar para crear un VPC de enlace ascendente al entorno existente. Asegúrese de ejecutar Copy START para guardar la configuración en cada switch una vez completada la configuración.

"Siguiente: Procedimiento de implementación del almacenamiento de NetApp (parte 1)."

Procedimiento de instalación de almacenamiento NetApp (parte 1)

En esta sección se describe el procedimiento de implementación del almacenamiento AFF de NetApp.

Instalación de la controladora de almacenamiento de NetApp C190 Series de AFF

Hardware Universe de NetApp

La aplicación NetApp Hardware Universe (HWU) proporciona componentes de hardware y software compatibles con cualquier versión específica de ONTAP. Proporciona información de configuración para todos los dispositivos de almacenamiento de NetApp compatibles actualmente con el software ONTAP. También se proporciona una tabla de compatibilidades de componentes.

Confirme que los componentes de hardware y software que desea utilizar son compatibles con la versión de ONTAP que tiene previsto instalar:

Acceda a "HWU" aplicación para ver las guías de configuración del sistema. Haga clic en la pestaña controladoras para ver la compatibilidad entre distintas versiones del software ONTAP y los dispositivos de almacenamiento de NetApp con las especificaciones que desea.

Como alternativa, para comparar componentes por dispositivo de almacenamiento, haga clic en Comparar sistemas de almacenamiento.

Requisitos previos de la controladora AFF serie 190
Para planificar la ubicación física de los sistemas de almacenamiento, consulte Hardware Universe de NetApp. Consulte las siguientes secciones: • Requisitos eléctricos • Cables de alimentación compatibles • Puertos y cables integrados

Controladoras de almacenamiento

Siga los procedimientos de instalación física de las controladoras en AFF "C190" Documentación.

ONTAP 9.6 de NetApp

Hoja de datos de configuración

Antes de ejecutar la secuencia de comandos de instalación, rellene la hoja de datos de configuración del manual del producto. La hoja de datos de configuración está disponible en la Guía de configuración de software de ONTAP 9.6.

Este sistema se establece en una configuración de clúster de dos nodos sin switch.

La siguiente tabla contiene información sobre la instalación y la configuración de ONTAP 9.6.

Detalles del clúster	Valor de detalles de clúster
Nodo del clúster: Dirección IP	<<var_nodeA_mgmt_ip>>
Máscara de red Del nodo a del clúster	<<var_nodeA_mgmt_mask>>
Nodo del clúster: Puerta de enlace	<<var_nodeA_mgmt_gateway>>
Nombre del nodo a del clúster	<<var_nodeA>>
Dirección IP del nodo B del clúster	<<var_nodeB_mgmt_ip>>
Máscara de red del nodo B del clúster	<<var_nodeB_mgmt_mask>>
Puerta de enlace del nodo B del clúster	<<var_nodeB_mgmt_gateway>>
Nombre del nodo B del clúster	<<var_nodeB>>
Dirección URL de ONTAP 9.6	<<var_url_boot_software>>
El nombre del clúster	<<var_clustername>>
Dirección IP de gestión del clúster	<<var_clustermgmt_ip>>
Puerta de enlace del clúster B.	<<var_clustermgmt_gateway>>
Máscara de red del clúster B.	<<var_clustermgmt_mask>>
Nombre de dominio	<<var_domain_name>>
IP del servidor DNS (puede introducir más de uno)	<var_dns_server_ip
La IP del servidor NTP (es posible introducir más de uno)	<<var_ntp_server_ip>>

Configure el nodo a

Para configurar el nodo A, complete los siguientes pasos:

1. Conéctese al puerto de la consola del sistema de almacenamiento. Tiene que ver un cargador-a del símbolo del sistema. Sin embargo, si el sistema de almacenamiento está en un bucle de reinicio, pulse Ctrl-C para salir del bucle de autoarranque cuando vea este mensaje:

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

   Permita que el sistema arranque.

   ```
   autoboot
   ```

2. Pulse Ctrl-C para acceder al menú Inicio.

Si ONTAP 9.6 no es la versión del software que se está arrancando, continúe con los pasos siguientes para instalar el software nuevo. Si ONTAP 9.6 es la versión que se va a arrancar, seleccione la opción 8 e y para reiniciar el nodo. A continuación, continúe con el paso 14.

3. Para instalar software nuevo, seleccione la opción 7.
4. Introduzca y para realizar una actualización.
5. Seleccione e0M para el puerto de red que desee usar para la descarga.
6. Introduzca y para reiniciar ahora.
7. Introduzca la dirección IP, la máscara de red y la puerta de enlace predeterminada para e0M en sus respectivos lugares.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

8. Especifique la dirección URL donde se puede encontrar el software.

Este servidor web debe ser pingable.

```
<<var_url_boot_software>>
```

9. Pulse Intro para el nombre de usuario, indicando que no hay nombre de usuario.
10. Introduzca y para establecer el software recién instalado como valor predeterminado que se utilizará para los siguientes reinicios.
11. Introduzca y para reiniciar el nodo.

Al instalar el software nuevo, el sistema podría realizar actualizaciones de firmware en el BIOS y las tarjetas adaptadoras, lo que provoca reinicios y posibles interrupciones en el cargador. Si se producen estas acciones, el sistema podría desviarse de este procedimiento.

12. Pulse Ctrl-C para acceder al menú Inicio.
13. Seleccione la opción 4 para Configuración limpia y inicializar todos los discos.
14. Introduzca y para poner a cero discos, restablezca la configuración e instale un nuevo sistema de archivos.
15. Introduzca y para borrar todos los datos de los discos.

La inicialización y creación del agregado raíz puede tardar 90 minutos o más en completarse, según el número y el tipo de discos conectados. Una vez finalizada la inicialización, el sistema de almacenamiento se reinicia. Tenga en cuenta que los SSD tardan mucho menos tiempo en inicializarse. Puede continuar con la configuración del nodo B mientras los discos del nodo A se están poniendo a cero.

Mientras el nodo A se está inicializando, empiece a configurar el nodo B.

Configure el nodo B

Para configurar el nodo B, complete los siguientes pasos:

1. Conéctese al puerto de la consola del sistema de almacenamiento. Tiene que ver un cargador-a del símbolo del sistema. Sin embargo, si el sistema de almacenamiento está en un bucle de reinicio, pulse Ctrl-C para salir del bucle de autoarranque cuando vea este mensaje:

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

2. Pulse Ctrl-C para acceder al menú Inicio.

   ```
   autoboot
   ```

3. Pulse Ctrl-C cuando se le solicite.

   > Si ONTAP 9.6 no es la versión del software que se está arrancando, continúe con los pasos siguientes para instalar el software nuevo. Si ONTAP 9.6 es la versión que se va a arrancar, seleccione la opción 8 e y para reiniciar el nodo. A continuación, continúe con el paso 14.

4. Para instalar software nuevo, seleccione la opción 7.A.
5. Introduzca y para realizar una actualización.
6. Seleccione e0M para el puerto de red que desee usar para la descarga.
7. Introduzca y para reiniciar ahora.
8. Introduzca la dirección IP, la máscara de red y la puerta de enlace predeterminada para e0M en sus respectivos lugares.

   ```
   <<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
   ```

9. Especifique la dirección URL donde se puede encontrar el software.

   > Este servidor web debe ser pingable.

   ```
   <<var_url_boot_software>>
   ```

10. Pulse Intro para el nombre de usuario, indicando que no hay nombre de usuario.
11. Introduzca y para establecer el software recién instalado como valor predeterminado que se utilizará para los siguientes reinicios.
12. Introduzca y para reiniciar el nodo.

Al instalar el software nuevo, el sistema podría realizar actualizaciones de firmware en el BIOS y las tarjetas adaptadoras, lo que provoca reinicios y posibles interrupciones en el cargador. Si se producen estas acciones, el sistema podría desviarse de este procedimiento.

13. Pulse Ctrl-C para acceder al menú Inicio.
14. Seleccione la opción 4 para Configuración limpia y inicializar todos los discos.
15. Introduzca y para poner a cero discos, restablezca la configuración e instale un nuevo sistema de archivos.
16. Introduzca y para borrar todos los datos de los discos.

La inicialización y creación del agregado raíz puede tardar 90 minutos o más en completarse, según el número y el tipo de discos conectados. Una vez finalizada la inicialización, el sistema de almacenamiento se reinicia. Tenga en cuenta que los SSD tardan mucho menos tiempo en inicializarse.

Continuación de la configuración del nodo a y de la configuración del clúster

Desde un programa de puertos de consola conectado al puerto de la consola De la controladora De almacenamiento A (nodo A), ejecute el script de configuración del nodo. Este script se muestra cuando ONTAP 9.6 arranca en el nodo por primera vez.

El procedimiento de configuración del nodo y de los clústeres ha cambiado ligeramente en ONTAP 9.6. El asistente de configuración de clúster se utiliza ahora para configurar el primer nodo de un clúster y el Administrador del sistema ONTAP de NetApp (anteriormente, OnCommand® System Manager) se utiliza para configurar el clúster.

1. Siga las instrucciones para configurar el nodo 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. Vaya a la dirección IP de la interfaz de gestión del nodo.

> La configuración del clúster también se puede realizar mediante la CLI. Este documento describe la configuración del clúster mediante la configuración guiada de System Manager.

3. Haga clic en Guided Setup para configurar el clúster.
4. Introduzca `<<var_clustername>>` del nombre del clúster y. `<<var_nodeA>>` y.. `<<var_nodeB>>` para cada uno de los nodos que va a configurar. Introduzca la contraseña que desea usar para el sistema de almacenamiento. Seleccione Switchless Cluster para el tipo de clúster. Introduzca la licencia base del clúster.
5. También es posible introducir licencias de funciones para Cluster, NFS e iSCSI.
6. Ve un mensaje de estado que indica que el clúster se está creando. Este mensaje de estado cambia por varios Estados. Este proceso tarda varios minutos.
7. Configure la red.

a. Anule la selección de la opción intervalo de direcciones IP.

b. Introduzca `<<var_clustermgmt_ip>>` En el campo Cluster Management IP Address, `<<var_clustermgmt_mask>>` En el campo máscara de red, y. `<<var_clustermgmt_gateway>>` En el campo Puerta de enlace. Utilice el… Selector en el campo Port para seleccionar e0M del nodo A.

c. La IP de gestión de nodos para el nodo A ya se ha rellenado. Introduzca `<<var_nodeA_mgmt_ip>>` Para el nodo B.

d. Introduzca `<<var_domain_name>>` En el campo DNS Domain Name. Introduzca `<<var_dns_server_ip>>` En el campo DNS Server IP Address.

> Puede introducir varias direcciones IP del servidor DNS.

e. Introduzca `10.63.172.162` En el campo servidor NTP primario.

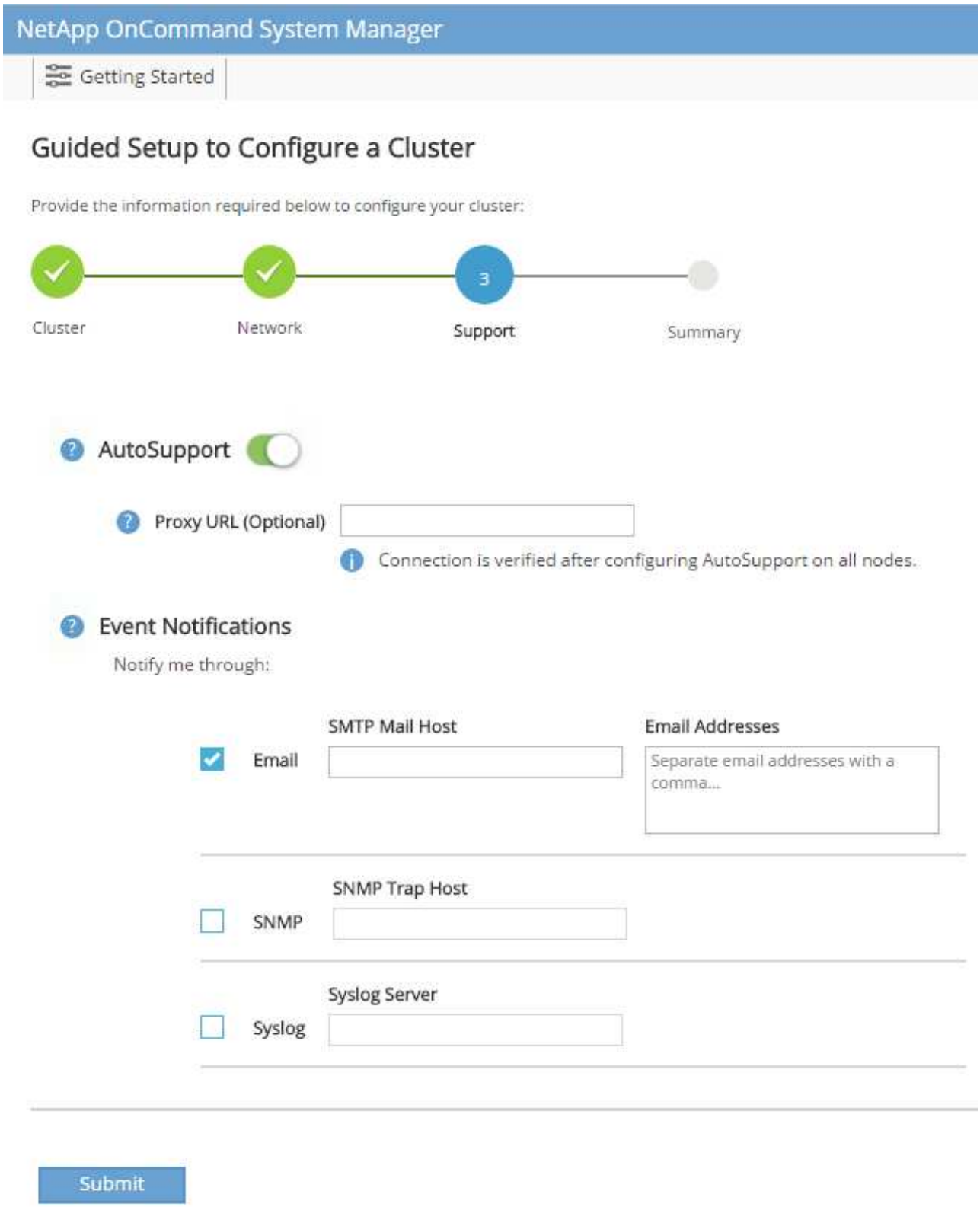
> También puede introducir un servidor NTP alternativo. La dirección IP `10.63.172.162` de `<<var_ntp_server_ip>>` Es el IP de gestión de Nexus.

8. Configure la información de soporte.

a. Si el entorno requiere un proxy para acceder a AutoSupport, introduzca la URL en Proxy URL.

b. Introduzca el host de correo SMTP y la dirección de correo electrónico para las notificaciones de eventos.

> Debe, como mínimo, configurar el método de notificación de eventos antes de continuar. Puede seleccionar cualquiera de los métodos.



Una vez que el sistema indica que ha finalizado la configuración del clúster, haga clic en Manage your Cluster para configurar el almacenamiento.

Continuación de la configuración del clúster de almacenamiento

Después de configurar los nodos de almacenamiento y el clúster base, puede continuar con la configuración del clúster de almacenamiento.

Ponga a cero todos los discos de repuesto

Para poner a cero todos los discos de repuesto del clúster, ejecute el siguiente comando:

```
disk zerospares
```

Configure la personalidad de los puertos UTA2 integrados

1. Compruebe el modo actual y el tipo actual de los puertos ejecutando el `ucadmin show` comando.

```
AFF C190::> ucadmin show
                      Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF C190_A     0c       cna       target     -        -          online
AFF C190_A     0d       cna       target     -        -          online
AFF C190_A     0e       cna       target     -        -          online
AFF C190_A     0f       cna       target     -        -          online
AFF C190_B     0c       cna       target     -        -          online
AFF C190_B     0d       cna       target     -        -          online
AFF C190_B     0e       cna       target     -        -          online
AFF C190_B     0f       cna       target     -        -          online
8 entries were displayed.
```

2. Compruebe que el modo actual de los puertos que se están utilizando es cna y que el tipo actual está establecido como objetivo. De lo contrario, cambie la personalidad de puerto mediante el siguiente comando:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

> Los puertos deben estar desconectados para que se ejecute el comando anterior. Para desconectar un puerto, ejecute el siguiente comando:

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

Si ha cambiado la personalidad del puerto, debe reiniciar cada nodo para que el cambio se aplique.

Cambie el nombre de las interfaces lógicas de gestión

Para cambiar el nombre de las interfaces lógicas de gestión (LIF), realice los pasos siguientes:

1. Muestra los nombres de las LIF de gestión actuales.

```
network interface show -vserver <<clustername>>
```

2. Cambie el nombre de la LIF de gestión del clúster.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_cluster_mgmt_lif_1 -newname cluster_mgmt
```

3. Cambie el nombre del LIF de gestión del nodo B.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF C190_B_1 -newname AFF C190-02_mgmt1
```

Configure la reversión automática en la gestión del clúster

Configure el parámetro de reversión automática en la interfaz de gestión del clúster.

```
network interface modify -vserver <<clustername>> -lif cluster_mgmt -auto-
revert true
```

Configure la interfaz de red del procesador de servicios

Para asignar una dirección IPv4 estática al procesador de servicios en cada nodo, ejecute los siguientes comandos:

```
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>>
```

Las direcciones IP de Service Processor deben estar en la misma subred que las direcciones IP de gestión de nodos.

Activar la recuperación tras fallos de almacenamiento en ONTAP

Para confirmar que la conmutación por error del almacenamiento está habilitada, ejecute los siguientes comandos de una pareja de conmutación por error:

1. Comprobar el estado de recuperación tras fallos del almacenamiento.

```
storage failover show
```

> Ambas <<var_nodeA>> y.. <<var_nodeB>> debe poder realizar una toma de control. Vaya al paso 3 si los nodos pueden realizar una toma de control.

2. Habilite la conmutación al nodo de respaldo en uno de los dos nodos.

```
storage failover modify -node <<var_nodeA>> -enabled true
```

> Habilitar la conmutación al nodo de respaldo en un solo nodo permite que se produzca en ambos nodos.

3. Compruebe el estado de alta disponibilidad del clúster de dos nodos.

> Este paso no es aplicable para clústeres con más de dos nodos.

```
cluster ha show
```

4. Vaya al paso 6 si está configurada la alta disponibilidad. Si se ha configurado la alta disponibilidad, verá el siguiente mensaje al emitir el comando:

```
High Availability Configured: true
```

5. Habilite el modo de alta disponibilidad solo para el clúster de dos nodos.

> No ejecute este comando para clústeres con más de dos nodos debido a que provoca problemas con la conmutación al nodo de respaldo.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. Compruebe que la asistencia de hardware está correctamente configurada y, si es necesario, modifique la dirección IP del partner.

```
storage failover hwassist show
```

El mensaje `Keep Alive Status: Error:` indica que una de las controladoras no recibió alertas de hwassist keep alive de su compañero, lo que indica que la asistencia de hardware no está configurada. Ejecute los siguientes comandos para configurar hardware Assist.

```
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>>
```

Cree un dominio de retransmisión MTU de trama gigante en ONTAP

Para crear un dominio de retransmisión de datos con un valor MTU de 9000, ejecute los siguientes comandos:

```
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
```

Quite los puertos de datos del dominio de retransmisión predeterminado

Los puertos de datos de 10 GbE se utilizan para el tráfico iSCSI/NFS y estos puertos deben eliminarse del dominio predeterminado. Los puertos e0e y e0f no se utilizan y deben eliminarse del dominio predeterminado.

Para quitar puertos del dominio de retransmisión, ejecute el siguiente comando:

```
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
```

Deshabilite el control de flujo en los puertos UTA2

Se recomienda utilizar las mejores prácticas de NetApp para deshabilitar el control de flujo en todos los puertos UTA2 conectados a dispositivos externos. Para desactivar el control de flujo, ejecute el siguiente comando:

```
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
```

Configure el grupo de interfaces LACP en ONTAP

Este tipo de grupo de interfaces requiere dos o más interfaces Ethernet y un switch compatible con LACP. asegúrese de que está configurado según los pasos de esta guía en la sección 5.1.

Desde el símbolo del sistema del clúster, complete los siguientes pasos:

```
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
```

Configure las tramas gigantes en ONTAP

Para configurar un puerto de red ONTAP para que utilice tramas gigantes (normalmente con una MTU de 9,000 bytes), ejecute los siguientes comandos desde el shell del clúster:

```
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
```

Crear VLAN en ONTAP

Para crear VLAN en ONTAP, complete los siguientes pasos:

1. Cree puertos VLAN NFS y añádalos al dominio de retransmisión de datos.

```
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. Cree puertos VLAN iSCSI y añádalos al dominio de retransmisión de datos.

```
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. Cree puertos MGMT-VLAN.

```
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>>
```

Crear agregados de datos en ONTAP

Durante el proceso de configuración de ONTAP, se crea un agregado que contiene el volumen raíz. Para crear agregados adicionales, determine el nombre del agregado, el nodo en el que se creará y el número de discos que contiene.

Para crear agregados, ejecute los siguientes comandos:

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

Conserve al menos un disco (seleccione el disco más grande) en la configuración como un repuesto. Una práctica recomendada es tener al menos un repuesto para cada tipo y tamaño de disco.

Empiece con cinco discos; puede añadir discos a un agregado cuando necesite almacenamiento adicional.

No se puede crear el agregado hasta que se complete el establecimiento en cero del disco. Ejecute el `aggr show` comando para mostrar el estado de creación del agregado. No continúe hasta que aggr1_NODEA esté en línea.

Configurar la zona horaria en ONTAP

Para configurar la sincronización horaria y establecer la zona horaria en el clúster, ejecute el siguiente comando:

```
timezone <<var_timezone>>
```

Por ejemplo, en el este de Estados Unidos, la zona horaria es América/Nueva York. Cuando haya comenzado a escribir el nombre de la zona horaria, pulse la tecla TAB para ver las opciones disponibles.

Configurar SNMP en ONTAP

Para configurar SNMP, realice los siguientes pasos:

1. Configure la información básica de SNMP, como la ubicación y el contacto. Cuando se sondean, esta información es visible como `sysLocation` y.. `sysContact` Variables en SNMP.

   ```
   snmp contact <<var_snmp_contact>>
   snmp location "<<var_snmp_location>>"
   snmp init 1
   options snmp.enable on
   ```

2. Configure las capturas SNMP para que se envíen a hosts remotos.

   ```
   snmp traphost add <<var_snmp_server_fqdn>>
   ```

Configure SNMPv1 en ONTAP

Para configurar SNMPv1, establezca la contraseña de texto sin formato secreta compartida denominada comunidad.

```
snmp community add ro <<var_snmp_community>>
```

Utilice la `snmp community delete all` comando con precaución. Si se utilizan cadenas de comunidad para otros productos de supervisión, este comando las quita.

Configure SNMPv3 en ONTAP

SNMPv3 requiere que defina y configure un usuario para la autenticación. Para configurar SNMPv3, lleve a cabo los siguientes pasos:

1. Ejecute el `security snmpusers` Comando para ver el ID del motor.
2. Cree un usuario llamado `snmpv3user`.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. Introduzca el ID de motor de la entidad autorizada y seleccione md5 como protocolo de autenticación.
4. Escriba una contraseña de longitud mínima de ocho caracteres para el protocolo de autenticación cuando se le solicite.
5. Seleccione des como protocolo de privacidad.
6. Escriba una contraseña de longitud mínima de ocho caracteres para el protocolo de privacidad cuando se le solicite.

Configure HTTPS de AutoSupport en ONTAP

La herramienta AutoSupport de NetApp envía información de resumen de soporte a NetApp mediante HTTPS. Para configurar AutoSupport, ejecute el siguiente comando:

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Cree una máquina virtual de almacenamiento

Para crear una máquina virtual de almacenamiento (SVM) de infraestructura, complete los siguientes pasos:

1. Ejecute el `vserver create` comando.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. Añada el agregado de datos a la lista de agregados de infra-SVM para VSC de NetApp.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. Elimine los protocolos de almacenamiento que no se utilicen de la SVM, con lo que dejará NFS e iSCSI.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. Habilite y ejecute el protocolo NFS en la SVM de infra-SVM.

```
nfs create -vserver Infra-SVM -udp disabled
```

5. Encienda la `SVM vstorage` Parámetro para el plugin VAAI para NFS de NetApp. A continuación, compruebe que NFS se ha configurado.

```
vserver nfs modify –vserver Infra-SVM –vstorage enabled
vserver nfs show
```

Los comandos están precedidos por `vserver` En la línea de comandos, debido a que las SVM se denominaban previamente vServers.

Configure NFSv3 en ONTAP

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Host ESXi dirección IP de NFS	<<var_esxi_hostA_nfs_ip>>
Dirección IP de NFS del host ESXi B	<<var_esxi_hostB_nfs_ip>>

Para configurar NFS en la SVM, ejecute los siguientes comandos:

1. Cree una regla para cada host ESXi en la política de exportación predeterminada.
2. Asigne una regla para cada host ESXi que se cree. Cada host tiene su propio índice de reglas. El primer host ESXi tiene el índice de regla 1, el segundo host ESXi tiene el índice de regla 2, etc.

```
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. Asigne la política de exportación al volumen raíz de la SVM de infraestructura.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

VSC de NetApp gestiona automáticamente las políticas de exportación si decide instalarlas después de configurar vSphere. Si no lo instala, debe crear reglas de políticas de exportación cuando se añadan servidores C-Series de Cisco UCS adicionales.

Cree el servicio iSCSI en ONTAP

Para crear el servicio iSCSI en la SVM, ejecute el comando siguiente. Este comando también inicia el servicio iSCSI y establece el IQN de iSCSI para la SVM. Comprobar que iSCSI se ha configurado.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Crear reflejo de uso compartido de carga del volumen raíz de la SVM en ONTAP

Para crear un reflejo de uso compartido de carga del volumen raíz de la SVM en ONTAP, complete los pasos siguientes:

1. Cree un volumen para que sea el reflejo de uso compartido de carga del volumen raíz de la SVM de infraestructura en cada nodo.

   ```
   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. Crear una programación de tareas para actualizar las relaciones de mirroring del volumen raíz cada 15 minutos.

   ```
   job schedule interval create -name 15min -minutes 15
   ```

3. Cree las relaciones de mirroring.

   ```
   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. Inicialice la relación de mirroring y compruebe que se haya creado.

   ```
   snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
   snapmirror show
   ```

Configure el acceso HTTPS en ONTAP

Para configurar el acceso seguro a la controladora de almacenamiento, lleve a cabo los siguientes pasos:

1. Aumente el nivel de privilegio para acceder a los comandos de certificado.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. En general, ya se encuentra en funcionamiento un certificado autofirmado. Verifique el certificado ejecutando el siguiente comando:

```
security certificate show
```

3. Para cada SVM que se muestra, el nombre común de certificado debe coincidir con el FQDN de DNS de la SVM. Los cuatro certificados predeterminados deben eliminarse y sustituirse por certificados autofirmados o certificados de una entidad de certificación.

> La práctica recomendada es eliminar certificados caducados antes de crear certificados. Ejecute el `security certificate delete` comando para eliminar certificados caducados. En el siguiente comando, use LA TABULACIÓN automática para seleccionar y eliminar cada certificado predeterminado.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. Para generar e instalar certificados autofirmados, ejecute los siguientes comandos como comandos de una sola vez. Generar un certificado de servidor para la SVM de infraestructura y la SVM de clúster. De nuevo, utilice LA TABULACIÓN automática como ayuda para completar estos comandos.

```
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. Para obtener los valores de los parámetros requeridos en el siguiente paso, ejecute el comando Security certificate show.
6. Habilite cada certificado que se acaba de crear mediante el `-server-enabled true` y.. `-client-enabled false` parámetros. De nuevo, utilice LA TABULACIÓN automática.

```
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. Configure y habilite el acceso SSL y HTTPS y deshabilite el acceso HTTP.

```
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>>
```

Es normal que algunos de estos comandos devuelvan un mensaje de error indicando que la entrada no existe.

8. Vuelva al nivel de privilegio de administrador y cree la configuración para permitir que la SVM esté disponible en la web.

```
set –privilege admin
vserver services web modify –name spi –vserver * -enabled true
```

Cree un volumen de FlexVol de NetApp en ONTAP

Para crear un volumen FlexVol® de NetApp, introduzca el nombre del volumen, el tamaño y el agregado en el que existe. Crear dos volúmenes de almacenes de datos de VMware y un volumen de arranque del servidor.

```
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
```

Crear LUN en ONTAP

Para crear dos LUN de arranque, ejecute los siguientes comandos:

```
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
```

Cuando se añade un servidor Cisco UCS C-Series adicional, debe crear una LUN de arranque adicional.

Creación de LIF iSCSI en ONTAP

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Nodo de almacenamiento a iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
Nodo de almacenamiento: Una máscara de red LIF01A de iSCSI	<<var_nodeA_iscsi_lif01a_mask>>
Nodo de almacenamiento a iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
Nodo de almacenamiento a máscara de red LIF01B de iSCSI	<<var_nodeA_iscsi_lif01b_mask>>
Nodo de almacenamiento B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
Máscara de red del nodo de almacenamiento B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_mask>>
ISCSI LIF01B del nodo de almacenamiento	<<var_nodeB_iscsi_lif01b_ip>>
Máscara de red LIF01B de nodo de almacenamiento B.	<<var_nodeB_iscsi_lif01b_mask>>

Creación de cuatro LIF iSCSI, dos en cada nodo.

```
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
```

Creación de LIF NFS en ONTAP

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Nodo de almacenamiento: LIF NFS 01 IP	<<var_nodeA_nfs_lif_01_ip>>
Nodo de almacenamiento máscara de red a LIF 01 de NFS	<<var_nodeA_nfs_lif_01_mask>>
Nodo de almacenamiento B LIF NFS 02 IP	<<var_nodeB_nfs_lif_02_ip>>
Máscara de red del nodo de almacenamiento B LIF NFS 02	<<var_nodeB_nfs_lif_02_mask>>

Cree una LIF NFS.

```
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
```

Añadir un administrador de SVM de infraestructura

En la siguiente tabla, se enumera la información necesaria para añadir un administrador de SVM.

Detalles	Valor de detalle
IP de Vsmgmt	<<var_svm_mgmt_ip>>
Máscara de red Vsmgmt	<<var_svm_mgmt_mask>>
Puerta de enlace predeterminada de Vsmgmt	<<var_svm_mgmt_gateway>>

Para añadir la interfaz lógica de administración de SVM y el administrador de SVM de la infraestructura a la red de gestión, realice los siguientes pasos:

1. Ejecute el siguiente comando:

```
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
```

> La IP de administración de SVM aquí debe estar en la misma subred que la IP de administración del clúster de almacenamiento.

2. Cree una ruta predeterminada para permitir que la interfaz de gestión de SVM llegue al mundo exterior.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. Establezca una contraseña para el usuario de SVM vsadmin y desbloquee el usuario.

```
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
```

"A continuación, ponga en marcha el servidor en rack C-Series de Cisco UCS."

Poner en marcha el servidor de montaje en rack Cisco UCS C-Series

En esta sección, se proporciona un procedimiento detallado para configurar un servidor de rack independiente Cisco UCS C-Series para su uso en la configuración exprés de FlexPod.

Realice la configuración inicial del servidor independiente Cisco UCS C-Series para CIMC

Complete estos pasos para la configuración inicial de la interfaz de CIMC para servidores independientes Cisco UCS C-Series.

En la siguiente tabla se enumera la información necesaria para configurar CIMC para cada servidor independiente Cisco UCS C-Series.

Detalles	Valor de detalle
Dirección IP de CIMC	<<cimc_ip>>
Máscara de subred CIMC	\<<cimc_netmask
Puerta de enlace predeterminada CIMC	<<cimc_gateway>>

La versión de CIMC utilizada en esta validación es CIMC 4.0.(4).

Todos los servidores

1. Conecte la mochila del teclado, vídeo y ratón (KVM) de Cisco (suministrada con el servidor) al puerto KVM de la parte frontal del servidor. Conecte un monitor VGA y un teclado USB a los puertos de mochila KVM adecuados.

   Encienda el servidor y pulse F8 cuando se le solicite que introduzca la configuración de CIMC.

2. En la utilidad de configuración de CIMC, defina las siguientes opciones:
   a. Modo de tarjeta de interfaz de red (NIC):

      Específico `[X]`

   b. IP (básico):

      IPV4: `[X]`

      DHCP habilitado: `[ ]`

      IP DE CIMC: `<<cimc_ip>>`

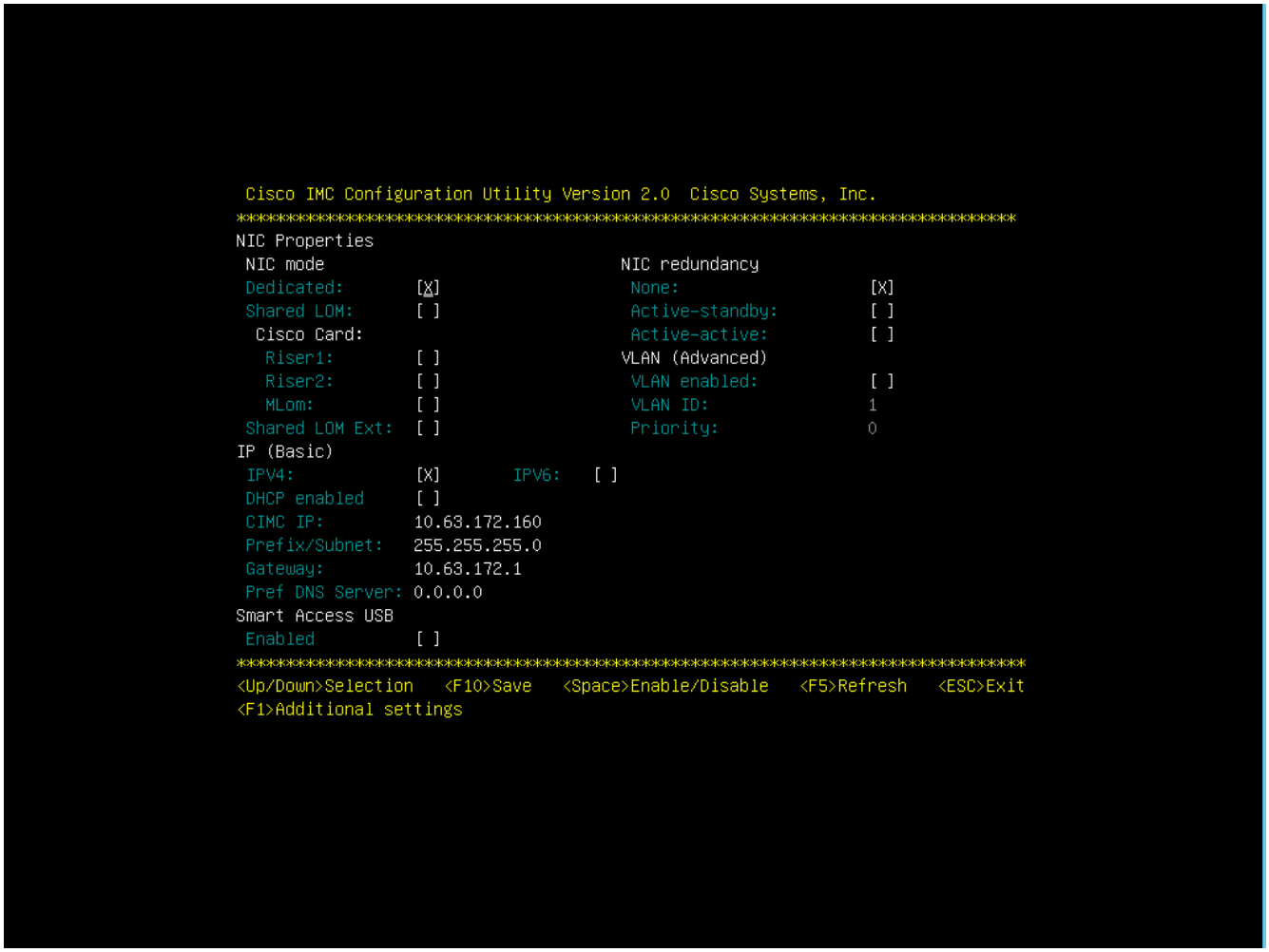
      Prefijo/subred: `<<cimc_netmask>>`

      Puerta de enlace: `<<cimc_gateway>>`

   c. VLAN (Advanced): Deje borrado para deshabilitar el etiquetado VLAN.

      Redundancia NIC

      Ninguna: `[X]`



3. Pulse F1 para ver los ajustes adicionales:
   a. Propiedades comunes:

      Nombre de host: `<<esxi_host_name>>`

      DNS dinámico: `[ ]`

      Valores predeterminados de fábrica: Dejar borrado.

   b. Usuario predeterminado (básico):

      Contraseña predeterminada: `<<admin_password>>`

      Vuelva a introducir la contraseña: `<<admin_password>>`

      Propiedades del puerto: Utilice los valores predeterminados.

   Perfiles de puerto: Dejar borrado.
4. Pulse F10 para guardar la configuración de la interfaz CIMC.
5. Una vez guardada la configuración, pulse Esc para salir.

Configurar arranque iSCSI de servidores Cisco UCS C-Series

En esta configuración de FlexPod Express, la VIC1457 se utiliza para el arranque iSCSI.

La tabla siguiente enumera la información necesaria para configurar el arranque iSCSI.

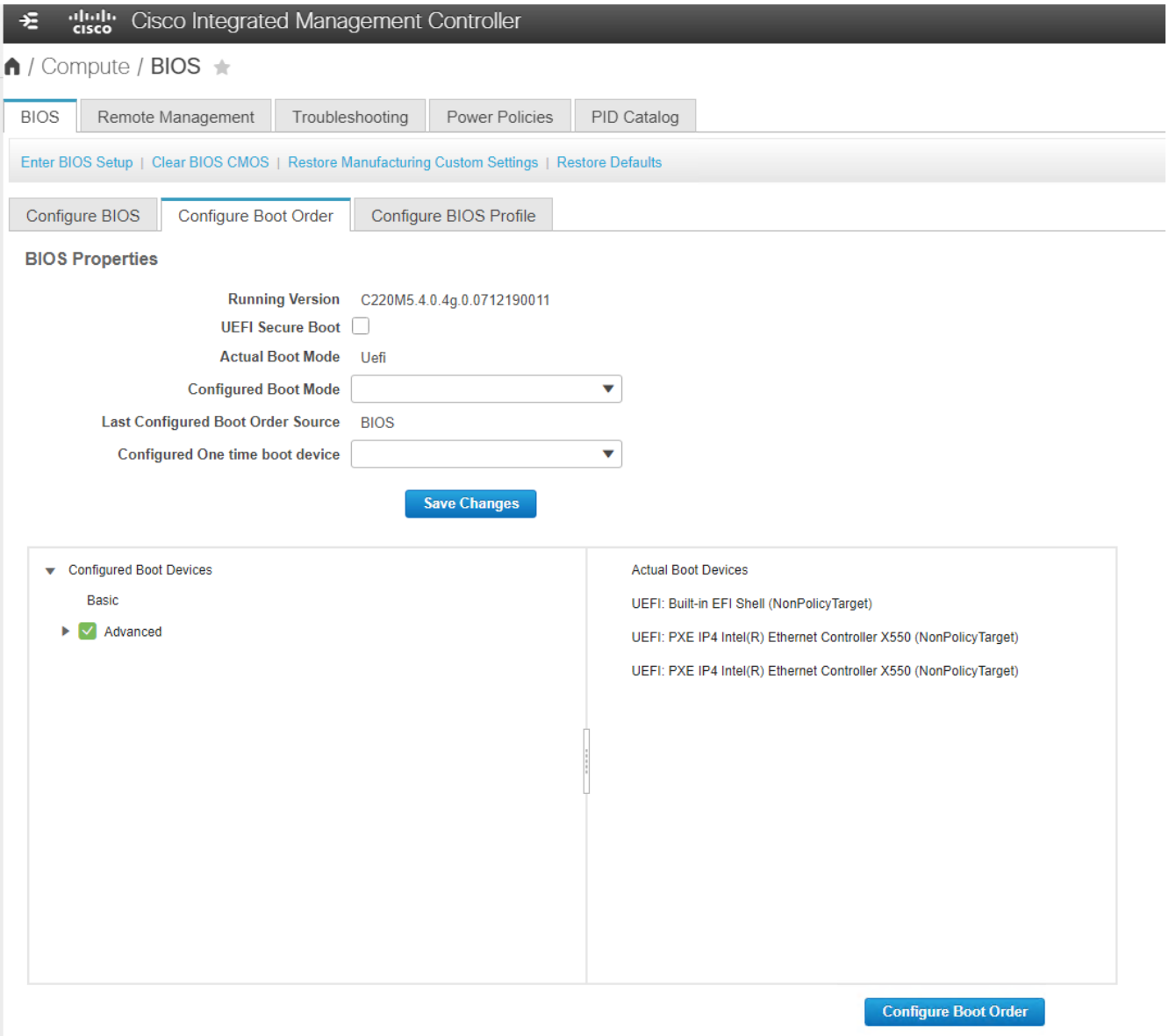
Un font en cursiva indica variables que son únicas para cada host ESXi.

Detalles	Valor de detalle
Nombre Del iniciador del host ESXi	<<var_ucs_initiator_name_A>>
Host ESXi iSCSI-A IP	<<var_esxi_host_iscsiA_ip>>
Máscara de red iSCSI-A del host ESXi	<<var_esxi_host_iscsiA_mask>>
ISCSI del host ESXi: Puerta de enlace predeterminada	<<var_esxi_host_iscsiA_gateway>>
Nombre B del iniciador del host ESXi	<<var_ucs_initiator_name_B>>
Host ESXi iSCSI-B IP	<<var_esxi_host_iscsiB_ip>>
Máscara de red iSCSI-B del host ESXi	<<var_esxi_host_iscsiB_mask>>
Puerta de enlace iSCSI-B del host ESXi	<<var_esxi_host_iscsiB_gateway>>
Dirección IP iscsi_lif01a	<<var_iscsi_lif01a>>
Dirección IP iscsi_lif02a	<<var_iscsi_lif02a>>
Dirección IP iscsi_lif01b	<<var_iscsi_lif01b>>
Dirección IP iscsi_lif02b	<<var_iscsi_lif02b>>
IQN de infr_SVM	<<var_SVM_IQN>>

Configuración del orden de arranque

Para establecer la configuración del orden de arranque, lleve a cabo los siguientes pasos:

1. En la ventana del navegador de la interfaz CIMC, haga clic en la ficha Compute (computación) y seleccione BIOS.
2. Haga clic en Configurar orden de arranque y, a continuación, en Aceptar.



3. Configure los siguientes dispositivos haciendo clic en el dispositivo en Agregar dispositivo de arranque y yendo a la ficha Opciones avanzadas:

   a. Agregar medios virtuales:

      NOMBRE: KVM-CD-DVD

      SUBTIPO: DVD KVM ASIGNADO

      Estado: Habilitado

      Orden: 1

   b. Agregar arranque iSCSI:

      Nombre: ISCSI-a

      Estado: Habilitado

      Orden: 2

Ranura: MLOM

Puerto: 1

c. Haga clic en Add iSCSI Boot:

Nombre: ISCSI-B

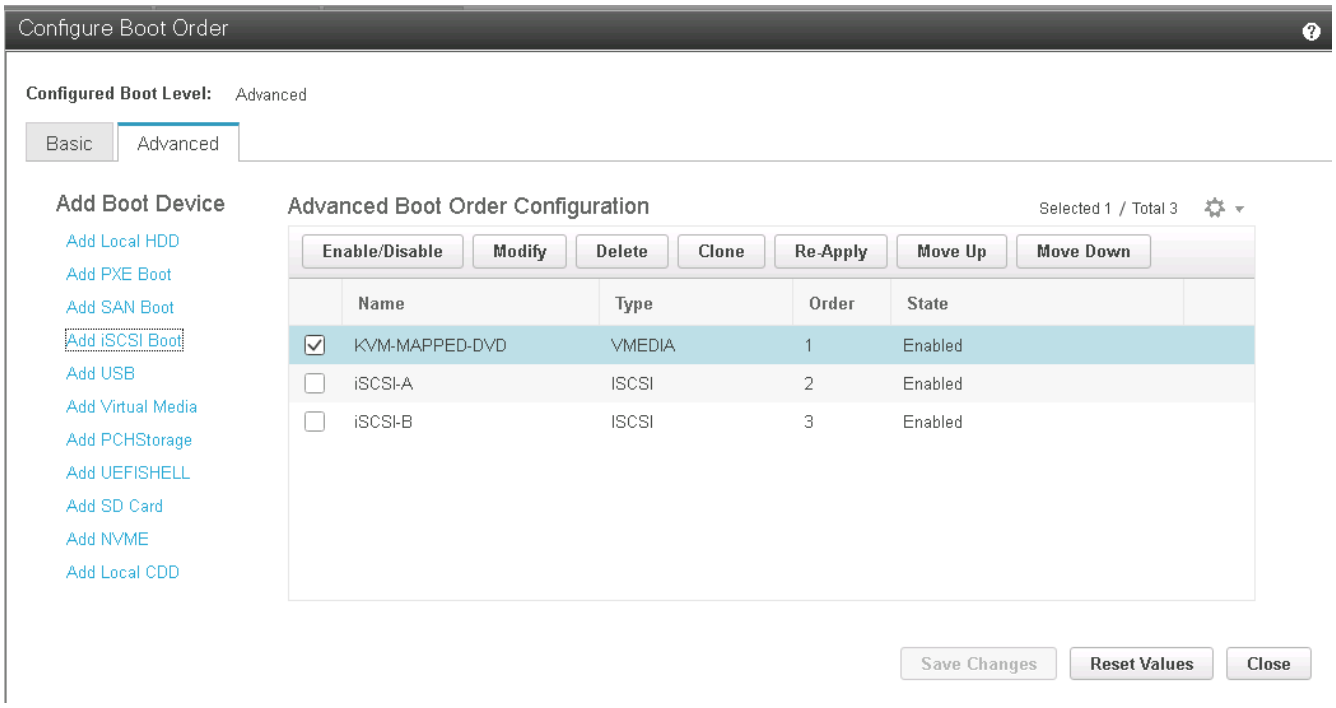
Estado: Habilitado

Pedido: 3

Ranura: MLOM

Puerto: 3

4. Haga clic en Agregar dispositivo.
5. Haga clic en Save Changes y, a continuación, en Close.

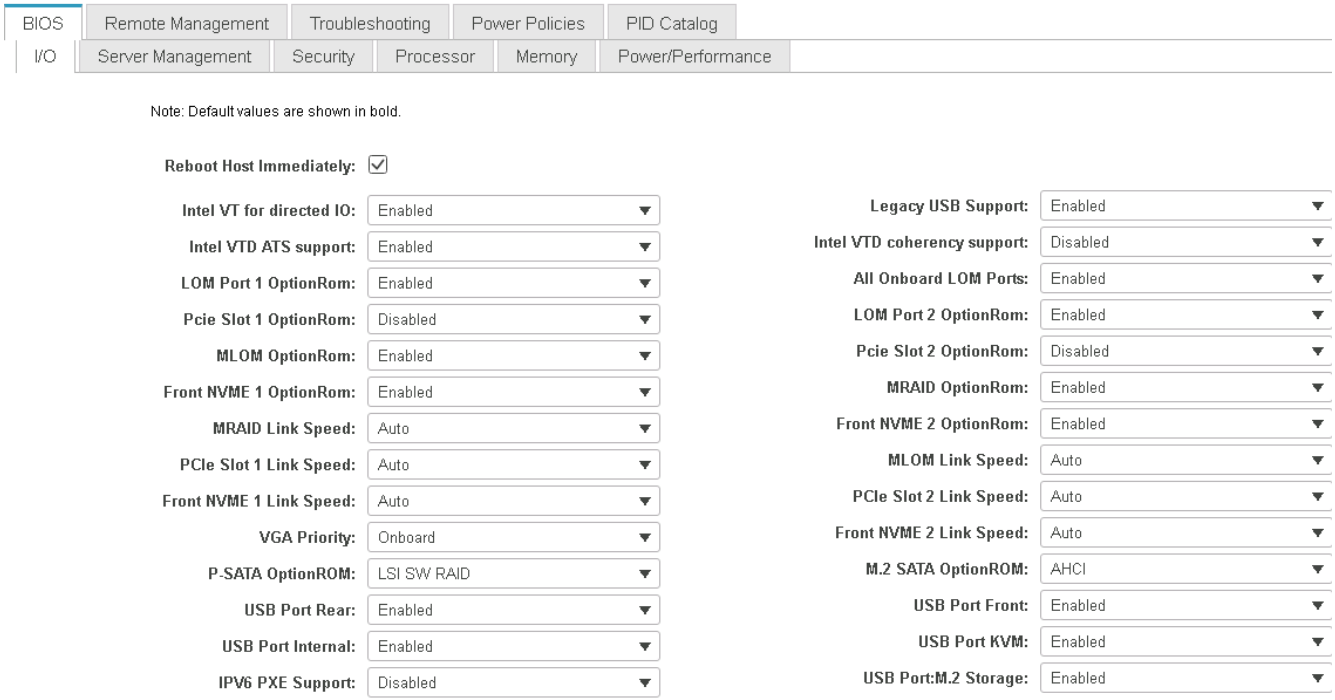


6. Reinicie el servidor para arrancar con el nuevo orden de inicio.

Desactivar la controladora RAID (si existe)

Siga estos pasos si el servidor C-Series contiene una controladora RAID. No se necesita una controladora RAID en el arranque desde la configuración SAN. De manera opcional, también puede quitar físicamente la controladora RAID del servidor.

1. En la pestaña Compute, haga clic en BIOS en el panel de navegación izquierdo de CIMC.
2. Seleccione Configurar BIOS.
3. Desplácese hacia abajo hasta la ranura PCIe:ROM de opción HBA.
4. Si el valor no está desactivado, configúrelo en Desactivado.

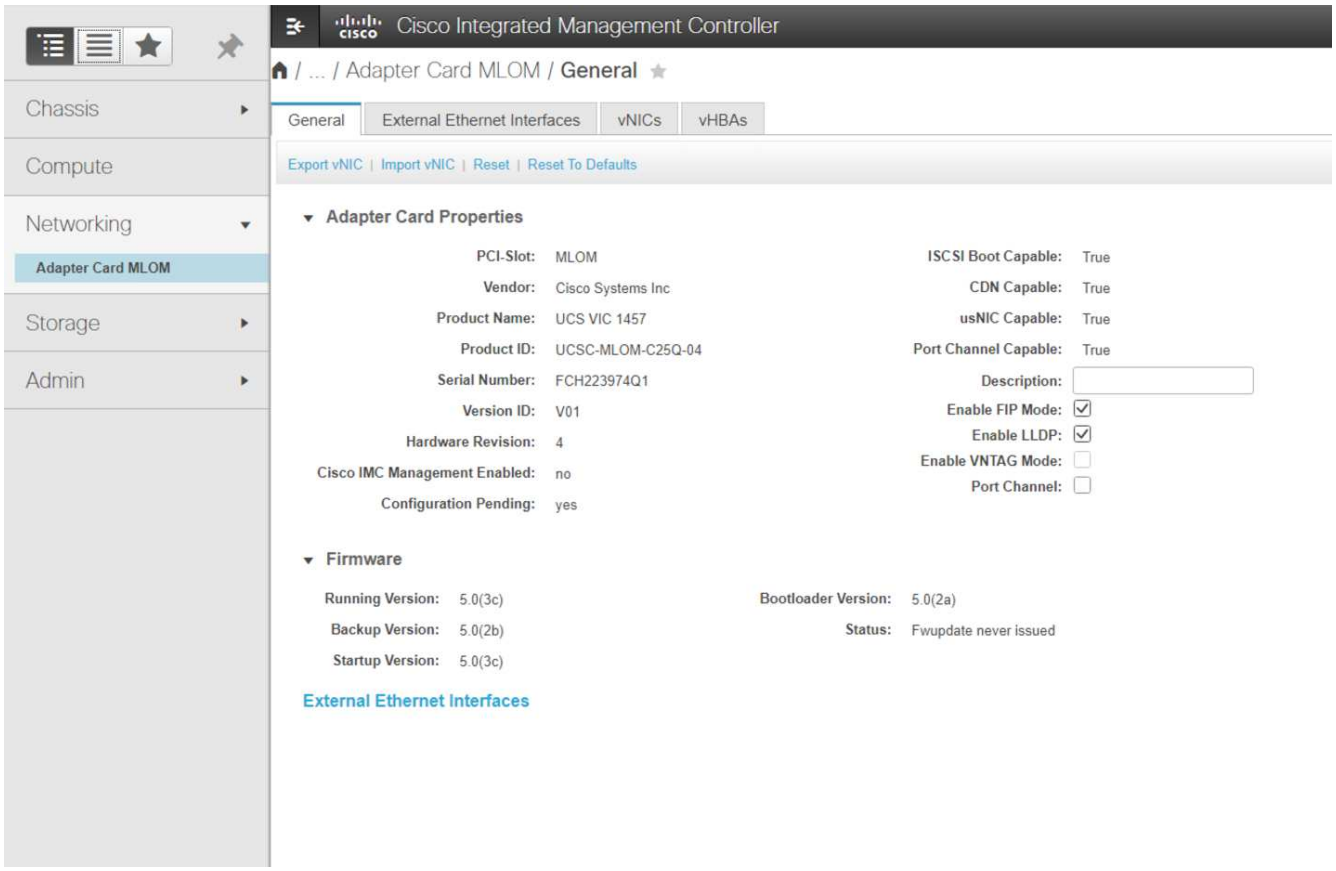


Configurar Cisco VIC1457 para el arranque iSCSI

Los pasos de configuración siguientes son para el VIC 1457 de Cisco para arranque iSCSI.

> La canalización de puertos predeterminada entre los puertos 0, 1, 2 y 3 se debe desactivar antes de poder configurar los cuatro puertos individuales. Si la canalización del puerto no está desactivada, sólo aparecen dos puertos para el VIC 1457. Realice los siguientes pasos para activar el canal de puerto en el CIMC:

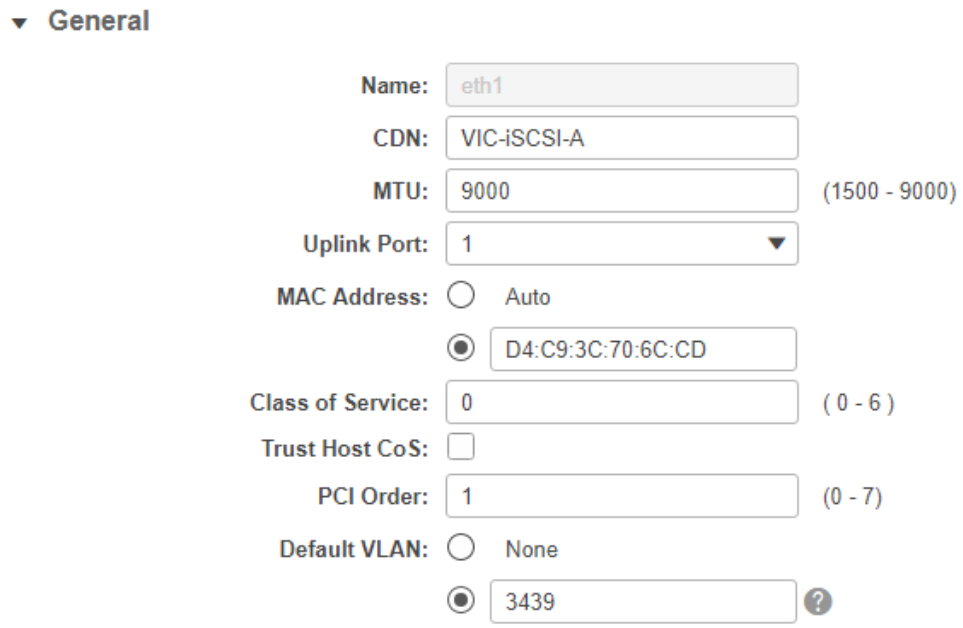
1. En la ficha redes, haga clic en la tarjeta adaptadora MLOM.
2. En la ficha General, desactive el canal de puerto.
3. Guarde los cambios y reinicie el CIMC.



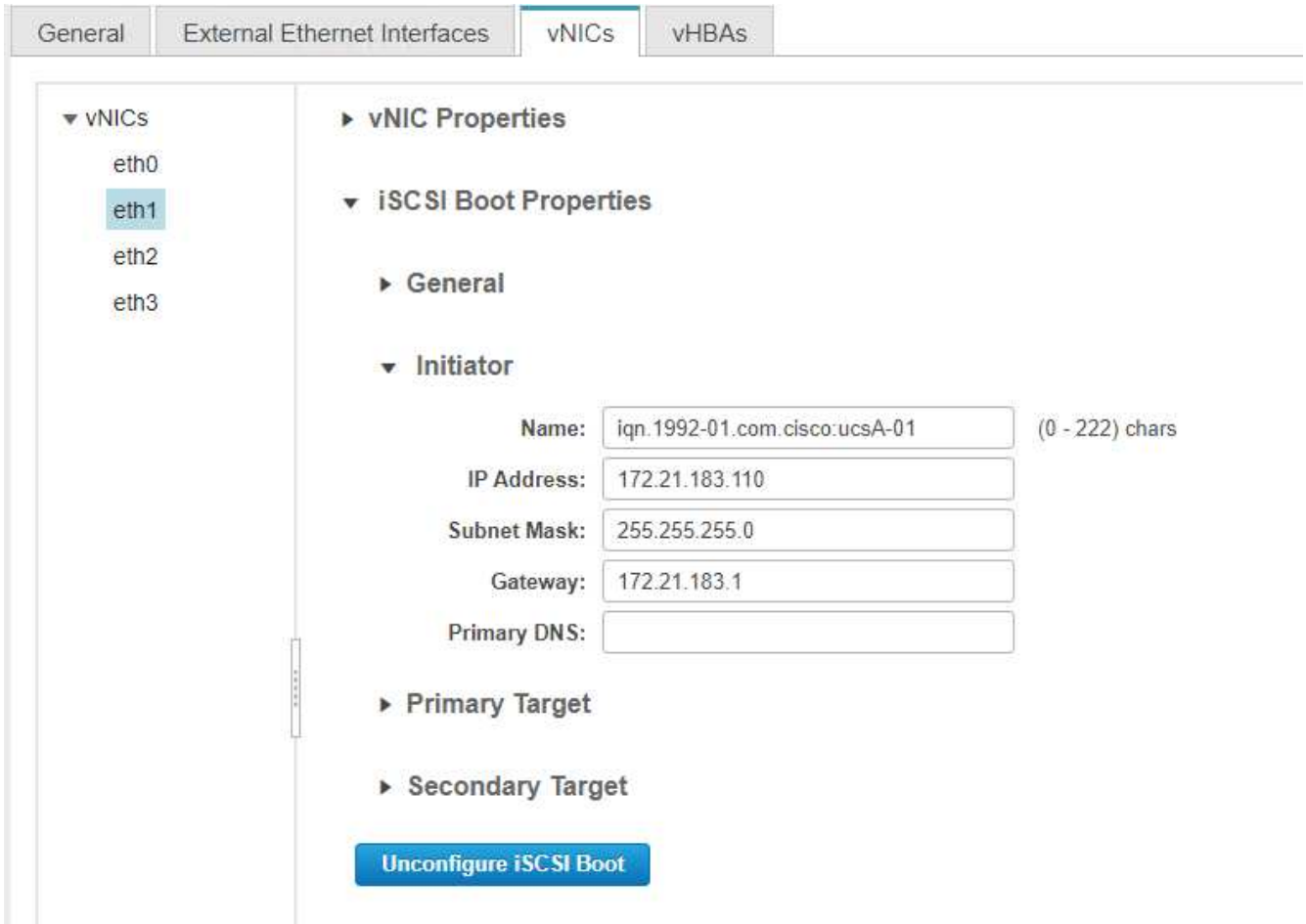
Cree NIC iSCSI

Para crear VNIC iSCSI, lleve a cabo los siguientes pasos:

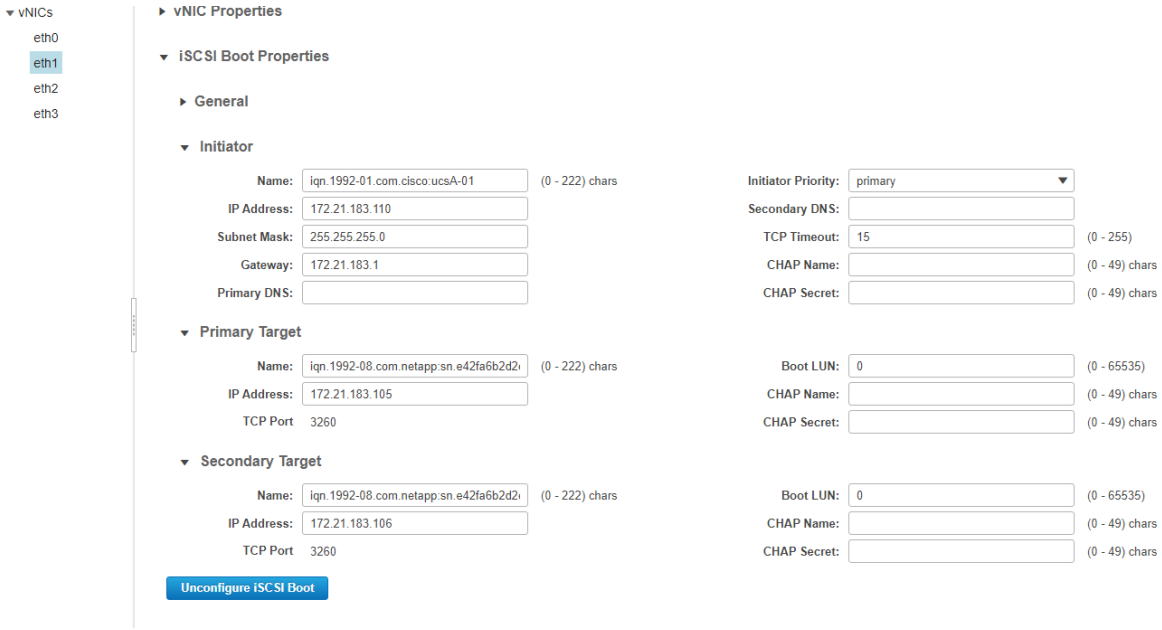
1. En la ficha redes, haga clic en adaptador de tarjeta MLOM.
2. Haga clic en Agregar VNIC para crear un VNIC.
3. En la sección Agregar VNIC, introduzca los siguientes ajustes:
   - Nombre: Eth1
   - Nombre de CDN: ISCSI-VNIC-A
   - MTU: 9000
   - VLAN predeterminada: `<<var_iscsi_vlan_a>>`
   - Modo VLAN: TRONCO
   - Activar inicio PXE: Comprobación
4. Haga clic en Agregar VNIC y, a continuación, en Aceptar.
5. Repita el proceso para agregar un segundo VNIC:
   - Asigne un nombre al VNIC eth3.
   - Nombre de CDN: ISCSI-VNIC-B
   - Introduzca `<<var_iscsi_vlan_b>>` Como VLAN.
   - Establezca el puerto de enlace ascendente en 3.



6. Seleccione el eth1 de VNIC a la izquierda.



7. En Propiedades de arranque iSCSI, introduzca los detalles del iniciador:
   - Nombre: `<<var_ucsa_initiator_name_a>>`
   - Dirección IP: `<<var_esxi_hostA_iscsiA_ip>>`
   - Máscara de subred: `<<var_esxi_hostA_iscsiA_mask>>`
   - Puerta de enlace: `<<var_esxi_hostA_iscsiA_gateway>>`



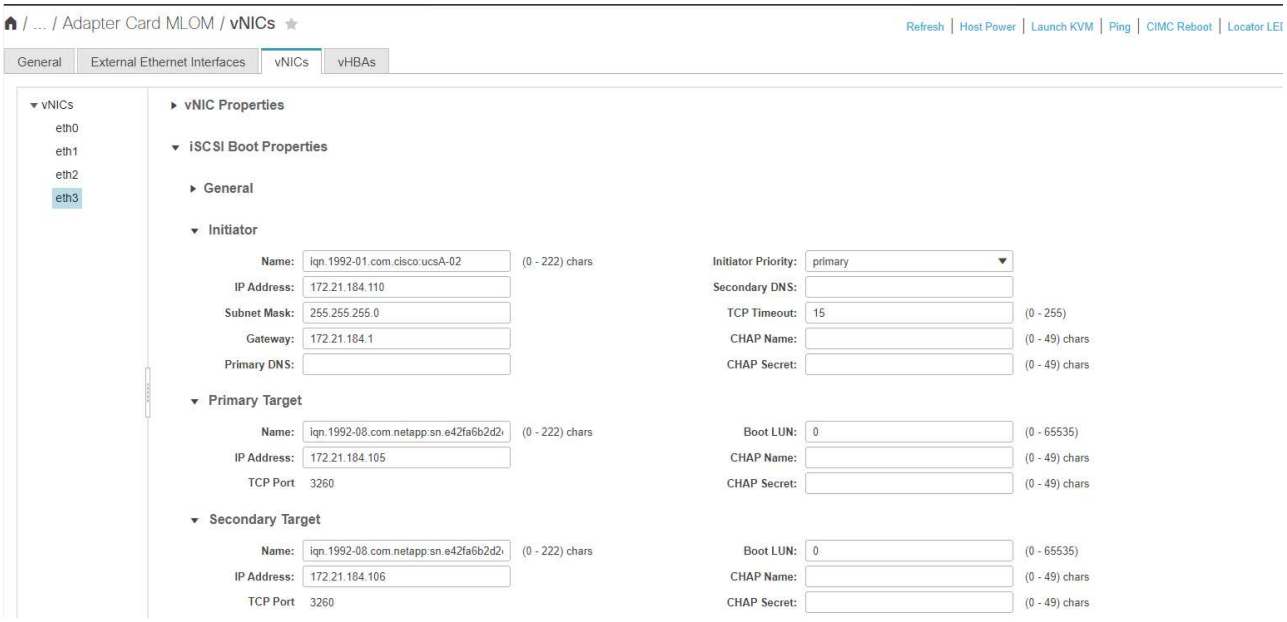
8. Introduzca los detalles del destino principal:
   - Nombre: Número IQN de infra-SVM
   - Dirección IP: Dirección IP de iscsi_lif01a
   - LUN de arranque: 0
9. Introduzca los detalles del destino secundario:
   - Nombre: Número IQN de infra-SVM
   - Dirección IP: Dirección IP de iscsi_lif02a
   - LUN de arranque:0

> Puede obtener el número IQN de almacenamiento ejecutando el `vserver iscsi show` comando.

> Asegúrese de registrar los nombres IQN de cada VNIC. Se necesitan para un paso más adelante. Además, los nombres IQN para los iniciadores deben ser únicos para cada servidor y para el VNIC de iSCSI.

10. Haga clic en Save Changes.
11. Seleccione VNIC eth3 y haga clic en el botón de inicio iSCSI que se encuentra en la parte superior de la sección interfaces de Ethernet del host.
12. Repita el proceso para configurar eth3.

13. Introduzca los detalles del iniciador:
    - Nombre: `<<var_ucsa_initiator_name_b>>`
    - Dirección IP: `<<var_esxi_hostb_iscsib_ip>>`
    - Máscara de subred: `<<var_esxi_hostb_iscsib_mask>>`
    - Puerta de enlace: `<<var_esxi_hostb_iscsib_gateway>>`



14. Introduzca los detalles del destino principal:
    - Nombre: Número IQN de infra-SVM
    - Dirección IP: Dirección IP de iscsi_lif01b
    - LUN de arranque: 0
15. Introduzca los detalles del destino secundario:
    - Nombre: Número IQN de infra-SVM
    - Dirección IP: Dirección IP de iscsi_lif02b
    - LUN de arranque: 0

> Puede obtener el número de IQN de almacenamiento mediante el `vserver iscsi show` comando.

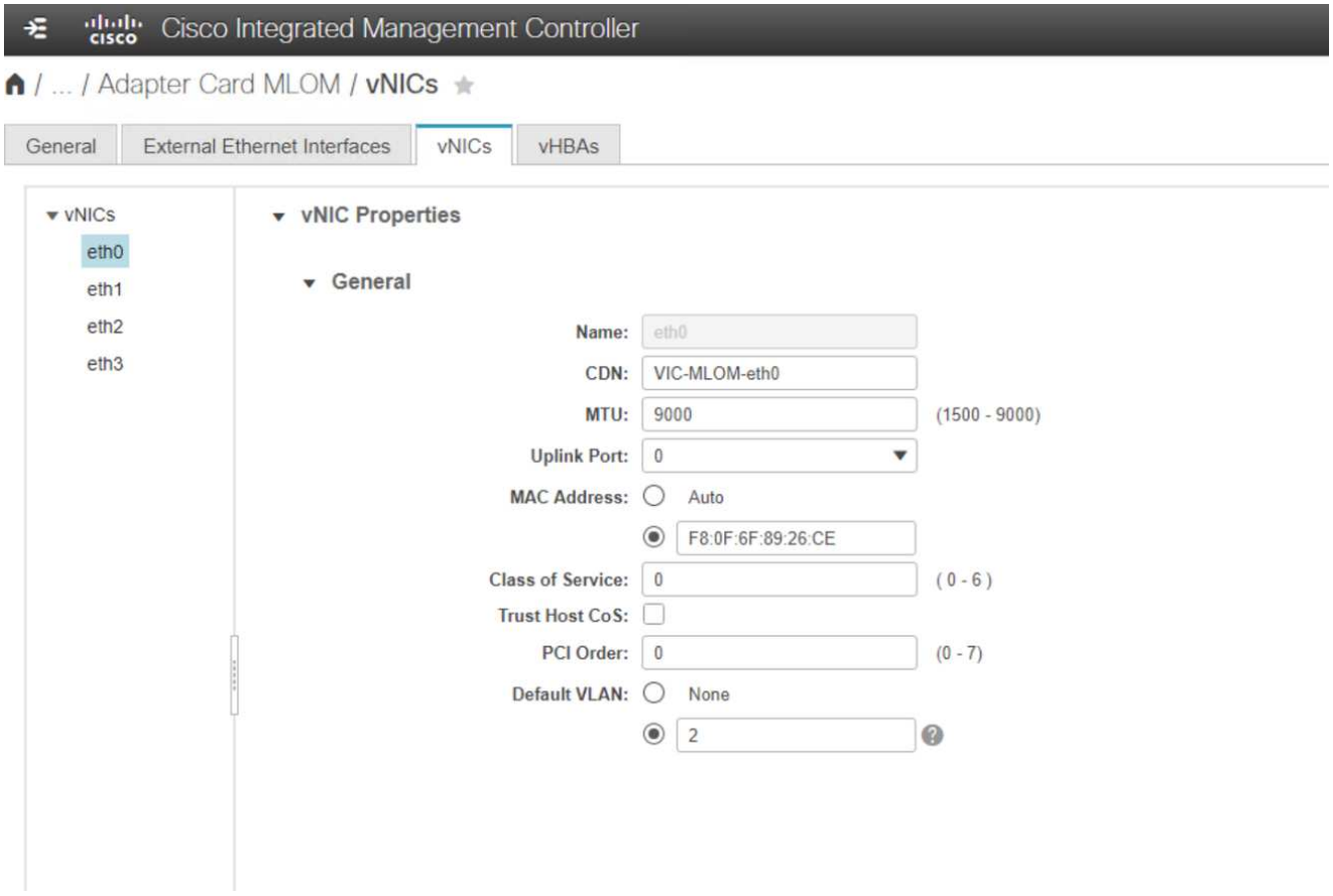
> Asegúrese de registrar los nombres IQN de cada VNIC. Se necesitan para un paso más adelante.

16. Haga clic en Save Changes.
17. Repita este proceso para configurar el arranque iSCSI para el servidor Cisco UCS B.

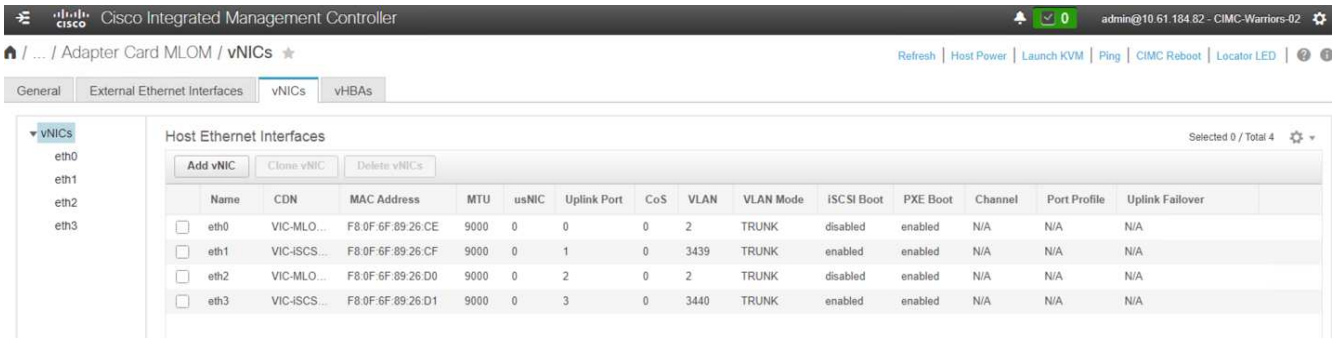
Configure las NIC virtuales para ESXi

Para configurar VNIC para ESXi, realice los siguientes pasos:

1. En la ventana del navegador de la interfaz CIMC, haga clic en Inventario y, a continuación, en Adaptadores Cisco VIC en el panel derecho.
2. En redes > Tarjeta adaptadora MLOM, seleccione la ficha vNIC y, a continuación, seleccione las vNIC debajo.
3. Seleccione eth0 y haga clic en Propiedades.
4. Establezca la MTU en 9000. Haga clic en Save Changes.
5. Establezca la VLAN como VLAN nativa 2.



6. Repita los pasos 3 y 4 en eth1, verificando que el puerto de enlace ascendente se establece en 1 para eth1.



Este procedimiento debe repetirse para cada nodo de servidor Cisco UCS inicial y cada nodo de servidor Cisco UCS adicional agregado al entorno.

"Siguiente: Procedimiento de implementación del almacenamiento AFF de NetApp (parte 2)."

Procedimiento de puesta en marcha del almacenamiento AFF de NetApp (parte 2)

Configurar el almacenamiento DE arranque SAN de ONTAP

Cree iGroups iSCSI

Para este paso, se necesitan los IQN de iniciadores iSCSI desde la configuración del servidor.

Para crear iGroups, ejecute los siguientes comandos desde la conexión SSH del nodo de gestión del clúster. Para ver los tres iGroups creados en este paso, ejecute el `igroup show` comando.

```
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>>
```

Este paso se debe completar cuando se añaden servidores Cisco UCS C-Series adicionales.

Asigne LUN de arranque a iGroups

```
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
```

Este paso se debe completar cuando se añaden servidores Cisco UCS C-Series adicionales.

"Siguiente: Procedimiento de puesta en marcha de VMware vSphere 6.7U2."

Procedimiento de puesta en marcha de VMware vSphere 6.7U2

En esta sección, se proporcionan los procedimientos detallados para la instalación de VMware ESXi 6.7U2 en una configuración FlexPod Express. Los procedimientos de implementación siguientes se personalizan para incluir las variables de entorno descritas en secciones anteriores.

Existen varios métodos para instalar VMware ESXi en dicho entorno. Este procedimiento utiliza la consola KVM virtual y las funciones de medios virtuales de la interfaz CIMC para servidores Cisco UCS C-Series para asignar medios de instalación remotos a cada servidor individual.

Este procedimiento se debe completar para el servidor Cisco UCS A y el servidor Cisco UCS B.

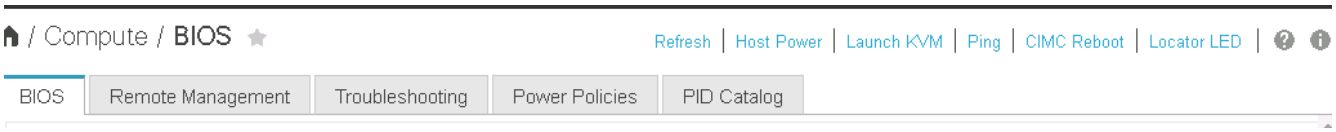
Este procedimiento debe completarse para los nodos adicionales que se añadan al clúster.

Inicie sesión en la interfaz de CIMC para servidores independientes de Cisco UCS C-Series

Los siguientes pasos detallan el método para iniciar sesión en la interfaz de CIMC para servidores independientes Cisco UCS C-Series. Debe iniciar sesión en la interfaz de CIMC para ejecutar el KVM virtual, que permite al administrador iniciar la instalación del sistema operativo a través de medios remotos.

Todos los hosts

1. Desplácese hasta un explorador web e introduzca la dirección IP para la interfaz de CIMC para Cisco UCS C-Series. Este paso inicia la aplicación GUI de CIMC.
2. Inicie sesión en la interfaz de usuario de CIMC con el nombre de usuario y las credenciales de administrador.
3. En el menú principal, seleccione la ficha servidor.
4. Haga clic en Iniciar la consola KVM.



5. En la consola KVM virtual, seleccione la ficha Medios virtuales.
6. Selecciona Mapa CD/DVD.

Es posible que primero tenga que hacer clic en Activar dispositivos virtuales. Seleccione Aceptar esta sesión si se le solicita.

7. Desplácese hasta el archivo de imagen ISO del instalador VMware ESXi 6.7U2 y haga clic en Open. Haga clic en asignar dispositivo.
8. Seleccione el menú de encendido y elija sistema de ciclo de encendido (arranque en frío). Haga clic en Yes.

Instale VMware ESXi

Los siguientes pasos describen cómo instalar VMware ESXi en cada host.

Descargue LA imagen personalizada de Cisco DE ESXI 6.7U2

1. Desplácese hasta la "Página de descarga de VMware vSphere" Para ISO personalizados.
2. Haga clic en Go to Downloads junto a la imagen personalizada de Cisco para el CD de instalación de ESXi 6.7U2.
3. Descargue la imagen personalizada de Cisco para el CD de instalación de ESXi 6.7U2 (ISO).
4. Cuando el sistema arranca, la máquina detecta la presencia del medio de instalación de VMware ESXi.
5. Seleccione el instalador de VMware ESXi en el menú que aparece. El instalador se carga, lo que puede tardar varios minutos.

6. Cuando el instalador haya terminado de cargarse, pulse Intro para continuar con la instalación.
7. Después de leer el contrato de licencia del usuario final, acepte y continúe con la instalación pulsando F11.
8. Seleccione el LUN de NetApp que se configuró anteriormente como disco de instalación para ESXi y pulse Intro para continuar con la instalación.

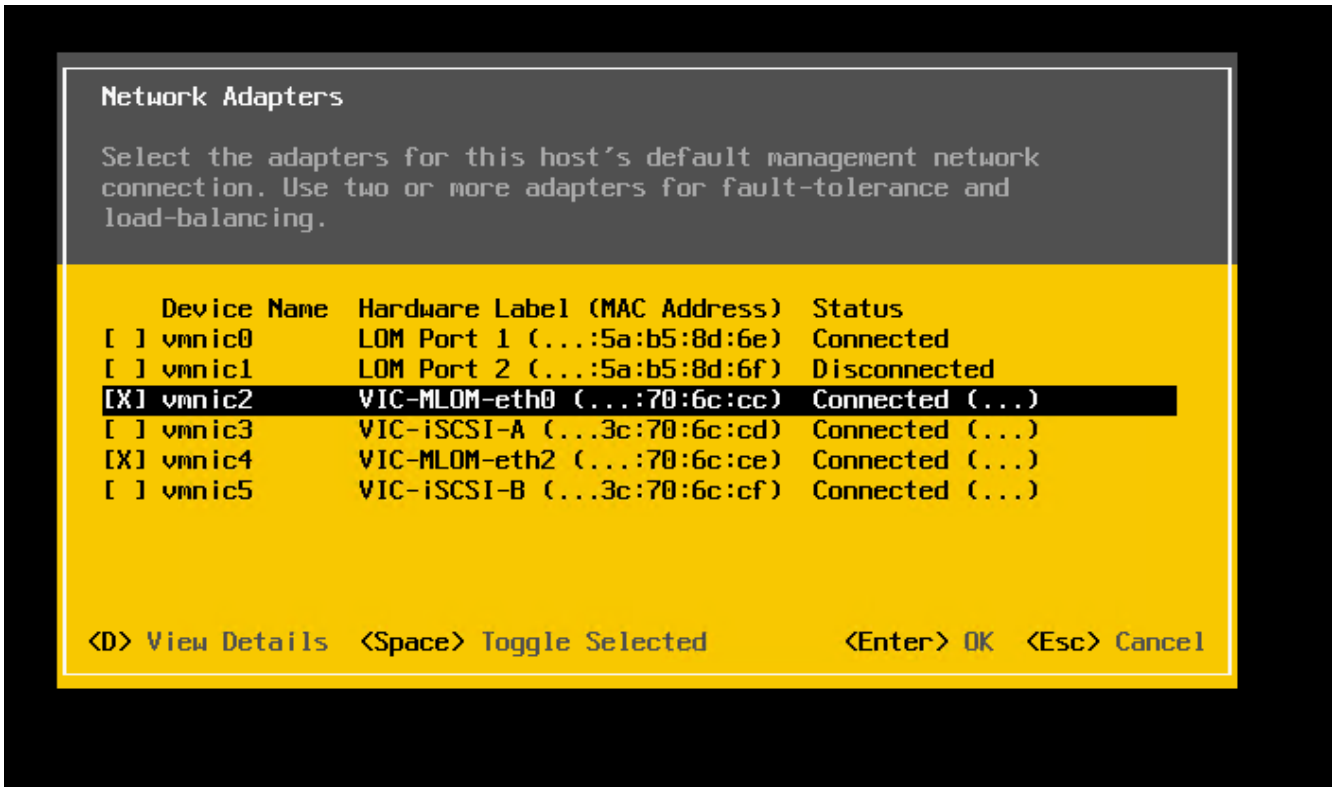
9. Seleccione la distribución de teclado adecuada y pulse Intro.
10. Introduzca y confirme la contraseña de root y pulse Intro.
11. El instalador le advierte que las particiones existentes se han eliminado en el volumen. Continúe con la instalación pulsando F11. El servidor se reinicia después de la instalación de ESXi.

Configure la red de gestión del host VMware ESXi

Los siguientes pasos describen cómo añadir la red de gestión de cada host VMware ESXi.

Todos los hosts

1. Una vez que el servidor haya terminado de reiniciarse, introduzca la opción de personalizar el sistema pulsando F2.
2. Inicie sesión con root como nombre de inicio de sesión y la contraseña raíz que se introdujo anteriormente durante el proceso de instalación.
3. Seleccione la opción Configure Management Network.
4. Seleccione Adaptadores de red y pulse Intro.
5. Seleccione los puertos deseados para vSwitch0. Pulse Intro.
6. Seleccione los puertos que corresponden a eth0 y eth1 en CIMC.



7. Seleccione VLAN (opcional) y presione Enter.
8. Introduzca el identificador de VLAN `<<mgmt_vlan_id>>`. Pulse Intro.
9. En el menú Configurar red de gestión, seleccione Configuración de IPv4 para configurar la dirección IP de la interfaz de gestión. Pulse Intro.
10. Utilice las teclas de flecha para resaltar establecer dirección IPv4 estática y utilice la barra espaciadora para seleccionar esta opción.
11. Introduzca la dirección IP para gestionar el host VMware ESXi `<<esxi_host_mgmt_ip>>`.
12. Introduzca la máscara de subred para el host VMware ESXi `<<esxi_host_mgmt_netmask>>`.
13. Introduzca la puerta de enlace predeterminada para el host VMware ESXi `<<esxi_host_mgmt_gateway>>`.
14. Pulse Intro para aceptar los cambios en la configuración de IP.
15. Acceda al menú de configuración de IPv6.
16. Utilice la barra de espacio para desactivar IPv6 deseleccionando la opción Habilitar IPv6 (reiniciar requerido). Pulse Intro.
17. Abra el menú para configurar los ajustes de DNS.
18. Dado que la dirección IP se asigna manualmente, la información DNS también debe introducirse manualmente.
19. Introduzca la dirección IP del servidor DNS primario `<<nameserver_ip>>`.
20. (Opcional) Introduzca la dirección IP del servidor DNS secundario.
21. Introduzca el FQDN para el nombre de host VMware ESXi: `<<esxi_host_fqdn>>`.
22. Pulse Intro para aceptar los cambios en la configuración de DNS.
23. Salga del submenú Configurar red de administración pulsando Esc.

24. Pulse y para confirmar los cambios y reiniciar el servidor.
25. Seleccione Troubleshooting Options y, a continuación, habilite ESXi Shell y SSH.

> Estas opciones de solución de problemas se pueden desactivar después de la validación de acuerdo con la política de seguridad del cliente.

26. Pulse Esc dos veces para volver a la pantalla principal de la consola.
27. Haga clic en Alt-F1 en el menú desplegable macros de CIMC > macros estáticas > Alt-F en la parte superior de la pantalla.
28. Inicie sesión con las credenciales adecuadas para el host ESXi.
29. En el símbolo del sistema de, introduzca la siguiente lista de comandos esxcli para habilitar la conectividad de red de forma secuencial.

