Procédures de déploiement

FlexPod

NetApp
October 30, 2025

Sommaire

Procédures de déploiement

Ce document décrit en détail la configuration d'un système FlexPod Express entièrement redondant et hautement disponible. Pour refléter cette redondance, les composants configurés à chaque étape sont appelés composant A ou composant B. Par exemple, les contrôleurs A et B identifient les deux contrôleurs de stockage NetApp provisionnés dans ce document. Les commutateurs A et B identifient une paire de commutateurs Cisco Nexus.

Ce document décrit également les étapes de provisionnement de plusieurs hôtes Cisco UCS, identifiés de manière séquentielle en tant que serveur A, serveur B, etc.

Pour indiquer que vous devez inclure dans une étape des informations concernant votre environnement, `<<text>>` s'affiche dans le cadre de la structure de commande. Reportez-vous à l'exemple suivant pour le `vlan create` commande :

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

Ce document vous permet de configurer entièrement l'environnement FlexPod Express. Dans ce processus, plusieurs étapes nécessitent l'insertion de conventions d'appellation spécifiques au client, d'adresses IP et de schémas de réseau local virtuel (VLAN). Le tableau ci-dessous décrit les réseaux VLAN requis pour le déploiement, comme indiqué dans ce guide. Ce tableau peut être complété en fonction des variables spécifiques du site et utilisé pour mettre en œuvre les étapes de configuration du document.

Si vous utilisez des VLAN de gestion intrabande et hors bande distincts, vous devez créer une route de couche 3 entre eux. Pour cette validation, un VLAN de gestion commun a été utilisé.

UN nom	Objectif VLAN	ID utilisé pour valider ce document
VLAN de gestion	VLAN pour les interfaces de gestion	3437
VLAN natif	VLAN auquel des trames non marquées sont attribuées	2
VLAN NFS	VLAN pour le trafic NFS	3438
VLAN VMware vMotion	VLAN désigné pour le déplacement de machines virtuelles d'un hôte physique vers un autre	3441
VLAN trafic des machines virtuelles	VLAN pour le trafic des applications des ordinateurs virtuels	3442
ISCSI-A-VLAN	VLAN pour le trafic iSCSI sur la structure A	3439
ISCSI-B-VLAN	VLAN pour le trafic iSCSI sur la structure B	3440

Les numéros de VLAN sont nécessaires dans toute la configuration de FlexPod Express. Les VLAN sont

appelés `<<var_xxxx_vlan>>`, où `xxxx` Utilise le VLAN (par exemple iSCSI-A).

Le tableau ci-dessous répertorie les machines virtuelles VMware créées.

Description de la machine virtuelle	Nom d'hôte
Serveur VMware vCenter	

Procédure de déploiement Cisco Nexus 3172P

La section suivante décrit la configuration du commutateur Cisco Nexus 3172P utilisée dans un environnement FlexPod Express.

Configuration initiale du commutateur Cisco Nexus 3172P

Les procédures suivantes décrivent la configuration des switchs Cisco Nexus utilisés dans un environnement de base FlexPod Express.

> Cette procédure suppose que vous utilisez un Cisco Nexus 3172P exécutant la version 7.0(3)I7(5) du logiciel NX-OS.

1. Au démarrage initial et à la connexion au port de console du commutateur, le setup Cisco NX-OS démarre automatiquement. Cette configuration initiale traite des paramètres de base, tels que le nom du commutateur, la configuration de l'interface mgmt0 et l'installation de Secure Shell (SSH).
2. Le réseau de gestion FlexPod Express peut être configuré de plusieurs façons. Les interfaces mgmt0 des commutateurs 3172P peuvent être connectées à un réseau de gestion existant ou les interfaces mgmt0 des commutateurs 3172P peuvent être connectées dans une configuration dos à dos. Cependant, ce lien ne peut pas être utilisé pour l'accès à une gestion externe, tel que le trafic SSH.

   Dans ce guide de déploiement, les commutateurs FlexPod Express Cisco Nexus 3172P sont connectés à un réseau de gestion existant.
3. Pour configurer les commutateurs Cisco Nexus 3172P, mettez le commutateur sous tension et suivez les invites à l'écran, comme illustré ici pour la configuration initiale des deux commutateurs, en remplaçant les valeurs appropriées pour les informations spécifiques au commutateur.

```
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. Vous voyez alors un résumé de votre configuration et vous êtes invité à le modifier. Si votre configuration est correcte, entrez `n`.

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

5. Il vous est ensuite demandé si vous souhaitez utiliser cette configuration et l'enregistrer. Si c'est le cas, entrez `y`.

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

6. Répétez cette procédure pour le commutateur Cisco Nexus B.

Activer les fonctionnalités avancées

Certaines fonctionnalités avancées doivent être activées dans Cisco NX-OS pour fournir des options de configuration supplémentaires.

> Le `interface-vlan` la fonction n'est nécessaire que si vous utilisez la fonction dos à dos `mgmt0` option décrite dans ce document. Cette fonction vous permet d'attribuer une adresse IP au VLAN de l'interface (interface virtuelle du commutateur), ce qui permet d'établir des communications de gestion intrabande avec le commutateur (par exemple via SSH).

1. Pour activer les fonctionnalités appropriées sur le commutateur Cisco Nexus A et le commutateur B, passez en mode configuration à l'aide de la commande `(config t)` et exécutez les commandes suivantes :

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

   Le hachage d'équilibrage de charge par défaut du canal de port utilise les adresses IP source et de destination pour déterminer l'algorithme d'équilibrage de charge sur les interfaces du canal de port. Vous pouvez optimiser la distribution entre les membres du canal de port en fournissant davantage d'entrées à l'algorithme de hachage au-delà des adresses IP source et de destination. C'est la même raison que NetApp recommande fortement d'ajouter les ports TCP source et de destination à l'algorithme de hachage.

2. À partir du mode de configuration (`config t`), entrez les commandes suivantes pour définir la configuration d'équilibrage de charge du canal de port global sur les commutateurs Cisco Nexus A et B :

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

Effectuer une configuration globale Spanning Tree

La plateforme Cisco Nexus utilise une nouvelle fonctionnalité de protection appelée Bridge assurance. La fonctionnalité Bridge assurance protège les données contre une liaison unidirectionnelle ou toute autre défaillance logicielle avec un périphérique qui continue à transférer le trafic de données lorsqu'il n'exécute plus l'algorithme Spanning Tree. Les ports peuvent être placés dans l'un des différents États, y compris le réseau ou la périphérie, selon la plate-forme.

NetApp recommande de définir la fonctionnalité Bridge assurance de sorte que tous les ports soient considérés comme des ports réseau par défaut. Ce paramètre oblige l'administrateur réseau à vérifier la configuration de chaque port. Il révèle également les erreurs de configuration les plus courantes, telles que les ports de périphérie non identifiés ou un voisin dont la fonction d'assurance de pont n'est pas activée. En outre, il est plus sûr d'avoir le bloc Spanning Tree de nombreux ports plutôt que trop peu, ce qui permet à l'état de port par défaut d'améliorer la stabilité globale du réseau.

Portez une attention particulière à l'état du Spanning Tree lors de l'ajout de serveurs, de stockage et de commutateurs uplink, surtout s'ils ne prennent pas en charge la garantie des ponts. Dans ce cas, vous devrez peut-être modifier le type de port pour que les ports soient actifs.

La protection BPDU (Bridge Protocol Data Unit) est activée par défaut sur les ports de périphérie comme une autre couche de protection. Pour éviter les boucles du réseau, cette fonction arrête le port si des BPDU provenant d'un autre commutateur sont visibles sur cette interface.

À partir du mode de configuration (`config t`), exécutez les commandes suivantes pour configurer les options par défaut de l'arborescence de Spanning Tree, y compris le type de port par défaut et la protection BPDU, sur le commutateur Cisco Nexus A et le commutateur B :

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

Définir les VLAN

Avant de configurer des ports individuels avec des VLAN différents, les VLAN de couche 2 doivent être définis sur le switch. Il est également recommandé de nommer les réseaux VLAN pour faciliter le dépannage à l'avenir.

À partir du mode de configuration (`config t`), exécutez les commandes suivantes pour définir et décrire les VLAN de couche 2 sur le commutateur Cisco Nexus A et le commutateur B :

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

Configurez les descriptions des ports d'accès et de gestion

Comme c'est le cas avec l'attribution de noms aux VLAN de couche 2, la définition de descriptions pour toutes les interfaces peut aider à la fois pour le provisionnement et le dépannage.

À partir du mode de configuration (`config t`) Dans chacun des commutateurs, entrez les descriptions de port suivantes pour la grande configuration de FlexPod Express :

Commutateur 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
```

Commutateur 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
```

Configuration des interfaces de gestion des serveurs et du stockage

Les interfaces de gestion pour le serveur et le stockage n'utilisent généralement qu'un seul VLAN. Configurez donc les ports de l'interface de gestion en tant que ports d'accès. Définissez le VLAN de gestion pour chaque commutateur et définissez le type de port de l'arborescence sur arête.

À partir du mode de configuration (`config t`), entrez les commandes suivantes pour configurer les paramètres de port pour les interfaces de gestion des serveurs et du stockage :

Commutateur Cisco Nexus A

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

Commutateur Cisco Nexus B

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

Effectuez la configuration globale du canal de port virtuel

Un canal de port virtuel (VPC) permet d'afficher comme un canal de port unique vers un troisième périphérique des liaisons physiquement connectées à deux commutateurs Cisco Nexus différents. Le troisième périphérique peut être un commutateur, un serveur ou tout autre périphérique réseau. Un VPC peut fournir des chemins d'accès multiples de couche 2, ce qui vous permet de créer une redondance en augmentant la bande passante, en activant plusieurs chemins parallèles entre les nœuds et en équilibrant la charge du trafic lorsque d'autres chemins existent.

Un VPC offre les avantages suivants :

- Activation d'un périphérique unique pour utiliser un canal de port sur deux périphériques en amont
- Suppression des ports bloqués par le protocole Spanning Tree
- Topologie sans boucle
- Utilisation de toute la bande passante disponible de la liaison montante
- Assurer une convergence rapide en cas de défaillance de la liaison ou d'un périphérique
- Résilience au niveau de la liaison
- Contribuer à la haute disponibilité

La fonctionnalité VPC nécessite une configuration initiale entre les deux commutateurs Cisco Nexus afin de fonctionner correctement. Si vous utilisez la configuration back-to-back mgt0, utilisez les adresses définies sur les interfaces et vérifiez qu'elles peuvent communiquer à l'aide de la commande ping `[switch_A/B_mgmt0_ip_addr]vrf` commande de gestion.

À partir du mode de configuration (`config t`), exécutez les commandes suivantes pour configurer la configuration globale VPC pour les deux commutateurs :

Commutateur 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
```

Commutateur 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
```

Configurer les canaux du port de stockage

Les contrôleurs de stockage NetApp permettent une connexion active/active au réseau via le protocole LACP (Link Aggregation Control Protocol). L'utilisation de LACP est recommandée, car elle ajoute à la fois la négociation et la journalisation entre les switchs. Du fait que le réseau est configuré pour VPC, cette approche vous permet de disposer de connexions actives-actives du stockage à des commutateurs physiques distincts. Chaque contrôleur dispose de deux liaisons vers chacun des commutateurs. Cependant, les quatre liaisons font partie du même VPC et du même groupe d'interface (IFGRP).

À partir du mode de configuration (`config t`), exécutez les commandes suivantes sur chacun des commutateurs pour configurer les interfaces individuelles et la configuration de canal de port résultante pour les ports connectés au contrôleur AFF NetApp.

1. Exécutez les commandes suivantes sur les commutateurs A et B pour configurer les canaux de port du contrôleur de stockage 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. Exécutez les commandes suivantes sur le commutateur A et le commutateur B pour configurer les canaux de port du contrôleur de stockage 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
```

Une MTU de 9 9000 a été utilisée pour la validation de cette solution. Toutefois, en fonction des exigences de l'application, vous pouvez configurer une valeur MTU appropriée. Il est important de définir la même valeur MTU sur l'ensemble de la solution FlexPod. Des configurations MTU incorrectes entre les composants entraînent la perte de paquets et la mise en paquets.

Configurez les connexions du serveur

Les serveurs Cisco UCS disposent d'une carte d'interface virtuelle à deux ports, VIC11387, utilisée pour le trafic de données et le démarrage du système d'exploitation ESXi via iSCSI. Ces interfaces sont configurées pour basculer les unes sur les autres, assurant ainsi une redondance supplémentaire au-delà d'une liaison

unique. La diffusion de ces liaisons sur plusieurs commutateurs permet au serveur de survivre même à une défaillance complète du commutateur.

À partir du mode de configuration (`config t`), exécutez les commandes suivantes pour configurer les paramètres de port des interfaces connectées à chaque serveur.

Commutateur Cisco Nexus A : configuration Cisco UCS Server-A et 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
```

Commutateur Cisco Nexus B : configuration Cisco UCS Server-A et 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
```

Une MTU de 9 9000 a été utilisée pour la validation de cette solution. Toutefois, en fonction des exigences de l'application, vous pouvez configurer une valeur MTU appropriée. Il est important de définir la même valeur MTU sur l'ensemble de la solution FlexPod. Des configurations MTU incorrectes entre les composants entraînent la perte de paquets et leur transmission devra être de nouveau effectuée. Cela aura un impact sur les performances globales de la solution.

Pour faire évoluer la solution en ajoutant des serveurs Cisco UCS, exécutez les commandes précédentes avec les ports de commutation que les nouveaux serveurs ont été branchés aux commutateurs A et B.

Uplink dans l'infrastructure réseau existante

En fonction de l'infrastructure réseau disponible, il est possible d'utiliser plusieurs méthodes et fonctionnalités pour faire passer l'environnement FlexPod par liaison ascendante. Si vous disposez déjà d'un environnement

Cisco Nexus, NetApp recommande d'utiliser des VPC pour uplink les commutateurs Cisco Nexus 3172P inclus dans l'environnement FlexPod dans l'infrastructure. Les liaisons montantes peuvent être des liaisons montantes 10 GbE pour une solution d'infrastructure 10GbE ou des liaisons 1GbE pour une solution d'infrastructure 1GbE si nécessaire. Les procédures décrites précédemment peuvent être utilisées pour créer une liaison montante VPC vers l'environnement existant. Assurez-vous de lancer la copie en cours pour enregistrer la configuration sur chaque commutateur une fois la configuration terminée.

"Suivant : procédure de déploiement du stockage NetApp (partie 1)"

Procédure de déploiement du stockage NetApp (partie 1)

Cette section décrit la procédure de déploiement du stockage NetApp AFF.

Installation des contrôleurs de stockage NetApp AFF2xx

NetApp Hardware Universe

L'application NetApp Hardware Universe (HWU) offre des composants matériels et logiciels pris en charge pour toute version ONTAP spécifique. Il fournit des informations de configuration pour toutes les appliances de stockage NetApp actuellement prises en charge par le logiciel ONTAP. Il fournit également un tableau des compatibilités de composants.

Vérifiez que les composants matériels et logiciels que vous souhaitez utiliser sont pris en charge avec la version de ONTAP que vous prévoyez d'installer :

1. Accédez au "HWU" application pour afficher les guides de configuration du système. Cliquez sur l'onglet contrôleurs pour afficher la compatibilité entre différentes versions du logiciel ONTAP et les appliances de stockage NetApp avec les spécifications souhaitées.
2. Vous pouvez également comparer les composants par appliance de stockage en cliquant sur Comparer les systèmes de stockage.

Conditions préalables pour le contrôleur AFF2XX Series
Pour planifier l'emplacement physique des systèmes de stockage, consultez le Hardware Universe NetApp. Consultez les sections suivantes : exigences électriques, cordons d'alimentation pris en charge, ports et câbles intégrés.

Contrôleurs de stockage

Suivez les procédures d'installation physique des contrôleurs dans "Documentation AFF A220".

NetApp ONTAP 9.4

Fiche de configuration

Avant d'exécuter le script d'installation, complétez la fiche de configuration du manuel du produit. La fiche de configuration est disponible dans le "Guide de configuration du logiciel ONTAP 9.4".

Ce système est configuré en cluster à 2 nœuds sans commutateur.

Le tableau suivant présente des informations sur l'installation et la configuration de ONTAP 9.4.

Détail du cluster	Valeur des détails du cluster
Adresse IP du nœud de cluster A	<<var_NODEA_mgmt_ip>>
Masque de réseau du nœud de cluster A	<<var_NODEA_mgmt_mask>>
Passerelle de nœud de cluster A	<<var_NODEA_mgmt_Gateway>>
Nom du nœud de cluster A	<<var_NODEA>>
Adresse IP du nœud B du cluster	<<var_NodeB_mgmt_ip>>
Masque de réseau du nœud B du cluster	<<var_NodeB_mgmt_mask>>
Passerelle de nœud B du cluster	<<var_NodeB_mgmt_Gateway>>
Nom du nœud B du cluster	<<var_NodeB>>
URL ONTAP 9.4	<<var_url_boot_software>>
Nom du cluster	<<var_clustername>>
Adresse IP de gestion du cluster	<<var_clustermgmt_ip>>
Passerelle du cluster B	<<var_clustermgmt_gateway>>
Masque de réseau du cluster B.	\<<var_clustermgmt_mask>
Nom de domaine	<<nom_domaine_var>>
IP du serveur DNS (vous pouvez entrer plusieurs adresses)	<<var_dns_server_ip>>
IP de serveur NTP (vous pouvez entrer plusieurs adresses)	<<var_ntp_server_ip>>

Configurez le nœud A

Pour configurer le nœud A, procédez comme suit :

1. Effectue la connexion au port console du système de stockage. Une invite chargeur-A s'affiche. Cependant, si le système de stockage est dans une boucle de redémarrage, appuyez sur Ctrl-C pour quitter la boucle AUTOBOOT lorsque le message suivant s'affiche :

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

2. Laissez le système démarrer.

   ```
   autoboot
   ```

3. Appuyez sur Ctrl-C pour accéder au menu de démarrage.

   Si ONTAP 9.4 n'est pas la version du logiciel en cours de démarrage, procédez comme suit pour installer le nouveau logiciel. Si ONTAP 9.4 est la version en cours de démarrage, sélectionnez les options 8 et y pour redémarrer le nœud. Ensuite, passez à l'étape 14.

4. Pour installer un nouveau logiciel, sélectionnez option `7`.

5. Entrez `y` pour effectuer une mise à niveau.
6. Sélectionnez `e0M` pour le port réseau que vous souhaitez utiliser pour le téléchargement.
7. Entrez `y` pour redémarrer maintenant.
8. Entrez l'adresse IP, le masque de réseau et la passerelle par défaut de e0M à leurs emplacements respectifs.

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

9. Entrez l'URL de l'emplacement du logiciel.

   Ce serveur Web doit être accessible.

```
<<var_url_boot_software>>
```

10. Appuyez sur entrée pour le nom d'utilisateur, indiquant aucun nom d'utilisateur.
11. Entrez `y` pour définir le nouveau logiciel installé comme logiciel par défaut à utiliser pour les redémarrages suivants.
12. Entrez `y` pour redémarrer le nœud.

    Lors de l'installation d'un nouveau logiciel, le système peut effectuer des mises à niveau du micrologiciel vers le BIOS et les cartes d'adaptateur, ce qui entraîne des redémarrages et des arrêts possibles à l'invite du chargeur-A. Si ces actions se produisent, le système peut différer de cette procédure.

13. Appuyez sur Ctrl-C pour accéder au menu de démarrage.
14. Sélectionnez option `4` Pour une configuration propre et une initialisation de tous les disques.
15. Entrez `y` pour zéro disque, réinitialisez la configuration et installez un nouveau système de fichiers.
16. Entrez `y` pour effacer toutes les données sur les disques.

    L'initialisation et la création de l'agrégat root peuvent prendre au moins 90 minutes, selon le nombre et le type de disques connectés. Une fois l'initialisation terminée, le système de stockage redémarre. Notez que l'initialisation des disques SSD prend beaucoup moins de temps. Vous pouvez continuer à utiliser la configuration du nœud B pendant que les disques du nœud A sont à zéro.

17. Lorsque le nœud A est en cours d'initialisation, commencez à configurer le nœud B.

Configurer le nœud B

Pour configurer le nœud B, procédez comme suit :

1. Effectue la connexion au port console du système de stockage. Une invite chargeur-A s'affiche. Cependant, si le système de stockage est dans une boucle de redémarrage, appuyez sur Ctrl-C pour quitter la boucle AUTOBOOT lorsque le message suivant s'affiche :

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

2. Appuyez sur Ctrl-C pour accéder au menu de démarrage.

```
autoboot
```

3. Appuyez sur Ctrl-C lorsque vous y êtes invité.

   Si ONTAP 9.4 n'est pas la version du logiciel en cours de démarrage, procédez comme suit pour installer le nouveau logiciel. Si ONTAP 9.4 est la version en cours de démarrage, sélectionnez les options 8 et y pour redémarrer le nœud. Ensuite, passez à l'étape 14.

4. Pour installer un nouveau logiciel, sélectionnez l'option 7.
5. Entrez `y` pour effectuer une mise à niveau.
6. Sélectionnez `e0M` pour le port réseau que vous souhaitez utiliser pour le téléchargement.
7. Entrez `y` pour redémarrer maintenant.
8. Entrez l'adresse IP, le masque de réseau et la passerelle par défaut de e0M à leurs emplacements respectifs.

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

9. Entrez l'URL de l'emplacement du logiciel.

   Ce serveur Web doit être accessible.

```
<<var_url_boot_software>>
```

10. Appuyez sur entrée pour le nom d'utilisateur, indiquant aucun nom d'utilisateur.
11. Entrez `y` pour définir le nouveau logiciel installé comme logiciel par défaut à utiliser pour les redémarrages suivants.
12. Entrez `y` pour redémarrer le nœud.

    Lors de l'installation d'un nouveau logiciel, le système peut effectuer des mises à niveau du micrologiciel vers le BIOS et les cartes d'adaptateur, ce qui entraîne des redémarrages et des arrêts possibles à l'invite du chargeur-A. Si ces actions se produisent, le système peut différer de cette procédure.

13. Appuyez sur Ctrl-C pour accéder au menu de démarrage.
14. Sélectionnez l'option 4 pour nettoyer la configuration et initialiser tous les disques.
15. Entrez `y` pour zéro disque, réinitialisez la configuration et installez un nouveau système de fichiers.
16. Entrez `y` pour effacer toutes les données sur les disques.

    L'initialisation et la création de l'agrégat root peuvent prendre au moins 90 minutes, selon le nombre et le type de disques connectés. Une fois l'initialisation terminée, le système de stockage redémarre. Notez que l'initialisation des disques SSD prend beaucoup moins de temps.

Suite de la configuration du nœud A et de la configuration du cluster

À partir d'un programme de port de console connecté au port de console Du contrôleur de stockage A (nœud A), exécutez le script de configuration du nœud. Ce script apparaît lors du premier démarrage de ONTAP 9.4 sur le nœud.

La procédure de configuration du nœud et du cluster a été légèrement modifiée dans ONTAP 9.4. L'assistant d'installation du cluster permet de configurer le premier nœud d'un cluster et System Manager sert à configurer le cluster.

