FlexPod Express avec VMware vSphere 6.7U1 et NetApp AFF A220 avec stockage DAS basé sur IP

FlexPod

NetApp
March 25, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/flexpod/express/express-direct-attach-aff220-deploy_program_summary.html on March 25, 2024. Always check docs.netapp.com for the latest.

Sommaire

FlexPod Express avec VMware vSphere 6.7U1 et NetApp AFF A220 avec stockage DAS basé sur IP 1
NVA-1131-DEPLOY : FlexPod Express avec VMware vSphere 6.7U1 et NetApp AFF A220 avec stockage basé sur IP à connexion directe 1
Présentation de la solution 1
Exigences technologiques 5
Informations sur le câblage FlexPod Express 6
Procédures de déploiement 7
Conclusion 113
Informations supplémentaires 114

FlexPod Express avec VMware vSphere 6.7U1 et NetApp AFF A220 avec stockage DAS basé sur IP

NVA-1131-DEPLOY : FlexPod Express avec VMware vSphere 6.7U1 et NetApp AFF A220 avec stockage basé sur IP à connexion directe

Sree Lakshmi Lanka, NetApp

Les tendances du secteur témoignent d'une vaste transformation des data centers en infrastructure partagée et cloud computing. Elles recherchent par ailleurs une solution simple et efficace pour les succursales et les bureaux distants, exploitant la technologie qu'elles connaissent bien dans leur data Center.

FlexPod Express est une architecture préconçue et conforme aux bonnes pratiques. Elle repose sur la gamme Cisco Unified Computing System (Cisco UCS), la gamme de commutateurs Cisco Nexus et les technologies de stockage NetApp. Ce sont les composants d'un système FlexPod Express qui ressemble à ceux de leurs homologues FlexPod Datacenter, ce qui favorise une synergie de gestion dans l'ensemble de l'environnement d'infrastructure IT à plus petite échelle. Les plateformes FlexPod Datacenter et FlexPod Express sont optimales pour la virtualisation, les systèmes d'exploitation sans système d'exploitation et les charges de travail d'entreprise.

Les solutions FlexPod Datacenter et FlexPod Express proposent une configuration de base et offrent la polyvalence nécessaire pour faire face à des cas d'utilisation et à des exigences très variés. Les clients FlexPod Datacenter existants peuvent gérer leur système FlexPod Express avec les outils auxquels ils sont habitués. Les nouveaux clients FlexPod Express peuvent facilement s'adapter à la gestion d'FlexPod Datacenter à mesure que leur environnement se développe.

FlexPod Express est une infrastructure idéale pour les bureaux distants, les succursales et les moyennes entreprises. Il s'agit également d'une solution idéale pour les clients qui souhaitent mettre en place une infrastructure pour une charge de travail dédiée.

FlexPod Express offre une infrastructure facile à gérer qui convient à quasiment tous les workloads.

Présentation de la solution

Cette solution FlexPod Express fait partie du programme d'infrastructure convergée FlexPod.

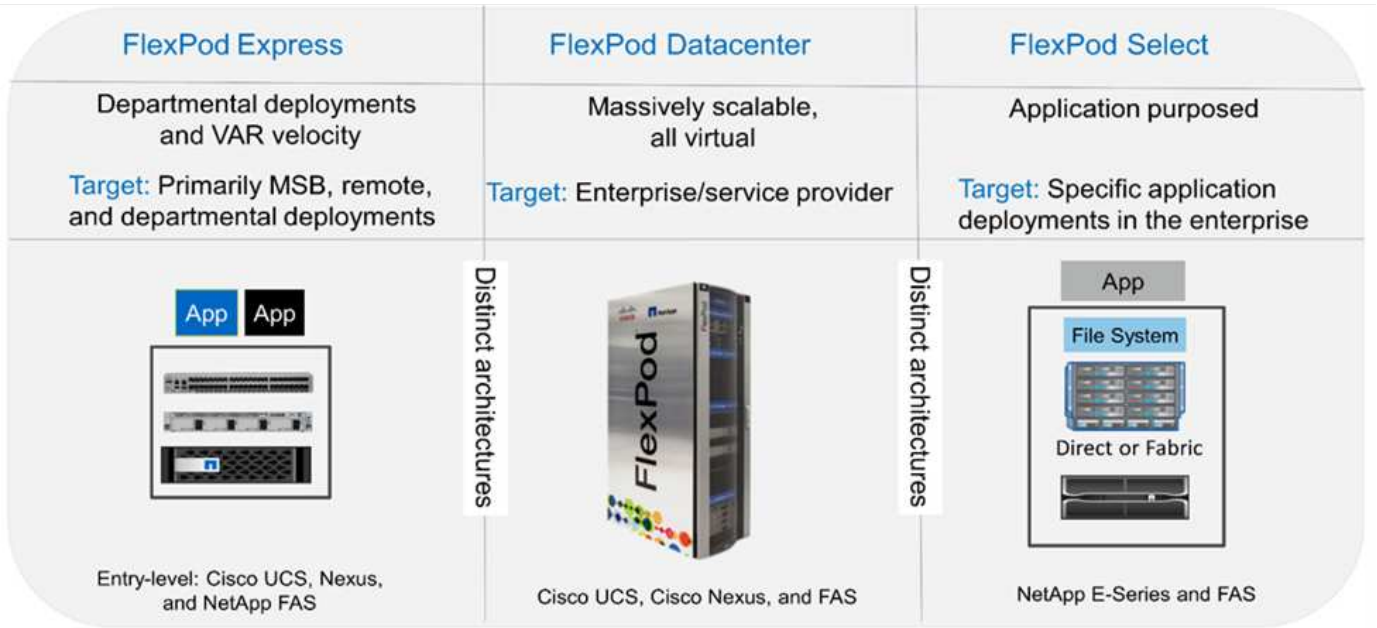
Programme FlexPod d'infrastructure convergée

Les architectures de référence FlexPod sont fournies sous la forme de conceptions validées par Cisco (CVD) ou d'architectures vérifiées NetApp (NVA). Les écarts en fonction des exigences du client par rapport à un CVD ou à une NVA donné sont autorisés si ces variations ne créent pas de configuration non prise en charge.

Comme le montre la figure ci-dessous, le programme FlexPod se compose de trois solutions : les Express FlexPod, le data Center FlexPod et FlexPod Select :

- **FlexPod Express** offre aux clients une solution d'entrée de gamme dotée de technologies Cisco et NetApp.
- **FlexPod Datacenter** offre une base polyvalente optimale pour diverses charges de travail et applications.
- **FlexPod Select** intègre les meilleurs aspects de FlexPod Datacenter et adapte l'infrastructure à une application donnée.

La figure suivante présente les composants techniques de la solution.



Programme d'architecture vérifiée NetApp

Le programme NVA propose une architecture vérifiée pour les solutions NetApp. NVA fournit une architecture de solution NetApp avec les qualités suivantes :

- Testée en profondeur
- Normative par nature
- Réduction des risques de déploiement
- Optimisée pour accélérer la mise en service

Ce guide détaille la conception de FlexPod Express avec un stockage NetApp DAS. Les sections suivantes répertorient les composants utilisés pour la conception de cette solution.

Composants matériels

- Avec AFF A220
- Cisco UCS Mini
- CISCO UCS B200 M5
- Cisco UCS VIC 1440/1480.
- Commutateurs Cisco Nexus 3000 Series

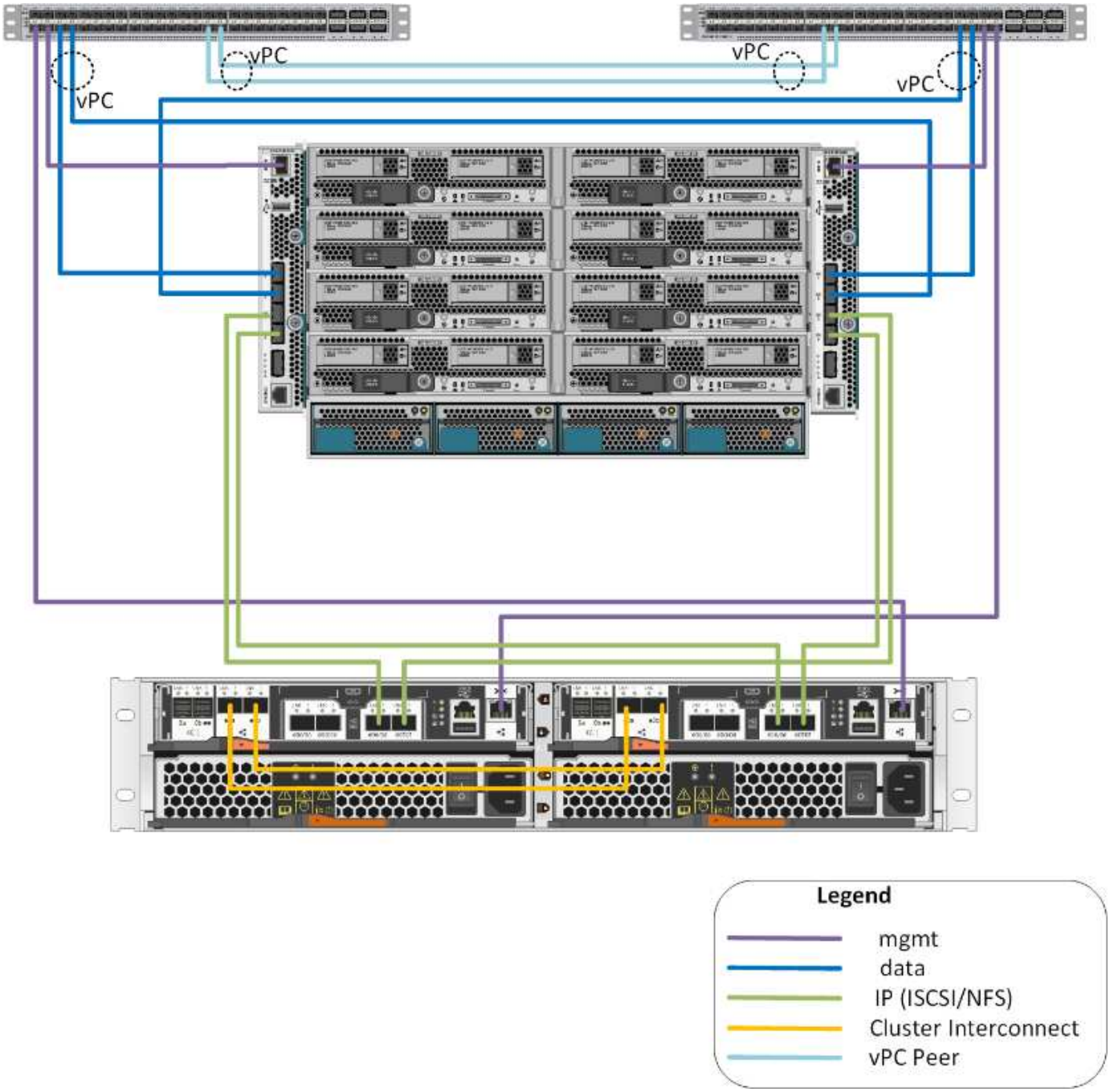
Composants logiciels

- NetApp ONTAP 9. 5
- VMware vSphere 6.7U1
- Cisco UCS Manager 4.0(1b)
- Micrologiciel Cisco NXOS 7.0(3)I6(1)

Technologie de la solution

Cette solution tire parti des dernières technologies de NetApp, Cisco et VMware. Le système comprend le nouveau NetApp AFF A220 exécutant ONTAP 9.5, deux commutateurs Cisco Nexus 31108VPC et des serveurs Cisco UCS B200 M5 exécutant VMware vSphere 6.7U1. Cette solution validée utilise le stockage IP Direct Connect sur la technologie 10GbE.

La figure suivante présente FlexPod Express avec VMware vSphere 6.7U1 Architecture Direct Connect basée sur IP.



Récapitulatif du cas d’utilisation

La solution FlexPod Express peut être appliquée à plusieurs cas d’utilisation, notamment :

- ROBO
- Moyennes entreprises
- Les environnements qui nécessitent une solution dédiée et économique

FlexPod Express est parfaitement adapté aux charges de travail virtualisées et mixtes.

Exigences technologiques

Un système FlexPod Express nécessite une combinaison de composants matériels et logiciels. FlexPod Express décrit également les composants matériels requis pour ajouter des nœuds d'hyperviseur au système par unités de deux.

Configuration matérielle requise

Quel que soit l'hyperviseur choisi, toutes les configurations FlexPod Express utilisent le même matériel. Par conséquent, même si les exigences de l'entreprise évoluent, les deux hyperviseurs peuvent s'exécuter sur le même matériel FlexPod Express.

Les composants matériels requis pour toutes les configurations FlexPod Express sont répertoriés dans le tableau suivant.

Sous-jacent	Quantité
PAIRE HAUTE DISPONIBILITÉ AFF A220	1
Serveur Cisco UCS B200 M5	2
Commutateur Cisco Nexus 31108PCV	2
Cisco UCS Virtual interface Card (VIC) 1440 pour serveur Cisco UCS B200 M5	2
Cisco UCS Mini avec deux interconnexions de fabric intégrées UCS-FI-M-6324	1

Configuration logicielle requise

Les composants logiciels requis pour implémenter les architectures des solutions FlexPod Express sont répertoriés dans le tableau suivant.

Logiciel	Version	Détails
Cisco UCS Manager	4.0(1b)	Pour Cisco UCS Fabric Interconnect FI-6324UP
Logiciels lame Cisco	4.0(1b)	Pour serveurs Cisco UCS B200 M5
Pilote nenic Cisco	1.0.25.0	Pour les cartes d'interface Cisco VIC 1440
Cisco NX-OS	7.0(3)I6(1)	Pour commutateurs Cisco Nexus 31108PCV
NetApp ONTAP	9.5	Pour les contrôleurs AFF A220

Le tableau suivant répertorie les logiciels requis pour toutes les implémentations VMware vSphere sur FlexPod Express.

Logiciel	Version
Appliance VMware vCenter Server	6.7U1

Logiciel	Version
Hyperviseur VMware vSphere ESXi	6.7U1

Informations sur le câblage FlexPod Express

Le câblage de la validation de référence est décrit dans les tableaux suivants.

Le tableau suivant répertorie les informations de câblage du commutateur Cisco Nexus 31108PCV A.

Périphérique local	Port local	Périphérique distant	Port distant
Commutateur Cisco Nexus 31108PCV A	Eth1/1	Contrôleur de stockage A AFF A220 NetApp	E0M
	Eth1/2	Cisco UCS-mini FI-A	mgmt0
	Eth1/3	Cisco UCS-mini FI-A	Eth1/1
	ETH 1/4	Cisco UCS-mini FI-B	Eth1/1
	ETH 1/13	CISCO NX 31108PCV B	ETH 1/13
	ETH 1/14	CISCO NX 31108PCV B	ETH 1/14

Le tableau suivant répertorie les informations de câblage du commutateur Cisco Nexus 31108PCV B.

Périphérique local	Port local	Périphérique distant	Port distant
Commutateur Cisco Nexus 31108PCV B	Eth1/1	Contrôleur de stockage B AFF A220 NetApp	E0M
	Eth1/2	Cisco UCS-mini FI-B	mgmt0
	Eth1/3	Cisco UCS-mini FI-A	Eth1/2
	ETH 1/4	Cisco UCS-mini FI-B	Eth1/2
	ETH 1/13	CISCO NX 31108PCV A	ETH 1/13
	ETH 1/14	CISCO NX 31108PCV A	ETH 1/14

Le tableau suivant répertorie les informations de câblage pour le contrôleur de stockage AFF A220 NetApp

Périphérique local	Port local	Périphérique distant	Port distant
Contrôleur de stockage A AFF A220 NetApp	e0a	Contrôleur de stockage B AFF A220 NetApp	e0a
	e0b	Contrôleur de stockage B AFF A220 NetApp	e0b
	e0e	Cisco UCS-mini FI-A	Eth1/3
	e0f	Cisco UCS-mini FI-B	Eth1/3
	E0M	CISCO NX 31108PCV A	Eth1/1

Le tableau suivant répertorie les informations de câblage pour le contrôleur de stockage B AFF A220 NetApp

Périphérique local	Port local	Périphérique distant	Port distant
Contrôleur de stockage B AFF A220 NetApp	e0a	Contrôleur de stockage B AFF A220 NetApp	e0a
	e0b	Contrôleur de stockage B AFF A220 NetApp	e0b
	e0e	Cisco UCS-mini FI-A	Eth1/4
	e0f	Cisco UCS-mini FI-B	Eth1/4
	E0M	CISCO NX 31108PCV B	Eth1/1

Le tableau suivant répertorie les informations de câblage pour Cisco UCS Fabric Interconnect A.

Périphérique local	Port local	Périphérique distant	Port distant
Interconnexion de fabric Cisco UCS A	Eth1/1	CISCO NX 31108PCV A	Eth1/3
	Eth1/2	CISCO NX 31108PCV B	Eth1/3
	Eth1/3	Contrôleur de stockage A AFF A220 NetApp	e0e
	Eth1/4	Contrôleur de stockage B AFF A220 NetApp	e0e
	mgmt0	CISCO NX 31108PCV A	Eth1/2

Le tableau suivant répertorie les informations de câblage pour Cisco UCS Fabric Interconnect B.

Périphérique local	Port local	Périphérique distant	Port distant
Interconnexion de fabric Cisco UCS B	Eth1/1	CISCO NX 31108PCV A	Eth1/4
	Eth1/2	CISCO NX 31108PCV B	Eth1/4
	Eth1/3	Contrôleur de stockage A AFF A220 NetApp	e0f
	Eth1/4	Contrôleur de stockage B AFF A220 NetApp	e0f
	mgmt0	CISCO NX 31108PCV B	Eth1/2

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. Les interconnexions de fabric A et Fabric Interconnect B sont les deux interconnexions de fabric Nexus intégrées.

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.

Nom du VLAN	Objectif VLAN	ID utilisé pour valider ce document
VLAN de gestion	VLAN pour les interfaces de gestion	18
VLAN natif	VLAN auquel des trames non marquées sont attribuées	2
VLAN NFS	VLAN pour le trafic NFS	104
VLAN VMware vMotion	VLAN désigné pour le déplacement de machines virtuelles (VM) d'un hôte physique à un autre	103
VLAN trafic des VM	VLAN pour le trafic des applications des VM	102
ISCSI-A-VLAN	VLAN pour le trafic iSCSI sur la structure A	124
ISCSI-B-VLAN	VLAN pour le trafic iSCSI sur la structure B	125

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 suivant répertorie les machines virtuelles VMware créées.

Description de la VM	Nom d'hôte
Serveur VMware vCenter	Seahawks-vcsa.cie.netapp.com

Procédure de déploiement de la solution Cisco Nexus 31108PCV

Cette section décrit en détail la configuration du commutateur Cisco Nexus 31308PCV utilisée dans un environnement FlexPod Express.

Configuration initiale du commutateur Cisco Nexus 31108PCV

Cette procédure décrit la configuration des commutateurs Cisco Nexus pour une utilisation dans un environnement FlexPod Express de base.

> Cette procédure suppose que vous utilisez un Cisco Nexus 31108PCV exécutant la version 7.0(3)I6(1) 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 31108PCV peuvent être connectées à un réseau de gestion existant, ou les interfaces mgmt0 des commutateurs 31108PCV 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 Cisco Nexus 31108PCV de FlexPod Express sont connectés à un réseau de gestion existant.

3. Pour configurer les commutateurs Cisco Nexus 31108PCV, 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 : 31108PCV-A
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
Configure the default gateway? (yes/no) [y]: y
IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
Configure advanced IP options? (yes/no) [n]: n
Enable the telnet service? (yes/no) [n]: n
Enable the ssh service? (yes/no) [y]: y
Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
Number of rsa key bits <1024-2048> [1024]: <enter>
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address : <<var_ntp_ip>>
Configure default interface layer (L3/L2) [L2]: <enter>
Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]:
<enter>
```

4. Un résumé de votre configuration s'affiche et vous êtes invité à modifier la configuration. Si votre configuration est correcte, entrez `n`.

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

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 les étapes 1 à 5 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.

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)`, Exécutez 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 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 de Spanning Tree par défaut, 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 différents VLAN, les VLAN de couche 2 doivent être définis sur le commutateur. 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 pour l'attribution de noms aux VLAN de couche 2, la définition de descriptions pour toutes les interfaces peut aider à l'approvisionnement et au 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 e0M
int eth1/2
  description Cisco UCS FI-A mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/1
int eth1/4
  description Cisco UCS FI-B eth1/1
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

Commutateur Cisco Nexus B

```
int eth1/1
  description AFF A220-B e0M
int eth1/2
  description Cisco UCS FI-B mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/2
int eth1/4
  description Cisco UCS FI-B eth1/2
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

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`), exécutez les commandes suivantes pour configurer les paramètres de port pour les interfaces de gestion des serveurs et du stockage :

Commutateur Cisco Nexus A

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Commutateur Cisco Nexus B

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Ajoutez l'interface de distribution NTP

Commutateur Cisco Nexus A

En mode de configuration globale, exécutez les commandes suivantes.

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-a-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-b-ntp-ip> use-vrf default
```

Commutateur Cisco Nexus B

En mode de configuration globale, exécutez les commandes suivantes.

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch- b-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-a-ntp-ip> use-vrf default
```

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 eth1/13-14
  channel-group 10 mode active
int Po10description vPC peer-link
switchport
switchport mode trunkswitchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
  channel-group 14 mode active
copy run start
```

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 eth1/13-14
  channel-group 10 mode active
int Po10
description vPC peer-link
switchport
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
```

```
  channel-group 14 mode active
copy run start
```

> Lors de cette validation de solution, une unité de transmission maximale (MTU) de 9 9000 a été utilisée. 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.

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 vous recommande d'utiliser des VPC pour uplink les commutateurs Cisco Nexus 31108PVC 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.

Procédure de déploiement du stockage NetApp (partie 1)

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

Installation du contrôleur de stockage NetApp AFF2xx

NetApp Hardware Universe

Le "NetApp Hardware Universe" (HWU) application 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. Sélectionnez l'onglet Comparer les systèmes de stockage pour afficher la compatibilité entre une autre version du logiciel ONTAP et les appliances de stockage NetApp avec vos 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 les sections suivantes : câbles d'alimentation pris en charge câbles et ports intégrés

Contrôleurs de stockage

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

NetApp ONTAP 9.5

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 9.5" (disponible dans le "Centre de documentation ONTAP 9"). Le tableau ci-dessous illustre les informations relatives à l'installation et à la configuration de ONTAP 9.5.

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

Détails du cluster	Valeur du détail 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 9.5	<<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>>
SERVEUR NTP A IP	<< switch-a-ntp-ip >>
IP DU SERVEUR NTP B	<< switch-b-ntp-ip >>

Configurer 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. 5 n'est pas la version du logiciel en cours de démarrage. poursuivez avec les étapes suivantes pour installer le nouveau logiciel. Si ONTAP 9. 5 est la version en cours de démarrage, sélectionnez l'option 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.

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. 5 n'est pas la version du logiciel en cours de démarrage. poursuivez avec les étapes suivantes 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.

Poursuivre la configuration du nœud A et 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 9.5 sur le nœud.

La procédure de configuration du nœud et du cluster a été légèrement modifiée dans ONTAP 9.5. 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 `<<switch-a-ntp-ip>>` Dans le champ serveur NTP principal.

      Vous pouvez également entrer un autre serveur NTP en tant que `<<switch- b-ntp-ip>>`.
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.

```
AFFA220-Clus::> ucadmin show
                      Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFFA220-Clus-01
              0c       cna      target     -        -          offline
AFFA220-Clus-01
              0d       cna      target     -        -          offline
AFFA220-Clus-01
              0e       cna      target     -        -          offline
AFFA220-Clus-01
              0f       cna      target     -        -          offline
AFFA220-Clus-02
              0c       cna      target     -        -          offline
AFFA220-Clus-02
              0d       cna      target     -        -          offline
AFFA220-Clus-02
              0e       cna      target     -        -          offline
AFFA220-Clus-02
              0f       cna      target     -        -          offline
8 entries were displayed.
```

2. 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 en exécutant 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.

Activez le Cisco Discovery Protocol

Pour activer le Cisco Discovery Protocol (CDP) sur les contrôleurs de stockage NetApp, exécutez la commande suivante :

```
node run -node * options cdpd.enable on
```

Activez le protocole de détection de couche de liaison sur tous les ports Ethernet

Activez l'échange des informations voisines par le protocole LLDP (Link-Layer Discovery Protocol) entre le stockage et les commutateurs réseau en exécutant la commande suivante. Cette commande active le protocole LLDP sur tous les ports de tous les nœuds du cluster.

```
node run * options lldp.enable on
```

Renommez les interfaces logiques de gestion

Pour renommer les interfaces logiques de gestion (LIF), 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_A_1 - newname AFF A220-01_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
   ```

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 les commandes suivantes :

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
```

La connexion directe Cisco UCS Mini à ONTAP ne prend pas en charge LACP.

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 e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_A -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
```

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 e0e-
<<var_nfs_vlan_id>>
network port vlan create -node <<var_nodeA>> -vlan-name e0f-
<<var_nfs_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0f-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>: e0e- <<var_nfs_vlan_id>>, <<var_nodeB>>: e0e-
<<var_nfs_vlan_id>> , <<var_nodeA>>:e0f- <<var_nfs_vlan_id>>,
<<var_nodeB>>:e0f-<<var_nfs_vlan_id>>
```

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

```
network port vlan create –node <<var_nodeA>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>: e0e- <<var_iscsi_vlan_A_id>>,<<var_nodeB>>: e0e-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>: e0f- <<var_iscsi_vlan_B_id>>,<<var_nodeB>>: e0f-
<<var_iscsi_vlan_B_id>>
```

3. Créez des ports MGMT-VLAN.

```
network port vlan create –node <<var_nodeA>> -vlan-name e0m-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0m-
<<mgmt_vlan_id>>
```

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` En ligne de commande, car les SVM étaient auparavant appelés serveurs

Configurez NFSv3 dans ONTAP

Le tableau ci-dessous 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 falsevserver export-
policy rule create –vserver Infra-SVM -policyname default –ruleindex 2
–protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>> -rorule sys –rwrule
sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. 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 B-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 le nom qualifié iSCSI (IQN) pour le 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

Pour créer un miroir de partage de charge du volume root du SVM dans ONTAP, effectuez les opérations suivantes :

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 DPvolume 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 nom de domaine complet 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_datastore_2 -aggregate
aggr1_nodeB -size 500GB - state online -policy default -junction-path
/infra_datastore_2 -space-guarantee none -percent- snapshot-space 0
```

```
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -juntion-path /infra_swap -space
-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Activez la déduplication dans ONTAP

Pour activer la déduplication sur les volumes appropriés une fois par jour, exécutez les commandes suivantes :

```
volume efficiency modify –vserver Infra-SVM –volume esxi_boot –schedule
sun-sat@0
volume efficiency modify –vserver Infra-SVM –volume infra_datastore_1
–schedule sun-sat@0
volume efficiency modify –vserver Infra-SVM –volume infra_datastore_2
–schedule sun-sat@0
```

Créer des LUN dans ONTAP

Pour créer deux LUN (Logical Unit Numbers) 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 ci-dessous 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 e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

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 a IP	<<var_NODEA_nfs_lif_01_a_ip>>
Nœud de stockage A NFS LIF 01 a masque réseau	<<var_NODEA_nfs_lif_01_a_mask>>
Nœud de stockage A NFS LIF 01 b IP	<<var_NODEA_nfs_lif_01_b_ip>>
Nœud de stockage A NFS LIF 01 b masque réseau	<<var_NODEA_nfs_lif_01_b_mask>>
Nœud de stockage B NFS LIF 02 a IP	<<var_NodeB_nfs_lif_02_a_ip>>
Nœud de stockage B NFS LIF 02 a masque réseau	<<var_NodeB_nfs_lif_02_a_mask>>
Nœud de stockage B NFS LIF 02 b IP	<<var_NodeB_nfs_lif_02_b_ip>>
Nœud de stockage B NFS LIF 02 b masque réseau	<<var_NodeB_nfs_lif_02_b_mask>>

1. Créer une LIF NFS.

```
network interface create -vserver Infra-SVM -lif nfs_lif01_a -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0e-
<<var_nfs_vlan_id>> –address <<var_nodeA_nfs_lif_01_a_ip>> - netmask <<
var_nodeA_nfs_lif_01_a_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif01_b -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0f-
<<var_nfs_vlan_id>> –address <<var_nodeA_nfs_lif_01_b_ip>> - netmask <<
var_nodeA_nfs_lif_01_b_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_a -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0e-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_a_ip>> - netmask <<
var_nodeB_nfs_lif_02_a_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_b -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0f-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_b_ip>> - netmask <<
var_nodeB_nfs_lif_02_b_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface show
```

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 la LIF d'administration d'un SVM d'infrastructure et d'un 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 la SVM `vsadmin` et déverrouillez 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
```

Configuration du serveur Cisco UCS

Base FlexPod Cisco UCS

Configuration initiale de l'interconnexion de fabric Cisco UCS 6324 pour les environnements FlexPod

Cette section décrit des procédures détaillées de configuration de Cisco UCS pour une utilisation dans un environnement ROBO FlexPod avec Cisco UCS Manager.

Interconnexion de fabric Cisco UCS 6324 A

Cisco UCS utilise des serveurs et des réseaux de couches d'accès. Ce système serveur nouvelle génération hautes performances fournit un datacenter avec un degré élevé d'agilité et d'évolutivité des charges de travail.

Cisco UCS Manager 4.0(1b) prend en charge l'interconnexion de fabric 6324 qui intègre Fabric Interconnect dans le châssis Cisco UCS et offre une solution intégrée pour réduire l'environnement de déploiement. Cisco UCS Mini simplifie la gestion du système et permet de réaliser des économies pour les déploiements à faible échelle.

Les composants matériels et logiciels prennent en charge la structure unifiée de Cisco, qui exécute plusieurs types de trafic de data Center sur un seul adaptateur réseau convergé.

Configuration initiale du système

Lors de la première accès à une Fabric Interconnect dans un domaine Cisco UCS, un assistant d'installation vous demande les informations suivantes requises pour configurer le système :

- Méthode d'installation (interface graphique ou interface de ligne de commande)
- Mode Configuration (restauration à partir de la sauvegarde complète du système ou de la configuration initiale)
- Type de configuration système (configuration autonome ou en cluster)
- Nom du système

- Mot de passe d’administrateur
- Adresse IPv4 et masque de sous-réseau du port de gestion ou adresse et préfixe IPv6
- Adresse IPv4 ou IPv6 de la passerelle par défaut
- Adresse IPv4 ou IPv6 du serveur DNS
- Nom de domaine par défaut

Le tableau suivant répertorie les informations nécessaires pour terminer la configuration initiale de Cisco UCS sur Fabric Interconnect A

Détails	**Détail/valeur**
Nom du système	<<var_ucs_clustername>>
Mot de passe administrateur	\<<var_password>
Adresse IP de gestion : Fabric Interconnect A	<<var_ucsa_mgmt_ip>>
Masque de réseau de gestion : Fabric Interconnect A	<<var_ucsa_mgmt_mask>>
Passerelle par défaut : Fabric Interconnect A	<<var_ucsa_mgmt_gateway>>
Adresse IP de cluster	<<var_ucs_cluster_ip>>
Adresse IP du serveur DNS	<<var_nameserver_ip>>
Nom de domaine	<<nom_domaine_var>>

Pour configurer le système Cisco UCS en vue de son utilisation dans un environnement FlexPod, procédez comme suit :

1. Connectez-vous au port console du premier Cisco UCS 6324 Fabric Interconnect A.

```
Enter the configuration method. (console/gui) ? console

  Enter the setup mode; setup newly or restore from backup.
(setup/restore) ? setup

  You have chosen to setup a new Fabric interconnect. Continue? (y/n): y

  Enforce strong password? (y/n) [y]: Enter

  Enter the password for "admin":<<var_password>>
  Confirm the password for "admin":<<var_password>>

  Is this Fabric interconnect part of a cluster(select 'no' for
standalone)? (yes/no) [n]: yes

  Enter the switch fabric (A/B) []: A

  Enter the system name: <<var_ucs_clustername>>

  Physical Switch Mgmt0 IP address : <<var_ucsa_mgmt_ip>>

  Physical Switch Mgmt0 IPv4 netmask : <<var_ucsa_mgmt_mask>>

  IPv4 address of the default gateway : <<var_ucsa_mgmt_gateway>>

  Cluster IPv4 address : <<var_ucs_cluster_ip>>

  Configure the DNS Server IP address? (yes/no) [n]: y

       DNS IP address : <<var_nameserver_ip>>

  Configure the default domain name? (yes/no) [n]: y
Default domain name: <<var_domain_name>>

  Join centralized management environment (UCS Central)? (yes/no) [n]:
no

 NOTE: Cluster IP will be configured only after both Fabric
Interconnects are initialized. UCSM will be functional only after peer
FI is configured in clustering mode.

  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. Vérifiez les paramètres affichés sur la console. S'ils sont corrects, répondez `yes` pour appliquer et enregistrer la configuration.
3. Attendez que l'invite de connexion vérifie que la configuration a été enregistrée.

Le tableau suivant répertorie les informations nécessaires pour terminer la configuration initiale de Cisco UCS sur Fabric Interconnect B.

