Procedimientos de implantación

FlexPod

NetApp
March 25, 2024

Tabla de contenidos

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.

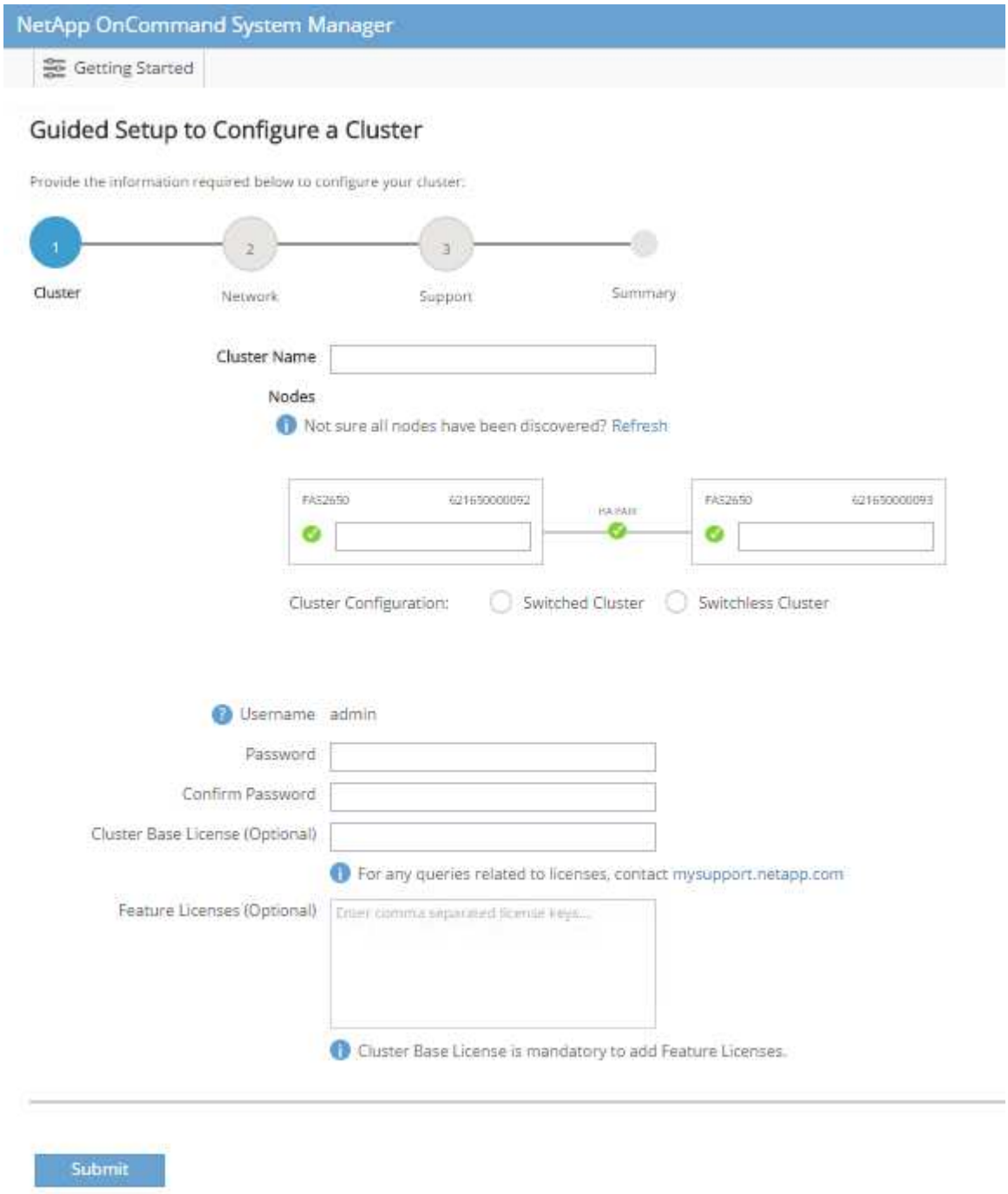
1. Siga las instrucciones para configurar el nodo A.

```
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.

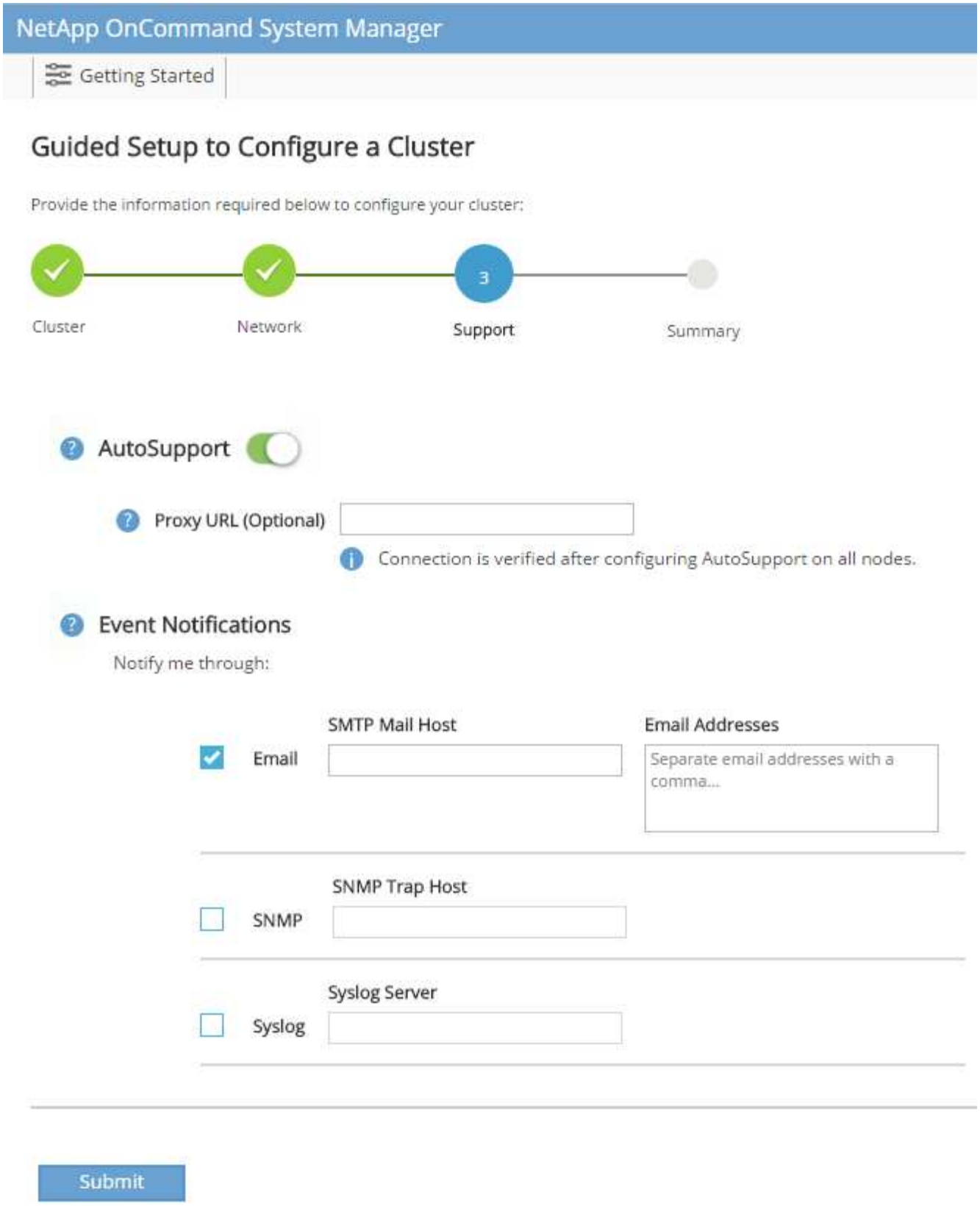
6. Ve un mensaje de estado que indica que el clúster se está creando. Este mensaje de estado cambia por varios Estados. Este proceso tarda varios minutos.
7. Configure la red.
   a. Anule la selección de la opción intervalo de direcciones IP.
   b. Introduzca `<<var_clustermgmt_ip>>` En el campo Cluster 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.

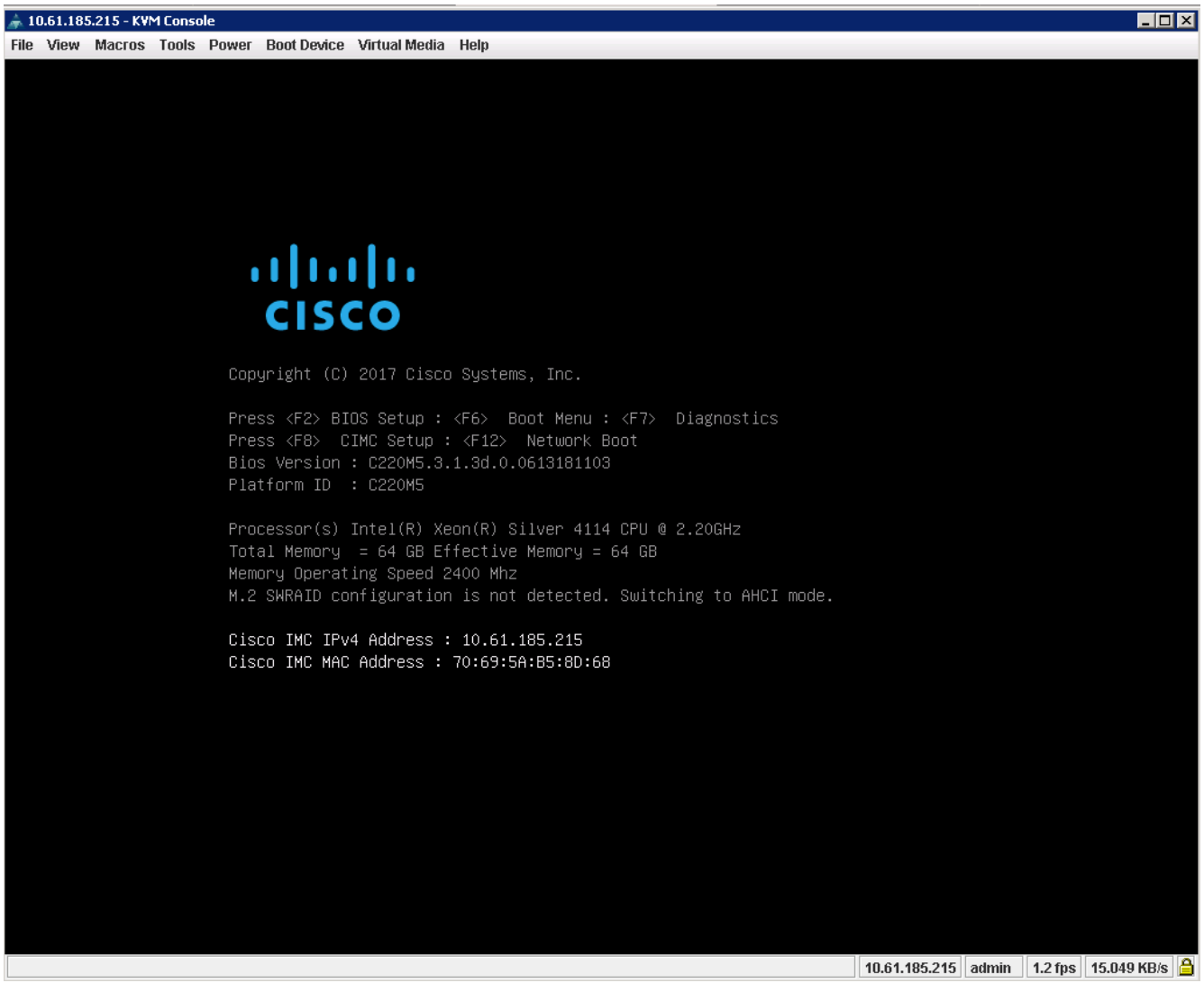
En la siguiente tabla se enumera la información necesaria para configurar CIMC para cada servidor independiente Cisco UCS C-Series.

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

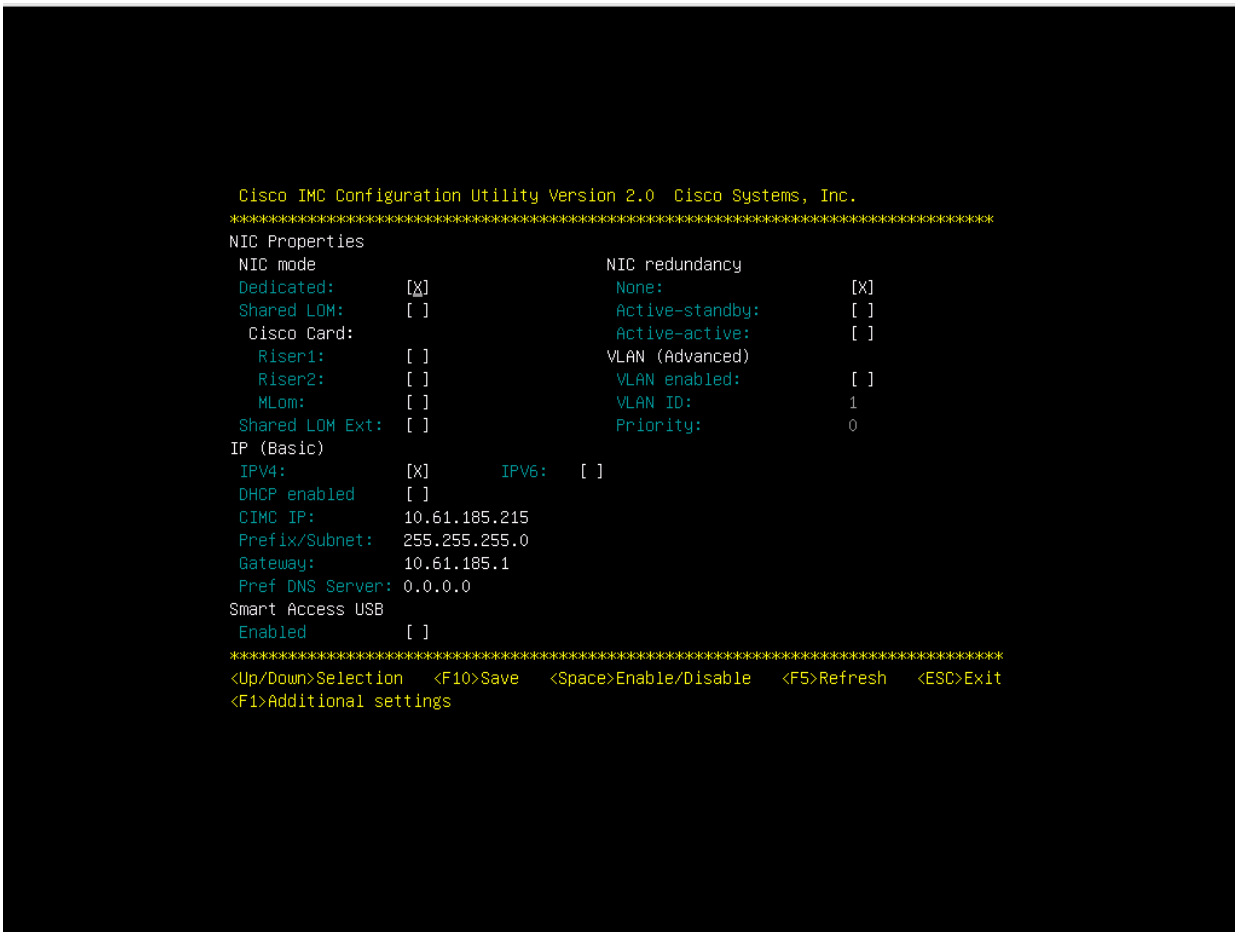
La versión de CIMC utilizada en esta validación es CIMC 3.1.3(g).