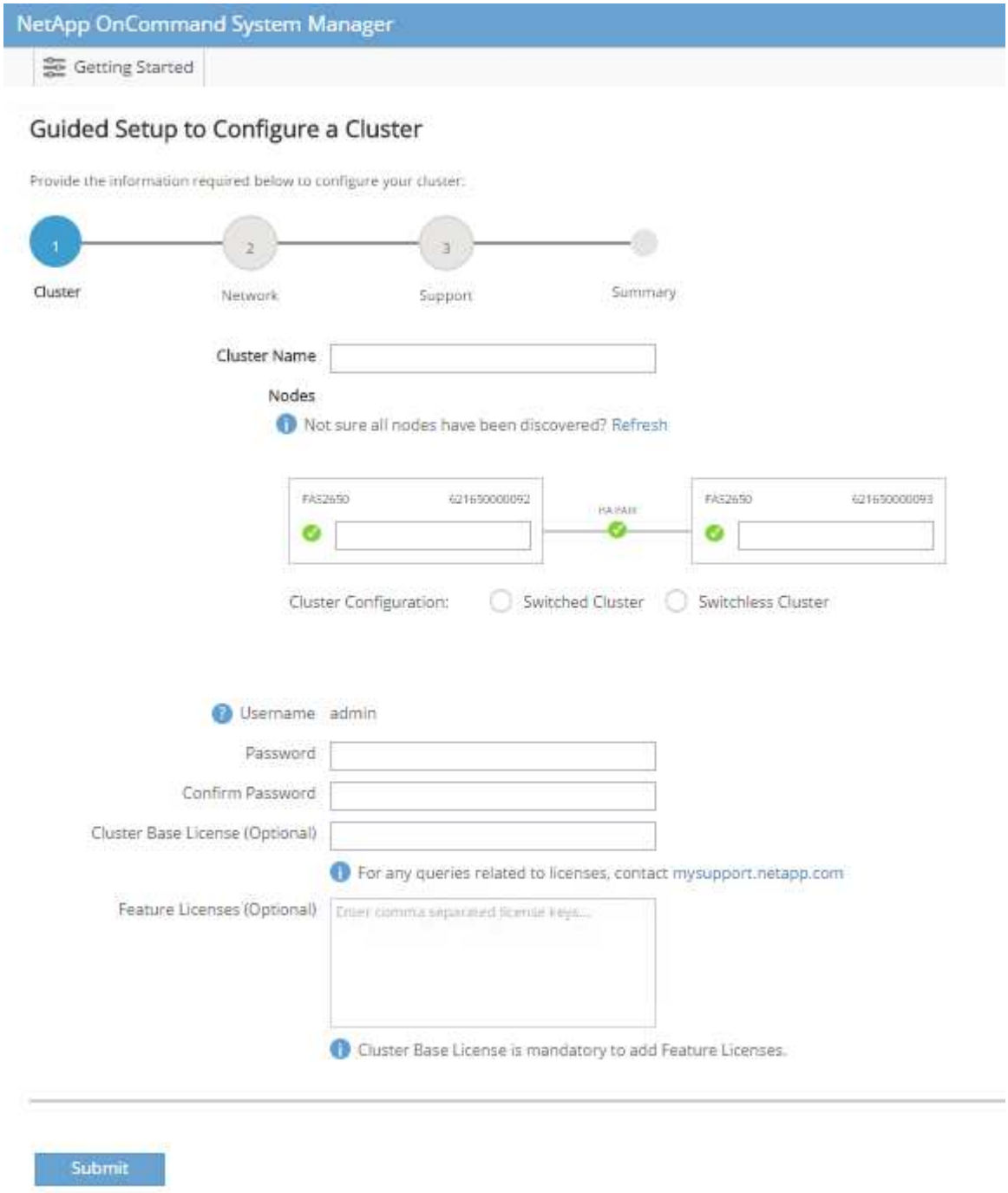
1. Suivez les invites pour configurer le nœud A.

```
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. Accédez à l'adresse IP de l'interface de gestion du nœud.

   La configuration du cluster peut également être effectuée au moyen de l'interface de ligne de commandes. Ce document décrit la configuration du cluster à l'aide de la configuration assistée de NetApp System Manager.

3. Cliquez sur installation assistée pour configurer le cluster.
4. Entrez `<<var_clustername>>` pour les noms de cluster et `<<var_nodeA>>` et `<<var_nodeB>>` pour chacun des nœuds que vous configurez. Saisissez le mot de passe que vous souhaitez utiliser pour le système de stockage. Sélectionnez Switchless Cluster pour le type de cluster. Indiquez la licence de base du cluster.



5. Vous pouvez également entrer des licences de fonctions pour Cluster, NFS et iSCSI.
6. Vous voyez un message de statut indiquant que le cluster est en cours de création. Ce message d'état passe en revue plusieurs États. Ce processus prend plusieurs minutes.
7. Configurez le réseau.
   a. Désélectionnez l'option Plage d'adresses IP.

b. Entrez `<<var_clustermgmt_ip>>` Dans le champ adresse IP de gestion du cluster, `<<var_clustermgmt_mask>>` Dans le champ masque réseau, et `<<var_clustermgmt_gateway>>` Dans le champ passerelle. Utilisez le … Sélecteur dans le champ Port pour sélectionner e0M du nœud A.

c. L'IP de gestion des nœuds du nœud A est déjà renseignée. Entrez `<<var_nodeA_mgmt_ip>>` Pour le nœud B.

d. Entrez `<<var_domain_name>>` Dans le champ Nom de domaine DNS. Entrez `<<var_dns_server_ip>>` Dans le champ adresse IP du serveur DNS.

   Vous pouvez entrer plusieurs adresses IP de serveur DNS.

e. Entrez `<<var_ntp_server_ip>>` Dans le champ serveur NTP principal.

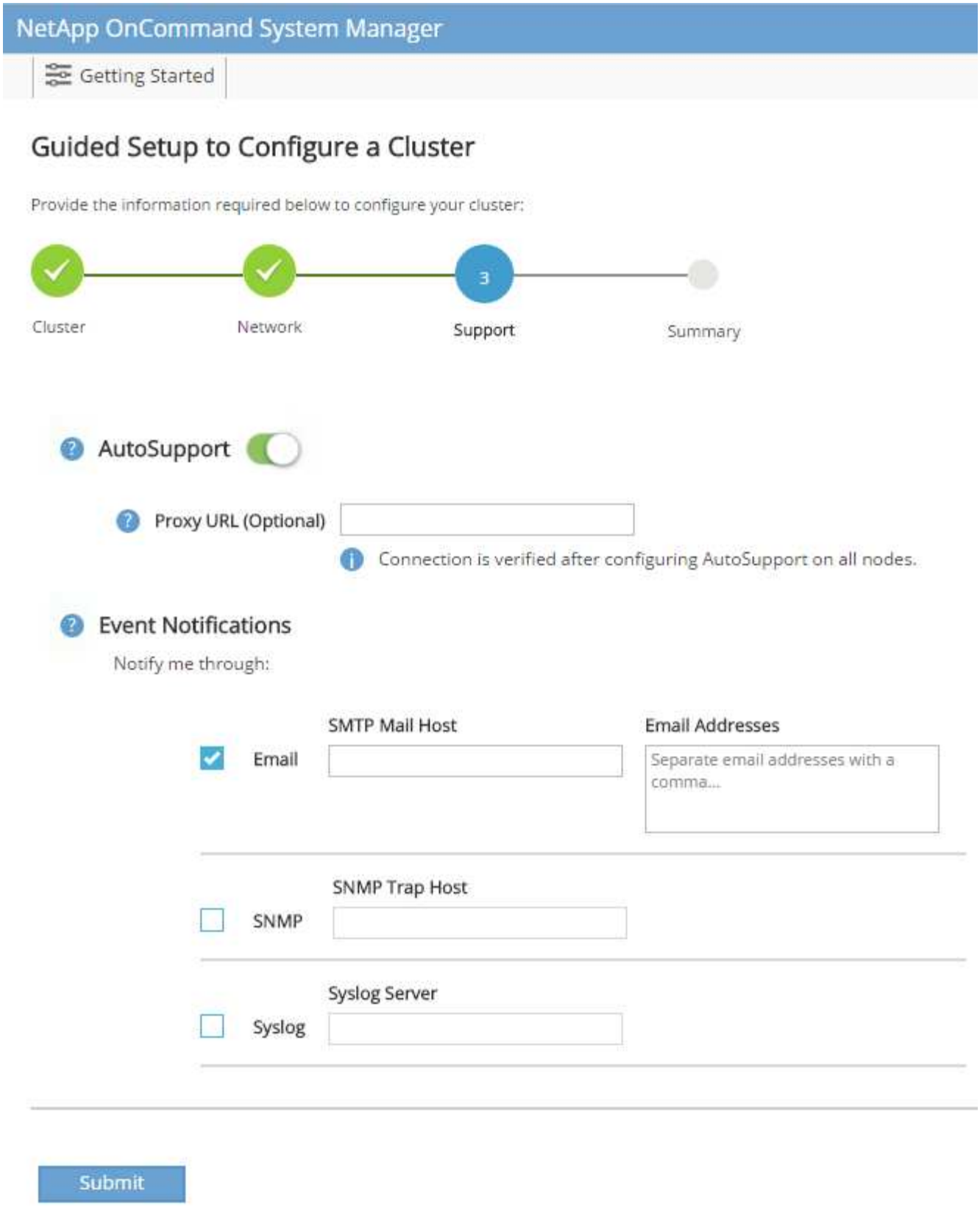
   Vous pouvez également entrer un autre serveur NTP.

8. Configuration des informations de support.

   a. Si votre environnement requiert un proxy pour accéder à AutoSupport, entrez l'URL dans l'URL du proxy.

   b. Entrez l'hôte de messagerie SMTP et l'adresse électronique pour les notifications d'événements.

      Vous devez au moins configurer la méthode de notification d'événement avant de pouvoir continuer. Vous pouvez sélectionner n'importe quelle méthode.



9. Lorsque la configuration du cluster est terminée, cliquez sur gérer le cluster pour configurer le stockage.

Suite de la configuration du cluster de stockage

Une fois la configuration des nœuds de stockage et du cluster de base terminée, vous pouvez poursuivre la configuration du cluster de stockage.

Zéro de tous les disques de spare

Pour mettre zéro tous les disques de spare du cluster, exécutez la commande suivante :

```
disk zerospares
```

Définissez l'option de personnalisation des ports UTA2 intégrés

1. Vérifiez le mode actuel et le type actuel des ports en exécutant le `ucadmin show` commande.

```
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. Vérifiez que le mode actuel des ports en cours d'utilisation est `cna` et que le type actuel est défini sur `target`. Si ce n'est pas le cas, modifiez la personnalité du port à l'aide de la commande suivante :

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

Les ports doivent être hors ligne pour exécuter la commande précédente. Pour mettre un port hors ligne, exécutez la commande suivante :

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

Si vous avez modifié la personnalité du port, vous devez redémarrer chaque nœud pour que le changement prenne effet.

Renommage des interfaces logiques de gestion

Pour renommer les LIFs de management, effectuez la procédure suivante :

1. Affiche les noms des LIF de gestion actuelles.

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

2. Renommer la LIF de gestion de cluster.

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

3. Renommez la LIF de gestion du nœud B.

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

Définissez le rétablissement automatique sur la gestion du cluster

Réglez le `auto-revert` paramètre de l'interface de gestion du cluster.

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

Configurez l'interface réseau du processeur de service

Pour attribuer une adresse IPv4 statique au processeur de service sur chaque nœud, exécutez les commandes suivantes :

```
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>>
```

Les adresses IP du processeur de service doivent se trouver dans le même sous-réseau que les adresses IP de gestion du nœud.

Activez le basculement du stockage dans ONTAP

Pour vérifier que le basculement du stockage est activé, exécutez les commandes suivantes dans une paire

de basculement :

1. Vérification de l'état du basculement du stockage

   ```
   storage failover show
   ```

   Les deux <<var_nodeA>> et <<var_nodeB>> doit pouvoir effectuer un basculement. Accédez à l'étape 3 si les nœuds peuvent effectuer un basculement.

2. Activez le basculement sur l'un des deux nœuds.

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

   L'activation du basculement sur un nœud l'active pour les deux nœuds.

3. Vérifiez l'état de la HA du cluster à deux nœuds.

   Cette étape ne s'applique pas aux clusters comptant plus de deux nœuds.

   ```
   cluster ha show
   ```

4. Passez à l'étape 6 si la haute disponibilité est configurée. Si la haute disponibilité est configurée, le message suivant s'affiche lors de l'émission de la commande :

   ```
   High Availability Configured: true
   ```

5. Activez le mode HA uniquement pour le cluster à deux nœuds.

   > N'exécutez pas cette commande pour les clusters avec plus de deux nœuds, car cela entraîne des problèmes de basculement.

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

6. Vérifiez que l'assistance matérielle est correctement configurée et modifiez, si nécessaire, l'adresse IP du partenaire.

   ```
   storage failover hwassist show
   ```

   Le message `Keep Alive Status : Error: did not receive hwassist keep alive alerts from partner` indique que l'assistance matérielle n'est pas configurée. Exécutez les commandes suivantes pour configurer l'assistance matérielle.

```
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>>
```

Créez un domaine de diffusion MTU de trames Jumbo dans ONTAP

Pour créer un domaine de diffusion de données avec un MTU de 9 9000, exécutez les commandes suivantes :

```
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
```

Supprime les ports de données du broadcast domain par défaut

Les ports de données 10 GbE sont utilisés pour le trafic iSCSI/NFS. Ces ports doivent être supprimés du domaine par défaut. Les ports e0e et e0f ne sont pas utilisés et doivent également être supprimés du domaine par défaut.

Pour supprimer les ports du broadcast domain, lancer la commande suivante :

```
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
```

Désactiver le contrôle de flux sur les ports UTA2

Il est recommandé par NetApp de désactiver le contrôle de flux sur tous les ports UTA2 connectés à des périphériques externes. Pour désactiver le contrôle de flux, lancer la commande suivante :

```
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
```

Configurez le protocole LACP IFGRP dans ONTAP

Ce type de groupe d'interface nécessite au moins deux interfaces Ethernet et un switch qui prend en charge LACP. S'assurer que le commutateur est correctement configuré.

Dans l'invite de cluster, effectuez la procédure suivante.

```
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
```

Configuration des trames Jumbo dans NetApp ONTAP

Pour configurer un port réseau ONTAP afin d'utiliser des trames Jumbo (qui possèdent généralement un MTU de 1 9,000 octets), exécutez les commandes suivantes depuis le shell du cluster :

```
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
```

Créez des VLAN dans ONTAP

Pour créer des VLAN dans ONTAP, procédez comme suit :

1. Créez des ports VLAN NFS et ajoutez-les au domaine de broadcast de données.

```
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. Créez des ports VLAN iSCSI et ajoutez-les au domaine de diffusion de données.

```
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. Créez des ports 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>>
```

Créez des agrégats dans ONTAP

Un agrégat contenant le volume root est créé lors du processus de setup ONTAP. Pour créer des agrégats supplémentaires, déterminez le nom de l'agrégat, le nœud sur lequel il doit être créé, ainsi que le nombre de disques qu'il contient.

Pour créer des agrégats, lancer les commandes suivantes :

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

Conservez au moins un disque (sélectionnez le plus grand disque) dans la configuration comme disque de rechange. Il est recommandé d'avoir au moins une unité de rechange pour chaque type et taille de disque.

Commencez par cinq disques ; vous pouvez ajouter des disques à un agrégat lorsque du stockage supplémentaire est requis.

L'agrégat ne peut pas être créé tant que la remise à zéro du disque n'est pas terminée. Exécutez le `aggr show` commande permettant d'afficher l'état de création de l'agrégat. Ne pas continuer avant `aggr1`_`nodeA` est en ligne.

Configurer le fuseau horaire dans ONTAP

Pour configurer la synchronisation de l'heure et pour définir le fuseau horaire sur le cluster, exécutez la commande suivante :

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

Par exemple, dans l'est des États-Unis, le fuseau horaire est `America/New York`. Après avoir commencé à saisir le nom du fuseau horaire, appuyez sur la touche Tab pour afficher les options disponibles.

Configurez SNMP dans ONTAP

Pour configurer le SNMP, procédez comme suit :

1. Configurer les informations de base SNMP, telles que l'emplacement et le contact. Lorsqu'elle est interrogée, cette information est visible comme `sysLocation` et `sysContact` Variables dans SNMP.

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

2. Configurez les interruptions SNMP pour envoyer aux hôtes distants.

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

Configurez SNMPv1 dans ONTAP

Pour configurer SNMPv1, définissez le mot de passe secret partagé en texte brut appelé communauté.

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

Utilisez le `snmp community delete all` commande avec précaution. Si des chaînes de communauté sont utilisées pour d'autres produits de surveillance, cette commande les supprime.

Configurez SNMPv3 dans ONTAP

SNMPv3 requiert la définition et la configuration d'un utilisateur pour l'authentification. Pour configurer SNMPv3, effectuez les étapes suivantes :

1. Exécutez le `security snmpusers` Commande permettant d'afficher l'ID du moteur.
2. Créez un utilisateur appelé `snmpv3user`.

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

3. Entrez l'ID moteur de l'entité faisant autorité et sélectionnez `md5` en tant que protocole d'authentification.
4. Lorsque vous y êtes invité, entrez un mot de passe de huit caractères minimum pour le protocole d'authentification.
5. Sélectionnez `des` comme protocole de confidentialité.
6. Entrez un mot de passe de huit caractères minimum pour le protocole de confidentialité lorsque vous y êtes invité.

Configurez AutoSupport HTTPS dans ONTAP

L'outil NetApp AutoSupport envoie à NetApp des informations de résumé du support via HTTPS. Pour configurer AutoSupport, lancer la commande suivante :

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

Créez un serveur virtuel de stockage

Pour créer une infrastructure de SVM (Storage Virtual machine), procédez comme suit :

1. Exécutez le `vserver create` commande.

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

2. Ajoutez l'agrégat de données à la liste INFRA-SVM pour NetApp VSC.

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

3. Retirer les protocoles de stockage inutilisés du SVM, tout en conservant les protocoles NFS et iSCSI.

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

4. Activer et exécuter le protocole NFS dans le SVM infra-SVM.

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

5. Allumez le `SVM vstorage` Paramètre du plug-in NetApp NFS VAAI. Ensuite, vérifiez que NFS a été

configuré.

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

Les commandes sont préfaites par `vserver` dans la ligne de commande, car les ordinateurs virtuels de stockage étaient auparavant appelés serveurs.

Configurez NFSv3 dans ONTAP

Le tableau suivant répertorie les informations nécessaires pour mener à bien cette configuration.

Détails	Valeur de détail
Hôte ESXi D'Une adresse IP NFS	<<var_esxi_hostA_nfs_ip>>
Adresse IP NFS de l'hôte ESXi B	<<var_esxi_hostB_nfs_ip>>

Pour configurer NFS sur le SVM, lancer les commandes suivantes :

1. Créez une règle pour chaque hôte ESXi dans la stratégie d'exportation par défaut.
2. Pour chaque hôte ESXi créé, attribuez une règle. Chaque hôte a son propre index de règles. Votre premier hôte ESXi dispose de l'index de règles 1, votre second hôte ESXi dispose de l'index de règles 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. Assigner la export policy au volume root du SVM d'infrastructure.

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

NetApp VSC gère automatiquement les règles d'exportation si vous choisissez de l'installer une fois vSphere configuré. Si vous ne l'installez pas, vous devez créer des règles d'export policy lorsque des serveurs Cisco UCS C-Series supplémentaires sont ajoutés.

Créez le service iSCSI dans ONTAP

Pour créer le service iSCSI, procédez comme suit :

1. Créer le service iSCSI sur la SVM. Cette commande démarre également le service iSCSI et définit l'IQN iSCSI pour la SVM. Vérifiez que le protocole iSCSI a été configuré.

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

Créer un miroir de partage de charge du volume racine du SVM dans ONTAP

1. Créer un volume pour être le miroir de partage de charge du volume root du SVM d'infrastructure sur chaque nœud.

```
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. Créer un programme de travail pour mettre à jour les relations de miroir de volume racine toutes les 15 minutes.

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

3. Créer les relations de mise en miroir.

```
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. Initialisez la relation de mise en miroir et vérifiez qu'elle a été créée.

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

Configurez l'accès HTTPS dans ONTAP

Pour configurer un accès sécurisé au contrôleur de stockage, procédez comme suit :

1. Augmentez le niveau de privilège pour accéder aux commandes de certificat.

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

2. En général, un certificat auto-signé est déjà en place. Vérifiez le certificat en exécutant la commande suivante :

```
security certificate show
```

3. Pour chaque SVM affiché, le nom commun du certificat doit correspondre au FQDN DNS du SVM. Les quatre certificats par défaut doivent être supprimés et remplacés par des certificats auto-signés ou des certificats d'une autorité de certification.

   La suppression de certificats expirés avant de créer des certificats est une bonne pratique. Exécutez le `security certificate delete` commande permettant de supprimer les certificats expirés. Dans la commande suivante, utilisez L'option D'achèvement PAR ONGLET pour sélectionner et supprimer chaque certificat par défaut.

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

4. Pour générer et installer des certificats auto-signés, exécutez les commandes suivantes en tant que commandes à durée unique. Générer un certificat de serveur pour l'infra-SVM et le SVM de cluster. Là encore, utilisez la saisie AUTOMATIQUE PAR TABULATION pour vous aider à compléter ces commandes.

```
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. Pour obtenir les valeurs des paramètres requis à l'étape suivante, exécutez la `security certificate show` commande.
6. Activez chaque certificat qui vient d'être créé à l'aide de `-server-enabled true` et `-client-enabled false` paramètres. Utilisez de nouveau la saisie AUTOMATIQUE PAR TABULATION.

```
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. Configurez et activez l'accès SSL et HTTPS, et désactivez l'accès 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>>
```

Il est normal que certaines de ces commandes renvoient un message d'erreur indiquant que l'entrée n'existe pas.

8. Ne rétablit pas le niveau de privilège admin et crée l'installation pour permettre la disponibilité de la SVM par le web.

```
set -privilege admin
vserver services web modify -name spi|ontapi|compat -vserver * -enabled
true
```

Créez un volume NetApp FlexVol dans ONTAP

Pour créer un volume NetApp FlexVol, entrez le nom, la taille et l'agrégat sur lequel il existe. Créer deux volumes de datastore VMware et un volume de démarrage de serveur.

```
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
```

Activez la déduplication dans ONTAP

Pour activer la déduplication sur les volumes appropriés, exécutez les commandes suivantes :

```
volume efficiency on -vserver Infra-SVM -volume infra_datastore_1
volume efficiency on -vserver Infra-SVM -volume esxi_boot
```

Créer des LUN dans ONTAP

Pour créer deux LUN de démarrage, exécutez les commandes suivantes :

```
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
```

Lorsque vous ajoutez un serveur Cisco UCS C-Series supplémentaire, vous devez créer un LUN de démarrage supplémentaire.

Création des LIFs iSCSI dans ONTAP

Le tableau suivant répertorie les informations nécessaires pour mener à bien cette configuration.

Détails	Valeur de détail
Nœud de stockage A iSCSI LIF01A	<<var_NODEA_iscsi_lif01a_ip>>
Masque de réseau LIF01A iSCSI du nœud de stockage	<<var_NODEA_iscsi_lif01a_masque>>
Nœud de stockage A iSCSI LIF01B	<<var_NODEA_iscsi_lif01b_ip>>
Masque de réseau LIF01B iSCSI sur le nœud de stockage	<<var_NODEA_iscsi_lif01b_mask>>
Nœud de stockage B iSCSI LIF01A	<<var_NodeB_iscsi_lif01a_ip>>
Masque de réseau du nœud de stockage B iSCSI LIF01A	<<var_NodeB_iscsi_lif01a_masque>>
Nœud de stockage B iSCSI LIF01B	<<var_NodeB_iscsi_lif01b_ip>>
Masque de réseau du nœud de stockage B iSCSI LIF01B	<<var_NodeB_iscsi_lif01b_mask>>

1. Création de quatre LIF iSCSI, deux sur chaque nœud

```
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
```

Création des LIFs NFS dans ONTAP

Le tableau suivant répertorie les informations nécessaires pour mener à bien cette configuration.