Détails	**Détail/valeur**
Nom du système	<<var_ucs_clustername>>
Mot de passe administrateur	\<<var_password>
Adresse IP de gestion-FI B	<<var_ucstm_mgmt_ip>>
Masque de réseau de gestion-FI B	<<var_ucstm_mgmt_mask>>
Passerelle par défaut FI B	<<var_ucstm_mgmt_gateway>>
Adresse IP du cluster	<<var_ucs_cluster_ip>>
Adresse IP du serveur DNS	<<var_nameserver_ip>>
Nom de domaine	<<nom_domaine_var>>

1. Connectez-vous au port de console du deuxième système Cisco UCS 6324 Fabric Interconnect B.

```
 Enter the configuration method. (console/gui) ? console

  Installer has detected the presence of a peer Fabric interconnect.
This Fabric interconnect will be added to the cluster. Continue (y/n) ?
y

  Enter the admin password of the peer Fabric
interconnect:<<var_password>>
    Connecting to peer Fabric interconnect... done
    Retrieving config from peer Fabric interconnect... done
    Peer Fabric interconnect Mgmt0 IPv4 Address: <<var_ucsb_mgmt_ip>>
    Peer Fabric interconnect Mgmt0 IPv4 Netmask: <<var_ucsb_mgmt_mask>>
    Cluster IPv4 address: <<var_ucs_cluster_address>>

    Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric
Interconnect Mgmt0 IPv4 Address

  Physical Switch Mgmt0 IP address : <<var_ucsb_mgmt_ip>>


  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. Attendez que l'invite de connexion confirme que la configuration a été enregistrée.

Connectez-vous à Cisco UCS Manager

Pour vous connecter à l'environnement Cisco Unified Computing System (UCS), procédez comme suit :

1. Ouvrez un navigateur Web et accédez à l'adresse de cluster Cisco UCS Fabric Interconnect.

   Vous devrez peut-être attendre au moins 5 minutes après la configuration du second Fabric Interconnect pour Cisco UCS Manager.

2. Cliquez sur le lien Launch UCS Manager pour lancer Cisco UCS Manager.
3. Acceptez les certificats de sécurité nécessaires.
4. Lorsque vous y êtes invité, entrez admin comme nom d'utilisateur et saisissez le mot de passe administrateur.
5. Cliquez sur connexion pour vous connecter à Cisco UCS Manager.

Logiciel Cisco UCS Manager version 4.0(1b)

Ce document suppose l'utilisation de la version 4.0(1b) du logiciel Cisco UCS Manager. Pour mettre à niveau le logiciel Cisco UCS Manager et le logiciel Cisco UCS 6324 Fabric Interconnect, reportez-vous à la "Guides

d'installation et de mise à niveau de Cisco UCS Manager."

Configurez le service d'appel principal Cisco UCS

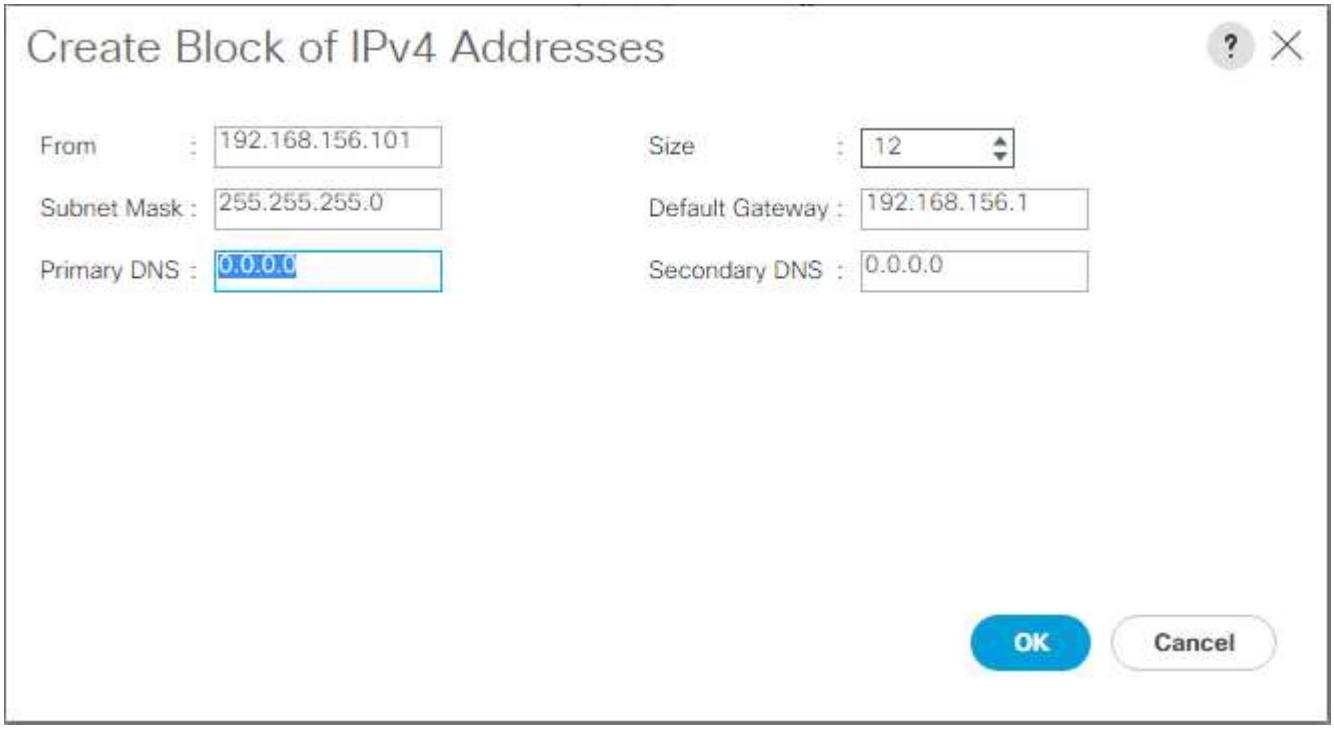
Cisco vous recommande fortement de configurer Call Home dans Cisco UCS Manager. La configuration du service d'appel en cas d'incident accélère la résolution des problèmes. Pour configurer Call Home, procédez comme suit :

1. Dans Cisco UCS Manager, cliquez sur Admin sur la gauche.
2. Sélectionnez tout > gestion des communications > appel.
3. Définissez l'état sur activé.
4. Remplissez tous les champs en fonction de vos préférences de gestion, puis cliquez sur Enregistrer les modifications et sur OK pour terminer la configuration de l'appel d'accueil.

Ajoutez un bloc d'adresses IP pour l'accès au clavier, à la vidéo et à la souris

Pour créer un bloc d'adresses IP pour l'accès au clavier, à la vidéo et à la souris (KVM) intrabande des serveurs dans l'environnement Cisco UCS, effectuez les opérations suivantes :

1. Dans Cisco UCS Manager, cliquez sur LAN sur la gauche.
2. Développez pools > racine > pools IP.
3. Cliquez avec le bouton droit de la souris sur IP Pool ext-mgmt et sélectionnez Créer un bloc d'adresses IPv4.
4. Entrez l'adresse IP de début du bloc, le nombre d'adresses IP requises, ainsi que le masque de sous-réseau et les informations relatives à la passerelle.



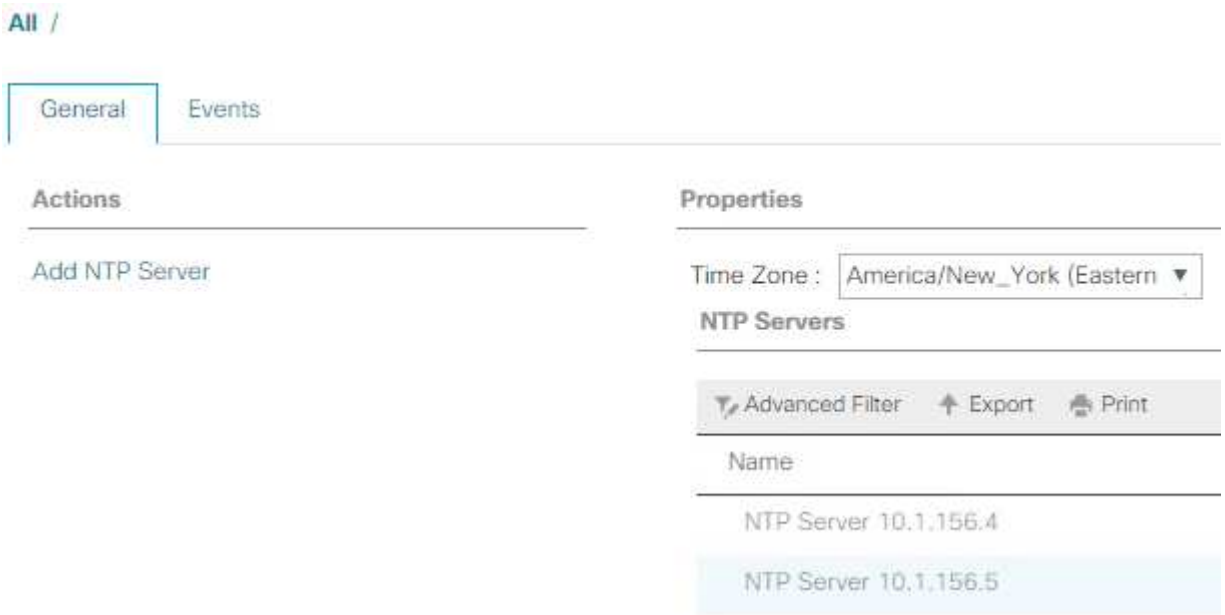
5. Cliquez sur OK pour créer le bloc.
6. Cliquez sur OK dans le message de confirmation.

Synchronisation de Cisco UCS avec NTP

Pour synchroniser l'environnement Cisco UCS avec les serveurs NTP des commutateurs Nexus, effectuez la procédure suivante :

1. Dans Cisco UCS Manager, cliquez sur Admin sur la gauche.
2. Développez tout > gestion du fuseau horaire.
3. Sélectionnez fuseau horaire.
4. Dans le volet Propriétés, sélectionnez le fuseau horaire approprié dans le menu fuseau horaire.
5. Cliquez sur Enregistrer les modifications et cliquez sur OK.
6. Cliquez sur Ajouter un serveur NTP.
7. Entrez `<switch-a-ntp-ip> or <Nexus-A-mgmt-IP>` Puis cliquez sur OK. Cliquez sur OK.

8. Cliquez sur Ajouter un serveur NTP.
9. Entrez `<switch-b-ntp-ip> or <Nexus-B-mgmt-IP>` Puis cliquez sur OK. Cliquez sur OK dans la confirmation.



Modifier la règle de découverte du châssis

La définition de la politique de découverte facilite l'ajout du châssis Cisco UCS B-Series et d'autres éléments Fabric Extender pour la connectivité Cisco UCS C-Series. Pour modifier la politique de détection du châssis, procédez comme suit :

1. Dans Cisco UCS Manager, cliquez sur Equipment à gauche et sélectionnez Equipment dans la deuxième liste.
2. Dans le volet de droite, sélectionnez l'onglet stratégies.
3. Dans Global Policies, définissez la stratégie de découverte châssis/FEX pour qu'elle corresponde au nombre minimal de ports uplink câblés entre le châssis ou les Fabric Extender (FEXes) et les Fabric Interconnect.
4. Définissez la préférence de regroupement de liens sur Canal de port. Si l'environnement en cours de configuration contient une grande quantité de trafic multidiffusion, définissez le paramètre de hachage du matériel de multidiffusion sur activé.
5. Cliquez sur Save Changes.
6. Cliquez sur OK.

Activez les ports de serveur, de liaison montante et de stockage

Pour activer les ports de serveur et de liaison montante, procédez comme suit :

1. Dans Cisco UCS Manager, dans le volet de navigation, sélectionnez l'onglet Equipement.
2. Développez Equipment > Fabric Interconnect > Fabric Interconnect A > module fixe.
3. Développez ports Ethernet.
4. Sélectionnez les ports 1 et 2 connectés aux commutateurs Cisco Nexus 31108, cliquez avec le bouton droit de la souris et sélectionnez configurer comme port Uplink.
5. Cliquez sur Oui pour confirmer les ports de liaison ascendante et cliquez sur OK.
6. Sélectionnez les ports 3 et 4 connectés aux contrôleurs de stockage NetApp, cliquez avec le bouton droit de la souris et sélectionnez configurer en tant que port d'appliance.
7. Cliquez sur Oui pour confirmer les ports de l'appliance.
8. Dans la fenêtre configurer comme port de l'appliance, cliquez sur OK.
9. Cliquez sur OK pour confirmer.
10. Dans le volet de gauche, sélectionnez module fixe sous Fabric Interconnect A.
11. Dans l'onglet ports Ethernet, vérifiez que les ports ont été correctement configurés dans la colonne rôle si. Si des serveurs C-Series de port ont été configurés sur le port d'évolutivité, cliquez dessus pour vérifier la connectivité des ports.

Equipment / Fabric Interconnects / Fabric Interconnect A (subordinate) / Fixed Module

General | Ethernet Ports | FC Ports | Faults | Events

Advanced Filter | Export | Print | All | Unconfigured | Network | Server | FCoE Uplink | Unified Uplink | Appliance Storage | FCoE Storage | Unified Storage | Monitor

Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer
1	0	1	00:DE:FB:30:36:88	Network	Physical	Up	Enabled	
1	0	2	00:DE:FB:30:36:89	Network	Physical	Up	Enabled	
1	0	3	00:DE:FB:30:36:8A	Appliance Storage	Physical	Up	Enabled	
1	0	4	00:DE:FB:30:36:8B	Appliance Storage	Physical	Up	Enabled	
1	5	1	00:DE:FB:30:36:8C	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	2	00:DE:FB:30:36:8D	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	3	00:DE:FB:30:36:8E	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	4	00:DE:FB:30:36:8F	Unconfigured	Physical	Sfp Not Present	Disabled	

12. Développez équipement > interconnexions de fabric > Fabric Interconnect B > module fixe.
13. Développez ports Ethernet.
14. Sélectionnez les ports Ethernet 1 et 2 connectés aux commutateurs Cisco Nexus 31108, cliquez avec le bouton droit de la souris et sélectionnez configurer comme port Uplink.
15. Cliquez sur Oui pour confirmer les ports de liaison ascendante et cliquez sur OK.
16. Sélectionnez les ports 3 et 4 connectés aux contrôleurs de stockage NetApp, cliquez avec le bouton droit de la souris et sélectionnez configurer en tant que port d'appliance.
17. Cliquez sur Oui pour confirmer les ports de l'appliance.
18. Dans la fenêtre configurer comme port de l'appliance, cliquez sur OK.
19. Cliquez sur OK pour confirmer.
20. Dans le volet de gauche, sélectionnez module fixe sous Fabric Interconnect B.
21. Dans l'onglet ports Ethernet, vérifiez que les ports ont été correctement configurés dans la colonne rôle si. Si des serveurs C-Series de port ont été configurés sur le port d'évolutivité, cliquez dessus pour vérifier la connectivité des ports.

Equipment / Fabric Interconnects / Fabric Interconnect B (primar... / Fixed Module / Ethernet Ports

Ethernet Ports

Advanced Filter | Export | Print | All | Unconfigured | Network | Server | FCoE Uplink | Unified Uplink | Appliance Storage | FCoE Storage | Unified Storage | Monitor

Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer
1	0	1	00:DE:FB:30:3A:C8	Network	Physical	Up	Enabled	
1	0	2	00:DE:FB:30:3A:C9	Network	Physical	Up	Enabled	
1	0	3	00:DE:FB:30:3A:CA	Appliance Storage	Physical	Up	Enabled	
1	0	4	00:DE:FB:30:3A:CB	Appliance Storage	Physical	Up	Enabled	
1	5	1	00:DE:FB:30:3A:CC	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	2	00:DE:FB:30:3A:CD	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	3	00:DE:FB:30:3A:CE	Unconfigured	Physical	Sfp Not Present	Disabled	
1	5	4	00:DE:FB:30:3A:CF	Unconfigured	Physical	Sfp Not Present	Disabled	

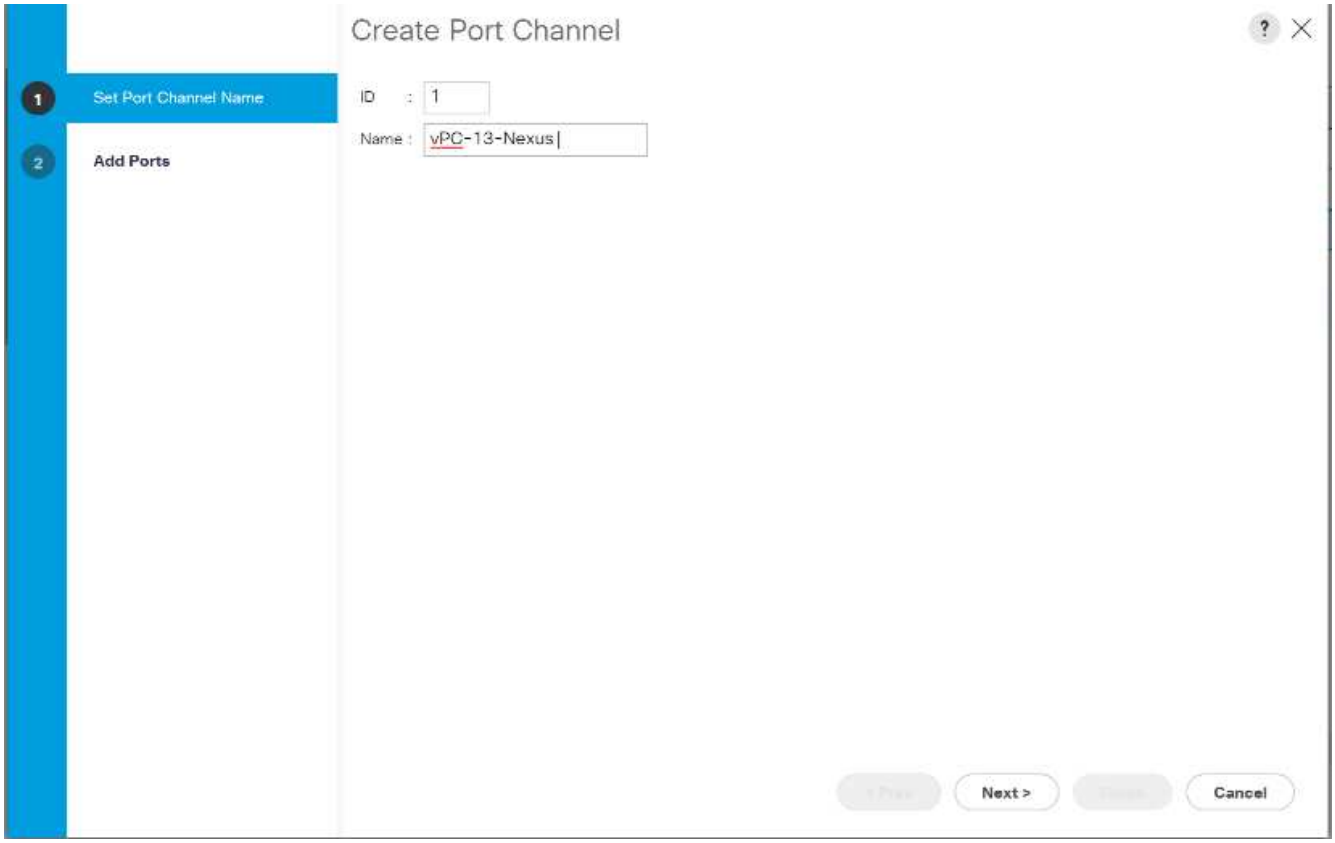
Créez des canaux de port uplink avec les commutateurs Cisco Nexus 31108

Pour configurer les canaux de port nécessaires dans l'environnement Cisco UCS, effectuez les opérations suivantes :

1. Dans Cisco UCS Manager, sélectionnez l'onglet LAN dans le volet de navigation.

> Cette procédure crée deux canaux de port : un de la structure A aux commutateurs Cisco Nexus 31108 et un de la structure B aux deux commutateurs Cisco Nexus 31108. Si vous utilisez des commutateurs standard, modifiez cette procédure en conséquence. Si vous utilisez des commutateurs 1 Gigabit Ethernet (1GbE) et des SFP GLC-T sur Fabric Interconnect, les vitesses d'interface des ports Ethernet 1/1 et 1/2 dans Fabric Interconnect doivent être définies à 1 Gbit/s.

2. Sous LAN > LAN Cloud, développez l'arborescence structure A.
3. Cliquez avec le bouton droit de la souris sur canaux de port.
4. Sélectionnez Créer un canal de port.
5. Entrez 13 comme ID unique du canal de port.
6. Entrez VPC-13-Nexus comme nom du canal du port.
7. Cliquez sur Suivant.



8. Sélectionnez les ports suivants à ajouter au canal de port :
   a. Les emplacements ID 1 et port 1
   b. Les emplacements ID 1 et 2
9. Cliquez sur >> pour ajouter les ports au canal de port.

10. Cliquez sur Terminer pour créer le canal de port. Cliquez sur OK.
11. Sous canaux de port, sélectionnez le nouveau canal de port créé.

    Le canal de port doit avoir un état général de mise en service.

12. Dans le volet de navigation, sous LAN > LAN Cloud, développez l'arborescence structure B.
13. Cliquez avec le bouton droit de la souris sur canaux de port.
14. Sélectionnez Créer un canal de port.
15. Entrez 14 comme ID unique du canal de port.
16. Entrez VPC-14-Nexus comme nom du canal du port. Cliquez sur Suivant.
17. Sélectionnez les ports suivants à ajouter au canal de port :
    a. Les emplacements ID 1 et port 1
    b. Les emplacements ID 1 et 2
18. Cliquez sur >> pour ajouter les ports au canal de port.
19. Cliquez sur Terminer pour créer le canal de port. Cliquez sur OK.
20. Sous canaux de port, sélectionnez le nouveau canal de port créé.
21. Le canal de port doit avoir un état général de mise en service.

Créer une organisation (facultatif)

Les entreprises ont recours à l'organisation des ressources et à la restriction de l'accès aux différents groupes de l'organisation IT, ce qui permet la colocation des ressources de calcul.

> Bien que ce document ne suppose pas l'utilisation d'organisations, cette procédure fournit des instructions pour en créer une.

Pour configurer une organisation dans l'environnement Cisco UCS, procédez comme suit :

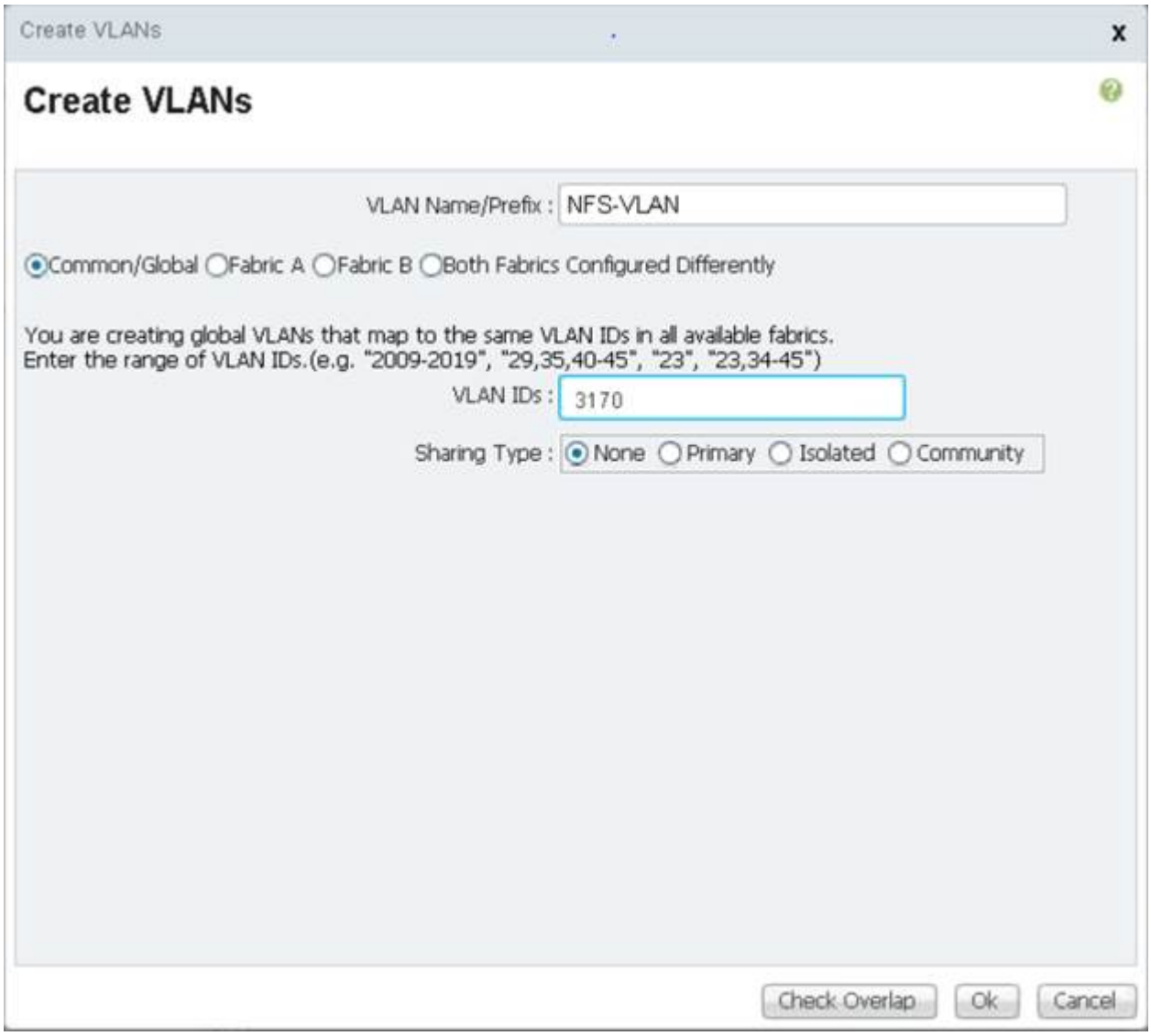
1. Dans Cisco UCS Manager, dans le menu Nouveau de la barre d'outils en haut de la fenêtre, sélectionnez Créer une organisation.
2. Saisissez un nom pour l'organisation.
3. Facultatif : saisissez une description pour l'organisation. Cliquez sur OK.
4. Cliquez sur OK dans le message de confirmation.

Configuration des ports de l'appliance de stockage et des VLAN de stockage

Pour configurer les ports de l'appliance de stockage et les VLAN de stockage, procédez comme suit :

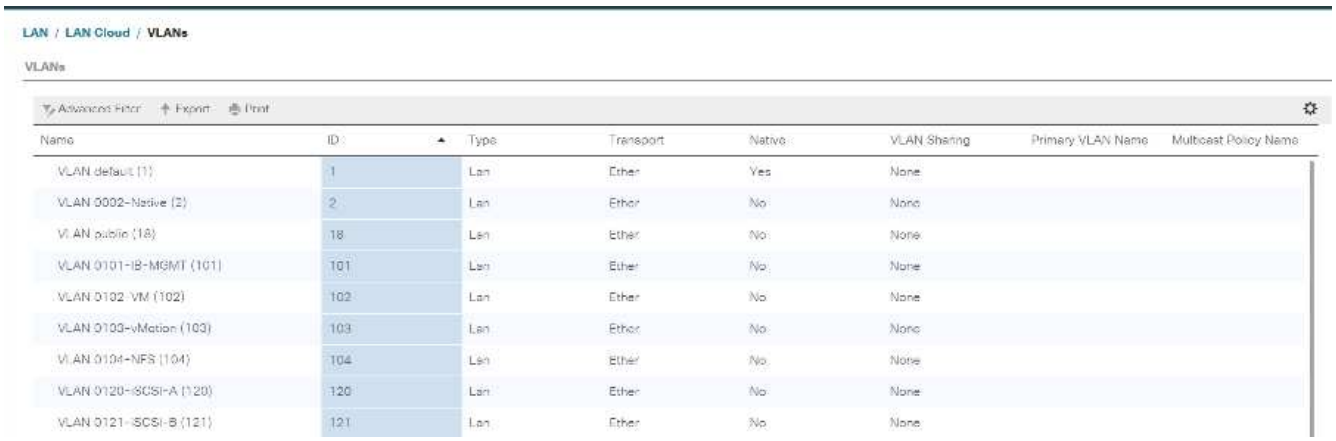
1. Dans Cisco UCS Manager, sélectionnez l'onglet LAN.
2. Étendez le cloud Appliances.
3. Cliquez avec le bouton droit de la souris sur réseaux locaux virtuels sous Appliances Cloud.
4. Sélectionnez Créer des VLAN.
5. Indiquez NFS-VLAN comme nom du VLAN NFS de l'infrastructure.
6. Laisser commun/Global sélectionné.

7. Entrez `<<var_nfs_vlan_id>>` Pour l'ID VLAN.
8. Laisser le type de partage défini sur aucun.

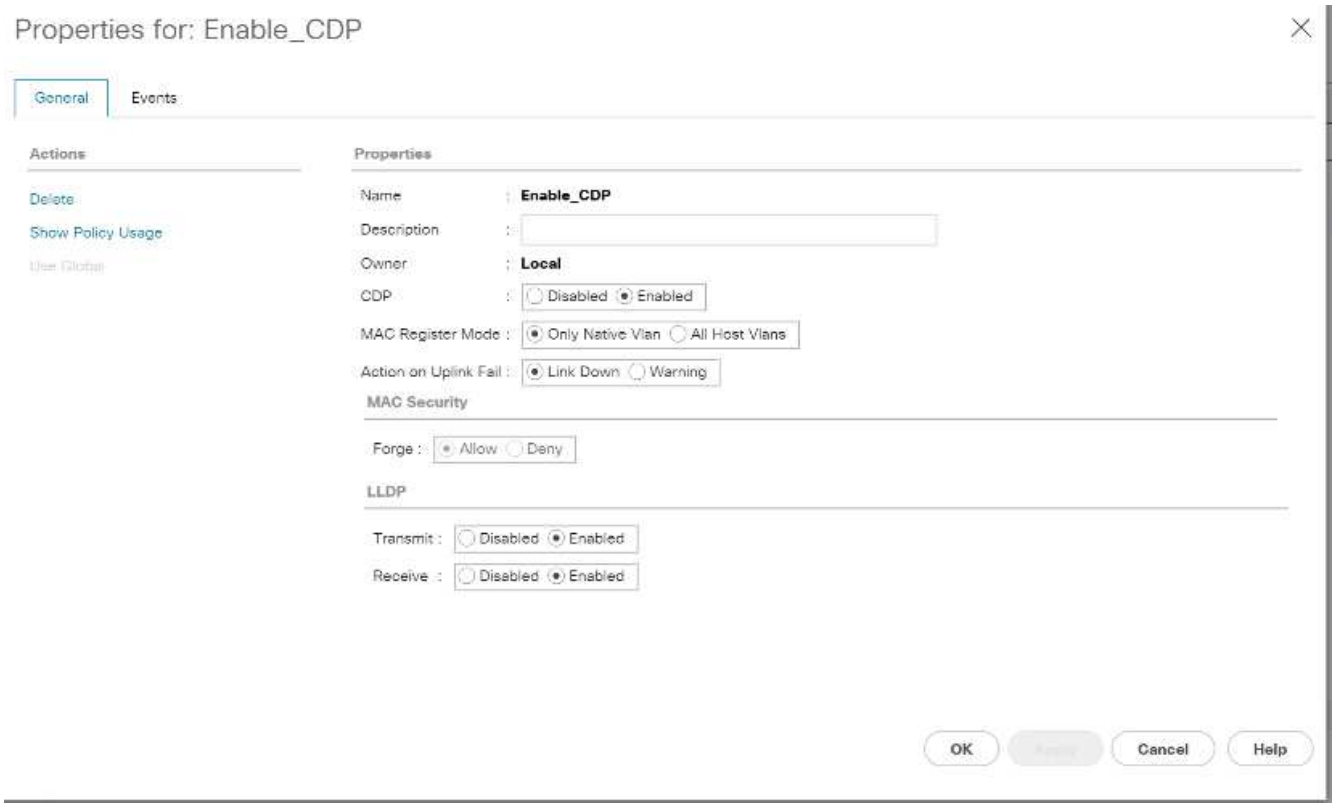


9. Cliquez sur OK, puis à nouveau sur OK pour créer le VLAN.
10. Cliquez avec le bouton droit de la souris sur réseaux locaux virtuels sous Appliances Cloud.
11. Sélectionnez Créer des VLAN.
12. Saisissez iSCSI-A-VLAN comme nom pour le VLAN Infrastructure iSCSI Fabric A.
13. Laisser commun/Global sélectionné.
14. Entrez `<<var_iscsi-a_vlan_id>>` Pour l'ID VLAN.
15. Cliquez sur OK, puis à nouveau sur OK pour créer le VLAN.
16. Cliquez avec le bouton droit de la souris sur réseaux locaux virtuels sous Appliances Cloud.
17. Sélectionnez Créer des VLAN.
18. Entrez iSCSI-B-VLAN comme nom pour le VLAN de structure B iSCSI de l'infrastructure.
19. Laisser commun/Global sélectionné.
20. Entrez `<<var_iscsi-b_vlan_id>>` Pour l'ID VLAN.

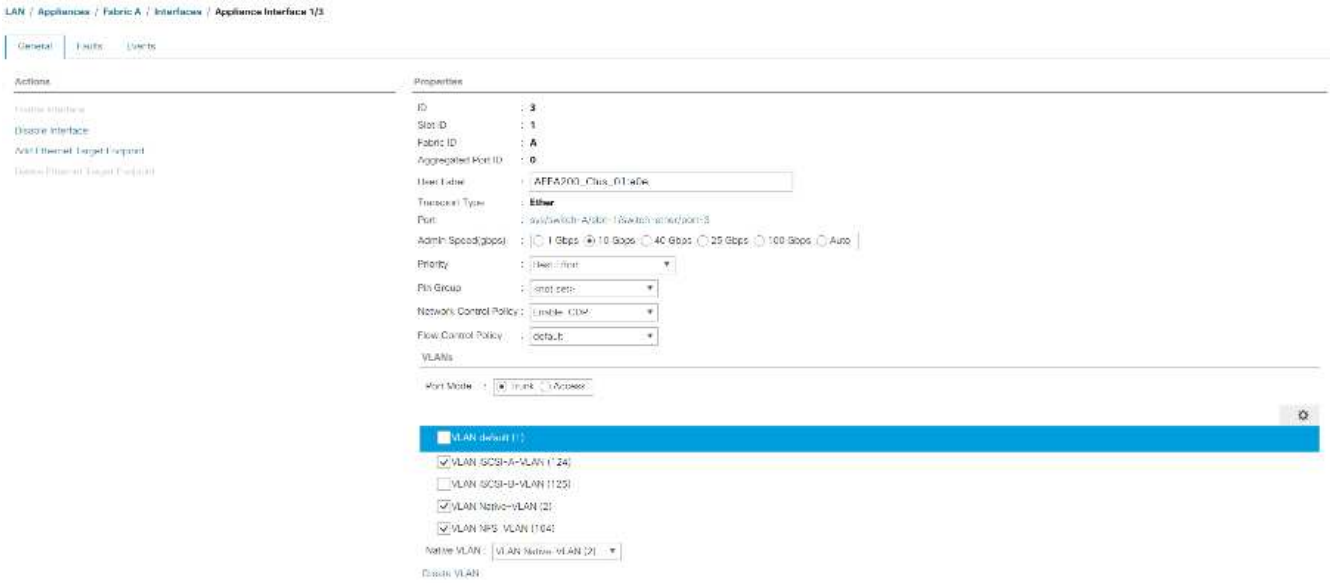
21. Cliquez sur OK, puis à nouveau sur OK pour créer le VLAN.
22. Cliquez avec le bouton droit de la souris sur réseaux locaux virtuels sous Appliances Cloud.
23. Sélectionnez Créer des VLAN.
24. Saisissez Native-VLAN comme nom pour le VLAN natif.
25. Laisser commun/Global sélectionné.
26. Entrez `<<var_native_vlan_id>>` Pour l'ID VLAN.
27. Cliquez sur OK, puis à nouveau sur OK pour créer le VLAN.



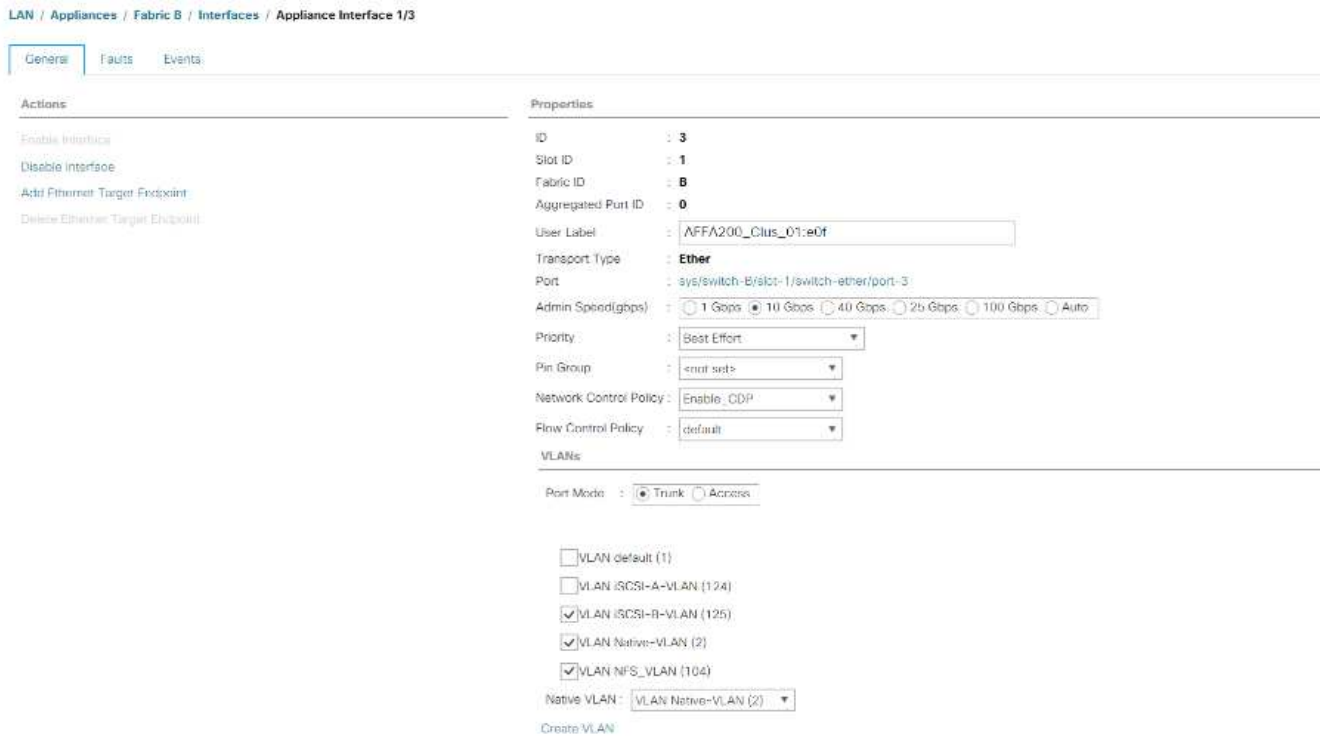
28. Dans le volet de navigation, sous LAN > stratégies, développez appareils et cliquez avec le bouton droit de la souris sur stratégies de contrôle du réseau.
29. Sélectionnez Créer une stratégie de contrôle réseau.
30. Nommez la règle `Enable_CDP_LLPD` Et sélectionnez activé en regard de CDP.
31. Activez les fonctions de transmission et de réception pour LLDP.



32. Cliquez sur OK, puis à nouveau sur OK pour créer la stratégie.
33. Dans le volet de navigation, sous LAN > Appliances Cloud, développez l'arborescence structure A.
34. Développez interfaces.
35. Sélectionnez interface de l'appareil 1/3.
36. Dans le champ libellé utilisateur, indiquez les informations indiquant le port du contrôleur de stockage, par exemple `<storage_controller_01_name>:e0e`. Cliquez sur Enregistrer les modifications et sur OK.
37. Sélectionnez la stratégie de contrôle réseau Activer_CDP, puis sélectionnez Enregistrer les modifications et OK.
38. Sous VLAN, sélectionnez iSCSI-A-VLAN, NFS et VLAN natif. Définissez le VLAN natif comme VLAN natif. Effacez la sélection VLAN par défaut.
39. Cliquez sur Enregistrer les modifications et sur OK.



40. Sélectionnez Appliance interface 1/4 sous Fabric A.