```
esxcli network vswitch standard policy failover set -v vSwitch0 -a
vmnic2,vmnic4 -l iphash
```

Configure el host ESXi

Utilice la información de la siguiente tabla para configurar cada host ESXi.

Detalles	Valor de detalle
Nombre de host ESXi	<<esxi_host_fqdn>>
La IP de gestión del host ESXi	<<esxi_host_mgmt_ip>>
Máscara de gestión de host ESXi	<<esxi_host_mgmt_netmask>>
Pasarela de gestión de host ESXi	<<esxi_host_mgmt_gateway>>
IP NFS del host ESXi	<<esxi_host_NFS_ip>>
Máscara de NFS del host ESXi	<<esxi_host_NFS_netmask>>
Puerta de enlace NFS del host ESXi	<<esxi_host_NFS_gateway>>
Host ESXi IP de vMotion	<<esxi_host_vMotion_ip>>
Máscara de vMotion del host ESXi	<<esxi_host_vMotion_netmask>>
Puerta de enlace vMotion del host ESXi	<<esxi_host_vMotion_gateway>>
Host ESXi iSCSI-A IP	<<esxi_host_iSCSI-A_ip>>
Máscara iSCSI-A del host ESXi	<<esxi_host_iSCSI-A_netmask>>
Puerta de enlace iSCSI-A del host ESXi	<<esxi_host_iSCSI-A_gateway>>
Host ESXi iSCSI-B IP	<<esxi_host_iSCSI-B_ip>>
Máscara iSCSI-B del host ESXi	<<esxi_host_iSCSI-B_netmask>>
Puerta de enlace iSCSI-B del host ESXi	<<esxi_host_SCSI-B_gateway>>

Inicie sesión en el host ESXi

Para iniciar sesión en el host ESXi, complete los siguientes pasos:

1. Abra la dirección IP de administración del host en un explorador Web.
2. Inicie sesión en el host ESXi con la cuenta raíz y la contraseña que especificó durante el proceso de instalación.
3. Lea la declaración sobre el Programa de mejora de la experiencia del cliente de VMware. Después de seleccionar la respuesta correcta, haga clic en Aceptar.

Configurar el arranque iSCSI

Para configurar el arranque iSCSI, lleve a cabo los siguientes pasos:

1. Seleccione Networking a la izquierda.
2. A la derecha, seleccione la ficha Switches virtuales.

3. Haga clic en iScsiBootvSwitch.
4. Seleccione Editar configuración.
5. Cambie la MTU a 9000 y haga clic en Save.
6. Cambie el nombre del puerto iSCSIBootPG a iSCSIBootPG-A.

> En esta configuración, se utilizan vmnic3 y vmnic5 para arranque iSCSI. Si tiene NIC adicionales en el host ESXi, puede tener distintos números vmnic. Para confirmar qué NIC se utilizan para el arranque iSCSI, haga coincidir las direcciones MAC de las NIC iSCSI de CIMC con los vmnics de ESXi.

7. En el panel central, seleccione la ficha NIC de VMkernel.
8. Seleccione Agregar NIC de VMkernel.
   a. Especifique un nuevo nombre de grupo de puertos de iScsiBootPG-B.

b. Seleccione iScsiBootvSwitch para el switch virtual.

c. Introduzca `<<iscsib_vlan_id>>` Para el ID de VLAN.

d. Cambie el MTU a 9000.

e. Expanda Configuración IPv4.

f. Seleccione Configuración estática.

g. Introduzca `<<var_hosta_iscsib_ip>>` Para Dirección.

h. Introduzca `<<var_hosta_iscsib_mask>>` Para Máscara de subred.

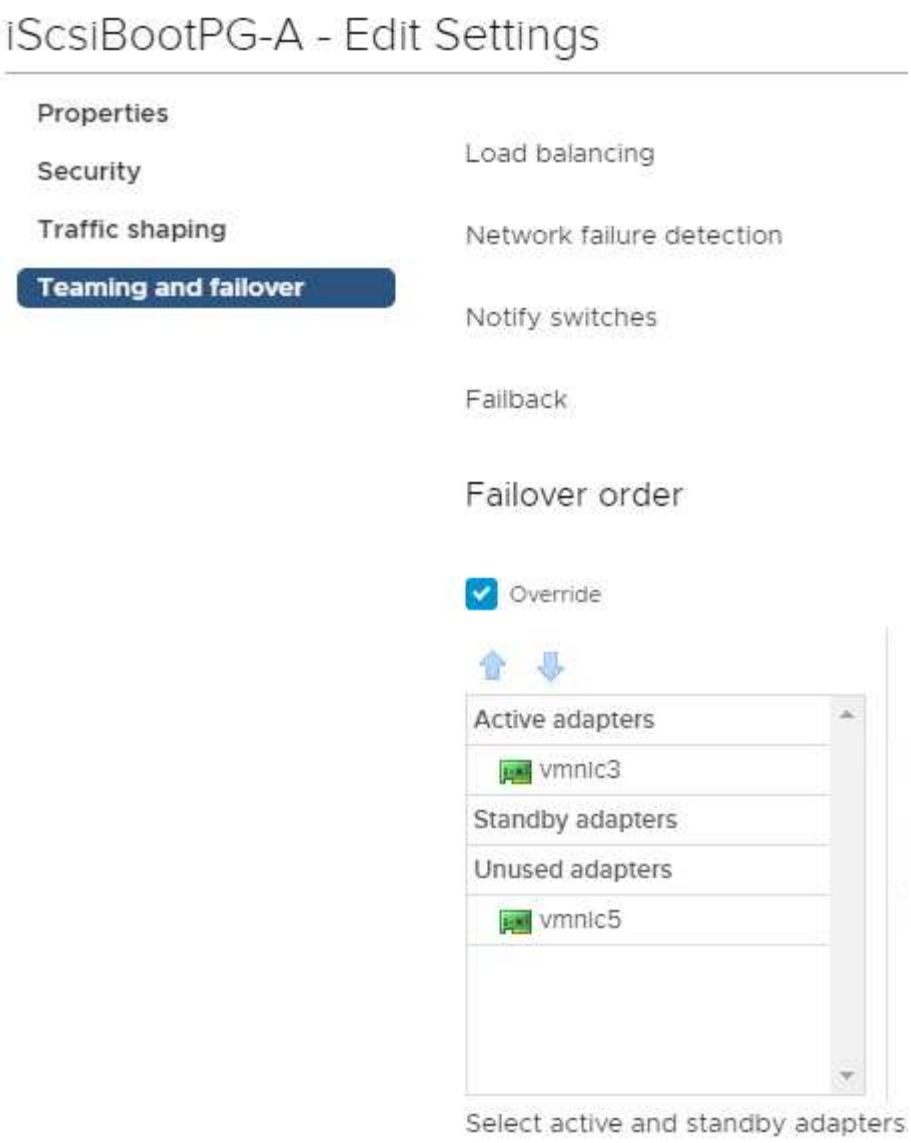
i. Haga clic en Crear.

Establezca la MTU en 9000 en iSCsiBootPG-A.

9. Para configurar la conmutación por error, lleve a cabo los siguientes pasos:

a. Haga clic en Edit Settings on iSCSIBootPG-A > Tiering and Failover > Failover Order > vmnic3. Vmnic3 debe estar activo y vmnic5 no se debe utilizar.

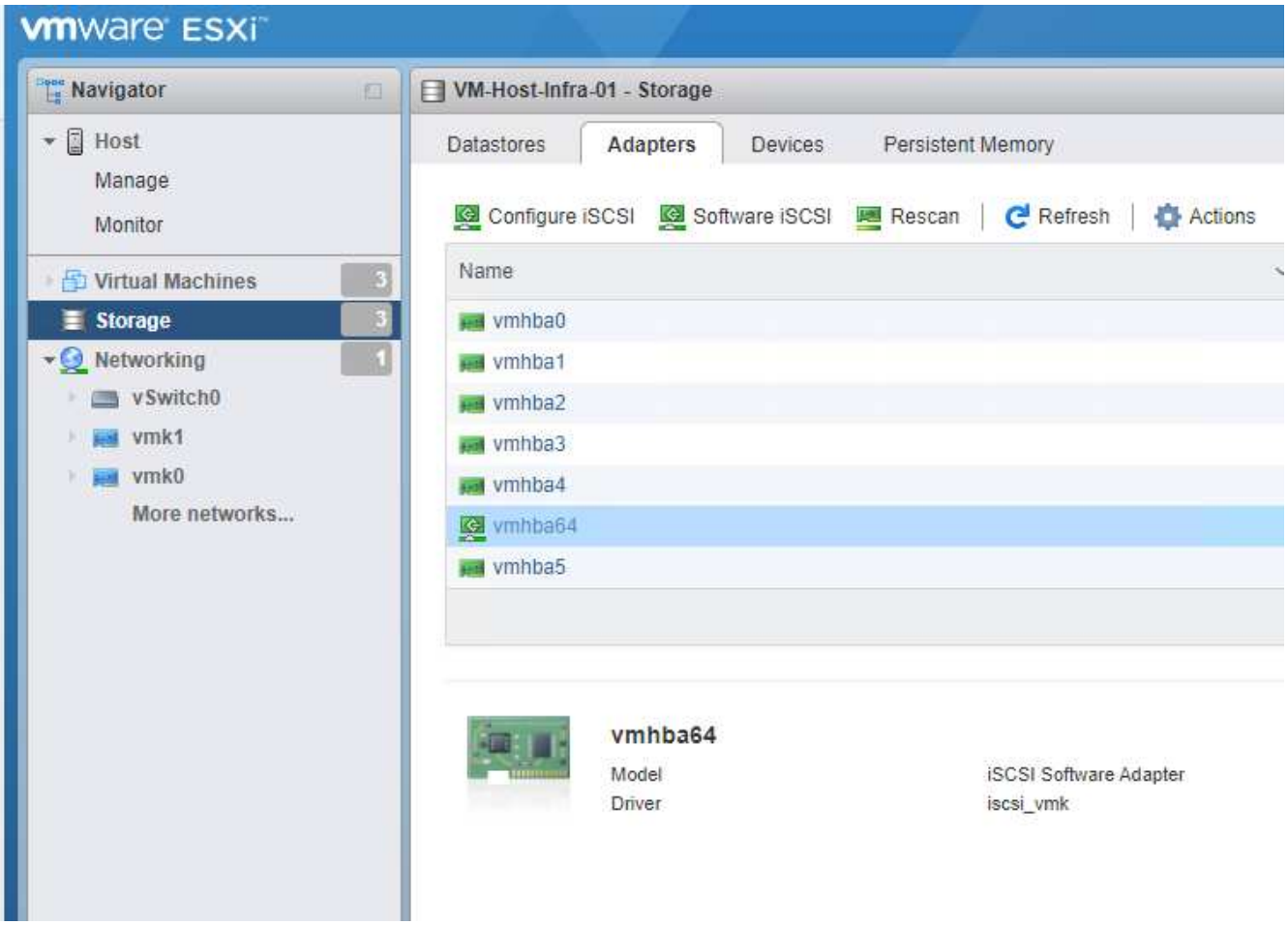
b. Haga clic en Editar configuración en iSCSIBootPG-B > equipos y failover > Orden de conmutación por error > vmnic5. Vmnic5 debe estar activo y vmnic3 no se debe utilizar.



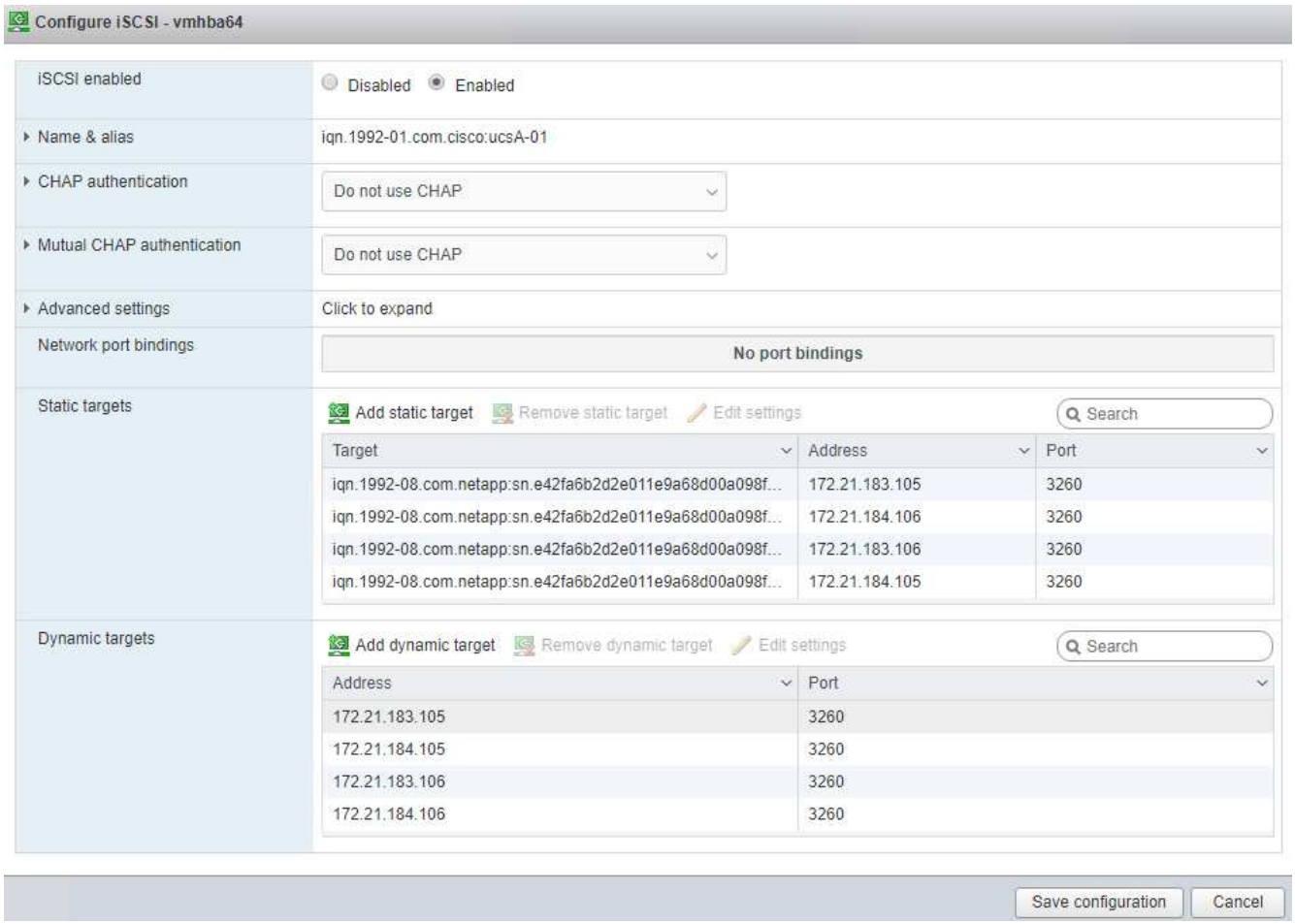
Configuración de accesos múltiples iSCSI

Para configurar la multivía iSCSI en los hosts ESXi, complete los pasos siguientes:

1. Seleccione Storage en el panel de navegación de la izquierda. Haga clic en Adaptadores.
2. Seleccione el adaptador de software iSCSI y haga clic en Configurar iSCSI.



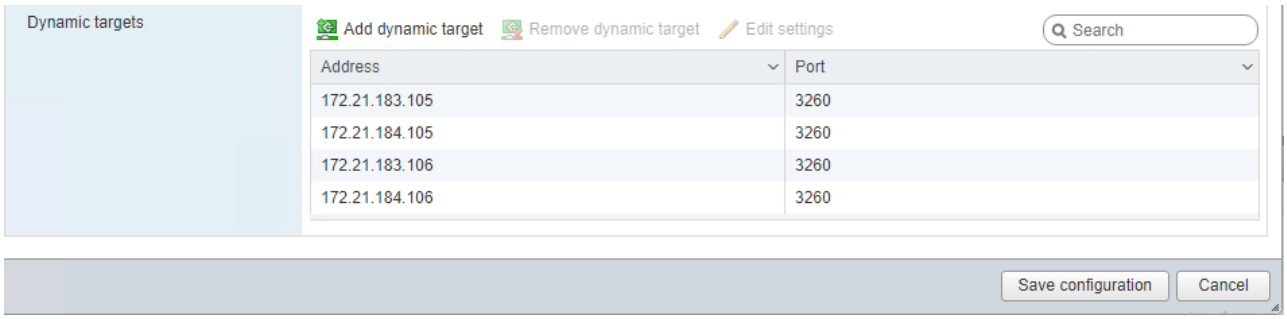
3. En Destinos dinámicos, haga clic en Agregar destino dinámico.



4. Introduzca la dirección IP `iscsi_lif01a`.

   a. Repita el proceso con las direcciones IP `iscsi_lif01b`, `iscsi_lif02a`, y. `iscsi_lif02b`.

   b. Haga clic en Save Configuration.



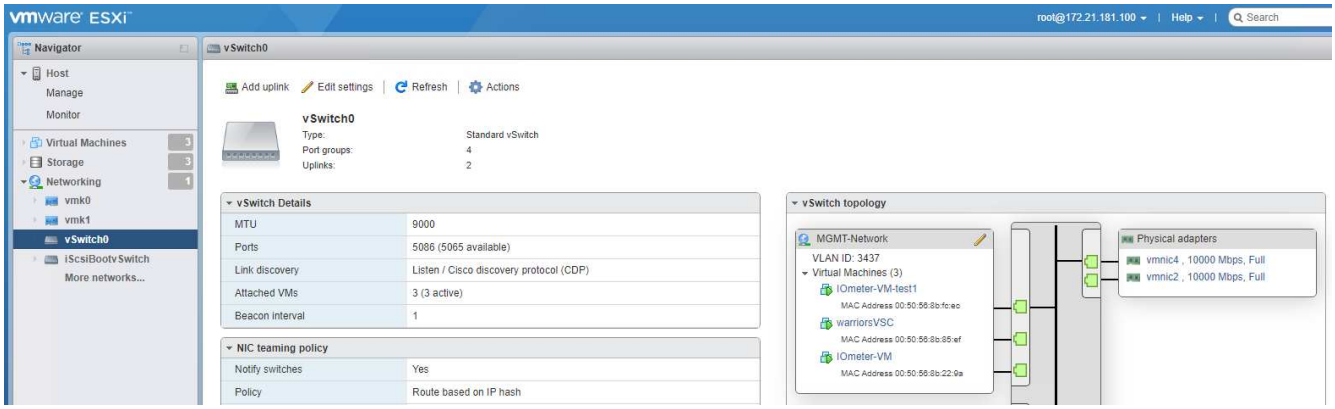
Puede encontrar las direcciones IP de LIF de iSCSI ejecutando el comando network interface show en el clúster de NetApp o mirando en la pestaña Network interfaces en System Manager.

Configure el host ESXi

Para configurar el arranque ESXi, complete los pasos siguientes:

1. En el panel de navegación de la izquierda, seleccione Networking.

2. Seleccione vSwitch0.



3. Seleccione Editar configuración.
4. Cambie el MTU a 9000.
5. Expanda NIC Teaming y verifique que tanto vmnic2 como vmnic4 estén configurados en activo y que NIC Teaming y Failover se establezcan en Route basado en IP Hash.

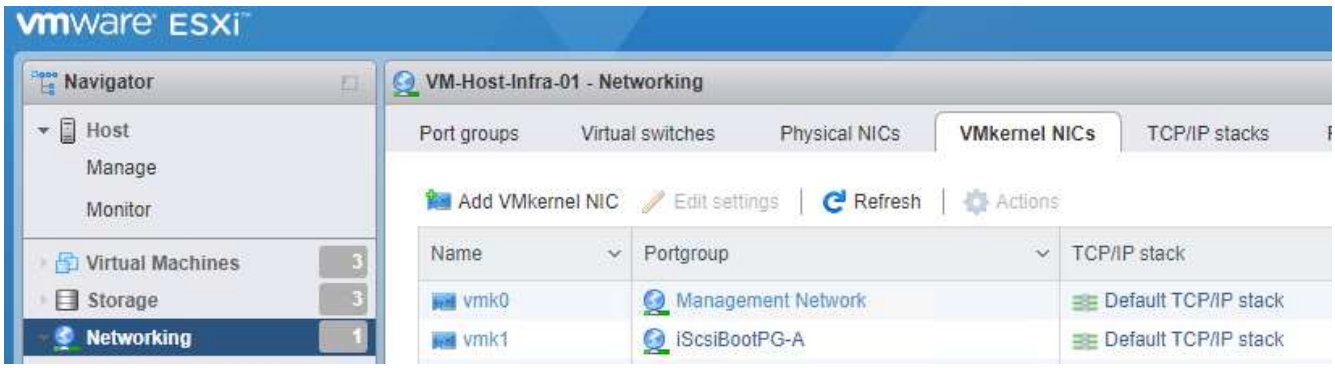
> El método hash IP del equilibrio de carga requiere que el conmutador físico subyacente se configure correctamente mediante SRC-DST-IP EtherChannel con un canal de puerto estático (modo activado). Es posible que experimente una conectividad intermitente debido a una posible configuración incorrecta del switch. En ese caso, apague temporalmente uno de los dos puertos de enlace ascendente asociados del switch Cisco para restaurar la comunicación con el puerto vmkernel de gestión de ESXi, a la vez que solucione problemas de la configuración del canal de puertos.

Configure los grupos de puertos y las NIC de VMkernel

Para configurar los grupos de puertos y las NIC de VMkernel, lleve a cabo los siguientes pasos:

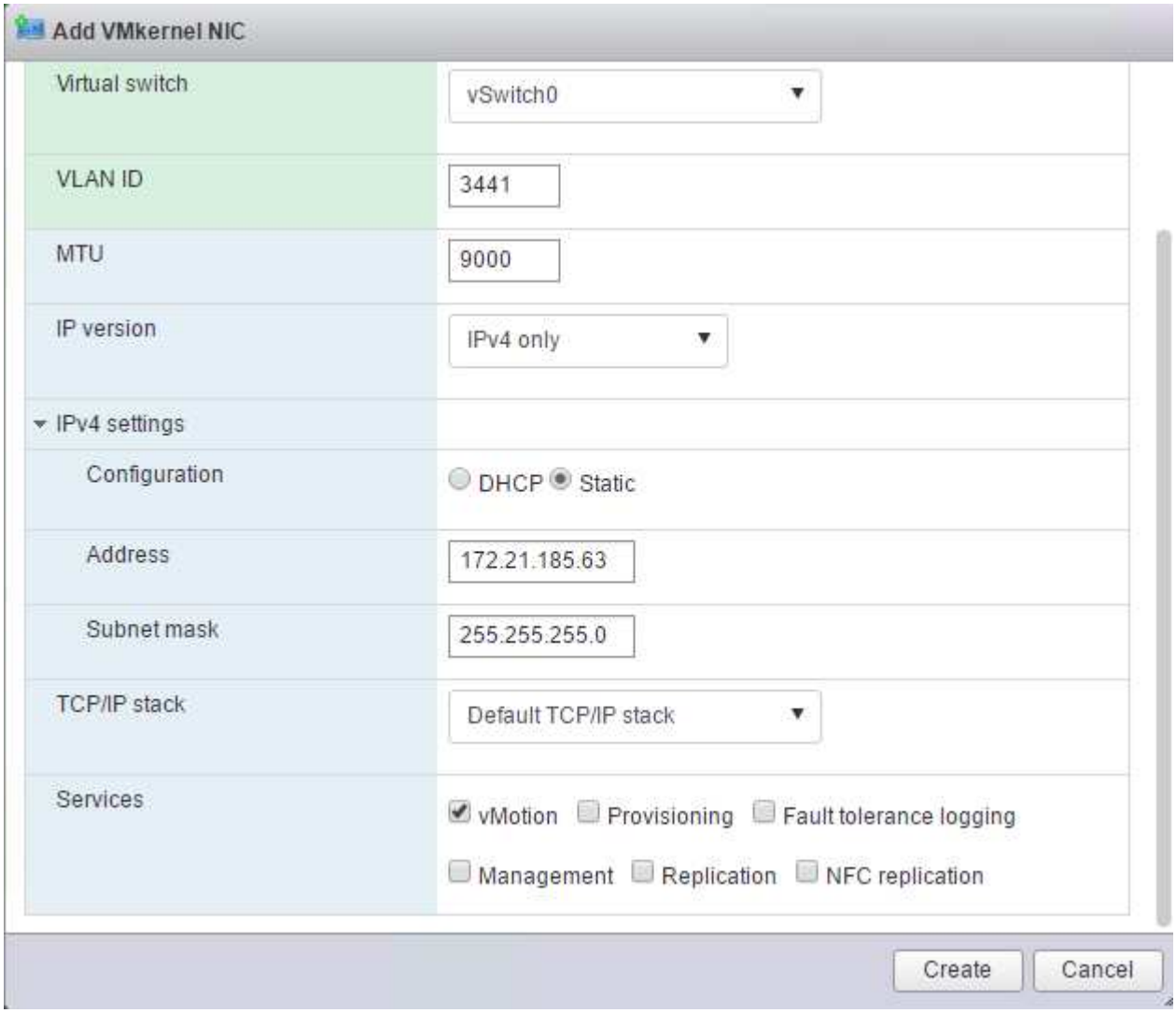
1. En el panel de navegación de la izquierda, seleccione Networking.
2. Haga clic con el botón derecho en la pestaña grupos de puertos.

3. Haga clic con el botón derecho en VM Network y seleccione Edit. Cambie el ID de VLAN a. `<<var_vm_traffic_vlan>>`.
4. Haga clic en Agregar grupo de puertos.
   a. Asigne el nombre MGMT-Network al grupo de puertos.
   b. Introduzca `<<mgmt_vlan>>` Para el ID de VLAN.
   c. Asegúrese de que vSwitch0 esté seleccionado.
   d. Haga clic en Guardar.
5. Haga clic en la ficha NIC de VMkernel.



6. Seleccione Agregar NIC de VMkernel.
   a. Seleccione Nuevo grupo de puertos.
   b. Asigne un nombre al grupo de puertos NFS-Network.
   c. Introduzca `<<nfs_vlan_id>>` Para el ID de VLAN.
   d. Cambie el MTU a 9000.
   e. Expanda Configuración IPv4.
   f. Seleccione Configuración estática.
   g. Introduzca `<<var_hosta_nfs_ip>>` Para Dirección.
   h. Introduzca `<<var_hosta_nfs_mask>>` Para Máscara de subred.
   i. Haga clic en Crear.
7. Repita este proceso para crear el puerto VMkernel de vMotion.
8. Seleccione Agregar NIC de VMkernel.
   a. Seleccione Nuevo grupo de puertos.
   b. Asigne un nombre al grupo de puertos vMotion.
   c. Introduzca `<<vmotion_vlan_id>>` Para el ID de VLAN.
   d. Cambie el MTU a 9000.
   e. Expanda Configuración IPv4.
   f. Seleccione Configuración estática.
   g. Introduzca `<<var_hosta_vmotion_ip>>` Para Dirección.
   h. Introduzca `<<var_hosta_vmotion_mask>>` Para Máscara de subred.

i. Asegúrese de que la casilla de comprobación vMotion esté seleccionada después de IPv4 Settings.

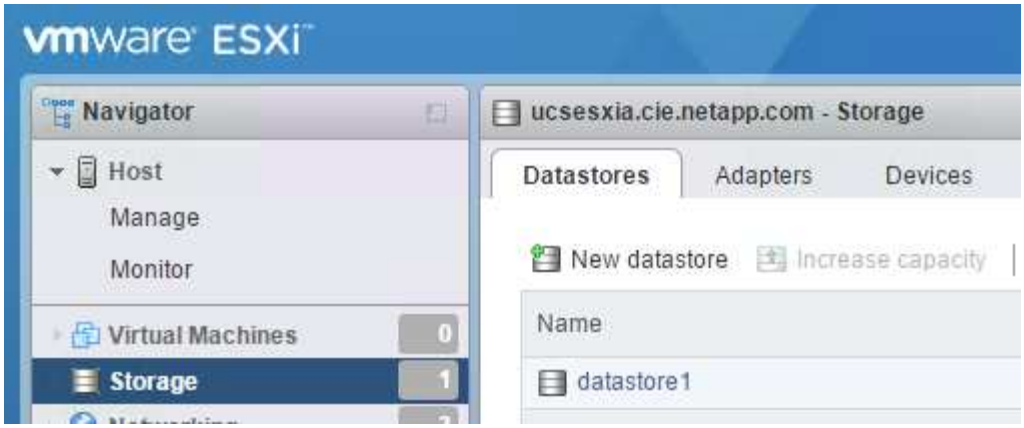


Hay muchas formas de configurar redes ESXi, por ejemplo, mediante el switch distribuido de VMware vSphere si la licencia lo permite. FlexPod Express admite configuraciones de red alternativas si se requieren para satisfacer los requisitos del negocio.

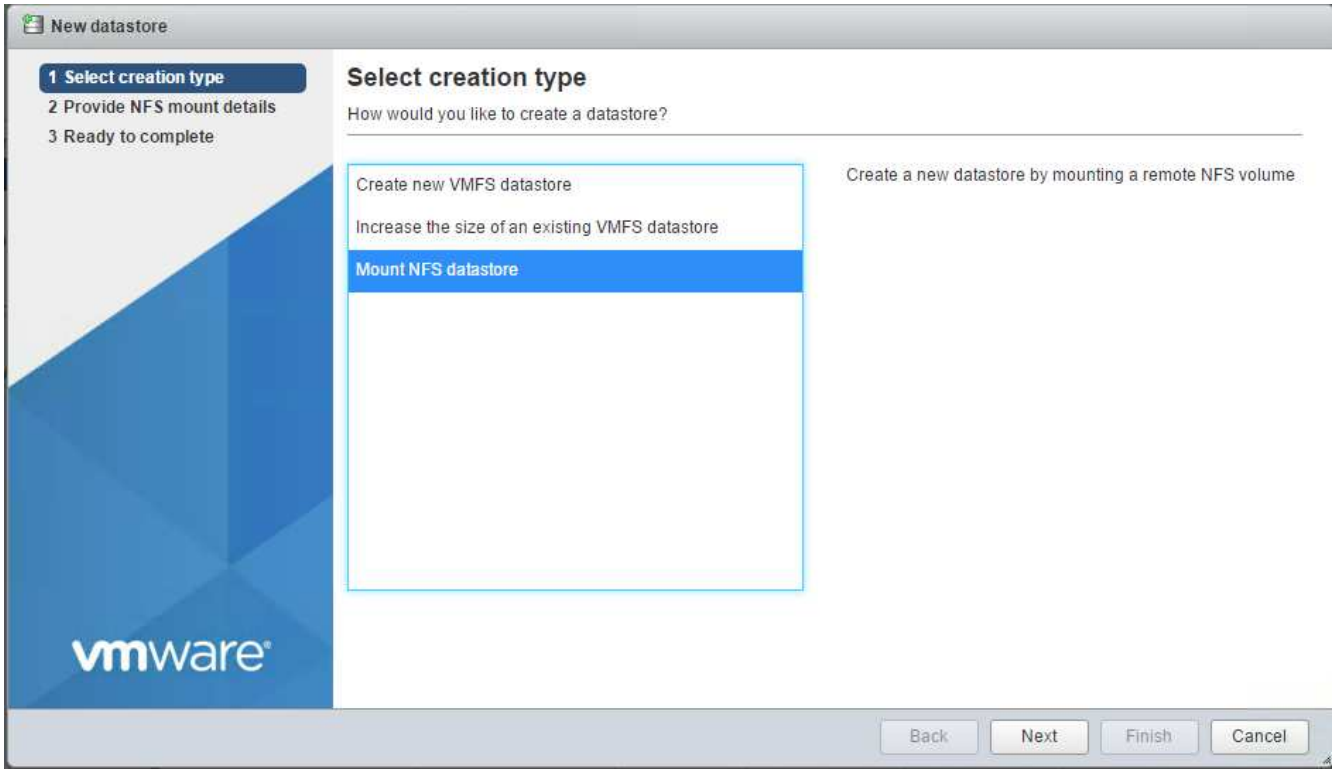
Monte los primeros almacenes de datos

Los primeros almacenes de datos que se van a montar son el `infra_datastore` Almacén de datos para las máquinas virtuales y para `infra_swap` Almacén de datos para archivos de intercambio de equipos virtuales.

1. Haga clic en Storage en el panel de navegación de la izquierda y después haga clic en New Datastore.



2. Seleccione Mount NFS Datastore.



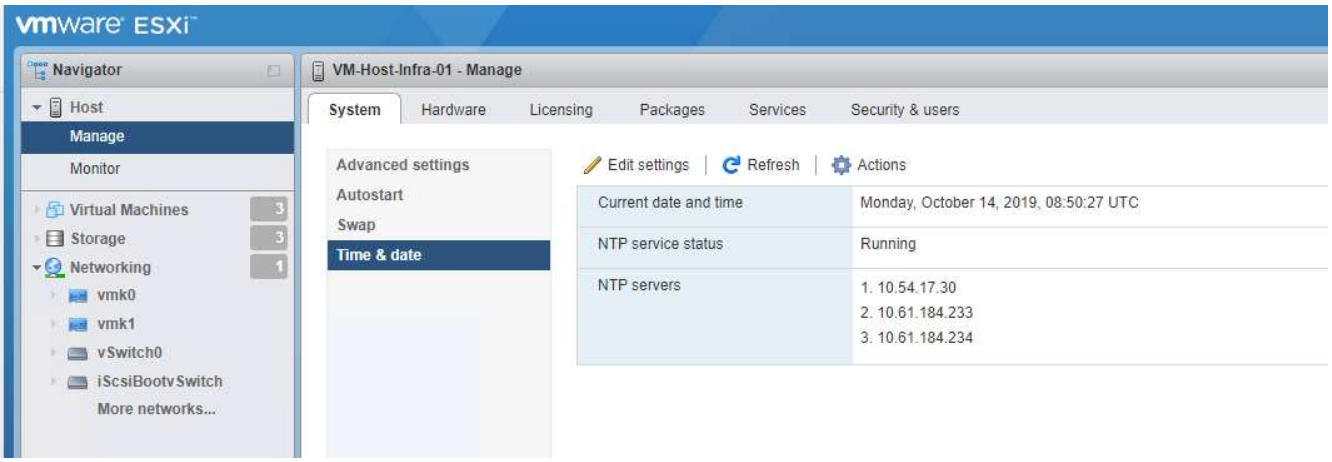
3. Introduzca la siguiente información en la página Provide NFS Mount Details:
   - Nombre: `infra_datastore`
   - Servidor NFS: `<<var_nodea_nfs_lif>>`
   - Compartir: `/infra_datastore`
   - Asegúrese de que la opción NFS 3 esté seleccionada.
4. Haga clic en Finalizar. Puede ver que la tarea se está completando en el panel tareas recientes.
5. Repita este proceso para montar el `infra_swap` almacén de datos:
   - Nombre: `infra_swap`
   - Servidor NFS: `<<var_nodea_nfs_lif>>`
   - Compartir: `/infra_swap`

- Asegúrese de que la opción NFS 3 esté seleccionada.

Configure NTP

Para configurar NTP para un host ESXi, complete los siguientes pasos:

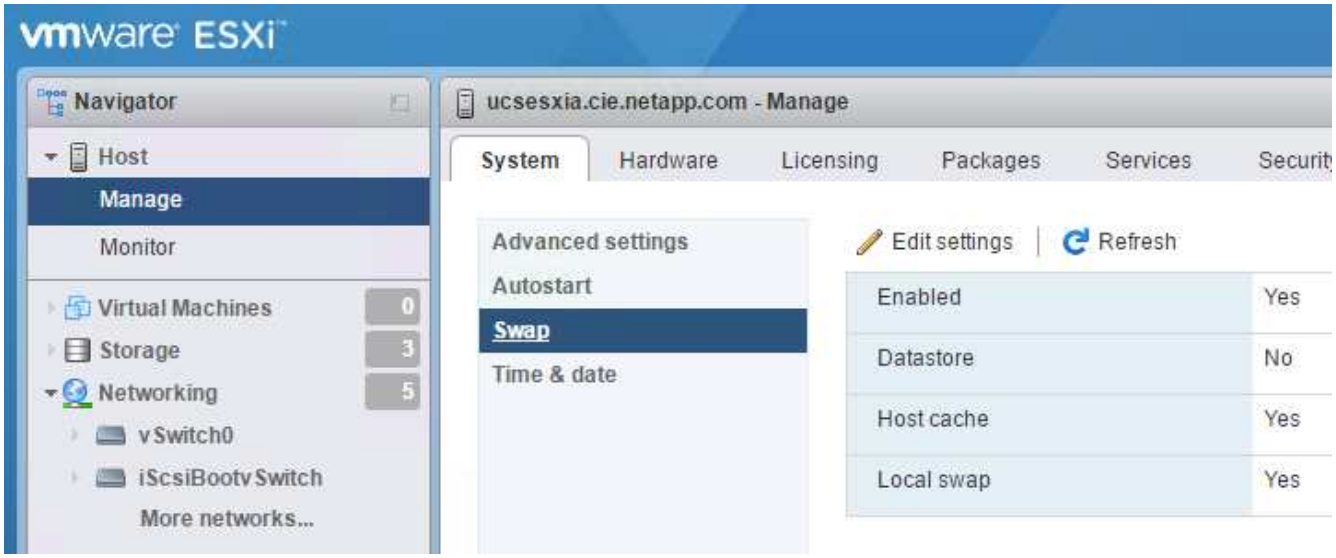
1. Haga clic en Administrar en el panel de navegación de la izquierda. Seleccione sistema en el panel derecho y, a continuación, haga clic en Hora y fecha.
2. Seleccione Use Network Time Protocol (Habilitar cliente NTP).
3. Seleccione Start and Stop with Host como política de inicio del servicio NTP.
4. Introduzca `<<var_ntp>>` Como servidor NTP. Puede establecer varios servidores NTP.
5. Haga clic en Guardar.



Mueva la ubicación del archivo de intercambio de la máquina virtual

Estos pasos proporcionan detalles para mover la ubicación del archivo de intercambio de la máquina virtual.

1. Haga clic en Administrar en el panel de navegación de la izquierda. Seleccione sistema en el panel derecho y, a continuación, haga clic en intercambiar.



2. Haga clic en Editar configuración. Seleccione `infra_swap` En las opciones del Datastore.

3. Haga clic en Guardar.

"Siguiente: Procedimiento de instalación de VMware vCenter Server 6.7U2."

Procedimiento de instalación de VMware vCenter Server 6.7U2

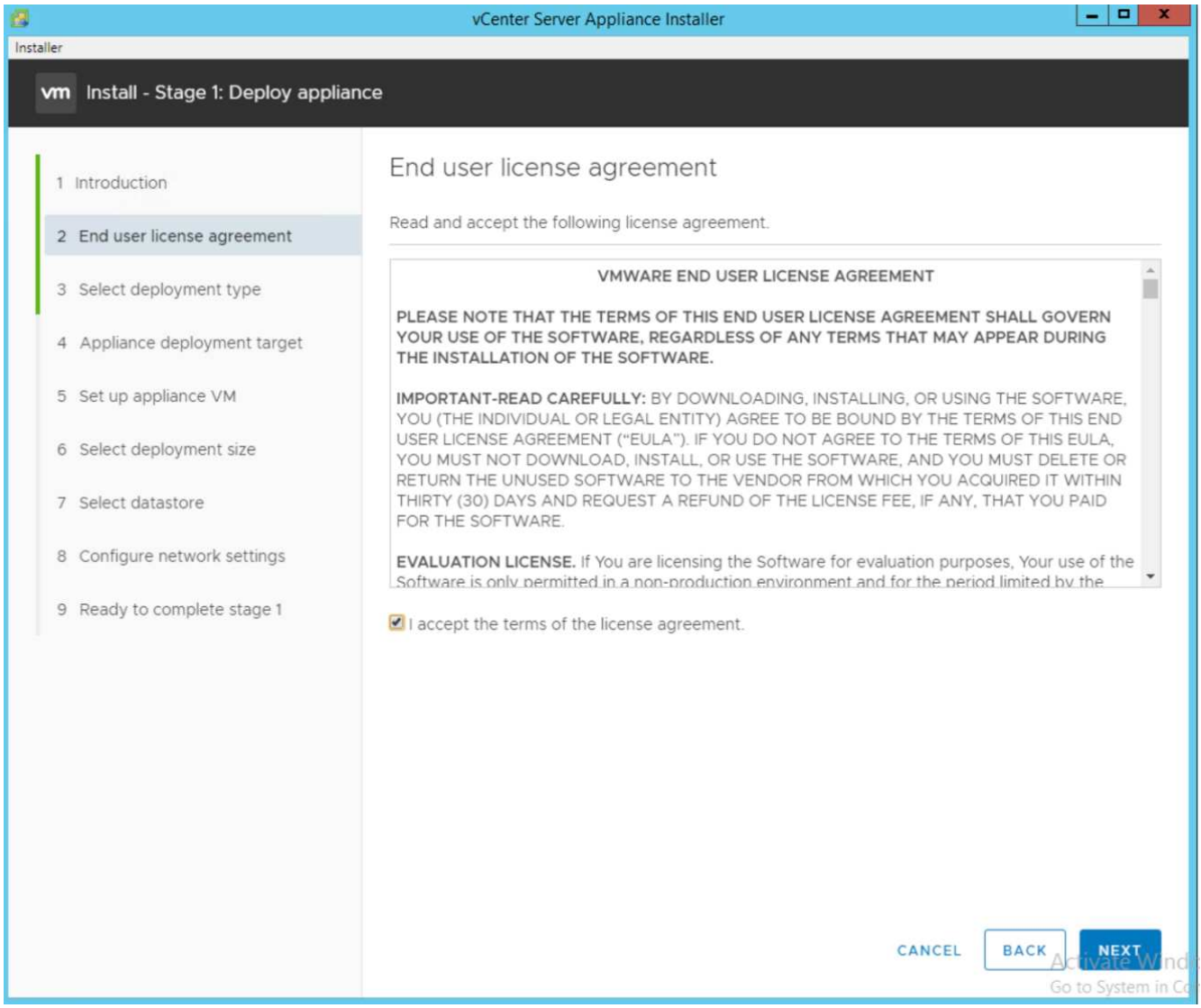
En esta sección, se proporcionan los procedimientos detallados para instalar VMware vCenter Server 6.7 en una configuración exprés de FlexPod.

FlexPod Express utiliza el dispositivo de VMware vCenter Server (VCSA).

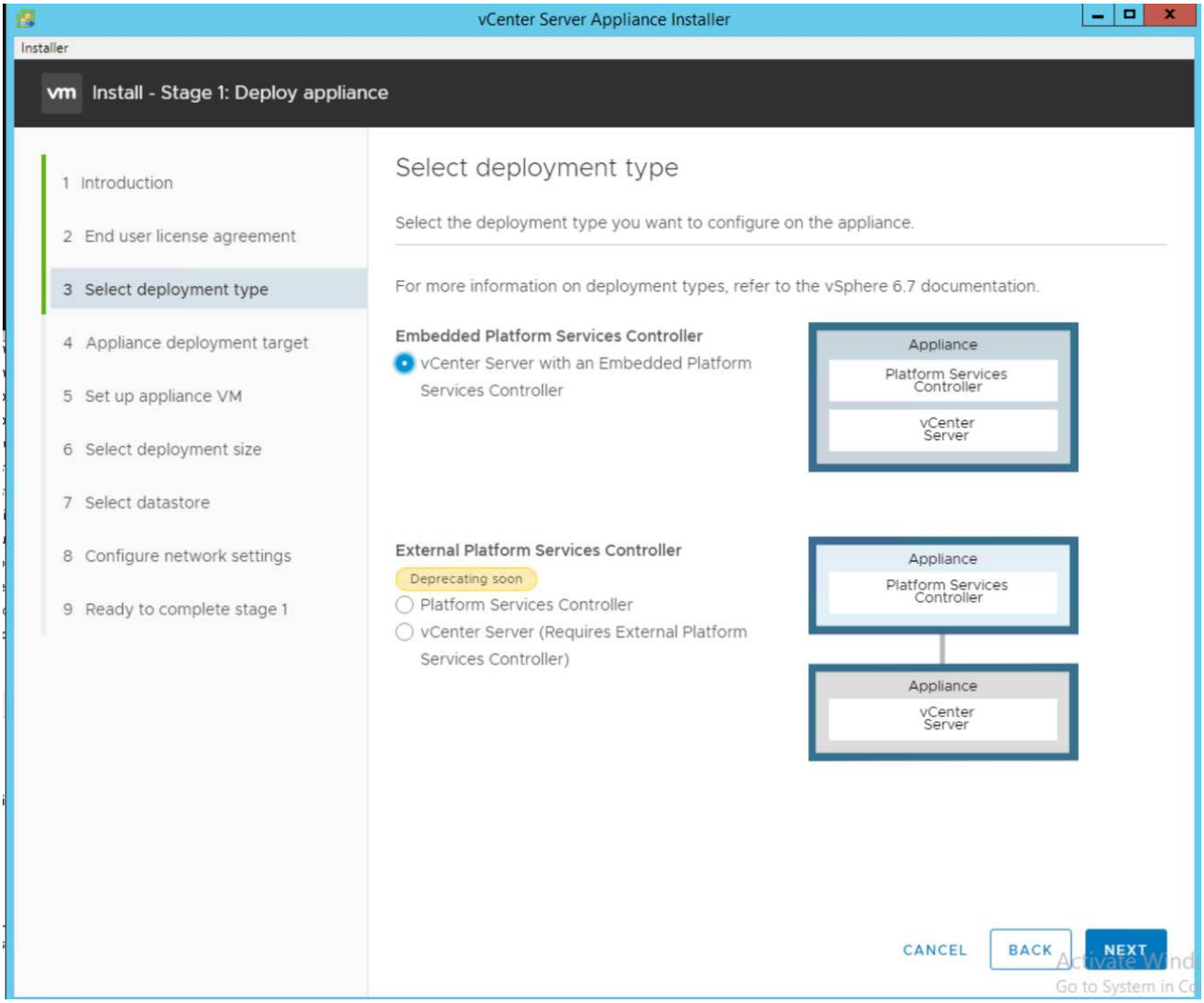
Descargue el dispositivo de VMware vCenter Server

Para descargar el dispositivo de VMware vCenter Server (VCSA), siga los pasos siguientes:

1. Descargue el VCSA. Acceda al enlace de descarga haciendo clic en el icono Get vCenter Server cuando gestione el host ESXi.
2. Descargue el VCSA desde el sitio de VMware.
3. Aunque se admite la instalación de Microsoft Windows vCenter Server, VMware recomienda VCSA para las nuevas implementaciones.
4. Monte la imagen ISO.
5. Vaya al directorio vcsa- ui-installer > win32. Haga doble clic `installer.exe`.
6. Haga clic en instalar.
7. Haga clic en Siguiente en la página Introducción.

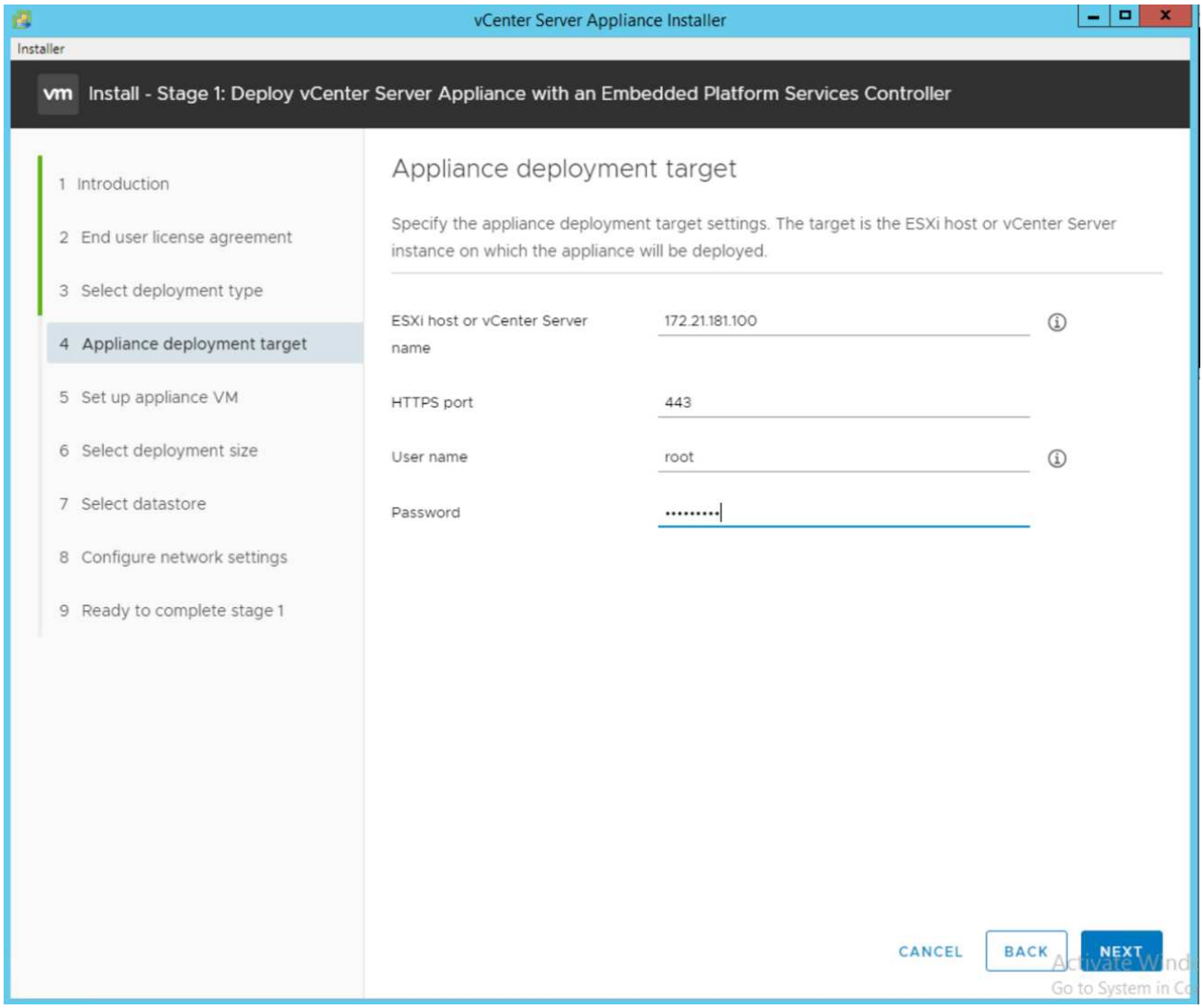


8. Seleccione Embedded Platform Services Controller (controladora de servicios de plataforma integrada) como tipo de implementación.

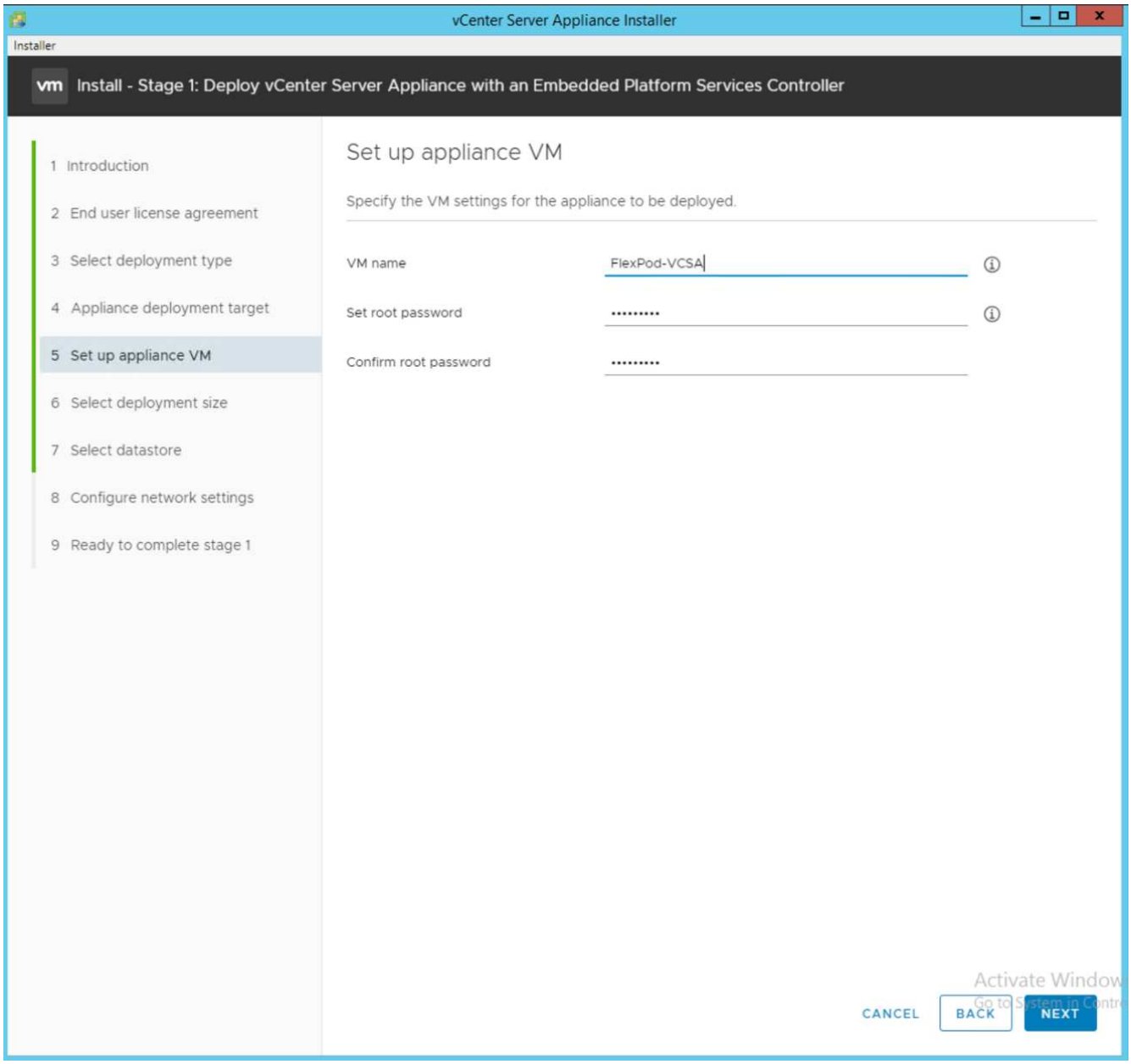


Si es necesario, también admite la puesta en marcha de la controladora de servicios de plataforma externa como parte de la solución FlexPod Express.

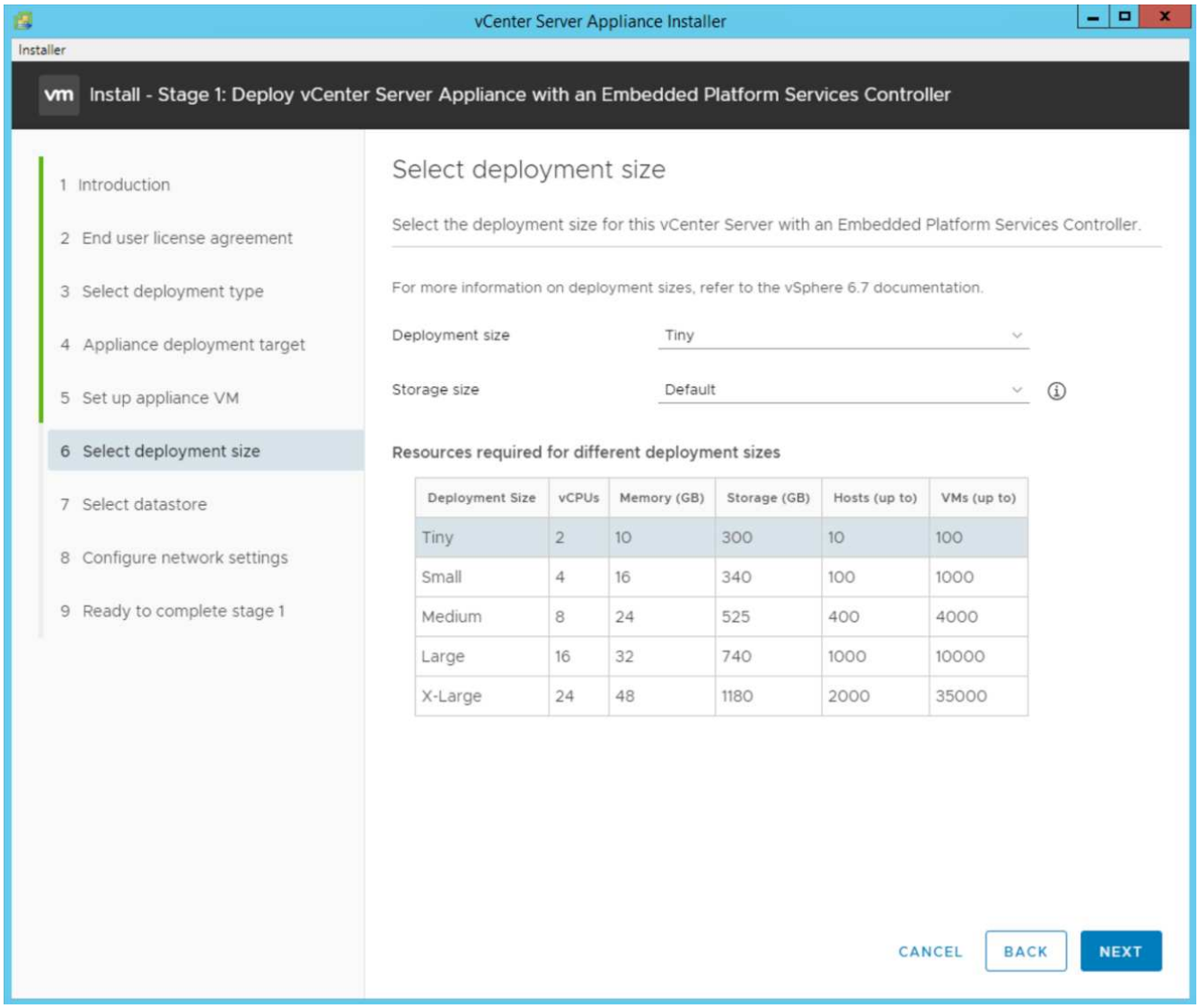
9. En Appliance Deployment Target, introduzca la dirección IP de un host ESXi que haya implementado, el nombre de usuario raíz y la contraseña raíz.



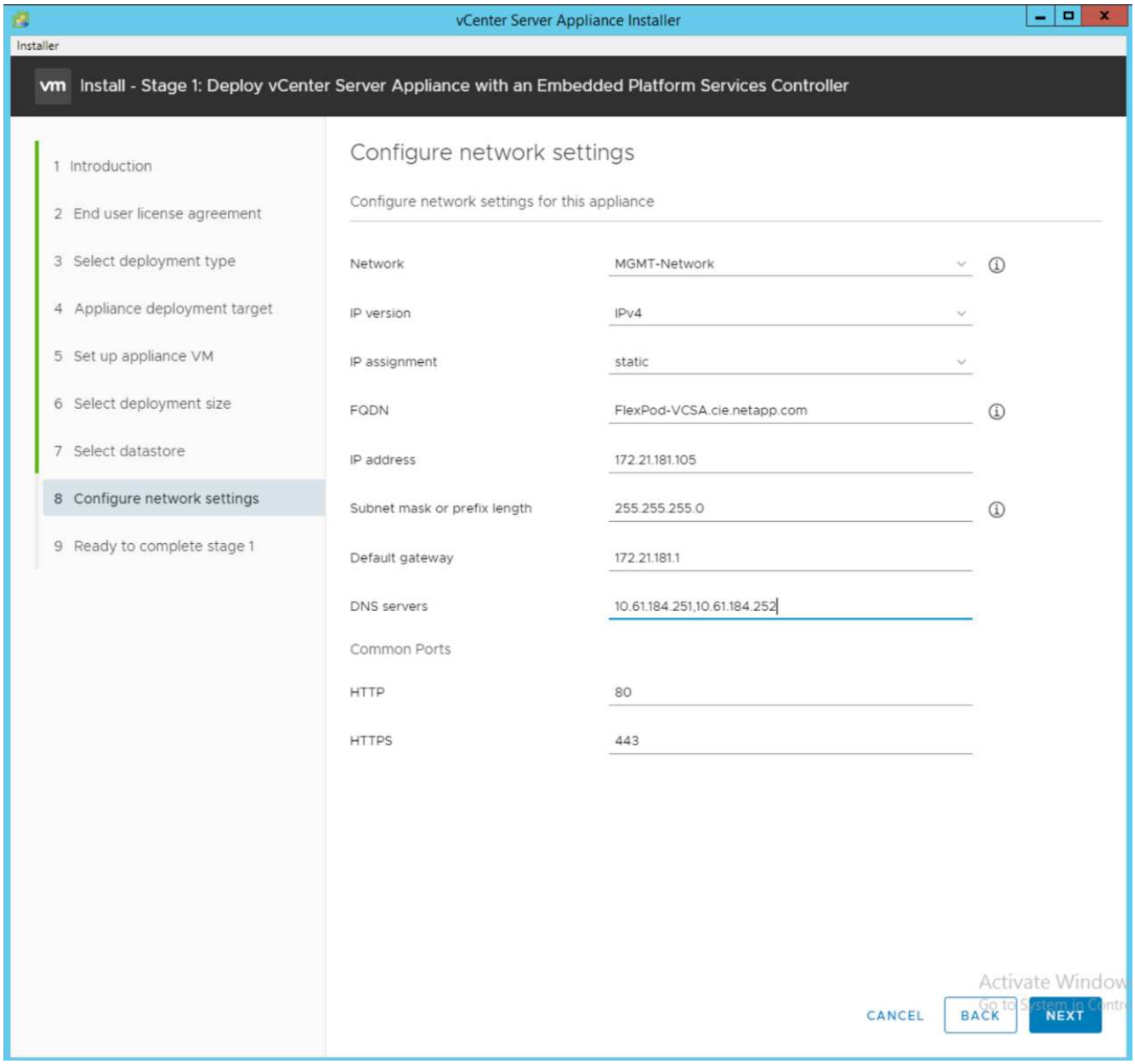
10. Para establecer el equipo virtual, introduzca VCSA como nombre de equipo virtual y la contraseña raíz que desea utilizar para el VCSA.



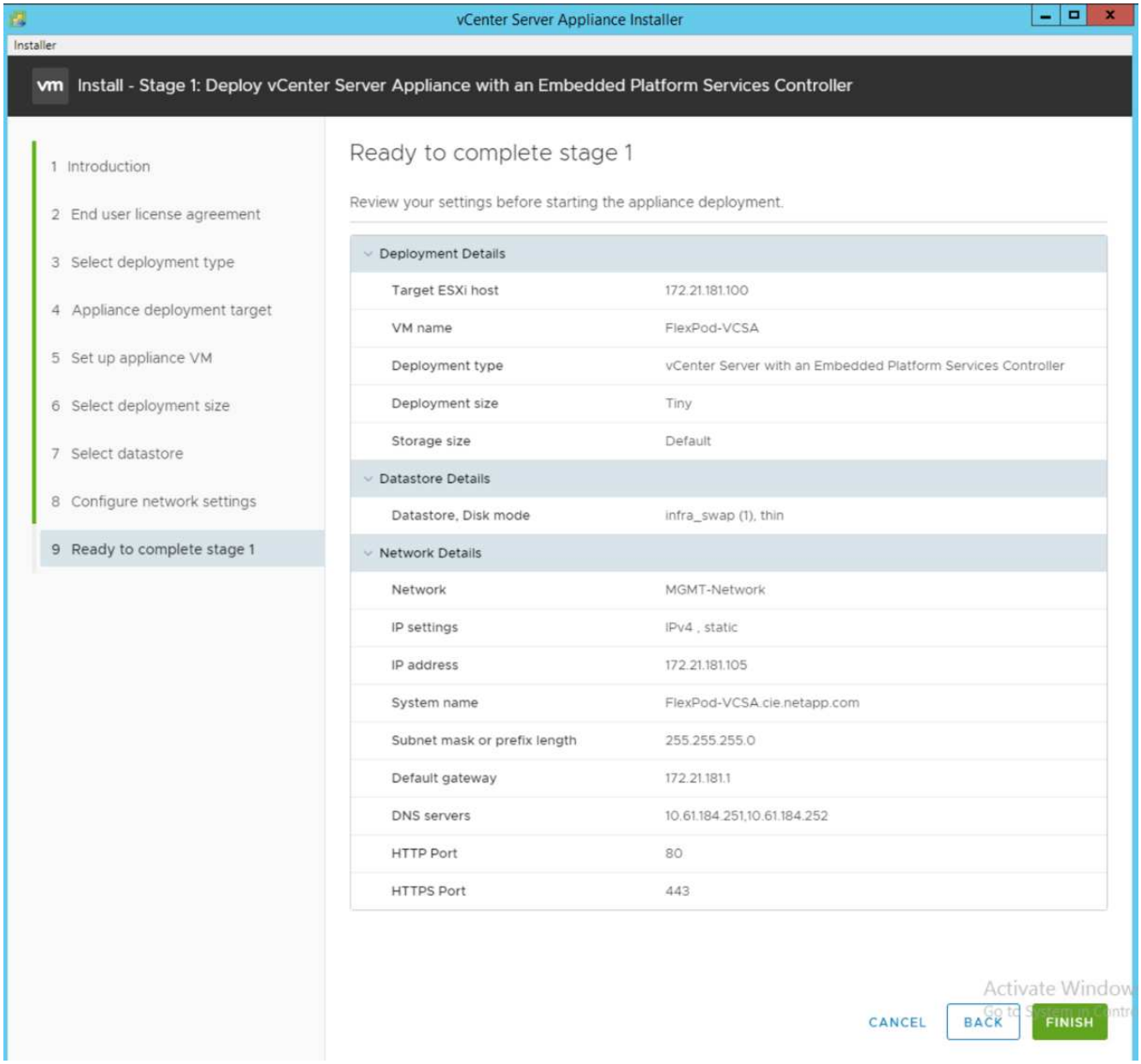
11. Seleccione el tamaño de puesta en marcha que mejor se adapte a su entorno. Haga clic en Siguiente.



12. Seleccione la `infra_datastore` almacén de datos. Haga clic en Siguiente.
13. Introduzca la siguiente información en la página Configure network settings y haga clic en Next.
    a. Seleccione MGMT-Network para Red.
    b. Introduzca el FQDN o IP que se va a utilizar para la VCSA.
    c. Introduzca la dirección IP que se utilizará.
    d. Introduzca la máscara de subred que desea utilizar.
    e. Introduzca la pasarela predeterminada.
    f. Introduzca el servidor DNS.
14. En la página Ready to Complete Stage 1, compruebe que los ajustes introducidos son correctos. Haga clic en Finalizar.

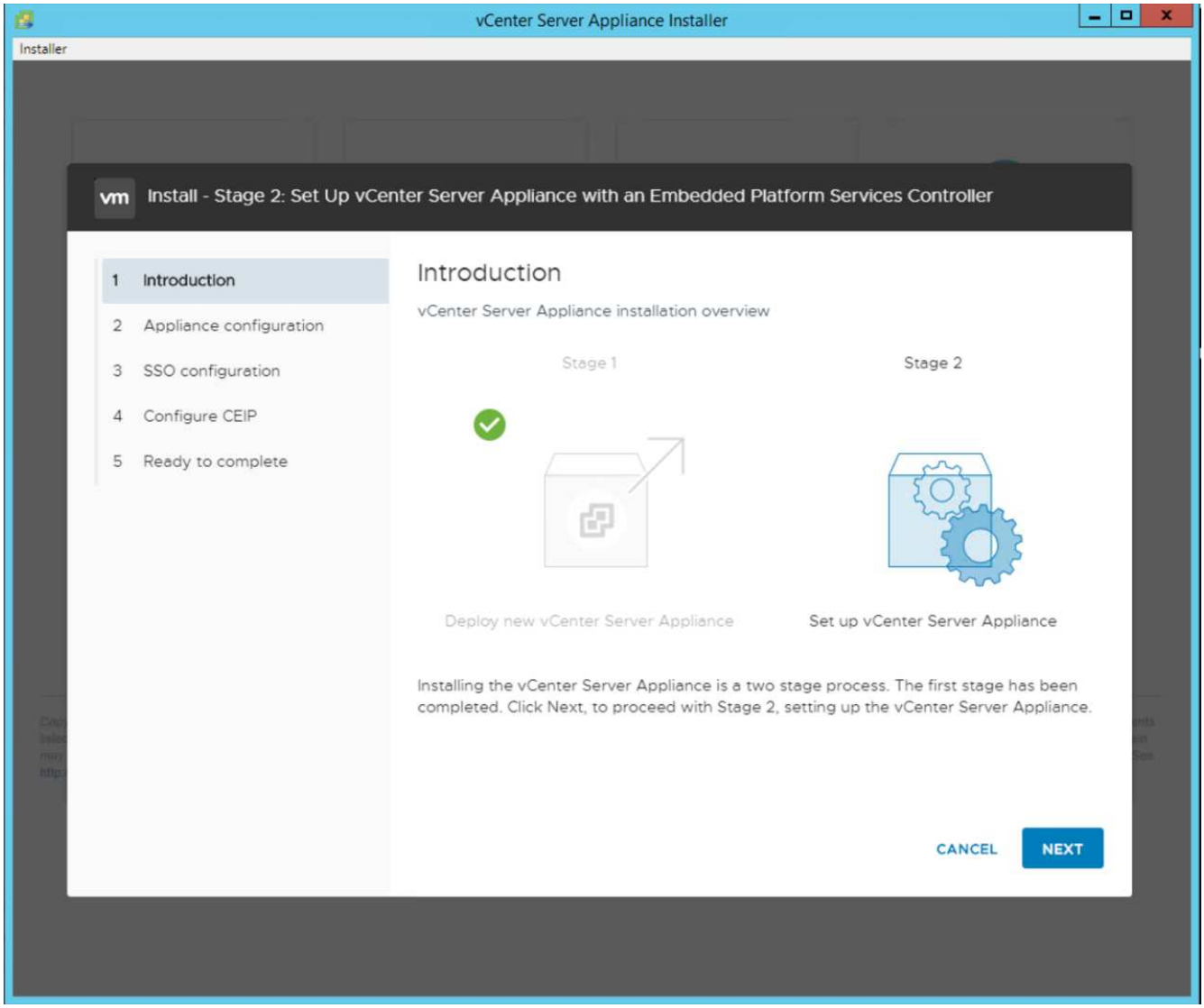


15. Revise la configuración en la etapa 1 antes de iniciar la implementación del dispositivo.

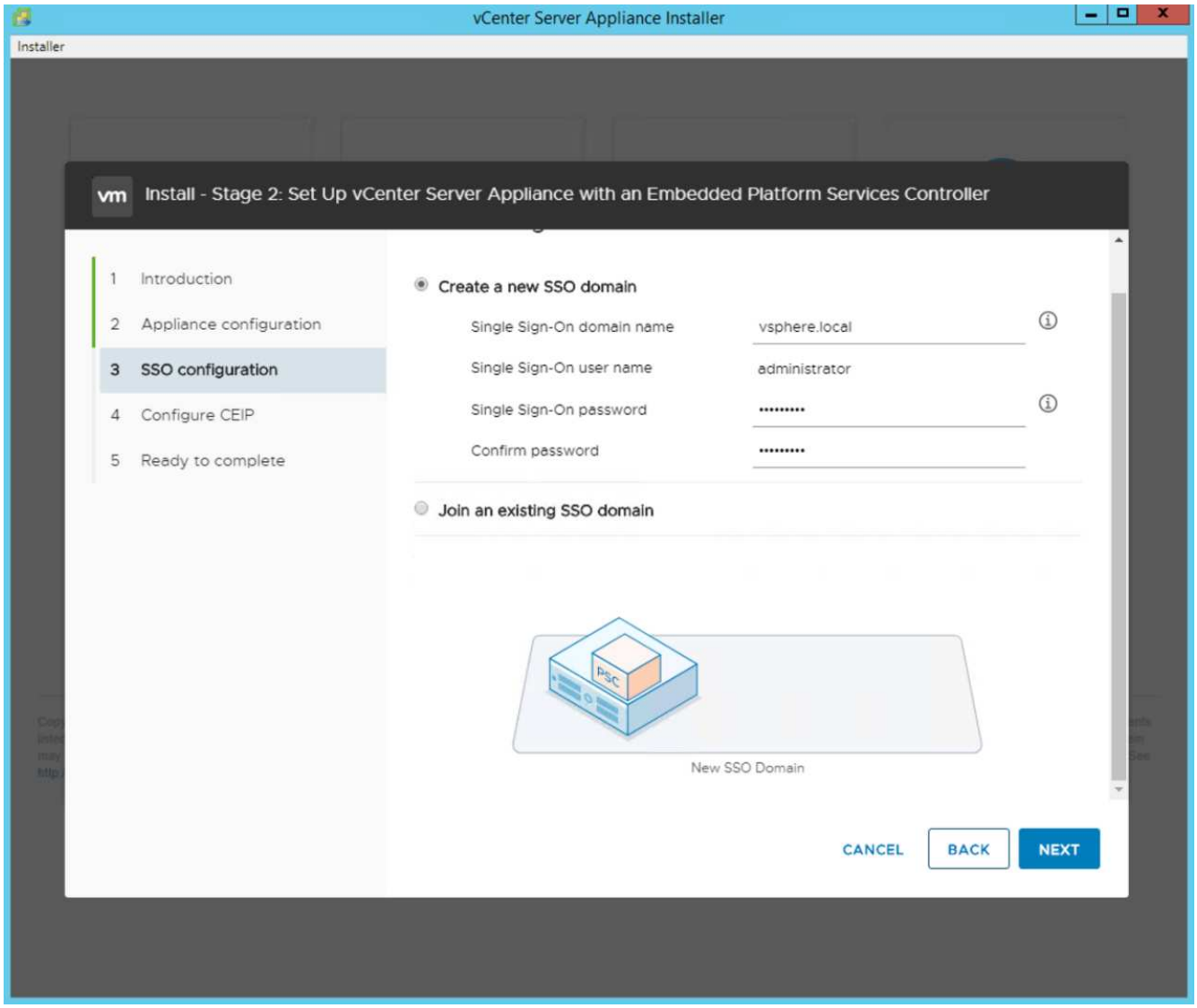


La VCSA se instala ahora. Este proceso tarda varios minutos.

16. Una vez completada la fase 1, aparece un mensaje que indica que se ha completado. Haga clic en continuar para iniciar la configuración de la fase 2.
17. En la página Introducción de fase 2, haga clic en Siguiente.

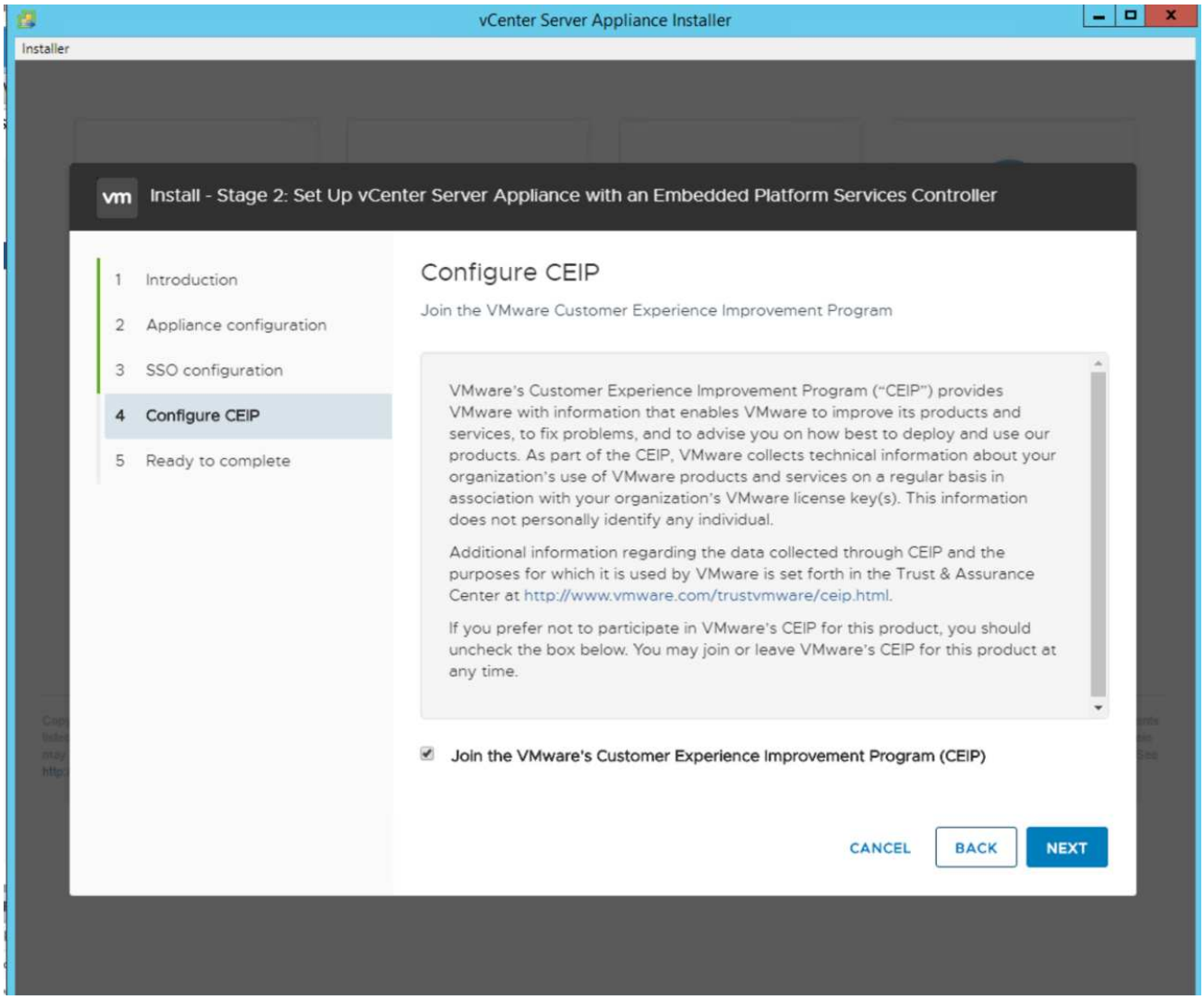


18. Introduzca `<<var_ntp_id>>` Para la dirección del servidor NTP. Puede introducir varias direcciones IP de NTP.
19. Si tiene pensado utilizar la alta disponibilidad (ha) de vCenter Server, asegúrese de que el acceso SSH esté habilitado.
20. Configure el nombre de dominio, la contraseña y el nombre del sitio de SSO. Haga clic en Siguiente.

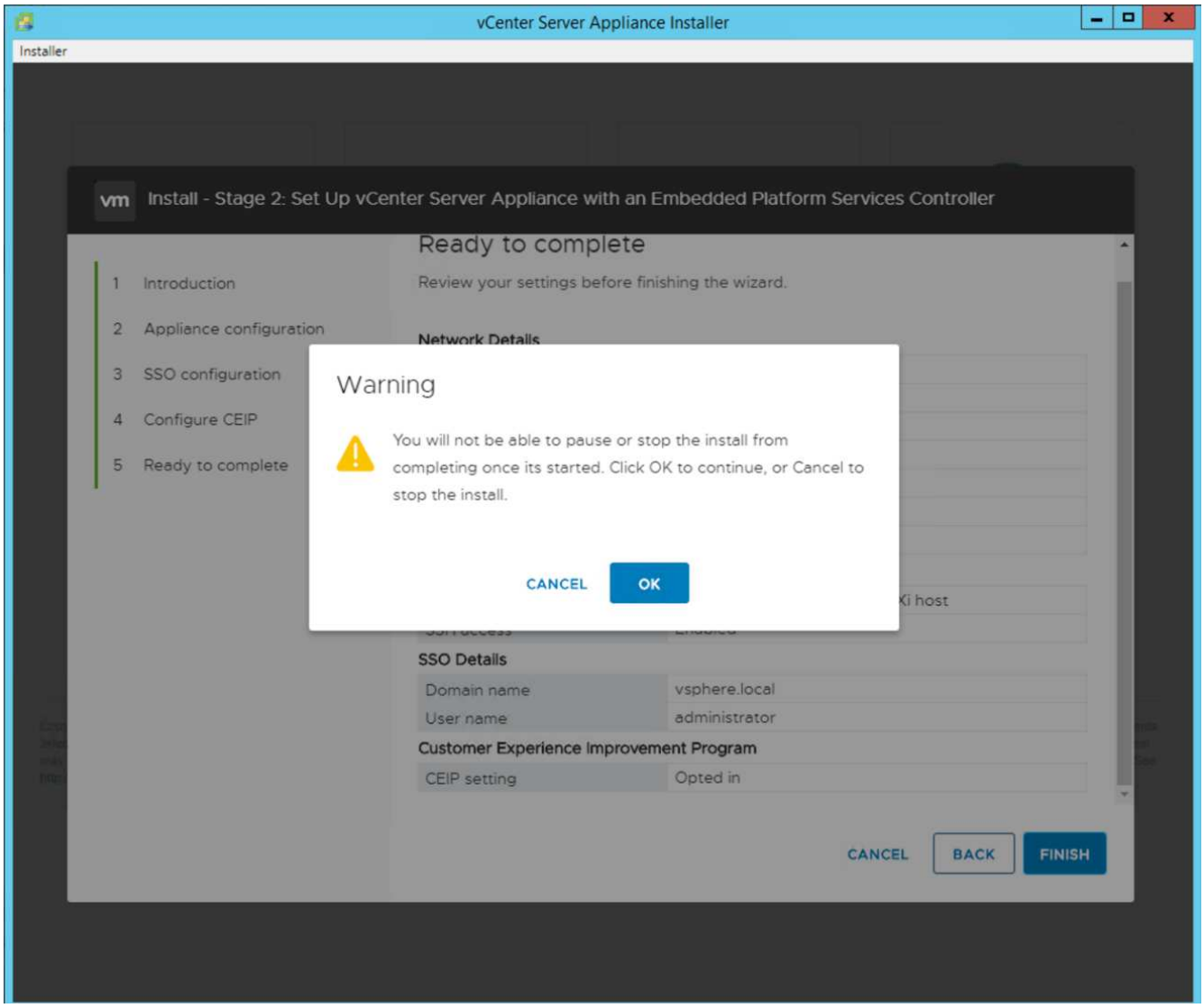


Registre estos valores para su referencia, especialmente si se desvía de la `vsphere.local` nombre de dominio.

21. Únase al programa de experiencia del cliente de VMware si lo desea. Haga clic en Siguiente.



22. Vea el resumen de la configuración. Haga clic en Finalizar o utilice el botón Atrás para editar la configuración.
23. Aparece un mensaje que indica que no podrá detener o detener la instalación una vez iniciada. Haga clic en OK para continuar.



La configuración del dispositivo continúa. Esto tarda varios minutos.

Aparece un mensaje que indica que la configuración se ha realizado correctamente.

24. Los enlaces que el instalador proporciona para acceder a vCenter Server pueden hacer clic.

"Siguiente: Configuración de clustering de VMware vCenter Server 6.7U2 y vSphere."

Configuración de clustering de VMware vCenter Server 6.7U2 y vSphere

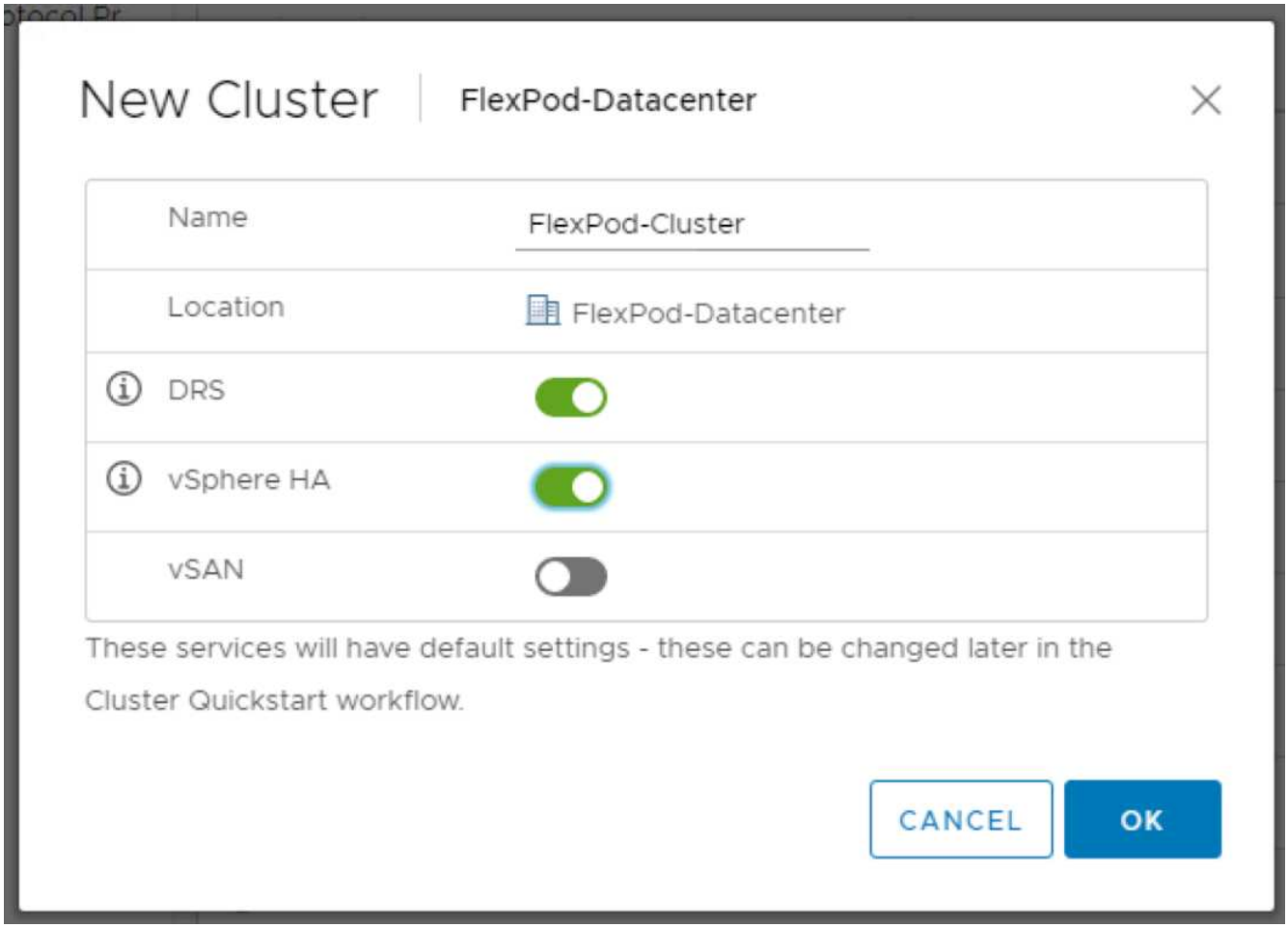
Para configurar la agrupación en clústeres de VMware vCenter Server 6.7 y vSphere, complete los pasos siguientes:

1. Vaya a. `https://<<FQDN or IP of vCenter>>/vsphere-client/`.
2. Haga clic en Launch vSphere Client.
3. Inicie sesión con el nombre de usuario mailto:administrator@vspehre.loc/ tl[Administrator]@vsphere.local y la contraseña SSO que introdujo durante el proceso de configuración de VCSA.
4. Haga clic con el botón derecho en el nombre de vCenter y seleccione New Datacenter.
5. Introduzca un nombre para el centro de datos y haga clic en Aceptar.

Cree un clúster de vSphere

Para crear un clúster de vSphere, complete los siguientes pasos:

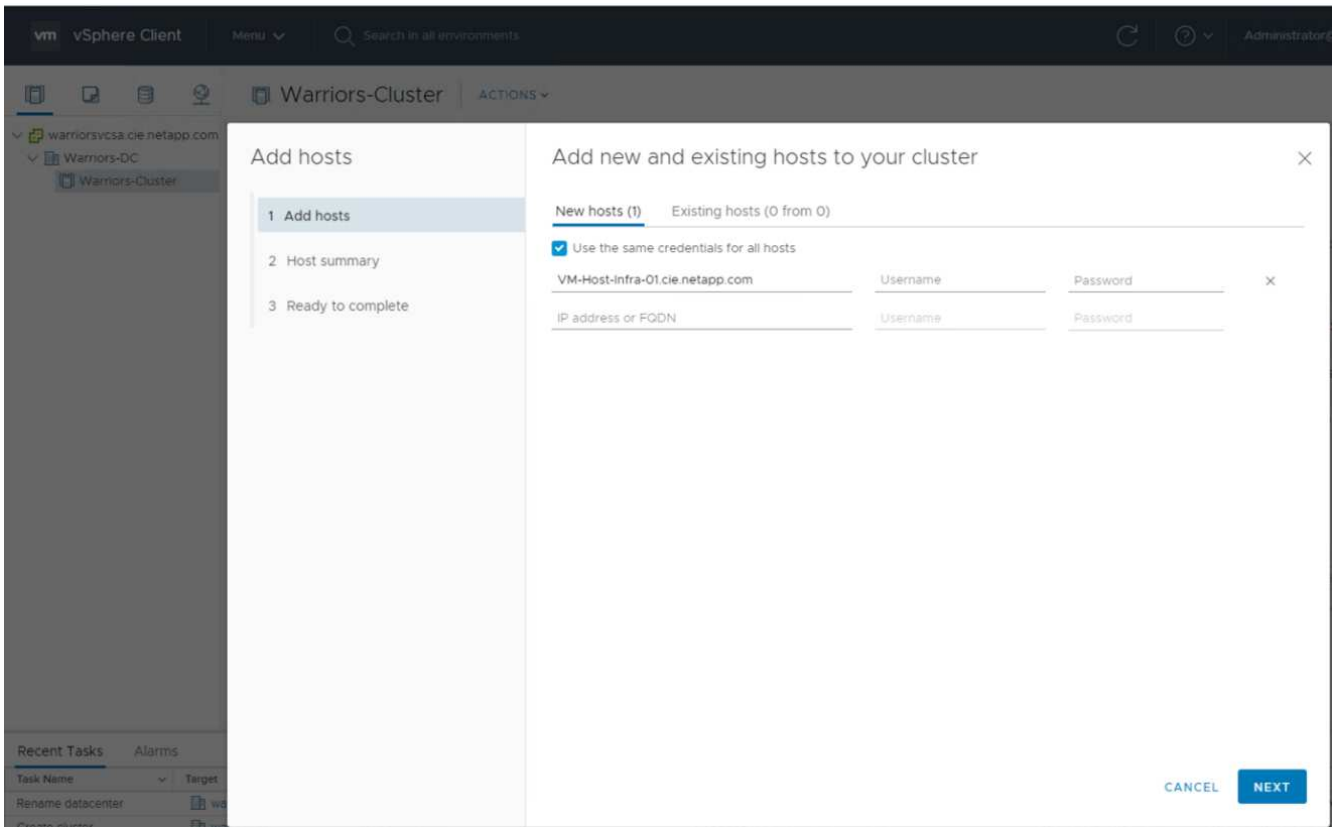
1. Haga clic con el botón derecho en el centro de datos recién creado y seleccione New Cluster.
2. Escriba un nombre para el clúster.
3. Active la recuperación ante desastres y vSphere ha seleccionando las casillas de verificación.
4. Haga clic en Aceptar.



Añada los hosts ESXi al clúster

Para añadir los hosts ESXi al clúster, complete los siguientes pasos:

1. Haga clic con el botón derecho en el clúster y seleccione Add Host.



2. Para añadir un host ESXi al clúster, complete los siguientes pasos:
   a. Introduzca la dirección IP o el FQDN del host. Haga clic en Siguiente.
   b. Introduzca el nombre de usuario raíz y la contraseña. Haga clic en Siguiente.
   c. Haga clic en Sí para reemplazar el certificado del host por un certificado firmado por el servidor de certificados VMware.
   d. Haga clic en Siguiente en la página Resumen de host.
   e. Haga clic en el icono verde + para añadir una licencia al host de vSphere.
3. Este paso se puede completar más adelante si se desea.
   a. Haga clic en Siguiente para desactivar el modo de bloqueo.
   b. Haga clic en Next en la página de ubicación de la máquina virtual.
   c. Revise la página Listo para completar. Utilice el botón Atrás para realizar cualquier cambio o seleccione Finalizar.
4. Repita los pasos 1 y 2 para el host Cisco UCS B.

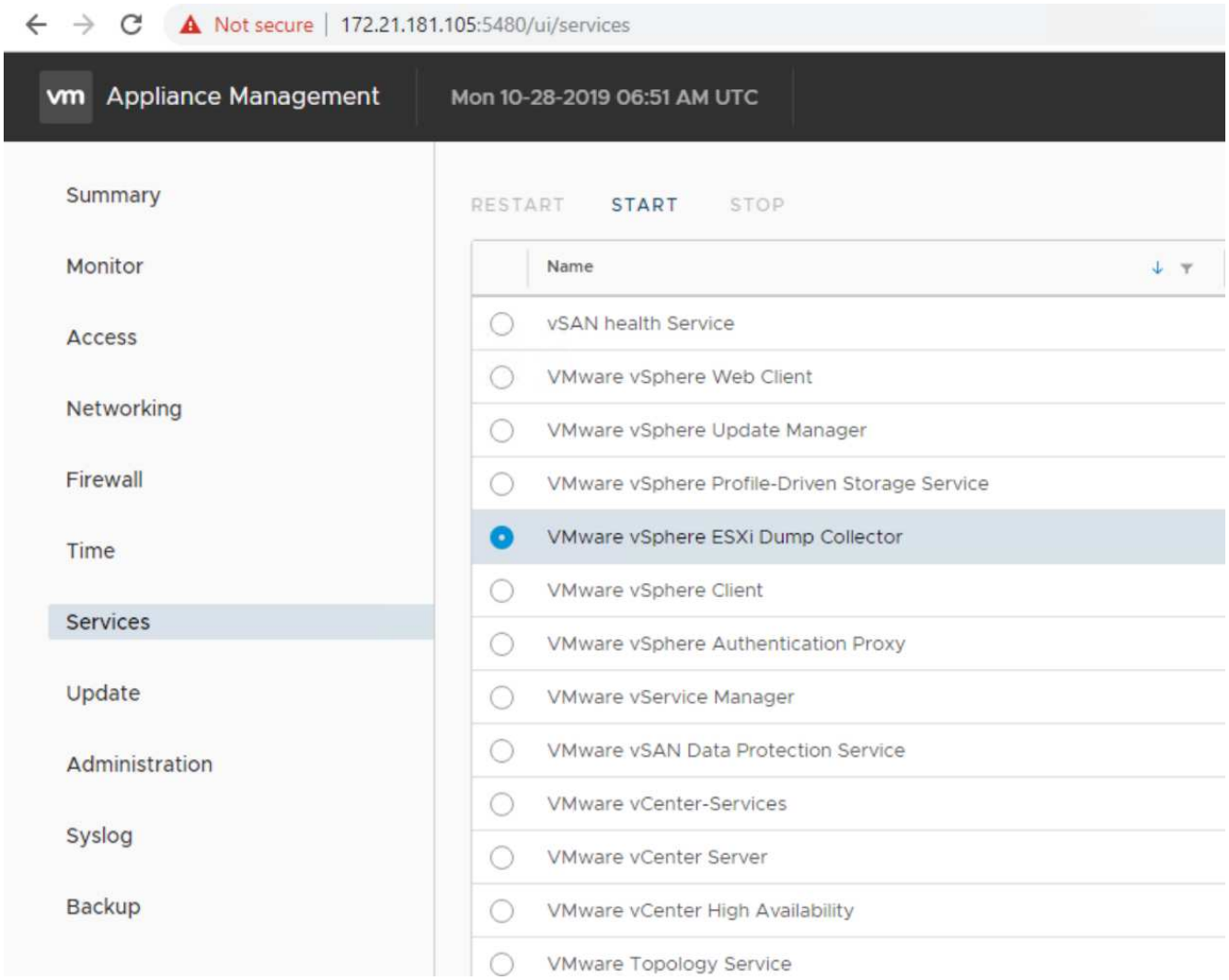
> Debe completar este proceso para los hosts adicionales que se agreguen a la configuración exprés de FlexPod.

Configure coredump en hosts ESXi

Para configurar coredump en hosts ESXi, complete los siguientes pasos:

1. Inicie sesión en https:// "VCenter" IP:5480/, escriba root para el nombre de usuario e introduzca la contraseña de root.

2. Haga clic en Services y seleccione VMware vSphere ESXI Dump collector.
3. Inicie el servicio de recopilador DE volcado DE ESXI de VMware vSphere.



4. Utilice SSH, conéctese al host ESXi de IP de gestión, introduzca root para el nombre de usuario e introduzca la contraseña raíz.
5. Ejecute los siguientes comandos:

```
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. El mensaje `Verified the configured netdump server is running` aparece después de introducir el comando final.

```
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
erified the configured netdump server is running
```

Este proceso debe completarse para cualquier host adicional que se añada a FlexPod Express.

`ip_address_of_core_dump_collector` En esta validación está la IP de vCenter.

"Siguiente: Procedimientos de puesta en marcha de Virtual Storage Console 9,6 de NetApp."

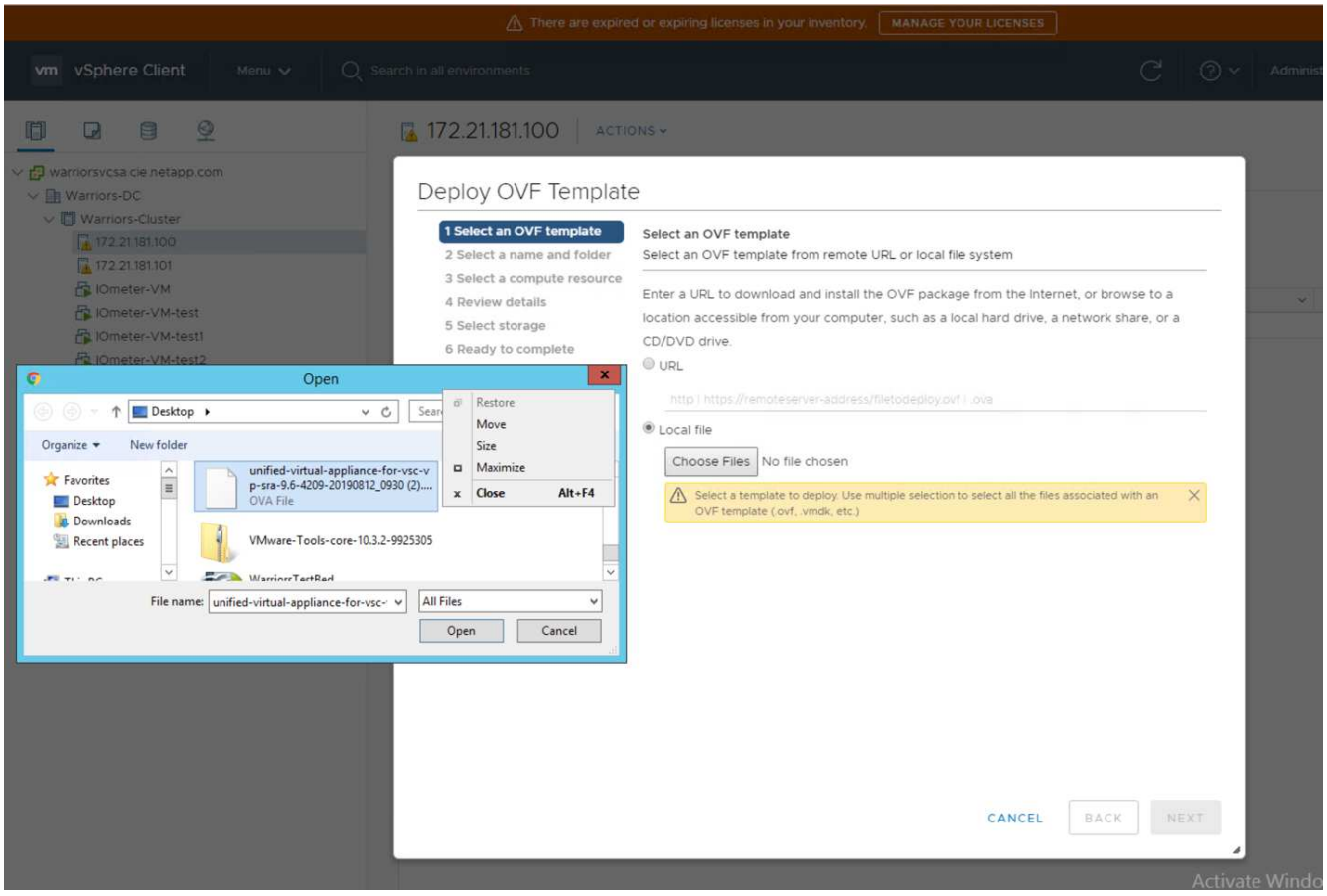
Procedimientos de puesta en marcha de Virtual Storage Console 9.6 de NetApp

En esta sección se describen los procedimientos de puesta en marcha de Virtual Storage Console (VSC) de NetApp.

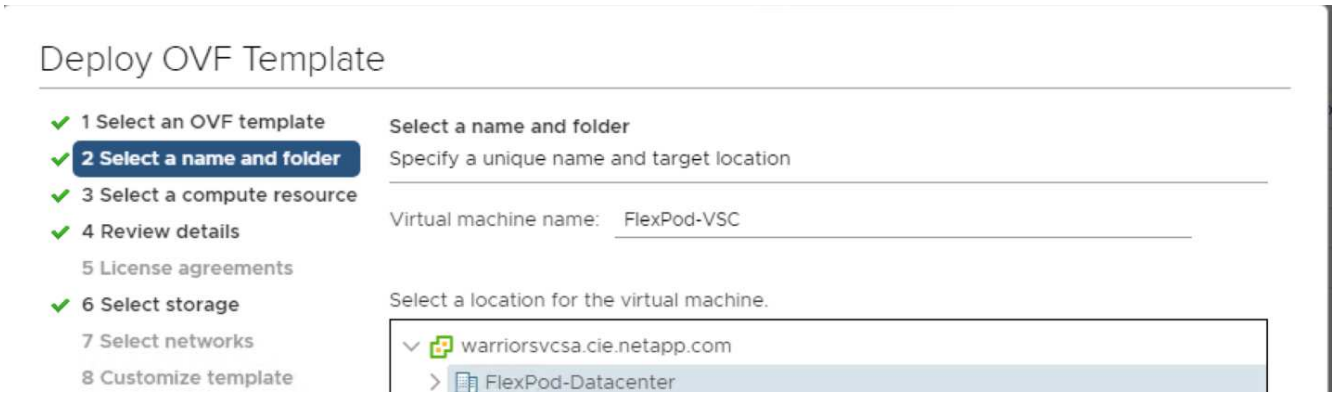
Instalar Virtual Storage Console 9.6

Para instalar el software VSC 9.6 mediante una implementación de formato de virtualización abierta (OVF), siga estos pasos:

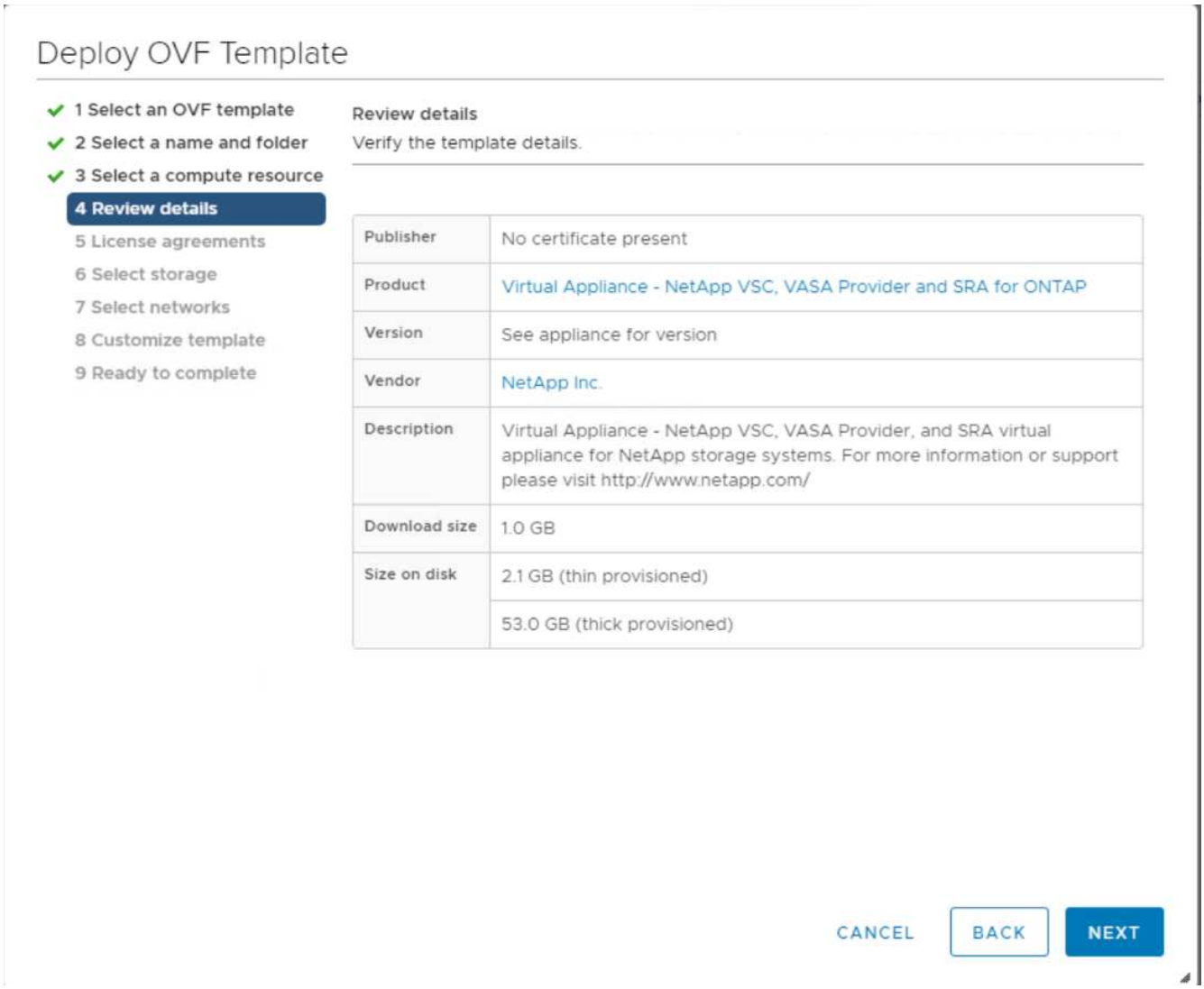
1. Vaya a vSphere Web Client > Host Cluster > Deploy OVF Template.
2. Desplácese hasta el archivo OVF de VSC descargado del sitio de soporte de NetApp.



3. Introduzca el nombre de la máquina virtual y seleccione el centro de datos o la carpeta en la que desea implementar. Haga clic en Siguiente.