Détails	Valeur de détail
Nœud de stockage A NFS LIF 01 IP	<<var_NODEA_nfs_lif_01_ip>>
Nœud de stockage A masque réseau NFS LIF 01	<<var_NODEA_nfs_lif_01_mask>>
Nœud de stockage B NFS LIF 02 IP	<<var_NodeB_nfs_lif_02_ip>>
Masque de réseau LIF 02 du nœud de stockage B NFS	<<var_NodeB_nfs_lif_02_mask>>

1. Créer une 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
```

Ajoutez un administrateur SVM d'infrastructure

Le tableau suivant répertorie les informations nécessaires pour mener à bien cette configuration.

Détails	Valeur de détail
IP de Vsmgmt	<<var_svm_mgmt_ip>>
Masque de réseau Vsmgmt	<<var_svm_mgmt_mask>>
Passerelle par défaut de Vsmgmt	<<var_svm_mgmt_gateway>>

Pour ajouter l'administrateur du SVM d'infrastructure et l'interface logique d'administration du SVM au réseau de gestion, effectuez les opérations suivantes :

1. Exécutez la commande suivante :

```
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
```

> L'IP de gestion SVM devrait ici se trouver dans le même sous-réseau que l'IP de gestion du cluster de stockage.

2. Créer une route par défaut pour permettre à l'interface de gestion du SVM d'atteindre le monde extérieur.

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

3. Définir un mot de passe pour l'utilisateur SVM vsadmin et déverrouiller l'utilisateur