41. Dans le champ libellé utilisateur, indiquez les informations indiquant le port du contrôleur de stockage, par exemple `<storage_controller_02_name>:e0e`. Cliquez sur Enregistrer les modifications et sur OK.
42. Sélectionnez la stratégie de contrôle réseau Activer_CDP, puis sélectionnez Enregistrer les modifications et OK.
43. Sous VLAN, sélectionnez iSCSI-A-VLAN, NFS et VLAN natif.
44. Définissez le VLAN natif comme VLAN natif.
45. Effacez la sélection VLAN par défaut.
46. Cliquez sur Enregistrer les modifications et sur OK.
47. Dans le volet de navigation, sous LAN > Appliances Cloud, développez l’arborescence Fabric B.
48. Développez interfaces.
49. Sélectionnez interface de l’appareil 1/3.
50. Dans le champ libellé utilisateur, indiquez les informations indiquant le port du contrôleur de stockage, par exemple `<storage_controller_01_name>:e0f`. Cliquez sur Enregistrer les modifications et sur OK.
51. Sélectionnez la stratégie de contrôle réseau Activer_CDP, puis sélectionnez Enregistrer les modifications et OK.
52. Sous VLAN, sélectionnez iSCSI-B-VLAN, NFS et VLAN natif. Définissez le VLAN natif comme VLAN natif. Désélectionnez le VLAN par défaut.

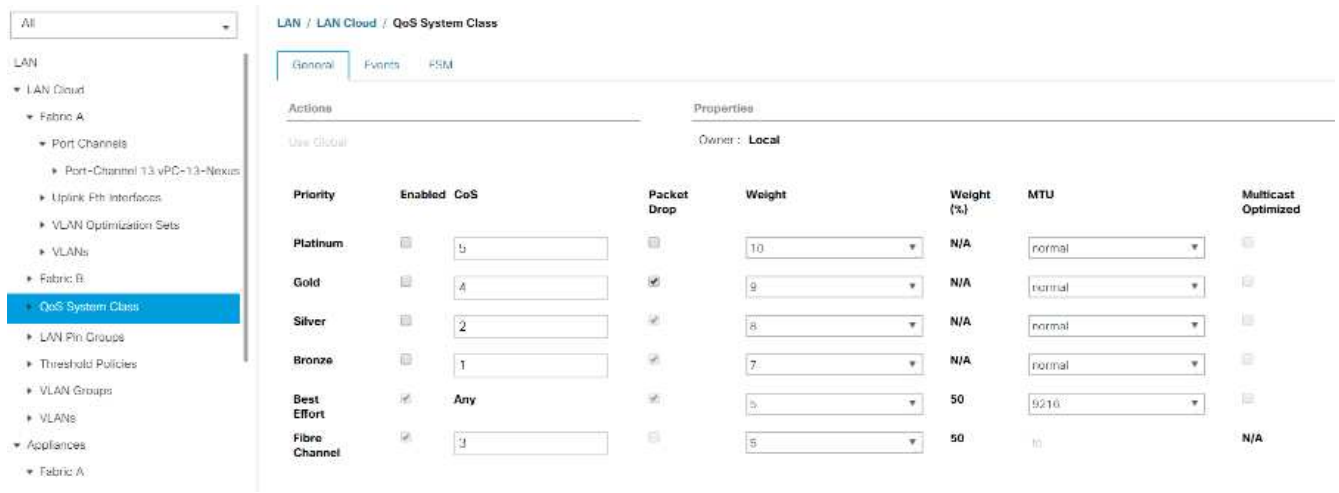


53. Cliquez sur Enregistrer les modifications et sur OK.
54. Sélectionnez Appliance interface 1/4 sous Fabric B.
55. Dans le champ libellé utilisateur, indiquez les informations indiquant le port du contrôleur de stockage, par exemple `<storage_controller_02_name>:e0f`. Cliquez sur Enregistrer les modifications et sur OK.
56. Sélectionnez la stratégie de contrôle réseau Activer_CDP, puis sélectionnez Enregistrer les modifications et OK.
57. Sous VLAN, sélectionnez iSCSI-B-VLAN, NFS et VLAN natif. Définissez le VLAN natif comme VLAN natif. Désélectionnez le VLAN par défaut.
58. Cliquez sur Enregistrer les modifications et sur OK.

Définissez des trames Jumbo dans la structure Cisco UCS

Pour configurer des trames Jumbo et permettre la qualité de service sur la structure Cisco UCS, effectuez les opérations suivantes :

1. Dans Cisco UCS Manager, dans le volet de navigation, cliquez sur l'onglet LAN.
2. Sélectionnez LAN > LAN Cloud > QoS System Class.
3. Dans le volet de droite, cliquez sur l'onglet général.
4. Sur la ligne meilleur effort, entrez 9216 dans la zone sous la colonne MTU.



5. Cliquez sur Save Changes.
6. Cliquez sur OK.

Châssis Cisco UCS

Pour accuser réception de tous les châssis Cisco UCS, procédez comme suit :

1. Dans Cisco UCS Manager, sélectionnez l'onglet Equipment, puis développez l'onglet Equipment à droite.
2. Développez Equipement > châssis.
3. Dans actions pour le châssis 1, sélectionnez accuser réception du châssis.
4. Cliquez sur OK, puis sur OK pour terminer la reconnaissance du châssis.
5. Cliquez sur Fermer pour fermer la fenêtre Propriétés.

Charger les images du firmware Cisco UCS 4.0(1b)

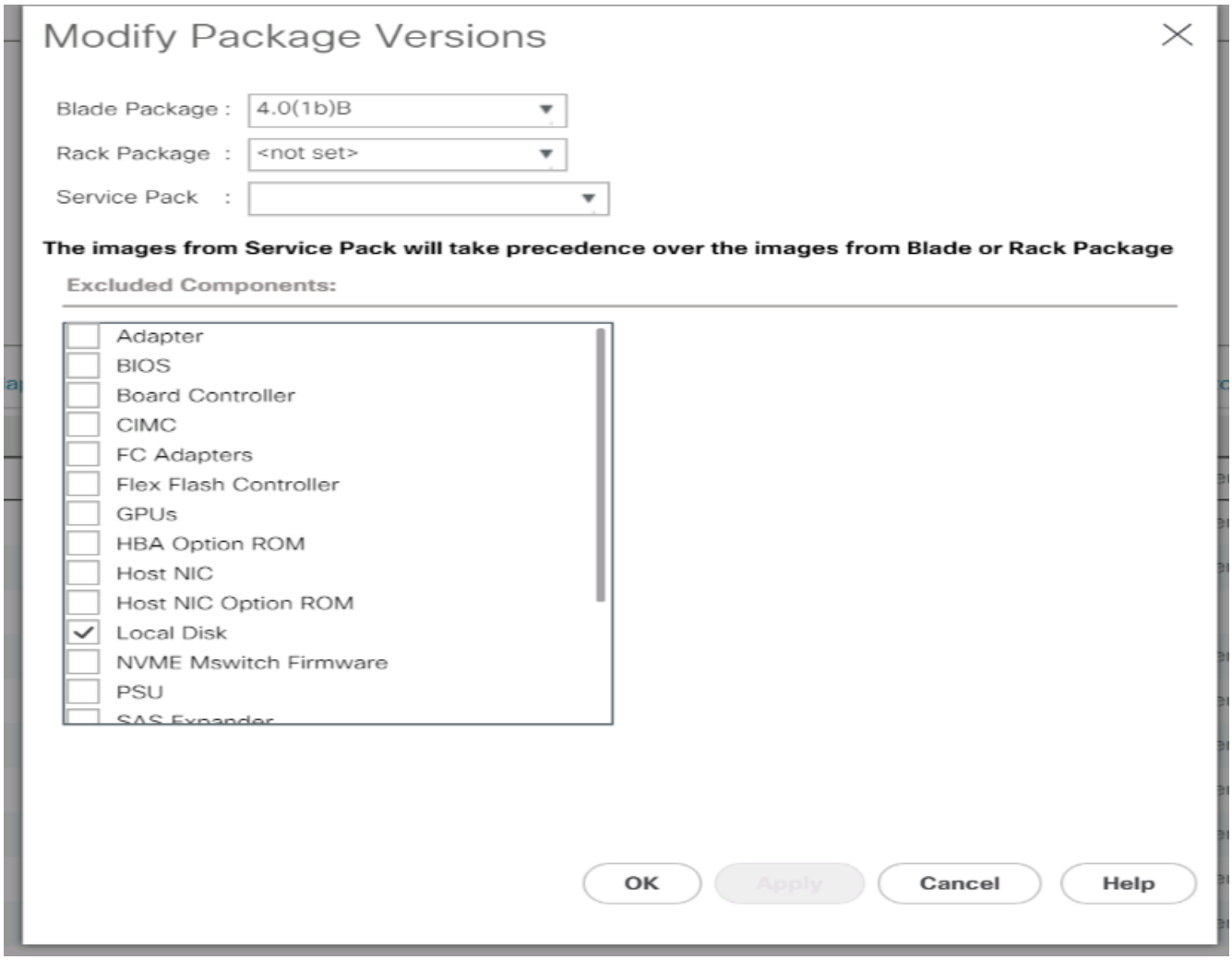
Pour mettre à niveau le logiciel Cisco UCS Manager et le logiciel Cisco UCS Fabric Interconnect vers la version 4.0(1b), reportez-vous à "Guides d'installation et de mise à niveau de Cisco UCS Manager".

Création du package de firmware hôte

Les stratégies de gestion du micrologiciel permettent à l'administrateur de sélectionner les packages correspondants pour une configuration de serveur donnée. Ces politiques incluent souvent des packages pour adaptateur, BIOS, contrôleur de carte, adaptateurs FC, carte de bus hôte (HBA) option ROM et les propriétés du contrôleur de stockage.

Pour créer une stratégie de gestion du firmware pour une configuration de serveur donnée dans l'environnement Cisco UCS, procédez comme suit :

1. Dans Cisco UCS Manager, cliquez sur serveurs sur la gauche.
2. Sélectionnez stratégies > racine.
3. Développez packages de microprogramme hôte.
4. Sélectionnez par défaut.
5. Dans le volet actions, sélectionnez Modifier les versions du package.
6. Sélectionnez la version 4.0(1b) pour les deux ensembles lames.



7. Cliquez sur OK, puis de nouveau sur OK pour modifier le progiciel du micrologiciel hôte.

Créez des pools d'adresses MAC

Pour configurer les pools d'adresses MAC nécessaires pour l'environnement Cisco UCS, procédez comme suit :

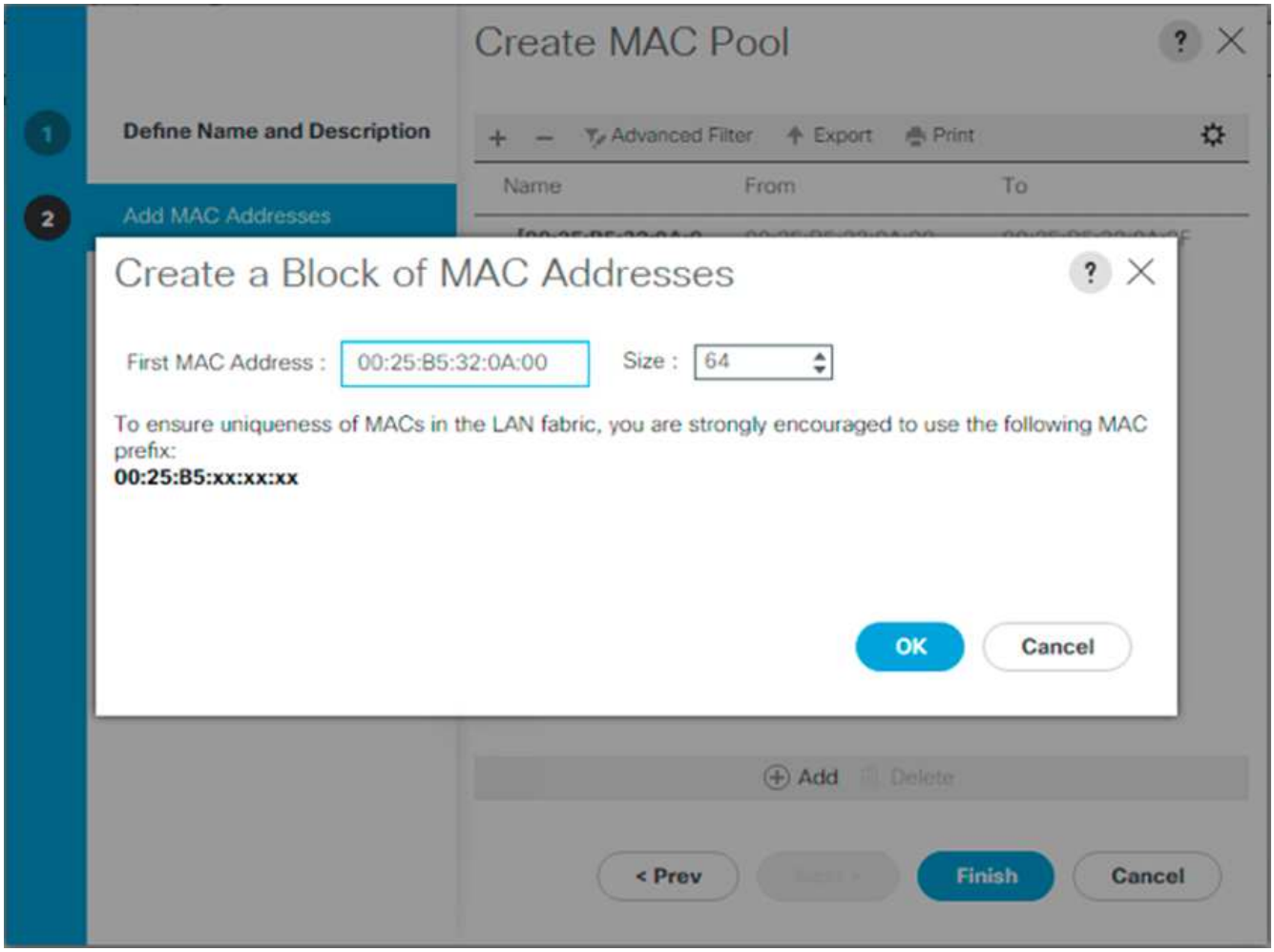
1. Dans Cisco UCS Manager, cliquez sur LAN sur la gauche.
2. Sélectionnez pools > racine.

   Dans cette procédure, deux pools d'adresses MAC sont créés, un pour chaque structure de commutation.

3. Cliquez avec le bouton droit de la souris sur pools MAC sous l'organisation racine.
4. Sélectionnez Créer un pool MAC pour créer le pool d'adresses MAC.
5. Saisissez MAC-Pool-A comme nom du pool MAC.
6. Facultatif : saisissez une description pour le pool MAC.
7. Sélectionnez Sequential comme option pour l'ordre d'affectation. Cliquez sur Suivant.
8. Cliquez sur Ajouter.
9. Spécifiez une adresse MAC de départ.

> Pour la solution FlexPod, il est recommandé de placer le port 0A sur le dernier octet de l'adresse MAC de départ pour identifier toutes les adresses MAC en tant qu'adresses de structure A. Dans notre exemple, nous avons présenté l'exemple de l'intégration des informations de numéro de domaine Cisco UCS qui nous donnent 00:25:B5:32:0A:00 comme première adresse MAC.

10. Spécifiez une taille suffisante pour le pool d'adresses MAC afin de prendre en charge les ressources serveur ou serveur lame disponibles. Cliquez sur OK.



11. Cliquez sur Terminer.
12. Dans le message de confirmation, cliquez sur OK.
13. Cliquez avec le bouton droit de la souris sur pools MAC sous l'organisation racine.
14. Sélectionnez Créer un pool MAC pour créer le pool d'adresses MAC.
15. Saisissez MAC-Pool-B comme nom du pool MAC.
16. Facultatif : saisissez une description pour le pool MAC.
17. Sélectionnez Sequential comme option pour l'ordre d'affectation. Cliquez sur Suivant.
18. Cliquez sur Ajouter.
19. Spécifiez une adresse MAC de départ.

> Pour la solution FlexPod, il est recommandé de placer 0B à côté du dernier octet de l'adresse MAC de départ pour identifier toutes les adresses MAC de ce pool comme adresses de structure B. Encore une fois, nous avons présenté notre exemple d'intégration des informations de numéro de domaine Cisco UCS qui nous donnent la priorité à notre première adresse MAC 00:25:B5:32:0B:00.

20. Spécifiez une taille suffisante pour le pool d'adresses MAC afin de prendre en charge les ressources serveur ou serveur lame disponibles. Cliquez sur OK.
21. Cliquez sur Terminer.
22. Dans le message de confirmation, cliquez sur OK.

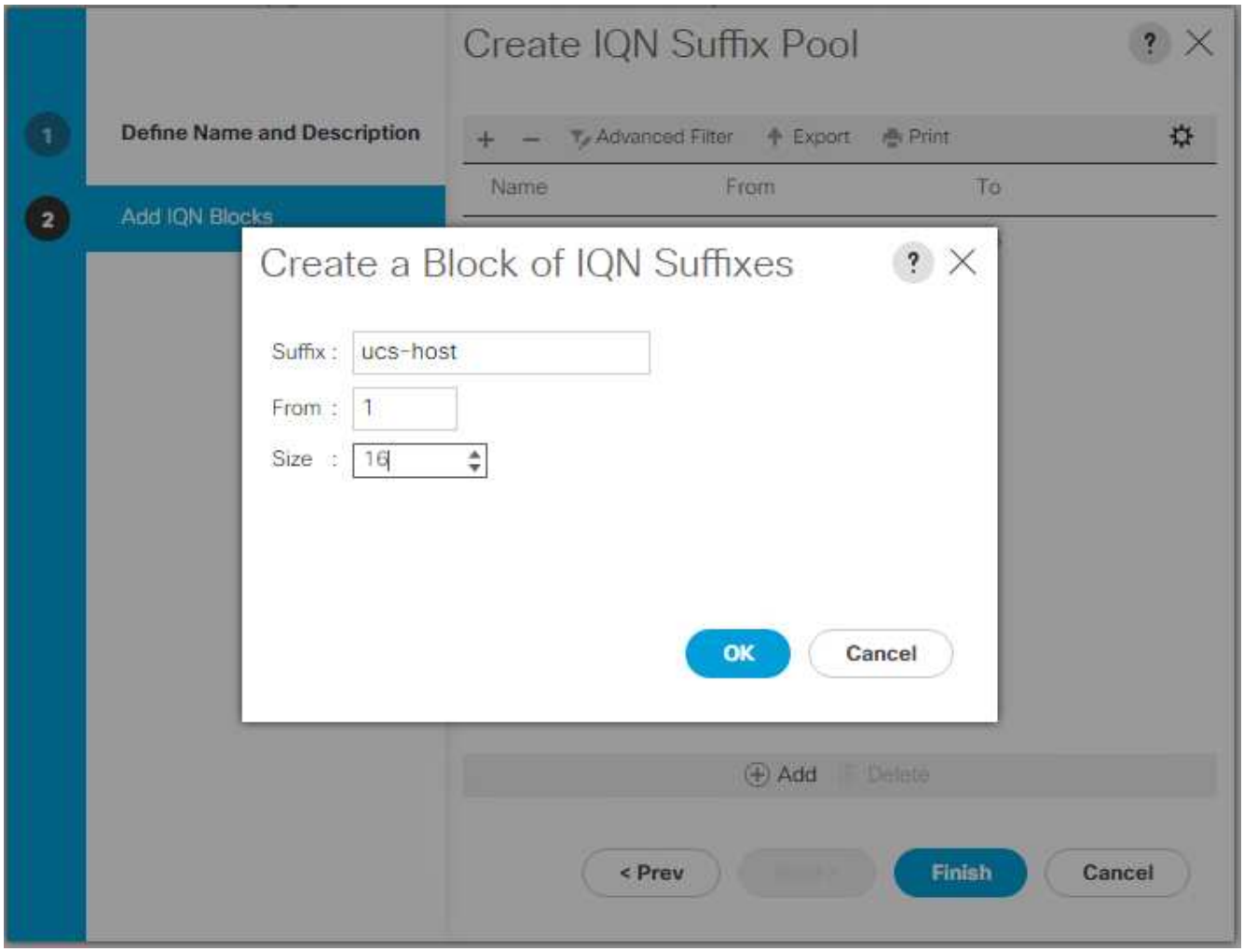
Créez le pool IQN iSCSI

Pour configurer les pools IQN nécessaires pour l'environnement Cisco UCS, procédez comme suit :

1. Dans Cisco UCS Manager, cliquez sur SAN sur la gauche.
2. Sélectionnez pools > racine.
3. Cliquez avec le bouton droit de la souris sur pools IQN.
4. Sélectionnez Créer un pool de suffixe IQN pour créer le pool IQN.
5. Entrez IQN-Pool pour le nom du pool IQN.
6. Facultatif : saisissez une description pour le pool IQN.
7. Entrez `iqn.1992-08.com.cisco` comme préfixe.
8. Sélectionnez Sequential pour l'ordre d'affectation. Cliquez sur Suivant.
9. Cliquez sur Ajouter.
10. Entrez `ucs-host` comme suffixe.

> Si plusieurs domaines Cisco UCS sont utilisés, il peut être nécessaire d'utiliser un suffixe IQN plus spécifique.

11. Entrez 1 dans le champ de.
12. Spécifiez la taille du bloc IQN suffisante pour prendre en charge les ressources serveur disponibles. Cliquez sur OK.



13. Cliquez sur Terminer.

Créer des pools d'adresses IP d'initiateur iSCSI

Pour configurer le démarrage iSCSI des pools IP nécessaires pour l'environnement Cisco UCS, effectuez les opérations suivantes :

1. Dans Cisco UCS Manager, cliquez sur LAN sur la gauche.
2. Sélectionnez pools > racine.
3. Cliquez avec le bouton droit de la souris sur pools IP.
4. Sélectionnez Créer un pool IP.
5. Entrez iSCSI-IP-Pool-A comme nom de pool IP.
6. Facultatif : saisissez une description pour le pool IP.
7. Sélectionnez Sequential pour l'ordre d'affectation. Cliquez sur Suivant.
8. Cliquez sur Ajouter pour ajouter un bloc d'adresse IP.
9. Dans le champ de, entrez le début de la plage à attribuer en tant qu'adresses IP iSCSI.
10. Définissez la taille sur un nombre suffisant d'adresses pour accueillir les serveurs. Cliquez sur OK.
11. Cliquez sur Suivant.
12. Cliquez sur Terminer.

13. Cliquez avec le bouton droit de la souris sur pools IP.
14. Sélectionnez Créer un pool IP.
15. Saisissez iSCSI-IP-Pool-B comme nom de pool IP.
16. Facultatif : saisissez une description pour le pool IP.
17. Sélectionnez Sequential pour l'ordre d'affectation. Cliquez sur Suivant.
18. Cliquez sur Ajouter pour ajouter un bloc d'adresse IP.
19. Dans le champ de, entrez le début de la plage à attribuer en tant qu'adresses IP iSCSI.
20. Définissez la taille sur un nombre suffisant d'adresses pour accueillir les serveurs. Cliquez sur OK.
21. Cliquez sur Suivant.
22. Cliquez sur Terminer.

Créer le pool de suffixe UUID

Pour configurer le pool de suffixe UUID (universellement unique identifier) nécessaire pour l'environnement Cisco UCS, procédez comme suit :

1. Dans Cisco UCS Manager, cliquez sur serveurs sur la gauche.
2. Sélectionnez pools > racine.
3. Cliquez avec le bouton droit de la souris sur pools de suffixe UUID.
4. Sélectionnez Créer un pool de suffixe UUID.
5. Indiquez UUID-Pool comme nom du pool de suffixe UUID.
6. Facultatif : saisissez une description pour le pool de suffixe UUID.
7. Conservez le préfixe à l'option dérivée.
8. Sélectionnez séquentiel pour l'ordre d'affectation.
9. Cliquez sur Suivant.
10. Cliquez sur Ajouter pour ajouter un bloc d'UUID.
11. Conservez le champ de sur le paramètre par défaut.
12. Spécifiez la taille du bloc UUID qui est suffisant pour prendre en charge les ressources serveur ou serveur lame disponibles. Cliquez sur OK.
13. Cliquez sur Terminer.
14. Cliquez sur OK.

Création d'un pool de serveurs

Pour configurer le pool de serveurs nécessaire pour l'environnement Cisco UCS, procédez comme suit :

> Envisagez de créer des pools de serveurs uniques pour atteindre la granularité requise dans votre environnement.

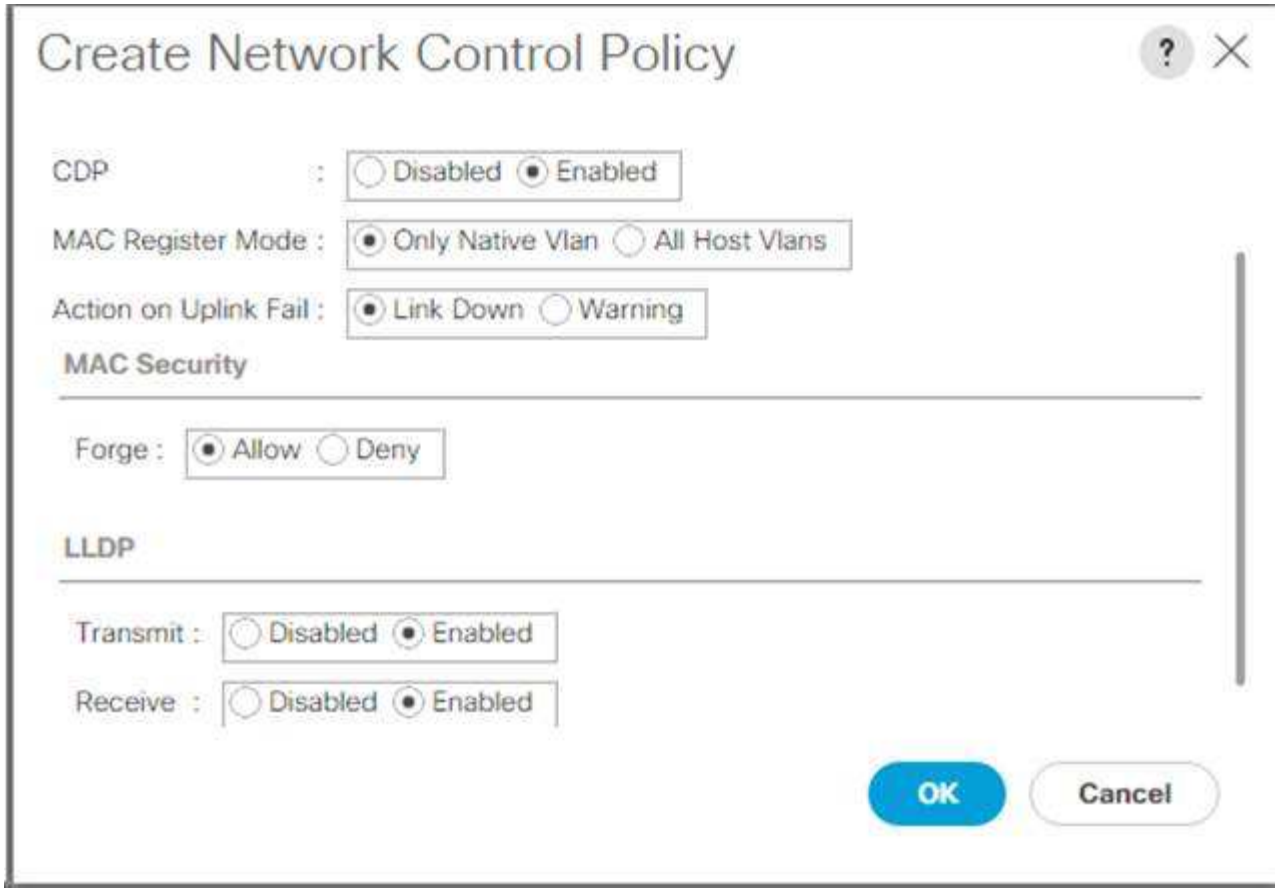
1. Dans Cisco UCS Manager, cliquez sur serveurs sur la gauche.
2. Sélectionnez pools > racine.
3. Cliquez avec le bouton droit de la souris sur pools de serveurs.

4. Sélectionnez Créer un pool de serveurs.
5. Entrez `Infra-Pool `comme nom du pool de serveurs.
6. Facultatif : saisissez une description pour le pool de serveurs. Cliquez sur Suivant.
7. Sélectionnez deux (ou plusieurs) serveurs à utiliser pour le cluster de gestion VMware et cliquez sur >> pour les ajouter au pool `serveur `Infra-Pool `.
8. Cliquez sur Terminer.
9. Cliquez sur OK.

Créez une stratégie de contrôle réseau pour le Cisco Discovery Protocol et le Link Layer Discovery Protocol

Pour créer une stratégie de contrôle réseau pour le protocole CDP (Cisco Discovery Protocol) et le protocole LLDP (Link Layer Discovery Protocol), procédez comme suit :

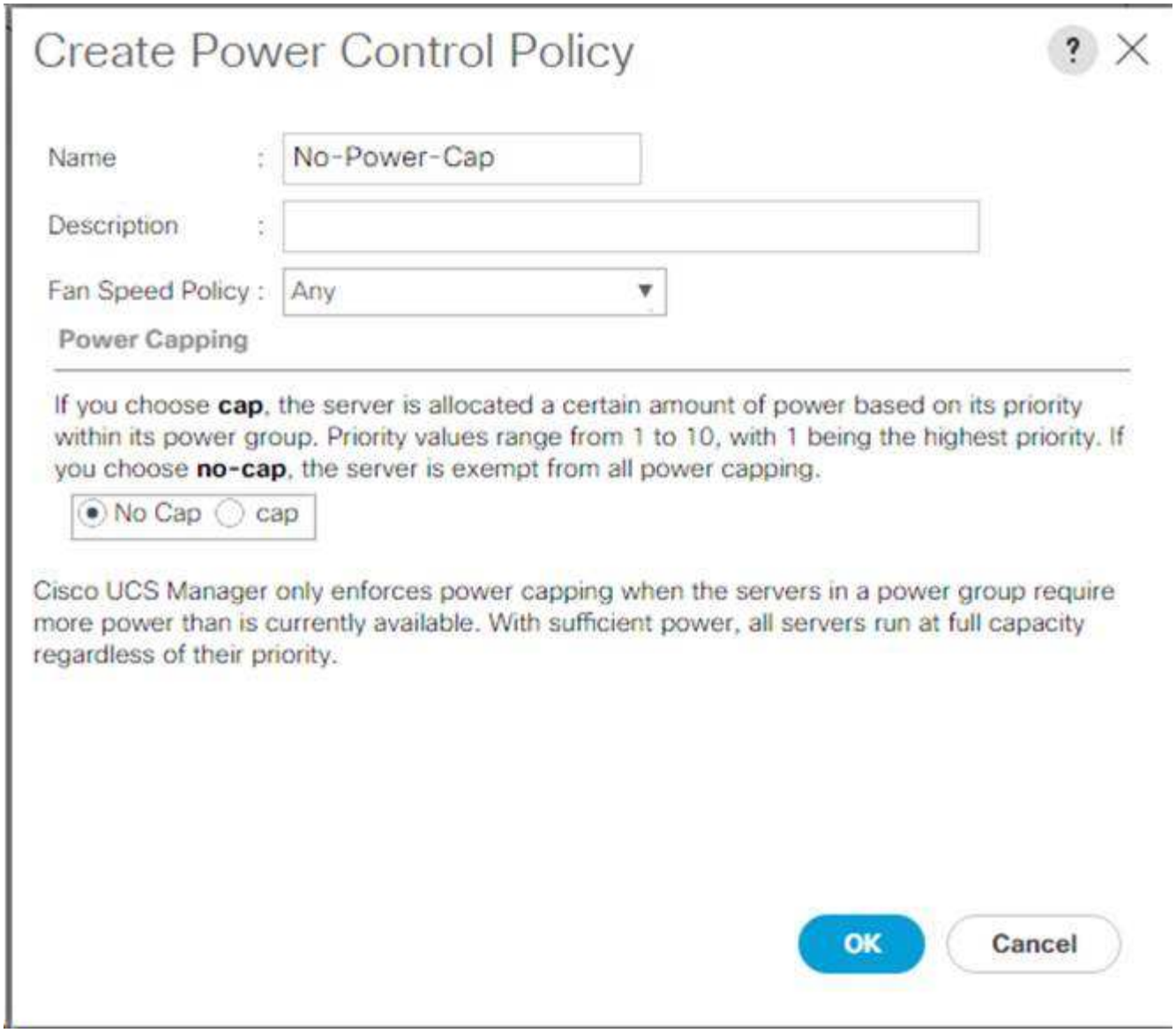
1. Dans Cisco UCS Manager, cliquez sur LAN sur la gauche.
2. Sélectionnez stratégies > racine.
3. Cliquez avec le bouton droit de la souris sur stratégies de contrôle du réseau.
4. Sélectionnez Créer une stratégie de contrôle réseau.
5. Entrez le nom de la stratégie Enable-CDP-LLDP.
6. Sous CDP, sélectionnez l'option Enabled.
7. Pour le mode LLDP, faites défiler l'écran vers le bas et sélectionnez activé pour la transmission et la réception.
8. Cliquez sur OK pour créer la stratégie de contrôle du réseau. Cliquez sur OK.



Créer une stratégie de contrôle de l'alimentation

Pour créer une stratégie de contrôle de l'alimentation pour l'environnement Cisco UCS, procédez comme suit :

1. Dans Cisco UCS Manager, cliquez sur l'onglet serveurs sur la gauche.
2. Sélectionnez stratégies > racine.
3. Cliquez avec le bouton droit sur stratégies de contrôle de l'alimentation.
4. Sélectionnez Créer une stratégie de contrôle de l'alimentation.
5. Entrez No-Power-Cap comme nom de la stratégie de contrôle de l'alimentation.
6. Définissez le paramètre de plafonnement de l'alimentation sur No Cap.
7. Cliquez sur OK pour créer la stratégie de contrôle de l'alimentation. Cliquez sur OK.



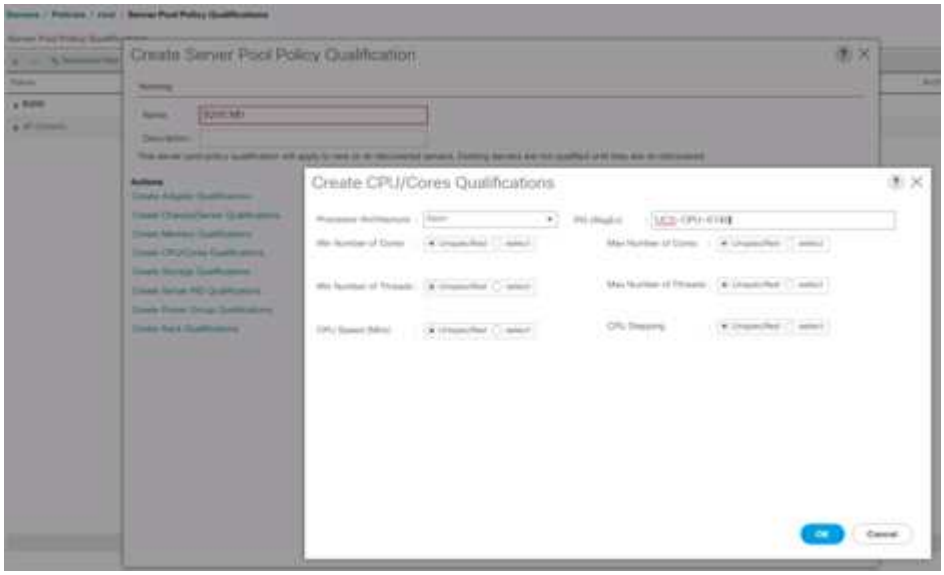
Créer une stratégie de qualification de pool de serveurs (facultatif)

Pour créer une stratégie facultative de qualification de pool de serveurs pour l'environnement Cisco UCS, effectuez les opérations suivantes :

> Cet exemple crée une règle pour les serveurs Cisco UCS B-Series dotés des processeurs Intel E2660 v4 Xeon Broadwell.

1. Dans Cisco UCS Manager, cliquez sur serveurs sur la gauche.
2. Sélectionnez stratégies > racine.
3. Sélectionnez qualifications de stratégie de pool de serveurs.
4. Sélectionnez Créer une qualification de stratégie de pool de serveurs ou Ajouter.
5. Nommez la stratégie Intel.
6. Sélectionnez Créer qualifications UC/noyaux.
7. Sélectionnez Xeon pour le processeur/l'architecture.

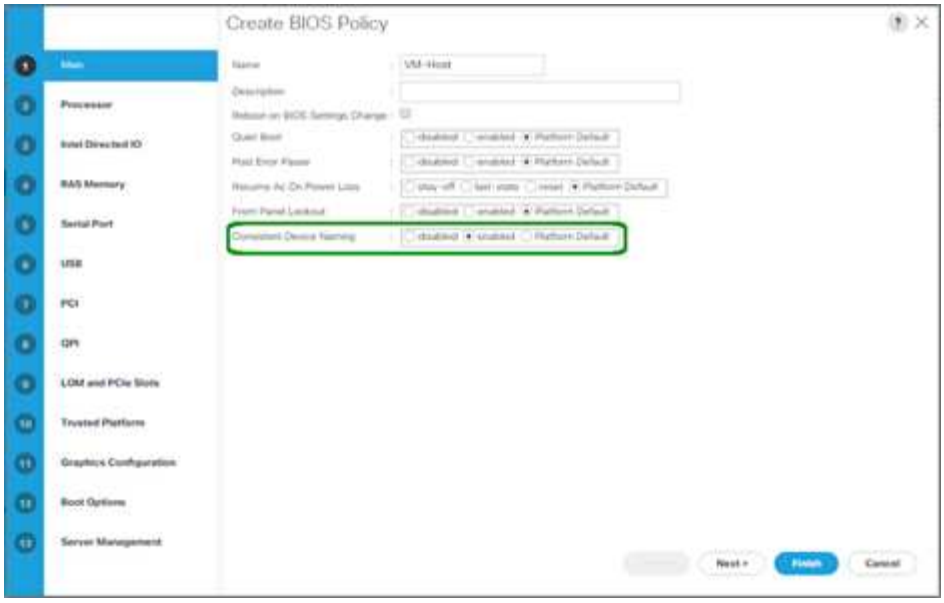
8. Entrez `<UCS-CPU- PID>` Comme ID de processus (PID).
9. Cliquez sur OK pour créer la qualification CPU/cœur.
10. Cliquez sur OK pour créer la stratégie, puis cliquez sur OK pour confirmer.



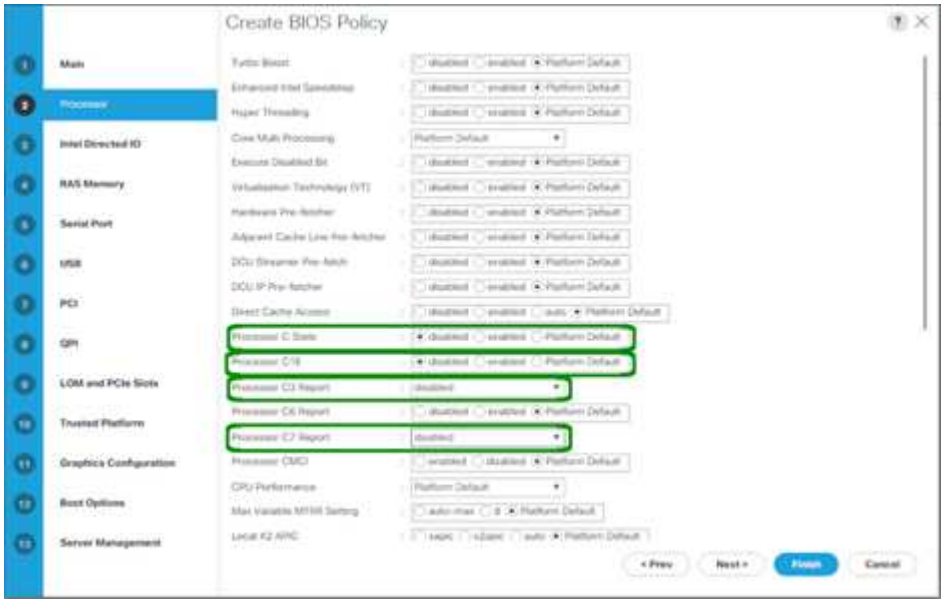
Créer une stratégie BIOS du serveur

Pour créer une stratégie de BIOS des serveurs pour l'environnement Cisco UCS, effectuez les opérations suivantes :

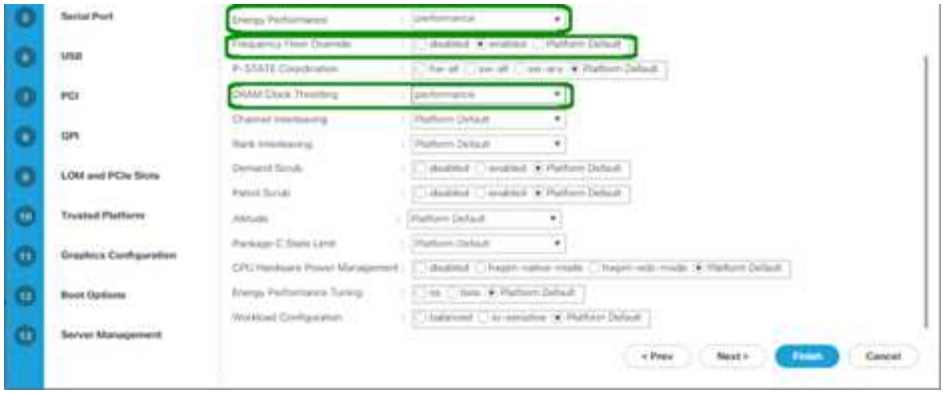
1. Dans Cisco UCS Manager, cliquez sur serveurs sur la gauche.
2. Sélectionnez stratégies > racine.
3. Cliquez avec le bouton droit de la souris sur stratégies BIOS.
4. Sélectionnez Créer une stratégie de BIOS.
5. Saisissez VM-Host comme nom de stratégie BIOS.
6. Définissez le paramètre de démarrage silencieux sur Désactivé.
7. Définissez le nom de périphérique cohérent sur activé.



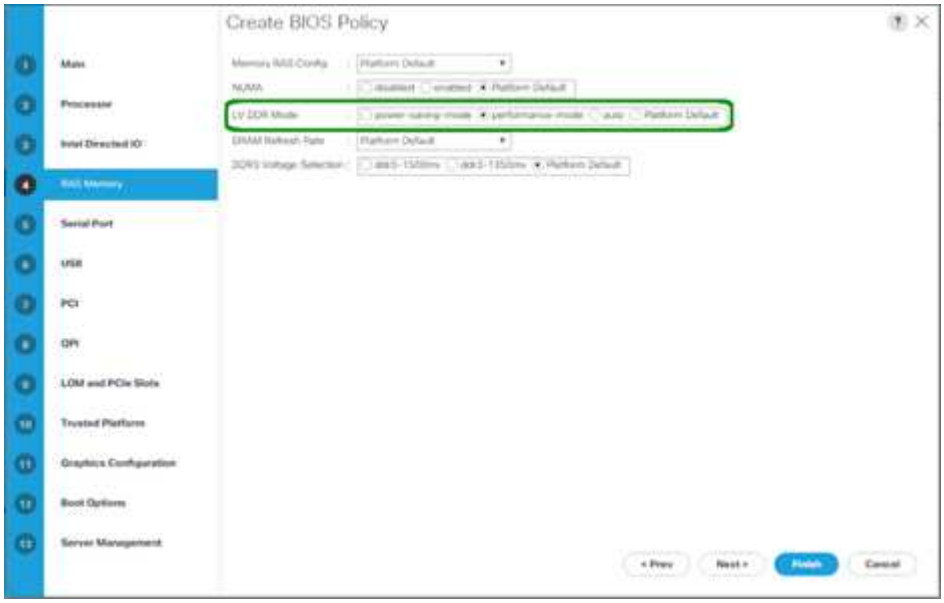
8. Sélectionnez l’onglet processeur et définissez les paramètres suivants :
    - État du processeur C : désactivé
    - Processeur C1E : désactivé
    - Rapport C3 du processeur : désactivé
    - Rapport C7 processeur : désactivé



9. Faites défiler jusqu’aux options de processeur restantes et définissez les paramètres suivants :
    - Performance énergétique : performances
    - Remplacement de l’étage de fréquence : activé
    - Régulation de l’horloge DRAM : performance



10. Cliquez sur mémoire RAS et définissez les paramètres suivants :
    - Mode DDR LV : mode performance

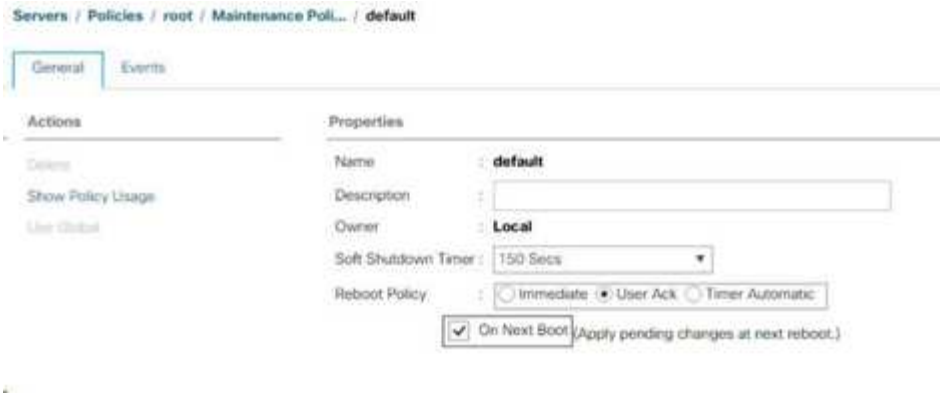


11. Cliquez sur Terminer pour créer la stratégie de BIOS.
12. Cliquez sur OK.

Mettez à jour la stratégie de maintenance par défaut

Pour mettre à jour la stratégie de maintenance par défaut, procédez comme suit :

1. Dans Cisco UCS Manager, cliquez sur serveurs sur la gauche.
2. Sélectionnez stratégies > racine.
3. Sélectionnez Maintenance Policies > Default.
4. Définissez la stratégie de redémarrage sur User Ack.
5. Sélectionnez démarrage suivant pour déléguer les fenêtres de maintenance aux administrateurs de serveur.



6. Cliquez sur Save Changes.
7. Cliquez sur OK pour accepter la modification.

Créer des modèles vNIC

Pour créer plusieurs modèles de cartes réseau virtuelles (vNIC) pour l'environnement Cisco UCS, suivez les procédures décrites dans cette section.

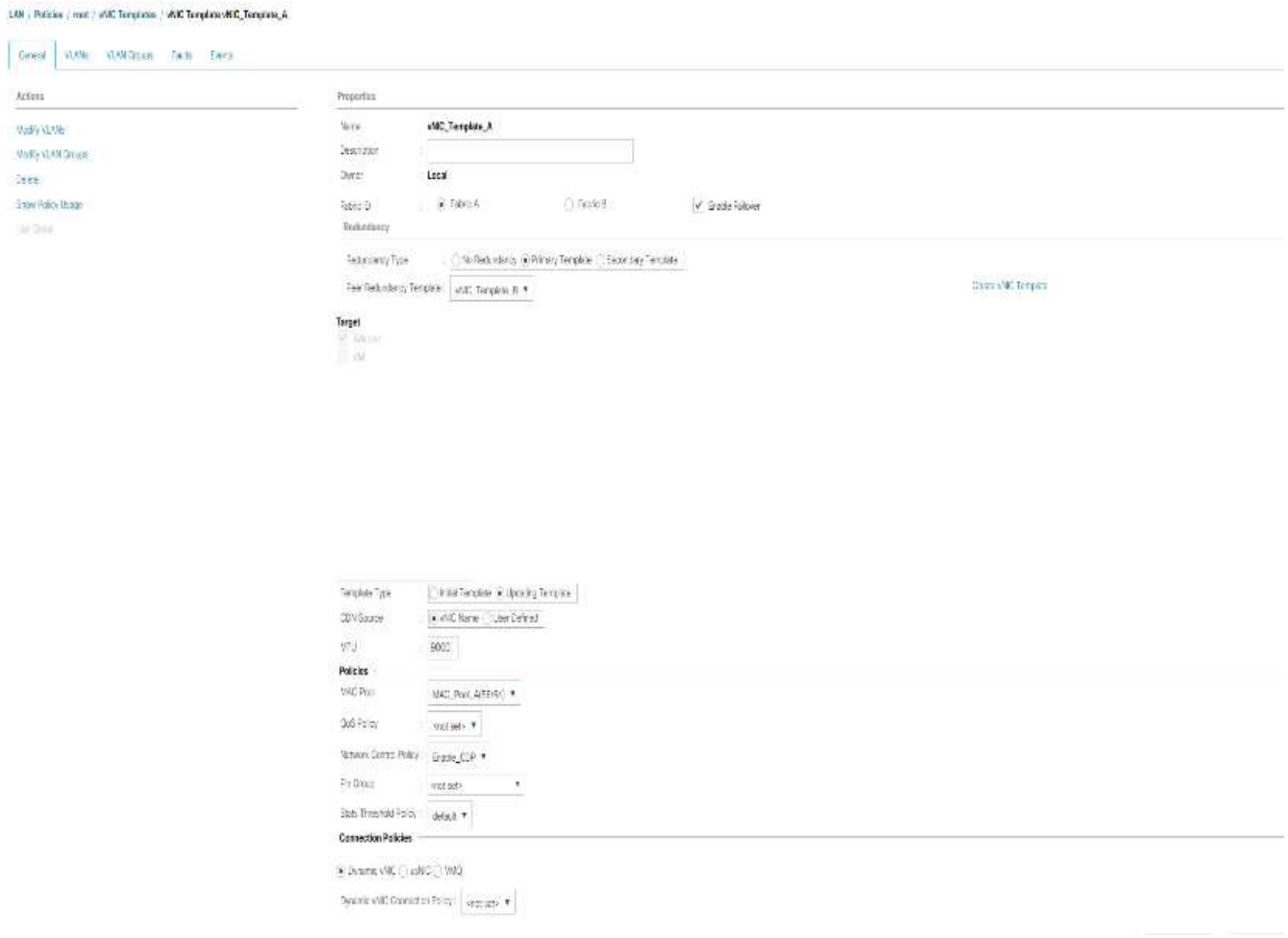
> Quatre modèles vNIC au total sont créés.

Créer des vNIC d'infrastructure

Pour créer une vNIC d'infrastructure, procédez comme suit :

1. Dans Cisco UCS Manager, cliquez sur LAN sur la gauche.
2. Sélectionnez stratégies > racine.
3. Cliquez avec le bouton droit de la souris sur modèles vNIC.
4. Sélectionnez Créer un modèle vNIC.
5. Entrez `Site-XX-vNIC_A` Comme nom de modèle vNIC.