Todos los servidores

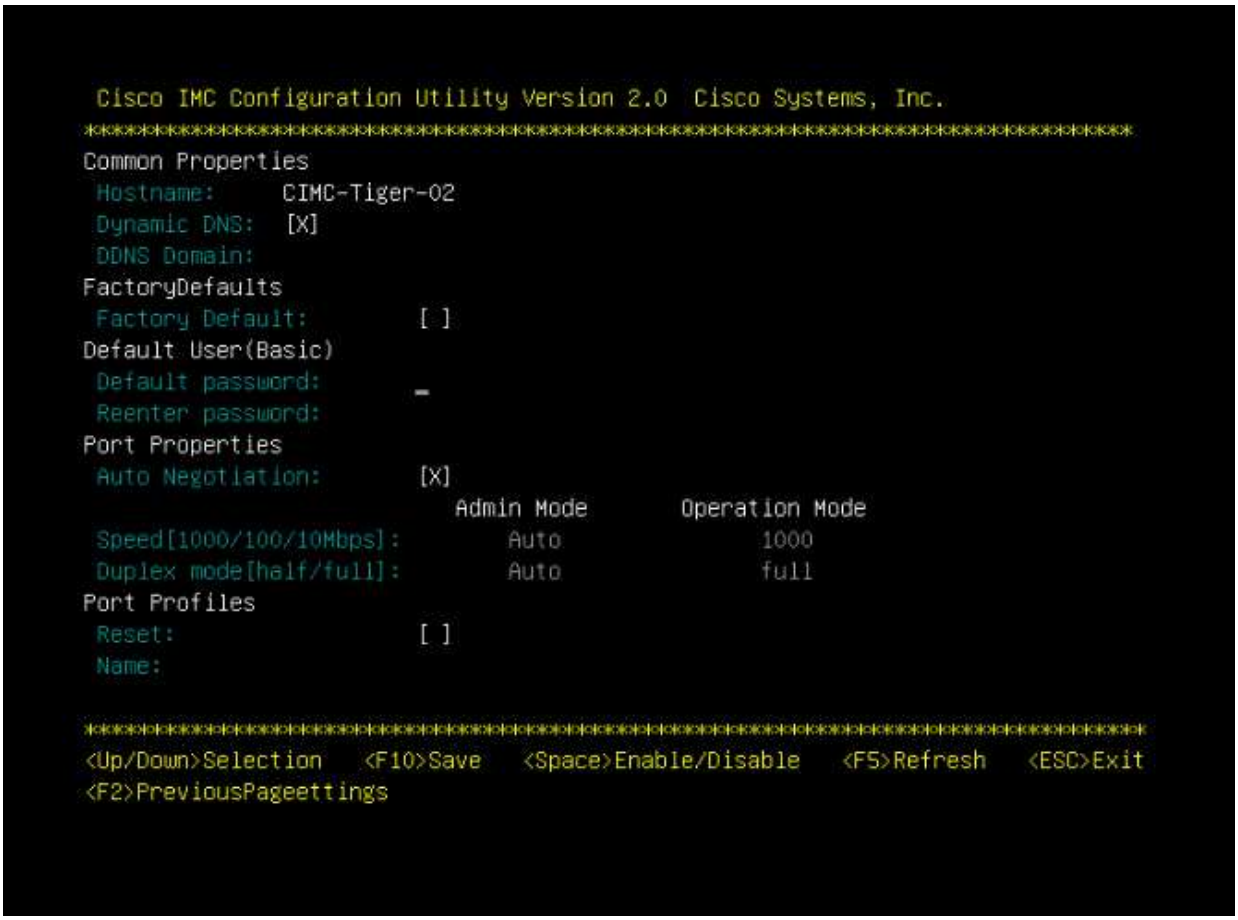
1. Conecte la mochila del teclado, vídeo y ratón (KVM) de Cisco (suministrada con el servidor) al puerto KVM de la parte frontal del servidor. Conecte un monitor VGA y un teclado USB a los puertos de mochila KVM adecuados.
2. Encienda el servidor y pulse F8 cuando se le solicite que introduzca la configuración 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.

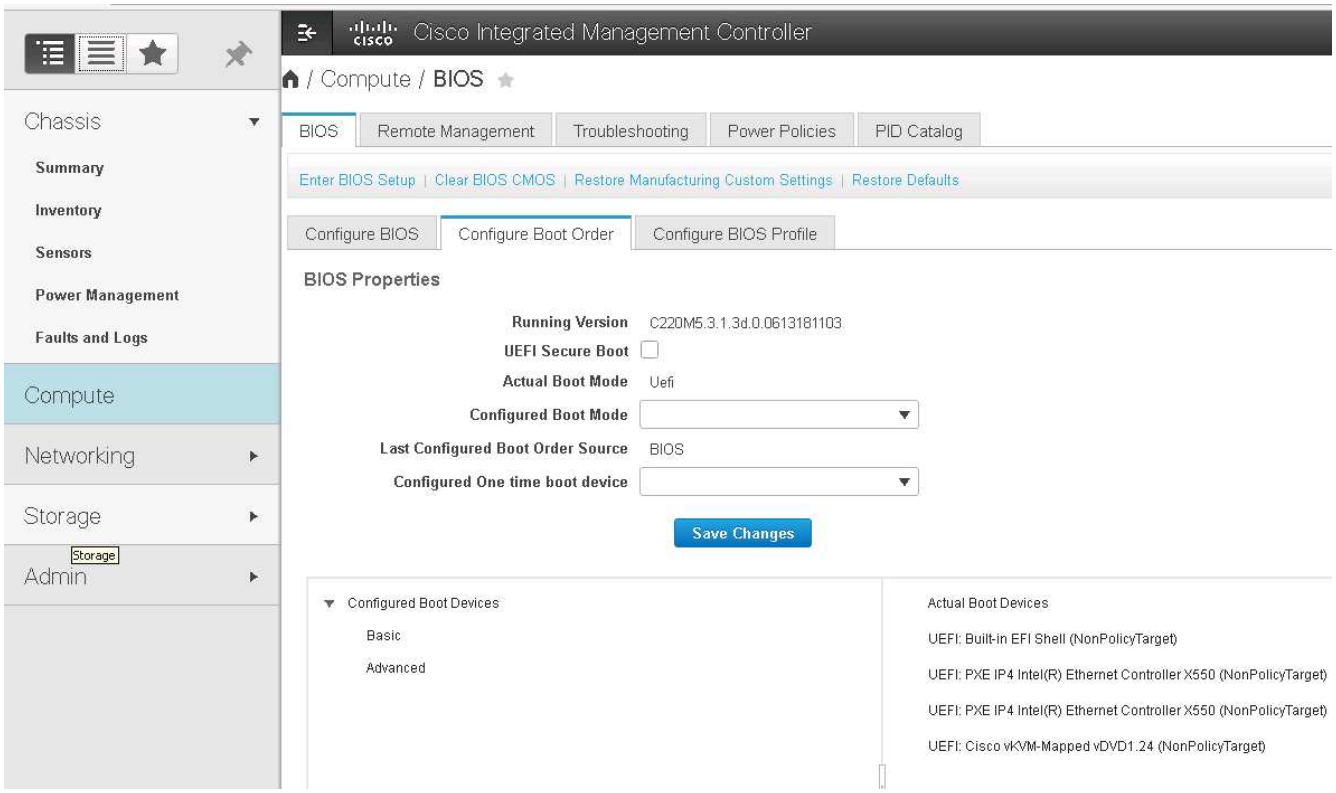
Detalles	Valor de detalle
Nombre Del iniciador del host ESXi	<<var_ucs_initiator_name_A>>
Host ESXi iSCSI-A IP	<<var_esxi_host_iscsiA_ip>>
Máscara de red iSCSI-A del host ESXi	<<var_esxi_host_iscsiA_mask>>
ISCSI del host ESXi: Puerta de enlace predeterminada	<<var_esxi_host_iscsiA_gateway>>
Nombre B 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

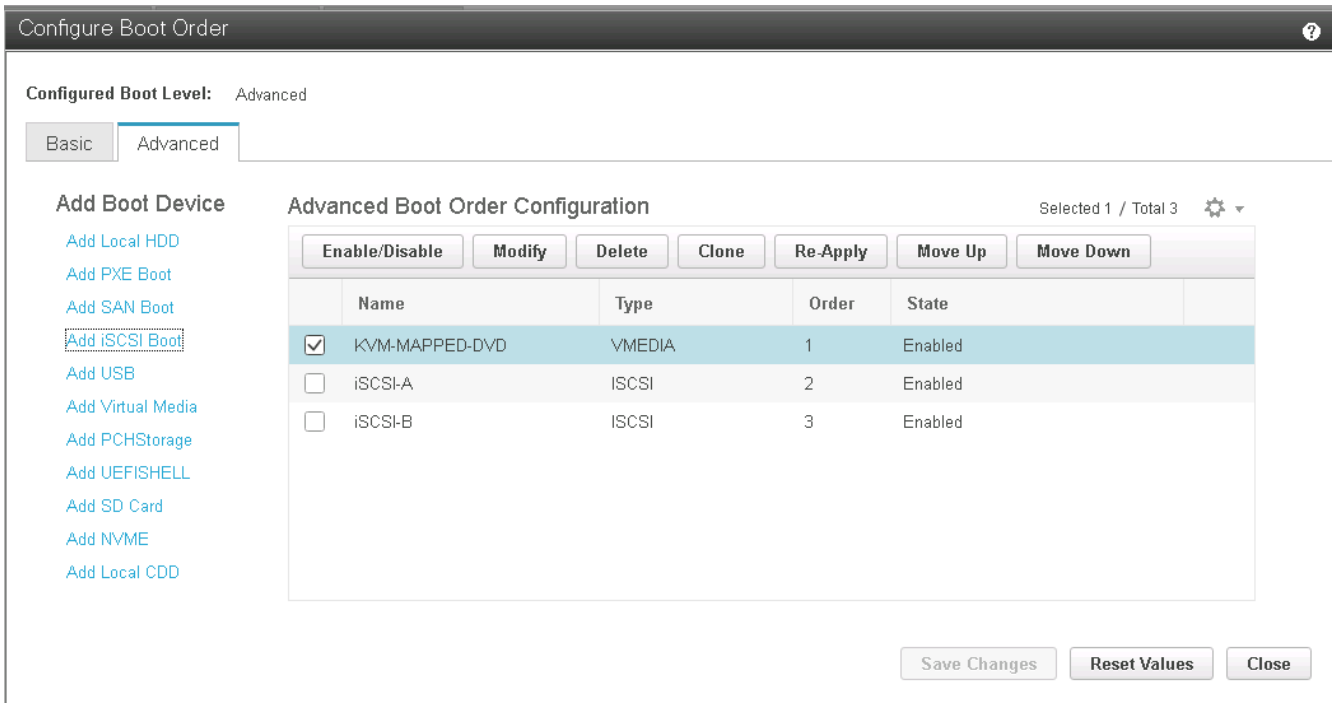
Para establecer la configuración del orden de arranque, lleve a cabo los siguientes pasos:

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.

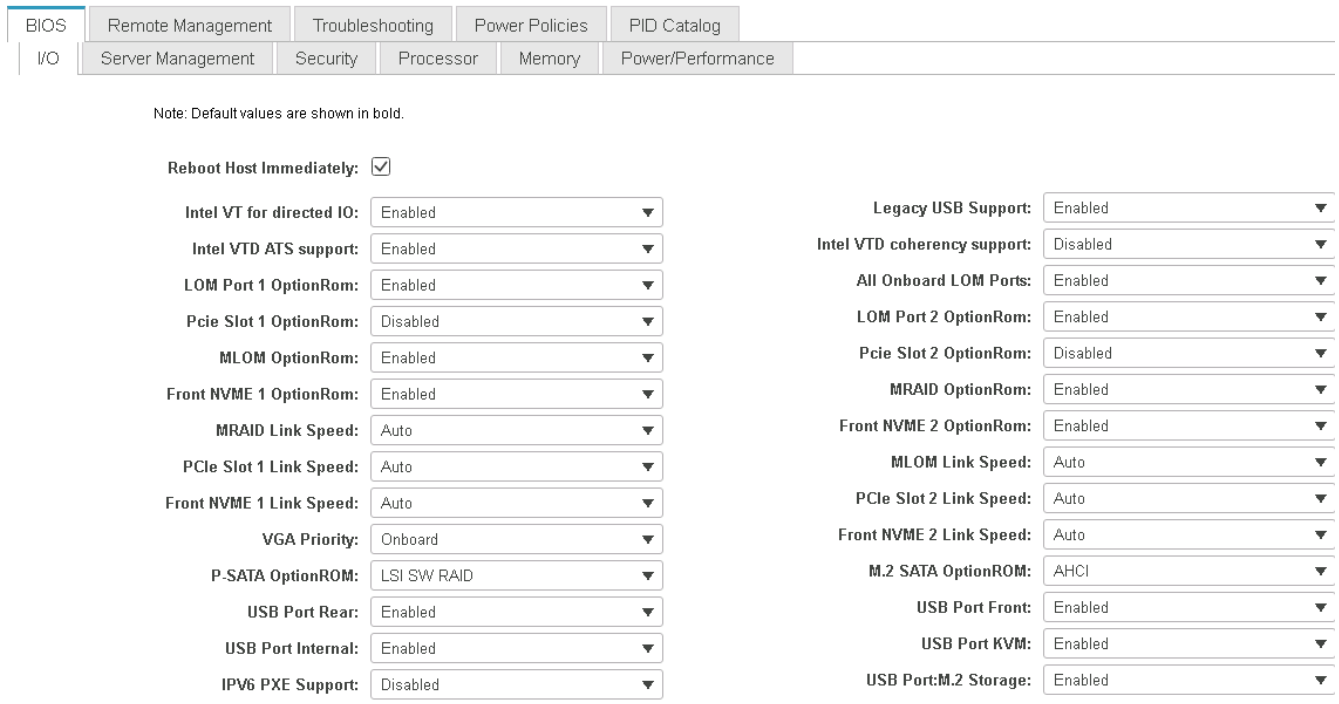


6. Reinicie el servidor para arrancar con el nuevo orden de inicio.

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.