```
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
```

"Suivant : procédure de déploiement du serveur en rack Cisco UCS C-Series"

Procédure de déploiement des serveurs en rack Cisco UCS C-Series

La section suivante fournit une procédure détaillée de configuration d'un serveur en rack autonome Cisco UCS C-Series à utiliser dans la configuration FlexPod Express.

Configurez le serveur autonome Cisco UCS C-Series initial pour le serveur de gestion intégré Cisco

Suivez ces étapes pour la configuration initiale de l'interface CIMC pour les serveurs autonomes Cisco UCS C-Series.

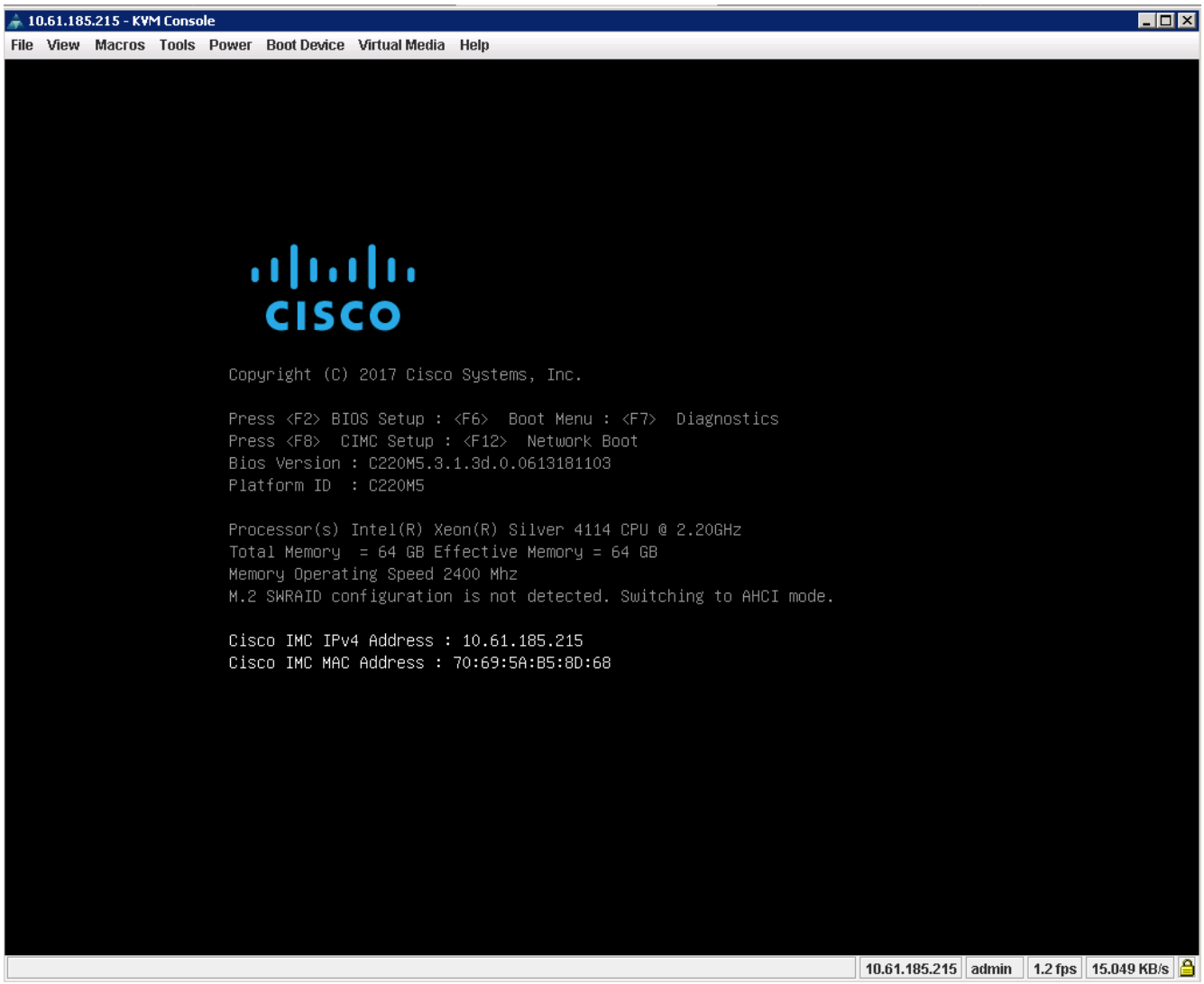
Le tableau suivant répertorie les informations nécessaires à la configuration de CIMC pour chaque serveur autonome Cisco UCS C-Series.

Détails	Valeur de détail
Adresse IP de CIMC	<<cimc_ip>>
Masque de sous-réseau CIMC	<<masque de réseau_cimc>>
Passerelle par défaut CIMC	<<cimc_gateway>>

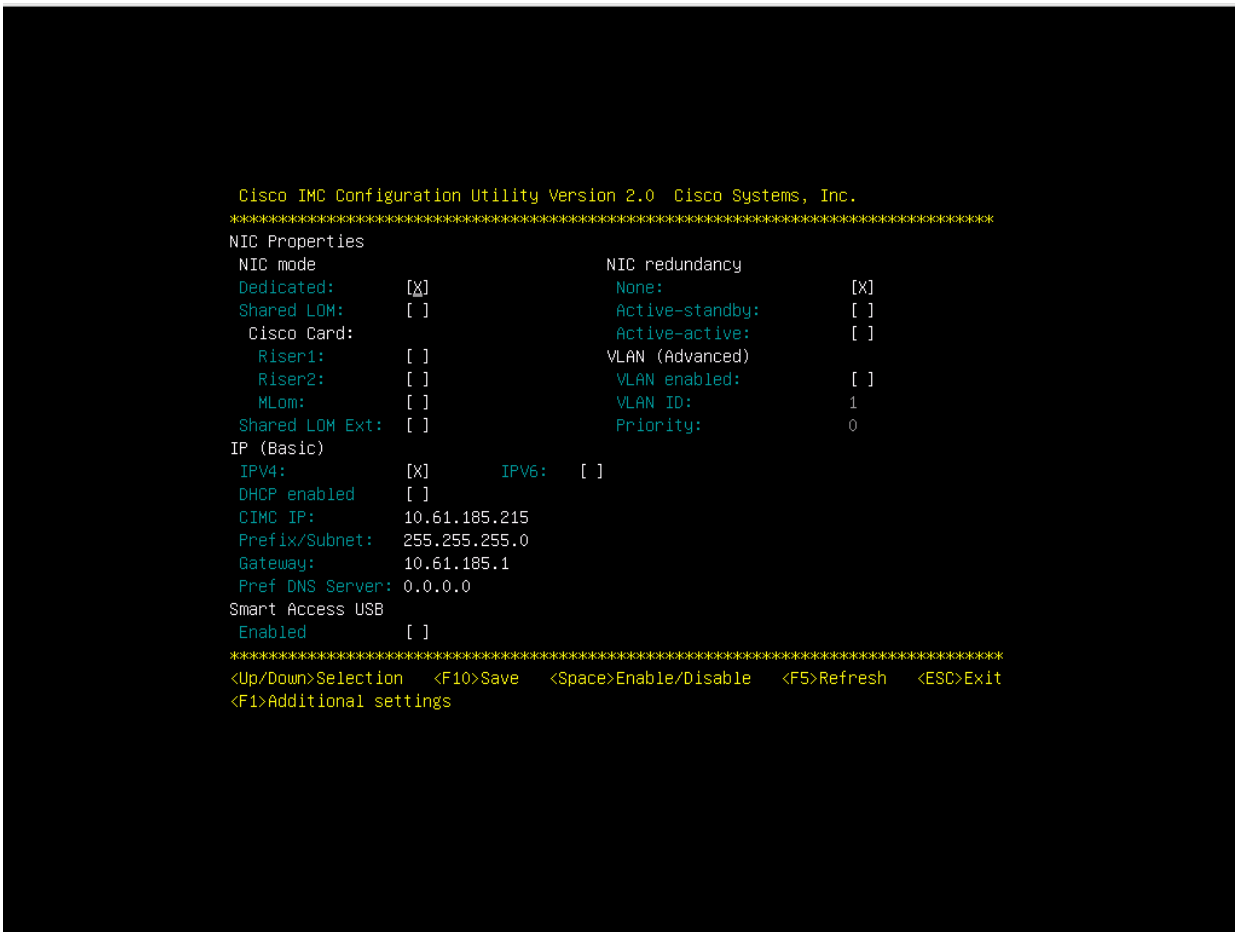
La version CIMC utilisée dans cette validation est CIMC 3.1.3(g).

Tous les serveurs

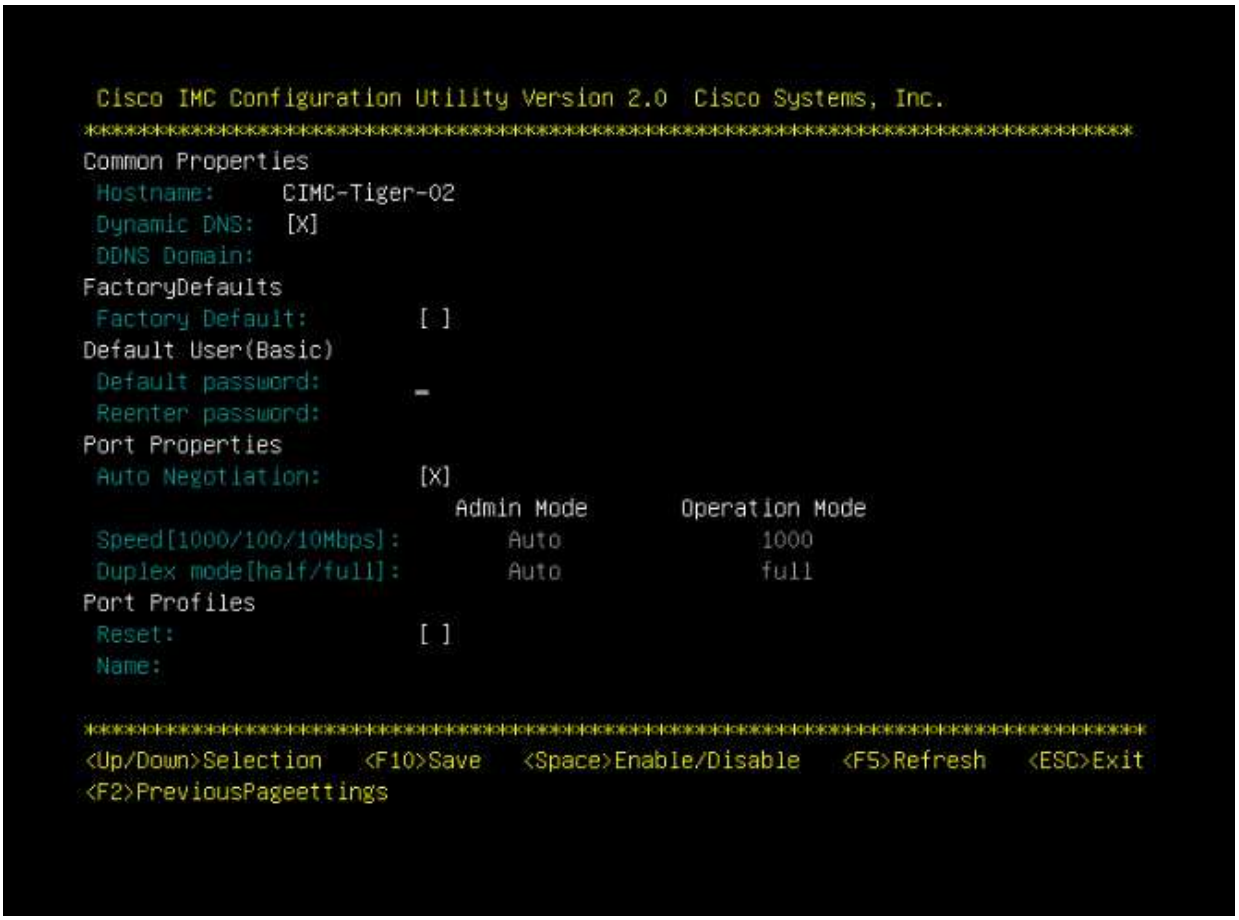
1. Reliez le dongle (KVM) du clavier, de la vidéo et de la souris Cisco (fourni avec le serveur) au port KVM situé à l'avant du serveur. Branchez un moniteur VGA et un clavier USB sur les ports de dongle KVM appropriés.
2. Mettez le serveur sous tension et appuyez sur F8 lorsque vous êtes invité à entrer dans la configuration CIMC.



3. Dans l'utilitaire de configuration de CIMC, définissez les options suivantes :
   - Mode carte d'interface réseau (NIC) :
     - Dédié [X]
   - IP (de base) :
     - IPV4 : [X]
     - DHCP activé : [ ]
     - CIMC IP : <<cimc_ip>>
     - Préfixe/sous-réseau : <<cimc_masque de réseau>>
     - Passerelle : <<cimc_Gateway>>
   - VLAN (avancé) : laissez désactivé pour désactiver le marquage VLAN.
     - Redondance des cartes réseau
     - Aucune : [x]



4. Appuyez sur F1 pour afficher d'autres paramètres.
   - Propriétés communes :
     - Nom d'hôte : <<nom_hôte_esxi>>
     - DNS dynamique : [ ]
     - Paramètres par défaut : laisser effacé.
   - Utilisateur par défaut (de base) :
     - Mot de passe par défaut : <<admin_password>>
     - Saisissez à nouveau le mot de passe : \<<admin_password>
     - Propriétés du port : utilisez les valeurs par défaut.
     - Profils de port : laisser désactivé.



5. Appuyez sur F10 pour enregistrer la configuration de l'interface CIMC.
6. Une fois la configuration enregistrée, appuyez sur Echap pour quitter.

Configuration du démarrage iSCSI des serveurs Cisco UCS C-Series

Dans cette configuration FlexPod Express, le VIC11387 est utilisé pour le démarrage iSCSI.

Le tableau suivant répertorie les informations nécessaires à la configuration du démarrage iSCSI.

La police en italique indique les variables uniques pour chaque hôte ESXi.

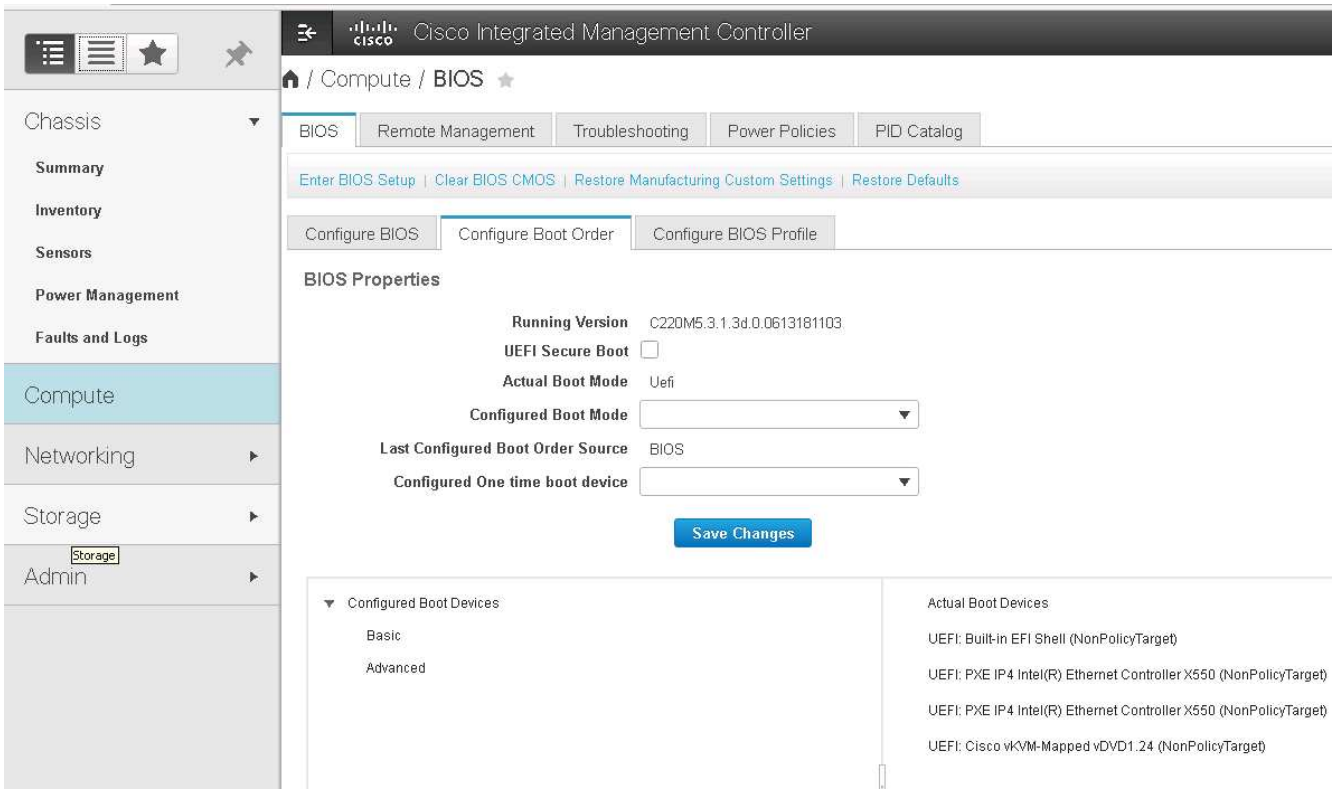
Détails	Valeur de détail
Initiateur hôte VMware ESXi a name	<<var_ucs_initiator_name_A>>
Hôte ESXi iSCSI-A IP	<<var_esxi_Host_iscsiA_ip>>
Masque de réseau iSCSI-A de l'hôte ESXi	<<var_esxi_host_iscsiA_mask>>
Hôte ESXi iSCSI : passerelle par défaut	<<var_esxi_Host_iscsiA_Gateway>>
Nom de l'initiateur B de l'hôte ESXi	<<var_ucs_initiator_name_B>>
Adresse IP iSCSI-B de l'hôte ESXi	<<var_esxi_Host_iscsiB_ip>>
Masque de réseau iSCSI-B de l'hôte ESXi	<<var_esxi_host_iscsiB_mask>>
Passerelle iSCSI-B de l'hôte ESXi	<<var_esxi_Host_iscsiB_Gateway>>

Détails	Valeur de détail
Adresse IP iscsi_lif01a	
Adresse IP iscsi_lif02a	
Adresse IP iscsi_lif01b	
Adresse IP iscsi_lif02b	
IQN de l'infra_SVM	

Configuration de l'ordre de démarrage

Pour définir la configuration de l'ordre de démarrage, procédez comme suit :

1. Dans la fenêtre du navigateur de l'interface CIMC, cliquez sur l'onglet serveur et sélectionnez BIOS.
2. Cliquez sur configurer l'ordre de démarrage, puis sur OK.



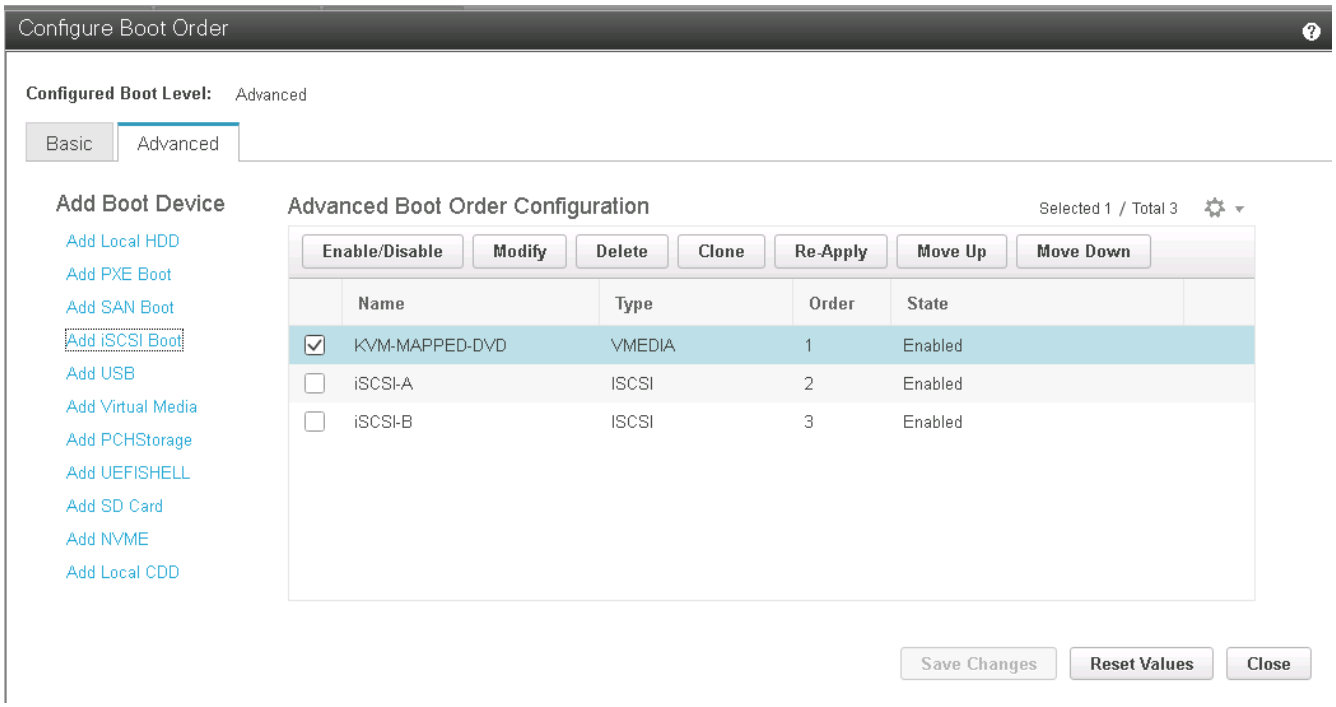
3. Configurez les périphériques suivants en cliquant sur le périphérique sous Ajouter un périphérique de démarrage et en accédant à l'onglet Avancé.
   - Ajouter un média virtuel
     - NOM : KVM-CD-DVD
     - SOUS-TYPE : DVD MAPPÉ KVM
     - État : activé
     - Ordre : 1
   - Ajouter un démarrage iSCSI.
     - Nom : iSCSI-A

- État : activé
- Ordre : 2
- Slot: MLOM
- Port : 0

◦ Cliquez sur Ajouter un démarrage iSCSI.

- Nom : iSCSI-B
- État : activé
- Ordre: 3
- Slot: MLOM
- Port : 1

4. Cliquez sur Ajouter un périphérique.
5. Cliquez sur Enregistrer les modifications, puis sur Fermer.

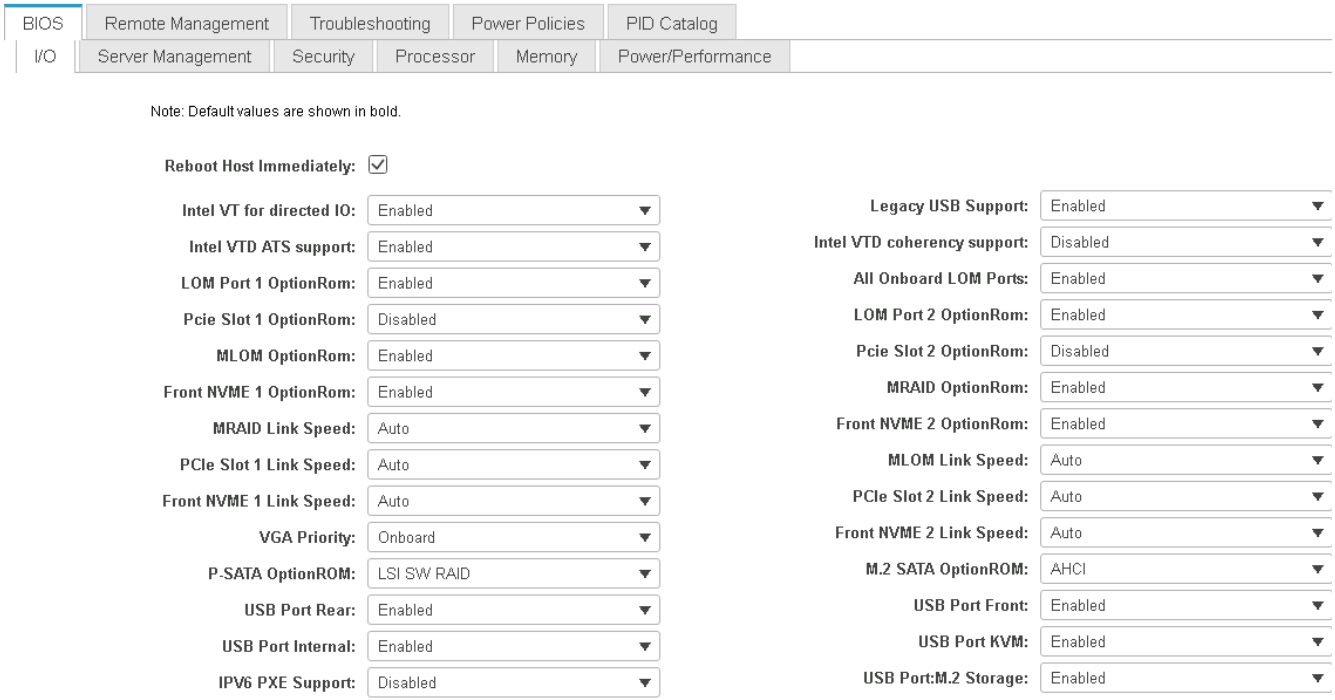


6. Redémarrez le serveur pour démarrer avec votre nouvel ordre de démarrage.

Désactiver le contrôleur RAID (le cas échéant)

Procédez comme suit si votre serveur C-Series contient un contrôleur RAID. Aucun contrôleur RAID n'est nécessaire dans l'amorçage à partir de la configuration SAN. Vous pouvez également retirer physiquement le contrôleur RAID du serveur.

1. Cliquez sur BIOS dans le volet de navigation de gauche de CIMC.
2. Sélectionnez configurer le BIOS.
3. Faites défiler vers le bas jusqu'à PCIe Slot:HBA option ROM.
4. Si la valeur n'est pas déjà désactivée, définissez-la sur Désactivé.

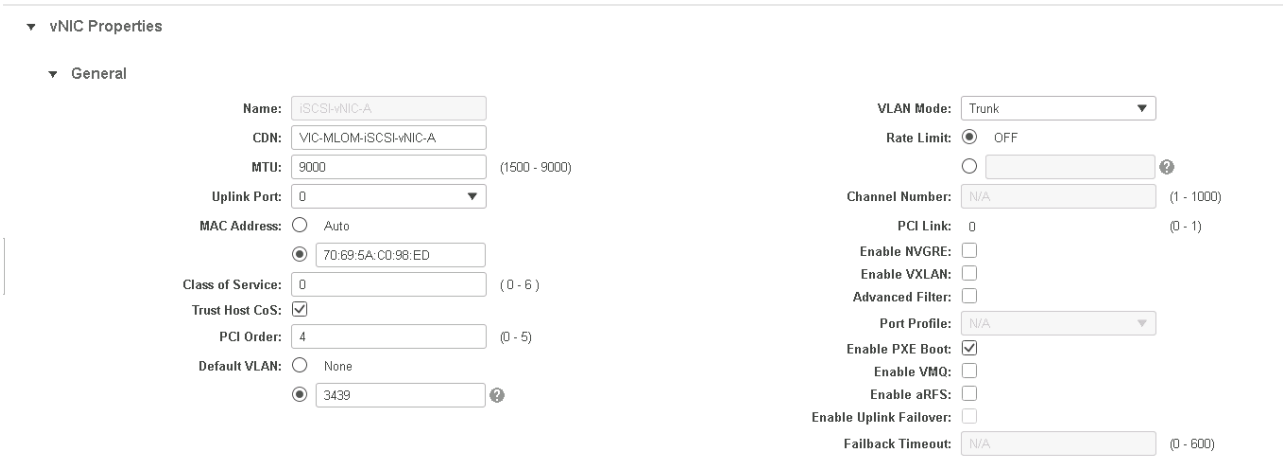


Configurer Cisco VIC11387 pour le démarrage iSCSI

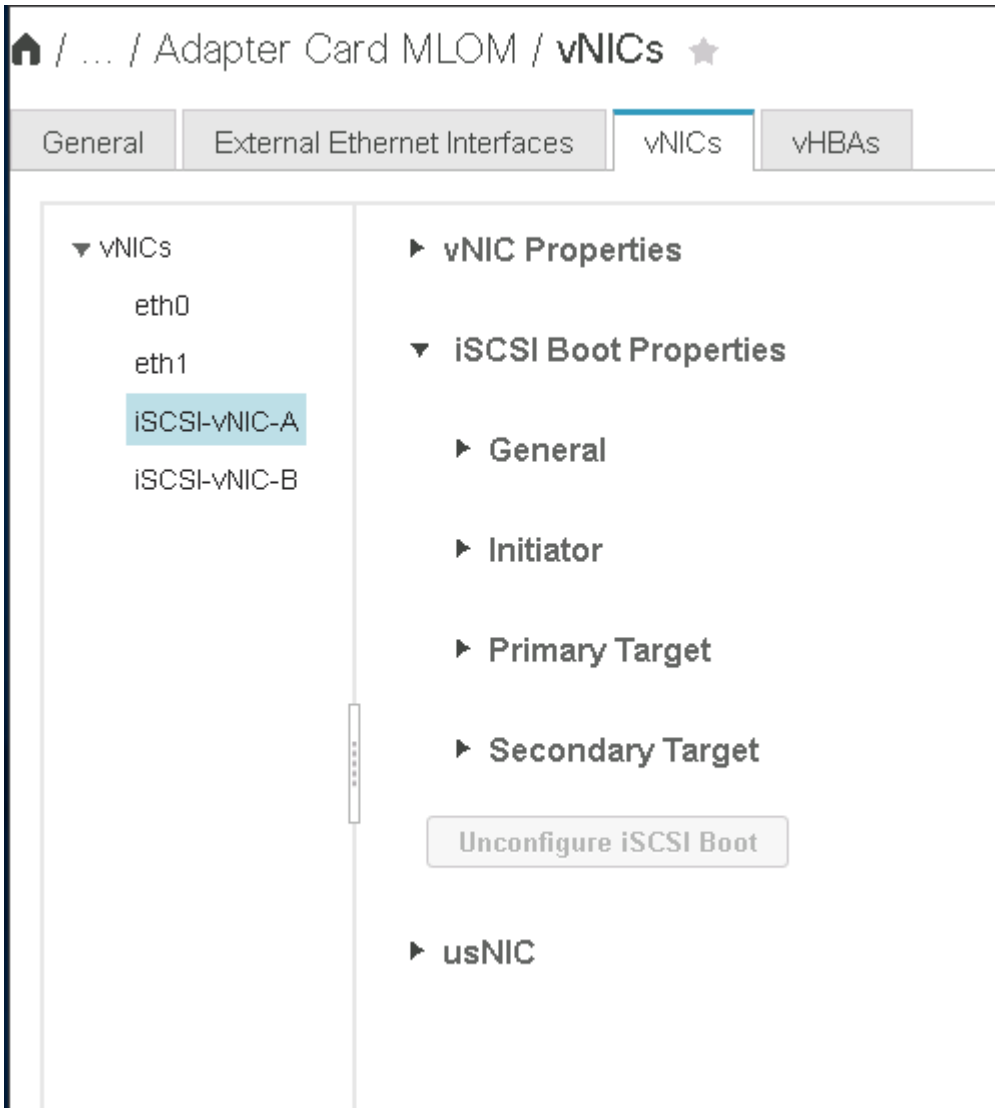
Les étapes de configuration suivantes concernent le Cisco VIC 1387 pour l'amorçage iSCSI.

Créez des vNIC iSCSI

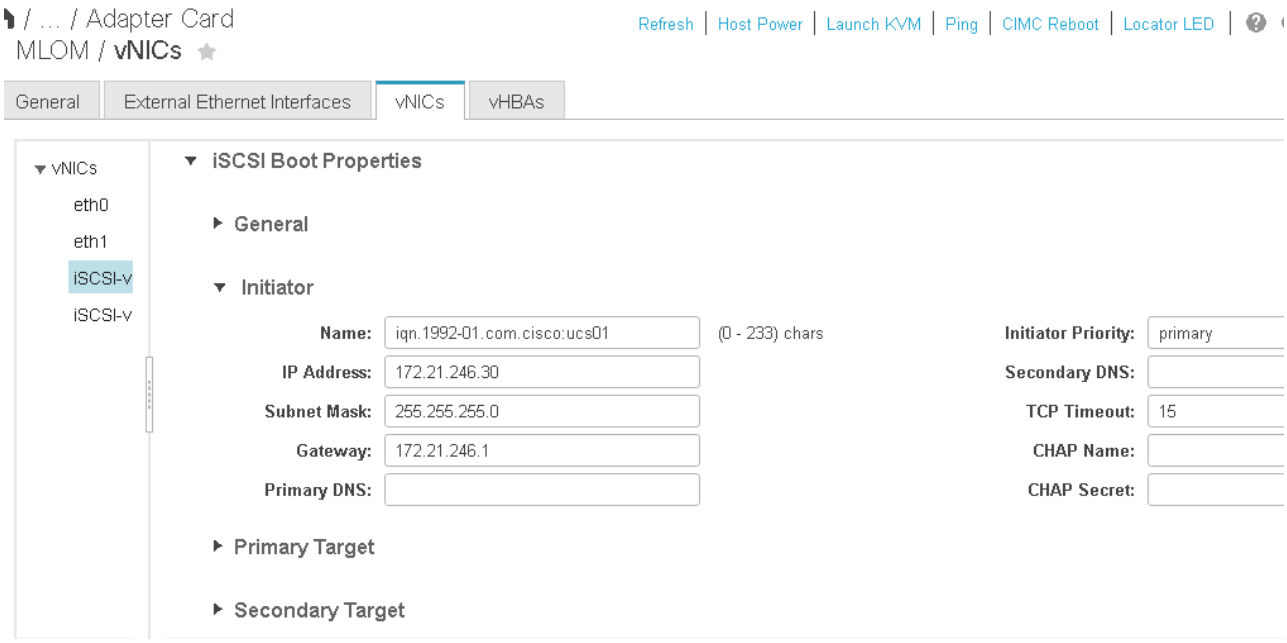
1. Cliquez sur Ajouter pour créer un vNIC.
2. Dans la section Ajouter vNIC, entrez les paramètres suivants :
   - Nom : iSCSI-vNIC-A
   - MTU : 9000
   - VLAN par défaut : `<<var_iscsi_vlan_a>>`
   - Mode VLAN : TRUNK
   - Activer le démarrage PXE : vérifier



3. Cliquez sur Ajouter vNIC, puis sur OK.
4. Répétez le processus pour ajouter un second vNIC.
   a. Nommez le vNIC `iSCSI-vNIC-B`.
   b. Entrez `<<var_iscsi_vlan_b>>` Comme le VLAN.
   c. Définissez le port de liaison montante sur `1`.
5. Sélectionnez le vNIC `iSCSI-vNIC-A` sur la gauche.



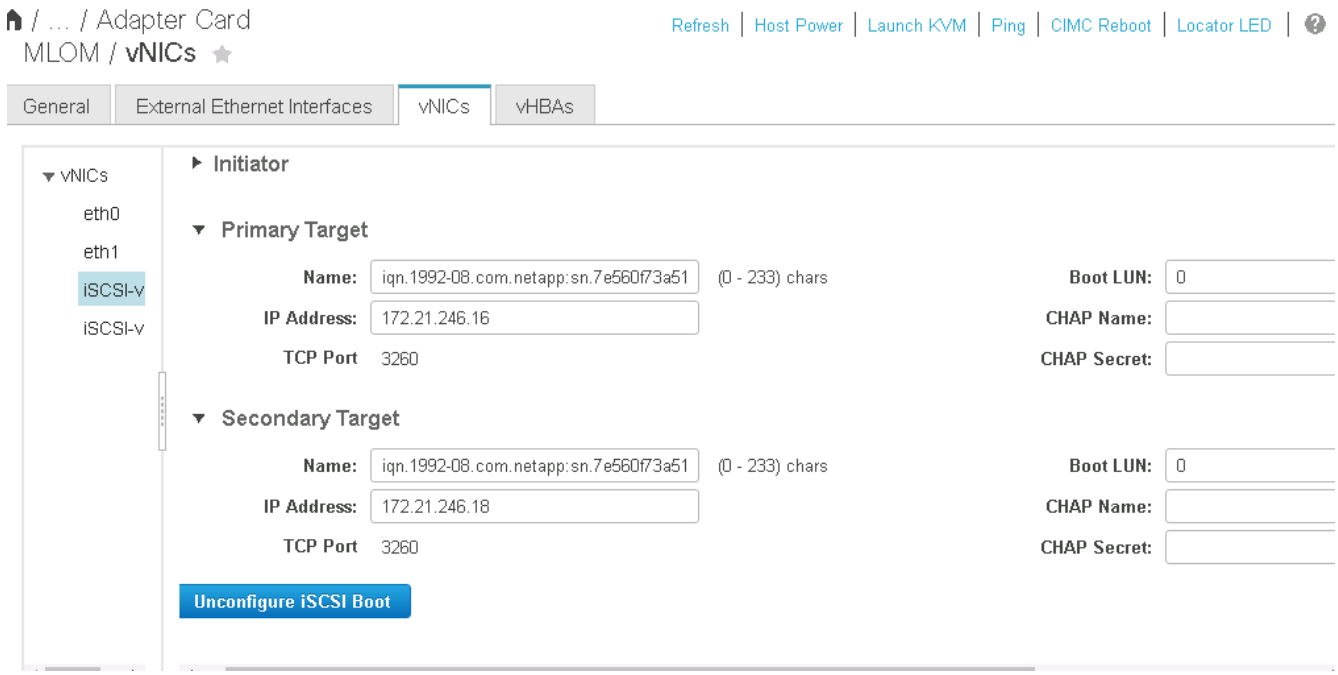
6. Sous Propriétés de démarrage iSCSI, entrez les détails de l'initiateur :
   - Nom : <<var_ucsa_initiator_name_a>>
   - Adresse IP : <<var_esxi_hostA_iscsiA_ip>>
   - Masque de sous-réseau : <<var_esxi_hostA_iscsiA_mask>>
   - Passerelle : <<var_esxi_hostA_iscsiA_Gateway>>



7. Entrez les détails de la cible principale.
   - Nom : numéro IQN de l'infra-SVM
   - Adresse IP : adresse IP de `iscsi_lif01a`
   - LUN de démarrage : 0
8. Entrez les détails de la cible secondaire.
   - Nom : numéro IQN de l'infra-SVM
   - Adresse IP : adresse IP de `iscsi_lif02a`
   - LUN de démarrage : 0

   Vous pouvez obtenir le numéro IQN de stockage en exécutant le `vserver iscsi show` commande.

   > Assurez-vous d'enregistrer les noms IQN pour chaque vNIC. Vous en avez besoin pour une étape ultérieure.



9. Cliquez sur configurer iSCSI.
10. Sélectionnez le vNIC `iSCSI-vNIC- B` Et cliquez sur le bouton iSCSI Boot situé en haut de la section Host Ethernet interfaces.
11. Répétez le processus à configurer `iSCSI-vNIC-B`.
12. Indiquez les détails de l'initiateur.
    - Nom : `<<var_ucsa_initiator_name_b>>`
    - Adresse IP : `<<var_esxi_hostb_iscsib_ip>>`
    - Masque de sous-réseau : `<<var_esxi_hostb_iscsib_mask>>`
    - Passerelle : `<<var_esxi_hostb_iscsib_gateway>>`
13. Entrez les détails de la cible principale.
    - Nom : numéro IQN de l'infra-SVM
    - Adresse IP : adresse IP de `iscsi_lif01b`
    - LUN de démarrage : 0
14. Entrez les détails de la cible secondaire.
    - Nom : numéro IQN de l'infra-SVM
    - Adresse IP : adresse IP de `iscsi_lif02b`
    - LUN de démarrage : 0

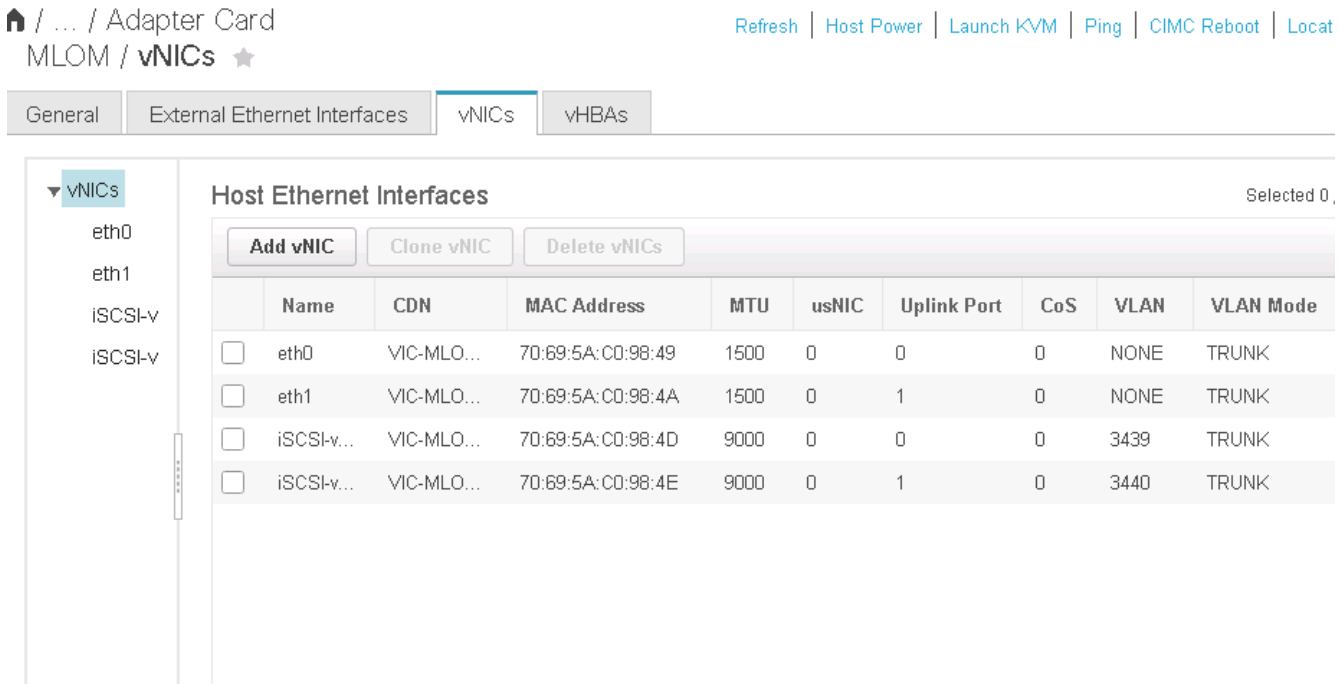
    Vous pouvez obtenir le numéro IQN de stockage en utilisant le `vserver iscsi show` commande.

    Assurez-vous d'enregistrer les noms IQN pour chaque vNIC. Vous en avez besoin pour une étape ultérieure.
15. Cliquez sur configurer ISCSI.

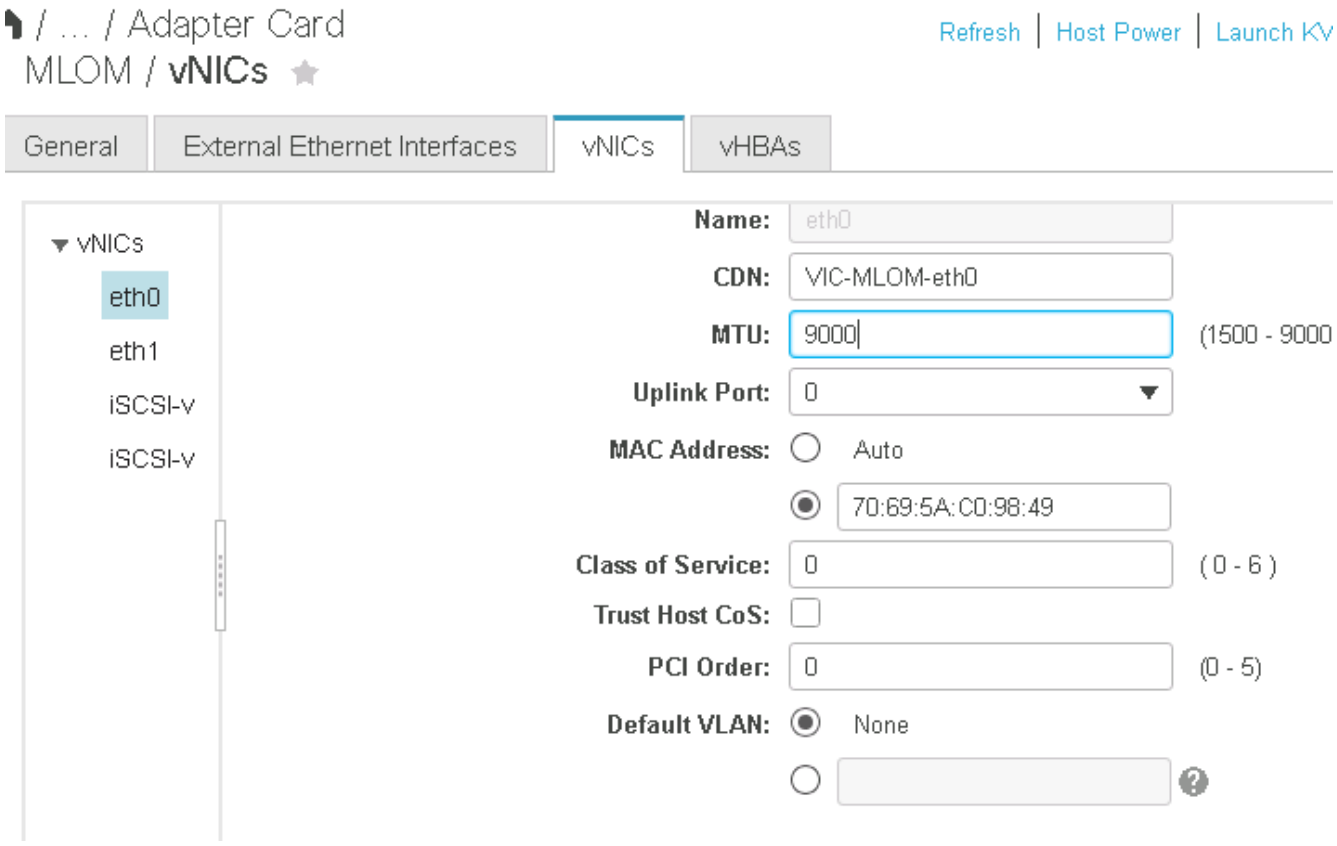
16. Répétez ce processus pour configurer l'initialisation iSCSI pour le serveur Cisco UCS B.

Configurer vNIC pour ESXi

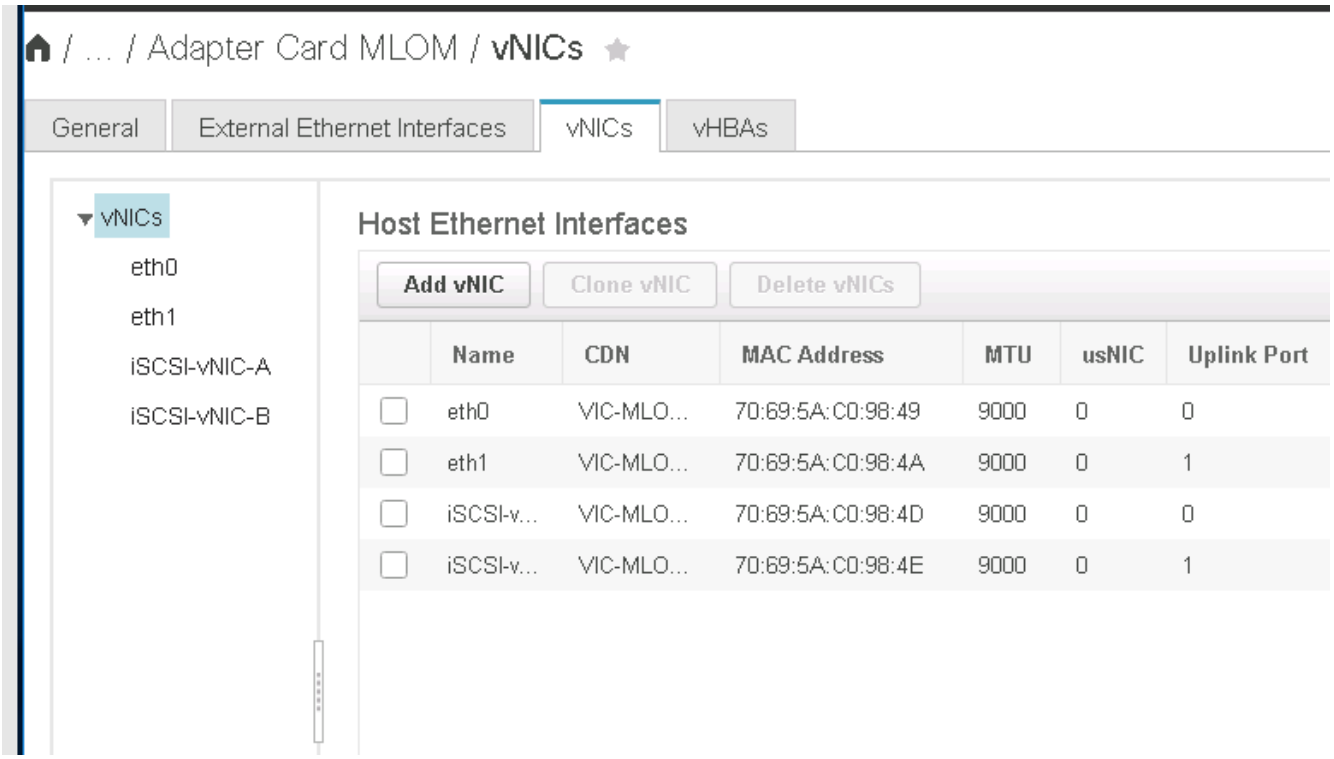
1. Dans la fenêtre du navigateur de l'interface CIMC, cliquez sur Inventaire, puis sur cartes Cisco VIC dans le volet droit.
2. Sous cartes d'adaptateur, sélectionnez Cisco UCS VIC 1387, puis les vNIC en dessous.



3. Sélectionnez eth0, puis cliquez sur Propriétés.
4. Définissez la MTU sur 9000. Cliquez sur Save Changes.



5. Répétez les étapes 3 et 4 pour eth1, en vérifiant que le port de liaison montante est défini sur `1` pour eth1.



Cette procédure doit être répétée pour chaque nœud initial Cisco UCS Server et chaque nœud Cisco UCS Server ajouté à l'environnement.

"Suivant : procédure de déploiement du stockage NetApp AFF (2e partie)"

Procédure de déploiement du stockage NetApp AFF (2e partie)

Configuration du stockage de démarrage SAN ONTAP

Création des igroups iSCSI

Pour créer des igroups, effectuez l'étape suivante :

Pour cette étape, vous avez besoin des IQN de l'initiateur iSCSI de la configuration du serveur.

1. Depuis la connexion SSH du nœud de gestion du cluster, exécutez les commandes suivantes. Pour afficher les trois groupes initiateurs créés lors de cette étape, exécutez la commande 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>>
```

Cette étape doit être effectuée lors de l'ajout de serveurs Cisco UCS C- Series supplémentaires.