6. Sélectionnez mettre à jour le modèle comme type de modèle.
7. Pour l'ID de structure, sélectionnez Fabric A.
8. Assurez-vous que l'option Activer le basculement n'est pas sélectionnée.
9. Sélectionnez modèle principal pour Type de redondance.
10. Laissez le modèle de redondance par pair défini sur `<not set>`.
11. Sous cible, assurez-vous que seule l'option carte est sélectionnée.
12. Réglez `Native-VLAN` En tant que VLAN natif.
13. Sélectionnez Nom vNIC pour la source CDN.
14. Pour MTU, saisissez 9000.
15. Sous VLAN autorisés, sélectionnez `Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic`, Et site-XX-vMotion. Utilisez la touche Ctrl pour effectuer cette sélection multiple.
16. Cliquez sur Sélectionner. Ces VLAN doivent maintenant apparaître sous certains VLAN.
17. Dans la liste Pool MAC, sélectionnez `MAC_Pool_A`.

18. Dans la liste Stratégie de contrôle du réseau, sélectionnez Pool-A.
19. Dans la liste Stratégie de contrôle du réseau, sélectionnez Activer-CDP-LLDP.
20. Cliquez sur OK pour créer le modèle vNIC.
21. Cliquez sur OK.

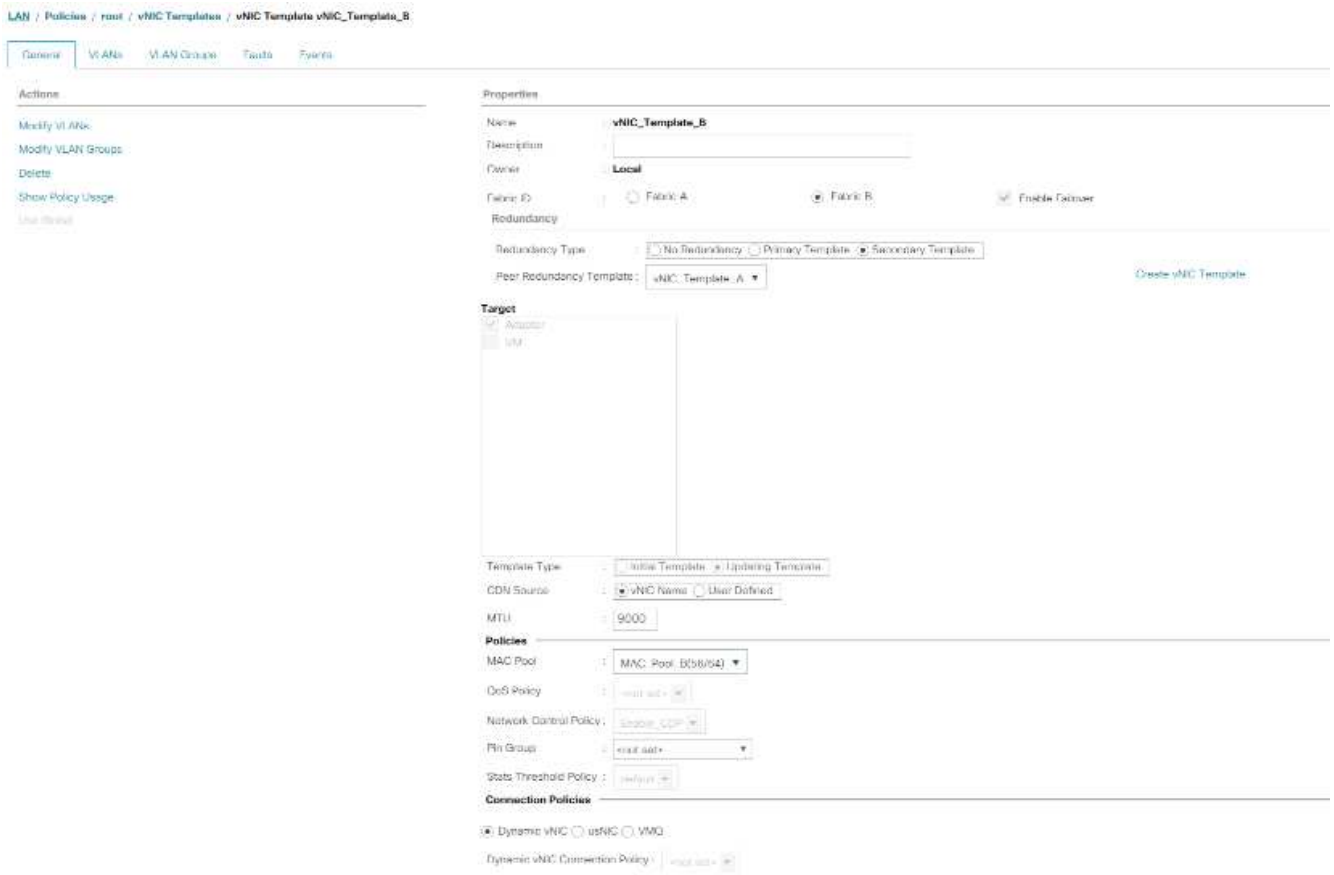


Pour créer le modèle de redondance secondaire Infra-B, procédez comme suit :

1. Dans Cisco UCS Manager, cliquez sur LAN sur la gauche.
2. Sélectionnez stratégies > racine.
3. Cliquez avec le bouton droit de la souris sur modèles vNIC.
4. Sélectionnez Créer un modèle vNIC.
5. Entrez `Site-XX-vNIC_B `comme nom de modèle vNIC.
6. Sélectionnez mettre à jour le modèle comme type de modèle.
7. Pour l'ID de structure, sélectionnez Fabric B.
8. Sélectionnez l'option Activer le basculement.

> La sélection du basculement est une étape essentielle pour améliorer le temps de basculement de liaison en le gérant au niveau matériel et pour éviter tout risque de défaillance de carte réseau non détectée par le commutateur virtuel.

9. Sélectionnez modèle principal pour Type de redondance.
10. Laissez le modèle de redondance par pair défini sur `vNIC_Template_A`.
11. Sous cible, assurez-vous que seule l'option carte est sélectionnée.
12. Réglez `Native-VLAN` En tant que VLAN natif.
13. Sélectionnez Nom vNIC pour la source CDN.
14. Pour MTU, entrez `9000`.
15. Sous VLAN autorisés, sélectionnez `Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic`, Et site-XX-vMotion. Utilisez la touche Ctrl pour effectuer cette sélection multiple.
16. Cliquez sur Sélectionner. Ces VLAN doivent maintenant apparaître sous certains VLAN.
17. Dans la liste Pool MAC, sélectionnez `MAC_Pool_B`.
18. Dans la liste Stratégie de contrôle réseau, sélectionnez Pool-B.
19. Dans la liste Stratégie de contrôle du réseau, sélectionnez Activer-CDP-LLDP.
20. Cliquez sur OK pour créer le modèle vNIC.
21. Cliquez sur OK.

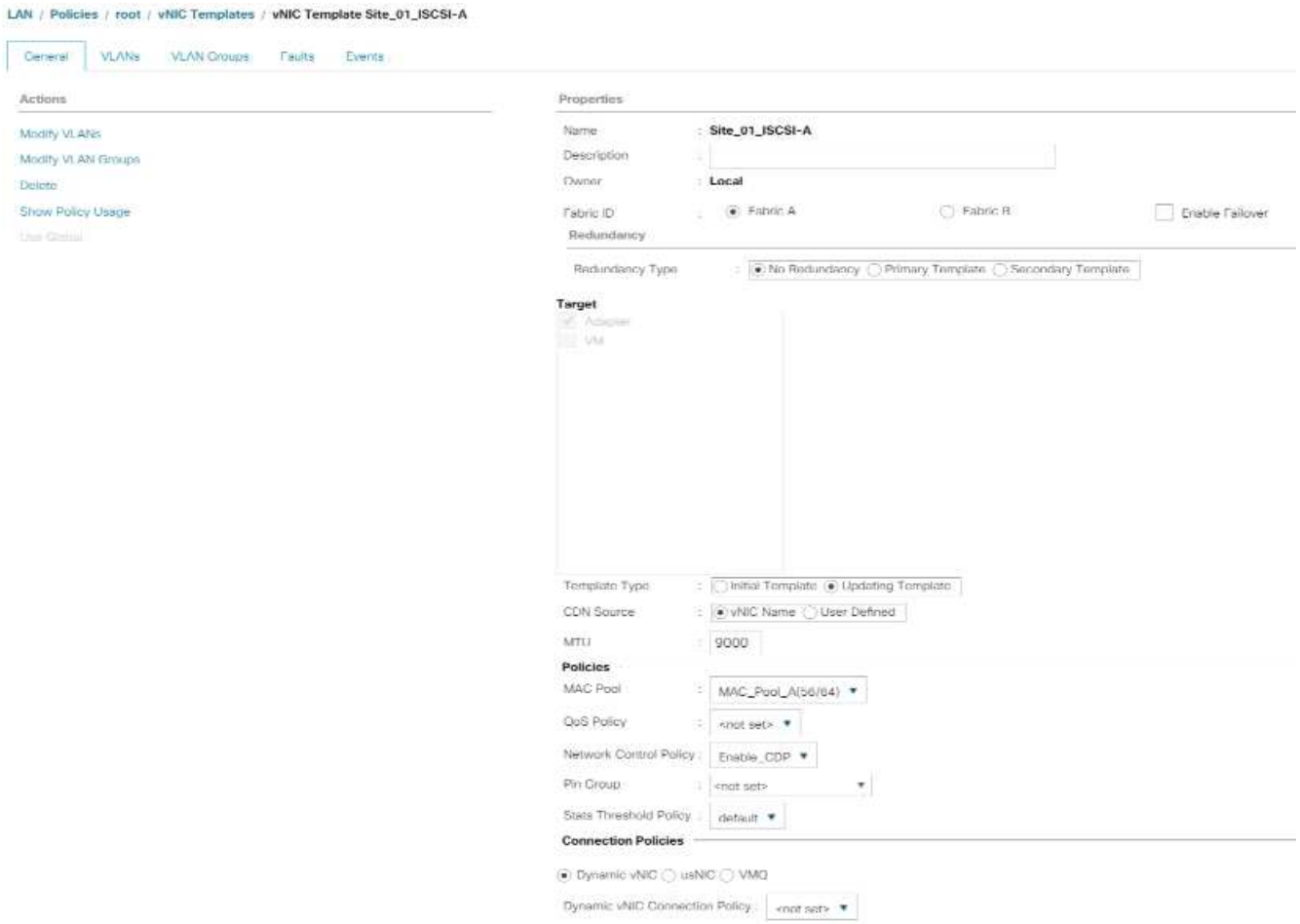


Créez des vNIC iSCSI

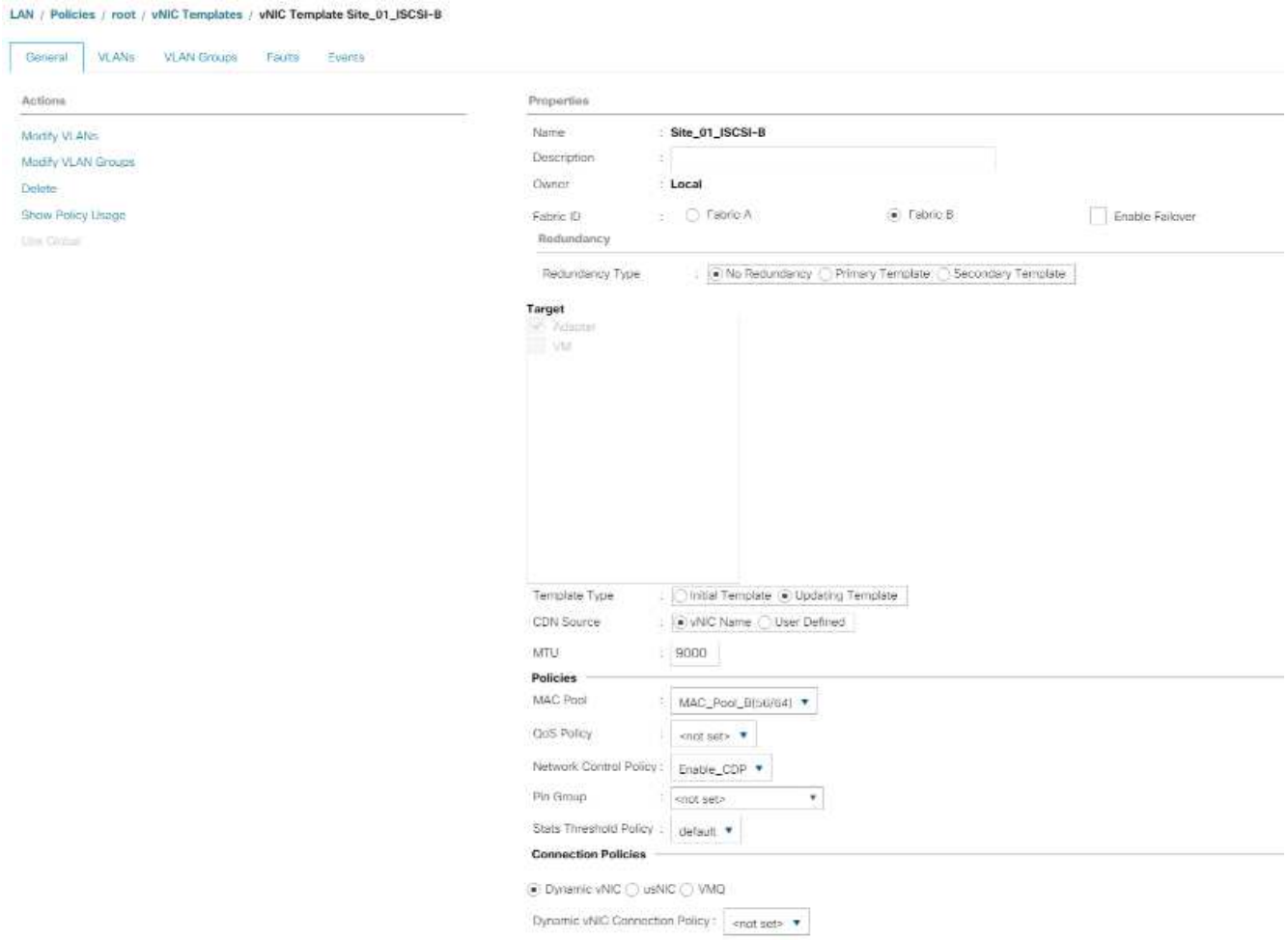
Pour créer des vNIC iSCSI, procédez comme suit :

1. Sélectionnez LAN sur la gauche.

2. Sélectionnez stratégies > racine.
3. Cliquez avec le bouton droit de la souris sur modèles vNIC.
4. Sélectionnez Créer un modèle vNIC.
5. Entrez `Site- 01-iSCSI_A` Comme nom de modèle vNIC.
6. Sélectionnez structure A. Ne sélectionnez pas l'option Activer le basculement.
7. Laissez le type de redondance défini sur sans redondance.
8. Sous cible, assurez-vous que seule l'option carte est sélectionnée.
9. Sélectionnez mise à jour du modèle pour le type de modèle.
10. Sous VLAN, sélectionnez uniquement site- 01-iSCSI_A_VLAN.
11. Sélectionnez site- 01-iSCSI_A_VLAN comme VLAN natif.
12. Laissez le nom vNIC défini pour la source CDN.
13. Sous MTU, saisissez 9000.
14. Dans la liste Pool MAC, sélectionnez MAC-Pool-A.
15. Dans la liste Stratégie de contrôle du réseau, sélectionnez Activer-CDP-LLDP.
16. Cliquez sur OK pour terminer la création du modèle vNIC.
17. Cliquez sur OK.



18. Sélectionnez LAN sur la gauche.
19. Sélectionnez stratégies > racine.
20. Cliquez avec le bouton droit de la souris sur modèles vNIC.
21. Sélectionnez Créer un modèle vNIC.
22. Entrez `Site- 01-iSCSI_B` Comme nom de modèle vNIC.
23. Sélectionnez structure B. Ne sélectionnez pas l'option Activer le basculement.
24. Laissez le type de redondance défini sur sans redondance.
25. Sous cible, assurez-vous que seule l'option carte est sélectionnée.
26. Sélectionnez mise à jour du modèle pour le type de modèle.
27. Sous VLAN, sélectionnez uniquement `Site- 01-iSCSI_B_VLAN`.
28. Sélectionnez `Site- 01-iSCSI_B_VLAN` En tant que VLAN natif.
29. Laissez le nom vNIC défini pour la source CDN.
30. Sous MTU, saisissez 9000.
31. Dans la liste Pool MAC, sélectionnez `MAC-Pool-B`.
32. Dans la liste Stratégie de contrôle du réseau, sélectionnez `Enable-CDP-LLDP`.
33. Cliquez sur OK pour terminer la création du modèle vNIC.
34. Cliquez sur OK.



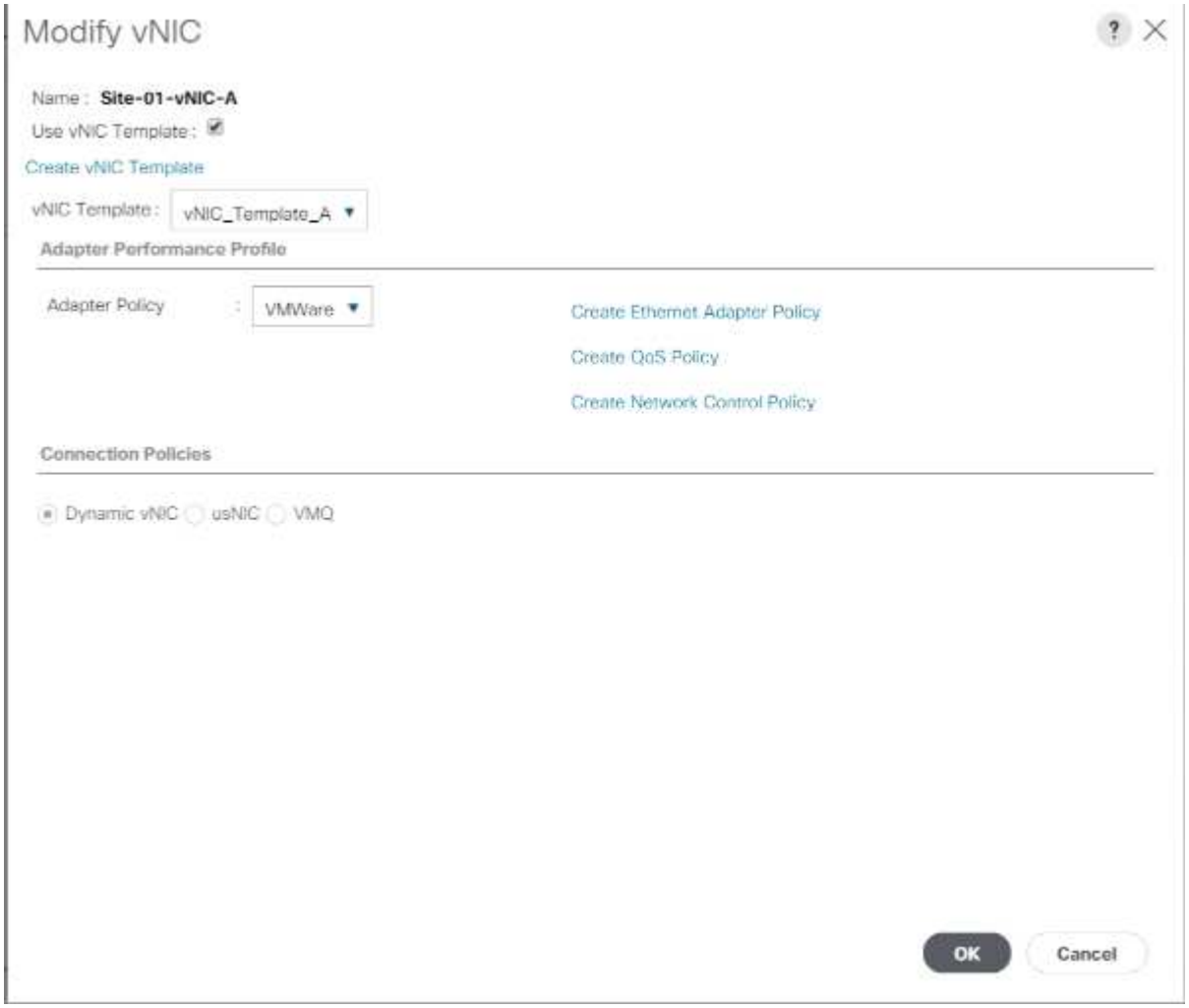
Créez une stratégie de connectivité LAN pour le démarrage iSCSI

Cette procédure s'applique à un environnement Cisco UCS dans lequel deux LIF iSCSI sont au nœud du cluster 1 (`iscsi_lif01a` et `iscsi_lif01b`) Et deux LIF iSCSI sont sur le nœud de cluster 2 (`iscsi_lif02a` et `iscsi_lif02b`). On suppose également que les LIF A sont connectées à l'environnement Fabric A (Cisco UCS 6324 A) et que B sont connectées à l'environnement Fabric B (Cisco UCS 6324 B).

Pour configurer la stratégie de connectivité LAN de l'infrastructure requise, procédez comme suit :

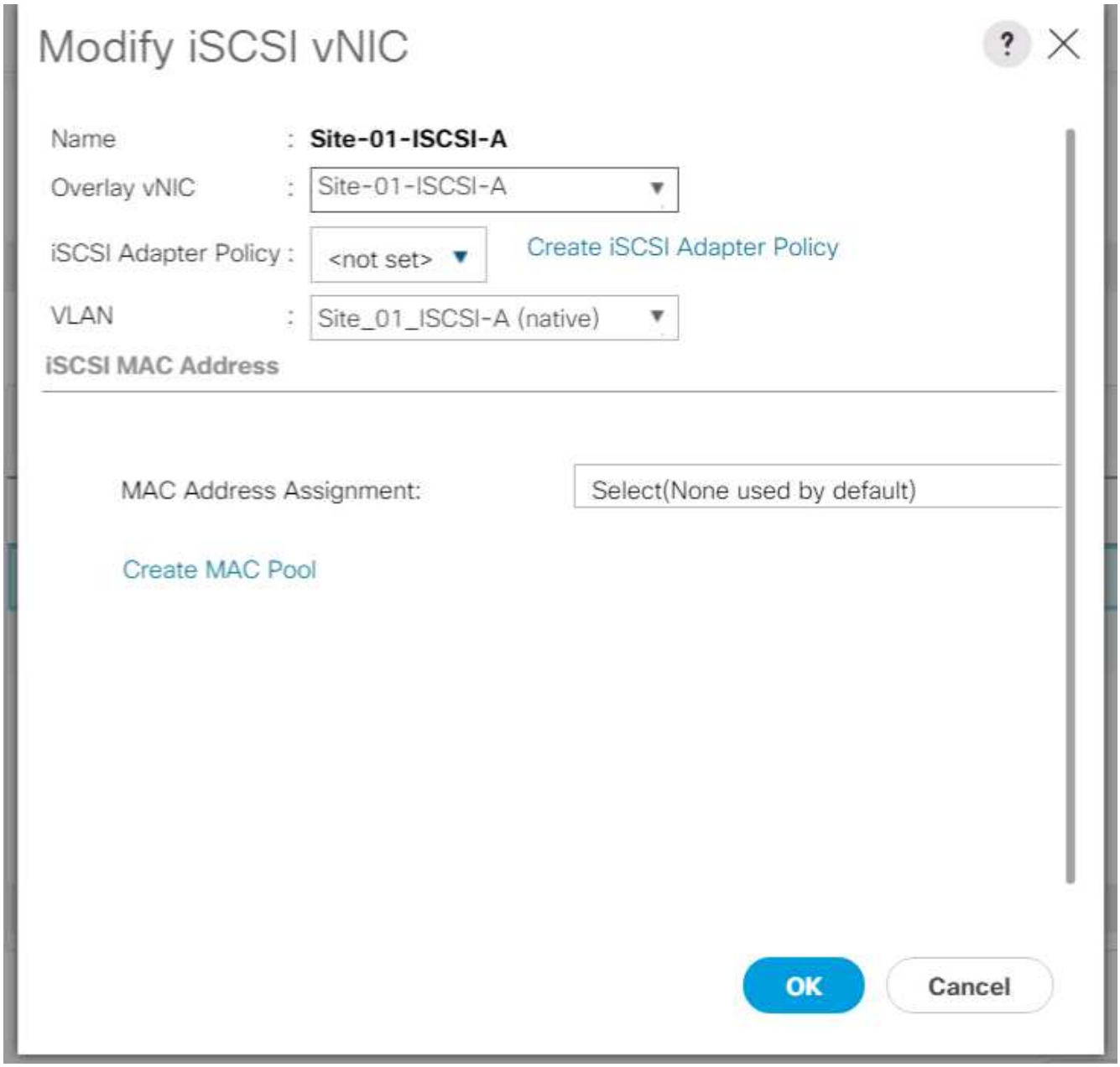
1. Dans Cisco UCS Manager, cliquez sur LAN sur la gauche.
2. Sélectionnez LAN > stratégies > racine.
3. Cliquez avec le bouton droit de la souris sur stratégies de connectivité LAN.
4. Sélectionnez Créer une stratégie de connectivité LAN.
5. Entrez `Site-XX-Fabric-A` comme nom de la règle.
6. Cliquez sur l'option Ajouter en haut pour ajouter un vNIC.
7. Dans la boîte de dialogue Créer vNIC, entrez `Site-01-vNIC-A` Comme nom du vNIC.
8. Sélectionnez l'option utiliser le modèle vNIC.
9. Dans la liste modèle vNIC, sélectionnez `vNIC_Template_A`.

10. Dans la liste déroulante adapter Policy, sélectionnez VMware.
11. Cliquez sur OK pour ajouter cette vNIC à la stratégie.

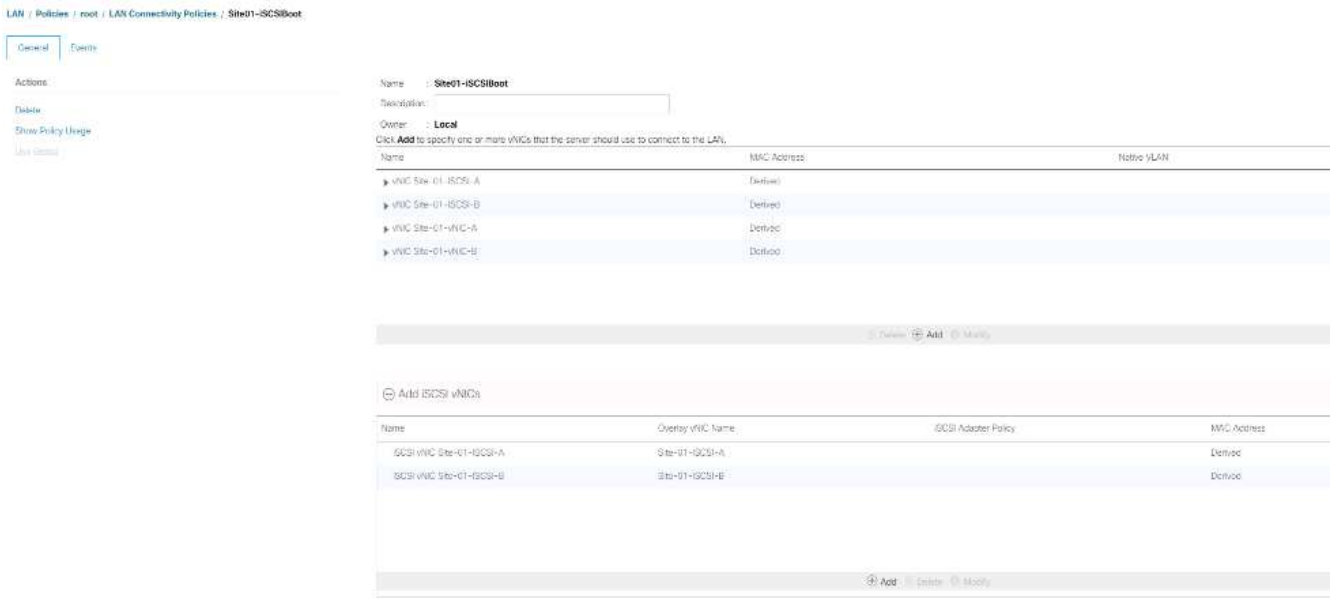


12. Cliquez sur l'option Ajouter en haut pour ajouter un vNIC.
13. Dans la boîte de dialogue Créer vNIC, entrez `Site-01-vNIC-B` Comme nom du vNIC.
14. Sélectionnez l'option utiliser le modèle vNIC.
15. Dans la liste modèle vNIC, sélectionnez `vNIC_Template_B`.
16. Dans la liste déroulante adapter Policy, sélectionnez VMware.
17. Cliquez sur OK pour ajouter cette vNIC à la stratégie.
18. Cliquez sur l'option Ajouter en haut pour ajouter un vNIC.
19. Dans la boîte de dialogue Créer vNIC, entrez `Site-01- iSCSI-A` Comme nom du vNIC.
20. Sélectionnez l'option utiliser le modèle vNIC.
21. Dans la liste modèle vNIC, sélectionnez `Site-01-iSCSI-A`.
22. Dans la liste déroulante adapter Policy, sélectionnez VMware.
23. Cliquez sur OK pour ajouter cette vNIC à la stratégie.
24. Cliquez sur l'option Ajouter en haut pour ajouter un vNIC.

25. Dans la boîte de dialogue Créer vNIC, entrez `Site-01-iSCSI-B` Comme nom du vNIC.
26. Sélectionnez l'option utiliser le modèle vNIC.
27. Dans la liste modèle vNIC, sélectionnez `Site-01-iSCSI-B`.
28. Dans la liste déroulante adapter Policy, sélectionnez VMware.
29. Cliquez sur OK pour ajouter cette vNIC à la stratégie.
30. Développez l'option Ajouter vNIC iSCSI.
31. Cliquez sur l'option Ajouter moins dans l'espace Ajouter vNIC iSCSI pour ajouter le vNIC iSCSI.
32. Dans la boîte de dialogue Créer une vNIC iSCSI, entrez `Site-01-iSCSI-A` Comme nom du vNIC.
33. Sélectionnez Overlay vNIC as `Site-01-iSCSI-A`.
34. Laissez l'option de stratégie de carte iSCSI sur non défini.
35. Sélectionnez le VLAN comme `Site-01-iSCSI-Site-A` (natif).
36. Sélectionnez aucun (utilisé par défaut) comme affectation d'adresse MAC.
37. Cliquez sur OK pour ajouter le vNIC iSCSI à la stratégie.



38. Cliquez sur l'option Ajouter moins dans l'espace Ajouter vNIC iSCSI pour ajouter le vNIC iSCSI.
39. Dans la boîte de dialogue Créer une vNIC iSCSI, entrez `Site-01-iSCSI-B` Comme nom du vNIC.
40. Sélectionnez Overlay vNIC comme site-01-iSCSI-B.
41. Laissez l'option de stratégie de carte iSCSI sur non défini.
42. Sélectionnez le VLAN comme `Site-01-iSCSI-Site-B` (natif).
43. Sélectionnez aucun (utilisé par défaut) comme affectation d'adresse MAC.
44. Cliquez sur OK pour ajouter le vNIC iSCSI à la stratégie.
45. Cliquez sur Save Changes.



Créez une politique vMedia pour le démarrage d'installation de VMware ESXi 6.7U1

Lors des étapes de configuration de NetApp Data ONTAP, un serveur Web HTTP est requis pour héberger NetApp Data ONTAP et les logiciels VMware. La politique vMedia créée ici correspond à VMware ESXi 6. 7U1 ISO vers le serveur Cisco UCS pour démarrer l'installation ESXi. Pour créer cette stratégie, procédez comme suit :

1. Dans Cisco UCS Manager, sélectionnez serveurs sur la gauche.
2. Sélectionnez stratégies > racine.
3. Sélectionnez stratégies vMedia.
4. Cliquez sur Ajouter pour créer une nouvelle stratégie vMedia.
5. Nommez la règle ESXi-6.7U1-HTTP.
6. Entrez les montages ISO pour ESXi 6.7U1 dans le champ Description.
7. Sélectionnez Oui pour essayer à nouveau en cas d'échec du montage.
8. Cliquez sur Ajouter.
9. Nommez le mount ESXi-6.7U1-HTTP.
10. Sélectionnez le type de périphérique CDD.
11. Sélectionnez le protocole HTTP.
12. Entrez l'adresse IP du serveur Web.

> Les adresses IP du serveur DNS n'ont pas été saisies précédemment dans l'adresse IP KVM. Il est donc nécessaire d'entrer l'adresse IP du serveur Web au lieu du nom d'hôte.

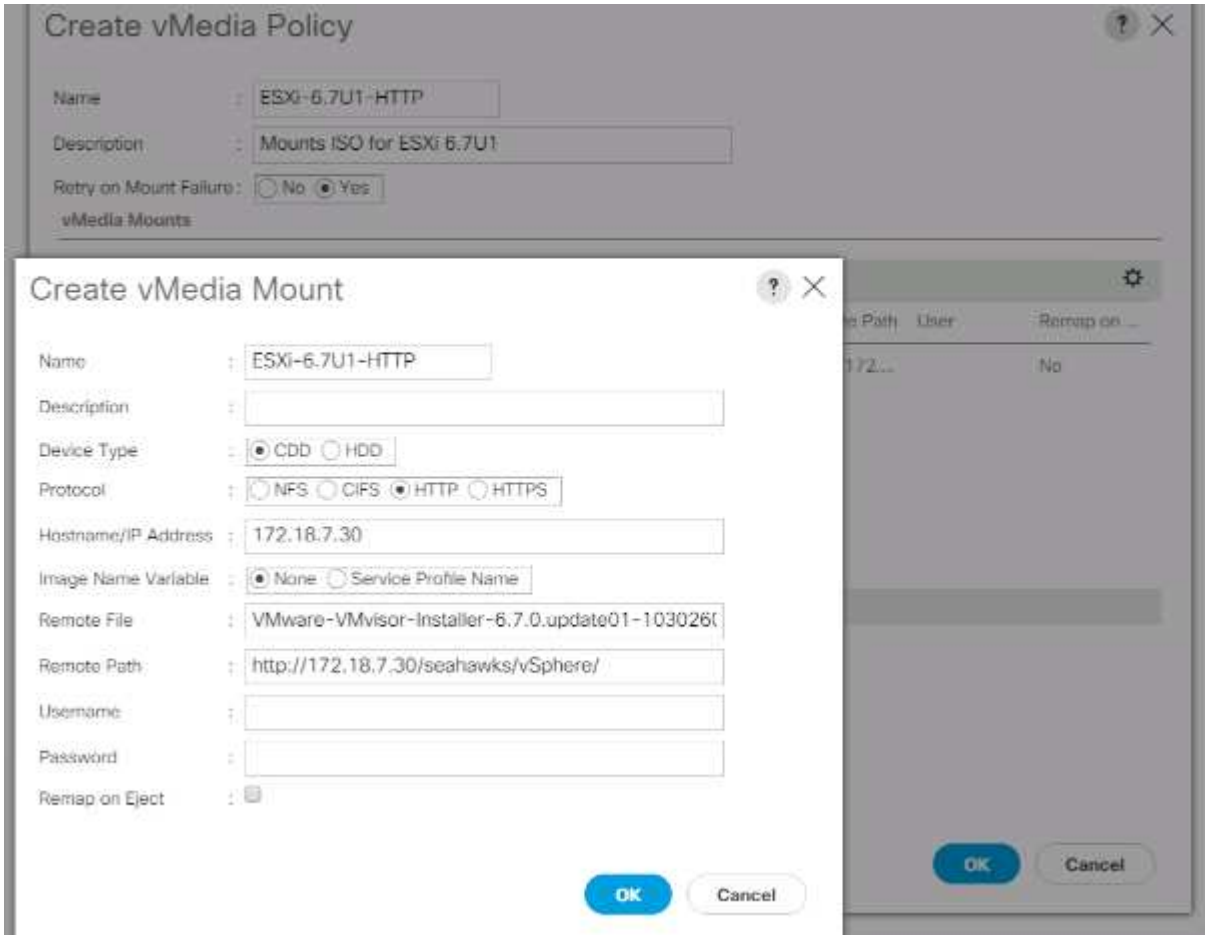
13. Entrez `VMware-VMvisor-Installer-6.7.0.update01-10302608.x86_64.iso` Comme nom de fichier distant.

    Cette norme ISO VMware ESXi 6.7U1 peut être téléchargée à partir de "Téléchargements VMware".

14. Entrez le chemin du serveur Web vers le fichier ISO dans le champ chemin distant.

15. Cliquez sur OK pour créer le montage vMedia.
16. Cliquez sur OK, puis de nouveau sur OK pour terminer la création de la stratégie vMedia.

    Pour tous les nouveaux serveurs ajoutés à l'environnement Cisco UCS, le modèle de profil de service vMedia peut être utilisé pour installer l'hôte ESXi. Lors du premier démarrage, l'hôte démarre dans le programme d'installation ESXi car le disque SAN monté est vide. Une fois ESXi installé, le vMedia n'est pas référencé tant que le disque d'amorçage est accessible.



Créer une stratégie de démarrage iSCSI

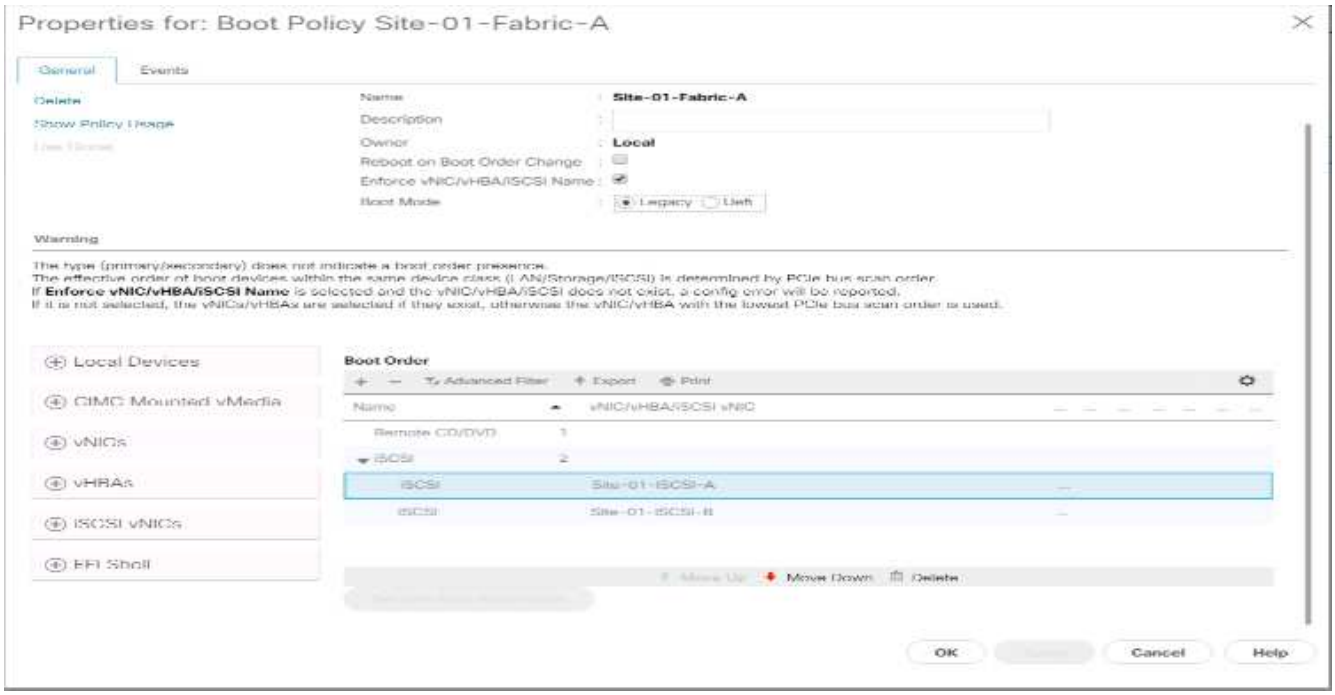
La procédure décrite dans cette section s'applique à un environnement Cisco UCS dans lequel deux interfaces logiques iSCSI (LIF) se trouvent sur le nœud de cluster 1 (`iscsi_lif01a` et `iscsi_lif01b`) Et deux LIF iSCSI sont sur le nœud de cluster 2 (`iscsi_lif02a` et `iscsi_lif02b`). On suppose également que les LIF A sont connectées à la structure A (Cisco UCS Fabric Interconnect A) et que les LIF B sont connectées à la structure B (Cisco UCS Fabric Interconnect B).

> Une politique d'amorçage est configurée dans cette procédure. La stratégie configure la cible principale à être `iscsi_lif01a`.

Pour créer une règle de démarrage pour l'environnement Cisco UCS, procédez comme suit :

1. Dans Cisco UCS Manager, cliquez sur serveurs sur la gauche.
2. Sélectionnez stratégies > racine.
3. Cliquez avec le bouton droit de la souris sur stratégies de démarrage.

4. Sélectionnez Créer une stratégie de démarrage.
5. Entrez `Site-01-Fabric-A` comme nom de la politique de boot.
6. Facultatif : saisissez une description pour la stratégie de démarrage.
7. Conservez l'option redémarrer lors de la modification de l'ordre de démarrage désactivée.
8. Le mode d'amorçage est hérité.
9. Développez le menu déroulant périphériques locaux et sélectionnez Ajouter CD/DVD distants.
10. Développez le menu déroulant vNIC iSCSI et sélectionnez Ajouter démarrage iSCSI.
11. Dans la boîte de dialogue Ajouter un démarrage iSCSI, entrez `Site-01-iSCSI-A`. Cliquez sur OK.
12. Sélectionnez Ajouter démarrage iSCSI.
13. Dans la boîte de dialogue Ajouter un démarrage iSCSI, entrez `Site-01-iSCSI-B`. Cliquez sur OK.
14. Cliquez sur OK pour créer la stratégie.



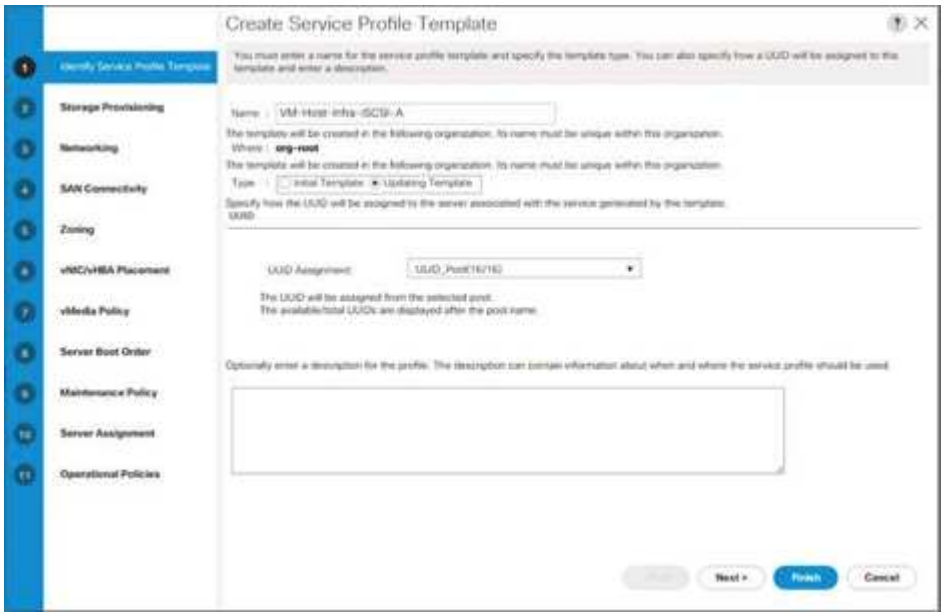
Créer un modèle de profil de service

Dans cette procédure, un modèle de profil de service pour les hôtes Infrastructure ESXi est créé pour l'amorçage Fabric A.

Pour créer le modèle de profil de service, procédez comme suit :

1. Dans Cisco UCS Manager, cliquez sur serveurs sur la gauche.
2. Sélectionnez modèles de profil de service > racine.
3. Cliquez avec le bouton droit de la souris sur root.
4. Sélectionnez Créer un modèle de profil de service pour ouvrir l'assistant Créer un modèle de profil de service.
5. Entrez `VM-Host-Infra-iSCSI-A` comme nom du modèle de profil de service. Ce modèle de profil de service est configuré pour démarrer à partir du nœud de stockage 1 sur la structure A.

6. Sélectionnez l’option mise à jour du modèle.
7. Sous UUID, sélectionnez `UUID_Pool` Comme pool UUID. Cliquez sur Suivant.



Configurer le provisionnement du stockage

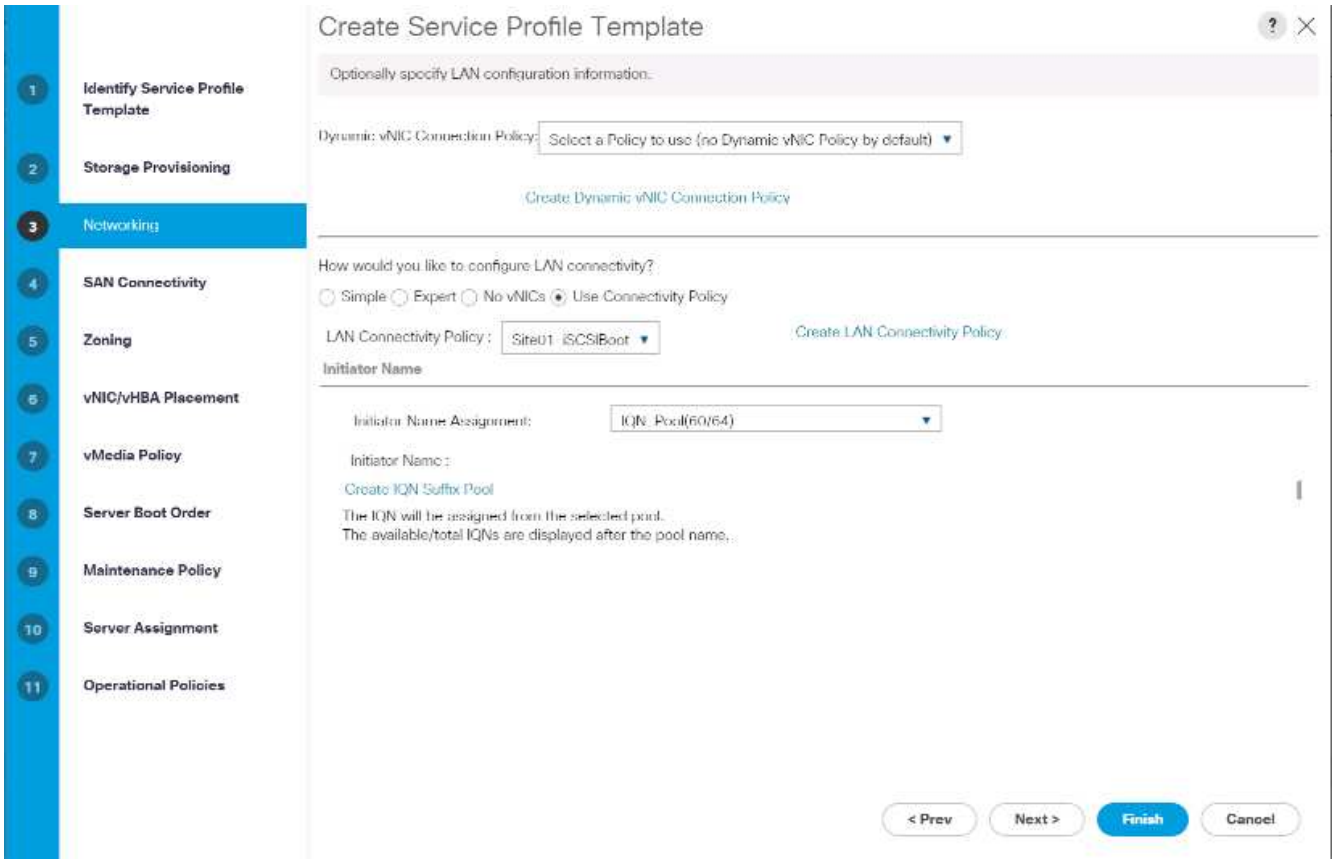
Pour configurer le provisionnement du stockage, procédez comme suit :

1. Si vous disposez de serveurs sans disque physique, cliquez sur Stratégie de configuration du disque local et sélectionnez la stratégie de stockage local d’amorçage SAN. Sinon, sélectionnez la stratégie de stockage local par défaut.
2. Cliquez sur Suivant.

Configurer les options de mise en réseau

Pour configurer les options de mise en réseau, procédez comme suit :

1. Conservez le paramètre par défaut de la stratégie de connexion vNIC dynamique.
2. Sélectionnez l’option utiliser la stratégie de connectivité pour configurer la connectivité LAN.
3. Sélectionnez iSCSI-Boot dans le menu déroulant Stratégie de connectivité LAN.
4. Sélectionnez `IQN_Pool` Dans attribution de nom d’initiateur. Cliquez sur Suivant.



Configurez la connectivité SAN

Pour configurer la connectivité SAN, procédez comme suit :

1. Pour les vHBA, sélectionnez non pour le mode de configuration de la connectivité SAN. option.
2. Cliquez sur Suivant.

Configurer la segmentation

Pour configurer le zoning, cliquez simplement sur Next (Suivant).

Configurez le positionnement vNIC/HBA

Pour configurer le placement de vNIC/HBA, procédez comme suit :

1. Dans la liste déroulante Sélectionner un placement, laissez la règle de placement comme laisser le système effectuer un placement.
2. Cliquez sur Suivant.

Configurez la stratégie vMedia

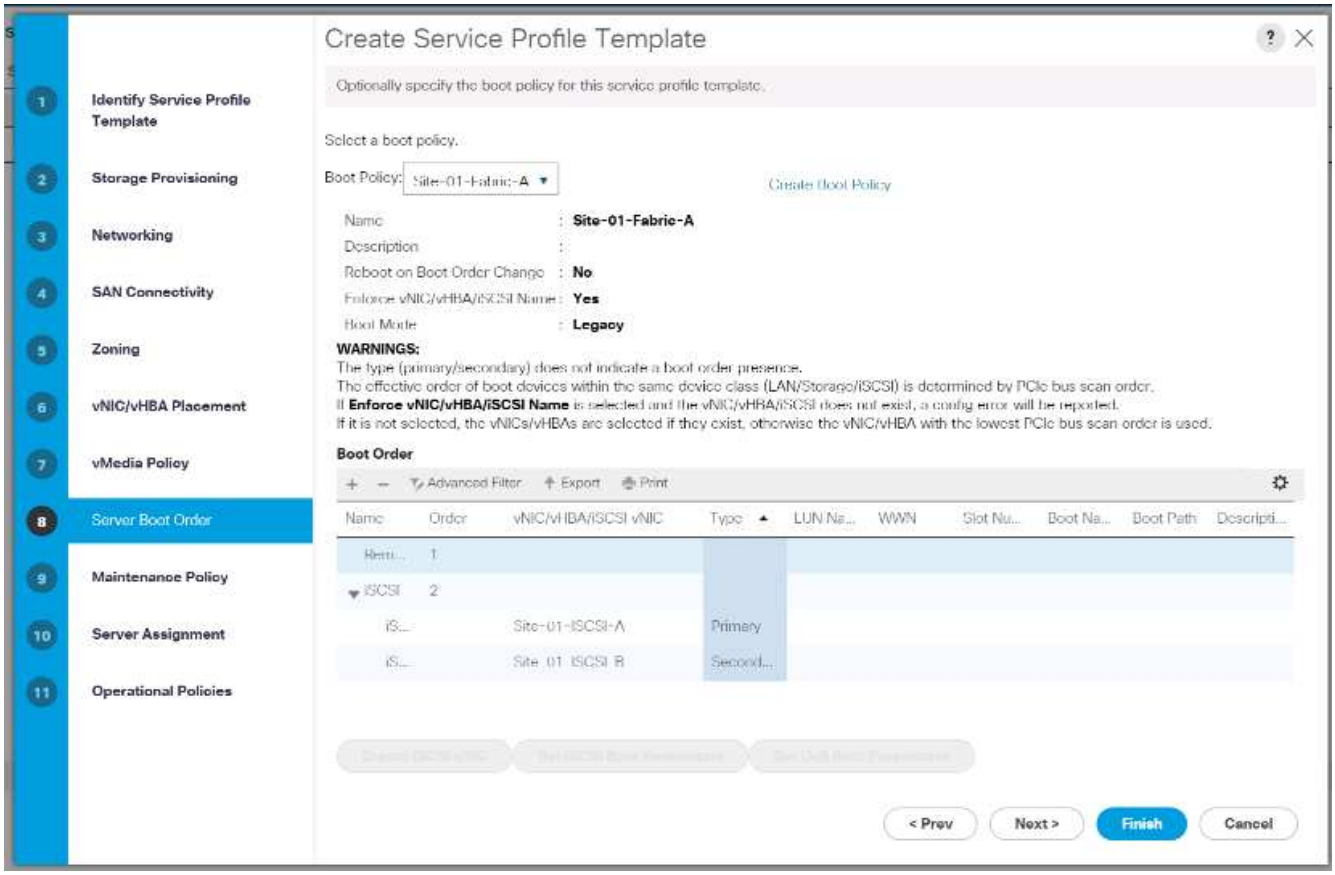
Pour configurer la stratégie vMedia, procédez comme suit :

1. Ne sélectionnez pas de stratégie vMedia.
2. Cliquez sur Suivant.

Configurer l'ordre de démarrage du serveur

Pour configurer l'ordre de démarrage du serveur, procédez comme suit :

1. Sélectionnez `Boot-Fabric-A` Pour la stratégie d'amorçage.



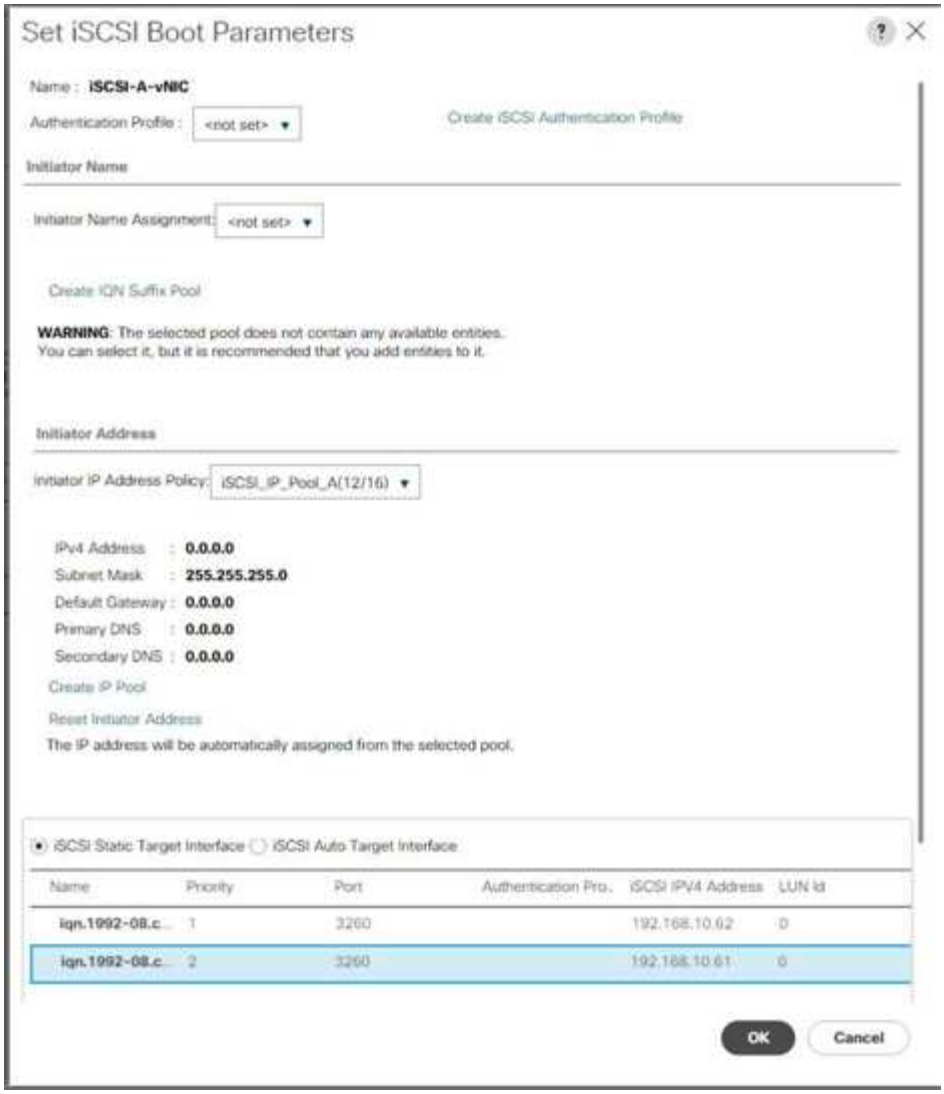
2. Dans l'ordre Boor, sélectionnez `Site-01- iSCSI-A`.
3. Cliquez sur définir les paramètres de démarrage iSCSI.
4. Dans la boîte de dialogue définir les paramètres de démarrage iSCSI, laissez l'option profil d'authentification ne pas être définie, sauf si vous avez créé un profil adapté à votre environnement de manière indépendante.
5. Laissez la boîte de dialogue attribution du nom de l'initiateur non définie pour utiliser le nom unique de l'initiateur du profil de service défini dans les étapes précédentes.
6. Réglez `iSCSI_IP_Pool_A` Comme stratégie d'adresse IP de l'initiateur.
7. Sélectionnez l'option iSCSI Static Target interface (interface cible statique iSCSI).
8. Cliquez sur Ajouter.
9. Entrez le nom de la cible iSCSI. Pour obtenir le nom de la cible iSCSI d'Infra-SVM, connectez-vous à l'interface de gestion du cluster de stockage et exécutez le `iscsi show` commande.