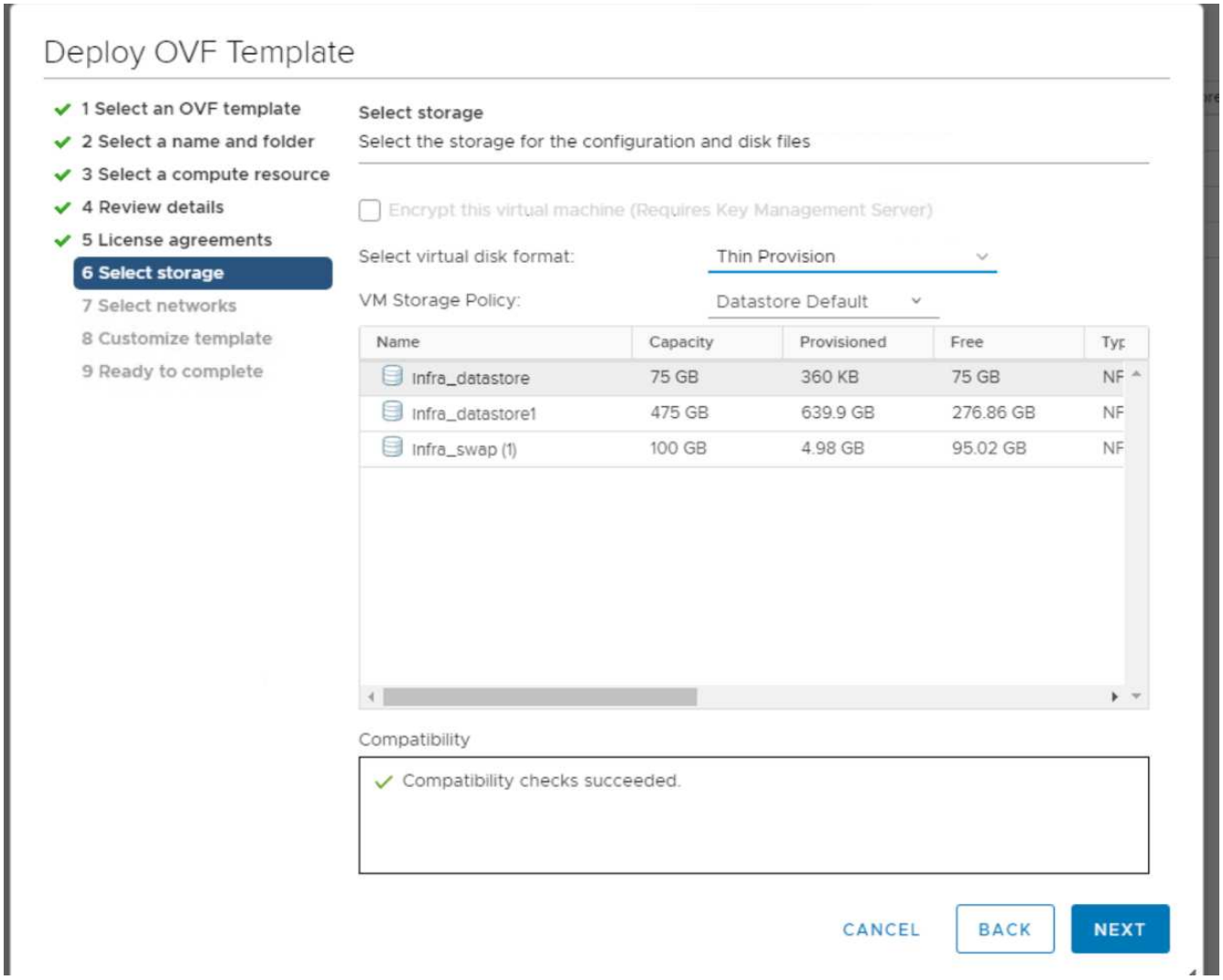


4. Seleccione el clúster FlexPod-Cluster ESXi y haga clic en Next.
5. Revise los detalles y haga clic en Next.

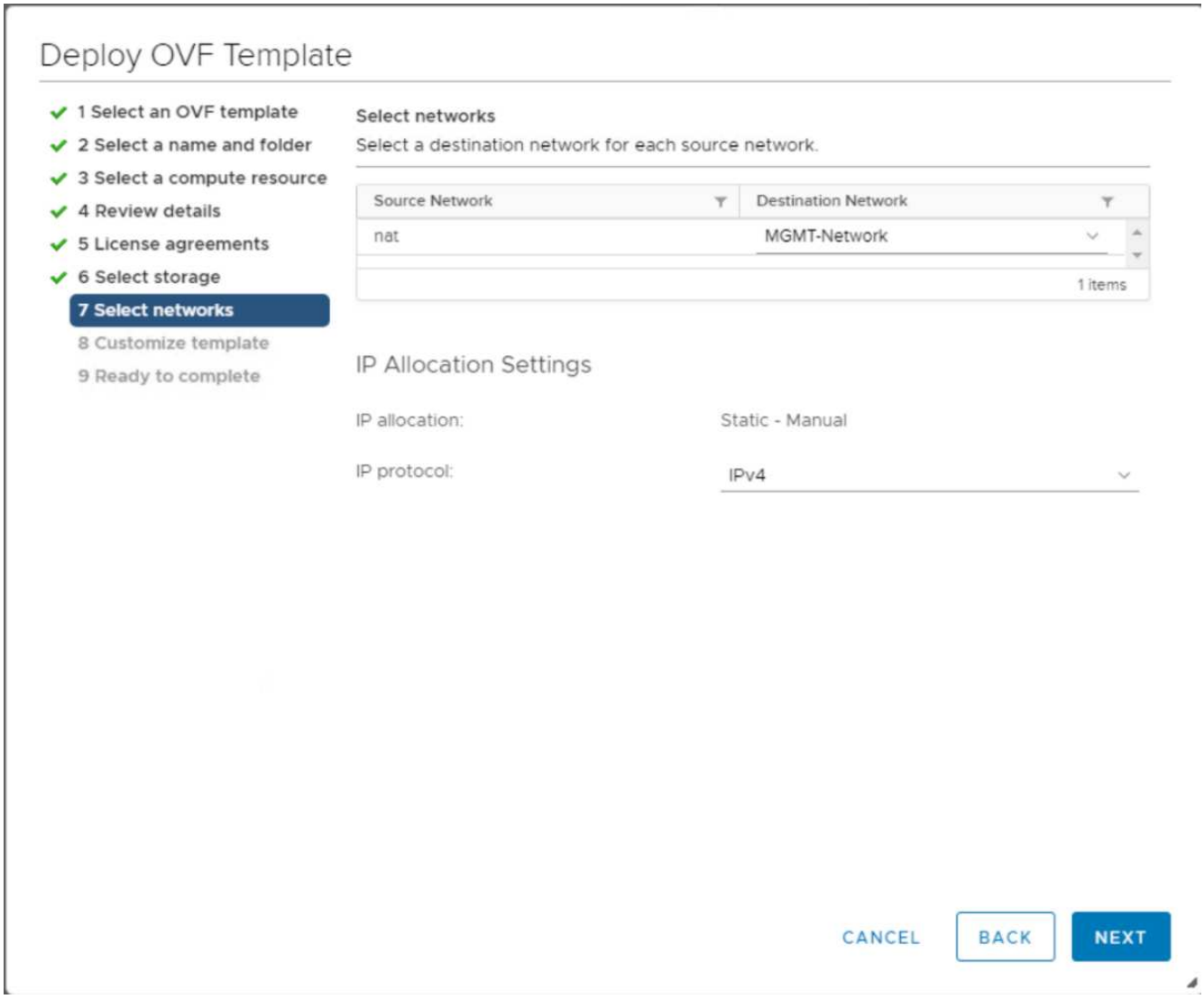


6. Haga clic en Aceptar para aceptar la licencia y haga clic en Siguiente.
7. Seleccione el formato de disco virtual de thin provisioning y uno de los almacenes de datos NFS. Haga clic

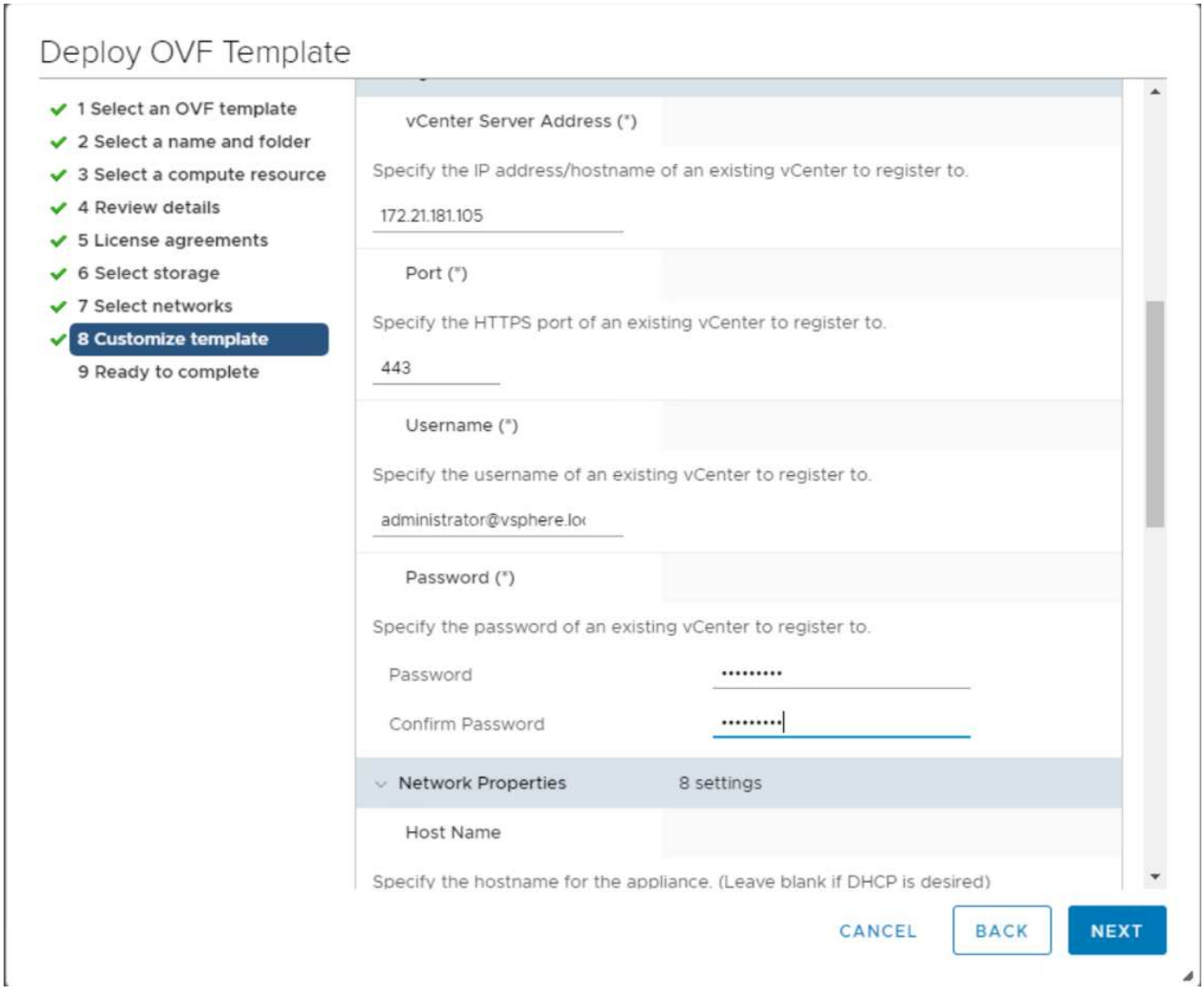
en Siguiente.



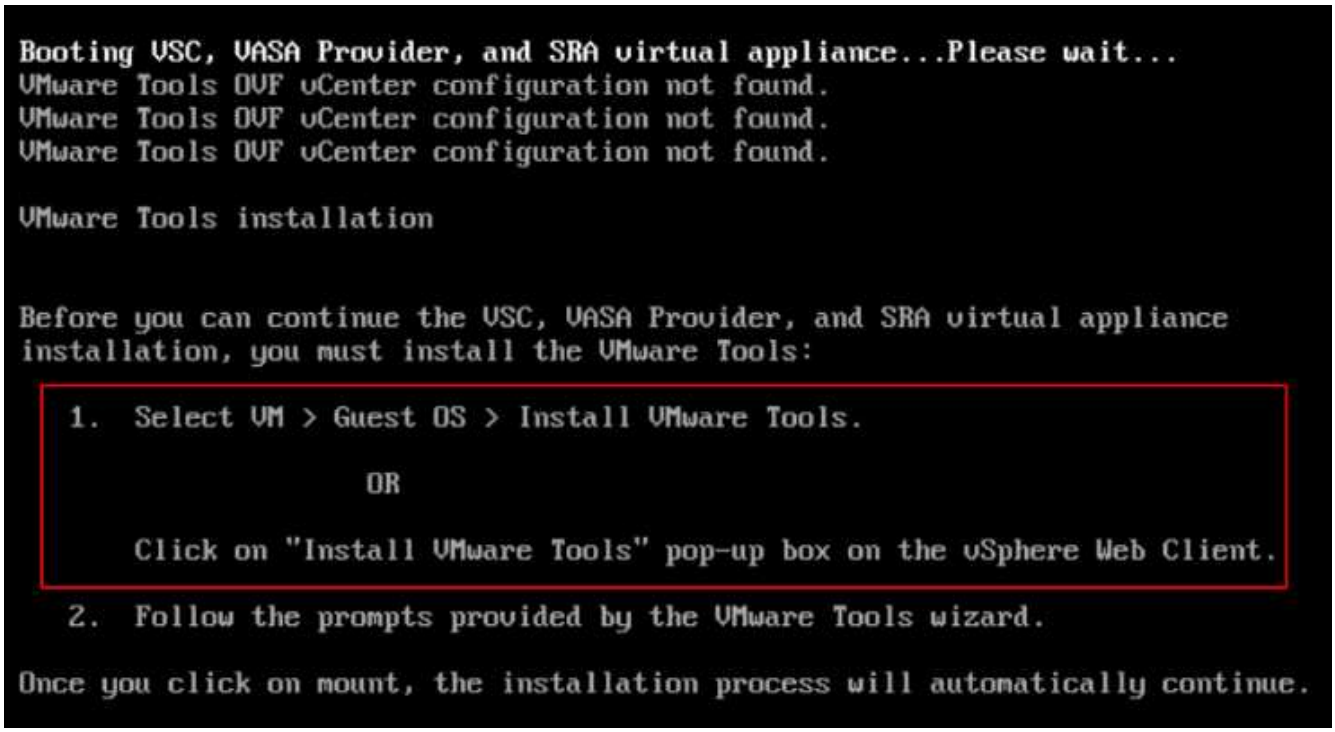
8. En Seleccionar redes, elija una red de destino y haga clic en Siguiente.



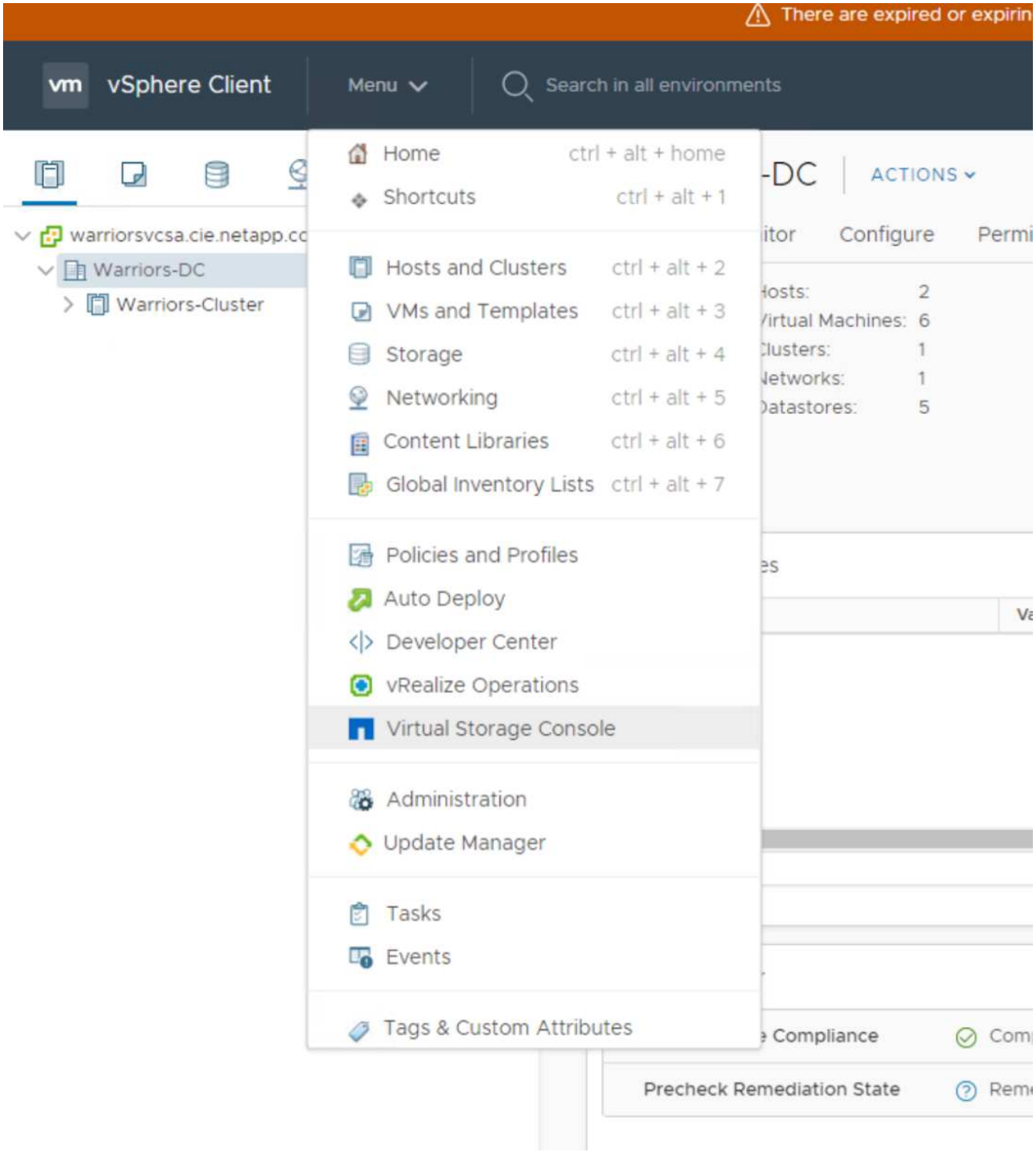
9. En Customize Template, introduzca la contraseña del administrador de VSC, el nombre o la dirección IP de vCenter y otros detalles de la configuración, y haga clic en Next.



10. Revise los detalles de la configuración introducidos y haga clic en Finish para completar la puesta en marcha de la máquina virtual de NetApp-VSC.
11. Encienda la máquina virtual de NetApp-VSC y abra la consola de equipos virtuales.
12. Durante el proceso de arranque de máquinas virtuales NetApp-VSC, verá un aviso para instalar las herramientas de VMware. En vCenter, seleccione NetApp-VSC VM > SO invitado > instalar VMware Tools.



13. La información de registro de vCenter y la configuración de la red se proporcionó durante la personalización de la plantilla OVF. Por lo tanto, una vez que se ejecuta la máquina virtual de NetApp-VSC, VSC, las API de vSphere para el reconocimiento del almacenamiento (VASA) y el adaptador de replicación de almacenamiento (SRA) de VMware se registran en vCenter.
14. Cierre la sesión en vCenter Client y vuelva a iniciarla. En el menú Inicio, confirme que VSC de NetApp está instalado.



Descargue e instale el complemento VAAI para NFS de NetApp

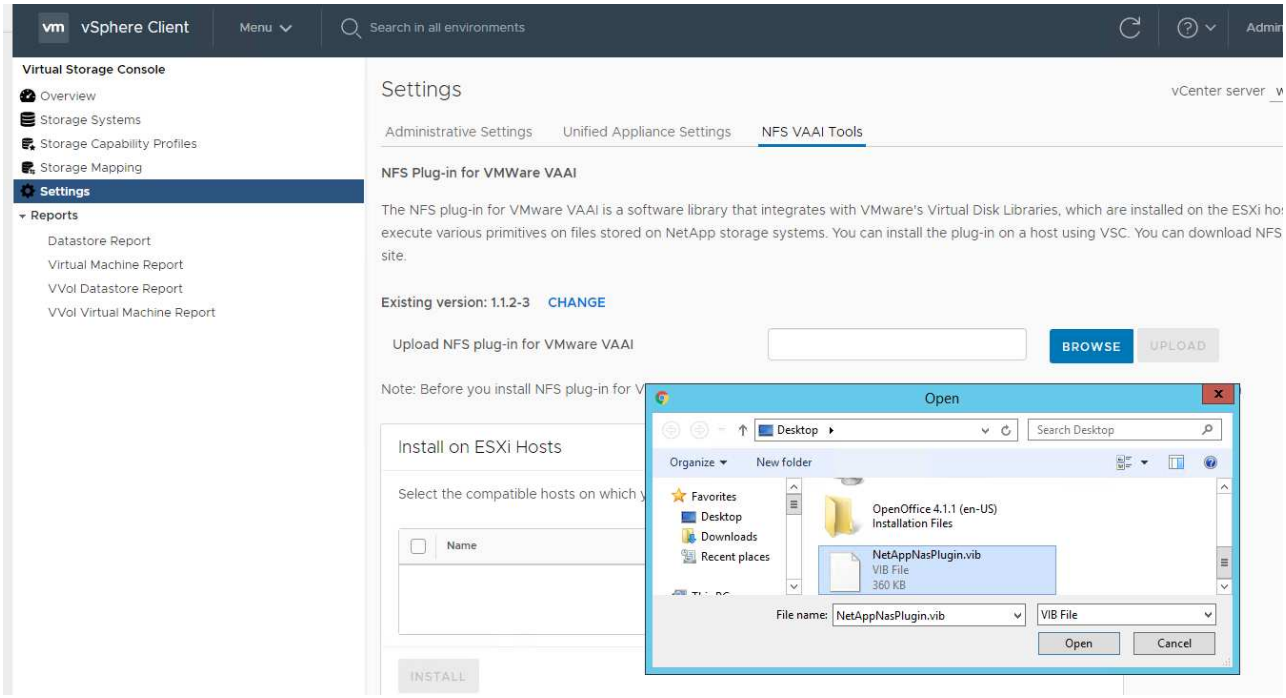
Para descargar e instalar el complemento VAAI para NFS de NetApp, complete los siguientes pasos:

1. Descargue el complemento NFS de NetApp 1.1.2 para VMware `.vib` Archivo desde la página de descarga del complemento NFS y guárdelo en el equipo local o en el host de administración.
2. Descargue el plugin de NetApp NFS para VMware VAAI:
   a. Vaya a la "página de descarga del software".

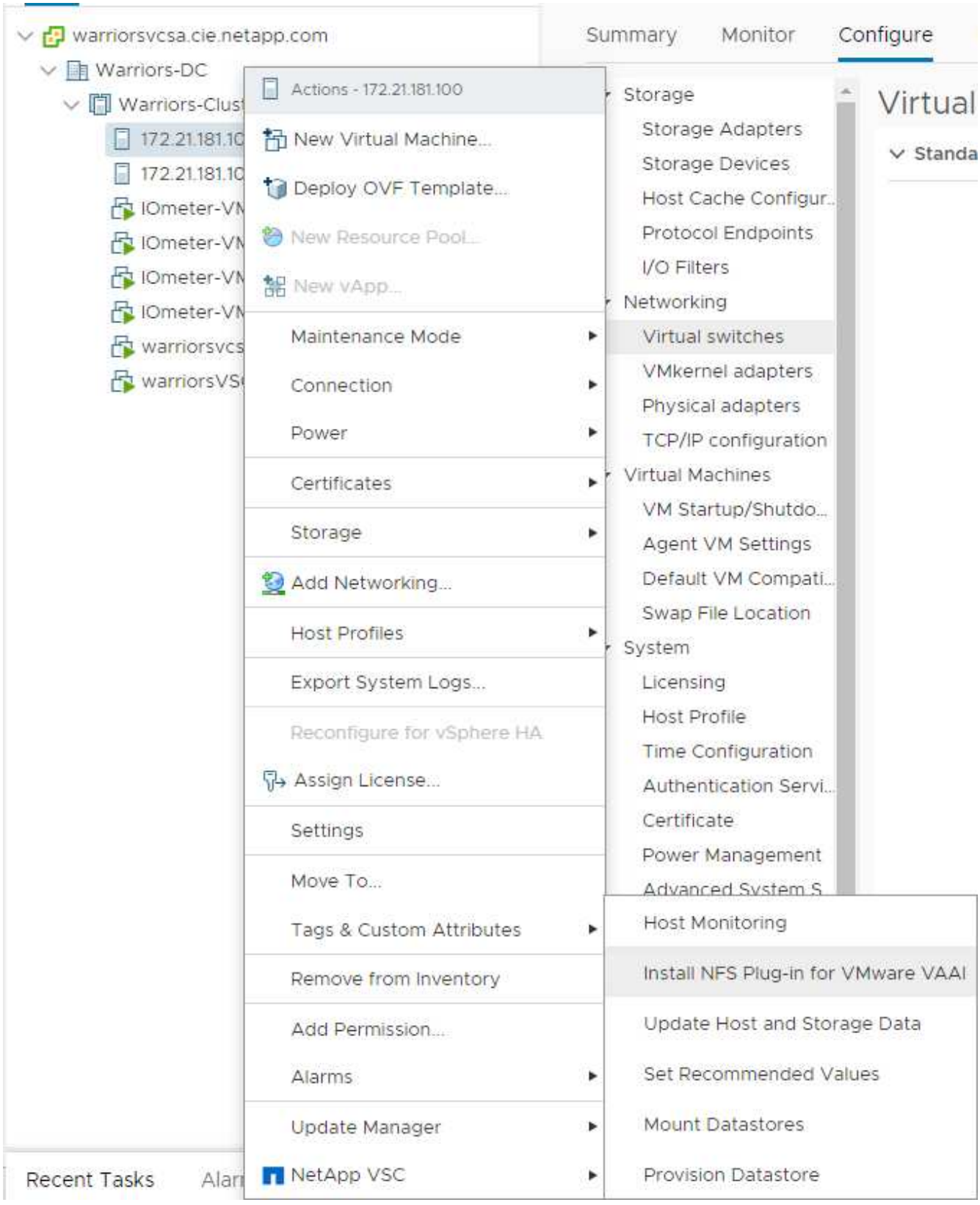
b. Desplácese hacia abajo y haga clic en NetApp NFS Plug-in for VMware VAAI.

c. En la pantalla de inicio del cliente web de vSphere, seleccione Virtual Storage Console.

d. En Virtual Storage Console > Configuración > NFS VAAI Tools, cargue el plugin de NFS seleccionando Select File y desplácese hasta la ubicación donde se almacena el plugin descargado.



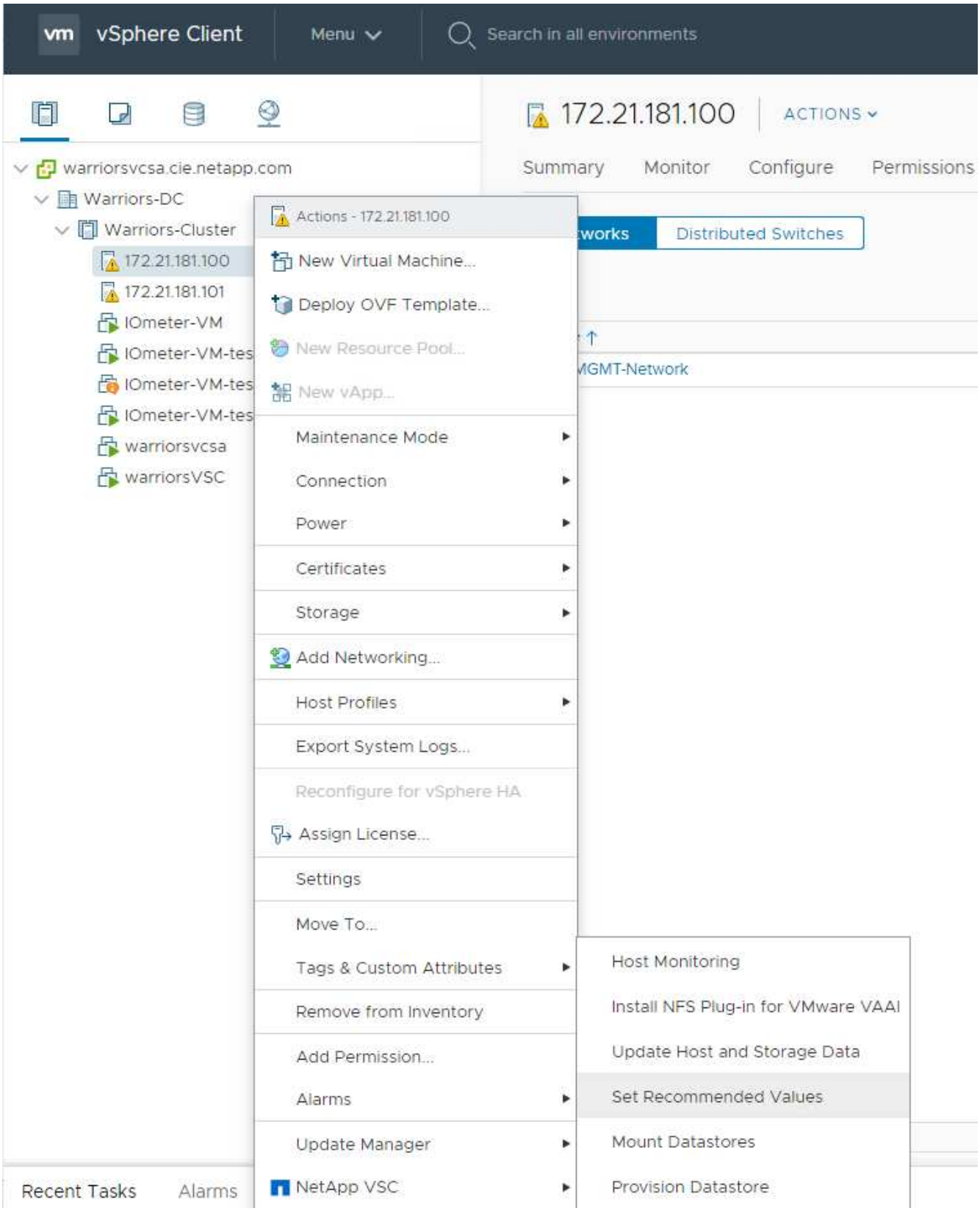
3. Haga clic en Upload para transferir el plugin a vCenter.
4. Seleccione el host y, a continuación, seleccione NetApp VSC > Install NFS Plug-in for VMware VAAI.



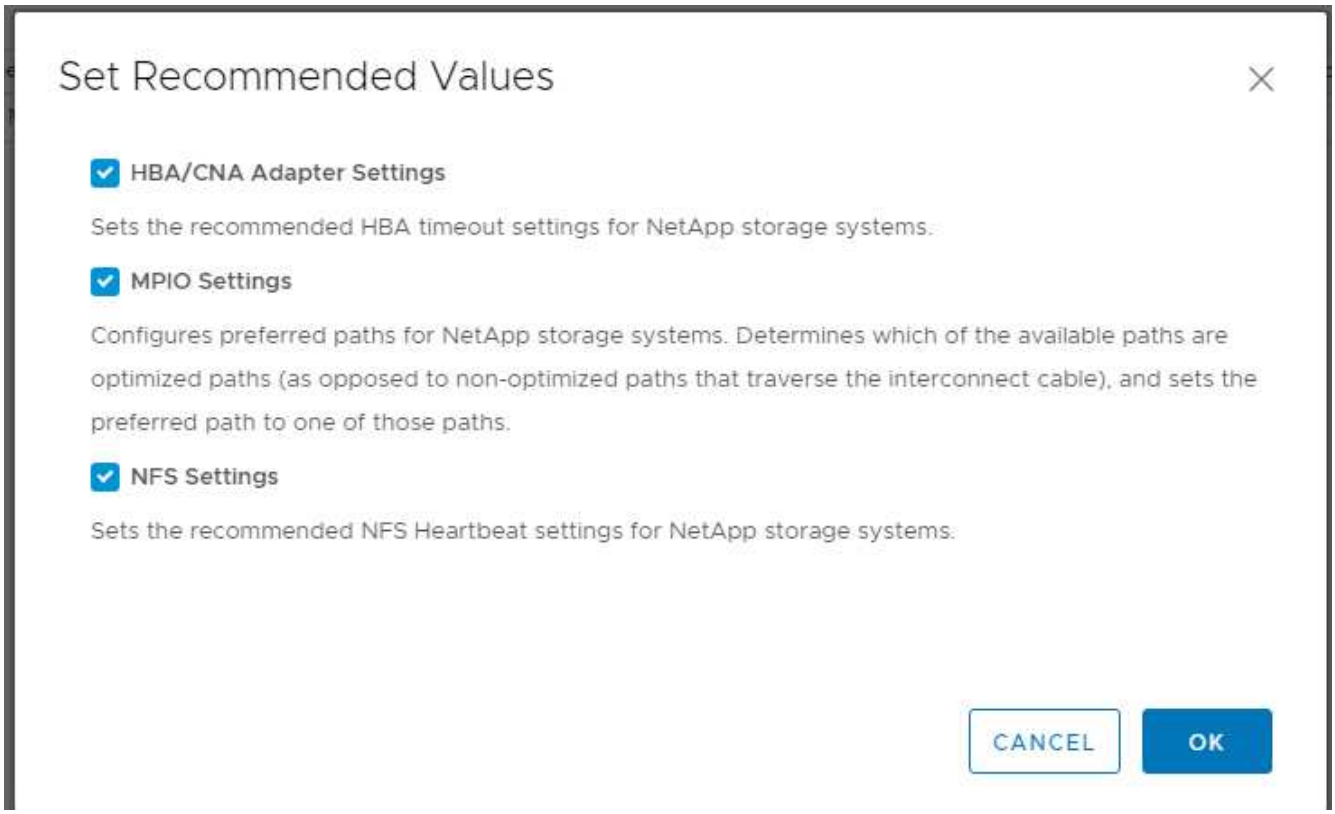
Use la configuración de almacenamiento óptima para los hosts ESXi

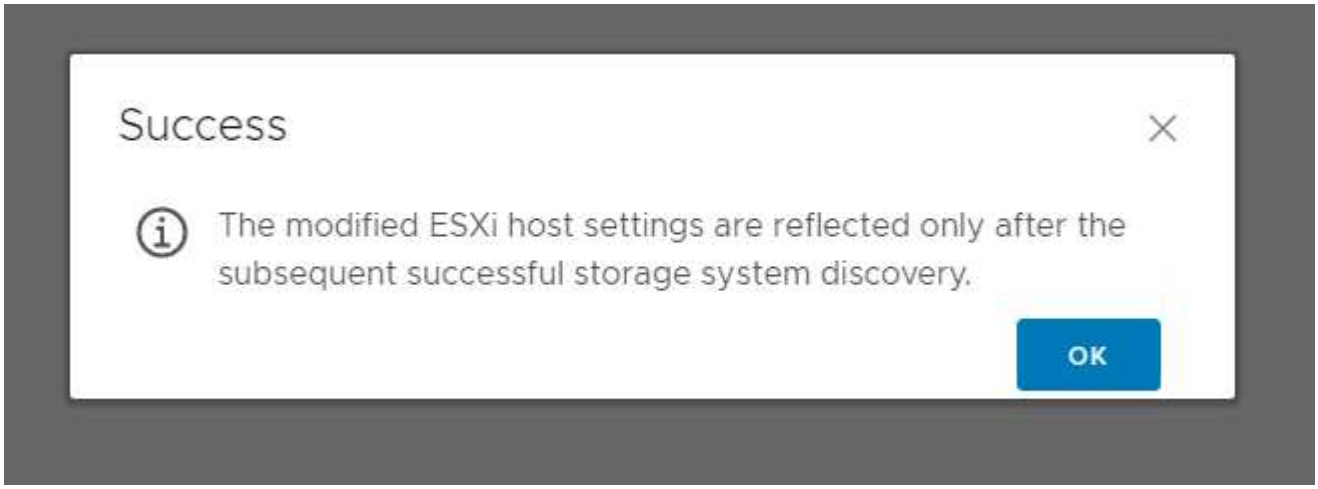
VSC permite configurar de forma automatizada ajustes relacionados con el almacenamiento para todos los hosts ESXi conectados a controladoras de almacenamiento de NetApp. Para utilizar esta configuración, lleve a cabo los siguientes pasos:

1. En la pantalla Inicio, seleccione vCenter > hosts and Clusters. Para cada host ESXi, haga clic con el botón derecho y seleccione NetApp VSC > Set Recommended Values.



2. Compruebe la configuración que desea aplicar a los hosts de vSphere seleccionados. Haga clic en Aceptar para aplicar la configuración.





3. Reinicie el host ESXI después de aplicar esta configuración.

Conclusión

FlexPod Express proporciona una solución sencilla y efectiva, ya que proporciona un diseño validado que utiliza componentes líderes del sector. Al escalar mediante la adición de componentes, FlexPod Express puede adaptarse a las necesidades específicas del negocio. FlexPod Express se diseñó para pequeñas y medianas empresas, oficinas remotas y otras empresas que requieren soluciones dedicadas.

Reconocimientos

Los autores quieren reconocer a John George por su apoyo y contribución a este diseño.

Dónde encontrar información adicional

Para obtener más información sobre la información descrita en este documento, consulte los siguientes documentos y/o sitios web:

Documentación de productos de NetApp

http://docs. "netapp".com

Guía exprés de FlexPod

Diseño de la arquitectura NVA-1139: FlexPod Express con Cisco UCS C-Series y AFF C190 Series de NetApp

"https://www.netapp.com/us/media/nva-1139-design.pdf"

Historial de versiones

Versión	Fecha	Historial de versiones del documento
Versión 1.0	Noviembre de 2019	Versión inicial.

Guía de diseño de FlexPod Express con Cisco UCS C-Series y AFF A220 Series

Diseño NVA-1125: FlexPod Express con Cisco UCS C-Series y AFF A220 Series

Savita Kumari, NetApp en colaboración con:

Las tendencias en el sector señalan una gran transformación de los centros de datos hacia una infraestructura compartida y cloud computing. Además, las organizaciones buscan una solución sencilla y eficaz para oficinas remotas y sucursales que aprovechen la tecnología con la que están familiarizados en su centro de datos.

FlexPod Express es una arquitectura de centro de datos prediseñada con las mejores prácticas que se basa en Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus y AFF de NetApp. Los componentes de FlexPod Express se asemejan a los centros de datos FlexPod, lo que permite sinergias de gestión en un entorno completo de infraestructura TECNOLÓGICA a una escala menor. FlexPod Datacenter y FlexPod Express son plataformas óptimas para virtualización y para sistemas operativos con configuración básica y cargas de trabajo empresariales.

"Siguiente: Resumen del programa."

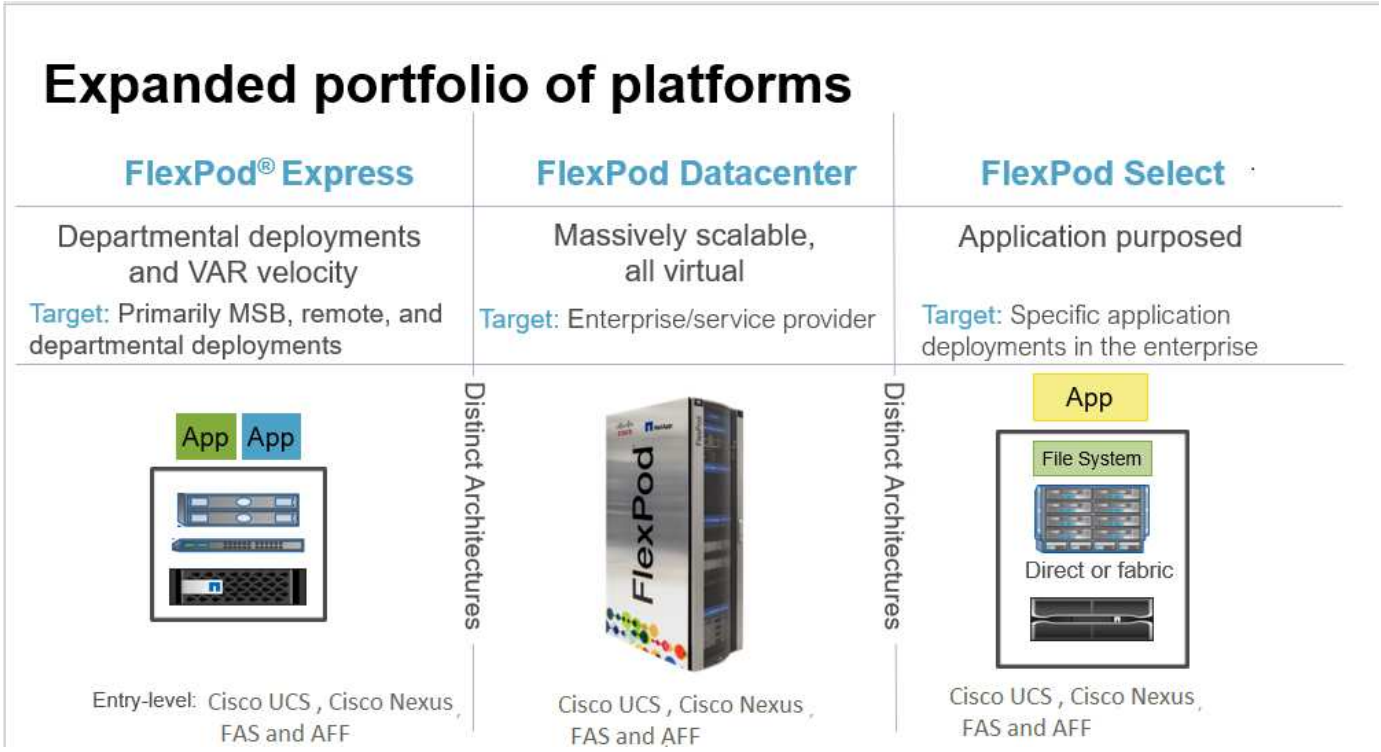
Resumen del programa

Cartera de infraestructuras convergentes FlexPod

Las arquitecturas de referencia de FlexPod se proporcionan como diseños validados por Cisco (CVD) o como arquitecturas verificadas de NetApp (NVA). Se permiten las desviaciones basadas en los requisitos del cliente de un CVD o NVA determinado si las variaciones no dan como resultado la puesta en marcha de configuraciones no compatibles.

Como se muestra en la siguiente figura, la cartera de FlexPod incluye tres soluciones: FlexPod Express, FlexPod Datacenter y FlexPod Select:

- **FlexPod Express.** ofrece una solución de gama básica que consiste en tecnologías de Cisco y NetApp.
- **FlexPod Datacenter.** proporciona una base multiuso óptima para diversas cargas de trabajo y aplicaciones.
- **FlexPod Select.** incorpora los mejores aspectos del centro de datos FlexPod y adapta la infraestructura a una aplicación determinada.



Programa Arquitectura validada por NetApp

El programa NVA ofrece a los clientes una arquitectura verificada para las soluciones NetApp. Una arquitectura validada de NetApp implica que la solución de NetApp tiene las siguientes cualidades:

- Ha sido probada a conciencia
- Tiene naturaleza prescriptiva
- Minimiza los riesgos de implementación
- Reduce el plazo de comercialización

Esta guía detalla el diseño de FlexPod Express con VMware vSphere. Además, este diseño aprovecha el nuevo sistema AFF A220, que ejecuta el software ONTAP 9.4 de NetApp, los switches Cisco Nexus 3172P y los servidores Cisco UCS C220 M5 como nodos de hipervisor.

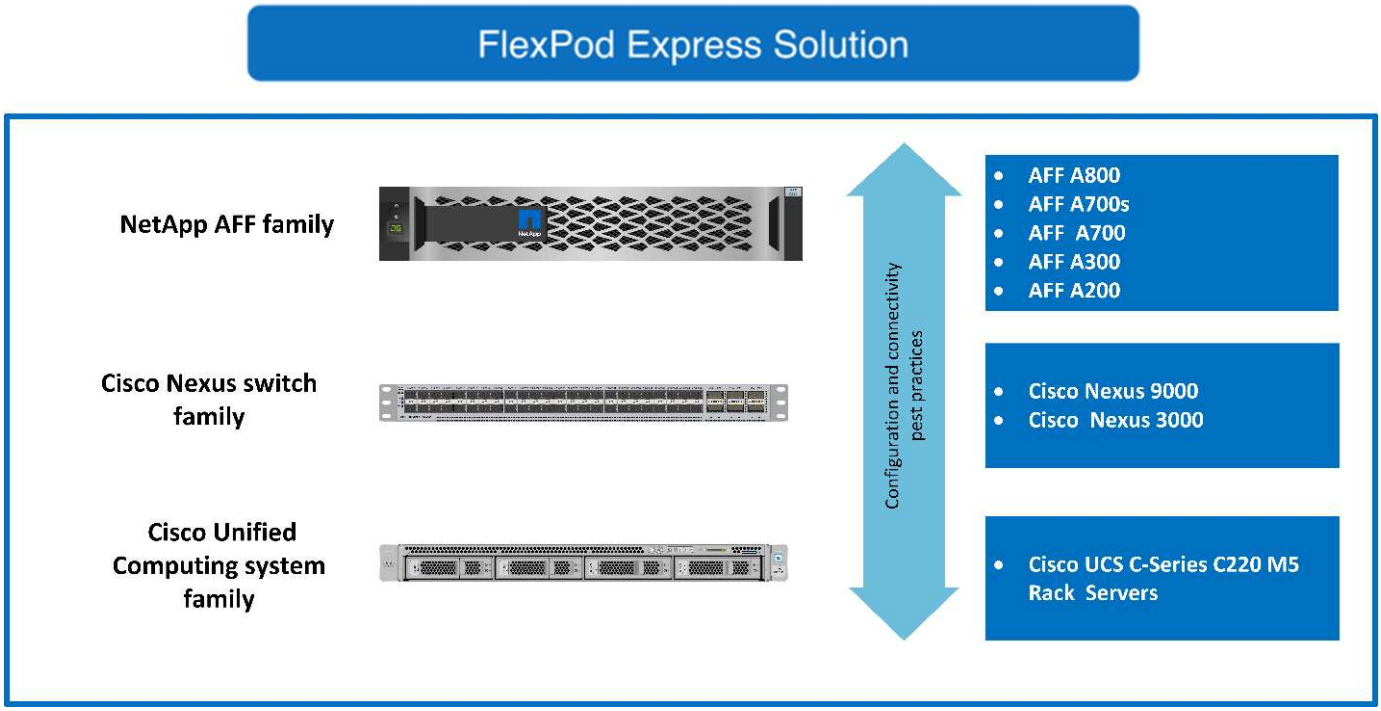
Aunque este documento está validado para AFF A220, esta solución también admite FAS2700.

"Siguiente: Descripción general de la solución."

Descripción general de la solución

FlexPod Express está diseñado para ejecutar cargas de trabajo de virtualización mixtas. Está pensado para oficinas remotas, sucursales y para pequeñas y medianas empresas. También es perfecto para empresas grandes que deseen implementar una solución dedicada para un propósito. Esta nueva solución para FlexPod Express añade nuevas tecnologías como ONTAP 9.4, AFF A220 de NetApp y VMware vSphere 6.7.

La siguiente figura muestra los componentes de hardware incluidos en la solución FlexPod Express.

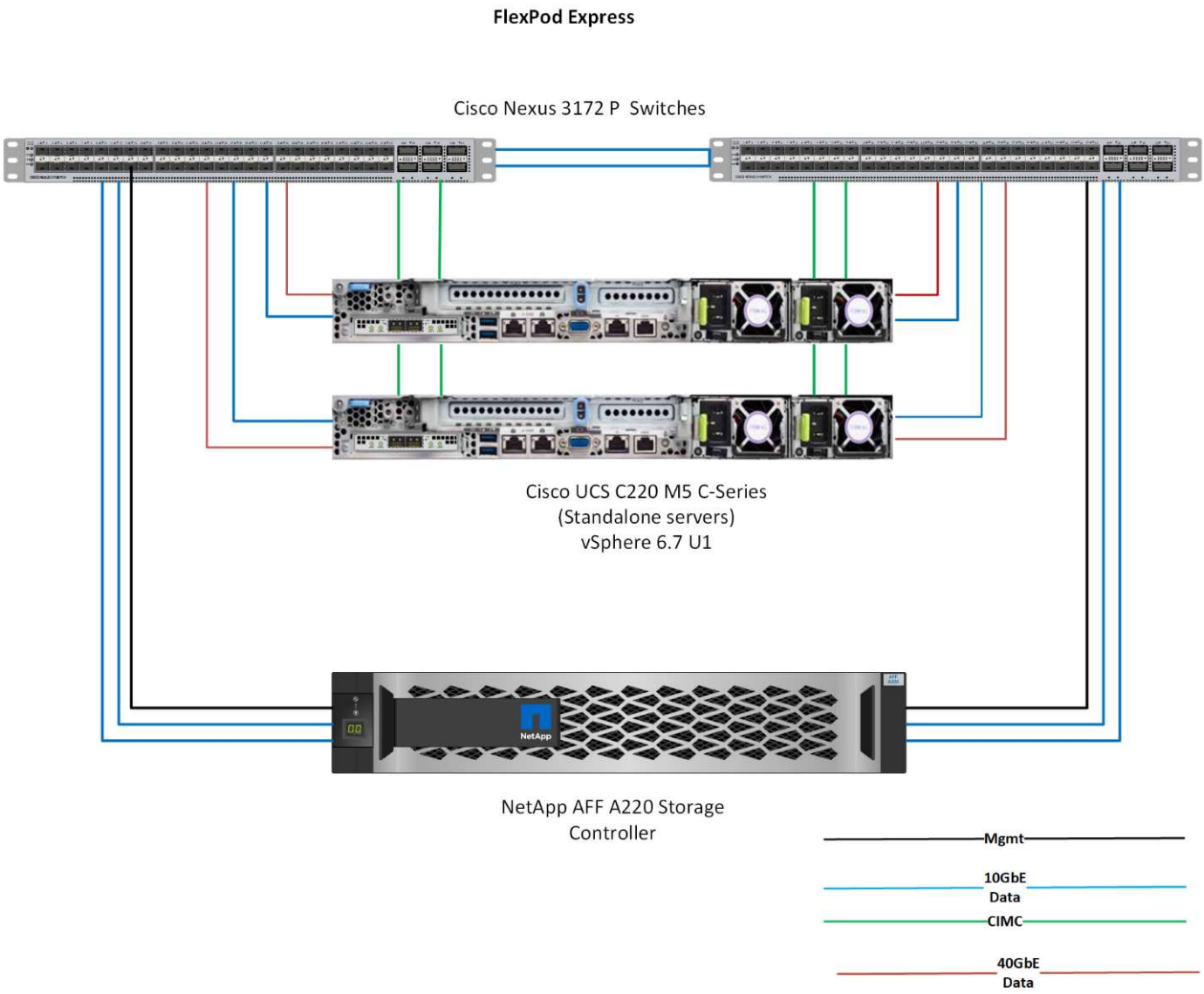


Público objetivo

Este documento está dirigido a los clientes que desean aprovechar una infraestructura creada para proporcionar eficiencia TECNOLÓGICA y permitir la innovación EN TECNOLOGÍA. El público de este documento incluye, sin limitarse a ellos, ingenieros de ventas, consultores de campo, personal de servicios profesionales, gestores DE TECNOLOGÍA, ingenieros de partners y clientes.

Tecnología de soluciones

Esta solución aprovecha las últimas tecnologías de NetApp, Cisco y VMware. Esta solución incluye el nuevo sistema AFF A220 de NetApp, que ejecuta el software ONTAP 9.4, switches Cisco Nexus 3172P duales y servidores de rack Cisco UCS C220 M5 que ejecutan VMware vSphere 6.7. Esta solución validada usa tecnología Ethernet de 10 GB (10GbE). En la siguiente figura se muestra una descripción general. También se ofrece orientación sobre cómo escalar agregando dos nodos de hipervisor a la vez para que la arquitectura FlexPod Express pueda adaptarse a las cambiantes necesidades empresariales de una organización.



40 GbE no está validado, pero es una infraestructura compatible.

"Siguiente: Requisitos tecnológicos."

Requisitos tecnológicos

FlexPod Express requiere una combinación de componentes de hardware y software que depende de la velocidad del hipervisor y de la red seleccionados. Además, FlexPod Express puede establecer los componentes de hardware necesarios para añadir nodos de hipervisor en unidades de dos.

Requisitos de hardware

Independientemente del hipervisor elegido, todas las configuraciones exprés de FlexPod utilizan el mismo hardware. Por lo tanto, aunque cambien los requisitos del negocio, cualquiera de los hipervisores puede ejecutarse en el mismo hardware de FlexPod Express.

La siguiente tabla enumera los componentes de hardware necesarios para todas las configuraciones exprés

de FlexPod e implementar la solución. Los componentes de hardware que se usan en cualquier implementación particular de la solución pueden variar en función de las necesidades del cliente.

Hardware subyacente	Cantidad
Clúster de dos nodos AFF A220	1
Servidor Cisco UCS C220 M5	2
Switch Cisco Nexus 3172P	2
Tarjeta de interfaz virtual (VIC) Cisco UCS 1387 para el servidor en rack Cisco UCS C220 M5	2
Adaptador Cisco CVR-QSFP-SFP10G	4

Requisitos de software

En las siguientes tablas, se enumeran los componentes de software necesarios para implementar las arquitecturas de la solución FlexPod Express.

La siguiente tabla enumera los requisitos de software para la implementación básica de FlexPod Express.

De NetApp	Versión	Detalles
Controladora de gestión integrada de Cisco (CIMC)	3.1.3	Para servidores en rack C220 M5
Cisco NX-OS	nxos.7.0.3.I7.5.bin	Para switches Cisco Nexus 3172P
ONTAP de NetApp	9.4	Para controladoras AFF A220

En la siguiente tabla se muestra el software necesario para todas las implementaciones de VMware vSphere en FlexPod Express.

De NetApp	Versión
Dispositivo VMware vCenter Server	6.7
VMware vSphere ESXi	6.7
Complemento VAAI de NetApp para ESXi	1.1.2

"Siguiente: Opciones de diseño."

Opciones de diseño

Se han elegido las siguientes tecnologías durante el proceso de creación de este diseño. Cada tecnología cumple un propósito específico en la solución de infraestructura Express de FlexPod.

Serie AFF A220 de NetApp con ONTAP 9.4

Esta solución aprovecha dos de los productos más recientes de NetApp: El software AFF A220 y ONTAP 9.4 de NetApp.

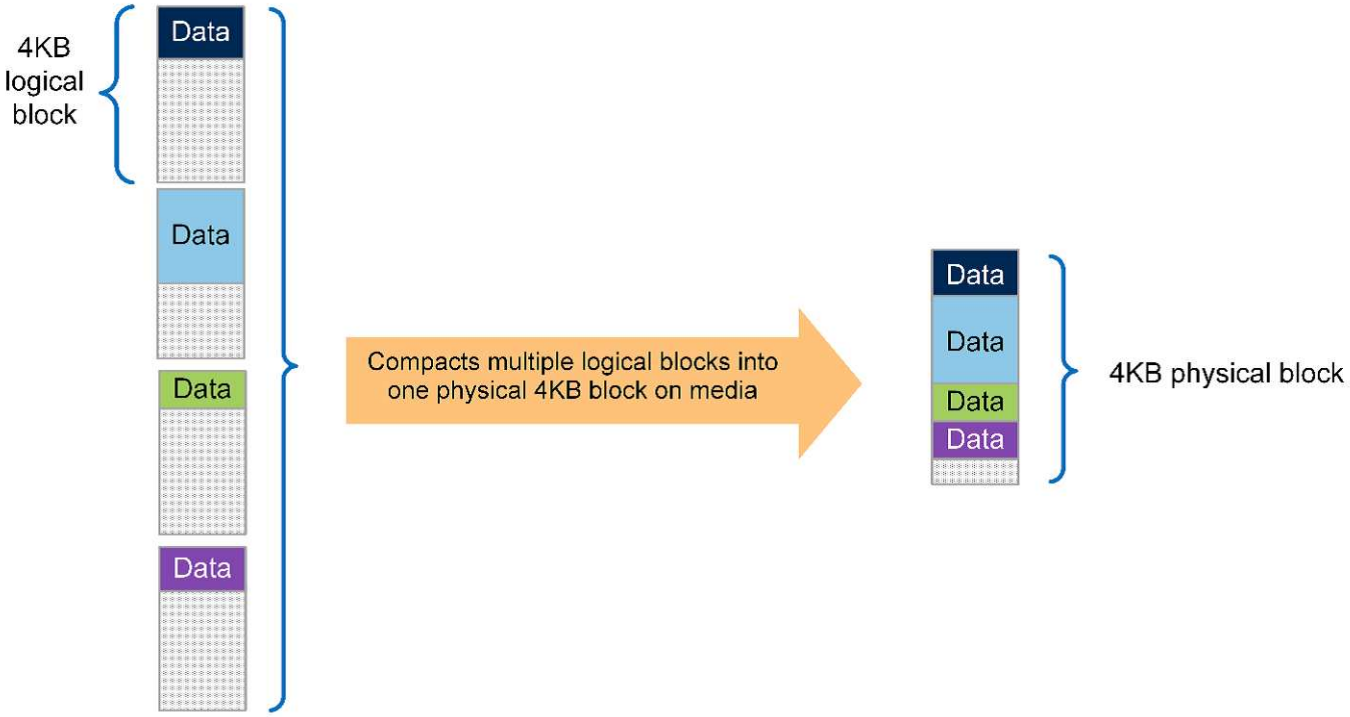
Sistema AFF A220

Si desea obtener más información sobre el sistema de hardware AFF A220, consulte "Página de inicio De AFF a-Series".

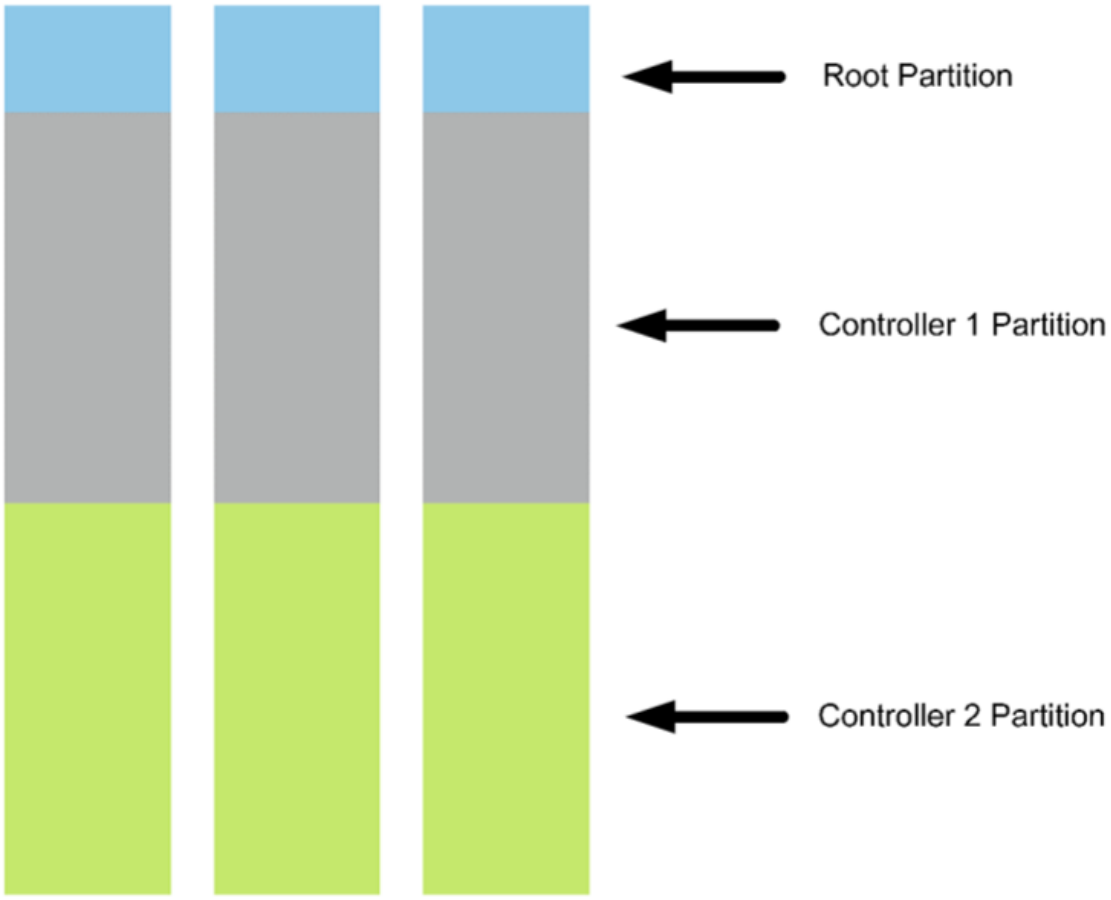
Software ONTAP 9.4

Los sistemas AFF A220 de NetApp utilizan el nuevo software ONTAP 9.4. ONTAP 9.4 es el software de gestión de datos empresariales líder del sector. Combina nuevos niveles de simplicidad y flexibilidad con potentes funcionalidades de gestión de datos, eficiencias de almacenamiento e integración del cloud líder.

ONTAP 9.4 cuenta con varias funciones que resultan adecuadas para la solución FlexPod Express. Lo más importante es el compromiso de NetApp con la eficiencia del almacenamiento, que puede ser una de las funciones más importantes para implementaciones pequeñas. Las características distintivas de la eficiencia del almacenamiento de NetApp, como la deduplicación, la compresión y el thin provisioning, están disponibles en ONTAP 9.4, además de compactación. Como el sistema WAFL de NetApp siempre escribe bloques de 4 KB, la compactación combina varios bloques en un bloque de 4 KB cuando los bloques no utilizan el espacio asignado de 4 KB. La siguiente figura ilustra este proceso.



Además, el sistema AFF A220 puede aprovechar la partición de datos raíz. Esta partición permite dividir el agregado raíz y dos agregados de datos en los discos del sistema. Por lo tanto, ambas controladoras en un clúster de AFF A220 de dos nodos pueden aprovechar el rendimiento de todos los discos del agregado. Consulte la figura siguiente.



Estas son solo algunas de sus funciones clave que complementan la solución FlexPod Express. Para obtener más información sobre las características y funciones adicionales de ONTAP 9.4, consulte la "Especificaciones técnicas del software de gestión de datos ONTAP 9". Consulte también NetApp "Centro de documentación de ONTAP 9" , que se ha actualizado para incluir ONTAP 9.4.

Serie Nexus 3000 de Cisco

El Cisco Nexus 3172P es un switch sólido y rentable que ofrece conmutación de 1/10/40/100Gbps. El switch Cisco Nexus 3172PQ, parte de la familia Unified Fabric, es un switch compacto de 1 unidad de rack (1RU) para las puestas en marcha de centros de datos en la parte superior del rack. (Ver la figura siguiente). Ofrece hasta setenta puertos de 1/10 GbE en 1RU o cuarenta y ocho puertos de 1/10 GbE más seis puertos de 40 GbE en 1RU. Además, para obtener la máxima flexibilidad de la capa física, también admite 1/10/40 Gbps.

Dado que todos los distintos modelos de la serie Cisco Nexus ejecutan el mismo sistema operativo subyacente, NX-OS, son compatibles con múltiples modelos Cisco Nexus en las soluciones FlexPod Express y FlexPod Datacenter.

Las especificaciones de rendimiento incluyen:

- Rendimiento del tráfico de velocidad de línea (ambas capas 2 y 3) en todos los puertos
- Unidades de transmisión máxima configurables (MTU) de hasta 9216 bytes (tramas gigantes)

Para obtener más información sobre los switches Cisco Nexus 3172, consulte "Hoja de datos de los conmutadores Cisco Nexus 3172PQ, 3172TQ, 3172TQ-32T, 3172PQ-XL y 3172TQ-XL".

Cisco UCS C-Series

Se eligió el servidor en rack Cisco UCS C-Series para FlexPod Express porque sus numerosas opciones de configuración permiten adaptarse a requisitos específicos en una puesta en marcha de FlexPod Express.

Los servidores de montaje en rack Cisco UCS C-Series ofrecen informática unificada en un factor de forma estándar del sector para reducir el TCO y aumentar la agilidad.

Los servidores de montaje en rack Cisco UCS C-Series ofrecen las siguientes ventajas:

- Un punto de entrada independiente del factor de forma en Cisco UCS
- Puesta en marcha de aplicaciones simplificada y rápida
- Ampliación de las innovaciones y ventajas de la informática unificada a los servidores en rack
- Mayor elección para el cliente gracias a sus ventajas únicas en un paquete de rack conocido

El servidor de montaje en rack Cisco UCS C220 M5 (en la figura anterior) se encuentra entre la infraestructura empresarial para uso general más versátil y los servidores de aplicaciones del sector. Se trata de un servidor en rack de dos sockets de alta densidad que ofrece un rendimiento y una eficiencia líderes en el sector para una amplia gama de cargas de trabajo, incluidas aplicaciones de virtualización, colaboración y con configuración básica. Los servidores en rack Cisco UCS serie C se pueden implementar como servidores independientes o como parte de Cisco UCS para aprovechar las innovaciones informáticas unificadas basadas en estándares de Cisco que ayudan a reducir el coste total de propiedad de los clientes y a aumentar la agilidad empresarial.

Para obtener más información sobre los servidores C220 M5, consulte "Hoja de datos del servidor en rack Cisco UCS C220 M5".

Opciones de conectividad para los servidores en rack C220 M5

Las opciones de conectividad para los servidores C220 M5 rack son las siguientes:

- **Cisco UCS VIC 1387**

  El Cisco UCS VIC 1387 (en la siguiente figura) ofrece dos puertos mejorados QSFP+ 40 GbE y FC sobre Ethernet (FCoE) en un factor de forma modular-LAN en la placa base (mLOM). La ranura mLOM se puede

utilizar para instalar un Cisco VIC sin consumir una ranura Peripheral Component Interconnect Express (PCIe), lo que proporciona una mayor capacidad de ampliación de E/S.

Para obtener más información acerca del adaptador Cisco UCS VIC 1387, consulte "Tarjeta de interfaz virtual 1387 de Cisco UCS" hoja de datos.

- **ADAPTADOR CVR-QSFP-SFP10G**

  El módulo QSA de Cisco convierte un puerto QSFP en un puerto SFP o SFP+. Con este adaptador, los clientes tienen la flexibilidad de usar cualquier módulo o cable SFP+ o SFP para conectarse a un puerto de menor velocidad en el otro extremo de la red. Esta flexibilidad permite una transición rentable a 40 GbE al optimizar el uso de plataformas QSFP de 40 GbE de alta densidad. Este adaptador es compatible con todos los cables ópticos SFP+ y con diversos módulos SFP de 1 GbE. Dado que este proyecto se ha validado utilizando conectividad 10 GbE y puesto que VIC 1387 utilizado es 40 GbE, se utiliza para la conversión el adaptador CVR-QSFP-SFP10G (en la siguiente figura).

VMware vSphere 6.7

VMware vSphere 6.7 es una opción de hipervisor para utilizar con FlexPod Express. VMware vSphere permite a las organizaciones reducir su huella de potencia y refrigeración a la vez que confirman que la capacidad de computación adquirida se ha aprovechado al máximo. Además, VMware vSphere permite la protección contra fallos de hardware (alta disponibilidad de VMware o ha de VMware) y el equilibrio de carga de recursos

informáticos en un clúster de hosts vSphere (Distributed Resource Scheduler de VMware o DRS de VMware).

Debido a que solo reinicia el kernel, VMware vSphere 6.7 permite a los clientes “arrancar rápidamente” donde cargan vSphere ESXi sin reiniciar el hardware. Esta función sólo está disponible con plataformas y controladores que se encuentran en la lista blanca de Quick Boot. VSphere 6.7 amplía las funcionalidades de vSphere Client, que puede realizar aproximadamente un 90% de lo que puede hacer vSphere Web Client.

En vSphere 6.7, VMware ha ampliado esta funcionalidad para permitir a los clientes establecer Enhanced vMotion Compatibility (EVC) por máquina virtual (VM) en lugar de hacerlo por host. En vSphere 6.7, VMware también ha expuesto las API que pueden utilizarse para crear clones instantáneos.

A continuación se muestran algunas de las funciones de vSphere 6.7 U1:

- VSphere Client basado en web HTML5 con todas las funciones
- VMotion para máquinas virtuales GRID vGPU de NVIDIA. Compatibilidad con Intel FPGA.
- VCenter Server reúnen la herramienta para pasar de PSC externo a PCS interno.
- Mejoras para VSAN (actualizaciones de HCI).
- Biblioteca de contenido mejorada.

Para obtener más información sobre vSphere 6.7 U1, consulte "Novedades de vCenter Server 6.7 Update 1". A pesar de que esta solución se validó con vSphere 6.7, es compatible con cualquier versión de vSphere que esté cualificada con los demás componentes de la herramienta de matriz de interoperabilidad de NetApp. NetApp recomienda implementar vSphere 6.7U1 para sus correcciones y funciones mejoradas.

Arquitectura de arranque

A continuación, se muestran las opciones compatibles de la arquitectura de arranque exprés de FlexPod:

- LUN SAN iSCSI
- Tarjeta SD Cisco FlexFlash
- Disco local

Dado que FlexPod Datacenter se arranca desde LUN de iSCSI, la capacidad de gestión de la solución se mejora mediante el uso del arranque iSCSI para FlexPod Express.

"Siguiente: Verificación de la solución."

Verificación de la solución

Cisco y NetApp diseñaron y crearon FlexPod Express para servir como una plataforma de infraestructura de primer nivel para sus clientes. Al ser diseñado con componentes líderes en el sector, los clientes pueden confiar en FlexPod Express como base de su infraestructura. De acuerdo con los principios fundamentales de la cartera de FlexPod, la arquitectura de FlexPod Express ha sido probada a conciencia por arquitectos e ingenieros de centros de datos de Cisco y NetApp. Desde la redundancia y la disponibilidad a cada funcionalidad individual, se valida toda la arquitectura FlexPod Express para infundir confianza en los clientes y fomentar la confianza en el proceso de diseño.

VMware vSphere 6.7 se verificó en los componentes de la infraestructura de FlexPod Express. Esta validación

incluye opciones de conectividad de enlace ascendente 10 GbE para el hipervisor.

"Siguiente: Conclusión."

Conclusión

FlexPod Express ofrece una solución sencilla y efectiva, ya que proporciona un diseño validado que utiliza componentes líderes en el sector. Al escalar y proporcionar opciones para la plataforma de hipervisor, FlexPod Express se puede adaptar a las necesidades específicas del negocio. FlexPod Express se ha diseñado teniendo en cuenta a las pequeñas y medianas empresas, las oficinas remotas y sucursales, y otras empresas que requieren soluciones dedicadas.

"Siguiente: Dónde encontrar información adicional."

Dónde encontrar información adicional

Si quiere obtener más información sobre la información descrita en este documento, consulte los siguientes documentos y sitios web:

- Documentación de NetApp

  "https://docs.netapp.com"

- Guía de puesta en marcha de FlexPod Express con VMware vSphere 6.7 y AFF A220 de NetApp

  "https://www.netapp.com/us/media/nva-1123-deploy.pdf"

Guía de puesta en marcha de FlexPod Express con Cisco UCS C-Series y AFF A220 Series

NVA-1123-PUESTA en MARCHA: FlexPod Express con VMware vSphere 6.7 y la guía de puesta en marcha de AFF A220 de NetApp

Savita Kumari, NetApp

En colaboración con: 

Las tendencias en el sector señalan una gran transformación de los centros de datos hacia una infraestructura compartida y cloud computing. Además, las organizaciones buscan una solución sencilla y eficaz para oficinas remotas y sucursales que aprovechen la tecnología con la que ya están familiarizados en su centro de datos.

FlexPod Express es una arquitectura de centro de datos prediseñada con las mejores prácticas que se basa en el Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus y las tecnologías de almacenamiento de NetApp. Los componentes de un sistema FlexPod Express se asemejan a los del centro

de datos FlexPod, lo que permite sinergias de gestión en todo el entorno de infraestructura DE TI a una escala menor. FlexPod Datacenter y FlexPod Express son plataformas óptimas para virtualización y para sistemas operativos con configuración básica y cargas de trabajo empresariales.

El centro de datos de FlexPod y FlexPod Express proporcionan una configuración básica y cuentan con la flexibilidad necesaria para ajustar su tamaño y optimizarse con el objetivo de acomodar distintos casos de uso y requisitos. Los clientes existentes de FlexPod Datacenter pueden gestionar su sistema FlexPod Express con las herramientas a las que están acostumbrados. Los nuevos clientes de FlexPod Express pueden adaptarse fácilmente a la gestión del centro de datos FlexPod cuando crezca su entorno.

FlexPod Express es una base de infraestructura óptima para oficinas remotas y sucursales y para pequeñas y medianas empresas. También es una solución óptima para los clientes que desean proporcionar infraestructura para cargas de trabajo dedicadas.

FlexPod Express proporciona una infraestructura fácil de gestionar que es adecuada para casi cualquier carga de trabajo.

Descripción general de la solución

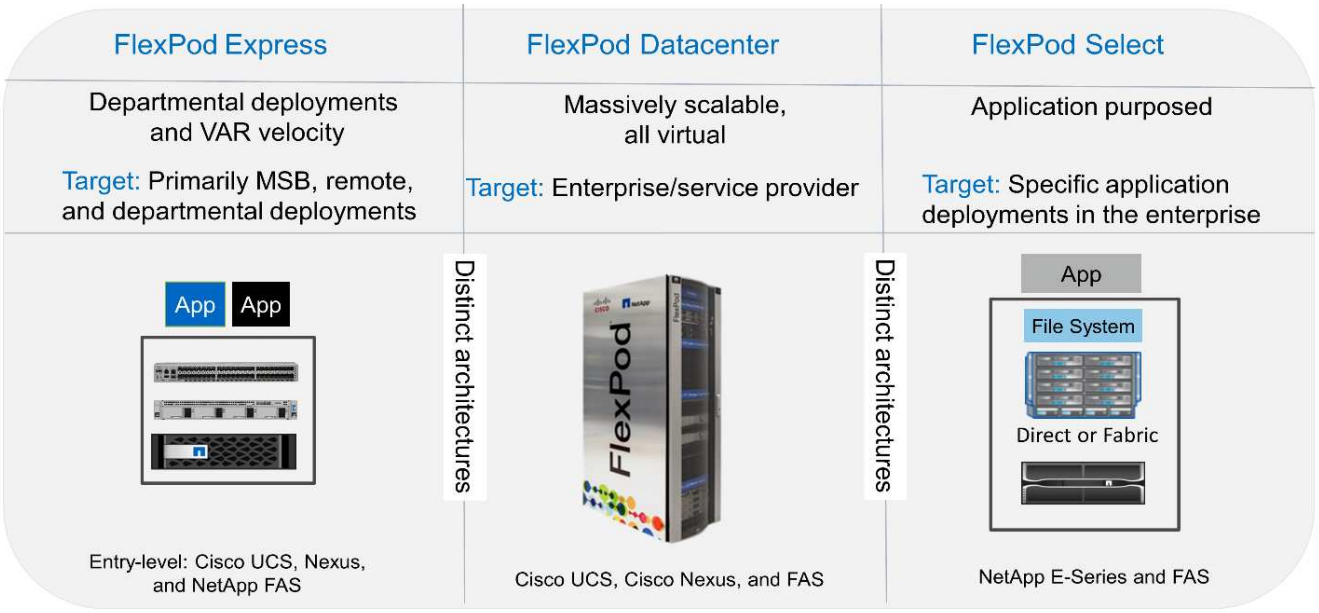
Esta solución FlexPod Express forma parte del programa de infraestructura convergente de FlexPod.

Programa de infraestructura convergente FlexPod

Las arquitecturas de referencia FlexPod se proporcionan como diseños validados por Cisco (CVD) o como arquitecturas verificadas por NetApp (NVA). Se permiten las desviaciones basadas en los requisitos de los clientes de un CVD o NVA determinado si estas variaciones no crean una configuración incompatible.

Como se muestra en la siguiente figura, el programa FlexPod incluye tres soluciones: FlexPod Express, FlexPod Datacenter y FlexPod Select:

- **FlexPod Express.** ofrece a los clientes una solución de gama básica con tecnologías de Cisco y NetApp.
- **FlexPod Datacenter.** proporciona una base multiuso óptima para diversas cargas de trabajo y aplicaciones.
- **FlexPod Select.** incorpora los mejores aspectos del centro de datos FlexPod y adapta la infraestructura a una aplicación determinada.



Programa Arquitectura validada por NetApp

El programa Arquitectura verificada de NetApp ofrece a los clientes una arquitectura verificada para soluciones NetApp. Una arquitectura verificada de NetApp ofrece una arquitectura de solución de NetApp con las siguientes cualidades:

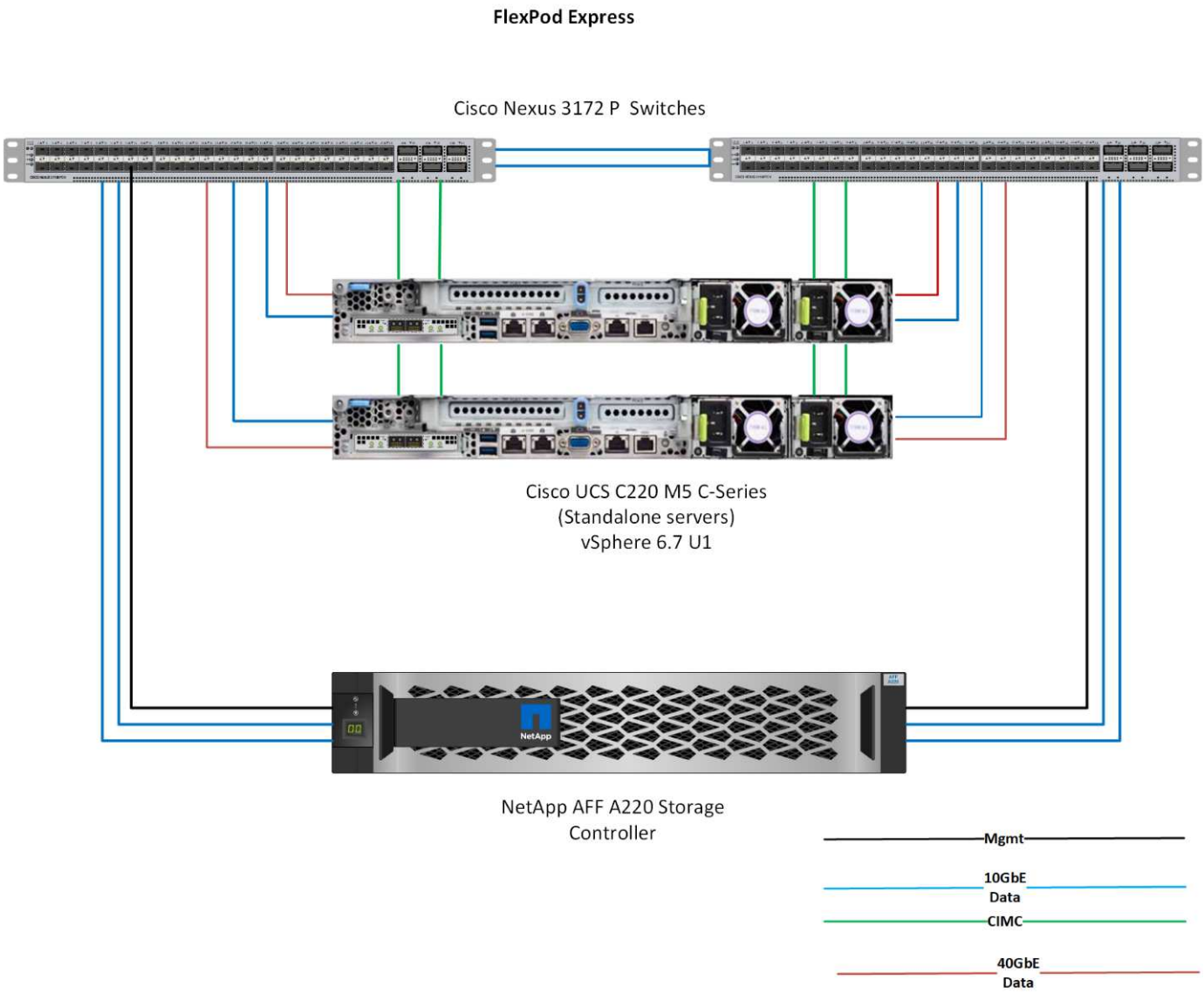
- Ha sido probada a conciencia
- Tiene naturaleza prescriptiva
- Minimiza los riesgos de implementación
- Reduce el plazo de comercialización

Esta guía detalla el diseño de FlexPod Express con VMware vSphere. Además, este diseño usa el nuevo sistema AFF A220, que ejecuta ONTAP 9.4 de NetApp, los servidores Cisco Nexus 3172P y Cisco UCS C-Series C220 M5 como nodos de hipervisor.

Tecnología de soluciones

Esta solución aprovecha las últimas tecnologías de NetApp, Cisco y VMware. Esta solución incluye el nuevo sistema AFF A220 de NetApp que ejecuta ONTAP 9.4, los conmutadores Cisco Nexus 3172P duales y los servidores de montaje en rack Cisco UCS C220 M5 que ejecutan VMware vSphere 6.7. Esta solución validada usa tecnología 10 GbE. También se ofrece orientación sobre cómo escalar la capacidad de computación mediante la adición de dos nodos de hipervisor a la vez para que la arquitectura FlexPod Express pueda adaptarse a las cambiantes necesidades empresariales de una organización.

La figura siguiente muestra FlexPod Express con arquitectura 10 GbE de VMware vSphere.



Esta validación utiliza conectividad de 10 GbE y un Cisco UCS VIC 1387, que es 40 GbE. Para lograr conectividad de 10 GbE, se utiliza el adaptador CVR-QSFP-SFP10G.

Resumen de casos de uso

La solución FlexPod Express puede aplicarse a varios casos prácticos, incluidos los siguientes:

- Oficinas remotas o sucursales
- Pequeñas y medianas empresas
- Entornos que requieren una solución dedicada y rentable

FlexPod Express está indicado para cargas de trabajo virtualizadas y mixtas.

A pesar de que esta solución se validó con vSphere 6.7, es compatible con cualquier versión de vSphere que esté cualificada con los demás componentes de la herramienta de matriz de interoperabilidad de NetApp. NetApp recomienda implementar vSphere 6.7U1 para sus correcciones y funciones mejoradas.

A continuación se muestran algunas de las características de vSphere 6.7 U1:

- Cliente vSphere basado en web HTML5 con todas las funciones
- VMotion para máquinas virtuales GRID vGPU de NVIDIA. Compatibilidad con Intel FPGA
- VCenter Server reúnen la herramienta para pasar de PSC externo a PCS interno
- Mejoras para VSAN (actualizaciones de HCI)
- Biblioteca de contenido mejorada

Para obtener más información sobre vSphere 6.7 U1, consulte "Novedades de vCenter Server 6.7 Update 1".

Requisitos tecnológicos

Un sistema FlexPod Express requiere una combinación de componentes de hardware y software. FlexPod Express también describe los componentes de hardware necesarios para añadir nodos de hipervisor al sistema en unidades de dos.

Requisitos de hardware

Independientemente del hipervisor elegido, todas las configuraciones exprés de FlexPod utilizan el mismo hardware. Por lo tanto, aunque cambien los requisitos del negocio, cualquiera de los hipervisores puede ejecutarse en el mismo hardware de FlexPod Express.

En la siguiente tabla se enumeran los componentes de hardware necesarios para todas las configuraciones exprés de FlexPod.

Hardware subyacente	Cantidad
Par de alta disponibilidad AFF A220	1
Servidor Cisco C220 M5	2
Switch Cisco Nexus 3172P	2
Tarjeta de interfaz virtual (VIC) Cisco UCS 1387 para el servidor C220 M5	2
ADAPTADOR CVR-QSFP-SFP10G	4

En la siguiente tabla se enumera el hardware necesario además de la configuración base para la implementación de 10 GbE.

Hardware subyacente	Cantidad
Servidor Cisco UCS C220 M5	2
Cisco VIC 1387	2
ADAPTADOR CVR-QSFP-SFP10G	4

Requisitos de software

En la siguiente tabla se enumeran los componentes de software necesarios para implementar las arquitecturas de las soluciones FlexPod Express.

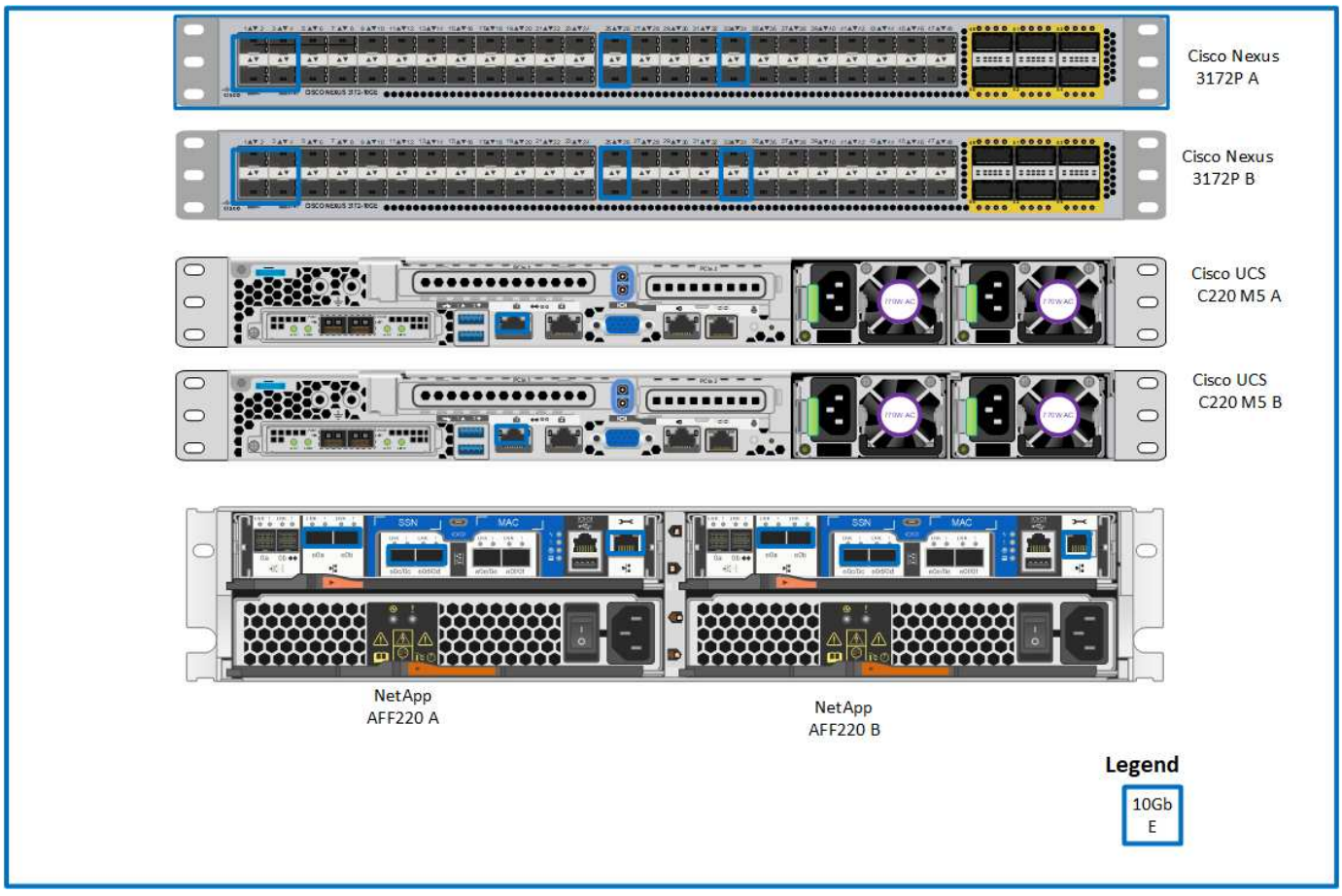
De NetApp	Versión	Detalles
Controladora de gestión integrada de Cisco (CIMC)	3.1 (3g)	Para los servidores en rack Cisco UCS C220 M5
Controlador nenic de Cisco	1.0.25.0	Para tarjetas de interfaz VIC 1387
Cisco NX-OS	nxos.7.0.3.I7.5.bin	Para switches Cisco Nexus 3172P
ONTAP de NetApp	9.4	Para controladoras AFF A220

En la siguiente tabla se enumera el software requerido para todas las implementaciones de VMware vSphere en FlexPod Express.

De NetApp	Versión
Dispositivo VMware vCenter Server	6.7
Hipervisor ESXi de VMware vSphere	6.7
Complemento VAAI de NetApp para ESXi	1.1.2

Información sobre el cableado exprés de FlexPod

La siguiente figura muestra el cableado de validación de referencia.



En la siguiente tabla se muestra información sobre el cableado del switch Cisco Nexus 3172P A.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Switch Cisco Nexus 3172P A	Eth1/1	Controladora De almacenamiento A AFF A220 de NetApp	e0c
	Eth1/2	Controladora de almacenamiento B de AFF A220 de NetApp	e0c
	Eth1/3	El servidor A independiente Cisco UCS C220 C-Series	MLOM1 con adaptador CVR-QSFP-SFP10G
	Eth1/4	Servidor B independiente Cisco UCS C220 C-Series	MLOM1 con adaptador CVR-QSFP-SFP10G
	Eth1/25	Switch Cisco Nexus 3172P B	Eth1/25
	Eth1/26	Switch Cisco Nexus 3172P B	Eth1/26
	Eth1/33	Controladora De almacenamiento A AFF A220 de NetApp	E0M
	Eth1/34	El servidor A independiente Cisco UCS C220 C-Series	CIMC

En la siguiente tabla se muestra información sobre el cableado del switch Cisco Nexus 3172P B.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Switch Cisco Nexus 3172P B	Eth1/1	Controladora De almacenamiento A AFF A220 de NetApp	e0d
	Eth1/2	Controladora de almacenamiento B de AFF A220 de NetApp	e0d
	Eth1/3	El servidor A independiente Cisco UCS C220 C-Series	MLOM2 con adaptador CVR-QSFP-SFP10G
	Eth1/4	Servidor B independiente Cisco UCS C220 C-Series	MLOM2 con adaptador CVR-QSFP-SFP10G
	Eth1/25	Switch Cisco Nexus 3172P A	Eth1/25
	Eth1/26	Switch Cisco Nexus 3172P A	Eth1/26
	Eth1/33	Controladora de almacenamiento B de AFF A220 de NetApp	E0M

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
	Eth1/34	Servidor B independiente Cisco UCS C220 C-Series	CIMC

La siguiente tabla muestra la información de cableado de la controladora de almacenamiento AFF A220 A. de NetApp

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Controladora De almacenamiento A AFF A220 de NetApp	e0a	Controladora de almacenamiento B de AFF A220 de NetApp	e0a
	e0b	Controladora de almacenamiento B de AFF A220 de NetApp	e0b
	e0c	Switch Cisco Nexus 3172P A	Eth1/1
	e0d	Switch Cisco Nexus 3172P B	Eth1/1
	E0M	Switch Cisco Nexus 3172P A	Eth1/33

La siguiente tabla muestra información de cableado para la controladora de almacenamiento B de AFF A220 de NetApp

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Controladora de almacenamiento B de AFF A220 de NetApp	e0a	Controladora De almacenamiento A AFF A220 de NetApp	e0a
	e0b	Controladora De almacenamiento A AFF A220 de NetApp	e0b
	e0c	Switch Cisco Nexus 3172P A	Eth1/2
	e0d	Switch Cisco Nexus 3172P B	Eth1/2
	E0M	Switch Cisco Nexus 3172P B	Eth1/33

Procedimientos de implantación

Este documento proporciona detalles para configurar un sistema FlexPod Express completamente redundante y de alta disponibilidad. Para reflejar esta redundancia, los componentes que se configuran en cada paso se denominan componente A o componente B. Por ejemplo, la controladora A y la controladora B identifican las dos controladoras de almacenamiento de NetApp que se aprovisionan en este documento. El

switch A y el switch B identifican un par de switches Cisco Nexus.

Además, en este documento se describen los pasos para aprovisionar varios hosts de Cisco UCS, que se identifican secuencialmente como servidor A, servidor B, etc.

Para indicar que debe incluir la información pertinente a su entorno en un paso, `<<text>>` aparece como parte de la estructura de comandos. Consulte el siguiente ejemplo de `vlan create` comando:

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

Este documento permite configurar completamente el entorno de FlexPod Express. En este proceso, varios pasos requieren que inserte convenciones de nomenclatura específicas del cliente, direcciones IP y esquemas de red de área local virtual (VLAN). En la siguiente tabla se describen las VLAN necesarias para la implementación, tal y como se explica en esta guía. Esta tabla se puede completar en función de las variables específicas del sitio y se puede utilizar para implementar los pasos de configuración del documento.

Si se utilizan VLAN de gestión fuera de banda y en banda independientes, debe crear una ruta de capa- 3 entre ellas. Para esta validación, se utilizó una VLAN de gestión común.

Un nombre	Propósito de VLAN	ID utilizado en la validación de este documento
VLAN de gestión	VLAN para interfaces de gestión	3437
VLAN nativa	VLAN a la que se asignan tramas no etiquetadas	2
VLAN NFS	VLAN para tráfico NFS	3438
VLAN de VMware vMotion	VLAN designada para mover máquinas virtuales de un host físico a otro	3441
VLAN de tráfico de equipos virtuales	VLAN para tráfico de aplicaciones de equipos virtuales	3442
ISCSI-A-VLAN	VLAN para tráfico iSCSI en la estructura A	3439
ISCSI-B-VLAN	VLAN para tráfico iSCSI en la estructura B	3440

Los números VLAN son necesarios en toda la configuración de FlexPod Express. Las VLAN se denominan `<<var_xxxx_vlan>>`, donde `xxxx` Es la finalidad de la VLAN (como iSCSI-A).

La siguiente tabla enumera las máquinas virtuales de VMware creadas.

Descripción de la máquina virtual	Nombre de host
Servidor VMware vCenter	

Procedimiento de puesta en marcha de Cisco Nexus 3172P

En la siguiente sección se detalla la configuración del switch Cisco Nexus 3172P

utilizada en un entorno de FlexPod Express.

Configuración inicial del switch Cisco Nexus 3172P

Los siguientes procedimientos describen cómo configurar los switches Cisco Nexus para su uso en un entorno FlexPod Express básico.

> Este procedimiento supone que está utilizando un Cisco Nexus 3172P con la versión 7.0(3)I7(5) del software NX-OS.

1. Tras el arranque y la conexión iniciales al puerto de la consola del switch, se inicia automáticamente la configuración de Cisco NX-OS. Esta configuración inicial trata los valores básicos, como el nombre del switch, la configuración de la interfaz mgmt0 y la configuración de Secure Shell (SSH).
2. La red de gestión del sistema FlexPod Express se puede configurar de varias maneras. Las interfaces mgmt0 de los conmutadores 3172P se pueden conectar a una red de gestión existente, o las interfaces mgmt0 de los conmutadores 3172P se pueden conectar en una configuración posterior. Sin embargo, este enlace no se puede utilizar para el acceso de gestión externo, como tráfico SSH.

   En esta guía de implementación, los switches FlexPod Express Cisco Nexus 3172P están conectados a una red de gestión existente.
3. Para configurar los switches Cisco Nexus 3172P, encienda el switch y siga las instrucciones en pantalla, como se muestra aquí para la configuración inicial de ambos conmutadores, sustituyendo los valores adecuados para la información específica del conmutador.

```
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. A continuación, verá un resumen de la configuración y se le preguntará si desea editarla. Si la configuración es correcta, introduzca `n`.

```
Would you like to edit the configuration? (yes/no) [n]: n
```

5. A continuación, se le preguntará si desea utilizar esta configuración y guardarla. Si es así, introduzca `y`.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Repita este procedimiento para el switch Cisco Nexus B.

Habilite funciones avanzadas

Determinadas características avanzadas deben estar habilitadas en Cisco NX-OS para proporcionar opciones de configuración adicionales.

> La `interface-vlan` la función sólo es obligatoria si se utiliza el back-to-back `mgmt0` opción descrita en este documento. Esta función permite asignar una dirección IP a la interfaz VLAN (interfaz virtual de switch), que habilita la comunicación de gestión en banda al switch (como a través de SSH).

1. Para habilitar las funciones adecuadas en los switches a y B de Cisco Nexus, escriba el modo de configuración mediante el comando `(config t)` y ejecute los siguientes comandos:

   ```
   feature interface-vlan
   feature lacp
   feature vpc
   ```

   El hash de equilibrio de carga del canal de puerto predeterminado utiliza las direcciones IP de origen y destino para determinar el algoritmo de equilibrio de carga en las interfaces del canal de puerto. Puede lograr una mejor distribución entre los miembros del canal de puerto proporcionando más entradas al algoritmo hash más allá de las direcciones IP de origen y destino. Por el mismo motivo, NetApp recomienda encarecidamente añadir los puertos TCP de origen y destino al algoritmo hash.

2. Desde el modo de configuración (`config t`), introduzca los siguientes comandos para establecer la configuración de equilibrio de carga del canal de puerto global en los conmutadores A y B de Cisco Nexus:

   ```
   port-channel load-balance src-dst ip-l4port
   ```

Realizar la configuración de árbol de expansión global

La plataforma Cisco Nexus utiliza una nueva función de protección llamada garantía de puente. La garantía de puente ayuda a proteger contra un enlace unidireccional u otro error de software con un dispositivo que continúa redirectando el tráfico de datos cuando ya no ejecuta el algoritmo de árbol expansivo. Los puertos se pueden colocar en uno de varios estados, incluyendo la red o el borde, dependiendo de la plataforma.

NetApp recomienda establecer la garantía de puente para que todos los puertos se consideren puertos de red de forma predeterminada. Este ajuste obliga al administrador de red a revisar la configuración de cada puerto. También revela los errores de configuración más comunes, como puertos de borde no identificados o un vecino que no tiene activada la función de garantía de puente. Además, es más seguro tener el bloque de árbol expansivo muchos puertos en lugar de muy pocos, lo que permite que el estado de puerto predeterminado mejore la estabilidad general de la red.

Preste especial atención al estado de árbol de expansión al agregar servidores, almacenamiento y switches ascendentes, especialmente si no admiten la garantía de puente. En estos casos, es posible que deba cambiar el tipo de puerto para que los puertos estén activos.

El protector de unidad de datos de protocolo puente (BPDU) está habilitado de forma predeterminada en puertos periféricos como otra capa de protección. Para evitar bucles en la red, esta característica cierra el puerto si se ven BPDU de otro switch en esta interfaz.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para configurar las opciones de árbol de expansión predeterminadas, incluidos el tipo de puerto predeterminado y el protector BPDU, en el conmutador A de Cisco Nexus y el conmutador B:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

Defina las VLAN

Antes de configurar puertos individuales con VLAN diferentes, se deben definir las VLAN de capa 2 en el switch. También se recomienda nombrar las VLAN para que la solución de problemas sea sencilla en el futuro.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para definir y describir las VLAN de capa 2 en el switch A y el switch B de Cisco Nexus:

```
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
```

Configurar el acceso y las descripciones de los puertos de gestión

Al igual que en la asignación de nombres a las VLAN de capa 2, las descripciones de configuración de todas las interfaces pueden ayudar tanto al aprovisionamiento como a la solución de problemas.

Desde el modo de configuración (`config t`) En cada uno de los conmutadores, introduzca las siguientes descripciones de puerto para la configuración grande de FlexPod Express:

Switch Cisco Nexus 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
```

Switch Cisco Nexus 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
```

Configurar las interfaces de gestión de almacenamiento y servidores

Las interfaces de gestión para el servidor y el almacenamiento suelen utilizar una sola VLAN. Por lo tanto, configure los puertos de la interfaz de gestión como puertos de acceso. Defina la VLAN de administración para cada switch y cambie el tipo de puerto de árbol expansivo a EDGE.

Desde el modo de configuración (`config t`), introduzca los siguientes comandos para configurar los ajustes del puerto para las interfaces de gestión tanto de los servidores como del almacenamiento:

Switch Cisco Nexus a

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Switch Cisco Nexus B

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Llevar a cabo la configuración global del canal de puertos virtuales

Un canal de puerto virtual (VPC) permite que los enlaces que están conectados físicamente a dos switches de Cisco Nexus diferentes aparezcan como un único canal de puerto a un tercer dispositivo. El tercer dispositivo puede ser un conmutador, un servidor o cualquier otro dispositivo de red. Un VPC puede proporcionar una multivía de nivel 2, que le permite crear redundancia aumentando el ancho de banda, permitiendo múltiples rutas paralelas entre los nodos y tráfico de equilibrio de carga donde haya rutas alternativas.

Un VPC proporciona las siguientes ventajas:

- Permitir que un único dispositivo utilice un canal de puerto a través de dos dispositivos de subida
- Eliminar puertos bloqueados del protocolo de árbol expansivo
- Proporciona una topología sin bucles
- Utilizando todo el ancho de banda disponible de enlace ascendente
- Proporcionar convergencia rápida si el enlace o un dispositivo falla
- Resiliencia a nivel de enlace
- Contribuir a proporcionar una alta disponibilidad

La función VPC requiere alguna configuración inicial entre los dos switches de Cisco Nexus para que funcionen correctamente. Si utiliza la configuración de mgmt0 de fondo, utilice las direcciones definidas en las interfaces y compruebe que se pueden comunicar mediante ping `[switch_A/B_mgmt0_ip_addr]vrf` comando de gestión.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para configurar la configuración global de VPC para ambos switches:

Switch Cisco Nexus 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
```

Switch Cisco Nexus 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
```

Configure los canales del puerto de almacenamiento

Las controladoras de almacenamiento de NetApp permiten una conexión activa-activa a la red mediante el protocolo de control de agregación de enlaces (LACP). El uso de LACP es preferido porque añade negociación y registro entre los switches. Debido a que la red está configurada para VPC, este enfoque permite disponer de conexiones activo-activo del almacenamiento para separar los switches físicos. Cada controladora tiene dos enlaces a cada uno de los switches. Sin embargo, los cuatro vínculos forman parte del mismo VPC y grupo de interfaces (IFGRP).

Desde el modo de configuración (`config t`), ejecute los siguientes comandos en cada uno de los switches para configurar las interfaces individuales y la configuración resultante del canal de puerto para los puertos conectados a la controladora AFF de NetApp.

1. Ejecute los siguientes comandos en el switch A y en el switch B a para configurar los canales de puertos de la controladora De almacenamiento A:

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. Ejecute los siguientes comandos en el switch A y en el switch B a para configurar los canales de puertos para la controladora de almacenamiento B.

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```

En esta validación de soluciones se utilizó una MTU de 9000. Sin embargo, en función de los requisitos de la aplicación, puede configurar un valor de MTU adecuado. Es importante establecer el mismo valor de MTU en la solución de FlexPod. Las configuraciones de MTU incorrectas entre componentes provocan la caída de paquetes y de estos paquetes.

Configurar las conexiones del servidor

Los servidores Cisco UCS tienen una tarjeta de interfaz virtual de dos puertos VIC1387, que se utiliza para el tráfico de datos y el arranque del sistema operativo ESXi mediante iSCSI. Estas interfaces se configuran para que se conmutan al nodo de respaldo entre sí, lo que proporciona redundancia adicional más allá de un solo enlace. Al distribuir estos enlaces a través de varios switches, el servidor puede sobrevivir incluso a un fallo

completo del switch.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para configurar los valores de puerto para las interfaces conectadas a cada servidor.

Switch Cisco Nexus A: Configuración de Cisco UCS Server-A y Cisco UCS Server-B.