Mappez les LUN de démarrage sur les igroups

Pour mapper les LUN de démarrage sur les igroups, exécutez les commandes suivantes depuis la connexion SSH de gestion du cluster :

```
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
```

Cette étape doit être effectuée lors de l'ajout de serveurs Cisco UCS C-Series supplémentaires.

"Suivant : procédure de déploiement de VMware vSphere 6.7."

Procédure de déploiement de VMware vSphere 6.7

Cette section décrit les procédures d'installation de VMware ESXi 6.7 dans une configuration FlexPod Express. Les procédures de déploiement suivantes sont personnalisées pour inclure les variables d'environnement décrites dans les sections

précédentes.

Il existe plusieurs méthodes pour installer VMware ESXi dans un tel environnement. Cette procédure utilise la console KVM virtuelle et les fonctions de média virtuel de l'interface CIMC pour les serveurs Cisco UCS C-Series pour mapper les supports d'installation à distance à chaque serveur.

Cette procédure doit être effectuée pour le serveur Cisco UCS A et le serveur Cisco UCS B.

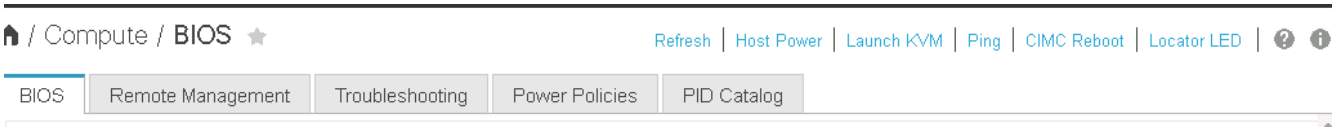
Cette procédure doit être effectuée pour tout nœud ajouté au cluster.

Connectez-vous à l'interface CIMC pour les serveurs autonomes Cisco UCS C-Series

La procédure suivante décrit en détail la méthode de connexion à l'interface CIMC pour les serveurs autonomes Cisco UCS C-Series. Vous devez vous connecter à l'interface CIMC pour exécuter le KVM virtuel, ce qui permet à l'administrateur de commencer l'installation du système d'exploitation par le biais du média distant.

Tous les hôtes

1. Accédez à un navigateur Web et entrez l'adresse IP de l'interface CIMC pour Cisco UCS C-Series. Cette étape lance l'application IUG de CIMC.
2. Connectez-vous à l'interface utilisateur de CIMC à l'aide du nom d'utilisateur et des informations d'identification de l'administrateur.
3. Dans le menu principal, sélectionnez l'onglet serveur.
4. Cliquez sur lancer la console KVM.



5. Dans la console KVM virtuelle, sélectionnez l'onglet Média virtuel.
6. Sélectionnez carte CD/DVD.

Vous devrez peut-être d'abord cliquer sur Activer les périphériques virtuels. Sélectionnez accepter cette session si vous y êtes invité.

7. Accédez au fichier image ISO du programme d'installation de VMware ESXi 6.7 et cliquez sur Ouvrir. Cliquez sur mapper le périphérique.
8. Sélectionnez le menu Marche/Arrêt et choisissez système de cycle d'alimentation (démarrage à froid). Cliquez sur Oui.

Installez VMware ESXi

La procédure suivante décrit l'installation de VMware ESXi sur chaque hôte.

Téléchargez l'image personnalisée DE VMWARE ESXI 6.7 Cisco

1. Accédez au "Page de téléchargement de VMware vSphere" Pour les ISO personnalisées.

2. Cliquez sur Go to Downloads en regard du CD d'installation de Cisco Custom image for ESXi 6.7 GA.
3. Téléchargez le CD d'installation Cisco Custom image for ESXi 6.7 GA (ISO).

Tous les hôtes

1. Lors du démarrage du système, la machine détecte la présence du support d'installation VMware ESXi.
2. Sélectionnez le programme d'installation de VMware ESXi dans le menu qui s'affiche.

   Le programme d'installation se charge. Cette opération prend plusieurs minutes.

3. Une fois le chargement terminé par le programme d'installation, appuyez sur entrée pour poursuivre l'installation.
4. Après avoir lu le contrat de licence de l'utilisateur final, acceptez-le et poursuivez l'installation en appuyant sur F11.
5. Sélectionnez le LUN NetApp précédemment configuré comme disque d'installation pour ESXi, et appuyez sur entrée pour poursuivre l'installation.

6. Sélectionnez la disposition de clavier appropriée et appuyez sur entrée.
7. Saisissez et confirmez le mot de passe racine, puis appuyez sur entrée.
8. Le programme d'installation vous avertit que les partitions existantes sont supprimées du volume. Poursuivre l'installation en appuyant sur F11. Le serveur redémarre après l'installation de ESXi.

Configurer la mise en réseau de gestion d'hôte VMware ESXi

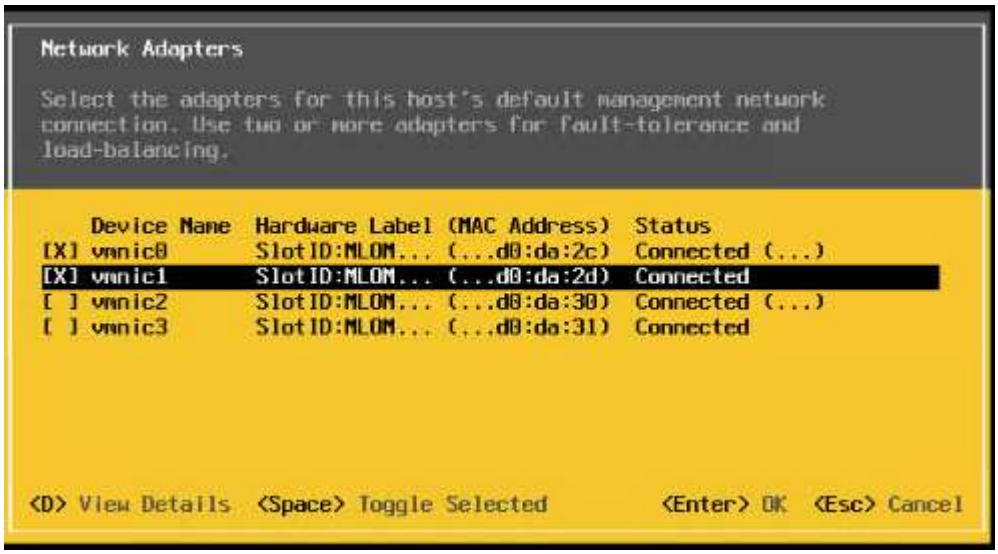
La procédure suivante décrit comment ajouter le réseau de gestion pour chaque hôte VMware ESXi.

Tous les hôtes

1. Une fois le redémarrage du serveur terminé, entrez l'option permettant de personnaliser le système en appuyant sur F2.
2. Connectez-vous avec root en tant que nom de connexion et mot de passe racine entrés précédemment au cours du processus d'installation.
3. Sélectionnez l'option configurer le réseau de gestion.
4. Sélectionnez cartes réseau et appuyez sur entrée.

5. Sélectionnez les ports souhaités pour vSwitch0. Appuyez sur entrée.

   Sélectionnez les ports qui correspondent à eth0 et eth1 dans CIMC.



6. Sélectionnez VLAN (facultatif) et appuyez sur entrée.
7. Saisissez l'ID du VLAN `<<mgmt_vlan_id>>`. Appuyez sur entrée.
8. Dans le menu configurer le réseau de gestion, sélectionnez Configuration IPv4 pour configurer l'adresse IP de l'interface de gestion. Appuyez sur entrée.
9. Utilisez les touches fléchées pour mettre en surbrillance définir l'adresse IPv4 statique et utilisez la barre d'espace pour sélectionner cette option.
10. Entrez l'adresse IP de gestion de l'hôte VMware ESXi `<<esxi_host_mgmt_ip>>`.
11. Saisissez le masque de sous-réseau de l'hôte VMware ESXi `<<esxi_host_mgmt_netmask>>`.
12. Entrez la passerelle par défaut de l'hôte VMware ESXi `<<esxi_host_mgmt_gateway>>`.
13. Appuyez sur entrée pour accepter les modifications apportées à la configuration IP.
14. Accédez au menu de configuration IPv6.
15. Utilisez la barre d'espace pour désactiver IPv6 en désélectionnant l'option Activer IPv6 (redémarrage requis). Appuyez sur entrée.
16. Accédez au menu pour configurer les paramètres DNS.
17. Étant donné que l'adresse IP est attribuée manuellement, les informations DNS doivent également être saisies manuellement.
18. Entrez l'adresse IP du serveur DNS principal[nameserver_ip].
19. (Facultatif) Entrez l'adresse IP du serveur DNS secondaire.
20. Entrez le FQDN du nom d'hôte VMware ESXi :[esxi_host_fqdn].
21. Appuyez sur entrée pour accepter les modifications apportées à la configuration DNS.
22. Quittez le sous-menu configurer le réseau de gestion en appuyant sur la touche Echap.
23. Appuyez sur y pour confirmer les modifications et redémarrer le serveur.
24. Déconnectez-vous de la console VMware en appuyant sur la touche Echap.

Configurer l’hôte ESXi

Vous avez besoin des informations du tableau suivant pour configurer chaque hôte ESXi.

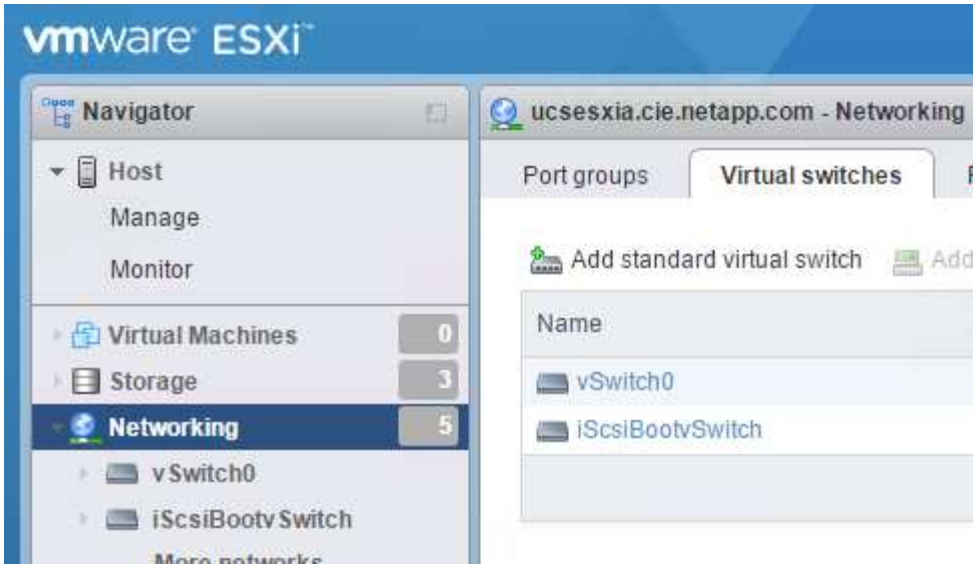
Détails	Valeur
Nom d’hôte ESXi	
IP de gestion d’hôte ESXi	
Masque de gestion d’hôte ESXi	
Passerelle de gestion de l’hôte ESXi	
IP NFS de l’hôte ESXi	
Masque NFS hôte ESXi	
Passerelle NFS de l’hôte ESXi	
IP vMotion hôte ESXi	
Masque vMotion hôte ESXi	
Passerelle vMotion de l’hôte ESXi	
Hôte ESXi iSCSI-A IP	
Masque iSCSI-A de l’hôte ESXi	
Passerelle iSCSI-A de l’hôte ESXi	
Adresse IP iSCSI-B de l’hôte ESXi	
Masque iSCSI-B de l’hôte ESXi	
Passerelle iSCSI-B de l’hôte ESXi	

Connectez-vous à l’hôte ESXi

1. Ouvrez l’adresse IP de gestion de l’hôte dans un navigateur Web.
2. Connectez-vous à l’hôte ESXi à l’aide du compte racine et du mot de passe que vous avez spécifié lors du processus d’installation.
3. Lisez la déclaration relative au Programme d’amélioration de l’expérience client VMware. Après avoir sélectionné la bonne réponse, cliquez sur OK.

Configurez le démarrage iSCSI

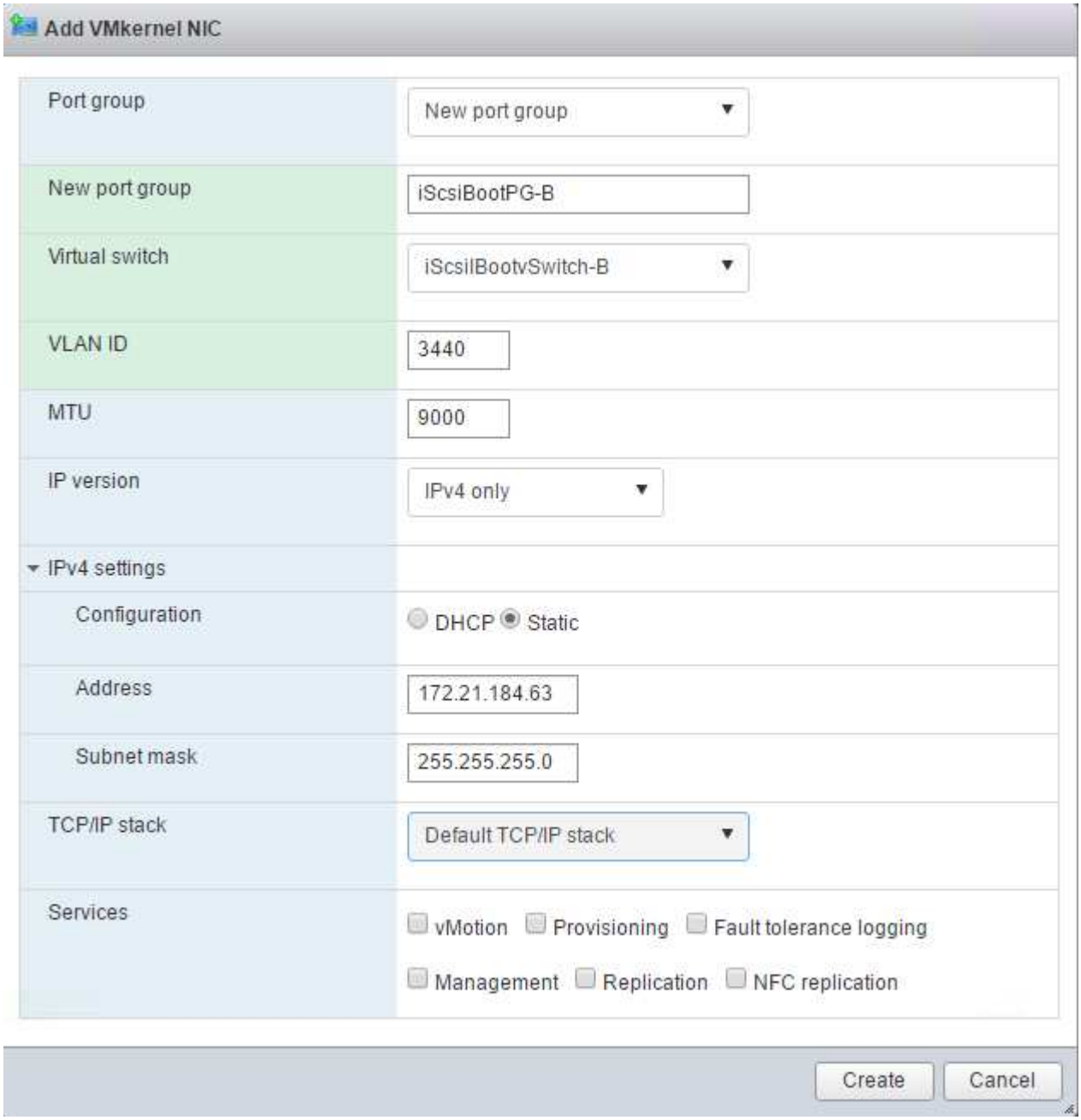
1. Sélectionnez réseau sur la gauche.
2. Sur la droite, sélectionnez l’onglet commutateurs virtuels.



3. Cliquez sur iSciBootvSwitch.
4. Sélectionnez Modifier les paramètres.
5. Définissez la MTU sur 9000 et cliquez sur Enregistrer.
6. Cliquez sur réseau dans le volet de navigation de gauche pour revenir à l'onglet commutateurs virtuels.
7. Cliquez sur Ajouter un commutateur virtuel standard.
8. Indiquez le nom `iScsiBootvSwitch-B` Pour le nom du vSwitch.
   - Définissez la MTU sur 9000.
   - Sélectionnez vmnic3 dans les options Uplink 1.
   - Cliquez sur Ajouter.

> Vmnic2 et vmnic3 sont utilisés pour le démarrage iSCSI dans cette configuration. Si vous disposez de cartes réseau supplémentaires dans votre hôte ESXi, vous pourriez avoir différents numéros vmnic. Pour vérifier quelles cartes réseau sont utilisées pour le démarrage iSCSI, faites correspondre les adresses MAC des cartes vNIC iSCSI dans CIMC aux adresses vmnics dans ESXi.

9. Dans le volet central, sélectionnez l'onglet VMkernel NIC.
10. Sélectionnez Ajouter une carte réseau VMkernel.
    - Spécifiez un nouveau nom de groupe de ports de `iScsiBootPG-B`.
    - Sélectionnez iSssiBootvSwitch-B pour le commutateur virtuel.
    - Entrez `<<iscsib_vlan_id>>` Pour l'ID VLAN.
    - Remplacez la MTU par 9000.
    - Développez Paramètres IPv4.
    - Sélectionnez Configuration statique.
    - Entrez `<<var_hosta_iscsib_ip>>` Pour adresse.
    - Entrez `<<var_hosta_iscsib_mask>>` Pour masque de sous-réseau.
    - Cliquez sur Créer .