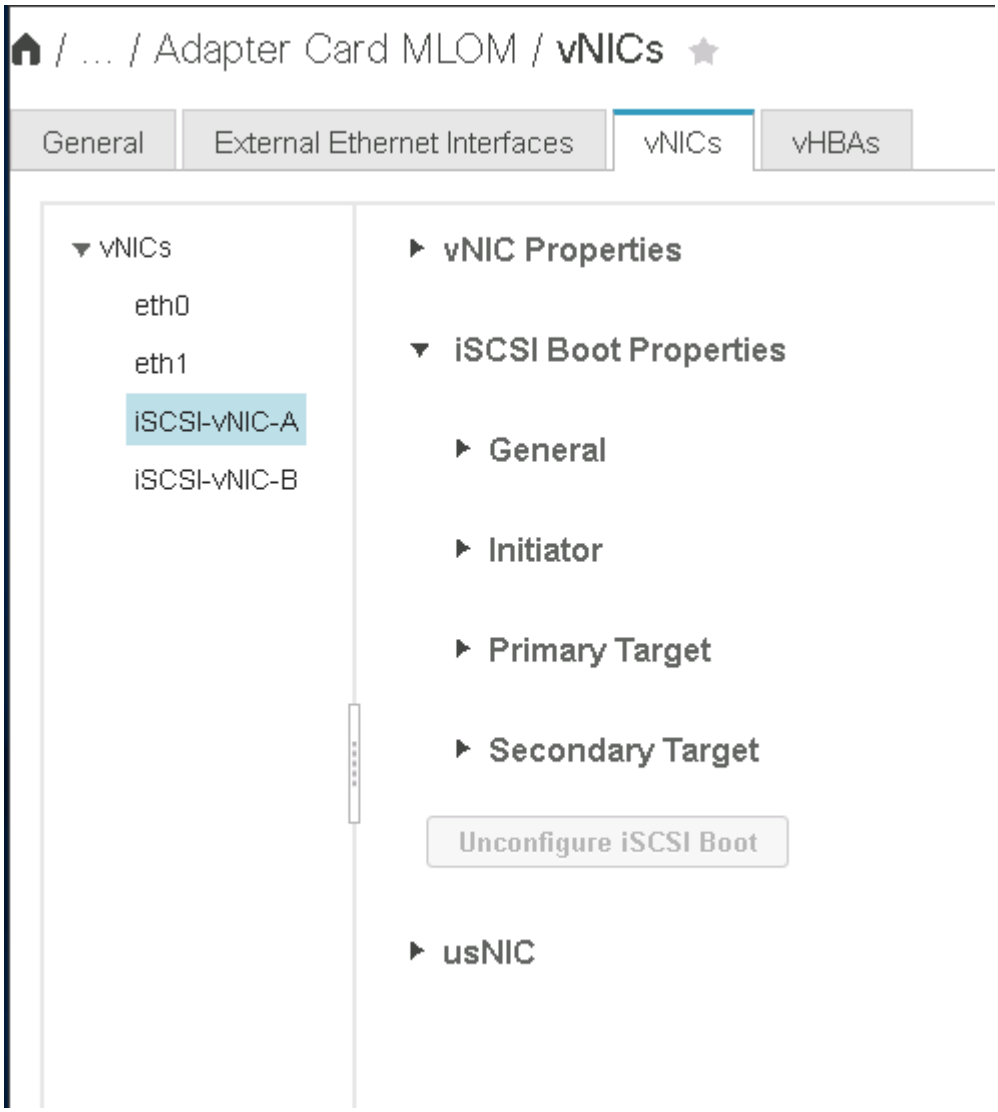
Configure Cisco VIC1387 para el arranque iSCSI

Los pasos de configuración siguientes son para el VIC 1387 de Cisco para arranque iSCSI.

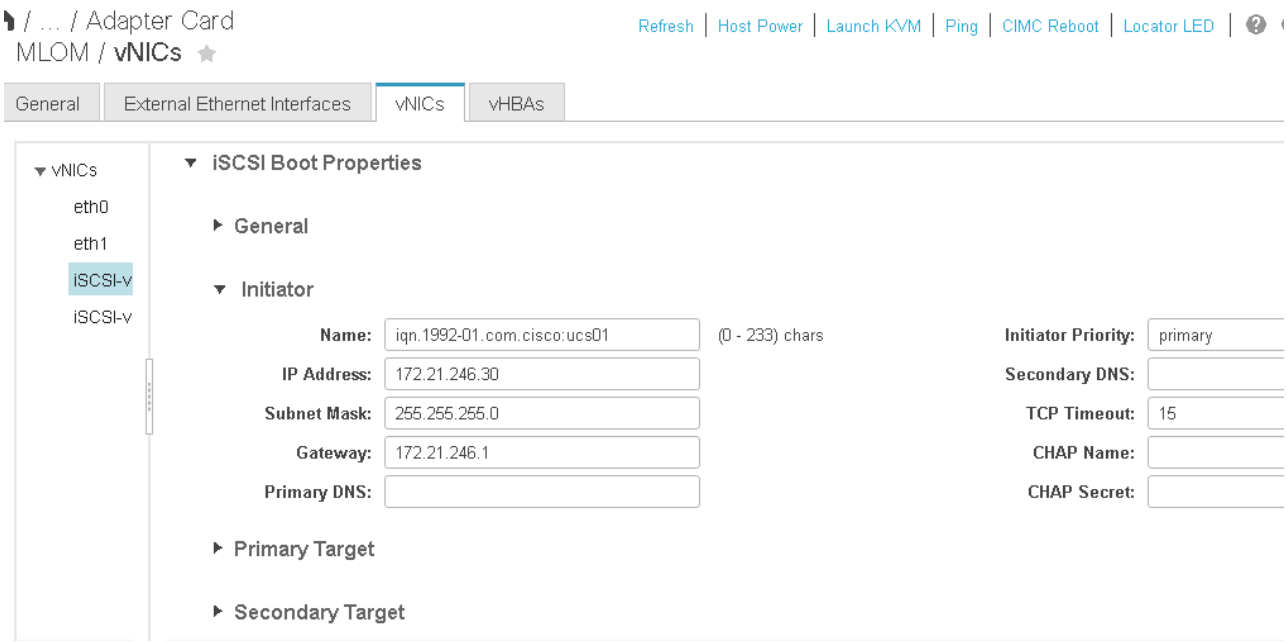
Cree NIC iSCSI

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.



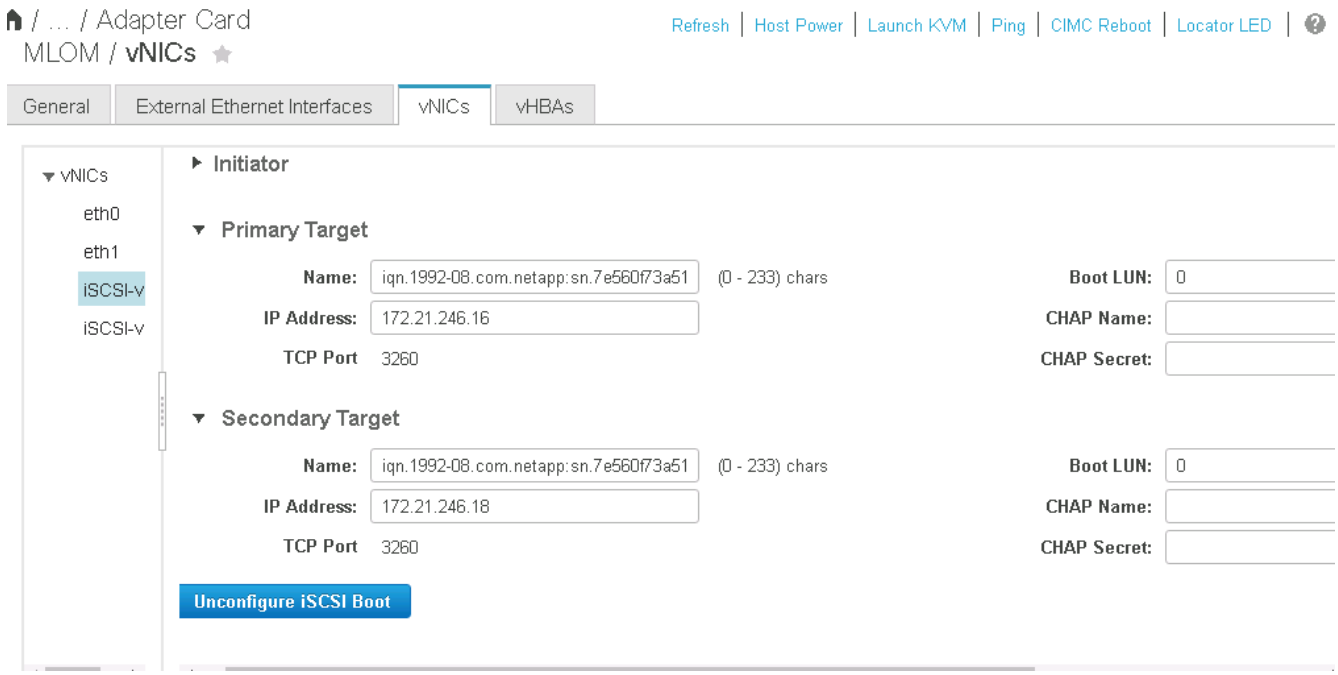
6. En Propiedades de arranque iSCSI, introduzca los detalles del iniciador:
   - Nombre: <<var_ucsa_initiator_name_a>>
   - Dirección IP: <<var_esxi_hostA_iscsiA_ip>>
   - Máscara de subred: <<var_esxi_hostA_iscsiA_mask>>
   - Puerta de enlace: <<var_esxi_hostA_iscsiA_gateway>>



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.

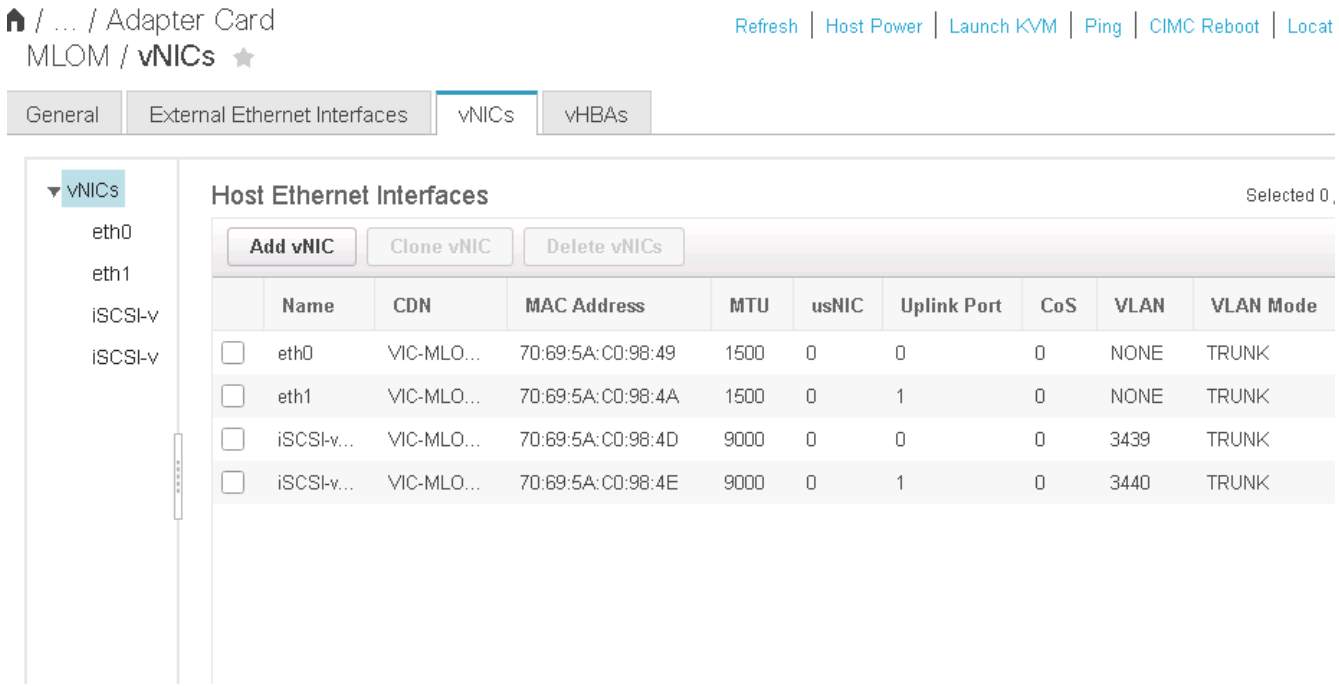
    > Asegúrese de registrar los nombres IQN de cada VNIC. Se necesitan para un paso más adelante.

15. Haga clic en Configurar ISCSI.