```
bb04-aff300::> iscsi show
          Target                          Target                          Status
Vserver   Name                            Alias                           Admin
--------- ----------------------------- ------------------------------- ------
Infra-SVM iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                          Infra-SVM                       up
```

10. Entrez l'adresse IP de `iscsi_lif_02a` Pour le champ adresse IPv4.

11. Cliquez sur OK pour ajouter la cible statique iSCSI.
12. Cliquez sur Ajouter.
13. Entrez le nom de la cible iSCSI.
14. Entrez l'adresse IP de `iscsi_lif_01a` Pour le champ adresse IPv4.

15. Cliquez sur OK pour ajouter la cible statique iSCSI.



Les adresses IP cibles ont été placées en premier avec le nœud de stockage 02 IP et le nœud de stockage 01 IP seconde. Cela suppose que la LUN de démarrage se trouve sur le nœud 01. L'hôte démarre en utilisant le chemin d'accès au nœud 01 si l'ordre dans cette procédure est utilisé.

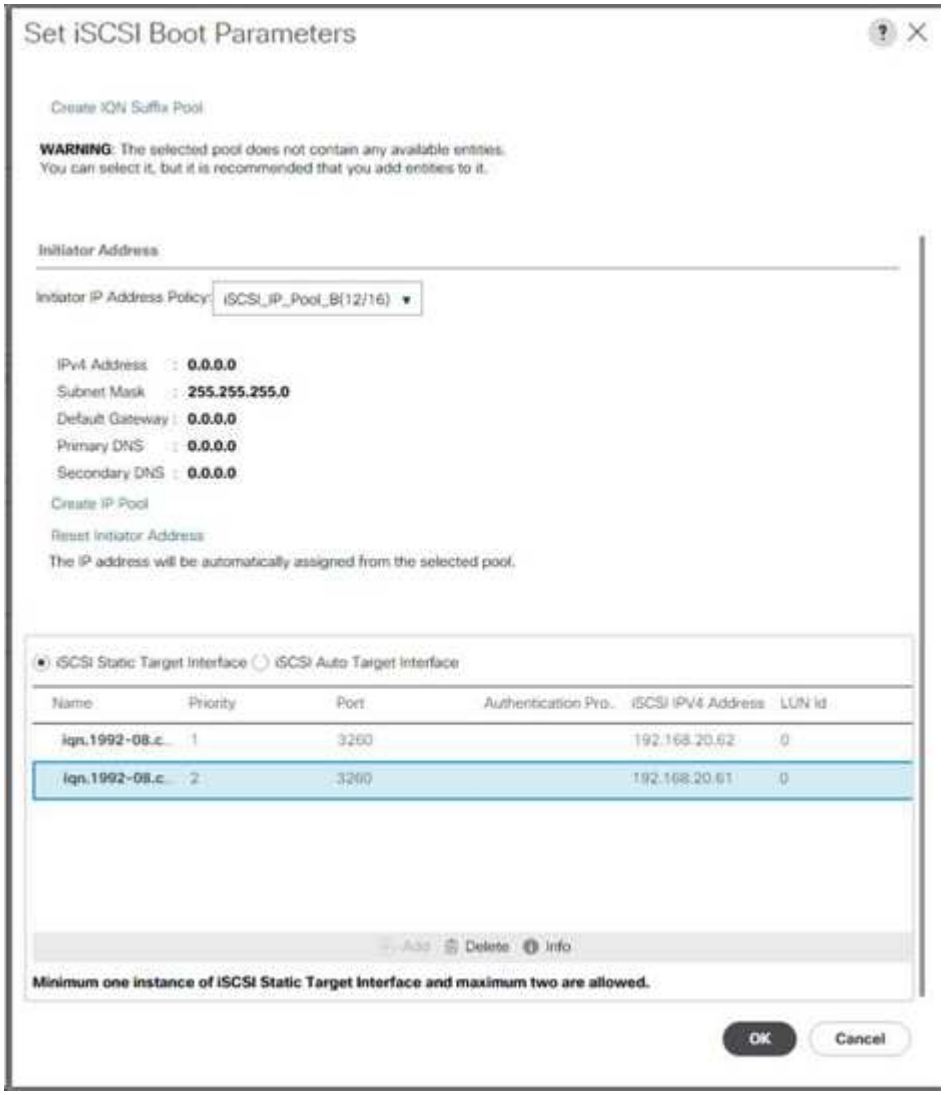
16. Dans l'ordre de démarrage, sélectionnez iSCSI-B-vNIC.
17. Cliquez sur définir les paramètres de démarrage iSCSI.
18. Dans la boîte de dialogue définir les paramètres de démarrage iSCSI, laissez l'option profil d'authentification non définie, sauf si vous avez créé un profil adapté à votre environnement de manière indépendante.
19. Laissez la boîte de dialogue attribution du nom de l'initiateur non définie pour utiliser le nom unique de l'initiateur du profil de service défini dans les étapes précédentes.
20. Réglez `iSCSI_IP_Pool_B` En tant que stratégie d'adresse IP de l'initiateur.
21. Sélectionnez l'option iSCSI Static Target interface.
22. Cliquez sur Ajouter.
23. Entrez le nom de la cible iSCSI. Pour obtenir le nom de la cible iSCSI d'Infra-SVM, connectez-vous à l'interface de gestion du cluster de stockage et exécutez le `iscsi show` commande.