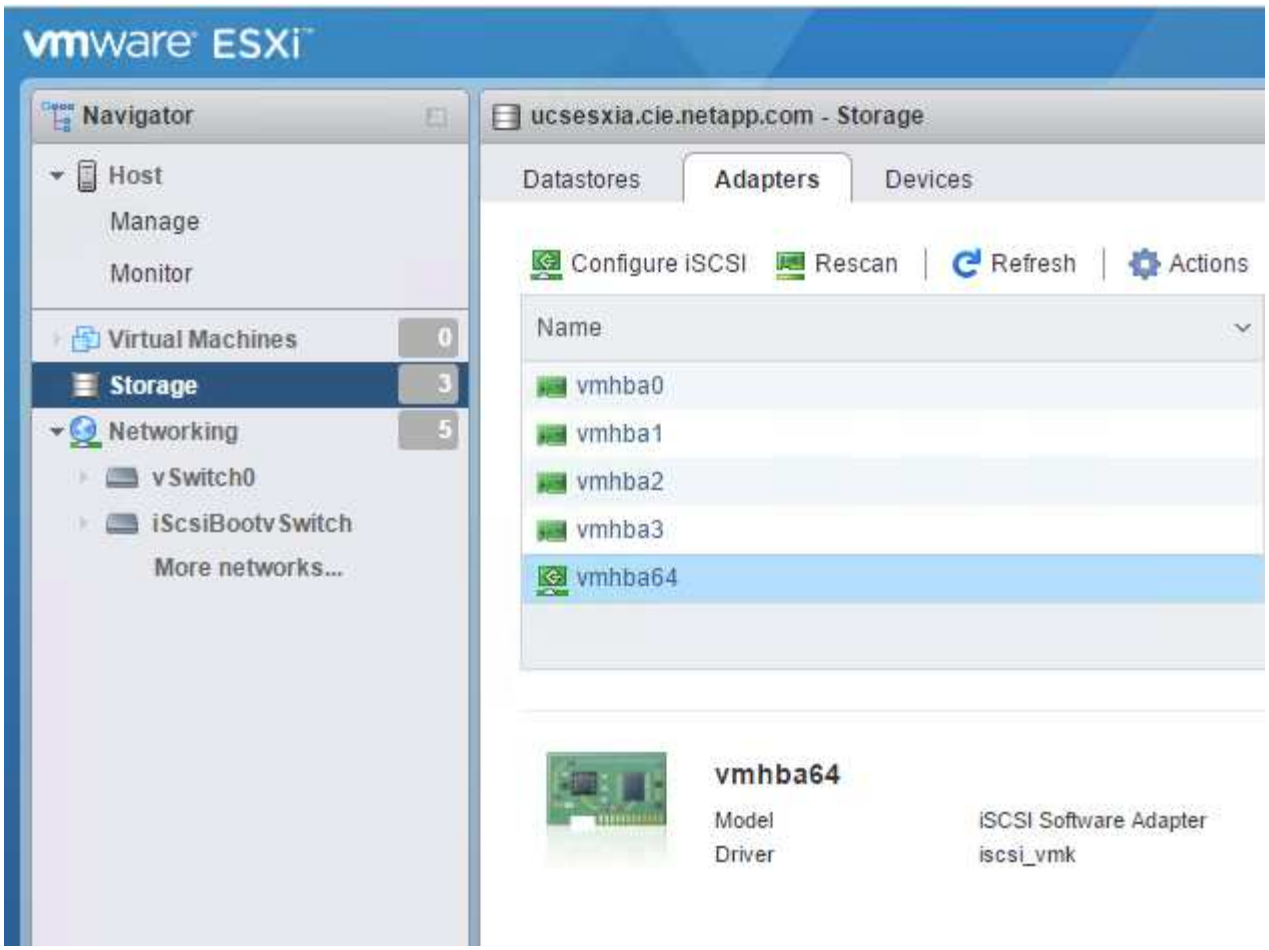


Définissez la MTU sur 9000 activé `iScsiBootPG- A.`

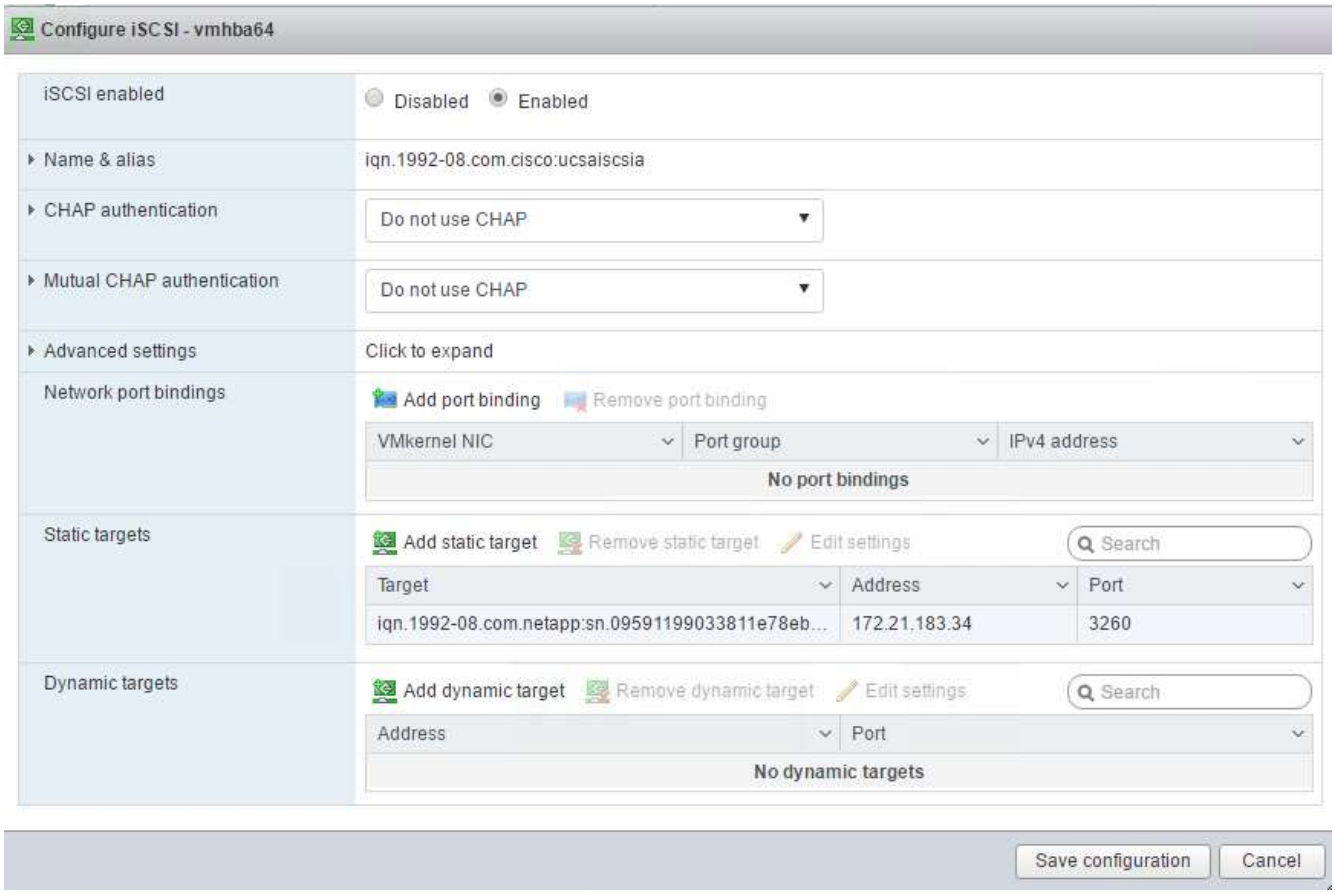
Configurez les chemins d'accès multiples iSCSI

Pour configurer les chemins d'accès multiples iSCSI sur les hôtes ESXi, procédez comme suit :

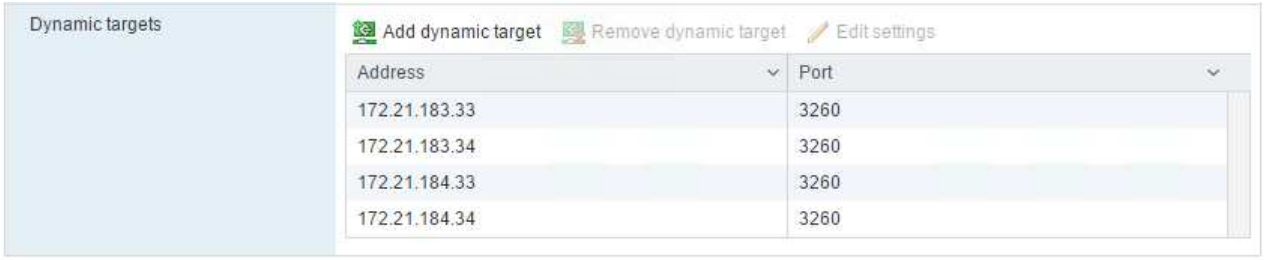
1. Sélectionnez stockage dans le volet de navigation de gauche. Cliquez sur adaptateurs.
2. Sélectionnez la carte logicielle iSCSI et cliquez sur configurer iSCSI.



3. Sous cibles dynamiques, cliquez sur Ajouter une cible dynamique.



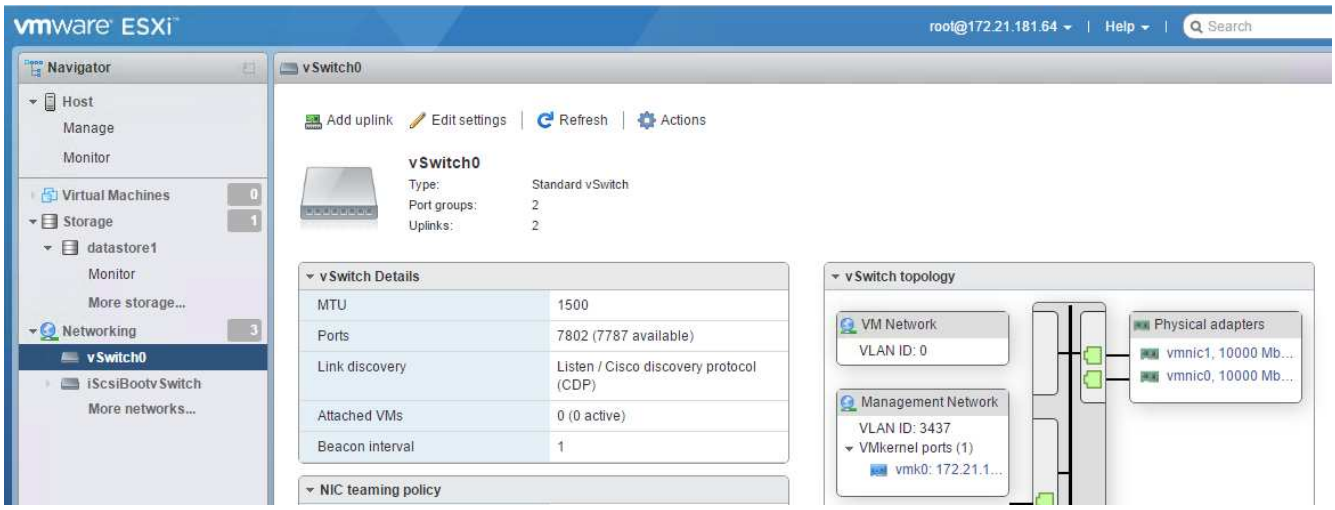
4. Saisissez l'adresse IP `iscsi_lif01a`.
   - Répétez l'opération avec les adresses IP `iscsi_lif01b`, `iscsi_lif02a`, et `iscsi_lif02b`.
   - Cliquez sur Enregistrer la configuration.



Vous pouvez trouver les adresses IP de la LIF iSCSI en exécutant la commande `network interface show `sur le cluster NetApp ou en consultant l'onglet Network interfaces dans OnCommand System Manager.

Configurer l'hôte ESXi

1. Dans le volet de navigation de gauche, sélectionnez réseau.
2. Sélectionnez vSwitch0.



3. Sélectionnez Modifier les paramètres.
4. Remplacez la MTU par 9000.
5. Développez agrégation de cartes réseau et vérifiez que vmnic0 et vmnic1 sont tous les deux définis sur actif.

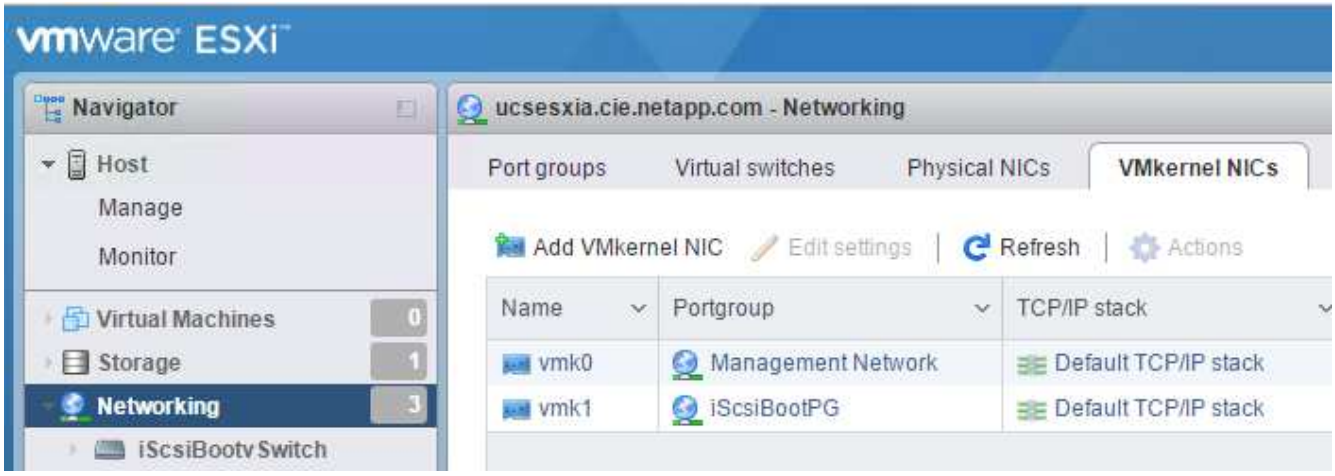
Configuration des groupes de ports et des NIC VMkernel

1. Dans le volet de navigation de gauche, sélectionnez réseau.
2. Cliquez avec le bouton droit de la souris sur l'onglet groupes de ports.

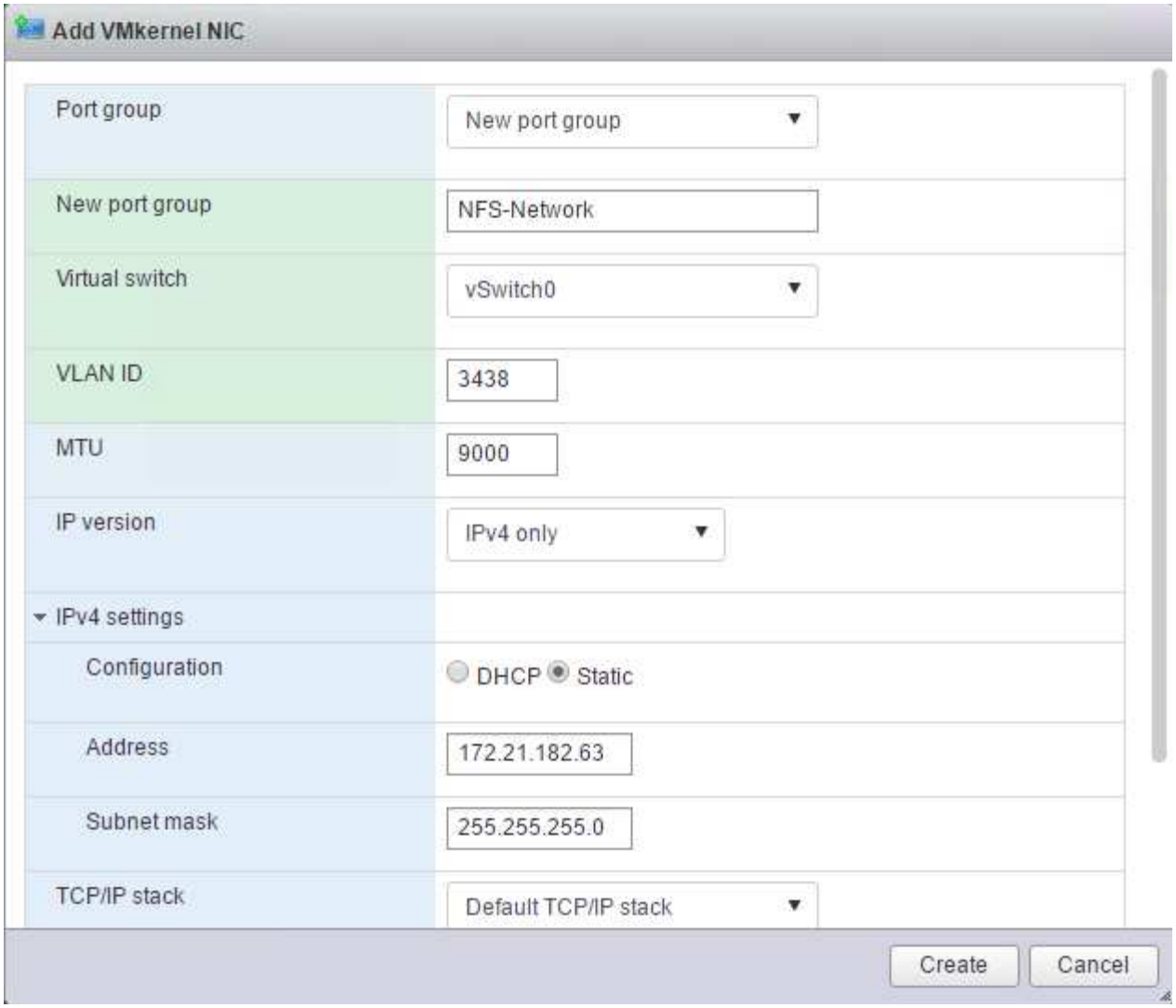
3. Cliquez avec le bouton droit de la souris sur réseau VM et sélectionnez Modifier. Définissez l'ID du VLAN sur `<<var_vm_traffic_vlan>>`.
4. Cliquez sur Ajouter un groupe de ports.
   - Nommer le groupe de ports `MGMT-Network`.
   - Entrez `<<mgmt_vlan>>` Pour l'ID VLAN.
   - Vérifiez que vSwitch0 est sélectionné.

- Cliquez sur Ajouter.

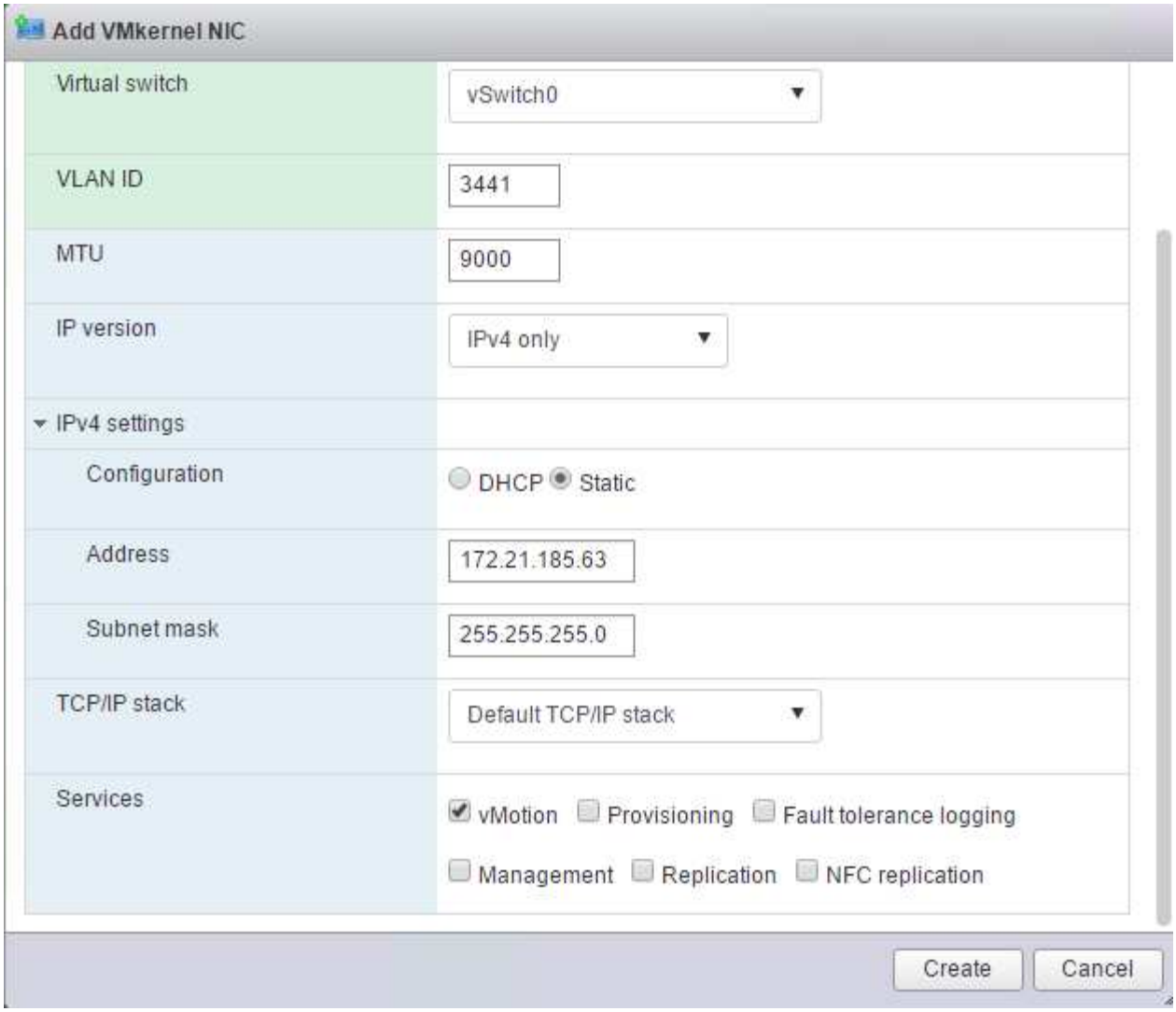
5. Cliquez sur l'onglet VMkernel NIC.



6. Sélectionnez Ajouter une carte réseau VMkernel.
   - Sélectionnez Nouveau groupe de ports.
   - Nommer le groupe de ports `NFS-Network`.
   - Entrez `<<nfs_vlan_id>>` Pour l'ID VLAN.
   - Remplacez la MTU par 9000.
   - Développez Paramètres IPv4.
   - Sélectionnez Configuration statique.
   - Entrez `<<var_hosta_nfs_ip>>` Pour adresse.
   - Entrez `<<var_hosta_nfs_mask>>` Pour masque de sous-réseau.
   - Cliquez sur Créer .



7. Répétez ce processus pour créer le port VMkernel vMotion.
8. Sélectionnez Ajouter une carte réseau VMkernel.
    a. Sélectionnez Nouveau groupe de ports.
    b. Nommez le port group vMotion.
    c. Entrez `<<vmotion_vlan_id>>` Pour l'ID VLAN.
    d. Remplacez la MTU par 9000.
    e. Développez Paramètres IPv4.
    f. Sélectionnez Configuration statique.
    g. Entrez `<<var_hosta_vmotion_ip>>` Pour adresse.
    h. Entrez `<<var_hosta_vmotion_mask>>` Pour masque de sous-réseau.
    i. Assurez-vous que la case vMotion est cochée après les paramètres IPv4.

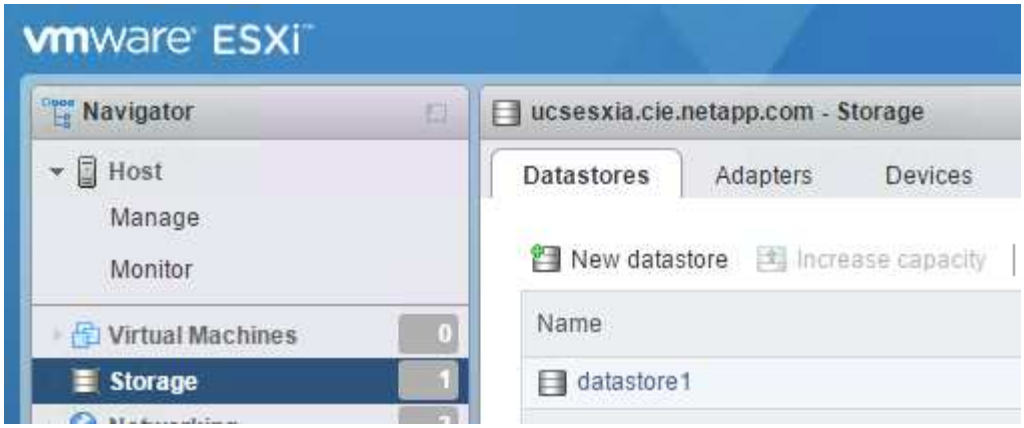


Il existe de nombreuses façons de configurer la mise en réseau VMware ESXi, y compris en utilisant le commutateur distribué VMware vSphere si votre licence le permet. Les autres configurations réseau sont prises en charge par FlexPod Express si elles sont requises pour répondre aux exigences de l'entreprise.

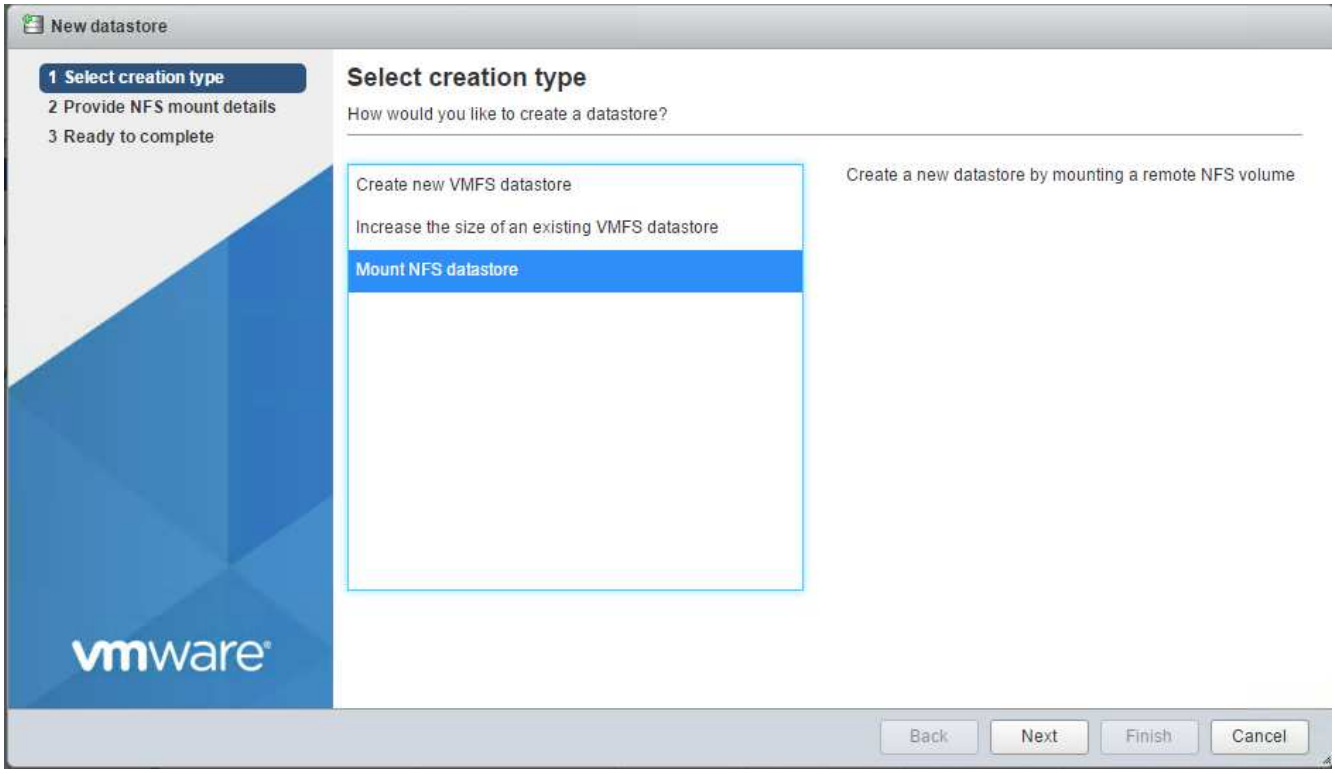
Montez les premiers datastores

Les premiers datastores à monter sont le datastore infra_datastore_1 pour machines virtuelles et le datastore infra_swap pour fichiers swap de machines virtuelles.