```
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 Switch B: Configuración de Cisco UCS Server-A y Cisco UCS Server-B.

```
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
```

En esta validación de soluciones se utilizó una MTU de 9000. Sin embargo, en función de los requisitos de la aplicación, puede configurar un valor de MTU adecuado. Es importante establecer el mismo valor de MTU en la solución de FlexPod. Las configuraciones de MTU incorrectas entre componentes dejarán de tener paquetes y estos paquetes deberán transmitirse de nuevo. Esto afectará al rendimiento general de la solución.

Para escalar la solución añadiendo servidores Cisco UCS adicionales, ejecute los comandos anteriores con los puertos del switch a los que se han conectado los servidores recién añadidos en los switches A y B.

Enlace ascendente a la infraestructura de red existente

En función de la infraestructura de red disponible, se pueden utilizar varios métodos y funciones para elevar el entorno FlexPod. Si hay un entorno Cisco Nexus existente presente, NetApp recomienda el uso de VPC para elevar los switches Cisco Nexus 3172P incluidos en el entorno FlexPod a la infraestructura. Los enlaces ascendentes pueden ser enlaces de subida de 10 GbE para una solución de infraestructura de 10 GbE o 1

GbE para una solución de infraestructura de 1 GbE si fuera necesario. Los procedimientos descritos anteriormente se pueden utilizar para crear un VPC de enlace ascendente al entorno existente. Asegúrese de ejecutar Copy RUN START para guardar la configuración en cada switch una vez completada la configuración.

"Siguiente: Procedimiento de instalación de almacenamiento de NetApp (parte 1)"

Procedimiento de instalación de almacenamiento NetApp (parte 1)

En esta sección se describe el procedimiento de implementación del almacenamiento AFF de NetApp.

Instalación de la controladora de almacenamiento de NetApp serie AFF2xx

Hardware Universe de NetApp

La aplicación NetApp Hardware Universe (HWU) proporciona componentes de hardware y software compatibles con cualquier versión específica de ONTAP. Proporciona información de configuración para todos los dispositivos de almacenamiento de NetApp compatibles actualmente con el software ONTAP. También se proporciona una tabla de compatibilidades de componentes.

Confirme que los componentes de hardware y software que desea utilizar son compatibles con la versión de ONTAP que tiene previsto instalar:

1. Acceda a "HWU" aplicación para ver las guías de configuración del sistema. Haga clic en la pestaña controladoras para ver la compatibilidad entre distintas versiones del software ONTAP y los dispositivos de almacenamiento de NetApp con las especificaciones que desea.
2. Como alternativa, para comparar componentes por dispositivo de almacenamiento, haga clic en Comparar sistemas de almacenamiento.

Requisitos previos de la controladora de la serie AFF2XX
Para planificar la ubicación física de los sistemas de almacenamiento, consulte Hardware Universe de NetApp. Consulte las siguientes secciones: Requisitos eléctricos, cables de alimentación admitidos y puertos y cables integrados.

Controladoras de almacenamiento

Siga los procedimientos de instalación física de los controladores de la "Documentación de AFF A220".

ONTAP 9.4 de NetApp

Hoja de datos de configuración

Antes de ejecutar la secuencia de comandos de instalación, rellene la hoja de datos de configuración del manual del producto. La hoja de datos de configuración está disponible en la "Guía de configuración de software de ONTAP 9.4".

Este sistema se establece en una configuración de clúster de dos nodos sin switch.

La siguiente tabla muestra información sobre la instalación y la configuración de ONTAP 9.4.

Detalles del clúster	Valor de detalles de clúster
Nodo del clúster: Dirección IP	<<var_nodeA_mgmt_ip>>
Máscara de red Del nodo a del clúster	<<var_nodeA_mgmt_mask>>
Nodo del clúster: Puerta de enlace	<<var_nodeA_mgmt_gateway>>
Nombre del nodo a del clúster	<<var_nodeA>>
Dirección IP del nodo B del clúster	<<var_nodeB_mgmt_ip>>
Máscara de red del nodo B del clúster	<<var_nodeB_mgmt_mask>>
Puerta de enlace del nodo B del clúster	<<var_nodeB_mgmt_gateway>>
Nombre del nodo B del clúster	<<var_nodeB>>
Dirección URL de ONTAP 9.4	<<var_url_boot_software>>
El nombre del clúster	<<var_clustername>>
Dirección IP de gestión del clúster	<<var_clustermgmt_ip>>
Puerta de enlace del clúster B.	<<var_clustermgmt_gateway>>
Máscara de red del clúster B.	<<var_clustermgmt_mask>>
Nombre de dominio	<<var_domain_name>>
IP del servidor DNS (puede introducir más de uno)	<<var_dns_server_ip>>
La IP del servidor NTP (es posible introducir más de uno)	<<var_ntp_server_ip>>

Configure el nodo a

Para configurar el nodo A, complete los siguientes pasos:

1. Conéctese al puerto de la consola del sistema de almacenamiento. Tiene que ver un cargador-a del símbolo del sistema. Sin embargo, si el sistema de almacenamiento está en un bucle de reinicio, pulse Ctrl-C para salir del bucle de autoarranque cuando vea este mensaje:

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

2. Permita que el sistema arranque.

   ```
   autoboot
   ```

3. Pulse Ctrl-C para acceder al menú Inicio.

   Si ONTAP 9.4 no es la versión del software que se está arrancando, continúe con los pasos siguientes para instalar el software nuevo. Si ONTAP 9.4 es la versión que se va a arrancar, seleccione la opción 8 e y para reiniciar el nodo. A continuación, continúe con el paso 14.

4. Para instalar software nuevo, seleccione opción `7`.

5. Introduzca `y` para realizar una actualización.
6. Seleccione `e0M` para el puerto de red que desea usar para la descarga.
7. Introduzca `y` para reiniciar ahora.
8. Introduzca la dirección IP, la máscara de red y la puerta de enlace predeterminada para e0M en sus respectivos lugares.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. Especifique la dirección URL donde se puede encontrar el software.

   Este servidor web debe ser pingable.

```
<<var_url_boot_software>>
```

10. Pulse Intro para el nombre de usuario, indicando que no hay nombre de usuario.
11. Introduzca `y` para establecer el software recién instalado como el predeterminado que se utilizará para los siguientes reinicios.
12. Introduzca `y` para reiniciar el nodo.

    Al instalar el software nuevo, el sistema podría realizar actualizaciones de firmware en el BIOS y las tarjetas adaptadoras, lo que provoca reinicios y posibles interrupciones en el cargador. Si se producen estas acciones, el sistema podría desviarse de este procedimiento.

13. Pulse Ctrl-C para acceder al menú Inicio.
14. Seleccione opción `4` Para una configuración limpia y inicializar todos los discos.
15. Introduzca `y` para poner a cero discos, restablezca la configuración e instale un nuevo sistema de archivos.
16. Introduzca `y` para borrar todos los datos de los discos.

    La inicialización y creación del agregado raíz puede tardar 90 minutos o más en completarse, según el número y el tipo de discos conectados. Una vez finalizada la inicialización, el sistema de almacenamiento se reinicia. Tenga en cuenta que los SSD tardan mucho menos tiempo en inicializarse. Puede continuar con la configuración del nodo B mientras los discos del nodo A se están poniendo a cero.

17. Mientras el nodo A se está inicializando, empiece a configurar el nodo B.

Configure el nodo B

Para configurar el nodo B, complete los siguientes pasos:

1. Conéctese al puerto de la consola del sistema de almacenamiento. Tiene que ver un cargador-a del símbolo del sistema. Sin embargo, si el sistema de almacenamiento está en un bucle de reinicio, pulse Ctrl-C para salir del bucle de autoarranque cuando vea este mensaje:

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Pulse Ctrl-C para acceder al menú Inicio.

```
autoboot
```

3. Pulse Ctrl-C cuando se le solicite.

   Si ONTAP 9.4 no es la versión del software que se está arrancando, continúe con los pasos siguientes para instalar el software nuevo. Si ONTAP 9.4 es la versión que se va a arrancar, seleccione la opción 8 e y para reiniciar el nodo. A continuación, continúe con el paso 14.

4. Para instalar software nuevo, seleccione la opción 7.
5. Introduzca `y` para realizar una actualización.
6. Seleccione `e0M` para el puerto de red que desea usar para la descarga.
7. Introduzca `y` para reiniciar ahora.
8. Introduzca la dirección IP, la máscara de red y la puerta de enlace predeterminada para e0M en sus respectivos lugares.

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. Especifique la dirección URL donde se puede encontrar el software.

   Este servidor web debe ser pingable.

```
<<var_url_boot_software>>
```

10. Pulse Intro para el nombre de usuario, indicando que no hay nombre de usuario.
11. Introduzca `y` para establecer el software recién instalado como el predeterminado que se utilizará para los siguientes reinicios.
12. Introduzca `y` para reiniciar el nodo.

    Al instalar el software nuevo, el sistema podría realizar actualizaciones de firmware en el BIOS y las tarjetas adaptadoras, lo que provoca reinicios y posibles interrupciones en el cargador. Si se producen estas acciones, el sistema podría desviarse de este procedimiento.

13. Pulse Ctrl-C para acceder al menú Inicio.
14. Seleccione la opción 4 para Configuración limpia y inicializar todos los discos.
15. Introduzca `y` para poner a cero discos, restablezca la configuración e instale un nuevo sistema de archivos.
16. Introduzca `y` para borrar todos los datos de los discos.

La inicialización y creación del agregado raíz puede tardar 90 minutos o más en completarse, según el número y el tipo de discos conectados. Una vez finalizada la inicialización, el sistema de almacenamiento se reinicia. Tenga en cuenta que los SSD tardan mucho menos tiempo en inicializarse.

Continuación de la configuración del nodo A y de la configuración del clúster

Desde un programa de puertos de consola conectado al puerto de la consola De la controladora De almacenamiento A (nodo A), ejecute el script de configuración del nodo. Este script se muestra cuando ONTAP 9.4 arranca en el nodo por primera vez.

> El procedimiento de configuración del nodo y de los clústeres ha cambiado ligeramente en ONTAP 9.4. El asistente de configuración de clúster ahora se utiliza para configurar el primer nodo de un clúster, y System Manager se utiliza para configurar el clúster.

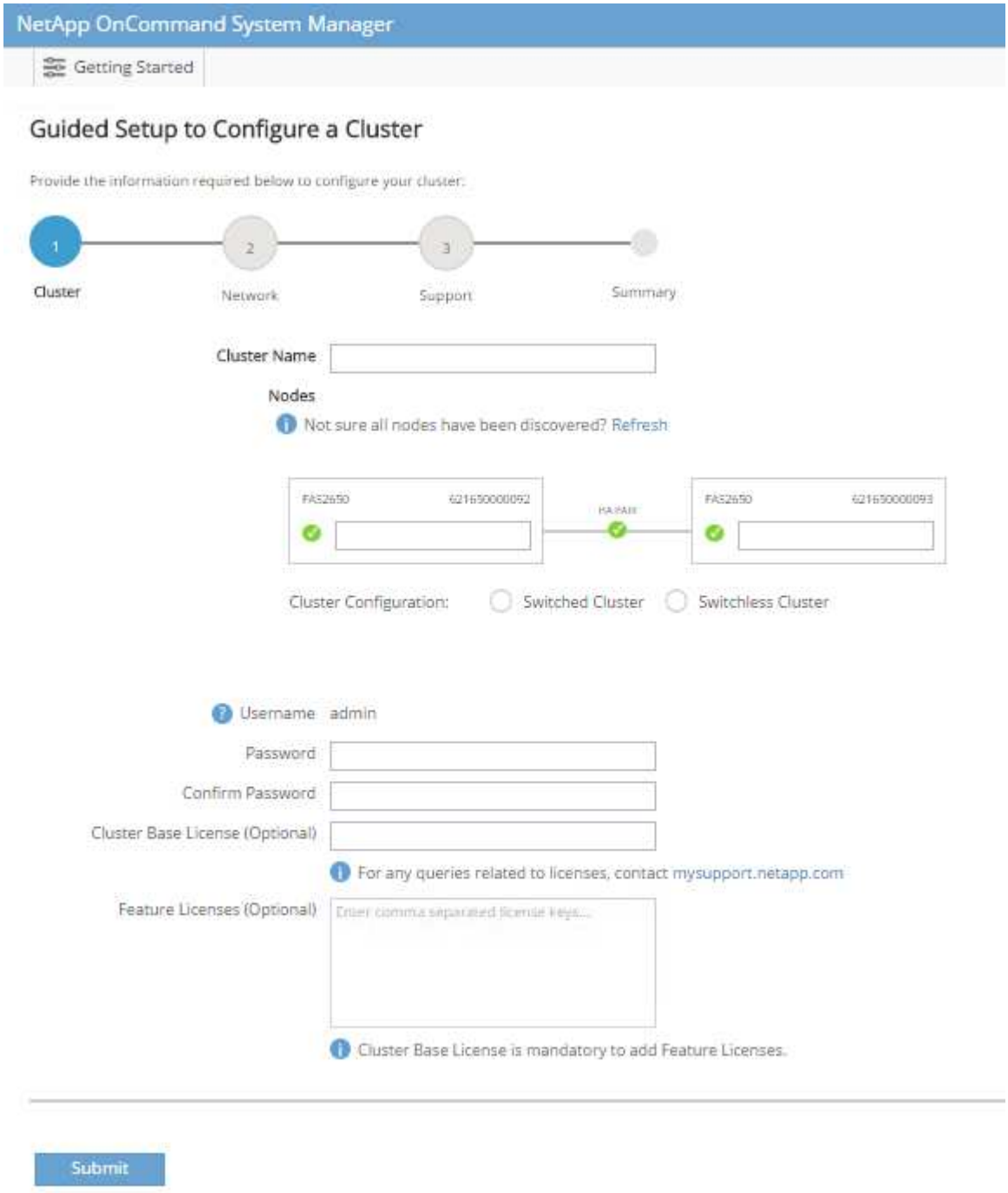
1. Siga las instrucciones para configurar el nodo A.

```
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. Vaya a la dirección IP de la interfaz de gestión del nodo.

La configuración del clúster también se puede realizar mediante la CLI. Este documento describe la configuración del clúster mediante la configuración guiada de System Manager de NetApp.

3. Haga clic en Guided Setup para configurar el clúster.
4. Introduzca `<<var_clustername>>` del nombre del clúster y. `<<var_nodeA>>` y.. `<<var_nodeB>>` para cada uno de los nodos que va a configurar. Introduzca la contraseña que desea usar para el sistema de almacenamiento. Seleccione Switchless Cluster para el tipo de clúster. Introduzca la licencia base del clúster.



5. También es posible introducir licencias de funciones para Cluster, NFS e iSCSI.
6. Ve un mensaje de estado que indica que el clúster se está creando. Este mensaje de estado cambia por varios Estados. Este proceso tarda varios minutos.

7. Configure la red.
   a. Anule la selección de la opción intervalo de direcciones IP.
   b. Introduzca `<<var_clustermgmt_ip>>` En el campo Cluster Management IP Address, `<<var_clustermgmt_mask>>` En el campo máscara de red, y. `<<var_clustermgmt_gateway>>` En el campo Puerta de enlace. Utilice el… Selector en el campo Port para seleccionar e0M del nodo A.
   c. La IP de gestión de nodos para el nodo A ya se ha rellenado. Introduzca `<<var_nodeA_mgmt_ip>>` Para el nodo B.
   d. Introduzca `<<var_domain_name>>` En el campo DNS Domain Name. Introduzca `<<var_dns_server_ip>>` En el campo DNS Server IP Address.

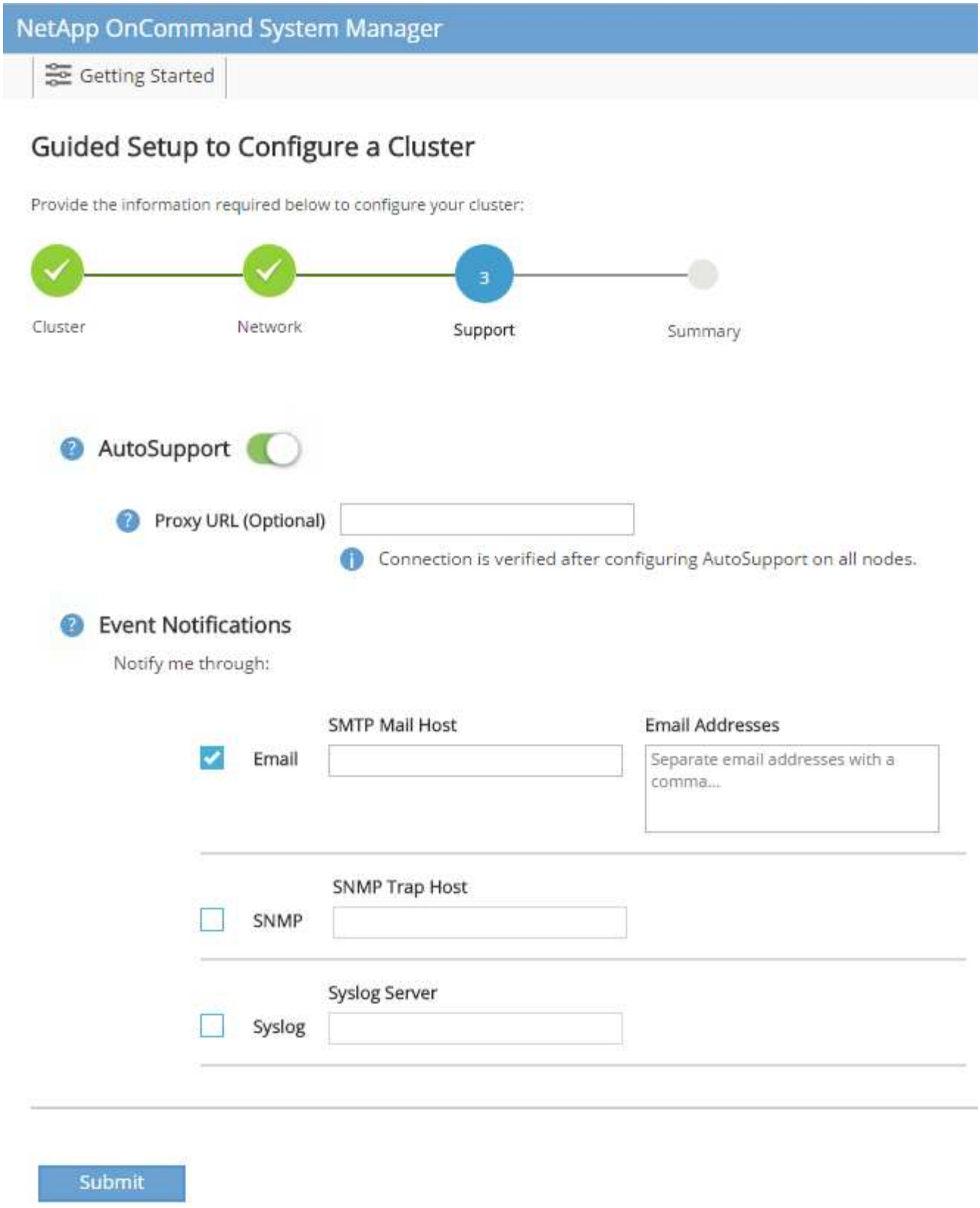
      Puede introducir varias direcciones IP del servidor DNS.

   e. Introduzca `<<var_ntp_server_ip>>` En el campo servidor NTP primario.

      También puede introducir un servidor NTP alternativo.

8. Configure la información de soporte.
   a. Si el entorno requiere un proxy para acceder a AutoSupport, introduzca la URL en Proxy URL.
   b. Introduzca el host de correo SMTP y la dirección de correo electrónico para las notificaciones de eventos.

      Debe, como mínimo, configurar el método de notificación de eventos antes de continuar. Puede seleccionar cualquiera de los métodos.



9. Cuando indique que ha finalizado la configuración del clúster, haga clic en Manage your Cluster para configurar el almacenamiento.

Continuación de la configuración del clúster de almacenamiento

Después de configurar los nodos de almacenamiento y el clúster base, puede continuar con la configuración del clúster de almacenamiento.

Ponga a cero todos los discos de repuesto

Para poner a cero todos los discos de repuesto del clúster, ejecute el siguiente comando:

```
disk zerospares
```

Configure la personalidad de los puertos UTA2 integrados

1. Verifique el modo actual y el tipo actual de puertos ejecutando el `ucadmin show` comando.

```
AFF A220::> ucadmin show
                      Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF A220_A     0c       fc       target     -        -          online
AFF A220_A     0d       fc       target     -        -          online
AFF A220_A     0e       fc       target     -        -          online
AFF A220_A     0f       fc       target     -        -          online
AFF A220_B     0c       fc       target     -        -          online
AFF A220_B     0d       fc       target     -        -          online
AFF A220_B     0e       fc       target     -        -          online
AFF A220_B     0f       fc       target     -        -          online
8 entries were displayed.
```

2. Compruebe que el modo actual de los puertos que se están utilizando es `cna` y que el tipo actual está establecido en `target`. De lo contrario, cambie la personalidad de puerto mediante el siguiente comando:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

Los puertos deben estar desconectados para que se ejecute el comando anterior. Para desconectar un puerto, ejecute el siguiente comando:

```
`network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down`
```

Si ha cambiado la personalidad del puerto, debe reiniciar cada nodo para que el cambio se aplique.

Cambiar el nombre de las interfaces lógicas de gestión (LIF)

Para cambiar el nombre de las LIF de administración, realice los pasos siguientes:

1. Muestra los nombres de las LIF de gestión actuales.

```
network interface show –vserver <<clustername>>
```

2. Cambie el nombre de la LIF de gestión del clúster.

```
network interface rename –vserver <<clustername>> –lif
cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
```

3. Cambie el nombre del LIF de gestión del nodo B.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF A220_B_1 -newname AFF A220-02_mgmt1
```

Configure la reversión automática en la gestión del clúster

Ajuste la `auto-revert` parámetro en la interfaz de gestión del clúster.

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-
revert true
```

Configure la interfaz de red del procesador de servicio

Para asignar una dirección IPv4 estática al procesador de servicios en cada nodo, ejecute los siguientes comandos:

```
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>>
```

Las direcciones IP de Service Processor deben estar en la misma subred que las direcciones IP de gestión de nodos.

Activar la recuperación tras fallos de almacenamiento en ONTAP

Para confirmar que la conmutación por error del almacenamiento está habilitada, ejecute los siguientes

comandos de una pareja de conmutación por error:

1. Comprobar el estado de recuperación tras fallos del almacenamiento.

```
storage failover show
```

   Ambas <<var_nodeA>> y.. <<var_nodeB>> debe poder realizar una toma de control. Vaya al paso 3 si los nodos pueden realizar una toma de control.

2. Habilite la conmutación al nodo de respaldo en uno de los dos nodos.

```
storage failover modify -node <<var_nodeA>> -enabled true
```

   Habilitar la conmutación al nodo de respaldo en un solo nodo permite que se produzca en ambos nodos.

3. Compruebe el estado de alta disponibilidad del clúster de dos nodos.

   Este paso no es aplicable para clústeres con más de dos nodos.

```
cluster ha show
```

4. Vaya al paso 6 si está configurada la alta disponibilidad. Si se ha configurado la alta disponibilidad, verá el siguiente mensaje al emitir el comando:

```
High Availability Configured: true
```

5. Habilite el modo de alta disponibilidad solo para el clúster de dos nodos.

   > No ejecute este comando para clústeres con más de dos nodos debido a que provoca problemas con la conmutación al nodo de respaldo.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. Compruebe que la asistencia de hardware está correctamente configurada y, si es necesario, modifique la dirección IP del partner.

```
storage failover hwassist show
```

   El mensaje `Keep Alive Status : Error: did not receive hwassist keep alive alerts from partner` indica que la asistencia de hardware no está configurada. Ejecute los siguientes comandos para configurar hardware Assist.

```
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>>
```

Cree un dominio de retransmisión MTU para tramas gigantes en ONTAP

Para crear un dominio de retransmisión de datos con un valor MTU de 9000, ejecute los siguientes comandos:

```
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
```

Quite los puertos de datos del dominio de retransmisión predeterminado

Los puertos de datos de 10 GbE se utilizan para el tráfico iSCSI/NFS y estos puertos deben eliminarse del dominio predeterminado. Los puertos e0e y e0f no se utilizan y deben eliminarse del dominio predeterminado.

Para quitar puertos del dominio de retransmisión, ejecute el siguiente comando:

```
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
```

Deshabilite el control de flujo en los puertos UTA2

Se recomienda utilizar las mejores prácticas de NetApp para deshabilitar el control de flujo en todos los puertos UTA2 conectados a dispositivos externos. Para desactivar el control de flujo, ejecute el siguiente comando:

```
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
```

Configure LACP con IFGRP en ONTAP

Este tipo de grupo de interfaces requiere dos o más interfaces Ethernet y un switch compatible con LACP. Asegúrese de que el interruptor está configurado correctamente.

Desde el símbolo del sistema del clúster, complete los siguientes pasos.

```
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
```

Configurar tramas gigantes en ONTAP de NetApp

Para configurar un puerto de red ONTAP para que utilice tramas gigantes (que normalmente tienen una MTU de 9,000 bytes), ejecute los siguientes comandos desde el shell del clúster:

```
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
```

Crear VLAN en ONTAP

Para crear VLAN en ONTAP, complete los siguientes pasos:

1. Cree puertos VLAN NFS y añádalos al dominio de retransmisión de datos.

```
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. Cree puertos VLAN iSCSI y añádalos al dominio de retransmisión de datos.

```
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. Cree puertos MGMT-VLAN.

```
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>>
```

Crear agregados en ONTAP

Durante el proceso de configuración de ONTAP, se crea un agregado que contiene el volumen raíz. Para crear agregados adicionales, determine el nombre del agregado, el nodo en el que se creará y el número de discos que contiene.

Para crear agregados, ejecute los siguientes comandos:

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

Conserve al menos un disco (seleccione el disco más grande) en la configuración como un repuesto. Una práctica recomendada es tener al menos un repuesto para cada tipo y tamaño de disco.

Empiece con cinco discos; puede añadir discos a un agregado cuando necesite almacenamiento adicional.

No se puede crear el agregado hasta que se complete el establecimiento en cero del disco. Ejecute el `aggr show` comando para mostrar el estado de creación del agregado. No continúe hasta `aggr1`_`nodeA` está en línea.

Configurar la zona horaria en ONTAP

Para configurar la sincronización horaria y establecer la zona horaria en el clúster, ejecute el siguiente comando:

```
timezone <<var_timezone>>
```

Por ejemplo, en el este de los Estados Unidos, la zona horaria es `America/New York`. Cuando haya comenzado a escribir el nombre de la zona horaria, pulse la tecla TAB para ver las opciones disponibles.

Configurar SNMP en ONTAP

Para configurar SNMP, realice los siguientes pasos:

1. Configure la información básica de SNMP, como la ubicación y el contacto. Cuando se sondean, esta información es visible como `sysLocation` y.. `sysContact` Variables en SNMP.

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. Configure las capturas SNMP para que se envíen a hosts remotos.

```
snmp traphost add <<var_snmp_server_fqdn>>
```

Configure SNMPv1 en ONTAP

Para configurar SNMPv1, establezca la contraseña de texto sin formato secreta compartida denominada comunidad.

```
snmp community add ro <<var_snmp_community>>
```

Utilice la `snmp community delete all` comando con precaución. Si se utilizan cadenas de comunidad para otros productos de supervisión, este comando las quita.

Configure SNMPv3 en ONTAP

SNMPv3 requiere que defina y configure un usuario para la autenticación. Para configurar SNMPv3, lleve a cabo los siguientes pasos:

1. Ejecute el `security snmpusers` Comando para ver el ID del motor.
2. Cree un usuario llamado `snmpv3user`.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. Introduzca el ID del motor de la entidad autoritativa y seleccione `md5` como protocolo de autenticación.
4. Escriba una contraseña de longitud mínima de ocho caracteres para el protocolo de autenticación cuando se le solicite.
5. Seleccione `des` como protocolo de privacidad.
6. Escriba una contraseña de longitud mínima de ocho caracteres para el protocolo de privacidad cuando se le solicite.

Configure HTTPS de AutoSupport en ONTAP

La herramienta AutoSupport de NetApp envía información de resumen de soporte a NetApp mediante HTTPS. Para configurar AutoSupport, ejecute el siguiente comando:

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Cree una máquina virtual de almacenamiento

Para crear una máquina virtual de almacenamiento (SVM) de infraestructura, complete los siguientes pasos:

1. Ejecute el `vserver create` comando.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. Añada el agregado de datos a la lista de agregados de infra-SVM para VSC de NetApp.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. Elimine los protocolos de almacenamiento que no se utilicen de la SVM, con lo que dejará NFS e iSCSI.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. Habilite y ejecute el protocolo NFS en la SVM de infra-SVM.

```
`nfs create -vserver Infra-SVM -udp disabled`
```

5. Encienda la `SVM vstorage` Parámetro para el plugin VAAI para NFS de NetApp. A continuación,

compruebe que NFS se ha configurado.

```
`vserver nfs modify –vserver Infra-SVM –vstorage enabled`
`vserver nfs show `
```

Los comandos están precedidos por `vserver` en la línea de comandos porque las máquinas virtuales de almacenamiento se denominaban servidores anteriormente.

Configure NFSv3 en ONTAP

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Host ESXi dirección IP de NFS	<<var_esxi_hostA_nfs_ip>>
Dirección IP de NFS del host ESXi B	<<var_esxi_hostB_nfs_ip>>

Para configurar NFS en la SVM, ejecute los siguientes comandos:

1. Cree una regla para cada host ESXi en la política de exportación predeterminada.
2. Asigne una regla para cada host ESXi que se cree. Cada host tiene su propio índice de reglas. El primer host ESXi tiene el índice de regla 1, el segundo host ESXi tiene el índice de regla 2, etc.

```
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. Asigne la política de exportación al volumen raíz de la SVM de infraestructura.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

VSC de NetApp gestiona automáticamente las políticas de exportación si decide instalarlas después de configurar vSphere. Si no lo instala, debe crear reglas de políticas de exportación cuando se añadan servidores C-Series de Cisco UCS adicionales.

Cree el servicio iSCSI en ONTAP

Para crear el servicio iSCSI, complete el paso siguiente:

1. Cree el servicio iSCSI en la SVM. Este comando también inicia el servicio iSCSI y establece el IQN de iSCSI para la SVM. Comprobar que iSCSI se ha configurado.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Crear reflejo de uso compartido de carga del volumen raíz de la SVM en ONTAP

1. Cree un volumen para que sea el reflejo de carga compartida del volumen raíz de la SVM de infraestructura en cada nodo.

```
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. Crear una programación de tareas para actualizar las relaciones de mirroring del volumen raíz cada 15 minutos.

```
job schedule interval create -name 15min -minutes 15
```

3. Cree las relaciones de mirroring.

```
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. Inicialice la relación de mirroring y compruebe que se haya creado.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

Configure el acceso HTTPS en ONTAP

Para configurar el acceso seguro a la controladora de almacenamiento, lleve a cabo los siguientes pasos:

1. Aumente el nivel de privilegio para acceder a los comandos de certificado.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. En general, ya se encuentra en funcionamiento un certificado autofirmado. Verifique el certificado ejecutando el siguiente comando:

```
security certificate show
```

3. Para cada SVM que se muestra, el nombre común de certificado debe coincidir con el FQDN de DNS de la SVM. Los cuatro certificados predeterminados deben eliminarse y sustituirse por certificados autofirmados o certificados de una entidad de certificación.

   La práctica recomendada es eliminar certificados caducados antes de crear certificados. Ejecute el `security certificate delete` comando para eliminar certificados caducados. En el siguiente comando, use LA TABULACIÓN automática para seleccionar y eliminar cada certificado predeterminado.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. Para generar e instalar certificados autofirmados, ejecute los siguientes comandos como comandos de una sola vez. Generar un certificado de servidor para la SVM de infraestructura y la SVM de clúster. De nuevo, utilice LA TABULACIÓN automática como ayuda para completar estos comandos.

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm. netapp.com
-type  server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. Para obtener los valores de los parámetros necesarios en el paso siguiente, ejecute el `security certificate show` comando.
6. Habilite cada certificado que se acaba de crear mediante el `-server-enabled true` y.. `-client-enabled false` parámetros. De nuevo, utilice LA TABULACIÓN automática.

```
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. Configure y habilite el acceso SSL y HTTPS y deshabilite el acceso HTTP.

```
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>>
```

Es normal que algunos de estos comandos devuelvan un mensaje de error indicando que la entrada no existe.

8. Vuelva al nivel de privilegio de administrador y cree la configuración para permitir que la SVM esté disponible en la web.

```
set –privilege admin
vserver services web modify –name spi|ontapi|compat –vserver * -enabled
true
```

Cree un volumen de FlexVol de NetApp en ONTAP

Para crear un volumen de FlexVol de NetApp, introduzca el nombre, el tamaño y el agregado del volumen en el que existe. Crear dos volúmenes de almacenes de datos de VMware y un volumen de arranque del servidor.

```
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
```

Habilite la deduplicación en ONTAP

Para activar la deduplicación en volúmenes adecuados, ejecute los siguientes comandos:

```
volume efficiency on –vserver Infra-SVM -volume infra_datastore_1
volume efficiency on –vserver Infra-SVM -volume esxi_boot
```

Crear LUN en ONTAP

Para crear dos LUN de arranque, ejecute los siguientes comandos:

```
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
```

Cuando se añade un servidor Cisco UCS C-Series adicional, se debe crear un LUN de arranque adicional.

Creación de LIF iSCSI en ONTAP

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Nodo de almacenamiento a iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
Nodo de almacenamiento: Una máscara de red LIF01A de iSCSI	<<var_nodeA_iscsi_lif01a_mask>>
Nodo de almacenamiento a iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
Nodo de almacenamiento a máscara de red LIF01B de iSCSI	<<var_nodeA_iscsi_lif01b_mask>>
Nodo de almacenamiento B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
Máscara de red del nodo de almacenamiento B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_mask>>
ISCSI LIF01B del nodo de almacenamiento	<<var_nodeB_iscsi_lif01b_ip>>
Máscara de red LIF01B de nodo de almacenamiento B.	<<var_nodeB_iscsi_lif01b_mask>>

1. Creación de cuatro LIF iSCSI, dos en cada nodo.

```
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
```

Creación de LIF NFS en ONTAP

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Nodo de almacenamiento: LIF NFS 01 IP	<<var_nodeA_nfs_lif_01_ip>>
Nodo de almacenamiento máscara de red a LIF 01 de NFS	<<var_nodeA_nfs_lif_01_mask>>
Nodo de almacenamiento B LIF NFS 02 IP	<<var_nodeB_nfs_lif_02_ip>>
Máscara de red del nodo de almacenamiento B LIF NFS 02	<<var_nodeB_nfs_lif_02_mask>>

1. Cree una LIF NFS.

```
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
```

Añada el administrador de SVM de infraestructura

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
IP de Vsmgmt	<<var_svm_mgmt_ip>>
Máscara de red Vsmgmt	<<var_svm_mgmt_mask>>
Puerta de enlace predeterminada de Vsmgmt	<<var_svm_mgmt_gateway>>

Para añadir la interfaz lógica de administración de SVM y el administrador de SVM de la infraestructura a la red de gestión, realice los siguientes pasos:

1. Ejecute el siguiente comando:

```
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
```

> La IP de administración de SVM aquí debe estar en la misma subred que la IP de administración del clúster de almacenamiento.

2. Cree una ruta predeterminada para permitir que la interfaz de gestión de SVM llegue al mundo exterior.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. Establezca una contraseña para el usuario de SVM vsadmin y desbloquee el usuario.

```
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
```

"Siguiente: Procedimiento de puesta en marcha de servidores en rack Cisco UCS C-Series"

Procedimiento para la puesta en marcha de servidores en rack Cisco UCS C-Series

En la siguiente sección, se proporciona un procedimiento detallado para configurar un servidor de montaje en rack independiente Cisco UCS C-Series para su uso en la configuración de FlexPod Express.

Realice la configuración inicial del servidor independiente Cisco UCS C-Series para Cisco Integrated Management Server

Complete estos pasos para la configuración inicial de la interfaz de CIMC para servidores independientes Cisco UCS C-Series.

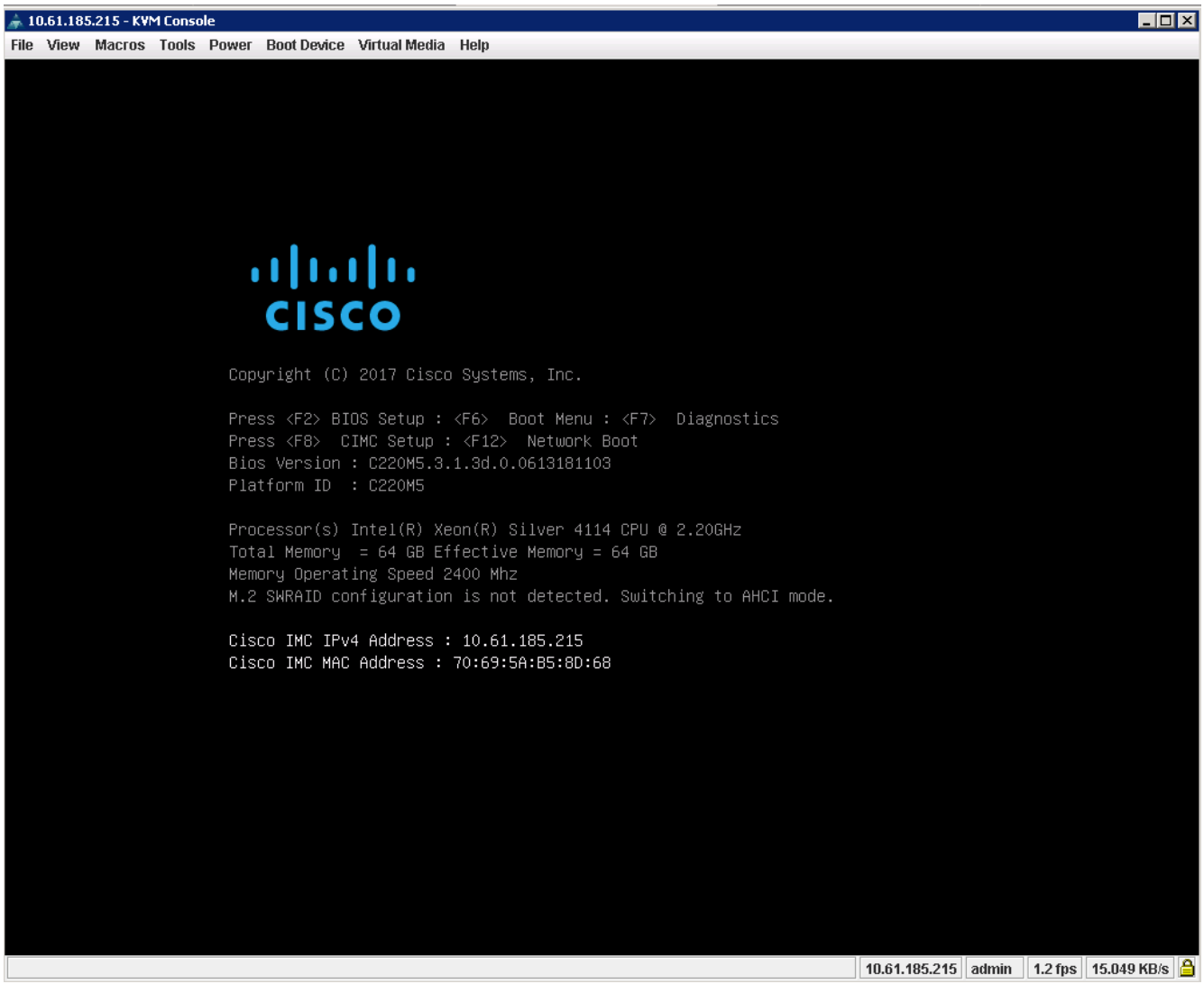
En la siguiente tabla se enumera la información necesaria para configurar CIMC para cada servidor independiente Cisco UCS C-Series.

Detalles	Valor de detalle
Dirección IP de CIMC	<<cimc_ip>>
Máscara de subred CIMC	<<cimc_netmask>>
Puerta de enlace predeterminada CIMC	<<cimc_gateway>>

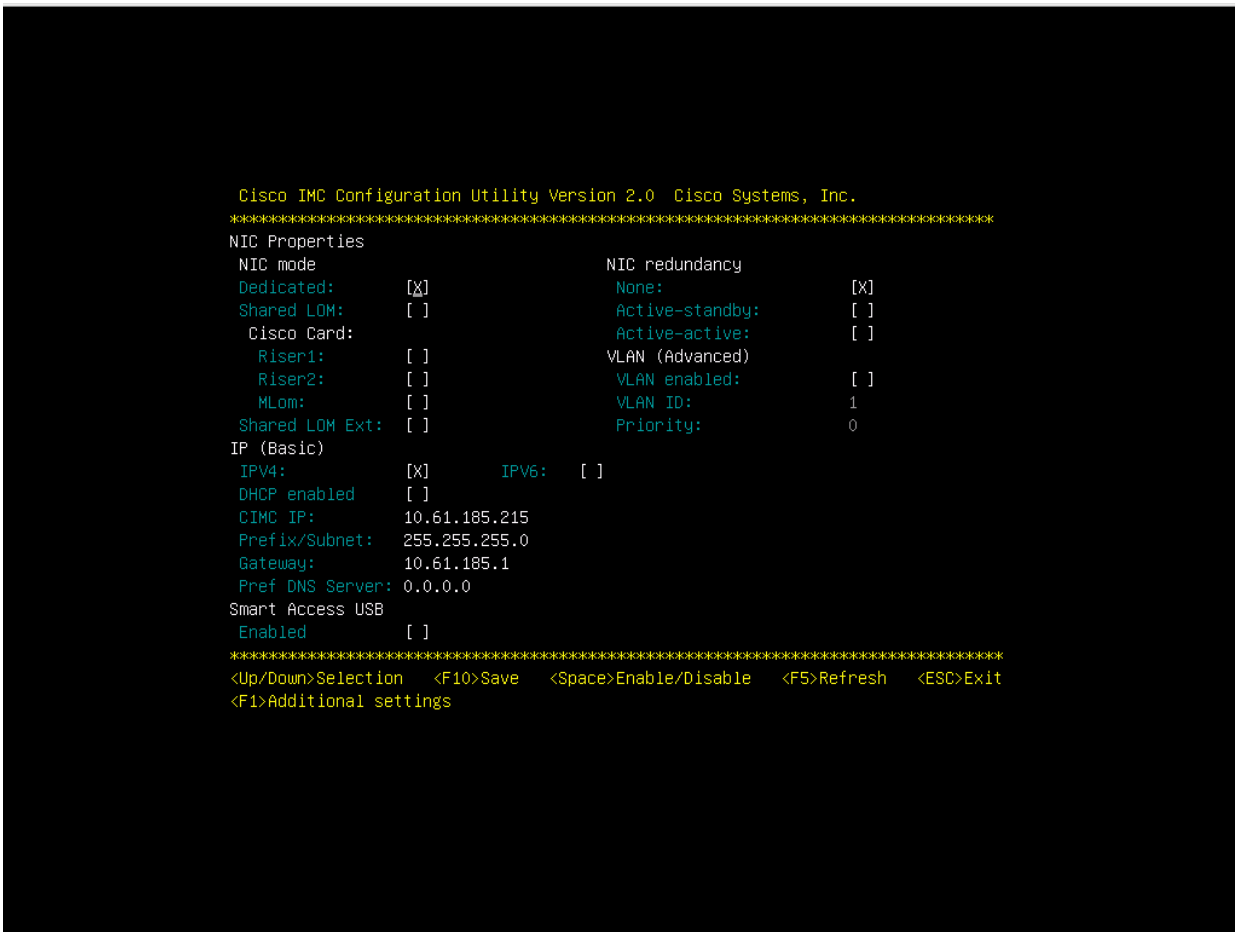
La versión de CIMC utilizada en esta validación es CIMC 3.1.3(g).

Todos los servidores

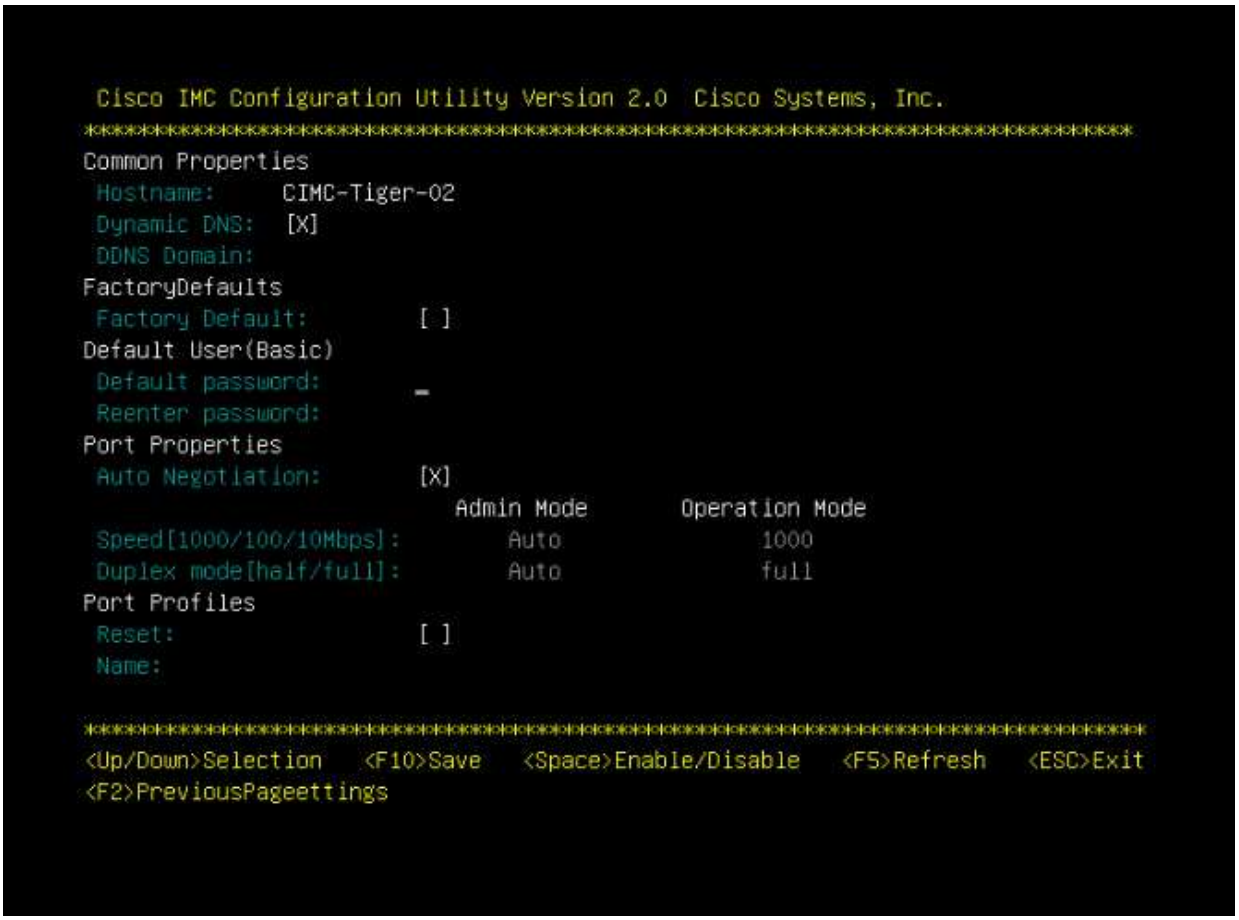
1. Conecte la mochila del teclado, vídeo y ratón (KVM) de Cisco (suministrada con el servidor) al puerto KVM de la parte frontal del servidor. Conecte un monitor VGA y un teclado USB a los puertos de mochila KVM adecuados.
2. Encienda el servidor y pulse F8 cuando se le solicite que introduzca la configuración de CIMC.



3. En la utilidad de configuración de CIMC, defina las siguientes opciones:
   - Modo de tarjeta de interfaz de red (NIC):
     - Dedicado [X]
   - IP (básico):
     - IPV4: [X]
     - DHCP habilitado: [ ]
     - IP de CIMC: <<cimc_ip>>
     - Prefijo/subred: <<cimc_netmask>>
     - Puerta de enlace: <<cimc_gateway>>
   - VLAN (Advanced): Deje borrado para deshabilitar el etiquetado VLAN.
     - Redundancia NIC
     - Ninguna: [X]



4. Pulse F1 para ver los ajustes adicionales.
   - Propiedades comunes:
     - Nombre del host: <<esxi_host_name>>
     - DNS dinámico: [ ]
     - Valores predeterminados de fábrica: Dejar borrado.
   - Usuario predeterminado (básico):
     - Contraseña predeterminada: <<admin_password>>
     - Vuelva a introducir la contraseña: <<admin_password>>
     - Propiedades del puerto: Utilice los valores predeterminados.
     - Perfiles de puerto: Dejar borrado.



5. Pulse F10 para guardar la configuración de la interfaz CIMC.
6. Una vez guardada la configuración, pulse Esc para salir.

Configurar arranque iSCSI de los servidores Cisco UCS C-Series

En esta configuración de FlexPod Express, la VIC1387 se utiliza para el arranque iSCSI.

La tabla siguiente enumera la información necesaria para configurar el arranque iSCSI.

La fuente en cursiva indica las variables que son únicas de cada host ESXi.

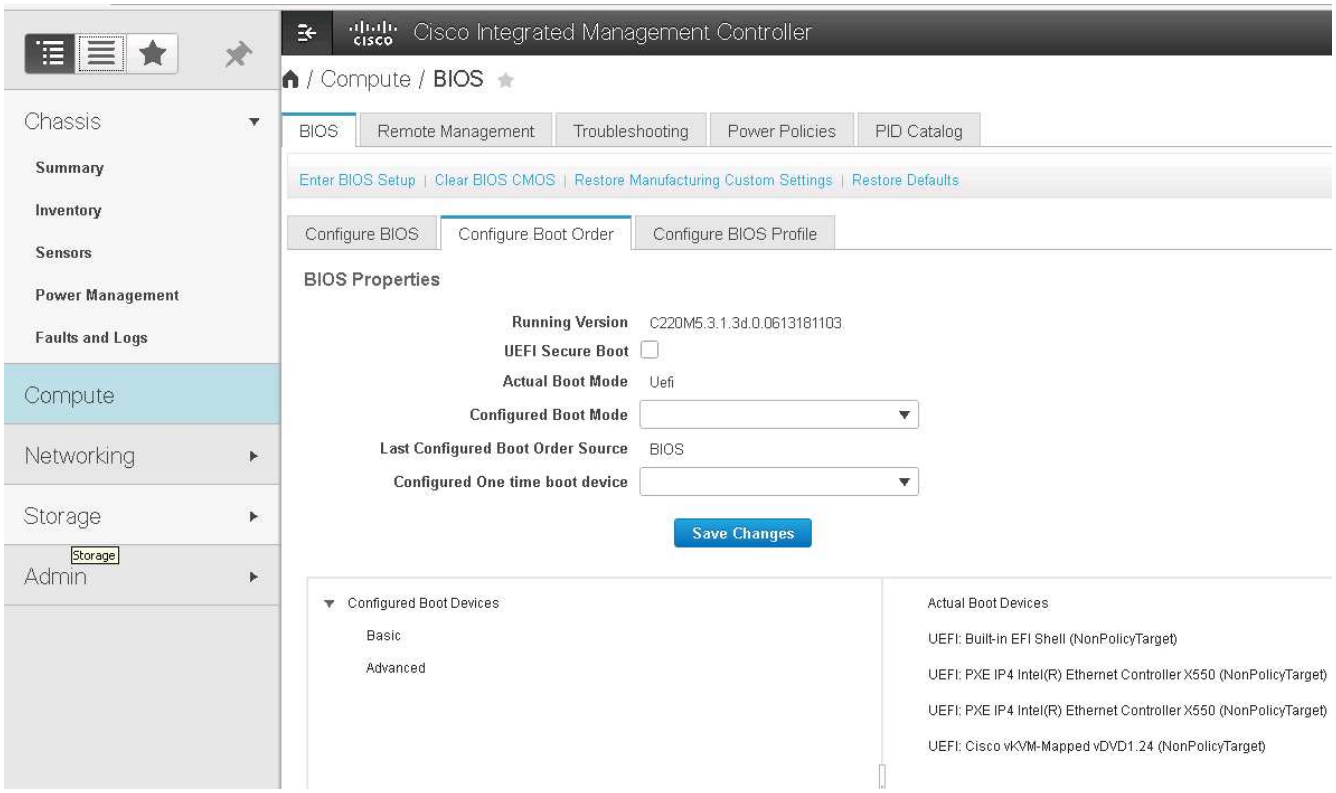
Detalles	Valor de detalle
Nombre Del iniciador del host ESXi	<<var_ucs_initiator_name_A>>
Host ESXi iSCSI-A IP	<<var_esxi_host_iscsiA_ip>>
Máscara de red iSCSI-A del host ESXi	<<var_esxi_host_iscsiA_mask>>
ISCSI del host ESXi: Puerta de enlace predeterminada	<<var_esxi_host_iscsiA_gateway>>
Nombre B del iniciador del host ESXi	<<var_ucs_initiator_name_B>>
Host ESXi iSCSI-B IP	<<var_esxi_host_iscsiB_ip>>
Máscara de red iSCSI-B del host ESXi	<<var_esxi_host_iscsiB_mask>>
Puerta de enlace iSCSI-B del host ESXi	<<var_esxi_host_iscsiB_gateway>>

Detalles	Valor de detalle
Dirección IP iscsi_lif01a	
Dirección IP iscsi_lif02a	
Dirección IP iscsi_lif01b	
Dirección IP iscsi_lif02b	
IQN de infr_SVM	

Configuración del orden de arranque

Para establecer la configuración del orden de arranque, lleve a cabo los siguientes pasos:

1. En la ventana del explorador de la interfaz CIMC, haga clic en la ficha servidor y seleccione BIOS.
2. Haga clic en Configurar orden de arranque y, a continuación, en Aceptar.



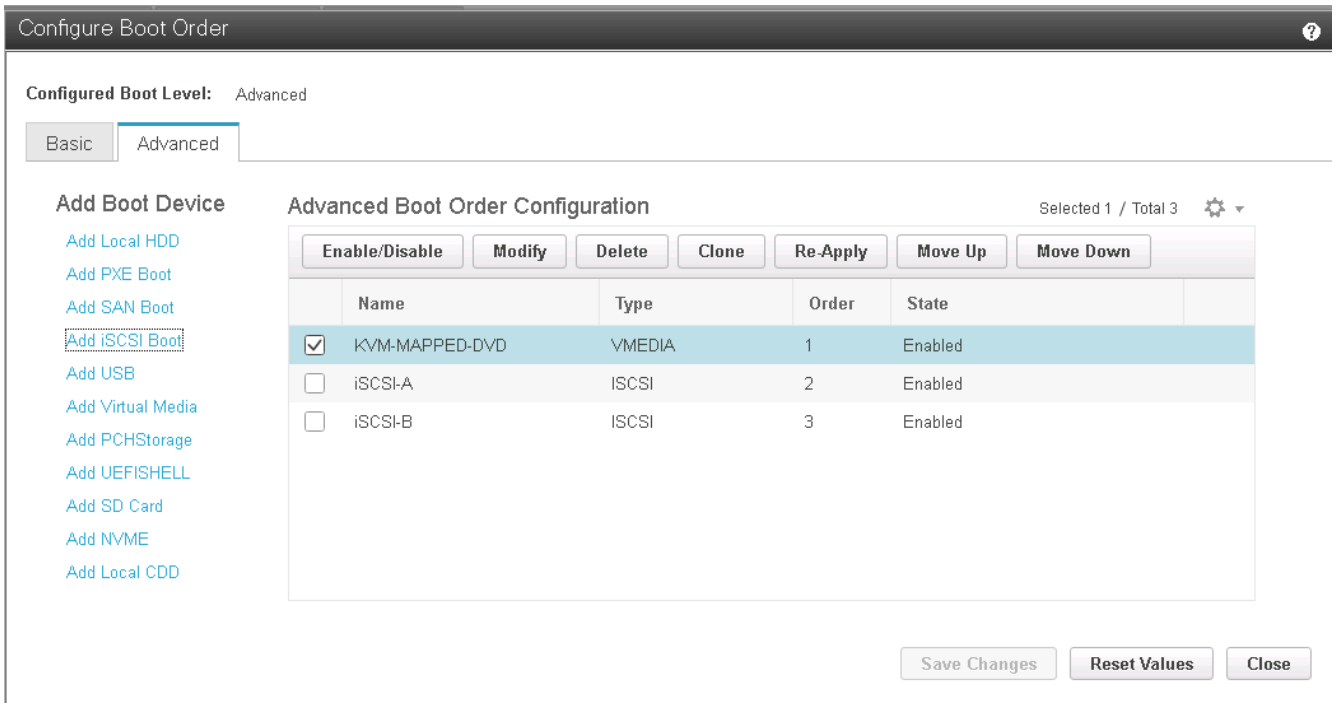
3. Para configurar los siguientes dispositivos, haga clic en el dispositivo en Agregar dispositivo de arranque y vaya a la ficha Opciones avanzadas.
   - Agregar medios virtuales
     - NOMBRE: KVM-CD-DVD
     - SUBTIPO: DVD KVM ASIGNADO
     - Estado: Habilitado
     - Orden: 1
   - Agregar arranque iSCSI.
     - Nombre: ISCSI-a

- Estado: Habilitado
- Orden: 2
- Ranura: MLOM
- Puerto: 0

◦ Haga clic en Add iSCSI Boot.

- Nombre: ISCSI-B
- Estado: Habilitado
- Pedido: 3
- Ranura: MLOM
- Puerto: 1

4. Haga clic en Agregar dispositivo.
5. Haga clic en Save Changes y, a continuación, en Close.

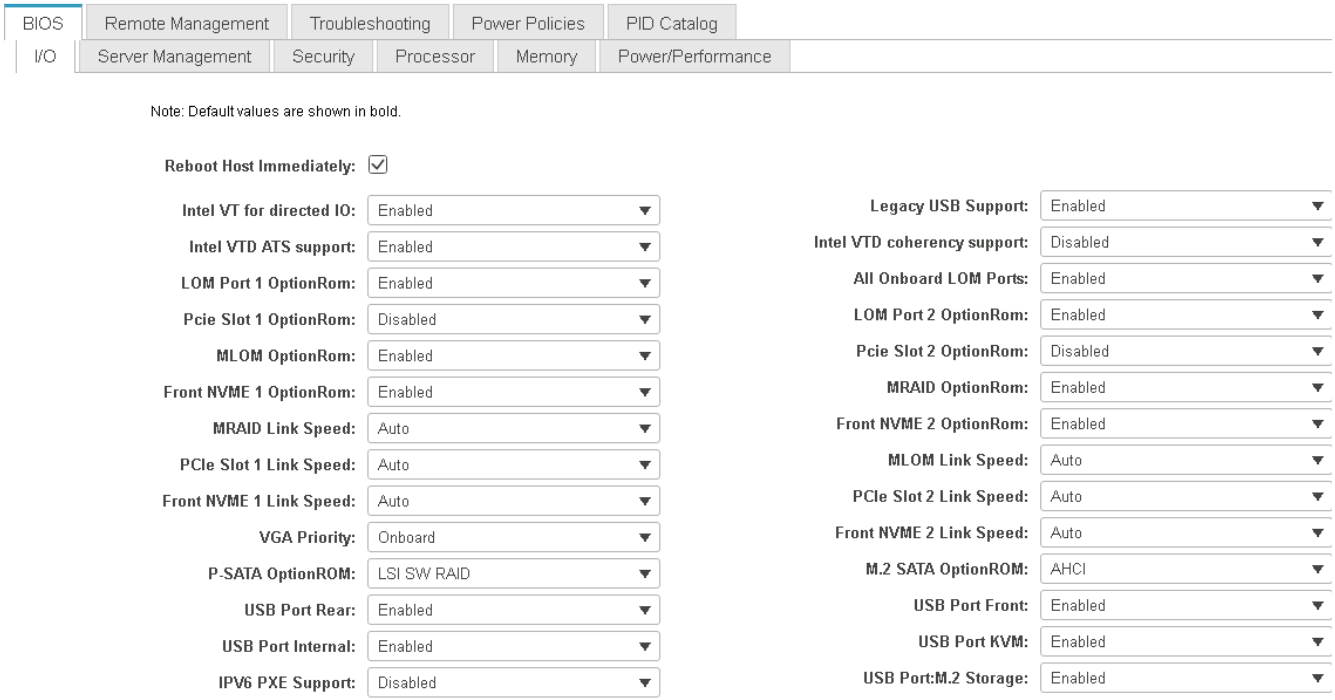


6. Reinicie el servidor para arrancar con el nuevo orden de inicio.

Desactivar la controladora RAID (si existe)

Siga estos pasos si el servidor C-Series contiene una controladora RAID. No se necesita una controladora RAID en el arranque desde la configuración SAN. De manera opcional, también puede quitar físicamente la controladora RAID del servidor.

1. Haga clic en BIOS en el panel de navegación izquierdo de CIMC.
2. Seleccione Configurar BIOS.
3. Desplácese hacia abajo hasta la ranura PCIe:ROM de opción HBA.
4. Si el valor no está desactivado, configúrelo en Desactivado.



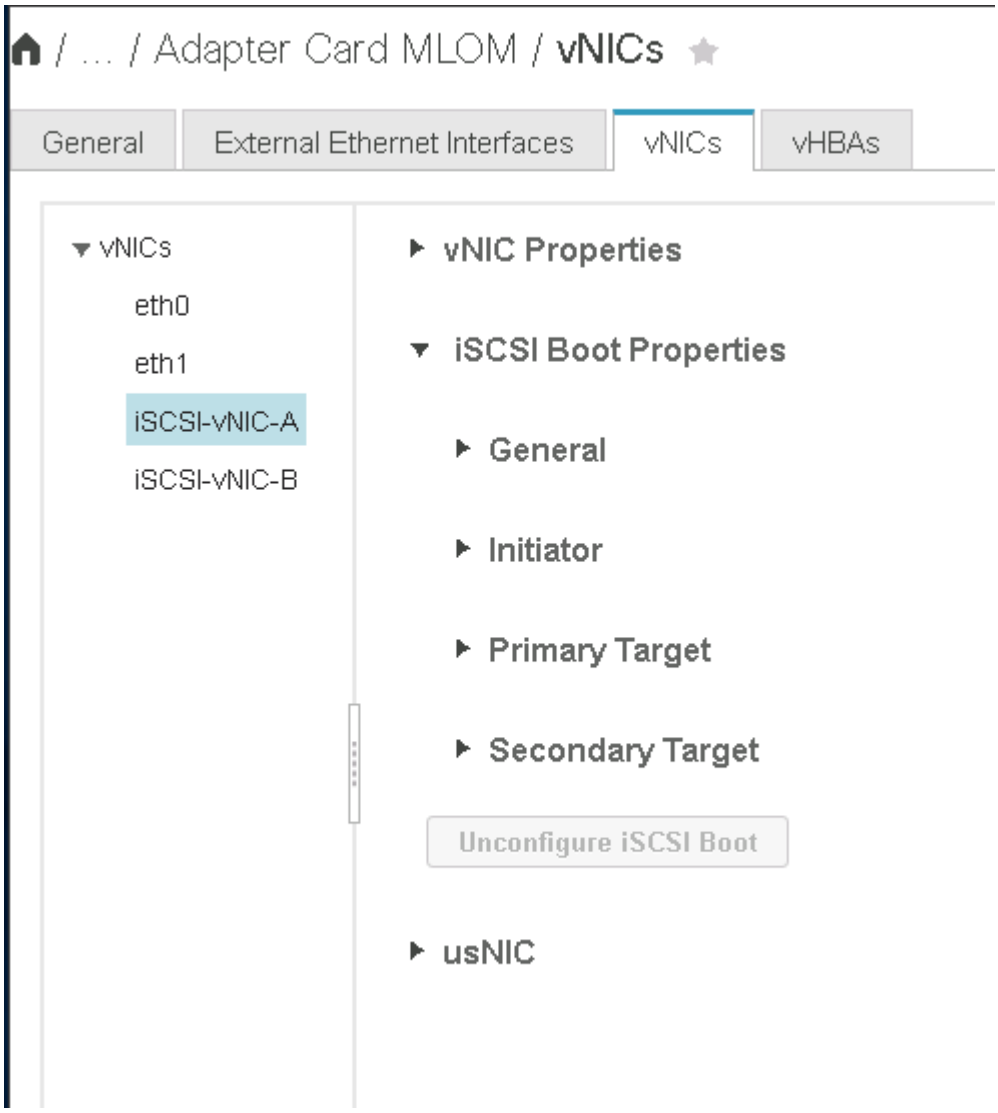
Configure Cisco VIC1387 para el arranque iSCSI

Los pasos de configuración siguientes son para el VIC 1387 de Cisco para arranque iSCSI.

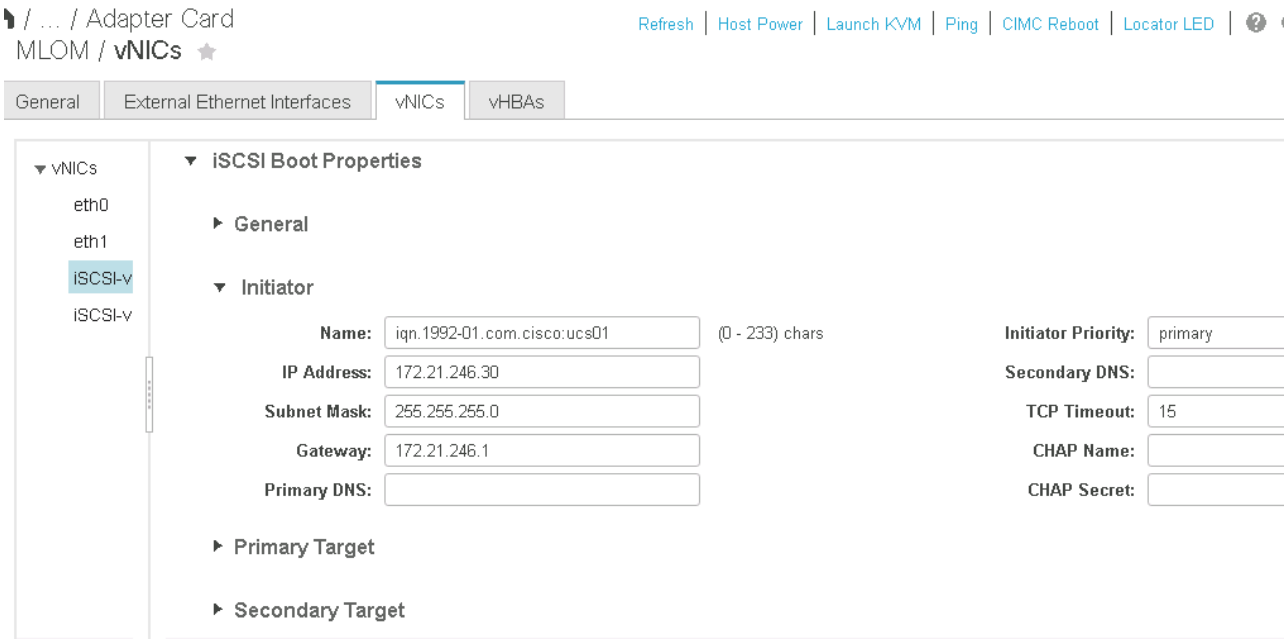
Cree NIC iSCSI

1. Haga clic en Agregar para crear un VNIC.
2. En la sección Agregar VNIC, introduzca los siguientes ajustes:
   - Nombre: ISCSI-VNIC-A
   - MTU: 9000
   - VLAN predeterminada: `<<var_iscsi_vlan_a>>`
   - Modo VLAN: TRONCO
   - Activar inicio PXE: Comprobación

3. Haga clic en Agregar VNIC y, a continuación, en Aceptar.
4. Repita el proceso para agregar un segundo VNIC.
   a. Nombre el VNIC `iSCSI-vNIC-B`.
   b. Introduzca `<<var_iscsi_vlan_b>>` Como VLAN.
   c. Establezca el puerto de enlace ascendente en `1`.
5. Seleccione el VNIC `iSCSI-vNIC-A` a la izquierda.



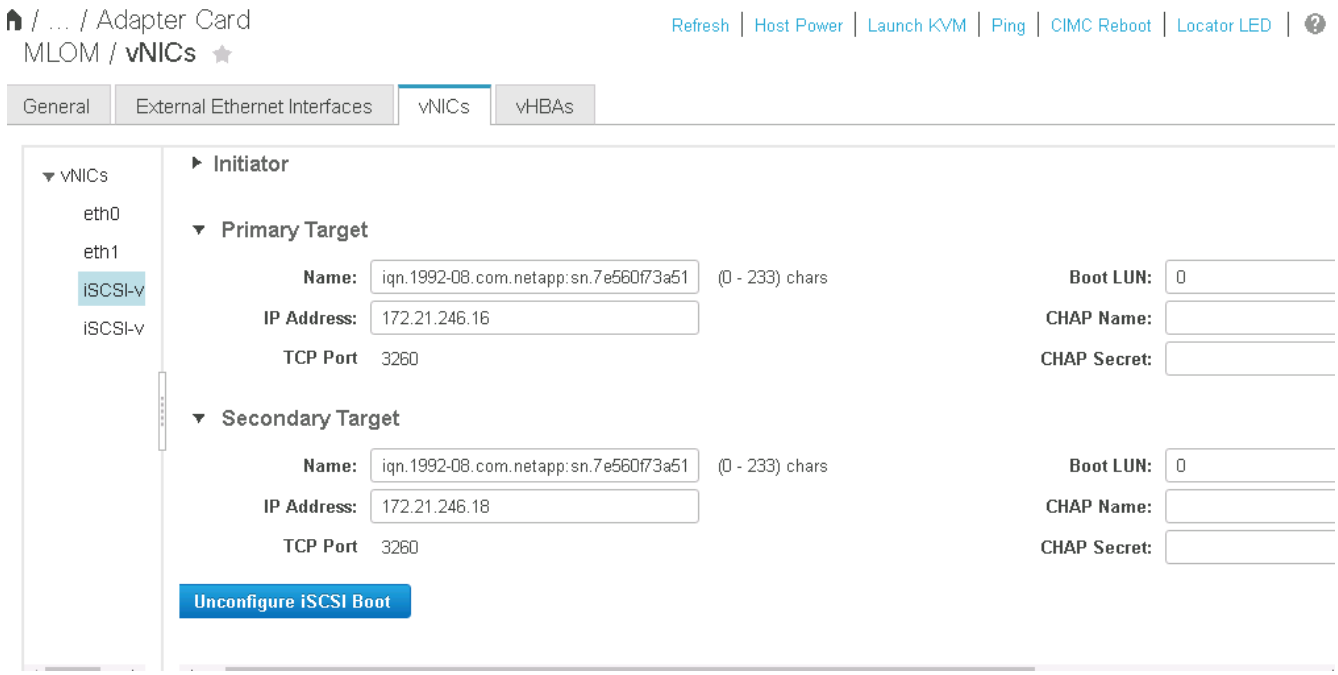
6. En Propiedades de arranque iSCSI, introduzca los detalles del iniciador:
   - Nombre: <<var_ucsa_initiator_name_a>>
   - Dirección IP: <<var_esxi_hostA_iscsiA_ip>>
   - Máscara de subred: <<var_esxi_hostA_iscsiA_mask>>
   - Puerta de enlace: <<var_esxi_hostA_iscsiA_gateway>>



7. Introduzca los detalles del destino principal.
   - Nombre: Número IQN de infra-SVM
   - Dirección IP: Dirección IP de `iscsi_lif01a`
   - LUN de arranque: 0
8. Introduzca los detalles del destino secundario.
   - Nombre: Número IQN de infra-SVM
   - Dirección IP: Dirección IP de `iscsi_lif02a`
   - LUN de arranque: 0

   Puede obtener el número IQN de almacenamiento ejecutando el `vserver iscsi show` comando.

   > Asegúrese de registrar los nombres IQN de cada VNIC. Se necesitan para un paso más adelante.



9. Haga clic en Configurar iSCSI.
10. Seleccione el VNIC `iSCSI-vNIC- B` Y haga clic en el botón de arranque iSCSI que se encuentra en la parte superior de la sección interfaces de Ethernet del host.
11. Repita el proceso para configurar `iSCSI-vNIC-B`.
12. Introduzca los detalles del iniciador.
    - Nombre: `<<var_ucsa_initiator_name_b>>`
    - Dirección IP: `<<var_esxi_hostb_iscsib_ip>>`
    - Máscara de subred: `<<var_esxi_hostb_iscsib_mask>>`
    - Puerta de enlace: `<<var_esxi_hostb_iscsib_gateway>>`
13. Introduzca los detalles del destino principal.
    - Nombre: Número IQN de infra-SVM
    - Dirección IP: Dirección IP de `iscsi_lif01b`
    - LUN de arranque: 0
14. Introduzca los detalles del destino secundario.
    - Nombre: Número IQN de infra-SVM
    - Dirección IP: Dirección IP de `iscsi_lif02b`
    - LUN de arranque: 0

    Puede obtener el número de IQN de almacenamiento mediante el `vserver iscsi show` comando.

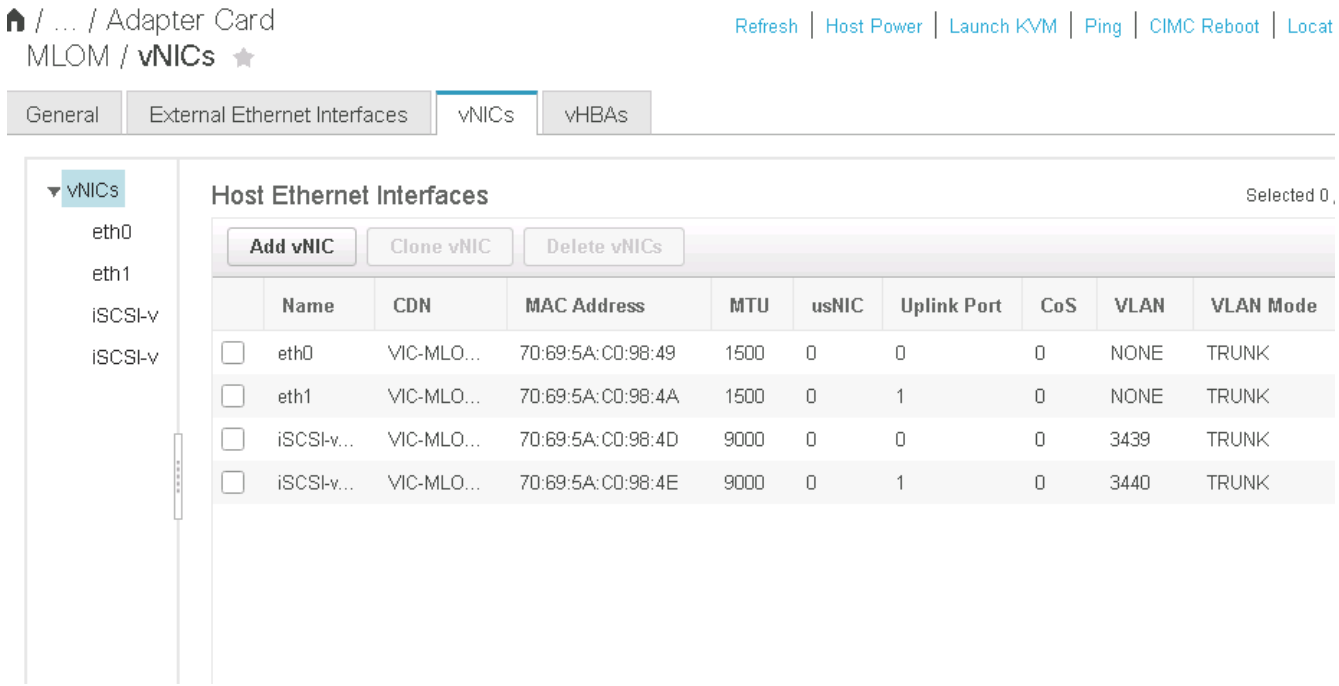
    Asegúrese de registrar los nombres IQN de cada VNIC. Se necesitan para un paso más adelante.

15. Haga clic en Configurar ISCSI.

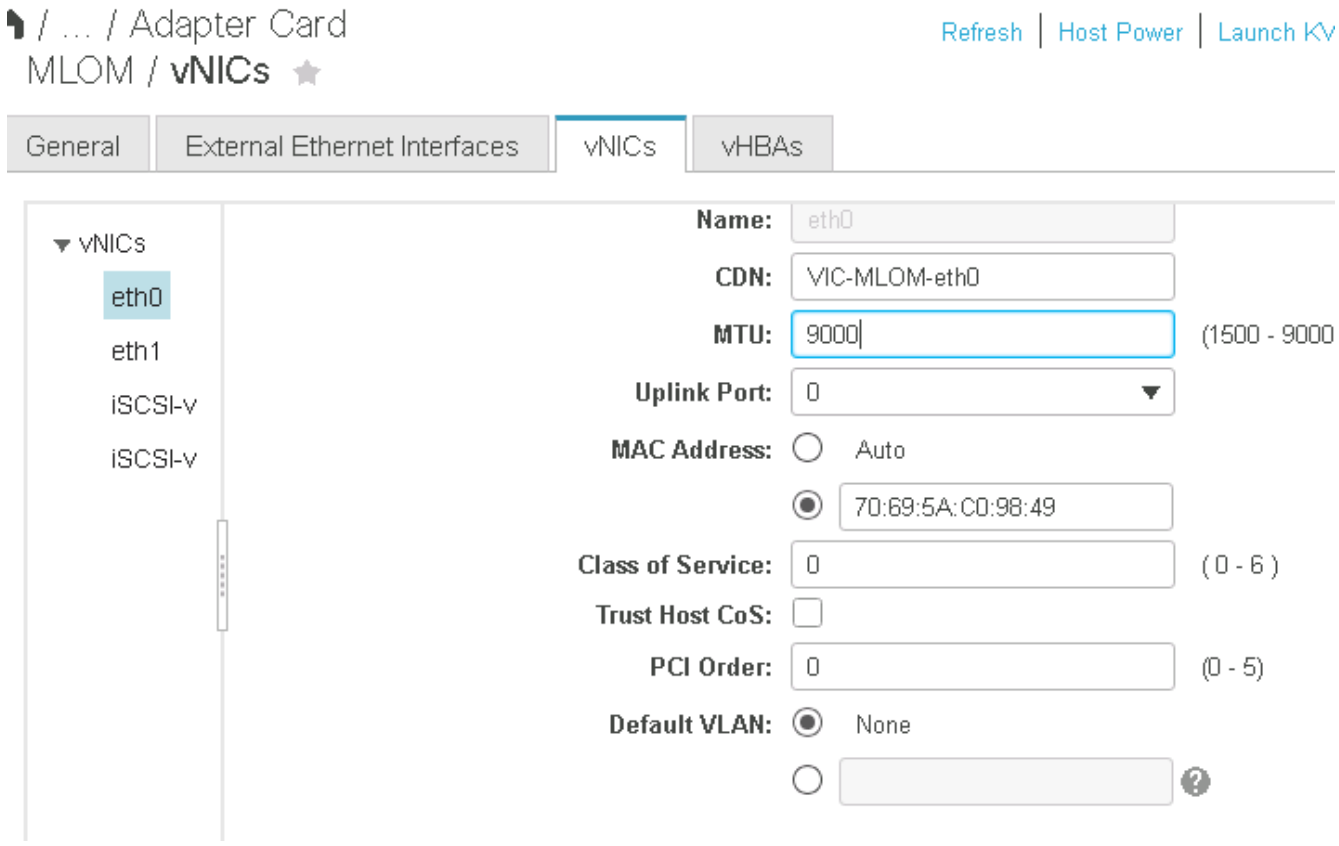
16. Repita este proceso para configurar el arranque iSCSI para el servidor Cisco UCS B.

Configure las NIC virtuales para ESXi

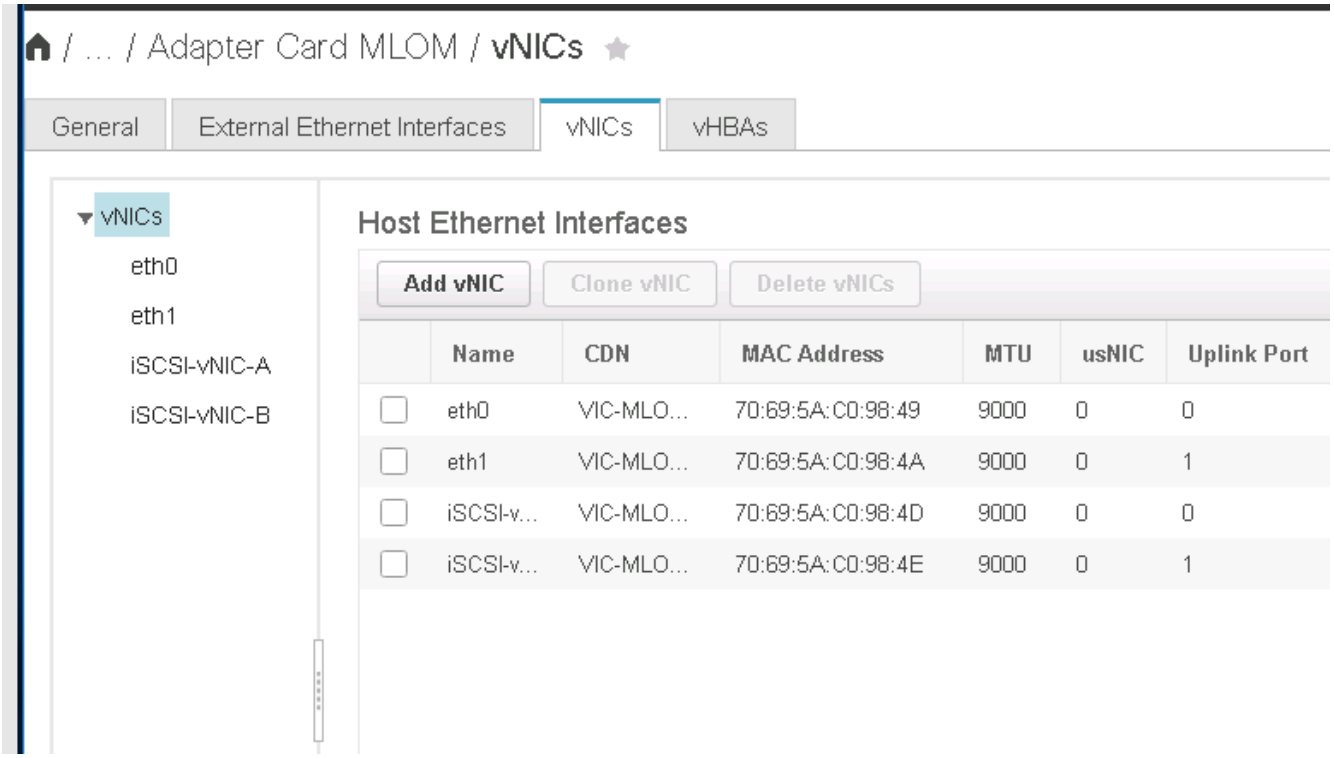
1. En la ventana del navegador de la interfaz CIMC, haga clic en Inventario y, a continuación, en Adaptadores Cisco VIC en el panel derecho.
2. En Tarjetas de adaptador, seleccione Cisco UCS VIC 1387 y, a continuación, seleccione las NIC de abajo.



3. Seleccione eth0 y haga clic en Propiedades.
4. Establezca la MTU en 9000. Haga clic en Save Changes.



5. Repita los pasos 3 y 4 en eth1, comprobando que el puerto de enlace ascendente está configurado en `1` en eth1.



Este procedimiento se debe repetir para cada nodo inicial de Cisco UCS Server y cada nodo adicional de Cisco UCS Server que se agregue al entorno.

"Siguiente: Procedimiento de implementación de almacenamiento AFF de NetApp (parte 2)"

Procedimiento de instalación de almacenamiento AFF de NetApp (parte 2)

Configuración del almacenamiento DE arranque SAN de ONTAP

Cree iGroups iSCSI

Para crear iGroups, complete el paso siguiente:

Para este paso, se necesitan los IQN de iniciadores iSCSI desde la configuración del servidor.

1. Desde la conexión SSH del nodo de gestión del clúster, ejecute los siguientes comandos. Para ver los tres iGroups creados en este paso, ejecute el comando igroup show.