```
bb04-aff300::> iscsi show
           Target                                Target                        Status
Vserver    Name                                  Alias                         Admin
---------- ------------------------------------- ---------------------------- ------
Infra-SVM  iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                                 Infra-SVM                     up
```

24. Entrez l'adresse IP de `iscsi_lif_02b` Pour le champ adresse IPv4.

25. Cliquez sur OK pour ajouter la cible statique iSCSI.
26. Cliquez sur Ajouter.
27. Entrez le nom de la cible iSCSI.
28. Entrez l'adresse IP de `iscsi_lif_01b` Pour le champ adresse IPv4.

29. Cliquez sur OK pour ajouter la cible statique iSCSI.

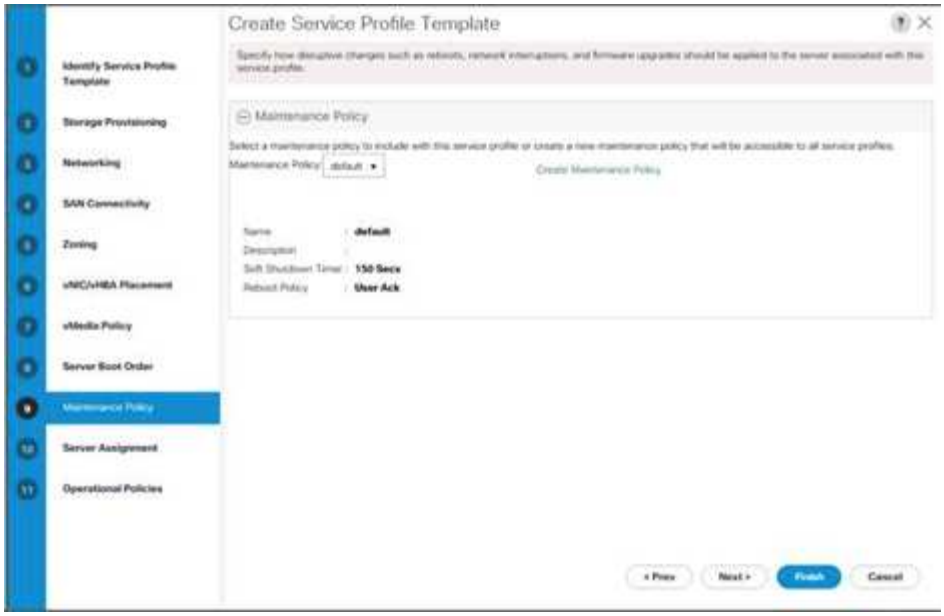


30. Cliquez sur Suivant.

Configurer la stratégie de maintenance

Pour configurer la stratégie de maintenance, procédez comme suit :

1. Définissez la stratégie de maintenance sur valeur par défaut.

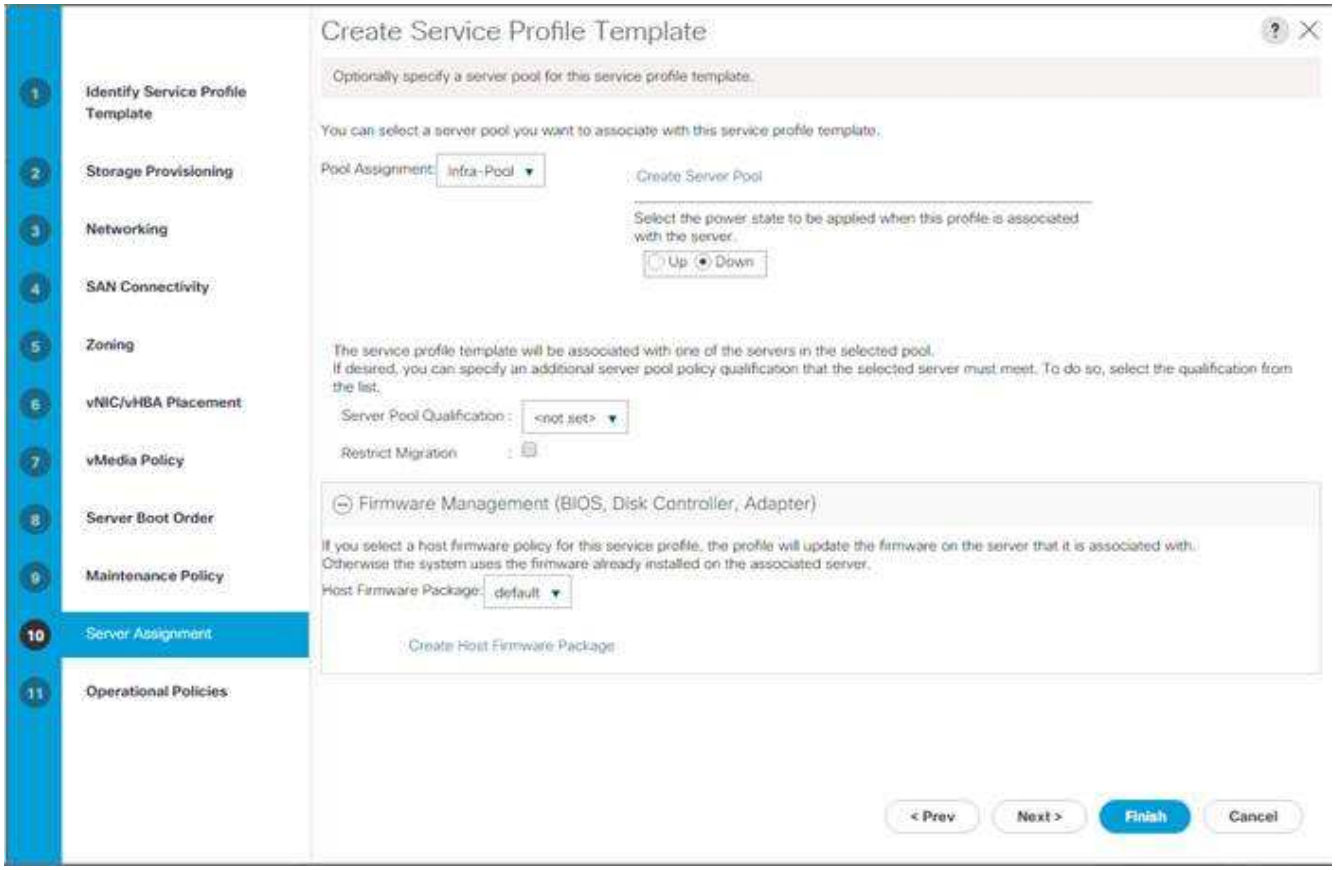


2. Cliquez sur Suivant.

Configurer l’affectation des serveurs

Pour configurer l’affectation du serveur, procédez comme suit :

1. Dans la liste Pool Assignment (affectation de pool), sélectionnez Infra-Pool.
2. Sélectionnez Down comme état d’alimentation à appliquer lorsque le profil est associé au serveur.
3. Développez gestion du micrologiciel en bas de la page et sélectionnez la stratégie par défaut.

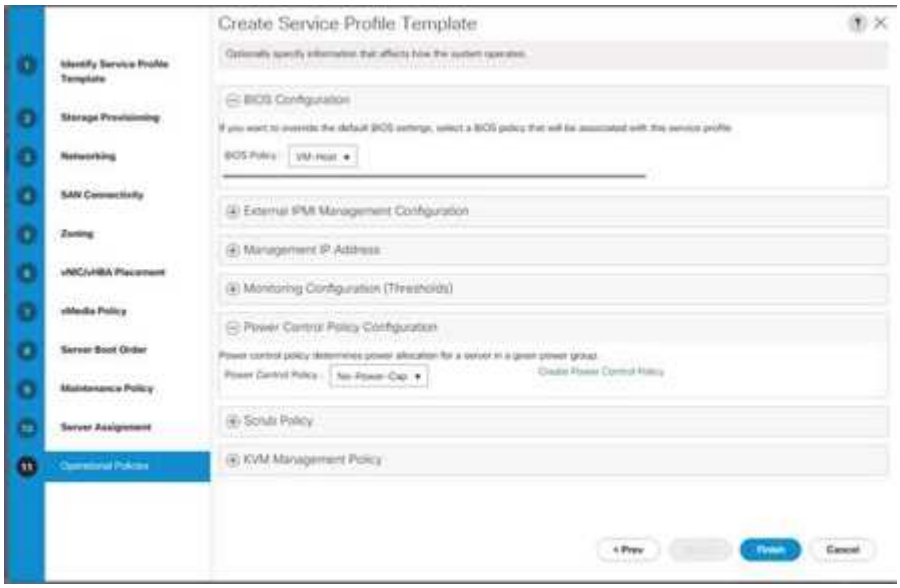


4. Cliquez sur Suivant.

Configuration des stratégies opérationnelles

Pour configurer les stratégies opérationnelles, procédez comme suit :

1. Dans la liste déroulante Stratégie du BIOS, sélectionnez VM-Host.
2. Développez Configuration de la stratégie de contrôle de l'alimentation et sélectionnez No-Power-Cap dans la liste déroulante Stratégie de contrôle de l'alimentation.



3. Cliquez sur Terminer pour créer le modèle de profil de service.
4. Cliquez sur OK dans le message de confirmation.

Créer un modèle de profil de service compatible vMedia

Pour créer un modèle de profil de service avec vMedia activé, procédez comme suit :

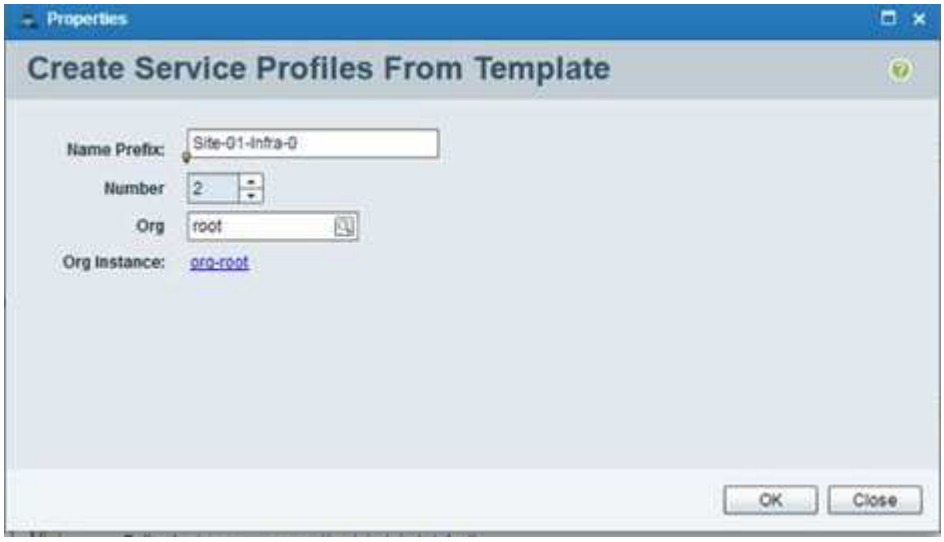
1. Connectez-vous à UCS Manager et cliquez sur serveurs sur la gauche.
2. Sélectionnez modèles de profil de service > racine > modèle de service VM-Host-Infra-iSCSI-A.
3. Cliquez avec le bouton droit de la souris sur VM-Host-Infra-iSCSI-A et sélectionnez Créer un clone.
4. Nommez le clone `VM-Host-Infra-iSCSI-A-vM`.
5. Sélectionnez le nouveau VM-Host-Infra-iSCSI-A-VM et sélectionnez l'onglet vMedia Policy à droite.
6. Cliquez sur Modifier la stratégie vMedia.
7. Sélectionnez ESXi-6. 7U1-HTTP vMedia Policy et cliquez sur OK.
8. Cliquez sur OK pour confirmer.

Créer des profils de service

Pour créer des profils de service à partir du modèle de profil de service, procédez comme suit :

1. Connectez-vous à Cisco UCS Manager et cliquez sur serveurs sur la gauche.
2. Développez serveurs > modèles de profil de service > racine > modèle de service <nom>.

3. Dans actions, cliquez sur Créer un profil de service à partir d'un modèle et effectuez les étapes suivantes :
   a. Entrez `Site- 01-Infra-0` comme préfixe de nom.
   b. Entrez `2` comme nombre d'instances à créer.
   c. Sélectionnez racine en tant qu'org.
   d. Cliquez sur OK pour créer les profils de service.



4. Cliquez sur OK dans le message de confirmation.
5. Vérifiez que les profils de service `Site-01-Infra-01` et `Site-01-Infra-02` ont été créés.

> Les profils de service sont automatiquement associés aux serveurs des pools de serveurs qui leur sont attribués.

Partie 2 de la configuration du stockage : démarrage des LUN et des groupes initiateurs

Configuration du stockage de démarrage ONTAP

Créer des groupes initiateurs

Pour créer des groupes initiateurs, effectuez la procédure suivante :

1. Lancer les commandes suivantes depuis la connexion SSH du nœud de gestion du cluster :