1. Cliquez sur stockage dans le volet de navigation de gauche, puis sur Nouveau datastore.



2. Sélectionnez Mount NFS datastore.



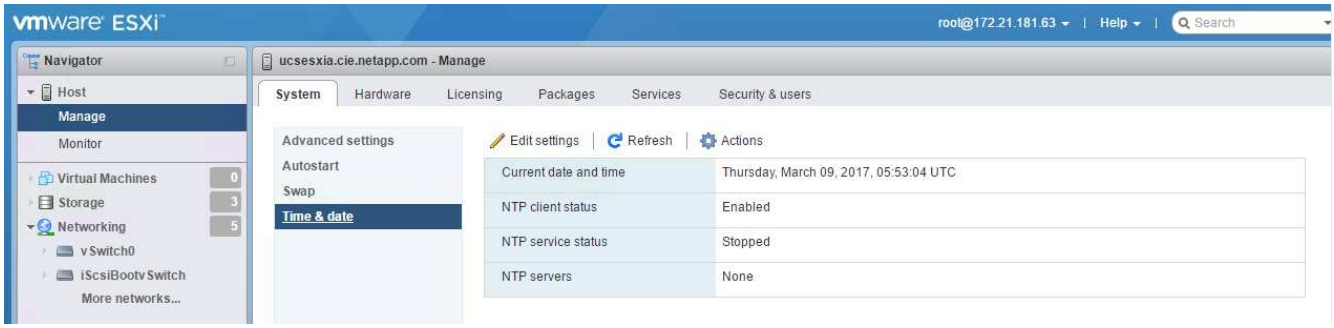
3. Entrez ensuite les informations suivantes dans la page Détails du montage NFS :
   - Nom : `infra_datastore_1`
   - Serveur NFS : `<<var_nodea_nfs_lif>>`
   - Partager : /infra_datastore_1
   - Assurez-vous que NFS 3 est sélectionné.
4. Cliquez sur Terminer. La tâche terminée s'affiche dans le volet tâches récentes.
5. Répétez ce processus pour monter le datastore infra_swap :
   - Nom : `infra_swap`
   - Serveur NFS : `<<var_nodea_nfs_lif>>`
   - Partager : `/infra_swap`

◦ Assurez-vous que NFS 3 est sélectionné.

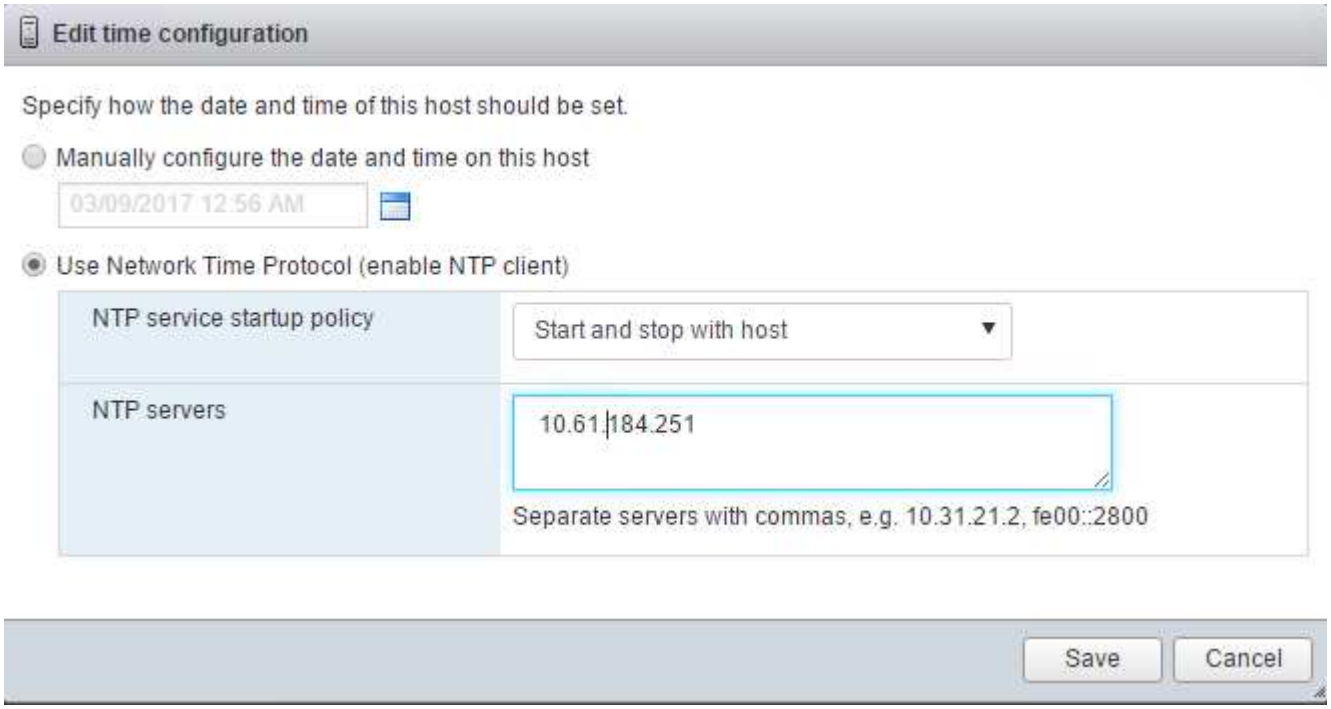
Configurez NTP

Pour configurer le protocole NTP pour un hôte ESXi, procédez comme suit :

1. Cliquez sur gérer dans le volet de navigation de gauche. Sélectionnez système dans le volet de droite, puis cliquez sur heure et date.



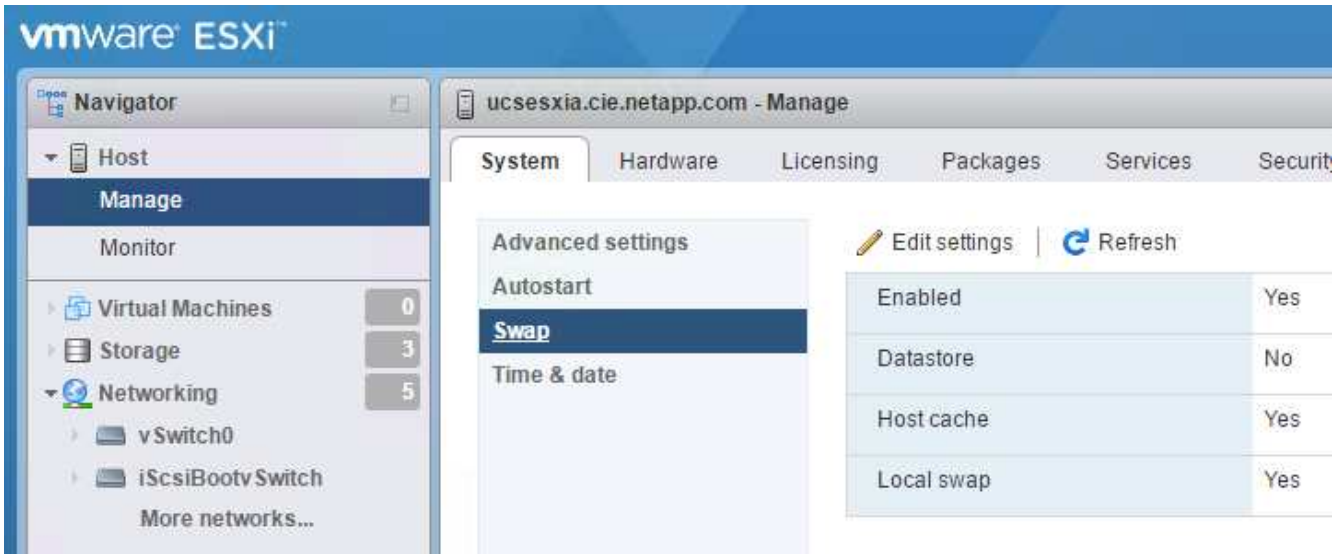
2. Sélectionnez utiliser le protocole d'heure du réseau (Activer le client NTP).
3. Sélectionnez Démarrer et Arrêter avec l'hôte comme stratégie de démarrage du service NTP.
4. Entrez `<<var_ntp>>` En tant que serveur NTP. Vous pouvez définir plusieurs serveurs NTP.
5. Cliquez sur Enregistrer.



Déplacer l'emplacement du fichier d'échange de la machine virtuelle

Ces étapes fournissent des détails sur le déplacement de l'emplacement du fichier d'échange de la machine virtuelle.

1. Cliquez sur gérer dans le volet de navigation de gauche. Sélectionnez système dans le volet de droite, puis cliquez sur Permuter.



2. Cliquez sur Modifier les paramètres. Sélectionnez infra_swap dans les options datastore.

3. Cliquez sur Enregistrer.

Installer le plug-in NetApp NFS 1.0.20 pour VMware VAAI

Pour installer le plug-in NetApp NFS 1.0.20 pour VMware VAAI, procédez comme suit.

1. Entrez les commandes suivantes pour vérifier que VAAI est activé :

```
esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
```

   Si VAAI est activé, ces commandes produisent la sortie suivante :

```
~ #  esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
~ # esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
```

2. Si VAAI n'est pas activé, entrez les commandes suivantes pour activer VAAI :

```
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedInit
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
```

Ces commandes produisent les valeurs de sortie suivantes :

```
~ # esxcfg-advcfg -s 1 /Data Mover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
~ #  esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
```