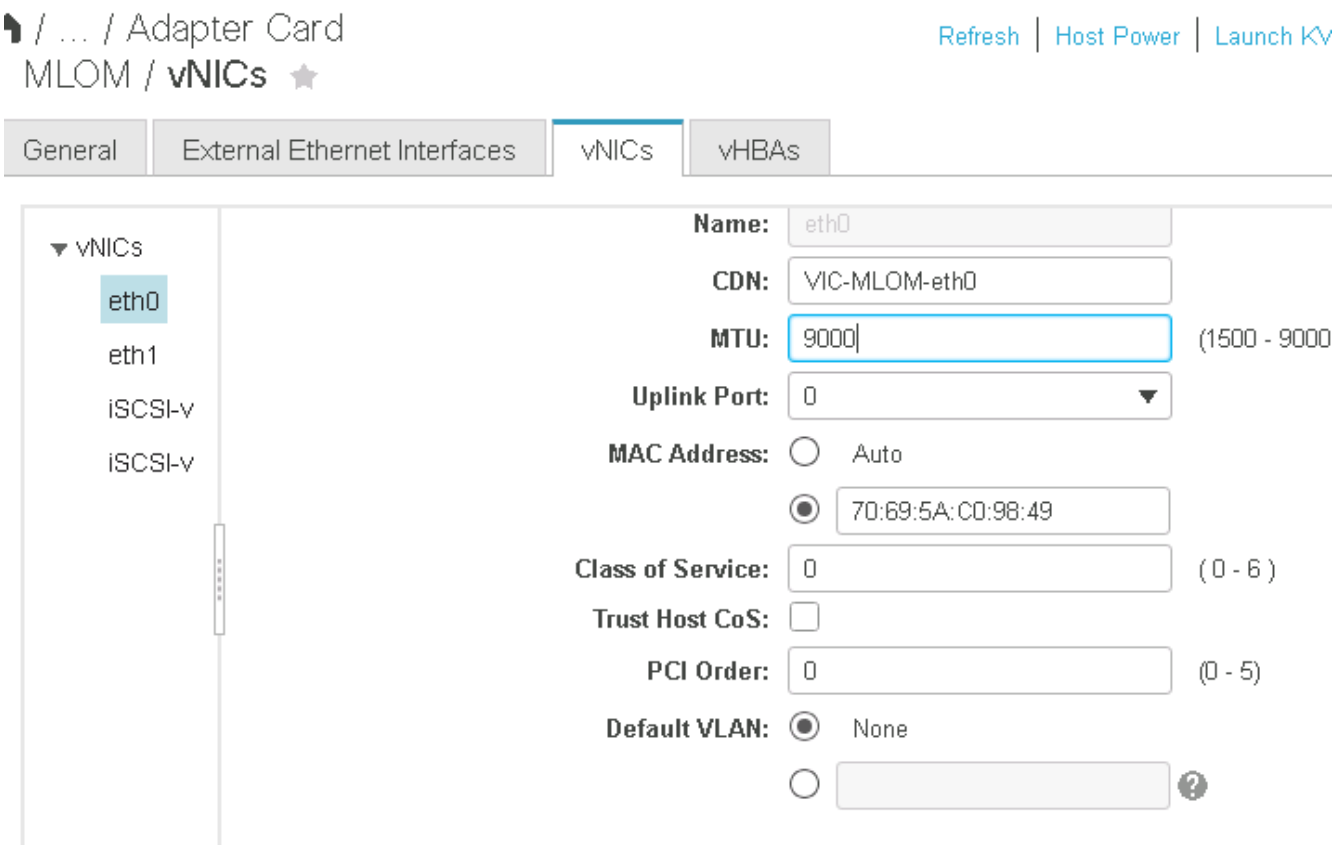
16. Repita este proceso para configurar el arranque iSCSI para el servidor Cisco UCS B.

Configure las NIC virtuales para ESXi

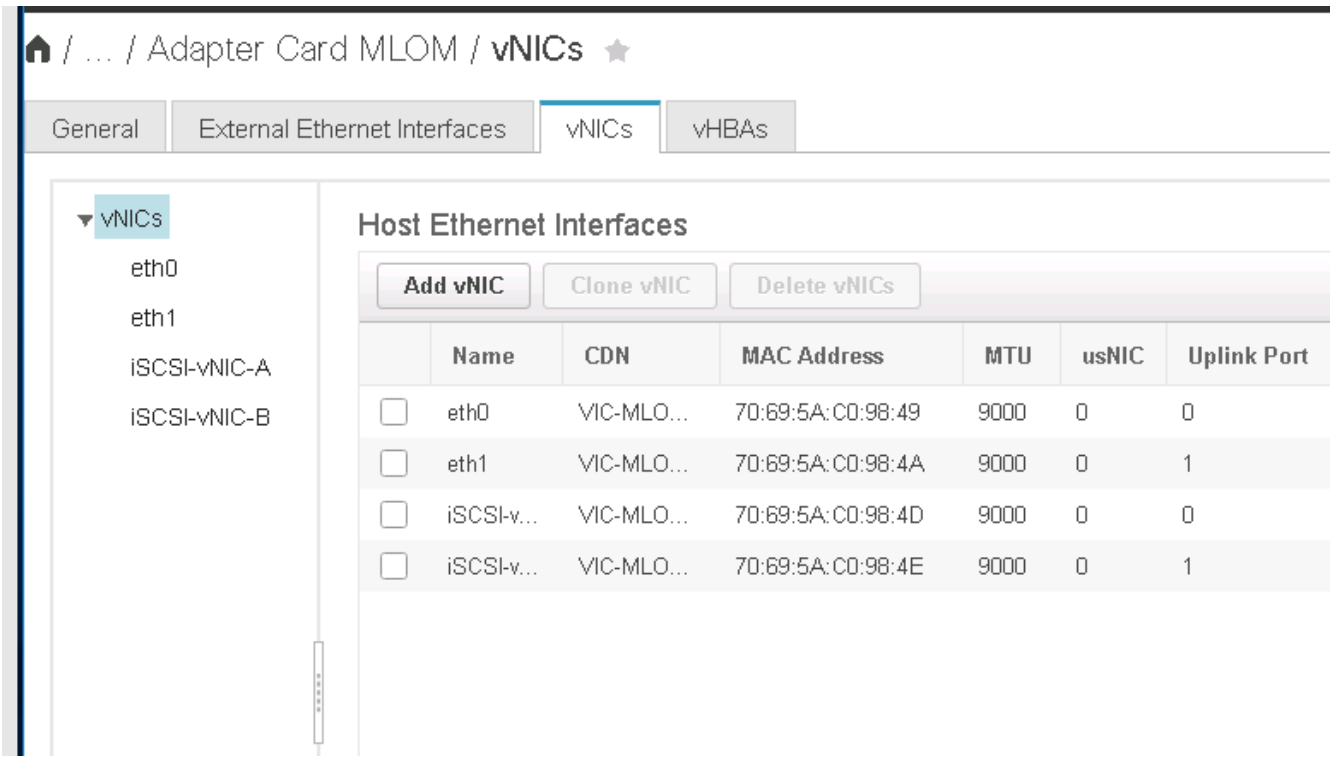
1. En la ventana del navegador de la interfaz CIMC, haga clic en Inventario y, a continuación, en Adaptadores Cisco VIC en el panel derecho.
2. En Tarjetas de adaptador, seleccione Cisco UCS VIC 1387 y, a continuación, seleccione las NIC de abajo.



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.

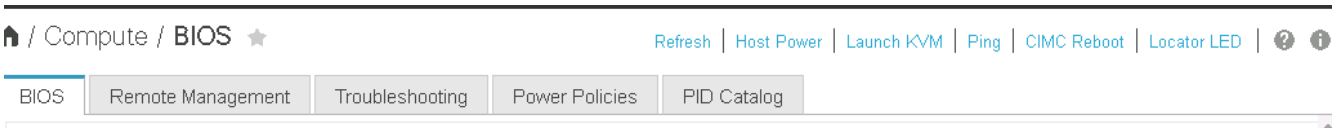
Este procedimiento debe completarse para los nodos adicionales que se añadan al clúster.

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.

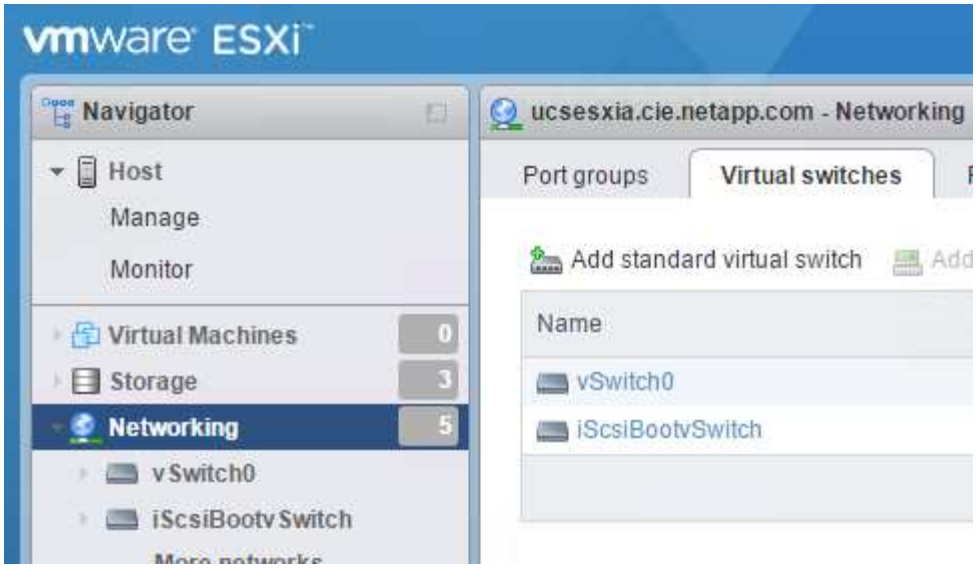
Detalles	Valor
Nombre de host ESXi	
La IP de gestión del host ESXi	
Máscara de gestión de host ESXi	
Pasarela de gestión de host ESXi	
IP NFS del host ESXi	
Máscara de NFS del host ESXi	
Puerta de enlace NFS del host ESXi	
Host ESXi IP de vMotion	
Máscara de vMotion del host ESXi	
Puerta de enlace vMotion 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

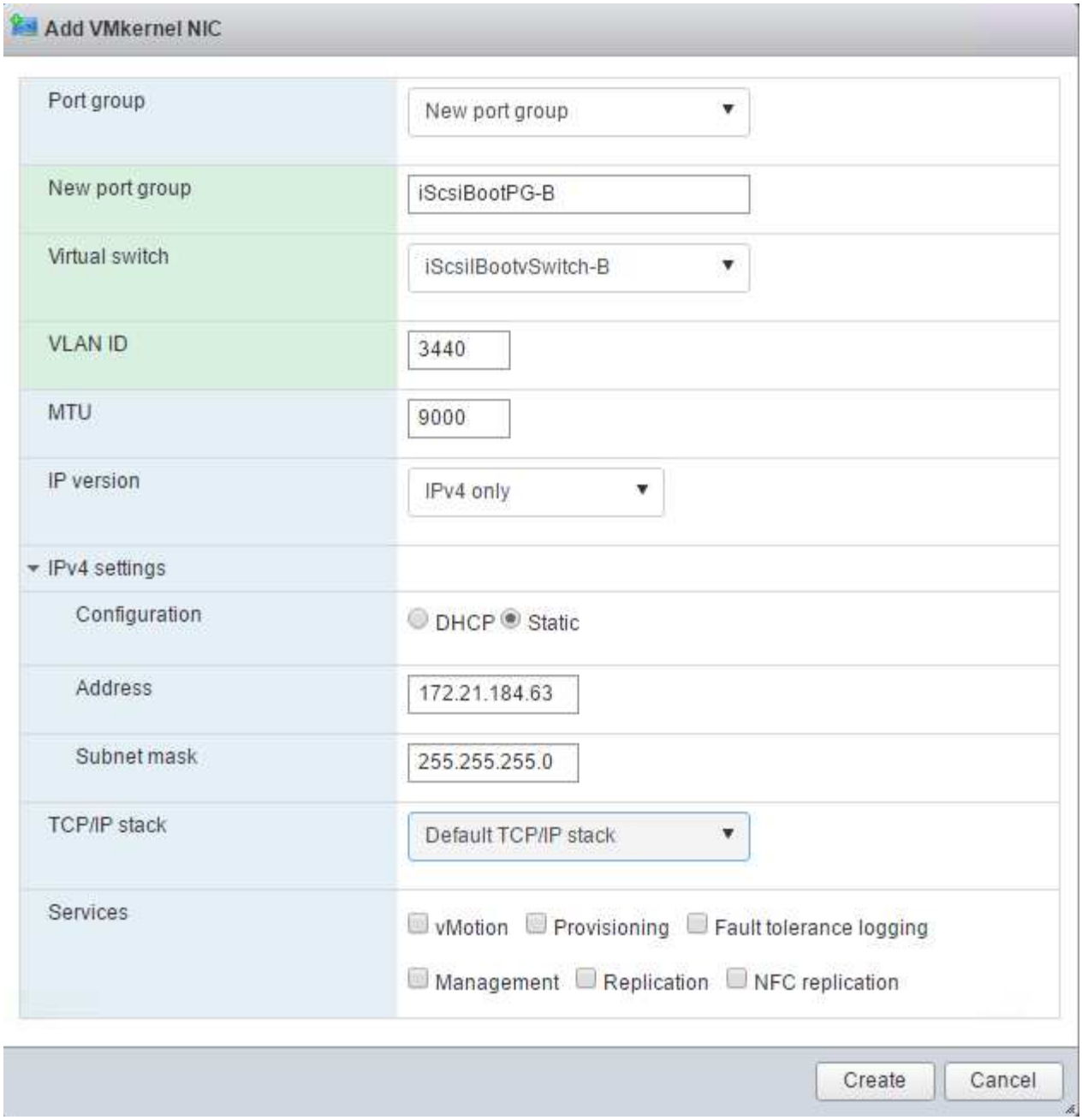
1. Seleccione Networking a la izquierda.
2. A la derecha, seleccione la ficha Switches virtuales.



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.

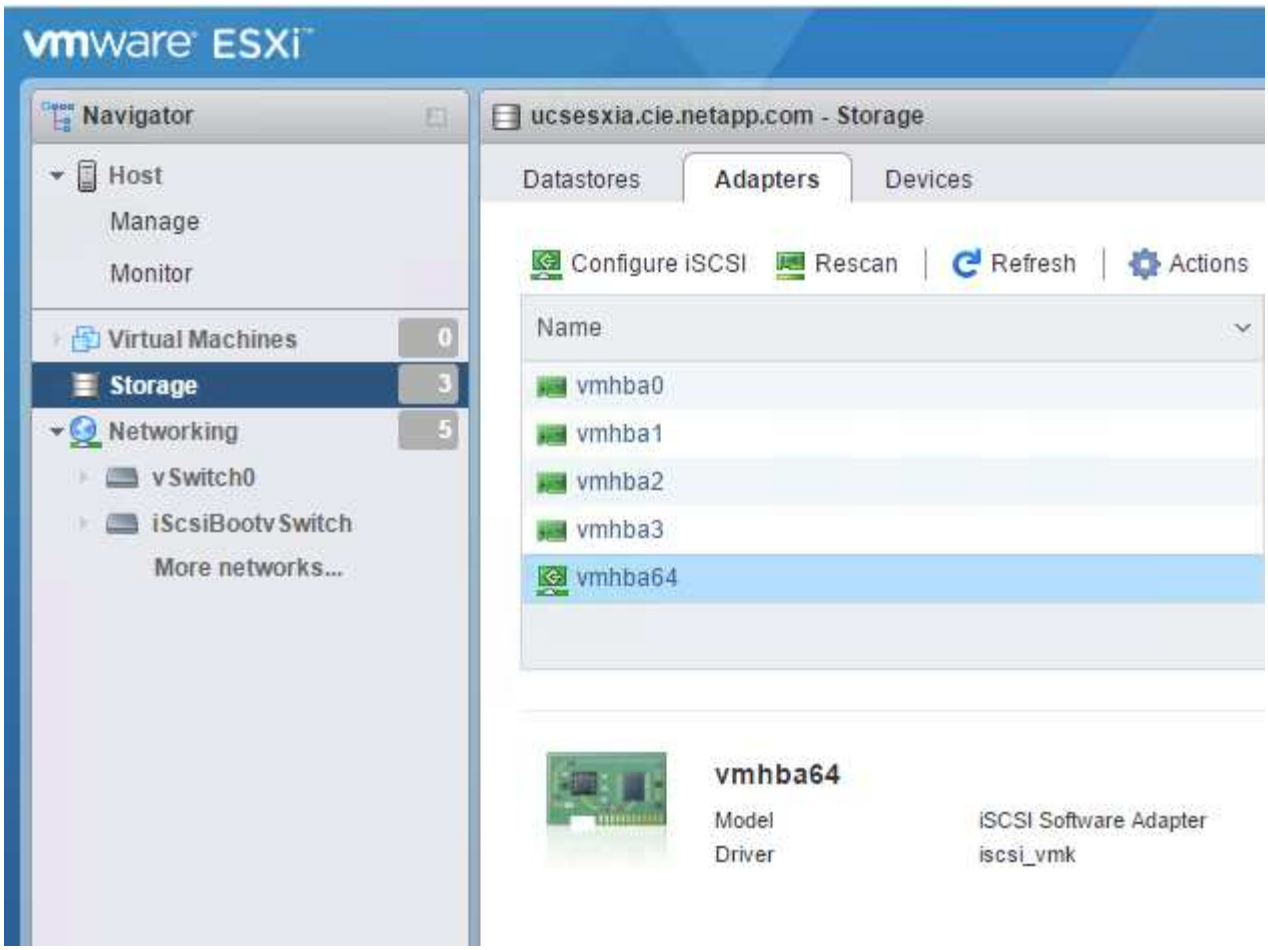


Establezca la MTU en 9000 on `iScsiBootPG- A`.