```
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-01 -protocol
iscsi -ostype vmware -initiator <vm-host-infra-01-iqn>
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-02 -protocol
iscsi -ostype vmware -initiator <vm-host-infra-02-iqn>
igroup create -vserver Infra-SVM -igroup MGMT-Hosts -protocol iscsi
-ostype vmware -initiator <vm-host-infra-01-iqn>, <vm-host-infra-02-iqn>
```

Utilisez les valeurs indiquées dans les tableaux 1 et 2 pour les informations IQN.

2. Pour afficher les trois igroups qui viennent de être créés, exécutez le `igroup show` commande.

Mappez les LUN de démarrage sur les igroups

Pour mapper les LUN de démarrage sur des igroups, effectuez l'étape suivante :

1. Depuis la connexion SSH de gestion du cluster de stockage, exécuter les commandes suivantes :

```
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra- A
-igroup VM-Host-Infra-01 -lun-id 0lun map -vserver Infra-SVM -volume
esxi_boot -lun VM-Host-Infra- B -igroup VM-Host-Infra-02 -lun-id 0
```

Procédure de déploiement de VMware vSphere 6.7U1

Cette section décrit les procédures d'installation de VMware ESXi 6.7U1 dans une configuration FlexPod Express. Une fois les procédures terminées, deux hôtes ESXi démarrés sont provisionnés.

Il existe plusieurs méthodes pour installer ESXi dans un environnement VMware. Ces procédures portent sur l'utilisation de la console KVM intégrée et des fonctionnalités de support virtuel de Cisco UCS Manager pour mapper le support d'installation à distance à des serveurs individuels et se connecter à leurs LUN de démarrage.

Téléchargez l'image personnalisée Cisco pour ESXi 6.7U1

Si l'image personnalisée VMware ESXi n'a pas été téléchargée, procédez comme suit pour terminer le téléchargement :

1. Cliquez sur le lien suivant : VMware vSphere Hypervisor (ESXi) 6.7U1.
2. Vous avez besoin d'un ID utilisateur et d'un mot de passe "vmware.com" pour télécharger ce logiciel.
3. Téléchargez le `.iso` fichier.

Cisco UCS Manager

Cisco UCS IP KVM permet à l'administrateur de commencer l'installation du système d'exploitation via un support distant. Il est nécessaire de se connecter à l'environnement Cisco UCS pour exécuter IP KVM.

Pour vous connecter à l'environnement Cisco UCS, procédez comme suit :

1. Ouvrez un navigateur Web et entrez l'adresse IP de l'adresse de cluster Cisco UCS. Cette étape lance l'application Cisco UCS Manager.
2. Cliquez sur le lien lancer UCS Manager sous HTML pour lancer l'interface graphique HTML 5 UCS Manager.
3. Si vous êtes invité à accepter les certificats de sécurité, acceptez-les si nécessaire.
4. Entrez-le lorsque vous y êtes invité `admin` comme nom d'utilisateur et saisissez le mot de passe d'administration.
5. Pour vous connecter à Cisco UCS Manager, cliquez sur connexion.

6. Dans le menu principal, cliquez sur serveurs sur la gauche.
7. Sélectionnez serveurs > profils de service > racine > `VM-Host-Infra-01`.
8. Cliquez avec le bouton droit de la souris `VM-Host-Infra-01` Et sélectionnez Console KVM.
9. Suivez les invites pour lancer la console KVM basée sur Java.
10. Sélectionnez serveurs > profils de service > racine > `VM-Host-Infra-02`.
11. Cliquez avec le bouton droit de la souris `VM-Host-Infra-02`. Et sélectionnez Console KVM.
12. Suivez les invites pour lancer la console KVM basée sur Java.

Configuration de l'installation de VMware ESXi

Hôtes ESXi VM-hôte-Infra-01 et VM-hôte- Infra-02

Pour préparer le serveur à l'installation du système d'exploitation, procédez comme suit sur chaque hôte ESXi :

1. Dans la fenêtre KVM, cliquez sur Virtual Media.
2. Cliquez sur Activer les périphériques virtuels.
3. Si vous êtes invité à accepter une session KVM non chiffrée, acceptez-la si nécessaire.
4. Cliquez sur Média virtuel et sélectionnez carte CD/DVD.
5. Accédez au fichier image ISO du programme d'installation ESXi et cliquez sur Ouvrir.
6. Cliquez sur mapper le périphérique.
7. Cliquez sur l'onglet KVM pour contrôler le démarrage du serveur.

Installer ESXi

Hôtes ESXi VM-hôte-Infra-01 et VM-hôte-Infra-02

Pour installer VMware ESXi sur le LUN de démarrage iSCSI des hôtes, effectuez les étapes suivantes sur chaque hôte :

1. Démarrez le serveur en sélectionnant Boot Server et en cliquant sur OK. Cliquez ensuite de nouveau sur OK.
2. Lors du redémarrage, la machine détecte la présence du support d'installation VMware ESXi. Sélectionnez le programme d'installation ESXi dans le menu de démarrage qui s'affiche.
3. Une fois le chargement du programme d'installation terminé, appuyez sur entrée pour poursuivre l'installation.
4. Lisez et acceptez le contrat de licence de l'utilisateur final (CLUF). Appuyez sur F11 pour accepter et continuer.
5. Sélectionnez le LUN 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 émet un avertissement indiquant que le disque sélectionné sera repartitionné. Appuyez sur F11 pour poursuivre l'installation.
9. Une fois l'installation terminée, sélectionnez l'onglet Média virtuel et effacez le repère P en regard du

support d'installation VMware ESXi. Cliquez sur Oui.

> L'image d'installation VMware ESXi doit être non mappée pour s'assurer que le serveur redémarre dans ESXi et non dans le programme d'installation.

10. Une fois l'installation terminée, appuyez sur entrée pour redémarrer le serveur.
11. Dans Cisco UCS Manager, associez le profil de service actuel au modèle de profil de service non-vMedia pour empêcher le montage de l'installation ESXi iso sur HTTP.

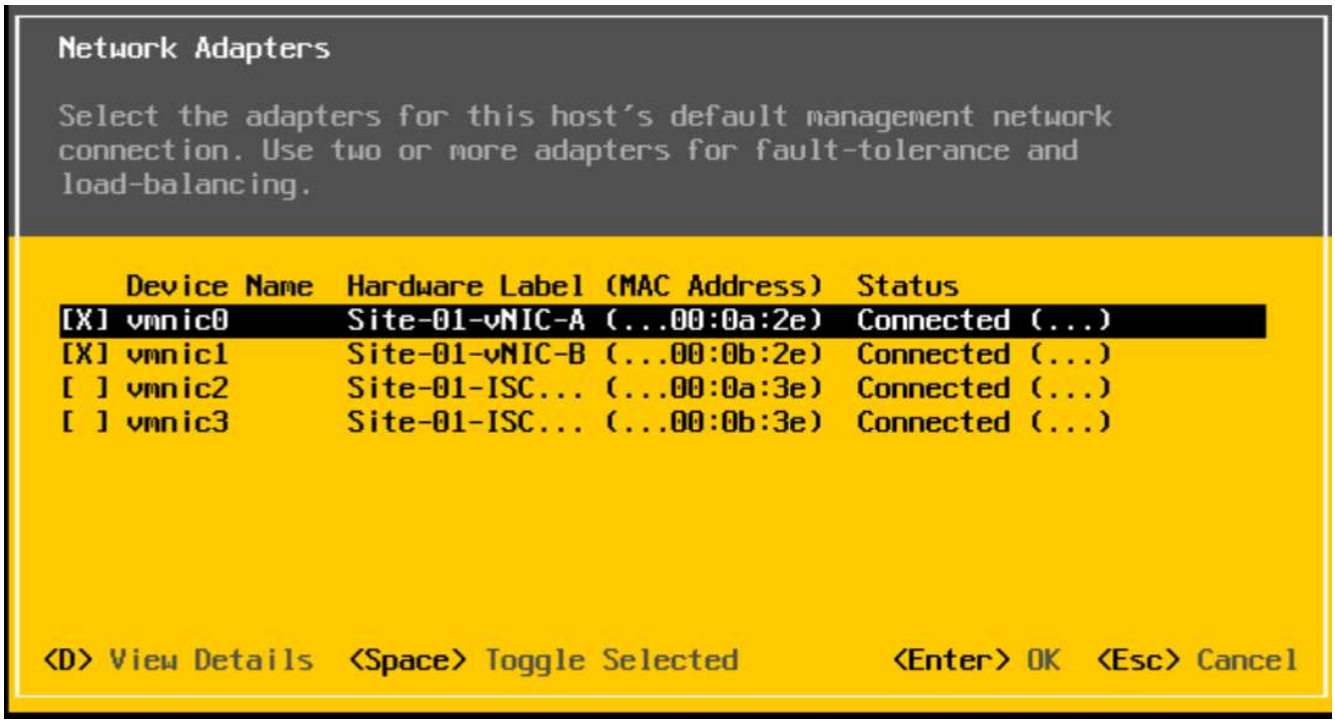
Configuration du réseau de gestion pour les hôtes ESXi

Il est nécessaire d'ajouter un réseau de gestion pour chaque hôte VMware afin de gérer l'hôte. Pour ajouter un réseau de gestion pour les hôtes VMware, procédez comme suit sur chaque hôte ESXi :

Hôte ESXi VM-hôte-Infra-01 et VM-hôte-Infra-02

Pour configurer chaque hôte ESXi avec accès au réseau de gestion, procédez comme suit :

1. Une fois le redémarrage du serveur terminé, appuyez sur F2 pour personnaliser le système.
2. Connectez-vous en tant que `root`, Saisissez le mot de passe correspondant et appuyez sur entrée pour vous connecter.
3. Sélectionnez Options de dépannage et appuyez sur entrée.
4. Sélectionnez Activer le shell ESXi et appuyez sur entrée.
5. Sélectionnez Activer SSH et appuyez sur entrée.
6. Appuyez sur Echap pour quitter le menu Options de dépannage.
7. Sélectionnez l'option configurer le réseau de gestion et appuyez sur entrée.
8. Sélectionnez cartes réseau et appuyez sur entrée.
9. Vérifiez que les numéros du champ Etiquette matérielle correspondent aux numéros du champ Nom du périphérique.
10. Appuyez sur entrée.



11. Sélectionnez l'option VLAN (facultatif) et appuyez sur entrée.
12. Entrez le `<ib-mgmt-vlan-id>` Puis appuyez sur entrée.
13. Sélectionnez Configuration IPv4 et appuyez sur entrée.
14. Sélectionnez l'option définir l'adresse IPv4 statique et la configuration réseau à l'aide de la barre d'espace.
15. Entrez l'adresse IP de gestion du premier hôte ESXi.
16. Saisissez le masque de sous-réseau du premier hôte ESXi.
17. Saisissez la passerelle par défaut pour le premier hôte ESXi.
18. Appuyez sur entrée pour accepter les modifications apportées à la configuration IP.
19. Sélectionnez l'option de configuration DNS et appuyez sur entrée.

> Étant donné que l'adresse IP est attribuée manuellement, les informations DNS doivent également être saisies manuellement.

20. Entrez l'adresse IP du serveur DNS principal.
21. Facultatif : saisissez l'adresse IP du serveur DNS secondaire.
22. Saisissez le FQDN du premier hôte ESXi.
23. Appuyez sur entrée pour accepter les modifications apportées à la configuration DNS.
24. Appuyez sur Echap pour quitter le menu configurer le réseau de gestion.
25. Sélectionnez Test Management Network pour vérifier que le réseau de gestion est correctement configuré et appuyez sur entrée.
26. Appuyez sur entrée pour exécuter le test, appuyez à nouveau sur entrée une fois le test terminé, vérifiez l'environnement en cas d'échec.
27. Sélectionnez à nouveau le bouton configurer le réseau de gestion et appuyez sur entrée.
28. Sélectionnez l'option de configuration IPv6 et appuyez sur entrée.

29. A l'aide de la barre d'espace, sélectionnez Désactiver IPv6 (redémarrage requis) et appuyez sur entrée.
30. Appuyez sur Echap pour quitter le sous-menu configurer le réseau de gestion.
31. Appuyez sur y pour confirmer les modifications et redémarrer l'hôte ESXi.

Réinitialiser l'adresse MAC vmk0 du port VMkernel de l'hôte VMware ESXi (facultatif)

Hôte ESXi VM-hôte-Infra-01 et VM-hôte-Infra-02

Par défaut, l'adresse MAC du port VMkernel de gestion vmk0 est identique à l'adresse MAC du port Ethernet sur lequel elle est placée. Si la LUN de démarrage de l'hôte ESXi est mappée à un serveur différent avec des adresses MAC différentes, un conflit d'adresse MAC se produit car vmk0 conserve l'adresse MAC attribuée, sauf si la configuration du système ESXi est réinitialisée. Pour réinitialiser l'adresse MAC de vmk0 en une adresse MAC aléatoire attribuée par VMware, procédez comme suit :

1. Dans l'écran principal du menu de la console VMware ESXi, appuyez sur Ctrl-Alt-F1 pour accéder à l'interface de ligne de commande de la console VMware. Dans le module UCSM KVM, Ctrl-Alt-F1 apparaît dans la liste des macros statiques.
2. Connectez-vous en tant que root.
3. Type `esxcfg-vmknic -l` pour obtenir une liste détaillée de l'interface vmk0. Vmk0 doit faire partie du groupe de ports du réseau de gestion. Notez l'adresse IP et le masque de réseau de vmk0.
4. Pour supprimer vmk0, entrez la commande suivante :