```
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>>
```

Este paso se debe completar cuando se añaden servidores Cisco UCS C- Series adicionales.

Asigne LUN de arranque a iGroups

Para asignar LUN de arranque a iGroups, ejecute los siguientes comandos desde la conexión SSH de administración del clúster:

```
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
```

Este paso se debe completar cuando se añaden servidores Cisco UCS C-Series adicionales.

"Siguiente: Procedimiento de puesta en marcha de VMware vSphere 6.7."

Procedimiento de puesta en marcha de VMware vSphere 6.7

En esta sección, se proporcionan los procedimientos detallados para la instalación de VMware ESXi 6.7 en una configuración exprés de FlexPod. Los procedimientos de implementación siguientes se personalizan para incluir las variables de entorno descritas en secciones anteriores.

Existen varios métodos para instalar VMware ESXi en dicho entorno. Este procedimiento utiliza la consola

KVM virtual y las funciones de medios virtuales de la interfaz CIMC para servidores Cisco UCS C-Series para asignar medios de instalación remotos a cada servidor individual.

Este procedimiento se debe completar para el servidor Cisco UCS A y el servidor Cisco UCS B.

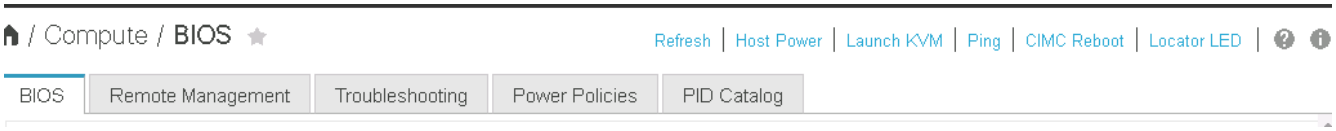
Este procedimiento debe completarse para los nodos adicionales que se añadan al clúster.

Inicie sesión en la interfaz de CIMC para servidores independientes de Cisco UCS C-Series

Los siguientes pasos detallan el método para iniciar sesión en la interfaz de CIMC para servidores independientes Cisco UCS C-Series. Debe iniciar sesión en la interfaz de CIMC para ejecutar el KVM virtual, que permite al administrador iniciar la instalación del sistema operativo a través de medios remotos.

Todos los hosts

1. Desplácese hasta un explorador web e introduzca la dirección IP para la interfaz de CIMC para Cisco UCS C-Series. Este paso inicia la aplicación GUI de CIMC.
2. Inicie sesión en la interfaz de usuario de CIMC con el nombre de usuario y las credenciales de administrador.
3. En el menú principal, seleccione la ficha servidor.
4. Haga clic en Iniciar la consola KVM.



5. En la consola KVM virtual, seleccione la ficha Medios virtuales.
6. Selecciona Mapa CD/DVD.

Es posible que primero tenga que hacer clic en Activar dispositivos virtuales. Seleccione Aceptar esta sesión si se le solicita.

7. Desplácese hasta el archivo de imagen ISO del instalador VMware ESXi 6.7 y haga clic en Open. Haga clic en asignar dispositivo.
8. Seleccione el menú de encendido y elija sistema de ciclo de encendido (arranque en frío). Haga clic en Yes.

Instale VMware ESXi

Los siguientes pasos describen cómo instalar VMware ESXi en cada host.

Descargue LA imagen personalizada de ESXI 6.7 Cisco

1. Desplácese hasta la "Página de descarga de VMware vSphere" Para ISO personalizados.
2. Haga clic en Ir a Descargas junto al CD de instalación de la imagen personalizada de Cisco para ESXi 6.7 GA.
3. Descargue la imagen personalizada de Cisco para el CD de instalación de ESXi 6.7 GA (ISO).

Todos los hosts

1. Cuando el sistema arranca, la máquina detecta la presencia del medio de instalación de VMware ESXi.
2. Seleccione el instalador de VMware ESXi en el menú que aparece.

   El instalador se carga. Esto tarda varios minutos.

3. Cuando el instalador haya terminado de cargarse, pulse Intro para continuar con la instalación.
4. Después de leer el contrato de licencia del usuario final, acepte y continúe con la instalación pulsando F11.
5. Seleccione el LUN de NetApp que se configuró anteriormente como disco de instalación para ESXi y pulse Intro para continuar con la instalación.

6. Seleccione la distribución de teclado adecuada y pulse Intro.
7. Introduzca y confirme la contraseña de root y pulse Intro.
8. El instalador le advierte que las particiones existentes se han eliminado en el volumen. Continúe con la instalación pulsando F11. El servidor se reinicia después de la instalación de ESXi.

Configure la red de gestión del host VMware ESXi

Los siguientes pasos describen cómo añadir la red de gestión de cada host VMware ESXi.

Todos los hosts

1. Una vez que el servidor haya terminado de reiniciarse, introduzca la opción de personalizar el sistema pulsando F2.
2. Inicie sesión con root como nombre de inicio de sesión y la contraseña raíz que se introdujo anteriormente durante el proceso de instalación.
3. Seleccione la opción Configure Management Network.
4. Seleccione Adaptadores de red y pulse Intro.
5. Seleccione los puertos deseados para vSwitch0. Pulse Intro.

   Seleccione los puertos que corresponden a eth0 y eth1 en CIMC.

6. Seleccione VLAN (opcional) y presione Enter.
7. Introduzca el identificador de VLAN `<<mgmt_vlan_id>>`. Pulse Intro.
8. En el menú Configurar red de gestión, seleccione Configuración de IPv4 para configurar la dirección IP de la interfaz de gestión. Pulse Intro.
9. Utilice las teclas de flecha para resaltar establecer dirección IPv4 estática y utilice la barra espaciadora para seleccionar esta opción.
10. Introduzca la dirección IP para gestionar el host VMware ESXi `<<esxi_host_mgmt_ip>>`.
11. Introduzca la máscara de subred para el host VMware ESXi `<<esxi_host_mgmt_netmask>>`.
12. Introduzca la puerta de enlace predeterminada para el host VMware ESXi `<<esxi_host_mgmt_gateway>>`.
13. Pulse Intro para aceptar los cambios en la configuración de IP.
14. Acceda al menú de configuración de IPv6.
15. Utilice la barra de espacio para desactivar IPv6 deseleccionando la opción Habilitar IPv6 (reiniciar requerido). Pulse Intro.
16. Abra el menú para configurar los ajustes de DNS.
17. Dado que la dirección IP se asigna manualmente, la información DNS también debe introducirse manualmente.
18. Introduzca la dirección IP del servidor DNS primario[nameserver_ip].
19. (Opcional) Introduzca la dirección IP del servidor DNS secundario.
20. Introduzca el FQDN para el nombre de host VMware ESXi:[esxi_host_fqdn].
21. Pulse Intro para aceptar los cambios en la configuración de DNS.
22. Salga del submenú Configurar red de administración pulsando Esc.
23. Pulse y para confirmar los cambios y reiniciar el servidor.
24. Cierre la sesión de la consola de VMware pulsando Esc.

Configure el host ESXi

Necesita la información de la siguiente tabla para configurar cada host ESXi.

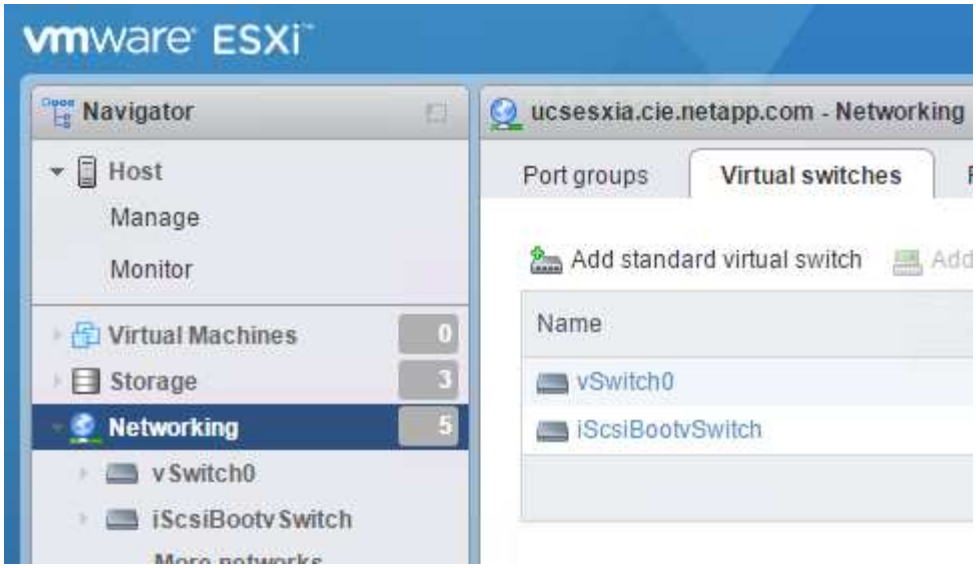
Detalles	Valor
Nombre de host ESXi	
La IP de gestión del host ESXi	
Máscara de gestión de host ESXi	
Pasarela de gestión de host ESXi	
IP NFS del host ESXi	
Máscara de NFS del host ESXi	
Puerta de enlace NFS del host ESXi	
Host ESXi IP de vMotion	
Máscara de vMotion del host ESXi	
Puerta de enlace vMotion del host ESXi	
Host ESXi iSCSI-A IP	
Máscara iSCSI-A del host ESXi	
Puerta de enlace iSCSI-A del host ESXi	
Host ESXi iSCSI-B IP	
Máscara iSCSI-B del host ESXi	
Puerta de enlace iSCSI-B del host ESXi	

Inicie sesión en el host ESXi

1. Abra la dirección IP de administración del host en un explorador Web.
2. Inicie sesión en el host ESXi con la cuenta raíz y la contraseña que especificó durante el proceso de instalación.
3. Lea la declaración sobre el Programa de mejora de la experiencia del cliente de VMware. Después de seleccionar la respuesta correcta, haga clic en Aceptar.

Configurar el arranque iSCSI

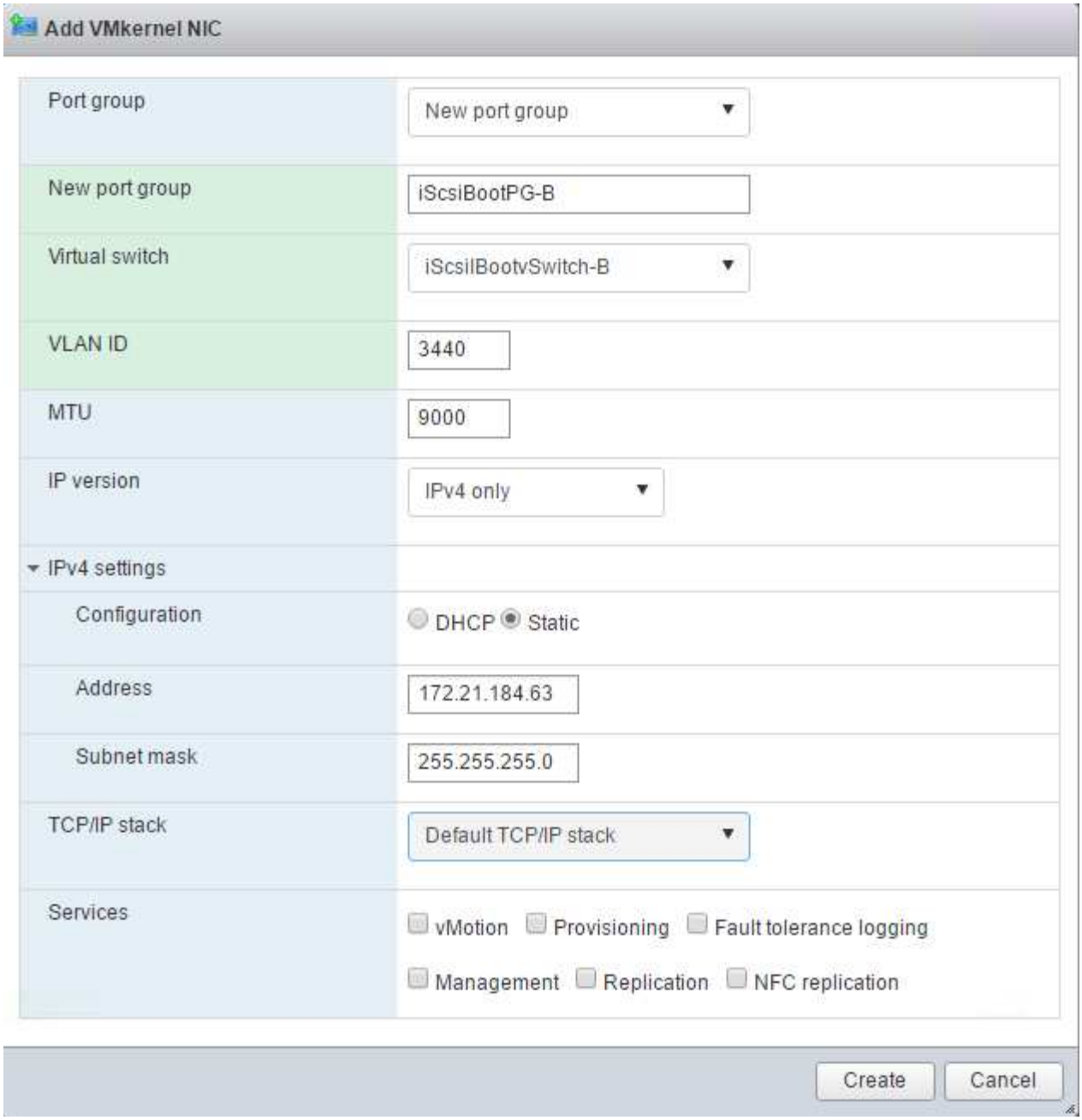
1. Seleccione Networking a la izquierda.
2. A la derecha, seleccione la ficha Switches virtuales.



3. Haga clic en iScsiBootvSwitch.
4. Seleccione Editar configuración.
5. Cambie la MTU a 9000 y haga clic en Save.
6. Haga clic en redes en el panel de navegación de la izquierda para volver a la ficha Switches virtuales.
7. Haga clic en Agregar conmutador virtual estándar.
8. Escriba el nombre `iScsiBootvSwitch-B` Para el nombre de vSwitch.
   - Establezca la MTU en 9000.
   - Seleccione vmnic3 en las opciones de Uplink 1.
   - Haga clic en Añadir.

> En esta configuración, se utilizan Vmnic2 y vmnic3 para el arranque iSCSI. Si tiene NIC adicionales en el host ESXi, puede tener distintos números vmnic. Para confirmar qué NIC se utilizan para el arranque iSCSI, haga coincidir las direcciones MAC de las NIC iSCSI de CIMC con los vmnics de ESXi.

9. En el panel central, seleccione la ficha NIC de VMkernel.
10. Seleccione Agregar NIC de VMkernel.
    - Especifique un nuevo nombre de grupo de puertos de `iScsiBootPG-B`.
    - Seleccione iScsiBootvSwitch-B para el conmutador virtual.
    - Introduzca `<<iscsib_vlan_id>>` Para el ID de VLAN.
    - Cambie el MTU a 9000.
    - Expanda Configuración IPv4.
    - Seleccione Configuración estática.
    - Introduzca `<<var_hosta_iscsib_ip>>` Para Dirección.
    - Introduzca `<<var_hosta_iscsib_mask>>` Para Máscara de subred.
    - Haga clic en Crear.

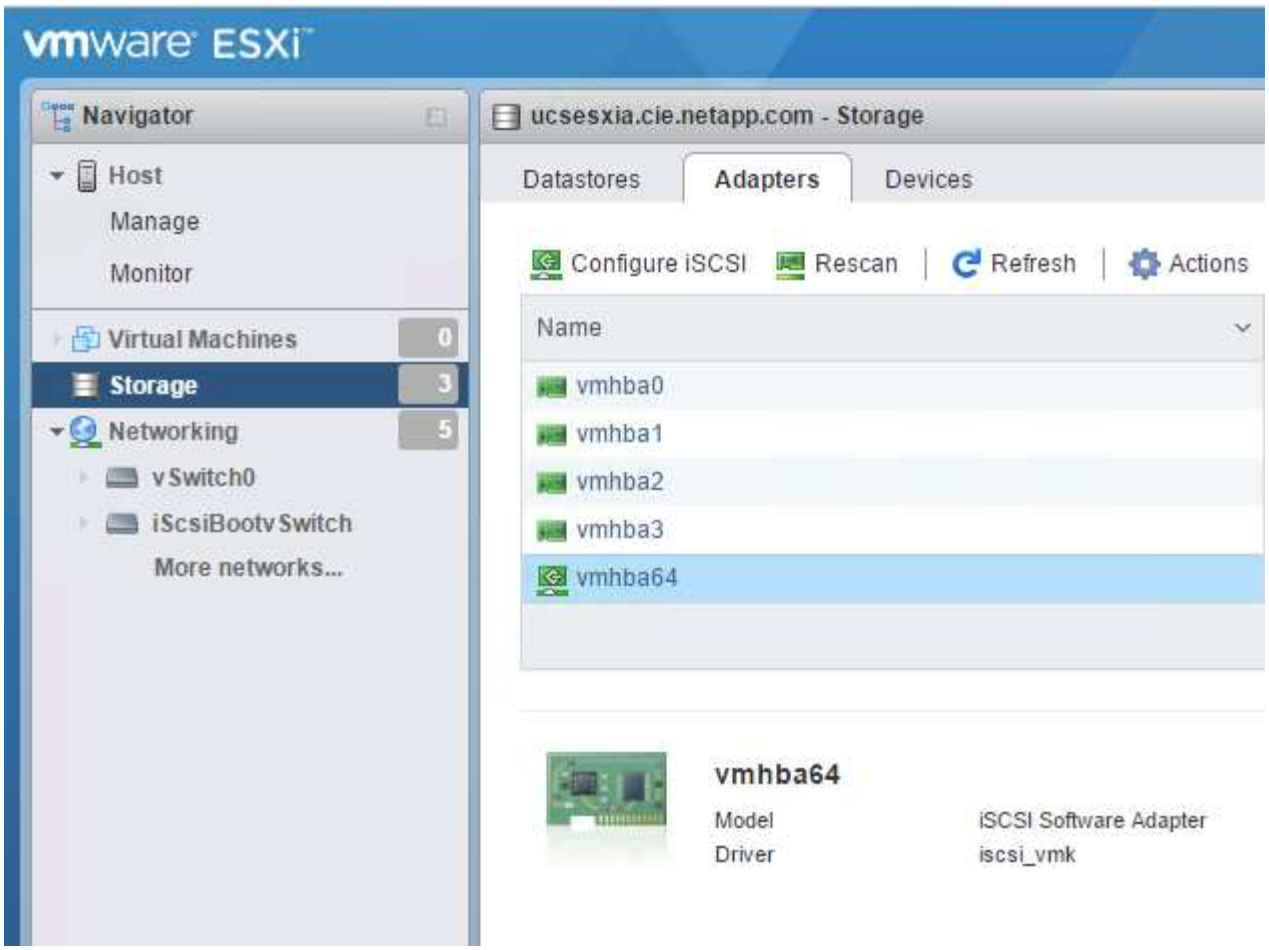


Establezca la MTU en 9000 on `iScsiBootPG- A`.

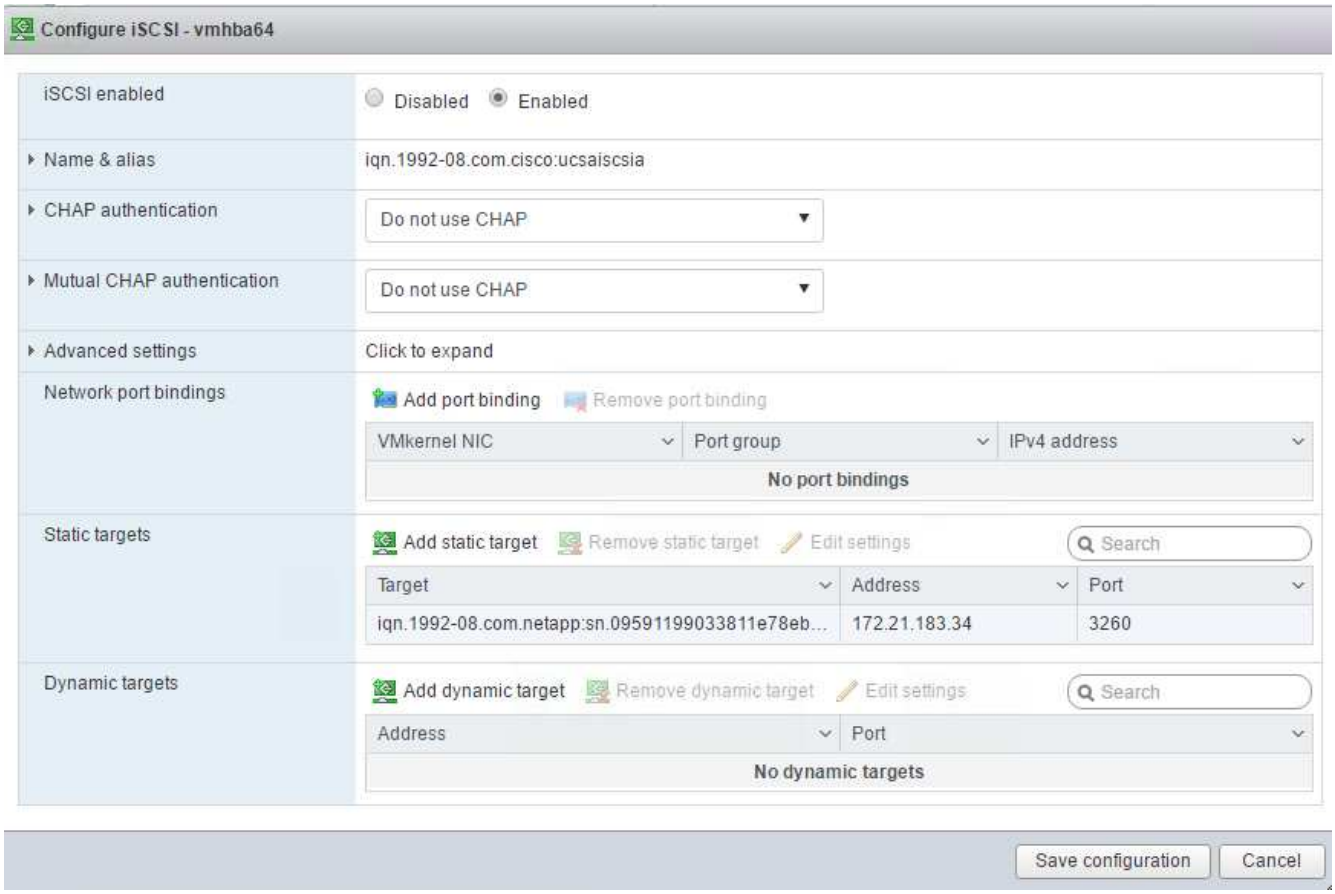
Configuración de accesos múltiples iSCSI

Para configurar la multivía iSCSI en los hosts ESXi, complete los pasos siguientes:

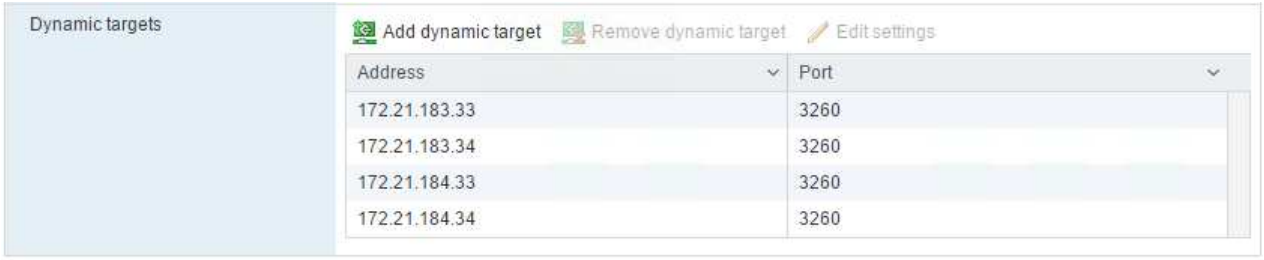
1. Seleccione Storage en el panel de navegación de la izquierda. Haga clic en Adaptadores.
2. Seleccione el adaptador de software iSCSI y haga clic en Configurar iSCSI.



3. En Destinos dinámicos, haga clic en Agregar destino dinámico.



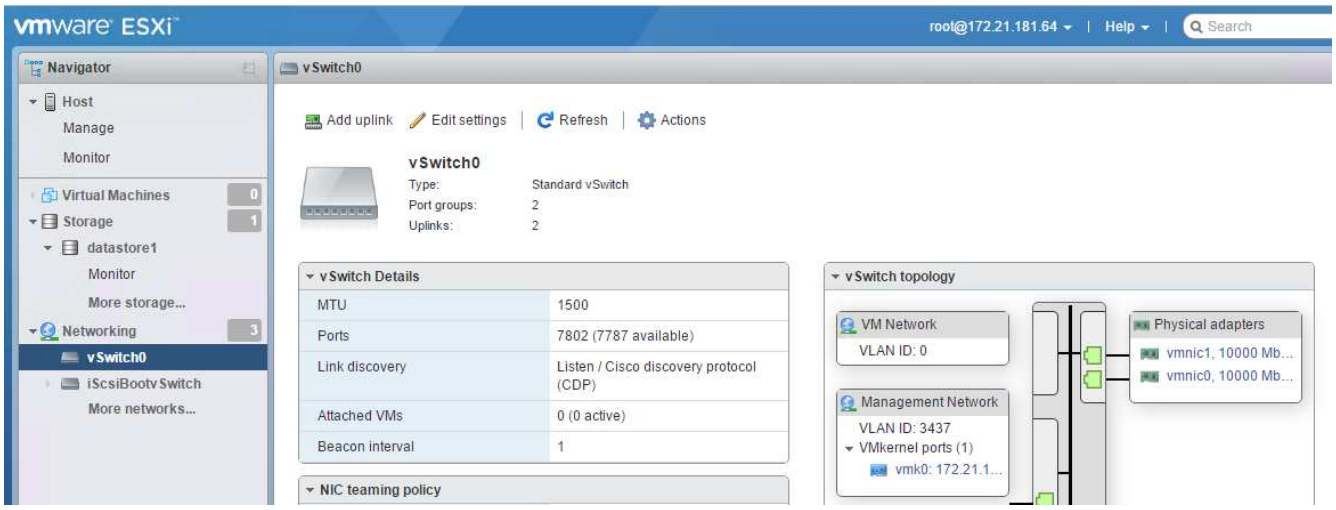
4. Introduzca la dirección IP `iscsi_lif01a`.
   - Repita el proceso con las direcciones IP `iscsi_lif01b`, `iscsi_lif02a`, y. `iscsi_lif02b`.
   - Haga clic en Save Configuration.



Para encontrar las direcciones IP de LIF iSCSI, ejecute el comando "network interface show "en el clúster de NetApp o consulte la pestaña Network interfaces en OnCommand System Manager.

Configure el host ESXi

1. En el panel de navegación de la izquierda, seleccione Networking.
2. Seleccione vSwitch0.



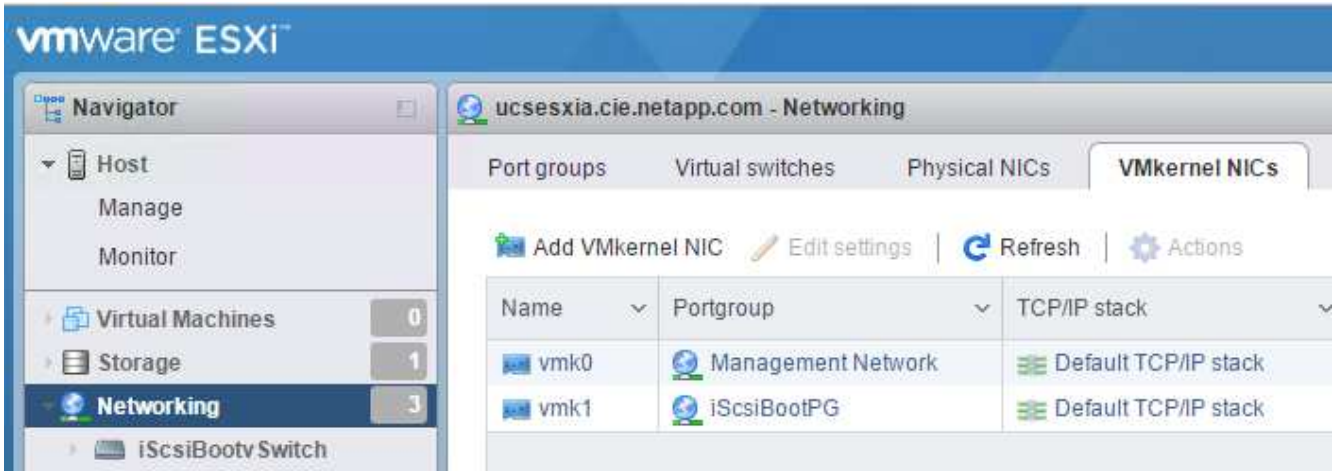
3. Seleccione Editar configuración.
4. Cambie el MTU a 9000.
5. Expanda NIC Teaming y verifique que tanto vmnic0 como vmnic1 estén definidos en activo.

Configurar grupos de puertos y NIC de VMkernel

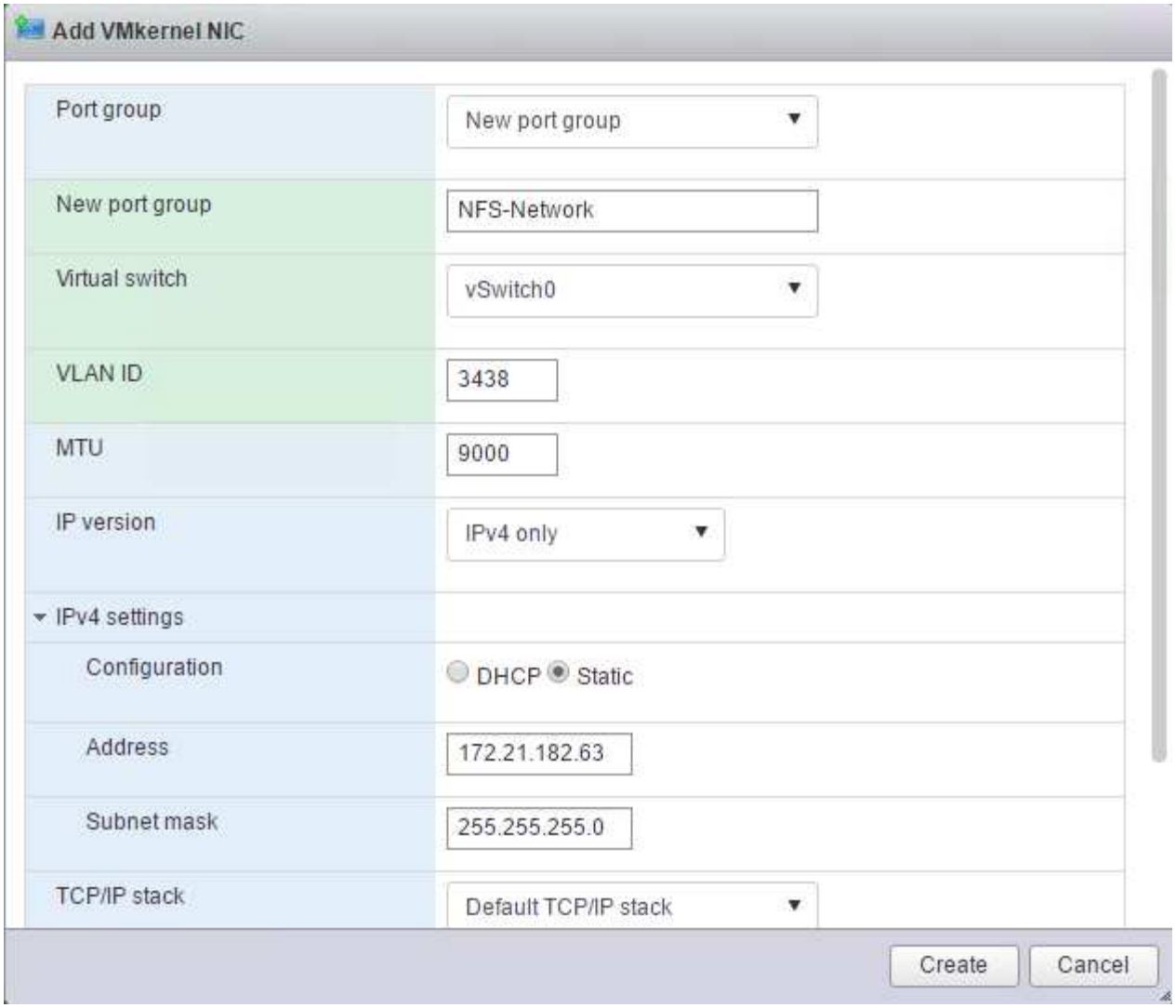
1. En el panel de navegación de la izquierda, seleccione Networking.
2. Haga clic con el botón derecho en la pestaña grupos de puertos.

3. Haga clic con el botón derecho en VM Network y seleccione Edit. Cambie el ID de VLAN a. `<<var_vm_traffic_vlan>>`.
4. Haga clic en Agregar grupo de puertos.
   - Asigne un nombre al grupo de puertos `MGMT-Network`.
   - Introduzca `<<mgmt_vlan>>` Para el ID de VLAN.
   - Asegúrese de que vSwitch0 esté seleccionado.
   - Haga clic en Añadir.

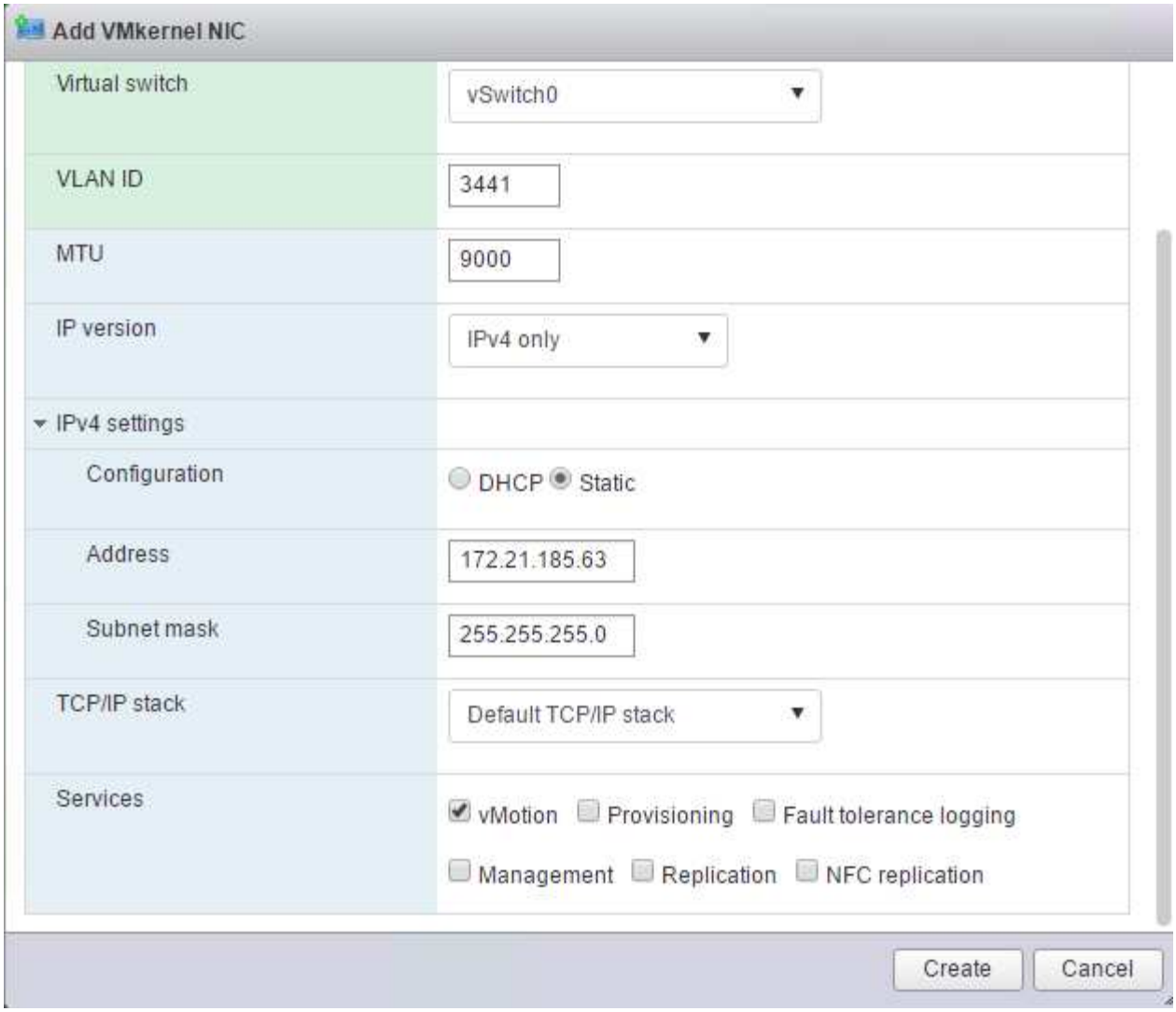
5. Haga clic en la ficha NIC de VMkernel.



6. Seleccione Agregar NIC de VMkernel.
   - Seleccione Nuevo grupo de puertos.
   - Asigne un nombre al grupo de puertos `NFS-Network`.
   - Introduzca `<<nfs_vlan_id>>` Para el ID de VLAN.
   - Cambie el MTU a 9000.
   - Expanda Configuración IPv4.
   - Seleccione Configuración estática.
   - Introduzca `<<var_hosta_nfs_ip>>` Para Dirección.
   - Introduzca `<<var_hosta_nfs_mask>>` Para Máscara de subred.
   - Haga clic en Crear.



7. Repita este proceso para crear el puerto VMkernel de vMotion.
8. Seleccione Agregar NIC de VMkernel.
    a. Seleccione Nuevo grupo de puertos.
    b. Asigne un nombre al grupo de puertos vMotion.
    c. Introduzca `<<vmotion_vlan_id>>` Para el ID de VLAN.
    d. Cambie el MTU a 9000.
    e. Expanda Configuración IPv4.
    f. Seleccione Configuración estática.
    g. Introduzca `<<var_hosta_vmotion_ip>>` Para Dirección.
    h. Introduzca `<<var_hosta_vmotion_mask>>` Para Máscara de subred.
    i. Asegúrese de que la casilla de comprobación vMotion esté seleccionada después de IPv4 Settings.

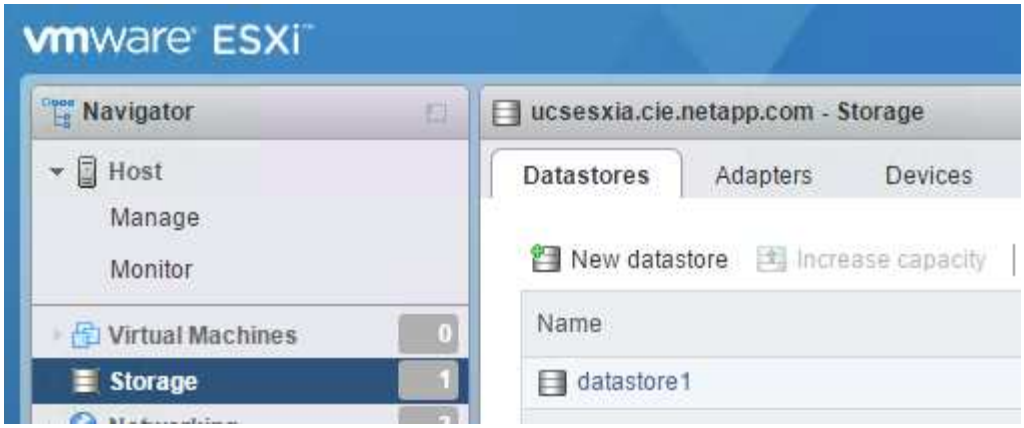


Hay muchas formas de configurar redes ESXi, por ejemplo, mediante el switch distribuido de VMware vSphere si la licencia lo permite. FlexPod Express admite configuraciones de red alternativas si se requieren para satisfacer los requisitos del negocio.

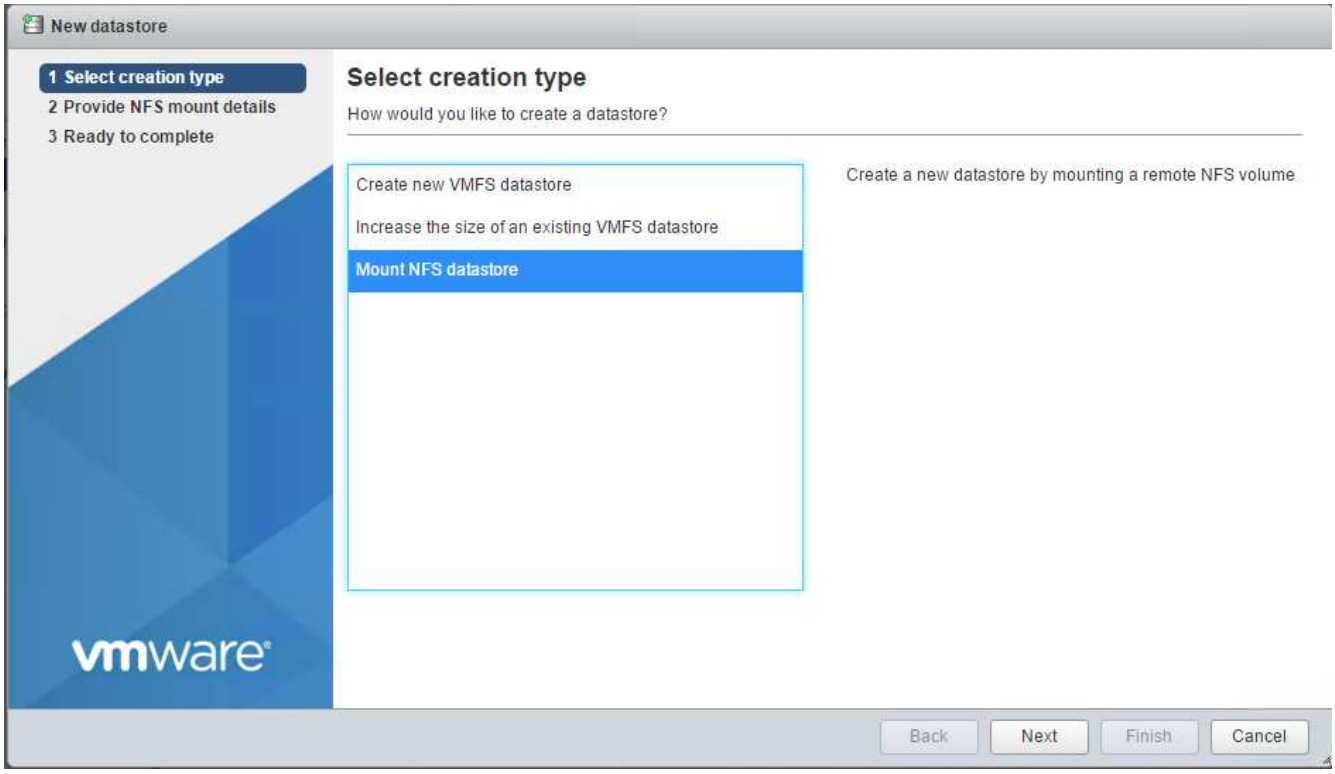
Montaje de los primeros almacenes de datos

Los primeros almacenes de datos que se van a montar son el almacén de datos de infra_datastore_1 para máquinas virtuales y el almacén de datos de infra_swap para archivos de intercambio de máquinas virtuales.

1. Haga clic en Storage en el panel de navegación de la izquierda y después haga clic en New Datastore.



2. Seleccione Mount NFS Datastore.



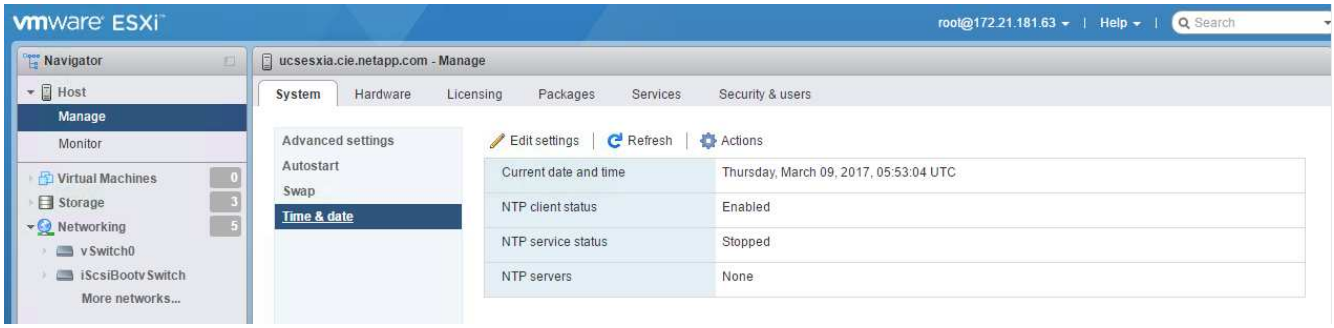
3. A continuación, introduzca la siguiente información en la página Provide NFS Mount Details:
   - Nombre: `infra_datastore_1`
   - Servidor NFS: `<<var_nodea_nfs_lif>>`
   - Compartir: /Infra_datastore_1
   - Asegúrese de que la opción NFS 3 esté seleccionada.
4. Haga clic en Finalizar. Puede ver que la tarea se está completando en el panel tareas recientes.
5. Repita este proceso para montar el almacén de datos infra_swap:
   - Nombre: `infra_swap`
   - Servidor NFS: `<<var_nodea_nfs_lif>>`
   - Compartir: `/infra_swap`

- Asegúrese de que la opción NFS 3 esté seleccionada.

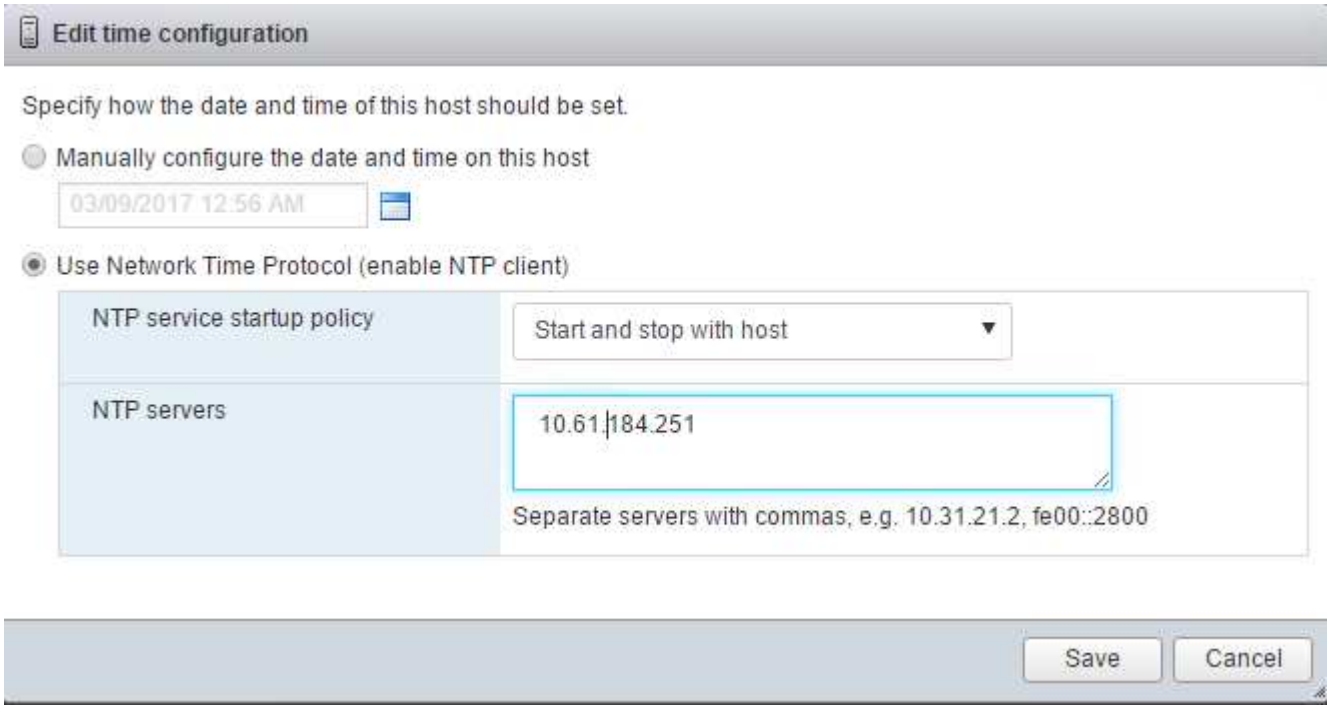
Configure NTP

Para configurar NTP para un host ESXi, complete los siguientes pasos:

1. Haga clic en Administrar en el panel de navegación de la izquierda. Seleccione sistema en el panel derecho y, a continuación, haga clic en Hora y fecha.



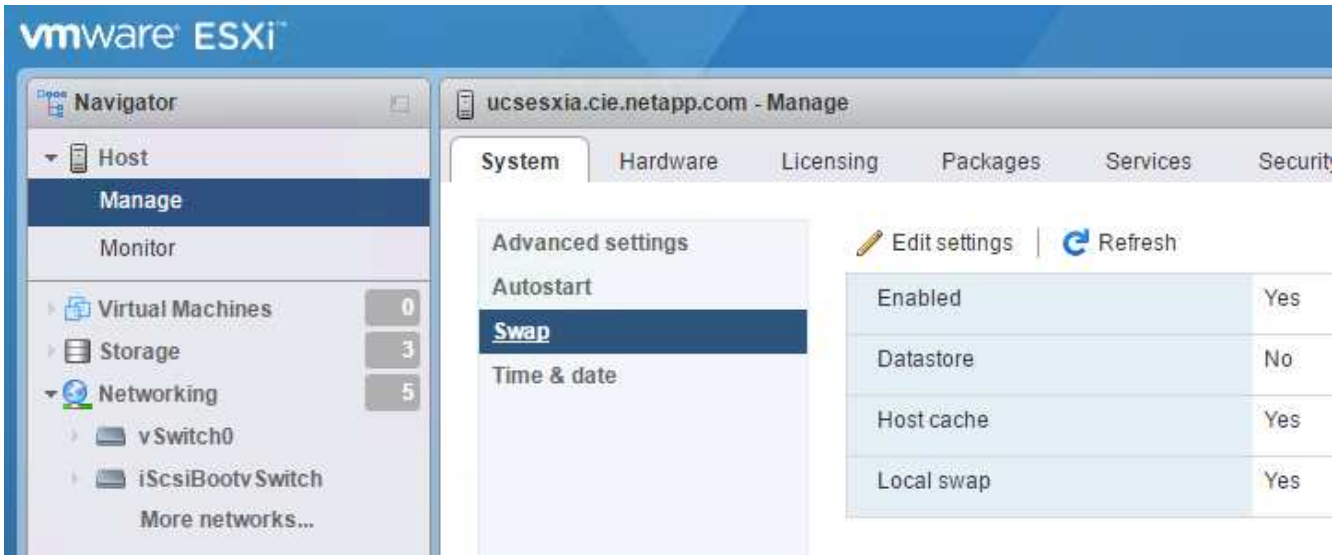
2. Seleccione Use Network Time Protocol (Habilitar cliente NTP).
3. Seleccione Start and Stop with Host como política de inicio del servicio NTP.
4. Introduzca `<<var_ntp>>` Como servidor NTP. Puede establecer varios servidores NTP.
5. Haga clic en Guardar.



Mueva la ubicación del archivo de intercambio de la máquina virtual

Estos pasos proporcionan detalles para mover la ubicación del archivo de intercambio de la máquina virtual.

1. Haga clic en Administrar en el panel de navegación de la izquierda. Seleccione sistema en el panel derecho y, a continuación, haga clic en intercambiar.



2. Haga clic en Editar configuración. Seleccione infra_swap desde las opciones de Datastore.

3. Haga clic en Guardar.

Instale el plugin de NetApp NFS 1.0.20 para VMware VAAI

Para instalar el complemento NFS de NetApp 1.0.20 para VMware VAAI, complete los pasos siguientes.

1. Introduzca los siguientes comandos para verificar que VAAI está habilitado:

```
esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
```

   Si VAAI está habilitada, estos comandos generan el siguiente resultado:

```
~ #  esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
~ # esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
```

2. Si VAAI no está habilitada, introduzca los siguientes comandos para habilitar VAAI:

```
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedInit
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
```

Estos comandos generan el siguiente resultado:

```
~ # esxcfg-advcfg -s 1 /Data Mover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
~ #  esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
```

3. Descargue el plugin de NetApp NFS para VMware VAAI:
   a. Vaya a la "página de descarga del software".
   b. Desplácese hacia abajo y haga clic en NetApp NFS Plug-in for VMware VAAI.
   c. Seleccione la plataforma ESXi.
   d. Descargue el paquete sin conexión (.zip) o el paquete en línea (.vib) del plugin más reciente.
4. Instale el plugin en el host ESXi mediante la CLI ESX.
5. Reinicie el host ESXI.

```
[root@vm-host-infra-04:~] ls /vmfs/volumes/datastore1/NetAppNasPlugin.vib
/vmfs/volumes/datastore1/NetAppNasPlugin.vib
[root@vm-host-infra-04:~] esxcli software vib install -v /vmfs/volumes/datastore1/NetAppNasPlugin.vib
Installation Result
   Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.
   Reboot Required: true
   VIBs Installed: NetApp_bootbank_NetAppNasPlugin_1.1.2-3
   VIBs Removed:
   VIBs Skipped:
[root@vm-host-infra-04:~]
```

"Siguiente: Instale VMware vCenter Server 6.7"

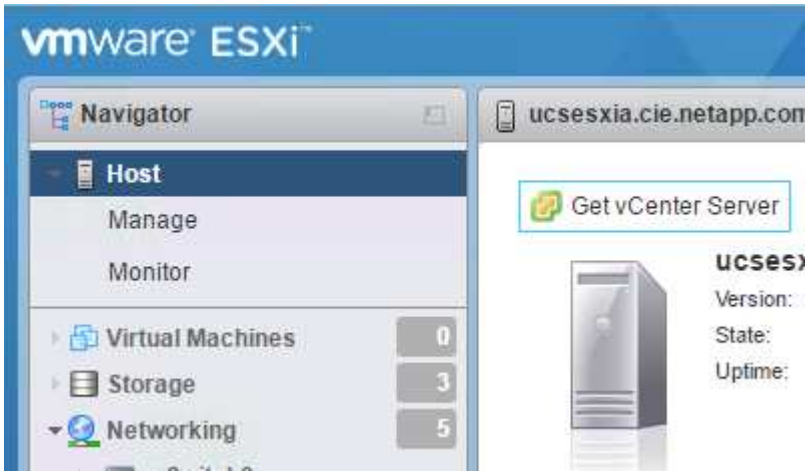
Instale VMware vCenter Server 6.7

En esta sección, se proporcionan los procedimientos detallados para instalar VMware vCenter Server 6.7 en una configuración exprés de FlexPod.

FlexPod Express utiliza el dispositivo de VMware vCenter Server (VCSA).

Descargue el dispositivo VMware vCenter Server

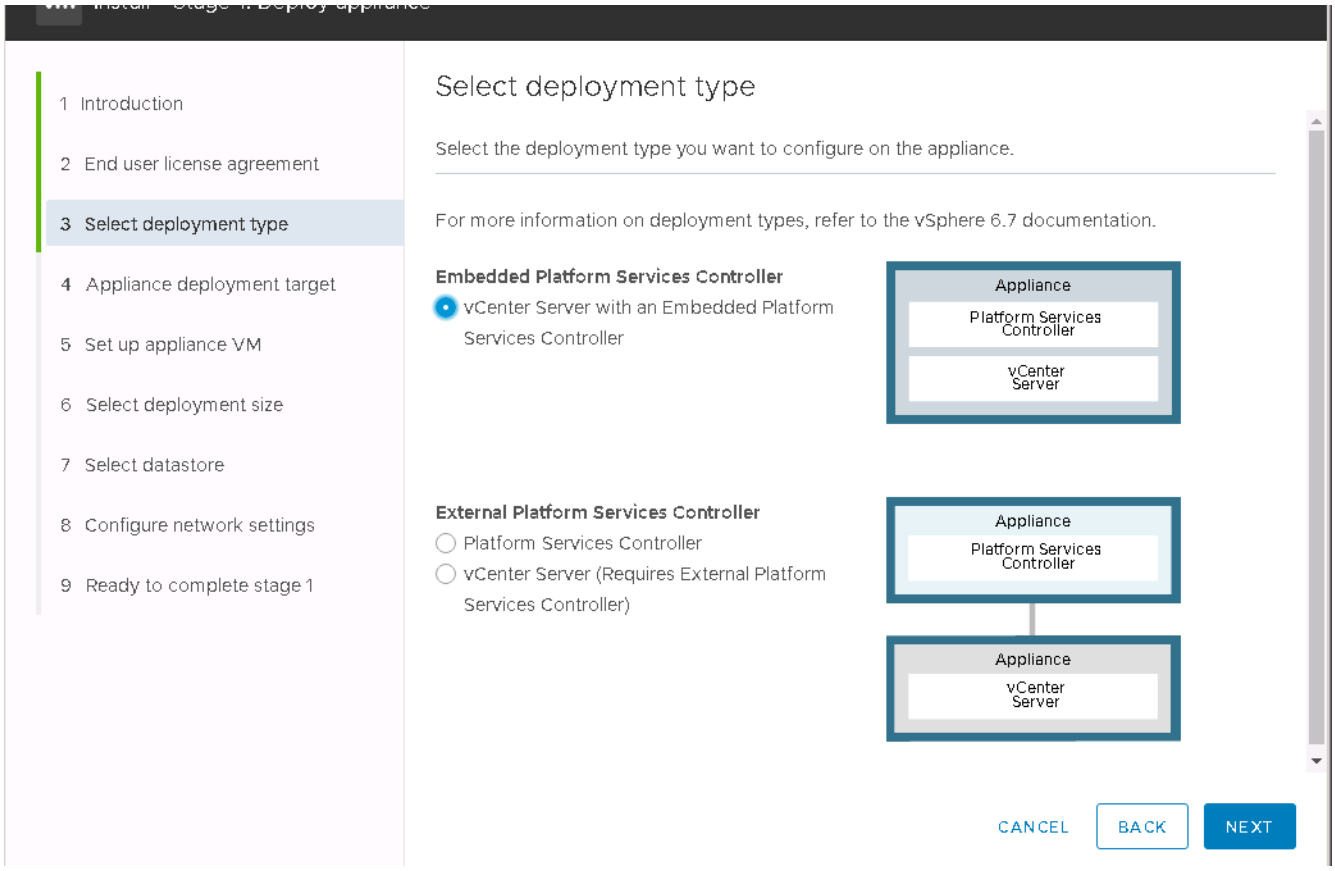
1. Descargue el VCSA. Acceda al enlace de descarga haciendo clic en el icono Get vCenter Server cuando gestione el host ESXi.



2. Descargue el VCSA desde el sitio de VMware.

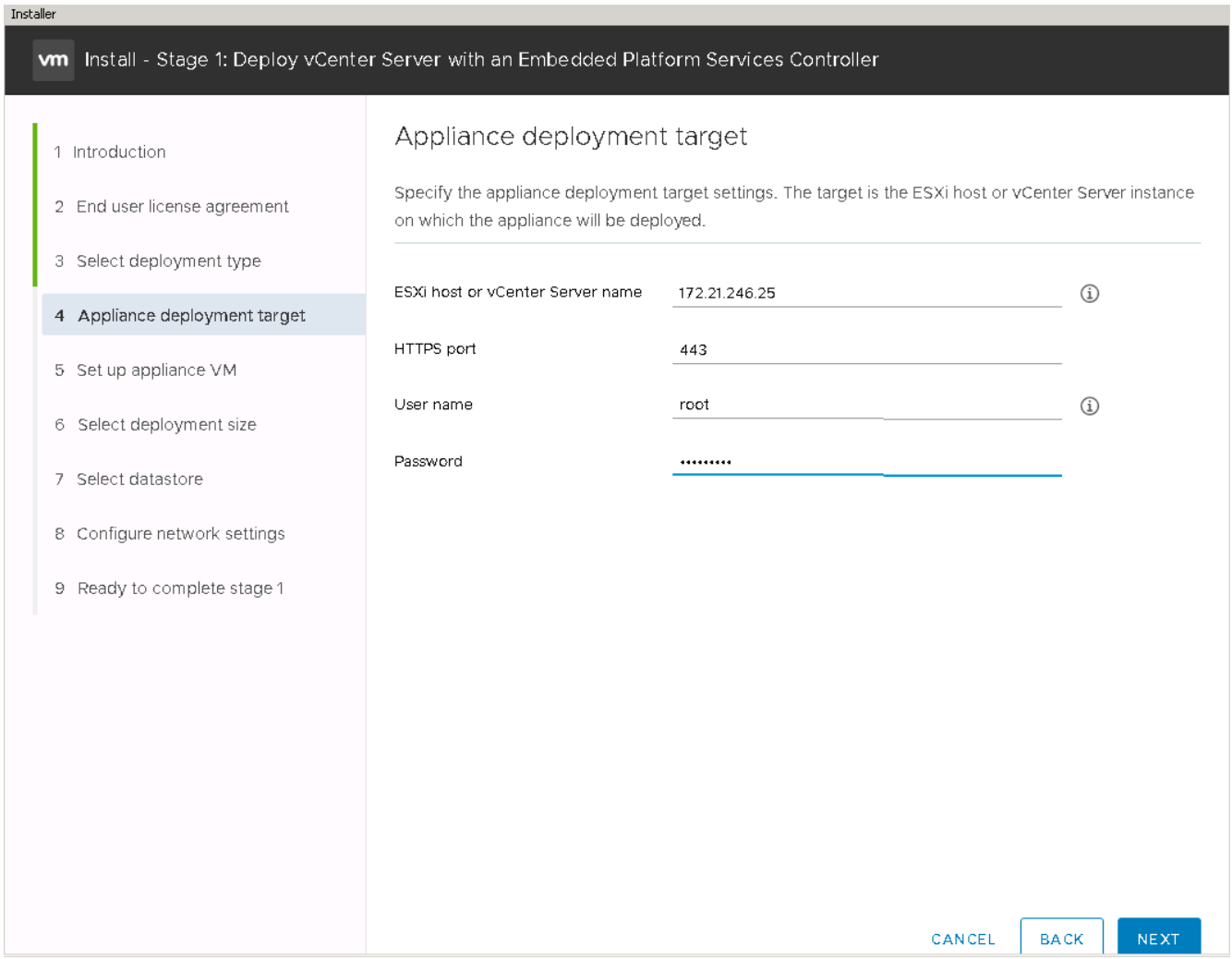
> Aunque se admite la instalación de Microsoft Windows vCenter Server, VMware recomienda VCSA para las nuevas implementaciones.

3. Monte la imagen ISO.
4. Desplácese al directorio vcsa-ui-installer> win32. Haga doble clic en Installer.exe.
5. Haga clic en instalar.
6. Haga clic en Siguiente en la página Introducción.
7. Acepte el acuerdo de licencia para el usuario final.
8. Seleccione Embedded Platform Services Controller (controladora de servicios de plataforma integrada) como tipo de implementación.

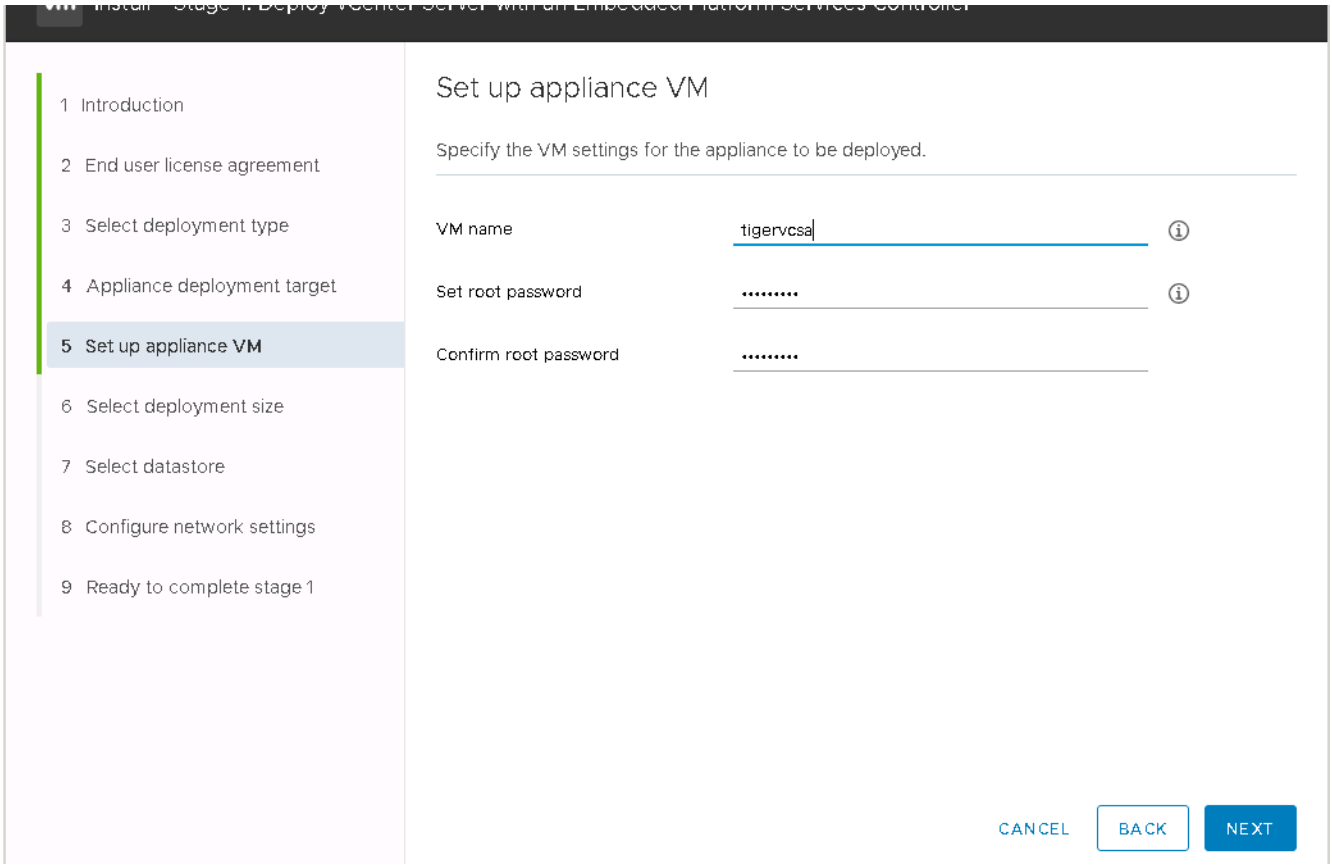


Si es necesario, también admite la puesta en marcha de la controladora de servicios de plataforma externa como parte de la solución FlexPod Express.

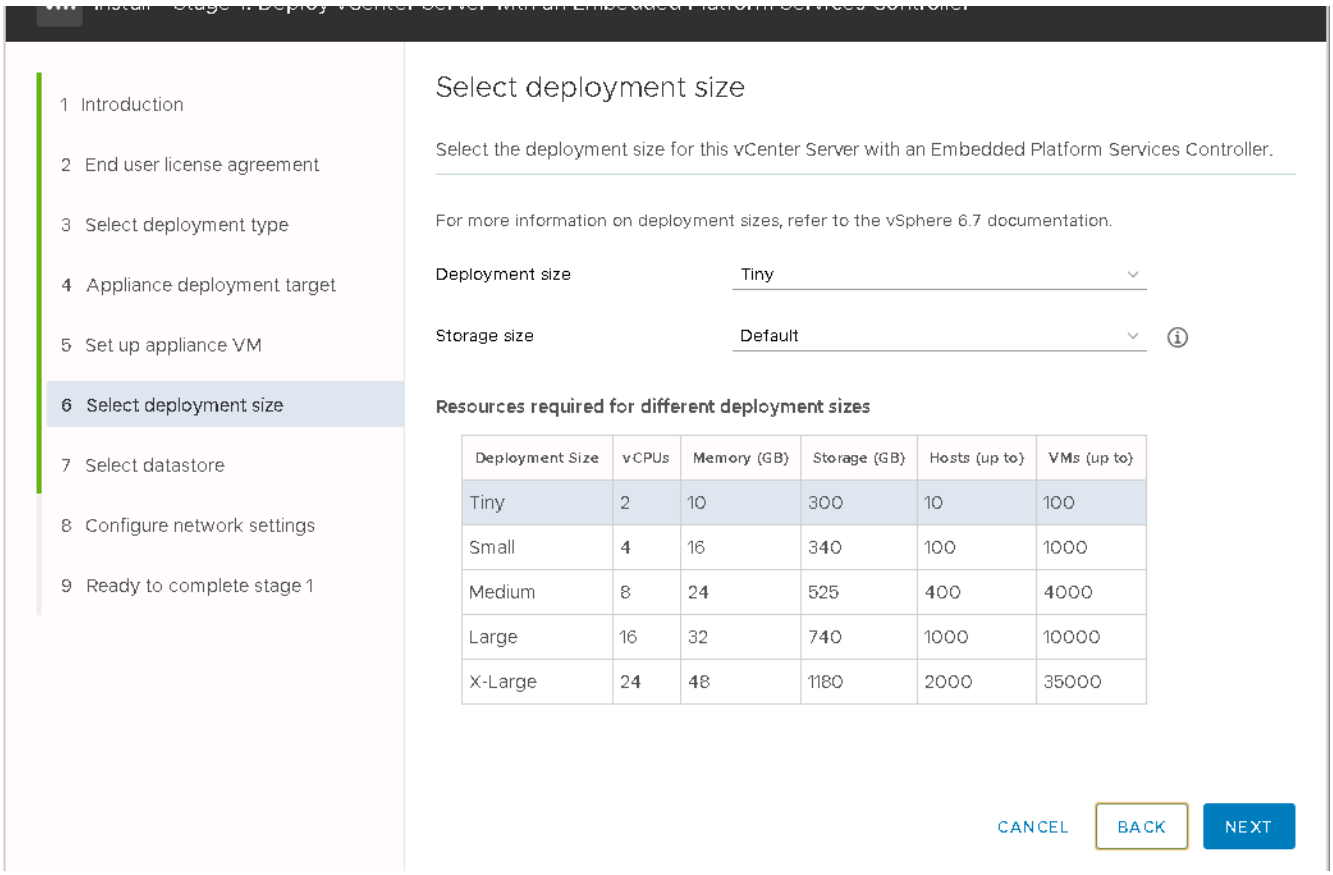
9. En Appliance Deployment Target, introduzca la dirección IP de un host ESXi implementado, así como el nombre de usuario raíz y la contraseña raíz.



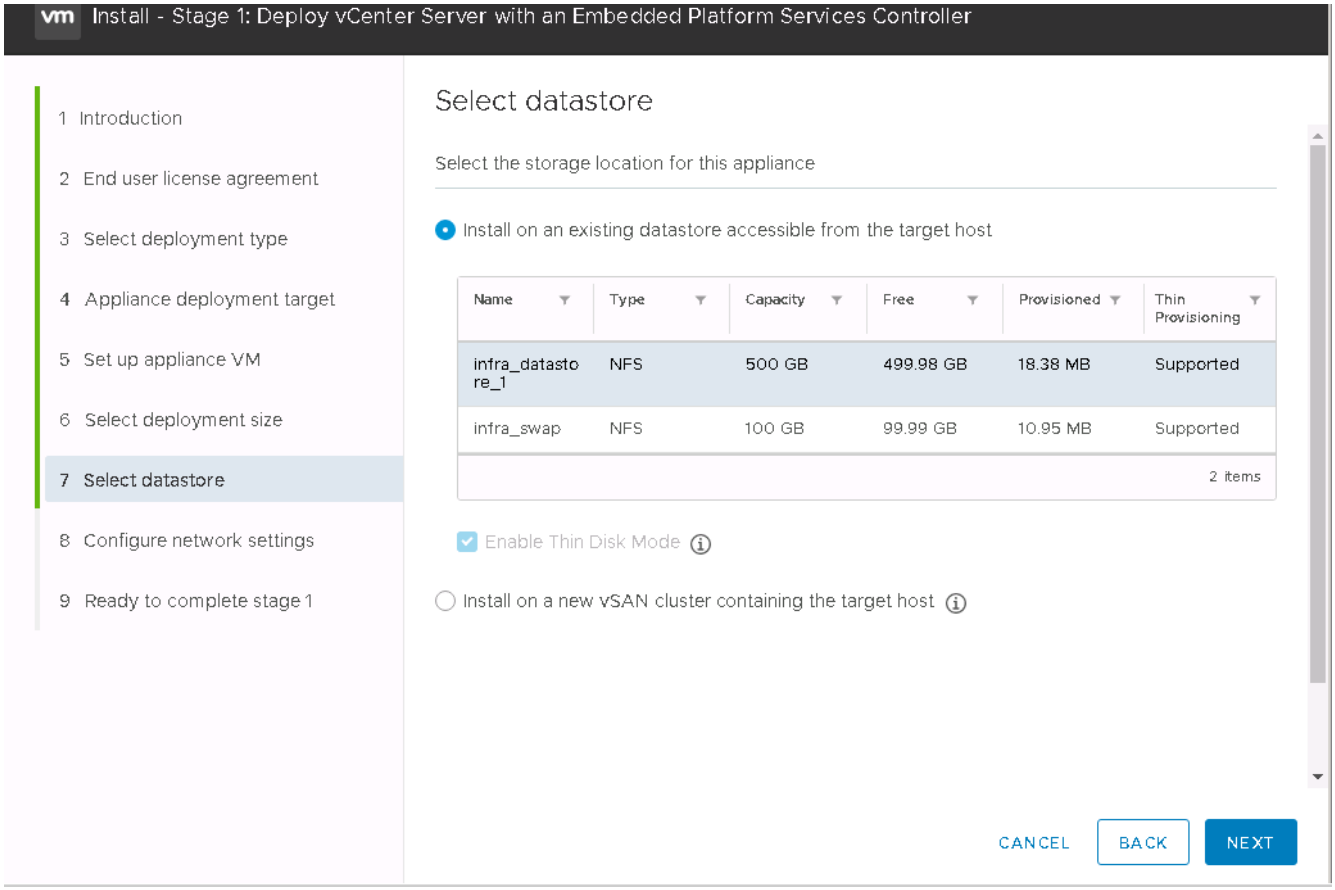
10. Introduzca para establecer la máquina virtual del dispositivo `VCSA` Como el nombre del equipo virtual y la contraseña raíz que desea utilizar para el VCSA.



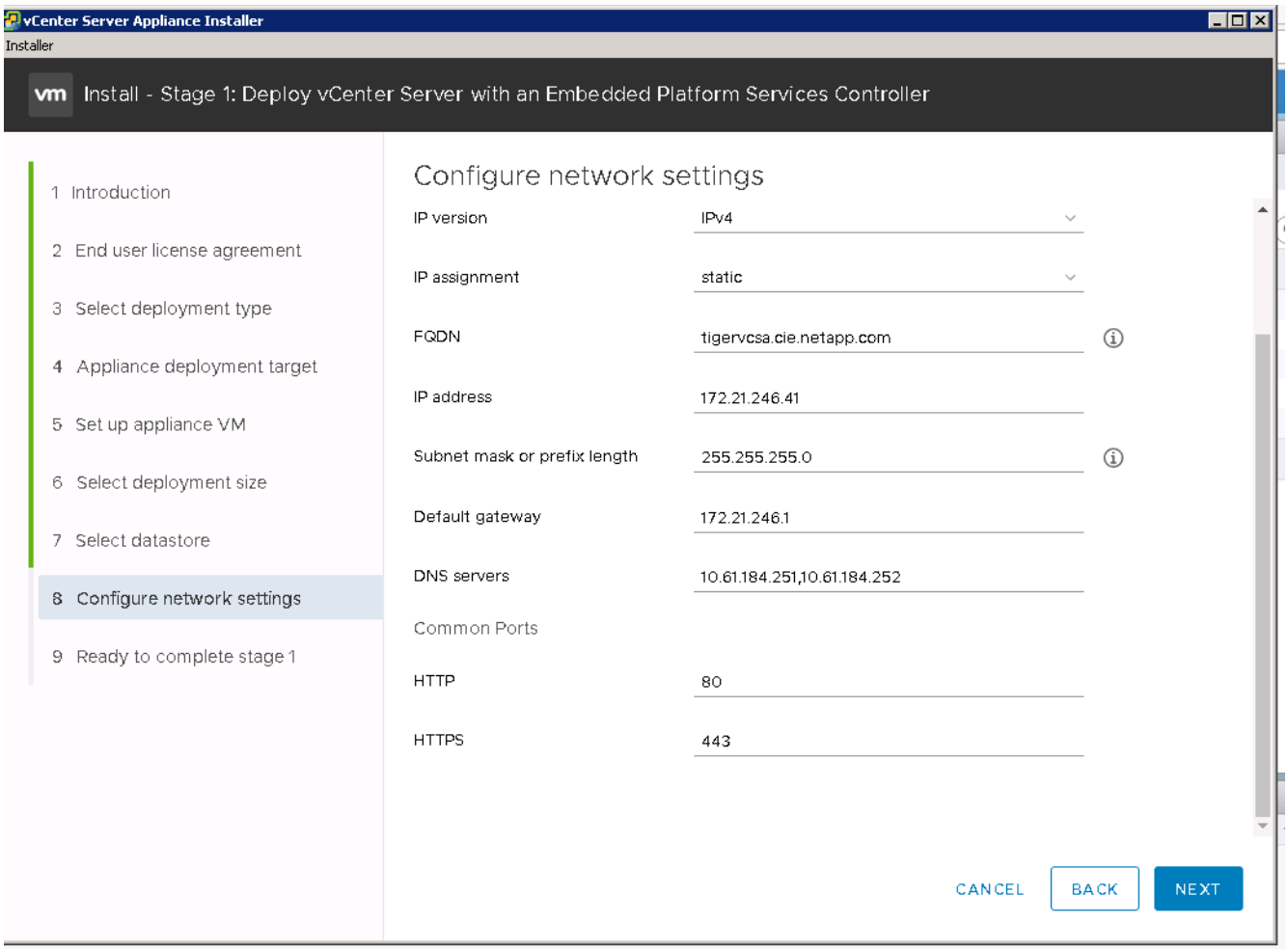
11. Seleccione el tamaño de puesta en marcha que mejor se adapte a su entorno. Haga clic en Siguiente.



12. Seleccione el almacén de datos de infra_datastore_1. Haga clic en Siguiente.

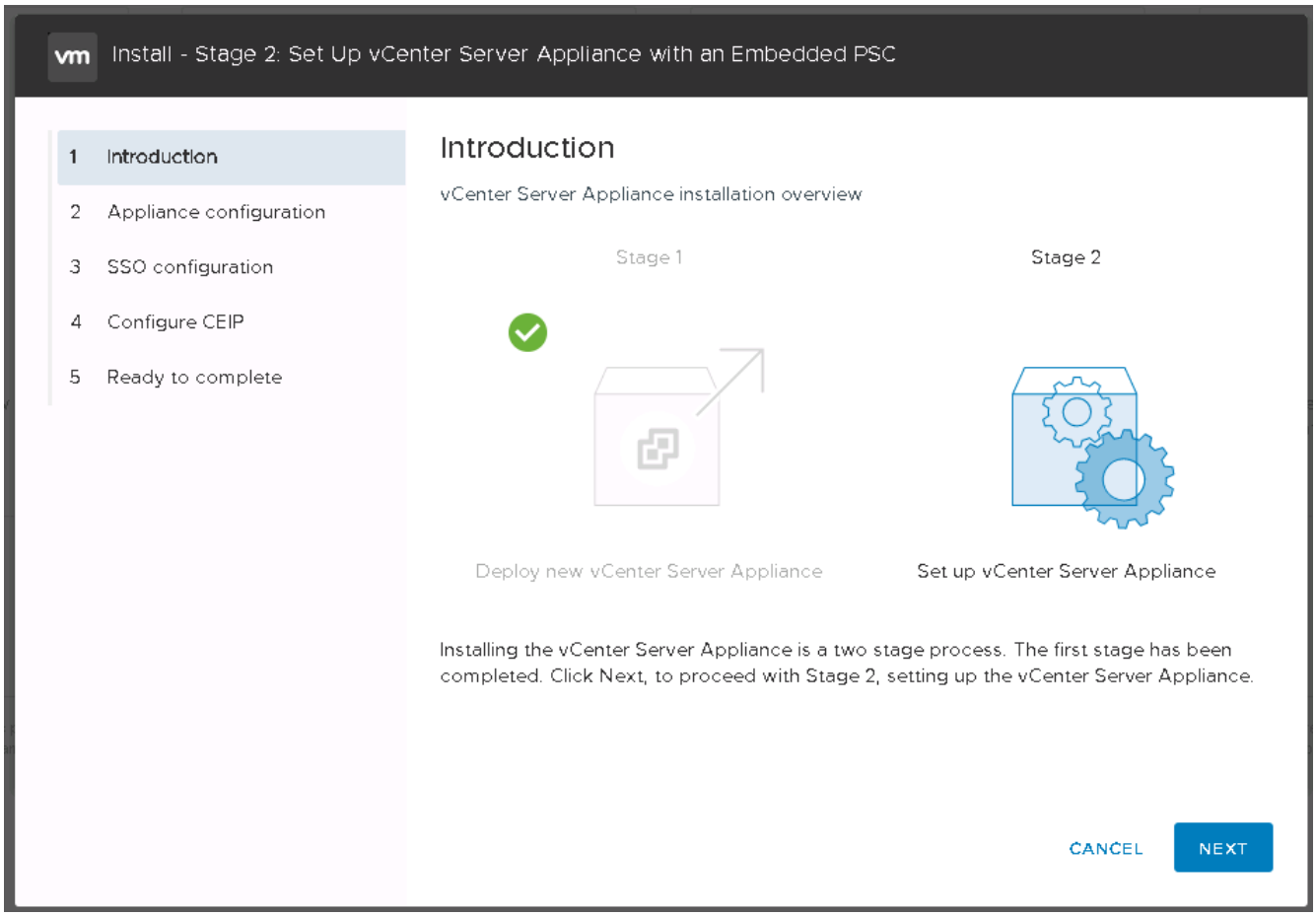


13. Introduzca la siguiente información en la página Configure network settings y haga clic en Next.
    a. Seleccione MGMT-Network para Red.
    b. Introduzca el FQDN o IP que se va a utilizar para la VCSA.
    c. Introduzca la dirección IP que se utilizará.
    d. Introduzca la máscara de subred que desea utilizar.
    e. Introduzca la pasarela predeterminada.
    f. Introduzca el servidor DNS.
14. En la página Ready to Complete Stage 1, compruebe que los ajustes introducidos son correctos. Haga clic en Finalizar.



La VCSA se instala ahora. Este proceso tarda varios minutos.

15. Una vez completada la fase 1, aparece un mensaje que indica que se ha completado. Haga clic en continuar para iniciar la configuración de la fase 2.
16. En la página Introducción de fase 2, haga clic en Siguiente.



17. Introduzca `<<var_ntp_id>>` Para la dirección del servidor NTP. Puede introducir varias direcciones IP de NTP.

    Si tiene pensado utilizar la alta disponibilidad (ha) de vCenter Server, asegúrese de que el acceso SSH esté habilitado.

18. Configure el nombre de dominio, la contraseña y el nombre del sitio de SSO. Haga clic en Siguiente.

    Registre estos valores para la referencia, especialmente si se desvía del nombre de dominio vsphere.local.

19. Únase al programa de experiencia del cliente de VMware si lo desea. Haga clic en Siguiente.
20. Vea el resumen de la configuración. Haga clic en Finalizar o utilice el botón Atrás para editar la configuración.
21. Aparece un mensaje que indica que no podrá detener o detener la instalación una vez iniciada. Haga clic en OK para continuar.

    La configuración del dispositivo continúa. Esto tarda varios minutos.

    Aparece un mensaje que indica que la configuración se ha realizado correctamente.

    Los enlaces que el instalador proporciona para acceder a vCenter Server pueden hacer clic.

"Siguiente: Configure VMware vCenter Server 6.7 y vSphere agrupando en clústeres."

Configure VMware vCenter Server 6.7 y el clustering de vSphere

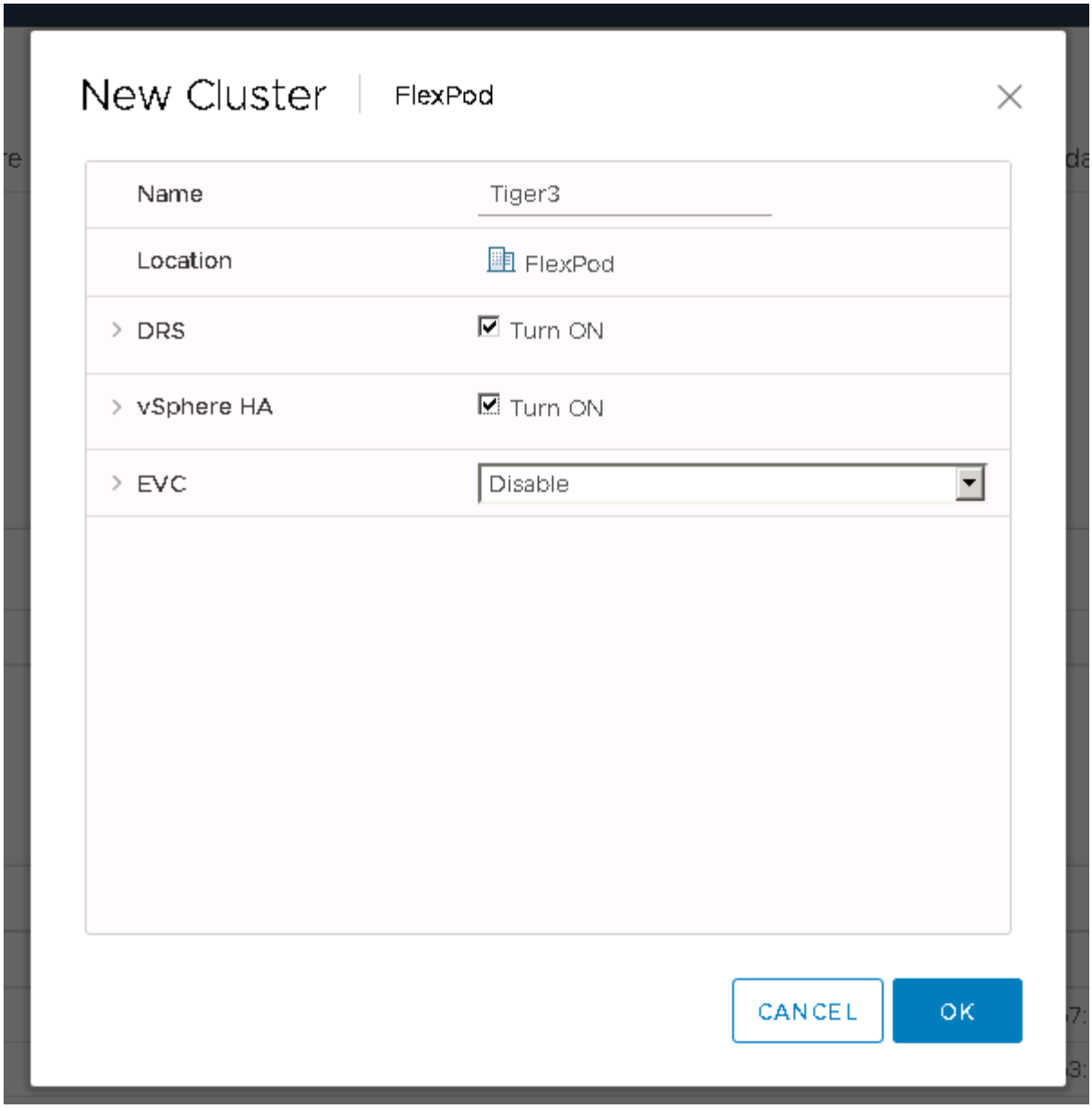
Para configurar la agrupación en clústeres de VMware vCenter Server 6.7 y vSphere, complete los pasos siguientes:

1. Desplácese hasta https://<<FQDN or IP of vCenter>>/vsphere-client/.
2. Haga clic en Launch vSphere Client.
3. Inicie sesión con el nombre de usuario mailto:administrator@vspehre.loc/ loc/[administrator@vsphere.loc/] y la contraseña SSO que introdujo durante el proceso de configuración de VCSA.
4. Haga clic con el botón derecho en el nombre de vCenter y seleccione New Datacenter.
5. Introduzca un nombre para el centro de datos y haga clic en Aceptar.

Cree un clúster de vSphere

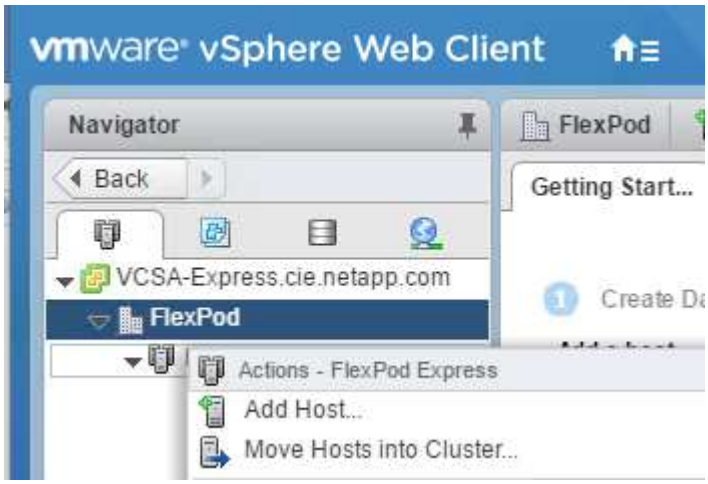
Complete los siguientes pasos para crear un clúster de vSphere:

1. Haga clic con el botón derecho en el centro de datos recién creado y seleccione New Cluster.
2. Escriba un nombre para el clúster.
3. Active la recuperación ante desastres y vSphere ha seleccionando las casillas de verificación.
4. Haga clic en Aceptar.



Añada hosts ESXi al clúster

1. Haga clic con el botón derecho en el clúster y seleccione Add Host.



2. Para añadir un host ESXi al clúster, complete los siguientes pasos:
   a. Introduzca la dirección IP o el FQDN del host. Haga clic en Siguiente.
   b. Introduzca el nombre de usuario raíz y la contraseña. Haga clic en Siguiente.
   c. Haga clic en Sí para reemplazar el certificado del host por un certificado firmado por el servidor de certificados VMware.
   d. Haga clic en Siguiente en la página Resumen de host.
   e. Haga clic en el icono verde + para añadir una licencia al host de vSphere.

      Este paso se puede completar más adelante si se desea.

   f. Haga clic en Siguiente para desactivar el modo de bloqueo.
   g. Haga clic en Next en la página de ubicación de la máquina virtual.
   h. Revise la página Listo para completar. Utilice el botón Atrás para realizar cualquier cambio o seleccione Finalizar.
3. Repita los pasos 1 y 2 para el host Cisco UCS B. Debe completar este proceso para los hosts adicionales que se agreguen a la configuración exprés de FlexPod.

Configure coredump en hosts ESXi

1. Utilice SSH, conéctese al host ESXi de IP de gestión, introduzca root para el nombre de usuario e introduzca la contraseña raíz.
2. Ejecute los siguientes comandos:

```
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. El mensaje `Verified the configured netdump server is running` aparece después de introducir el comando final.

Este proceso debe completarse para cualquier host adicional que se añada a FlexPod Express.

Conclusión

FlexPod Express proporciona una solución sencilla y efectiva, ya que proporciona un diseño validado que utiliza componentes líderes del sector. Al escalar agregando componentes adicionales, FlexPod Express puede adaptarse según las necesidades específicas del negocio. FlexPod Express se diseñó teniendo en cuenta a las pequeñas y medianas empresas, oficinas remotas y otras empresas que precisan soluciones dedicadas.

Dónde encontrar información adicional

Para obtener más información sobre la información descrita en este documento, consulte

los siguientes documentos y/o sitios web:

- Documentación de productos de NetApp

  "http://docs.netapp.com"

- Guía de diseño de FlexPod Express con VMware vSphere 6.7 y AFF A220 de NetApp

  "https://www.netapp.com/us/media/nva-1125-design.pdf"

FlexPod Express con VMware vSphere 6.7U1 y NetApp AFF A220 con almacenamiento basado en IP directamente incluido

NVA-1131-DEPLOY: FlexPod Express con VMware vSphere 6.7U1 y NetApp AFF A220 con almacenamiento basado en IP directamente incluido

Sree Lakshmi Lanka, NetApp

Las tendencias en el sector señalan una gran transformación de los centros de datos hacia una infraestructura compartida y cloud computing. Además, las organizaciones buscan una solución sencilla y eficaz para oficinas remotas y sucursales que aprovechen la tecnología con la que ya están familiarizados en su centro de datos.

FlexPod Express es una arquitectura prediseñada de prácticas recomendadas que se basa en el Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus y las tecnologías de almacenamiento de NetApp. Los componentes de un sistema FlexPod Express se asemejan a los del centro de datos FlexPod, lo que permite sinergias de gestión en todo el entorno de infraestructura DE TI a una escala menor. FlexPod Datacenter y FlexPod Express son plataformas óptimas para virtualización y sistemas operativos con configuración básica y cargas de trabajo empresariales.

El centro de datos FlexPod y FlexPod Express proporcionan una configuración básica y disponen de la versatilidad necesaria para ajustar el tamaño y optimizarse con el objetivo de acomodar distintos casos de uso y requisitos. Los clientes existentes de FlexPod Datacenter pueden gestionar su sistema FlexPod Express con las herramientas a las que están acostumbrados. Los nuevos clientes de FlexPod Express pueden adaptarse fácilmente a la gestión del centro de datos FlexPod cuando crezca su entorno.

FlexPod Express es una base de infraestructura óptima para oficinas remotas y sucursales (robo) y para pequeñas y medianas empresas. También es una solución óptima para los clientes que desean proporcionar infraestructura para cargas de trabajo dedicadas.

FlexPod Express proporciona una infraestructura fácil de gestionar que es adecuada para casi cualquier carga de trabajo.

Descripción general de la solución

Esta solución FlexPod Express forma parte del programa de infraestructura convergente de FlexPod.

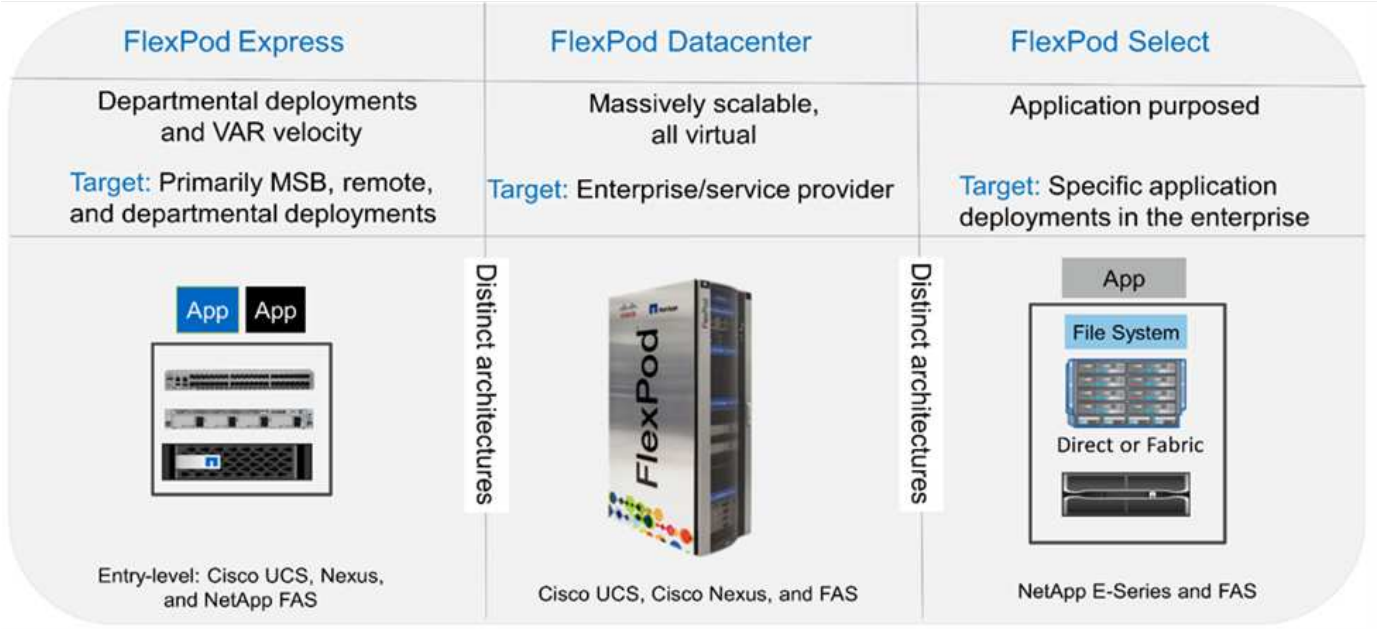
Programa de infraestructura convergente FlexPod

Las arquitecturas de referencia FlexPod se proporcionan como diseños validados por Cisco (CVD) o como arquitecturas verificadas por NetApp (NVA). Se permiten las desviaciones basadas en los requisitos de los clientes de un CVD o NVA determinado si estas variaciones no crean una configuración incompatible.

Como se muestra en la siguiente figura, el programa FlexPod incluye tres soluciones: FlexPod Express, FlexPod Datacenter y FlexPod Select:

- **FlexPod Express** ofrece a los clientes una solución de gama básica con tecnologías de Cisco y NetApp.
- **FlexPod Datacenter** proporciona una base multiuso óptima para diversas cargas de trabajo y aplicaciones.
- **FlexPod Select** incorpora los mejores aspectos del centro de datos FlexPod y adapta la infraestructura a una aplicación determinada.

En la siguiente figura se muestran los componentes técnicos de la solución.



Programa Arquitectura validada por NetApp

El programa NVA ofrece a los clientes una arquitectura verificada para las soluciones NetApp. NVA proporciona una arquitectura de solución de NetApp con las siguientes cualidades:

- Ha sido probada a conciencia
- Tiene naturaleza prescriptiva
- Minimiza los riesgos de implementación
- Reduce el plazo de comercialización

En esta guía se detalla el diseño de FlexPod Express con almacenamiento de NetApp de conexión directa. Las secciones siguientes enumeran los componentes utilizados para el diseño de esta solución.

Componentes de hardware

- AFF A220 de NetApp
- Cisco UCS Mini
- CISCO UCS B200 M5
- Cisco UCS VIC 1440/1480.
- Switches Cisco Nexus serie 3000

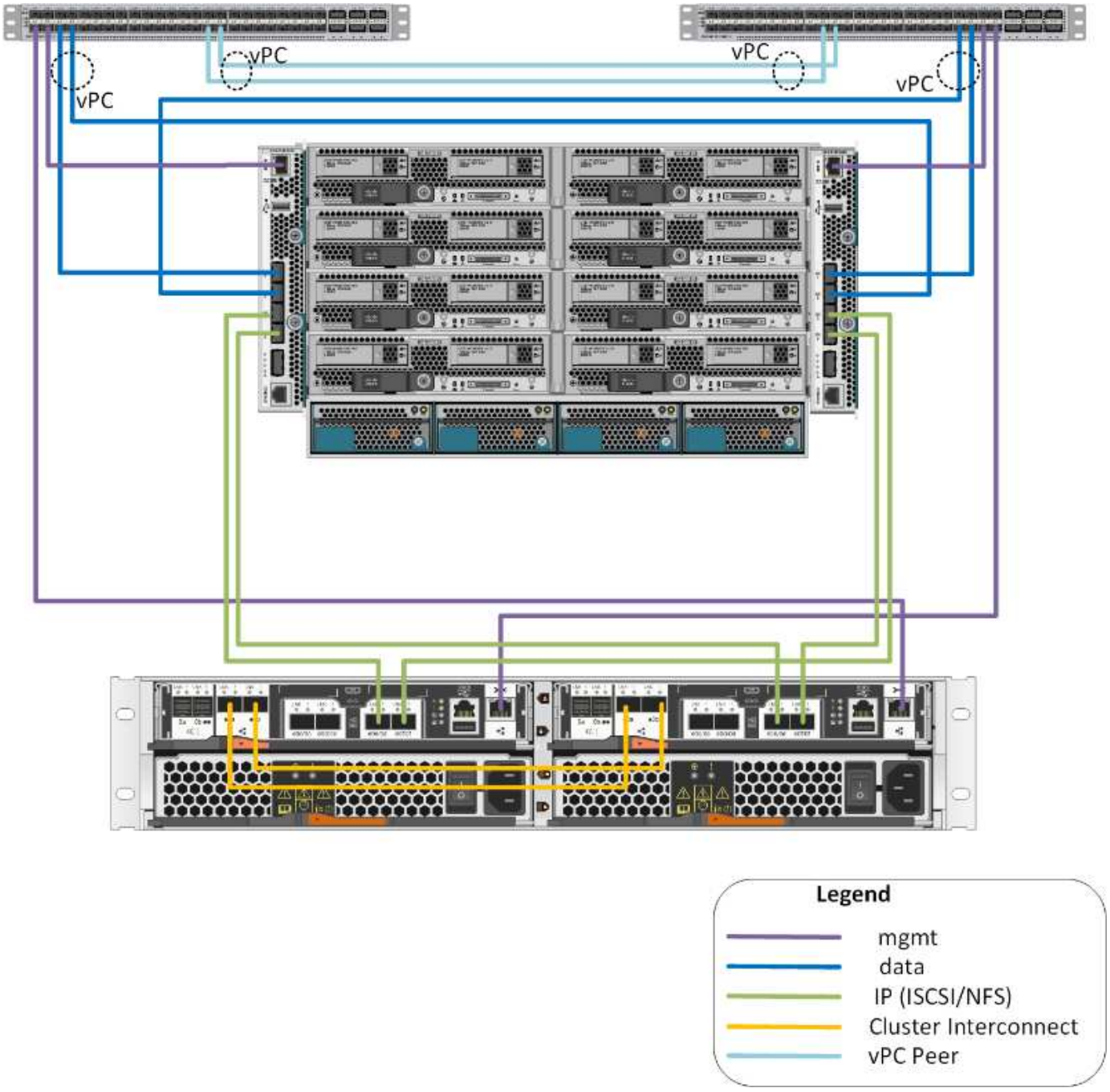
Componentes de software

- ONTAP 9 de NetApp. 5
- VMware vSphere 6.7U1
- Cisco UCS Manager 4.0(1b)
- Firmware Cisco NXOS 7.0(3)I6(1)

Tecnología de soluciones

Esta solución aprovecha las últimas tecnologías de NetApp, Cisco y VMware. Incluye el nuevo AFF A220 de NetApp que ejecute ONTAP 9.5, los conmutadores Cisco Nexus 31108PCV duales y los servidores Cisco UCS B200 M5 que ejecutan VMware vSphere 6.7U1. Esta solución validada usa almacenamiento IP de Direct Connect con tecnología 10GbE.

La siguiente figura muestra FlexPod Express con VMware vSphere 6.7U1, una arquitectura Direct Connect basada en IP.



Resumen de casos de uso

La solución FlexPod Express puede aplicarse a varios casos prácticos, incluidos los siguientes:

- ROBOS
- Pequeñas y medianas empresas
- Entornos que requieren una solución dedicada y rentable

FlexPod Express está indicado para cargas de trabajo virtualizadas y mixtas.

Requisitos tecnológicos

Un sistema FlexPod Express requiere una combinación de componentes de hardware y

software. FlexPod Express también describe los componentes de hardware necesarios para añadir nodos de hipervisor al sistema en unidades de dos.

Requisitos de hardware

Independientemente del hipervisor elegido, todas las configuraciones exprés de FlexPod utilizan el mismo hardware. Por lo tanto, aunque cambien los requisitos del negocio, cualquiera de los hipervisores puede ejecutarse en el mismo hardware de FlexPod Express.

En la siguiente tabla se enumeran los componentes de hardware necesarios para todas las configuraciones exprés de FlexPod.

Hardware subyacente	Cantidad
Par de alta disponibilidad AFF A220	1
Servidor Cisco UCS B200 M5	2
Switch Cisco Nexus 31108PCV	2
Tarjeta de interfaz virtual (VIC) Cisco UCS 1440 para el servidor Cisco UCS B200 M5	2
Cisco UCS Mini con dos interconexiones de estructura UCS-FI-M-6324 integradas	1

Requisitos de software

En la siguiente tabla se enumeran los componentes de software necesarios para implementar las arquitecturas de las soluciones Express de FlexPod.

De NetApp	Versión	Detalles
Administrador de Cisco UCS	4.0(1b)	Para Cisco UCS Fabric Interconnect FI-6324UP
Software blade Cisco	4.0(1b)	Para servidores Cisco UCS B200 M5
Controlador nenic de Cisco	1.0.25.0	Para tarjetas de interfaz Cisco VIC 1440
Cisco NX-OS	7.0(3)I6(1)	Para switches Cisco Nexus 31108PCV
ONTAP de NetApp	9.5	Para controladoras AFF A220

En la siguiente tabla se muestra el software necesario para todas las implementaciones de VMware vSphere en FlexPod Express.

De NetApp	Versión
Dispositivo VMware vCenter Server	6.7U1
Hipervisor ESXi de VMware vSphere	6.7U1

Información de cableado exprés de FlexPod

El cableado de validación de referencia se documenta en las siguientes tablas.

La tabla siguiente enumera información de cableado para el switch Cisco Nexus 31108PCV A.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Switch Cisco Nexus 31108PCV A	Eth1/1	Controladora De almacenamiento A AFF A220 de NetApp	E0M
	Eth1/2	Cisco UCS-mini FI-A.	mgmt0
	Eth1/3	Cisco UCS-mini FI-A.	Eth1/1
	ETH 1/4	Cisco UCS-mini FI-B	Eth1/1
	ETH 1/13	CISCO NX 31108PCV B	ETH 1/13
	ETH 1/14	CISCO NX 31108PCV B	ETH 1/14

En la siguiente tabla se muestra la información de cableado del switch Cisco Nexus 31108PCV B.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Switch Cisco Nexus 31108PCV B	Eth1/1	Controladora de almacenamiento B de AFF A220 de NetApp	E0M
	Eth1/2	Cisco UCS-mini FI-B	mgmt0
	Eth1/3	Cisco UCS-mini FI-A.	Eth1/2
	ETH 1/4	Cisco UCS-mini FI-B	Eth1/2
	ETH 1/13	CISCO NX 31108PCV A	ETH 1/13
	ETH 1/14	CISCO NX 31108PCV A	ETH 1/14

En la siguiente tabla se muestra información de cableado para la controladora de almacenamiento AFF A220 A. de NetApp

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Controladora De almacenamiento A AFF A220 de NetApp	e0a	Controladora de almacenamiento B de AFF A220 de NetApp	e0a
	e0b	Controladora de almacenamiento B de AFF A220 de NetApp	e0b
	e0e	Cisco UCS-mini FI-A.	Eth1/3
	e0f	Cisco UCS-mini FI-B	Eth1/3
	E0M	CISCO NX 31108PCV A	Eth1/1

La siguiente tabla enumera información de cableado para la controladora de almacenamiento AFF A220 B.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Controladora de almacenamiento B de AFF A220 de NetApp	e0a	Controladora de almacenamiento B de AFF A220 de NetApp	e0a
	e0b	Controladora de almacenamiento B de AFF A220 de NetApp	e0b
	e0e	Cisco UCS-mini FI-A.	Eth1/4
	e0f	Cisco UCS-mini FI-B	Eth1/4
	E0M	CISCO NX 31108PCV B	Eth1/1

La siguiente tabla enumera la información de cableado para Cisco UCS Fabric Interconnect A.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Interconexión de estructura Cisco UCS a	Eth1/1	CISCO NX 31108PCV A	Eth1/3
	Eth1/2	CISCO NX 31108PCV B	Eth1/3
	Eth1/3	Controladora De almacenamiento A AFF A220 de NetApp	e0e
	Eth1/4	Controladora de almacenamiento B de AFF A220 de NetApp	e0e
	mgmt0	CISCO NX 31108PCV A	Eth1/2

La siguiente tabla enumera información de cableado para Cisco UCS Fabric Interconnect B.

Dispositivo local	Puerto local	Dispositivo remoto	Puerto remoto
Interconexión de estructura B de Cisco UCS	Eth1/1	CISCO NX 31108PCV A	Eth1/4
	Eth1/2	CISCO NX 31108PCV B	Eth1/4
	Eth1/3	Controladora De almacenamiento A AFF A220 de NetApp	e0f
	Eth1/4	Controladora de almacenamiento B de AFF A220 de NetApp	e0f
	mgmt0	CISCO NX 31108PCV B	Eth1/2

Procedimientos de implantación

Este documento proporciona detalles para configurar un sistema FlexPod Express completamente redundante y de alta disponibilidad. Para reflejar esta redundancia, los componentes que se configuran en cada paso se denominan componente A o componente B. Por ejemplo, la controladora A y la controladora B identifican las dos

controladoras de almacenamiento de NetApp que se aprovisionan en este documento. El switch A y el switch B identifican un par de switches Cisco Nexus. La interconexión de estructura A y la interconexión de estructura B son las dos interconexiones de estructura Nexus integradas.

Además, en este documento se describen los pasos para aprovisionar varios hosts de Cisco UCS, que se identifican secuencialmente como servidor A, servidor B, etc.