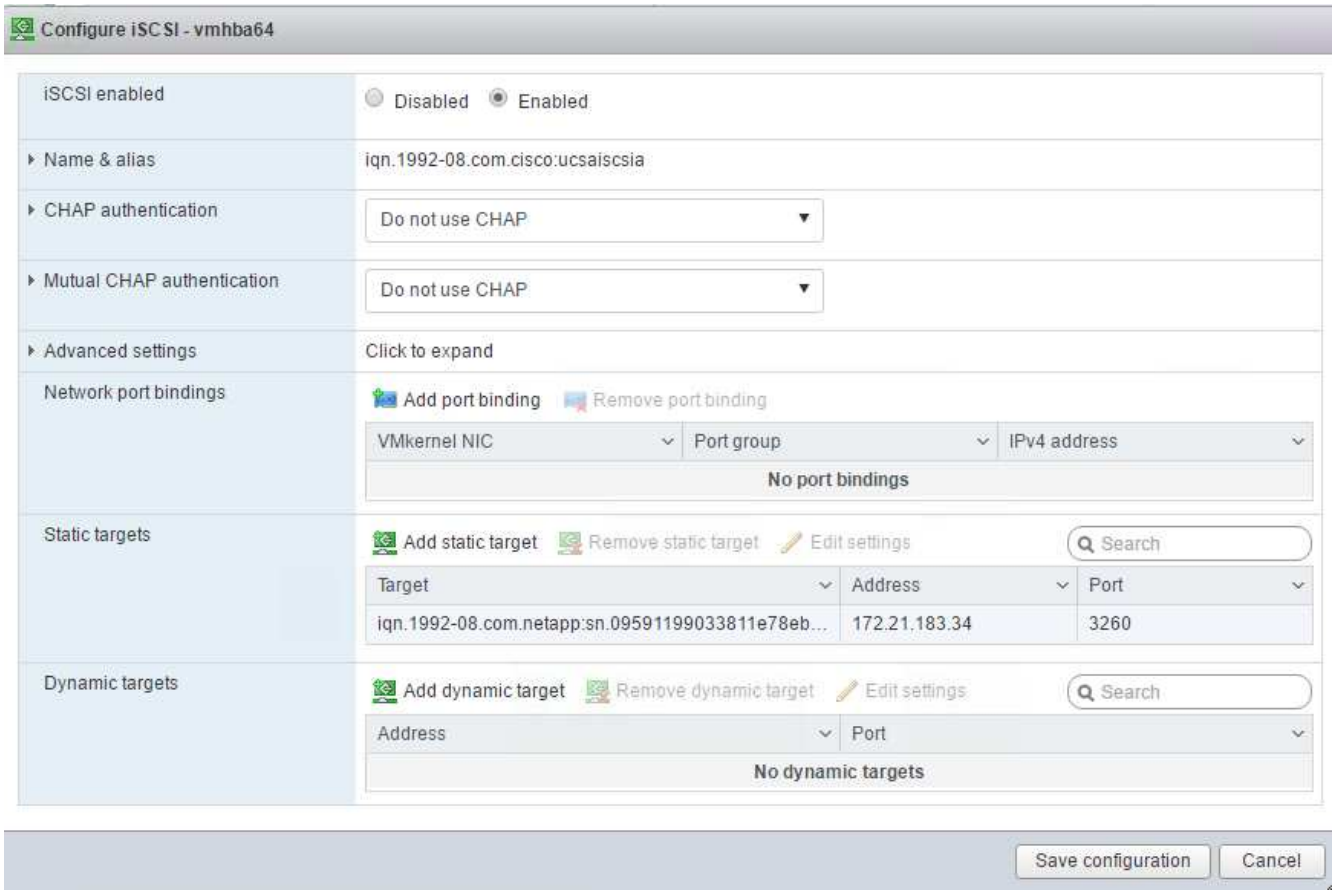
Configuración de accesos múltiples iSCSI

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

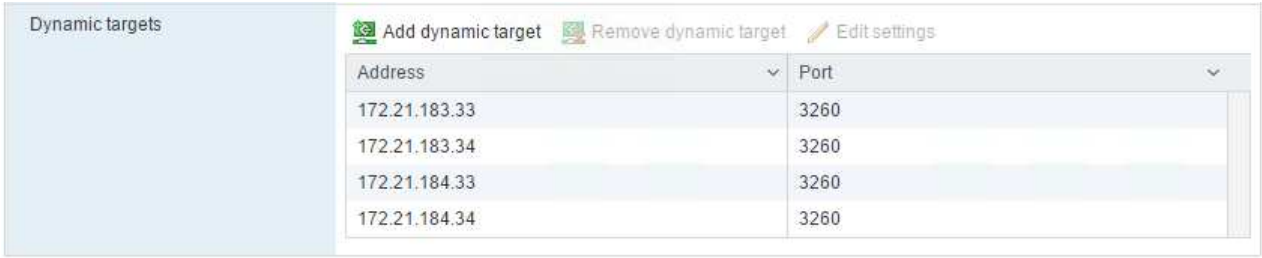
1. Seleccione Storage en el panel de navegación de la izquierda. Haga clic en Adaptadores.
2. Seleccione el adaptador de software iSCSI y haga clic en Configurar iSCSI.



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



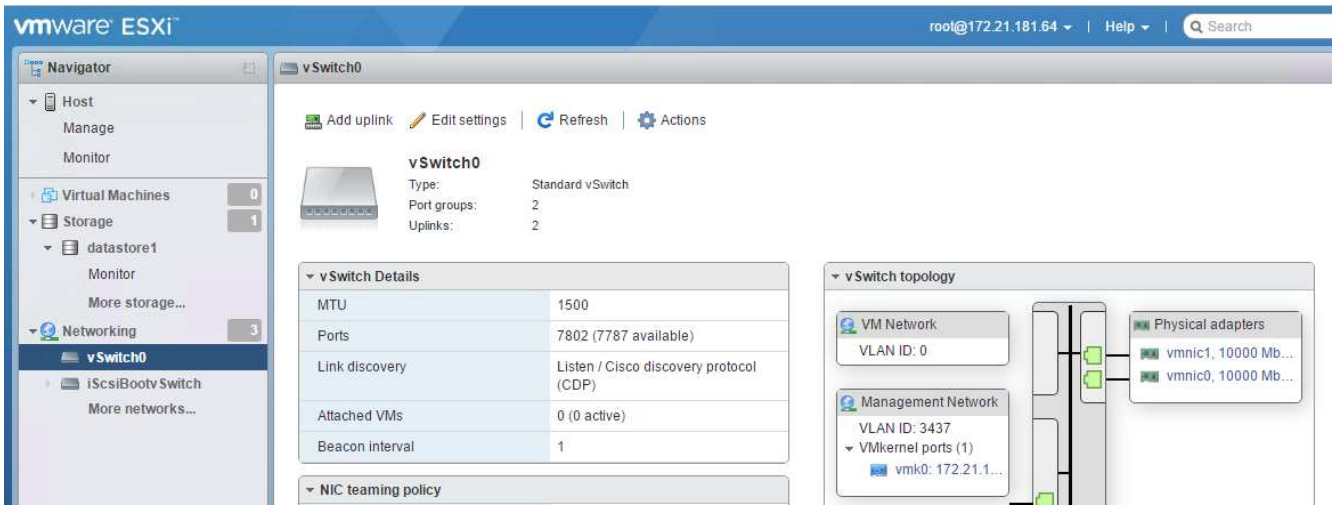
4. Introduzca la dirección IP `iscsi_lif01a`.
   - Repita el proceso con las direcciones IP `iscsi_lif01b`, `iscsi_lif02a`, y. `iscsi_lif02b`.
   - Haga clic en Save Configuration.



> 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.



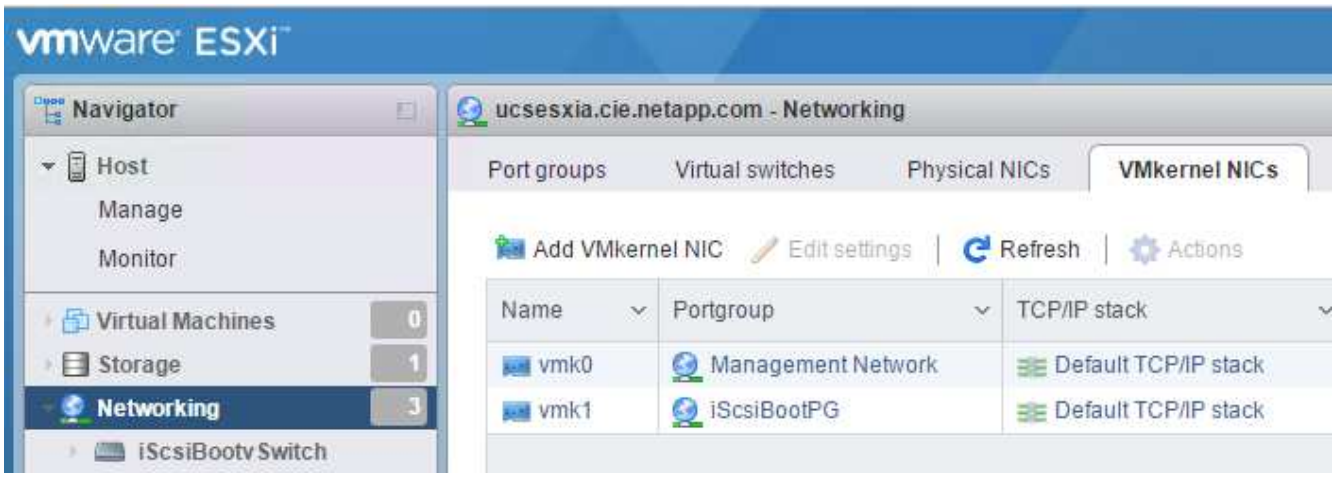
3. Seleccione Editar configuración.
4. Cambie el MTU a 9000.
5. Expanda NIC Teaming y verifique que tanto vmnic0 como vmnic1 estén definidos en activo.

Configurar grupos de puertos y NIC de VMkernel

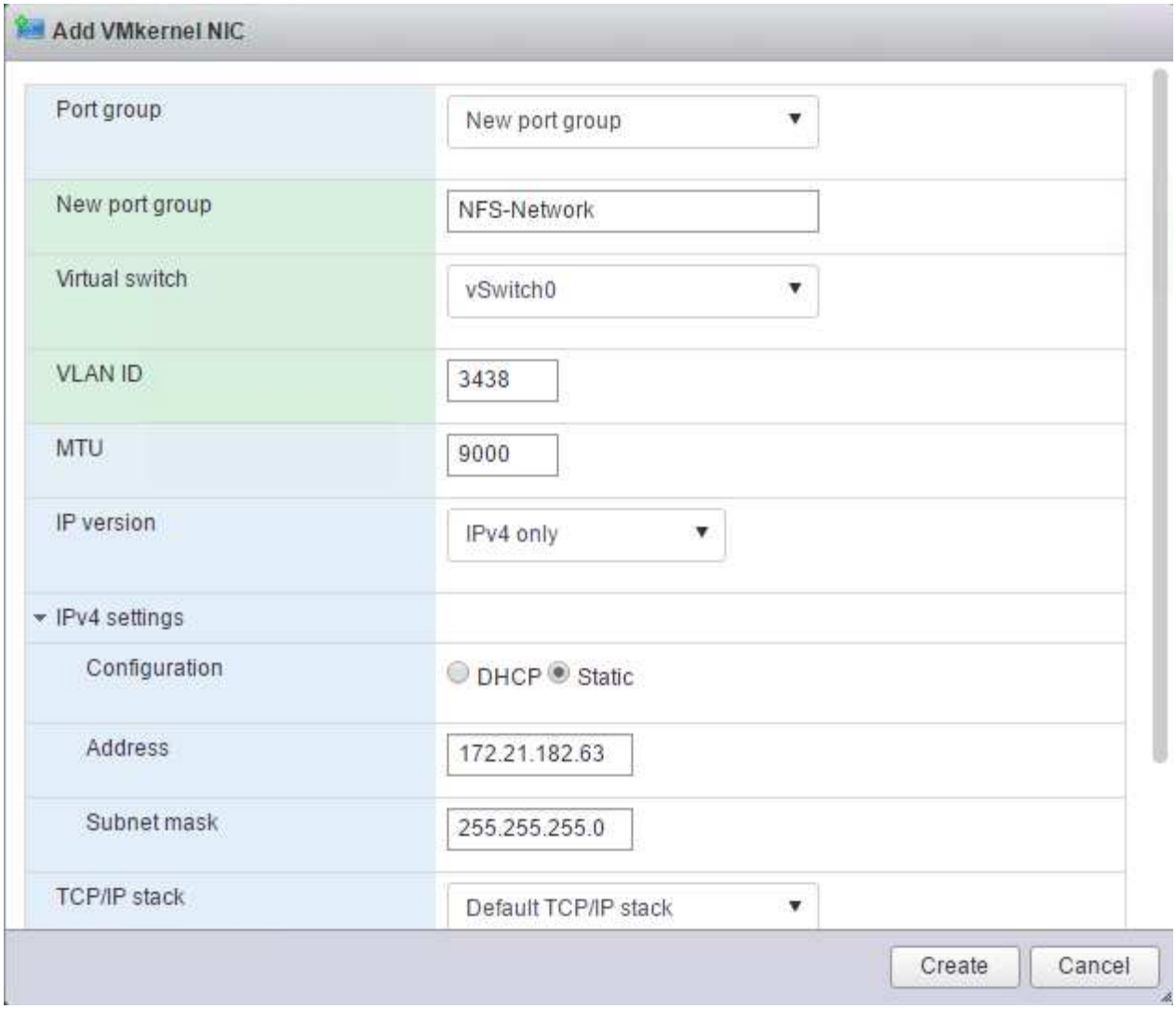
1. En el panel de navegación de la izquierda, seleccione Networking.
2. Haga clic con el botón derecho en la pestaña grupos de puertos.

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.

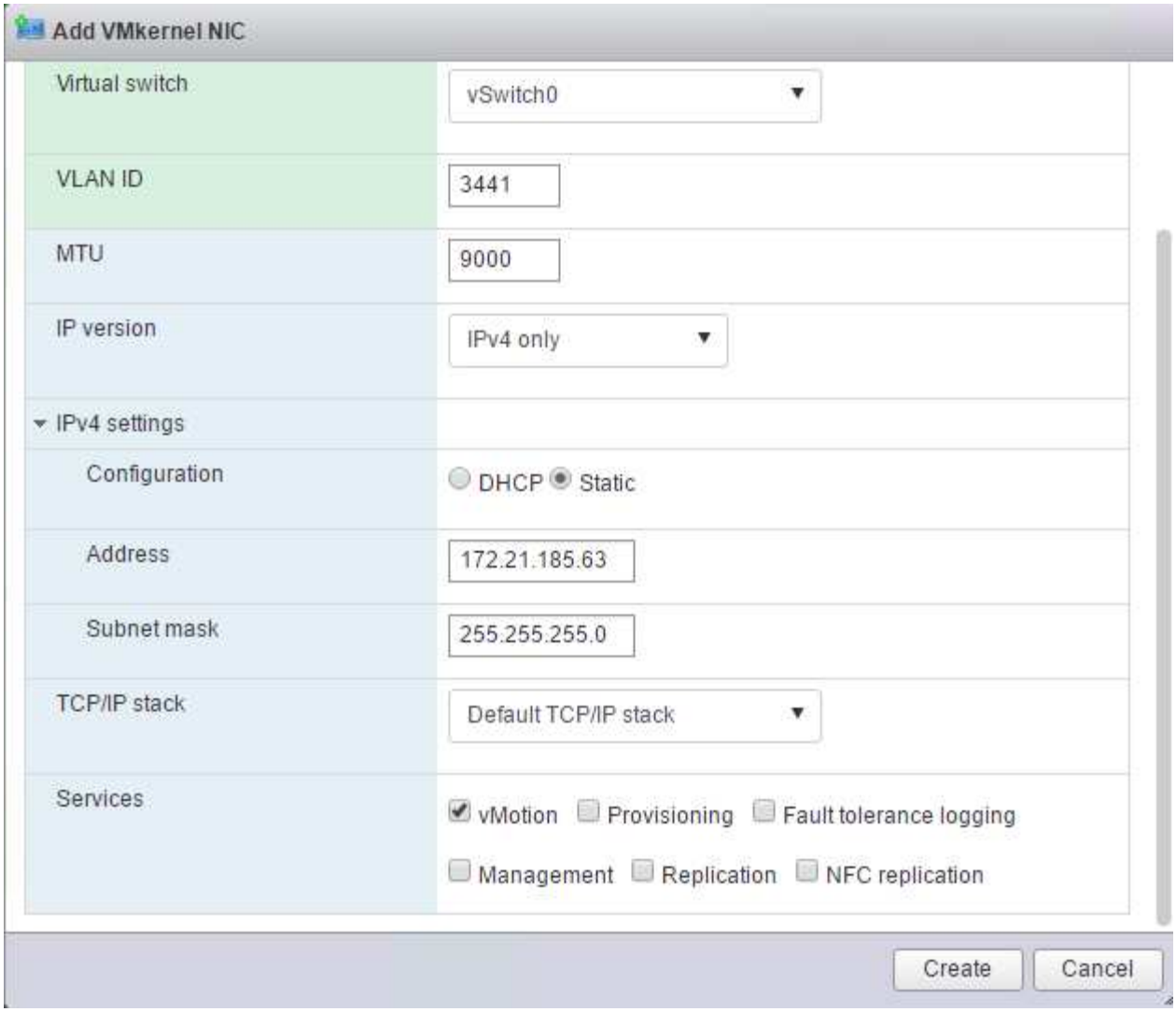
5. Haga clic en la ficha NIC de VMkernel.



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.