```
esxcfg-vmknic –d "Management Network"
```

5. Pour ajouter de nouveau vmk0 avec une adresse MAC aléatoire, entrez la commande suivante :

```
esxcfg-vmknic –a –i <vmk0-ip> -n <vmk0-netmask> "Management Network"".
```

6. Vérifiez que vmk0 a été ajouté avec une adresse MAC aléatoire

```
esxcfg-vmknic –l
```

7. Type `exit` pour se déconnecter de l'interface de ligne de commande.
8. Appuyez sur Ctrl-Alt-F2 pour revenir à l'interface de menu de la console VMware ESXi.

Connectez-vous aux hôtes VMware ESXi avec le client hôte VMware

Hôte ESXi VM-hôte-Infra-01

Pour vous connecter à l'hôte VM-Host-Infra-01 ESXi à l'aide du client hôte VMware, procédez comme suit :

1. Ouvrez un navigateur Web sur le poste de travail de gestion et accédez au `VM-Host-Infra-01` Adresse IP de gestion.
2. Cliquez sur Ouvrir le client hôte VMware.
3. Entrez `root` pour le nom d'utilisateur.

4. Entrez le mot de passe root.
5. Cliquez sur connexion pour vous connecter.
6. Répétez cette procédure pour vous connecter à `VM-Host-Infra-02` dans un onglet ou une fenêtre de navigateur séparé.

Installation des pilotes VMware pour la carte Cisco Virtual interface Card (VIC)

Téléchargez et extrayez le bundle hors ligne du pilote VIC VMware suivant sur la station de travail de gestion :

- Pilote nenic version 1.0.25.0

Hôtes ESXi VM-hôte-Infra-01 et VM-hôte-Infra-02

Pour installer les pilotes VIC VMware sur l'hôte VMware ESXi VM-Host-Infra-01 et VM-Host-Infra-02, procédez comme suit :

1. Dans chaque client hôte, sélectionnez Storage.
2. Cliquez avec le bouton droit de la souris sur datastore1 et sélectionnez Parcourir.
3. Dans le navigateur du datastore, cliquez sur Télécharger.
4. Accédez à l'emplacement enregistré des pilotes VIC téléchargés et sélectionnez VMW-ESX-6.7.0-nenic-1.0.25.0-offline_bundle-11271332.zip.
5. Dans le navigateur du datastore, cliquez sur Télécharger.
6. Cliquez sur Ouvrir pour charger le fichier dans datastore1.
7. Assurez-vous que le fichier a été téléchargé sur les deux hôtes ESXi.
8. Placez chaque hôte en mode Maintenance, si ce n'est pas déjà le cas.
9. Connectez-vous à chaque hôte ESXi via ssh à partir d'une connexion shell ou d'un terminal putty.
10. Connectez-vous en tant que root avec le mot de passe root.
11. Exécutez les commandes suivantes sur chaque hôte :

    ```
    esxcli software vib update -d /vmfs/volumes/datastore1/VMW-ESX-6.7.0-
    nenic-1.0.25.0-offline_bundle-11271332.zip
    reboot
    ```

12. Connectez-vous au client hôte sur chaque hôte une fois le redémarrage terminé et quittez le mode maintenance.

Configuration de ports VMkernel et du commutateur virtuel

Hôte ESXi VM-hôte-Infra-01 et VM-hôte-Infra-02

Pour configurer les ports VMkernel et les commutateurs virtuels sur les hôtes ESXi, procédez comme suit :

1. Dans le client hôte, sélectionnez mise en réseau sur la gauche.
2. Dans le volet central, sélectionnez l'onglet commutateurs virtuels.
3. Sélectionnez vSwitch0.
4. Sélectionnez Modifier les paramètres.

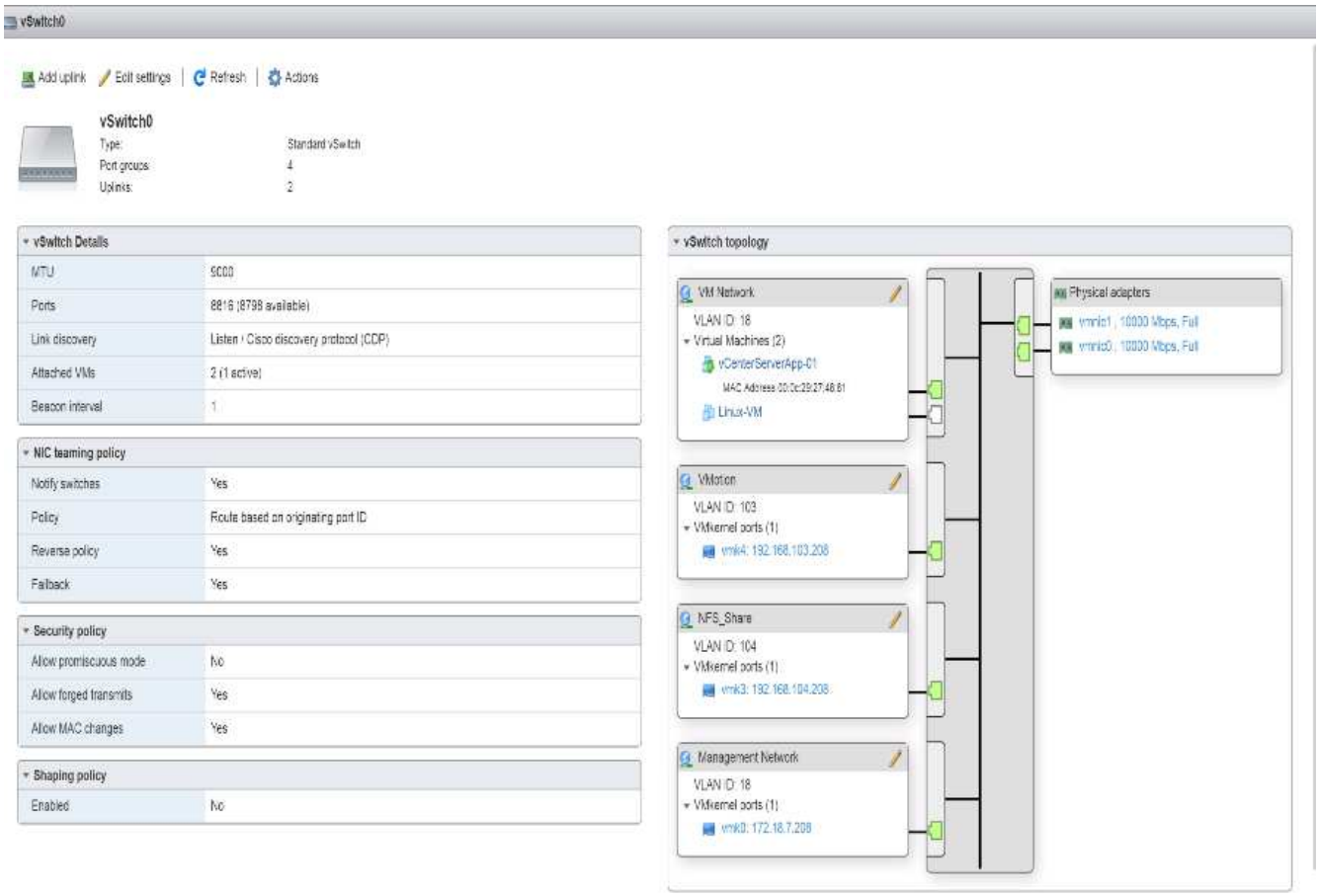
5. Remplacez la MTU par 9000.
6. Développer le regroupement de cartes réseau.
7. Dans la section ordre de basculement, sélectionnez vmnic1 et cliquez sur Marquer actif.
8. Vérifiez que vmnic1 a maintenant l'état actif.
9. Cliquez sur Enregistrer.
10. Sélectionnez réseau sur la gauche.
11. Dans le volet central, sélectionnez l'onglet commutateurs virtuels.
12. Sélectionnez iSssiBootvSwitch.
13. Sélectionnez Modifier les paramètres.
14. Remplacez la MTU par 9000
15. Cliquez sur Enregistrer.
16. Sélectionnez l'onglet VMkernel NIC.
17. Sélectionnez vmk1 iScsiBootPG.
18. Sélectionnez Modifier les paramètres.
19. Remplacez la MTU par 9000.
20. Développez les paramètres IPv4 et modifiez l'adresse IP en dehors du serveur UCS iSCSI-IP-Pool-A.

> Pour éviter les conflits d'adresses IP si les adresses de pool IP iSCSI Cisco UCS doivent être réattribuées, il est recommandé d'utiliser différentes adresses IP dans le même sous-réseau pour les ports VMkernel iSCSI.

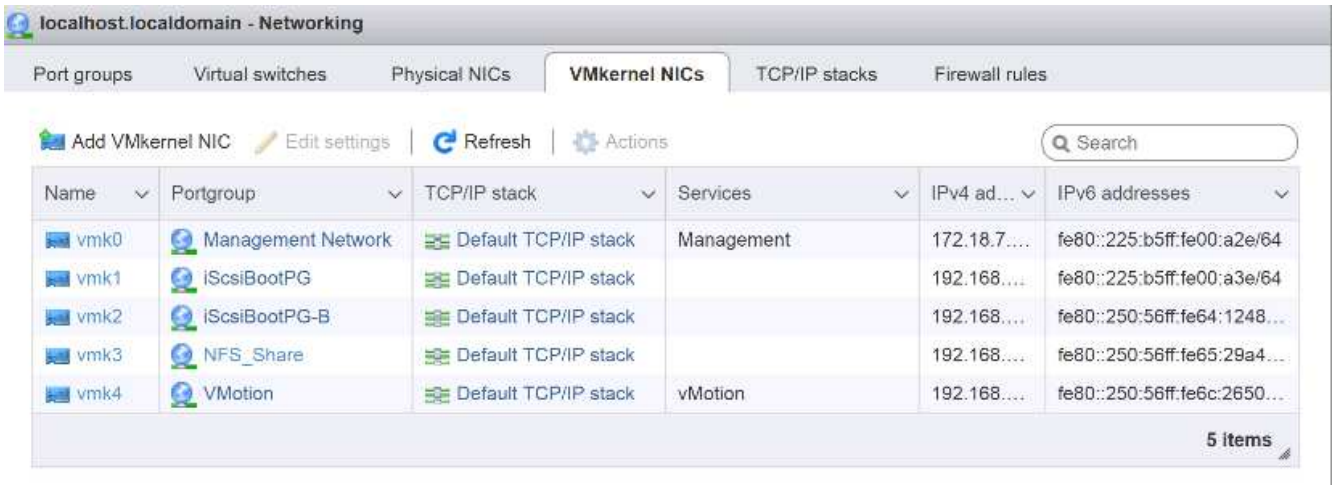
21. Cliquez sur Enregistrer.
22. Sélectionnez l'onglet commutateurs virtuels.
23. Sélectionnez le commutateur virtuel standard Add.
24. Indiquez un nom de `iScsciBootvSwitch-B` Pour le nom du vSwitch.
25. Définissez la MTU sur 9000.
26. Sélectionnez vmnic3 dans le menu déroulant Uplink 1.
27. Cliquez sur Ajouter.
28. Dans le volet central, sélectionnez l'onglet VMkernel NIC.
29. Sélectionnez Ajouter une carte réseau VMkernel
30. Spécifiez un nouveau nom de groupe de ports de iScsiBootPG-B.
31. Sélectionnez iSciBootvSwitch-B pour le commutateur virtuel.
32. Définissez la MTU sur 9000. Ne saisissez pas d'ID de VLAN.
33. Sélectionnez statique pour les paramètres IPv4 et développez l'option pour fournir l'adresse et le masque de sous-réseau dans la configuration.

> Pour éviter les conflits d'adresses IP, si les adresses de pool IP iSCSI Cisco UCS doivent être réattribuées, il est recommandé d'utiliser différentes adresses IP dans le même sous-réseau pour les ports VMkernel iSCSI.

34. Cliquez sur Créer .
35. Sur la gauche, sélectionnez réseau, puis sélectionnez l'onglet groupes de ports.
36. Dans le volet central, cliquez avec le bouton droit de la souris sur VM Network et sélectionnez Supprimer.
37. Cliquez sur Supprimer pour terminer la suppression du groupe de ports.
38. Dans le volet central, sélectionnez Ajouter un groupe de ports.
39. Attribuez un nom au réseau de gestion du groupe de ports et entrez `<ib-mgmt-vlan-id>` Dans le champ ID VLAN, et vérifier que vSwitch0 commutateur virtuel est sélectionné.
40. Cliquez sur Ajouter pour finaliser les modifications du réseau IB-MGMT.
41. En haut de la page, sélectionnez l'onglet VMkernel NIC.
42. Cliquez sur Ajouter une carte réseau VMkernel.
43. Pour Nouveau port group, entrez VMotion.
44. Pour le commutateur virtuel, sélectionnez vSwitch0 sélectionné.
45. Entrez `<vmotion-vlan-id>` Pour l'ID VLAN.
46. Remplacez la MTU par 9000.
47. Sélectionnez Paramètres IPv4 statiques et développez Paramètres IPv4.
48. Entrez l'adresse IP et le masque de réseau vMotion de l'hôte ESXi.
49. Sélectionnez la pile vMotion TCP/IP.
50. Sélectionnez vMotion sous Services.
51. Cliquez sur Créer .
52. Cliquez sur Ajouter une carte réseau VMkernel.
53. Pour Nouveau groupe de ports, entrez NFS_Share.
54. Pour le commutateur virtuel, sélectionnez vSwitch0 sélectionné.
55. Entrez `<infra-nfs-vlan-id>` Pour l'ID VLAN
56. Remplacez la MTU par 9000.
57. Sélectionnez Paramètres IPv4 statiques et développez Paramètres IPv4.
58. Entrez l'adresse IP et le masque de réseau NFS de l'infrastructure hôte ESXi.
59. Ne sélectionnez aucun des Services.
60. Cliquez sur Créer .
61. Sélectionnez l'onglet commutateurs virtuels, puis vSwitch0. Les propriétés des NIC VMkernel vSwitch0 doivent être similaires à l'exemple suivant :



62. Sélectionnez l’onglet VMkernel NIC pour confirmer les cartes virtuelles configurées. Les adaptateurs répertoriés doivent être similaires à l’exemple suivant :



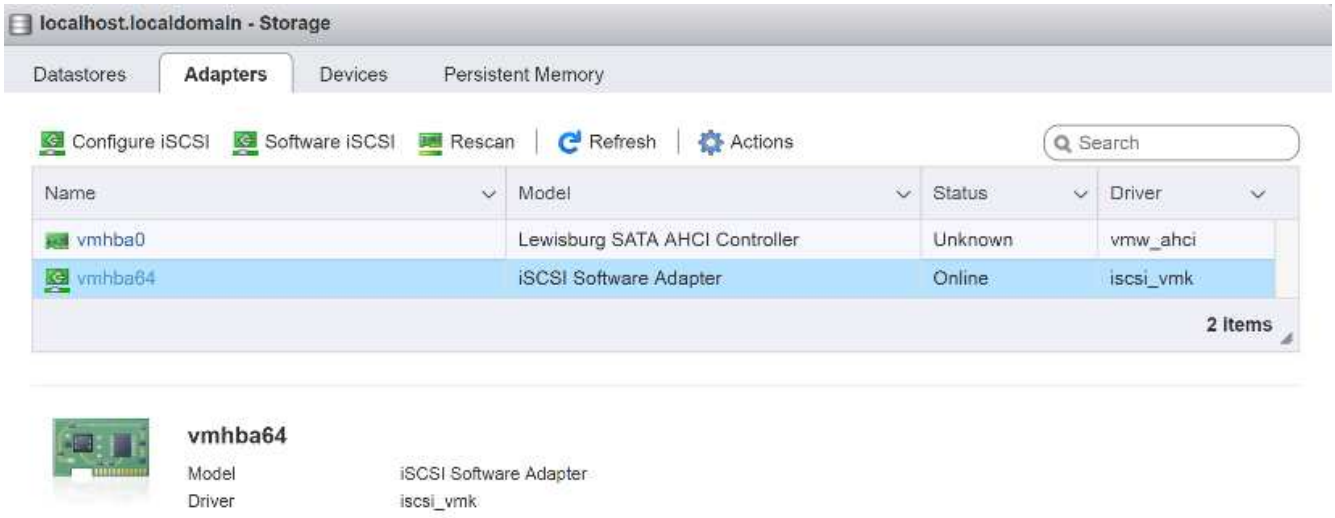
Configuration des chemins d’accès multiples iSCSI

Hôtes ESXi VM-hôte-Infra-01 et VM-hôte-Infra-02

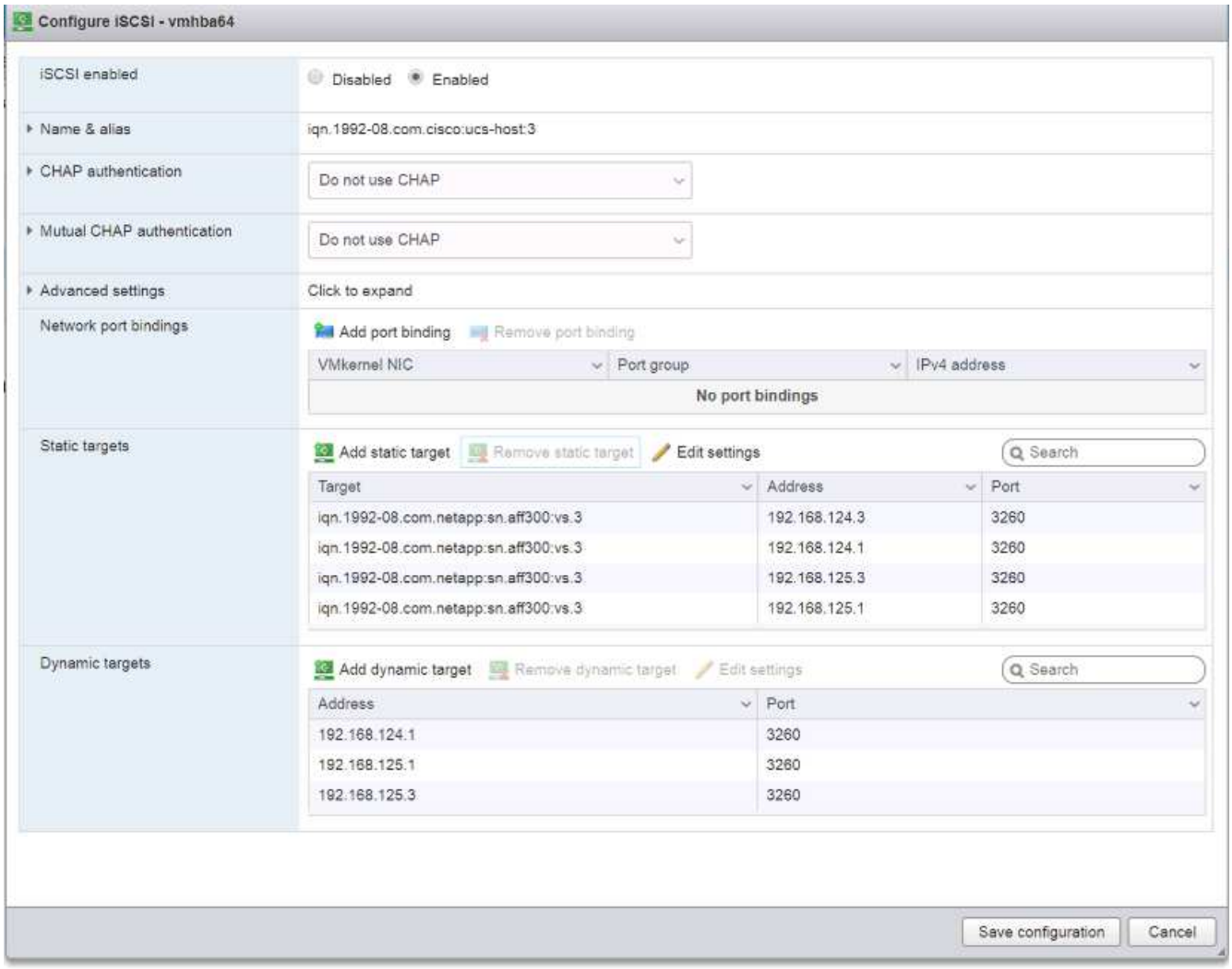
Pour configurer les chemins d’accès multiples iSCSI sur l’hôte ESXi VM-Host-Infra-01 et VM-Host-Infra-02, procédez comme suit :

1. Dans chaque client hôte, sélectionnez Storage (stockage) sur la gauche.

2. Dans le volet central, cliquez sur cartes.
3. Sélectionnez la carte logicielle iSCSI et cliquez sur configurer iSCSI.



4. Sous cibles dynamiques, cliquez sur Ajouter une cible dynamique.
5. Saisissez l'adresse IP de `iSCSI_lif01a`.
6. Répétez l'entrée des adresses IP suivantes : `iscsi_lif01b`, `iscsi_lif02a`, et `iscsi_lif02b`.
7. Cliquez sur Enregistrer la configuration.



Pour obtenir toutes les `iscsi_lif` Adresses IP, connectez-vous à l'interface de gestion du cluster de stockage NetApp et exécutez le `network interface show` commande.

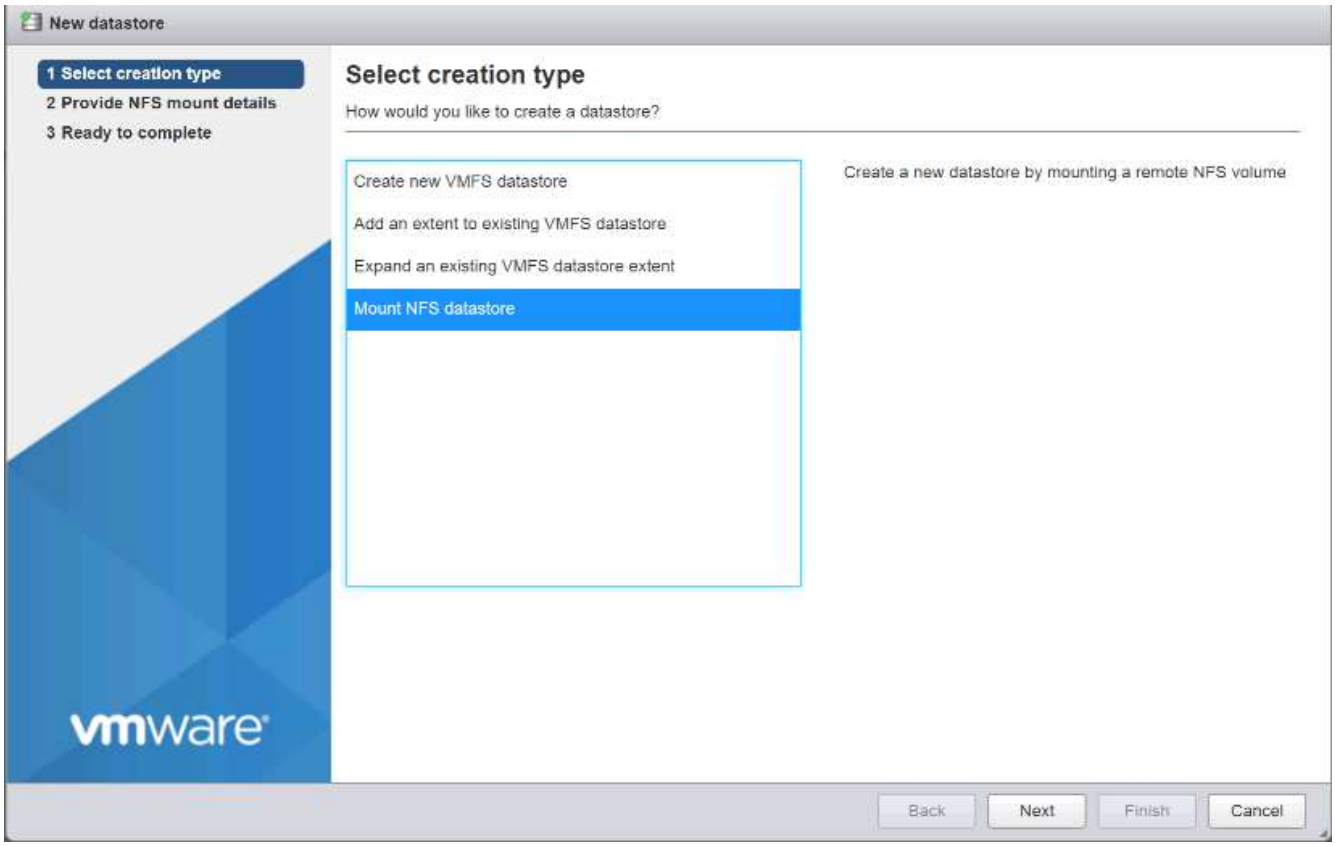
> L'hôte réanalyse automatiquement l'adaptateur de stockage et les cibles sont ajoutées aux cibles statiques.

Montez les datastores requis

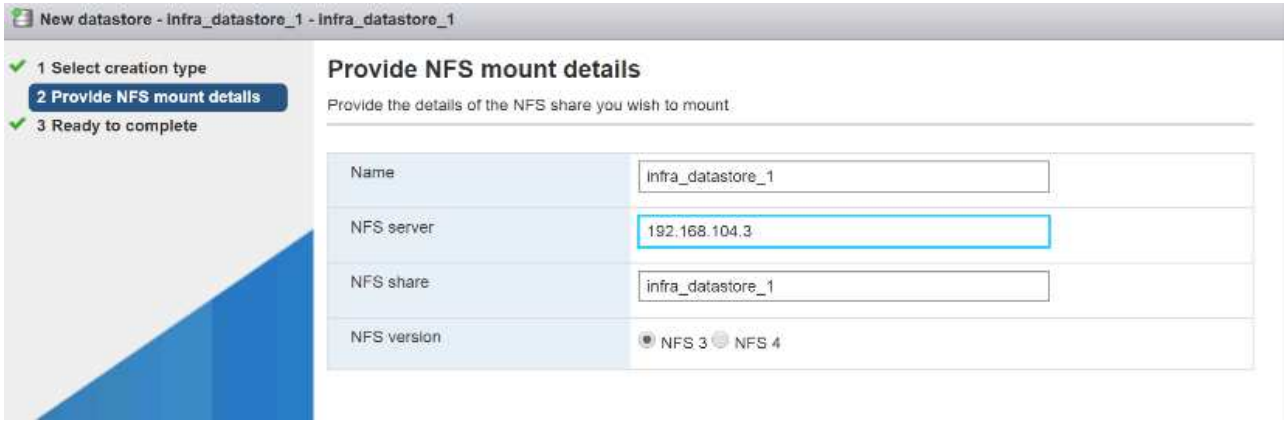
Hôtes ESXi VM-hôte-Infra-01 et VM-hôte-Infra-02

Pour monter les datastores requis, procédez comme suit sur chaque hôte ESXi :

1. Dans le client hôte, sélectionnez Storage (stockage) sur la gauche.
2. Dans le volet central, sélectionnez datastores.
3. Dans le volet central, sélectionnez Nouveau datastore pour ajouter un nouveau datastore.
4. Dans la boîte de dialogue Nouveau datastore, sélectionnez Mount NFS datastore et cliquez sur Next (Suivant).

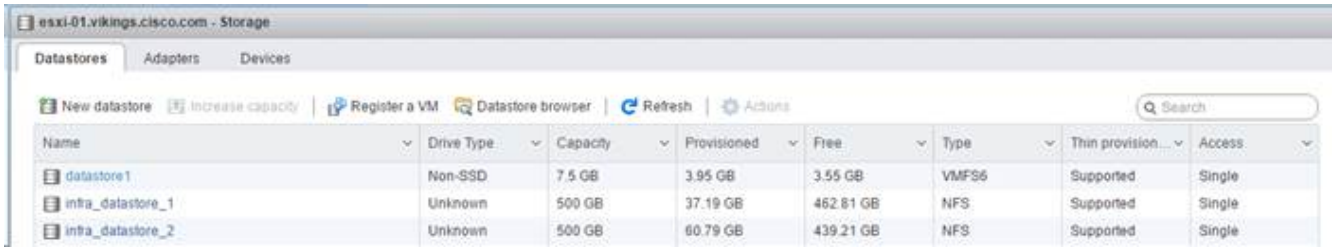


5. Sur la page Détails du montage NFS, procédez comme suit :
   a. Entrez `infra_datastore_1` nom du datastore.
   b. Entrez l'adresse IP du `nfs_lif01_a` LIF pour le serveur NFS.
   c. Entrez `/infra_datastore_1` Pour le partage NFS.
   d. Laissez la version NFS définie sur NFS 3.
   e. Cliquez sur Suivant.



6. Cliquez sur Terminer. Le datastore doit maintenant apparaître dans la liste datastore.
7. Dans le volet central, sélectionnez Nouveau datastore pour ajouter un nouveau datastore.
8. Dans la boîte de dialogue New datastore (Nouveau datastore), sélectionnez Mount NFS datastore (installer datastore NFS) et cliquez sur Next (Suivant).

9. Sur la page Détails du montage NFS, procédez comme suit :
    a. Entrez `infra_datastore_2` nom du datastore.
    b. Entrez l'adresse IP du `nfs_lif02_a` LIF pour le serveur NFS.
    c. Entrez `/infra_datastore_2` Pour le partage NFS.
    d. Laissez la version NFS définie sur NFS 3.
    e. Cliquez sur Suivant.
10. Cliquez sur Terminer. Le datastore doit maintenant apparaître dans la liste datastore.



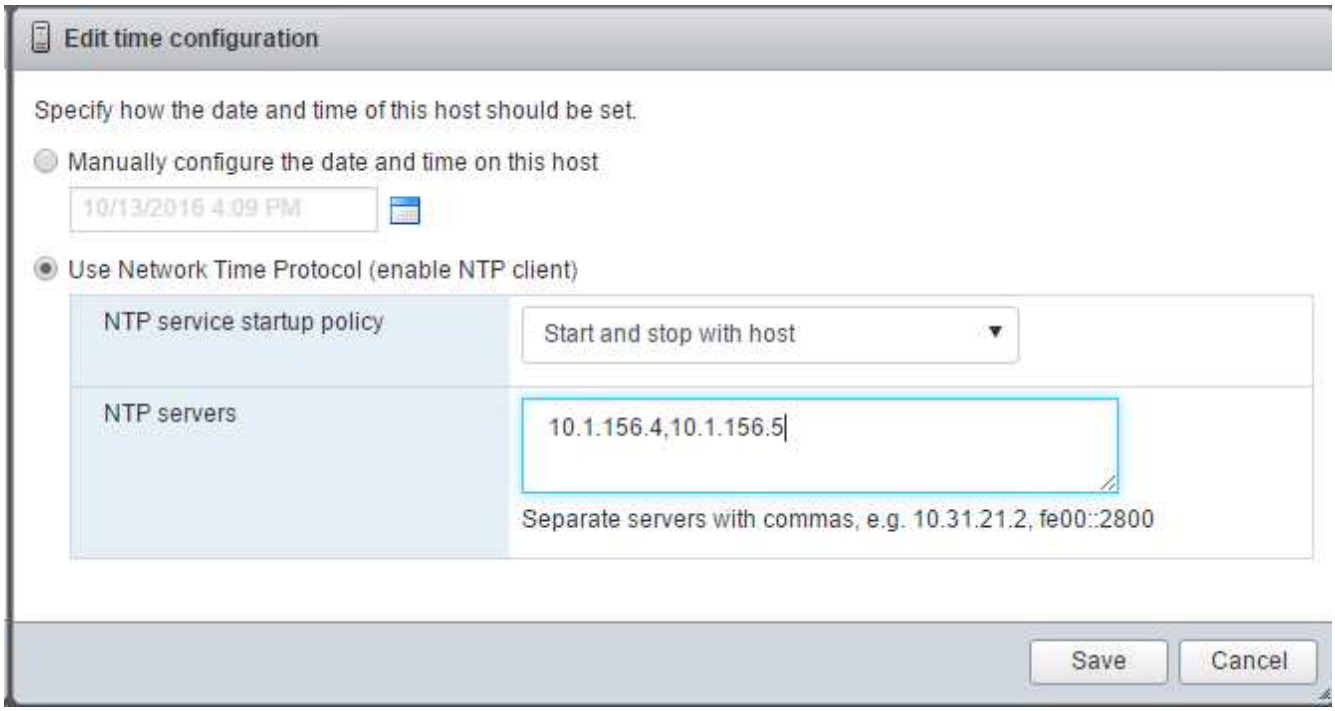
11. Montez les deux datastores sur les deux hôtes ESXi.

Configurez le protocole NTP sur les hôtes ESXi

Hôtes ESXi VM-hôte-Infra-01 et VM-hôte-Infra-02

Pour configurer le protocole NTP sur les hôtes ESXi, procédez comme suit sur chaque hôte :

1. Dans le client hôte, sélectionnez gérer à gauche.
2. Dans le volet central, sélectionnez l'onglet heure et date.
3. Cliquez sur Modifier les paramètres.
4. Assurez-vous que l'option utiliser le protocole d'heure du réseau (activer le client NTP) est sélectionnée.
5. Utilisez le menu déroulant pour sélectionner Démarrer et Arrêter avec l'hôte.
6. Saisissez les deux adresses NTP du commutateur Nexus dans la zone serveurs NTP séparés par une virgule.



7. Cliquez sur Enregistrer pour enregistrer les modifications de configuration.
8. Sélectionnez actions > service NTP > Démarrer.
9. Vérifiez que le service NTP est en cours d'exécution et que l'horloge est à présent réglée à environ l'heure correcte

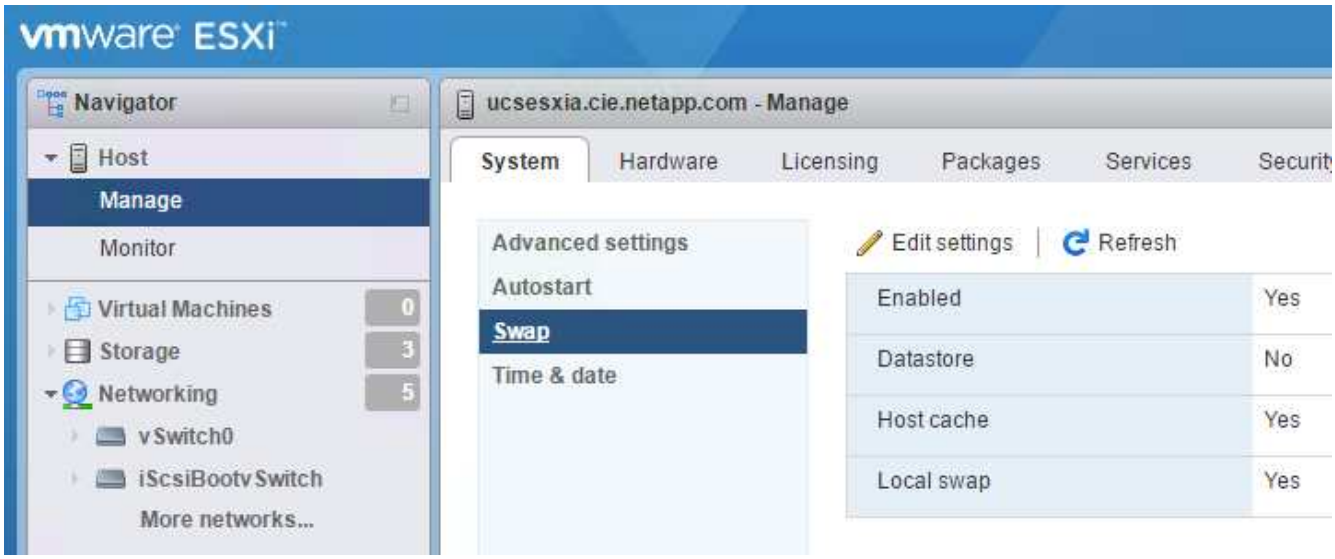
> L'heure du serveur NTP peut varier légèrement par rapport à l'heure de l'hôte.

Configurer le swap d'hôte VMware ESXi

Hôtes ESXi VM-hôte-Infra-01 et VM-hôte-Infra-02

Pour configurer le swap d'hôte sur les hôtes VMware ESXi, procédez comme suit sur chaque hôte :

1. Cliquez sur gérer dans le volet de navigation de gauche. Sélectionnez système dans le volet de droite et 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 1.1.2 pour VMware VAAI

Pour installer le plug-in NetApp NFS 1. 1.2 pour VMware VAAI, effectuez les étapes suivantes.

1. Téléchargez le plug-in NetApp NFS pour VMware VAAI :
   a. Accédez au "Page de téléchargement de logiciels NetApp".
   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.
2. Le plug-in NetApp NFS pour VMware VAAI est en attente de la qualification IMT avec ONTAP 9.5. Des informations sur l'interopérabilité seront bientôt disponibles sur le site NetApp IMT.
3. Installez le plug-in sur l'hôte ESXi à l'aide de la CLI ESX.
4. Redémarrez l'hôte ESXI.

Installez VMware vCenter Server 6.7

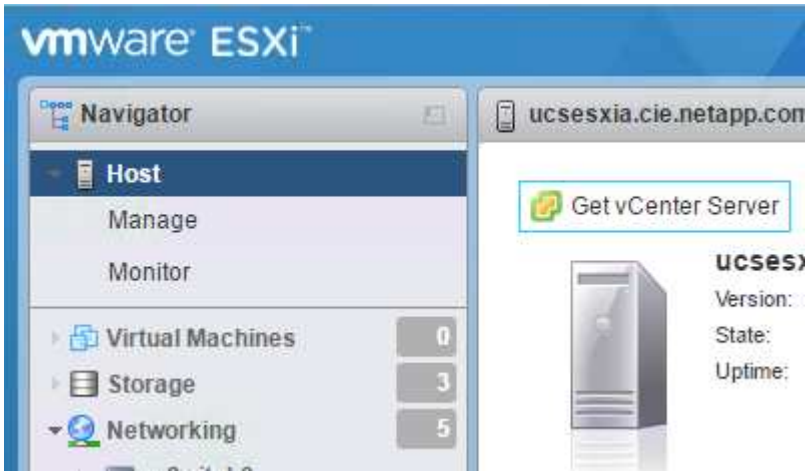
Cette section décrit les procédures détaillées d'installation de VMware vCenter Server 6.7 dans une configuration FlexPod Express.

> FlexPod Express utilise VMware vCenter Server Appliance (VCSA).

Installez l'appliance de serveur VMware vCenter

Pour installer VCSA, procédez comme suit :

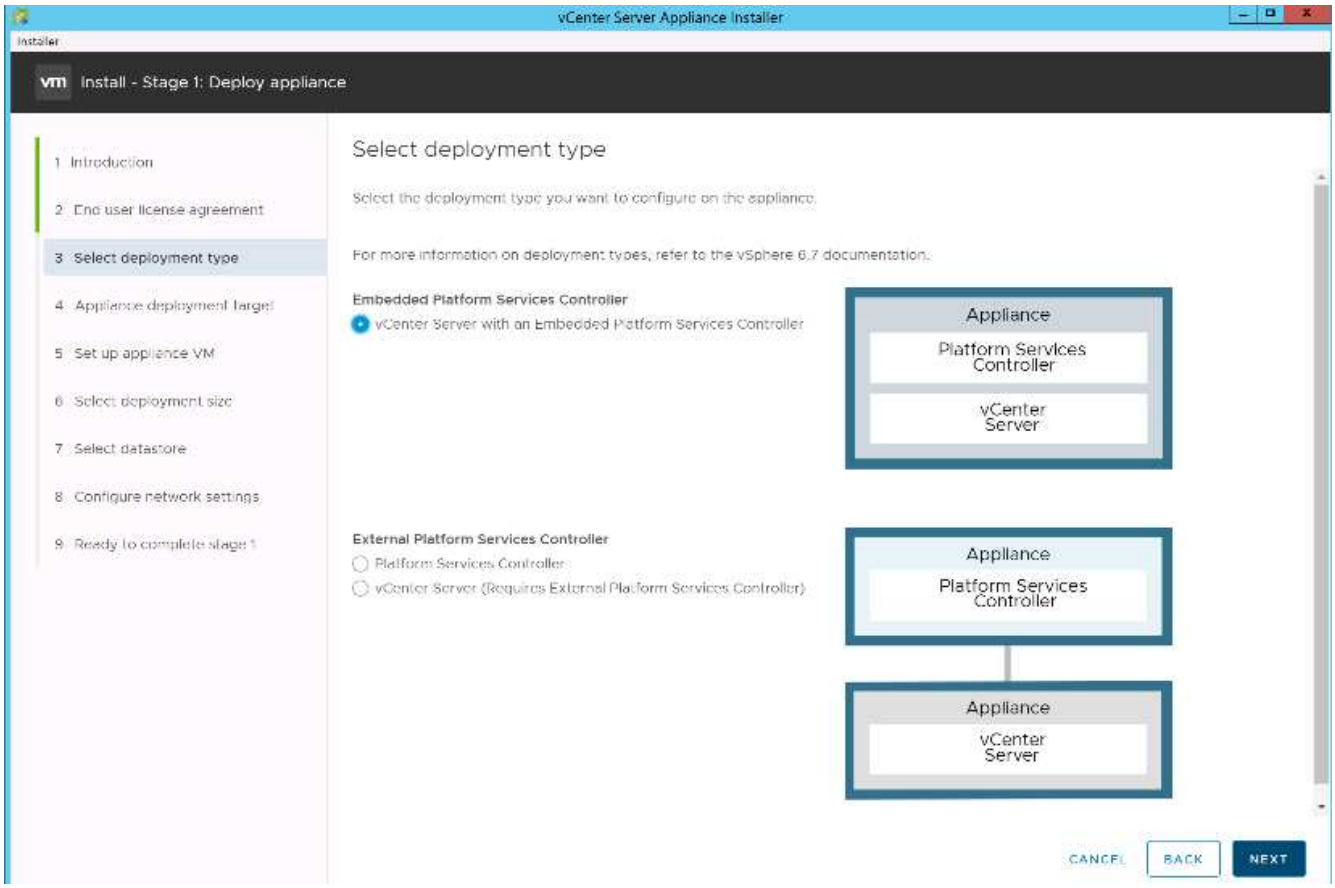
1. Téléchargez le VCSA. Accédez au lien de téléchargement en cliquant sur l'icône obtenir vCenter Server lors de la gestion de l'hôte ESXi.



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

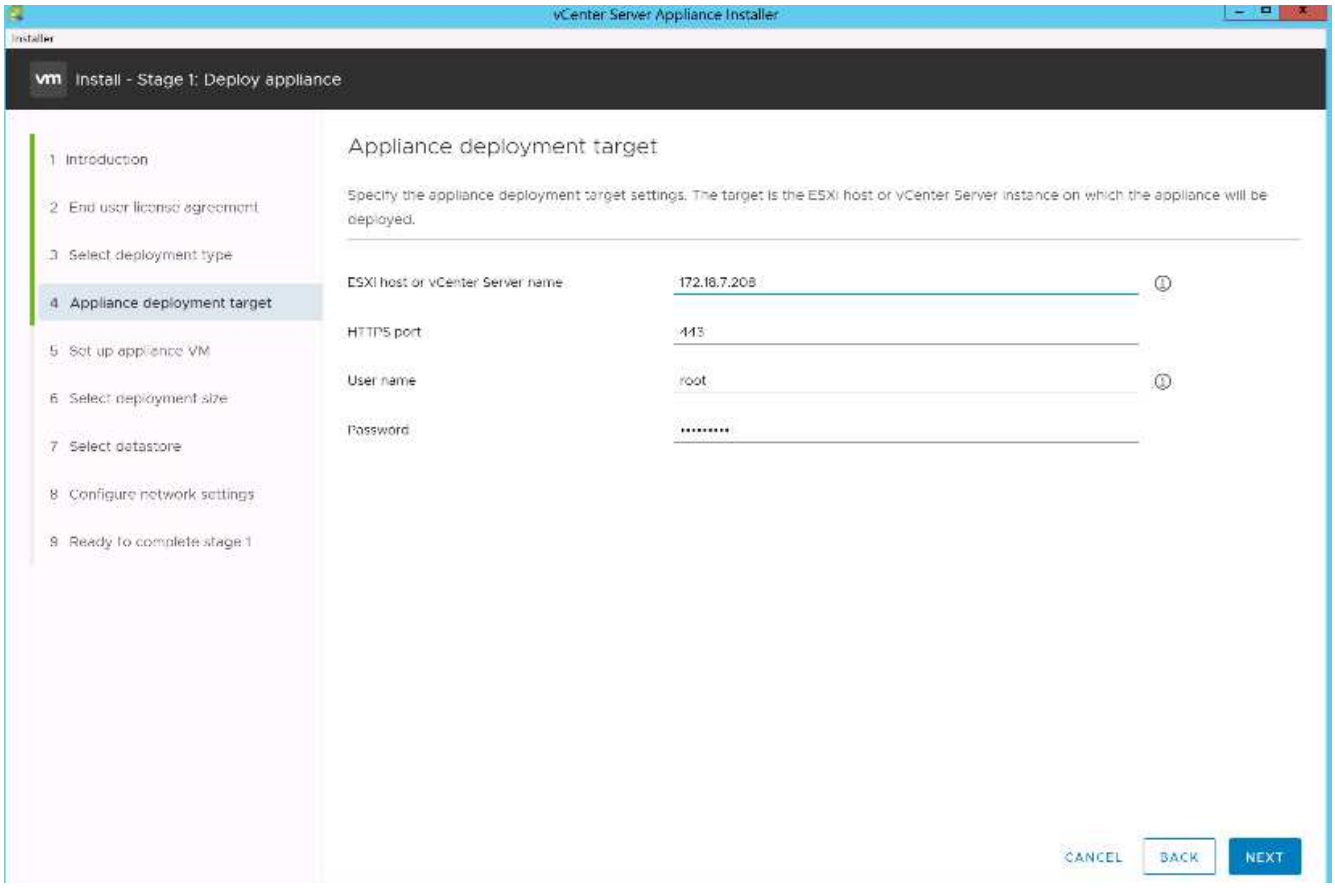
> Bien que l'installation de Microsoft Windows vCenter Server soit prise en charge, VMware recommande le VCSA pour les nouveaux déploiements.

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

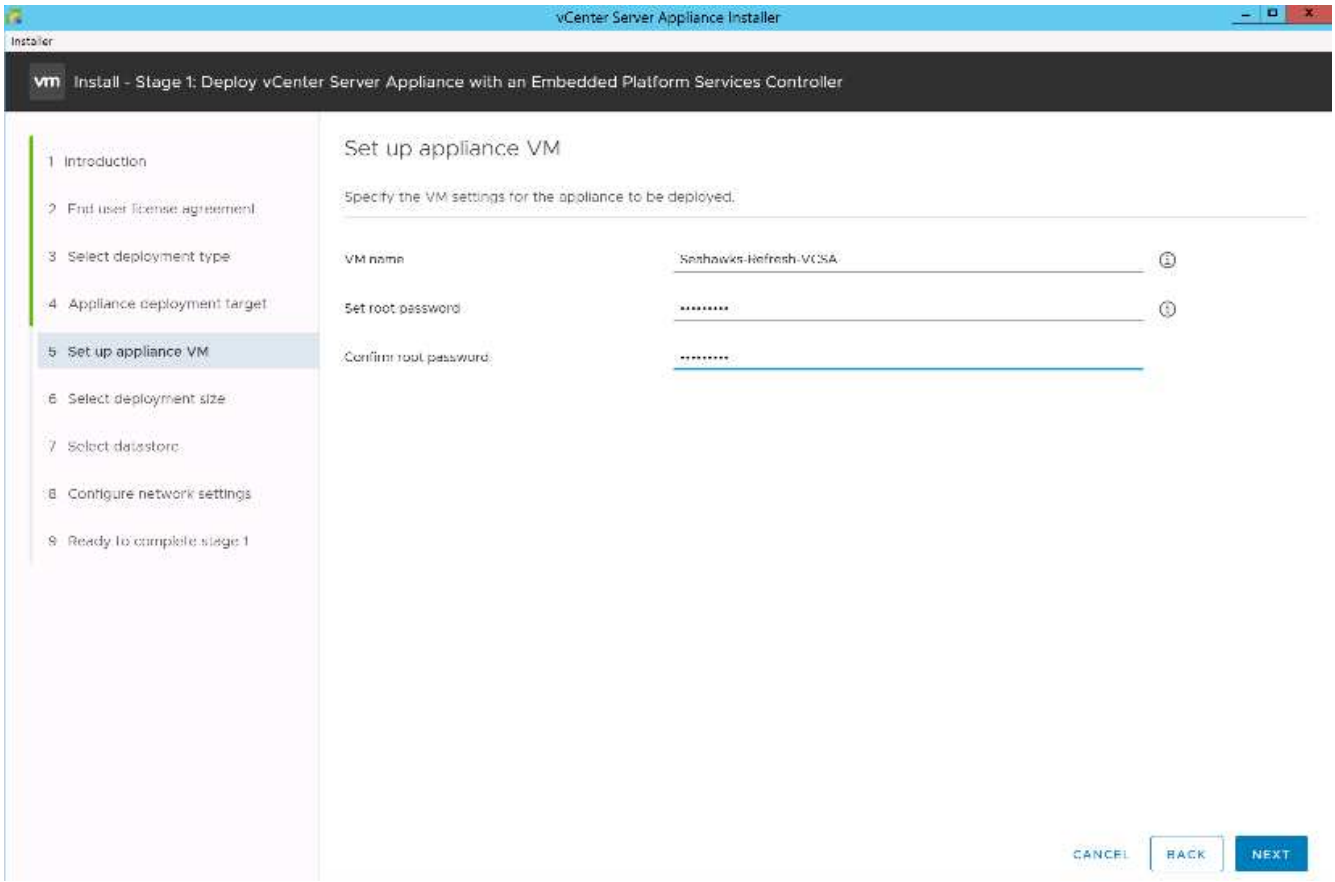


Si nécessaire, le déploiement de contrôleur de services de plateforme externe est également pris en charge dans le cadre de la solution FlexPod Express.

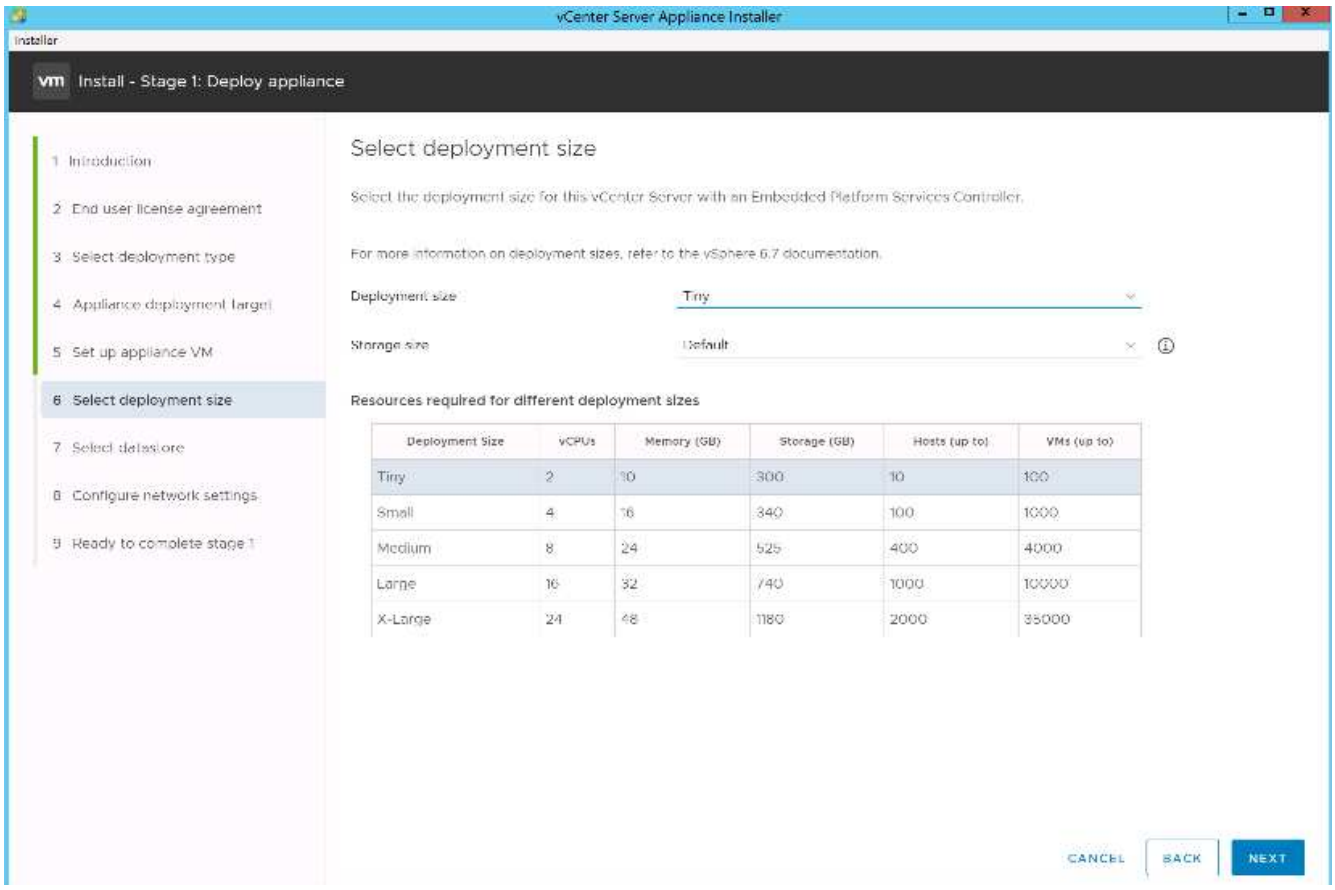
9. Sur la page cible de déploiement de l'appliance, entrez l'adresse IP d'un hôte ESXi déployé, le nom d'utilisateur root et le mot de passe root. Cliquez sur Suivant.



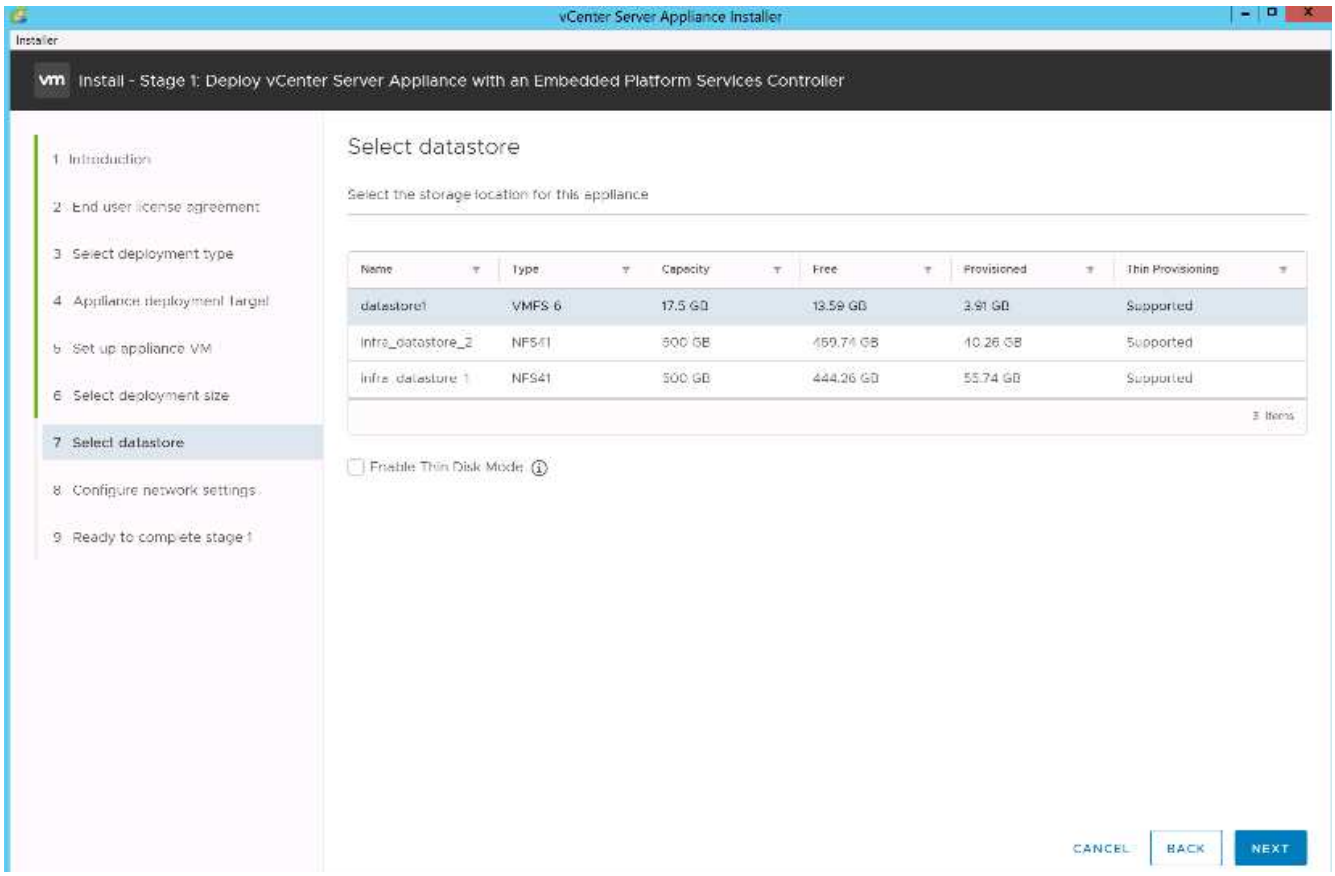
10. Définissez la machine virtuelle de l'appliance en saisissant VCSA comme nom de machine virtuelle et mot de passe root que vous souhaitez utiliser pour le VCSA. Cliquez sur Suivant.



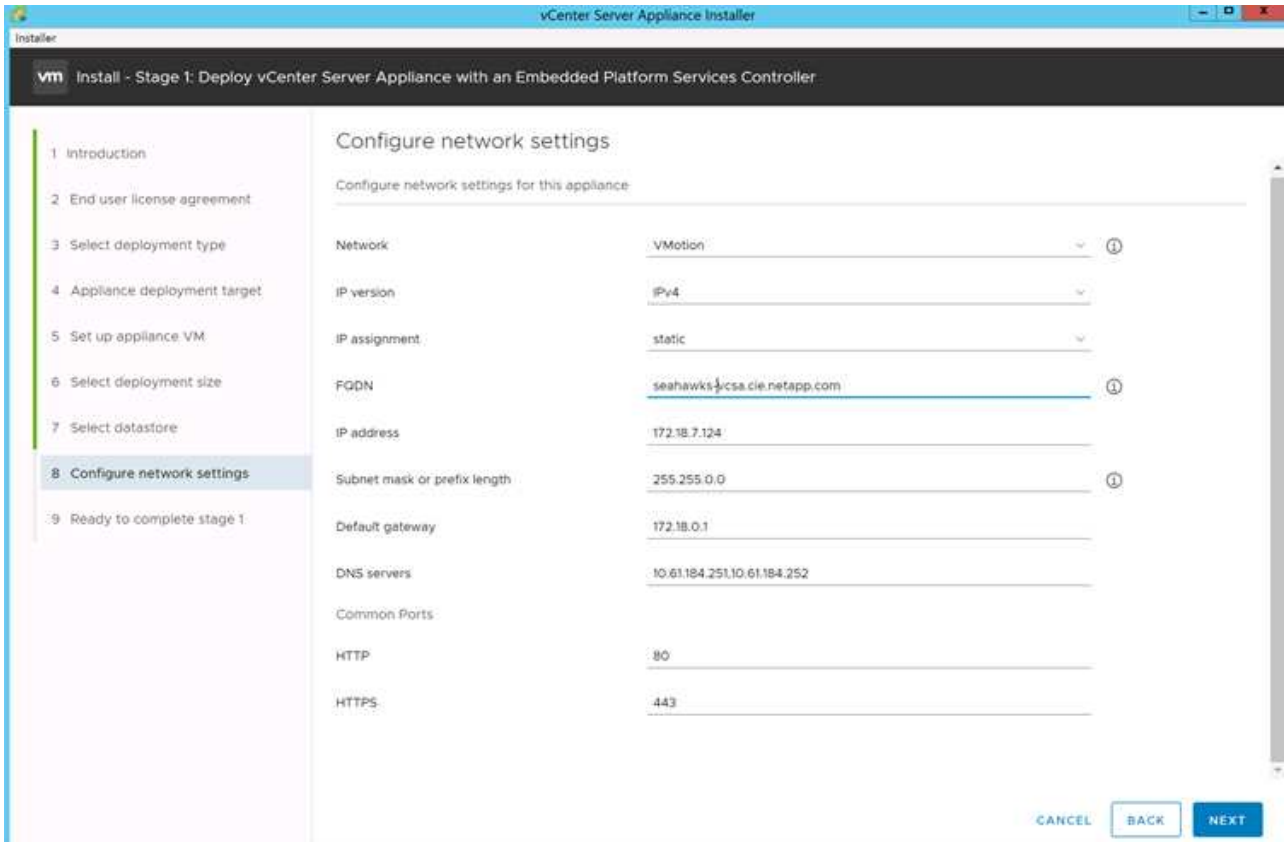
11. Choisissez la taille de déploiement qui correspond le mieux à votre environnement. Cliquez sur Suivant.



12. Sélectionner `infra_datastore_1` datastore. Cliquez sur Suivant.



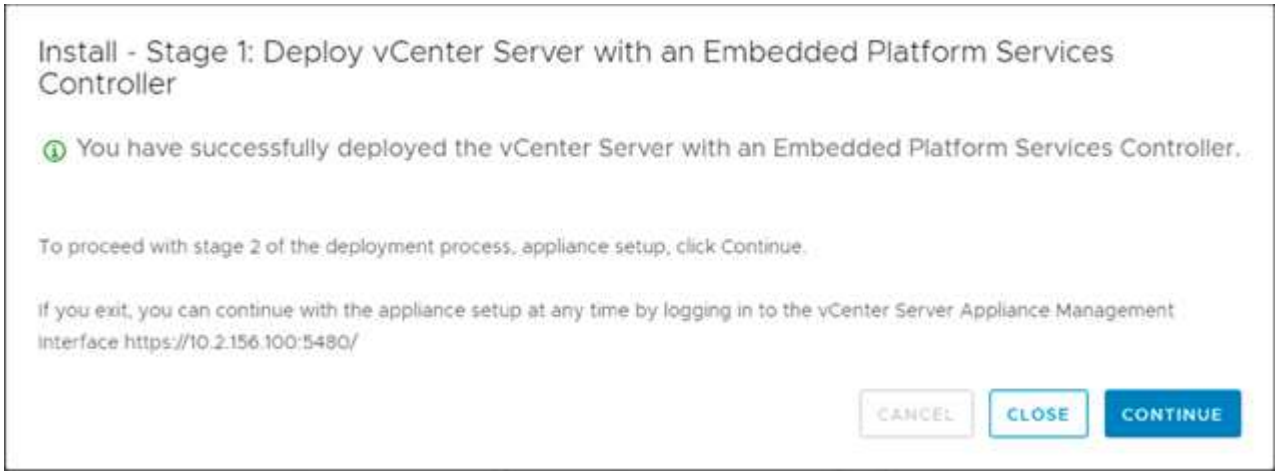
13. Entrez les informations suivantes sur la page configurer les paramètres réseau et cliquez sur Suivant.
    a. Sélectionnez MGMT-Network comme réseau.
    b. Saisissez le nom de domaine complet ou l’adresse IP à utiliser pour le VCSA.
    c. Entrez l’adresse IP à utiliser.
    d. Entrez le masque 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 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 `vsphere.local` nom de domaine.

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 pouvez 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.

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

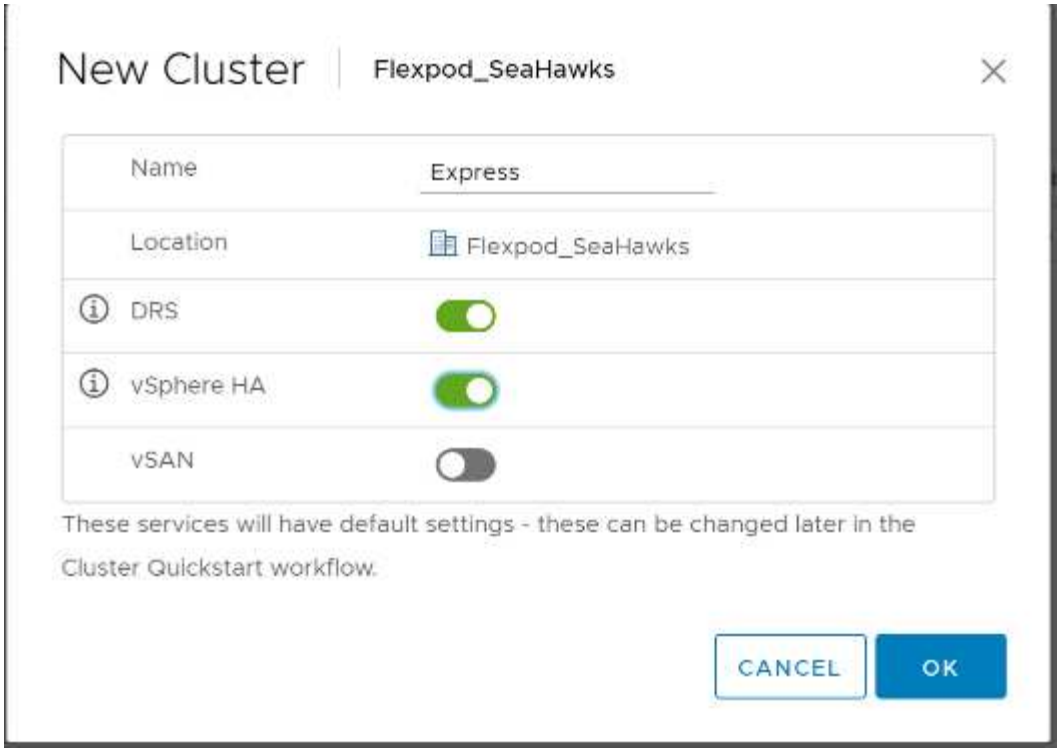
Pour configurer VMware vCenter Server 6.7 et la mise en cluster vSphere, procédez comme suit :

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 adminis@vsphere.locusmabl et du mot de passe SSO que vous avez saisi lors du 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.

Créer un cluster vSphere.

Pour créer un cluster vSphere, procédez comme suit :

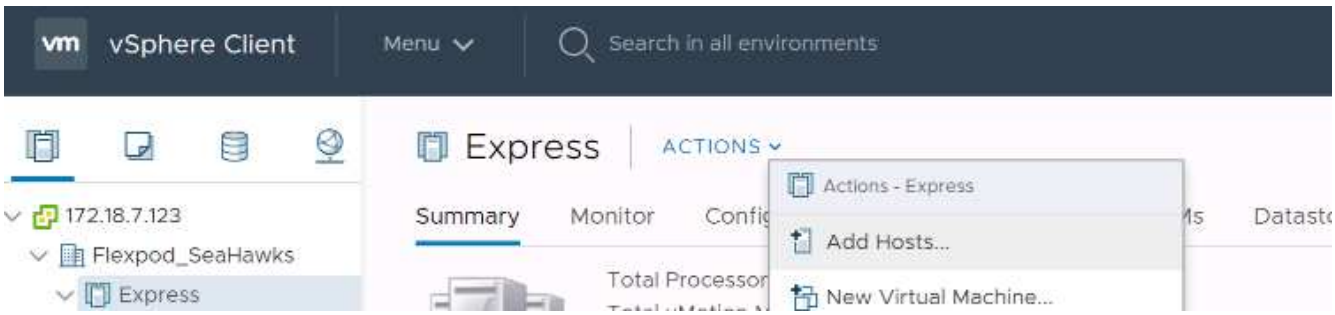
1. Cliquez avec le bouton droit de la souris sur le nouveau centre de données et sélectionnez Nouveau cluster.
2. Indiquez un nom pour le cluster.
3. Sélectionnez et activez les options HA DRS et vSphere.
4. Cliquez sur OK.



Ajouter des hôtes ESXi au cluster

Pour ajouter des hôtes ESXi au cluster, procédez comme suit :

1. Sélectionnez Ajouter hôte dans le menu actions du cluster.



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

Configuration du collecteur de vidage ESXi pour les hôtes démarrés iSCSI

Les hôtes ESXi démarrés avec iSCSI à l'aide de l'initiateur logiciel VMware iSCSI doivent être configurés pour effectuer des vidages principaux vers le collecteur de vidage ESXi intégré à vCenter. Le collecteur de vidage n'est pas activé par défaut sur l'appliance vCenter. Cette procédure doit être exécutée à la fin de la section déploiement vCenter. Pour configurer le collecteur de vidage ESXi, procédez comme suit :

1. Connectez-vous au client Web vSphere sous la forme administrator@vsphere.lockub et sélectionnez Home.
2. Dans le volet central, cliquez sur Configuration du système.
3. Dans le volet de gauche, sélectionnez Services.
4. Sous Services, cliquez sur VMware vSphere ESXi Dump Collector.
5. Dans le volet central, cliquez sur l'icône de démarrage verte pour démarrer le service.
6. Dans le menu actions, cliquez sur Modifier le type de démarrage.
7. Sélectionnez automatique.
8. Cliquez sur OK.
9. Connectez-vous à chaque hôte ESXi en utilisant ssh comme root.
10. Exécutez les commandes suivantes :

```
esxcli system coredump network set -v vmk0 -j <vcenter-ip>
esxcli system coredump network set -e true
esxcli system coredump network check
```

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

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

Conclusion

FlexPod Express propose une solution simple et efficace qui repose sur des composants leaders. Les FlexPod Express peuvent être adaptées à des besoins spécifiques en ajoutant des composants supplémentaires. Le système FlexPod Express a été conçu pour répondre aux besoins des petites et moyennes entreprises, des bureaux de mission et d'autres entreprises qui ont besoin de solutions dédiées.

Informations supplémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- NVA- 1130-DESIGN : FlexPod Express avec VMware vSphere 6.7U1 et NetApp AFF A220 avec stockage DAS basé sur IP NVA Design

  "https://www.netapp.com/us/media/nva-1130-design.pdf"

- Centre de documentation sur les systèmes AFF et FAS

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

- Centre de documentation ONTAP 9

  "http://docs.netapp.com/ontap-9/index.jsp"

- Documentation produit NetApp

  "https://docs.netapp.com"

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.