Para indicar que debe incluir la información pertinente a su entorno en un paso, `<<text>>` aparece como parte de la estructura de comandos. Consulte el siguiente ejemplo de `vlan create` comando:

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

Este documento permite configurar completamente el entorno de FlexPod Express. En este proceso, varios pasos requieren que inserte convenciones de nomenclatura específicas del cliente, direcciones IP y esquemas de red de área local virtual (VLAN). En la siguiente tabla se describen las VLAN necesarias para la implementación, tal y como se explica en esta guía. Esta tabla se puede completar en función de las variables específicas del sitio y se puede utilizar para implementar los pasos de configuración del documento.

Si utiliza VLAN de gestión fuera de banda y en banda independientes, debe crear una ruta de capa 3 entre ellas. Para esta validación, se utilizó una VLAN de gestión común.

Nombre de la VLAN	Propósito de VLAN	ID utilizado para validar este documento
VLAN de gestión	VLAN para interfaces de gestión	18
VLAN nativa	VLAN a la que se asignan tramas no etiquetadas	2
VLAN NFS	VLAN para tráfico NFS	104
VLAN de VMware vMotion	VLAN designada para mover máquinas virtuales (VM) de un host físico a otro	103
VLAN de tráfico de la máquina virtual	VLAN para tráfico de aplicaciones de equipos virtuales	102
ISCSI-A-VLAN	VLAN para tráfico iSCSI en la estructura A	124
ISCSI-B-VLAN	VLAN para tráfico iSCSI en la estructura B	125

Los números VLAN son necesarios en toda la configuración de FlexPod Express. Las VLAN se denominan `<<var_xxxx_vlan>>`, donde `xxxx` Es la finalidad de la VLAN (como iSCSI-A).

La siguiente tabla enumera las máquinas virtuales de VMware creadas.

Descripción de VM	Nombre de host
Servidor VMware vCenter	Seahawks-vcsa.cie.netapp.com

Procedimiento de puesta en marcha de Cisco Nexus 31108PCV

En esta sección se detalla la configuración del switch Cisco Nexus 31308PCV utilizada en un entorno FlexPod Express.

Configuración inicial del switch Cisco Nexus 31108PCV

Este procedimiento describe cómo configurar los switches Cisco Nexus para su uso en un entorno FlexPod Express básico.

> En este procedimiento se asume que está utilizando un Cisco Nexus 31108PCV con la versión de software NX-OS 7.0(3)I6(1).

1. Tras el arranque y la conexión iniciales al puerto de la consola del switch, se inicia automáticamente la configuración de Cisco NX-OS. Esta configuración inicial trata los valores básicos, como el nombre del switch, la configuración de la interfaz mgmt0 y la configuración de Secure Shell (SSH).
2. La red de gestión del sistema FlexPod Express se puede configurar de varias maneras. Las interfaces mgmt0 de los conmutadores 31108PCV se pueden conectar a una red de administración existente, o las interfaces mgmt0 de los conmutadores 31108PCV se pueden conectar en una configuración posterior. Sin embargo, este enlace no se puede utilizar para el acceso de gestión externo, como tráfico SSH.

   En esta guía de puesta en marcha, los switches Cisco Nexus 31108PCV de FlexPod Express están conectados a una red de gestión existente.
3. Para configurar los switches Cisco Nexus 31108PCV, encienda el switch y siga las indicaciones que aparecen en pantalla, como se muestra aquí para la configuración inicial de ambos switches, sustituyendo los valores adecuados para la información específica del switch.

   ```
   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. Se muestra un resumen de la configuración y se le pregunta si desea editar la configuración. Si la configuración es correcta, introduzca `n`.

```
Would you like to edit the configuration? (yes/no) [n]: no
```

5. A continuación, se le preguntará si desea utilizar esta configuración y guardarla. Si es así, introduzca `y`.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Repita los pasos del 1 al 5 para el switch Cisco Nexus B.

Habilite funciones avanzadas

Determinadas características avanzadas deben estar habilitadas en Cisco NX-OS para proporcionar opciones

de configuración adicionales.

1. Para habilitar las funciones adecuadas en los switches a y B de Cisco Nexus, escriba el modo de configuración mediante el comando `(config t)` y ejecute los siguientes comandos:

```
feature interface-vlan
feature lacp
feature vpc
```

> El hash de equilibrio de carga del canal de puerto predeterminado utiliza las direcciones IP de origen y destino para determinar el algoritmo de equilibrio de carga en las interfaces del canal de puerto. Puede lograr una mejor distribución entre los miembros del canal de puerto proporcionando más entradas al algoritmo hash más allá de las direcciones IP de origen y destino. Por el mismo motivo, NetApp recomienda encarecidamente añadir los puertos TCP de origen y destino al algoritmo hash.

2. Desde el modo de configuración `(config t)`, Ejecute los siguientes comandos para establecer la configuración de equilibrio de carga del canal de puertos global en los conmutadores A y B de Cisco Nexus:

```
port-channel load-balance src-dst ip-l4port
```

Realizar la configuración de árbol de expansión global

La plataforma Cisco Nexus utiliza una nueva función de protección llamada garantía de puente. La garantía de puente ayuda a proteger contra un enlace unidireccional u otro error de software con un dispositivo que continúa redirectando el tráfico de datos cuando ya no ejecuta el algoritmo de árbol expansivo. Los puertos se pueden colocar en uno de varios estados, incluyendo la red o el borde, dependiendo de la plataforma.

NetApp recomienda establecer la garantía de puente para que todos los puertos se consideren puertos de red de forma predeterminada. Este ajuste obliga al administrador de red a revisar la configuración de cada puerto. También revela los errores de configuración más comunes, como puertos de borde no identificados o un vecino que no tiene activada la función de garantía de puente. Además, es más seguro tener el bloque de árbol expansivo muchos puertos en lugar de muy pocos, lo que permite que el estado de puerto predeterminado mejore la estabilidad general de la red.

Preste especial atención al estado de árbol de expansión al agregar servidores, almacenamiento y switches ascendentes, especialmente si no admiten la garantía de puente. En estos casos, es posible que deba cambiar el tipo de puerto para que los puertos estén activos.

El protector de unidad de datos de protocolo puente (BPDU) está habilitado de forma predeterminada en puertos periféricos como otra capa de protección. Para evitar bucles en la red, esta característica cierra el puerto si se ven BPDU de otro switch en esta interfaz.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para configurar las opciones de árbol expansivo predeterminadas, incluidos el tipo de puerto predeterminado y el protector BPDU, en el conmutador A de Cisco Nexus y el conmutador B:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

Defina las VLAN

Antes de configurar puertos individuales con VLAN diferentes, se deben definir las VLAN de capa 2 en el switch. También se recomienda nombrar las VLAN para que la solución de problemas sea sencilla en el futuro.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para definir y describir las VLAN de capa 2 en el switch A y el switch B de Cisco Nexus:

```
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
```

Configurar el acceso y las descripciones de los puertos de gestión

Como es el caso, la asignación de nombres a las VLAN de capa 2, las descripciones de configuración de todas las interfaces pueden ayudar tanto al aprovisionamiento como a la solución de problemas.

Desde el modo de configuración (`config t`) En cada uno de los conmutadores, introduzca las siguientes descripciones de puerto para la configuración grande de FlexPod Express:

Switch Cisco Nexus 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
```

Switch Cisco Nexus 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
```

Configurar las interfaces de gestión de almacenamiento y servidores

Las interfaces de gestión para el servidor y el almacenamiento suelen utilizar una sola VLAN. Por lo tanto, configure los puertos de la interfaz de gestión como puertos de acceso. Defina la VLAN de administración para cada switch y cambie el tipo de puerto de árbol expansivo a EDGE.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para configurar los ajustes de puerto para las interfaces de administración tanto de los servidores como del almacenamiento:

Switch Cisco Nexus a

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Switch Cisco Nexus B

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Añada la interfaz de distribución de NTP

Switch Cisco Nexus a

Desde el modo de configuración global, ejecute los siguientes comandos.

```
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
```

Switch Cisco Nexus B

Desde el modo de configuración global, ejecute los siguientes comandos.

```
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
```

Llevar a cabo la configuración global del canal de puertos virtuales

Un canal de puerto virtual (VPC) permite que los enlaces que están conectados físicamente a dos switches de Cisco Nexus diferentes aparezcan como un único canal de puerto a un tercer dispositivo. El tercer dispositivo puede ser un conmutador, un servidor o cualquier otro dispositivo de red. Un VPC puede proporcionar una multivía de nivel 2, que le permite crear redundancia aumentando el ancho de banda, permitiendo múltiples rutas paralelas entre los nodos y tráfico de equilibrio de carga donde haya rutas alternativas.

Un VPC proporciona las siguientes ventajas:

- Permitir que un único dispositivo utilice un canal de puerto a través de dos dispositivos de subida
- Eliminar puertos bloqueados del protocolo de árbol expansivo
- Proporciona una topología sin bucles
- Utilizando todo el ancho de banda disponible de enlace ascendente
- Proporcionar convergencia rápida si el enlace o un dispositivo falla
- Resiliencia a nivel de enlace
- Contribuir a proporcionar una alta disponibilidad

La función VPC requiere alguna configuración inicial entre los dos switches de Cisco Nexus para que funcionen correctamente. Si utiliza la configuración de mgmt0 de fondo, utilice las direcciones definidas en las interfaces y compruebe que se pueden comunicar mediante ping `<<switch_A/B_mgmt0_ip_addr>>vrf` comando de gestión.

Desde el modo de configuración (`config t`), ejecute los siguientes comandos para configurar la configuración global de VPC para ambos switches:

Switch Cisco Nexus 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
```

Switch Cisco Nexus B

```
vpc domain 1
peer-switch
role priority 20
peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10
description vPC peer-link
switchport
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
```

```
  channel-group 14 mode active
copy run start
```

En esta validación de solución se utilizó una unidad de transmisión máxima (MTU) de 9000. Sin embargo, en función de los requisitos de la aplicación, puede configurar un valor de MTU adecuado. Es importante establecer el mismo valor de MTU en la solución de FlexPod. Las configuraciones de MTU incorrectas entre componentes provocan la eliminación de paquetes.

Enlace ascendente a la infraestructura de red existente

En función de la infraestructura de red disponible, se pueden utilizar varios métodos y funciones para elevar el entorno FlexPod. Si existe un entorno Cisco Nexus existente, NetApp recomienda utilizar VPC para conectar los switches Cisco Nexus 31108PVC incluidos en el entorno FlexPod a la infraestructura. Los enlaces ascendentes pueden ser enlaces de subida de 10 GbE para una solución de infraestructura de 10 GbE o 1 GbE para una solución de infraestructura de 1 GbE si fuera necesario. Los procedimientos descritos anteriormente se pueden utilizar para crear un VPC de enlace ascendente al entorno existente. Asegúrese de ejecutar Copy RUN START para guardar la configuración en cada switch una vez completada la configuración.

Procedimiento de instalación de almacenamiento NetApp (parte 1)

En esta sección se describe el procedimiento de implementación del almacenamiento AFF de NetApp.

Instalación de la controladora de almacenamiento de NetApp serie AFF2xx

Hardware Universe de NetApp

La "Hardware Universe de NetApp" (HWU) proporciona componentes de hardware y software compatibles con cualquier versión específica de ONTAP. Proporciona información de configuración para todos los dispositivos de almacenamiento de NetApp compatibles actualmente con el software ONTAP. También se proporciona una tabla de compatibilidades de componentes.

Confirme que los componentes de hardware y software que desea utilizar son compatibles con la versión de ONTAP que tiene previsto instalar:

1. Acceda a "HWU" aplicación para ver las guías de configuración del sistema. Seleccione la pestaña Comparar sistemas de almacenamiento para ver la compatibilidad entre diferentes versiones del software ONTAP y los dispositivos de almacenamiento de NetApp con las especificaciones que desea.
2. Como alternativa, para comparar componentes por dispositivo de almacenamiento, haga clic en Comparar sistemas de almacenamiento.

Requisitos previos de la controladora de la serie AFF2XX
Para planificar la ubicación física de los sistemas de almacenamiento, consulte las siguientes secciones: Requisitos eléctricos cables de alimentación compatibles puertos y cables integrados

Controladoras de almacenamiento

Siga los procedimientos de instalación física de los controladores de la "Documentación de AFF A220".

ONTAP 9.5 de NetApp

Hoja de datos de configuración

Antes de ejecutar la secuencia de comandos de instalación, rellene la hoja de datos de configuración del manual del producto. La hoja de datos de configuración está disponible en la "Guía de configuración de software de ONTAP 9.5" (disponible en la "Centro de documentación de ONTAP 9"). La siguiente tabla muestra información sobre la instalación y la configuración de ONTAP 9.5.

Este sistema se establece en una configuración de clúster de dos nodos sin switch.

Detalles del clúster	Valor de detalles del clúster
Nodo del clúster: Dirección IP	<<var_nodeA_mgmt_ip>>
Máscara de red Del nodo a del clúster	<<var_nodeA_mgmt_mask>>
Nodo del clúster: Puerta de enlace	<<var_nodeA_mgmt_gateway>>
Nombre del nodo a del clúster	<<var_nodeA>>
Dirección IP del nodo B del clúster	<<var_nodeB_mgmt_ip>>
Máscara de red del nodo B del clúster	<<var_nodeB_mgmt_mask>>
Puerta de enlace del nodo B del clúster	<<var_nodeB_mgmt_gateway>>
Nombre del nodo B del clúster	<<var_nodeB>>
Dirección URL de ONTAP 9.5	<<var_url_boot_software>>
El nombre del clúster	<<var_clustername>>
Dirección IP de gestión del clúster	<<var_clustermgmt_ip>>
Puerta de enlace del clúster B.	<<var_clustermgmt_gateway>>
Máscara de red del clúster B.	<<var_clustermgmt_mask>>
Nombre de dominio	<<var_domain_name>>
IP del servidor DNS (puede introducir más de uno)	<<var_dns_server_ip>>
SERVIDOR NTP: UNA IP	<< switch-a-ntp-ip >>
IP DEL SERVIDOR NTP B.	<< switch-b-ntp-ip >>

Configure el nodo A

Para configurar el nodo A, complete los siguientes pasos:

1. Conéctese al puerto de la consola del sistema de almacenamiento. Tiene que ver un cargador-a del símbolo del sistema. Sin embargo, si el sistema de almacenamiento está en un bucle de reinicio, pulse Ctrl- C para salir del bucle de autoarranque cuando vea este mensaje:

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. Permita que el sistema arranque.

```
autoboot
```

3. Pulse Ctrl- C para acceder al menú Inicio.

   Si es ONTAP 9. 5 no es la versión del software que se está arrancando, continúe con los pasos siguientes para instalar el software nuevo. Si es ONTAP 9. 5 es la versión que se va a arrancar, seleccione la opción 8 e y para reiniciar el nodo. A continuación, continúe con el paso 14.

4. Para instalar software nuevo, seleccione opción `7`.
5. Introduzca `y` para realizar una actualización.
6. Seleccione `e0M` para el puerto de red que desea usar para la descarga.
7. Introduzca `y` para reiniciar ahora.
8. Introduzca la dirección IP, la máscara de red y la puerta de enlace predeterminada para e0M en sus respectivos lugares.

   ```
   <<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
   ```

9. Especifique la dirección URL donde se puede encontrar el software.

   Este servidor web debe ser pingable.

10. Pulse Intro para el nombre de usuario, indicando que no hay nombre de usuario.
11. Introduzca `y` para establecer el software recién instalado como el predeterminado que se utilizará para los siguientes reinicios.
12. Introduzca `y` para reiniciar el nodo.

    Al instalar el software nuevo, el sistema podría realizar actualizaciones de firmware en el BIOS y las tarjetas adaptadoras, lo que provoca reinicios y posibles interrupciones en el cargador. Si se producen estas acciones, el sistema podría desviarse de este procedimiento.

13. Pulse Ctrl- C para acceder al menú Inicio.
14. Seleccione opción `4` Para una configuración limpia y inicializar todos los discos.
15. Introduzca `y` para poner a cero discos, restablezca la configuración e instale un nuevo sistema de archivos.
16. Introduzca `y` para borrar todos los datos de los discos.

    La inicialización y creación del agregado raíz puede tardar 90 minutos o más en completarse, según el número y el tipo de discos conectados. Una vez finalizada la inicialización, el sistema de almacenamiento se reinicia. Tenga en cuenta que los SSD tardan mucho menos tiempo en inicializarse. Puede continuar con la configuración del nodo B mientras los discos del nodo A se están poniendo a cero.

17. Mientras el nodo A se está inicializando, empiece a configurar el nodo B.

Configure el nodo B

Para configurar el nodo B, complete los siguientes pasos:

1. Conéctese al puerto de la consola del sistema de almacenamiento. Tiene que ver un cargador-a del símbolo del sistema. Sin embargo, si el sistema de almacenamiento está en un bucle de reinicio, pulse Ctrl-C para salir del bucle de autoarranque cuando vea este mensaje:

   ```
   Starting AUTOBOOT press Ctrl-C to abort...
   ```

2. Pulse Ctrl-C para acceder al menú Inicio.

   ```
   autoboot
   ```

3. Pulse Ctrl-C cuando se le solicite.

   Si es ONTAP 9. 5 no es la versión del software que se está arrancando, continúe con los pasos siguientes para instalar el software nuevo. Si ONTAP 9.4 es la versión que se va a arrancar, seleccione la opción 8 e y para reiniciar el nodo. A continuación, continúe con el paso 14.

4. Para instalar software nuevo, seleccione la opción 7.
5. Introduzca `y` para realizar una actualización.
6. Seleccione `e0M` para el puerto de red que desea usar para la descarga.
7. Introduzca `y` para reiniciar ahora.
8. Introduzca la dirección IP, la máscara de red y la puerta de enlace predeterminada para e0M en sus respectivos lugares.

   ```
   <<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
   ```

9. Especifique la dirección URL donde se puede encontrar el software.

   Este servidor web debe ser pingable.

   ```
   <<var_url_boot_software>>
   ```

10. Pulse Intro para el nombre de usuario, indicando que no hay nombre de usuario
11. Introduzca `y` para establecer el software recién instalado como el predeterminado que se utilizará para los siguientes reinicios.
12. Introduzca `y` para reiniciar el nodo.

    Al instalar el software nuevo, el sistema podría realizar actualizaciones de firmware en el BIOS y las tarjetas adaptadoras, lo que provoca reinicios y posibles interrupciones en el cargador. Si se producen estas acciones, el sistema podría desviarse de este procedimiento.

13. Pulse Ctrl-C para acceder al menú Inicio.
14. Seleccione la opción 4 para Configuración limpia y inicializar todos los discos.
15. Introduzca `y` para poner a cero discos, restablezca la configuración e instale un nuevo sistema de archivos.
16. Introduzca `y` para borrar todos los datos de los discos.

    La inicialización y creación del agregado raíz puede tardar 90 minutos o más en completarse, según el número y el tipo de discos conectados. Una vez finalizada la inicialización, el sistema de almacenamiento se reinicia. Tenga en cuenta que los SSD tardan mucho menos tiempo en inicializarse.

Continuación de la configuración Del nodo a y de la configuración del clúster

Desde un programa de puertos de consola conectado al puerto de la consola De la controladora De almacenamiento A (nodo A), ejecute el script de configuración del nodo. Este script se muestra cuando ONTAP 9.5 arranca en el nodo por primera vez.

El procedimiento de configuración del nodo y de los clústeres ha cambiado ligeramente en ONTAP 9.5. El asistente de configuración de clúster ahora se utiliza para configurar el primer nodo de un clúster, y System Manager se utiliza para configurar el clúster.

1. Siga las instrucciones para configurar el nodo 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. Vaya a la dirección IP de la interfaz de gestión del nodo.

> La configuración del clúster también se puede realizar mediante la CLI. Este documento describe la configuración del clúster mediante la configuración guiada de System Manager de NetApp.

3. Haga clic en Guided Setup para configurar el clúster.
4. Introduzca `<<var_clustername>>` del nombre del clúster y. `<<var_nodeA>>` y.. `<<var_nodeB>>` para cada uno de los nodos que va a configurar. Introduzca la contraseña que desea usar para el sistema de almacenamiento. Seleccione Switchless Cluster para el tipo de clúster. Introduzca la licencia base del clúster.
5. También es posible introducir licencias de funciones para Cluster, NFS e iSCSI.
6. Ve un mensaje de estado que indica que el clúster se está creando. Este mensaje de estado cambia por varios Estados. Este proceso tarda varios minutos.
7. Configure la red.
   a. Anule la selección de la opción intervalo de direcciones IP.

b. Introduzca `<<var_clustermgmt_ip>>` En el campo Cluster Management IP Address, `<<var_clustermgmt_mask>>` En el campo máscara de red, y. `<<var_clustermgmt_gateway>>` En el campo Puerta de enlace. Use el … Selector en el campo Port para seleccionar e0M del nodo A.

c. La IP de gestión de nodos para el nodo A ya se ha rellenado. Introduzca `<<var_nodeA_mgmt_ip>>` Para el nodo B.

d. Introduzca `<<var_domain_name>>` En el campo DNS Domain Name. Introduzca `<<var_dns_server_ip>>` En el campo DNS Server IP Address.

   Puede introducir varias direcciones IP del servidor DNS.

e. Introduzca `<<switch-a-ntp-ip>>` En el campo servidor NTP primario.

   También puede introducir un servidor NTP alternativo como `<<switch- b-ntp-ip>>`.

8. Configure la información de soporte.
   a. Si el entorno requiere un proxy para acceder a AutoSupport, introduzca la URL en Proxy URL.
   b. Introduzca el host de correo SMTP y la dirección de correo electrónico para las notificaciones de eventos.

      Debe, como mínimo, configurar el método de notificación de eventos antes de continuar. Puede seleccionar cualquiera de los métodos.

9. Cuando indique que ha finalizado la configuración del clúster, haga clic en Manage your Cluster para configurar el almacenamiento.

Continuación de la configuración del clúster de almacenamiento

Después de configurar los nodos de almacenamiento y el clúster base, puede continuar con la configuración del clúster de almacenamiento.

Ponga a cero todos los discos de repuesto

Para poner a cero todos los discos de repuesto del clúster, ejecute el siguiente comando:

```
disk zerospares
```

Configure la personalidad de los puertos UTA2 integrados

1. Verifique el modo actual y el tipo actual de puertos ejecutando el `ucadmin show` comando.

```
AFFA220-Clus::> ucadmin show
                     Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFFA220-Clus-01
              0c       cna      target     -        -          offline
AFFA220-Clus-01
              0d       cna      target     -        -          offline
AFFA220-Clus-01
              0e       cna      target     -        -          offline
AFFA220-Clus-01
              0f       cna      target     -        -          offline
AFFA220-Clus-02
              0c       cna      target     -        -          offline
AFFA220-Clus-02
              0d       cna      target     -        -          offline
AFFA220-Clus-02
              0e       cna      target     -        -          offline
AFFA220-Clus-02
              0f       cna      target     -        -          offline
8 entries were displayed.
```

2. Compruebe que el modo actual de los puertos que se están utilizando es `cna` y que el tipo actual está establecido en `target`. De lo contrario, cambie la personalidad de puerto ejecutando el siguiente comando:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

Los puertos deben estar desconectados para que se ejecute el comando anterior. Para desconectar un puerto, ejecute el siguiente comando:

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

Si ha cambiado la personalidad del puerto, debe reiniciar cada nodo para que el cambio se aplique.

Habilite el protocolo de detección de Cisco

Para habilitar el protocolo de detección de Cisco (CDP) en las controladoras de almacenamiento de NetApp, ejecute el siguiente comando:

```
node run -node * options cdpd.enable on
```

Habilite el protocolo de detección de capa de enlace en todos los puertos Ethernet

Habilite el intercambio de información cercana del protocolo de detección de capa de enlace (LLDP) entre los switches de red y almacenamiento ejecutando el siguiente comando. Este comando habilita LLDP en todos los puertos de todos los nodos del clúster.

```
node run * options lldp.enable on
```

Cambie el nombre de las interfaces lógicas de gestión

Para cambiar el nombre de las interfaces lógicas de gestión (LIF), realice los pasos siguientes:

1. Muestra los nombres de las LIF de gestión actuales.

   ```
   network interface show –vserver <<clustername>>
   ```

2. Cambie el nombre de la LIF de gestión del clúster.

   ```
   network interface rename –vserver <<clustername>> –lif
   cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
   ```

3. Cambie el nombre del LIF de gestión del nodo B.

   ```
   network interface rename -vserver <<clustername>> -lif
   cluster_setup_node_mgmt_lif_AFF A220_A_1 - newname AFF A220-01_mgmt1
   ```

Configure la reversión automática en la gestión del clúster

Ajuste la `auto-revert` parámetro en la interfaz de gestión del clúster.

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-
revert true
```

Configure la interfaz de red del procesador de servicio

Para asignar una dirección IPv4 estática al procesador de servicios en cada nodo, ejecute los siguientes comandos:

```
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>>
```

Las direcciones IP de Service Processor deben estar en la misma subred que las direcciones IP de gestión de nodos.

Activar la recuperación tras fallos de almacenamiento en ONTAP

Para confirmar que la conmutación por error del almacenamiento está habilitada, ejecute los siguientes comandos de una pareja de conmutación por error:

1. Comprobar el estado de recuperación tras fallos del almacenamiento.

   ```
   storage failover show
   ```

   Ambas `<<var_nodeA>>` y.. `<<var_nodeB>>` debe poder realizar una toma de control. Vaya al paso 3 si los nodos pueden realizar una toma de control.

2. Habilite la conmutación al nodo de respaldo en uno de los dos nodos.

   ```
   storage failover modify -node <<var_nodeA>> -enabled true
   ```

3. Compruebe el estado de alta disponibilidad del clúster de dos nodos.

   Este paso no es aplicable para clústeres con más de dos nodos.

   ```
   cluster ha show
   ```

4. Vaya al paso 6 si está configurada la alta disponibilidad. Si se ha configurado la alta disponibilidad, verá el siguiente mensaje al emitir el comando:

   ```
   High Availability Configured: true
   ```

5. Habilite el modo de alta disponibilidad solo para el clúster de dos nodos.

   No ejecute este comando para clústeres con más de dos nodos debido a que provoca problemas con la conmutación al nodo de respaldo.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. Compruebe que la asistencia de hardware está correctamente configurada y, si es necesario, modifique la dirección IP del partner.

```
storage failover hwassist show
```

El mensaje `Keep Alive Status : Error: did not receive hwassist keep alive alerts from partner` indica que la asistencia de hardware no está configurada. Ejecute los siguientes comandos para configurar hardware Assist.

```
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>>
```

Cree un dominio de retransmisión MTU para tramas gigantes en ONTAP

Para crear un dominio de retransmisión de datos con un valor MTU de 9000, ejecute los siguientes comandos:

```
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
```

Quite los puertos de datos del dominio de retransmisión predeterminado

Los puertos de datos de 10 GbE se utilizan para el tráfico iSCSI/NFS y estos puertos deben eliminarse del dominio predeterminado. Los puertos e0e y e0f no se utilizan y deben eliminarse del dominio predeterminado.

Para quitar puertos del dominio de retransmisión, ejecute el siguiente comando:

```
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
```

Deshabilite el control de flujo en los puertos UTA2

Se recomienda utilizar las mejores prácticas de NetApp para deshabilitar el control de flujo en todos los puertos UTA2 conectados a dispositivos externos. Para desactivar el control de flujo, ejecute los siguientes comandos:

```
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
```

La conexión mínima directa de Cisco UCS a ONTAP no es compatible con LACP.

Configurar tramas gigantes en ONTAP de NetApp

Para configurar un puerto de red ONTAP para que utilice tramas gigantes (que normalmente tienen una MTU de 9,000 bytes), ejecute los siguientes comandos desde el shell del clúster:

```
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
```

Crear VLAN en ONTAP

Para crear VLAN en ONTAP, complete los siguientes pasos:

1. Cree puertos VLAN NFS y añádalos al dominio de retransmisión de datos.

```
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. Cree puertos VLAN iSCSI y añádalos al dominio de retransmisión de datos.

```
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. Cree puertos MGMT-VLAN.

```
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>>
```

Crear agregados en ONTAP

Durante el proceso de configuración de ONTAP, se crea un agregado que contiene el volumen raíz. Para crear agregados adicionales, determine el nombre del agregado, el nodo en el que se creará y el número de discos que contiene.

Para crear agregados, ejecute los siguientes comandos:

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

Conserve al menos un disco (seleccione el disco más grande) en la configuración como un repuesto. Una práctica recomendada es tener al menos un repuesto para cada tipo y tamaño de disco.

Empiece con cinco discos; puede añadir discos a un agregado cuando necesite almacenamiento adicional.

No se puede crear el agregado hasta que se complete el establecimiento en cero del disco. Ejecute el `aggr show` comando para mostrar el estado de creación del agregado. No continúe hasta `aggr1_nodeA` está en línea.

Configurar la zona horaria en ONTAP

Para configurar la sincronización horaria y establecer la zona horaria en el clúster, ejecute el siguiente comando:

```
timezone <<var_timezone>>
```

Por ejemplo, en el este de los Estados Unidos, la zona horaria es `America/New_York`. Cuando haya comenzado a escribir el nombre de la zona horaria, pulse la tecla TAB para ver las opciones disponibles.

Configurar SNMP en ONTAP

Para configurar SNMP, realice los siguientes pasos:

1. Configure la información básica de SNMP, como la ubicación y el contacto. Cuando se sondean, esta información es visible como `sysLocation` y.. `sysContact` Variables en SNMP.

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. Configure las capturas SNMP para que se envíen a hosts remotos.

```
snmp traphost add <<var_snmp_server_fqdn>>
```

Configure SNMPv1 en ONTAP

Para configurar SNMPv1, establezca la contraseña de texto sin formato secreta compartida denominada comunidad.

```
snmp community add ro <<var_snmp_community>>
```

Utilice la `snmp community delete all` comando con precaución. Si se utilizan cadenas de comunidad para otros productos de supervisión, este comando las quita.

Configure SNMPv3 en ONTAP

SNMPv3 requiere que defina y configure un usuario para la autenticación. Para configurar SNMPv3, lleve a cabo los siguientes pasos:

1. Ejecute el `security snmpusers` Comando para ver el ID del motor.
2. Cree un usuario llamado `snmpv3user`.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. Introduzca el ID del motor de la entidad autoritativa y seleccione `md5` como protocolo de autenticación.
4. Escriba una contraseña de longitud mínima de ocho caracteres para el protocolo de autenticación cuando se le solicite.
5. Seleccione `des` como protocolo de privacidad.
6. Escriba una contraseña de longitud mínima de ocho caracteres para el protocolo de privacidad cuando se le solicite.

Configure HTTPS de AutoSupport en ONTAP

La herramienta AutoSupport de NetApp envía información de resumen de soporte a NetApp mediante HTTPS. Para configurar AutoSupport, ejecute el siguiente comando:

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Cree una máquina virtual de almacenamiento

Para crear una máquina virtual de almacenamiento (SVM) de infraestructura, complete los siguientes pasos:

1. Ejecute el `vserver create` comando.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume- security-style unix
```

2. Añada el agregado de datos a la lista de agregados de infra-SVM para VSC de NetApp.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. Elimine los protocolos de almacenamiento que no se utilicen de la SVM, con lo que dejará NFS e iSCSI.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. Habilite y ejecute el protocolo NFS en la SVM de infra-SVM.

```
nfs create -vserver Infra-SVM -udp disabled
```

5. Encienda la `SVM vstorage` Parámetro para el plugin VAAI para NFS de NetApp. A continuación,

compruebe que NFS se ha configurado.

```
vserver nfs modify –vserver Infra-SVM –vstorage enabled
vserver nfs show
```

Los comandos están precedidos por `vserver` En la línea de comandos porque las SVM se denominaban servidores anteriormente

Configure NFSv3 en ONTAP

En la siguiente tabla se muestra la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Host ESXi dirección IP de NFS	<<var_esxi_hostA_nfs_ip>>
Dirección IP de NFS del host ESXi B	<<var_esxi_hostB_nfs_ip>>

Para configurar NFS en la SVM, ejecute los siguientes comandos:

1. Cree una regla para cada host ESXi en la política de exportación predeterminada.
2. Asigne una regla para cada host ESXi que se cree. Cada host tiene su propio índice de reglas. El primer host ESXi tiene el índice de regla 1, el segundo host ESXi tiene el índice de regla 2, etc.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid falsevserver export-
policy rule create –vserver Infra-SVM -policyname default –ruleindex 2
–protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>> -rorule sys –rwrule
sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. Asigne la política de exportación al volumen raíz de la SVM de infraestructura.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

VSC de NetApp gestiona automáticamente las políticas de exportación si decide instalarlas después de configurar vSphere. Si no lo instala, debe crear reglas de políticas de exportación cuando se añadan servidores Cisco UCS B-Series adicionales.

Cree el servicio iSCSI en ONTAP

Para crear el servicio iSCSI, complete el paso siguiente:

1. Cree el servicio iSCSI en la SVM. Este comando también inicia el servicio iSCSI y establece el nombre completo de iSCSI (IQN) para la SVM. Comprobar que iSCSI se ha configurado.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Crear reflejo de uso compartido de carga del volumen raíz de la SVM en ONTAP

Para crear un reflejo de uso compartido de carga del volumen raíz de la SVM en ONTAP, complete los pasos siguientes:

1. Cree un volumen para que sea el reflejo de uso compartido de carga del volumen raíz de la SVM de infraestructura en cada nodo.

```
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. Crear una programación de tareas para actualizar las relaciones de mirroring del volumen raíz cada 15 minutos.

```
job schedule interval create -name 15min -minutes 15
```

3. Cree las relaciones de mirroring.

```
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. Inicialice la relación de mirroring y compruebe que se haya creado.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol snapmirror
show
```

Configure el acceso HTTPS en ONTAP

Para configurar el acceso seguro a la controladora de almacenamiento, lleve a cabo los siguientes pasos:

1. Aumente el nivel de privilegio para acceder a los comandos de certificado.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. En general, ya se encuentra en funcionamiento un certificado autofirmado. Verifique el certificado ejecutando el siguiente comando:

```
security certificate show
```

3. Para cada SVM que se muestra, el nombre común del certificado debe coincidir con el nombre de dominio completo (FQDN) de DNS de la SVM. Los cuatro certificados predeterminados deben eliminarse y sustituirse por certificados autofirmados o certificados de una entidad de certificación.

   La práctica recomendada es eliminar certificados caducados antes de crear certificados. Ejecute el `security certificate delete` comando para eliminar certificados caducados. En el siguiente comando, use LA TABULACIÓN automática para seleccionar y eliminar cada certificado predeterminado.

```
security certificate delete [TAB] ...
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM - type server -serial 552429A6
```

4. Para generar e instalar certificados autofirmados, ejecute los siguientes comandos como comandos de una sola vez. Generar un certificado de servidor para la SVM de infraestructura y la SVM de clúster. De nuevo, utilice LA TABULACIÓN automática como ayuda para completar estos comandos.

```
security certificate create [TAB] ...
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 - country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email- addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. Para obtener los valores de los parámetros necesarios en el paso siguiente, ejecute el `security certificate show` comando.
6. Habilite cada certificado que se acaba de crear mediante el `-server-enabled true` y.. `-client-enabled false` parámetros. De nuevo, utilice LA TABULACIÓN automática.

```
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. Configure y habilite el acceso SSL y HTTPS y deshabilite el acceso HTTP.

```
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>>
```

Es normal que algunos de estos comandos devuelvan un mensaje de error indicando que la entrada no existe.

8. Vuelva al nivel de privilegio de administrador y cree la configuración para permitir que la SVM esté disponible en la web.

```
set –privilege admin
vserver services web modify –name spi|ontapi|compat –vserver * -enabled
true
```

Cree un volumen de FlexVol de NetApp en ONTAP

Para crear un volumen FlexVol® de NetApp, introduzca el nombre del volumen, el tamaño y el agregado en el que existe. Crear dos volúmenes de almacenes de datos de VMware y un volumen de arranque del servidor.

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB - state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent- snapshot-space 0
volume create -vserver Infra-SVM -volume infra_datastore_2 -aggregate
aggr1_nodeB -size 500GB - state online -policy default -junction-path
/infra_datastore_2 -space-guarantee none -percent- snapshot-space 0
```

```
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -juntion-path /infra_swap -space
-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Habilite la deduplicación en ONTAP

Para activar la deduplicación en los volúmenes adecuados una vez al día, ejecute los siguientes comandos:

```
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
```

Crear LUN en ONTAP

Para crear dos números de unidad lógica de arranque (LUN), ejecute los siguientes comandos:

```
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
```

Cuando se añade un servidor Cisco UCS C-Series adicional, se debe crear un LUN de arranque adicional.

Creación de LIF iSCSI en ONTAP

En la siguiente tabla se muestra la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Nodo de almacenamiento a iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
Nodo de almacenamiento: Una máscara de red LIF01A de iSCSI	<<var_nodeA_iscsi_lif01a_mask>>
Nodo de almacenamiento a iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
Nodo de almacenamiento a máscara de red LIF01B de iSCSI	<<var_nodeA_iscsi_lif01b_mask>>
Nodo de almacenamiento B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
Máscara de red del nodo de almacenamiento B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_mask>>
ISCSI LIF01B del nodo de almacenamiento	<<var_nodeB_iscsi_lif01b_ip>>
Máscara de red LIF01B de nodo de almacenamiento B.	<<var_nodeB_iscsi_lif01b_mask>>

1. Creación de cuatro LIF iSCSI, dos en cada nodo.

```
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
```

Creación de LIF NFS en ONTAP

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
Nodo de almacenamiento: LIF NFS 01 a IP	<<var_nodeA_nfs_lif_01_a_ip>>
Nodo de almacenamiento A LIF NFS 01 una máscara de red	<<var_nodeA_nfs_lif_01_a_mask>>
Nodo de almacenamiento A LIF NFS 01 b IP	<<var_nodeA_nfs_lif_01_b_ip>>
Nodo de almacenamiento a máscara de red LIF 01 b de LIF	<<var_nodeA_nfs_lif_01_b_mask>>
Nodo de almacenamiento B LIF NFS 02 a IP	<<var_nodeB_nfs_lif_02_a_ip>>
Nodo de almacenamiento B LIF NFS 02 a máscara de red	<<var_nodeB_nfs_lif_02_a_mask>>
Nodo de almacenamiento B LIF NFS 02 b IP	<<var_nodeB_nfs_lif_02_b_ip>>
Nodo de almacenamiento B LIF NFS 02 b máscara de red	<<var_nodeB_nfs_lif_02_b_mask>>

1. Cree una LIF NFS.

```
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
```

Añada el administrador de SVM de infraestructura

En la siguiente tabla, se enumera la información necesaria para completar esta configuración.

Detalles	Valor de detalle
IP de Vsmgmt	<<var_svm_mgmt_ip>>
Máscara de red Vsmgmt	<<var_svm_mgmt_mask>>
Puerta de enlace predeterminada de Vsmgmt	<<var_svm_mgmt_gateway>>

Para añadir la LIF de administrador de SVM de infraestructura y de administración de SVM a la red de gestión, realice los siguientes pasos:

1. Ejecute el siguiente comando:

```
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
```

La IP de administración de SVM aquí debe estar en la misma subred que la IP de administración del clúster de almacenamiento.

2. Cree una ruta predeterminada para permitir que la interfaz de gestión de SVM llegue al mundo exterior.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>> network route show
```

3. Establezca una contraseña para la SVM `vsadmin` usuario y desbloquear el usuario.

```
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
```

Configuración de servidor Cisco UCS

Base de Cisco UCS de FlexPod

Realice la configuración inicial de la interconexión de estructura Cisco UCS 6324 para entornos FlexPod.

En esta sección se proporcionan procedimientos detallados para configurar Cisco UCS para su uso en un entorno FlexPod robo mediante Cisco UCS Manager.

Cisco UCS Fabric Interconnect 6324 A

Cisco UCS utiliza servidores y redes de capa de acceso. Este sistema de servidores de última generación de alto rendimiento proporciona un centro de datos con un alto grado de escalabilidad y agilidad de las cargas de trabajo.

Cisco UCS Manager 4.0(1b) es compatible con la interconexión de estructura 6324 que integra la interconexión de estructura en el chasis Cisco UCS y proporciona una solución integrada para un entorno de puesta en marcha más pequeño. Cisco UCS Mini simplifica la gestión del sistema y ahorra costes en puestas en marcha a baja escala.

Los componentes de hardware y software son compatibles con la estructura unificada de Cisco, que ejecuta varios tipos de tráfico de centros de datos a través de un único adaptador de red convergente.

Configuración inicial del sistema

La primera vez que accede a una interconexión de estructura en un dominio de Cisco UCS, el asistente de configuración le solicita la siguiente información necesaria para configurar el sistema:

- Método de instalación (GUI o CLI)
- Modo de configuración (restauración a partir de una copia de seguridad completa del sistema o la configuración inicial)
- Tipo de configuración del sistema (configuración en clúster o independiente)
- Nombre del sistema

- Contraseña de administrador
- La dirección IPv4 del puerto de gestión y la máscara de subred, o el prefijo y la dirección IPv6
- Dirección IPv4 o IPv6 de la pasarela predeterminada
- Dirección IPv4 o IPv6 del servidor DNS
- Nombre de dominio predeterminado

La siguiente tabla enumera la información necesaria para completar la configuración inicial de Cisco UCS en Fabric Interconnect A

Detalles	**Detalle/valor**
Nombre del sistema	<<var_ucs_clustername>>
Contraseña de administrador	<<var_password>>
Dirección IP de administración: Interconexión de estructura A	<<var_ucsa_mgmt_ip>>
Máscara de red de gestión: Interconexión de estructura A	<<var_ucsa_mgmt_mask>>
Puerta de enlace predeterminada: Interconexión de estructura A	<<var_ucsa_mgmt_gateway>>
Dirección IP del clúster	<<var_ucs_cluster_ip>>
Dirección IP del servidor DNS	<<var_nameserver_ip>>
Nombre de dominio	<<var_domain_name>>

Para configurar Cisco UCS para su uso en un entorno FlexPod, complete los pasos siguientes:

1. Conéctese al puerto de la consola de la primera interconexión de estructura a Cisco UCS 6324

```
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. Revise la configuración que se muestra en la consola. Si son correctos, responda `yes` para aplicar y guardar la configuración.
3. Espere a que se muestre la solicitud de inicio de sesión para comprobar que la configuración se ha guardado.

La siguiente tabla enumera la información necesaria para completar la configuración inicial de Cisco UCS en Fabric Interconnect B.

Detalles	**Detalle/valor**
Nombre del sistema	<<var_ucs_clustername>>
Contraseña de administrador	<<var_password>>
Dirección IP de administración B	<<var_ucsb_mgmt_ip>>
Netmask-FI B de gestión	<<var_ucsb_mgmt_mask>>
Gateway-FI B predeterminada	<<var_ucsb_mgmt_gateway>>
Dirección IP del clúster	<<var_ucs_cluster_ip>>
Dirección IP del servidor DNS	<<var_nameserver_ip>>
Nombre de dominio	<<var_domain_name>>

1. Conéctese al puerto de la consola del segundo Cisco UCS 6324 Fabric Interconnect B.

```
 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. Espere a que la solicitud de inicio de sesión confirme que la configuración se ha guardado.

Inicie sesión en Cisco UCS Manager

Para iniciar sesión en el entorno de Cisco Unified Computing System (UCS), complete los siguientes pasos:

1. Abra un explorador web y desplácese hasta la dirección del clúster de Cisco UCS Fabric Interconnect.

   Puede que tenga que esperar al menos 5 minutos tras configurar la segunda interconexión de estructura para que aparezca Cisco UCS Manager.

2. Haga clic en el enlace Iniciar UCS Manager para iniciar Cisco UCS Manager.
3. Acepte los certificados de seguridad necesarios.
4. Cuando se lo pida, introduzca admin como nombre de usuario e introduzca la contraseña de administrador.
5. Haga clic en Login para iniciar sesión en Cisco UCS Manager.

Software Cisco UCS Manager, versión 4.0(1b)

En este documento se asume el uso del software Cisco UCS Manager, versión 4.0(1b). Para actualizar el software Cisco UCS Manager y el software Cisco UCS 6324 Fabric Interconnect, consulte "Guías de instalación y actualización de Cisco UCS Manager."

Configure Cisco UCS Call Home

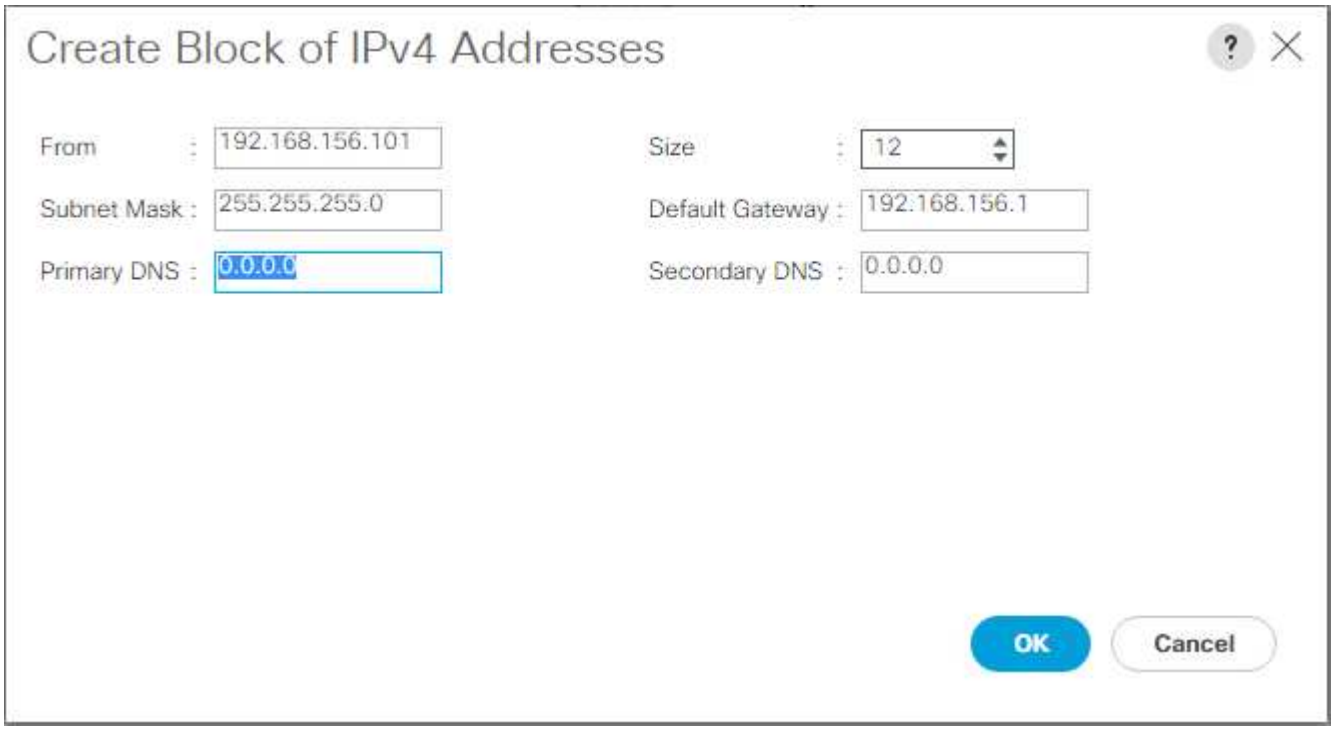
Cisco recomienda encarecidamente que configure Call Home en Cisco UCS Manager. La configuración de Call Home acelera la resolución de los casos de soporte. Para configurar Call Home, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, haga clic en Admin a la izquierda.
2. Seleccione All > Communication Management > Call Home.
3. Cambie el estado a Activado.
4. Rellene todos los campos según sus preferencias de administración y haga clic en Guardar cambios y en Aceptar para completar la configuración de Call Home.

Agregue bloque de direcciones IP para el acceso al teclado, vídeo y ratón

Para crear un bloque de direcciones IP para el acceso de teclado, vídeo y ratón en banda en el entorno Cisco UCS, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, haga clic en LAN a la izquierda.
2. Expanda Pools > raíz > grupos IP.
3. Haga clic con el botón derecho del ratón en IP Pool ext-mgmt y seleccione Crear bloque de direcciones IPv4.
4. Introduzca la dirección IP de inicio del bloque, el número de direcciones IP necesarias y la información de máscara de subred y puerta de enlace.



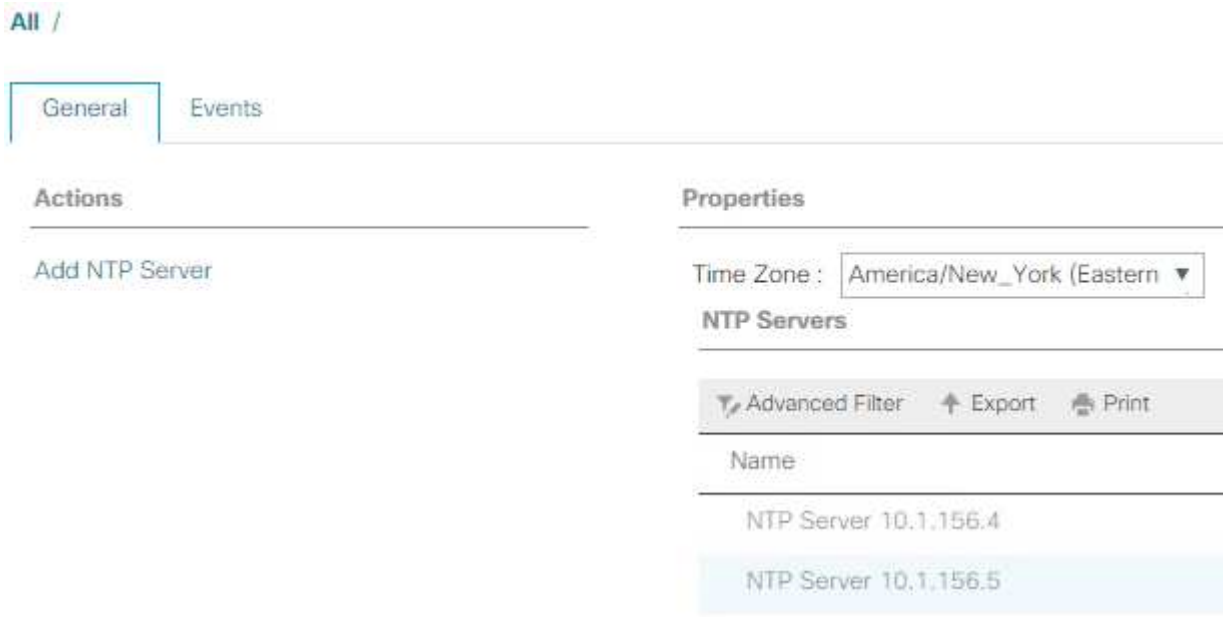
5. Haga clic en OK para crear el bloque.
6. Haga clic en Aceptar en el mensaje de confirmación.

Sincronice Cisco UCS con NTP

Para sincronizar el entorno Cisco UCS con los servidores NTP en los switches Nexus, realice los siguientes pasos:

1. En Cisco UCS Manager, haga clic en Admin a la izquierda.
2. Expanda todo > Administración de zonas horarias.
3. Seleccione Time Zone.
4. En el panel Propiedades, seleccione la zona horaria adecuada en el menú Zona horaria.
5. Haga clic en Save Changes y haga clic en OK.
6. Haga clic en Add NTP Server.
7. Introduzca `<switch-a-ntp-ip> or <Nexus-A-mgmt-IP>` Y haga clic en Aceptar. Haga clic en Aceptar.

8. Haga clic en Add NTP Server.
9. Introduzca `<switch-b-ntp-ip> or <Nexus-B-mgmt-IP>` Y haga clic en Aceptar. Haga clic en Aceptar en la confirmación.



Edite la política de detección del chasis

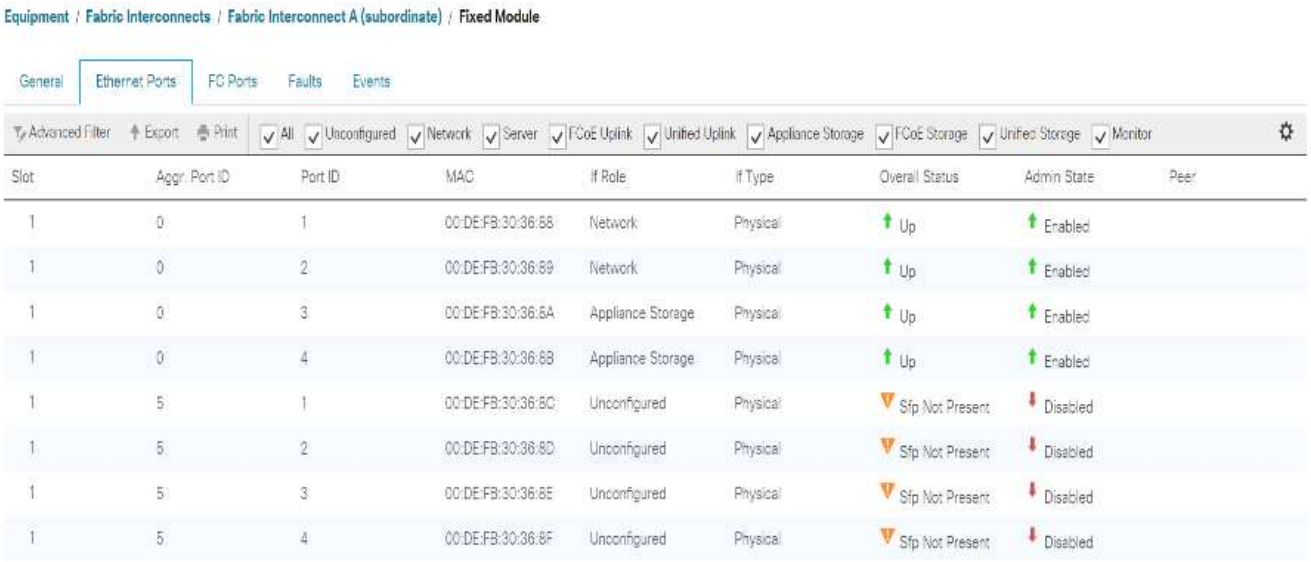
La configuración de la política de detección simplifica la adición de chasis Cisco UCS B-Series y de extensores de estructura adicionales para ampliar la conectividad de Cisco UCS C-Series. Para modificar la política de detección del chasis, complete los siguientes pasos:

1. En Cisco UCS Manager, haga clic en Equipment a la izquierda y seleccione Equipment en la segunda lista.
2. En el panel derecho, seleccione la ficha Directivas.
3. En Directivas globales, establezca la directiva de descubrimiento chasis/FEX para que coincida con el número mínimo de puertos de enlace ascendente conectados entre el chasis o los extensores de estructura (FEXes) y las interconexiones de estructura.
4. Establezca la preferencia de agrupación de enlaces en Canal de puertos. Si el entorno que se está configurando contiene una gran cantidad de tráfico de multidifusión, establezca el valor hash de hardware de multidifusión en Activado.
5. Haga clic en Save Changes.
6. Haga clic en Aceptar.

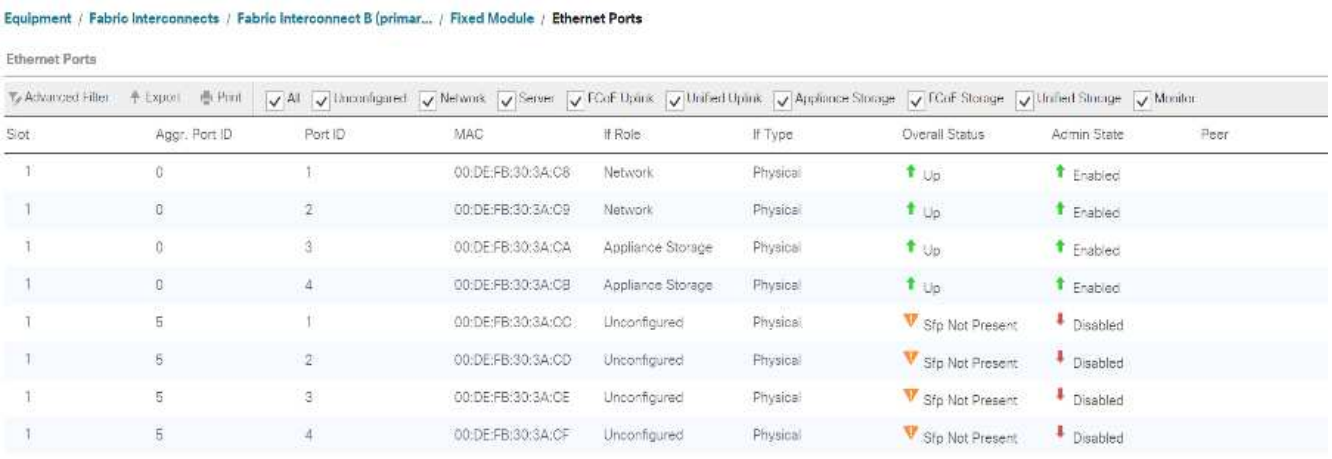
Habilite puertos de servidor, enlace ascendente y almacenamiento

Para habilitar los puertos de servidor y enlace ascendente, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, en el panel de navegación, seleccione la pestaña equipos.
2. Expanda Equipo > interconexiones de estructura > interconexión de estructura A > módulo fijo.
3. Expanda puertos Ethernet.
4. Seleccione los puertos 1 y 2 conectados a los switches Cisco Nexus 31108, haga clic con el botón derecho del ratón y seleccione Configurar como puerto de enlace ascendente.
5. Haga clic en Sí para confirmar los puertos de enlace ascendente y haga clic en Aceptar.
6. Seleccione los puertos 3 y 4 que están conectados a las controladoras de almacenamiento de NetApp, haga clic con el botón derecho y seleccione Configurar como puerto de dispositivo.
7. Haga clic en Yes para confirmar los puertos del dispositivo.
8. En la ventana Configurar como puerto de dispositivo, haga clic en Aceptar.
9. Haga clic en OK para confirmar.
10. En el panel izquierdo, seleccione módulo fijo en interconexión de estructura A.
11. En la pestaña puertos Ethernet, confirme que los puertos se han configurado correctamente en la columna If Role. Si se han configurado servidores C-Series de puertos en el puerto de escalabilidad, haga clic en él para verificar la conectividad de los puertos.



12. Expanda Equipo > interconexiones de estructura > interconexión de estructura B > módulo fijo.
13. Expanda puertos Ethernet.
14. Seleccione los puertos Ethernet 1 y 2 conectados a los switches Cisco Nexus 31108, haga clic con el botón derecho del ratón y seleccione Configurar como puerto de enlace ascendente.
15. Haga clic en Sí para confirmar los puertos de enlace ascendente y haga clic en Aceptar.
16. Seleccione los puertos 3 y 4 que están conectados a las controladoras de almacenamiento de NetApp, haga clic con el botón derecho y seleccione Configurar como puerto de dispositivo.
17. Haga clic en Yes para confirmar los puertos del dispositivo.
18. En la ventana Configurar como puerto de dispositivo, haga clic en Aceptar.
19. Haga clic en OK para confirmar.
20. En el panel izquierdo, seleccione módulo fijo en interconexión de estructura B.
21. En la pestaña puertos Ethernet, confirme que los puertos se han configurado correctamente en la columna If Role. Si se han configurado servidores C-Series de puertos en el puerto de escalabilidad, haga clic en él para verificar la conectividad de los puertos.



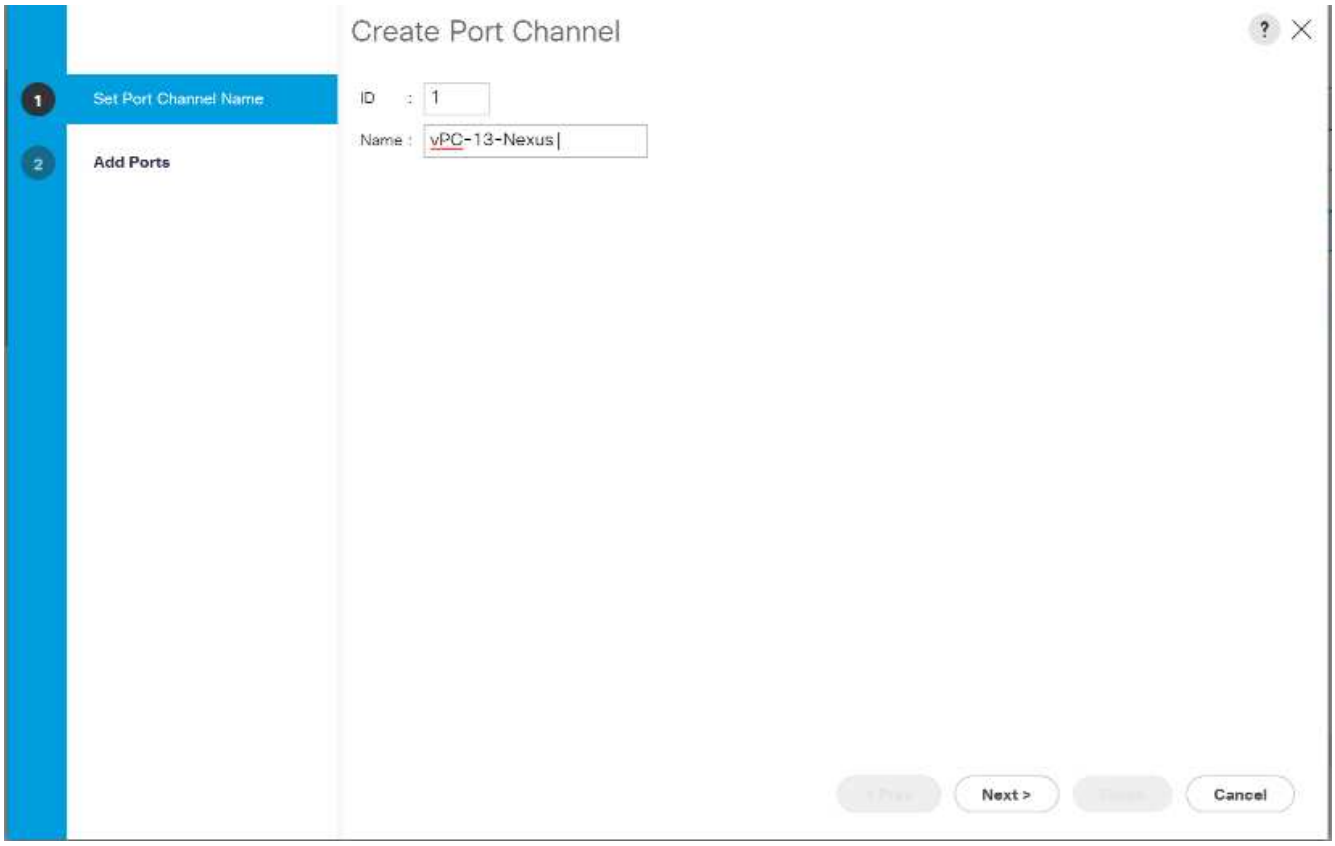
Cree canales de puertos de enlace ascendente con switches Cisco Nexus 31108

Para configurar los canales de puerto necesarios en el entorno Cisco UCS, complete los siguientes pasos:

1. En Cisco UCS Manager, seleccione la pestaña LAN en el panel de navegación.

> En este procedimiento se crean dos canales de puerto: Uno desde la estructura a hasta los switches Cisco Nexus 31108 y uno desde la estructura B a los dos switches Cisco Nexus 31108. Si está utilizando interruptores estándar, modifique este procedimiento en consecuencia. Si utiliza 1 switch Gigabit Ethernet (1 GbE) y SFP GLC-T en las interconexiones de estructura, las velocidades de interfaz de los puertos Ethernet 1/1 y 1/2 en las interconexiones de estructura deben configurarse en 1 Gbps.

2. En LAN > LAN Cloud, expanda el árbol de Fabric A.
3. Haga clic con el botón derecho del ratón en Canales de puerto.
4. Seleccione Crear canal de puerto.
5. Introduzca 13 como el ID único del canal del puerto.
6. Introduzca VPC-13-Nexus como nombre del canal de puerto.
7. Haga clic en Siguiente.



8. Seleccione los siguientes puertos para añadir al canal de puerto:
   a. ID de ranura 1 y puerto 1
   b. ID de ranura 1 y puerto 2
9. Haga clic en >> para agregar los puertos al canal de puerto.
10. Haga clic en Finish para crear el canal del puerto. Haga clic en Aceptar.

11. En Canales de puerto, seleccione el canal de puerto recién creado.

    El canal del puerto debe tener un estado general de subida.

12. En el panel de navegación, en LAN > LAN Cloud, expanda el árbol de la estructura B.
13. Haga clic con el botón derecho del ratón en Canales de puerto.
14. Seleccione Crear canal de puerto.
15. Introduzca 14 como el ID único del canal del puerto.
16. Introduzca VPC-14-Nexus como nombre del canal de puerto. Haga clic en Siguiente.
17. Seleccione los siguientes puertos para añadir al canal de puerto:
    a. ID de ranura 1 y puerto 1
    b. ID de ranura 1 y puerto 2
18. Haga clic en >> para agregar los puertos al canal de puerto.
19. Haga clic en Finish para crear el canal del puerto. Haga clic en Aceptar.
20. En Canales de puerto, seleccione el puerto-canal recién creado.
21. El canal del puerto debe tener un estado general de subida.

Crear una organización (opcional)

Las organizaciones se utilizan para organizar los recursos y restringir el acceso a varios grupos dentro de la organización DE TI, con lo que permiten el multi-tenancy de los recursos informáticos.

> Aunque este documento no asume el uso de las organizaciones, este procedimiento proporciona instrucciones para crear una.

Para configurar una organización en el entorno Cisco UCS, complete los pasos siguientes:

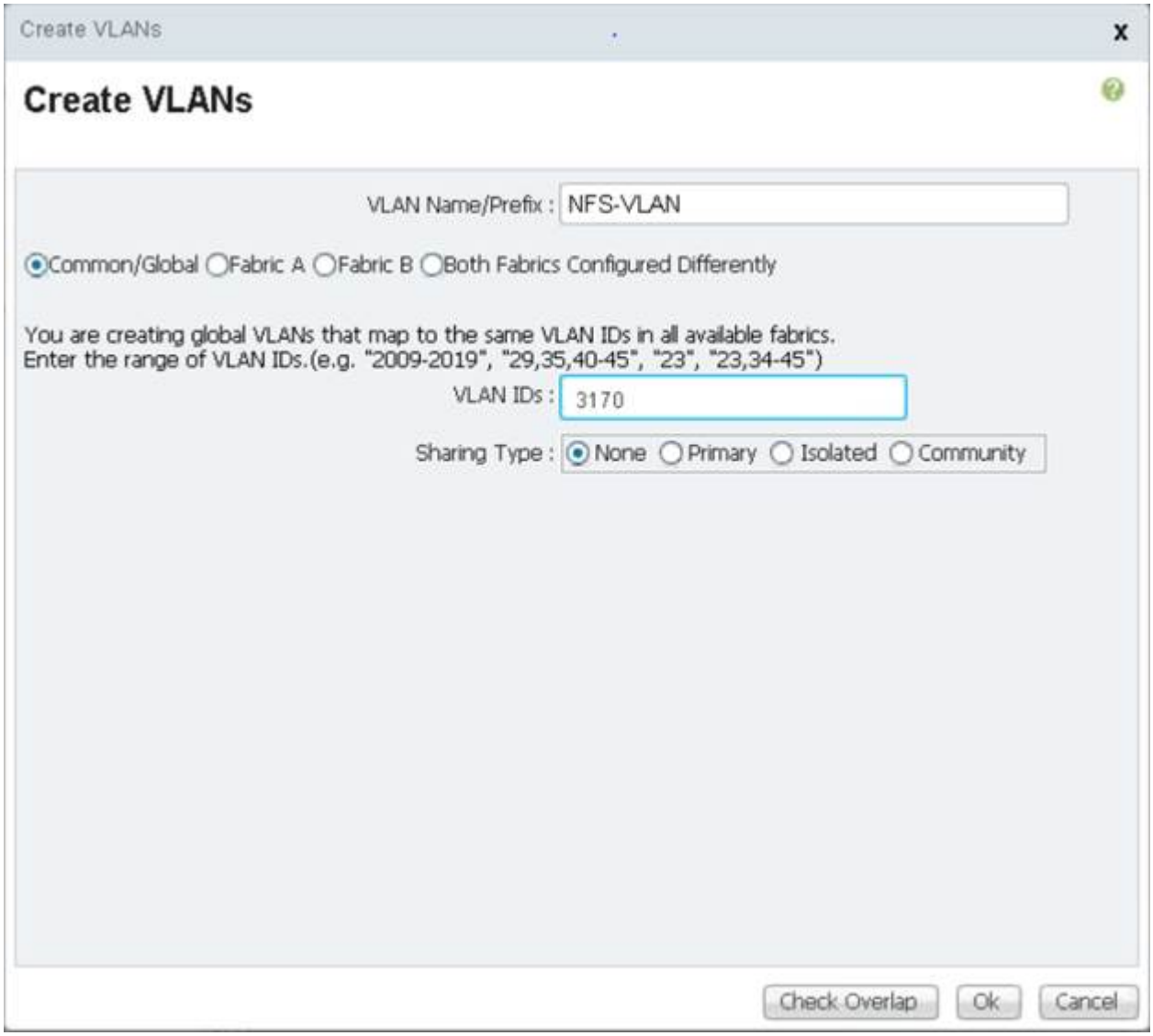
1. En Cisco UCS Manager, en el menú Nuevo de la barra de herramientas, en la parte superior de la ventana, seleccione Crear organización.
2. Escriba un nombre para la organización.
3. Opcional: Introduzca una descripción para la organización. Haga clic en Aceptar.
4. Haga clic en Aceptar en el mensaje de confirmación.

Configure los puertos del dispositivo de almacenamiento y las VLAN de almacenamiento

Para configurar los puertos del dispositivo de almacenamiento y las VLAN de almacenamiento, siga estos pasos:

1. En Cisco UCS Manager, seleccione la pestaña LAN.
2. Amplíe el cloud de dispositivos.
3. Haga clic con el botón derecho en Appliances Cloud.
4. Seleccione Create VLAN.
5. Introduzca NFS-VLAN como el nombre de la VLAN de Infrastructure NFS.
6. Deje común/Global seleccionado.
7. Introduzca `<<var_nfs_vlan_id>>` Para el ID de VLAN.

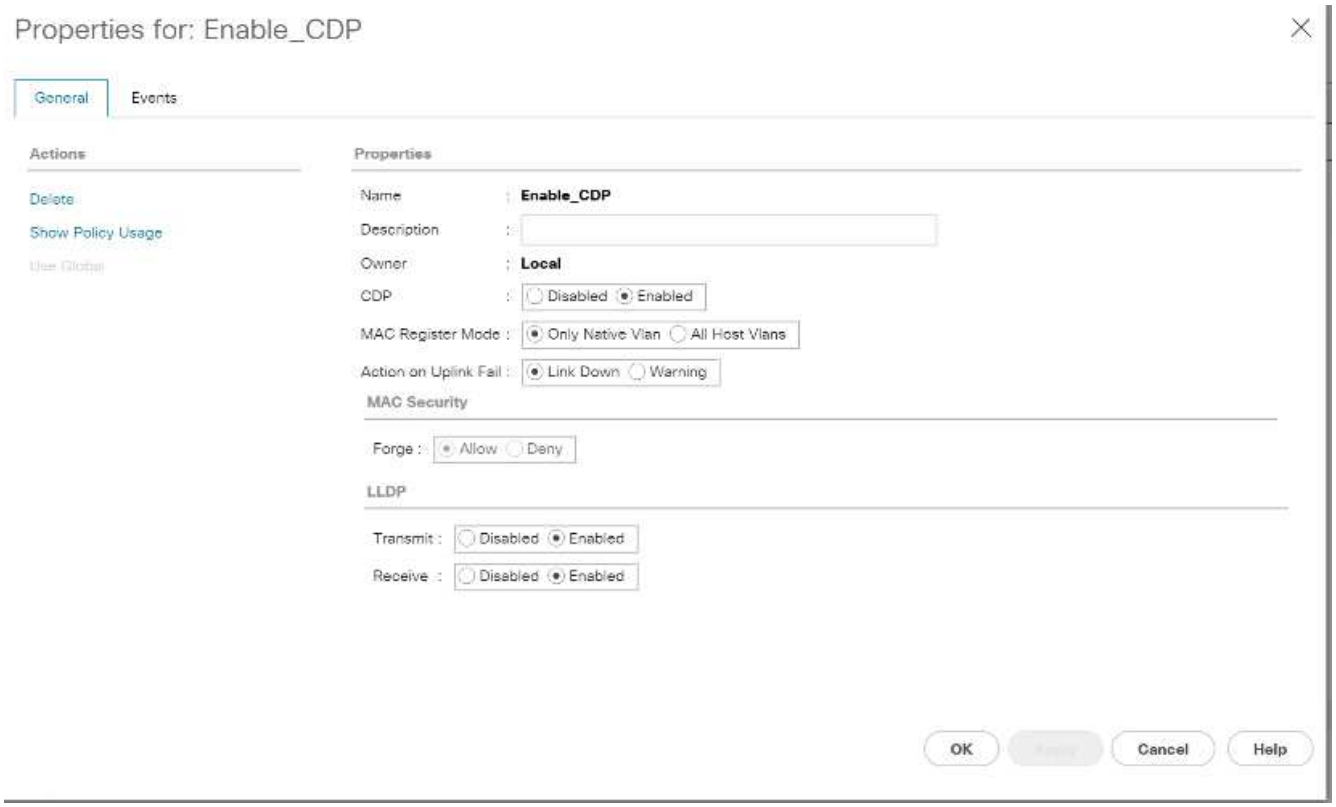
8. Tipo de uso compartido de baja establecido en Ninguno.



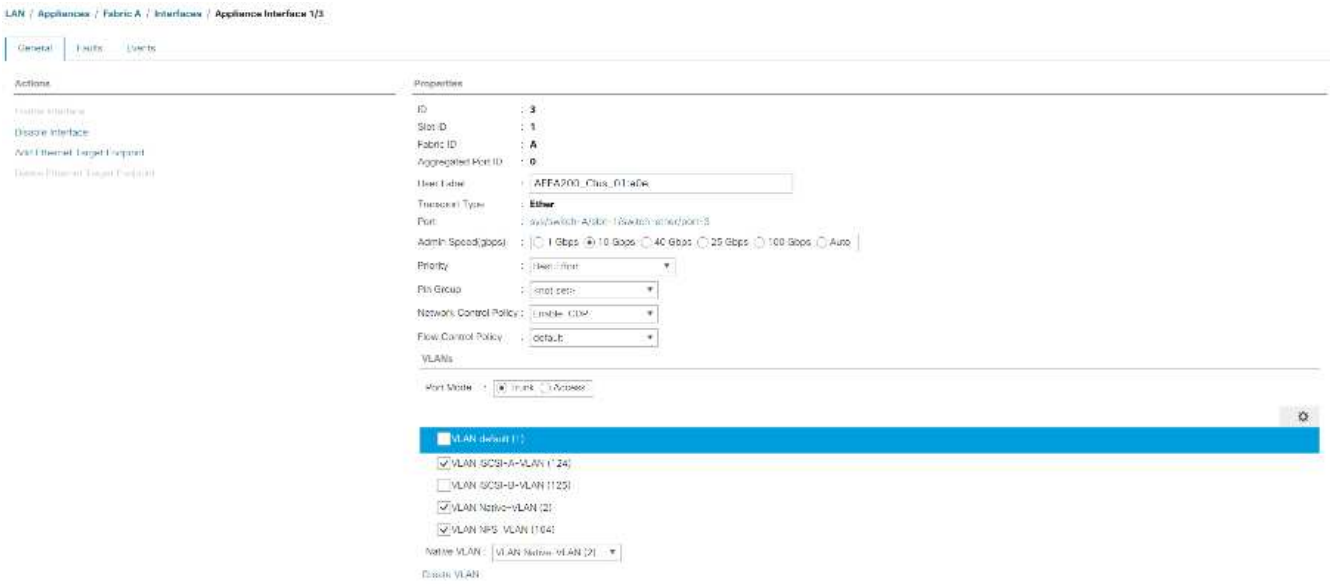
9. Haga clic en OK y, a continuación, vuelva a hacer clic en OK para crear la VLAN.
10. Haga clic con el botón derecho en Appliances Cloud.
11. Seleccione Create VLAN.
12. Introduzca iSCSI-A-VLAN como nombre para la infraestructura iSCSI Fabric A VLAN.
13. Deje común/Global seleccionado.
14. Introduzca `<<var_iscsi-a_vlan_id>>` Para el ID de VLAN.
15. Haga clic en OK y, a continuación, vuelva a hacer clic en OK para crear la VLAN.
16. Haga clic con el botón derecho en Appliances Cloud.
17. Seleccione Create VLAN.
18. Introduzca iSCSI-B-VLAN como nombre para la VLAN de infraestructura iSCSI Fabric B.
19. Deje común/Global seleccionado.
20. Introduzca `<<var_iscsi-b_vlan_id>>` Para el ID de VLAN.
21. Haga clic en OK y, a continuación, vuelva a hacer clic en OK para crear la VLAN.

22. Haga clic con el botón derecho en Appliances Cloud.
23. Seleccione Create VLAN.
24. Introduzca Native-VLAN como nombre de la VLAN nativa.
25. Deje común/Global seleccionado.
26. Introduzca `<<var_native_vlan_id>>` Para el ID de VLAN.
27. Haga clic en OK y, a continuación, vuelva a hacer clic en OK para crear la VLAN.

28. En el panel de navegación, en LAN > Directivas, expanda dispositivos y haga clic con el botón derecho del ratón en Directivas de control de red.
29. Seleccione Crear Directiva de control de red.
30. Asigne un nombre a la política `Enable_CDP_LLPD` Y seleccione habilitado junto a CDP.
31. Habilite las funciones de transmisión y recepción para LLDP.



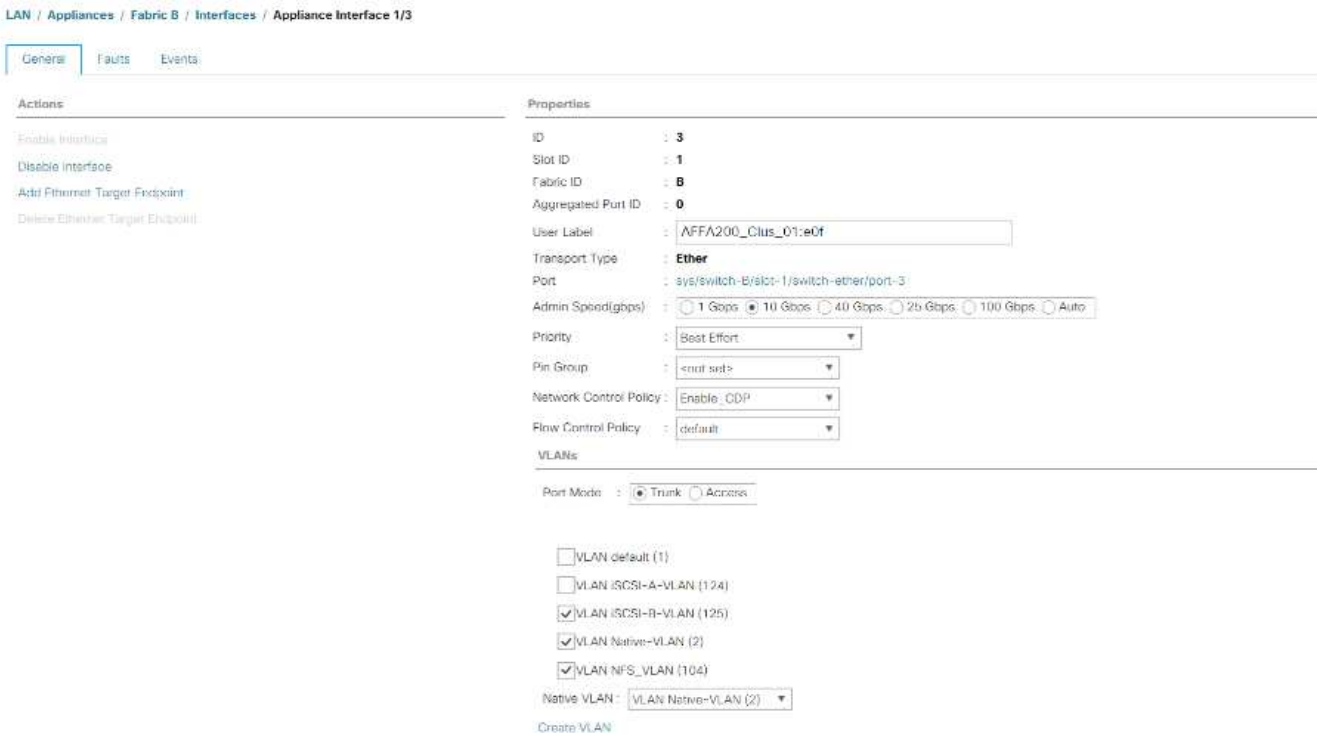
32. Haga clic en Aceptar y, a continuación, vuelva a hacer clic en Aceptar para crear la directiva.
33. En el panel de navegación, en LAN > Appliances Cloud, expanda el árbol de Fabric A.
34. Amplíe las interfaces.
35. Seleccione interfaz de dispositivo 1/3.
36. En el campo etiqueta de usuario, incluya información que indique el puerto de la controladora de almacenamiento; por ejemplo `<storage_controller_01_name>:e0e`. Haga clic en Save Changes y OK.
37. Seleccione Enable_CDP Network Control Policy y seleccione Save Changes (Guardar cambios) y OK (Aceptar).
38. En VLAN, seleccione iSCSI-A-VLAN, NFS VLAN y la VLAN nativa. Establezca la VLAN nativa como VLAN nativa. Borre la selección de VLAN predeterminada.
39. Haga clic en Save Changes y OK.



40. Seleccione Appliance Interface 1/4 en Fabric A.
41. En el campo etiqueta de usuario, incluya información que indique el puerto de la controladora de almacenamiento; por ejemplo `<storage_controller_02_name>:e0e`. Haga clic en Save Changes y OK.
42. Seleccione Enable_CDP Network Control Policy y seleccione Save Changes (Guardar cambios) y OK (Aceptar).
43. En VLAN, seleccione iSCSI-A-VLAN, NFS VLAN y la VLAN nativa.
44. Establezca la VLAN nativa como VLAN nativa.
45. Borre la selección de VLAN predeterminada.
46. Haga clic en Save Changes y OK.
47. En el panel de navegación, en LAN > Appliances Cloud, expanda el árbol de Fabric B.
48. Amplíe las interfaces.
49. Seleccione interfaz de dispositivo 1/3.
50. En el campo etiqueta de usuario, incluya información que indique el puerto de la controladora de

almacenamiento; por ejemplo `<storage_controller_01_name>:e0f`. Haga clic en Save Changes y OK.

51. Seleccione Enable_CDP Network Control Policy y seleccione Save Changes (Guardar cambios) y OK (Aceptar).
52. En VLAN, seleccione iSCSI-B-VLAN, NFS VLAN y la VLAN nativa. Establezca la VLAN nativa como VLAN nativa. Anule la selección de la VLAN predeterminada.



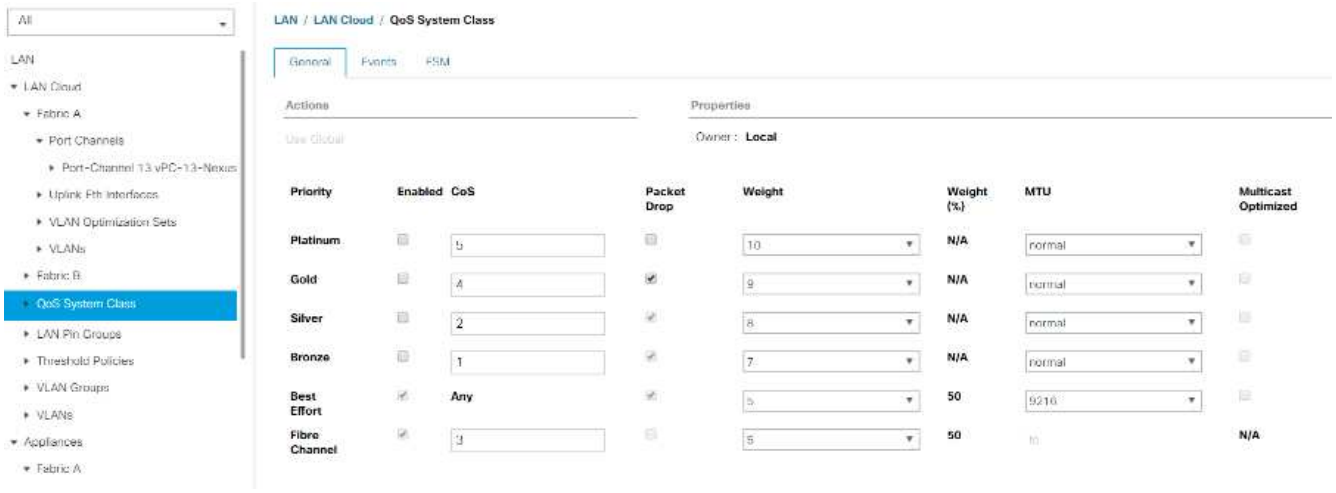
53. Haga clic en Save Changes y OK.
54. Seleccione interfaz de dispositivo 1/4 en Fabric B.
55. En el campo etiqueta de usuario, incluya información que indique el puerto de la controladora de almacenamiento; por ejemplo `<storage_controller_02_name>:e0f`. Haga clic en Save Changes y OK.
56. Seleccione Enable_CDP Network Control Policy y seleccione Save Changes (Guardar cambios) y OK (Aceptar).
57. En VLAN, seleccione iSCSI-B-VLAN, NFS VLAN y la VLAN nativa. Establezca la VLAN nativa como VLAN nativa. Anule la selección de la VLAN predeterminada.
58. Haga clic en Save Changes y OK.

Establezca las tramas gigantes en la estructura de Cisco UCS

Para configurar tramas gigantes y permitir la calidad de servicio en la estructura Cisco UCS, realice los siguientes pasos:

1. En Cisco UCS Manager, en el panel de navegación, haga clic en la pestaña LAN.
2. Seleccione LAN > LAN Cloud > QoS System Class.
3. En el panel derecho, haga clic en la ficha General .

4. En la fila esfuerzo, introduzca 9216 en el cuadro situado bajo la columna MTU.



5. Haga clic en Save Changes.
6. Haga clic en Aceptar.

Reconozca el chasis de Cisco UCS

Para reconocer todos los chasis Cisco UCS, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, seleccione la pestaña Equipo y, a continuación, expanda la pestaña equipos de la derecha.
2. Expanda Equipo > chasis.
3. En acciones para el chasis 1, seleccione reconocer chasis.
4. Haga clic en Aceptar y, a continuación, en Aceptar para completar el reconocimiento del chasis.
5. Haga clic en Cerrar para cerrar la ventana Propiedades.

Cargar imágenes de firmware de Cisco UCS 4.0(1b)

Para actualizar el software Cisco UCS Manager y el software Cisco UCS Fabric Interconnect a la versión 4.0(1b), consulte "Guías de instalación y actualización de Cisco UCS Manager".

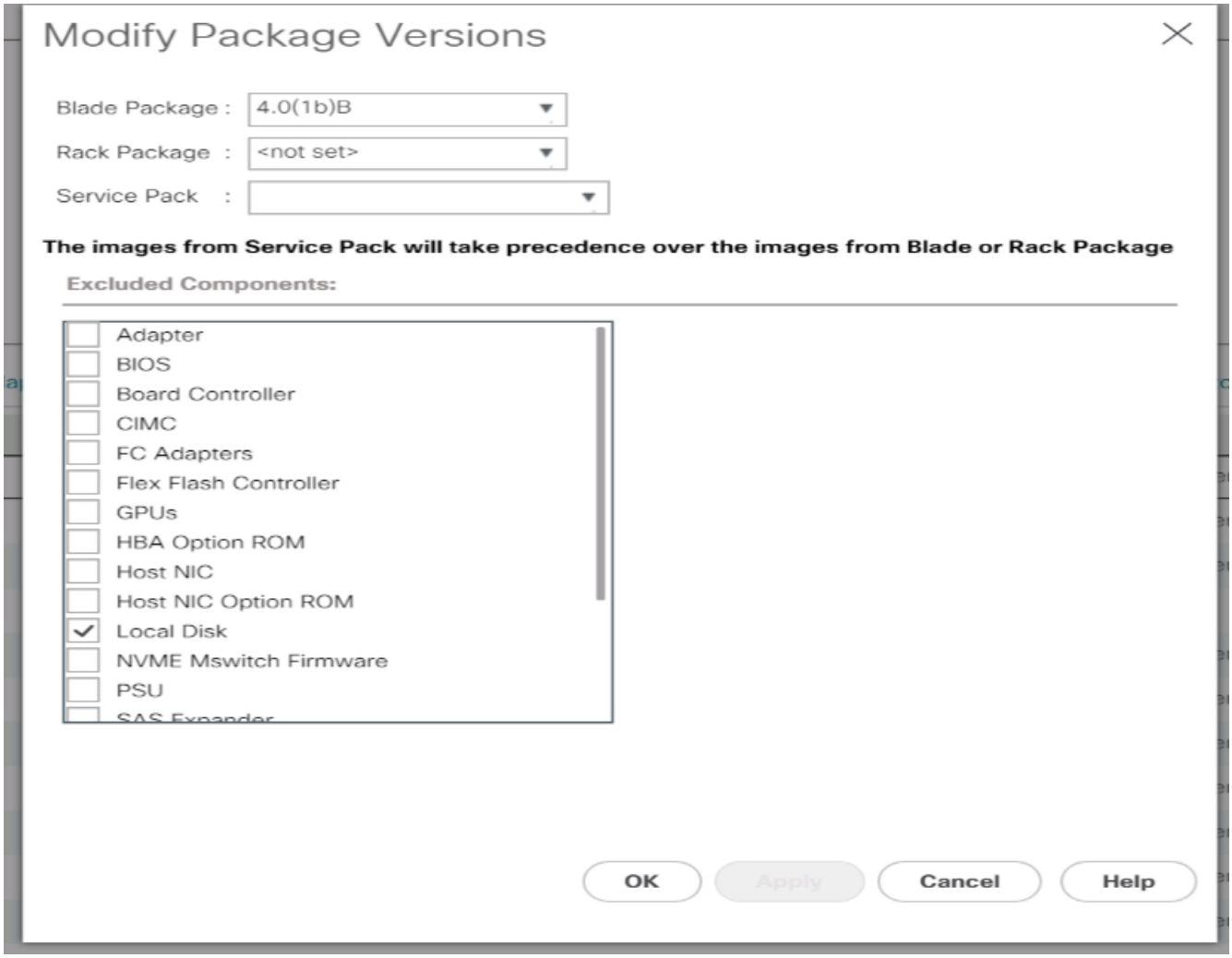
Cree un paquete de firmware del host

Las directivas de administración de firmware permiten al administrador seleccionar los paquetes correspondientes para una configuración de servidor determinada. Estas políticas suelen incluir paquetes para adaptadores, BIOS, controlador de placa, adaptadores de FC, ROM de opción del adaptador de bus de host (HBA) y propiedades de la controladora de almacenamiento.

Para crear una política de gestión de firmware para una configuración de servidor determinada en el entorno de Cisco UCS, lleve a cabo los pasos siguientes:

1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Policies > root.
3. Expanda Paquetes de firmware del host.
4. Seleccione predeterminado.

5. En el panel acciones, seleccione Modificar versiones de paquete.
6. Seleccione la versión 4.0(1b) para los dos paquetes blade.



7. Haga clic en OK y, a continuación, en OK de nuevo para modificar el paquete de firmware del host.

Crear pools de direcciones MAC

Para configurar los pools de direcciones MAC necesarios para el entorno Cisco UCS, realice los siguientes pasos:

1. En Cisco UCS Manager, haga clic en LAN a la izquierda.
2. Seleccione Pools > raíz.

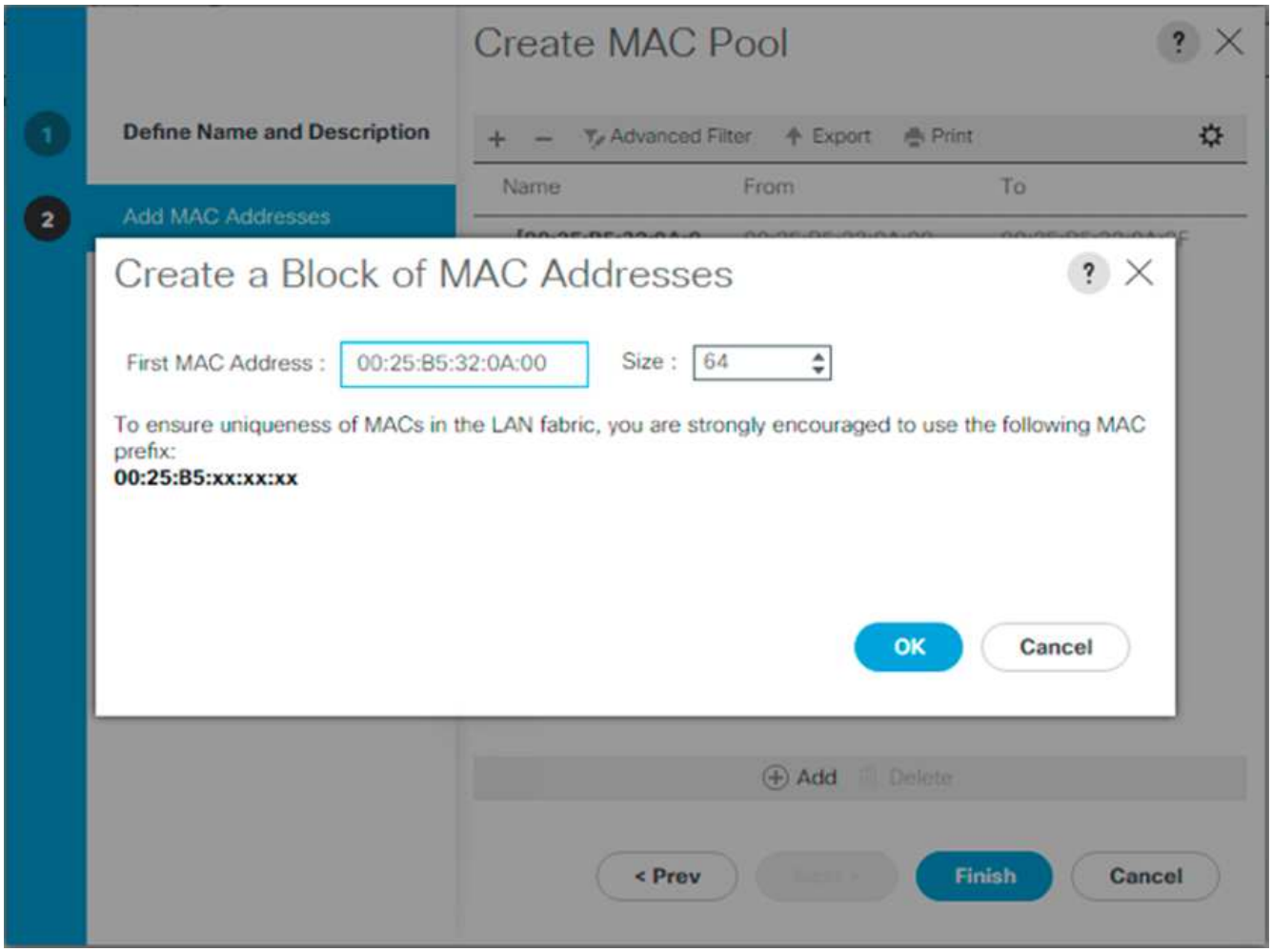
   En este procedimiento, se crean dos grupos de direcciones MAC, uno para cada estructura de conmutación.

3. Haga clic con el botón derecho del ratón en grupos MAC de la organización raíz.
4. Seleccione Crear pool MAC para crear el pool de direcciones MAC.
5. Introduzca MAC-Pool-A como nombre del pool MAC.
6. Opcional: Introduzca una descripción para el grupo MAC.
7. Seleccione secuencial como opción para Orden de asignación. Haga clic en Siguiente.

8. Haga clic en Añadir.
9. Especifique una dirección MAC inicial.

> Para la solución FlexPod, se recomienda colocar 0A en el octeto siguiente al último de la dirección MAC inicial para identificar todas las direcciones MAC como direcciones de la estructura A. En nuestro ejemplo, hemos seguido el ejemplo de incrustar también la información de número de dominio de Cisco UCS, que nos proporciona 00:25:B5:32:0A:00 como primera dirección MAC.

10. Especifique un tamaño para el grupo de direcciones MAC que sea suficiente para admitir los recursos de servidor o blade disponibles. Haga clic en Aceptar.



11. Haga clic en Finalizar.
12. En el mensaje de confirmación, haga clic en Aceptar.
13. Haga clic con el botón derecho del ratón en grupos MAC de la organización raíz.
14. Seleccione Crear pool MAC para crear el pool de direcciones MAC.
15. Introduzca MAC-Pool-B como nombre del pool MAC.
16. Opcional: Introduzca una descripción para el grupo MAC.
17. Seleccione secuencial como opción para Orden de asignación. Haga clic en Siguiente.
18. Haga clic en Añadir.

19. Especifique una dirección MAC inicial.

> Para la solución FlexPod, se recomienda colocar 0B en el siguiente al último octeto de la dirección MAC inicial para identificar todas las direcciones MAC de este grupo como direcciones de la estructura B. Una vez más, hemos seguido adelante en nuestro ejemplo de incrustar también la información de número de dominio de Cisco UCS, que nos proporciona 00:25:B5:32:0B:00 como nuestra primera dirección MAC.

20. Especifique un tamaño para el grupo de direcciones MAC que sea suficiente para admitir los recursos de servidor o blade disponibles. Haga clic en Aceptar.
21. Haga clic en Finalizar.
22. En el mensaje de confirmación, haga clic en Aceptar.