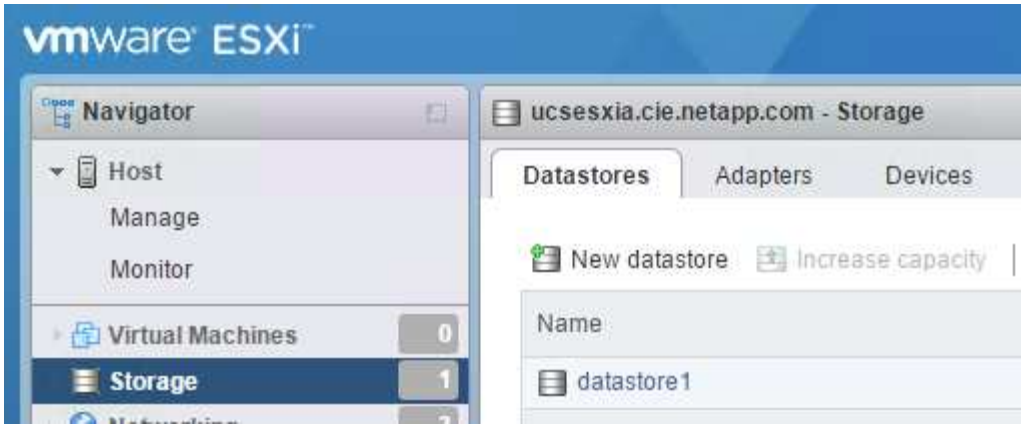


Hay muchas formas de configurar redes ESXi, por ejemplo, mediante el switch distribuido de VMware vSphere si la licencia lo permite. FlexPod Express admite configuraciones de red alternativas si se requieren para satisfacer los requisitos del negocio.

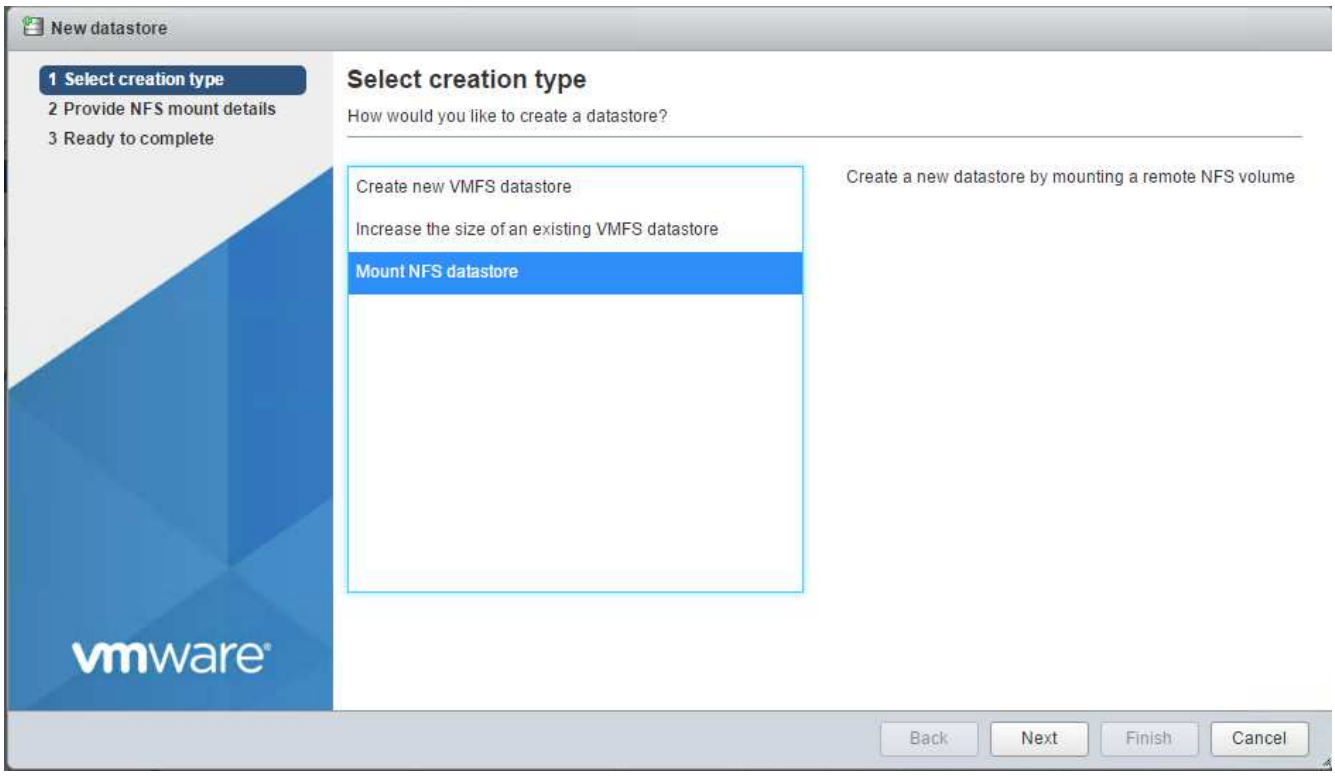
Montaje de los primeros almacenes de datos

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.



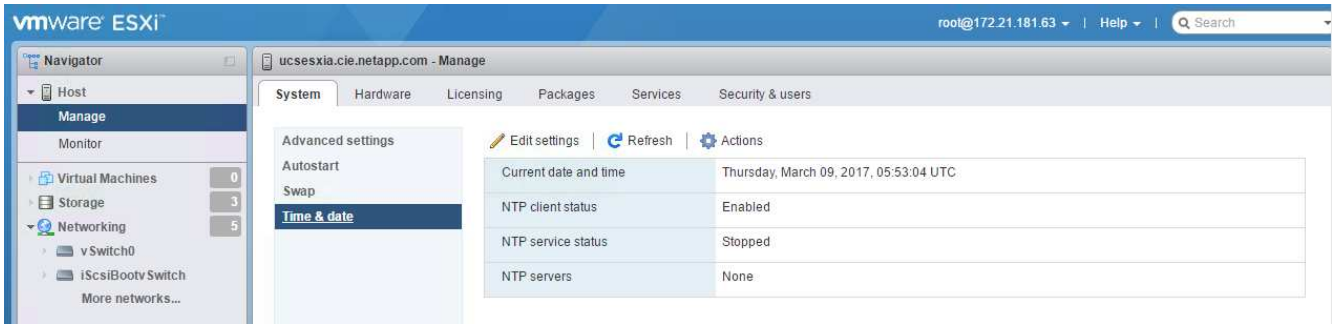
3. A continuación, introduzca la siguiente información en la página Provide NFS Mount Details:
   - Nombre: `infra_datastore_1`
   - Servidor NFS: `<<var_nodea_nfs_lif>>`
   - Compartir: /Infra_datastore_1
   - Asegúrese de que la opción NFS 3 esté seleccionada.
4. Haga clic en Finalizar. Puede ver que 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.

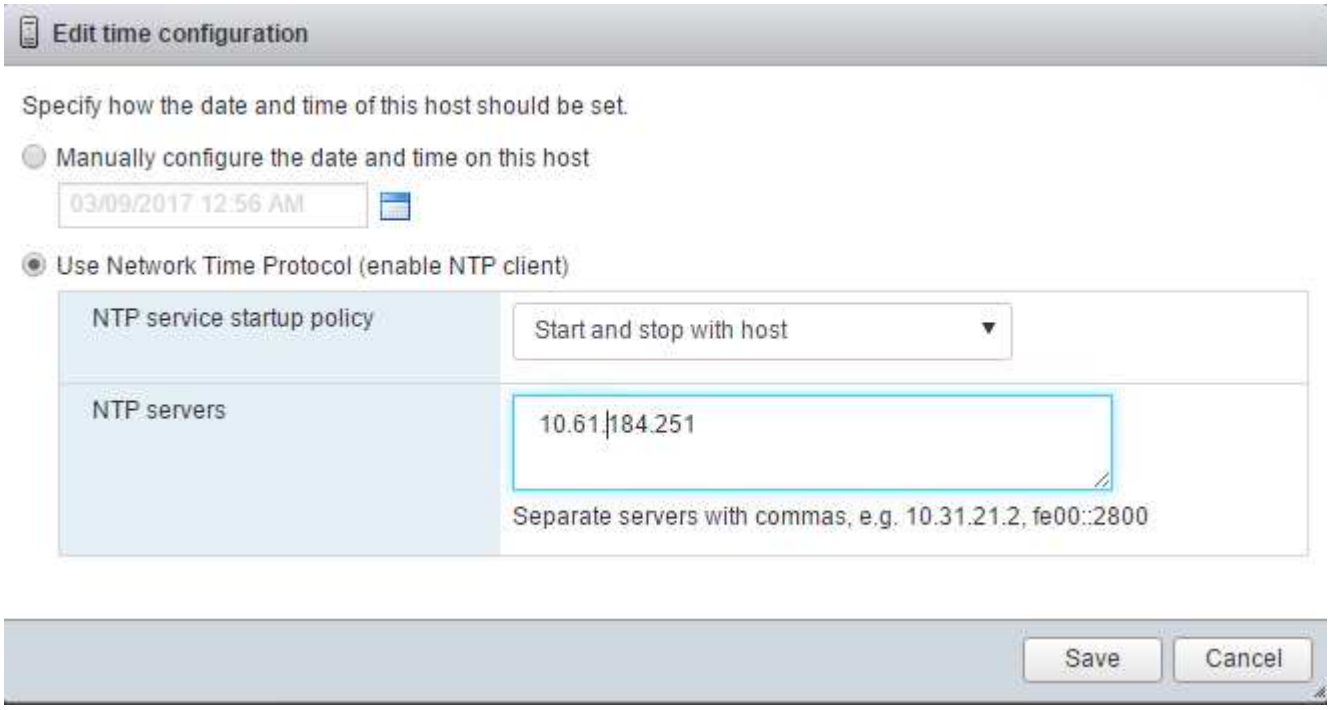
Configure NTP

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.



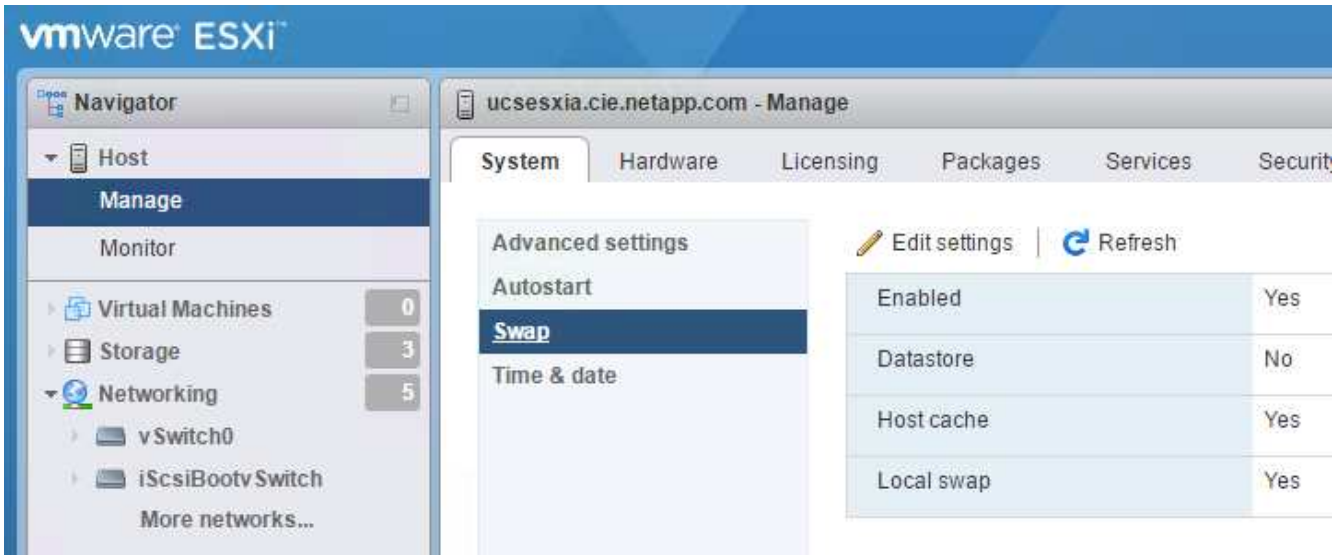
2. Seleccione Use Network Time Protocol (Habilitar cliente NTP).
3. Seleccione Start and Stop with Host como política de inicio del servicio NTP.
4. Introduzca `<<var_ntp>>` Como servidor NTP. Puede establecer varios servidores NTP.
5. Haga clic en Guardar.



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"

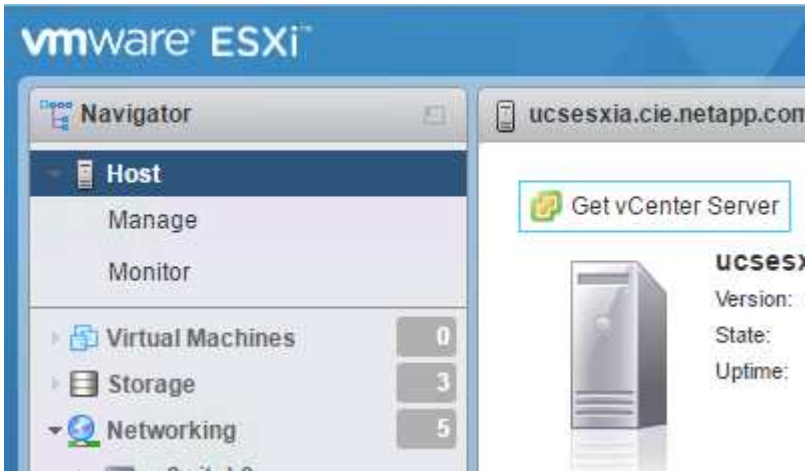
Instale VMware vCenter Server 6.7

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

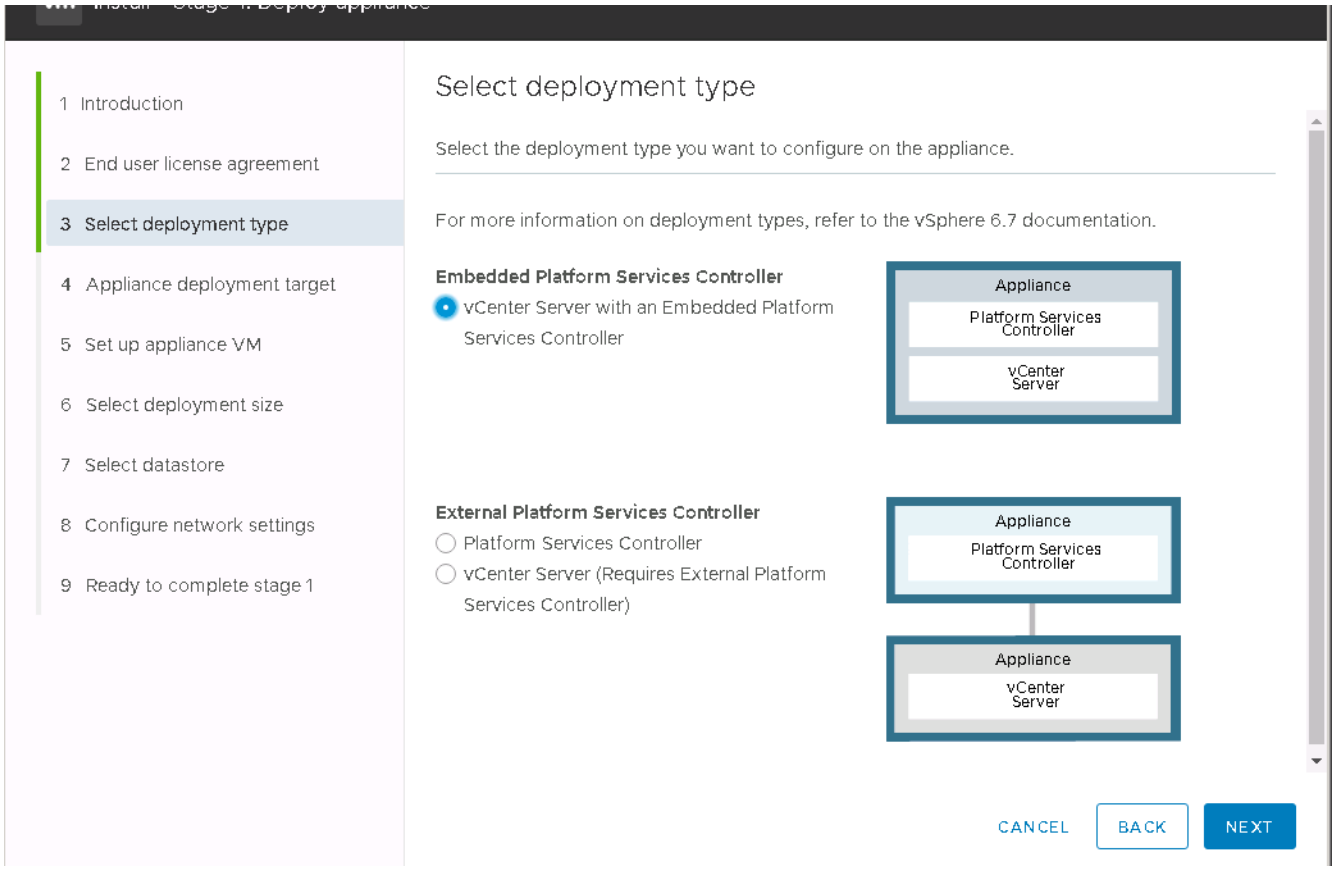
1. Descargue el VCSA. Acceda al enlace de descarga haciendo clic en el icono Get vCenter Server cuando gestione el host ESXi.