3. Téléchargez le plug-in NetApp NFS pour VMware VAAI :
   a. Accédez au "page de téléchargement de logiciels".
   b. Faites défiler l'écran et cliquez sur Plug-in NetApp NFS pour VMware VAAI.
   c. Sélectionnez la plate-forme ESXi.
   d. Téléchargez le bundle hors ligne (.zip) ou en ligne (.vib) du plug-in le plus récent.
4. Installez le plug-in sur l'hôte ESXi à l'aide de la CLI ESX.
5. Redémarrez l'hôte 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:~]
```

"Installez VMware vCenter Server 6.7"

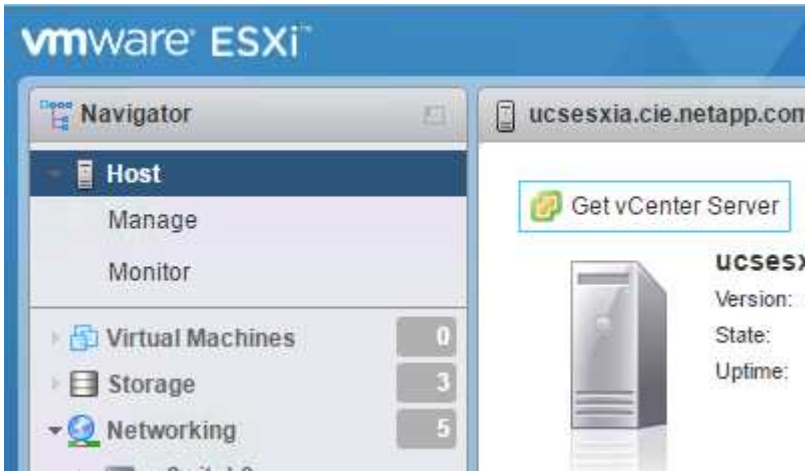
Installez VMware vCenter Server 6.7

Cette section décrit les procédures détaillées d'installation de VMware vCenter Server 6.7 dans une configuration FlexPod Express.

FlexPod Express utilise VMware vCenter Server Appliance (VCSA).

Téléchargez l’appliance du serveur VMware vCenter

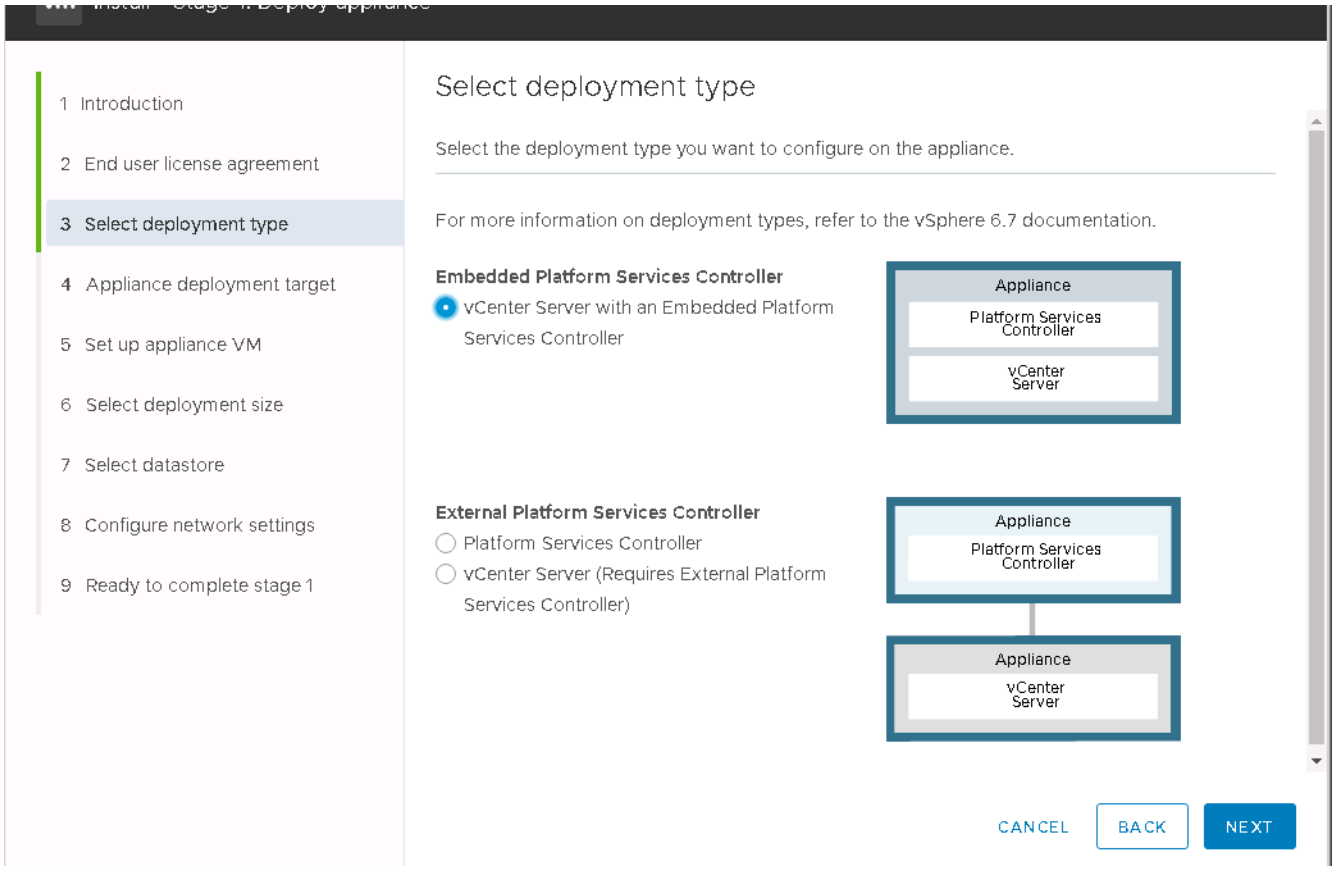
1. Téléchargez le VCSA. Accédez au lien de téléchargement en cliquant sur l’icône obtenir vCenter Server lors de la gestion de l’hôte ESXi.



2. Téléchargez le VCSA à partir du site de VMware.

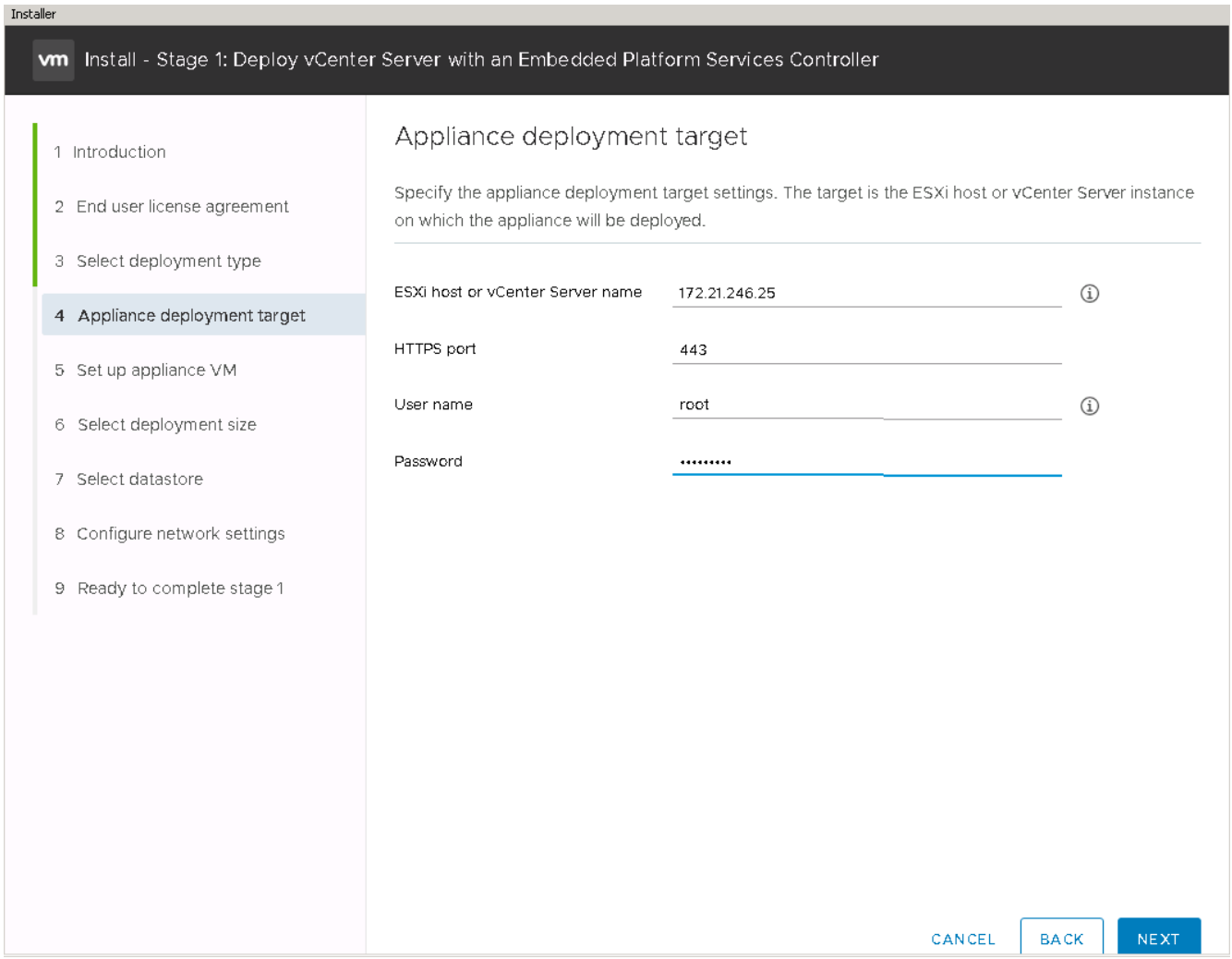
> Bien que l’installation de Microsoft Windows vCenter Server soit prise en charge, VMware recommande le VCSA pour les nouveaux déploiements.

3. Montez l’image ISO.
4. Accédez au répertoire vcsa-ui-installer> win32. Double-cliquez sur installer.exe.
5. Cliquez sur installation.
6. Cliquez sur Suivant sur la page Introduction.
7. Acceptez le contrat de licence de l’utilisateur final.
8. Sélectionnez Embedded Platform Services Controller comme type de déploiement.

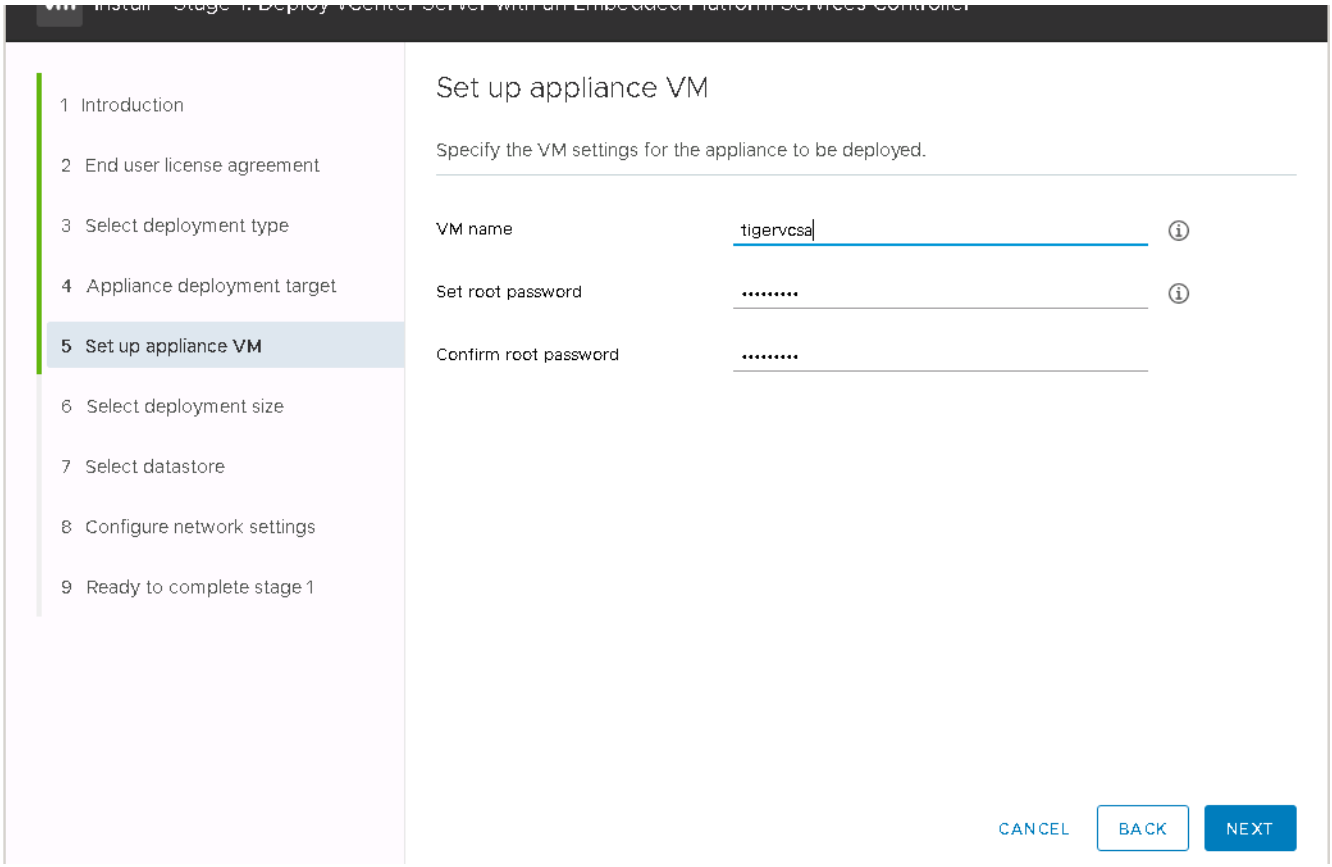


Si nécessaire, le déploiement de contrôleur de services de plateforme externe est également pris en charge dans le cadre de la solution FlexPod Express.

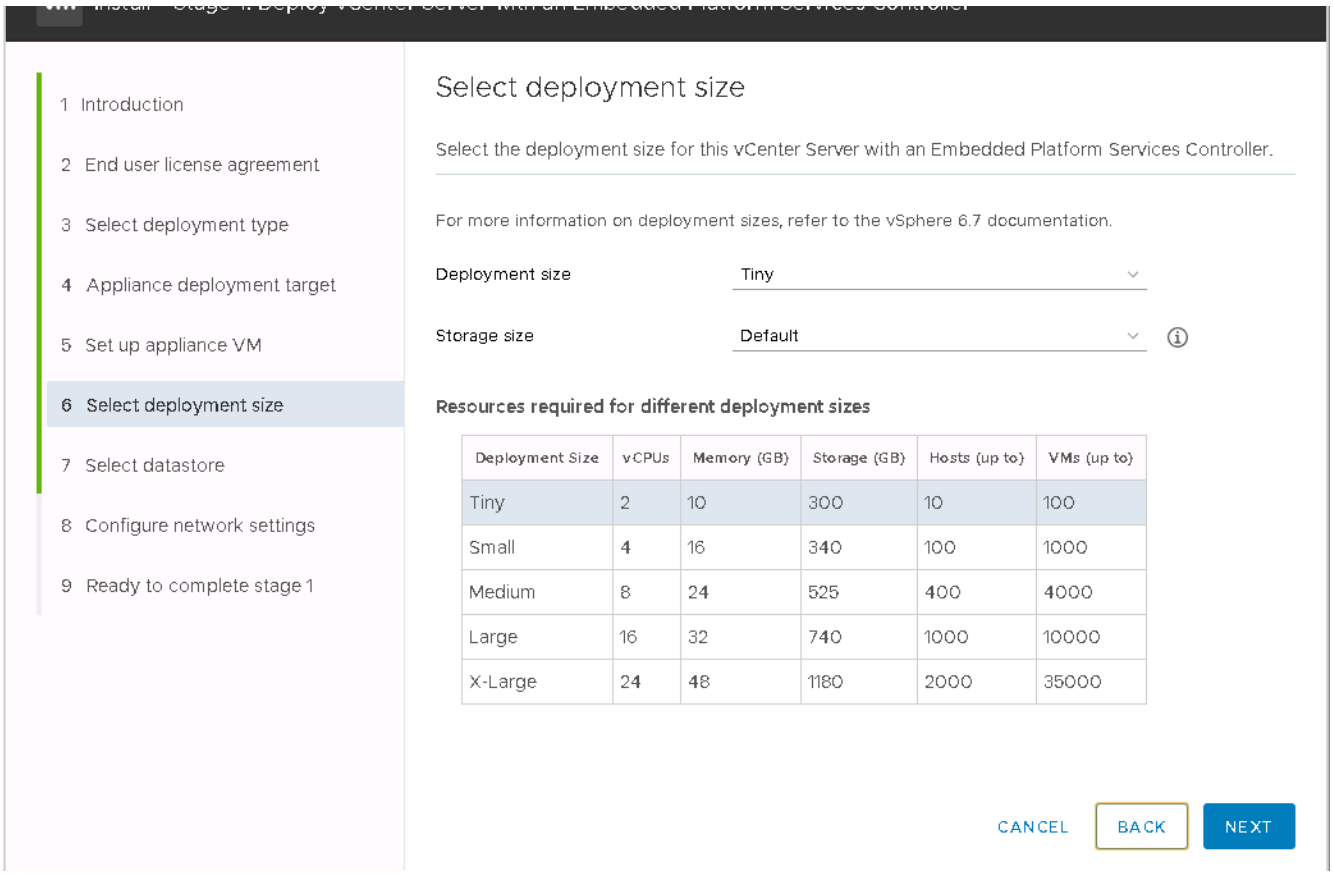
9. Dans la cible de déploiement de l'appliance, entrez l'adresse IP d'un hôte ESXi déployé, ainsi que le nom d'utilisateur root et le mot de passe root.



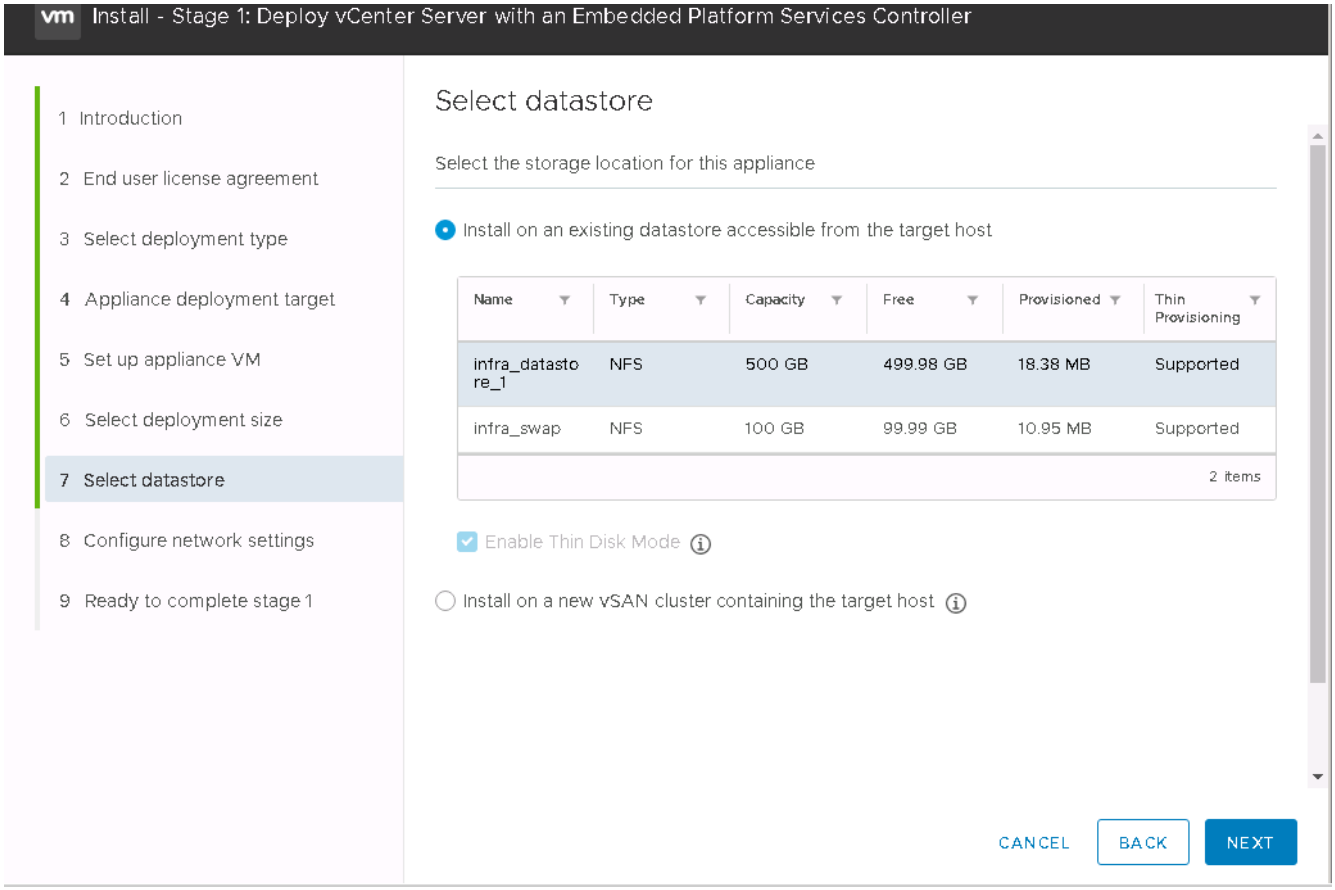
10. Configurez la machine virtuelle de l'appliance en saisissant `VCSA` Comme nom de la VM et mot de passe root, vous souhaitez utiliser pour le VCSA.



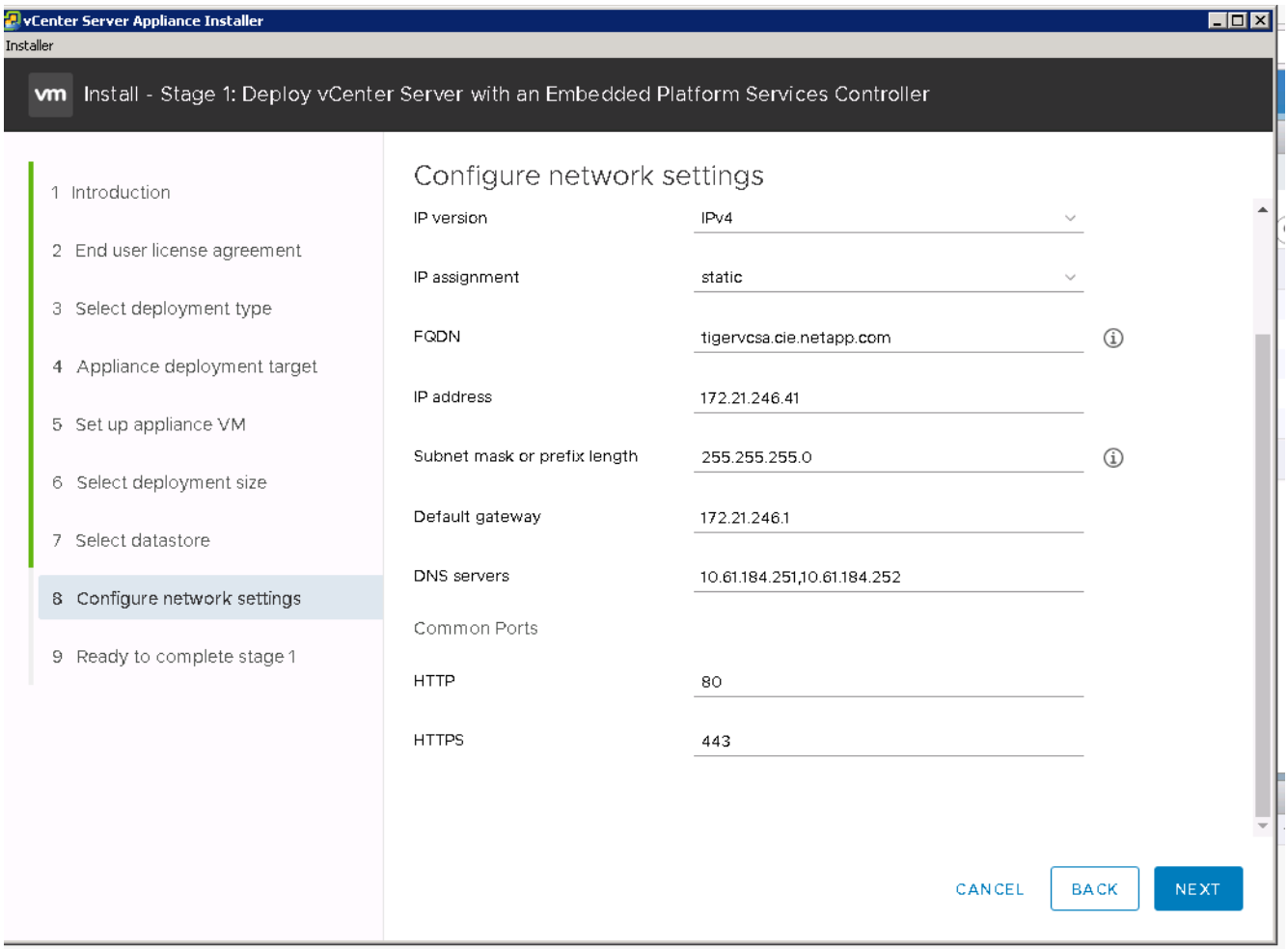
11. Choisissez la taille de déploiement qui correspond le mieux à votre environnement. Cliquez sur Suivant.



12. Sélectionnez le datastore infra_datastore_1. Cliquez sur Suivant.

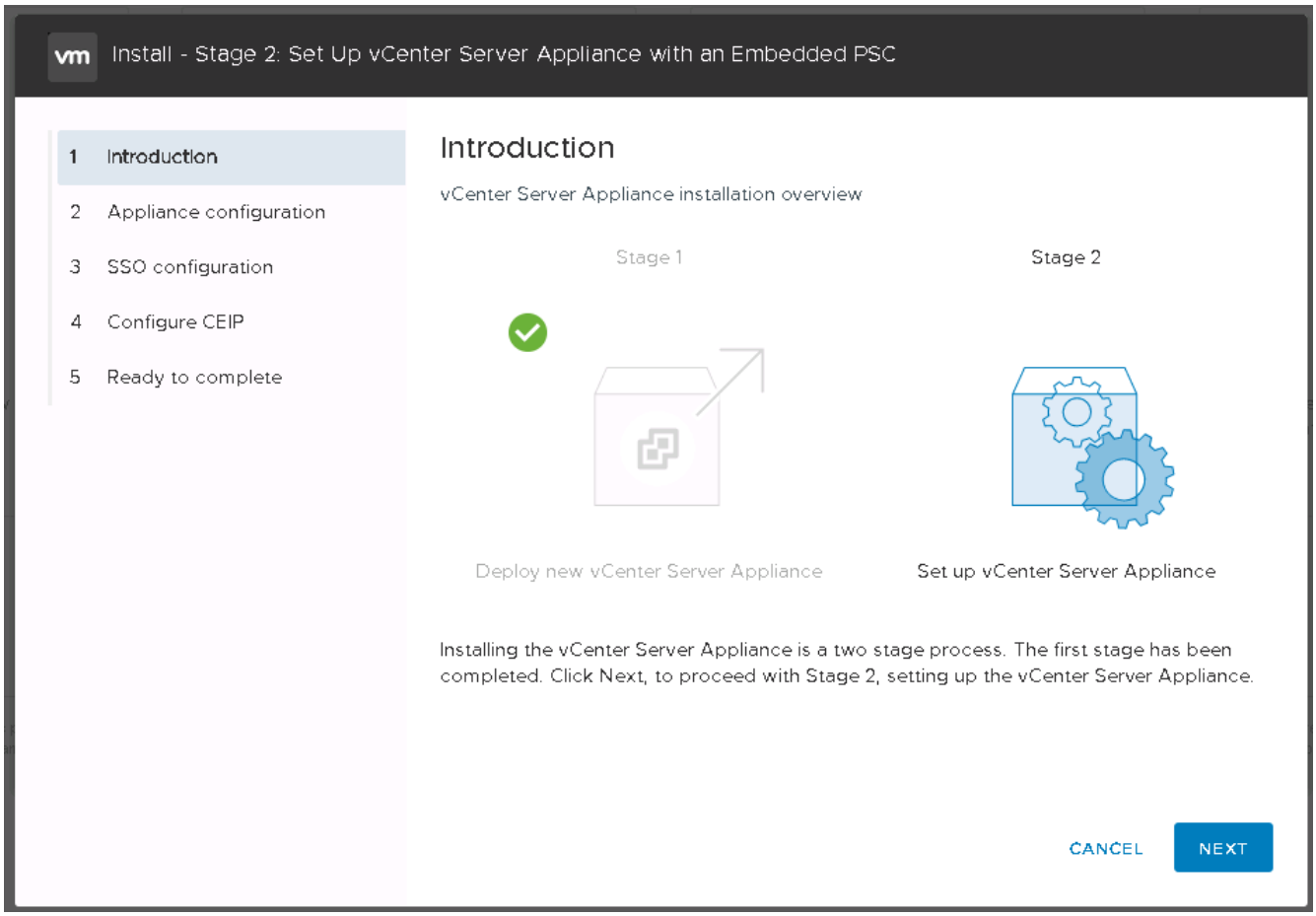


13. Entrez les informations suivantes sur la page configurer les paramètres réseau et cliquez sur Suivant.
    a. Sélectionnez MGMT-réseau pour le réseau.
    b. Saisissez le nom de domaine complet ou l'adresse IP à utiliser pour le VCSA.
    c. Entrez l'adresse IP à utiliser.
    d. Entrez le masque de sous-réseau à utiliser.
    e. Saisissez la passerelle par défaut.
    f. Entrez le serveur DNS.
14. Sur la page prêt à terminer l'étape 1, vérifiez que les paramètres saisis sont corrects. Cliquez sur Terminer.



Le VCSA s'installe maintenant. Ce processus prend plusieurs minutes.

15. Une fois l'étape 1 terminée, un message s'affiche indiquant qu'il est terminé. Cliquez sur Continuer pour commencer la configuration de l'étape 2.
16. Sur la page Introduction de l'étape 2, cliquez sur Suivant.



17. Entrez `<<var_ntp_id>>` Pour l'adresse du serveur NTP. Vous pouvez entrer plusieurs adresses IP NTP.

    Si vous prévoyez d'utiliser la haute disponibilité (HA) de vCenter Server, assurez-vous que l'accès SSH est activé.

18. Configurez le nom de domaine SSO, le mot de passe et le nom du site. Cliquez sur Suivant.

    Notez ces valeurs pour votre référence, en particulier si vous vous écartez du nom de domaine vsphere.local.

19. Rejoignez le programme VMware Customer Experience si nécessaire. Cliquez sur Suivant.
20. Affichez le récapitulatif de vos paramètres. Cliquez sur Terminer ou utilisez le bouton Retour pour modifier les paramètres.
21. Un message s'affiche indiquant que vous ne pourrez pas interrompre ou arrêter l'installation une fois qu'elle a démarré. Cliquez sur OK pour continuer.

    La configuration de l'appareil continue. Cette opération prend plusieurs minutes.

    Un message s'affiche pour indiquer que la configuration a réussi.

    Vous pouvez cliquer sur les liens que le programme d'installation fournit pour accéder à vCenter Server.

"Suivant : configuration de VMware vCenter Server 6.7 et de la mise en cluster vSphere."

Configuration de VMware vCenter Server 6.7 et de la mise en cluster vSphere

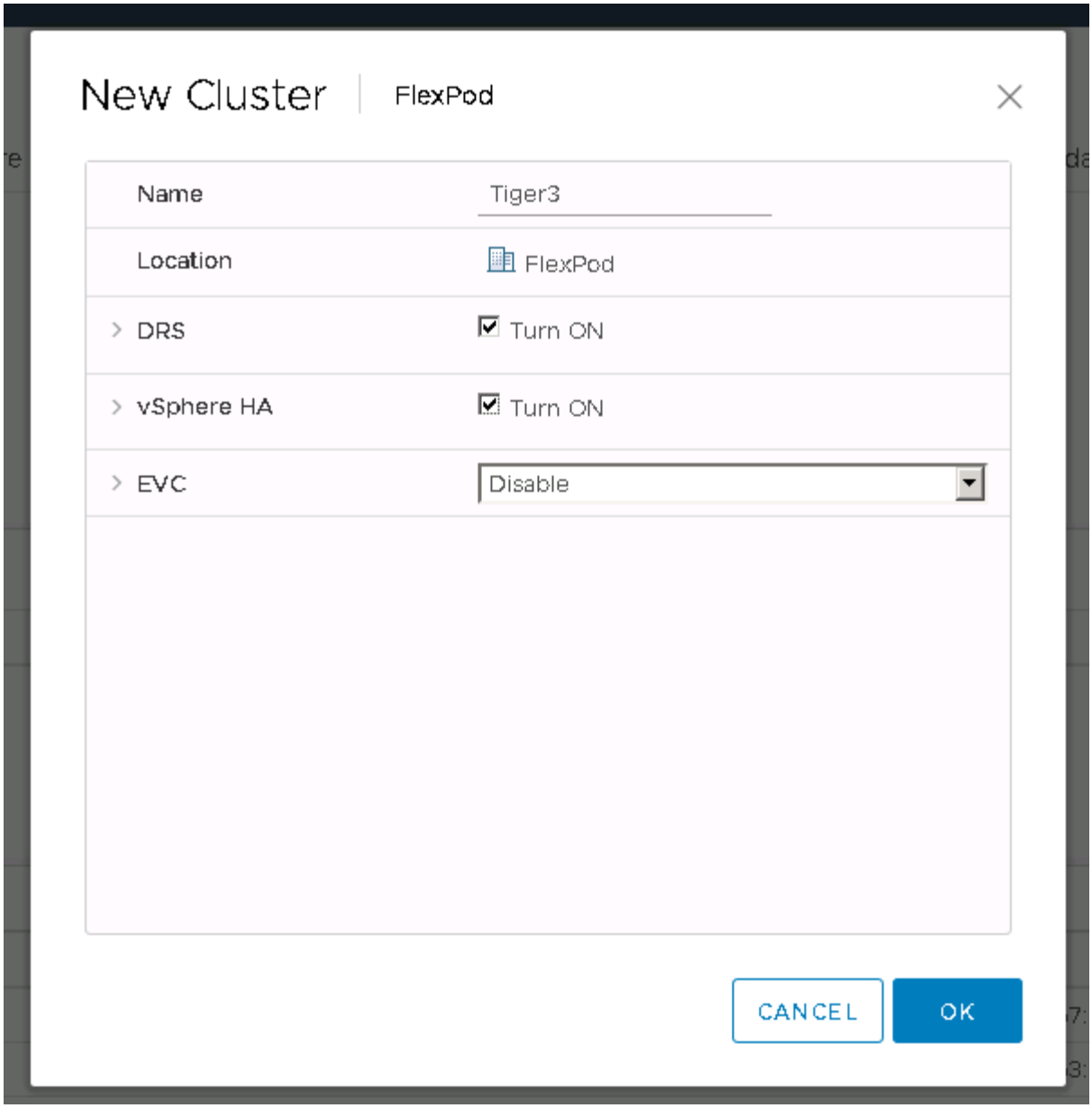
Pour configurer VMware vCenter Server 6.7 et la mise en cluster vSphere, procédez comme suit :

1. Accédez à https://\<<FQDN ou IP of vCenter>/vsphere-client/.
2. Cliquez sur lancer vSphere client.
3. Connectez-vous à l'aide du nom d'utilisateur mailto:administrator@vspehre.lockub l[administrator@vsphere.lockemb^] et du mot de passe SSO que vous avez saisi pendant le processus d'installation de VCSA.
4. Cliquez avec le bouton droit de la souris sur le nom du vCenter et sélectionnez Nouveau centre de données.
5. Entrez un nom pour le centre de données et cliquez sur OK.

Créez le cluster vSphere

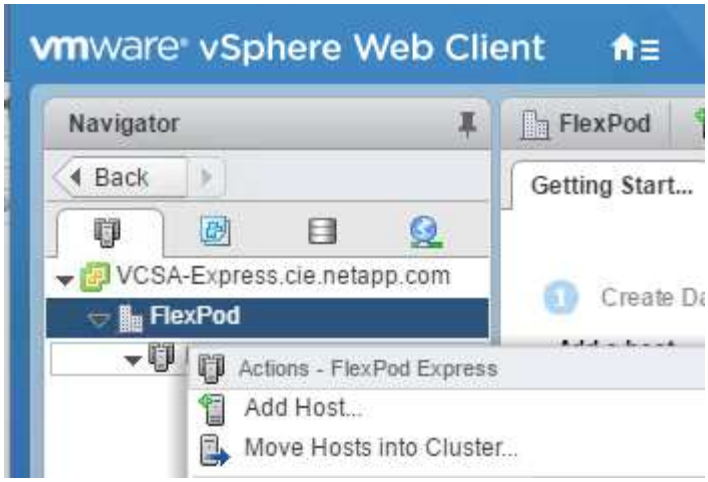
Pour créer un cluster vSphere, procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur le nouveau centre de données et sélectionnez Nouveau cluster.
2. Indiquez un nom pour le cluster.
3. Activez la reprise sur incident et vSphere HA en cochant les cases.
4. Cliquez sur OK.



Ajoutez des hôtes ESXi au cluster

1. Cliquez avec le bouton droit de la souris sur le cluster et sélectionnez Ajouter un hôte.



2. Pour ajouter un hôte ESXi au cluster, procédez comme suit :
   a. Entrez l'IP ou le FQDN de l'hôte. Cliquez sur Suivant.
   b. Entrez le nom d'utilisateur root et le mot de passe. Cliquez sur Suivant.
   c. Cliquez sur Oui pour remplacer le certificat de l'hôte par un certificat signé par le serveur de certificats VMware.
   d. Cliquez sur Suivant sur la page Récapitulatif de l'hôte.
   e. Cliquez sur l'icône verte + pour ajouter une licence à l'hôte vSphere.

      Si vous le souhaitez, cette étape peut être effectuée ultérieurement.

   f. Cliquez sur Suivant pour laisser le mode de verrouillage désactivé.
   g. Cliquez sur Next (Suivant) sur la page VM location.
   h. Consultez la page prêt à terminer. Utilisez le bouton Retour pour effectuer des modifications ou sélectionnez Terminer.
3. Répétez les étapes 1 et 2 pour l'hôte Cisco UCS B. Ce processus doit être effectué pour tout hôte supplémentaire ajouté à la configuration FlexPod Express.

Configurer coredump sur les hôtes ESXi

1. À l'aide de SSH, connectez-vous à l'hôte IP ESXi de gestion, entrez root pour le nom d'utilisateur et entrez le mot de passe racine.
2. Exécutez les commandes suivantes :

```
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. Le message `Verified the configured netdump server is running` s'affiche après la saisie de la commande finale.

Ce processus doit être effectué pour tout hôte supplémentaire ajouté à FlexPod Express.