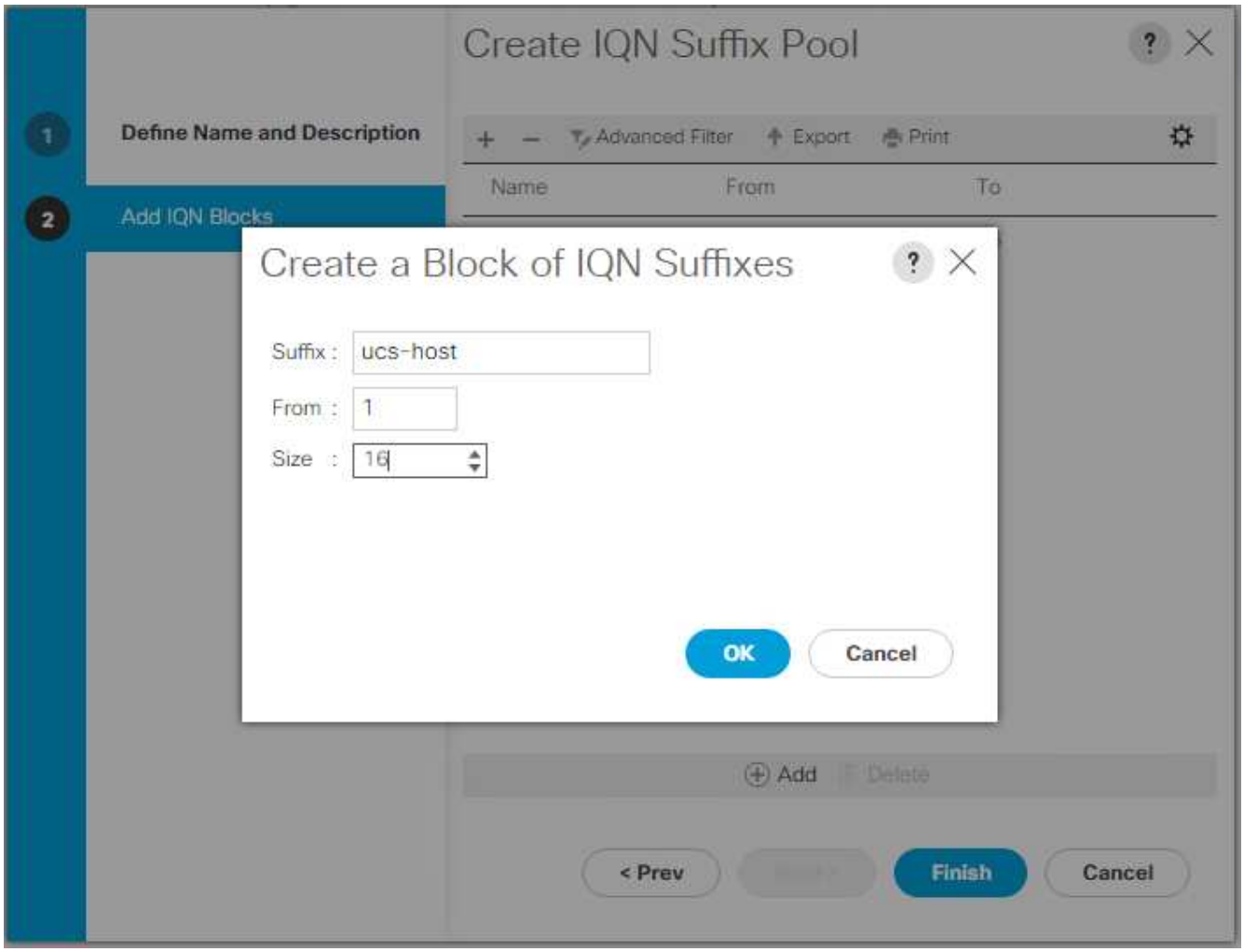
Cree un pool IQN de iSCSI

Para configurar los pools IQN necesarios para el entorno Cisco UCS, complete los siguientes pasos:

1. En Cisco UCS Manager, haga clic en SAN a la izquierda.
2. Seleccione Pools > raíz.
3. Haga clic con el botón derecho en IQN Pools.
4. Seleccione Create IQN Suffix Pool para crear el pool IQN.
5. Introduzca IQN-Pool para el nombre del pool IQN.
6. Opcional: Introduzca una descripción para el pool de IQN.
7. Introduzca `iqn.1992-08.com.cisco` como prefijo.
8. Seleccione secuencial para orden de asignación. Haga clic en Siguiente.
9. Haga clic en Añadir.
10. Introduzca `ucs-host` como sufijo.

> Si se utilizan varios dominios de Cisco UCS, es posible que deba utilizar un sufijo IQN más específico.

11. Introduzca 1 en el campo de.
12. Especifique el tamaño del bloque de IQN suficiente para admitir los recursos del servidor disponibles. Haga clic en Aceptar.



13. Haga clic en Finalizar.

Cree pools de direcciones IP del iniciador de iSCSI

Para configurar el arranque iSCSI de los pools IP necesarios para el entorno Cisco UCS, realice los pasos siguientes:

1. En Cisco UCS Manager, haga clic en LAN a la izquierda.
2. Seleccione Pools > raíz.
3. Haga clic con el botón derecho en IP Pools.
4. Seleccione Crear Pool IP.
5. Introduzca iSCSI-IP-Pool-A como nombre del pool IP.
6. Opcional: Introduzca una descripción para el grupo IP.
7. Seleccione secuencial para la orden de asignación. Haga clic en Siguiente.
8. Haga clic en Agregar para agregar un bloque de dirección IP.
9. En el campo from, introduzca el principio del rango que se asignará como direcciones IP de iSCSI.
10. Establezca el tamaño en direcciones suficientes para acomodar los servidores. Haga clic en Aceptar.
11. Haga clic en Siguiente.
12. Haga clic en Finalizar.

13. Haga clic con el botón derecho en IP Pools.
14. Seleccione Crear Pool IP.
15. Introduzca iSCSI-IP-Pool-B como nombre del pool IP.
16. Opcional: Introduzca una descripción para el grupo IP.
17. Seleccione secuencial para la orden de asignación. Haga clic en Siguiente.
18. Haga clic en Agregar para agregar un bloque de dirección IP.
19. En el campo from, introduzca el principio del rango que se asignará como direcciones IP de iSCSI.
20. Establezca el tamaño en direcciones suficientes para acomodar los servidores. Haga clic en Aceptar.
21. Haga clic en Siguiente.
22. Haga clic en Finalizar.

Cree un pool de sufijos UUID

Para configurar el pool de sufijos de identificador único universal (UUID) necesario para el entorno de Cisco UCS, complete los siguientes pasos:

1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Pools > raíz.
3. Haga clic con el botón derecho en grupos de sufijo de UUID.
4. Seleccione Crear pool de sufijo de UUID.
5. Introduzca UUID-Pool como el nombre del pool de sufijos de UUID.
6. Opcional: Introduzca una descripción para el pool de sufijos UUID.
7. Mantenga el prefijo en la opción derivada.
8. Seleccione secuencial para la orden de asignación.
9. Haga clic en Siguiente.
10. Haga clic en Add para añadir un bloque de UUID.
11. Mantenga el campo de en el valor predeterminado.
12. Especifique un tamaño para el bloque UUID que sea suficiente para admitir los recursos blade o de servidor disponibles. Haga clic en Aceptar.
13. Haga clic en Finalizar.
14. Haga clic en Aceptar.

Cree un pool de servidores

Para configurar el pool de servidores necesario para el entorno Cisco UCS, lleve a cabo los pasos siguientes:

> Considere la posibilidad de crear pools de servidores únicos para lograr la granularidad necesaria en su entorno.

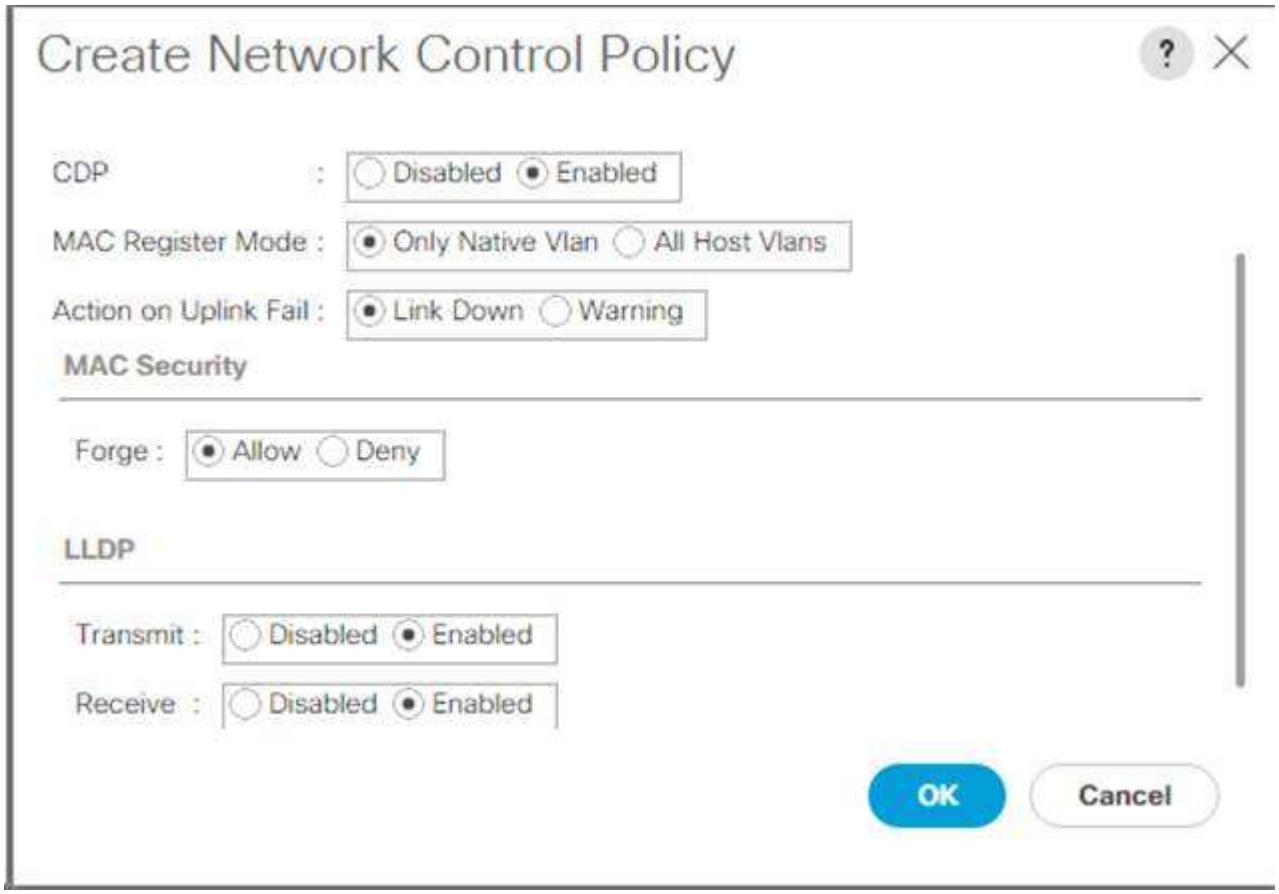
1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Pools > raíz.
3. Haga clic con el botón derecho en grupos de servidores.

4. Seleccione Crear Pool de servidores.
5. Escriba "Infra-Pool" como nombre del pool de servidores.
6. Opcional: Introduzca una descripción para el pool de servidores. Haga clic en Siguiente.
7. Seleccione dos (o más) servidores que se utilizarán para el clúster de gestión de VMware y haga clic en >> para añadirlos al pool "servidor de infra-Pool".
8. Haga clic en Finalizar.
9. Haga clic en Aceptar.

Cree una política de control de red para el protocolo de descubrimiento de Cisco y el protocolo de detección de la capa de enlace

Para crear una política de control de red para el protocolo de descubrimiento de Cisco (CDP) y el protocolo de detección de capas de vínculo (LLDP), lleve a cabo los siguientes pasos:

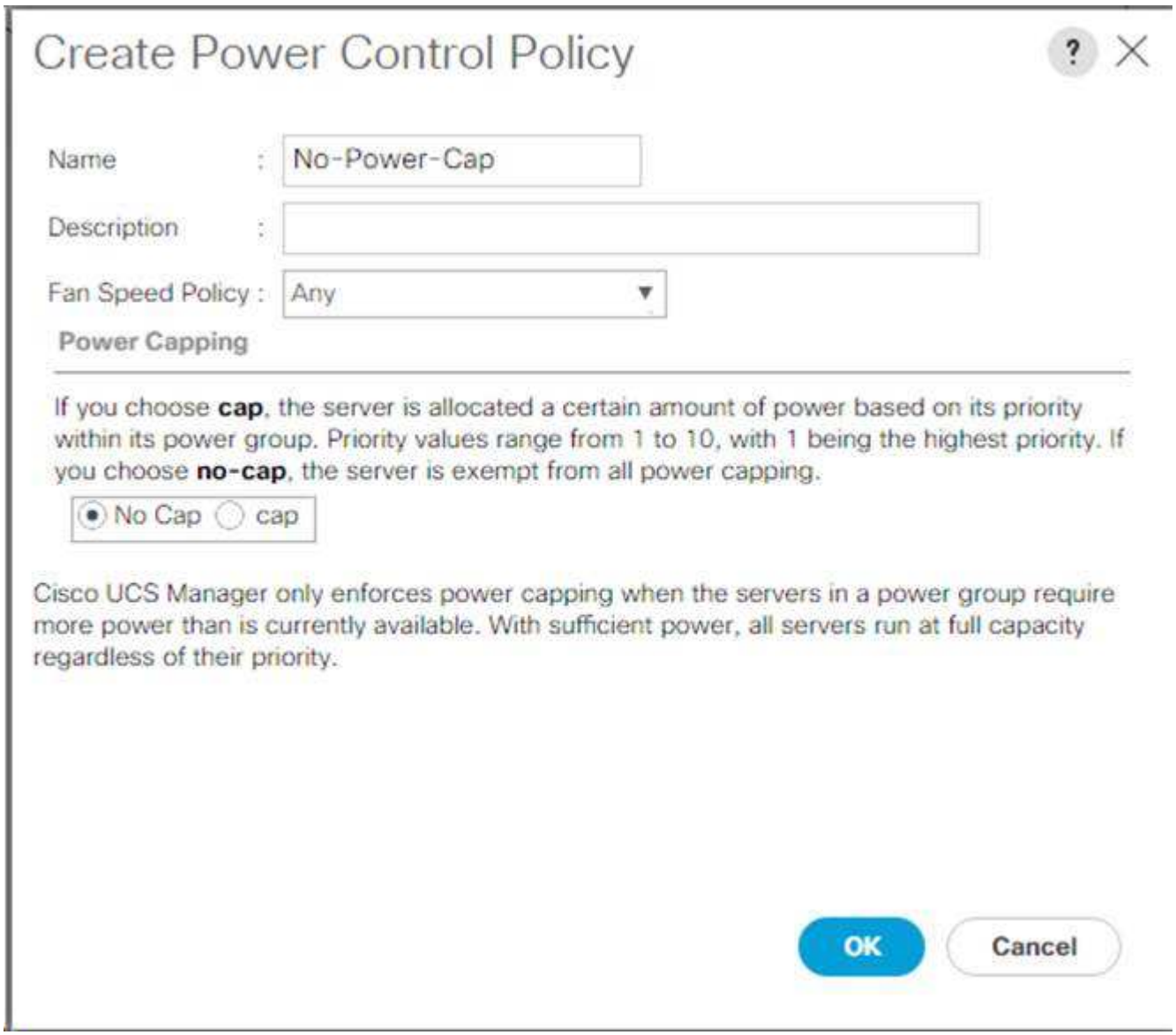
1. En Cisco UCS Manager, haga clic en LAN a la izquierda.
2. Seleccione Policies > root.
3. Haga clic con el botón derecho en Directivas de control de red.
4. Seleccione Crear Directiva de control de red.
5. Introduzca el nombre de la política Enable-CDP-LLDP.
6. Para CDP, seleccione la opción Enabled.
7. Para LLDP, desplácese hacia abajo y seleccione Enabled tanto para transmisión como para recepción.
8. Haga clic en Aceptar para crear la directiva de control de red. Haga clic en Aceptar.



Crear política de control de potencia

Para crear una política de control de alimentación para el entorno Cisco UCS, lleve a cabo los pasos siguientes:

1. En Cisco UCS Manager, haga clic en la pestaña servidores de la izquierda.
2. Seleccione Policies > root.
3. Haga clic con el botón derecho del ratón en Directivas de control de energía.
4. Seleccione Crear política de control de alimentación.
5. Introduzca sin tapa de alimentación como nombre de la política de control de alimentación.
6. Cambie la configuración de la tapa de alimentación a sin tapa.
7. Haga clic en Aceptar para crear la política de control de alimentación. Haga clic en Aceptar.

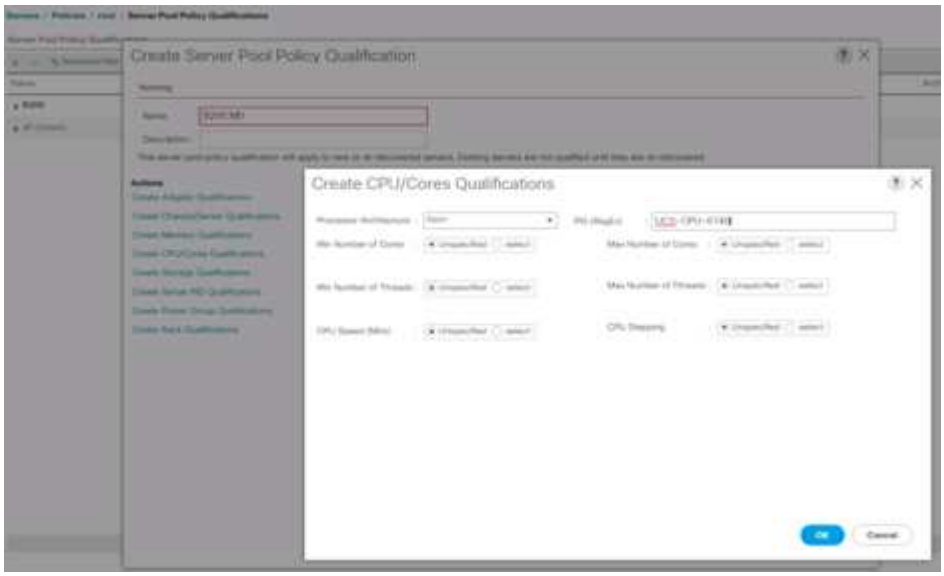


Crear política de calificación de pool de servidores (opcional)

Para crear una política de cualificación de pool de servidores opcional para el entorno Cisco UCS, realice los pasos siguientes:

Este ejemplo crea una política para los servidores Cisco UCS B-Series con los procesadores Intel E2660 v4 Xeon Broadwell.

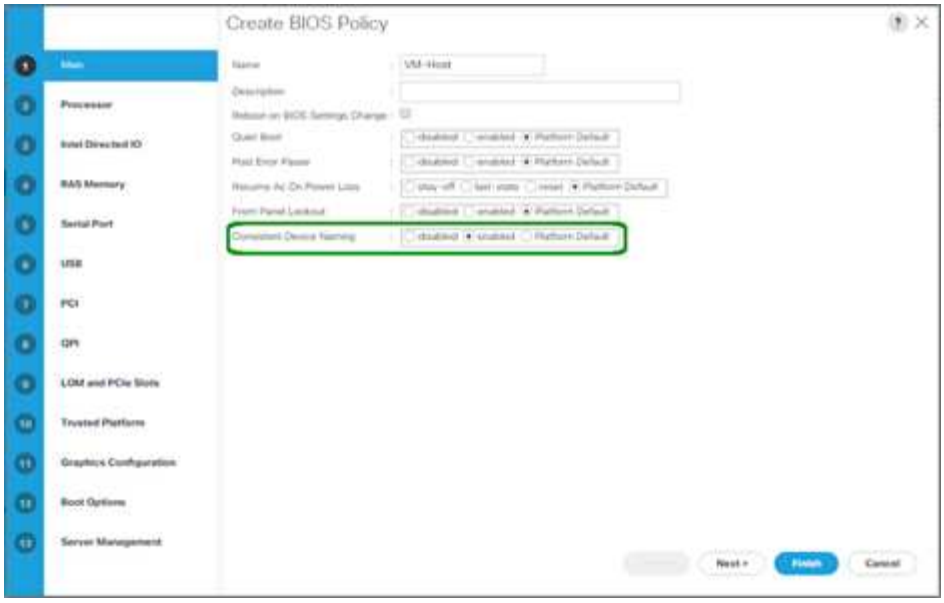
1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Policies > root.
3. Seleccione requisitos de directiva de pool de servidores.
4. Seleccione Crear calificación de directiva de grupo de servidores o Agregar.
5. Asigne un nombre a la política Intel.
6. Seleccione Crear CPU/calificaciones de núcleos.
7. Seleccione Xeon en el procesador/arquitectura.
8. Introduzca `<UCS-CPU- PID>` Como el ID de proceso (PID).
9. Haga clic en Aceptar para crear la calificación CPU/Core.
10. Haga clic en Aceptar para crear la directiva y, a continuación, haga clic en Aceptar para confirmar la directiva.



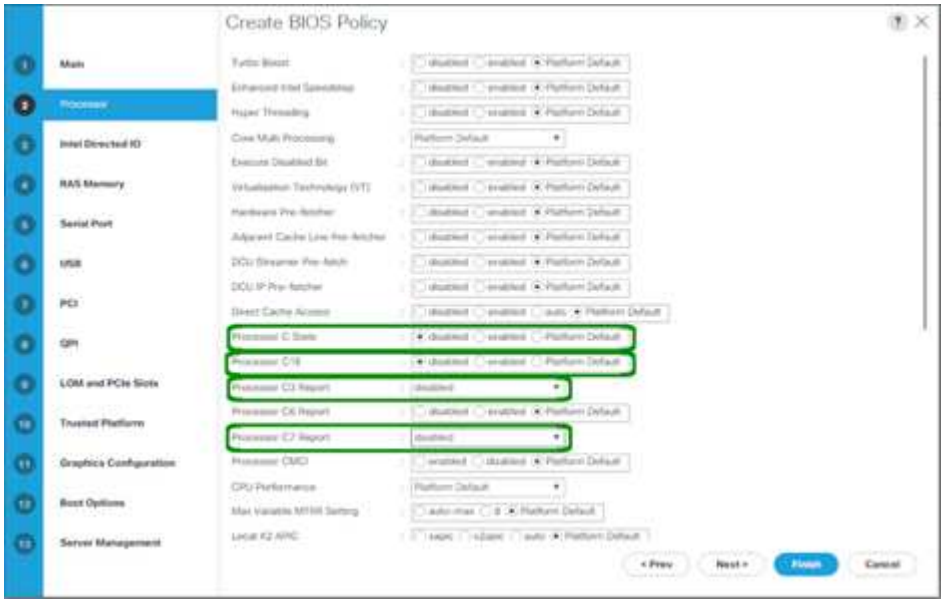
Crear directiva de BIOS del servidor

Para crear una política de BIOS de servidor para el entorno Cisco UCS, complete los pasos siguientes:

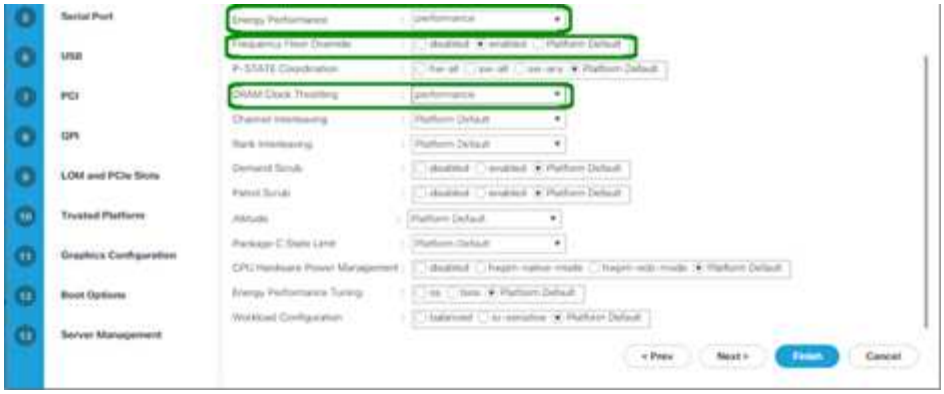
1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Policies > root.
3. Haga clic con el botón derecho del ratón en Directivas de BIOS.
4. Seleccione Crear directiva de BIOS.
5. Escriba VM-Host como nombre de la política del BIOS.
6. Cambie la configuración de arranque silencioso a Desactivado.
7. Cambie la asignación de nombres de dispositivos coherente a Activado.



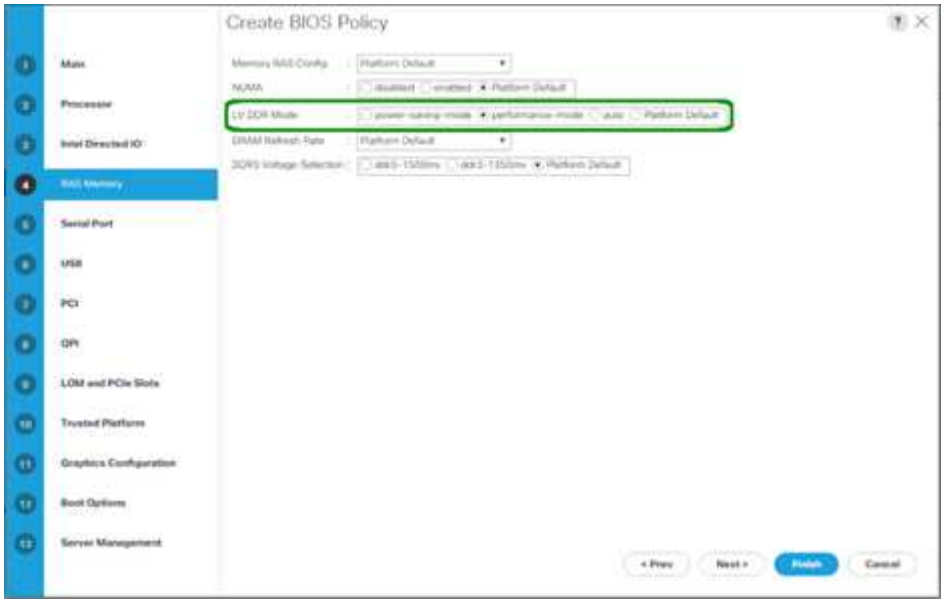
8. Seleccione la ficha procesador y configure los siguientes parámetros:
   - Estado del procesador C: Desactivado
   - Procesador C1E: Desactivado
   - Informe C3 del procesador: Desactivado
   - Informe del procesador C7: Desactivado



9. Desplácese hasta las opciones restantes del procesador y configure los siguientes parámetros:
   - Rendimiento energético: Rendimiento
   - Sustitución de suelo de frecuencia: Activada
   - Regulación del reloj DRAM: Rendimiento



10. Haga clic en memoria RAS y establezca los siguientes parámetros:
    - Modo DDR LV: Modo de rendimiento

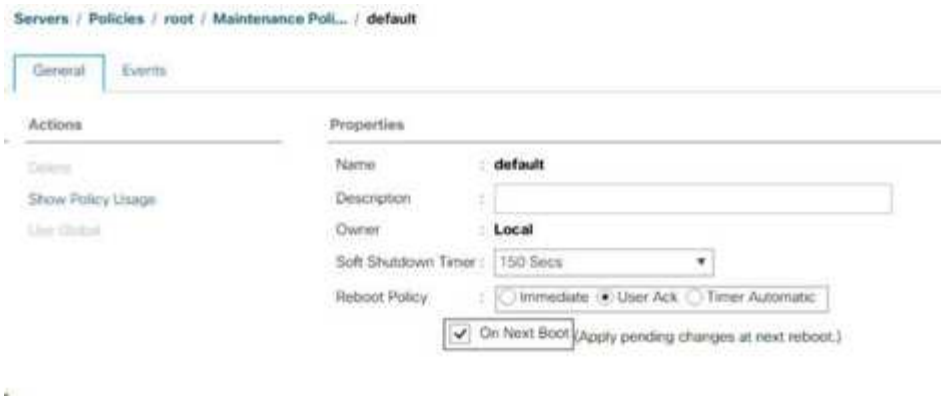


11. Haga clic en Finalizar para crear la directiva de BIOS.
12. Haga clic en Aceptar.

Actualice la directiva de mantenimiento predeterminada

Para actualizar la directiva de mantenimiento predeterminada, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Policies > root.
3. Seleccione Directivas de mantenimiento > predeterminado.
4. Cambie la directiva de reinicio a Ack de usuario.
5. Seleccione en Siguiente arranque para delegar las ventanas de mantenimiento a los administradores del servidor.



6. Haga clic en Save Changes.
7. Haga clic en Aceptar para aceptar el cambio.

Cree plantillas VNIC

Para crear varias plantillas de tarjeta de interfaz de red virtual (VNIC) para el entorno de Cisco UCS, complete los procedimientos descritos en esta sección.

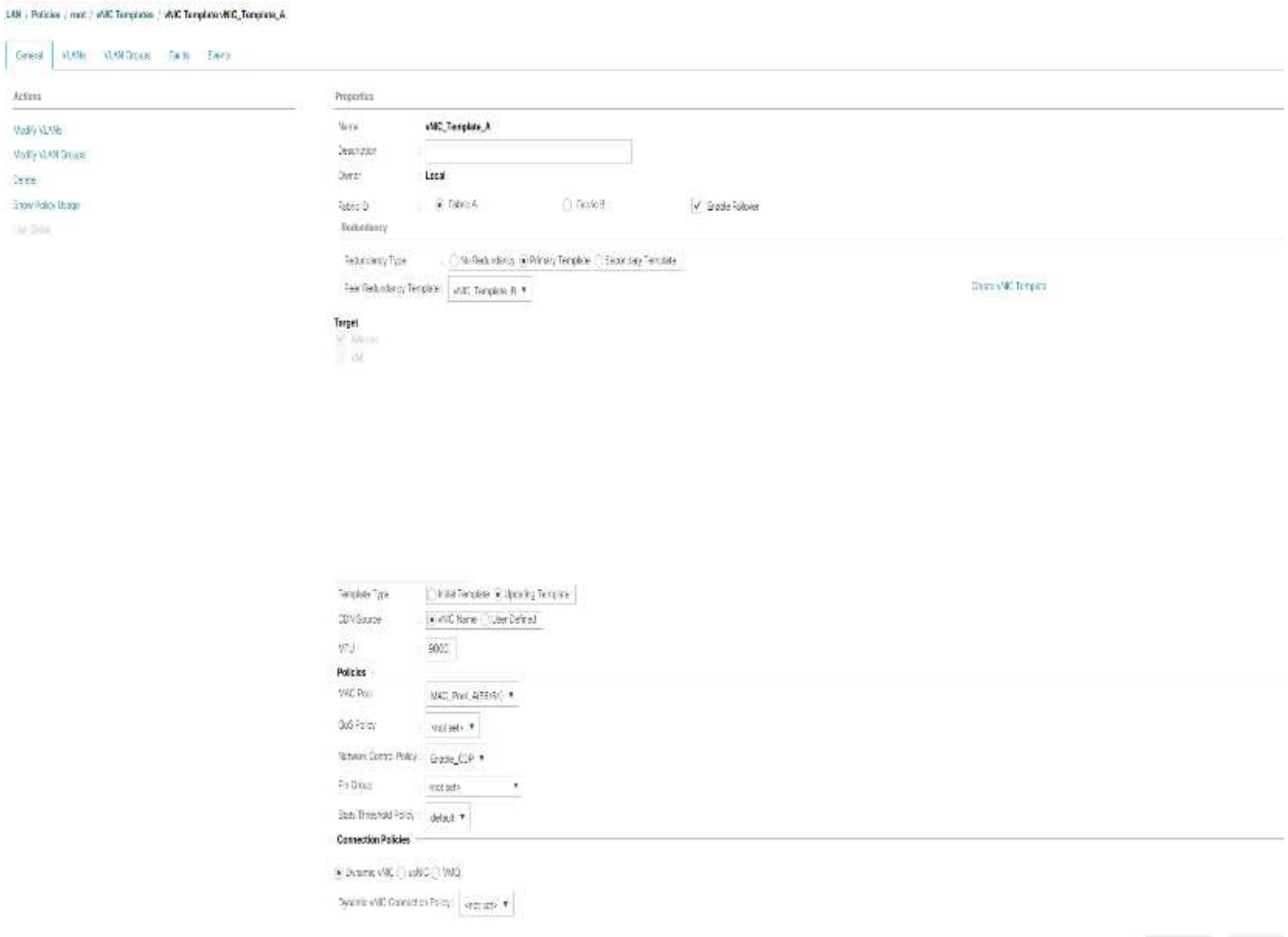
Se crea un total de cuatro plantillas VNIC.

Crear NIC virtuales de infraestructura

Para crear una infraestructura VNIC, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, haga clic en LAN a la izquierda.
2. Seleccione Policies > root.
3. Haga clic con el botón derecho del ratón en Plantillas VNIC.
4. Seleccione Crear plantilla VNIC.
5. Introduzca `Site-XX-vNIC_A` Como nombre de plantilla VNIC.
6. Seleccione Actualizar plantilla como el Tipo de plantilla.
7. Para Fabric ID, seleccione Fabric A.
8. Asegúrese de que la opción Activar conmutación por error no esté seleccionada.
9. Seleccione plantilla principal para Tipo de redundancia.
10. Deje la plantilla de redundancia del mismo nivel establecida en `<not set>`.
11. En destino, asegúrese de que sólo está seleccionada la opción adaptador.
12. Configurado `Native-VLAN` Como la VLAN nativa.
13. Seleccione Nombre VNIC para el origen CDN.
14. Para MTU, introduzca 9000.
15. En VLAN permitidas, seleccione `Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic`, Y Site-XX-vMotion. Utilice la tecla Ctrl para realizar esta selección múltiple.
16. Haga clic en Select. Estas VLAN ahora deben aparecer en las VLAN seleccionadas.
17. En la lista MAC Pool, seleccione `MAC_Pool_A`.

18. En la lista Directiva de control de red, seleccione Pool-A.
19. En la lista Network Control Policy, seleccione Enable-CDP-LLDP.
20. Haga clic en Aceptar para crear la plantilla VNIC.
21. Haga clic en Aceptar.

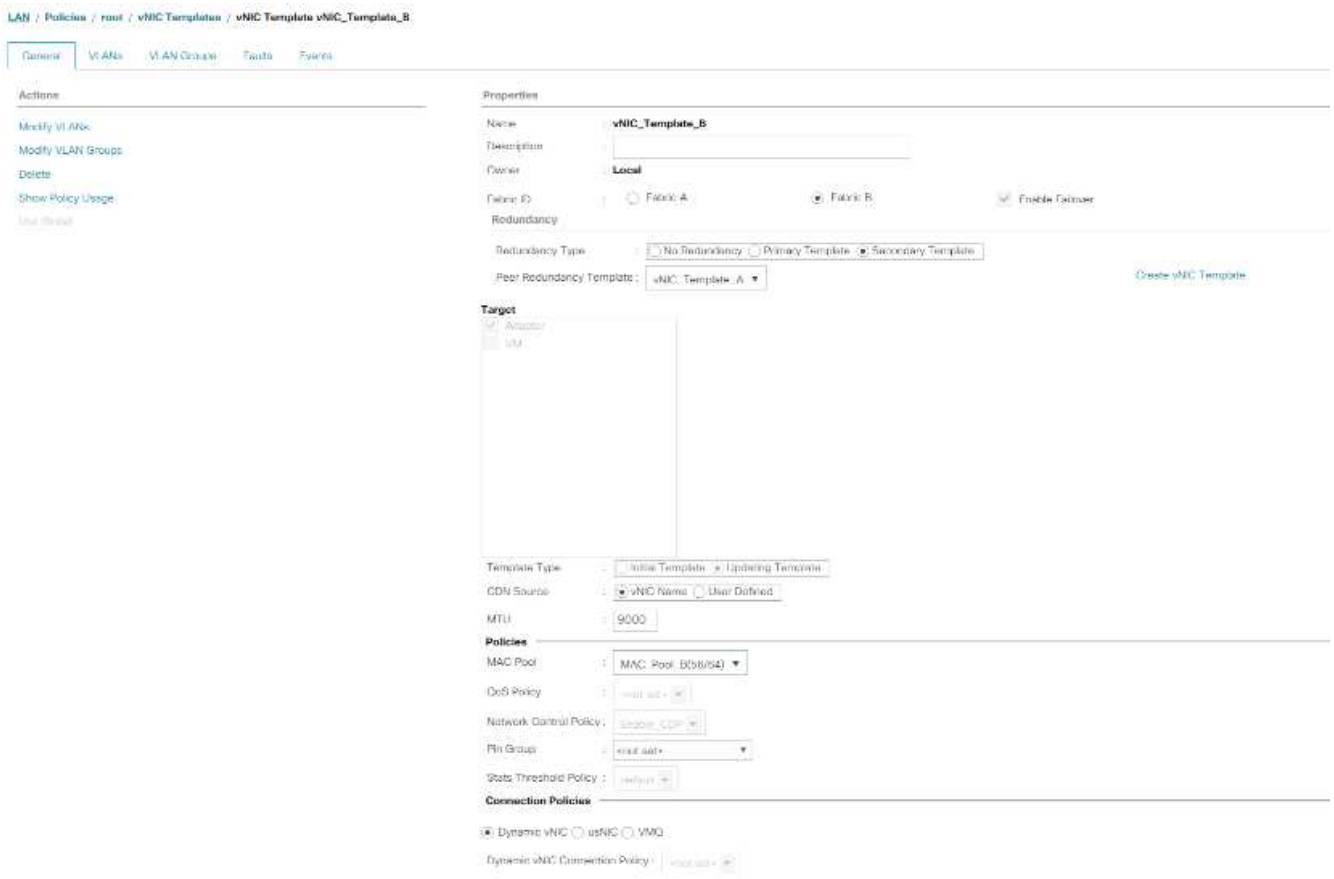


Para crear la plantilla de redundancia secundaria infra-B, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, haga clic en LAN a la izquierda.
2. Seleccione Policies > root.
3. Haga clic con el botón derecho del ratón en Plantillas VNIC.
4. Seleccione Crear plantilla VNIC.
5. Introduzca "site-XX-VNIC_B 'como nombre de plantilla VNIC.
6. Seleccione Actualizar plantilla como el Tipo de plantilla.
7. Para Fabric ID, seleccione Fabric B.
8. Seleccione la opción Habilitar conmutación por error.

La selección de la opción de recuperación tras fallos es un paso crítico para mejorar el tiempo de recuperación tras fallos de enlaces, ya que la gestión se lleva a cabo a nivel de hardware y la protección frente a cualquier posible fallo de NIC que no detecte el switch virtual.

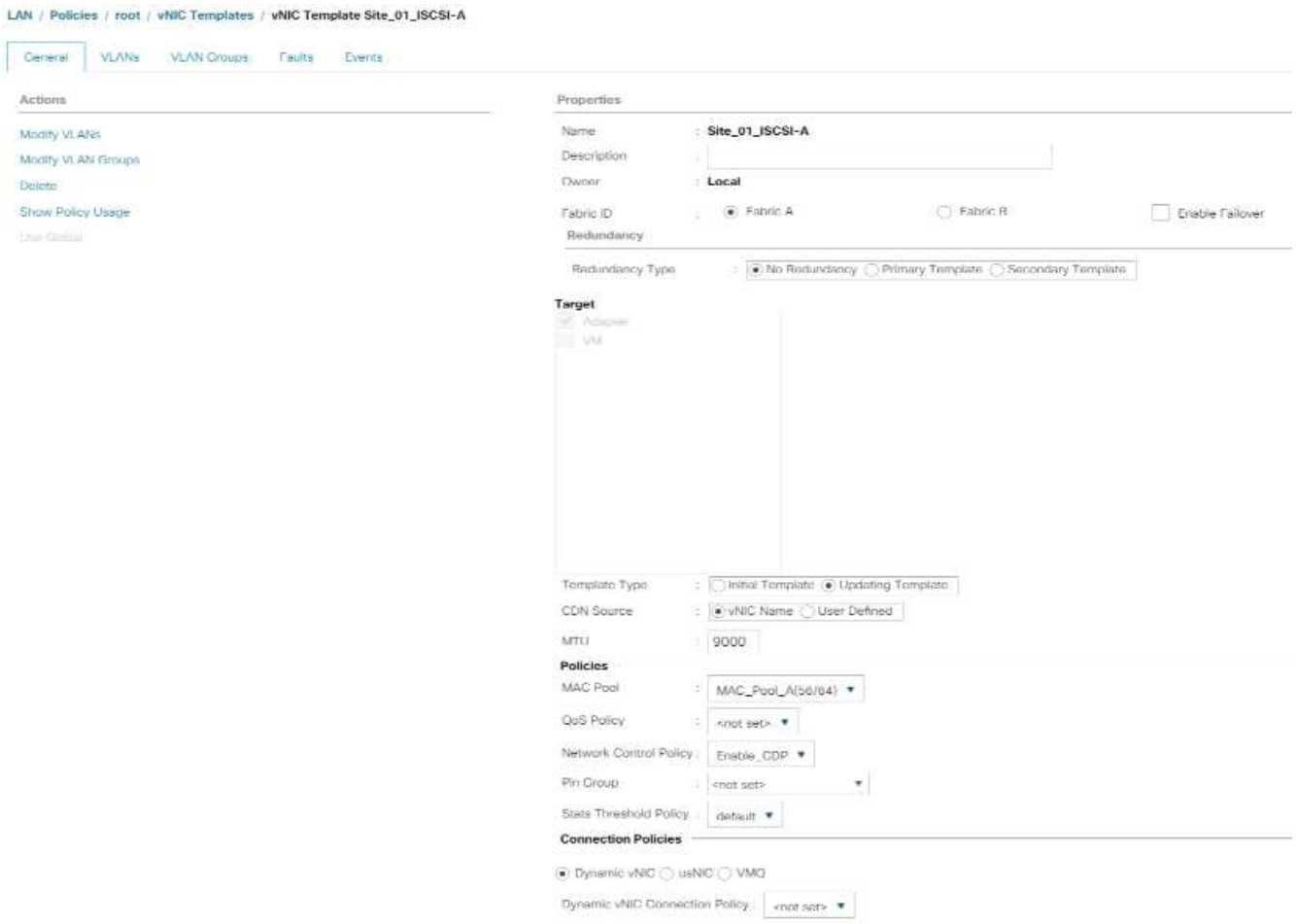
9. Seleccione plantilla principal para Tipo de redundancia.
10. Deje la plantilla de redundancia del mismo nivel establecida en `vNIC_Template_A`.
11. En destino, asegúrese de que sólo está seleccionada la opción adaptador.
12. Configurado `Native-VLAN` Como la VLAN nativa.
13. Seleccione Nombre VNIC para el origen CDN.
14. Para MTU, introduzca `9000`.
15. En VLAN permitidas, seleccione `Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic`, Y Site-XX-vMotion. Utilice la tecla Ctrl para realizar esta selección múltiple.
16. Haga clic en Select. Estas VLAN ahora deben aparecer en las VLAN seleccionadas.
17. En la lista MAC Pool, seleccione `MAC_Pool_B`.
18. En la lista Directiva de control de red, seleccione Pool-B.
19. En la lista Network Control Policy, seleccione Enable-CDP-LLDP.
20. Haga clic en Aceptar para crear la plantilla VNIC.
21. Haga clic en Aceptar.



Cree NIC iSCSI

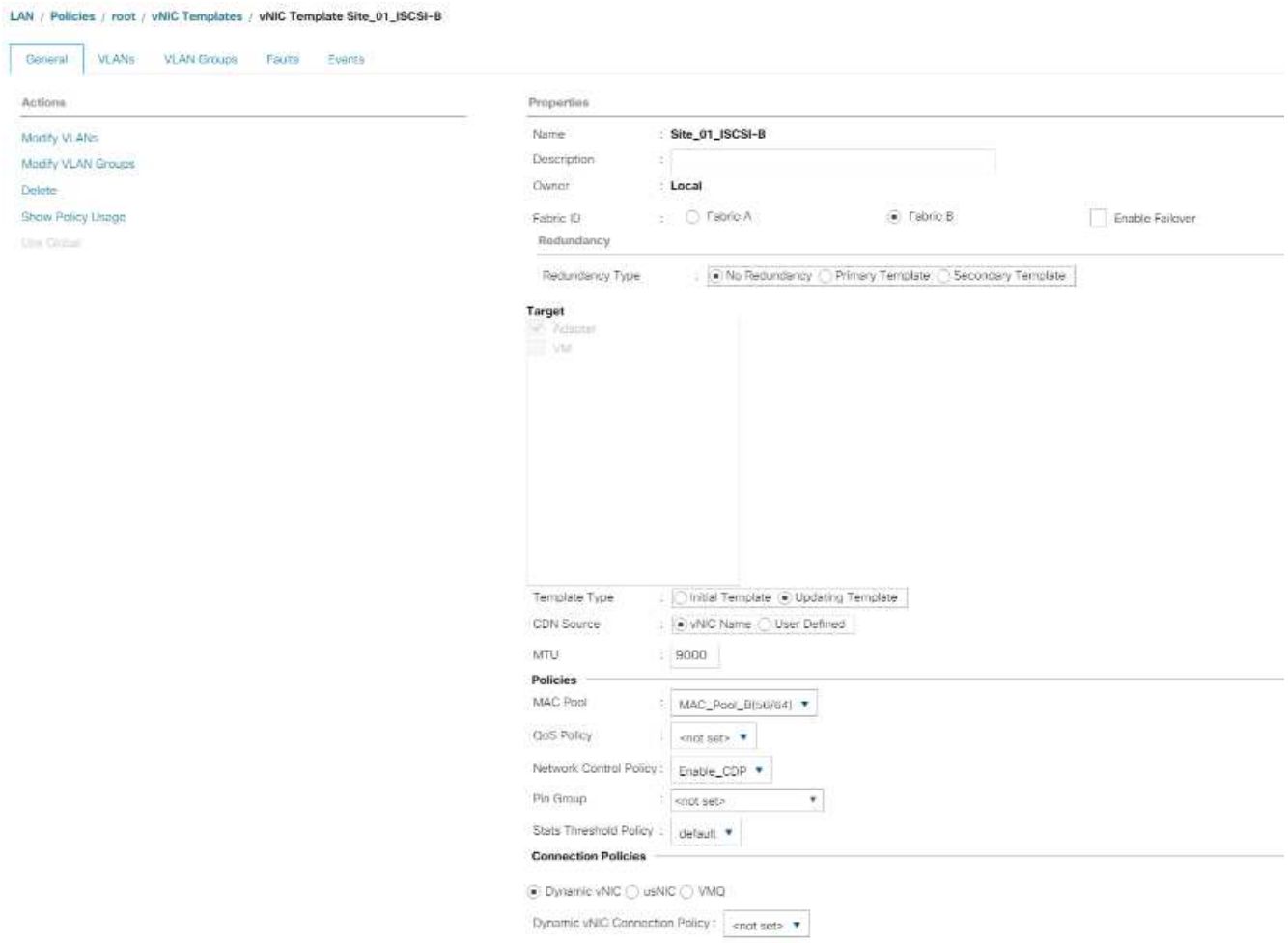
Para crear NIC iSCSI, lleve a cabo los siguientes pasos:

1. Seleccione LAN a la izquierda.
2. Seleccione Policies > root.
3. Haga clic con el botón derecho del ratón en Plantillas VNIC.
4. Seleccione Crear plantilla VNIC.
5. Introduzca `Site- 01-iSCSI_A` Como nombre de plantilla VNIC.
6. Seleccione Fabric A. No seleccione la opción Activar conmutación por error.
7. Deje el tipo de redundancia establecido en sin redundancia.
8. En destino, asegúrese de que sólo está seleccionada la opción adaptador.
9. Seleccione Actualizar plantilla para Tipo de plantilla.
10. En VLAN, seleccione Only Site- 01-iSCSI_A_VLAN.
11. Seleccione Site- 01-iSCSI_A_VLAN como VLAN nativa.
12. Deje el nombre VNIC establecido para el origen CDN.
13. En MTU, introduzca 9000.
14. En la lista MAC Pool, seleccione MAC-Pool-A.
15. En la lista Network Control Policy, seleccione Enable-CDP-LLDP.
16. Haga clic en Aceptar para completar la creación de la plantilla VNIC.
17. Haga clic en Aceptar.



18. Seleccione LAN a la izquierda.
19. Seleccione Policies > root.
20. Haga clic con el botón derecho del ratón en Plantillas VNIC.
21. Seleccione Crear plantilla VNIC.
22. Introduzca `Site- 01-iSCSI_B` Como nombre de plantilla VNIC.
23. Seleccione Fabric B. No seleccione la opción Activar conmutación por error.
24. Deje el tipo de redundancia establecido en sin redundancia.
25. En destino, asegúrese de que sólo está seleccionada la opción adaptador.
26. Seleccione Actualizar plantilla para Tipo de plantilla.
27. En VLAN, seleccione solo `Site- 01-iSCSI_B_VLAN`.
28. Seleccione `Site- 01-iSCSI_B_VLAN` Como la VLAN nativa.
29. Deje el nombre VNIC establecido para el origen CDN.
30. En MTU, introduzca 9000.
31. En la lista Pool MAC, seleccione `MAC-Pool-B`.
32. En la lista Directiva de control de red, seleccione `Enable-CDP-LLDP`.
33. Haga clic en Aceptar para completar la creación de la plantilla VNIC.

34. Haga clic en Aceptar.



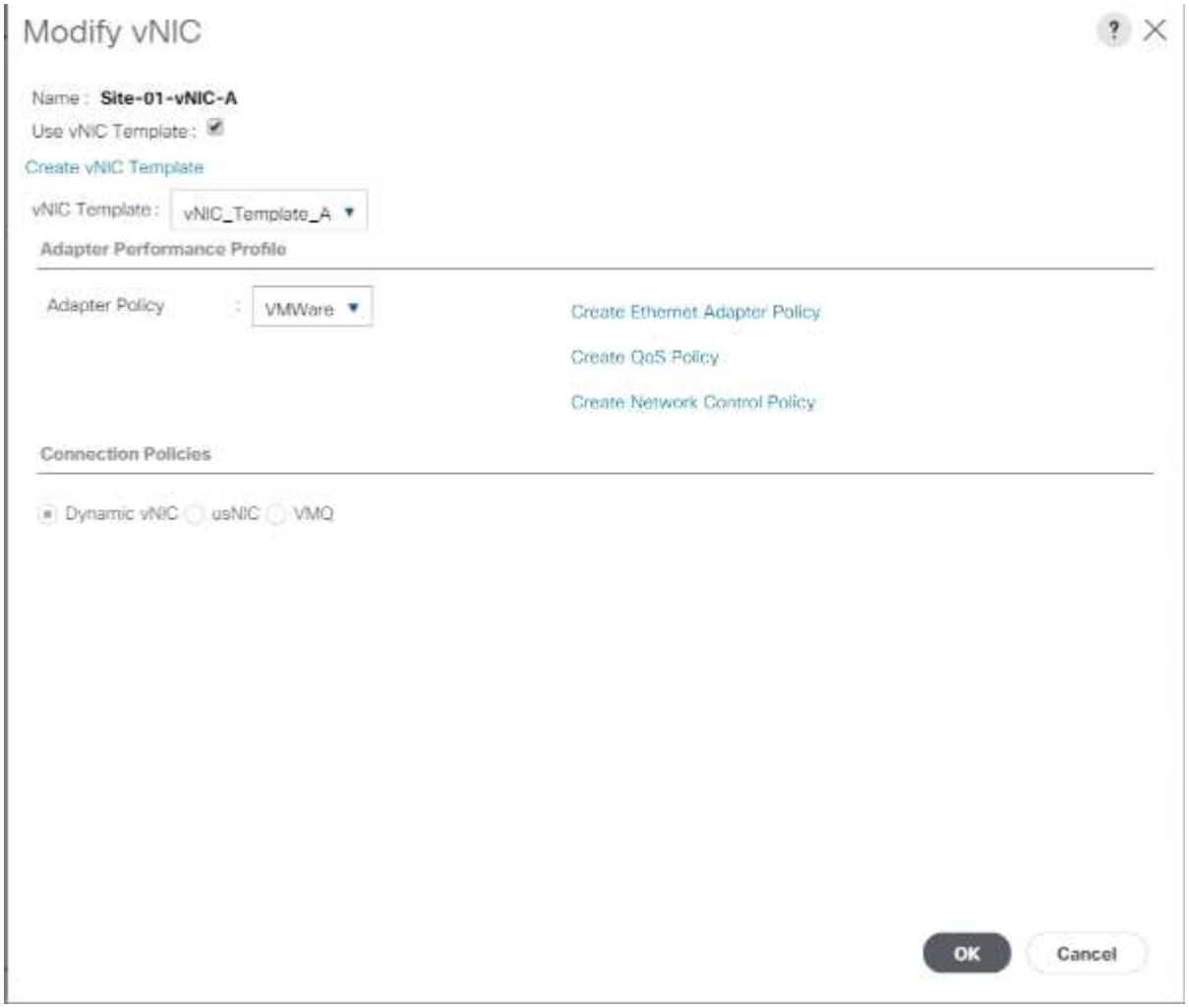
Cree una política de conectividad LAN para el arranque iSCSI

Este procedimiento se aplica a un entorno de Cisco UCS en el que hay dos LIF iSCSI en el nodo de clúster 1 (`iscsi_lif01a` y.. `iscsi_lif01b`) Y dos LIF iSCSI están en el nodo de cluster 2 (`iscsi_lif02a` y.. `iscsi_lif02b`). Asimismo, se supone que los LIF A están conectados al tejido A (Cisco UCS 6324 A) y que los LIF B están conectados al tejido B (Cisco UCS 6324 B).

Para configurar la directiva de conectividad LAN de la infraestructura necesaria, lleve a cabo los siguientes pasos:

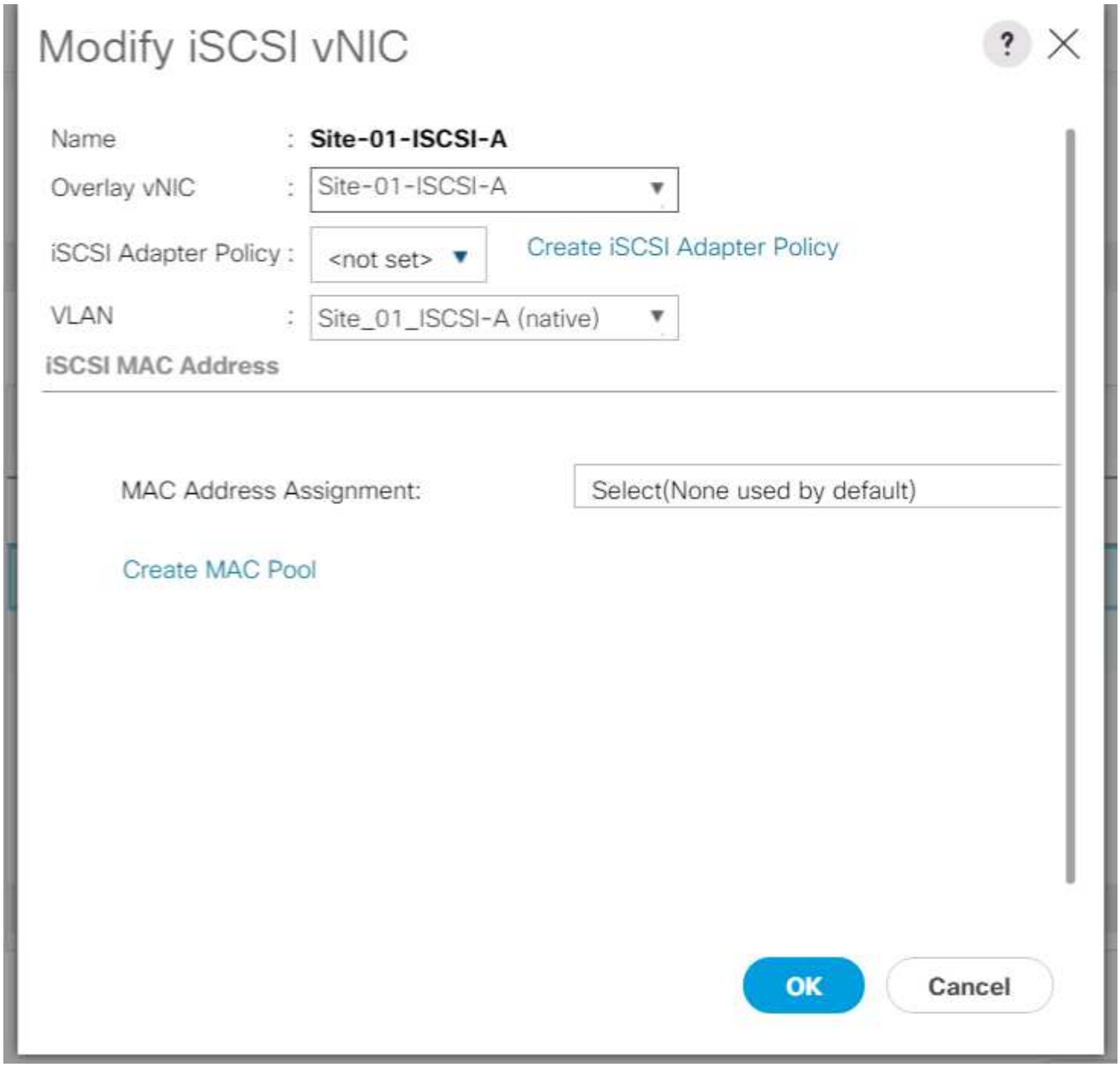
1. En Cisco UCS Manager, haga clic en LAN a la izquierda.
2. Seleccione LAN > Directivas > raíz.
3. Haga clic con el botón derecho del ratón en Directivas de conectividad LAN.
4. Seleccione Crear directiva de conectividad LAN.
5. Introduzca `Site-XX-Fabric-A` como nombre de la política.
6. Haga clic en la opción Agregar superior para agregar un VNIC.
7. En el cuadro de diálogo Crear VNIC, introduzca `Site-01-vNIC-A` Como nombre del VNIC.

8. Seleccione la opción usar plantilla VNIC.
9. En la lista plantilla VNIC, seleccione `vNIC_Template_A`.
10. En la lista desplegable Adapter Policy, seleccione VMware.
11. Haga clic en Aceptar para agregar este VNIC a la directiva.

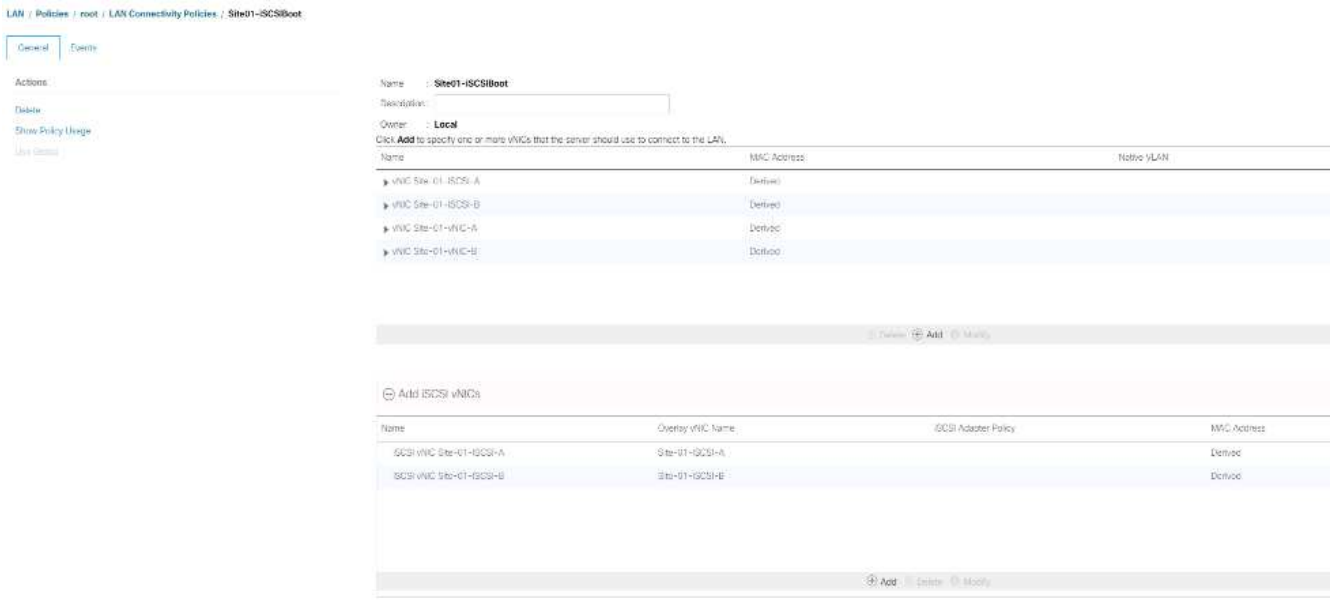


12. Haga clic en la opción Agregar superior para agregar un VNIC.
13. En el cuadro de diálogo Crear VNIC, introduzca `Site-01-vNIC-B` Como nombre del VNIC.
14. Seleccione la opción usar plantilla VNIC.
15. En la lista plantilla VNIC, seleccione `vNIC_Template_B`.
16. En la lista desplegable Adapter Policy, seleccione VMware.
17. Haga clic en Aceptar para agregar este VNIC a la directiva.
18. Haga clic en la opción Agregar superior para agregar un VNIC.
19. En el cuadro de diálogo Crear VNIC, introduzca `Site-01- iSCSI-A` Como nombre del VNIC.
20. Seleccione la opción usar plantilla VNIC.
21. En la lista plantilla VNIC, seleccione `Site-01-iSCSI-A`.
22. En la lista desplegable Adapter Policy, seleccione VMware.

23. Haga clic en Aceptar para agregar este VNIC a la directiva.
24. Haga clic en la opción Agregar superior para agregar un VNIC.
25. En el cuadro de diálogo Crear VNIC, introduzca `Site-01-iSCSI-B` Como nombre del VNIC.
26. Seleccione la opción usar plantilla VNIC.
27. En la lista plantilla VNIC, seleccione `Site-01-iSCSI-B`.
28. En la lista desplegable Adapter Policy, seleccione VMware.
29. Haga clic en Aceptar para agregar este VNIC a la directiva.
30. Expanda la opción Agregar NIC iSCSI.
31. Haga clic en la opción Agregar inferior del espacio Agregar vNIC iSCSI para agregar el VNIC iSCSI.
32. En el cuadro de diálogo Create iSCSI VNIC, introduzca `Site-01-iSCSI-A` Como nombre del VNIC.
33. Seleccione Overlay VNIC AS `Site-01-iSCSI-A`.
34. Deje la opción iSCSI Adapter Policy (Política del adaptador iSCSI) en no configurado.
35. Seleccione la VLAN como `Site-01-iSCSI-Site-A` (nativo).
36. Seleccione Ninguno (utilizado de forma predeterminada) como asignación de dirección MAC.
37. Haga clic en Aceptar para agregar el VNIC iSCSI a la directiva.



38. Haga clic en la opción Agregar inferior del espacio Agregar vNIC iSCSI para agregar el VNIC iSCSI.
39. En el cuadro de diálogo Create iSCSI VNIC, introduzca `Site-01-iSCSI-B` Como nombre del VNIC.
40. Seleccione Overlay VNIC como Site-01-iSCSI-B.
41. Deje la opción iSCSI Adapter Policy (Política del adaptador iSCSI) en no configurado.
42. Seleccione la VLAN como `Site-01-iSCSI-Site-B` (nativo).
43. Seleccione Ninguno (utilizado de forma predeterminada) como asignación de direcciones MAC.
44. Haga clic en Aceptar para agregar el VNIC iSCSI a la directiva.
45. Haga clic en Save Changes.



Cree la política vMedia para el arranque de instalación de VMware ESXi 6.7U1

En los pasos de configuración de Data ONTAP de NetApp es necesario un servidor web HTTP, que se utiliza para alojar Data ONTAP de NetApp y software VMware. La política de vMedia creada aquí asigna VMware ESXi 6. 7U1 ISO al servidor Cisco UCS para arrancar la instalación ESXi. Para crear esta directiva, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, seleccione Servers a la izquierda.
2. Seleccione Policies > root.
3. Seleccione vMedia Policies.
4. Haga clic en Agregar para crear una nueva directiva de vMedia.
5. Asigne un nombre a la política ESXi-6.7U1-HTTP.
6. Introduzca Mounts ISO para ESXi 6.7U1 en el campo Description.
7. Seleccione Sí si Reintentar en caso de fallo de montaje.
8. Haga clic en Añadir.
9. Asigne el nombre Mount ESXi-6.7U1-HTTP.
10. Seleccione el tipo de dispositivo CDD.
11. Seleccione el protocolo HTTP.
12. Introduzca la dirección IP del servidor web.

> Las IP del servidor DNS no se han introducido anteriormente en la IP del KVM, por lo tanto, es necesario introducir la IP del servidor web en lugar del nombre de host.

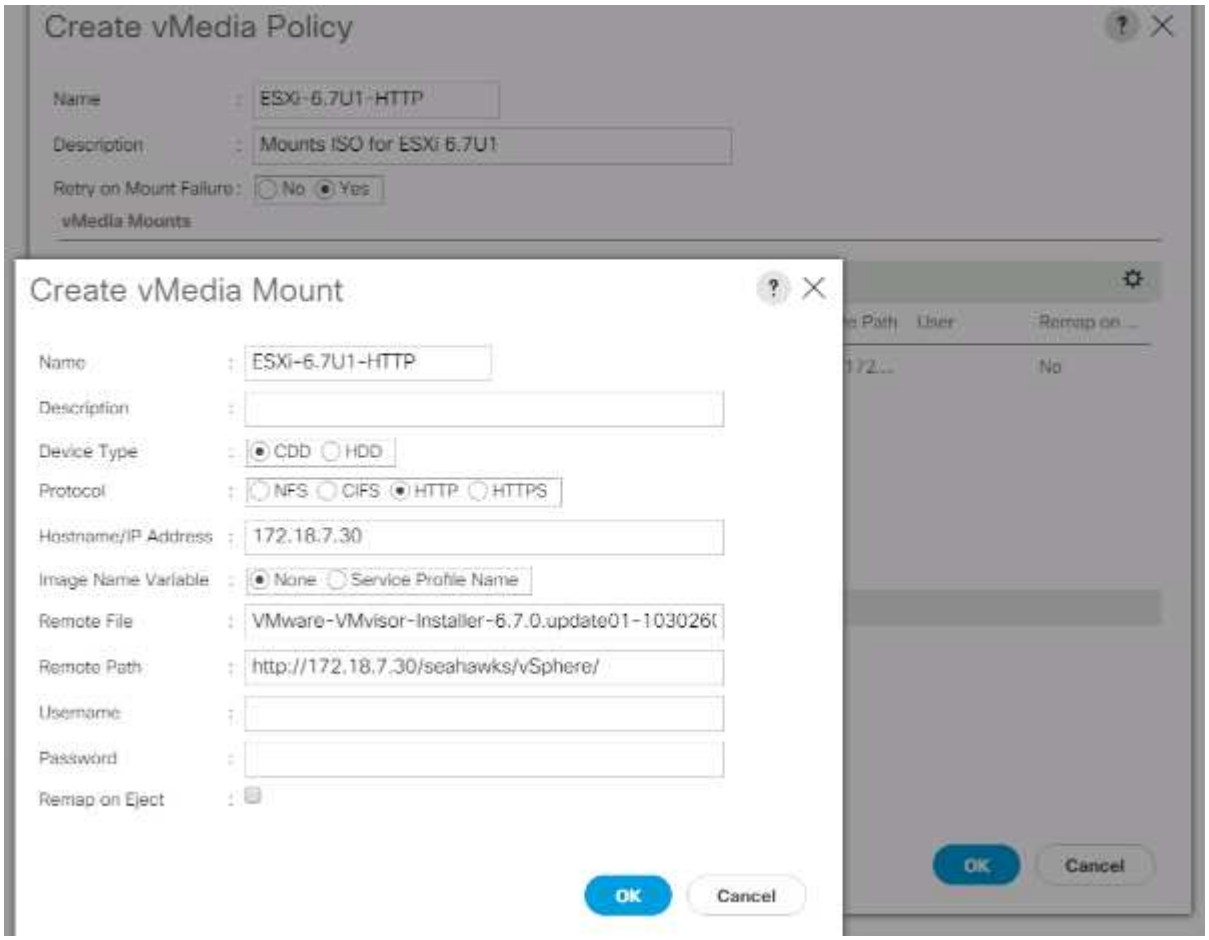
13. Introduzca `VMware-VMvisor-Installer-6.7.0.update01-10302608.x86_64.iso` Como nombre de archivo remoto.

    Este VMware ESXi 6.7U1 ISO se puede descargar desde "Descargas de VMware".

14. Introduzca la ruta del servidor web al archivo ISO en el campo Remote Path.

15. Haga clic en Aceptar para crear el montaje vMedia.
16. Haga clic en Aceptar y, a continuación, vuelva a Aceptar para completar la creación de la política de vMedia.

    Para cualquier servidor nuevo añadido al entorno Cisco UCS, se puede utilizar la plantilla de perfil de servicio vMedia para instalar el host ESXi. En el primer arranque, el host arranca en el instalador de ESXi desde que el disco montado en SAN está vacío. Una vez instalado ESXi, no se hace referencia a vMedia mientras se pueda acceder al disco de arranque.



Crear política de arranque iSCSI

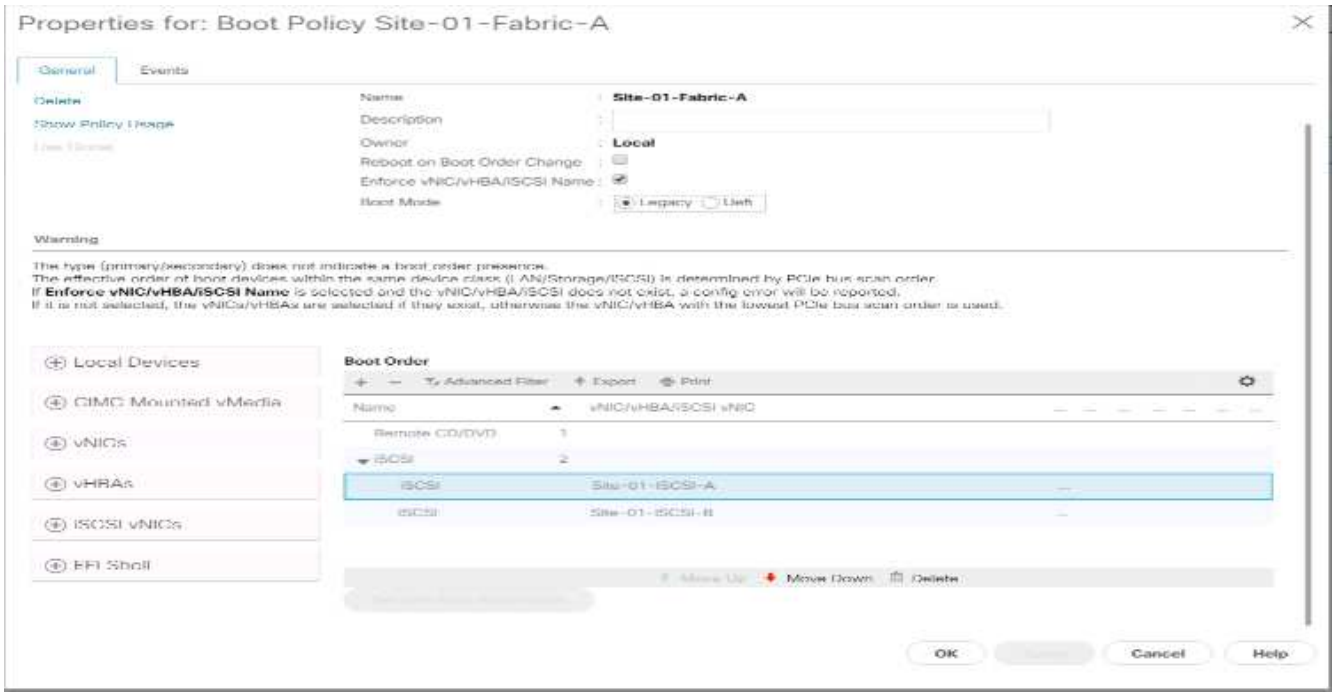
El procedimiento de esta sección se aplica a un entorno Cisco UCS en el que hay dos interfaces lógicas iSCSI (LIF) en el nodo de clúster 1 (`iscsi_lif01a` y.. `iscsi_lif01b`) Y dos LIF iSCSI están en el nodo de cluster 2 (`iscsi_lif02a` y.. `iscsi_lif02b`). Además, se supone que las LIF A están conectadas a la estructura A (Cisco UCS Fabric Interconnect A) y que los LIF B están conectados a la estructura B (Cisco UCS Fabric Interconnect B).

> Hay una política de arranque configurada en este procedimiento. La directiva configura el destino principal que se va a utilizar `iscsi_lif01a`.

Para crear una política de arranque para el entorno Cisco UCS, complete los pasos siguientes:

1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Policies > root.

3. Haga clic con el botón derecho del ratón en Directivas de arranque.
4. Seleccione Crear directiva de arranque.
5. Introduzca `Site-01-Fabric-A` como nombre de la directiva de arranque.
6. Opcional: Introduzca una descripción para la directiva de arranque.
7. Mantenga desactivada la opción Reiniciar en orden de arranque.
8. El modo de arranque es heredado.
9. Expanda el menú desplegable dispositivos locales y seleccione Agregar CD/DVD remoto.
10. Expanda el menú desplegable NIC iSCSI y seleccione Agregar inicio iSCSI.
11. En el cuadro de diálogo Add iSCSI Boot, introduzca `Site-01-iSCSI-A`. Haga clic en Aceptar.
12. Seleccione Add iSCSI Boot.
13. En el cuadro de diálogo Add iSCSI Boot, introduzca `Site-01-iSCSI-B`. Haga clic en Aceptar.
14. Haga clic en OK para crear la directiva.



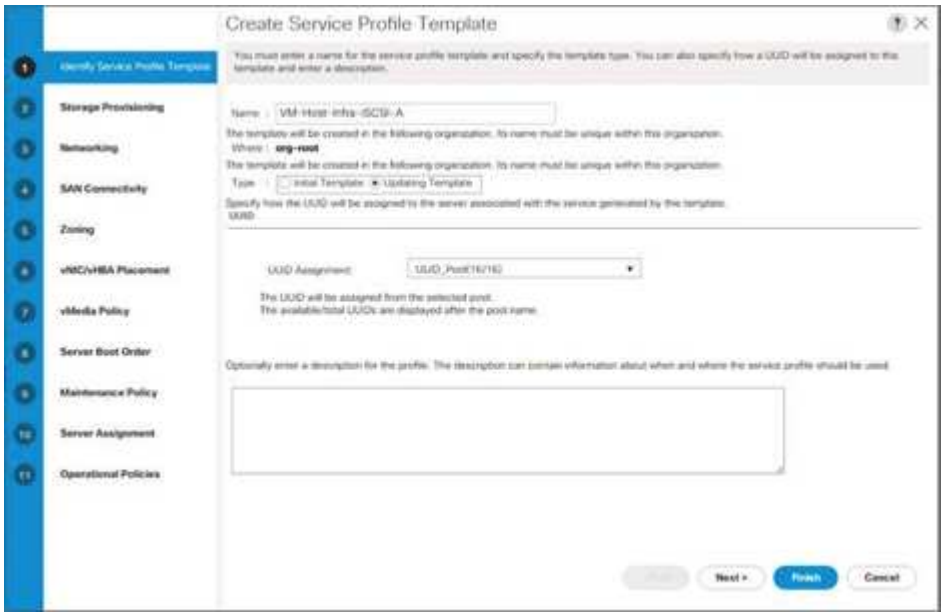
Crear plantilla de perfil de servicio

En este procedimiento, se crea una plantilla de perfil de servicio para los hosts ESXi de infraestructura para el arranque de Fabric A.

Para crear la plantilla de perfil de servicio, lleve a cabo los siguientes pasos:

1. En Cisco UCS Manager, haga clic en Servers (servidores) a la izquierda.
2. Seleccione Plantillas de perfil de servicio > raíz.
3. Haga clic con el botón derecho del ratón en root.
4. Seleccione Crear plantilla de perfil de servicio para abrir el asistente Crear plantilla de perfil de servicio.
5. Introduzca `VM-Host-Infra-iSCSI-A` como nombre de la plantilla de perfil de servicio. Esta plantilla de perfil de servicio está configurada para arrancar desde el nodo de almacenamiento 1 en la estructura A.

6. Seleccione la opción Actualizar plantilla.
7. En UUID, seleccione `UUID_Pool` Como pool de UUID. Haga clic en Siguiente.



Configure el aprovisionamiento del almacenamiento

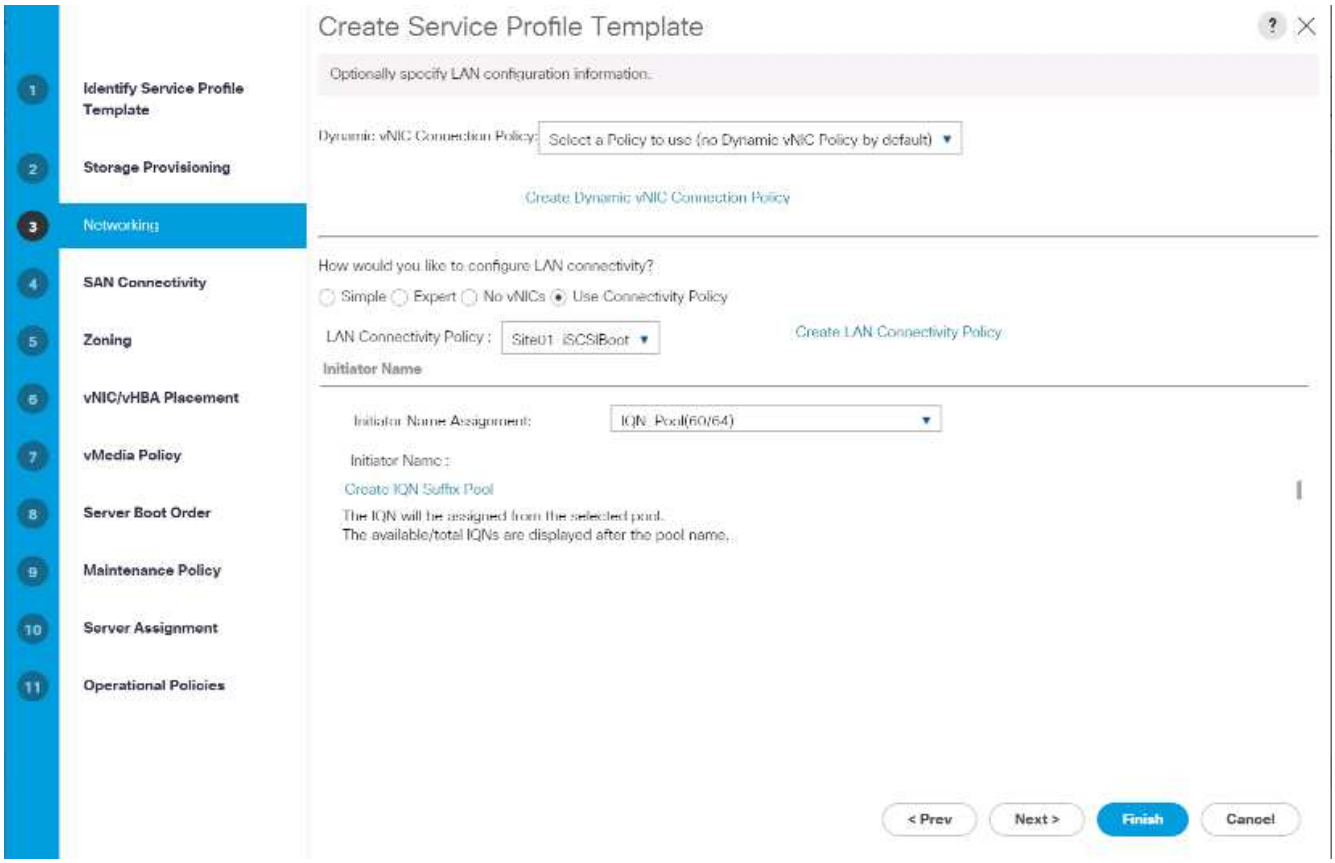
Para configurar el aprovisionamiento de almacenamiento, complete los siguientes pasos:

1. Si tiene servidores sin discos físicos, haga clic en Directiva de configuración de disco local y seleccione la Directiva de almacenamiento local de arranque DE SAN. De lo contrario, seleccione la Política de almacenamiento local predeterminada.
2. Haga clic en Siguiente.

Configuración de las opciones de red

Para configurar las opciones de red, lleve a cabo los siguientes pasos:

1. Mantenga la configuración predeterminada de la directiva de conexión dinámica de VNIC.
2. Seleccione la opción usar directiva de conectividad para configurar la conectividad LAN.
3. Seleccione iSCSI-Boot en el menú desplegable LAN Connectivity Policy.
4. Seleccione `IQN_Pool` En asignación de nombre de iniciador. Haga clic en Siguiente.



Configurar la conectividad SAN

Para configurar la conectividad SAN, siga estos pasos:

1. En el caso de vHBA, seleccione no para el ¿Cómo desea configurar la conectividad DE SAN? opción.
2. Haga clic en Siguiente.

Configurar la división en zonas

Para configurar la división en zonas, haga clic en Next.

Configurar la colocación de VNIC/HBA

Para configurar la colocación de VNIC/HBA, lleve a cabo los siguientes pasos:

1. En la lista desplegable Seleccionar ubicación, deje la política de colocación como permitir que el sistema realice la colocación.
2. Haga clic en Siguiente.

Configure la directiva vMedia

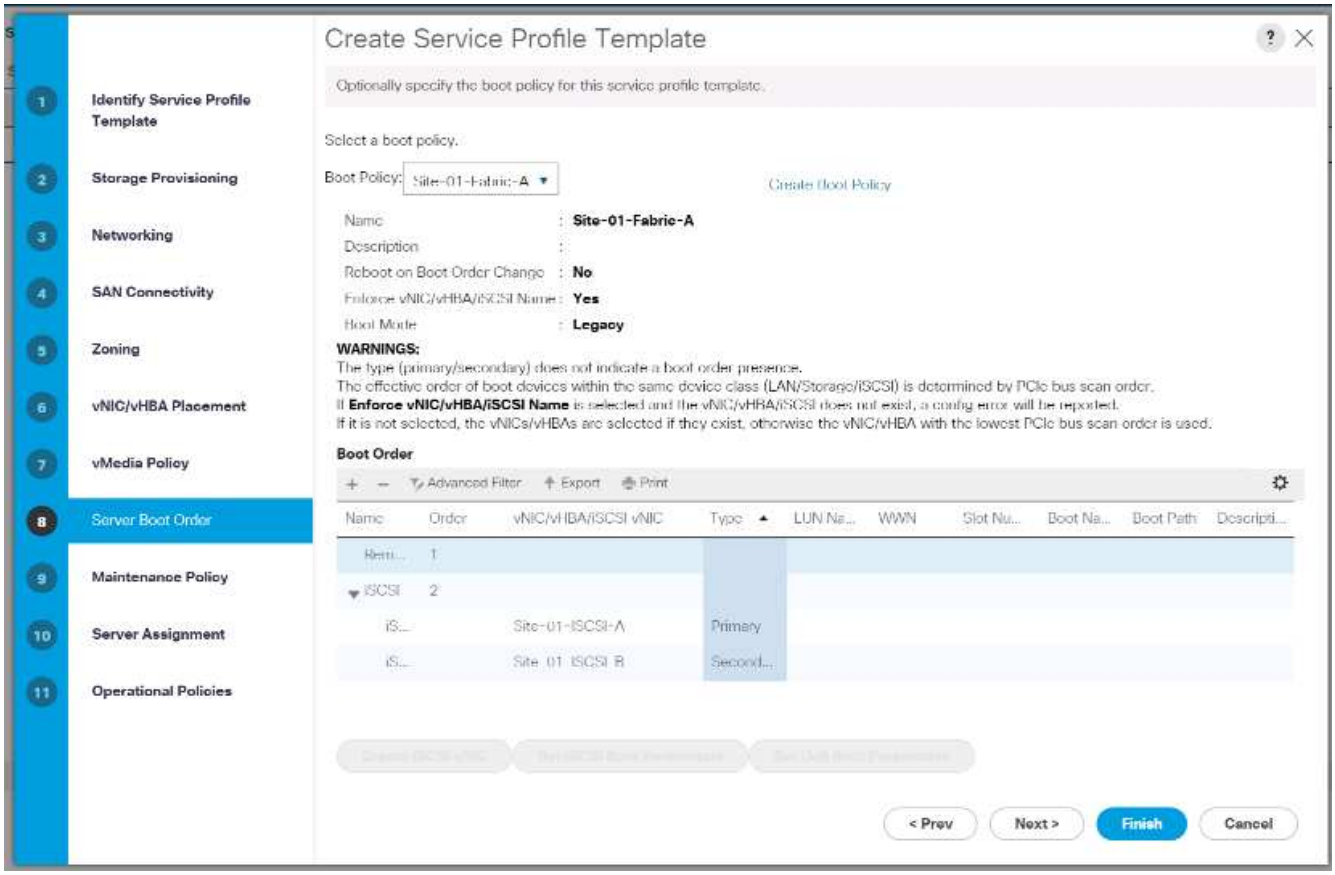
Para configurar la directiva vMedia, realice los siguientes pasos:

1. No seleccione una política de vMedia.
2. Haga clic en Siguiente.

Configurar el orden de arranque del servidor

Para configurar el orden de arranque del servidor, lleve a cabo los siguientes pasos:

1. Seleccione `Boot-Fabric-A` Para Directiva de inicio.



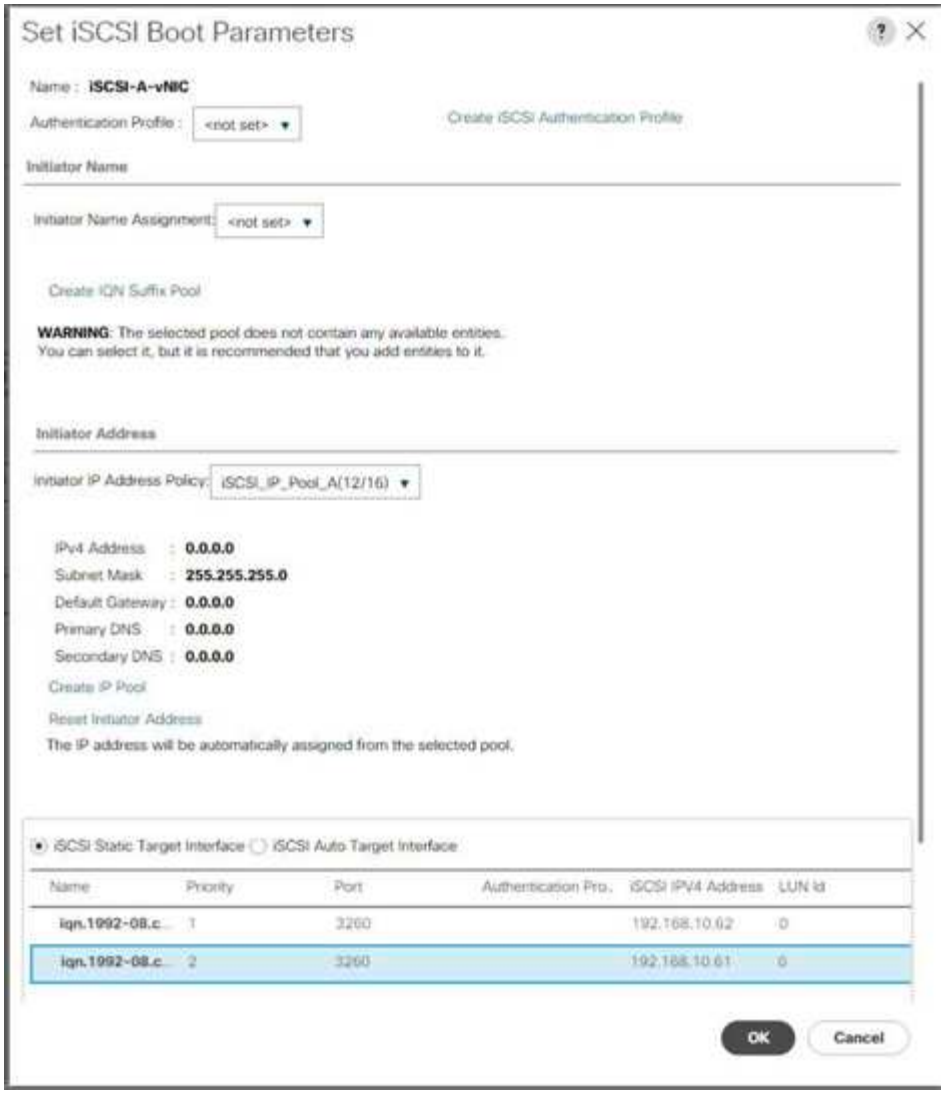
2. En el orden Boor, seleccione `Site-01- iSCSI-A`.
3. Haga clic en Set iSCSI Boot Parameters.
4. En el cuadro de diálogo definir parámetros de arranque iSCSI, deje la opción Perfil de autenticación en sin establecer a menos que haya creado de forma independiente uno adecuado para su entorno.
5. Deje el cuadro de diálogo asignación de nombre de iniciador no establecido para utilizar el nombre de iniciador de perfil de servicio único definido en los pasos anteriores.
6. Configurado `iSCSI_IP_Pool_A` Como directiva de dirección IP del iniciador.
7. Seleccione la opción iSCSI Static Target Interface (interfaz de destino estática iSCSI).
8. Haga clic en Añadir.
9. Introduzca el nombre del destino iSCSI. Para obtener el nombre de destino iSCSI de infra-SVM, inicie sesión en la interfaz de gestión de clústeres de almacenamiento y ejecute el `iscsi show` comando.

```
bb04-aff300::> iscsi show
            Target                          Target                          Status
Vserver     Name                            Alias                           Admin
----------- ------------------------------- ------------------------------- ------
Infra-SVM   iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                            Infra-SVM                       up
```

10. Introduzca la dirección IP de `iscsi_lif_02a` Para el campo Dirección IPv4.

11. Haga clic en OK para añadir el destino estático iSCSI.
12. Haga clic en Añadir.
13. Introduzca el nombre del destino iSCSI.
14. Introduzca la dirección IP de `iscsi_lif_01a` Para el campo Dirección IPv4.

15. Haga clic en OK para añadir el destino estático iSCSI.



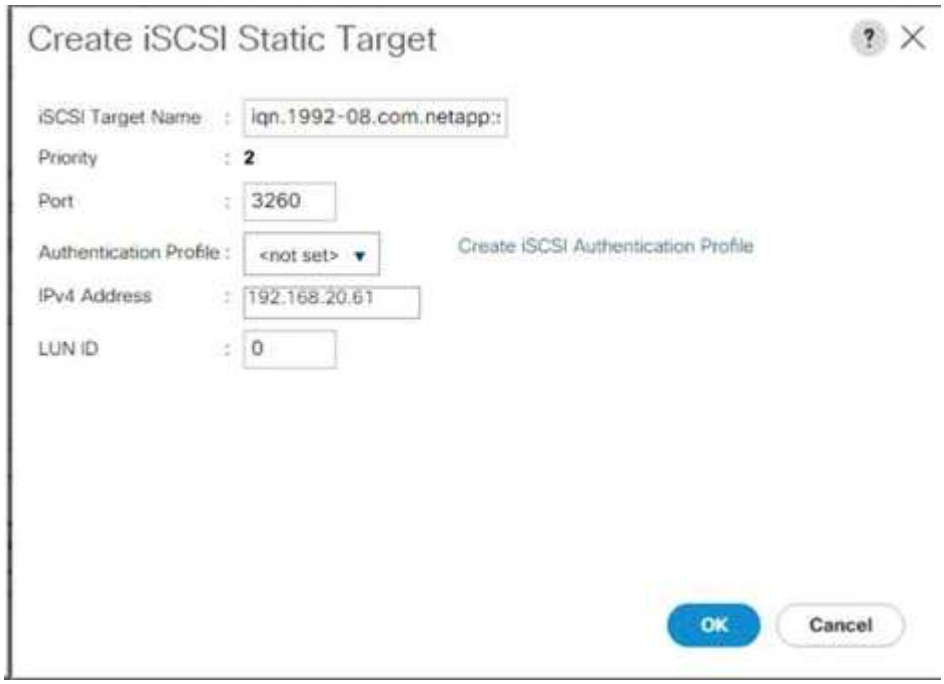
Las IP de destino se colocaron con el nodo de almacenamiento 02 IP primero y el nodo de almacenamiento 01 IP segundo. Se asume que la LUN de arranque está en el nodo 01. El host arranca mediante la ruta al nodo 01 si se utiliza el orden de este procedimiento.

16. En el orden de arranque, seleccione iSCSI-B-VNIC.
17. Haga clic en Set iSCSI Boot Parameters.
18. En el cuadro de diálogo definir parámetros de arranque iSCSI, deje la opción Perfil de autenticación como no establecido a menos que haya creado de forma independiente uno adecuado para su entorno.
19. Deje el cuadro de diálogo asignación de nombre de iniciador no establecido para utilizar el nombre de iniciador de perfil de servicio único definido en los pasos anteriores.
20. Configurado `iSCSI_IP_Pool_B` Como política de dirección IP del iniciador.
21. Seleccione la opción iSCSI Static Target Interface (interfaz de destino estático iSCSI).
22. Haga clic en Añadir.
23. Introduzca el nombre del destino iSCSI. Para obtener el nombre de destino iSCSI de infra-SVM, inicie sesión en la interfaz de gestión de clústeres de almacenamiento y ejecute el `iscsi show` comando.

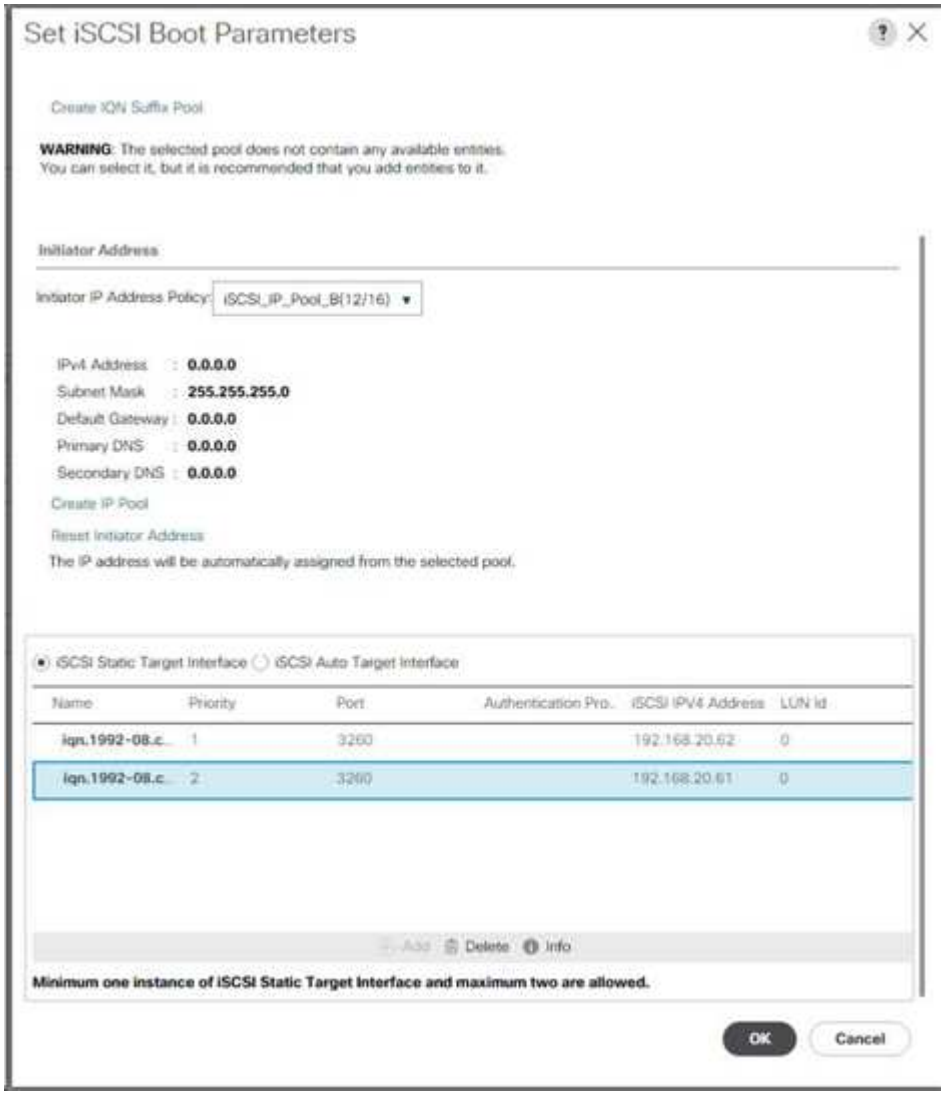
```
bb04-aff300::> iscsi show
          Target                          Target                         Status
Vserver   Name                            Alias                          Admin
--------- ------------------------------- ------------------------------ ------
Infra-SVM  iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                          Infra-SVM                      up
```

24. Introduzca la dirección IP de `iscsi_lif_02b` Para el campo Dirección IPv4.

25. Haga clic en OK para añadir el destino estático iSCSI.
26. Haga clic en Añadir.
27. Introduzca el nombre del destino iSCSI.
28. Introduzca la dirección IP de `iscsi_lif_01b` Para el campo Dirección IPv4.