2. Descargue el VCSA desde el sitio de VMware.

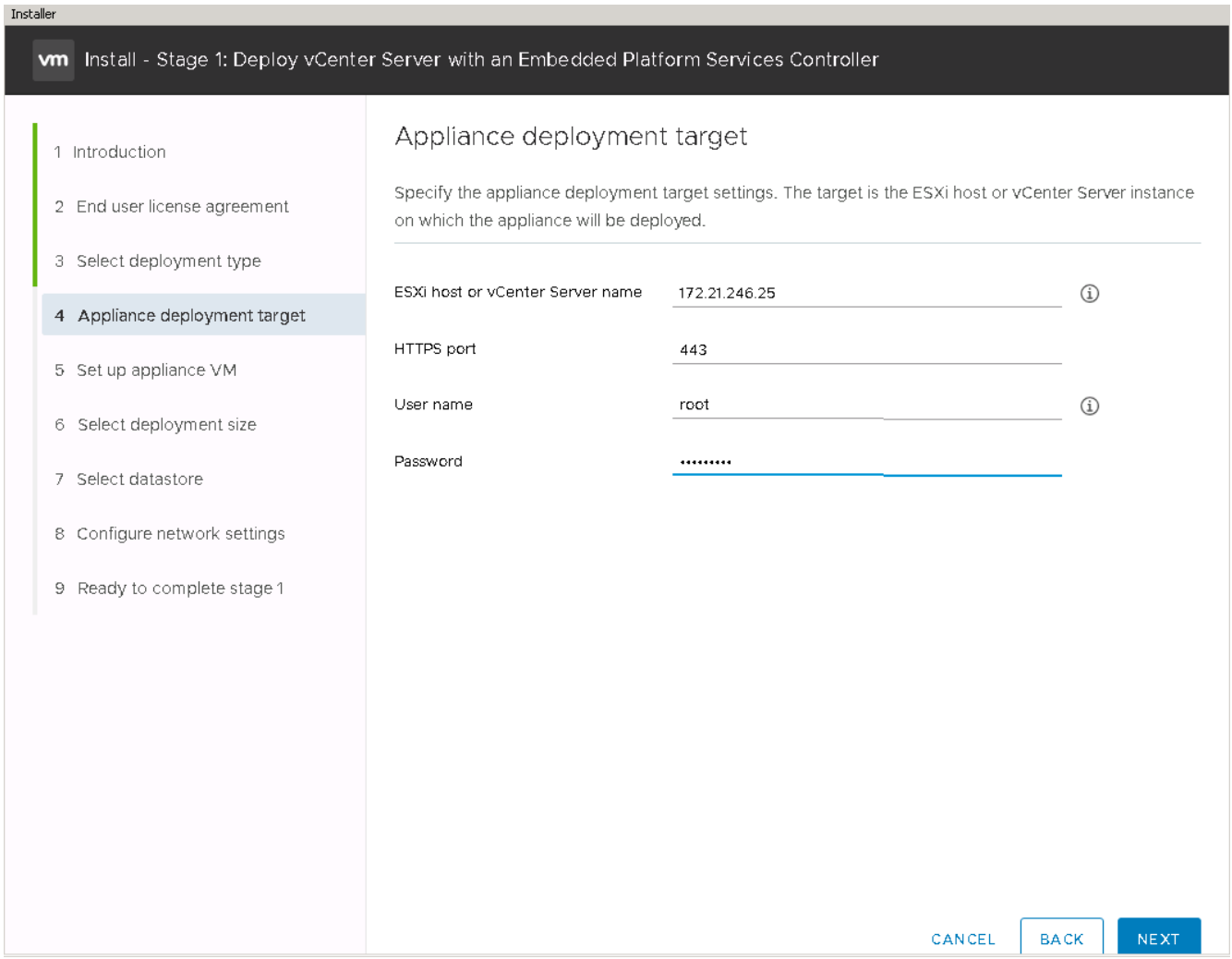
> Aunque se admite la instalación de Microsoft Windows vCenter Server, VMware recomienda VCSA para las nuevas implementaciones.

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.

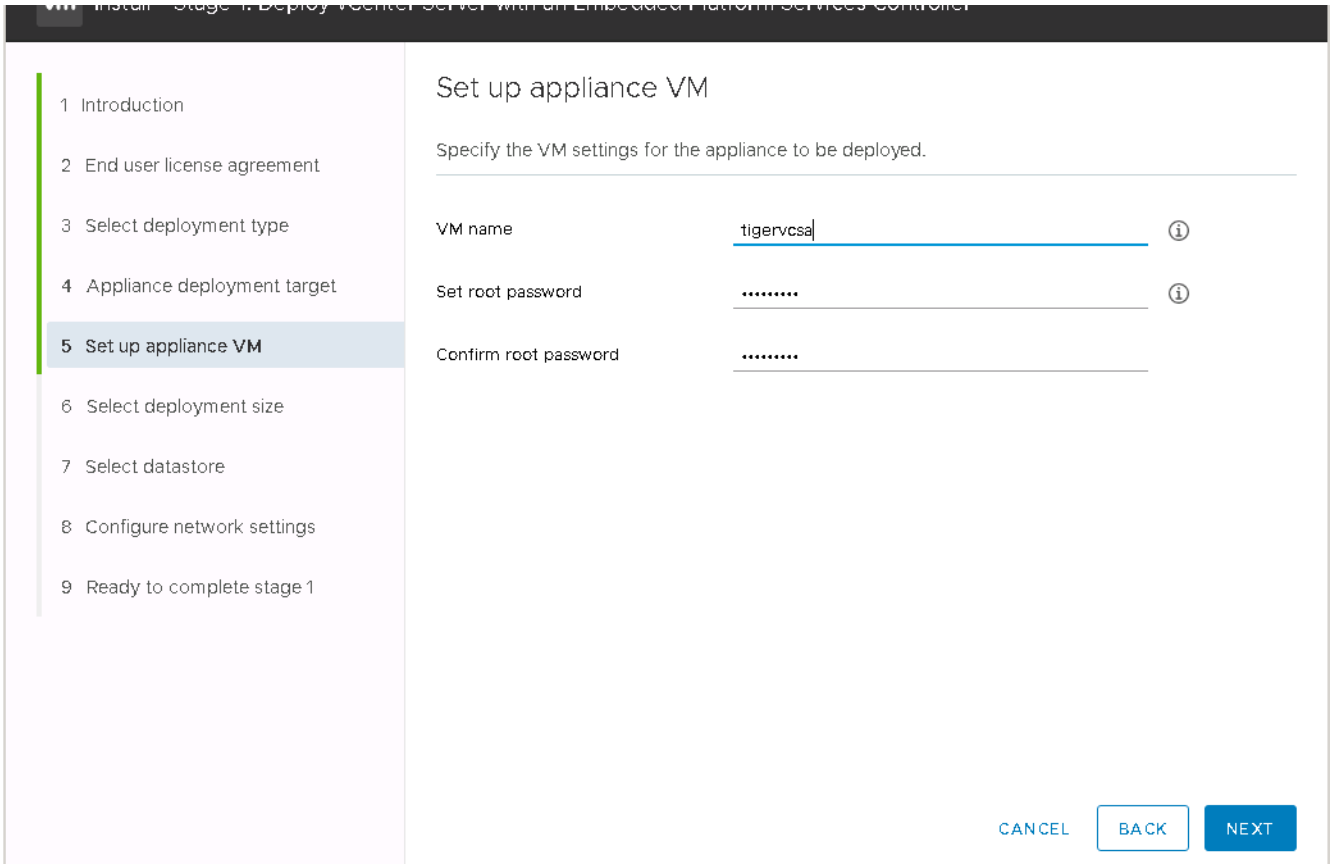


Si es necesario, también admite la puesta en marcha de la controladora de servicios de plataforma externa como parte de la solución FlexPod Express.

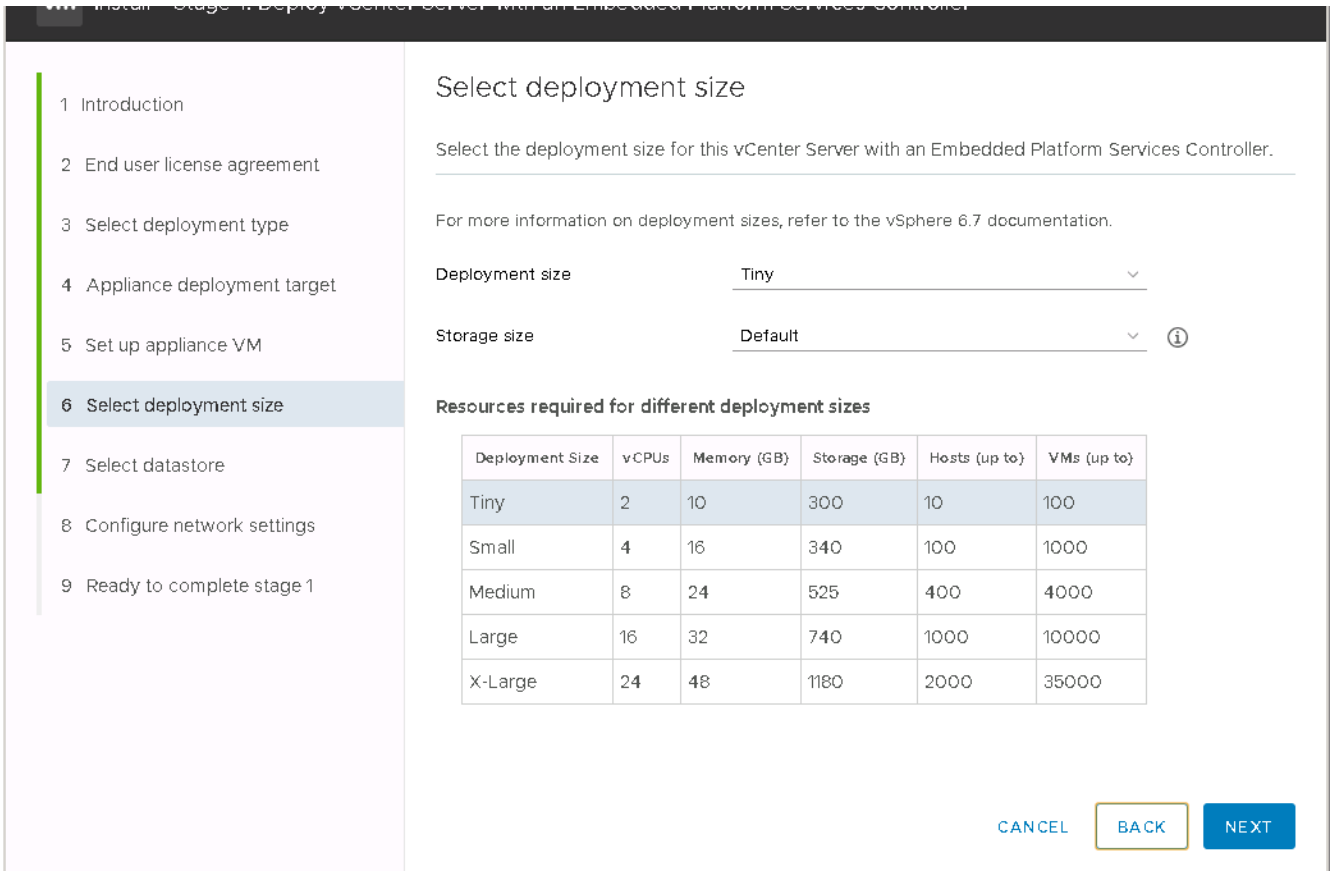
9. En Appliance Deployment Target, introduzca la dirección IP de un host ESXi implementado, así como el nombre de usuario raíz y la contraseña raíz.