29. Haga clic en OK para añadir el destino estático iSCSI.

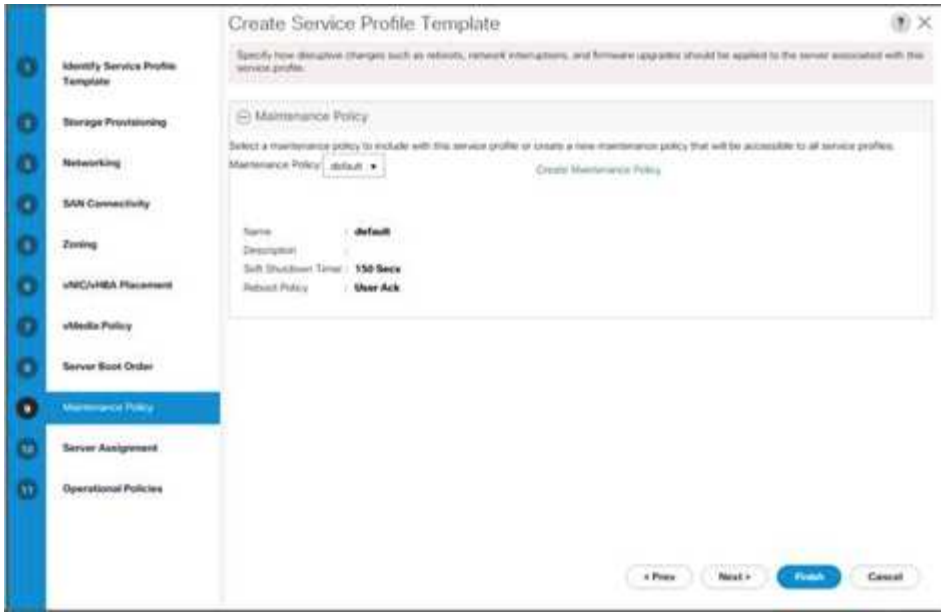


30. Haga clic en Siguiente.

Configure la directiva de mantenimiento

Para configurar la directiva de mantenimiento, lleve a cabo los siguientes pasos:

1. Cambie la directiva de mantenimiento a predeterminada.

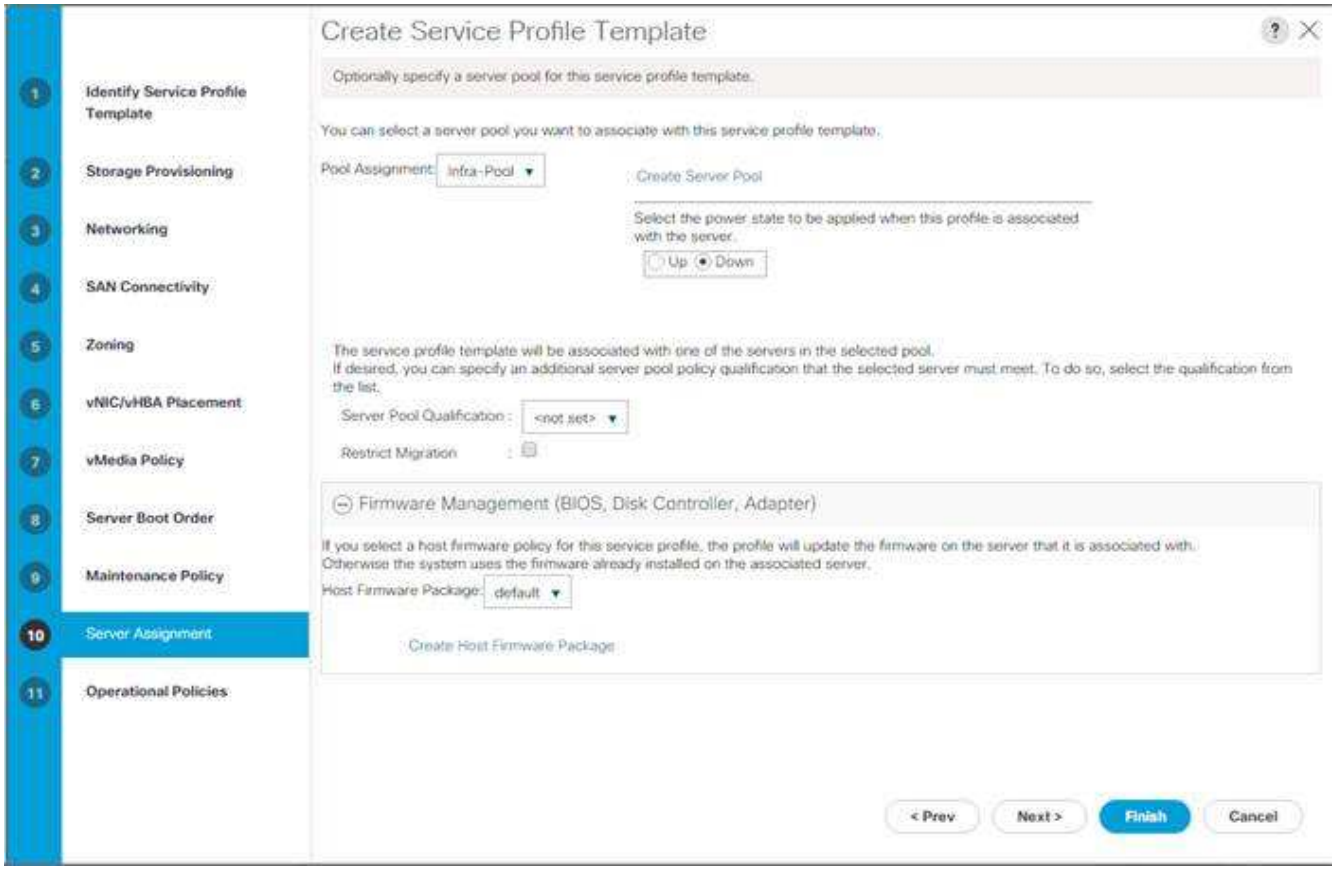


2. Haga clic en Siguiente.

Configurar la asignación de servidores

Para configurar la asignación del servidor, lleve a cabo los siguientes pasos:

1. En la lista asignación de grupos, seleccione Infra-Pool.
2. Seleccione Down como estado de alimentación que se va a aplicar cuando el perfil esté asociado al servidor.
3. Expanda Administración de firmware en la parte inferior de la página y seleccione la directiva predeterminada.

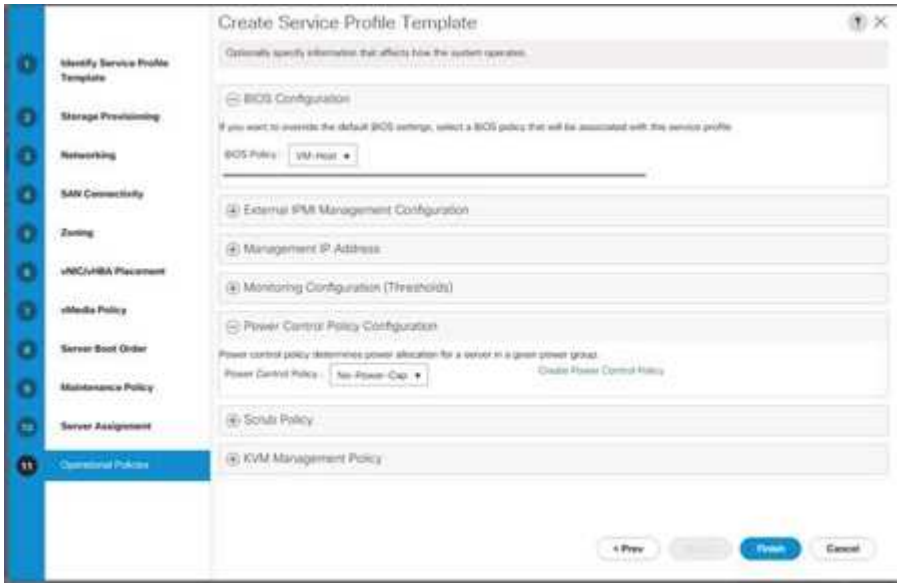


4. Haga clic en Siguiente.

Configure las políticas operativas

Para configurar las directivas operativas, realice los siguientes pasos:

1. En la lista desplegable BIOS Policy, seleccione VM-Host.
2. Expanda Configuración de la política de control de alimentación y seleccione sin límite de alimentación en la lista desplegable Política de control de alimentación.



3. Haga clic en Finalizar para crear la plantilla de perfil de servicio.
4. Haga clic en Aceptar en el mensaje de confirmación.

Crear una plantilla de perfil de servicio habilitada para vMedia

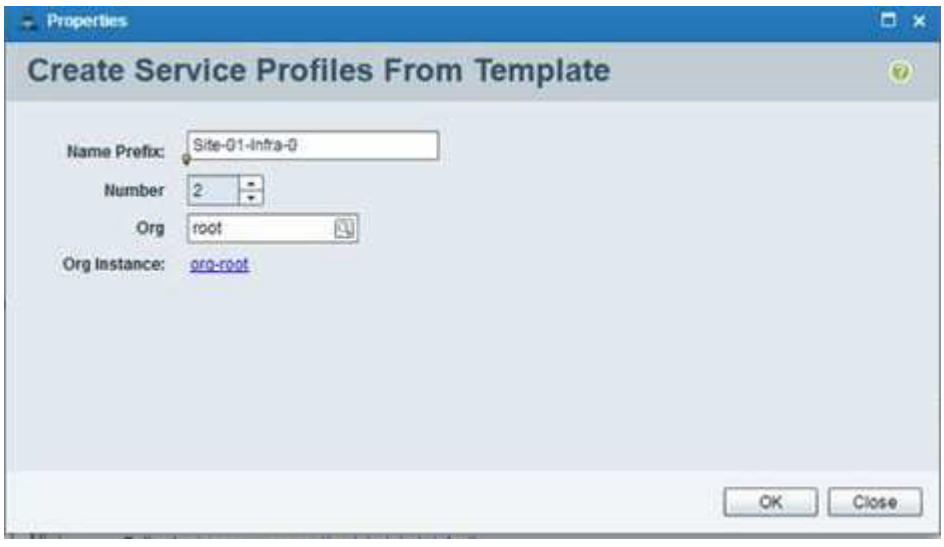
Para crear una plantilla de perfil de servicio con vMedia activado, lleve a cabo los siguientes pasos:

1. Conéctese a UCS Manager y haga clic en servidores a la izquierda.
2. Seleccione Plantillas de perfil de servicio > raíz > plantilla de servicio VM-Host-Infra-iSCSI-A.
3. Haga clic con el botón derecho en VM-Host-Infra-iSCSI-A y seleccione Create a Clone.
4. Asigne un nombre al clon `VM-Host-Infra-iSCSI-A-vM`.
5. Seleccione la VM-Host-infra-iSCSI-A-VM recién creada y seleccione la ficha vMedia Policy a la derecha.
6. Haga clic en Modificar la directiva de vMedia.
7. Seleccione ESXi-6. 7U1-HTTP vMedia Policy y haga clic en Aceptar.
8. Haga clic en OK para confirmar.

Crear perfiles de servicio

Para crear perfiles de servicio a partir de la plantilla de perfil de servicio, lleve a cabo los siguientes pasos:

1. Conéctese a Cisco UCS Manager y haga clic en servidores a la izquierda.
2. Expanda servidores > Plantillas de perfil de servicio > raíz > <name> de plantilla de servicio.
3. En acciones, haga clic en Crear perfil de servicio desde plantilla y compita los siguientes pasos:
   a. Introduzca `Site- 01-Infra-0` como prefijo de nombre.
   b. Introduzca `2` como el número de instancias que se van a crear.
   c. Seleccione root como org.
   d. Haga clic en Aceptar para crear los perfiles de servicio.



4. Haga clic en Aceptar en el mensaje de confirmación.
5. Compruebe que los perfiles de servicio `Site-01-Infra-01` y.. `Site-01-Infra-02` se han creado.

Los perfiles de servicio se asocian automáticamente con los servidores de sus pools de servidores asignados.

Parte de configuración del almacenamiento 2: Arranque de las LUN y los iGroups

Configuración del almacenamiento de arranque de ONTAP

Cree iGroups

Para crear grupos iniciadores (iGroups), complete los pasos siguientes:

1. Ejecute los siguientes comandos desde la conexión SSH del nodo de gestión del clúster:

```
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>
```

Utilice los valores enumerados en la tabla 1 y la tabla 2 para obtener la información de IQN.

2. Para ver los tres iGroups recién creados, ejecute el `igroup show` comando.

Asigne LUN de arranque a iGroups

Para asignar LUN de arranque a iGroups, complete el paso siguiente:

1. Desde la conexión SSH de administración del clúster de almacenamiento, ejecute los siguientes comandos:

```
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
```

Procedimiento de implementación de VMware vSphere 6.7U1

En esta sección, se proporcionan los procedimientos detallados para la instalación de VMware ESXi 6.7U1 en una configuración FlexPod Express. Una vez finalizados los procedimientos, se aprovisionan dos hosts ESXi arrancados.

Existen varios métodos para instalar ESXi en un entorno VMware. Estos procedimientos se centran en cómo utilizar la consola KVM incorporada y las funciones de medios virtuales de Cisco UCS Manager para asignar medios de instalación remotos a servidores individuales y conectarse a sus LUN de arranque.

Descargue la imagen personalizada de Cisco para ESXi 6.7U1

Si no se ha descargado la imagen personalizada de VMware ESXi, complete los siguientes pasos para completar la descarga:

1. Haga clic en el siguiente enlace: VMware vSphere Hypervisor (ESXi) 6.7U1.
2. Necesita un ID de usuario y una contraseña en "vmware.com" para descargar este software.
3. Descargue el `.iso` archivo.

Administrador de Cisco UCS

Cisco UCS IP KVM permite al administrador iniciar la instalación del sistema operativo a través de medios remotos. Es necesario iniciar sesión en el entorno Cisco UCS para ejecutar el KVM de IP.

Para iniciar sesión en el entorno de Cisco UCS, complete los siguientes pasos:

1. Abra un explorador web e introduzca la dirección IP para la dirección del clúster de Cisco UCS. Este paso inicia la aplicación Cisco UCS Manager.
2. Haga clic en el enlace Iniciar UCS Manager en HTML para iniciar la GUI de HTML 5 UCS Manager.
3. Si se le solicita que acepte los certificados de seguridad, acepte según sea necesario.
4. Cuando se le solicite, introduzca `admin` como nombre de usuario e introduzca la contraseña administrativa.
5. Para iniciar sesión en Cisco UCS Manager, haga clic en Iniciar sesión.
6. En el menú principal, haga clic en servidores a la izquierda.
7. Seleccione servidores > Perfiles de servicios > raíz > `VM-Host-Infra-01`.
8. Haga clic con el botón derecho del ratón `VM-Host-Infra-01` Y seleccione KVM Console.
9. Siga las indicaciones para iniciar la consola KVM basada en Java.
10. Seleccione servidores > Perfiles de servicios > raíz > `VM-Host-Infra-02`.
11. Haga clic con el botón derecho del ratón `VM-Host-Infra-02`. Y seleccione KVM Console.
12. Siga las indicaciones para iniciar la consola KVM basada en Java.

Configure la instalación de VMware ESXi

ESXi aloja VM-Host-infra-01 y VM-Host- infra-02

Para preparar el servidor para la instalación del sistema operativo, complete los siguientes pasos en cada host ESXi:

1. En la ventana KVM, haga clic en Medios virtuales.
2. Haga clic en Activar dispositivos virtuales.
3. Si se le solicita que acepte una sesión KVM sin cifrar, acepte según sea necesario.
4. Haga clic en Medios virtuales y seleccione Mapa CD/DVD.
5. Desplácese hasta el archivo de imagen ISO del instalador ESXi y haga clic en Open.
6. Haga clic en asignar dispositivo.
7. Haga clic en la ficha KVM para supervisar el inicio del servidor.

Instalar ESXi

ESXi aloja VM-Host-Infra-01 y VM-Host-Infra-02

Para instalar VMware ESXi en el LUN de inicio iSCSI de los hosts, realice los pasos siguientes en cada host:

1. Inicie el servidor seleccionando Boot Server (servidor de inicio) y haciendo clic en OK (Aceptar). A continuación, vuelva a hacer clic en Aceptar.
2. En el reinicio, la máquina detecta la presencia de los medios de instalación de ESXi. Seleccione el instalador de ESXi en el menú de arranque que aparece.
3. Cuando el instalador haya terminado de cargarse, presione Entrar para continuar con la instalación.
4. Leer y aceptar el contrato de licencia para usuario final (CLUF). Pulse F11 para aceptar y continuar.
5. Seleccione el LUN que se configuró anteriormente como disco de instalación para ESXi y pulse Intro para continuar con la instalación.
6. Seleccione la distribución de teclado adecuada y pulse Intro.
7. Introduzca y confirme la contraseña de root y pulse Intro.
8. El instalador emite una advertencia de que el disco seleccionado se volverá a particionar. Pulse F11 para continuar con la instalación.
9. Una vez finalizada la instalación, seleccione la pestaña Virtual Media y borre la Marca P junto al medio de instalación de ESXi. Haga clic en Yes.

> Debe anular la asignación de la imagen de instalación de ESXi para asegurarse de que el servidor se reinicie en ESXi y no en el instalador.

10. Una vez finalizada la instalación, pulse Intro para reiniciar el servidor.
11. En Cisco UCS Manager, enlace el perfil de servicio actual a la plantilla de perfil de servicio que no es vMedia para evitar el montaje de la instalación de ESXi iso a través de HTTP.

Configure las redes de gestión para los hosts ESXi

Es necesario añadir una red de gestión para cada host VMware para gestionar el host. Para añadir una red de gestión para los hosts VMware, complete los siguientes pasos en cada host ESXi:

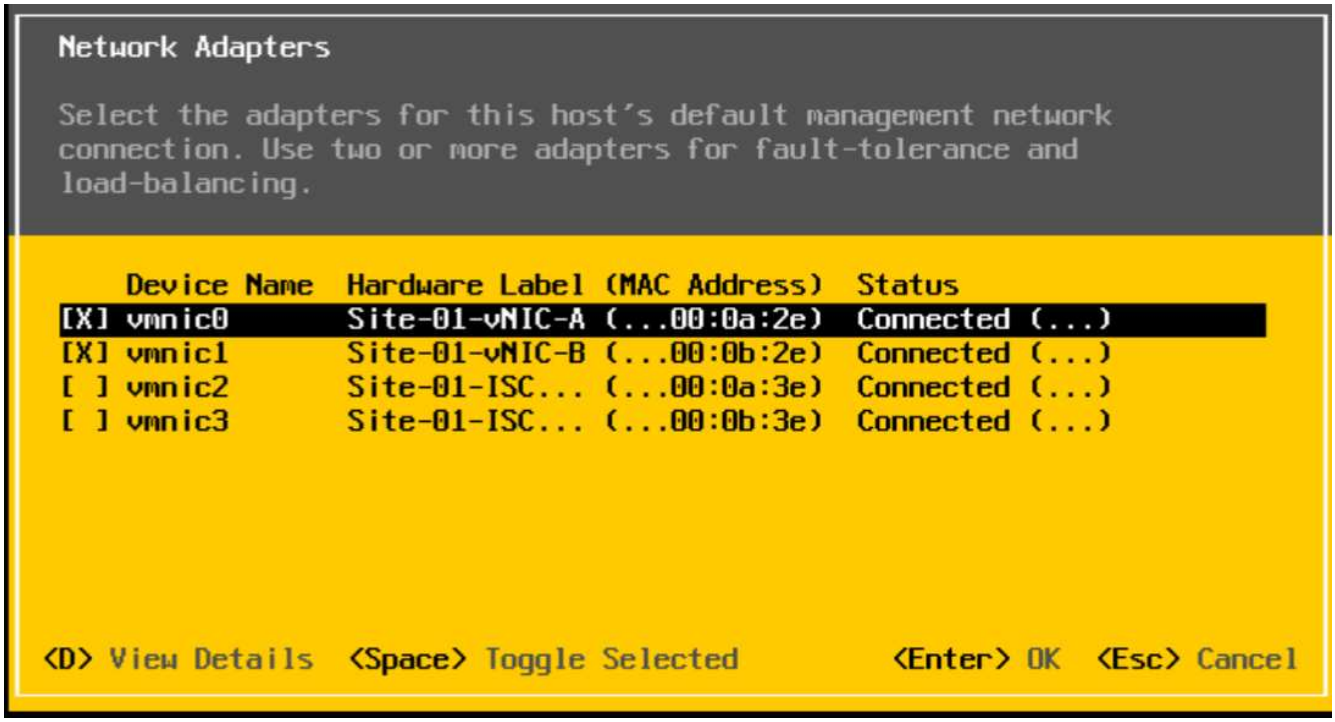
ESXi Host VM-Host-Infra-01 y VM-Host-Infra-02

Para configurar cada host ESXi con acceso a la red de gestión, complete los pasos siguientes:

1. Cuando el servidor haya terminado de reiniciarse, pulse F2 para personalizar el sistema.
2. Inicie sesión como `root`, Introduzca la contraseña correspondiente y pulse Intro para iniciar sesión.
3. Seleccione Opciones de solución de problemas y pulse Intro.
4. Seleccione Enable ESXi Shell y pulse Enter.
5. Seleccione Habilitar SSH y pulse Intro.
6. Pulse Esc para salir del menú Opciones de solución de problemas.
7. Seleccione la opción Configure Management Network y pulse Intro.
8. Seleccione Adaptadores de red y pulse Intro.
9. Compruebe que los números del campo etiqueta de hardware coinciden con los números del campo

Nombre del dispositivo.

10. Pulse Intro.



11. Seleccione la opción VLAN (opcional) y pulse Intro.
12. Introduzca el `<ib-mgmt-vlan-id>` Y pulse Intro.
13. Seleccione IPv4 Configuration y presione Enter.
14. Seleccione la opción establecer la dirección IPv4 estática y la configuración de red mediante la barra espaciadora.
15. Introduzca la dirección IP para gestionar el primer host ESXi.
16. Introduzca la máscara de subred para el primer host ESXi.
17. Introduzca la puerta de enlace predeterminada para el primer host ESXi.
18. Pulse Intro para aceptar los cambios en la configuración de IP.
19. Seleccione la opción DNS Configuration y presione Enter.

> Dado que la dirección IP se asigna manualmente, la información DNS también debe introducirse manualmente.

20. Introduzca la dirección IP del servidor DNS primario.
21. Optional: Introduzca la dirección IP del servidor DNS secundario.
22. Introduzca el FQDN para el primer host ESXi.
23. Pulse Intro para aceptar los cambios en la configuración de DNS.
24. Pulse Esc para salir del menú Configurar red de gestión.
25. Seleccione Test Management Network (Red de administración de pruebas) para comprobar que la red de gestión está configurada correctamente y pulse Intro.
26. Pulse Intro para ejecutar la prueba, pulse Intro de nuevo una vez que haya finalizado la prueba, revise el

entorno si hay un fallo.

27. Seleccione de nuevo Configurar red de administración y pulse Intro.
28. Seleccione la opción IPv6 Configuration y presione Enter.
29. Mediante la barra espaciadora, seleccione Disable IPv6 (Reiniciar requerido) y pulse Intro.
30. Pulse Esc para salir del submenú Configurar red de administración.
31. Pulse y para confirmar los cambios y reiniciar el host ESXi.

Restablecer la dirección MAC del puerto de VMkernel de host VMware ESXi vmk0 (opcional)

ESXi Host VM-Host-Infra-01 y VM-Host-Infra-02

De forma predeterminada, la dirección MAC del puerto de VMkernel de gestión vmk0 es la misma que la dirección MAC del puerto Ethernet en el que se coloca. Si el LUN de arranque del host ESXi se reasigna a un servidor diferente con direcciones MAC diferentes, se producirá un conflicto de dirección MAC porque vmk0 conserva la dirección MAC asignada a menos que se restablezca la configuración del sistema ESXi. Para restablecer la dirección MAC de vmk0 a una dirección MAC asignada por VMware aleatoria, complete los siguientes pasos:

1. En la pantalla principal del menú de la consola ESXi, pulse Ctrl-Alt-F1 para acceder a la interfaz de línea de comandos de VMware Console. En el KVM UCSM, Ctrl-Alt-F1 aparece en la lista de macros estáticas.
2. Inicie sesión como root.
3. Tipo `esxcfg-vmknic –l` para obtener una lista detallada de la interfaz vmk0. Vmk0 debe formar parte del grupo de puertos de la red de gestión. Anote la dirección IP y la máscara de red de vmk0.
4. Para eliminar vmk0, introduzca el siguiente comando:

```
esxcfg-vmknic –d “Management Network”
```

5. Para volver a añadir vmk0 con una dirección MAC aleatoria, introduzca el siguiente comando:

```
esxcfg-vmknic –a –i <vmk0-ip> -n <vmk0-netmask> “Management Network””.
```

6. Verifique que vmk0 se ha añadido de nuevo con una dirección MAC aleatoria

```
esxcfg-vmknic –l
```

7. Tipo `exit` para cerrar la sesión en la interfaz de línea de comandos.
8. Pulse Ctrl-Alt-F2 para volver a la interfaz de menús de la consola ESXi.

Inicie sesión en hosts VMware ESXi con el cliente host de VMware

Host ESXi VM-host-Infra-01

Para iniciar sesión en el host ESXi de VM-Host-Infra-01 con el cliente host de VMware, complete los siguientes pasos:

1. Abra un explorador Web en la estación de trabajo de gestión y desplácese hasta `VM-Host-Infra-01` Dirección IP de administración.
2. Haga clic en Open the VMware Host Client.
3. Introduzca `root` para el nombre de usuario.
4. Introduzca la contraseña de raíz.
5. Haga clic en Iniciar sesión para conectarse.
6. Repita este proceso para iniciar sesión en `VM-Host-Infra-02` en una pestaña o ventana del navegador por separado.

Instalación de controladores de VMware para la tarjeta de interfaz virtual (VIC) de Cisco

Descargue y extraiga el paquete sin conexión del controlador VIC de VMware a la estación de trabajo de gestión:

- Controlador Nenic versión 1.0.25.0

ESXi aloja VM-Host-Infra-01 y VM-Host-Infra-02

Para instalar los controladores VIC de VMware en el host de ESXi VM-Host-Infra-01 y VM-Host-Infra-02, lleve a cabo los siguientes pasos:

1. En cada cliente host, seleccione almacenamiento.
2. Haga clic con el botón derecho del ratón en datastor1 y seleccione examinar.
3. En el explorador Datastore, haga clic en Upload.
4. Desplácese hasta la ubicación guardada de los controladores VIC descargados y seleccione VMW-ESX-6.7.0-nenic-1.0.25.0-offline_Bundle-11271332.zip.
5. En el explorador Datastore, haga clic en Upload.
6. Haga clic en Abrir para cargar el archivo en datos1.
7. Asegúrese de que el archivo se haya cargado en ambos hosts ESXi.
8. Coloque cada host en modo de mantenimiento si no lo está ya.
9. Conéctese a cada host ESXi a través de ssh desde una conexión de shell o un terminal de putty.
10. Inicie sesión como root con la contraseña root.
11. Ejecute los siguientes comandos en cada host:

```
esxcli software vib update -d /vmfs/volumes/datastore1/VMW-ESX-6.7.0-
nenic-1.0.25.0-offline_bundle-11271332.zip
reboot
```

12. Inicie sesión en el cliente host en cada host una vez que se haya completado el reinicio y salga del modo de mantenimiento.

Configure los puertos de VMkernel y el conmutador virtual

ESXi Host VM-Host-Infra-01 y VM-Host-Infra-02

Para configurar los puertos de VMkernel y los switches virtuales en los hosts ESXi, complete los pasos siguientes:

1. En Host Client, seleccione Networking en la izquierda.
2. En el panel central, seleccione la ficha conmutadores virtuales.
3. Seleccione vSwitch0.
4. Seleccione Editar configuración.
5. Cambie el MTU a 9000.
6. Amplíe NIC Teaming.
7. En la sección Orden de conmutación por error, seleccione vmnic1 y haga clic en Marcar activo.
8. Verifique que vmnic1 ahora tenga el estado Active.
9. Haga clic en Guardar.
10. Seleccione Networking a la izquierda.
11. En el panel central, seleccione la ficha conmutadores virtuales.
12. Seleccione iScsiBootvSwitch.
13. Seleccione Editar configuración.
14. Cambie el MTU a 9000
15. Haga clic en Guardar.
16. Seleccione la ficha NIC de VMkernel.
17. Seleccione vmk1 iScsiBootPG.
18. Seleccione Editar configuración.
19. Cambie el MTU a 9000.
20. Expanda Configuración de IPv4 y cambie la dirección IP a una dirección fuera de UCS iSCSI-IP-Pool-A.

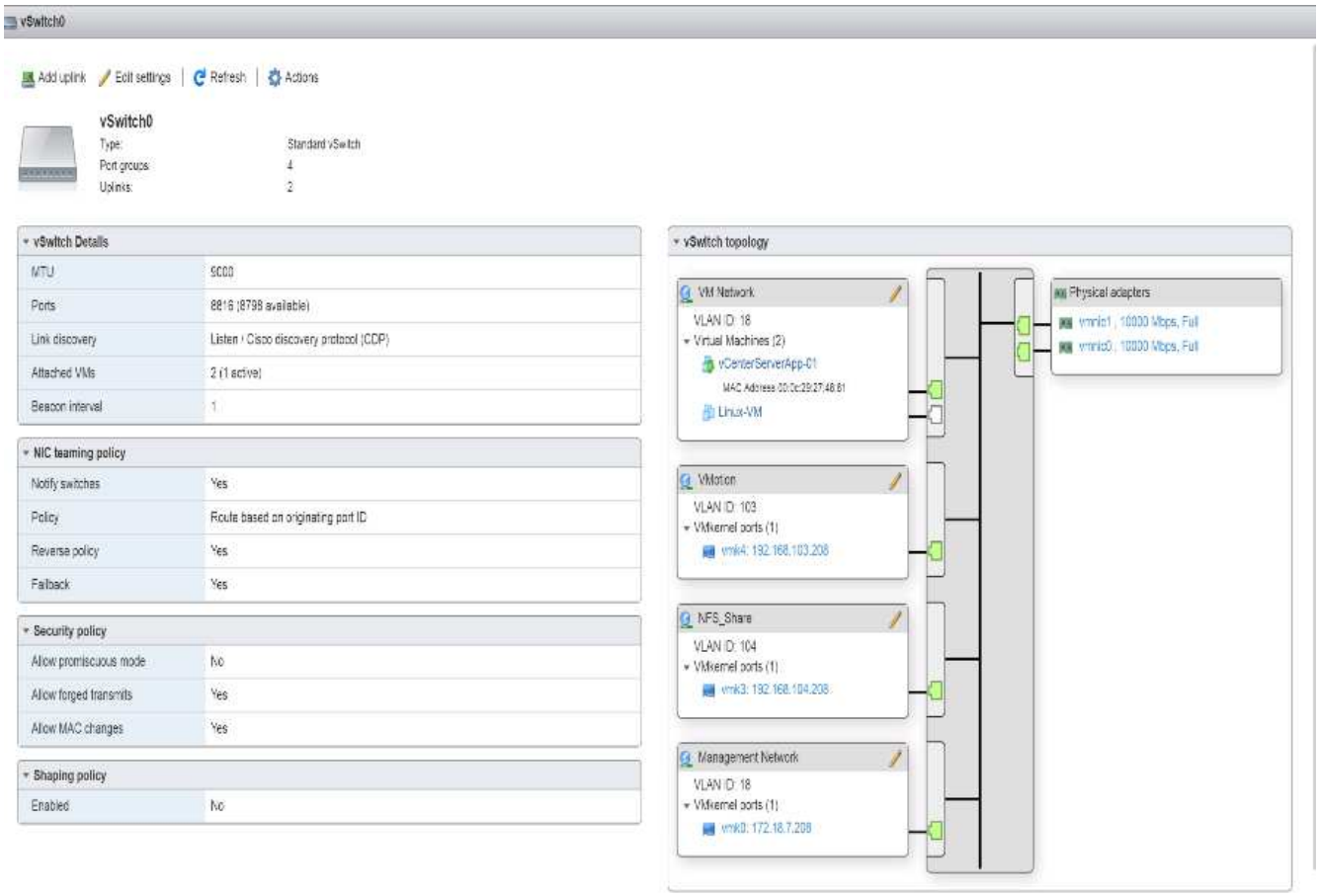
> Para evitar conflictos de direcciones IP si las direcciones IP Pool de Cisco UCS se deben volver a asignar, se recomienda utilizar direcciones IP diferentes en la misma subred para los puertos de VMkernel de iSCSI.

21. Haga clic en Guardar.
22. Seleccione la ficha switches virtuales.
23. Seleccione el conmutador virtual estándar Add.
24. Escriba un nombre de `iScsciBootvSwitch-B` Para el nombre de vSwitch.
25. Establezca la MTU en 9000.
26. Seleccione vmnic3 en el menú desplegable Uplink 1.
27. Haga clic en Añadir.
28. En el panel central, seleccione la ficha NIC de VMkernel.
29. Seleccione Agregar NIC de VMkernel
30. Especifique un nombre de grupo de puertos nuevo de iScsiBootPG-B.
31. Seleccione iScciBootvSwitch-B para el conmutador virtual.
32. Establezca la MTU en 9000. No introduzca un ID de VLAN.

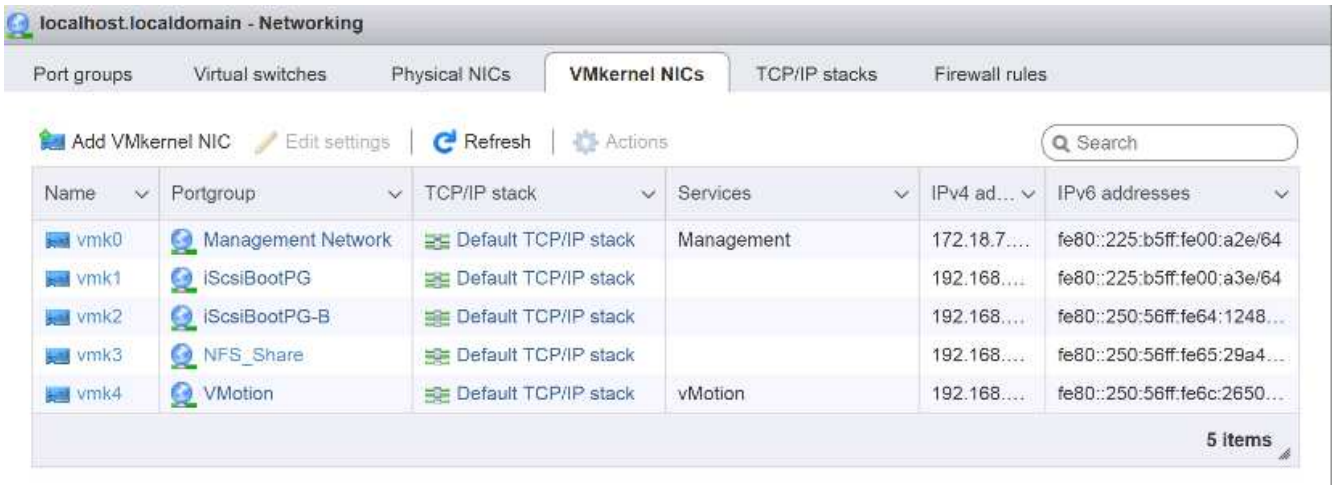
33. Seleccione Static (estático) para la configuración IPv4 y expanda la opción para proporcionar la dirección y la máscara de subred dentro de la configuración.

> Para evitar conflictos de direcciones IP, si las direcciones IP Pool de Cisco UCS se deben volver a asignar, se recomienda utilizar direcciones IP diferentes en la misma subred para los puertos VMkernel de iSCSI.

34. Haga clic en Crear.
35. A la izquierda, seleccione Networking (redes) y, a continuación, seleccione la ficha Port groups (grupos de puertos).
36. En el panel central, haga clic con el botón derecho del ratón en VM Network y seleccione Remove.
37. Haga clic en Quitar para completar la eliminación del grupo de puertos.
38. En el panel central, seleccione Agregar grupo de puertos.
39. Asigne el nombre al grupo de puertos Management Network e introduzca `<ib-mgmt-vlan-id>` En el campo VLAN ID, y asegúrese de que esté seleccionado Virtual Switch vSwitch0.
40. Haga clic en Agregar para finalizar las ediciones de la red IB-MGMT.
41. En la parte superior, seleccione la ficha NIC de VMkernel.
42. Haga clic en Add VMkernel NIC.
43. Para el grupo de puertos nuevo, introduzca VMotion.
44. En el conmutador virtual, seleccione vSwitch0 seleccionado.
45. Introduzca `<vmotion-vlan-id>` Para el ID de VLAN.
46. Cambie el MTU a 9000.
47. Seleccione Configuración IPv4 estática y expanda Configuración de IPv4.
48. Introduzca la dirección IP y la máscara de red del host ESXi.
49. Seleccione la pila vMotion TCP/IP.
50. Seleccione vMotion en Services.
51. Haga clic en Crear.
52. Haga clic en Add VMkernel NIC.
53. Para New Port group, introduzca NFS_Share.
54. En el conmutador virtual, seleccione vSwitch0 seleccionado.
55. Introduzca `<infra-nfs-vlan-id>` Para el ID de VLAN
56. Cambie el MTU a 9000.
57. Seleccione Configuración IPv4 estática y expanda Configuración de IPv4.
58. Introduzca la dirección IP y la máscara de red de NFS de la infraestructura del host ESXi.
59. No seleccione ninguno de los Servicios.
60. Haga clic en Crear.
61. Seleccione la pestaña Switches virtuales y seleccione vSwitch0. Las propiedades de los NIC de VMkernel vSwitch0 deberían ser similares al ejemplo siguiente:



62. Seleccione la ficha NIC de VMkernel para confirmar los adaptadores virtuales configurados. Los adaptadores enumerados deben ser similares al ejemplo siguiente:



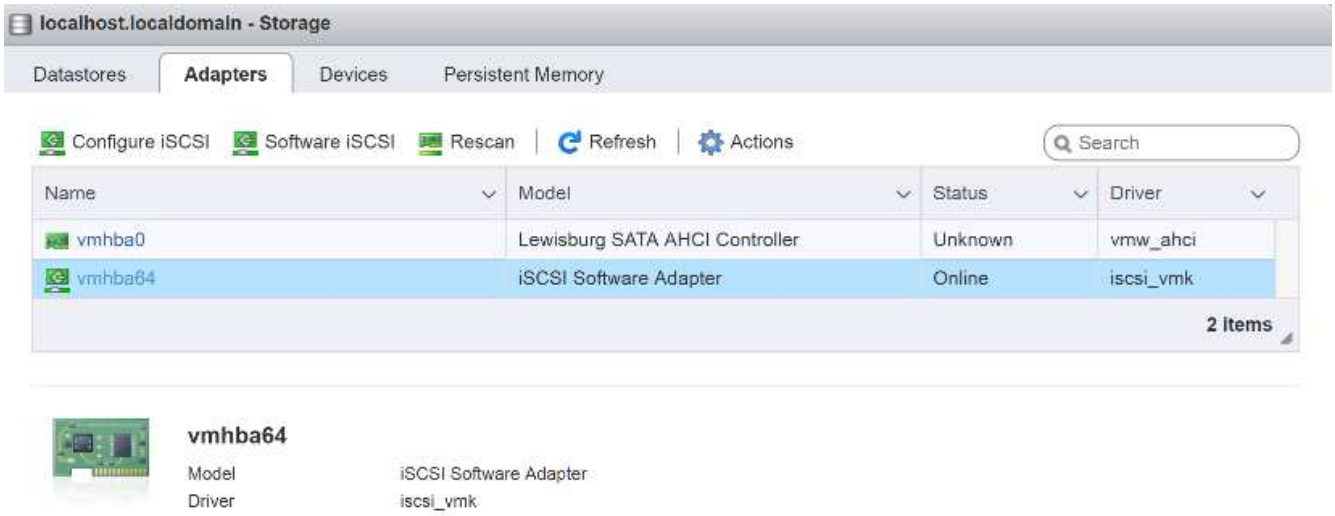
Configure la multivía iSCSI

ESXi aloja VM-Host-Infra-01 y VM-Host-Infra-02

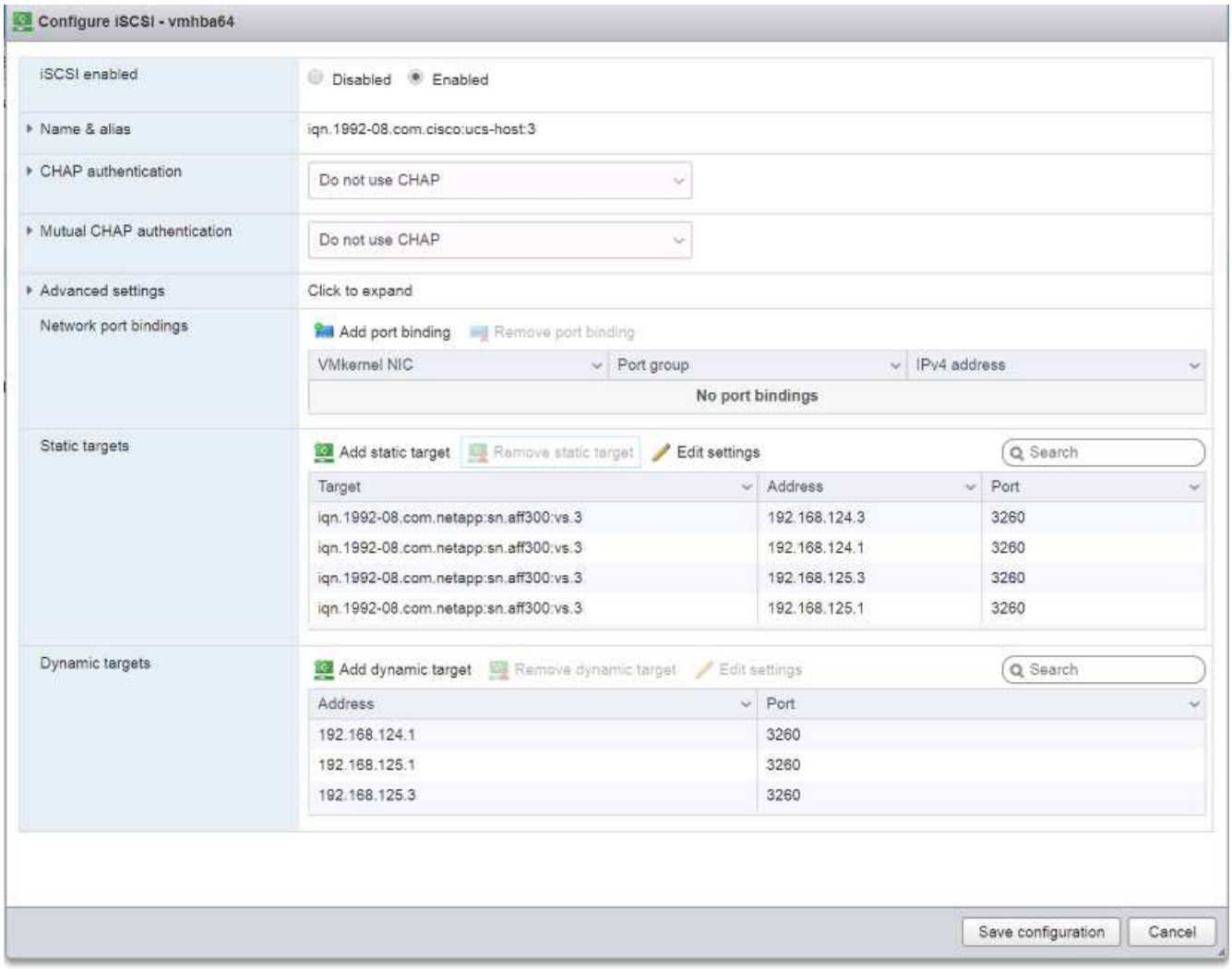
Para configurar la función multivía de iSCSI en el host ESXi VM-Host-Infra-01 y VM-Host-Infra-02, complete los siguientes pasos:

1. En cada cliente host, seleccione almacenamiento a la izquierda.

2. En el panel central, haga clic en Adaptadores.
3. Seleccione el adaptador de software iSCSI y haga clic en Configurar iSCSI.



4. En Destinos dinámicos, haga clic en Agregar destino dinámico.
5. Introduzca la dirección IP de `iSCSI_lif01a`.
6. Repita esto para introducir estas direcciones IP: `iscsi_lif01b`, `iscsi_lif02a`, y. `iscsi_lif02b`.
7. Haga clic en Save Configuration.



Para obtener todo el `iscsi_lif` Las direcciones IP, inicie sesión en la interfaz de gestión del clúster de almacenamiento de NetApp y ejecute el `network interface show` comando.

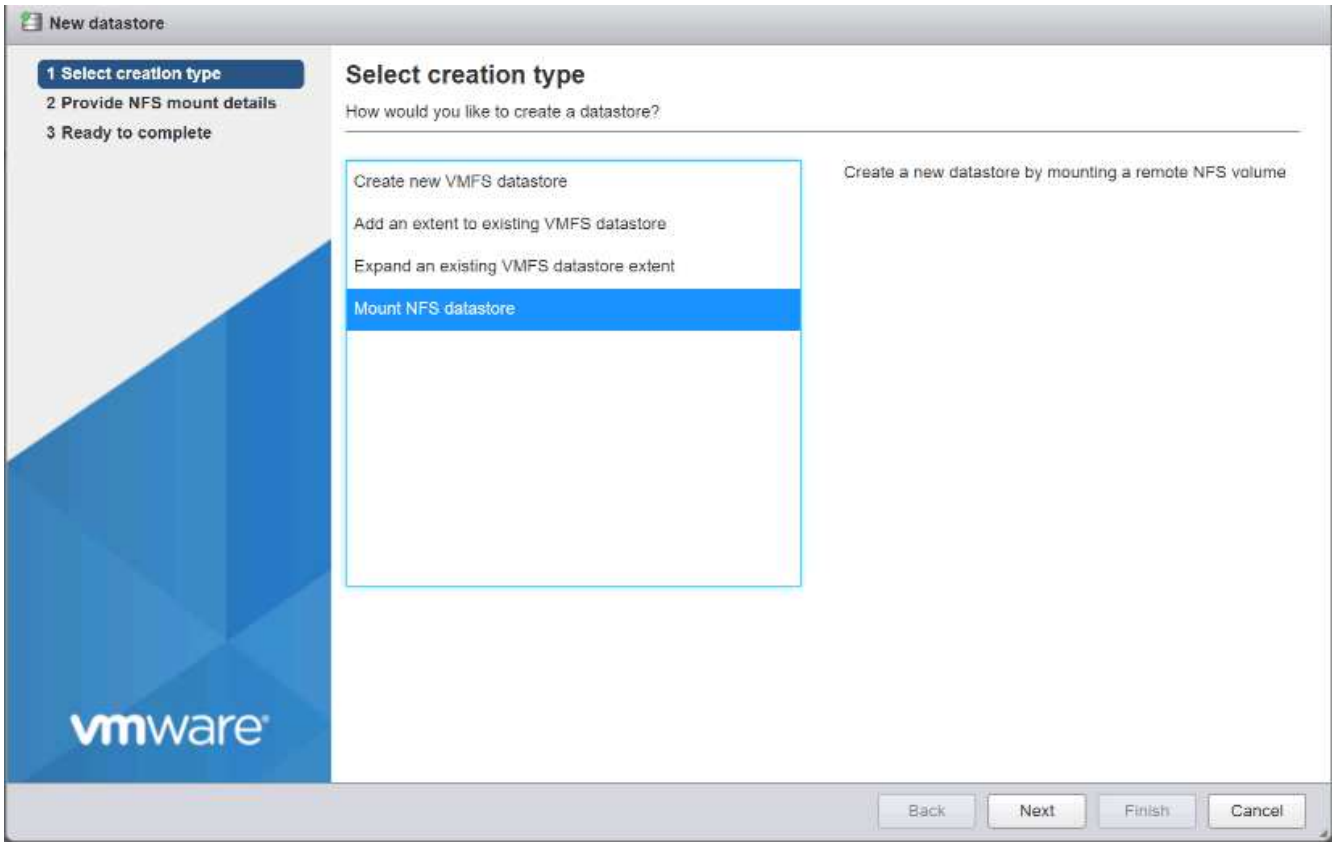
> El host vuelve a buscar automáticamente el adaptador de almacenamiento y los destinos se agregan a los destinos estáticos.

Montar los almacenes de datos necesarios

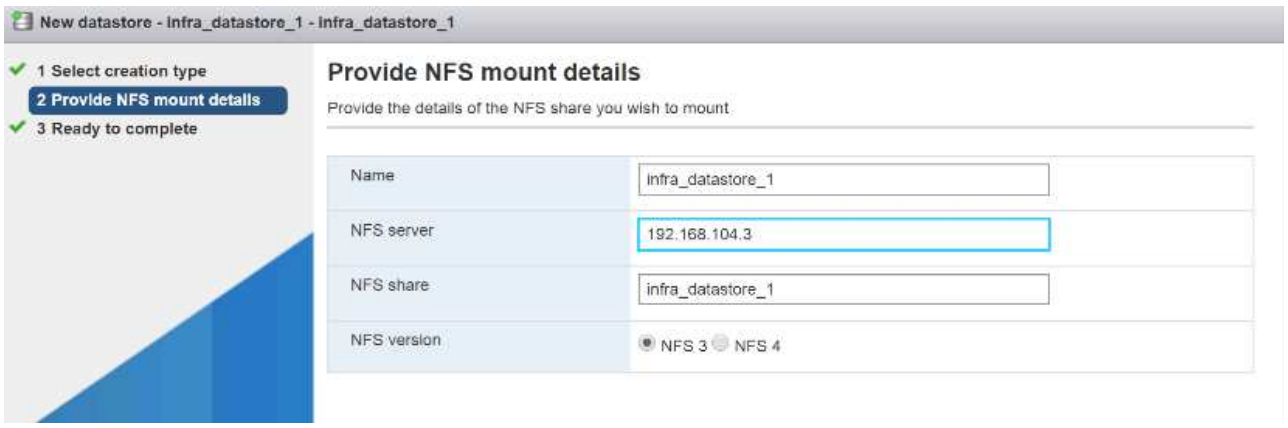
ESXi aloja VM-Host-Infra-01 y VM-Host-Infra-02

Para montar los almacenes de datos necesarios, complete los siguientes pasos en cada host ESXi:

1. En Host Client, seleccione Storage a la izquierda.
2. En el panel central, seleccione datastores.
3. En el panel central, seleccione New Datastore para añadir un almacén de datos nuevo.
4. En el cuadro de diálogo New datastore, seleccione Mount NFS datastore y haga clic en Next.



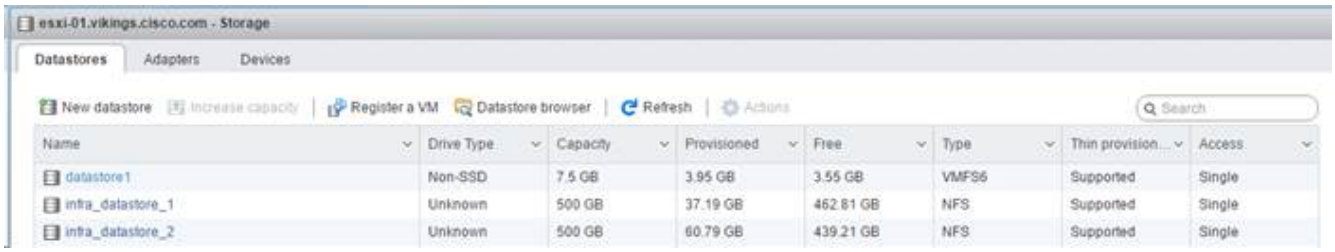
5. En la página Provide NFS Mount Details, complete los siguientes pasos:
   a. Introduzca `infra_datastore_1` para el nombre del almacén de datos.
   b. Introduzca la dirección IP para el `nfs_lif01_a` LIF para el servidor NFS.
   c. Introduzca `/infra_datastore_1` Para el recurso compartido NFS.
   d. Deje la versión de NFS configurada en NFS 3.
   e. Haga clic en Siguiente.



6. Haga clic en Finalizar. El almacén de datos ahora debe aparecer en la lista de almacenes de datos.
7. En el panel central, seleccione New Datastore para añadir un almacén de datos nuevo.
8. En el cuadro de diálogo New Datastore, seleccione Mount NFS Datastore y haga clic en Next.
9. En la página Provide NFS Mount Details, complete los siguientes pasos:

a. Introduzca `infra_datastore_2` para el nombre del almacén de datos.
b. Introduzca la dirección IP para el `nfs_lif02_a` LIF para el servidor NFS.
c. Introduzca `/infra_datastore_2` Para el recurso compartido NFS.
d. Deje la versión de NFS configurada en NFS 3.
e. Haga clic en Siguiente.

10. Haga clic en Finalizar. El almacén de datos ahora debe aparecer en la lista de almacenes de datos.



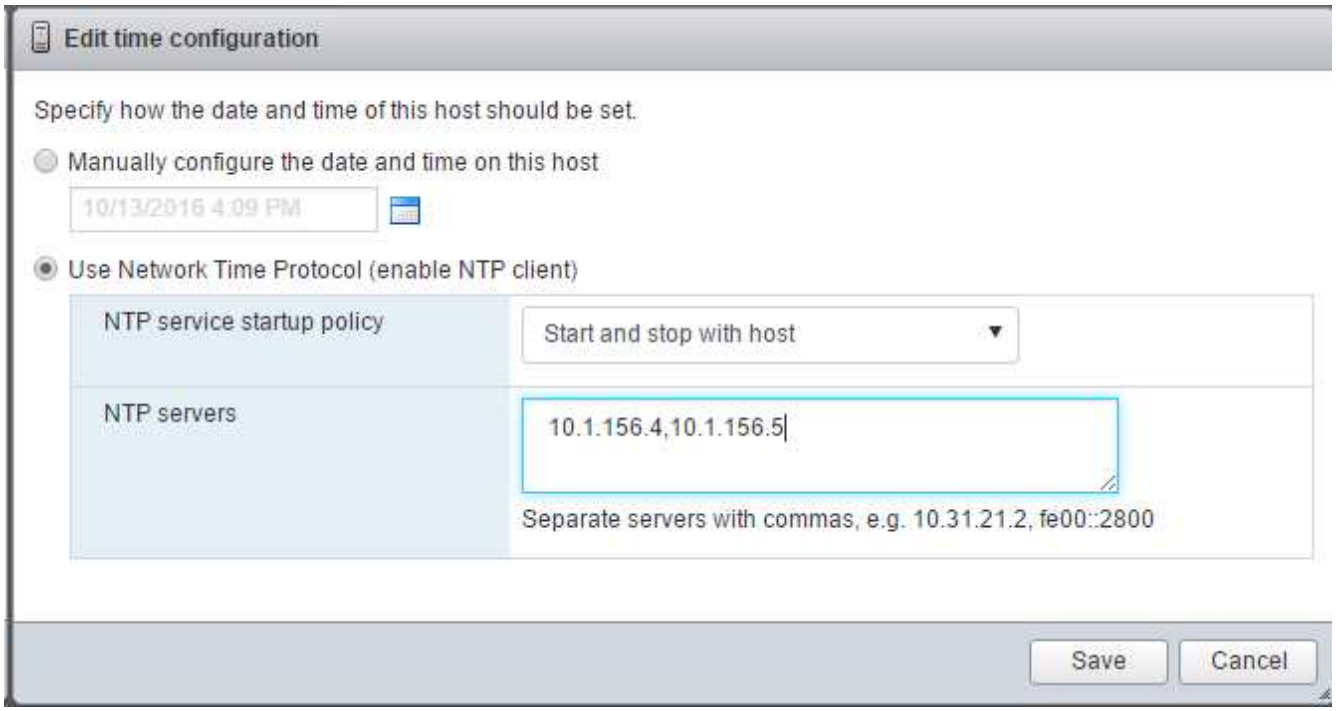
11. Montar ambos almacenes de datos en ambos hosts ESXi.

Configure NTP en hosts ESXi

ESXi aloja VM-Host-Infra-01 y VM-Host-Infra-02

Para configurar NTP en los hosts ESXi, complete los siguientes pasos en cada host:

1. En Host Client, seleccione Manage a la izquierda.
2. En el panel central, seleccione la ficha Hora y fecha.
3. Haga clic en Editar configuración.
4. Asegúrese de que esté seleccionada la opción Use Network Time Protocol (habilitar cliente NTP).
5. Use el menú desplegable para seleccionar Inicio y Detener con Host.
6. Introduzca las dos direcciones NTP del switch Nexus en el cuadro servidores NTP separados por una coma.



7. Haga clic en Guardar para guardar los cambios de configuración.
8. Seleccione Actions > NTP service > Start.
9. Compruebe que el servicio NTP está en ejecución y que el reloj está ahora ajustado aproximadamente a la hora correcta

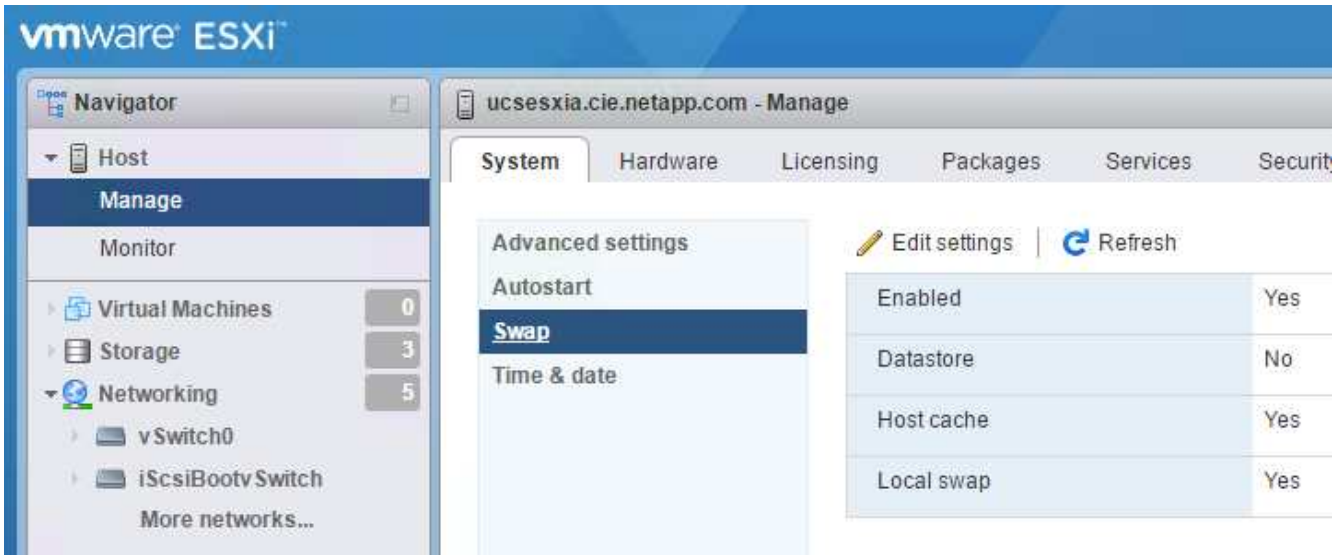
El tiempo del servidor NTP puede variar ligeramente respecto del tiempo del host.

Configurar el intercambio del host ESXi

ESXi aloja VM-Host-Infra-01 y VM-Host-Infra-02

Para configurar el intercambio del host en los hosts ESXi, siga estos pasos en cada host:

1. Haga clic en Administrar en el panel de navegación de la izquierda. Seleccione sistema en el panel derecho y haga clic en intercambiar.



2. Haga clic en Editar configuración. Seleccione `infra_swap` En las opciones del Datastore.

3. Haga clic en Guardar.

Instale el plugin de NetApp NFS 1.1.2 para VMware VAAI

Para instalar el complemento NFS de NetApp 1. 1.2 para VMware VAAI, realice los siguientes pasos.

1. Descargue el plugin de NetApp NFS para VMware VAAI:
   a. Vaya a la "Página de descarga del software NetApp".
   b. Desplácese hacia abajo y haga clic en NetApp NFS Plug-in for VMware VAAI.
   c. Seleccione la plataforma ESXi.
   d. Descargue el paquete sin conexión (.zip) o el paquete en línea (.vib) del plugin más reciente.
2. El complemento NFS de NetApp para VAAI de VMware está pendiente para la cualificación de IMT con ONTAP 9.5; los detalles de interoperabilidad se publicarán en el próximamente en el IMT de NetApp.
3. Instale el plugin en el host ESXi mediante la CLI ESX.
4. Reinicie el host ESXI.

Instale VMware vCenter Server 6.7

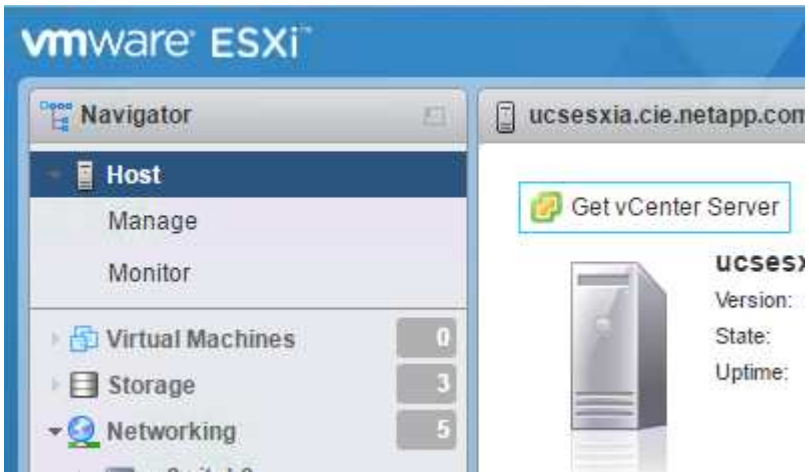
En esta sección, se proporcionan los procedimientos detallados para instalar VMware vCenter Server 6.7 en una configuración exprés de FlexPod.

FlexPod Express utiliza el dispositivo de VMware vCenter Server (VCSA).

Instale el dispositivo VMware vCenter Server

Para instalar VCSA, lleve a cabo los siguientes pasos:

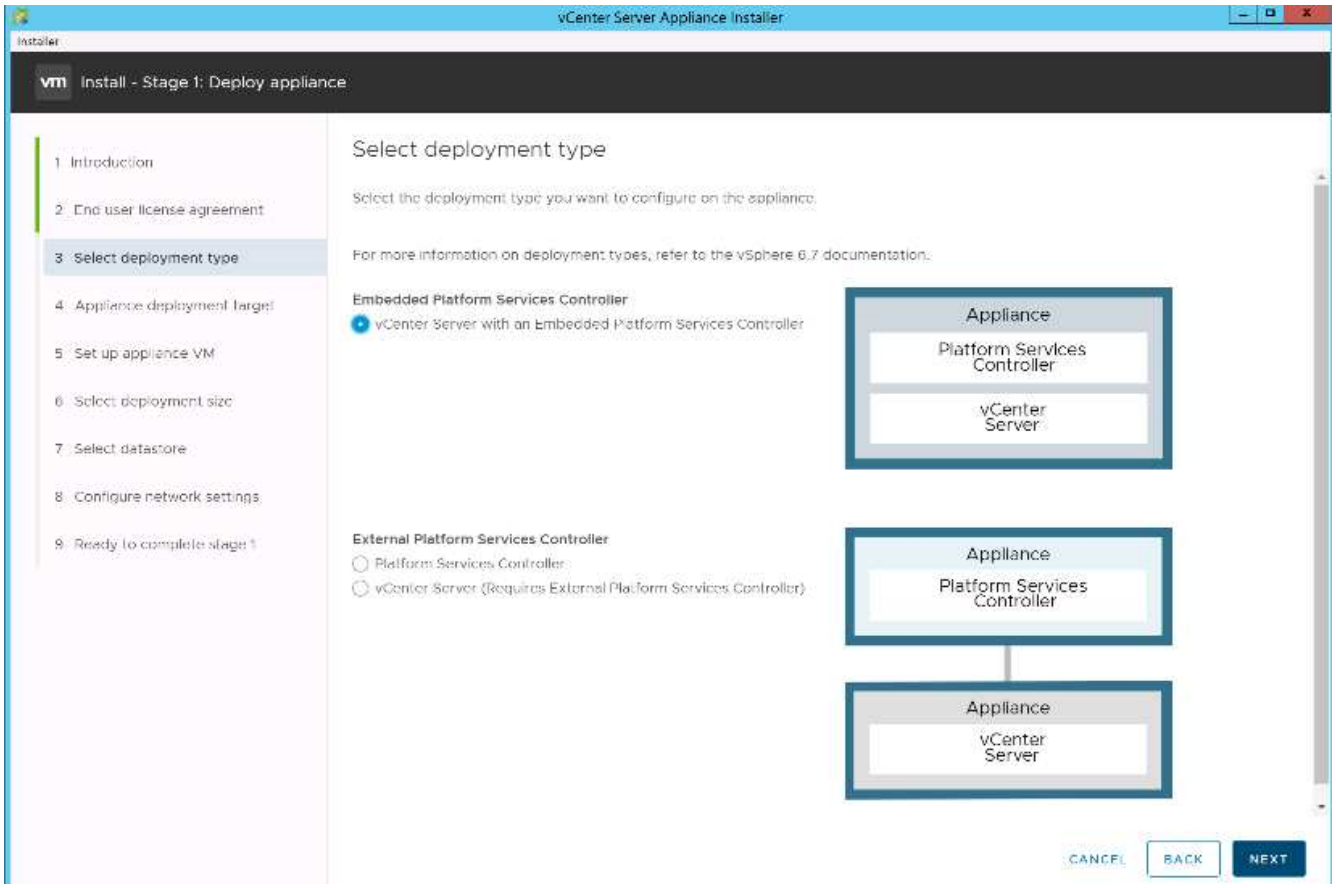
1. Descargue el VCSA. Acceda al enlace de descarga haciendo clic en el icono Get vCenter Server cuando gestione el host ESXi.



2. Descargue el VCSA desde el sitio de VMware.

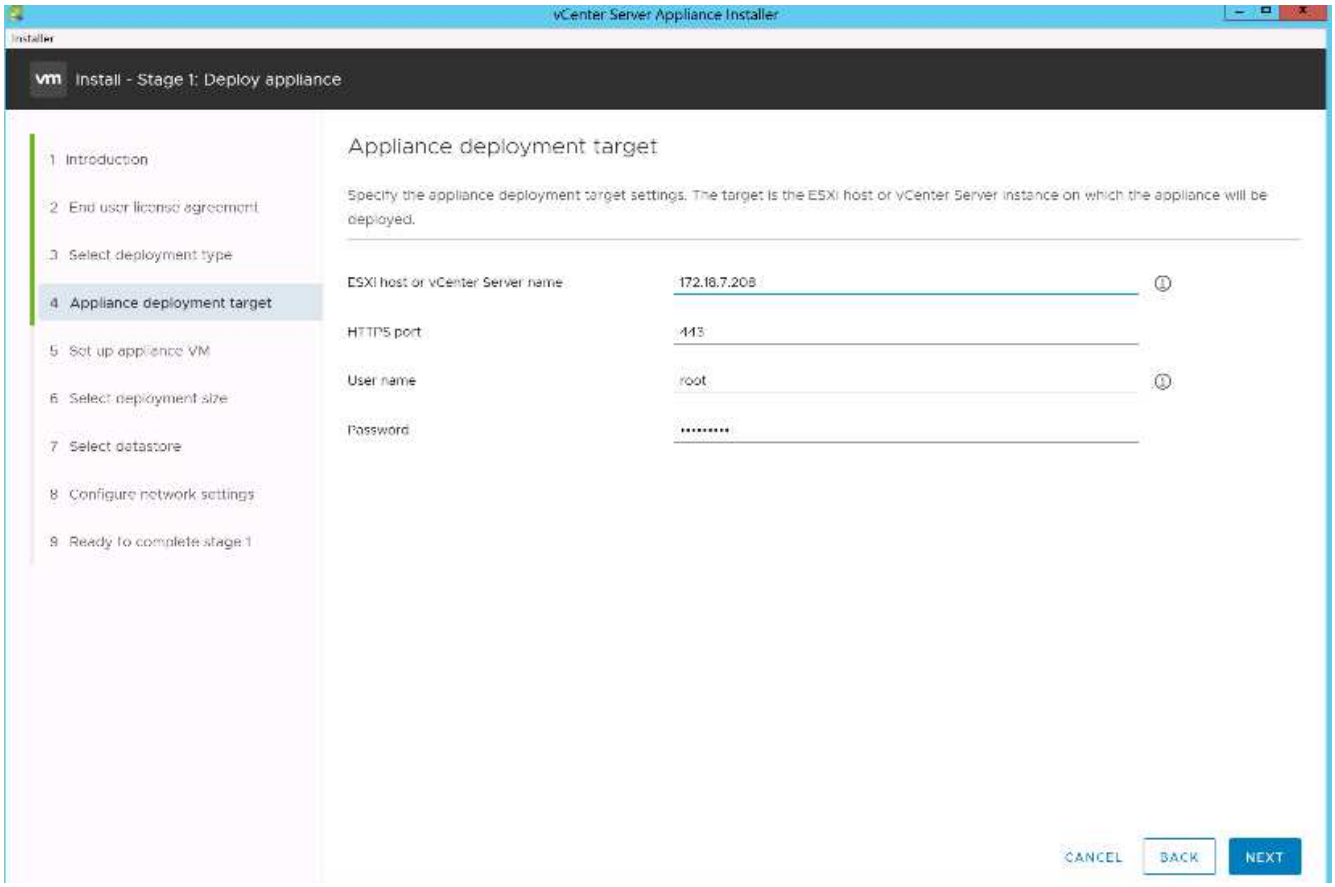
Aunque se admite la instalación de Microsoft Windows vCenter Server, VMware recomienda VCSA para las nuevas implementaciones.

3. Monte la imagen ISO.
4. Desplácese hasta la `vcsa-ui-installer` > `win32` directorio. Haga doble clic `installer.exe`.
5. Haga clic en instalar.
6. Haga clic en Siguiente en la página Introducción.
7. Acepte el contrato de licencia para usuario final.
8. Seleccione Embedded Platform Services Controller (controladora de servicios de plataforma integrada) como tipo de implementación.

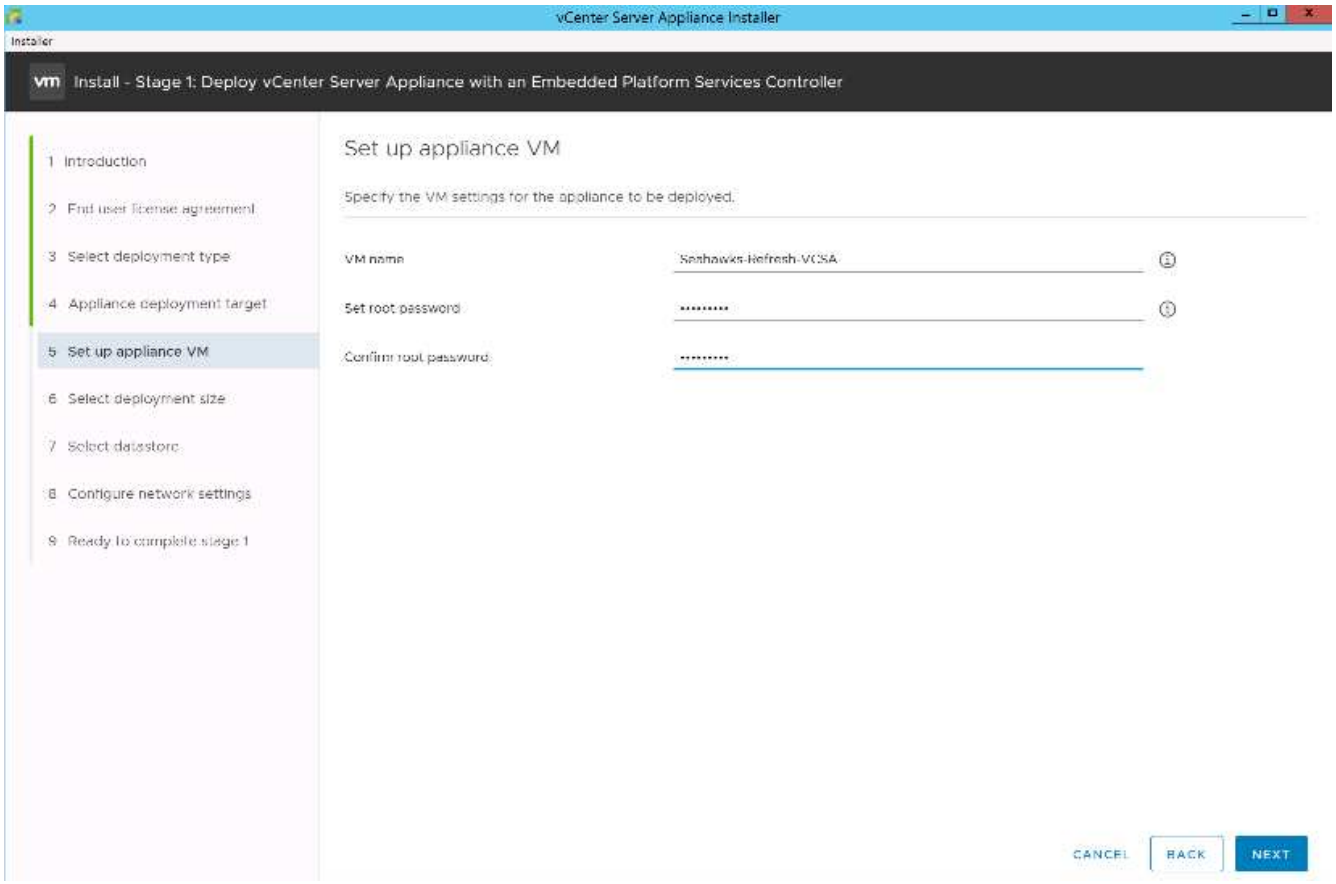


Si es necesario, también admite la puesta en marcha de la controladora de servicios de plataforma externa como parte de la solución FlexPod Express.

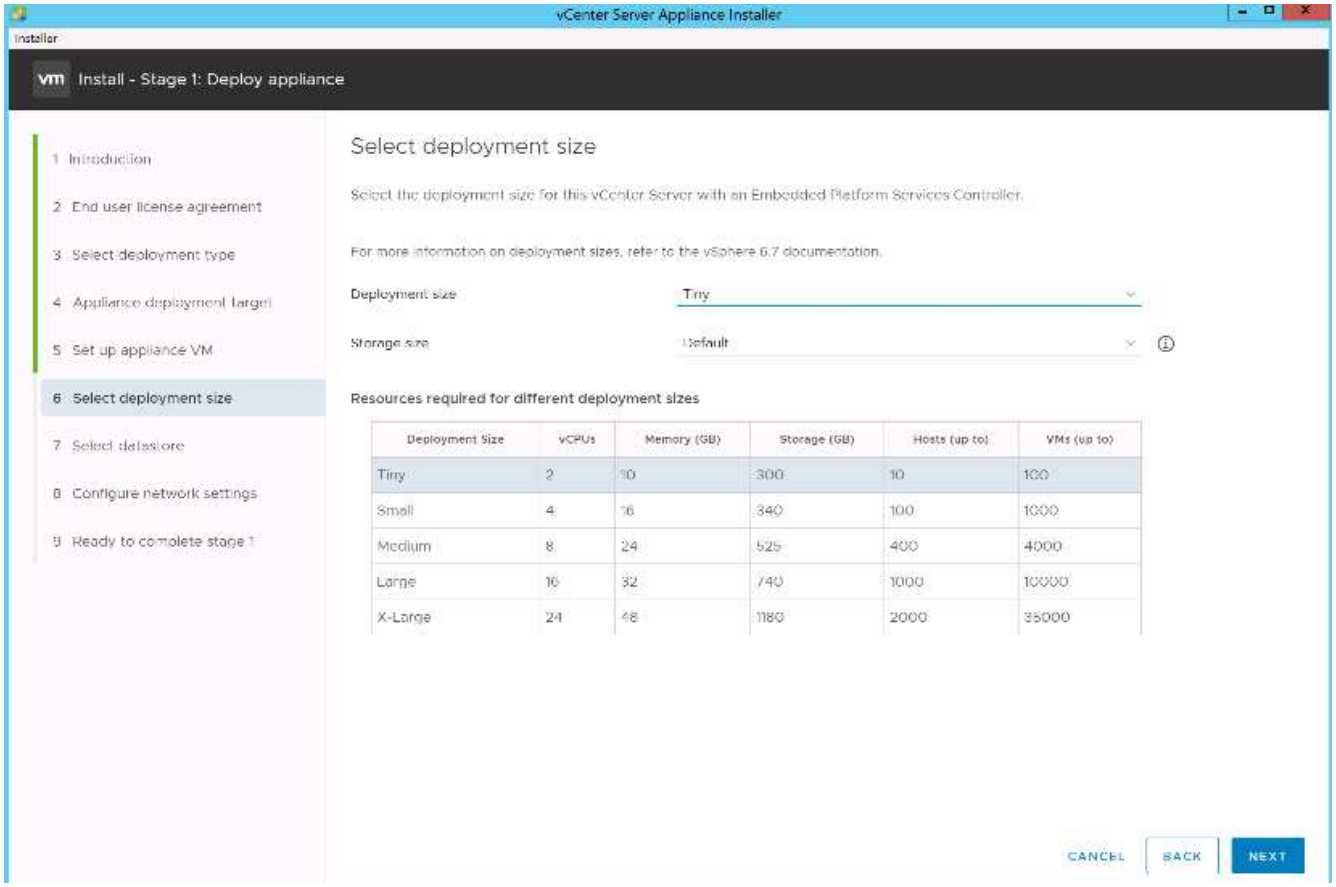
9. En la página Appliance Deployment Target, introduzca la dirección IP de un host ESXi que haya implementado, el nombre de usuario raíz y la contraseña raíz. Haga clic en Siguiente.



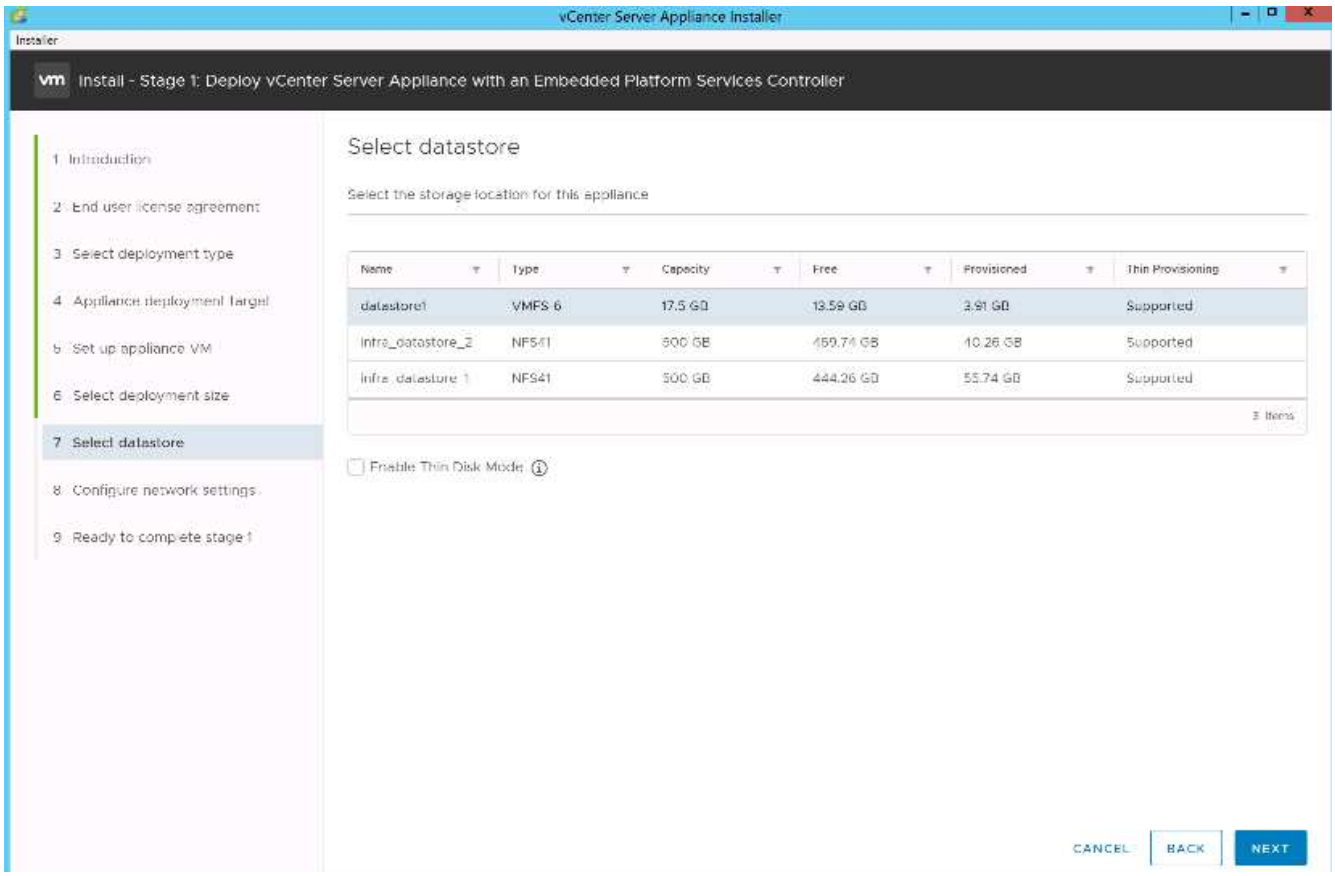
10. Para establecer el equipo virtual, introduzca VCSA como nombre de equipo virtual y la contraseña de raíz que desea utilizar para el VCSA. Haga clic en Siguiente.



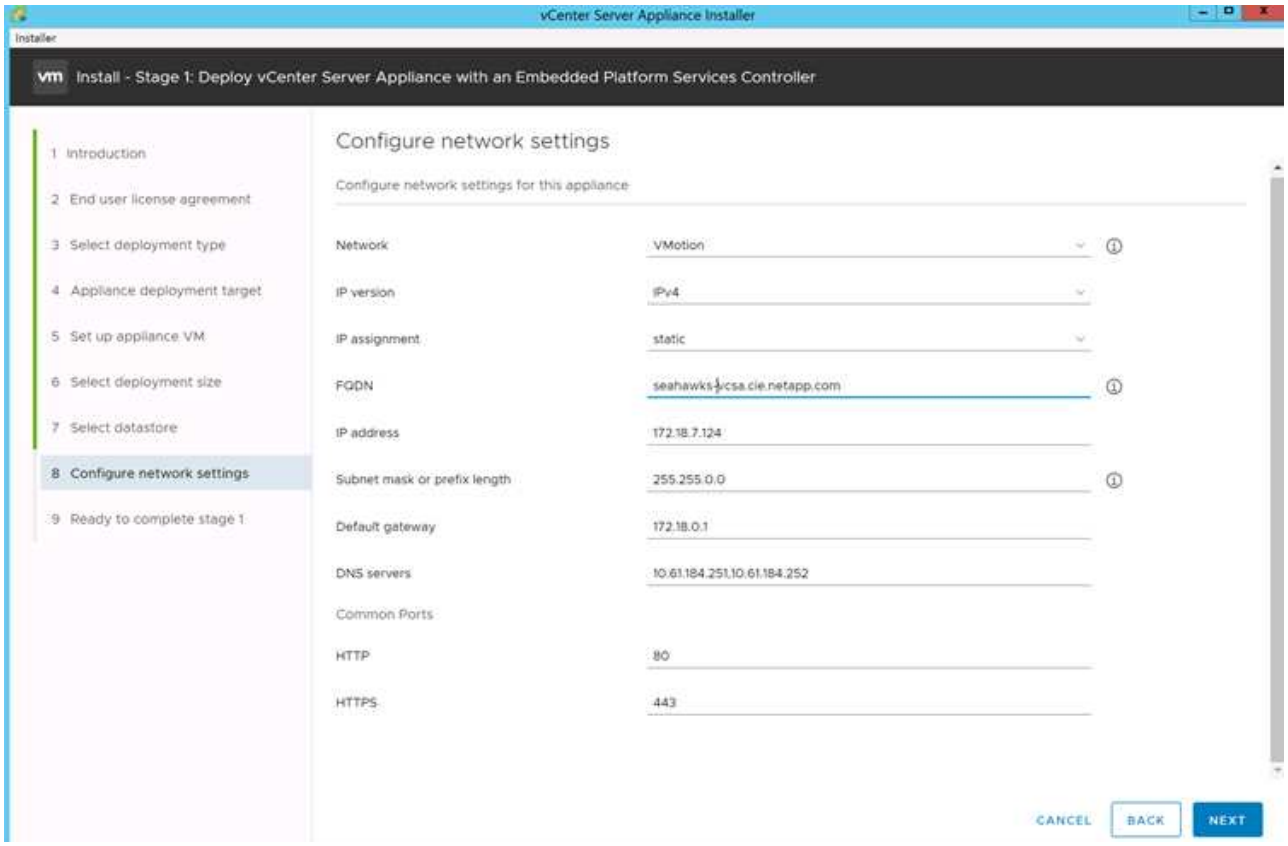
11. Seleccione el tamaño de puesta en marcha que mejor se adapte a su entorno. Haga clic en Siguiente.



12. Seleccione la `infra_datastore_1` almacén de datos. Haga clic en Siguiente.



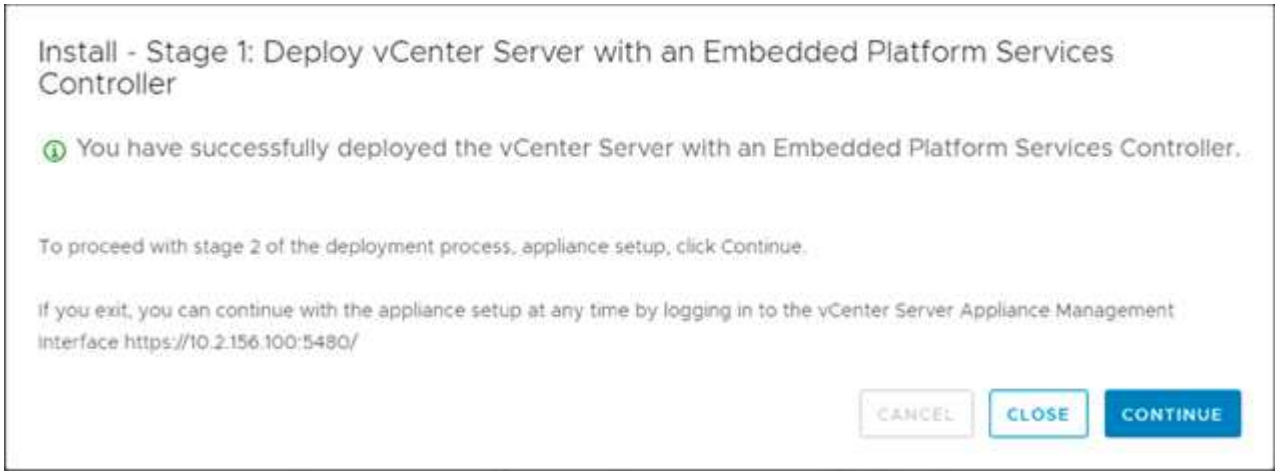
13. Introduzca la siguiente información en la página Configure Network Settings y haga clic en Next.
    a. Seleccione MGMT-Network como su red.
    b. Introduzca el FQDN o IP que se va a utilizar para la VCSA.
    c. Introduzca la dirección IP que se utilizará.
    d. Introduzca la máscara de subred que desea utilizar.
    e. Introduzca la pasarela predeterminada.
    f. Introduzca el servidor DNS.



14. En la página Ready to Complete Stage 1, compruebe que los ajustes introducidos son correctos. Haga clic en Finalizar.

    La VCSA se instala ahora. Este proceso tarda varios minutos.

15. Una vez completada la fase 1, aparece un mensaje que indica que se ha completado. Haga clic en continuar para iniciar la configuración de la fase 2.



16. En la página Introducción de fase 2, haga clic en Siguiente.
17. Introduzca `<<var_ntp_id>>` Para la dirección del servidor NTP. Puede introducir varias direcciones IP de NTP.

    Si planea utilizar la alta disponibilidad de vCenter Server, asegúrese de que el acceso SSH esté habilitado.

18. Configure el nombre de dominio, la contraseña y el nombre del sitio de SSO. Haga clic en Siguiente.

    Registre estos valores para su referencia, especialmente si se desvía de la `vsphere.local` nombre de dominio.

19. Únase al programa de experiencia del cliente de VMware si lo desea. Haga clic en Siguiente.
20. Vea el resumen de la configuración. Haga clic en Finalizar o utilice el botón Atrás para editar la configuración.
21. Aparece un mensaje que indica que no puede pausar o detener la instalación para que se complete después de que se haya iniciado. Haga clic en OK para continuar.

    La configuración del dispositivo continúa. Esto tarda varios minutos.

    Aparece un mensaje que indica que la configuración se ha realizado correctamente.

    Los enlaces que el instalador proporciona para acceder a vCenter Server pueden hacer clic.

Configure VMware vCenter Server 6.7 y el clustering de vSphere

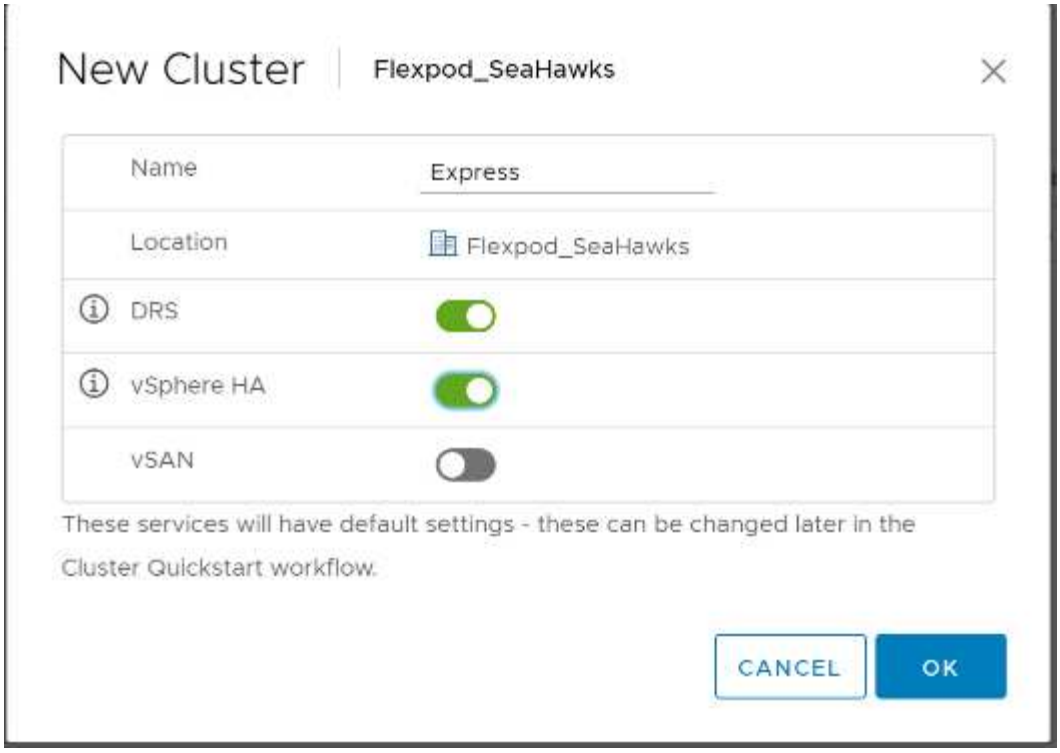
Para configurar la agrupación en clústeres de VMware vCenter Server 6.7 y vSphere, complete los pasos siguientes:

1. Desplácese hasta https://<<FQDN or IP of vCenter>>/vsphere-client/.
2. Haga clic en Launch vSphere Client.
3. Inicie sesión con el nombre de usuario administrator@vsphere.loc/ y la contraseña SSO que introdujo durante el proceso de configuración de VCSA.
4. Haga clic con el botón derecho en el nombre de vCenter y seleccione New Datacenter.
5. Introduzca un nombre para el centro de datos y haga clic en Aceptar.

Crear clúster vSphere.

Para crear un clúster de vSphere, complete los siguientes pasos:

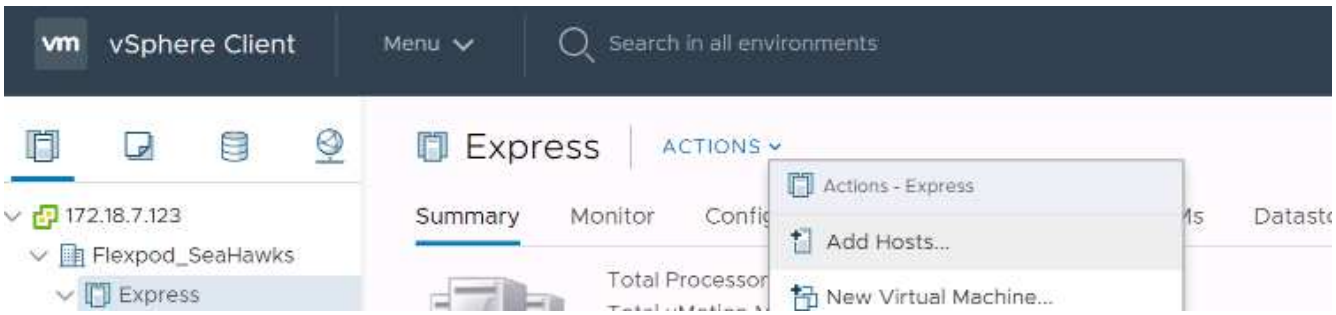
1. Haga clic con el botón derecho en el centro de datos recién creado y seleccione New Cluster.
2. Escriba un nombre para el clúster.
3. Seleccione y habilite las opciones de DRS y vSphere ha.
4. Haga clic en Aceptar.



Agregue hosts ESXi al Cluster

Para añadir hosts ESXi al clúster, complete los siguientes pasos:

1. Seleccione Add Host en el menú Actions del clúster.



2. Para añadir un host ESXi al clúster, complete los siguientes pasos:
   a. Introduzca la dirección IP o el FQDN del host. Haga clic en Siguiente.
   b. Introduzca el nombre de usuario raíz y la contraseña. Haga clic en Siguiente.
   c. Haga clic en Sí para reemplazar el certificado del host por un certificado firmado por el servidor de certificados VMware.
   d. Haga clic en Siguiente en la página Resumen de host.
   e. Haga clic en el icono verde + para añadir una licencia al host de vSphere.

      Este paso se puede completar más adelante si se desea.

   f. Haga clic en Siguiente para desactivar el modo de bloqueo.
   g. Haga clic en Next en la página de ubicación de la máquina virtual.

h. Revise la página Listo para completar. Utilice el botón Atrás para realizar cualquier cambio o seleccione Finalizar.

3. Repita los pasos 1 y 2 para el host Cisco UCS B.

   Debe completar este proceso para los hosts adicionales que se agreguen a la configuración exprés de FlexPod.

Configure coredump en hosts ESXi

Configuración de colector ESXi para hosts arrancados con iSCSI

Los hosts ESXi que se inician con iSCSI mediante el iniciador del software iSCSI de VMware se deben configurar para hacer volcados de memoria al colector ESXi que forma parte de vCenter. Dump Collector no está habilitado de forma predeterminada en vCenter Appliance. Este procedimiento se debe ejecutar al final de la sección de puesta en marcha de vCenter. Para configurar ESXi Dump Collector, siga estos pasos:

1. Inicie sesión en vSphere Web Client como administrator@vsphere.local y seleccione Home.
2. En el panel central, haga clic en Configuración del sistema.
3. En el panel izquierdo, seleccione Servicios.
4. En Services, haga clic en VMware vSphere ESXi Dump Collector.
5. En el panel central, haga clic en el icono verde de inicio para iniciar el servicio.
6. En el menú acciones, haga clic en Editar tipo de inicio.
7. Seleccione automático.
8. Haga clic en Aceptar.
9. Conéctese a cada host ESXi usando ssh como raíz.
10. Ejecute los siguientes comandos:

```
esxcli system coredump network set –v vmk0 –j <vcenter-ip>
esxcli system coredump network set –e true
esxcli system coredump network check
```

El mensaje `Verified the configured netdump server is running` aparece después de ejecutar el comando final.

Este proceso debe completarse para cualquier host adicional que se añada a FlexPod Express.

Conclusión

FlexPod Express proporciona una solución sencilla y efectiva, ya que proporciona un diseño validado que utiliza componentes líderes del sector. Al escalar agregando componentes adicionales, FlexPod Express puede adaptarse según las necesidades específicas del negocio. FlexPod Express se diseñó teniendo en cuenta a las pequeñas y medianas empresas, oficinas remotas y otras empresas que precisan soluciones dedicadas.

Información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- Arquitectura validada de NetApp: 1130 FlexPod Express con VMware vSphere 6.7U1 y NetApp AFF A220 con IP directamente vinculada=basado en Diseño NVA de almacenamiento

  "https://www.netapp.com/us/media/nva-1130-design.pdf"

- Centro de documentación para sistemas AFF y FAS

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

- Centro de documentación de ONTAP 9

  "http://docs.netapp.com/ontap-9/index.jsp"

- Documentación de productos de NetApp

  "https://docs.netapp.com"

FlexPod Express para VMware vSphere 7,0 con Cisco UCS Mini y NetApp AFF/FAS - NVA - Deployment

Jyh-shing Chen, NetApp

La solución FlexPod Express para VMware vSphere 7,0 con Cisco UCS Mini y la solución AFF/FAS de NetApp aprovecha Cisco UCS Mini con servidores blade B200 M5, interconexiones de estructura en chasis Cisco UCS 6324, switches Cisco Nexus 31108PC-V u otros switches conformes a la normativa y el par de alta disponibilidad de controladoras de la serie FAS2700, AFF A220, C190 o el par de alta disponibilidad de controladoras de la serie, Que ejecuta el software para la gestión de datos ONTAP 9,7 de NetApp. Este documento de puesta en marcha de Arquitectura verificada de NetApp (NVA) contiene los pasos detallados necesarios para configurar los componentes de la infraestructura y para implementar VMware vSphere 7,0 y las herramientas asociadas para crear una infraestructura virtual basada en FlexPod Express de alta fiabilidad y alta disponibilidad.

"FlexPod Express para VMware vSphere 7,0 con Cisco UCS Mini y NetApp AFF/FAS - NVA - Deployment"