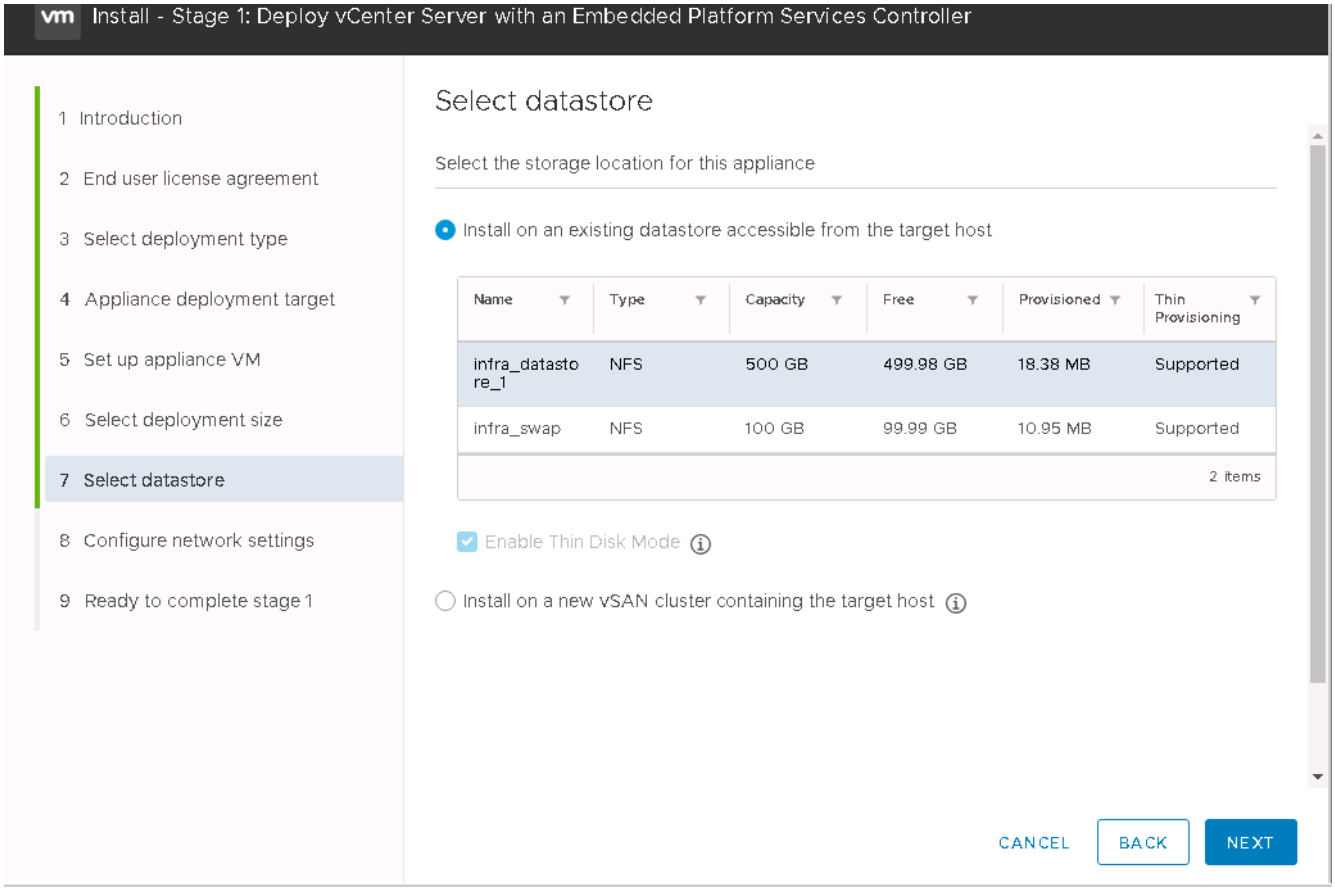
10. Introduzca para establecer la máquina virtual del dispositivo `VCSA` Como el nombre del equipo virtual y la contraseña raíz que desea utilizar para el VCSA.



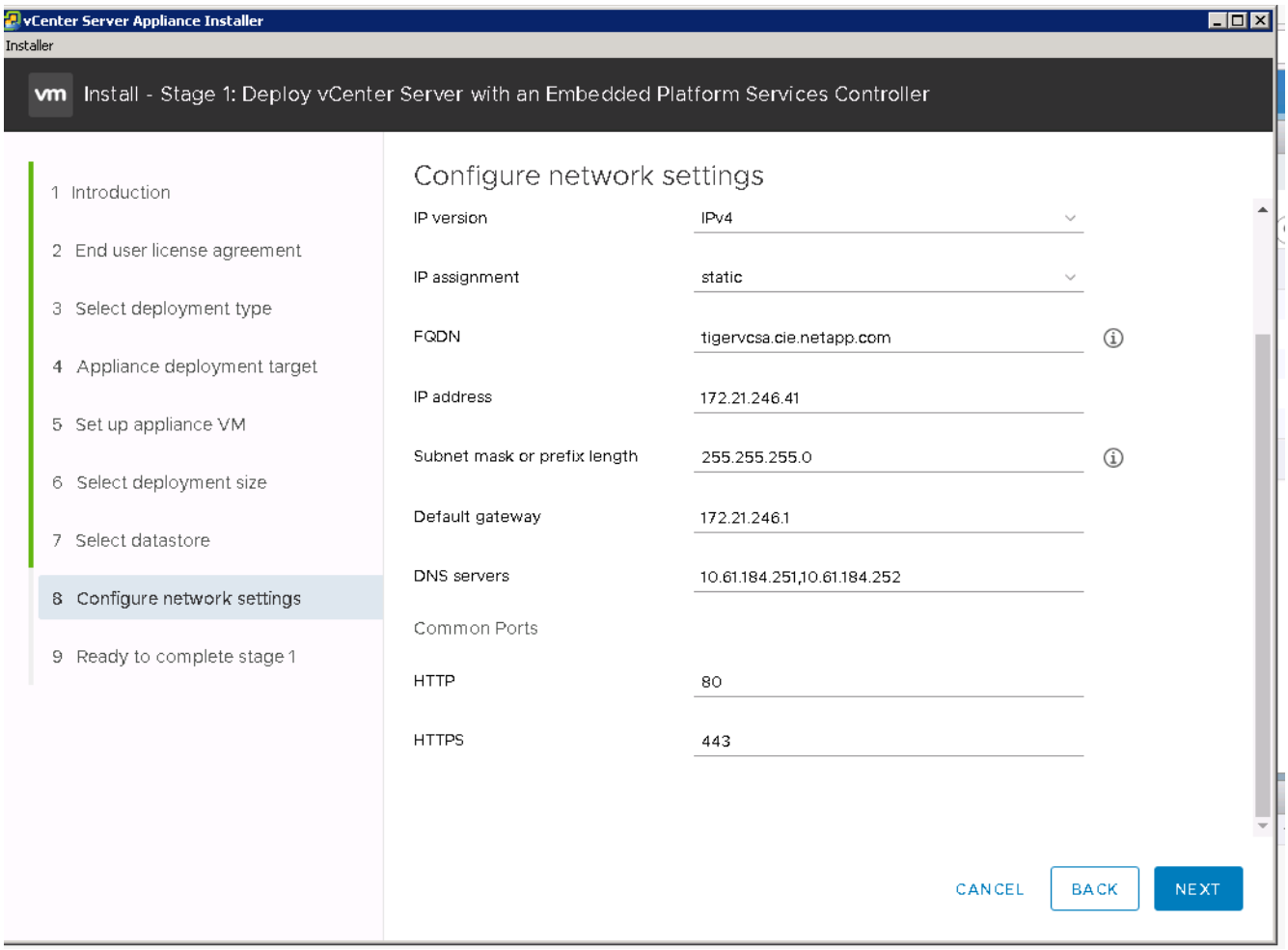
11. Seleccione el tamaño de puesta en marcha que mejor se adapte a su entorno. Haga clic en Siguiente.



12. Seleccione el almacén de datos de infra_datastore_1. Haga clic en Siguiente.

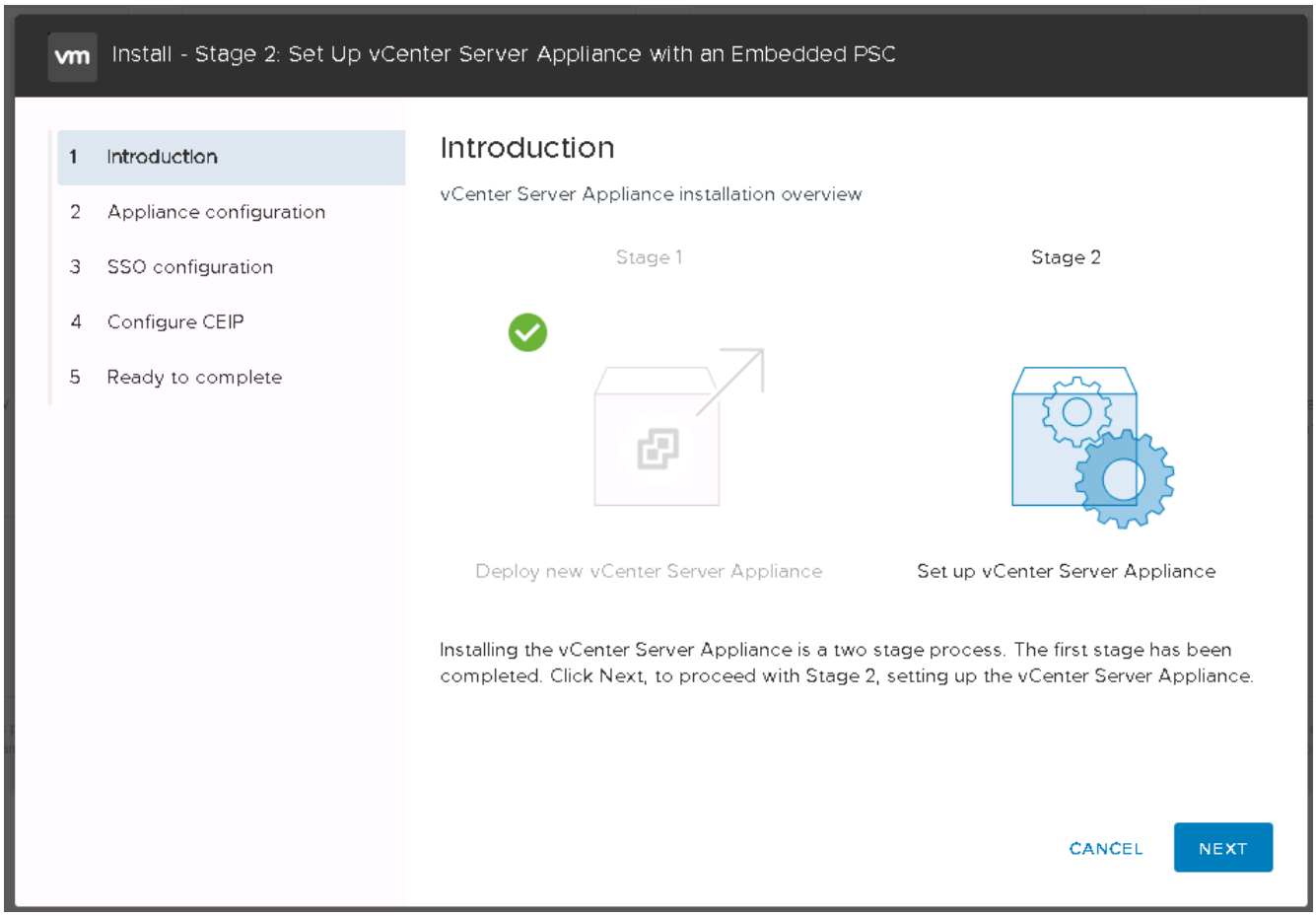


13. Introduzca la siguiente información en la página Configure network settings y haga clic en Next.
    a. Seleccione MGMT-Network para Red.
    b. Introduzca el FQDN o IP que se va a utilizar para la VCSA.
    c. Introduzca la dirección IP que se utilizará.
    d. Introduzca la máscara de subred que 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

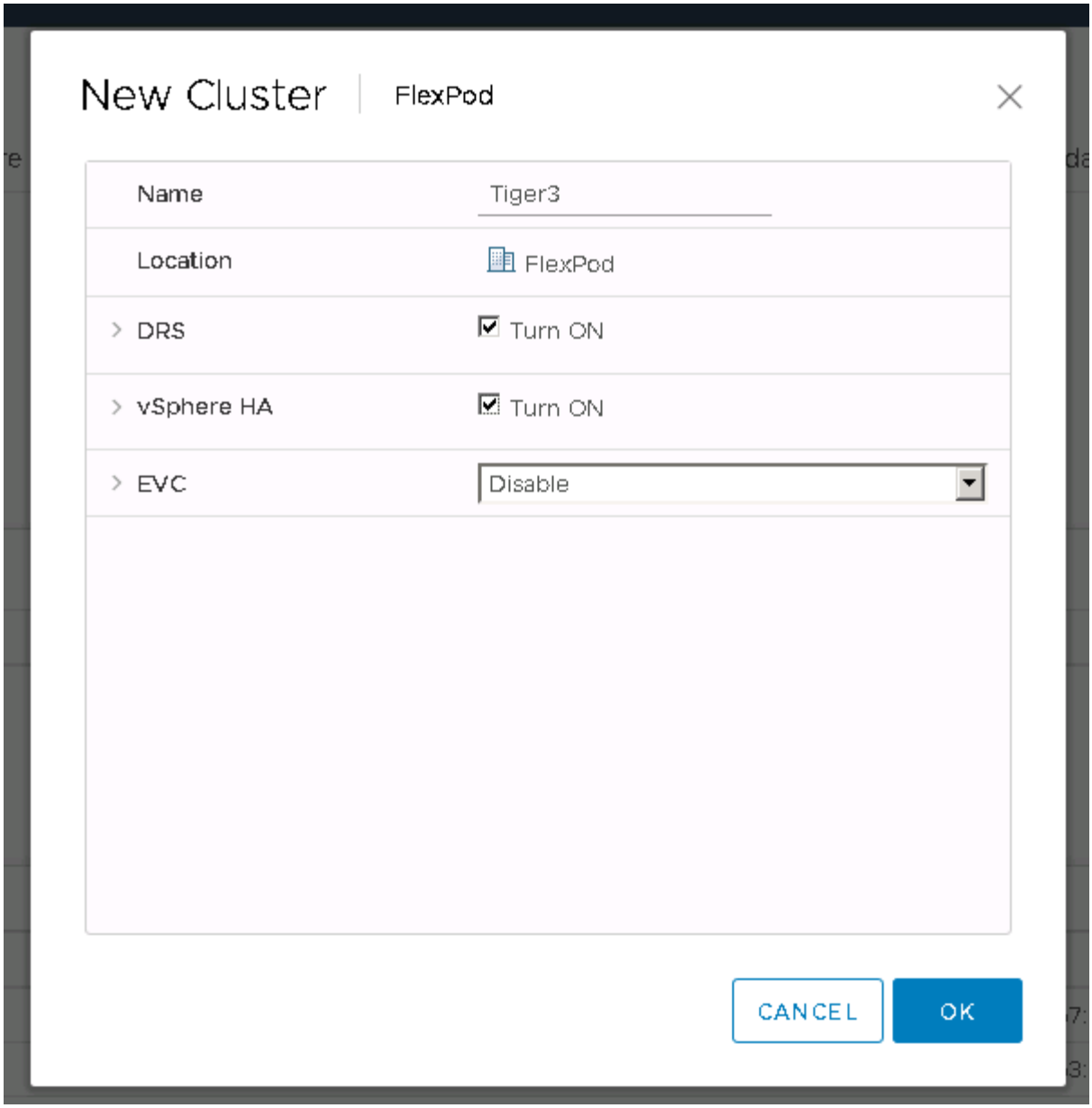
Para configurar la agrupación en clústeres de VMware vCenter Server 6.7 y vSphere, complete los pasos siguientes:

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

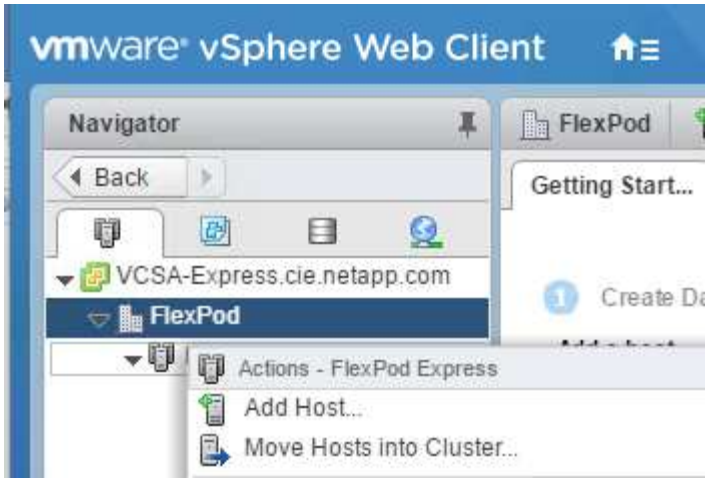
Complete los siguientes pasos para crear un clúster de vSphere:

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.